

Dltec do Brasil®

www.dltec.com.br

info@dltec.com.br | 413045.7810



DLTEC DO
BRASIL

CONECTIVIDADE IP (TÓPICO 3.0 DO CCNA 200-301)

Conectividade IP

Dltec do Brasil®

Todos os direitos reservados©

Copyright © 2020.

É expressamente proibida cópia, reprodução parcial, reprografia, fotocópia ou qualquer forma de extração de informações deste sem prévia autorização da DLteC do Brasil conforme legislação vigente.

O conteúdo dessa apostila é uma adaptação da matéria online do Curso CONECTIVIDADE IP.

Aviso Importante!

Esse material é de propriedade da DLteC do Brasil e é protegido pela lei de direitos autorais 9610/98.

Seu uso pessoal e intransferível é somente para os alunos devidamente matriculados no curso. A cópia e distribuição é expressamente proibida e seu descumprimento implica em processo cível de danos morais e material previstos na legislação contra quem copia e para quem distribui.

Para mais informação visite www.dltec.com.br

Seja muito bem-vindo(a) ao curso Curso Conectividade IP, o qual faz parte da trilha da certificação Cisco CCNA 200-301, da DlteC!

Aqui, você terá todo o background necessário para aprender sobre Conectividade IP em Redes com dispositivos Cisco e também ser aprovado(a) no exame 200-301 da Cisco ao final da trilha. O exame citado anteriormente é conhecido também como exame CCNA ou Cisco Certified Network Associate.

Os assuntos encontram-se distribuídos conforme o Blueprint do exame – sendo assim, esteja bastante atento(a) a todo o conteúdo que aqui será apresentado. Não perca de vista o peso de cada tópico – isso é importante para você ter uma noção de quanto investirá o seu tempo em cada um.

Busque praticar o máximo de exercícios possíveis e, além disso, busque compreender cada assunto de maneira objetiva. Não esqueça o propósito principal: ser aprovado(a).

A DlteC estará com você em todos os momentos dessa jornada!

Bons estudos!

Introdução

Olá!

Como parte integrante da Trilha para a Certificação **CCNA 200-301** da DlteC do Brasil, esta apostila representa uma adaptação textual do material disponibilizado online do **Curso Conectividade IP**.

O conteúdo desse curso cobre o tópico 3.0 (IP Connectivity) da certificação Cisco CCNA 200-301.

Por isso, recomendamos que você a utilize como um importante recurso offline. Combinando-a com o conteúdo online, você estará muito mais bem preparado(a) para realizar o exame **200-301 (CCNA: Cisco Certified Network Associate)**.

É de suma importância que você, além de participar dos fóruns, realize o máximo possível de exercícios e simulados (todos encontrados na trilha do 200-301 Online).

Lembre-se que o curso Fundamentos de Redes Cisco é Pré-requisito para esse curso.

Esperamos que você aproveite ao máximo este material, que foi idealizado com o intuito verdadeiro de fazê-lo(a) obter êxito no exame. Estamos torcendo pelo seu sucesso!

Bons estudos!

Conectividade IP

Peso: 25%

Objetivos

Ao final desse curso você deverá ter conhecimentos sobre:

- A tabela de roteamento IP em roteadores e switches L3 Cisco
- Significado dos seus campos e como interpretar as informações da tabela de roteamento
- Saber como os roteadores tomam suas decisões de roteamento
- Conceito de longest match, distância administrativa e métrica de protocolos de roteamento dinâmico
- Rotas estáticas IPv4 e IPv6
- Rotas default, network, host e flutuantes
- Configurações e verificações do funcionamento do protocolo OSPFv2 (IPv4)
- Conceitos como adjacências, redes ponto a ponto, broadcast, eleição de DR e BDR, assim como router-id do OSPF
- Descrever o funcionamento e o propósito dos protocolos de redundância de primeiro salto, tais como HSRP, VRRP e GLBP

Sumário

1	Introdução	7
1.1	Introdução	7
1.2	Sobre a Cisco e o CCNA - Cisco Certified Network Associate	8
1.3	Plano de Estudos para o CCNA	9
1.4	Como Estudar com o Material da DlteC	10
2	Tópicos do Curso vs Blueprint do CCNA 200-310 – Peso 20%	11
2.1	Introdução	11

3 Visão Geral do Roteamento em Dispositivos Cisco	12	5.7 Rotas Estáticas de Host ou Host-Route	51
3.1 Introdução	12	5.8 Bônus: Roteamento em Clientes de Rede	52
3.2 Processo de Encaminhamento de Pacotes	13	5.8.1 Problemas Comuns de Alcançabilidade em Clientes	53
3.2.1 Process Switching	13	6 Roteamento Estático com IPv6	54
3.2.2 Fast Switching e CEF	15	6.1 Introdução	54
3.2.3 Questões sobre Processo de Roteamento e Desempenho	16	6.2 O Comando "ipv6 route"	54
3.3 Tabela de Roteamento IPv4	18	6.3 Criando Network Routes	55
3.4 Tabela de Roteamento IPv6	21	6.4 Criando Rotas Padrões	57
3.5 Interfaces Diretamente Conectadas	22	6.4.1 Rota Padrão via SLAAC e Autoconfiguração	58
3.5.1 Verificando as Interfaces Diretamente Conectadas	23	6.5 Criando Rotas Estáticas Flutuantes no IPv6	60
3.6 Roteamento entre VLANs	25	6.6 Criando Rota de Host no IPv6	61
3.6.1 Roteamento entre VLANs com Roteadores	26	7 Conceitos de Roteamento Dinâmico	63
3.6.2 Roteamento entre VLANs com Switches Camada 3	28	7.1 Introdução	63
4 Como o Roteador Escolhe a Melhor Rota	31	7.2 Protocolo de Roteamento versus Protocolo Roteado	64
4.1 Introdução	31	7.3 Funções de um Protocolo de Roteamento Dinâmico	64
4.2 Distância Administrativa	32	7.4 IGP versus EGP	67
4.3 Métrica dos Protocolos de Roteamento	34	7.5 Algoritmos dos Protocolos de Roteamento Dinâmicos	68
4.4 Balanceamento de Cargas	36	7.6 Características Comuns dos IGPs	69
4.5 Regra do "Longest Match"	38	7.7 Funcionamento Básico de um Protocolo Distance Vector	70
4.6 Resumindo a Escolha da Melhor Rota	39	7.8 Funcionamento Básico dos Protocolos Link State	72
5 Configurando e Verificando Rotas Estáticas IPv4	40	7.9 Protocolo Advanced Distance Vector	74
5.1 Introdução	40	7.10 Path Vector: BGP	76
5.2 Opções do Comando IP-Route	41	8 Visão Geral do OSPFv2 e Configurações do OSPF Single Area	79
5.3 Network Routes ou Rotas Estáticas para Redes Remotas	41	8.1 Introdução	79
5.4 O que é Melhor Interface ou IP na Rota Estática?	47	8.2 Características do OSPFv2	79
5.5 Configurando uma Rota Padrão (Default-Gateway)	48	8.3 Nomenclatura do OSPF – Tipos de Redes, Áreas e Roteadores	81
5.6 Rota Estática Flutuante (Floating Static)	49	8.4 Operação do OSPF	83
		8.4.1 Tipos de Mensagens do OSPF	83

8.4.2	Estabelecimento de Vizinhanças e Troca de Banco de Dados	84
8.4.3	Principais Tipos de LSAs	88
8.4.4	Alteração na Topologia e Atualizações Periódicas	90
8.4.5	Tipos de Redes Suportadas pelo OSPF	91
8.4.6	Escolha do melhor caminho pelo OSPF	92
8.4.7	Timers de Hello e Dead	95
8.4.8	Parâmetro Router ID	97
8.5	Configuração do OSPF Single Area Com Comando Network	98
8.5.1	Dicas sobre o Comando Network e Wildcard Mask	100
8.5.2	Verificando as Configurações do OSPF	101
8.6	Configurando OSPFv2 via Interface	106
8.7	Detalhando a Eleição do DR e BDR em Redes Broadcast	108
8.7.1	Exemplo de Eleição de DR e BDR	109
8.8	Anunciando a Rota Padrão pelo OSPF	112
8.9	Balanceamento de Cargas no OSPF	113
8.10	Resumo dos Comandos Show para OSPF	115
8.11	Resumo dos Comandos de Configuração Utilizados no OSPF	116
9	First Hop Redundancy Protocols (FHRP)	117
9.1	Introdução	117
9.2	Entendendo Funcionamento do HSRP	119
9.2.1	Entendendo o Failover com HSRP	121
9.2.2	Balanceando Cargas com HSRP	122
9.3	Entendendo Funcionamento do VRRP	123
9.4	Entendendo Funcionamento do GLBP	124
9.5	Ativando e Verificando o HSRP Básico	125
9.5.1	Preemption	128
9.5.2	Problemas mais comuns ao Configurar o HSRP	128

1 Introdução

1.1 Introdução

Bem-vindo ao **Curso Conectividade IP**, o qual também faz parte do conteúdo preparatório para a prova de certificação **CCNA 200-301**.

O curso **Conectividade IP** possui como objetivo fornecer ao aluno uma visão abrangente sobre o funcionamento do roteamento de forma geral, tanto IPv4 como IPv6, assim como as configurações do roteamento estático e OSPF.

Ao final do curso, você deverá ser capaz de:

- Interpretar a tabela de roteamento IP em roteadores e switches L3 Cisco.
- Saber o significado dos seus campos e como interpretar as informações da tabela de roteamento.
- Saber como os roteadores tomam suas decisões de roteamento.
- Entender o conceito de longest match, distância administrativa e métrica de protocolos de roteamento dinâmico.
- Configurar rotas estáticas IPv4 e IPv6.
 - Rotas default, network, host e flutuantes.
- Configurações e verificações do funcionamento do protocolo OSPFv2 (IPv4).
- Compreender os conceitos como adjacências, redes ponto a ponto, broadcast, eleição de DR e BDR, assim como router-id do OSPF.
- Descrever o funcionamento e o propósito dos protocolos de redundância de primeiro salto, tais como HSRP, VRRP e GLBP.

Mesmo que você não esteja trilhando os estudos para a certificação CCNA 200-301 você pode sim fazer esse curso para aumentar seus conhecimentos no mundo de Redes e mais especificamente sobre o processo de roteamento e conectividade IP utilizando equipamentos do fabricante Cisco.

Mas se você está na trilha da certificação, saiba que esse curso aborda o **Tópico 3.0 ou "IP Connectivity"**, o qual corresponde a **25% das questões do exame CCNA 200-301**.

Como a nova prova terá aproximadamente entre 100 e 120 questões, podemos dizer que **devem cair de 25 a 30 questões** relacionadas ao conteúdo desse curso, dependendo da quantidade total de questões que forem sorteadas para seu exame específico.

Não esqueça que ao final do curso você poderá emitir o seu certificado!

1.2 Sobre a Cisco e o CCNA - Cisco Certified Network Associate

A Cisco é uma empresa líder mundial em TI e redes, tendo seus produtos e tecnologias utilizadas por diversas empresas dos mais variados segmentos de mercado no mundo todo.

Fundada em 1984 por Len Bosack e Sandy Lerner atua até os dias de hoje com tecnologia de ponta e inovações que auxiliam no crescimento do mercado de TI.

A Cisco atua na área de Redes (com os famosos Roteadores e Switches), Software, Internet das Coisas, Mobilidade e Comunicação sem fio, Segurança, Colaboração (Voz e Vídeo sobre IP), Data Center, Cloud, Pequenos e Médios Negócios e Provedores de Serviço.

Para garantir que os profissionais que atuam com seus produtos e tecnologias realmente tem os conhecimentos técnicos necessários para desempenhar um bom trabalho, a Cisco desenvolveu um programa de **Certificação** com **Três Níveis** no início:

- **Associate ou CCNA (Cisco Certified Network Associate)**
- Professional ou CCNP (Cisco Certified Network Professional)
- Expert ou CCIE (Cisco Certified Internetwork Expert)

Mais especificamente falando da certificação **CCNA ou Cisco Certified Network Associate** é uma das primeiras certificações lançadas pela Indústria de Redes e com certeza a mais famosa até os dias de hoje.

A primeira versão de CCNA data de 1998 chamada de 640-407, o qual foi atualizado sete vezes até a última mudança feita em 2016 com a versão 200-125 (CCNA Routing and Switching em uma prova) e as versões do 100-105 e 200-105 (Modelo em duas provas: CCENT/ICND-1 + ICND-2).

Em **julho de 2019** foi anunciada uma grande mudança em maioria das certificações Cisco e o CCNA volta ao que era no início, sendo uma certificação unificada para diversas áreas e englobando não somente assuntos de Roteamento e Switching, mas também segurança, redes sem fio e automação de Redes.

Esse curso que você está prestes a iniciar faz parte da nossa trilha para a certificação **CCNA 200-301**.

O que se espera de um CCNA no mercado de trabalho?

Um profissional certificado CCNA deve conhecer uma larga gama de tecnologias e configurações de diversos equipamentos Cisco, tais como Roteadores, Switches, Access Points e Wireless LAN Controllers.

Além disso, deve estar preparado para a nova geração da Infraestrutura de TI, a qual a automação e programabilidade será cada vez mais utilizada.

Não confunda programabilidade com a necessidade de ser um programador, pois um profissional CCNA no mercado faz a operação e manutenção da Rede, não necessariamente precisará ser um programador e sim entender como utilizar algumas ferramentas e interagir com APIs.

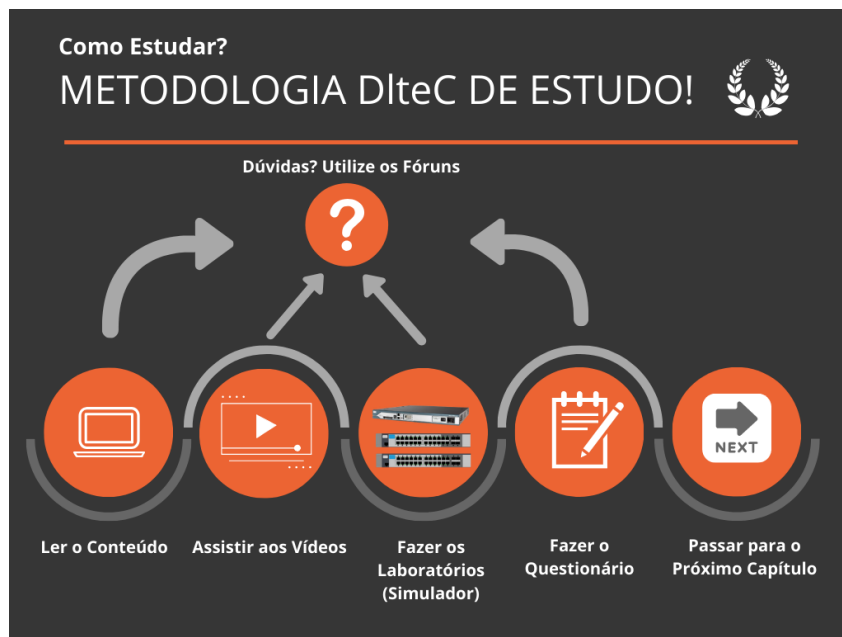
É o primeiro passo de uma carreira promissora e que tem muitas possibilidades de crescimento nas mais diversas áreas de tecnologia de rede.

A seguir vamos falar sobre como a preparação para o **CCNA** está dividida no **Portal da DlteC** e como você deverá utilizar nosso material para conquistar sua certificação.

1.3 Plano de Estudos para o CCNA

Nesse novo modelo de prova existe apenas um caminho para obtenção da certificação CCNA que é através do exame 200-301, ou seja, não existe mais opção em duas provas como na versão anterior.

O **plano de estudos** para você ter sucesso na **CCNA** é o seguinte:



1. Ativar a trilha do curso **CCNA 200-301** no Menu Cursos (somente se você ainda não ativou)
2. Estudar o conteúdo de cada Capítulo dentro da trilha (sequência de capítulos/cursos expressa a seguir)
3. Repetir os comandos e demonstrações práticas realizadas pelo Prof. Marcelo durante as vídeo aulas como laboratório
4. Fazer os simulados que estão dentro do curso "**CCNA 200-301**"
5. A qualquer momento tirar as dúvidas do conteúdo utilizando os fóruns correspondentes de cada capítulo (*)
6. Passar para o próximo capítulo
7. Realizar a prova Final para treinar e obter o certificado do curso CCNA 200-301 (média da aprovação igual ou acima a 70 pontos em um total de 100)
8. Fazer o preparatório Final com laboratórios e questionários (em inglês) específicos para a certificação
9. Agendar a prova e realizá-la

O exame CCNA 200-301 é composto por uma prova em computador que pode ter de 100 a 120 questões (depende do sorteio que é feito por candidato).

Essas questões devem ser resolvidas em 120 minutos no dia do exame.

Cada um dos capítulos do curso um **Peso** associado na prova e quanto maior o peso, maior será a quantidade de questões desse assunto no exame, sendo que seguimos as recomendações da Cisco na divisão de questões para que você treine em um ambiente o mais real possível.

Para ser aprovado(a), você deverá conseguir obter entre 800 e 850 pontos de um máximo 1000 pontos no exame.

Se você ativou esse curso com o objetivo de tirar a certificação então a partir de agora, foco total no objetivo: **OBTER A CERTIFICAÇÃO.**

Você será aprovado(a) – já coloque isso “na cabeça”.

Para isso, pratique os comandos, leia os tópicos com cautela e, de preferência, marque logo o dia do seu exame (para você já ter uma data limite).

Faça o seu cronograma, estipule as horas de estudo e, sinceramente, não tem erro.

Repita essa frase todos os dias: **Eu serei aprovado(a).**

Se você assumir esse compromisso com sinceridade e vontade de vencer, tudo **dará certo.**

Estamos ao seu lado! Bons estudos!

(*) Os fóruns do curso são exclusivos para TIRAR AS DÚVIDAS DO CURSO, caso você tenha dúvidas do dia a dia ou que não tenham correlação com o curso utilize os grupos do Facebook ou Telegram para troca de ideias.

1.4 Como Estudar com o Material da DLteC

Nesse curso você terá **vídeoaulas, material de leitura e laboratórios em simuladores** para o aprendizado do conteúdo.

Posso somente ler ou assistir aos vídeos? NÃO RECOMENDAMOS!

O ideal é você assistir aos vídeos e na sequência ler os conteúdos ou...

... se preferir leia os conteúdos e depois assistia aos vídeos, tanto faz.

POR QUE LER E ASSISTIR?

Simples, porque **um conteúdo complementa o outro.** Principalmente se você está se preparando para a prova de certificação é crucial que você tanto veja os vídeos como a matéria de leitura!

Os questionários ou simulados com questões de prova estão dentro da estrutura da trilha do CCNA 200-301.

Siga a sequência sugerida no plano de estudos e **faça os questionários apenas depois** de ter lido, assistido aos vídeos e feito os laboratórios em simulador. Assim você terá um aproveitamento muito melhor do curso.

2 Tópicos do Curso vs Blueprint do CCNA 200-310 – Peso 20%

2.1 Introdução

Na tabela abaixo seguem os itens do blueprint ou conteúdo do exame Cisco CCNA 200-301 relacionados ao conteúdo do curso. Os capítulos que não aparecem explicitamente aqui fazem parte da matéria e complementam o aprendizado. Estude TODO o conteúdo do curso.

IP Connectivity	
Conectividade IP (Roteamento IPv4 e IPv6)	Capítulos do Curso
3.1 Interpret the components of routing table	Visão Geral do Roteamento em Dispositivos Cisco
3.1.a Routing protocol code	Tabela de Roteamento IPv4 e Tabela de Roteamento IPv6
3.1.b Prefix	
3.1.c Network mask	
3.1.d Next hop	
3.1.e Administrative distance	
3.1.f Metric	
3.1.g Gateway of last resort	
3.2 Determine how a router makes a forwarding decision by default	Como o Roteador Escolhe a Melhor Rota
3.2.a Longest match	Regra do “Longest Match”
3.2.b Administrative distance	Distância Administrativa
3.2.c Routing protocol metric	Métrica dos Protocolos de Roteamento e Conceitos de Roteamento Dinâmico
3.3 Configure and verify IPv4 and IPv6 static routing	Configurando e Verificando Rotas Estáticas IPv4 e Roteamento Estático com IPv6
3.3.a Default route	
3.3.b Network route	
3.3.c Host route	
3.3.d Floating static	
3.4 Configure and verify single area OSPFv2	Visão Geral do OSPFv2 e Configurações do OSPF Single Area
3.4.a Neighbor adjacencies	
3.4.b Point-to-point	
3.4.c Broadcast (DR/BDR selection)	
3.4.d Router ID	
3.5 Describe the purpose of first hop redundancy protocol	First Hop Redundancy Protocols (FHRP)

3 Visão Geral do Roteamento em Dispositivos Cisco

3.1 Introdução



Nesse capítulo vamos estudar os princípios básicos de roteamento em roteadores e dispositivos L3 Cisco.

A principal função de um roteador é **encaminhar pacotes** através da rede e ele cumpre essa missão utilizando os **protocolos de roteamento**, os quais foram projetados para alimentar a principal tabela que um roteador mantém a "**tabela de roteamento**" ou "**routing table**".

A tabela de roteamento guarda as informações das redes que um roteador pode alcançar, caso determinada rede não seja conhecida pelo roteador, ou seja, a **rota** para aquela rede não está na tabela de roteamento, ele descartará a rota e enviará uma mensagem de "unreachable" (fora de alcance) através do protocolo ICMP para o computador que estava tentando se comunicar com a rede em questão.

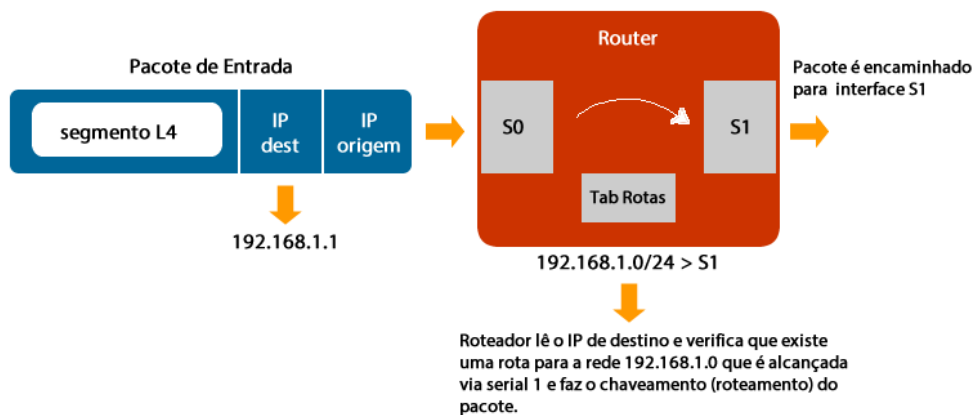
Portanto, sempre que entra um pacote IP em um roteador ele lê o **endereço de destino** contido no pacote e verifica se a rede a que esse pacote IP pertence está presente em sua tabela de roteamento. Caso não esteja, ou ele descarta o pacote ou então envia para uma rede **padrão (default gateway)**, a qual pode ser uma rota para a internet, por exemplo.

A seguir vamos estudar os processos que podem ser utilizados pelos roteadores para encaminhar os pacotes entre suas diversas interfaces.

3.2 Processo de Encaminhamento de Pacotes

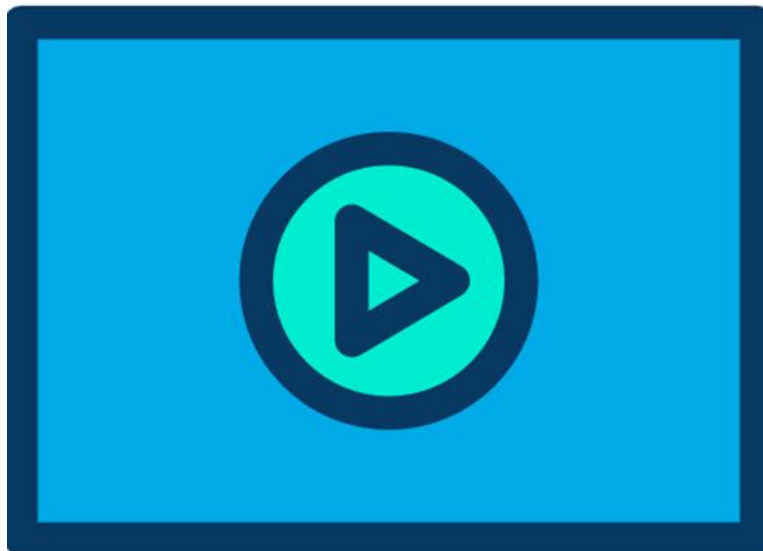
O processo de roteamento clássico é a ação do roteador receber um pacote, analisar seu endereço IP de destino, verificar em sua tabela de roteamento se existe uma rota, remontar o quadro de camada 2 e encaminhar esse pacote pela interface de saída definida nessa rota.

Veja a figura abaixo com um diagrama resumido do processo de roteamento.



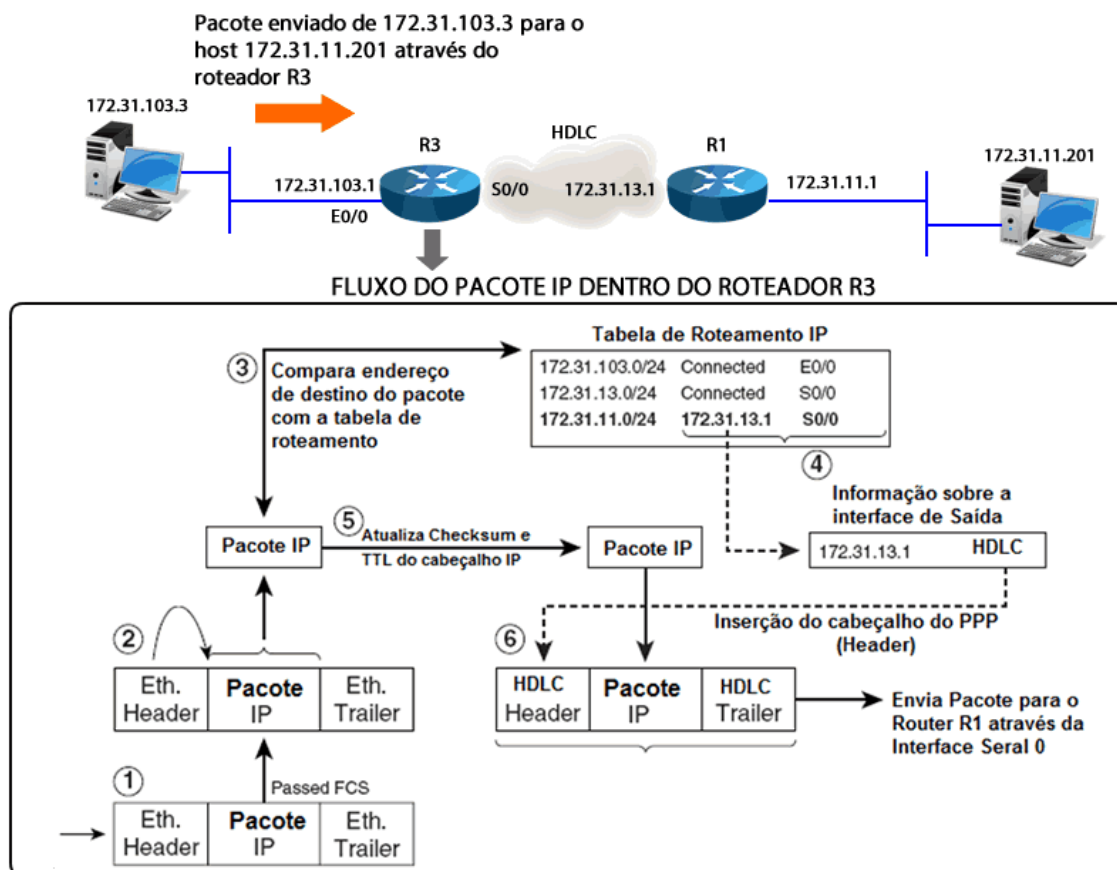
Se não houver uma rota explícita definida na tabela de roteamento, o roteador verifica se existe uma rota padrão (Gateway of last resort) e encaminha para a saída definida nessa rota ou então, se não houver a rota padrão configurada, ele simplesmente descarta o pacote e envia uma informação de destino inalcançável (destination unreachable) através do ICMP para o host de origem.

3.2.1 Process Switching



Este é o processo mais simples de roteamento chamado **Process Switching**, onde a CPU é envolvida a todo o momento para ler e decidir para que interface encaminhar o pacote IP.

Veja o fluxo detalhado do encaminhamento de um pacote utilizando o Process Switching na figura abaixo. Nesse exemplo um computador conectado à LAN do R3 envia um pacote para o host conectado à LAN do R1.



Os passos que o roteador segue para fazer o roteamento por padrão seguem a sequência conforme mostrado na figura. Veja abaixo a explicação de cada passo:

1. O quadro de camada 2 é recebido pela Interfaces Eth 0/0 do roteador e se o FCS (checksum de camada 2) estiver correto ele é processado, caso contrário ele é descartado. Vamos supor que o quadro está com o FCS correto e passa para a próxima etapa.
2. Agora o quadro de camada 2 (Ethernet) é removido e o pacote IP é enviado para a camada de rede do roteador R3.
3. O roteador R3 verifica o **IP de destino** do pacote IP e **procura pelo prefixo mais específico** na tabela de roteamento para poder encaminhar o pacote para uma interface de saída, ou seja, verifica a melhor rota para encaminhar o pacote sempre pela máscara de sub-rede ou prefixo **mais longo** (longest match - quanto mais bits "1" na máscara melhor o caminho). O pacote então é encaminhado para a interface de saída. Como o IP de destino é o 172.31.11.201 o roteador verifica que há uma rota de saída através da sua serial 0 que está diretamente conectada ao IP 172.31.13.1 do seu roteador vizinho.
4. Como foi encontrada uma saída viável para o pacote IP um novo quadro de camada 2 precisa ser remontado conforme o tipo de interface de saída (nesse caso utilizando o encapsulamento conforme protocolo HDLC). Nessa etapa o roteador verifica e prepara as informações de camada 2 para a etapa final de encapsulamento e envio pela camada física.
5. O pacote IP é atualizado com o incremento do campo de TTL e tem seu checksum recalculado, pois o TTL foi alterado.

6. O pacote IP é encapsulado dentro do novo quadro de camada 2 (nesse caso um quadro HDLC) e encaminhado para a camada física através da interface serial 0.

O item 6 é conhecido também como "frame rewrite", ou seja, quando o roteador reescreve o quadro de camada-2 com as novas informações conforme o link de próximo salto do pacote IP.

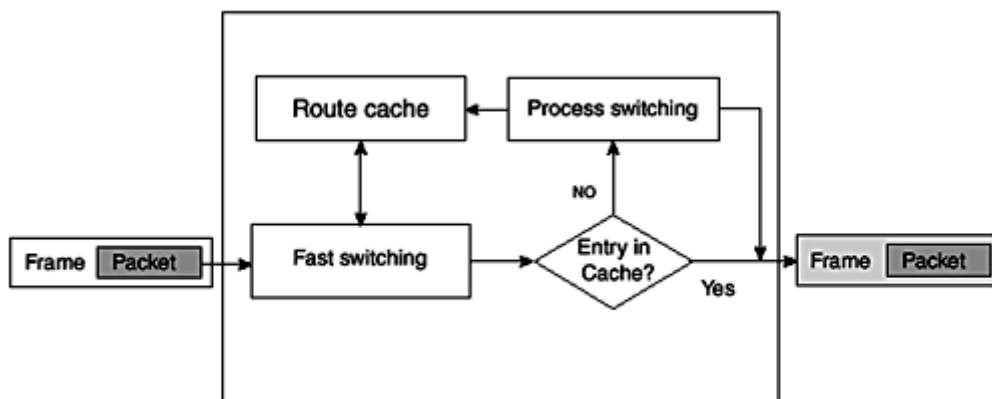
Uma vez recebida a informação pelo roteador R1 ele seguirá o mesmo processo para encaminhar o pacote recebido na interface serial para sua LAN, para que assim o host de destino seja alcançado.

3.2.2 Fast Switching e CEF

Além do processo mostrado anteriormente, existem outros dois processos mais rápidos e econômicos em termos de utilização da CPU que podem ser utilizados pelos roteadores Cisco:

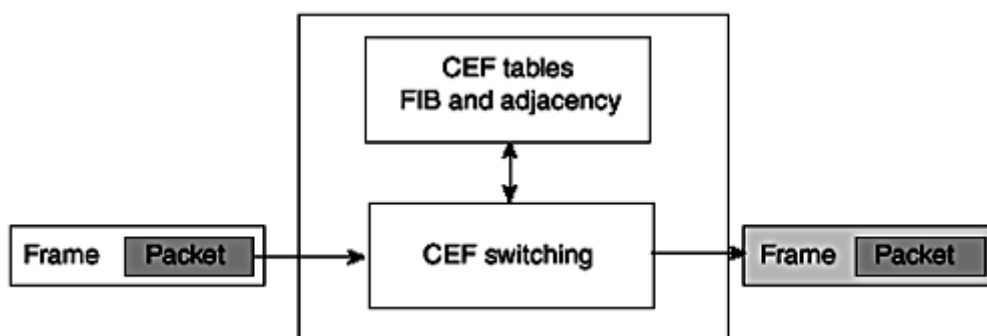
- **Fast Switching**
- **CEF (Cisco Express Forwarding)**

O **Fast Switching** foi criado para agilizar o processo de verificação do melhor caminho e encaminhamento para a interface de saída quando temos fluxos repetidos de pacotes, pois quando temos pacotes de uma mesma origem e mesmo destino a consulta feita é igual e repetida.



Portanto, o primeiro pacote aciona a criação de uma entrada no **Fast-switching cache** (router cache) que agiliza o processo de encaminhamento, porém continua utilizando a CPU para essas verificações.

Já quando utilizamos o **CEF (Cisco Express Forwarding)** o roteador cria o **Forwarding Information Base (FIB)**, a qual é uma base de dados que contém TODAS as rotas conhecidas. Esse é o padrão em maioria dos roteadores e switches L3.



Esta tabela ou banco de dados contém tudo o que o roteador precisa saber para encaminhar um pacote e agiliza muito o processo de roteamento.

Se formos fazer uma comparação bem simplificada é como se o roteador utilizando o **Process Switching** tivesse que calcular manualmente tudo o que ele precisa para fazer o encaminhamento dos pacotes, isso tudo para cada pacote recebido, ou seja, um a um.

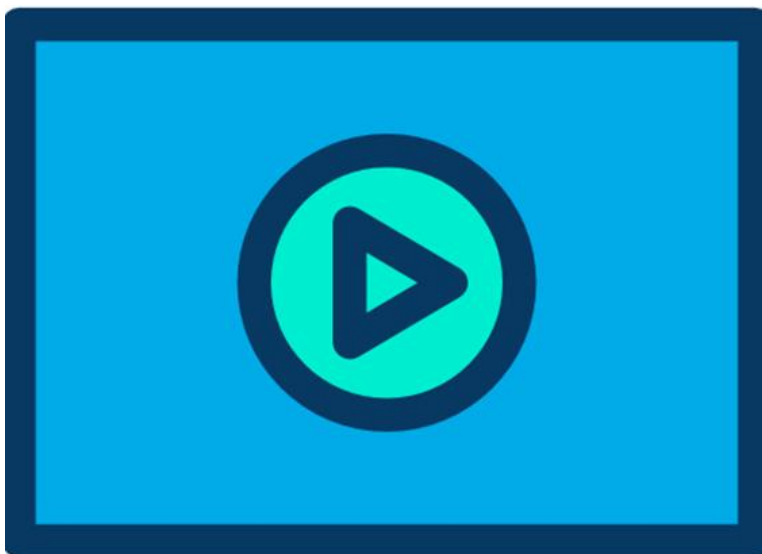
Já com o **Fast Switching** ele utiliza uma memória de cálculo, onde ele faz a conta uma vez quando recebe o primeiro pacote e depois lembra as respostas para os próximos pacotes que vêm na sequência (cache).

Por último, quando o roteador utiliza o **CEF** para encaminhar os pacotes é como se ele tivesse uma planilha do Excel e quando os números são inseridos nas células essa planilha já dá o resultado calculado, acelerando o processo como um todo.

Portanto tanto o CEF quanto o Fast Switching visam economizar tempo e processamento nas etapas 3 e 4 do processo de roteamento, ou seja, na pesquisa da melhor rota na tabela de roteamento e no levantamento dos dados para montagem do quadro de camada 2.

Lembrete importante: Seja qual for o processo utilizado sempre a escolha da melhor rota é feita através do prefixo mais longo ou longest match.

3.2.3 Questões sobre Processo de Roteamento e Desempenho



Nesse ponto você já deve ter notado que o processo de roteamento não é tão simples, não é só encaminhar um pacote pura e simplesmente.

Note que o roteador precisa fazer alguns processos que consomem memória RAM, por exemplo, armazenar os pacotes recebidos para serem processados, e também processador (CPU), por exemplo, ler o endereço de destino de cada pacote para saber qual interface de saída deve encaminhá-lo se estiver utilizando Process Switching.

Ao receber um quadro de camada 2 o roteador deve ler o endereço MAC e decidir se deve processar e encaminhar aquele pacote, para isso ele deve verificar se seu endereço MAC está contido no campo de endereço de destino do quadro.

Se estiver, antes de processar o conteúdo dos dados que geralmente é um pacote IP, o roteador deve ler o campo FCS e verificar se o quadro está íntegro, pois se houver erros esse quadro deve ser descartado.

Um detalhe, se o MAC de destino for um broadcast o roteador também será obrigado a processar o pacote IP.

Após essa fase, supondo que o quadro tinha o MAC de destino igual ao do roteador e estava íntegro o roteador deve descartar o cabeçalho de camada 2 e gravar esse pacote em um espaço de memória RAM chamado buffer ou fila de entrada para ser processado.

Ao processar o pacote IP o roteador deve verificar o checksum, que é similar ao FCS e verificar se o pacote está íntegro.

Caso contenha erros o pacote será descartado, senão será processado. O processamento se dá com a leitura do endereço de destino do pacote IP.

Se o IP de destino for igual ao configurado em uma das interfaces do roteador ele enviará para as camadas superiores para que a informação seja tratada.

Agora, se o endereço for diferente o roteador terá que analisar a tabela de roteamento, usando a regra do **"longest match"** e escolher uma interface de saída para fazer o encaminhamento.

Uma vez definida a interface de saída o roteador precisará inserir o pacote IP em um novo quadro de camada 2, conforme protocolo configurado na interface de saída, por exemplo, um quadro HDLC se for uma interface serial.

Caso a interface de saída seja padrão ethernet, por exemplo, uma interface Gigabit via fibra óptica, antes de montar e enviar o quadro o roteador precisará fazer uma solicitação ARP pelo MAC do roteador remoto, chamado se "next hop" ou "próximo salto", para aí sim montar o quadro de camada 2 e encaminhar o pacote.

Se formos resumir todo esse trabalho em passos temos:

- Passo 1: roteador recebe quadro de camada 2 através de uma de suas interfaces.
- Passo 2: toma decisão sobre processar ou não o quadro de entrada recebido por uma das interfaces.
- Passo 3: desencapsula o pacote IP (remover o cabeçalho de camada 2).
- Passo 4: escolhe para onde encaminhar o pacote (interface de saída).
- Passo 5: faz o frame rewrite, encapsulando o pacote conforme quadro de camada 2 da interface de saída.
- Passo 6: transmite o quadro no meio físico (envio dos bits).

Todo esse processamento consome tempo de uso do processador dos roteadores (ciclos de CPU) e podem congestionar o dispositivo elevando o uso da CPU de tal maneira que o roteador pode ficar lento ou até mesmo parar de funcionar.

Por esse motivo se você procurar especificações de capacidade de roteadores normalmente ela virá expressa em **pacotes por segundo (PPS – Packet per Second)** e não em bits por segundo (bps).

Devido a esses problemas potenciais os roteadores Cisco podem ser configurados com diferentes metodologias de encaminhamento, conforme estudamos anteriormente, tais como o CEF e Fast Switching, pois essas tecnologias visam minimizar o impacto do roteamento sobre a CPU dos roteadores.

Se colocarmos em ordem de desempenho o CEF vem em primeiro lugar, depois o Fast Switching e por último o process switching, porém a escolha de qual usar depende de vários fatores que não serão tratados nesse curso devido a sua complexidade.

O comando "**show processes**" ou "**show processes cpu**" você pode verificar quando de CPU está sendo utilizado pelo roteador em porcentagem. O normal é esse índice de utilização estar entre 20% e 25% ou abaixo. Veja exemplo abaixo.

```
R1#show processes
```

```
CPU utilization for five seconds: 1%/100%; one minute: 0%; five minutes: 0%
```

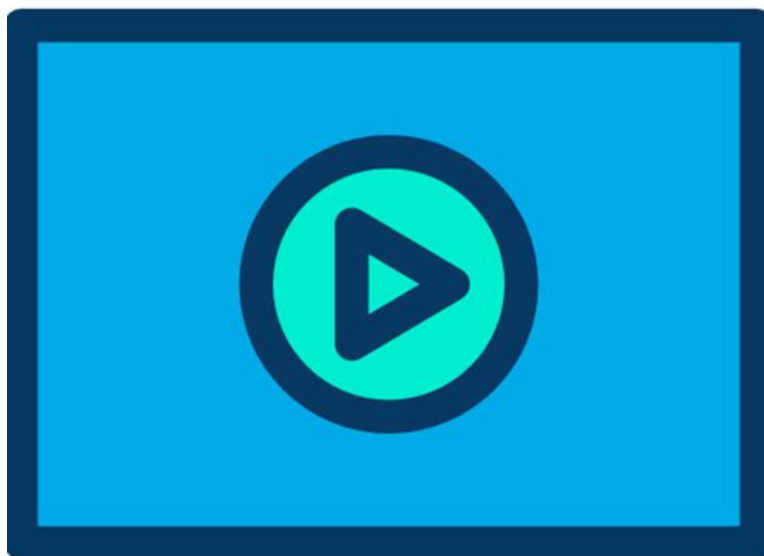
PID	QTy	PC	Runtime (ms)	Invoked	uSecs	Stacks	TTY	Process
1	Cwe	6381F45C	12	42	285	3968/6000	0	Chunk Manager
2	Csp	60610EFC	404	1584	255	2432/3000	0	Load Meter

```
### Saídas Omitidas ###
```

Além da sobrecarga de recebimento de pacotes e forma de processamento outros motivos podem fazer o uso da CPU aumentar, como o já citado comando "debug".

Você pode também verificar o histórico com o comando "**show processes cpu history**".

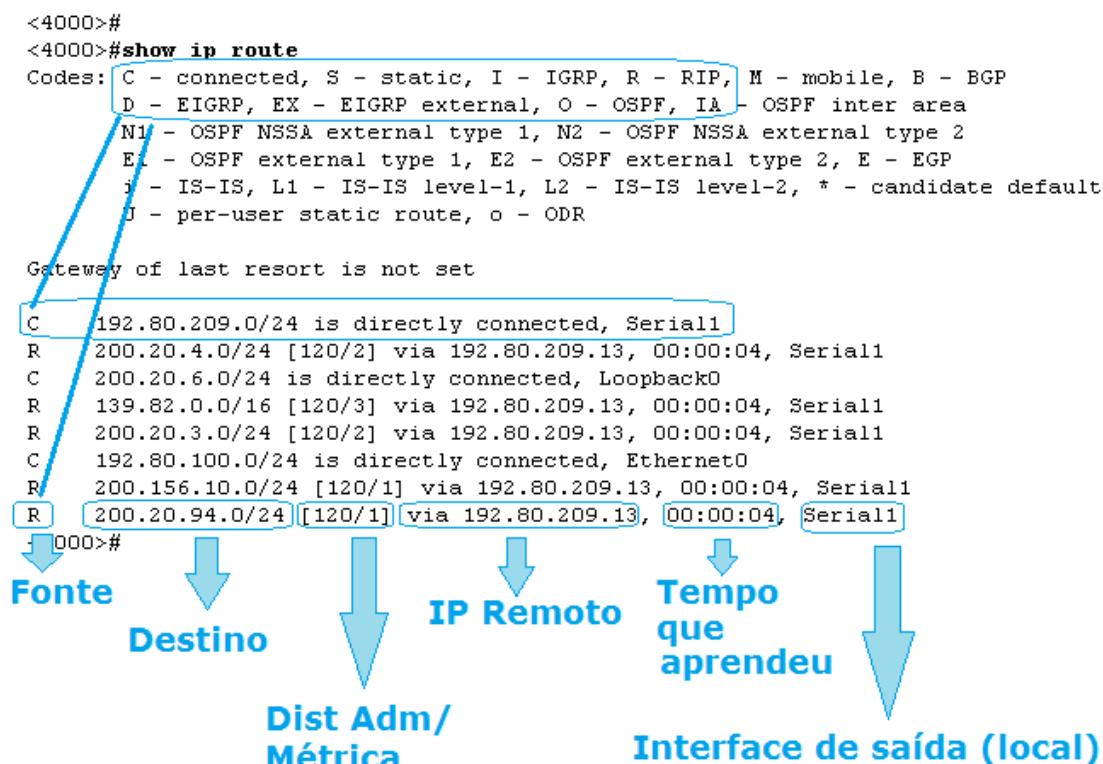
3.3 Tabela de Roteamento IPv4



Como estudamos anteriormente, o processo de roteamento, seja ele estático ou dinâmico, tem a finalidade de instalar uma "rota" para um determinado "destino" na "tabela de roteamento IP" do roteador.

Antes de continuarmos a estudar como inserir rotas vamos fazer um estudo do que a tabela de roteamento nos fornece de informações, pois saber interpretar essa tabela é fundamental para sua vida prática e para o exame.

Veja a figura abaixo com a saída do comando “**show ip route**”.



Note que logo após o comando temos uma legenda (**Routing protocol code**) com o tipo a fonte de aprendizado daquela rota, veja os principais abaixo:

- **C**: diretamente conectada (uma rede IP configurada em uma interface que está UP/UP).
- **L**: rota local.
- **S**: rota inserida manualmente ou estática.
- **R**: rota aprendida pelo RIP.
- **D**: rota aprendida pelo EIGRP.
- **O**: rota aprendida pelo OSPF.
- **B**: rota aprendida pelo BGP.

Em versões de Cisco IOS 15 ou acima existe mais um tipo de rota que é criada quando configuramos uma interface diretamente conectada que é a rota Local (L).

Essa rota traz o endereço IP da interface configurada com uma máscara /32 (rota de host).

Logo abaixo temos a frase “**Gateway of last resort is not set**”, a qual significa que não existe **rota padrão** (gateway) configurada.

Nesse caso se chegar um pacote com um destino que **não esteja especificado** na tabela, esse **pacote será descartado** ou “dropado”.

Quando temos uma rota padrão especificada nesse campo é especificado o IP do gateway.

Logo abaixo do gateway padrão temos as rotas, sendo que na primeira linha temos uma rota para uma rede diretamente conectada, nesse caso o roteador avisa com a frase “**is directly connected**” e depois da vírgula indica qual interface ela está conectada.

Quando vemos esse tipo de rota quer dizer que aquela interface, nesse exemplo a serial1, tem um IP da rede 192.80.209.0 configurado nela e a interface está UP/UP.

Para ver o IP que está configurado nela podemos utilizar o **"show ip interface brief"**.

Agora vamos para a última linha do comando que está em destaque, onde o roteador mostra uma rota aprendida pelo RIP.

Note que quando a saída da tabela de roteamento é referente a um protocolo de roteamento dinâmico muitas outras informações são mostradas. Temos os seguintes parâmetros:

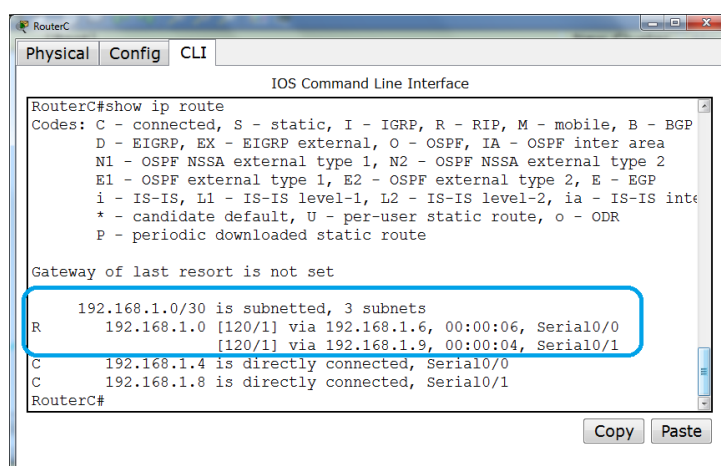
- **200.20.94.0 /24**: rede de destino ou prefixo (**Prefix**) e a máscara de rede (comprimento do prefixo ou **Network mask**).
- **[120/1]**: 120 é a distância administrativa (**Administrative Distance**) e 1 é a métrica (**Metric**) (*estudaremos mais tarde o que significam esses parâmetros*).
- **Via 192.80.209.13**: é o IP do próximo salto (**Next Hop**), ou seja, o IP do vizinho por onde o roteador enviará os pacotes destinados à rede 200.20.94.0/24.
- **00:00:04**: tempo em que essa rota foi aprendida, nesse exemplo a quatro segundos.
- **Serial 1**: a interface local que será utilizada para encaminhar os pacotes à rede 200.20.94.0/24. Com esse parâmetro e o **"via 192.80.209.13"** sabemos que a interface serial 1 do roteador local, o qual você executou o show ip route, está conectado com um roteador com IP 192.80.209.13.

Além disso, em algumas situações quando temos sub-redes você pode ter rotas **primárias e secundárias**.

As rotas primárias indicam somente que uma rede class A, B ou C foi **"subnetada"** (**subnetted** ou quebrada em sub-redes), não sendo utilizada para encaminhar rotas.

Somente as rotas com uma letra na frente são utilizadas para encaminhamento.

Veja o exemplo na figura abaixo e perceba que acima da rota com o **R** indicando que ela foi aprendida pelo RIP temos a frase **"192.168.1.0/30 is subnetted, 3 subnets"**, a qual é somente uma indicação que esta rede foi dividida em sub-redes e temos 3 sub-redes, a 192.168.1.0, 192.168.1.4 e 192.168.1.8.



```
RouterC#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

 192.168.1.0/30 is subnetted, 3 subnets
 R    192.168.1.0 [120/1] via 192.168.1.6, 00:00:06, Serial0/0
      [120/1] via 192.168.1.9, 00:00:04, Serial0/1
 C    192.168.1.4 is directly connected, Serial0/0
 C    192.168.1.8 is directly connected, Serial0/1
RouterC#
```

3.4 Tabela de Roteamento IPv6

Para verificar essas informações podemos utilizar o comando "**show ipv6 route**", lembrando que para o IPv4 é "**show ip route**".

A interpretação da tabela de roteamento IPv4 e IPv6 é basicamente a mesma, pois temos os seguintes campos informativos:

- **Routing protocol code:** códigos das fontes de roteamento ou codes na tabela.
- **Prefix:** prefixo da rede.
- **Network mask:** no IPv6 é o comprimento do prefix, pois não existe mais o conceito máscara de sub-rede.
- **Next hop:** IPv6 do próximo salto.
- **Administrative distance:** distância administrativa (mesmo valores do IPv4 e quanto menor melhor).
- **Metric:** métrica dos protocolos de roteamento (quanto menor melhor).
- **Gateway of last resort:** gateway padrão será exibido com um asterisco (*) na tabela de roteamento.

Veja exemplo da tabela de roteamento IPv6 abaixo.

```
R1#show ipv6 route
IPv6 Routing Table - 6 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
        U - Per-user Static route, M - MIPv6
        I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
        O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
        ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
        D - EIGRP, EX - EIGRP external
C  2340:1111:AAAA:1::/64 [0/0]
via ::, FastEthernet0/0
L  2340:1111:AAAA:1::1/128 [0/0]
   via ::, FastEthernet0/0
C  2340:1111:AAAA:2::/64 [0/0]
   via ::, Serial0/0
L  2340:1111:AAAA:2::1/128 [0/0]
   via ::, Serial0/0
L  FF00::/8 [0/0]
   via ::, Null0
```

Note na primeira linha em destaque temos a rede diretamente conectada à fast 0/0 2340:1111:AAAA:1::/64 (identificada com "C") e logo abaixo temos uma rota local para o endereço IP configurado nessa interface 2340:1111:AAAA:1::1/128 indicada com um "L" de Local na frente.

Após a rota, entre colchetes, temos as informações de distância administrativa e métrica, basicamente as mesmas informações que utilizamos no IPv4 para classificar as rotas entre diferentes protocolos de roteamento (distância administrativa) ou entre um mesmo protocolo (métrica).

Para as rotas diretamente conectadas ambos os valores são zero e as regras são as mesmas que estudamos no IPv4.

Por exemplo, rotas estáticas tem distância administrativa "1".

Quanto menor a distância administrativa e a métrica melhor é a rota, mesma regra de desempate que utilizarmos para o IPv4 devemos utilizar para o.

Você pode utilizar os comandos "**show ipv6 route connected**" e "**show ipv6 route local**" para verificar somente as rotas conectadas e locais respectivamente, veja exemplo abaixo.

```
R1#show ipv6 route connected
```

```
IPv6 Routing Table - 6 entries
```

```
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
```

```
U - Per-user Static route, M - MIPv6
```

```
I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
```

```
O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
```

```
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
```

```
D - EIGRP, EX - EIGRP external
```

```
C 2340:1111:AAAA:1::/64 [0/0]
```

```
via ::, FastEthernet0/0
```

```
C 2340:1111:AAAA:2::/64 [0/0]
```

```
via ::, Serial0/0
```

```
R1#show ipv6 route local
```

```
IPv6 Routing Table - 6 entries
```

```
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
```

```
U - Per-user Static route, M - MIPv6
```

```
I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
```

```
O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
```

```
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
```

```
D - EIGRP, EX - EIGRP external
```

```
L 2340:1111:AAAA:1::1/128 [0/0]
```

```
via ::, FastEthernet0/0
```

```
L 2340:1111:AAAA:2::1/128 [0/0]
```

```
via ::, Serial0/0
```

```
L FF00::/8 [0/0]
```

```
via ::, Null0
```

```
R1#
```

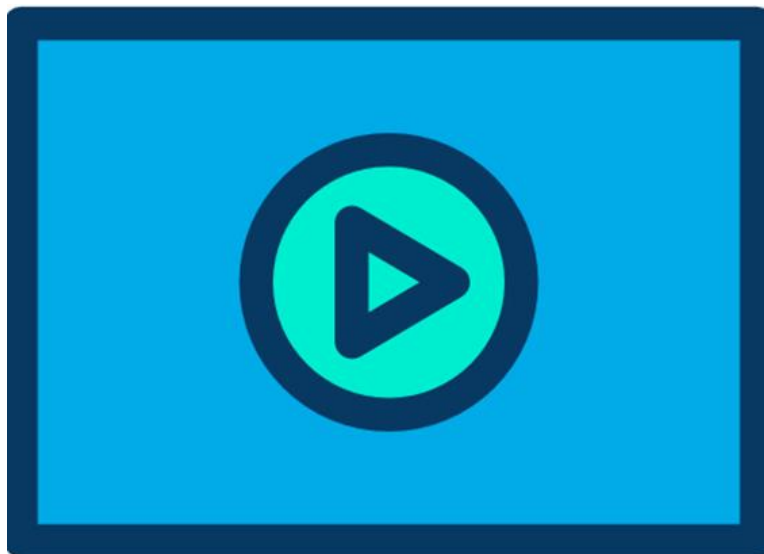
3.5 Interfaces Diretamente Conectadas

Como já estudamos no curso Fundamentos de Redes Cisco, as **Redes Diretamente Conectadas** ou "**Directly Connected**" (indicadas com um "**C**" na tabela de roteamento) pertencem às Interfaces do roteador, ou seja, são as redes IP que foram configuradas nas interfaces de LAN e WAN presentes no roteador em questão.

Essas rotas são essenciais, pois sem interfaces configuradas e rotas diretamente conectadas o roteador não consegue receber ou encaminhar os pacotes IP.

Portanto, com as interfaces configuradas e ativas processo de roteamento em um roteador é iniciado, o qual a princípio é capaz de encaminhar pacotes somente entre essas interfaces.

3.5.1 Verificando as Interfaces Diretamente Conectadas



Se uma rede **directly connected** foi mostrada em sua tabela de roteamento quer dizer que a interface que ela está referenciada foi configurada com um endereço pertencente àquela rede e a interface está **UP/UP**.

Elas são inseridas automaticamente pelo roteador à sua tabela de roteamento assim que uma interface tem um endereço IP configurado e seu status alterado para "UP/UP" (comando no shutdown).

Elas são a base para o funcionamento do roteamento estático e dinâmico, pois sem redes IP diretamente conectadas a outros roteadores não existe roteamento ou encaminhamento de pacotes.

Veja abaixo o que ocorre com uma interface fast 0/0 quando é configurada e sua rota é adicionada à tabela de roteamento. Para isso inserimos o comando "debug ip routing", o qual mostra alterações na tabela de roteamento, portando quando configurarmos a interface e inserirmos o comando "no shut" o debug deve mostrar uma rota sendo inserida na tabela de roteamento, veja a saída dos comandos a seguir.

```
Router#debug ip routing
IP routing debugging is on
Router#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int fast 0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shut
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
RT: interface FastEthernet0/0 added to routing table
RT: SET_LAST_RDB for 192.168.1.0/24
NEW rdb: is directly connected
RT: add 192.168.1.0/24 via 0.0.0.0, connected metric [0/0]
RT: NET-RED 192.168.1.0/24
Router(config-if)#
```

Como o comando "debug ip routing" monitora a entrada e saída de rotas na tabela de roteamento, após o comando "no shut" ser inserido uma mensagem de que a interface foi para

UP (mensagem: %LINEPROTO-5-UPDOWN: Line protocol ...) foi gerada e a rede IP configurada na interface é adicionada à tabela de roteamento (Mensagem: RT: interface FastEthernet0/0 added to routing table).

Agora através dessa rede pacotes IP podem ser encaminhados e ela já pode fazer parte do processo de roteamento estático ou dinâmico para conexão com redes remotas.

Com o comando "**show ip route**" você conseguirá verificar que a rede adicionada foi para a tabela de roteamento e a letra **C** no início da linha indica que a rota é pertencente a uma rede diretamente conectada. Veja a saída do comando abaixo.

```
R1#show ip route
```

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default, U - per-user static route
        o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
        + - replicated route, % - next hop override
```

```
Gateway of last resort is not set
```

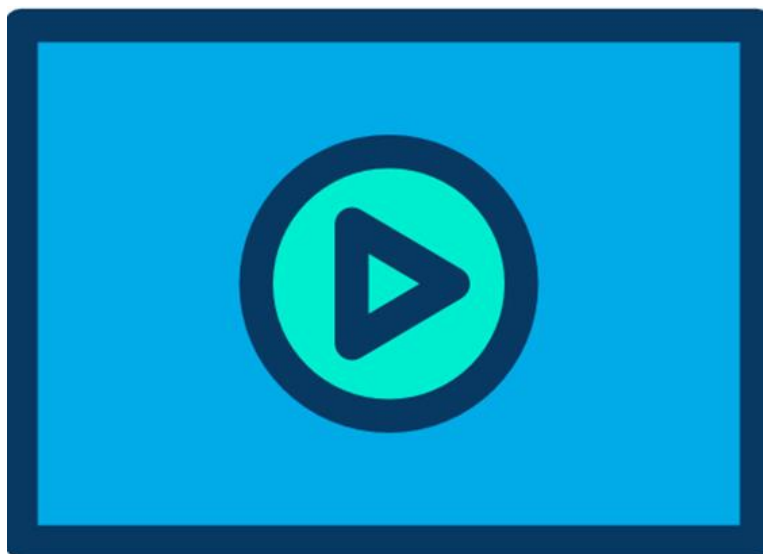
```
          192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C          192.168.1.0/24 is directly connected, FastEthernet0/0
L          192.168.1.1/32 is directly connected, FastEthernet0/0
R1#
```

Logo abaixo da rota para a rede classe C 192.168.1.0 com máscara padrão /24 (255.255.255.0) temos a entrada apontando para a própria interface 192.168.1.1 com máscara de host /32 (255.255.255.255). Essa entrada não será verificada em versões 12.x do Cisco IOS.

Com o comando "**show ip interface brief**" você pode verificar o status da interface caso a rota não tenha subido na tabela de roteamento.

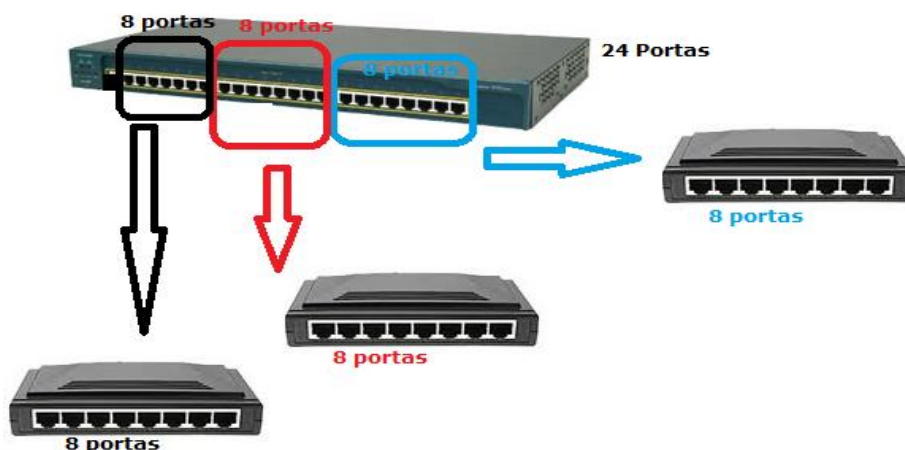
Lembre-se que para a interface subir a camada física e de enlace devem estar corretamente configuradas e conectadas.

3.6 Roteamento entre VLANs



Como estudado no curso **Acesso à Rede Cabeada e Sem Fio**, ao criar uma VLAN as portas alocadas nela formam um domínio de broadcast único.

É como se cada VLAN que criada criássemos um switch novo com as portas que alocamos nessa VLAN, veja figura abaixo onde criamos três VLANs em um switch de 24 portas, formando três domínios de broadcasts novos.



Para fazer essas VLANs se comunicarem podemos conectar uma porta alocada em cada VLAN a um roteador, o que seria impraticável pelo número de portas em roteadores necessárias, portanto o que é feito na prática é configurar uma ou mais portas com o protocolo 802.1Q e conectar o switch a um dispositivo de camada-3 (roteador ou switch camada 3) para que ele faça o roteamento entre as diferentes VLANs.

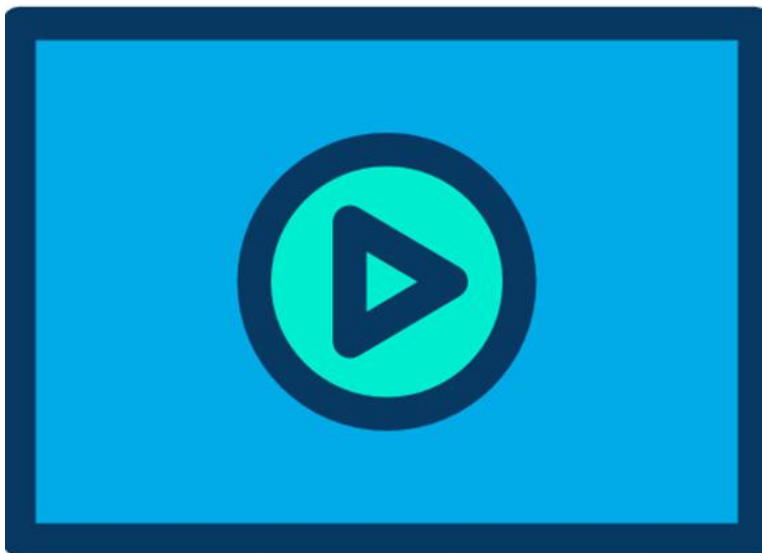
O uso dos roteadores fazendo o roteamento entre VLANs é mais comum em redes com poucos hosts (até 300 computadores), formando uma topologia chamada "router-on-a-stick".

Acima de 300 hosts já se recomenda o uso de switches camada-3.

Você vai notar uma coisa muito importante: "o roteamento entre VLANs é realizado através de Interfaces Diretamente Conectadas", por isso mesmo estamos estudando aqui esse assunto!

Vamos estudar como configurar o roteamento entre VLANs a seguir.

3.6.1 Roteamento entre VLANs com Roteadores



Por padrão somente hosts de uma mesma VLAN podem se comunicar.

Para que computadores de VLANs diferentes se comuniquem é necessário que um equipamento de camada-3 seja inserido na rede e devidamente configurado para efetuar o encaminhamento do tráfego entre as VLANs.

Lembrem que cada VLAN está configurada em um domínio de broadcast diferente, ou seja, cada uma possui sua própria rede ou sub-rede IP, por isso para haver comunicação um roteador precisará realizar o roteamento entre as redes, ou seja, encaminhar os pacotes de uma rede para outra.

Para suportar roteamento entre VLANs, seja em redes entroncadas via ISL ou 802.1Q, a interface LAN do roteador deve ser **subdividida** e essas novas **interfaces lógicas** são chamadas **subinterfaces**.

O roteamento entre VLANs em roteadores é realizado criando sub-interfaces lógicas em uma Fastethernet ou Gigabitethernet. A interface LAN física deve estar sem endereço IP configurado, pois ele será configurado nas sub-interfaces lógicas.

Podemos fazer uma analogia que vamos "**fatiara interface física**" para passar várias VLAN's, que são **interfaces lógicas**. Caso não fosse possível essa configuração o roteador necessitaria uma interface LAN por VLAN configurada no switch.

Você pode escolher qualquer número de sub-interface em um range de 0 até 4294967295, conforme mostrado abaixo.

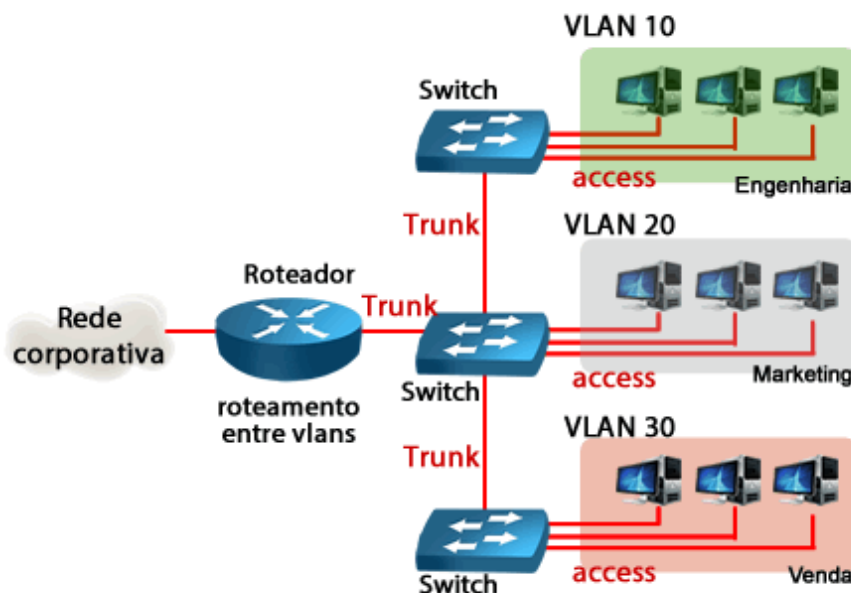
```
Router0(config)#int f0/0.?  
<0-4294967295> FastEthernet interface number  
Router0(config)#int f0/0.10  
%LINK-5-CHANGED: Interface FastEthernet0/0.10, changed state to up  
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.10, changed state to up  
Router0(config-subif)#
```

Assim que você cria a sub-interface, se a interface principal estiver ativada, ela sobe para UP e a rede IP configurada nela é inserida na tabela de roteamento.

Uma forma interessante de configuração que facilita a manutenção é colocar o número da sub-interface igual ao da VLAN a ser configurada nela, por exemplo, você vai configurar a VLAN 10 no roteador, entre com o comando "interface fast 0/0.10", assim você poderá analisar os problemas de roteamento entre VLANs mais facilmente.

As informações de VLAN também serão criadas nas sub-interfaces com o comando "**encapsulation dot1q 10**", onde o parâmetro "**dot1q**" representa o protocolo **802.1Q** e o valor "**10**" representa a **VLAN 10**.

A seguir estudaremos outro exemplo de configuração de roteamento entre VLAN executado por um roteador 2811, onde ele irá rotear as VLANs 10 e 20 com protocolo 802.1Q e a VLAN 30 com protocolo ISL, conforme topologia abaixo.



```
2811#config t
2811(config)#int fast 0/0      ! Configurando a interface física
2811(config-if)#no ip address
2811(config-if)#no shut
2811(config)#interface fastethernet 0/0.1 ! criando a sub-interface 0/0.1
2811(config-subif)#encapsulation dot1q 10 ! VLAN 10 via 802.1Q
2811(config-subif)#ip address 192.168.1.1 255.255.255.0
2811(config-subif)#exit
2811(config)#interface fastethernet 0/0.2 ! criando a sub-interface 0/0.2
2811(config-subif)#encapsulation dot1q 20 ! VLAN 20 via 802.1Q
2811(config-subif)#ip address 192.168.2.1 255.255.255.0
2811(config-subif)#exit
2811(config)#int f0/0.3      ! criando a subinterface 0/0.3
2811(config-subif)#encapsulation dot1q 30 ! VLAN 30 via 802.1Q
2811(config-subif)#ip address 192.168.3.1 255.255.255.0
2811(config-subif)#exit
2811(config)#
```

Reforçando, o comando **"encapsulation"** define o protocolo de camada-2 a ser utilizado na subinterface, o **"dot1q"** representa o **802.1Q**.

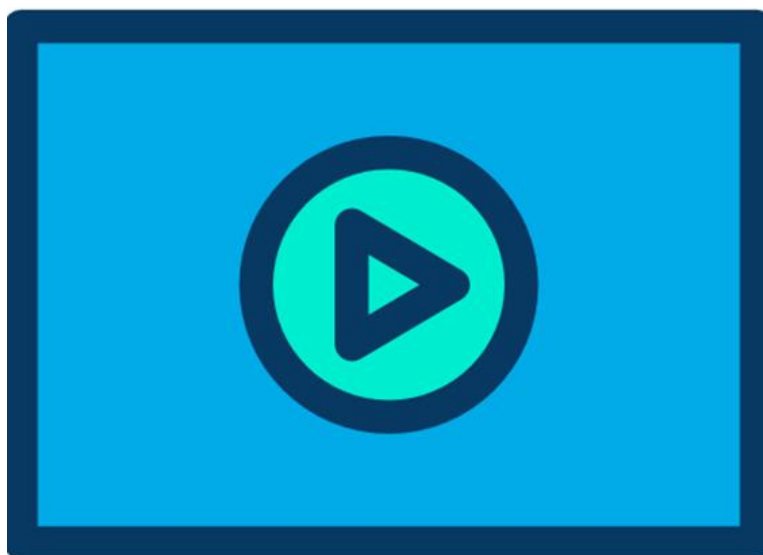
O número colocado após o parâmetro "dot1q" ou "isl" é o número da VLAN que o roteador irá encaminhar.

Além dessa configuração é necessário configurar os endereços IPs das sub-interfaces, pois cada VLAN necessita de uma rede ou sub-rede IP própria, com o comando "ip address" conforme já ensinado anteriormente.

É importante notar que a interface principal fica sem endereço IP, eles são configurados em cada sub-interface, conforme exemplo apresentado.

Essa topologia com switches na rede LAN e um roteador fazendo o roteamento entre VLANs é conhecida como **"router-on-a-stick"** ou **ROAS**.

3.6.2 Roteamento entre VLANs com Switches Camada 3

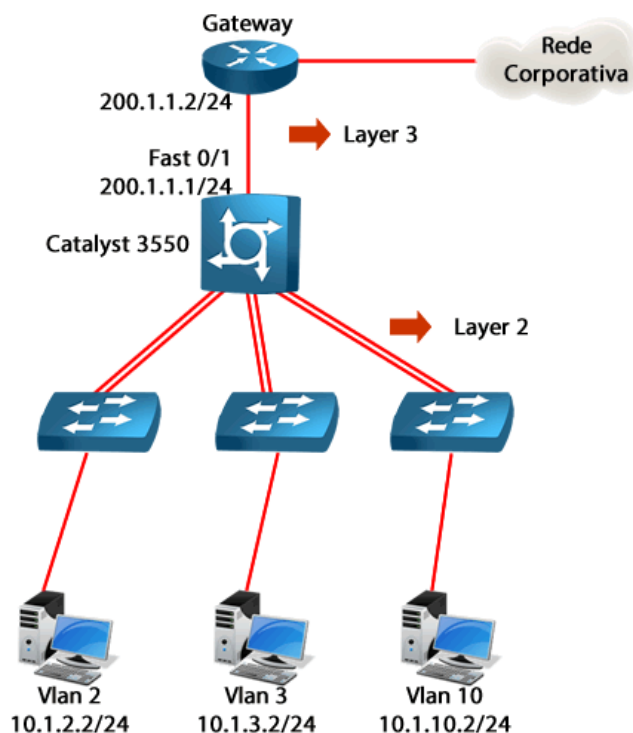


Normalmente em redes com arquitetura em três camadas utilizamos switches Layer 3 nas camadas de distribuição e núcleo, sendo que o roteamento entre VLANs é recomendado ser configurado nos switches de distribuição.

A diferença de um switch camada 3 para um roteador é que ele pode realizar roteamento de pacotes de maneira semelhante ao encaminhamento dos quadros, ou seja, através de hardware ao invés de software como nos roteadores, isso torna os switches camada 3 até mais rápido que os roteadores para o encaminhamento dos pacotes.

Os switches Layer 3 da Cisco que rodam IOS são na realidade switches layer 2 por padrão e para terem a facilidade de roteamento IP (Layer 3) você deve utilizar um IOS mais avançado, que suporte o protocolo IP, e também habilitar o protocolo IP com o comando **"ip routing"** em modo de configuração global, o mesmo comando que já vem habilitado por padrão nos roteadores.

Vamos mostrar um exemplo de configuração de roteamento entre VLANs em um switch layer 3 modelo Catalyst 3550, veja a topologia na figura abaixo.



Vamos partir do pressuposto que as configurações básicas do switch 3550 foram realizadas e os switches de acesso também, portanto vamos apenas nos preocupar com ativar o roteamento IP no 3550 e configurar o roteamento entre VLANs.

Note na topologia que temos as VLANs 2, 3 e 10 e vamos alocar o primeiro IP de cada VLAN para o 3550. Vamos iniciar ativando o protocolo IP e depois configurando o roteamento entre VLANs.

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#ip routing
Switch(config)#interface Vlan2
Switch(config-if)#ip address 10.1.2.1 255.255.255.0
Switch(config-if)#no shutdown
Switch(config)#interface Vlan3
Switch(config-if)#ip address 10.1.3.1 255.255.255.0
Switch(config-if)#no shutdown
Switch(config)#interface Vlan10
Switch(config-if)#ip address 10.1.10.1 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#
```

Note que o roteamento entre VLANs nada mais é que criar uma interface VLAN para cada sub-rede e ativá-la. Quando o switch é Layer-2 apenas uma interface VLAN é permitida, a de gerenciamento, quando tentamos ativar mais uma ele coloca a anterior em shutdown.

Essas interfaces são chamadas SVIs ou Switched Virtual Interfaces.

Agora com o comando **show ip route** podemos verificar a tabela de roteamento no switch 3550, veja abaixo.

```
Switch#show ip route
### Saídas omitidas ###
Gateway of last resort is 200.1.1.2 to network 0.0.0.0

    200.1.1.0/30 is subnetted, 1 subnets
C       200.1.1.0 is directly connected, FastEthernet0/48
    10.0.0.0/24 is subnetted, 3 subnets
C       10.1.10.0 is directly connected, Vlan10
C       10.1.3.0 is directly connected, Vlan3
C       10.1.2.0 is directly connected, Vlan2
S*  0.0.0.0/0 [1/0] via 200.1.1.2
```

Note que para cada interface VLAN criada foi inserida uma rota diretamente conectada na tabela de roteamento do switch, tendo o mesmo efeito da configuração das sub-interfaces no roteador quando utilizamos a topologia "**router-on-a-stick**", ou seja, switches conectados diretamente ao roteador através de um link layer-2.

Com essa configuração o switch camada-3 fará o encaminhamento de pacotes entre as redes locais dos switches de acesso conectados a ele.

4 Como o Roteador Escolhe a Melhor Rota

4.1 Introdução

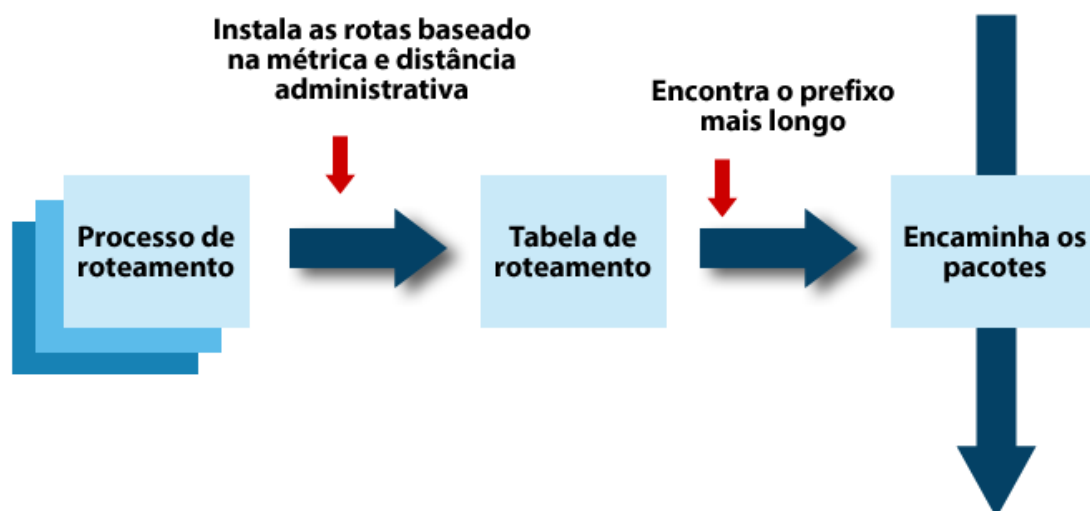


Nesse capítulo vamos estudar como os roteadores escolhem as rotas que devem ser mostradas e utilizadas como escolha para o encaminhamento dos pacotes entre suas diversas interfaces de saída.

As regras servem tanto para o IPv4 como para o IPv6, porém utilizaremos o IPv4 como exemplo.

A escolha vai sempre girar em torno de três parâmetros:

- Distância administrativa (AD ou Administrative Distance)
- Métrica (Metric)
- Longest Match



Mesmo não sabendo nada sobre um protocolo de roteamento, ou seja, sobre como ele funciona, com poucos dados você será capaz de dizer se a rota que ele aprendeu será ou não utilizada pelo roteador em sua tabela de roteamento.

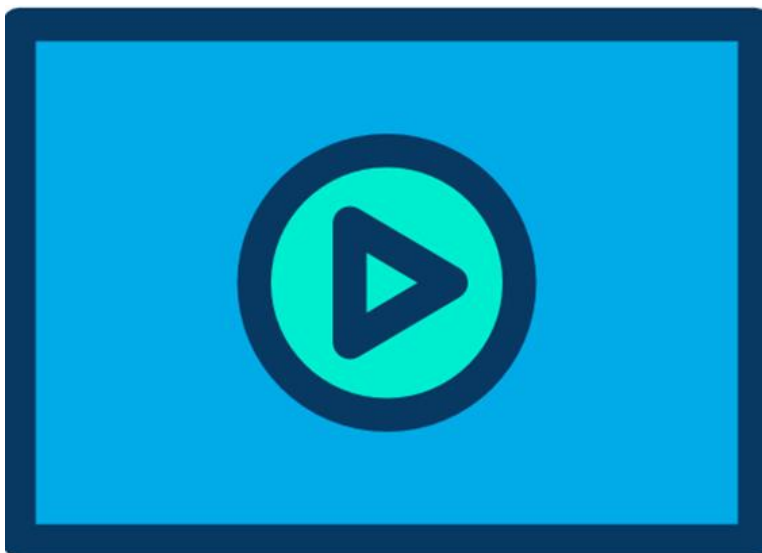
Imagine que temos um roteador com diversos protocolos de roteamento configurado nele, portanto teremos várias fontes de roteamento para algumas redes.

Como o roteador escolhe qual delas é mais confiável?

Vamos além, e se tivermos mais de uma rota apontando para a mesma rede de destino na tabela de roteamento? Qual dessas rotas o roteador vai utilizar?

Esse é o objetivo desse tópico do curso!

4.2 Distância Administrativa



Os roteadores Cisco suportam diversos protocolos de roteamento simultaneamente, mas como eles decidem que informação utilizar?

Que rota aprendida por que protocolo de roteamento deve entrar na tabela?

Portanto, estamos decidindo aqui a fonte de roteamento ou routing source que irá popular a tabela de roteamento.

Quando um roteador aprende a informação sobre o caminho até uma rede (rota) através de mais de uma fonte de roteamento, ou seja, aprendeu rota para uma mesma rede de destino através de mais de um protocolo de roteamento, a **distância administrativa (AD ou Administrative Distance)** é utilizada como fator de escolha da rota que deve ser utilizada para decidir que rota deve ser adicionada à tabela de roteamento do roteador (routing table).

Nesse caso, o roteador escolhe a rota aprendida pelo protocolo de roteamento com **menor distância administrativa**.

Cada protocolo ou entrada de roteamento possui uma distância administrativa padrão, porém ela pode ser configurada manualmente. Veja a tabela abaixo com as ADs padrões.

Origem das Rotas	AD
Interface diretamente conectada	0
Rota estática com IP como referência	1
Rota estática com Interface como referência	1
EIGRP – rota sumário	5
External Border Gateway Protocol (BGP)	20
EIGRP interno	90
IGRP	100
OSPF	110
Intermediate System-to-Intermediate System (IS-IS)	115
Routing Information Protocol (RIP)	120
Exterior Gateway Protocol (EGP)	140
On Demand Routing (ODR)	160
EIGRP – rota externa	170
BGP interno	200
Desconhecido	255

Para construir a tabela de roteamento, além da distância administrativa temos também o conceito da métrica das rotas que é utilizada quando um mesmo protocolo de roteamento aprende mais de uma entrada para o mesmo caminho.

Assim como o AD, a **menor métrica** é a que irá ser inserida na tabela de roteamento.

As distâncias administrativas são as mesmas no IPv4 e IPv6, porém alguns protocolos de roteamento podem ter o nome um pouco diferente.

Por exemplo, o OSPF no IPv4 chama-se OSPFv2 e no IPv6 OSPFv3, mas ambos têm AD 110.

4.3 Métrica dos Protocolos de Roteamento

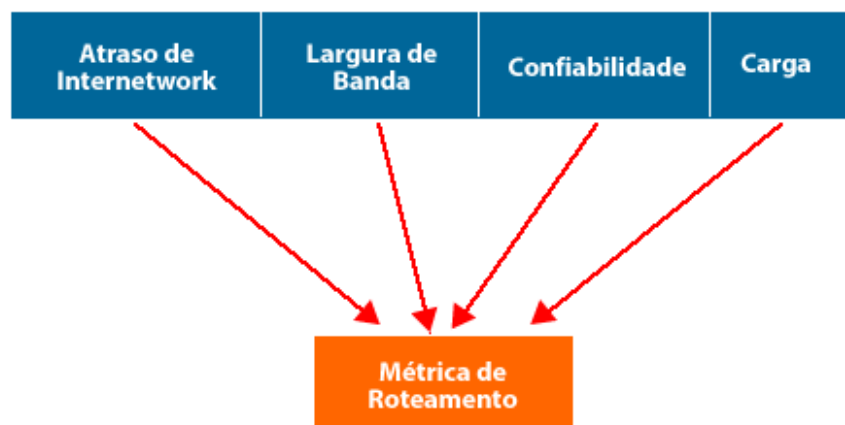


Lembre-se que o AD é um fator de decisão ENTRE DIFERENTES FONTES DE ROTEAMENTO, já a métrica é utilizada para escolha da melhor rota dentro de um mesmo protocolo de roteamento.

A métrica é um cálculo feito pelo algoritmo de roteamento para determinar um valor, normalmente chamado de custo ou "cost" em inglês. Esse valor define basicamente quão boa é a rota para aquele protocolo de roteamento específico.

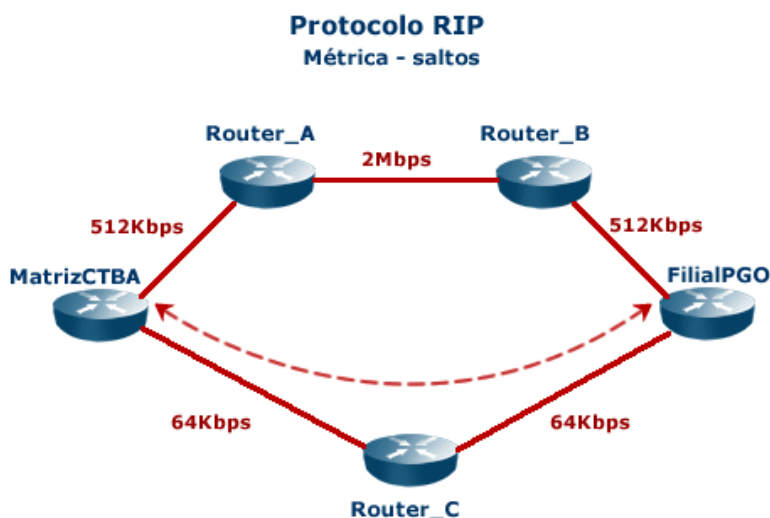
Cada protocolo de roteamento possui um tipo de métrica, por exemplo, no RIP a métrica utilizada é o número de saltos, já protocolos mais avançados como EIGRP e OSPF consideram a velocidade do link em suas métricas.

Veja a figura abaixo com exemplos de parâmetros utilizados no seu cálculo.



Vamos a um exemplo de como a métrica pode influenciar na escolha dos caminhos.

Considere a rede da figura abaixo, para o roteador "MatrizCTBA" enviar um pacote para o "FilialPGO" ele utilizará o caminho do "Router_C", pois o protocolo RIP utiliza como métrica o número de saltos (hops).

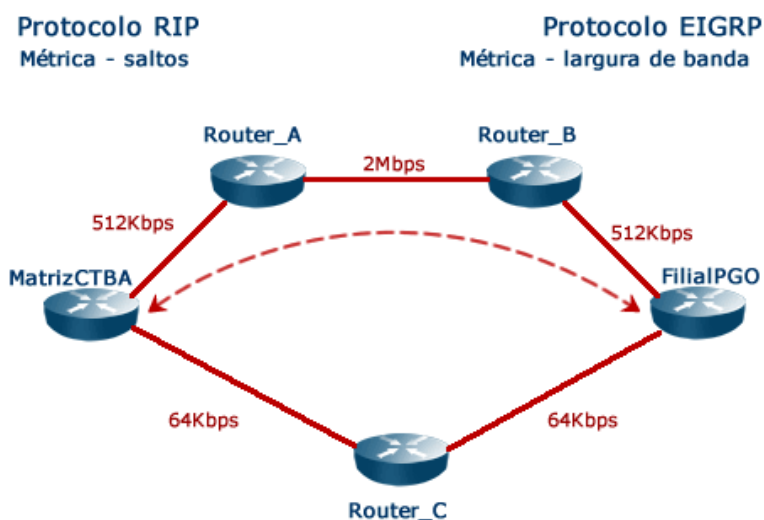


Agora imagine que você também configurou o protocolo EIGRP nessa mesma rede, conforme mostrado agora na figura a seguir.

Nesse novo cenário o roteador deverá primeiramente escolher qual dos dois protocolos ele utilizará para determinar o melhor caminho, o RIP ou o EIGRP.

Nesse caso a escolha será pelo protocolo EIGRP, pois a distância administrativa do EIGRP é **90** enquanto a do RIP é **120**.

O roteador sempre irá escolher o protocolo que possui a menor distância administrativa.



Depois de decidido o protocolo ele deverá escolher o melhor caminho através da métrica. No caso do EIGRP será através do "Router_A" e "Router_B".

Isso porque o EIGRP leva em consideração a informação de **largura de banda** para o cálculo da melhor métrica e não o número de saltos.

O link pelo "Router_A" e "Router_B" possui largura de banda de 512Kbps e 2Mbps respectivamente, sendo muito melhor do que um caminho com menos saltos, mas onde a largura de banda é de apenas 64Kbps.

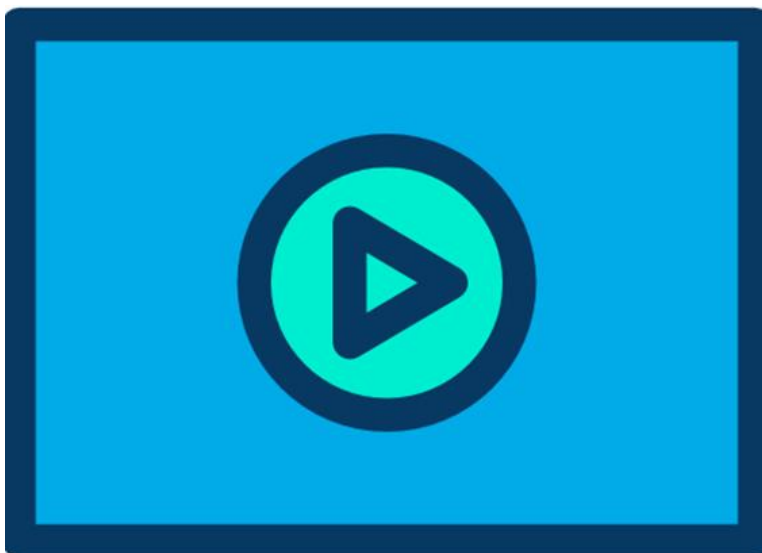
Dica prática: você pode verificar a distância administrativa e a métrica de uma rota específica com o comando "show ip route" adicionando a rede no final do comando. Veja exemplo abaixo:

```
Switch-Cisco(config)#ip route 200.0.0.0 255.0.0.0 fast 0/23
Switch-Cisco(config)#end
Switch-Cisco#sho ip route 200.0.0.0
Routing entry for 200.0.0.0/8, supernet
  Known via "static", distance 1, metric 0 (connected)
  Redistributing via eigrp 100
  Advertised by eigrp 100 metric 1000 1 1 1 1
  Routing Descriptor Blocks:
  * directly connected, via FastEthernet0/23
    Route metric is 0, traffic share count is 1

Switch-Cisco#sho ip route | include 200.0.0.0
S    200.0.0.0/8 is directly connected, FastEthernet0/23
```

Note que mesmo sendo uma rota estática que aponta para uma interface local de saída a distância administrativa da rota continua sendo "1", porém ela é inserida na tabela de roteamento como "directly connected".

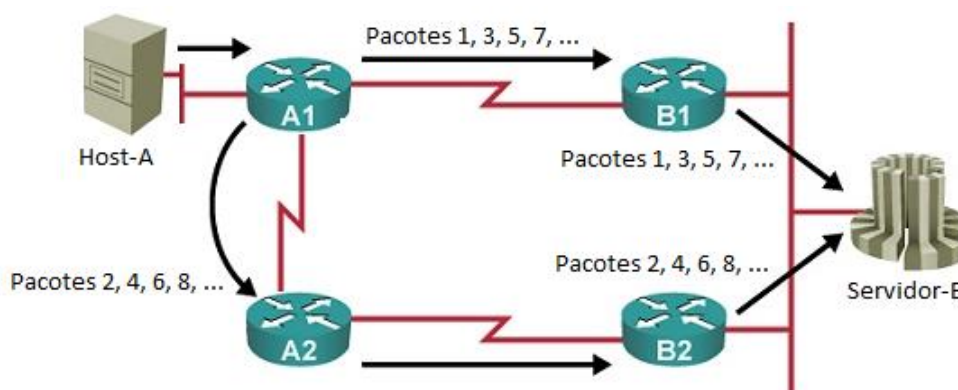
4.4 Balanceamento de Cargas



O balanceamento de carga ocorre quando um roteador aprende mais de uma rota para uma determinada rede de destino com a mesma distância administrativa e métrica.

É uma propriedade que pode ser usada em protocolos de roteamento dinâmicos como RIP, OSPF e EIGRP visando utilizar um segundo link backup para compartilhar o envio de dados.

Veja a abaixo com um exemplo de balanceamento de carga de custos iguais por pacotes (per packet).



Quando o protocolo de roteamento ativa o balanceamento de carga em dois ou mais links se um host envia pacotes para uma rede de destino o roteador divide os pacotes (per packet) ou fluxos (per flow ou per destination – por destino) entre as interfaces balanceando (dividindo) o envio dos pacotes (carga) entre esses caminhos.

No balanceamento de carga por pacotes os roteadores enviam um pacote para cada interface que participa do processo.

No balanceamento por fluxo (ou destino) o balanceamento de carga é realizado por conexão TCP ou UDP aberta, ou seja, se um usuário solicitou uma página de internet aquele fluxo vai seguir até o final por um link, quando um segundo usuário abrir outra sessão na sequência o fluxo dele será encaminhado ao segundo link.

Por padrão os roteadores Cisco fazem o entre rotas de métricas iguais ou custos iguais chamado **"equal cost path load sharing"**, em inglês.

Além disso, por padrão a carga é balanceada em até 4 links de custos iguais automaticamente nos protocolos de roteamento dinâmico RIP, EIGRP e OSPF.

Na tabela de roteamento você consegue verificar o balanceamento de carga através de entradas repetidas para a mesma rede com distância administrativa e custos (métricas) iguais.

Essa propriedade melhora o uso dos links, pois diminui a sobrecarga de termos uma topologia redundante com link principal e backup em espera (stand-by) entrando em atividade somente em caso de problemas, assim como o balanceamento de carga evita que o link backup fique ocioso.

Veja exemplo da saída de uma tabela de roteamento com rotas em balanceamento ativo.

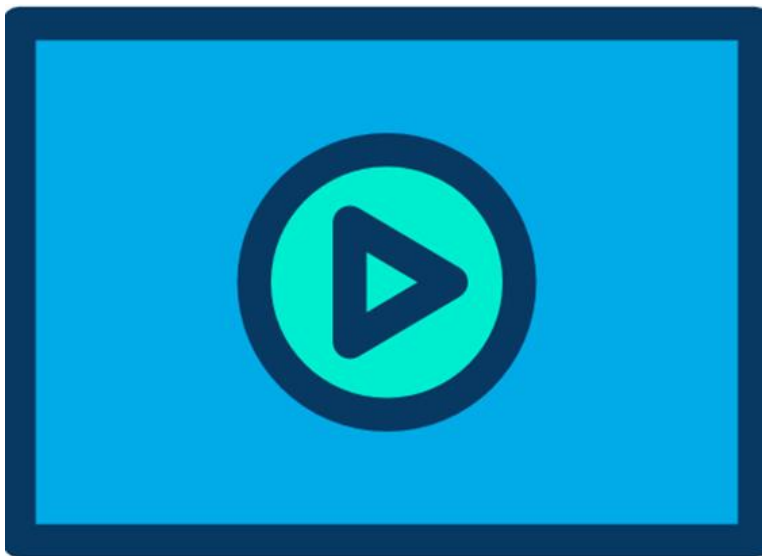
```
router# show ip route
....
172.30.0.0/16 is variably subnetted, 1 subnets, 1 masks
R       172.30.32.0/20 [120/2] via 10.1.1.2
        172.30.32.0/20 [120/2] via 10.1.1.1
S*      0.0.0.0/0 [1/0] via 10.1.1.3
```

Note que a rede 172.30.32.0 tem duas saídas possíveis indicadas na tabela de roteamento, através de 10.1.1.2 e 10.1.1.1.

Note também que ambas as rotas têm a mesma métrica "2", por isso o balanceamento foi ativado entre elas.

O RIP e OSPF tem o mesmo funcionamento para o balanceamento de cargas, já o EIGRP também suporta balanceamento entre rotas com métricas diferentes ou **unequal cost path load sharing**, porém o padrão dos três protocolos é fazer somente entre rotas de mesmo custo.

4.5 Regra do "Longest Match"



Antes de analisarmos a regra do Longest Match você deve lembrar que uma "rota" em uma rede IP versão 4 nada mais é que o endereço de rede com uma máscara de sub-rede.

Lembre-se de que uma rede IP é dividida em:

- **Endereço de Rede ou Subrede** → primeiro IP de uma rede ou sub-rede IP (todos os bits de host estão em zero).
- **IPs Válidos** (endereço de host ou hosts válidos) → do segundo ao penúltimo IP de uma rede ou sub-rede IP.
- **Endereço de Broadcast** → último IP de uma rede ou sub-rede IP (todos os bits de host estão em um).

Portanto, quando você tem em uma rede LAN configurados computadores com IPs classe C 192.168.1.1, 192.168.1.2, 192.168.1.3 e 192.168.1.10 com máscara 255.255.255.0 (/24) você deve ter nos roteadores uma rota para a rede 192.168.1.0 /24 que no final apontem para a Interface de LAN que esses hosts estão conectados.

Porém, se em um dos roteadores tivermos as seguintes rotas abaixo, para qual das interfaces o roteador irá encaminhar os pacotes se ele receber um pacote com IP de destino 192.168.1.10?

- 192.168.1.0 255.255.255.0 (/24): serial 0
- 192.168.1.0. 255.255.255.240 (/28): serial 1

É nesse tipo de situação que usamos a regra do prefixo mais longo, nesse caso apesar do IP 192.168.1.10 estar contido nas duas redes apresentadas o roteador irá encaminhar para a **serial 1**, pois ela tem o **prefixo mais longo**.

É como se comparássemos assim, você precisa encontrar uma pessoa e tem 3 informações:

- 1) O Fulano da Silva está no Brasil.
- 2) O Fulano da Silva está no Paraná.
- 3) O Fulano da Silva está na Av. Sete de Setembro, 3728, conjunto 500, em Curitiba Paraná.

Qual das três você escolheria para encontrar o Fulano? Com certeza a terceira.

A mesma análise é para a escolha através do prefixo mais longo, pois na rota 192.168.1.0 /24 temos os IPs de 192.168.1.1 até 192.168.1.254, totalizando 254 hosts, porém com a rota 192.168.1.0 /28 temos apenas os IPs de 192.168.1.1 até 192.168.1.14, totalizando apenas 14 hosts, por isso essa informação é mais confiável, pois há **maior probabilidade de encontrarmos** o host nessa rede de menor tamanho.

Portanto, um IP de destino estiver contido em mais de uma rota ele sempre vai ser encaminhado para rota com o maior número de bits "1" na máscara de sub-rede.

4.6 Resumindo a Escolha da Melhor Rota

Lembre-se, um roteador pode aprender rotas de diversas fontes de roteamento, tais como rotas:

- Diretamente conectadas
- Estáticas (configuradas pelos admsde rede)
- Dinâmicas (via protocolo de roteamento dinâmico)
- Padrão (default gateway)

Sempre a rota com menor distância administrativa é a que entra na tabela de roteamento.

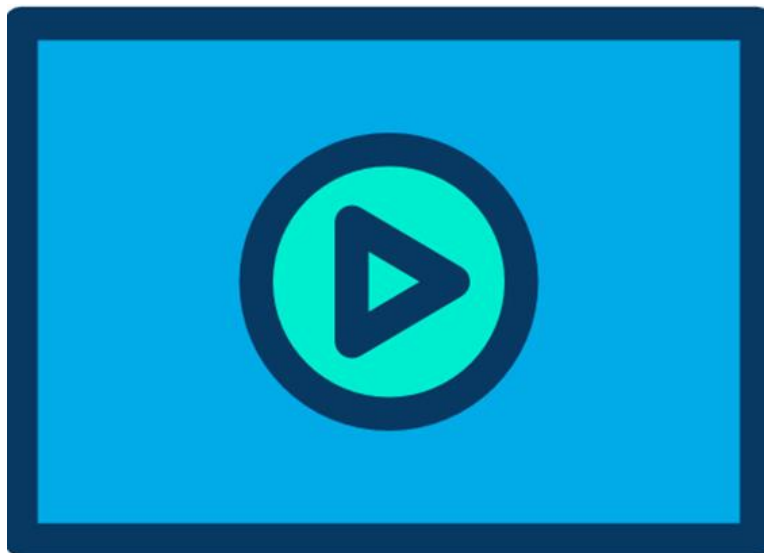
Se uma rede de destino tem dois caminhos ou duas rotas de saída quem entra na tabela de roteamento?

1. Menor distância administrativa (AD ou Administrative distance)
2. Se ADs forem iguais entre a rota com a menor métrica
3. Se as Métricas e os ADs forem iguais o roteador faz por padrão o balanceamento de cargas e mantém todas as rotas na tabela de roteamento

Com as rotas já instaladas na tabela de roteamento, se existir sobreposição de um IP de destino em várias rotas, ou seja, o IP de destino está contido na faixa de endereços de mais de uma rota, **VENCE O LONGEST MATCH** (rota com mais bits "1" na máscara ou prefixo).

5 Configurando e Verificando Rotas Estáticas IPv4

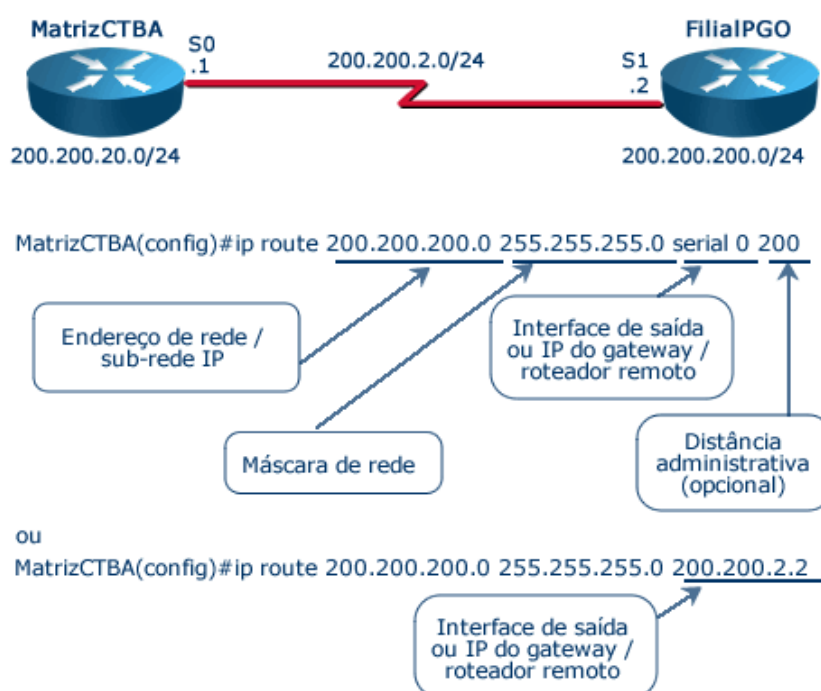
5.1 Introdução



O método mais simples e econômico de fazer a configuração de roteamento nos roteadores Cisco é utilizando Rotas Estáticas, pois não há nenhuma necessidade de cálculo ou processamento por parte do roteador, uma vez que o administrador já definiu os melhores caminhos e simplesmente instruiu ao roteador via o comando **"ip route"** como os destinos remotos podem ser alcançados.

As rotas estáticas então nada mais são que entradas manuais feitas por um administrador de redes e utilizadas principalmente em redes stub (redes de apenas uma saída), para configuração de um gateway default.

A figura abaixo mostra a sintaxe para configuração de uma rota estática.



Nesse exemplo o roteador "MatrizCTBA" aprendeu estaticamente uma rota para a rede LAN do roteador "FilialPGO" (rede de destino 200.200.200.0/24), a qual pode ser encontrada via a "serial 0", esse parâmetro poderia ser ainda o endereço IP da serial do roteador vizinho.

5.2 Opções do Comando IP-Route

Vamos analisar as opções do comando IP Route abaixo.

```
Dltec-FW-GW(config)#ip route 10.0.0.0 255.255.255.0 192.168.1.1 ?
<1-255>      Distance metric for this route
  name        Specify name of the next hop
  permanent   permanent route
  tag         Set tag for this route
  track       Install route depending on tracked item
<cr>
```

O primeiro **<1-255>** já estudamos, que é a distância administrativa, vamos ver exemplo do uso no item sobre rotas flutuantes.

O **"name"** é apenas uma referência, assim como o description das interfaces.

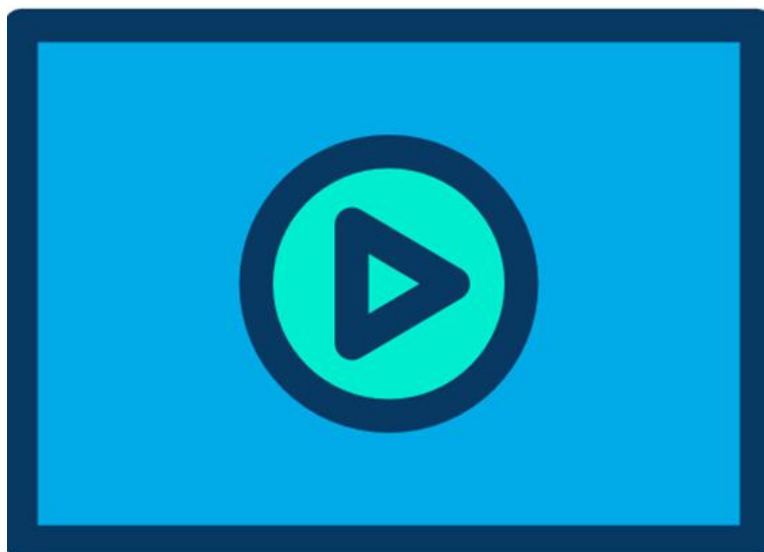
Já a opção **"permanent"** cria uma rota permanente, ou seja, se você referenciar a rota a uma interface, por exemplo, e essa interface cair a rota continuará na tabela, porém você vai ter problemas com esse destino, pois esse comando não é "mágico", ou seja, se a rota está fora os pacotes serão dropados (descartados).

A opção **"tag"** coloca uma marcação na rota, normalmente utilizada pelos CCNPs na configuração de "route-maps".

E por último temos a opção **"track"** que pode ser utilizada em conjunto com o IP SLA para ativar a rota quando uma determinada condição ocorrer.

A seguir vamos estudar um exemplo ilustrativo de configuração do roteamento de uma pequena rede com apenas dois roteadores via rotas estáticas.

5.3 Network Routes ou Rotas Estáticas para Redes Remotas



Uma Network Route é uma rota para uma rede remota, por exemplo, a rede 200.200.200.0/24 é alcançada via serial e você precisa configurar uma rota para essa rede, isso é feito via "Network Route".

Vamos estudar a configuração desse tipo de rota com um exemplo prático.

Nesse exemplo que faremos agora será simular a configuração de um laboratório com dois roteadores e dois roteadores partindo do "zero", ou seja, como se abrissemos a caixa dos roteadores novos para configurá-los com o mínimo possível de comandos gerais.

Para iniciar temos que pensar primeiro nas redes IP que utilizaremos para configurar as interfaces. Teremos uma rede LAN via Fastethernet em cada roteador e uma rede WAN interligando os roteadores via interface Serial, totalizando 3 redes IP.

Vamos escolher redes Classe C privadas para o laboratório, podendo ser a 192.168.1.0 e 192.168.2.0 para as redes LAN, e para a rede WAN vamos utilizar a rede 192.168.10.0. Veja na figura a seguir a escolha dos endereços IP por interface.



Vamos considerar que o laboratório já foi montado e corretamente conectado com os devidos cabos, sendo que na conexão serial do roteador R1 foi colocado um cabo DCE e o DTE foi conectado ao roteador R2. Além disso, utilizaremos o protocolo HDLC nas interfaces seriais.

Para as interfaces de LAN, as Fastethernets foram conectadas com cabos diretos entre as portas Fast 0/0 dos roteadores e as Fast 0/1 dos switches.

Estamos prontos para ligar os roteadores, clique aqui para ver a saída do comando "show ip route" no roteador R1 sem configuração abaixo. Note que não existe rota na tabela de roteamento.

```
Router#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
```

Gateway of last resort is not set

Agora vamos configurar as interfaces seriais e Fastethernet do roteador R1, conforme configurações abaixo.

```

Router#
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# hostname R1
R1(config)#int f0/0
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#
*Mar 1 00:12:28.363: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to
up
*Mar 1 00:12:29.363: %LINEPROTO-5-UPDOWN: Line protocol on
Interface FastEthernet0/0, changed state to up
R1(config-if)#int s0
R1(config-if)#ip address 192.168.10.1 255.255.255.0
R1(config-if)#clock rate 128000
R1(config-if)#no shut
R1(config-if)#
*Mar 1 00:13:13.907: %LINK-3-UPDOWN: Interface Serial0, changed state to up
*Mar 1 00:13:14.907: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0,
changed state to up
*Mar 1 00:13:36.323: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0,
changed state to down
R1(config-if)#end
R1#
*Mar 1 00:14:02.079: %SYS-5-CONFIG_I: Configured from console by console
R1#show ip route
R1#sho ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C 192.168.1.0/24 is directly connected, FastEthernet0/0

R1#

```

Note que a interface Fast 0/0 ficou "up", enquanto a serial ficou "Down", isto se deve ao fato de não termos configurado o roteador da outra ponta, o R2.

Por esse motivo, apenas a rota para a rede LAN aparece na tabela de roteamento como diretamente conectada.

O próximo passo será configurar as interfaces do roteador R2, veja as configurações e show ip route abaixo.

```
Router#
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# hostname R2
R2(config)#int f0/0
R2(config-if)#ip address 192.168.2.1 255.255.255.0
R2(config-if)#no shut
R2(config-if)#
00:06:02: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
00:06:03: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
changed state to up
R2(config-if)#int s0
R2(config-if)#ip address 192.168.10.2 255.255.255.0
R2(config-if)#clock rate 128000
R2(config-if)#no shut
R2(config-if)#
00:06:35: %LINK-3-UPDOWN: Interface Serial0, changed state to up
00:06:36: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0, changed state
to up
R2(config-if)#end
R2#
00:07:48: %SYS-5-CONFIG_I: Configured from console by console
R2#sho ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C      192.168.10.0/24 is directly connected, Serial0
C      192.168.2.0/24 is directly connected, FastEthernet0/0
R2#
```

Com a interface serial do roteador R2 configurada, ambas as interfaces subiram e na tabela de roteamento de R2 apareceram as duas rotas diretamente conectadas, a rede da serial e a rede da Fast.

Vamos ver a saída do comando para R1 e verificar se o mesmo ocorreu. Clique aqui e veja a saída do comando para o roteador R1.

```
R1#sho ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
```

Gateway of last resort is not set

```
C      192.168.10.0/24 is directly connected, Serial0
C      192.168.1.0/24 is directly connected, FastEthernet0/0
R1#
```

Comparando as tabelas de roteamento vemos que os roteadores R1 e R2 conhecem a rota 192.168.10.0, a qual é a rede WAN comum aos dois roteadores. Porém, um não conhece a rede LAN do outro.

No cenário atual se um micro conectado ao switch da rede LAN do roteador 1 tentar trocar arquivos ou mensagens com um micro do switch 2 ele não terá sucesso, pois os roteadores não sabem como encontrar a rede LAN um do outro.

Vamos agora configurar uma rota estática (Network Route) em cada roteador ensinando o caminho para as redes LAN um do outro. Note que eles conseguem alcançar as redes LAN um do outro através de suas interfaces seriais e essa facilidade que utilizaremos abaixo para fazer a configuração toda a partir de R1 via Telnet.

```
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
! entrando com a rota para a LAN de R2
R1(config)#ip route 192.168.2.0 255.255.255.0 serial 0
R1(config)#end
R1#sho ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
```

Gateway of last resort is not set

```
C      192.168.10.0/24 is directly connected, Serial0
C      192.168.1.0/24 is directly connected, FastEthernet0/0
S      192.168.2.0/24 is directly connected, Serial0
```

```
R1#
R1#telnet 192.168.10.2
Trying 192.168.10.2 ... Open
```

User Access Verification

Password:

R2>enable

Password:

```

R2#
R2#conf
Enter configuration commands, one per line. End with CNTL/Z.
! Entrando com a rota para a LAN de R1
R2(config)#ip route 192.168.1.0 255.255.255.0 serial 0
R2(config)#end
R2#sho ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

```

```

C      192.168.10.0/24 is directly connected, Serial0
S      192.168.1.0/24 is directly connected, Serial0
C      192.168.2.0/24 is directly connected, FastEthernet0/0

```

R2#

Note que após entrarmos com as redes LAN de maneira estática nos routers, ela aparece no comando "show ip route" diferenciada com um "S" na frente, o que representa "static" ou estático em português.

Agora vamos testar com o comando ping se os roteadores conseguem alcançar a LAN remota, conforme saídas abaixo.

```

R2#ping 192.168.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/20/28 ms
R2#
R1#ping 192.168.2.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/14/16 ms
R1#

```

Podemos perceber que com as rotas estáticas o ping funcionou 100% em ambos os roteadores.

O ponto de exclamação no ping significa que o Echo Req enviado teve uma resposta bem sucedida.

Se desse problema poderia aparecer um ponto (.) se o tempo de espera pela resposta expirar ou a letra U se o destino for inalcançável ou algum filtro no destino está aplicado impedindo uma resposta do host.

5.4 O que é Melhor Interface ou IP na Rota Estática?

Nessa altura desse tópico de rotas estáticas você pode ter ficado com a pergunta: **“O que é melhor configurar como saída então? Um IP do próximo salto ou uma interface local?”**.

Em questões práticas no exame de certificação CCNA você deve configurar com o que for solicitado, se não for especificado nada valem os dois formatos.

Na prática, quando utilizamos a interface local de saída o roteamento tem menos passos de processamento, pois o roteador não precisa resolver ou verificar quem é a interface de saída daquele IP.

Por exemplo, se configurarmos **“ip route 192.168.1.0 255.255.255.0 192.168.10.10”** toda vez que chegar um pacote cujo destino é a rede 192.168.1.0 ele deve ser encaminhado ao IP 192.168.10.10, porém o roteador não encaminha a um IP e sim para uma Interface, portanto antes de encaminhar o roteador terá que descobrir para qual interface possui a rede que o IP 192.168.10.10 pertence.

Ao passo que se configurarmos **“ip route 192.168.1.0 255.255.255.0 serial 0”** o roteador não precisará fazer a análise anterior, pois ele já sabe que precisará encaminhar para a interface serial 0, economizando um passo para encaminhar o pacote.

Existem também restrições para apontar para uma serial local quando temos uma rede Broadcast, por exemplo, uma rede Ethernet, Fast ou Giga.

Em uma rede fast temos um switch e diversos hosts na mesma LAN, se criarmos a rota **“ip route 102.10.1.0 255.255.255.240 fast 0/0”** o roteador encaminhar pacotes para a rede 102.10.1.0 /28 para a porta fast que chega a um switch e temos diversos hosts nessa rede, portanto quem será responsável por receber e encaminhar esses pacotes?

Por isso que no caso de rotas estáticas que tem saída em uma **rede LAN** o correto é utilizar o **IP do próximo salto** como destino, assim teremos certeza de que o vizinho correto irá receber os pacotes e encaminhá-los até a rede de destino.

Lembre-se que o IP do próximo salto **SEMPRE** será um IP de um roteador vizinho pertencente a uma rede diretamente conectada, não utiliza IPs de redes remotas.

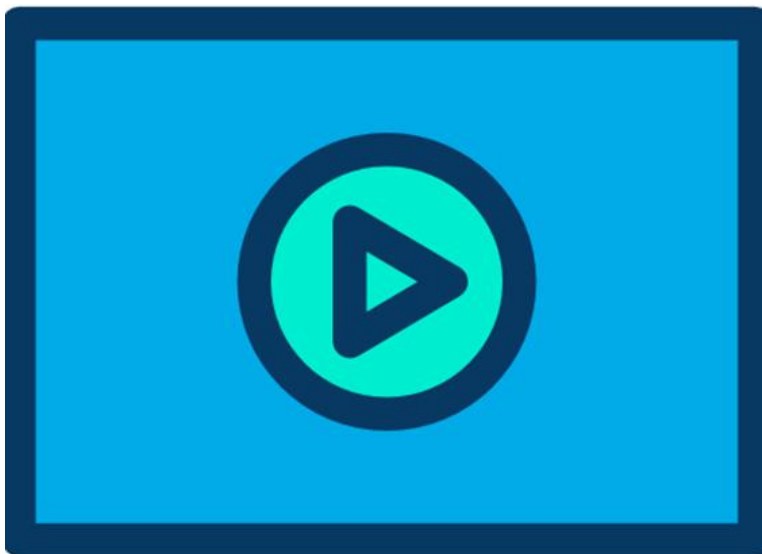
Outro ponto interessante é que ao configurarmos rotas estáticas apontando para interfaces o Cisco IOS remove e insere a rota automaticamente conforme a interface de saída fica UP ou Down.

Você pode fazer com que a rota nunca saia da tabela de roteamento com a opção **“permanent”** no final do comando, veja exemplo a seguir.

```
R1(config)#ip route 10.0.0.0 255.0.0.0 fast 0/0 ?
<1-255>      Distance metric for this route
  A.B.C.D     Forwarding router's address
  DHCP        Default Gateway obtained from DHCP
  multicast    multicast route
  name         Specify name of the next hop
permanent     permanent route
  tag          Set tag for this route
  track        Install route depending on tracked item
<cr>
```

```
R1(config)#ip route 10.0.0.0 255.0.0.0 fast 0/0 permanent
```

5.5 Configurando uma Rota Padrão (Default-Gateway)



A rota padrão ou Gateway of last resort nos roteadores tem a função de ser o IP para qual o equipamento vai enviar os pacotes quando não houver uma entrada na tabela de roteamento.

Quando um roteador recebe um pacote para encaminhar ele analisa a rede de destino e busca em sua tabela de roteamento uma rota correspondente.

Sem uma rota padrão o roteador irá buscar a rota para determinado endereço em sua tabela de roteamento e caso não seja encontrada, o pacote será descartado.

Por esse motivo a rota padrão é intitulada muitas vezes como a “**saída para internet**” ou **saída padrão**, pois quando não há rota específica para a rede de destino o pacote é encaminhado para ela.

Nos roteadores ela deve ser configurada com uma rota estática para a rede 0.0.0.0 com máscara 0.0.0.0, ou seja, todos os IP's menos os que ele conhece na tabela de roteamento.

Para a configuração de um gateway default você pode utilizar o comando visto nos tópicos anteriores “ip route 0.0.0.0 0.0.0.0 interface/gateway”. Abaixo segue mais um exemplo prático onde o gateway default é o IP 10.0.1.20:

```
R1720A(config)#ip route 0.0.0.0 0.0.0.0 10.0.1.20
```


Na tabela de roteamento você reconhecerá a rota padrão com um asterisco (*) ao lado dela, além de aparecer o IP no campo "Gateway of last resort is...", conforme figura ao lado.

```
R1720A(config)#ip route 0.0.0.0 0.0.0.0 10.0.1.20
R1720A(config)#end

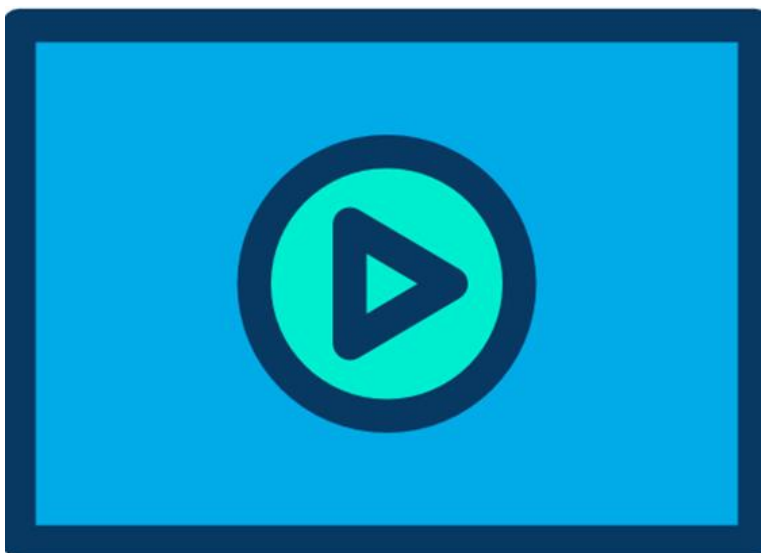
R1720A#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
Gateway of last resort is 10.0.1.20 to network 0.0.0.0
 10.0.0.0/24 is subnetted, 2 subnets
C    10.0.1.0 is directly connected, FastEthernet0/0
S*   0.0.0.0/0 [1/0] via 10.0.1.20
R1720A#
```

O maior cuidado que se deve ter com a configuração das rotas padrões é a de não causar **loops de roteamento** entre dois roteadores.

Por exemplo, se em um roteador você criar uma rota padrão apontando para a interface do vizinho e no vizinho criar uma rota apontando para o primeiro router, quando um dos dois enviar um pacote não conhecido nas tabelas de roteamento dos dois, um ficará enviando para o outro o mesmo pacote até que o TTL padrão configurado pelo protocolo IP seja esgotado.

Apesar de ser um problema simples acontece muito na prática.

5.6 Rota Estática Flutuante (Floating Static)



As rotas estáticas flutuantes são utilizadas para servirem como backup de uma rota principal, a qual pode ser uma outra rota estática ou uma rota aprendida através de um protocolo de roteamento dinâmico.

O segredo da configuração de rotas estáticas flutuantes ou "floating static" é o uso correto do parâmetro "administrative distance" (AD ou distância administrativa) que existe na configuração das rotas estáticas no comando "ip route".

Para que a rota seja flutuante ou backup sua distância administrativa deve ser maior que o AD da rota principal, pois quanto menor a distância administrativa melhor será a rota para o roteador.

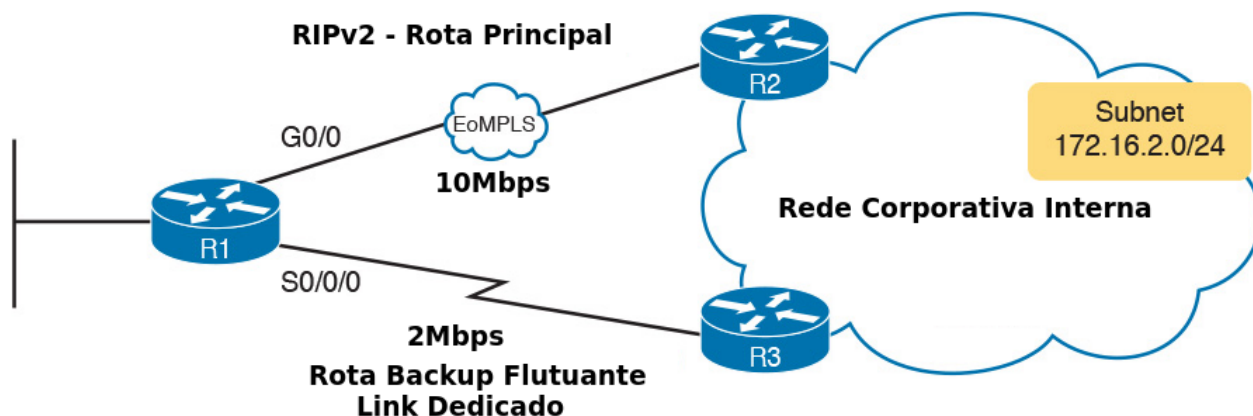
Por exemplo, por padrão o AD de uma rota estática que aponta para um IP do próximo salto é 1, se temos que criar uma rota flutuante para o mesmo destino basta colocar o AD dessa segunda rota maior que 1. Veja abaixo.

```
R1(config)#ip route 0.0.0.0 0.0.0.0 serial0/0
R1(config)#ip route 0.0.0.0 0.0.0.0 serial0/1 100
```

Nesse exemplo teremos a rota principal para a Internet apontando para serial0/0 e a rota apontando para serial0/1 ficará como stand-by, pois seu AD é 100 e maior que da rota principal que é 1.

Caso a rota principal via interface serial0/0 caia, imediatamente o roteador subirá a saída para a Internet via serial0/1, a qual estava configurada, mas não ativa na tabela de roteamento, por isso o nome "flutuante".

Esse mesmo tipo de configuração pode ser utilizado em conjunto com protocolos de roteamento dinâmico como RIP (AD 120), EIGRP (AD 90) e OSPF (AD 110). Veja exemplo na figura abaixo.



Como o RIP tem distância administrativa 120, para criar uma rota backup flutuante via serial 0/0/0 podemos utilizar um AD 130, por exemplo. Veja a configuração abaixo:

```
R1(config)#ip route 172.16.2.0 255.255.255.0 s0/0/0 130
```

Se a rota do RIP cair vamos ter as seguintes saídas na tabela de roteamento.

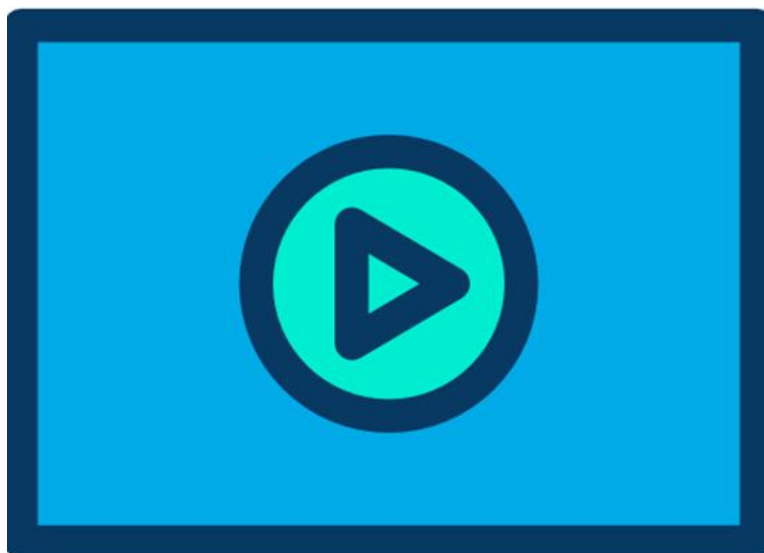
```
R1# show ip route static
! Saída omitida...

172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
S 172.16.2.0/24 is directly connected, Serial0/0/0

R1# show ip route 172.16.2.0
Routing entry for 172.16.2.0/24
Known via "static", distance 130, metric 0 (connected)
Routing Descriptor Blocks:
* directly connected, via Serial0/0/0
Route metric is 0, traffic share count is 1
```

Para verificar a distância administrativa da rota utilizamos o comando "show ip route" seguido da rota em questão 172.16.2.0.

5.7 Rotas Estáticas de Host ou Host-Route



Outra configuração interessante é a criação de uma rota para **um host específico ou Host Route**, por exemplo, você deseja alcançar um host de IP 200.150.160.1/24 que está conectado a sua interface fastethernet mas a rede dele não está presente em sua tabela de roteamento, o seguinte comando pode ser utilizado:

```
R1720A(config)#ip route 200.150.160.1 255.255.255.255 fastEthernet 0
```

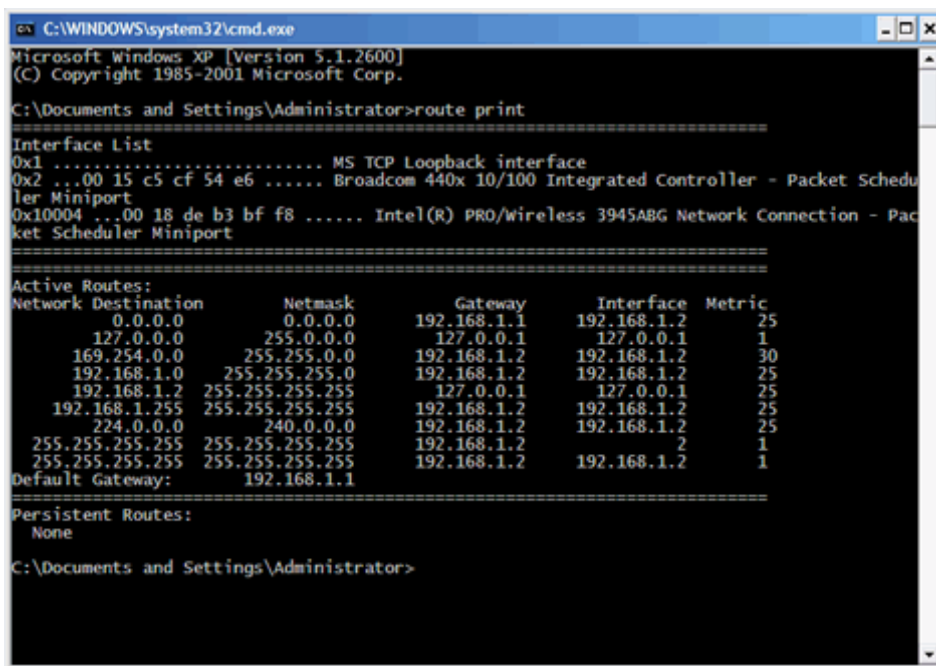
Note que a máscara de rede utilizada foi uma /32 e não a /24, pois a /32 é a qual especifica um host único.

Portanto uma rota estática IPv4 utilizando uma máscara /32 representa uma Host-Route!

5.8 Bônus: Roteamento em Clientes de Rede

O processo de roteamento dos roteadores normalmente é bem mais complexo que o realizado em computadores clientes, pois alguns servidores também podem fazer o papel de roteador.

Até mesmo seu computador possui uma tabela de roteamento. Para você visualizá-la basta abrir o prompt de comando e digitar o comando **"route print"** no Windows. Veja a figura abaixo e note que várias rotas estão presentes em um computador.



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>route print

=====
Interface List
=====
0x1 ..... MS TCP Loopback interface
0x2 ...00 15 c5 cf 54 e6 ..... Broadcom 440x 10/100 Integrated Controller - Packet Scheduler Miniport
0x10004 ...00 18 de b3 bf f8 ..... Intel(R) PRO/Wireless 3945ABG Network Connection - Packet Scheduler Miniport
=====

Active Routes:
Network Destination    Netmask          Gateway         Interface        Metric
0.0.0.0                0.0.0.0          192.168.1.1     192.168.1.2      25
127.0.0.0              255.0.0.0        127.0.0.1      127.0.0.1        1
169.254.0.0            255.255.0.0      192.168.1.2     192.168.1.2      30
192.168.1.0            255.255.255.0    192.168.1.2     192.168.1.2      25
192.168.1.2            255.255.255.255  127.0.0.1      127.0.0.1        25
192.168.1.255          255.255.255.255  192.168.1.2     192.168.1.2      25
224.0.0.0              240.0.0.0        192.168.1.2     192.168.1.2      25
255.255.255.255        255.255.255.255  192.168.1.2     192.168.1.2      2
255.255.255.255        255.255.255.255  192.168.1.2     192.168.1.2      1
Default Gateway:       192.168.1.1

Persistent Routes:
None

C:\Documents and Settings\Administrator>
```

Por exemplo, a rota para a rede (Network Destination) **"0.0.0.0"** com máscara (Netmask) **"0.0.0.0"** representa a saída para Internet, ou seja, está indicando para onde os pacotes de redes desconhecidas devem ser encaminhados. Se a rede de destino não estiver contida em nenhuma das rotas contida na tabela ele enviará o pacote para esse **gateway** com IP 192.168.1.1.

Note que na segunda linha temos uma rota para a rede de Loopback 127.0.0.1, logo abaixo uma rota para a rede Zeroconf 169.254.0.0 e a seguir para a rede em que o computador está alocado que é a 192.168.1.0 com máscara 255.255.255.0.

Logo abaixo da entrada para a rede 192.168.1.0 temos o IP do próprio computador configurado com uma máscara que chamados de "máscara de host", porque ela tem todos os bits configurados em um (255.255.255.255). Note que os campos gateway e interface apontam para o IP de loopback 127.0.0.1, o que representa que essa é uma interface local.

No Linux e MAC OS-X o comando a ser utilizado é o **"netstat -rs"**, porém as saídas e redes padrões são bem semelhantes ao que observamos para um computador padrão Windows.

É importante ter em mente que maioria das redes os clientes não irão conhecer rotas ou encaminhar pacotes entre diferentes redes, eles apenas recebem um endereço de gateway através do serviço de DHCP e quando não conhecem uma rede de destino encaminham os pacotes para esse gateway, o qual fará o papel de intermediário entre os dispositivos de uma LAN e o mundo externo, seja ele outras redes da Intranet ou até mesmo a Internet.

5.8.1 Problemas Comuns de Alcançabilidade em Clientes

Os problemas mais comuns em clientes quando estamos estudando roteamento são relacionados à parte física, ou seja, cabos rompidos ou com problemas intermitentes, de conectividade com o servidor DHCP ou com o servidor DNS.

Quando temos um cabo rompido ou com intermitência, haverá um aviso de conectividade que maioria dos sistemas operacionais fornece em sua interface gráfica para indicar um cabo desconectado.

Se o cabo estiver conectado e mesmo assim o computador apresenta problemas alguns testes devem ser realizados para identificar onde o problema de acesso a serviços da Intranet ou Internet está acontecendo. Uma metodologia interessante de ser utilizada é seguir os passos abaixo:

1. Fazer ping para o endereço de Loopback para detectar problemas com a própria interface de rede do computador. Se o teste for bem sucedido passe para o próximo teste.
2. Utilizar o comando `ipconfig/ifconfig` e verificar se o computador conseguiu pegar endereço via DHCP.
3. Se aparecer na configuração um endereço da rede 169.254.0.0 é sinal de que o computador não conseguiu adquirir endereço via DHCP e se autoconfigurou.
4. Utilize os comandos em máquinas Windows **`ipconfig /release`** e **`ipconfig /renew`** liberar e tentar renovar o endereço IP com o servidor DHCP. Se mesmo assim o computador não pegar um IP esperado via DHCP o problema ainda pode ser físico ou o cabo do switch foi conectado a uma porta errada, por exemplo.
5. Caso a aplicação dos comandos do item 4 resultou em um IP que você sabe que é da rede daquele computador é sinal de que a renovação de IP solucionou o problema inicial. Agora vamos utilizar o ping para testar a conectividade da seguinte maneira:
 - a. Primeiro pingar o próprio IP, basicamente é o mesmo teste do passo 1;
 - b. Em segundo lugar pingar o gateway;
 - c. Por último pingar o endereço ou os endereços do DNS, pois normalmente pode haver um DNS primário (principal) e um secundário.

Se o próprio IP da máquina não pingar é aconselhável verificar o driver da placa de rede. Se o gateway não responder pode ter algum filtro (firewall) ou problema em algum dos sentidos da comunicação. Se ambos pingarem você pode testar pingar para outros endereços da sua Intranet.

Se o DNS não pingar está descoberto o problema de acesso do computador, nesse caso o administrador de redes deve verificar se é um problema isolado, ou seja, somente do computador em questão, ou generalizado em todos ou um grupo de usuários para poder identificar quais os próximos passos a serem tomados.

Caso os três testes funcionem significa que pode estar havendo uma filtragem do tráfego que o usuário está tentando realizar ou então simplesmente o serviço que ele está acessando está indisponível. Você pode utilizar o computador de outro usuário na mesma sub-rede e realizar o teste de acesso que o usuário com problemas está tentando realizar e verificar se é um problema com o micro dele ou em outras máquinas acontece o mesmo.

Além disso, é interessante verificar se o acesso que ele está dizendo que não funciona está permitido pela política da empresa, às vezes é um bloqueio padrão.

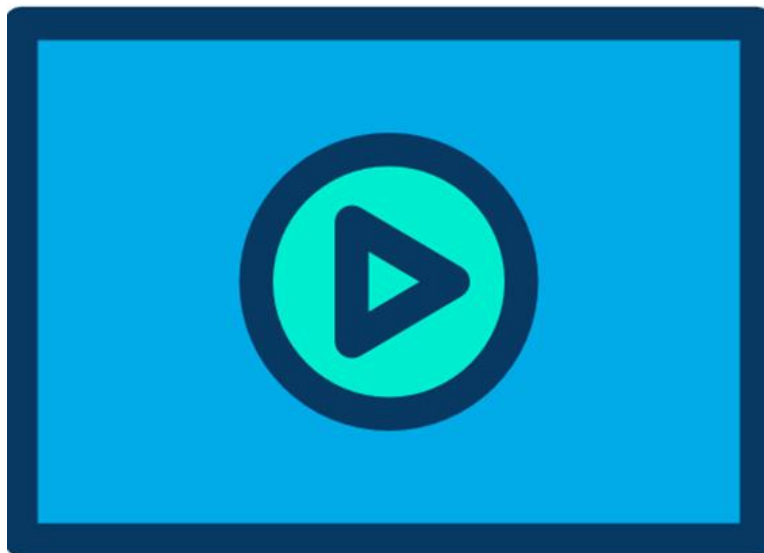
6 Roteamento Estático com IPv6

6.1 Introdução



Agora vamos estudar as configurações de roteamento estático para IPv6, o qual é o foco do CCNA.

6.2 O Comando "ipv6 route"



As rotas estáticas e/ou padrões para o IPv6 são configuradas com o comando "**ipv6 route**".

A sintaxe do comando segue abaixo e tem algumas opções a mais em relação ao IPv4:

```
Router(config)#ipv6 route ipv6-prefix/prefix-length {ipv6-address | interface-  
type interface-number [ipv6-address]} [administrative-distance] [administrative-  
multicast-distance unicast multicast] [track track-number] [tag tag]
```


Note que ao invés de rede e máscara (Network e Mask) para o IPv4, agora no IPv6 temos "ipv6-prefix/prefix-length" separados por uma barra.

Na sequência temos a saída dos pacotes que ainda podem ser um endereço IPv6 remoto (ipv6-address) ou interface de saída (interface-type interface-number [ipv6-address]).

Note que na interface de saída existe a opção de ser especificado um endereço IPv6.

Um detalhe importante sobre isso é que se o endereço IP de próximo salto for um Link Local (FE80) você precisará especificar a interface de saída no comando.

Em seguida temos as opções:

- [administrative-distance]: distância administrativa da rota (padrão 1)
- [administrative-multicast-distance unicast multicast]: distância administrativa para multicast (não faz parte do CCNA)
- [tag tag]: marcação da rota (não faz parte do CCNA)
- [track track-number]: número utilizado pelo IP SLA monitorar a rota (será utilizado em capítulo posterior)

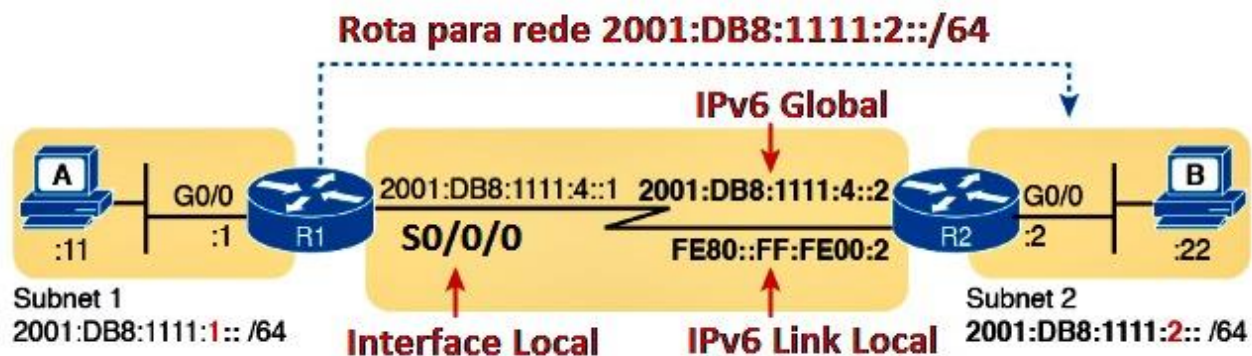
Podem aparecer mais opções dependendo da versão do Cisco IOS, porém para o CCNA essas são suficientes.

Vamos analisar isso durante as configurações dos diferentes tipos de rotas estáticas para o IPv6.

6.3 Criando Network Routes

Assim como para o IPv4 podemos configurar uma rota estática no IPv6 apontando para o IP de próximo salto (diretamente conectado) ou para a interface local de saída.

Veja a representação na imagem abaixo.



Por exemplo, para criar uma rota no roteador R1 para a rede remota 2001:DB8:1111:2::/64 você pode utilizar como referência a interface serial local S0/0/0 ou um dos IPs versões 6 remotos, tanto o de link local, que inicia como FE80, como o Unique Global 2001:DB8:1111:4::2.

O comando poderia ser quaisquer uma das alternativas abaixo:

- Ipv6 route 2001:DB8:1111:2::/64 S0/0/0
- Ipv6 route 2001:DB8:1111:2::/64 S0/0/0 FE80::FF:FE00:2
- Ipv6 route 2001:DB8:1111:2::/64 2001:DB8:1111:4::2

Note que quando utilizamos o endereço de link local precisamos especificar antes qual a interface de saída dele, pois ele não é como o endereço global que deve ser único na rede IPv6 toda, ele precisa ser único apenas na sua rede local, por isso é preciso informar a interface de saída também.

Veja um exemplo abaixo onde será criada a rota para a rede 2000::/64 através da serial 0/0/0:

```
dltec(config)#ipv6 route 2000::/64 serial 0/0/0
```

Quando utilizamos como destino um IPv6 de próximo salto um link-local precisaremos também definir a interface de saída dessa rota, pois a rede FE80::/10 pertence à todas as interfaces.

```
R1(config)#ipv6 route 2000::/64 fe80::1
% Interface has to be specified for a link-local nexthop
R1(config)#ipv6 route 2000::/64 fast 0/0 fe80::1
R1(config)#
```

Note acima que ao tentar criar uma rota apontando para o endereço FE80::1 recebemos uma mensagem que para o link local precisamos definir a interface de saída.

Veja que a mesma configuração apontando para o IP global pode ou não ter a interface de saída definida, os dois métodos são aceitos:

```
R1(config)#ipv6 route 2000::/64 fast 0/0 2000::1
R1(config)#ipv6 route 2000::/64 2000::1
```

Com o comando "show ipv6 route" podemos visualizar a tabela de roteamento IPv6.

```
dltec#sho ipv6 route
IPv6 Routing Table - default - 4 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
        B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP
        I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
        D - EIGRP, EX - EIGRP external, ND - Neighbor Discovery
S   2000::/64 [1/0], tag 2
    via FastEthernet0/0, directly connected
S   2001:DB8:1::/64 [1/0]
    via 2001:DB8:1::1, FastEthernet0/0
S   2001:DB8:42:1::/64 [1/0]
    via Null0, directly connected
L   FF00::/8 [0/0]
    via Null0, receive
dltec#
```

As regras de distância administrativa no IPv6 são iguais às que estudamos para o IPv4, ou seja, rotas estáticas que apontam para uma interface de saída tem AD 1 e são marcadas como se fossem diretamente conectadas "directly connected" na linha abaixo da rota na tabela de roteamento.

Já rotas que apontam para o próximo salto tem AD 1 por padrão e informam o IP do próximo salto logo abaixo da rota na tabela de roteamento.

6.4 Criando Rotas Padrões



Para criar uma rota padrão para o roteador IPv6 é só criar uma rota estática conforme criamos anteriormente apontando para a rede `::/0`. Veja exemplo abaixo.

```
R1(config)#ipv6 route ::/0 fast 0/0 2000::1
```

A configuração acima é bem interessante e vale também para uma rota estática normal, não somente para a padrão, pois em uma interface LAN temos diversos endereços e ao definirmos além da interface fast também o IPv6 remoto resolvemos o problema de alcance e vinculamos a interface da rota.

Veja saída do `show ip route` com os comandos aplicados anteriormente e note que o roteador padrão no IPv6 não aparece com a mensagem de "Gateway of last resort" como tínhamos na tabela do IPv4.

```
R1#show ipv6 route
IPv6 Routing Table - 8 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
S    ::/0 [1/0]
    via 2000::1, FastEthernet0/0
S    2000::/64 [1/0]
    via ::, Serial0/0
    via FE80::1, FastEthernet0/0
C    2340:1111:AAAA:1::/64 [0/0]
    via ::, FastEthernet0/0
L    2340:1111:AAAA:1::1/128 [0/0]
    via ::, FastEthernet0/0
C    2340:1111:AAAA:2::/64 [0/0]
    via ::, Serial0/0
L    2340:1111:AAAA:2::1/128 [0/0]
    via ::, Serial0/0
S    2340:1111:AAAA:3::/64 [1/0]
    via ::, Serial0/0
```

```
L   FF00::/8 [0/0]
    via ::, Null0
R1#
```

Você pode também criar rotas padrões com os exemplos dados no tópico anterior, apontando diretamente para uma interface serial, para um IPv6 global de próximo salto ou para um endereço de Link Local e sua interface de saída. Veja exemplos abaixo:

- Ipv6 route ::/0 S0/0/0
- Ipv6 route ::/0 S0/0/0 FE80::FF:FE00:2
- Ipv6 route ::/0 2001:DB8:1111:4::2

6.4.1 Rota Padrão via SLAAC e Autoconfiguração

Outra forma que um roteador pode adquirir uma rota padrão é automaticamente através do SLAAC, ou seja, na autoconfiguração. Lembre-se que via NDP na autoconfiguração o roteador aprenderá os seguintes itens:

- **Endereço da interface:** utilizando o processo do SLAAC autoconfigura sua interface conforme prefixo passado na mensagem de RA.
- **Rota Local /128:** o roteador adiciona uma rota local (/128) para o endereço autoconfigurado, assim como é feito com quaisquer endereços locais das interfaces.
- **Prefixo da Rota Conectada:** adiciona o prefixo da rota diretamente conectada (/64) aprendida pela mensagem de RA via NDP.
- **Default route:** R1 adiciona a rota padrão com prefixo ::/0 apontando para o próximo salto que é o roteador que enviou a mensagem de resposta do processo de SLAAC.

Veja exemplo a seguir, onde os roteadores R1 e R2 estão diretamente conectados via Interface Giga 1/0. R1 será o roteador local e R2 será configurado com autoconfiguração.

Vamos começar por R1, o qual será o roteador que passará o prefixo da rede na LAN via SLAAC.

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ipv6 unicast-routing
R1(config)#int g1/0
R1(config-if)#ipv6 enable
R1(config-if)#ipv6 address 2000::1/64
R1(config-if)#no shut
R1(config-if)#end
R1#
```

Agora segue a configuração de R2, onde ele terá sua interface configurada via autoconfig e também com a opção para pegar a rota padrão (default).

```
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#ipv6 unicast-routing
R2(config)#int g1/0
R2(config-if)#ipv6 enable
R2(config-if)#ipv6 address ?
WORD                                General prefix name
X:X:X:X::X                          IPv6 link-local address
X:X:X:X::X/<0-128>                   IPv6 prefix
autoconfig                          Obtain address using autoconfiguration
dhcp                                 Obtain a ipv6 address using dhcp

R2(config-if)#ipv6 address autoconfig ?
default  Insert default route
<cr>
```

```
R2(config-if)#ipv6 address autoconfig default
R2(config-if)#end
R2#
```

Veja a saída da tabela de roteamento de R2 com as informações pegadas via autoconfiguração passadas pela NDP através de R1.

```
R2#sho ipv6 route
IPv6 Routing Table - default - 4 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
        B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP
        I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
        D - EIGRP, EX - EIGRP external, NM - NEMO, ND - Neighbor Discovery
        l - LISP
        O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
        ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
S   ::/0 [2/0]
    via FE80::C800:5FF:FE54:1C, GigabitEthernet1/0
C   2000::/64 [0/0]
    via GigabitEthernet1/0, directly connected
L   2000::C801:20FF:FEA8:1C/128 [0/0]
    via GigabitEthernet1/0, receive
L   FF00::/8 [0/0]
    via Null0, receive
```

Note que a rota padrão tem distância administrativa 2, pois esse é o valor da rota aprendida via NDP. Essa é uma das poucas diferenças do IPv6, as demais distâncias administrativas são as mesmas estudadas para o IPv4.

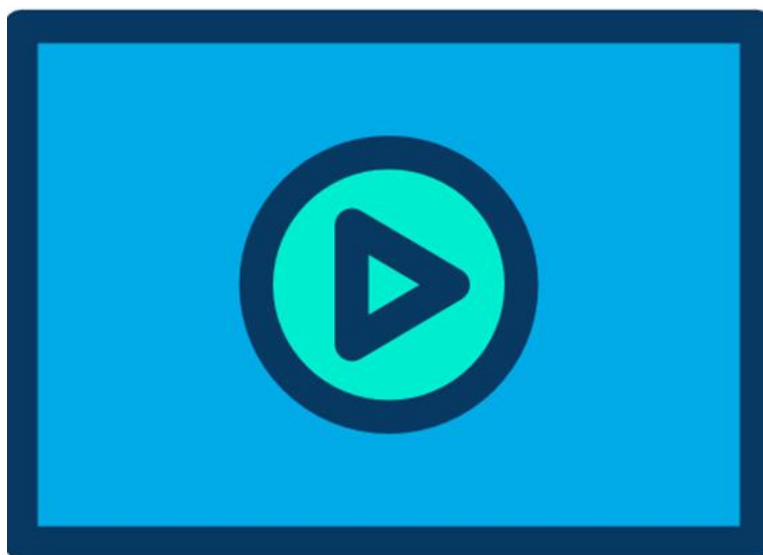
Logo após vem a informação do prefixo 2000::/64 aprendido via NDP e na sequência o endereço IPv6 autoconfigurado na Interface via EUI-64 (2000::C801:20FF:FEA8:1C/128), inserido como uma rota local (L).

Em versões de Cisco IOS mais atuais você pode encontrar as duas primeiras informações anteriores com um índice diferente, pois a rota padrão pode ser marcada como "ND" ao invés de estática, assim como o prefixo local pode ser aprendido como "NDp" ao invés de diretamente conectado (C). Veja exemplo abaixo.

```
R2#sho ipv6 route
### Saídas Omitidas ###
ND   ::/0 [2/0]
      via FE80::C800:5FF:FE54:1C, GigabitEthernet1/0
NDp  2000::/64 [2/0]
      via GigabitEthernet1/0, directly connected
L    2000::C801:20FF:FEA8:1C/128 [0/0]
      via GigabitEthernet1/0, receive
L    FF00::/8 [0/0]
      via Null0, receive
```

Note que nesse caso a distância administrativa do prefixo local também é passado de zero para 2, o qual é a AD do NDP.

6.5 Criando Rotas Estáticas Flutuantes no IPv6

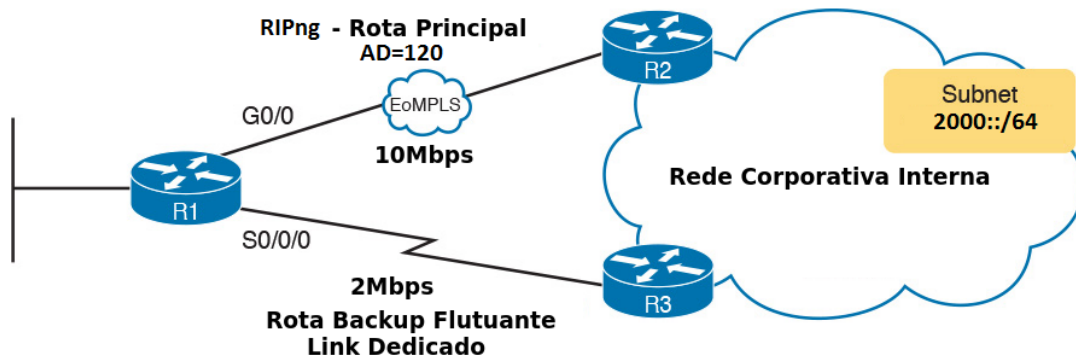


O mesmo princípio que utilizamos para criar rotas backup flutuantes para o IPv4 funciona aqui no IPv6.

Portanto se quisermos ter uma rota reserva em standby para outros protocolos de roteamento ou até mesmo para uma rota estática principal basta alterar a distância administrativa da rota estática reserva para que ela seja maior que a principal.

Por exemplo, se a rota reserva for para o protocolo RIPng (versão do IPv6 do RIPv2) basta colocarmos a AD como 130, pois a AD do RIPng é 120, assim como do RIPv2. O mesmo serve para o EIGRPv6 que tem AD 90, portanto uma rota estática com AD 91 já serviria como reserva, ou então para o OSPFv3 que tem AD 110, nesse caso uma rota com AD 111 já serviria como reserva.

Veja exemplo abaixo com a mesma topologia que utilizamos para o IPv4, mas agora aplicada ao IPv6. A seguir apresentaremos a configuração da rota flutuante de R1.



```
R1(config)#ipv6 route 2000::/64 S0/0/0 130
```

Com os comandos `show ipv6 route` e `show ipv6 route 2000::/64` você pode verificar a tabela de roteamento completa e a informação específica da rota para 2000::/64. Se você derrubar a interface principal G0/0 vai ter as saídas abaixo.

```
R1# show ipv6 route static
```

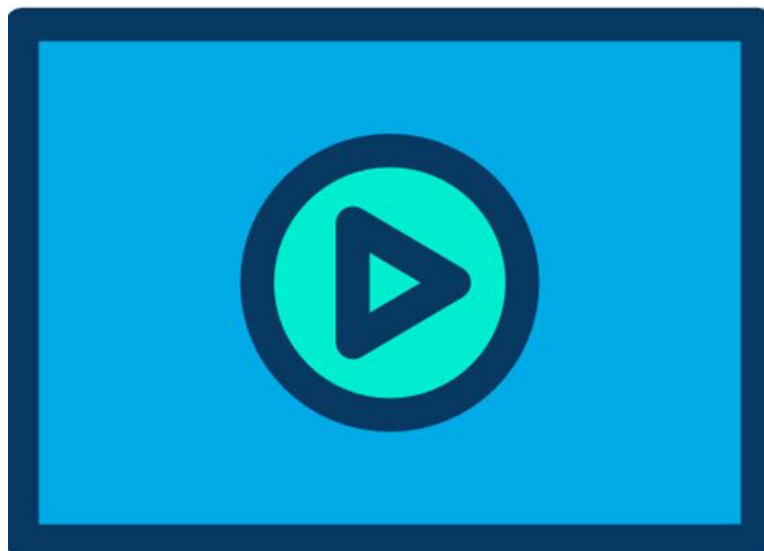
```
### Saídas Omitidas ###
```

```
S 2000::/64 [130/0]  
via 2000::2
```

```
R1# show ipv6 route 2000::/64
```

```
Routing entry for 2000::/64  
Known via "static", distance 130, metric 0  
Route count is 1/1, share count 0  
Routing paths:  
2000::2  
Last updated 00:01:35 ago
```

6.6 Criando Rota de Host no IPv6



Assim como estudamos para o IPv4, o IPv6 também permite a criação de rotas estáticas para hosts específicos, basta utilizar a máscara /128, pois é a quantidade de bits que um host utiliza.

Se você lembrar para o IPv4 utilizávamos a máscara /32, que é o tamanho completo da máscara do IPv4.

As regras de criação desse tipo de rota podem ser quaisquer uma das estudadas anteriormente, por exemplo, veja abaixo uma rota para o host 2001::100/128 criada utilizando o endereço global local 2000::10.

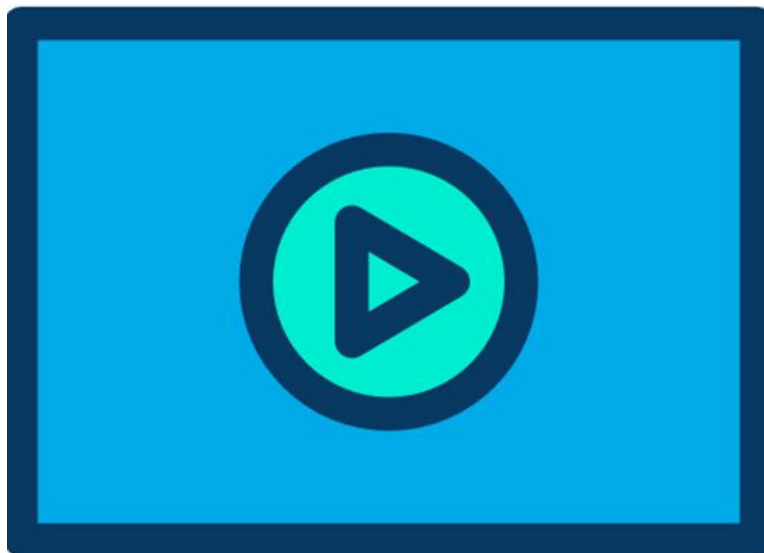
```
R1(config)#ipv6 route 2001::100/128 2001::10
```

Veja outro exemplo apontando para o endereço de link local.

```
R1(config)#ipv6 route 2001::100/128 giga0/0 FE80::10
```

7 Conceitos de Roteamento Dinâmico

7.1 Introdução



Nos capítulos anteriores estudamos o roteamento local (rotas diretamente conectadas) e como rotear entre dois pontos utilizando rotas estáticas.

Também aprendemos que as rotas estáticas são bastante **leves** para o roteador, pois quem faz o trabalho de “pensar” e “calcular” as melhores rotas é o administrador de redes, por isso elas são econômicas em termos de uso da memória RAM e CPU.

Mas e se a topologia contiver **50 roteadores** cada um com **10 rotas**, totalizando **500 rotas**, será que o roteamento estático é uma boa opção?

Com certeza não, pois o **trabalho manual** para criar novas rotas ou apagar rotas não utilizadas seria tão grande que não compensaria a economia de memória e CPU.

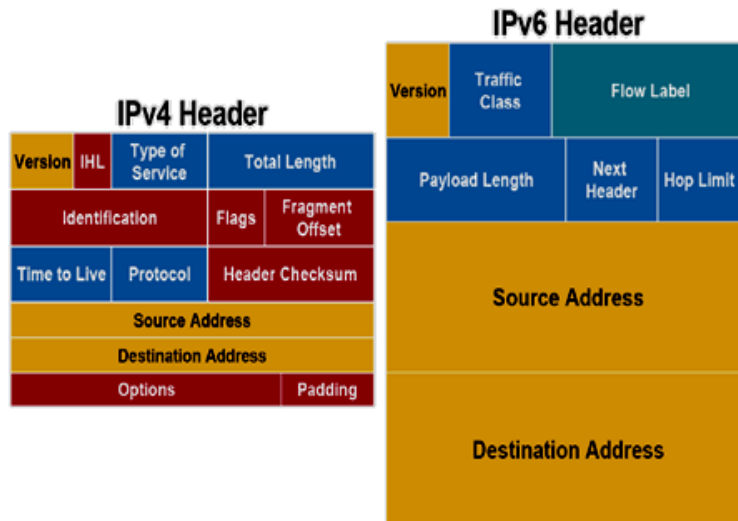
Quando a rede cresce e mais pontos são adicionados é recomendado utilizar um **protocolo de roteamento dinâmico**.

Com o roteamento dinâmico o administrador de redes faz uma **configuração inicial**, ensinando apenas as redes que devem participar do processo de roteamento e o resto **o próprio protocolo de roteamento trata** de maneira dinâmica.

Rotas inseridas ou apagadas das configurações com o protocolo de roteamento configurado são automaticamente inseridas ou excluídas nas tabelas de roteamento dos roteadores que estão participando daquele domínio de roteamento sem a intervenção do administrador.

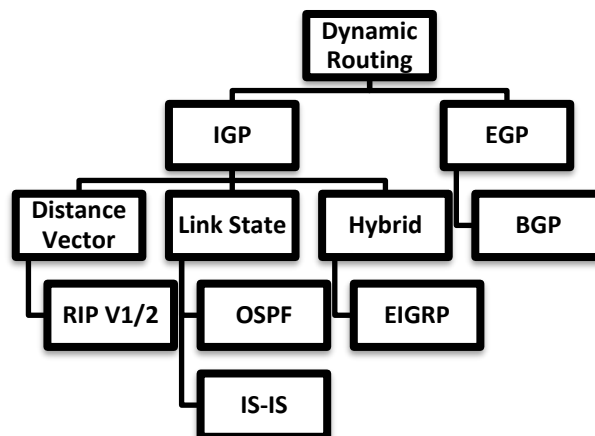
7.2 Protocolo de Roteamento versus Protocolo Roteado

Já estudamos que os protocolos IP versão 4 ou versão 6 são protocolos roteados ou roteáveis, pois eles por si só não descobrem rotas ou caminhos na rede.



Os protocolos IP versão 4 e 6 fornecem o formato dos pacotes e informações de controle.

Quem têm a função de ler esses protocolos roteados, ou seja, ler os endereços e redes IP configuradas e descobrir dinamicamente as melhores rotas são os protocolos de roteamento dinâmicos.



7.3 Funções de um Protocolo de Roteamento Dinâmico

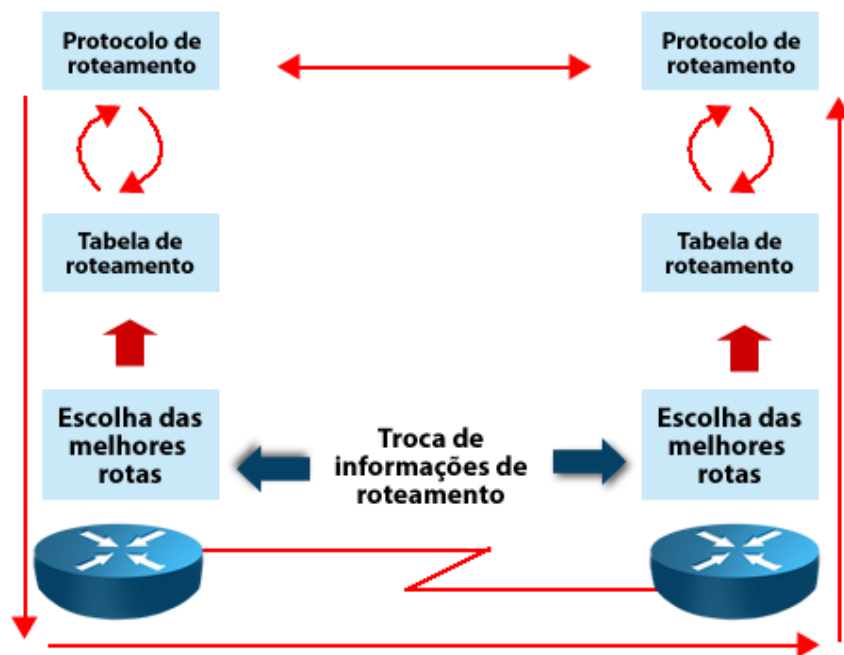
O funcionamento macro dos protocolos de roteamento é bem semelhante, pois eles são processos habilitados nos roteadores que coletam informações das suas redes diretamente conectadas, repassando essas informações aos demais roteadores da rede em momentos oportunos.

Com essas informações trocadas, um banco de dados é criado, analisado e através de um parâmetro de decisão chamado "**métrica**" a **melhor rota é inserida na tabela de roteamento**.

Podemos resumir as funções básicas dos protocolos de roteamento em:

- Aprender as informações de roteamento (sub-redes) dos seus vizinhos de rede;
- Ensinar a outros vizinhos sobre suas sub-redes e as demais aprendidas;
- Se mais de um caminho for descoberto utilizar a métrica como critério de desempate e incluir a rota na tabela de roteamento;
- Utilizar mecanismos que para os casos de mudanças na rede essas alterações sejam percebidas em sua própria tabela de roteamento e sejam repassadas aos vizinhos.

Veja a figura a seguir com uma ilustração das funções básicas de um protocolo de roteamento dinâmico.



Os protocolos de roteamento devem também atuar sobre **alterações na rede** por motivos de:

- **Problemas**, tais como **a queda de um link** de uma operadora ou um dispositivo que saiu do ar por falta de energia elétrica. Nesses casos a indisponibilidade daquelas redes deve ser refletida para todos os dispositivos.
- **Adição de novas redes** pelo administrador de redes, pois as redes são dinâmicas e novos pontos podem ser adicionados à topologia atual.
- **Exclusão de redes** pelo administrador de redes, pois assim como novas filiais podem ser criadas outras podem ser fechadas.

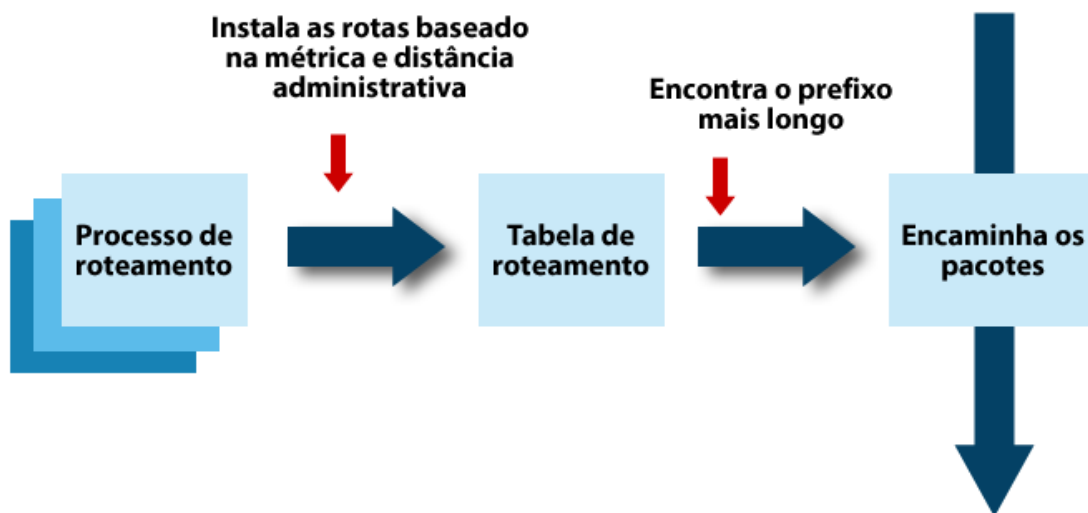
Atualmente na Internet o protocolo de roteamento utilizado é o BGP-4 (Border Gateway Protocol – versão 4).

Já nas Intranets utilizamos o RIP (versões 1 e 2), OSPF ou IS-IS que são protocolos abertos, ou seja, funcionam entre fabricantes diferentes, e existe também o protocolo proprietário da Cisco que é muito famoso chamado EIGRP.

Apesar de no início o EIGRP ser um protocolo proprietário, em 2013 a Cisco divulgou seu código, tornando o EIGRP de conhecimento público.

Portanto, temos protocolos para serem utilizados dentro dos sistemas autônomos, chamados de IGP, e para fazer a comunicação entre os sistemas autônomos, chamados de EGP.

Para resumir o funcionamento geral dos protocolos de roteamento veja a figura a seguir.



Um ou mais **processos de roteamento** podem ser ativados em um roteador, sendo que eles irão trocar informações e escolher internamente suas melhores rotas para cada destino baseado em uma "**métrica**" padrão que depende de cada protocolo.

Por exemplo, no RIP a melhor rota é a que tem menos saltos até o destino, já para o OSPF a melhor rota é a que tem menor custo (conta baseada no somatório da velocidade de cada link até o destino) sendo que a rota que tem a menor métrica (menor valor calculado) é considerada vencedora.

Caso tenhamos apenas um protocolo de roteamento habilitado essa rota com a menor métrica é instalada na tabela de roteamento.

Quando temos mais de um protocolo habilitado que vai para a tabela de roteamento é o que possui a menor **Distância Administrativa**, valor padrão utilizado para desempate entre protocolos diferentes (menor é melhor).

Uma vez decidida qual rota a ser utilizada ela é instalada na tabela de roteamento e a decisão sobre para que interface rotear é baseado no prefixo mais longo.

7.4 IGP versus EGP



Uma das classificações dos protocolos de roteamento é sobre onde ele é utilizado:

- **IGP – Interior Gateway Protocol:** protocolos utilizados dentro de um domínio de roteamento ou sistema autônomo.
- **EGP – Exterior Gateway Protocol:** protocolos utilizados para comunicação entre diferentes domínios de roteamento ou sistema autônomo.

Essa terminologia vem da Internet, a qual é uma rede mundial formada por diversas redes IP de empresas, provedores de serviços de Internet (ISP), entidades governamentais (como faculdades e redes de pesquisa) e outras entidades chamadas de **Sistemas Autônomos** (AS – Autonomous System).

Portanto, protocolos IGP são usados no interior dos sistemas autônomos e os EGP para conectar essas diversas entidades através da Internet.

O protocolo EGP atualmente utilizado é o BGP-4, todos os demais são IGPs (RIP, EIGRP, IS-IS e OSPFv2).

Falando sobre roteamento IPv6, basicamente os protocolos de roteamento IGP continuam com a mesma estrutura, ou seja, o RIP, EIGRP e OSPF utilizados no IPv4 foram adaptados para transportar e rotear prefixos de rede IPv6.

O nome dos protocolos mudou um pouco:

- RIP passa a se chamar RIPng e tem a mesma base do RIP versão 2.
- EIGRP passa a ser chamado de EIGRPv6.
- OSPFv2 ou OSPF agora passa a ser OSPFv3 para o IPv6.

O IS-IS e BGP não mudaram muito em sua estrutura, porém para eles serem capazes de rotear IPv6 foram necessárias extensões ao protocolo original.

7.5 Algoritmos dos Protocolos de Roteamento Dinâmicos

Cada protocolo de roteamento funciona segundo um **algoritmo** que dita como ele deve enviar suas informações, o que está contido nessas informações, quando enviá-las e assim por diante.

Basicamente podemos dividir os IGP's em três categorias:

- **Vetor de distância** (Distance Vector – RIP v1/v2, RIPng e IGRP)
- **Estado de enlace** (Link State ou SPF – OSPFv2, OSPFv3 e IS-IS)
- **Vetor de Distância Avançado ou Híbrido** (Advanced Distance Vector - EIGRP e EIGRPv6)

Já os EGP's (BGP) são considerados **Path Vector**.

Ser um protocolo vetor de distância ou Distance Vector significa que as rotas são anunciadas como vetores com uma distância e direção.

A distância é definida em termos de uma métrica, como contagem de saltos para o RIP, e a direção é simplesmente a interface de saída para esses pacotes.

Também é conhecido como algoritmo de Bellman-Ford.

Os protocolos de roteamento do vetor de distância pedem que o roteador anuncie periodicamente a tabela de roteamento inteira para cada um de seus vizinhos. As atualizações periódicas são enviadas em intervalos regulares (30 segundos para o RIP e 90 segundos para o IGRP).

Mesmo que a topologia não tenha sido alterada, as atualizações periódicas continuarão sendo enviadas a todos os vizinhos indefinidamente.

Os roteadores que usam roteamento do vetor de distância não conhecem a topologia da rede onde estão inseridos, pois eles têm apenas a visão da rede através de seus vizinhos diretamente conectados, as demais redes são vistas por eles através de uma interface de saída e uma métrica, porém sem conhecimento do caminho que o pacote fará até chegar ao seu destino.

Os protocolos de roteamento link-state também são conhecidos como protocolos de roteamento pelo caminho mais curto e são criados a partir do algoritmo SPF criado por Edsger Dijkstra, por isso pode ser chamado também de algoritmo de Dijkstra.

Os protocolos de roteamento link-state IP mais famosos são o Protocolo OSPF versão 2 (Open Shortest Path First) e o IS-IS (Intermediate-System-to-Intermediate-System).

Os protocolos de estado de enlace não trocam tabela de roteamento e sim mensagens sobre seus enlaces chamadas LSAs (Link State Advertisements).

Os protocolos híbridos ou vetores de distância avançados utilizam características dos vetores de distância e dos protocolos link-state, por isso o nome híbrido.

Como foi construído com mais características de vetores de distância que link-state recebe a designação de vetor de distância avançado.

7.6 Características Comuns dos IGP's

Existem algumas características que foram citadas sobre os protocolos de roteamento e a tabela abaixo resume o mais importante que pode ser cobrado em prova.

Protocolo	Tipo	Classful/ Classless	Métrica	Dist. Admi.	Escalabilidade	Tempo de convergência	Consumo de recurso
RIP v1	Distance Vector	Classful	Salto	120	15 saltos	Lento	Mem- baixo CPU – baixo BW – alto
RIP v2	Distance Vector	Classless	Salto	120	15 saltos	Lento	Mem- baixo CPU – baixo BW – alto
IGRP	Distance Vector	Classful	Banda passante, atraso, confiabilidade, carga	100	255 saltos	Rápido	Mem- baixo CPU – baixo BW – alto
EIGRP	Advanced Distance Vector ou Híbrido	Classless	Banda passante, atraso, confiabilidade, carga	90	Milhares de roteadores	Rápido	Mem- médio CPU – baixo BW – baixo
OSPF	Link State	Classless	Custo (depende fabricante)	110	Aprox. 50 roteadores por área	Rápido	Mem- alto CPU – alto BW – baixo

O IS-IS tem as mesmas características gerais do OSPF.

Além disso, o RIP-v1 não suporta sumarização e os demais protocolos suportam.

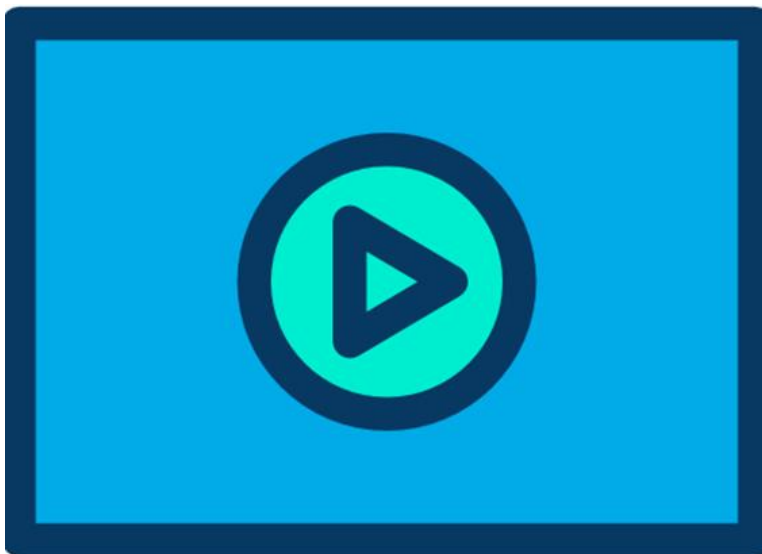
Também sobre a forma de envio de updates para os vizinhos, o RIPv1 e IGRP utilizam broadcast, já o EIGRP e OSPF utilizam multicast.

Lembrem que quando na tabela o protocolo é classificado como classful quer dizer que ele não envia a máscara na tabela de roteamento e por isso não suporta VLSM nem CIDR.

Os protocolos classless suportam VLSM e CIDR porque enviam a máscara em seus anúncios de roteamento.

A seguir vamos estudar um pouco mais das características dos protocolos Distance Vector, Advanced Distance Vector e Path Vector. As características do Link State serão estudadas em conjunto com o protocolo OSPF no próximo capítulo.

7.7 Funcionamento Básico de um Protocolo Distance Vector



Vamos estudar melhor o princípio de funcionamento do roteamento em protocolos Vetor de Distância analisando o funcionamento do RIP.

O RIP versões 1 e 2 utilizam o mesmo processo para determinar as melhores rotas e fazer com que as informações de roteamento de toda rede estejam consistentes, processo chamado de "convergência", onde todos os roteadores conhecem as mesmas informações sobre todas as redes.

Portanto, o RIP por padrão de 30 em 30 segundos envia sua tabela de roteamento para seus vizinhos diretamente conectados.

Quando ele recebe uma tabela de roteamento de um dos seus vizinhos ele analisa as redes recebidas, compara com sua própria tabela de roteamento e verifica se as rotas recebidas através de seu vizinho estão ou não presentes em sua tabela.

Caso a rota não esteja presente, o roteador insere a rota em sua tabela de roteamento, vinculando um "vetor", ou seja, a interface que ele alcança essa rede inserida na tabela de roteamento.

Se a rota já existe em sua tabela de roteamento existem três possibilidades:

1. A rede recebida tem a métrica maior que a rota que está em sua tabela de roteamento? Nesse caso o roteador descarta a informação e mantém a sua própria rota, pois a métrica é pior do que a já inserida em sua tabela.
2. A rede recebida tem métrica menor que a inserida em sua tabela de roteamento? Nesse caso ela é melhor que a rota anterior e o roteador descarta a informação atual, inserindo essa nova rota em sua tabela de roteamento.
3. A rota tem métrica igual à rota que está atualmente inserida na tabela de roteamento? Nesse caso o roteador fará por padrão o balanceamento de carga e deixará ambas as entradas na tabela de roteamento. Por padrão os roteadores RIP fazem balanceamento de carga com até quatro rotas de métricas iguais.

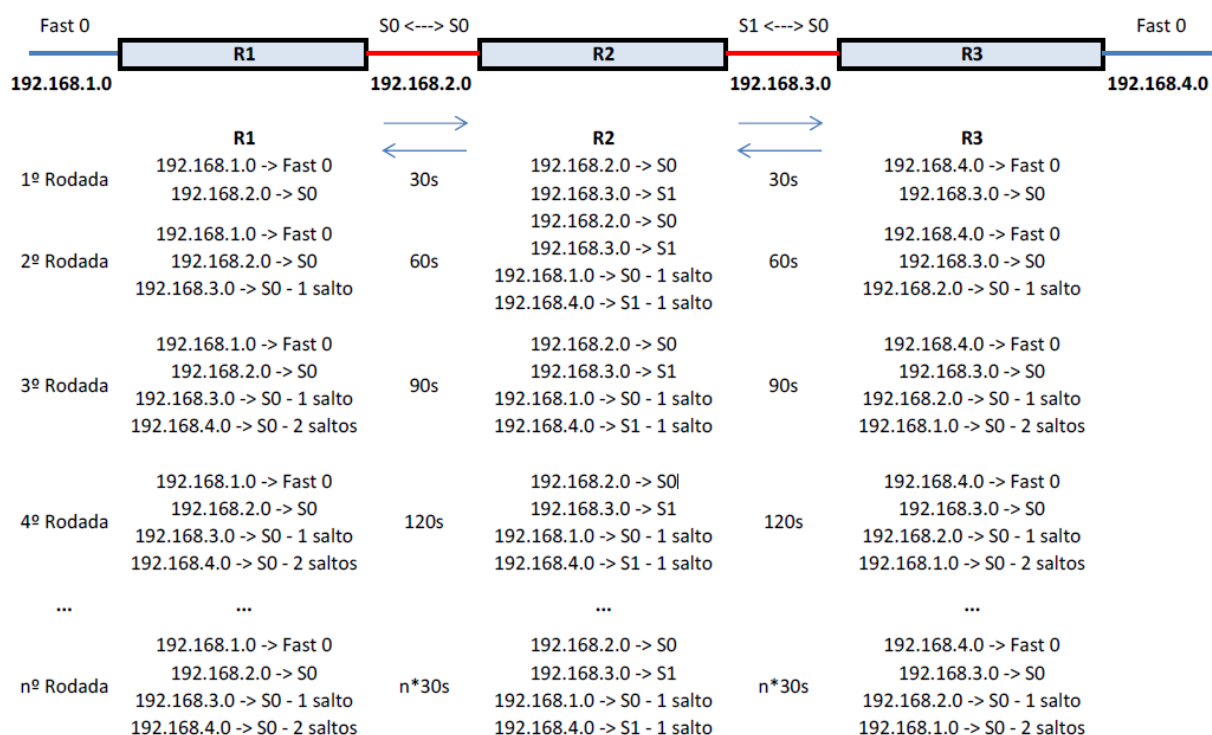
Portanto, o processo de convergência do RIP é incremental e a cada rodada de envio e recebimento de tabelas entre os vizinhos os roteadores vão conhecendo mais informações até o momento que eles conhecem informações de todas as redes.

É importante lembrar que no início os roteadores conhecem apenas as redes diretamente conectadas.

Quando ativamos o RIP os roteadores mandam na primeira rodada as redes diretamente conectadas aos seus vizinhos.

Na segunda rodada eles já conhecem suas redes conectadas e as redes de seus vizinhos.

Na terceira rodada eles irão conhecer as redes de três saltos, ou seja, até os vizinhos de seus vizinhos, e assim vai até conhecerem todas as redes com um limite de 15 saltos de profundidade. Veja a figura a seguir que ilustra esse processo.



Vamos analisar a convergência no roteador R1, na primeira atualização ele envia as redes dele mesmo e recebe as redes diretamente conectadas do R2.

Na segunda rodada, o roteador R1 recebe as rotas diretamente conectadas de R2 ele verifica que a rede 192.168.3.0 não existe em sua tabela de roteamento, por isso insere essa nova informação com métrica 1.

Já para a rede 192.168.2.0, como ele já possui essa entrada em sua tabela de roteamento como diretamente conectada (com métrica zero) e a recebida do R2 está com 1 salto, o router R1 mantém rota original e descartará a informação recebida sobre essa rota através do R2.

Na terceira rodada o roteador R1 envia toda sua tabela de roteamento novamente. Em seu anúncio teremos as rotas 192.168.1.0 e 192.168.2.0 com métrica 1 e a rota 192.168.1.3 com métrica 2 sendo anunciada ao roteador R2.

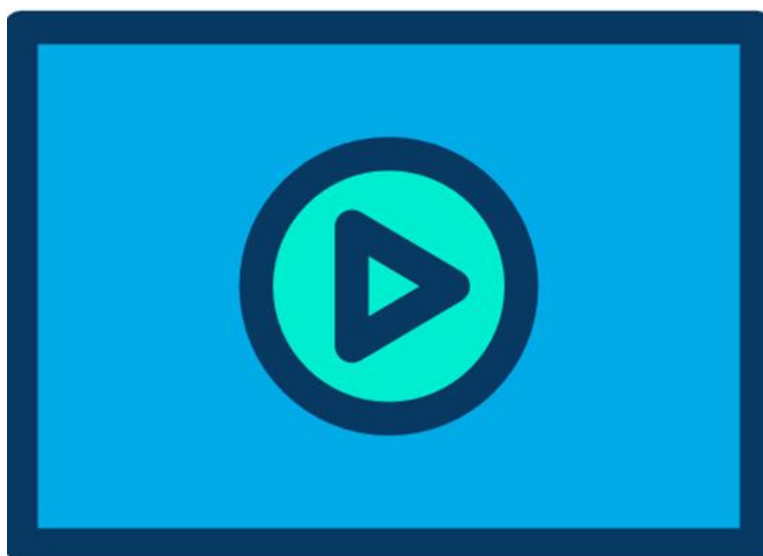
Já o R2 envia para R1 as redes 192.168.2.0 e 192.168.3.0 com métrica 1, pois estão diretamente conectadas, e as rotas 192.168.1.0 e 192.168.4.0 com métrica 2.

Quando R1 recebe essas informações descarta as informações sobre as rotas conhecidas (192.168.1.0, 192.168.2.0 e 192.168.3.0) e a nova rota 192.168.4.0 que ainda não é conhecida é inserida em sua tabela de roteamento com métrica 2.

Nesse ponto R1 já aprendeu as informações sobre todas as rotas utilizadas na topologia, portanto dizemos que o protocolo convergiu.

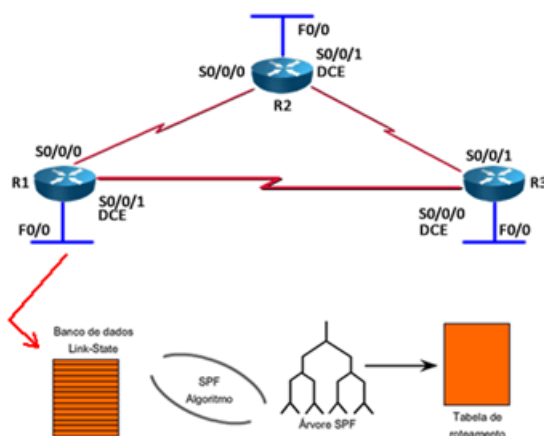
Processo semelhante era utilizado pelo IGRP, protocolo Distance Vector descontinuado pela Cisco e precursor do EIGRP.

7.8 Funcionamento Básico dos Protocolos Link State



Diferente dos protocolos vetor de distância, como o RIP, o OSPF é um protocolo Link State e **não troca tabelas de roteamento** e sim troca informações sobre os seus links através de **LSAs (link state advertisements)**.

As LSAs informam sobre o estado das interfaces dos roteadores adjacentes e são utilizadas para que o roteador possa montar um **banco de dados topológico** e calcular então, através do algoritmo **Shortest Path First** (SPF ou Algoritmo de Dijkstra), o melhor caminho para se chegar ao destino e montar a tabela de roteamento do roteador. Na figura abaixo você tem o resumo da operação do OSPF.



Um protocolo link-state procura com a troca de informações sobre suas interfaces montar um “mapa” da rede, ou seja, primeiro ele descobre os vizinhos que estão em uma mesma área, depois trocam informações (LSAs) que informam cada interface que esse vizinho possui, a que outro vizinho ou rede ela está conectada e qual o “custo” dessa interface.

Com essas informações é possível organizar os vizinhos em um mapa e definir quais os melhores custos para chegar a cada rede que está dentro dessa área OSPF.

Portanto, os roteadores link state como o OSPF e o IS-IS conhecem o caminho para chegar até as redes de destino em uma mesma área, por isso os protocolos link-state são mais pesados que os demais protocolos de roteamento, pois dependendo do tamanho das áreas (quantidade de roteadores) pode haver centenas ou até milhares de LSAs.

Existe uma recomendação de até 50 roteadores por área para minimizar o efeito da inundação de LSAs, porém isso é variável e depende de cada ambiente.

No início do processo, quando ligamos os roteadores OSPF, eles devem **estabelecer** uma “**adjacência**” com seus vizinhos utilizando um protocolo chamado **Hello**.

Esse protocolo é utilizado para formar e manter o vínculo entre os vizinhos.

Depois de formada a adjacência os roteadores enviam suas LSAs para toda a área através de um processo chamado de “**flooding**” ou **inundação**.

As informações recebidas são armazenadas em um banco de dados de estado de enlaces ou **LSDB** (Link State Data base). As informações contidas nas LSAs e armazenadas no banco de dados são geralmente:

- Rede e máscara
- Endereço IP
- Tipo de rede
- Custo do link (métrica)
- Vizinho diretamente conectado (se houver)

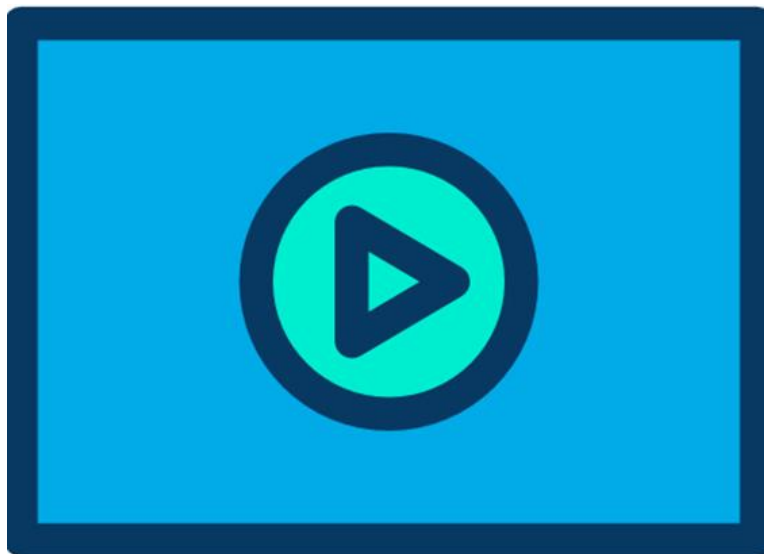
Após o processo inicial de flooding, quando os roteadores receberam todas as LSAs e seus bancos de dados estão completos, os roteadores rodam o algoritmo SPF para montar uma **árvore SPF** e determinar **o melhor caminho** para as redes de destino, alimentando a tabela de roteamento.

As melhores redes são determinadas através do **custo** de cada caminho (soma dos custos dos links do caminho).

Uma vez finalizado o processo de **convergência** (todos os roteadores conhecem as mesmas informações de roteamento), as atualizações de roteamento ocorrerão novamente somente quando houver **alterações na rede** (interfaces down ou novos componentes inseridos).

Os protocolos vetor de distância como RIP enviam periodicamente suas tabelas para os vizinhos mesmo não havendo alterações.

7.9 Protocolo Advanced Distance Vector



O protocolo EIGRP (Enhanced Interior Gateway Routing Protocol) é considerado muitas vezes como Híbrido, pois ele tem as características tanto de um Distance Vector como de um Link State.

Veja os termos em inglês abaixo que podem ser utilizados para enquadrar o EIGRP em relação ao seu algoritmo de roteamento macro:

- **Balanced Hybrid Routing Protocol** – protocolo de roteamento híbrido balanceado ou
- **Advanced Distance Vector Protocol** – protocolo de roteamento vetor de distância avançado.

Ser um protocolo vetor de distância (ou distance vector) significa que as rotas são anunciadas com uma informação de direção (vetor) e uma distância para serem alcançadas.

Lembre-se que no OSPF, ou seja, em protocolos link-state os roteadores não trocam rotas e sim LSAs para montar um “mapa da rede”.

A distância é definida em termos de uma métrica, por exemplo, contagem de saltos para o RIP, e a direção é simplesmente a interface de saída para esses pacotes.

Para calcular a melhor rota o RIP utiliza um algoritmo conhecido como Bellman-Ford, já o EIGRP utiliza o **DUAL** (diffusing update algorithm).

Vamos abaixo analisar o que diferencia o EIGRP desses outros protocolos Distance Vector, tal como o RIP, e faz com que ele seja considerado avançado. Veja a lista abaixo:

1. O RIP não forma adjacências ou vizinhanças, simplesmente enviam suas mensagens aos vizinhos, por padrão, sem nenhuma autenticação ou validação. Em outras palavras, qualquer roteador poderia trocar rotas com eles!
2. O EIGRP tem um processo de formação de adjacência mais simples que o utilizado pelos protocolos link state.
3. O vetor de distância normal envia a tabela de rotas completa periodicamente mesmo que o processo de convergência tenha finalizado.
4. O EIGRP faz o processo de convergência inicial e depois de finalizado troca apenas mensagens de hello, assim como os protocolos link states.

5. Quando há alteração na topologia os distance vectors comuns enviam um flash update (atualização disparada por eventos ou triggered update) com toda a tabela de roteamento.
6. Quando há alteração na topologia o EIGRP é capaz de enviar updates parciais com apenas as informações ou rotas alteradas.
7. Já o OSPF, que é link state, também trabalha dessa forma, enviando informações parciais contendo apenas as alterações da rede.

Outras características que o EIGRP tem e que nem os distance vectors ou link state possuem são:

- Tem a capacidade de manter uma rota principal e uma ou mais backups em sua tabela de topologias, permitindo que em caso de queda da rota principal a rota backup assuma o tráfego sem recálculo da melhor rota.
- Suportar mais de um protocolo de camada-3 no mesmo processo de roteamento.
- Não precisa de reflooding, como no caso do OSPF, que mesmo sem alterações na topologia precisa fazer um novo processo de flooding de LSAs a cada 30 minutos (padrão).
- Pode ter a largura de banda máxima utilizada em um link para envio de informações de roteamento, podendo ser otimizado em links de baixa velocidade.
- Tem protocolo próprio de camada-4 para envio de updates de roteamento – RTP (Reliable Transport Protocol).
- Utiliza o DUAL para calcular as rotas livres de loop.

A métrica do EIGRP pode ser composta por vários itens como largura de banda (bandwidth), atraso (delay), confiabilidade (reliability) e carga (txload e rxload).

Por padrão ela é composta apenas pela largura de banda e delay, conforme mostrado na fórmula abaixo.

$$\text{Métrica} = \left[\frac{10,000,000}{\text{menor largura de banda [kbps]}} + \frac{\text{soma dos delays [\mu sec]}}{10} \right] * 256$$

O EIGRP calcula a métrica das rotas, sendo que a melhor métrica calculada (menor valor) é chamada de distância viável ou "**Feasible Distance**" (**FD**) e será inserida na tabela de roteamento. A rota é marcada como rota principal na tabela de topologia com o termo "successor" ou rota sucessora.

Quando um roteador remoto recebe essa rota via anúncio do EIGRP, ele irá registrar em seu banco de dados topológico como a **distância reportada ou anunciada (Reported Distance – RD ou Advertised Distance – AD)** dessa rota.

Esses dois valores FD e RD são utilizados para determinar se existem loops na rede e no caso de existir uma rota backup, se ela pode ou não ser utilizada sem necessidade de recálculo quando a rota principal cair.

Portanto, a distância reportada (RD - melhor métrica que o vizinho calculou para a mesma rede) e juntamente com a distância viável (FD - melhor métrica calculada no roteador local) é utilizada pelo DUAL para definir se a rota pode ser armazenada como um caminho alternativo, chamada de rota **Feasible Successor**.

Essa condição é que a Distância Reportada pelo vizinho seja menor que a distância calculada no roteador local, ou seja, $RD/AD < FD$. Essa condição é chamada de feasible condition.

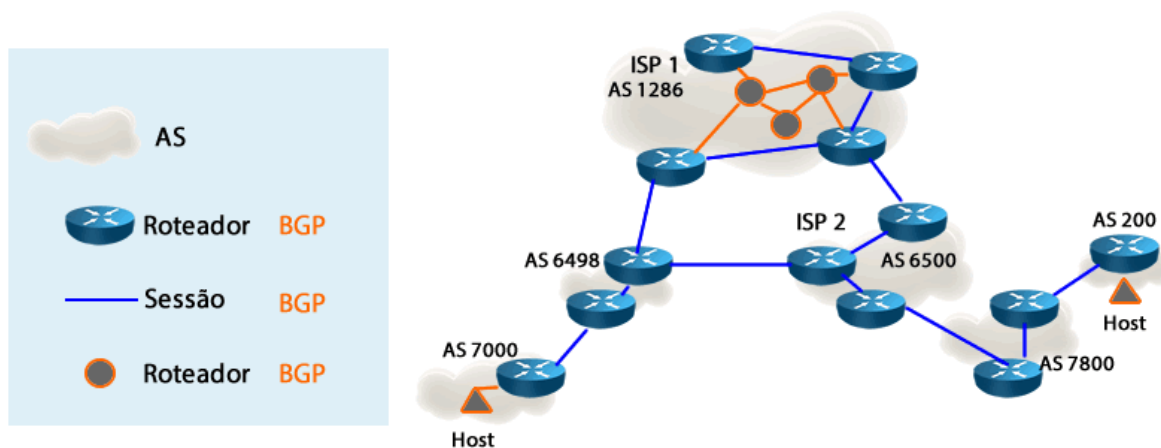
7.10 Path Vector: BGP



O BGP (Border Gateway Protocol) é um protocolo de roteamento externo (EGP ou External Gateway Protocol), ou seja, sua função é trocar informações de roteamento entre redes ou sistemas autônomos diferentes.

É o protocolo usado entre os prestadores de serviços de Internet (ISPs) e pode ser usado entre uma empresa e um ou mais ISPs.

Acompanhe na figura abaixo onde temos uma nuvem de roteadores BGP interconectando vários sistemas autônomos, tais como ISP's e demais empresas que são AS's.



Um detalhe interessante de se notar é que o BGP foi construído para a confiabilidade, controle e escalabilidade, porém não se preocupando com a velocidade, portanto, ele se comporta de maneira diferente dos protocolos de roteamento internos ou IGP's que estudamos até o momento.

Você vai notar quando iniciar suas configurações de BGP que até para subir ele é mais lento que o OSPF e EIGRP.

Vamos abaixo a algumas definições e termos importantes do mundo do BGP:

- Os roteadores rodando BGP são denominados "**BGP speakers**".
- Utiliza o conceito de **Sistemas Autônomos (AS - Autonomous Systems)**, sendo que um sistema autônomo é um grupo de redes sob uma administração comum.
- Normalmente os sistemas autônomos executam um Interior Gateway Protocols (IGP) dentro do sistema, tais como OSPF, EIGRP, RIP ou IS-IS.
- Para conexão entre os ASs utilizamos um Exterior Gateway Protocol (EGP), o qual temos o BGP versão 4 como única opção de EGP atualmente utilizada na Internet. O roteamento entre sistemas autônomos é chamado "roteamento interdomain" ou "interdomain routing".
- Existem duas versões de BGP: EBGp (BGP Externo para uso entre ASs) e IBGP (BGP Interno para uso dentro do AS). A distância administrativa para rotas EBGp é 20, já a distância administrativa para rotas IBGP é de 200.
- Os vizinhos do BGP são chamados de "pares" ou "peers" e devem ser configurados estaticamente, não há descoberta dinâmica de vizinhos como no OSPF e EIGRP.
- O BGP utiliza a camada de transporte na porta TCP 179 para troca incremental de mensagens, atualizações de roteamento e keepalives periódicos.
- Os roteadores podem executar apenas uma instância de BGP (apenas um número de AS configurado em cada roteador).

O BGP é um protocolo considerado "path-vector" ou "vetor de caminho", sendo que uma rota BGP para determinada rede de destino é formada por uma lista de sistemas autônomos que determinam o caminho até aquela rede.

Se compararmos com os IGPs o BGP é bem parecido com o RIP, porém ao invés de número de saltos entre roteadores ele utiliza a quantidade de sistemas autônomos que essa rota irá atravessar até o destino.

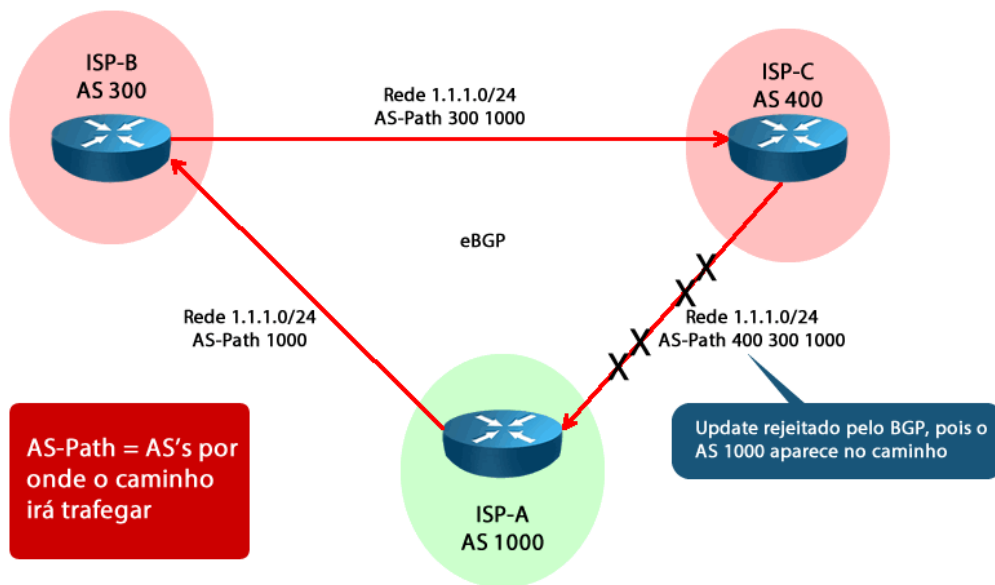
Essa métrica pode também ser composta por outros valores de decisão, ou seja, o administrador de redes pode influenciar de maneira mais flexível nessa tomada de decisão.

O mecanismo de prevenção de loop do BGP é o próprio número de sistema autônomo de todos os ASs por onde uma rota deve passar até alcançar a rede de destino.

Quando uma atualização de roteamento sai do sistema autônomo, esse número de AS é prefixado na lista de sistemas autônomos da atualização de roteamento.

Quando um sistema autônomo recebe uma atualização ele examina essa lista e se encontrar seu próprio número de sistema autônomo nela a atualização é descartada, pois existe um loop nesse caminho.

Veja a figura abaixo com um exemplo da detecção de loop pelo AS 1000 quando recebe a rota para a rede 1.1.1.0/24 anunciada por ele mesmo através do AS 400.



8 Visão Geral do OSPFv2 e Configurações do OSPF Single Area

8.1 Introdução



O **OSPF** é um protocolo de roteamento baseado no **Estado de Enlace (Link State)**, os quais utilizam o **algoritmo SPF** (Shortest path first – Caminho mais curto primeiro) para calcular as melhores rotas.

O OSPF teve seu desenvolvimento no final dos anos 80 e atualmente possui duas versões, sendo a versão 2 para o protocolo IPv4 (OSPFv2) e a versão 3 para o protocolo IP versão 6 (OSPFv3).

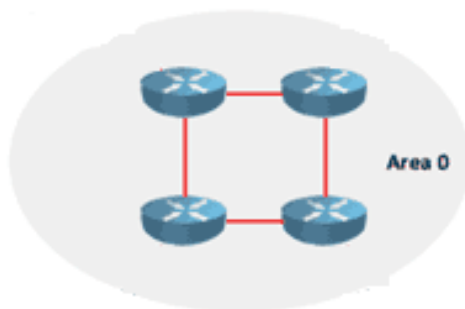
Nesse capítulo vamos estudar tanto o funcionamento como a configuração do OSPFv2 com área única, ou seja, single area.

8.2 Características do OSPFv2

Abaixo seguem as principais características do **OSPFv2**:

- Protocolo aberto definido na **RFC 2328**, podendo ser configurado entre roteadores Cisco e de outros fabricantes.
- Suporta roteamento **classless**, isto é, repassa a máscara em seus updates e permite o uso de **VLSM** e **CIDR**.
- A métrica do OSPF é determinada pelo **custo** do link, que por padrão é igual a "**100.000.000/Largura de banda**" em bps.
- Utiliza **multicast** para troca de informações entre os roteadores (endereços 224.0.0.5 e 224.0.0.6).
- A distância administrativa padrão é **110**.
- Utiliza **áreas** para melhor organizar o fluxo de informações entre os roteadores (envio de LSAs).
- Cada roteador no mínimo mapeia a topologia de sua própria área da rede, o que facilita a solução de possíveis problemas que possam ocorrer.
- Requer um projeto hierárquico para reduzir o overhead de roteamento, acelerar a convergência e isolar redes instáveis em áreas específicas.

A configuração do OSPF pode ser em uma única área (**OSPF Single Area** - área única) onde todas as interfaces devem pertencer à **área zero**.

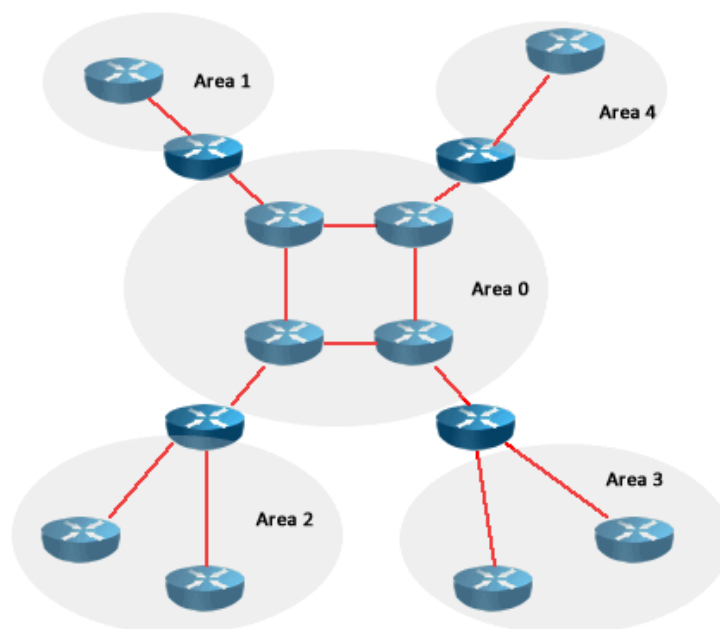


Já o **OSPF Multiarea** utiliza mais áreas para dividir melhor as redes e teremos obrigatoriamente uma área de **backbone** ou **zero** e as demais áreas conectas a ela.

Não podemos ter topologia sem a área zero, pois as demais áreas precisam da área zero para se comunicar.

A área zero é chamada de "**backbone**" porque serve como **trânsito** para informações entre as áreas regulares, por exemplo, se um computador conectado à área 1 quiser se comunicar com um computador conectado à área 2, esse pacote IP será encaminhado entre as áreas passando através do **backbone (área 0)**.

Veja na figura a seguir uma topologia de rede OSPF multiarea, formada por uma área de backbone (área zero) e áreas regulares (demais áreas diferentes de zero).



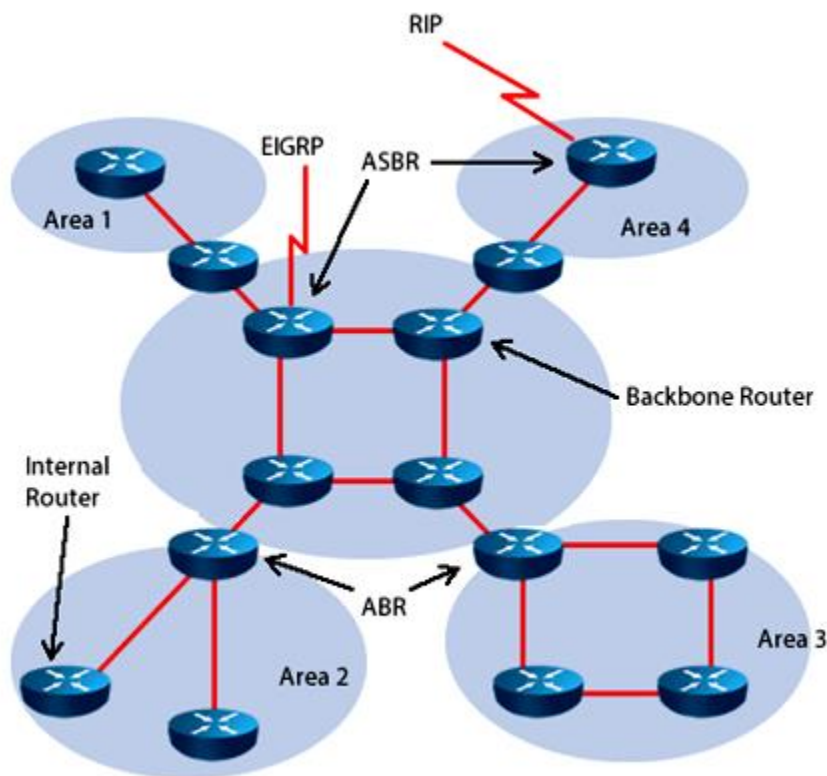
8.3 Nomenclatura do OSPF – Tipos de Redes, Áreas e Roteadores



Vamos agora ver algumas nomenclaturas e termos utilizados para dividir as redes, roteadores e áreas no OSPF.

Vamos iniciar com o conjunto de termos do OSPF definem as funções dos roteadores na rede, sendo que cada dispositivo pode ter várias funções conforme descrito abaixo (acompanhe também na próxima figura):

- **Internal Router:** um roteador interno tem todas as interfaces em uma única área e esses roteadores mantêm um banco de dados de estado de link para sua própria área apenas.
- **Backbone Router:** esse tipo de roteador tem pelo menos uma interface atribuída a área zero, por isso são roteadores de backbone.
- **Roteador de borda de área (ABR - Area Border Router):** esse tipo de roteador tem interfaces em duas ou mais áreas. Os ABRs separam o flooding de LSA entre as áreas, fazem a sumarização de rotas e anunciam rotas padrão. Eles mantêm uma base de dados de link-state para cada área à qual estão conectados.
- **Roteador de limite de Sistema Autônomo (ASBR - Autonomous System Boundary Router):** esses roteadores têm interfaces dentro e fora do domínio de roteamento OSPF, podendo estar conectado com uma rede EIGRP e configurado para redistribuição de rotas, fazendo com que diferentes domínios de roteamento troquem informações entre si.



Existe também diversos tipos de áreas, abaixo seguem as principais:

- **Área de backbone:** esta é a área zero, a qual interliga todas as outras áreas.
- **Área normal:** são as demais áreas ou "Non-backbone areas" (áreas a partir de 1). No seu banco de dados existem rotas internas e externas.

O CCNA foca na área de Backbone, pois ele cobra a configuração do OSPF single área que utiliza apenas a área zero ou de backbone.

Além da diversidade de tipos de roteadores no OSPF Multiarea temos também diferentes tipos de rotas quando usamos esse tipo de topologia, abaixo segue a descrição dos principais tipos:

- **Interna ou Intra-área (O - Intra-area route):** rotas que pertencem à mesma área OSPF.
- **Inter Área (O IA - Inter-area route):** rotas que pertencem ao mesmo processo OSPF, porém a áreas diferentes da que o roteador está configurado.
- **Externa (O E1/2 - External route):** rotas aprendidas por fontes externas ao OSPF, por exemplo, uma rota padrão aprendida pelo comando "default-information originate" ou por redistribuição.

Note que aqui utilizamos a nomenclatura completa do OSPF para você ter noção dos termos e saber que no CCNP Enterprise ainda tem muita coisa a ser aprendida, porém o que é importante para o CCNA está grifado em amarelo!

Esses termos grifados são os relativos ao OSPF Single Area.

8.4 Operação do OSPF



Basicamente o processo do OSPF inicia pela formação de adjacências ou vizinhanças e passa pelas seguintes etapas ou fases até a sincronização completa ou convergência:

1. Ativação do processo de roteamento
2. Inicialização e estabelecimento das vizinhanças ou adjacências
3. Troca do banco de dados de estado de enlace (LSBD – Link state data base) através do envio das LSAs locais de cada roteador
4. Finalização da convergência e montagem da tabela de roteamento
5. Roteadores entram em Full (carregamento completo do OSPF) e em operação normal, ou seja, após as rotas calculadas os roteadores podem encaminhar o tráfego
6. Durante a operação pode haver atualizações do estado dos enlaces por mudanças na rede (problemas ou adições de novos roteadores OSPF ou redes à topologia)
7. Atualizações periódicas no caso de não haver alterações na topologia (reflooding a cada 30 minutos)

A seguir vamos estudar como o OSPF troca mensagens, estabelece vizinhança, troca informações de roteamento, escolhe as melhores rotas e funciona na sua operação normal.

8.4.1 Tipos de Mensagens do OSPF

O OSPF utiliza vários tipos de mensagens diferentes para estabelecer e manter relacionamentos com seus vizinhos, assim como para manter as informações de roteamento corretas.

OSPF usa cinco tipos de pacotes, porém eles não são transportados pelo UDP ou TCP, ao invés disso, ele é executado diretamente sobre IP (protocolo IP 89) usando um cabeçalho exclusivo do OSPF.

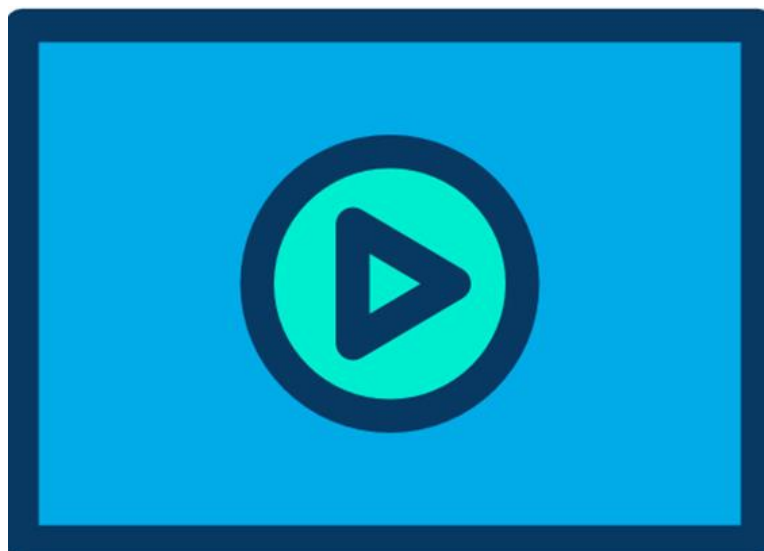
Abaixo segue o formato do pacote do OSPFv2.

Version	Type	Packet Length	
OSPF Router ID			
OSPF Area ID			
Checksum		Authentication Type	
Authentication Data			
Authentication Data			
LS age		Options	LS type
Link State ID			
Advertising Router			
LS sequence number			
LS checksum		Length	
Link State Data			

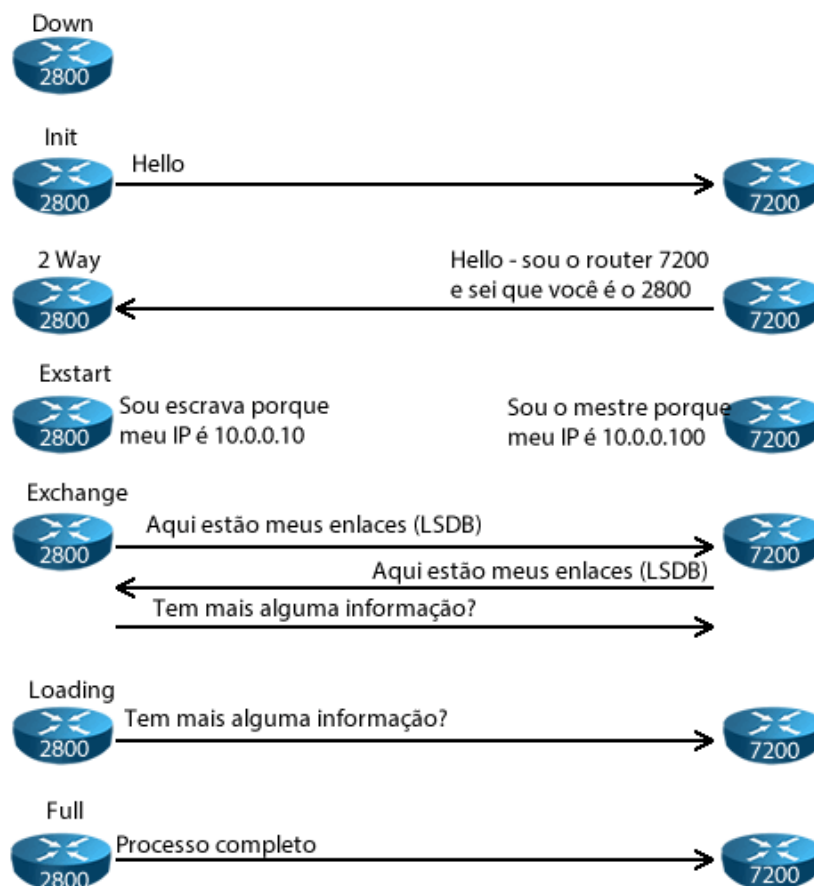
O campo version para IPv4 deve trazer a versão 2 e o Type especifica o tipo do pacote OSPF será transportado, sendo que os cinco tipos de pacotes OSPF são:

1. **Hello:** Identificam vizinhos e servem como um keepalive.
2. **Database Description (DBD):** Trata-se de um resumo do LSDB (banco de dados link-state), incluindo RID e o número de sequência de cada LSA no LSDB.
3. **Link State Request (LSR):** O pedido de Link State Update (LSU) contém o tipo de LSU solicitado e o ID do roteador solicitante.
4. **Link State Update (LSU):** Contém uma entrada LSA completa, incluindo informações de topologia, por exemplo, o RID do roteador local e o RID e custo de cada vizinho. Uma LSU pode conter múltiplos LSA's.
5. **Link State Acknowledgment (LSAck):** Utilizado para reconhecer o recebimento de todos os outros pacotes OSPF exceto pacotes de hellos, os quais não precisam de reconhecimento.

8.4.2 Estabelecimento de Vizinhanças e Troca de Banco de Dados



Na figura abaixo temos o resumo de todos os passos até o roteador estar no estado **Full Loaded**, indicando que pode trocar pacotes porque sua tabela de roteamento foi alimentada com as rotas calculadas pelo OSPF (convergência).



Note na figura anterior que quando um roteador OSPF é ligado ele inicia em um estado chamado "**down**" e envia um pacote **hello** em **multicast** esperando que outros roteadores OSPF diretamente conectados respondam essa mensagem para poder estabelecer uma vizinhança e trocar informações sobre o OSPF.

Esse pacote de hello contém o RID (router ID ou identificação do roteador) do próprio roteador e informando que não tem nenhum vizinho naquele link (RID do vizinho nulo), quando esse pacote é enviado o roteador entra em um estado chamado de "**init**".

Os roteadores ficam nesse estado até que recebam seu próprio RID na resposta de um vizinho.

Nessa troca de pacotes de hello várias informações são enviadas e os roteadores formarão vizinhança **apenas se os parâmetros abaixo estiverem iguais** em ambos os roteadores:

- Mesma sub-rede e máscara configurada em ambas as interfaces.
- Valores de intervalo (timers) de Dead e Hello iguais.
- As interfaces devem pertencer à mesma área OSPF.
- Passar na autenticação se estiver habilitado (opcional).
- Se estiver sendo utilizada rede stub ambas as interfaces devem ter o mesmo flag (identificação da área stub – o estudo desse parâmetro faz parte do CCNP ROUTE).

Caso tudo esteja correto na troca de mensagens de hello iniciais, o roteador inclui todos os roteadores na sua **tabela de vizinhança** e passa para o estado chamado "**two-way**".

As informações sobre os vizinhos guardadas no banco de dados de vizinhança (neighbor database) podem ser consultadas com o comando "**show ip ospf neighbor**". Veja a figura a seguir com um resumo até os dois routers ficarem em 2-way.



1. Estado inicial em Down, link sobre ou é configurado no processo do OSPF.
2. Envio do hello com seu RID e passa para Init.
3. Recebe hello contando o RID do vizinho e seu próprio RID como reconhecido passa para 2-way.
4. R2 também recebe uma resposta do seu hello com seu RID listado e passa para 2-way.

No próximo passo, os roteadores determinam quem será "**mestre**" e "**escravo**" para troca de LSAs, pois deve haver uma ordem para não "dar bagunça".

Nessa fase os roteadores OSPF estão em um estado chamado "**Exstart**".

Após esse passo (definido que inicia a troca de LSAs) os roteadores devem trocar as **LSAs** para montar o **banco de dados topológico** e entram em um estado chamado "**Exchange**".

Portanto, nessa fase ocorre a troca de informações sobre as bases de dados dos estados dos enlaces dos roteadores (**LSDB** – Link State Data Base).

O roteador local inunda a rede com todas as suas LSAs para que seus vizinhos tenham o mesmo banco de dados local.

Esse processo não é feito através da troca de LSAs uma a uma, mas sim através de "pacotes de LSAs".

Primeiro os roteadores trocam pacotes chamados **Database Description** (DD), os quais contêm uma lista das LSAs que são conhecidas por eles.

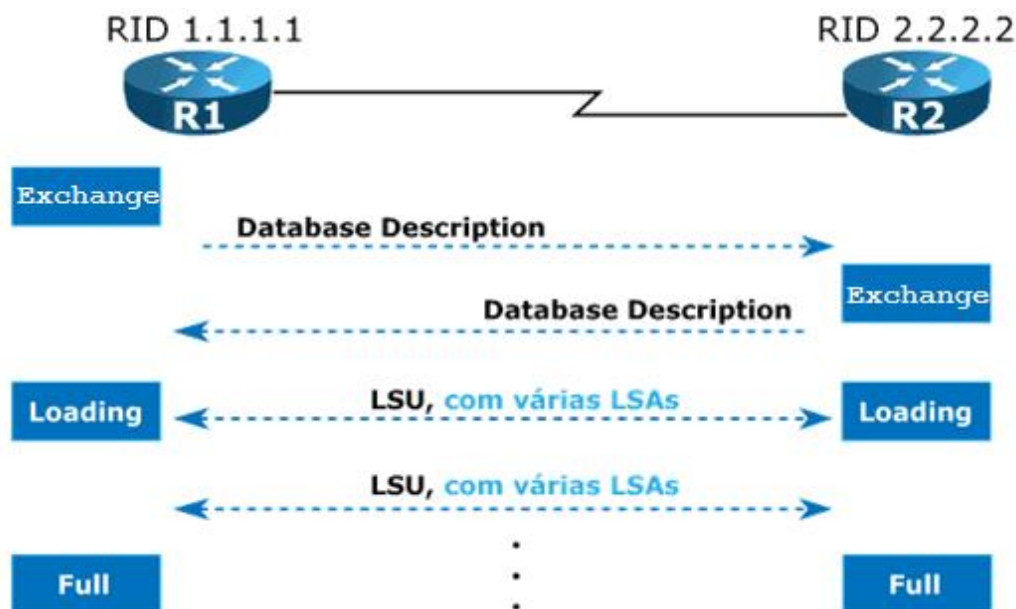
Por exemplo, ele recebe um pacote de DD contendo 20 LSAs, das quais 10 ele conhece, portanto ele precisa solicitar só as 10 restantes que ele não conhece.

Isso permite que o roteador solicite apenas as LSAs que ele não conhece utilizando um pacote chamado **Link-State Request** (LSR).

Portanto, seguindo o exemplo anterior, o roteador enviaria um LSR contendo as 10 LSAs que ele não conhece.

As LSAs solicitadas no pacote de LSR são passadas via um pacote chamado **Link-State Update** (LSU), a qual agrupa a lista de LSAs solicitadas em apenas uma mensagem, tornando o processo de flooding de LSAs mais rápido e eficiente.

Veja a figura abaixo com um resumo da troca de bando de dados (LSDB).



Depois de finalizar a troca de informações de LSDB os roteadores executam o algoritmo **SPF**, calculam e inserem as melhores rotas na tabela de roteamento e entram no estado "**full**", o que significa que já podem fazer a troca de tráfego de acordo com suas tabelas de roteamento montadas pelo OSPF com base nas mesmas informações.

O estado **full** significa que todos os roteadores conhecem **todas as LSAs** dos demais roteadores e houve a **convergência da rede**, ou seja, foi montado o banco de dados topológico, executado o SPF e as melhores rotas foram calculadas e instaladas na tabela de roteamento.

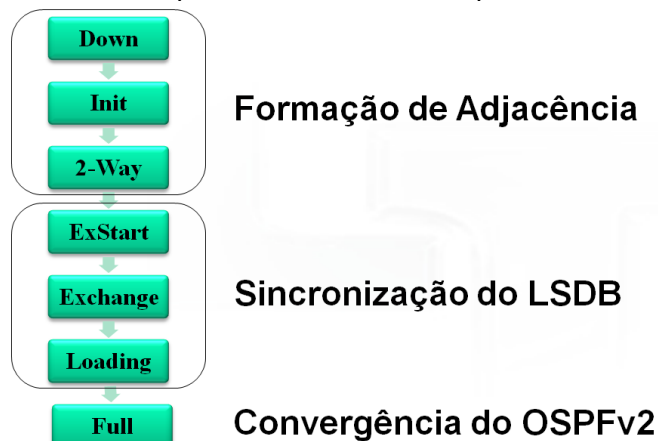
Quando ocorre isso, o roteador emite uma mensagem avisando que está no estado de full para o console do roteador conforme abaixo:

```
00:00:20: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.0.2 on Serial0/0/1 from LOADING to FULL, Loading Done
```

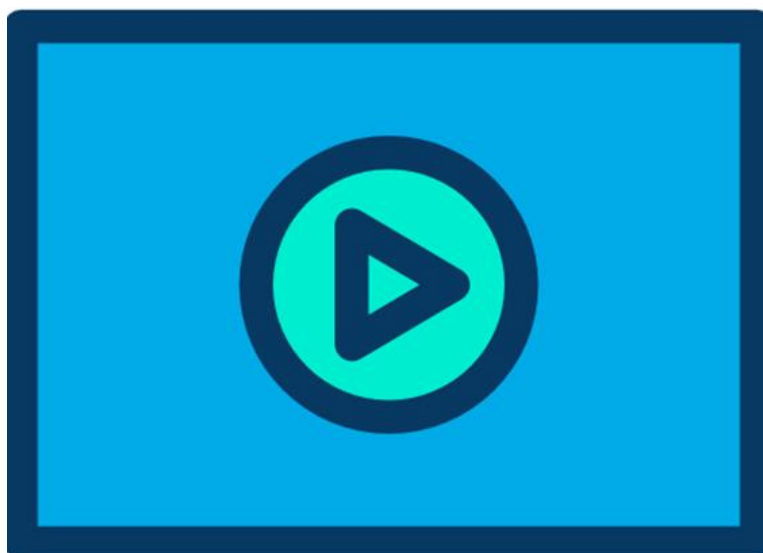
Resumindo o processo de estabelecimento de vizinhanças o roteador passa pelos seguintes estados até ficar full-loaded em sequência:

- **Down > Init > Two-way > Exstart > Exchange > Loading > Full.**

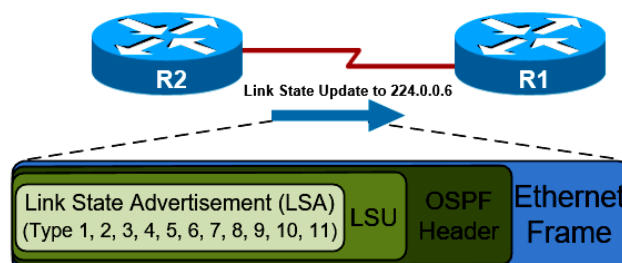
Na figura a seguir tem o resumo do processo e onde cada passo se encaixa.



8.4.3 Principais Tipos de LSAs



O OSPF utiliza diferentes tipos de LSAs ou anúncios de link state para anunciar diferentes tipos de rotas. Para você ter uma ideia o OSPFv2 tem 11 tipos de LSA, porém vamos falar aqui apenas dos principais tipos para um CCNA.



Veja abaixo uma descrição dos cinco principais tipos de LSA em um total de 11:

- **LSA Tipo-1 (Router LSA 1):** Anuncia rotas **intra-área**. São geradas por um roteador OSPF e inundadas apenas dentro da área. Recebem a letra "**O**" na tabela de roteamento.
- **LSA Tipo-2 (Network LSA 2):** Anuncia roteadores em um link de **acesso múltiplo** (rede broadcast ethernet) dentro da própria área, ou seja, são geradas por um roteador DR. São inundadas apenas dentro da área e recebem também a designação "**O**" na tabela de roteamento.

Portanto, os dois primeiros tipos de LSAs representam links ou rotas que estão dentro da mesma área (intra área), por exemplo, em uma topologia single-area apenas LSAs do tipo 1 e 2 são encontradas no banco de dados de LSAs (LSDB).

- **LSA Tipo-3 (Summary LSA 3):** Anuncia rotas **inter-area** e são geradas por um **ABR**. São inundadas em áreas adjacentes (vizinhas) e recebem a designação "**O IA**" na tabela de rotas.

Resumindo, uma LSA do tipo-3 são as rotas aprendidas por um ABR e ensinadas para a área zero.

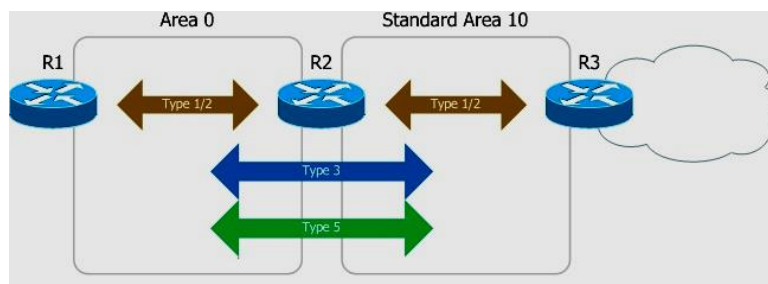
Note que a área de backbone vai conhecer essas rotas, mas não o detalhe da topologia interna da rede da área remota.

- **LSA Tipo-5 (External LSA 5):** Anuncia rotas em domínio de roteamento gerado por um ASBR. Essa mensagem de LSA é inundada para áreas adjacentes e recebe a designação "O" na tabela de roteamento com um dos dois sufixos (O E1 ou O E2):
 - E1- a métrica é aumentada a cada roteador que passa pela rede.
 - E2- a métrica fica fixa e não aumenta ao passar por outros roteadores na rede (padrão).

Essas duas LSAs são utilizadas quando temos redes externas simples, por exemplo, as aprendidas via comando "**default-information originate**" que vamos estudar mais para frente nesse capítulo.

As LSAs do tipo-5 são as rotas que esse ASBR aprendeu em um domínio de roteamento externo e inseriu dentro do OSPF como rotas externas (marcadas como **O E2** por padrão).

Portanto as LSAs do tipo 1 e 2 ficam dentro de uma mesma área para definir a topologia local, já as LSAs do tipo 3 e 5 são enviadas pela área de backbone para informar como encontrar as redes de áreas remotas e redes externas respectivamente.



Legal tudo isso, mas o que tem dentro de uma LSA?

São informações que permitam ao OSPF criar um mapa da rede! Veja abaixo o que as LSAs do tipo 1, 2 e 3 trazem de informações:

- **LSA do tipo-1 (Router LSA 1)** -> descreve um roteador -> traz seu router RID, interfaces, IP/máscara e estado da interface (link state).
- **LSA do tipo-2 (Network 2)** -> descreve uma rede que possui DR/BDR (multiacesso) -> traz os endereços do DR e BDR, sub-rede (subnet ID) e máscara (prefixo).
- **LSA do tipo-3 (Summary 3)** -> traz informações de outras áreas -> sub-rede (Subnet ID), máscara e RID do ABR que enviou a LSA.

Essas informações podem ser verificadas com o comando **"show ip ospf database"**.

8.4.4 Alteração na Topologia e Atualizações Periódicas

Após a rede convergir, o OSPF entra em operação normal e não são mais trocadas informações sobre os estados dos enlaces até que haja uma alteração na topologia.

As alterações podem ser causadas por problemas de rede, como uma interface que fica Down ou um roteador que é desligado, ou então pela inserção de novas redes ou roteadores na topologia pelo crescimento natural das empresas.

Quando ocorre uma alteração na topologia, o roteador OSPF que teve uma ou várias redes comprometidas ou adicionadas envia em multicast um pacote **LSU** (Link State Update).

O vizinho confirma o recebimento da LSU com um ACK e faz flooding do LSU para todos os roteadores da rede utilizando um endereço de multicast também.

Cada LSA é confirmada separadamente com um LSAck.

Portanto, quando ocorre uma alteração na topologia os caminhos entre os roteadores serão recalculados e novamente o algoritmo SPF entra em ação para determinar as rotas nesse novo estado da topologia após as alterações.

Você consegue analisar quantas vezes o SPF foi recalculado com o comando **"show ip ospf"**.

Se houver um período de inatividade na rede, ou seja, nenhuma alteração foi notificada por nenhum dos roteadores OSPF, existe a troca de LSAs entre os roteadores para garantir que não ocorreu nenhuma alteração, o padrão do timer de inatividade é de **30 minutos**.

Portanto, se nada ocorrer em uma rede OSPF haverá uma reenvio de informações de LSAs de 30 em 30 minutos (inundação ou **reflooding**).

8.4.5 Tipos de Redes Suportadas pelo OSPF



O protocolo OSPF suporta **5 tipos de redes**:

- Ponto a ponto ou **point-to-point** (redes WAN como PPP, HDLC e Frame-relay ponto-a-ponto)
- Multiacesso com broadcast ou **Broadcast** (redes Ethernet e Fastethernet)
- Rede multiacesso sem broadcast ou **NBMA** (Frame-relay com split-horizon)
- Ponto a multiponto ou **point-to-multipoint**
- Links virtuais ou **virtual links**

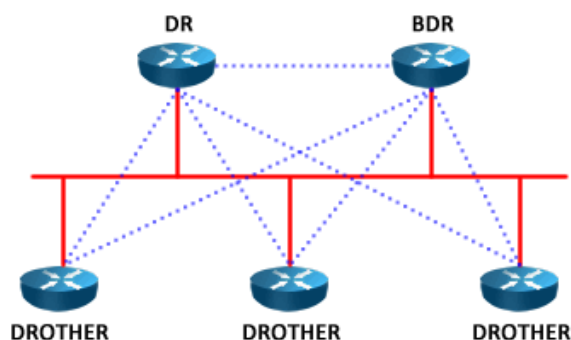
Redes **ponto a ponto** são redes tipicamente WAN ou LAN conectadas diretamente entre si, nas quais existem apenas dois equipamentos conectados.

Para esses equipamentos as LSAs são enviadas normalmente entre eles e a adjacência é formada entre os dois equipamentos.

No caso de **redes multiacesso** ou **compartilhadas**, ou seja, onde existe mais de um equipamento na mesma rede IP, como em redes LAN, será necessária a eleição de um roteador designado (**DR – Designated Router**) e seu backup (**BDR – Backup Designated Router**).

Todos os demais roteadores formam adjacência somente com eles (DR e BDR), **não formando vizinhança entre si**.

Na figura a seguir temos uma rede multiacesso com broadcast, ou seja, uma típica rede LAN com padrão da família Ethernet.



É simples entender o motivo, imagine uma rede LAN em um Data Center onde temos 100 roteadores interconectados na mesma sub-rede.

Esses roteadores teriam que formar adjacências entre si, resultando em mais de 4000 adjacências por roteador.

Quanto de memória RAM e CPU teríamos que reservar para esse processamento de informações quando os pacotes de link-state começassem a ser trocado?

Com certeza MUITO.

Com apenas um DR e um BDR são formadas duas adjacências por roteador que não é DR ou BDR.

E entre dois roteadores que não são DR ou BDR o que ocorre?

A adjacência entre eles fica em **2-way**, nunca chegam a full-loaded, eles ficam full-loaded apenas com os roteadores DR e BDR.

Os roteadores que não são DR ou BDR são chamados **DROTHER**.

Portanto, quando temos redes padrão ethernet ou frame-relay NBMA, antes da troca de LSAs há uma eleição de DR e BDR, sendo que após essa eleição quem recebe e repassa as DD (Database Description), LSRs e LSUs são apenas o DR e BDR.

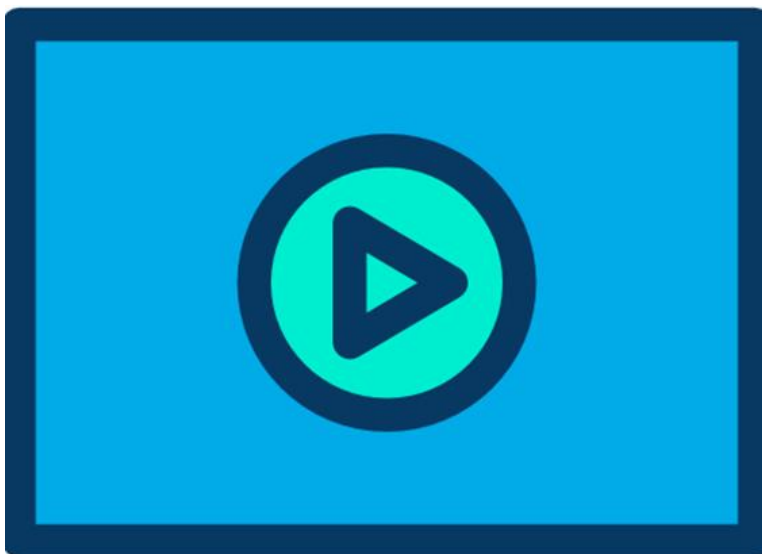
Os demais roteadores (DROTHER) não enviam pacotes sobre troca de LSAs entre si.

Resumindo quando precisamos de eleição de DR e BDR nas redes com o protocolo OSPF:

- **Ponto-a-ponto** (PPP e HDLC): NÃO
- **Multiacesso com broadcast** (Ethernet e Fastethernet): SIM
- **Rede Multiacesso sem Broadcast ou NBMA** (Frame-relay com split-horizon – todos roteadores na mesma sub-rede IP): SIM

As redes NBMA, links virtuais e redes multiponto não fazem parte do conteúdo do CCNA.

8.4.6 Escolha do melhor caminho pelo OSPF



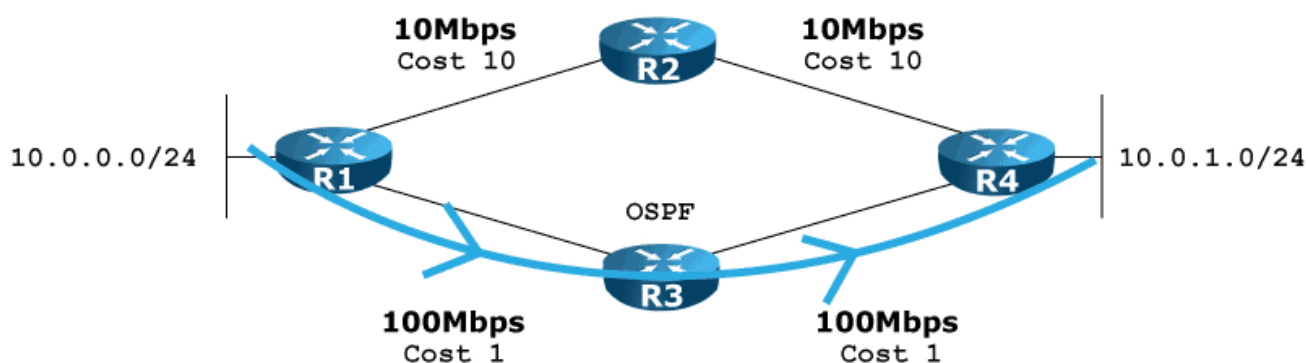
Após o roteador OSPF trocar as LSDBs (Banco de dados dos estados de enlace) o algoritmo SPF é executado, uma árvore com todos os enlaces e roteadores pertencentes à mesma área é criada com todos os caminhos possíveis.

O próprio roteador é posicionado no topo dessa árvore e a partir dela os caminhos (rotas) com "**menor custo**" (menor métrica baseada na largura de banda da interface) serão adicionados à tabela de roteamento.

Veja a figura abaixo onde para a rede 10.0.0.0 /24 (conectada ao roteador R1) alcançar a rede 10.0.1.0 /24 (conectada ao R2) existem duas opções: via R2 através de dois links de 10Mbps ou via R3 através de dois links de 100Mbps.

Tanto o OSPF como o EIGRP **por padrão escolherão sempre a rota com maior largura de banda** total pelo caminho.

Já o RIP iria fazer o balanceamento de carga nesse exemplo, pois para ele as duas rotas têm a mesma métrica de dois saltos.



Esta métrica, chamada custo no OSPF, é a soma da divisão do valor de **100.000.000** (100 milhões) pela largura de banda da interface em **bps** (10^8 / bandwidth/bps).

Por exemplo, em um link Ethernet (10Mbps ou 10.000.000bps) temos o custo de "100.000.000/10.000.000", o que nos dá um custo igual a 10.

Em um link de 64kbps teremos um custo de "100.000.000/64000", o que nos dá um custo igual a 1562.

Os valores da métrica são números inteiros, por isso desconsideramos o resto da divisão.

Portanto entre um link de 64k e uma saída Ethernet o OSPF prefere a Ethernet, pois a métrica é menor.

Se o caminho passa por vários links a métrica é a soma desses links, por exemplo, se temos dois roteadores com interfaces fastethernet conectados por um link serial de 64kbps o custo desse caminho será a soma de $(100.000.000/64.000) + (100.000.000/100.000.000) = 1562 + 1 = 1563$.

A métrica da interface local não entra na conta da métrica!

Você pode configurar manualmente o custo de uma interface com o comando, em modo de configuração de interface, "**ip ospf cost**".

Por exemplo, para configurar o custo de uma interface para 65 basta entrar na interface e digitar "**ip ospf cost 65**".

Essa configuração faz com que o roteador ignore o comando bandwidth e não seja mais necessário o cálculo do custo pelo OSPF, pois você já inseriu o comando de maneira manual.

Por padrão, o custo das interfaces OSPF está referenciado a um custo onde a maior velocidade é de 100 Mbps.

Portanto, para uma interface de 1Gbps o custo seria 1, o mesmo de uma interface de 100Mbps.

Sendo assim, em roteadores mais novos com interfaces LAN a gigabit será necessário ajustar esse valor no protocolo de roteamento através do comando "**auto-cost reference-bandwidth**" em modo de configuração de roteamento.

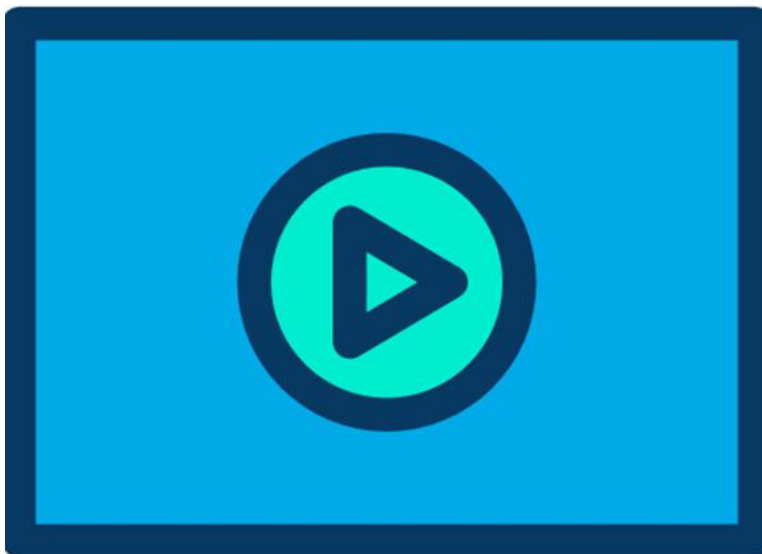
Acompanhe o exemplo abaixo onde vamos ajustar para a base ser um link de 1 Gbps:

```
R1(config)#router ospf 1
R1(config-router)#auto-cost reference-bandwidth 1000
```

Com esse ajuste uma interface de 1Gbps terá custo 1 ($1.000\text{Mbps}/1\text{Gbps}=1$) e uma interface de 100Mbps terá custo 10 ($1000\text{Mbps}/100\text{Mbps}=10$).

Um cuidado com esse comando é de não utilizar valores muito grandes, pois links de baixa velocidade, por exemplo, 64kbps, podem acabar ficando com uma métrica tão alta que acabam sendo considerados com custo infinito e não anunciados pelo OSPF!

8.4.7 Timers de Hello e Dead



Para que o OSPF funcione entre dois roteadores, além das configurações que analisamos anteriormente estarem corretas, são necessários que os **timers** de **hello** e **dead** sejam os mesmos em ambos os vizinhos.

Esses timers são definidos por interface e significam:

- **Hello:** timer de envio de pacotes do protocolo de hello, utilizado para identificar se a conexão entre os processos do OSPF nos roteadores está ok e para a formação de uma adjacência.
- **Dead:** temporizador que indica quando a comunicação entre dois roteadores OSPF foi considerada como interrompida, geralmente 4 vezes o valor do Hello.

Esses parâmetros são pré-requisitos para estabelecimento de uma adjacência (vizinhança) entre dois roteadores OSPF e devem ser iguais em ambos os roteadores.

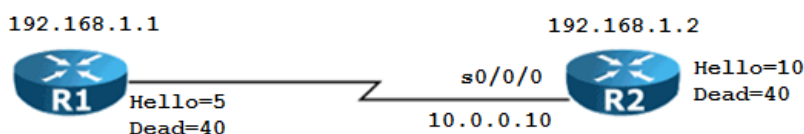
Caso sejam diferentes os roteadores não trocarão informações de roteamento.

Veja a seguir os comandos para alteração dos timers para 5 segundos de hello e 20 segundos para o dead.

```
Router(config)#interface Loopback0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#ip ospf hello-interval 5
Router(config-if)#ip ospf dead-interval 20
```

Esses timers podem ser visualizados no comando "**show ip ospf interface**".

Veja ao abaixo a saída do comando "**debug ip ospf events**" para um roteador com problemas de hello e dead configurados com valores diferentes entre dois roteadores com OSPF.



```
R1#debug ip ospf events
```

OSPF events debugging is on

R1#

01:02:16: OSPF: Rcv hello from 192.168.1.2 area 0 from Serial0/0/0 10.0.0.10

01:02:16: OSPF: Mismatched hello parameters from 10.0.0.10

01:02:16: OSPF: Dead R 40 C 40 Hello R 10 C 5 Mask R 255.255.255.252 C 255.255.255.252

O valor de Dead R 40 é o Dead Timer do vizinho, o valor C 40 representa o mesmo temporizador do roteador local, portanto o Dead está igual.

Depois temos as informações de Hello, onde seguimos a mesma lógica, ou seja, o vizinho tem hello configurado com 10s (R10) e o roteador local está com hello a cada 5 segundos (C 5), por isso temos que entrar em um dos dois e alterar o temporizador de hello para resolver esse critério de formação de vizinhança.

Vamos alterar o valor para o padrão no roteador local que é de 10s e verificar como será a comunicação até fechar a adjacência. Acompanhe na saída do debug a seguir.

R1(config-if)#no ip ospf hello-interval 5

R1(config-if)#

01:05:56: OSPF: Rcv hello from 192.168.1.2 area 0 from Serial0/0/0 10.0.0.10

01:05:56: OSPF: 2 Way Communication to 192.168.1.2 on Serial0/0/0, state 2WAY

01:05:56: OSPF: Send DBD to 192.168.1.2 on Serial0/0/0 seq 0x192a opt 0x00 flag 0x7 len 32

01:05:56: OSPF: End of hello processing

01:05:56: OSPF: Neighbor change Event on interface Serial0/0/0

01:05:56: OSPF: Rcv DBD from 192.168.1.2 on Serial0/0/0 seq 0xa54 opt 0x00 flag 0x7 len 32 mtu 1500 state EXSTART

01:05:56: OSPF: NBR Negotiation Done. We are the SLAVE

01:05:56: OSPF: Send DBD to 192.168.1.2 on Serial0/0/0 seq 0xa54 opt 0x00 flag 0x2 len 72

01:05:56: OSPF: Rcv DBD from 192.168.1.2 on Serial0/0/0 seq 0xa55 opt 0x00 flag 0x3 len 72 mtu 1500 state EXCHANGE

01:05:56: OSPF: Send DBD to 192.168.1.2 on Serial0/0/0 seq 0xa55 opt 0x00 flag 0x0 len 32

01:05:56: OSPF: Rcv DBD from 192.168.1.2 on Serial0/0/0 seq 0xa56 opt 0x00 flag 0x1 len 32 mtu 1500 state EXCHANGE

01:05:56: OSPF: Send DBD to 192.168.1.2 on Serial0/0/0 seq 0xa56 opt 0x00 flag 0x0 len 32

01:05:56: Exchange Done with 192.168.1.2 on Serial0/0/0

01:05:56: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.2 on Serial0/0/0 from EXCHANGE to FULL, Exchange Done

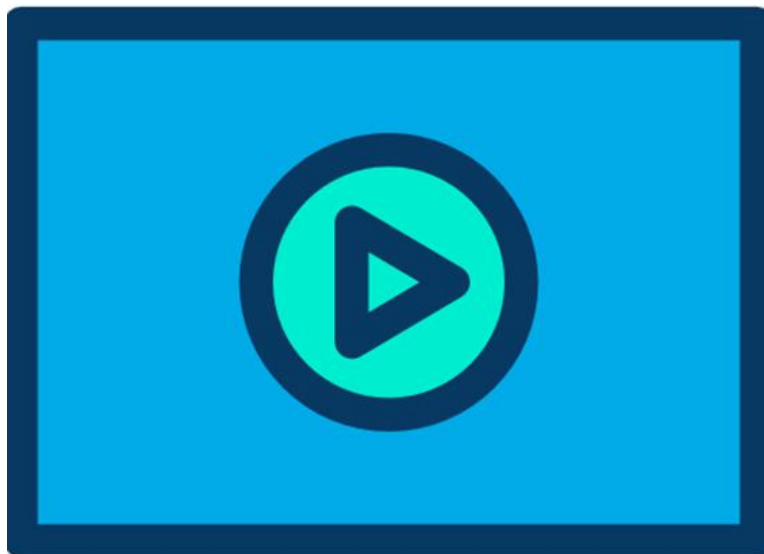
01:05:56: OSPF: Send DBD to 192.168.1.2 on Serial0/0/0 seq 0xa56 opt 0x00 flag 0x0 len 32

01:06:06: OSPF: Rcv hello from 192.168.1.2 area 0 from Serial0/0/0 10.0.0.10

01:06:06: OSPF: End of hello processing

Perceba que após consertar os valores a adjacência é formada, os roteadores entram em Full state e os hello são recebidos e processados sem erros.

8.4.8 Parâmetro Router ID



A configuração do Router ID é colocada como opcional porque mesmo que você não a declare na configuração do OSPF o roteador irá escolher seu identificador sozinho.

O router ID ou RID, valor que é um endereço IP (32 bits – 4 octetos em decimal pontuado) será utilizado na seguinte ordem de prioridade:

1. Valor configurado no comando RID na configuração do OSPF;
2. Valor do maior endereço IP de loopback configurada no roteador, caso o comando router-id não tenha sido definido na configuração do roteador OSPF;
3. Valor do maior endereço IP das interfaces ativas do roteador, caso não existe nenhuma loopback.

Por que essa informação é importante?

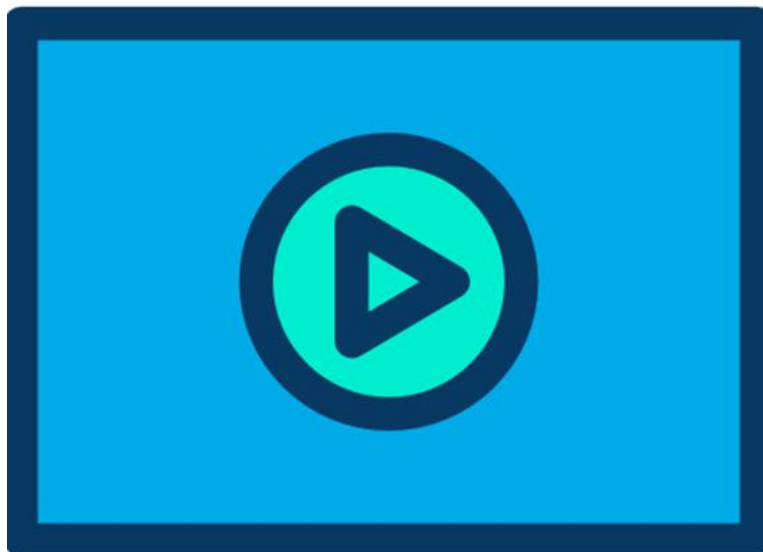
Porque o roteador monta seu processo em cima do RID, o qual deve ser único na rede.

Se você repetir esse valor terá problemas de instabilidade na rede, processos que sobem e caem.

O RID também é utilizado para definir quem será o DR e BDR em redes Multiacesso. O roteador com maior RID será o DR, o segundo maior o BDR e os demais DROTHER.

Você pode verificar quem é DR ou BDR em uma rede multiacesso com o comando **"show ip ospf neighbors"** ou **"show ip ospf interface"**.

8.5 Configuração do OSPF Single Area Com Comando Network



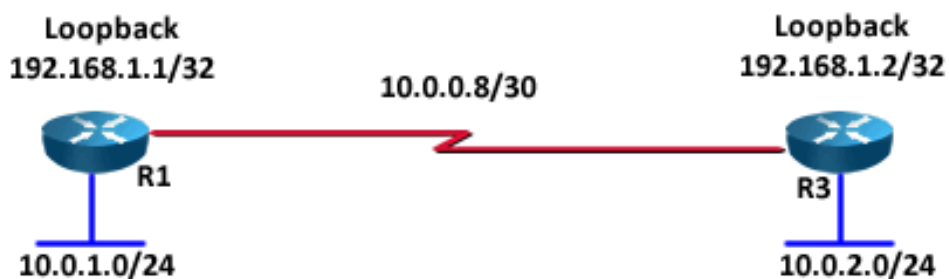
Vamos agora a um exemplo prático da configuração básica do OSPF seguindo a topologia mostrada na figura.

Vamos partir do princípio de que todas as interfaces foram configuradas corretamente, inclusive com o parâmetro bandwidth e vamos apenas configurar o OSPF.

Para configurar o OSPF básico vamos utilizar o passo a passo abaixo:

- Criar a interface loopback
- Definir as redes e máscaras curingas diretamente conectadas
- Entrar em modo de configuração do roteador OSPF
- Configurar o router-ID (mesmo IP definido na Loopback)
- Inserir as interfaces no processo de roteamento com o comando network
- Desativar o envio e recebimento de Hellos com o `passive-interface` em interfaces que não estão conectadas a outros roteadores OSPF

Veja a topologia do exemplo prático a seguir.



Vamos partir do princípio de que todas as interfaces foram configuradas corretamente, inclusive com o parâmetro bandwidth e vamos apenas configurar o OSPF.

Iniciando a config pelo roteador RA

Passo	1	-	Criando	a	loopback
RA#config					term
RA(config)#interface			loopback		0
RA(config-int)#ip		address	192.168.1.1		255.255.255.255
RA(config-int)#					

Passo 2 – Definindo as redes e máscaras curingas das redes diretamente conectadas

LAN	do	RA	-	10.0.1.0	/24	ou	255.255.255.0
Máscara curinga=	255.255.255.255 - 255.255.255.0 = 0.0.0.255						
WAN	RA	-		10.0.0.8	/30	ou	255.255.255.252
Máscara curinga=	255.255.255.255 - 255.255.255.252 = 0.0.0.3						

Passo 3 – Entrando na configuração do roteador OSPF e Configurando Router-ID

RA(config-int)#router		ospf		1
RA(config-router)#router-id	192.168.1.1			

Passo	4	-	Anunciando	as	redes
RA(config-router)#network		10.0.1.0	0.0.0.255	area	0
RA(config-router)#network		10.0.0.8	0.0.0.3	area	0

Passo 5 – Desativando Interfaces não Necessárias e Salvando a Configuração

RA(config-router)#passive-interface fast 0/0	
RA(config-router)#end	
RA#copy	running-config
RA#	startup-config

O comando passive-interface é utilizado para desativar o envio de recebimentos de Hellos e formação de adjacências, mas não do anúncio da interface no processo de roteamento.

Nesse exercício, como não temos outros roteadores OSPF na LAN simplesmente desativamos o envio de hellos nela e evitamos que adjacências indesejadas sejam formadas.

Outra maneira de configurar é em modo de configuração do roteador OSPF e digitar "passive-interface default", desabilitando o OSPF em todas as interfaces, depois liberar apenas as que devem formar adjacência com o comando "no passive-interface serial 0/0/0".

Configuração do roteador RB

RB#config					term
RB(config)#interface			loopback		0
RB(config-int)#ip		address	192.168.1.2		255.255.255.255
RB(config-int)#router ospf	1				
RB(config-router)#router-id					192.168.1.2
RB(config-router)#network		10.0.2.0	0.0.0.255	area	0
RB(config-router)#network	10.0.0.8 0.0.0.3 area 0				
RB(config-router)#passive-interface					fast0/0
00:02:51: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.1 on Serial0/0/0 from	LOADING				
to	FULL,		Loading		Done

```
RB (config-router) #end
RB#copy running-config startup-config
RB#
```

Quando o OSPF se comunicou e **trocou as informações** das LSAs corretamente, a mensagem que o estado foi alterado de Load para Full deve aparecer, indicando que o processo subiu, houve criação de adjacências e as LSP's (pacotes do link-state) foram trocadas **com sucesso**, conforme destacado em amarelo na saída das configurações do roteador RB.

8.5.1 Dicas sobre o Comando Network e Wildcard Mask

O comando network no OSPF exige uma máscara curinga e a área que aquela rede vai pertencer.

No "**OSPF Single Area**" a área fica sempre **zero**, pois se temos uma área só ela obrigatoriamente deve ser a área de backbone ou área zero.

Você pode definir as interfaces e redes que participarão no OSPF de duas maneiras: fechada pelas interfaces (IP mais máscara 0.0.0.0) ou aberta pela rede/sub-rede.

A maneira mais simples e segura de se configurar o comando network no OSPF é utilizando a máscara curinga (wildcard mask) 0.0.0.0 e fechar pelo IP das interfaces.

Portanto, esse tipo de configuração exige que utilizemos o endereço IP exato que está configurado em cada interface do roteador que precisa fazer parte do processo de roteamento do OSPF.

Por exemplo, o roteador tem o IP 192.168.1.1/24 configurado em sua interface fast0/0 e a rede dessa interface deve ser anunciada pelo OSPF, portanto o comando network fechado para a interface será "network 192.168.1.1 0.0.0.0 area 0".

Resumindo, fechado pelo IP você precisará anunciar todos os IPs configurados nas interfaces que devem ter suas redes anunciadas pelo OSPF.

Essa forma de configurar o comando network torna mais simples e mais seguro sabermos que interfaces estão ativadas no roteamento OSPF.

Podemos também utilizar máscaras curingas mais complexas para definição das possíveis interfaces que podem ser ativadas no OSPF e fazer um comando network aberto pela Rede/Sub-rede.

Por exemplo, temos a interface com o IP 192.168.1.1/28 (255.255.255.240) e queremos que sua rede seja anunciada na área zero, podemos criar o comando network definindo a sub-rede inteira diminuindo o broadcast (255.255.255.255) da máscara de sub-rede: 255.255.255.255 - 255.255.255.240 = 0.0.0.15, portanto o comando será: "network 192.168.1.0 0.0.0.15 area 0".

Veja que essa configuração implica que quaisquer interfaces na faixa de endereços da sub-rede de 192.168.1.1 até 192.168.1.14 se configuradas no roteador farão parte do processo de roteamento.

Outra forma de fazer o comando network aberto pela rede é anunciando a rede classful inteira, porém não é muito usual nem recomendado.

Por exemplo, você usa as sub-redes 10.0.0.0/24, 10.0.1.0/24 e 10.0.2.0/24, portanto poderia fazer um comando anunciando a rede 10 cheia: "network 10.0.0.0 0.255.255.255 area 0".

Assim qualquer IP de 10.0.0.1 a 10.255.255.254 se configurado em uma interface UP fará parte do processo de roteamento e a rede configurada na interface será anunciada pelo OSPF.

Por último tem a configuração "network de preguiçoso", essa é a menos indica, mas na pressa funciona muito bem (*risos*)... Basta você anunciar a Internet toda no comando, ou seja, em termos de IP seria a rede 0.0.0.0 com a máscara 0.0.0.0 (0.0.0.0/0).

Se transformarmos isso em máscara curinga fica "0.0.0.0 255.255.255.255", ou seja, "network 0.0.0.0 255.255.255.255 area 0".

Com esse comando quaisquer interfaces UP entrarão no processo de roteamento e terão suas redes/sub-redes anunciadas pelo OSPF.

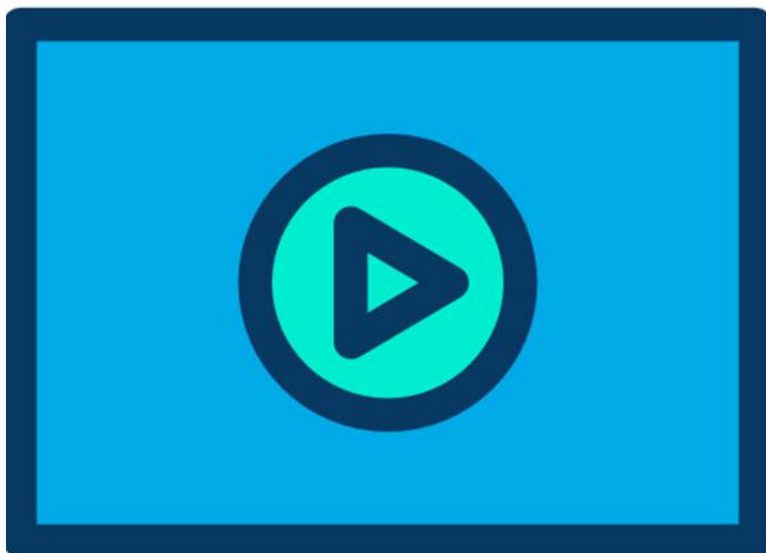
Por isso mesmo esse método é o menos seguro de todos, não utilize na sua empresa, apenas em laboratório, combinado?

Você pode também encontrar questões onde será necessária a análise reversa, por exemplo, dado um comando network ou um "show ip protocols" achar que interfaces do roteador entrarão no processo de roteamento.

Lembre-se que nesses casos a máscara curinga que utilizamos no OSPF é a mesma que utilizamos nas ACLs, ou seja, onde é **zero** quer dizer que deve haver correspondência e onde temos **bit um** tanto faz.

Se o assunto ficou confuso por causa das máscaras curinga siga em frente mesmo assim, pois teremos mais para frente no curso de Segurança da trilha do CCNA um capítulo sobre ACL e você vai com certeza dominar as máscaras curinga.

8.5.2 Verificando as Configurações do OSPF



Para verificar as configurações utilize o comando **"show running-config"**, para mostrar a tabela de roteamento o **"show ip route"** e para manter o OSPF utilize os comandos **"show ip ospf ..."**.

```
RA#show ip ospf ?
      <1-65535>
border-routers  Border
database
interface
neighbor
virtual-links  Virtual

Process and Boundary Router ID
Database
Interface
Neighbor link
Information summary information list information
<cr>
```

RA#

Os dois comandos mais importantes são o **"show ip ospf neighbor"** e **"show ip ospf interface"**.

O comando **"show ip ospf neighbor"** mostrará a "tabela de vizinhança" (neighbor table), onde são listados os vizinhos diretamente conectados do seu roteador com o estado da adjacência. Veja a saída do comando a seguir.

```
RA#sho ip ospf neighbor
Neighbor ID    Pri   State           Dead Time   Address      Interface
192.168.1.2    0     FULL/ -         00:00:39   10.0.0.10    Serial0/0/0
RA#
```

O Roteador ID do vizinho é mostrado no campo **"Neighbor ID"**, o parâmetro PRI refere-se à prioridade do roteador vizinho e o State em Full representa que uma vizinhança foi estabelecida por completo com esse roteador mostrado no comando, se um status diferente aparecer pode significar que existem problemas no estabelecimento da vizinhança.

Normalmente esse problema de estabelecimento de vizinhanças está relacionado aos valores dos timers de Hello e Dead, os quais devem ser os mesmos em ambos os roteadores e veremos com o próximo comando no slide seguinte.

O campo Dead Time indica quanto tempo o roteador espera para considerar que o seu vizinho "morreu" e retirá-lo da sua base de dados.

Os campos Address e Interface são referentes ao roteador remoto, ou seja, são o endereço IP da interface que o roteador utilizou para fazer a vizinhança e o número dessa interface.

No comando "**show ip ospf interface**" você poderá verificar o tipo de rede, prioridade do OSPF, roteador ID, quem é DR e BDR, custo do link, timers de hello e dead e outras informações.

```
RA#show ip ospf interface
Serial0/0/0 is up, line protocol is up
  Internet address is 10.0.0.9/30, Area 0
  Process ID 1, Router ID 192.168.1.1, Network Type POINT-TO-POINT, Cost: 125
  Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:04
  Index 1/1, flood queue length 0
    Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 192.168.1.2
  Suppress hello for 0 neighbor(s)
FastEthernet0/0 is up, line protocol is up
  Internet address is 10.0.1.1/24, Area 0
  Process ID 1, Router ID 192.168.1.1, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 192.168.1.1, Interface address 10.0.1.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:06
  Index 2/2, flood queue length 0
    Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
RA#
```

Observe acima os campos em destaque os quais são explicados na sequência abaixo para a interface serial Ponto a Ponto:

- **Roteador ID 192.168.1.1**→ Indica qual o ID do roteador, o qual normalmente é o endereço IP da interface de Loopback configurada ou o maior IP do roteador se não configurarmos uma Loopback.
- **Network Type POINT-TO-POINT**→ Indica o tipo de rede, com essa informação saberemos se vai ou não haver a necessidade de eleição de DR e BDR (somente para redes LAN ou WAN com Frame-relay NBMA).
- **Cost: 125**→ Custo acumulado do caminho, lembrando que o custo de cada caminho é $10^8/\text{Bandwidth}$, por isso temos que nos certificar se o comando bandwidth foi configurado corretamente nas interfaces seriais. Para as interfaces de LAN não é necessário inserir o bandwidth. A velocidade do link WAN configurado foi de 800kbps, portanto o custo da interface será $1000000000/800000 = 125$. Para a rede LAN temos uma interface Fastethernet, ou seja, $1000000000/100000000$
- **Priority 0**→ Indica a prioridade configurada para a interface, esse parâmetro será estudado quando configurarmos redes que exigem eleição de DR e BDR.
- **No designated roteador on this network / No backup designated roteador on this network**→ Se houver eleição de DR/BDR nesse campo será mostrado os IDs dos roteadores eleitos.
- **Timer intervals configured, Hello 10, Dead 40**→ Valores dos contadores de hello e dead, os quais devem ser iguais em ambas as pontas para que seja formada uma adjacência. Se esses valores forem diferentes o OSPF entre os vizinhos não irá subir.

Note as diferenças dos campos descritos acima para a interface fastethernet 0/0:

```
FastEthernet0/0 is up, line protocol is up
Internet address is 10.0.1.1/24, Area 0
Process ID 1, Roteador ID 192.168.1.1, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State DR, Priority 1
Designated Roteador (ID) 1.1.1.1, Interface address 10.0.1.1
No backup designated roteador on this network
Timer intervals configured, Hello 10, Dead 40
```

Como a interface fast é uma interface do tipo broadcast multiacesso, mesmo não tendo outro roteador nessa LAN ela faz a eleição de DR/BDR assumindo o papel de DR.

Note que o ID de Designated Roteador é igual ao próprio Roteador ID do roteador, pois ele mesmo se elegeu como DR.

Vamos agora analisar o comando **show ip route**. Veja que a métrica ou o custo acumulado para chegar até a rede LAN do vizinho RB é de 126, ou seja, 125 da rede WAN mais 1 da rede LAN.

```
RA#sho ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
Gateway of last resort is not set
10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C 10.0.0.8/30 is directly connected, Serial0/0/0
C 10.0.1.0/24 is directly connected, FastEthernet0/0
O 10.0.2.0/24 [110/126] via 10.0.0.10, 00:02:44, Serial0/0/0
192.168.1.0/32 is subnetted, 1 subnets
C 192.168.1.1 is directly connected, Loopback0
RA#
```

Você também pode utilizar o comando **"show ip route ospf"** para ver apenas as rotas aprendidas pelo protocolo OSPF, veja exemplo abaixo.

```
RoteadorB#show ip route ospf
10.0.0.0/24 is subnetted, 5 subnets
O 10.0.0.0 [110/101] via 192.168.1.6, 00:00:10, Serial0/0/0
O 10.0.1.0 [110/101] via 192.168.1.6, 00:00:10, Serial0/0/0
O 10.0.4.0 [110/101] via 192.168.1.9, 00:00:10, Serial0/0/1
192.168.1.0/30 is subnetted, 3 subnets
O 192.168.1.0 [110/1662] via 192.168.1.6, 00:00:10, Serial0/0/0
O*E2 0.0.0.0/0 [110/1] via 192.168.1.9, 00:00:10, Serial0/0/1
```


Outro comando interessante é o "show ip ospf", pois nele você tem dados básicos sobre a configuração e também do cálculo do algoritmo SPF. Veja exemplo a seguir tirado do roteador da vídeo aula referente a esse tópico.

R1#sho ip ospf**Routing Process "ospf 1" with ID 192.168.1.1**

Start time: 00:07:45.714, Time elapsed: 00:08:07.686

Supports only single TOS(TOS0) routes

Supports opaque LSA

Supports Link-local Signaling (LLS)

Supports area transit capability

Supports NSSA (compatible with RFC 3101)

Event-log enabled, Maximum number of events: 1000, Mode: cyclic

Router is not originating router-LSAs with maximum metric

Initial SPF schedule delay 5000 msec

Minimum hold time between two consecutive SPF's 10000 msec

Maximum wait time between two consecutive SPF's 10000 msec

Incremental-SPF disabled

Minimum LSA interval 5 secs

Minimum LSA arrival 1000 msec

LSA group pacing timer 240 secs

Interface flood pacing timer 33 msec

Retransmission pacing timer 66 msec

Number of external LSA 0. Checksum Sum 0x000000

Number of opaque AS LSA 0. Checksum Sum 0x000000

Number of DCbitless external and opaque AS LSA 0

Number of DoNotAge external and opaque AS LSA 0

Number of areas in this router is 1. 1 normal 0 stub 0 nssa

Number of areas transit capable is 0

External flood list length 0

IETF NSF helper support enabled

Cisco NSF helper support enabled

Reference bandwidth unit is 100 mbps

Area BACKBONE(0) (Inactive)**Number of interfaces in this area is 4 (1 loopback)**

Area has no authentication

SPF algorithm last executed 00:07:14.068 ago**SPF algorithm executed 4 times**

Area ranges are

Number of LSA 1. Checksum Sum 0x00E03A

Number of opaque link LSA 0. Checksum Sum 0x000000

Number of DCbitless LSA 0

Number of indication LSA 0

Number of DoNotAge LSA 0

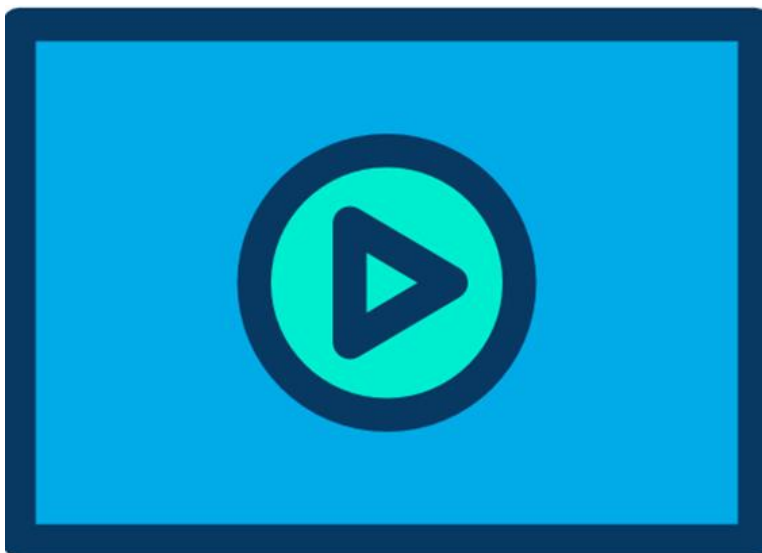
Flood list length 0

Nas opções destacadas você vai ter:

- Process-ID e o Router-ID: Routing Process "ospf 1" with ID 192.168.1.1
- Número de áreas configuradas: Number of areas in this router is 1. 1 normal 0 stub 0 nssa
- As características das áreas, nesse caso apenas a área de Backbone ou área zero:
 - Area BACKBONE(0) (Inactive)
 - Número de interfaces configuradas: Number of interfaces in this area is 4 (1 loopback)
 - Quando o algoritmo do SPF rodou pela última vez: SPF algorithm last executed 00:07:14.068 ago
 - Quantas vezes ele foi executado para a área zero: SPF algorithm executed 4 times

Note que se o algoritmo SPF está sendo executado muitas vezes é sinal que há instabilidade em uma ou mais interfaces daquela área em específico, pois ele é executado por área.

8.6 Configurando OSPFv2 via Interface



Existe uma novidade na configuração do OSPF que evita o uso do comando network e de máscaras curinga para definir as interfaces que farão parte do processo de roteamento.

Ao invés disso, você define a área e as interfaces que farão parte dessas áreas diretamente em modo de configuração de interface, não necessitando mais do uso da máscara curinga.

O resultado acaba sendo o mesmo que da configuração indireta das interfaces que farão parte do processo do OSPF via comando network, porém bem mais simples porque economizamos alguns cálculos de máscara curinga.

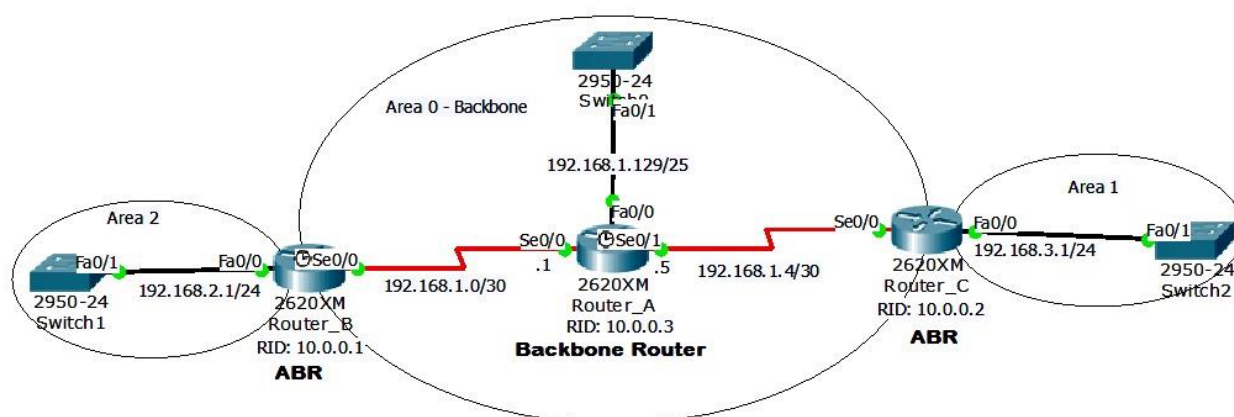
Apesar disso, as definições mais avançadas como passive-interface, router-ID, anúncio de rota padrão e outras continuam necessitando ser realizadas em modo de configuração do protocolo de roteamento.

Portanto, os passos de configuração para seguir podem ser resumidos em:

1. Crie a interface loopback que será utilizada como router-ID
2. Ative o processo de roteamento OSPF definindo o process-ID
3. Configure o router-ID, passive interface e anúncio da rota padrão (se necessário_ dentro do modo do roteador OSPF
4. Entre em modo de interface e defina a área com o comando **"ip ospf process-id area area-id"**

Note que os passos 1, 2 e 3 são os mesmos que configuramos, portanto vamos passar um exemplo de configuração do roteador C apresentado no tópico passado com essa nova forma de configuração.

Vamos considerar que os endereços IP das interfaces serial e fastethernet já estão configurados.



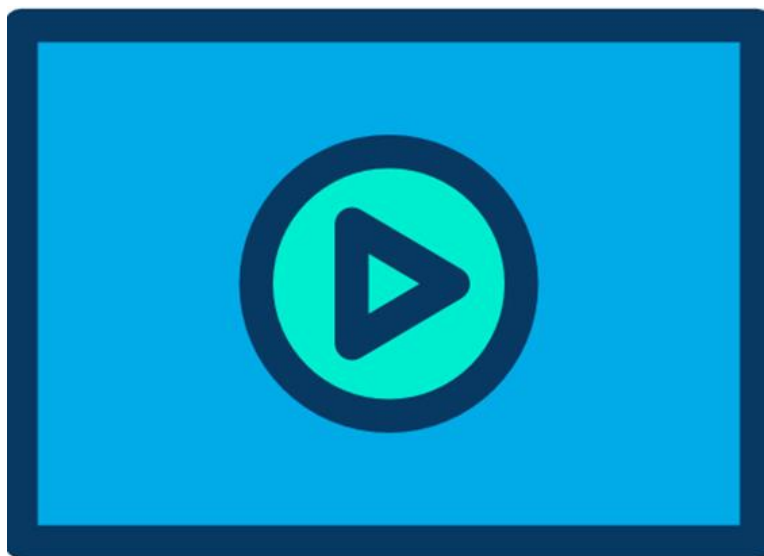
Configuração do Roteador C – Área 1

```
Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname Roteador_C
Roteador_C(config-if)#int loopback 0
Roteador_C(config-if)#ip add 10.0.0.2 255.255.255.255
Roteador_A(config-if)#int f0/0
Roteador_C(config-if)#exit
Roteador_C(config)#router ospf 1
Roteador_A(config-router)#router-id 10.0.0.2
Roteador_A(config-router)#passive-interface fast0/0
Roteador_C(config-router)#exit
Roteador_C(config)#int s0/0
Roteador_C(config-if)#ip ospf 1 area 0
Roteador_C(config-if)#
Roteador_A(config-if)#int f0/0
Roteador_A(config-if)# ip ospf 1 area 1
```

Você não precisa obrigatoriamente seguir os passos 1, 2 e 3, porém aí o OSPF vai ficar com a configuração padrão do router-ID que é o maior IP de loopback configurada se ela existir, senão o router-ID será o maior IP configurado em uma interface ativa.

Apesar de ter sido mostrado no item de OSPF Multiarea a configuração via interface funciona também para o OSPF Single Area, basta definir a "área 0" em todas as interfaces.

8.7 Detalhando a Eleição do DR e BDR em Redes Broadcast



Já estudamos que em **redes multiacesso** com ou sem broadcast (Ethernet, Fastethernet e Frame-relay NBMA) será necessária "a eleição" ou escolha de um **roteador designado** (DR ou Designated Roteador) e um roteador para ser seu **backup** (BDR ou Backup Designated Roteador), mas porque isso precisou ser implementado nesses tipos de rede?

O que essa utilização de um roteador designado e seu backup traz de melhorias?

A eleição de um roteador designado e um backup em redes multiacesso se dá pela possibilidade de termos diversos roteadores OSPF configurados na mesma rede e a formação de adjacência entre eles consumiria muita largura de banda dessa rede LAN ou WAN NBMA.

Por exemplo, em uma rede ponto a ponto os dois vizinhos precisam formar adjacência somente entre si, já em uma rede Fastethernet com cinco roteadores OSPF cada um deles precisaria formar 4 adjacências com seus vizinhos, como temos 5 roteadores seriam 20 conexões entre eles.

Agora imagine isso em um Data Center com 100 roteadores, seriam 99 adjacências por roteador vezes 100 roteadores, ou seja, 9900 conexões para troca de informação sobre o OSPF!

Por esse motivo foram criadas as funções de DR e BDR, para que os roteadores pudessem formar adjacência somente com dois outros dispositivos, economizando banda em redes multiacesso. Portanto, o roteador DR serve como ponto central para receber e enviar as LSAs entre os demais roteadores.

O BDR serve como backup para caso o DR fique indisponível não seja preciso recalculer todas as rotas novamente, pois o BDR tem uma cópia da base de dados topológica do DR.

Essa eleição é realizada com o **protocolo de Hello** do OSPF e escolhe-se o roteador com maior Priority ID ou com maior Router ID.

O priority ID padrão é 1, podendo ser configurada de 0 a 255.

Já o router ID é o valor configurado no comando "router-id" ou o maior endereço de Loopback (se existir interface loopback configurada) ou o maior endereço IP configurado no roteador, nessa sequência de preferência.

A eleição é feita por rede ou sub-rede Broadcast ou NBMA.

O comando para alterar a prioridade deve ser inserido por interface, abaixo segue a sintaxe:

```
Router(config-if)#ip ospf priority 100
```

A prioridade 0 evita que o roteador participe da eleição de DR e BDR. O valor máximo para a prioridade é 255.

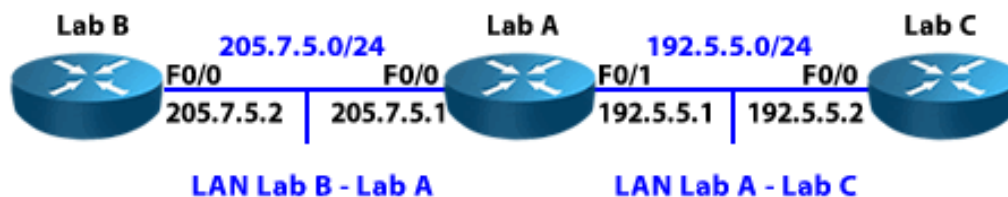
Quando o DR é eleito, ele permanece como DR até que ele falhe, o processo OSPF no DR falhe ou a interface multiacesso no DR falhe.

É possível influenciar o processo de eleição do DR & BDR das seguintes maneiras:

- Ligando o roteador DR primeiro, seguido do BDR, e depois ligue todos os outros roteadores.
- Colocando em Shutdown todas as interfaces em todos os roteadores, seguido de um "no shutdown" no DR, depois no BDR, e depois nos outros roteadores.

8.7.1 Exemplo de Eleição de DR e BDR

Vamos ver no exemplo a seguir o processo de eleição de DR e BDR. Parte-se do pressuposto que todas as demais configurações estão realizadas e em perfeito estado.



Configuração do Lab_A

```
hostname                               Lab_A
interface                               FastEthernet0/0
ip address 205.7.5.1                    255.255.255.0
duplex auto
speed auto
!
interface                               FastEthernet0/1
ip address 192.5.5.1                    255.255.255.0
duplex auto
speed auto
!
router ospf 1
network 192.5.5.0 0.0.0.255 area 0
network 205.7.5.0 0.0.0.255 area 0
```

Configuração do Lab_B

```

hostname                               Lab_B
interface                               FastEthernet0/0
ip address                             205.7.5.2      255.255.255.0
duplex                                 auto
speed                                 auto
!
router ospf                             1
network 205.7.5.0 0.0.0.255 area 0

```

Configuração do Lab_C

```

hostname                               Lab_C
interface                               FastEthernet0/0
ip address                             192.5.5.2      255.255.255.0
duplex                                 auto
speed                                 auto
!
router ospf                             1
network 192.5.5.0 0.0.0.255 area 0

```

Analisando as configurações mostradas responda as questões abaixo:

1. Qual a prioridade de cada roteador?
2. Qual o router ID de cada roteador?
3. Quem será o DR para a rede 205.7.5.0? E o BDR?
4. Quem será o DR para a rede 192.5.5.0? E o BDR?

O comando **"show ip ospf interface"** abaixo ajudará a responder essas questões, apesar de ser possível chegar aos resultados apenas analisando as configurações.

Portanto sabemos que a prioridade de cada roteador é 1, pois não foi alterado o padrão. Já o roteador ID é o maior IP do roteador, pois não temos interfaces de Loopback configuradas.

Analisando os IPs dos roteadores podemos chegar a conclusão que o Roteador-ID do Lab_A é 205.7.5.1, do Lab_B é 205.7.5.2 e do Lab_C é 192.5.5.2, pois esses são os maiores IPs configurados em cada roteador.

Agora podemos definir quem será eleito DR e BDR por rede ou subrede IP LAN, pois no caso da rede 205.7.5.0, a qual está entre A e B, o roteador Lab_B tem maior roteador ID, sendo escolhido como DR e o Lab_A como BDR, pois não tem outro roteador na rede.

Já para a rede 192.5.5.0 o DR é o Lab_A, pois ele tem o maior roteador ID, ficando como BDR o Lab_C.

Os demais roteadores que não são DR nem BDR serão chamados de DROTHER.

Analise a saída do comando **show ip ospf interface** e confirme a análise que fizemos anteriormente.

```

LAB_A#show ip ospf interface
FastEthernet0/0 is up, line protocol is up
  Internet Address 205.7.5.1/24, Area 0
    Process ID 1, Router ID 205.7.5.1, Network Type BROADCAST, Cost: 1
      Transmit Delay is 1 sec, State BDR, Priority 1
    Designated Router (ID) 205.7.5.2, Interface address 205.7.5.2

```

```

Backup Designated router (ID) 205.7.5.1, Interface address 205.7.5.1
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
      Hello due in 00:00:02
      Index 2/2, flood queue length 0
      Next 0x0(0)/0x0(0)
      Last flood scan length is 2, maximum is 2
      Last flood scan time is 0 msec, maximum is 0 msec
      Neighbor Count is 1, Adjacent neighbor count is 1
      Adjacent with neighbor 205.7.5.2 (Designated Router)
      Suppress hello for 0 neighbor(s)
FastEthernet0/1 is up, line protocol is up
      Internet Address 192.5.5.1/24, Area 0
      Process ID 1, Router ID 205.7.5.1, Network Type BROADCAST, Cost: 1
      Transmit Delay is 1 sec, State DR, Priority 1
      Designated Router (ID) 205.7.5.1, Interface address 192.5.5.1
Backup Designated router (ID) 192.5.5.2, Interface address 192.5.5.2
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
      Hello due in 00:00:07
      Index 1/1, flood queue length 0
      Next 0x0(0)/0x0(0)
      Last flood scan length is 2, maximum is 2
      Last flood scan time is 0 msec, maximum is 0 msec
      Neighbor Count is 1, Adjacent neighbor count is 1
      Adjacent with neighbor 192.5.5.2 (Backup Designated Router)
Suppress hello for 0 neighbor(s)

```

Resumindo, para eleger o DR e BDR o OSPF utiliza os seguintes parâmetros em ordem de prioridade:

- **Priority**→ Prioridade configurada na interface, quem tem o maior valor é escolhido como DR. Caso a prioridade não tenha sido configurada o valor padrão é 1 e não serve como critério de eleição.
- **Maior "router-id"**→ lembre-se que o router ID é em ordem de preferência o valor configurado no comando "router-id", maior IP entre as interfaces loopback configuradas ou maior endereço IP válido entre as interfaces ou sub-interfaces configuradas.

Você também pode forçar uma eleição de determinado roteador como DR e BDR alterando o parâmetro "ip ospf priority" dentro do modo de configuração de interface. Exemplo:

```

Router#conf
Router(config)#int
Router(config-if)#ip
Router(config-if)#^Z
Router#

```

t
0/0
priority 100

8.8 Anunciando a Rota Padrão pelo OSPF

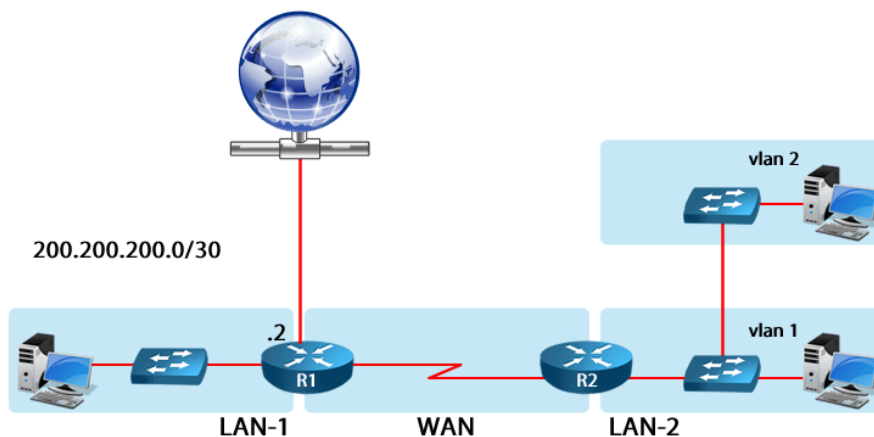


Para fazer com que a rota padrão seja anunciada diretamente pelo OSPF a partir do roteador conectado à Internet utilize o comando **"default-information originate"** dentro do modo de configuração do OSPF.

A rota padrão deve ter sido configurada via roteamento estático nesse roteador.

Veja a topologia a seguir onde o roteador R1 está conectado com a Internet.

Para que a rota padrão seja anunciada diretamente pelo OSPF precisamos apenas configurar normalmente uma rota estática padrão em R1 e depois inserir o comando citado no parágrafo anterior dentro da configuração do OSPF no roteador R1.



Veja a configuração necessária para toda a rede conhecer a Internet, considerando que o OSPF já está configurado e rodando normalmente.

```
R1#conf
R1(config)#ip route 0.0.0.0 0.0.0.0 200.200.200.1
R1(config)#router ospf 1
R1(config-router)#default-information originate
R1(config-router)#^Z
R1#
```

Apenas com a configuração acima, a rota padrão aprendida através do roteador R1 será passada dinamicamente pelo OSPF para os demais roteadores como uma rota Externa do tipo 2, marcada por padrão como "O E2".

Sem essa configuração, o administrador de redes teria que entrar roteador por roteador e configurar manualmente uma saída padrão!

8.9 Balanceamento de Cargas no OSPF

Até o momento consideramos que temos apenas uma rota para determinada rede de destino com a melhor métrica, mas o que acontece se o OSPF encontrar duas rotas para um mesmo destino com a mesma métrica, ou seja, com o mesmo custo?

Por padrão o OSPF faz o balanceamento de cargas (em inglês Load Balancing) entre até quatro rotas por padrão, podendo ser aumentado até 6 em IOSs mais antigos (versão 12.x) e na versão 15 maioria suporta um máximo de 32 rotas balanceando cargas.

Podemos verificar essa informação no comando **"show ip protocols"** no campo "Maximum path", veja exemplo abaixo.

```
R1#show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 1.1.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Maximum path: 4
  Routing for Networks:
    172.16.1.0 0.0.0.255 area 0
    192.168.1.0 0.0.0.3 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    2.2.2.2          110          00:59:05
  Distance: (default is 110)

R1#
```

Para alterar esse comportamento precisamos entrar em modo de configuração de roteamento e utilizar o comando "maximum-paths". Veja exemplo abaixo onde vamos desativar o balanceamento de cargas.

```
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#router ospf 1
R1(config-router)#maximum-paths ?
<1-32> Number of paths

R1(config-router)#maximum-paths 1
R1(config-router)#
```

Com o valor do maximum-path igual a 1 o roteador balanceia carga com um link, ou seja, só a melhor métrica funciona.

Nessa versão de IOS utilizada o roteador suporta até 32 rotas fazendo o **Equal Cost Load Balancing** (balanceamento de carga entre rotas de mesmo custo).

O OSPF não suporta balanceamento de cargas entre métricas de custos diferentes, esse recurso somente o EIGRP suporta.

Você pode alterar a métrica entre duas rotas no OSPF para forçar um balanceamento de cargas se for necessário.

O balanceamento de carga pode ser confirmado no comando show ip route, veja exemplo abaixo.

```
Matriz-B#sho ip rou
### Saídas omitidas ###

Gateway of last resort is 10.0.0.1 to network 0.0.0.0

    10.0.0.0/24 is subnetted, 5 subnets
C      10.0.0.0 is directly connected, FastEthernet0/0
C      10.0.1.0 is directly connected, FastEthernet0/1
O      10.0.2.0 [110/102] via 10.0.0.1, 00:09:15, FastEthernet0/0
O      10.0.3.0 [110/102] via 10.0.0.1, 00:09:15, FastEthernet0/0
    192.168.0.0/32 is subnetted, 1 subnets
C      192.168.0.20 is directly connected, Loopback0
    192.168.1.0/30 is subnetted, 3 subnets
O      192.168.1.0 [110/1563] via 10.0.0.1, 00:09:15, FastEthernet0/0
O      192.168.1.4 [110/101] via 10.0.0.1, 00:09:15, FastEthernet0/0
O*E2 0.0.0.0/0 [110/1] via 10.0.0.1, 00:09:15, FastEthernet0/0
      [110/1] via 10.0.1.1, 00:09:15, FastEthernet0/1
```

Note que a rota padrão está sendo balanceada, pois ela tem duas entradas na tabela de roteamento, uma apontando para a fast 0/0 e a segunda apontando para a fast 0/1, indicando que os pacotes com destino à Internet serão balanceados através dessas duas interfaces.

Outra maneira de observar as informações sobre o balanceamento de cargas é com o comando `show ip route` e depois seguido da rede em questão que você deseja analisar, veja exemplo abaixo.

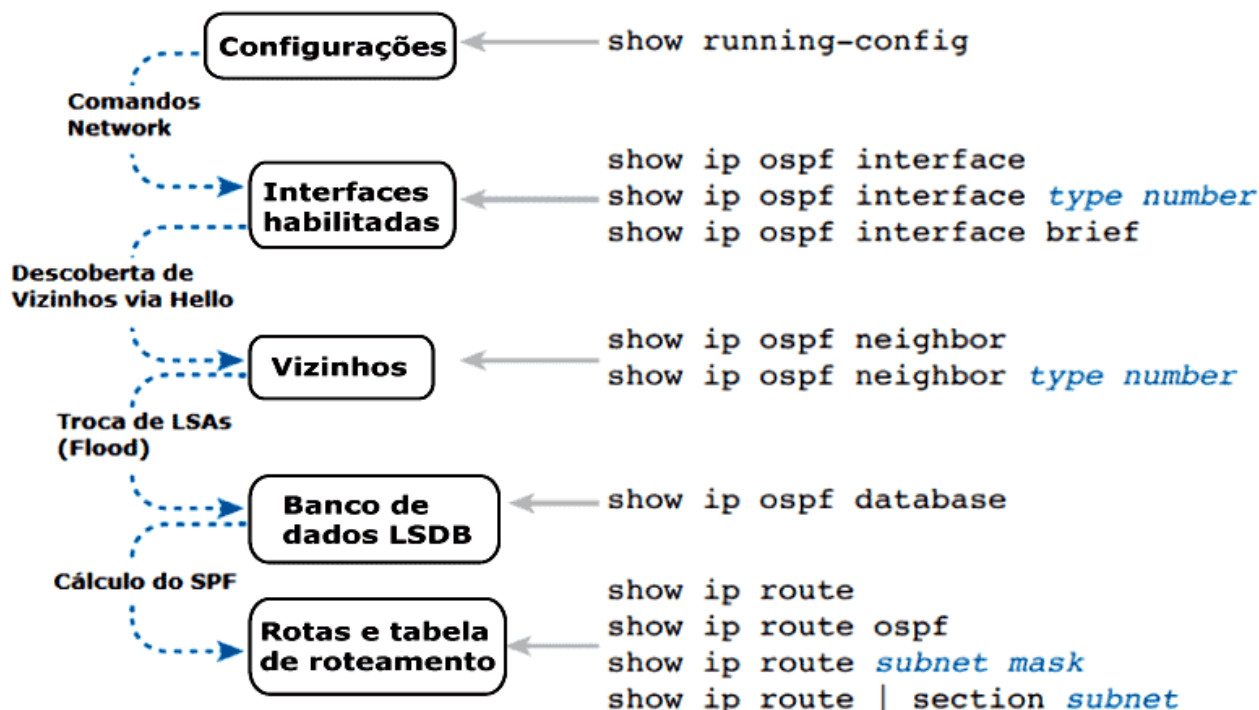
```
Matriz-B#show ip route 0.0.0.0
Routing entry for 0.0.0.0/0, supernet
Known via "ospf 1", distance 110, metric 1, candidate default path
  Tag 1, type extern 2, forward metric 1
  Last update from 10.0.0.1 on FastEthernet0/0, 00:09:32 ago
Routing Descriptor Blocks:
* 10.0.0.1, from 192.168.0.3, 00:09:32 ago, via FastEthernet0/0
  Route metric is 1, traffic share count is 1
  10.0.1.1, from 192.168.0.3, 00:09:32 ago, via FastEthernet0/1
  Route metric is 1, traffic share count is 1
Matriz-B#
```

Temos a indicação que os pacotes para a Internet estão sendo balanceados através da fast 0/0, enviando para o próximo salto 10.0.0.1.

Além disso, ela traz que foi aprendida via o ASBR 192.168.0.3, RID do roteador Filial-2. Logo abaixo tem a segunda interface que está balanceando cargas via 10.0.1.1 pela fast 0/1.

8.10 Resumo dos Comandos Show para OSPF

A seguir temos uma figura com os comandos e em que situação podemos utilizar cada um deles.



Portanto, essa divisão é bem didática pois começa com o `show running-config` para ajudar a revisar os comandos aplicados, depois precisamos verificar se o comando `network` realmente adicionou ao processo de roteamento as interfaces corretamente (interfaces habilitadas).

Com as interfaces corretamente adicionadas ao processo no comando network e os requisitos para formação de vizinhança satisfeita devem-se formar vizinhanças, as quais podem ser verificadas com os comandos que apontam para a caixa "Vizinhos".

Após a formação de vizinhança os roteadores devem trocar suas LSAs para montar o banco de dados de LSAs (LSDB – Link State Data Base).

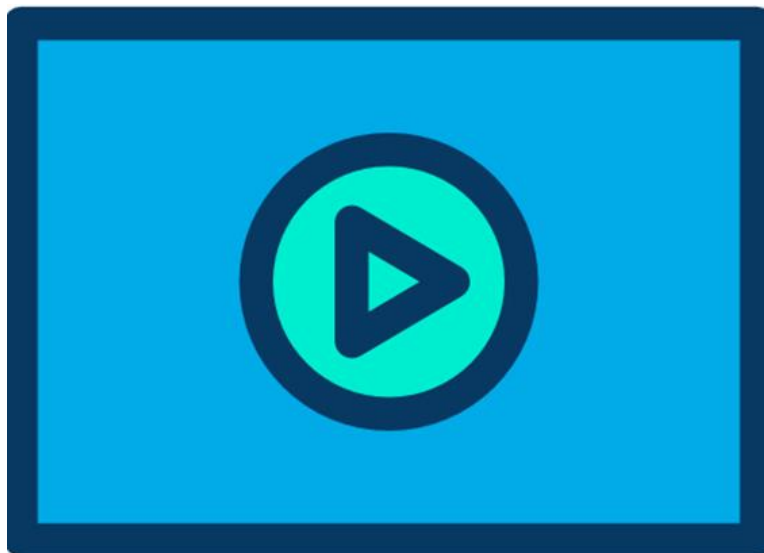
Uma vez montado o banco de dados devemos verificar as rotas na tabela de roteamento com os comandos descritos em rotas e tabela de roteamento.

8.11 Resumo dos Comandos de Configuração Utilizados no OSPF

- **router ospf process-id** -> cria o processo OSPF com um ID ou entra em um processo criado com determinado PID (ID de processo).
- **network end-IP masc-curinga area area-id** -> ativa interfaces que batam com o IP e a máscara curinga no processo do OSPF, ou seja, as redes dessas interfaces passarão a ser anunciadas.
- **ip ospf process-id area area-id** -> define a área da interface OSPF em modo de interface, sem necessidade do uso do comando Network.
- **ip ospf cost custo** -> define um custo manual para uma interface OSPF, deve ser aplicado em modo de interface.
- **bandwidth banda/kpbs** -> as interfaces devem ter o comando bandwidth (Kbps) definido ou senão a banda considerada na serial pelo OSPF será de um link T1 (1,5Mbps).
- **auto-cost reference-bandwidth valor** -> altera a referência do cálculo do custo, por padrão definida como uma interface de 100Mbps.
- **router-id id-IPv4** -> define um router ID manualmente para o OSPF.
- **interface loopback número** -> cria uma interface loopback.
- **maximum-paths num-de-caminhos** -> define o número máximo de links que podem fazer balanceamento de cargas caso o custo entre eles para uma mesma rede seja igual. Por padrão vem configurado com o valor 4.
- **passive-interface tipo num** -> desabilita envio e recebimento de hellos na interface listada no comando.
- **passive-interface default** -> desabilita envio e recebimento de hellos em todas as interfaces do roteador.
- **no passive-interface tipo num** -> ativa envio e recebimento de hellos em uma interface desabilitada pelos dois comandos anteriores.

9 First Hop Redundancy Protocols (FHRP)

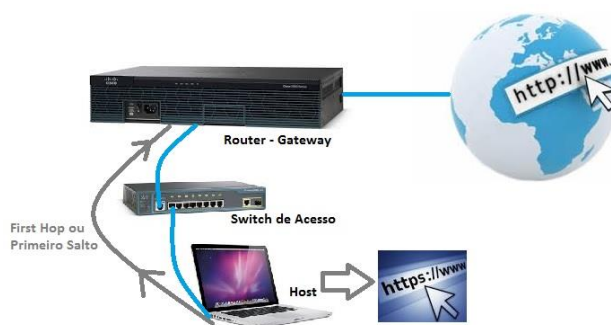
9.1 Introdução



O que é First Hop? Já ouviu falar sobre esse termo?

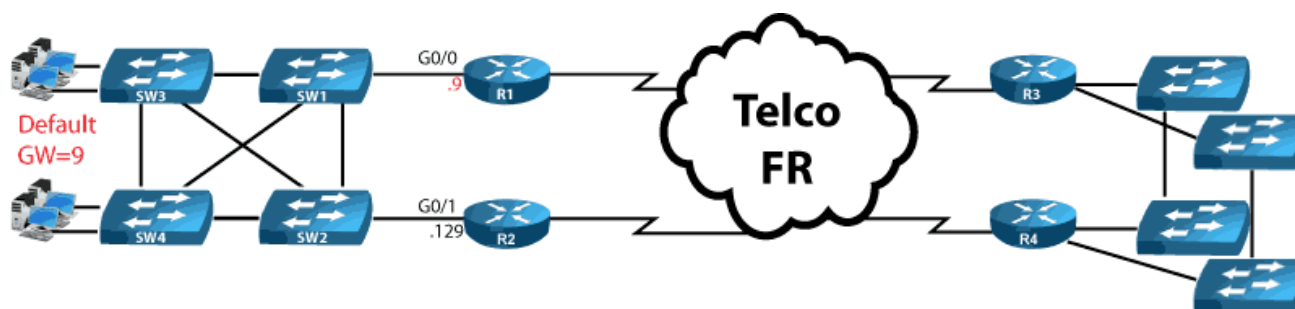
Em português significa primeiro salto, ou seja, é o primeiro salto que um host dá na rede para acessar os recursos daquela rede.

Normalmente o primeiro salto em camada-3 de um PC será para seu Default-Gateway, correto?



Na topologia acima, o que ocorre se o Gateway cair? Os PCs ficarão sem acesso aos recursos da Internet e da Intranet conectadas ao Gateway, concorda?

Como podemos resolver esse problema? Simples, colocando outro gateway como mostrado na topologia abaixo. Veja que temos dois Gateways: R1 com IP 192.168.1.9 e R2 com IP 192.168.1.129.



Como o DHCP nos passa um gateway, os PCs tem atualmente o roteador R1 com o IP 192.168.1.9 como seu gateway padrão.

Mesmo com toda essa redundância o que vai acontecer, por exemplo, quando o roteador R1 cair, com os computadores que tem seu endereço IP como gateway padrão? As opções que conhecemos até o momento seriam:

1. Ao cair R1, entrar nos computadores locais ou no servidor DHCP e alterar manualmente o endereço do gateway padrão para o endereço "**192.168.1.129**" referente à R2.
2. Quando R2 for reestabelecido teremos que fazer o processo contrário, ou seja, voltar à condição anterior do gateway configurando os computadores, um a um, manualmente ou através da alteração do gateway no servidor DHCP.

Esse procedimento deveria ser realizado toda vez que R1, seu link com a LAN ou com a WAN ficasse indisponível.

Você poderia pensar também em inserir um segundo gateway na placa de rede dos clientes, porém essa solução não funciona na maioria dos sistemas operacionais e o host acaba tendo problemas de conectividade.

Os protocolos classificados como **FHRP** ou **First Hop Redundancy Protocol** tratam esse problema que pode ocorrer no primeiro salto dos hosts, ou seja, entre o computador do usuário final e seu gateway padrão.

Mas como isso pode ser feito? Simplificando o assunto ao máximo, imagine que pudéssemos configurar um mesmo endereço IP e MAC para R1 e R2, porém somente um deles irá responder ao usuário final fazendo com que esse problema de queda do link ou do equipamento seja transparente a ele? Resolveria o problema, concorda?

Vamos então simplificar o que um protocolo FHRP faria no caso da queda de R1 ou sua conectividade com a rede de maneira generalizada:

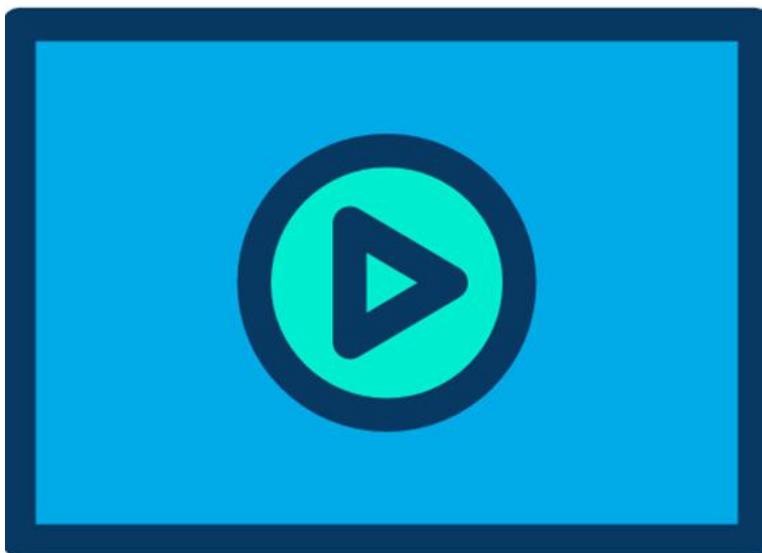
1. Os hosts não sofrem nenhuma alteração, continuam como o esperado com um gateway configurado em sua placa de rede.
2. Os roteadores padrão R1 e R2 compartilham um endereço IP virtual para a sub-rede 19.168.1.0/24, o qual é definido nas configurações do protocolo FHRP ativado em ambos os roteadores.
3. Os hosts utilizam o endereço IP virtual definido no FHRP como seu default gateway.
4. Os roteadores trocam mensagens do protocolo FHRP para definir qual dos dois atuará e como será essa atuação durante a operação normal de rede, por exemplo, R1 será o principal e R2 fica como standby até R1 falhar.
5. Quando ocorre um problema na rede os roteadores trocam mensagens através do protocolo FHRP para escolher quem assumirá as responsabilidades do roteador que falhou.

Com isso conseguiremos fazer a redundância no primeiro salto, ou seja, entre os computadores dos usuários e seu gateway de maneira transparente, pois nada precisará ser feito na configuração da placa de rede dos computadores.

Os três protocolos principais da família FHRP são:

- **HSRP (Hot Standby Router Protocol Cisco):** protocolo definido pela Cisco, trabalha com um roteador ativo e outro em standby (Active/standby). Permite balanceamento de cargas por sub-rede.
- **VRRP (Virtual Router Redundancy Protocol):** protocolo aberto definido pela IETF (RFC 5798), assim como HSRP um dos roteadores ficará ativo e os demais em standby (Active/standby). Permite balanceamento de cargas por sub-rede.
- **GLBP (Gateway Load Balancing Protocol):** protocolo definido pela Cisco, permite que ambos os roteadores trabalhem simultaneamente (ativo/ativo - Active/active). Permite balanceamento de cargas por host.

9.2 Entendendo Funcionamento do HSRP

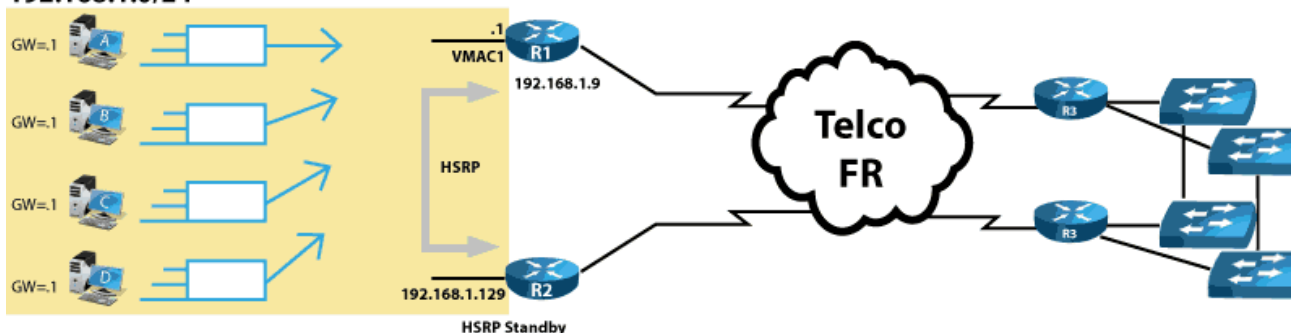


Devido aos conceitos de funcionamento do HSRP e VRRP serem muito similares vamos explicar o funcionamento de ambos e depois vamos mostrar a configuração da mesma topologia com o protocolo HSRP.

O HSRP trabalha com um conceito de **Ativo/Standby** que pode ser chamado também como **Ativo/Passivo** em algumas bibliografias. Isso quer dizer que por sub-rede apenas um roteador ficará ativo enviando o tráfego, o outro roteador ficará como passivo ou standby até que o primeiro roteador falhe.

O roteador HSRP ativo possui configurado um endereço IP virtual vinculado também a um endereço MAC virtual. Essa configuração faz parte do processo de ativação do HSRP nos roteadores, porém o roteador continua tendo o seu endereço IP configurado com o comando "ip address" em sua interface. O IP virtual é um endereço na mesma sub-rede da interface ou sub-interface, porém diferente. Já o MAC virtual é criado automaticamente pelo roteador.

Como a arquitetura do HSRP é ativo/passivo (ou standby), todos os roteadores participando do processo conhecem o endereço IP virtual, mas o único que responde as requisições enviadas é o roteador ativo (principal). Veja a figura abaixo.

192.168.1.0/24

Os computadores agora não utilizam nem o endereço 192.168.1.9 ou 192.168.1.129 como gateway, mas sim um endereço IP virtual 192.168.1.1 como gateway (GW). Além disso, as requisições ARP solicitando o MAC do gateway 192.168.1.1 não são mais respondidas utilizando o MAC físico de R1 e sim um MAC virtual (VMAC) definido automaticamente pelo roteador.

Note também que mensagens do HSRP são trocadas entre R1 (ativo ou active) e R2 (passivo ou standby). Portanto, nos passos de configuração do HSRP ambos os roteadores precisam de configurações específicas, por exemplo, definir o IP virtual, definir quem será o ativo e quem será o passivo ou standby.

O HSRP tem duas versões (1 e 2) e em ambas a configuração do **IP virtual** é tarefa do administrador de redes. Já o MAC virtual (VMAC) é definido através de uma regra básica dependendo da versão que o HSRP está utilizando e o grupo configurado pelo administrador de redes.

O **HSRP versão 1** utiliza a faixa de endereços 0000.0C07.ACxy como MAC virtual dos roteadores, onde xy é o número do grupo do HSRP em hexadecimal configurado na interface. Por exemplo, se o HSRP for configurado no grupo **1** o virtual MAC será 0000.0C07.AC**01**. Portanto, computadores naquele segmento de rede terão as suas requisições do Address Resolution Protocol (ARP) respondidas com esse endereço MAC 0000.0C07.AC**01** independente do MAC real da interface de LAN do roteador ativo.

A **versão 2 do HSRP** permite a configuração de um número de grupo estendido de 0 a 4095 e utiliza um novo range de MACs virtuais, os quais podem ir de **0000.0C9F.F000** até **0000.0C9F.FFFF**. Em hexadecimal **0** pode ser escrito como **000** e **4095** é **FFF**, por isso os valores do range de MACs virtuais no HSRP-v2 tem nos três últimos algarismos o valor do grupo HSRP configurado pelo administrador de redes convertido em hexadecimal, assim como no HSRP v1, porém com três dígitos ao invés de dois apenas.

O HSRP envia mensagens em multicast no endereço 224.0.0.2 através da porta UDP 1985. A versão 2 do HSRP utiliza o endereço 224.0.0.102 ao invés do anterior.

Além disso, o HSRP versão 2 suporta IPv6 e envio de hellos em milissegundos.

Normalmente o HSRP envia mensagens de hello para verificar se o roteador ativo está “no ar” de 3 em 3 segundos, caso o roteador ativo não envie hello em 10 segundos (mais ou menos 3 vezes do timer de hello) o standby vai assumir a rede como ativo.

Podemos alterar esse valor para diminuir o tempo do roteador standby assumir como principal em caso de falha do ativo. No HSRP versão 2 esse valor pode ser diminuído para menos de 1 segundo.

Também existe uma diferença na quantidade de grupos HSRP que podem ser criados entre as versões 1 e 2, sendo que a 1 suporta de 0 a 255 e a versão 2 de 0 a 4095.

9.2.1 Entendendo o Failover com HSRP

Quando os roteadores têm o HSRP ou VRRP configurado há uma troca inicial de pacotes entre eles e é decidido quem será ativo e passivo. Após essa troca inicial o roteador ativo responde às solicitações ARP dos clientes utilizando o IP virtual (igual para todos os roteadores HSRP/VRRP) e seu MAC virtual (também o mesmo).

Caso haja um problema em R1, através de mensagens do HSRP ou de temporizadores de timeout (não recebimento de mensagens) **R2 será colocado como ativo e R1 passará a ser o standby**, porém **nada mudará para os clientes**, ou seja, o endereço IP e MAC virtuais continuarão os mesmos. Esse processo é chamado de **Failover**.

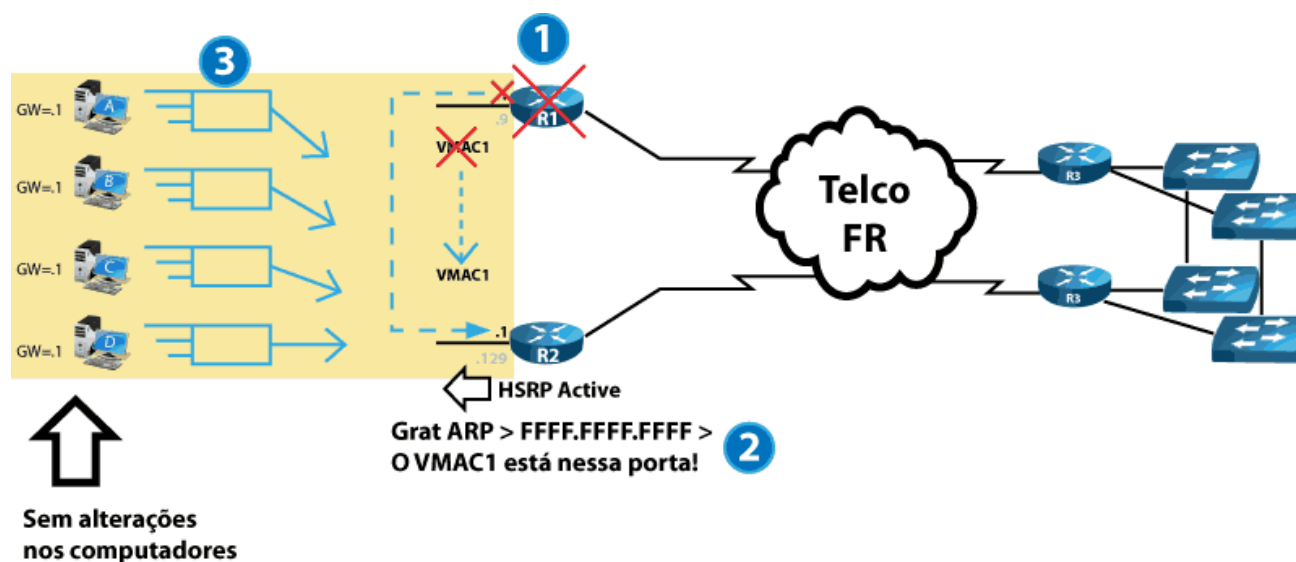
Mas espera um pouco, as entradas das tabelas MAC dos switches SW-1 até SW-4 vinculam o MAC virtual à porta que conecta ao roteador R1, como esse problema é resolvido pelo HSRP?

De uma maneira bem simples, quando R2 assume como ativo ele envia mensagens em broadcast avisando que o IP virtual e o MAC virtual agora pertencem a ele.

Essas mensagens são chamadas de **Gratuitous ARP**, nada mais é que um ARP Reply para que os switches de SW-1 a SW-4 apaguem o vínculo do MAC virtual com a porta que conecta R1 e estabeleçam um novo vínculo com a porta que conecta o roteador R2.

Lembrem-se que essa é uma das regras que estudamos nos switches, quando ele recebe uma informação nova sobre o mesmo MAC a antiga é apagada e o endereço é vinculado à nova porta.

Portanto, todas as ações para R2 assumir como ativo **estão restritas a ele mesmo e aos switches de acesso**, não envolvendo em nenhum momento os computadores dos usuários finais, ou seja, o processo é transparente aos computadores. Veja figura abaixo com um resumo do processo de Failover do HSRP.



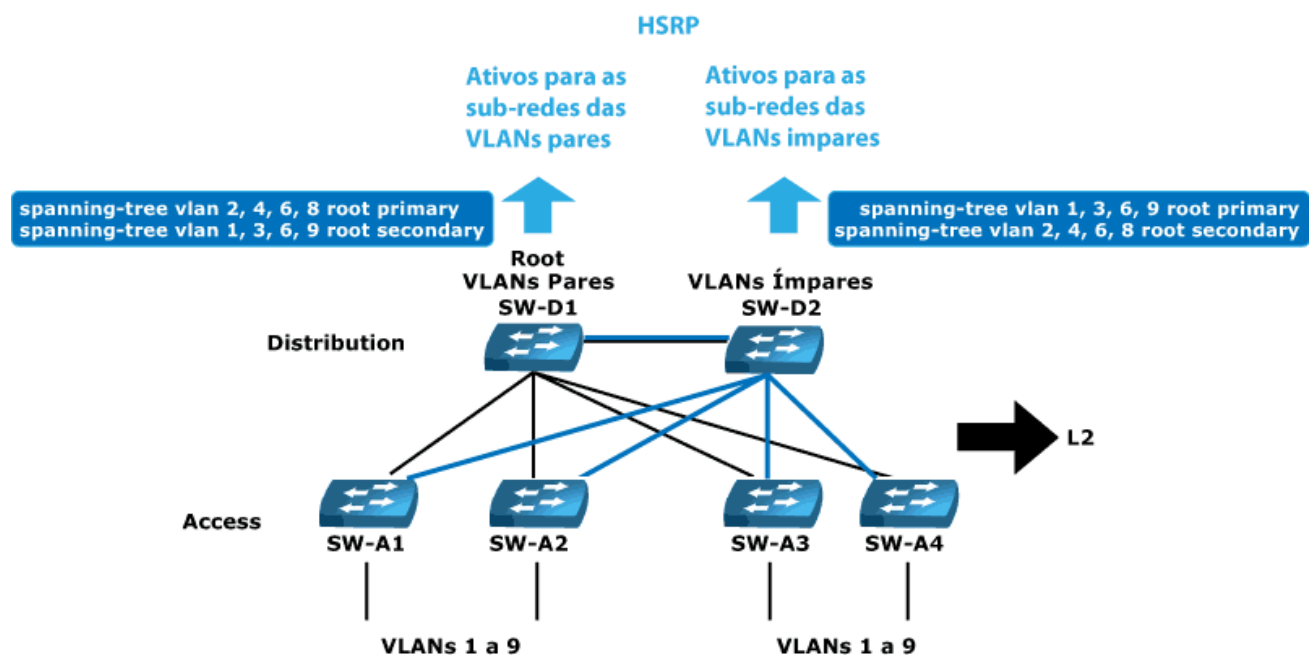
1. Via mensagens e/ou temporizadores do HSRP, R2 descobre que houve falha em R1 e é passado para o estado de ativo.
2. Gratuitous ARP são enviados por R2 para ensinar aos switches que o MAC virtual VMAC1 está agora com o roteador R2.
3. Os hosts da sub-rede 192.168.1.0/24 não são alterados, porém os switches passam a encaminhar quadros com destino o VMAC1 para a porta onde R2 está conectado.

9.2.2 Balanceando Cargas com HSRP

O HSRP é tratado por sub-rede, por isso para fazer balanceamento de cargas através dele precisamos fazer uma configuração com a mesma filosofia que estudamos para compartilhar cargas entre VLANs em switches de distribuição, ou seja, um roteador assume algumas sub-redes como ativo e o outro roteador assume as demais.

Assim é possível o balanceamento de cargas, porém dependendo do tráfego gerado em cada uma das VLANs pode haver sobrecarga em um dos roteadores, isso deve ser analisado com ferramentas de monitoração externas para definir como será realizada essa divisão das sub-redes entre os roteadores HSRP.

Vamos a um exemplo prático utilizando switches camada-3 ao invés de roteadores como gateway para os computadores dos usuários finais. Veja topologia a seguir.



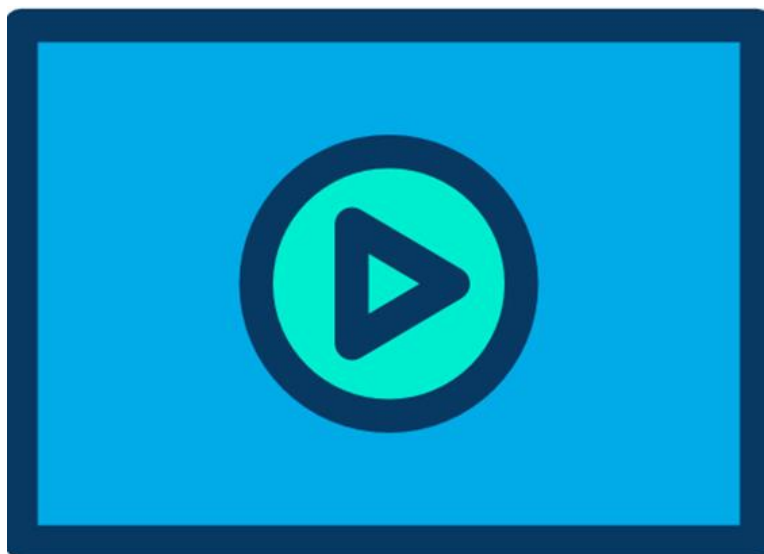
Nesse exemplo, SW-D1 está encaminhando pacotes das sub-redes das VLANs pares, assim como está ativo no HSRP para essas sub-redes. Caso SW-D1 tenha problemas o switch SW-D2 assume as sub-redes das VLANs pares.

O mesmo conceito pode ser utilizado quando temos roteadores como dispositivos de camada-3 em uma topologia Router-on-a-Stick (ROAS).

Um dos roteadores pode ser definido como ativo para parte das sub-redes e o segundo roteador ficaria ativo para o restante das sub-redes, sendo que um ficaria como passivo do outro assumindo todas as sub-redes caso haja problemas com um deles.

O mesmo princípio pode ser utilizado para o VRRP.

9.3 Entendendo Funcionamento do VRRP



O **VRRP** ou **Virtual Router Redundancy Protocol** é um protocolo aberto que serve como alternativa ao HSRP definido pela IETF na RFC 2338.

Ele pode ser utilizado em roteadores e switches L3 Cisco que precisam fazer FHRP com equipamentos de outros fabricantes.

O VRRP e o HSRP são tão parecidos que você precisa aprender apenas as diferenças de nomenclatura entre os dois, por isso vamos estudar essas diferenças rapidamente nesse tópico.

O VRRP fornece redundância do gateway para um grupo de roteadores.

O roteador ativo ou active do HSRP é chamado de "**virtual master router**" ou roteador mestre no VRRP, já os roteadores standby do HSRP são chamados de "**backups**" no VRRP, portanto eles ficam em estado de backup (backup state) ao invés de ficar no estado de standby como estudamos para o HSRP.

O "master router" é aquele com maior prioridade no grupo VRRP, a qual varia de 0 a 255, porém os roteadores VRRP podem utilizar a faixa de 1 a 254. O valor padrão também é 100 no VRRP.

O VRRP utiliza o endereço de multicast 224.0.0.18, porém não utiliza nem o UDP nem o TCP para transmissão de mensagens, pois elas são montadas diretamente no pacote IP e identificadas com o número de protocolo 112 no cabeçalho do pacote IP.

O virtual MAC utilizado pelo VRRP está no range de 00-00-5e-00-01-00 até 00-00-5e-00-01-FF, sendo que seu formato é **00-00-5e-00-01**-<num-VRRP-group> em hexadecimal.

Por exemplo, se o VRRP foi configurado no grupo **1** seu MAC virtual será 00-00-5e-00-01-**01**.

O suporte ao VRRP deve ser verificado antes do planejamento da sua configuração em switches, pois nem todas as versões de Cisco IOS ou modelos de switches L3 suportam esse recurso.

9.4 Entendendo Funcionamento do GLBP

Os protocolos HSRP e VRRP tiveram seu desenvolvimento e lançamento anteriores ao **GLBP (Gateway Load Balancing Protocol)**. Isso se deve ao fato de que ele é um protocolo definido pela Cisco para suprir a necessidade de um melhor balanceamento de cargas do que o realizado pelos anteriores, pois o fluxo de uma sub-rede é quase que imprevisível e torna o HSRP e o VRRP mais difíceis para o administrador de redes prever qual a melhor distribuição dessas sub-redes por roteador ou switch camada-3.

O GLBP faz o balanceamento de cargas por destino utilizando uma arquitetura ativo/ativo para encaminhamento dos pacotes, ou seja, você utiliza os dois roteadores para envio de informações por isso o nome ativo/ativo sem a necessidade de fazer o esquema mostrado de balanceamento por sub-redes do HSRP e VRRP.

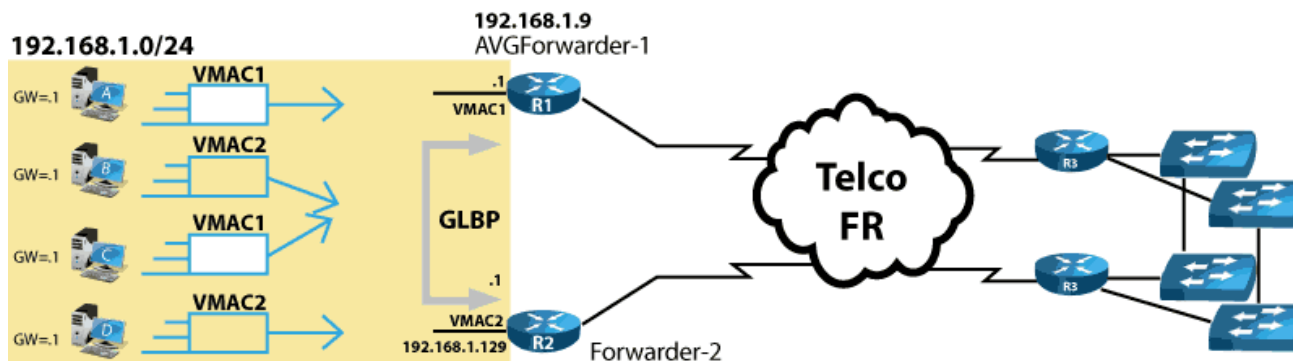
A grande diferença do GLBP é que um roteador atua em um papel especial chamado **Active Virtual Gateway (AVG - Gateway Virtual Ativo)**. Os demais roteadores utilizam o mesmo endereço IP virtual, porém cada um possui um MAC virtual próprio, sendo que o AVG pode responder aos ARP Requests com um MAC virtual diferente para cada host solicitante. Qual o resultado desse tipo de operação? Alguns computadores enviarão informações para o MAC virtual de um roteador e outros para o MAC virtual do segundo roteador, permitindo o balanceamento de cargas por destino, conforme mencionado no início das explicações.

Os roteadores que fazem parte do GLBP e farão o encaminhamento dos pacotes são chamados de **forwarders** ou **encaminhadores**, inclusive o próprio roteador escolhido como AVG pode ser um dos encaminhadores.

Os roteadores forwarders podem ser chamados de **AVF** ou **Active Virtual Forwarder**.

Portanto, diferente dos protocolos da família FHRP anteriores, os computadores que estão utilizando roteadores configurados via GLBP enviarão seus pacotes para um único endereço IP virtual, porém cada host de rede receberá o MAC de destino de um dos dois roteadores forwarders, conforme distribuição feita pelo AVG.

Por exemplo, temos os roteadores R1 e R2 configurados com o protocolo GLBP, onde R1 é o AVG e forwarder e R2 é apenas forwarder. Quando o computador-1 enviar um pacote para o IP virtual do GLBP ele receberá o VMAC-1 configurado em R1, porém quando o computador-2 enviar uma requisição ARP na sequência ele receberá o VMAC-2 configurado em R2. Veja a figura a seguir com a ilustração sobre a operação do GLBP.



No exemplo da figura anterior os computadores A, B, C e D enviam quadros um após do outro, portanto o AVG (R1) envia seu próprio VMAC-1 na resposta à requisição ARP do computador A. Depois ele envia o VMAC-2 de R2 como resposta ao ARP Request do computador-B, na sequência de novo seu VMAC-1 como resposta ao ARP Req do computador C e por último envia o VMAC-2 como resposta à solicitação do roteador D. No final A e C estão enviando pacotes por R1 (utilizando o VMAC-1) e B e D através de R2 (utilizando o VMAC-2).

Esse processo mostrado acima ilustra como o GLBP faz o balanceamento de cargas, porém existe ainda o processo de assumir o tráfego do outro roteador caso ele caia. O GLBP troca mensagens entre os roteadores para verificar se eles estão ativos, caso um forwarder falhe o que estiver funcionando deve assumir o virtual MAC daquele que caiu para que o tráfego continue normalmente e os usuários finais não percebem que ocorreu um problema na rede, pois o GLBP também deve ser transparente para os usuários finais.

Por padrão o GLBP utiliza o endereço de multicast 224.0.0.102 para enviar suas mensagens de hello a cada 3 segundos através da porta UDP 3222.

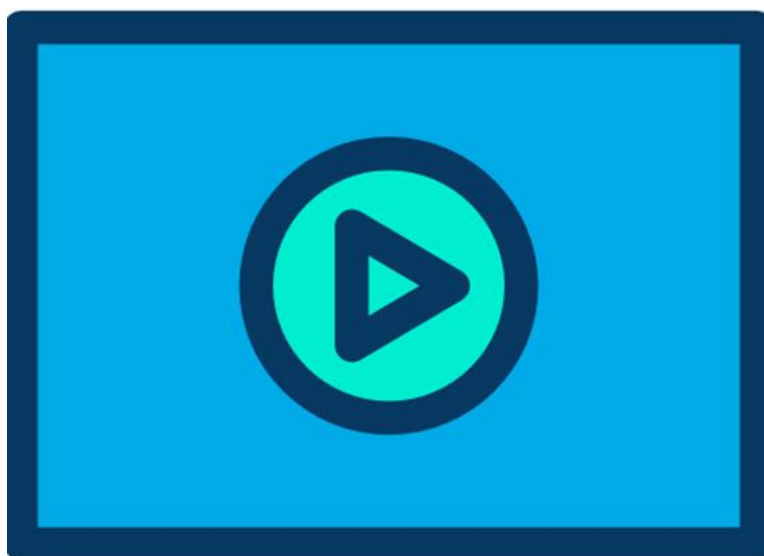
O roteador definido como Active Virtual Gateway (AVG) em um determinado grupo é quem define o endereço MAC virtual que cada roteador do grupo irá utilizar. O formato segue o padrão 0007.B400.**xyyy**, onde xx é o número do grupo que o GLBP foi configurado e yy é um sequencial diferente para cada AVF, por exemplo 01, 02, 03, etc.

Se tomarmos como exemplo a topologia da figura anterior, o roteador R1 será escolhido como AVG e será o primeiro forwarder do GLBP, já o roteador R2 será o segundo forwarder. Se o grupo configurado for o número 1 teremos os seguintes MACs virtuais:

- Forwarder 1 e AVG será R1 com o MAC virtual 0007.B400.0101.
- Forwarder 2 será R2 com o MAC virtual 0007.B400.0102.

Você pode visualizar na tabela ARP dos hosts quem eles estão utilizando como gateway (forwarder) e identificar o roteador que está sendo utilizado como forwarder se entender bem a regrinha acima.

9.5 Ativando e Verificando o HSRP Básico



A ativação básica do HSRP é bastante simples e envolve apenas três comandos em modo de configuração de interface:

1. **standby group num-do-grupo:** define o grupo que os roteadores participando do HSRP estarão configurados e compartilharão o mesmo IP e MAC virtuais, deve ser o mesmo em todos os roteadores. Opcionalmente você pode definir um nome para o grupo com a opção "name" na sequência.
2. **Standby num-do-grupo ip endereço-ip-virtual:** define o endereço IP virtual do grupo que deve ser o mesmo em todos os roteadores.
3. **standby num-do-grupo priority valor-prioridade:** define a prioridade dos roteadores, o roteador com o maior valor será o ativo e os demais serão os passivos. O valor padrão é 100.

Abaixo segue a configuração de R1 e R2, sendo que R1 será o ativo e R2 passivo. Vamos utilizar o número 1 para definir o grupo HSRP.

R1# show running-config

! Linhas omitidas propositalmente

!

```
interface GigabitEthernet0/0
ip address 192.168.1.9 255.255.255.0
standby 1 name grupo-HSRP-teste
standby version 2
standby 1 ip 192.168.1.1
standby 1 priority 110
```

R2# show running-config

! Linhas omitidas propositalmente

!

```
interface GigabitEthernet0/0
ip address 192.168.1.129 255.255.255.0
standby 1 name grupo-HSRP-teste
standby version 2
standby 1 ip 192.168.1.1
```

Note que a configuração é a mesma em ambos os roteadores, porém a prioridade mais alta foi definida em R1 porque ele precisa ser o ativo, conforme planejamento inicial.

Para verificar as configurações do HSRP podemos utilizar os comandos:

- **show running-config**
- **show standby brief:** traz em uma linha informações sobre o grupo HSRP, se o roteador é standby ou ativo e seu endereço IP virtual.
- **show standby:** detalha as informações sobre o HSRP, incluindo as informações acima, o MAC virtual e muitos outros detalhes.

Veja a saída dos comandos abaixo.

```
R1#show standby brief
                P indicates configured to preempt.
                |
InterfaceGrp  Pri P State      Active      StandbyVirtual IP
Gig0/01      110  Active    local      192.168.1.129192.168.1.1
Router#
```

Portanto em R1 temos o HSRP configurado na interface Giga0/0 (campo Interface), ele está no grupo HSRP 1 (campo Grp), seu estado está como ativo (Campo State - Active), o endereço IP do roteador passivo está no campo Stanby como 192.168.1.129, ou seja, o IP do R2.

O endereço virtual está mostrado no campo "Virtual IP" e configurado como 192.168.1.1. Agora veja a saída para R2 abaixo e compare os comandos.

Note que no campo "Active" ele mostra a informação "local", ou seja, o próprio R1 é o roteador ativo. Também no campo "Pri" temos a prioridade de R1 que foi configurada como 110 para que ele pudesse ser escolhido como ativo, pois o padrão é 100.

```
R2#show standby brief
                P indicates configured to preempt.
                |
Interface  Grp  Pri P State      Active      Standby      Virtual IP
Gig0/0    1    100  Standby  192.168.1.9    local      192.168.1.1
Router#
```

Note que para R2 a interface é a Giga0/0 (campo Interface), ele também está no grupo HSRP 1 (campo Grp), sua prioridade é 100 (campo Pri) e seu estado é standby ou passivo (campo State), pois a prioridade de R1 é maior.

Depois podemos ver o IP de R1 (192.168.1.9) mostrado como ativo (campo Active), no campo Standby mostra que o próprio R2 está como passivo (local) e o endereço virtual é 192.168.1.1 (campo Virtual IP), o mesmo de R1.

Agora vamos verificar as informações completas com o comando "**show standby**" e descobrir o MAC virtual configurado pelo HSRP.

```
Router#show standby
GigabitEthernet0/0 - Group 1 (version 2)
  State is Active
    5 state changes, last state change 00:01:33
  Virtual IP address is 192.168.1.1
  Active virtual MAC address is 0000.0C9F.F001
    Local virtual MAC address is 0000.0C9F.F001 (v2 default)
    Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.622 secs
    Preemption disabled
    Active router is local
  Standby router is 192.168.1.129
  Priority 110 (configured 110)
    Group name is hsrp-Gig0/0-1 (default)
Router#
```


Como configuramos o HSRP versão 2 seu MAC virtual inicia com **0000.0C9F.F** e tem o final **001**, o qual é o número do grupo que configuramos no comando "**standby 1 ip 192.168.1.1**" em hexadecimal.

9.5.1 Preemption

Pense um pouco nessa pergunta:

"Um roteador chamado R1 estava configurado com prioridade mais alta para ser o ativo. O R1 cai e o roteador R2 com prioridade menor detecta (10 segundos sem receber hello) passa de standby para ativo, assumindo a rede como gateway. Após alguns minutos R1 volta a funcionar normalmente. O que vai acontecer com essa rede após o retorno em operação de R1? Quem será o roteador ativo quando o roteador R1 voltar?"

Pense um pouco, não leia os parágrafos abaixo!

O comportamento padrão do HSRP é que o roteador que assumiu a rede fique como ativo, ou seja, mesmo que R1 retorne ao estado operacional R2 será o ativo até cair.

Para alterar esse comportamento podemos configurar o recurso chamado "preemption", que é o direito de assumir a rede sempre que ele esteja operacional.

Para que o roteador principal seja sempre o ativo quando operacional acrescente o sub-comando "standby 1 preempt" na configuração do HSRP do roteador ativo apenas.

Você pode verificar se o recurso está ativo no comando "**show standby**" na linha relativa ao Preemption. Se estiver escrito "Preemption disabled" é porque o recurso está inativo, se aparecer como enabled é porque foi configurado.

9.5.2 Problemas mais comuns ao Configurar o HSRP

Abaixo segue uma lista do que precisamos garantir para que o HSRP funcione corretamente:

- Os roteadores devem ser configurados como a mesma versão de HSRP version (standby version {1 | 2})
- Também devem ser configurados no mesmo grupo HSRP (standby num-grupo ...).
- Ter o mesmo IP virtual] (standby grupo end-IP).
- O endereço IP virtual deve estar na mesma sub-rede da LAN ou VLAN local.
- As interfaces físicas ou virtuais devem estar na mesma LAN ou VLAN.
- Não devem existir ACLs filtrando mensagens do HSRP (UDP porta 1985 e version 1 usa o IP de multicast 224.0.0.2, para version 2 o IP é 224.0.0.102).

Normalmente quando o administrador de redes configura duas interfaces HSRP que deveriam estar no mesmo grupo com versões de HSRP diferentes vai aparecer uma mensagem de IP duplicado, por exemplo:

```
*Mar  9 17:54:01.724: %IP-4-DUPADDR: Duplicate address 192.168.0.1 on
GigabitEthernet0, sourced by 0000.0c07.ac01
```

Note que o VMAC acima é da versão 1 do HSRP, se você planejou utilizar a versão 2 já sabe onde está o problema.

Você vai notar nessa situação que ambos os roteadores acabam ficando como ativo, pois cada um está em uma versão diferente do HSRP.

Um problema semelhante pode ocorrer se você configurar dois roteadores com o mesmo IP Virtual, mas grupos HSRP diferentes. Por exemplo, era para configurar as interfaces no grupo 1 e em uma delas você configura por engano no grupo 2.

Assim sobrem dois processos em grupos diferentes com o mesmo endereço IP virtual, ocorrendo novamente um conflito de IPs.

9.5.3 Resumo dos Comandos Utilizados no Capítulo

Segue abaixo resumo dos comandos de configuração do capítulo importantes para o exame de certificação. Lembre-se que todos os comandos do HSRP estudados nesse capítulo foram inseridos em modo de configuração de interface.

- **Comandos do HSRP:**

- **standby num-grupo ip end-ip-virtual:** comando para ativar o HSRP e definir o IP virtual associado a um grupo específico.
- **standby num-grupo priority 0-a-255:** comando para definir a prioridade a do roteador HSRP e configurar qual será o ativo em um grupo específico. O maior valor ganha, sendo que o padrão é 100.
- **standby num-grupo name nome-descritivo:** define um nome descritivo para um determinado grupo HSRP.
- **standby version 1-ou-2:** define a versão do HSRP para todos os grupos configurados em uma interface. Lembre-se que a versão 1 do HSRP permite dos grupos 0 a 255 e a versão 2 de 0 a 4095.
- **standby num-grupo preempt:** faz com que o roteador ativo seja sempre ativo quando operacional.

10 Conclusão do Curso

10.1 Conclusão

Bem pessoal, chegamos ao final de mais um curso!

É muito importante que nesse ponto do curso você tenha domínio dos seguintes itens:

- A tabela de roteamento IP em roteadores e switches L3 Cisco
- Significado dos seus campos e como interpretar as informações da tabela de roteamento
- Saber como os roteadores tomam suas decisões de roteamento
- Conceito de longest match, distância administrativa e métrica de protocolos de roteamento dinâmico
- Rotas estáticas IPv4 e IPv6
- Rotas default, network, host e flutuantes
- Configurações e verificações do funcionamento do protocolo OSPFv2 (IPv4)
- Conceitos como adjacências, redes ponto a ponto, broadcast, eleição de DR e BDR, assim como router-id do OSPF
- Descrever o funcionamento e o propósito dos protocolos de redundância de primeiro salto, tais como HSRP, VRRP e GLBP

Lembre-se que esse curso conta também com vídeo aulas, questionários e laboratórios extras que estão dentro da trilha do CCNA para quem está se preparando para a prova de certificação ou então quer ter os conhecimentos de um profissional nível associado exigido pela Cisco.