UNIDADE 3 – SWITCHES, VLANS E ROTEAMENTO IP
MÓDULO 1 – SWITCHING E VLANS
01

1 - APRENDIZAGEM DO SWITCH

Conforme (Filippetti, 2008) e Sybex - CCNP Switching Study Guide, a comutação (switching) na camada de enlace é baseada no endereço MAC da placa de rede do dispositivo para fazer a filtragem da rede.

Os switches utilizam chips especiais ASICs (***A**pplication **S**pecific **I**ntegrated **C**ircuit*) para formar e manter as tabelas de filtragem. São rápidos, pois não analisam a Camada de Rede, somente os endereços de *hardware* dos frames antes de decidir pelo encaminhamento ou abando no dos quadros.

O que torna a comutação na camada de enlace tão eficiente é a não modificação no pacote de dados, somente no quadro que a encapsula. Também é menos susceptível a erros.

Pode ser utilizada para testar conectividade entre grupos de trabalho e para a segmentação da rede (quebra do domínio de colisão). Ela aumenta a largura da banda disponível para cada usuário.

A camada de enlace acomoda switches e bridges, porém existem diferenças importantes:

Bridges	Switches
• bridges rodam *softwares*, portanto são lentos; • bridges podem ter apenas uma ocorrência de Spanning Tree; • bridges podem ter até 16 portas;	• switches processam ASICs (*hardware*), portanto são rápidos; • switches podem ter várias ocorrências de Spanning Tree; • switches podem ter centenas de portas; • switches têm baixo custo, alta eficiência, baixa latência/espera (low latency), velocidade transmissão depende do meio (wire speed transmission) e processo de comutação baseado em *hardware*.

02

Todo switch monta na memória RAM dele uma **tabela MAC** que mapeia os endereços físicos dos dispositivos às portas (interfaces) às quais eles se encontram conectados. Assim que um switch é ligado, essa tabela encontra-se vazia. Quando um dispositivo inicia a transmissão e uma porta do switch recebe um quadro, o switch armazena o endereço MAC dos dispositivos transmissores em sua tabela MAC e registra as respectivas interfaces à porta que cada dispositivo está conectado.

No primeiro momento, o switch inunda a rede (broadcast), com esse frame, uma vez que ele ainda não possui, na tabela MAC, o registro da localização do dispositivo destinatário. Quando um dispositivo responde a esse quadro enviando outro de volta, o switch capturará o endereço MAC desse dispositivo e o armazenará na tabela MAC dele associando o endereço MAC desse dispositivo à interface (porta) que recebeu o quadro.

O switch tem agora dois endereços em sua tabela MAC, podendo estabelecer uma conexão ponto a ponto entre os dois dispositivos. Os quadros pertencentes a essa transmissão serão encaminhados apenas aos dois dispositivos participantes. Nenhuma porta do switch irá receber os quadros a não ser às duas portas mapeadas.

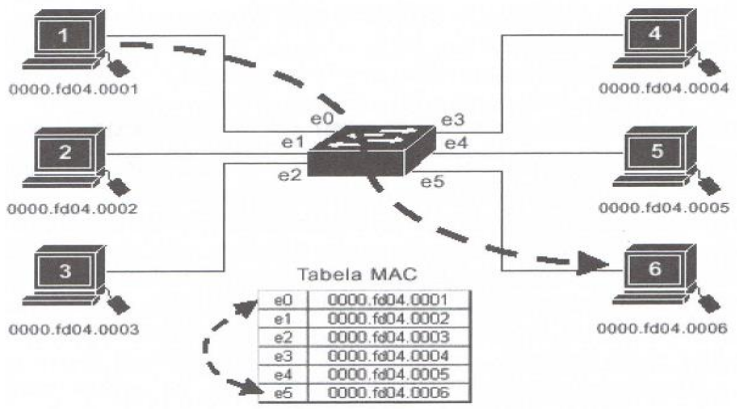
Veja a figura a seguir, que ilustra o **processo de aprendizagem do switch**.

1 – a estação 1 quer se comunicar com a 6;

2 – a tabela MAC já se encontra formada;

3 – cada porta de conexão do switch tem o MAC de cada estação associada à mesma;

4 – a comunicação ocorre somente entre as estações interessadas.



Comunicação ente rede comutada

Fonte: CCNA 4.1-Felippetti, 2008

03

1.2 - Filtragem do Switch

Assim que o quadro chega à interface de um switch, o endereço do *hardware* de destino é comparado com a tabela MAC.

Se o endereço de destino for conhecido e estiver presente na tabela, então o frame é encaminhado apenas para a porta de saída associada àquele endereço (frame filtering).

Se o endereço MAC não estiver listado na tabela do switch então é propagado para todas as interfaces ativas (*broadcasting*), com exceção da interface na qual ele foi recebido. Se um dispositivo responder a essa transmissão então a tabela MAC é atualizada com a localização desse dispositivo (interface).

04

2 - STP – Spanning Tree Protocol

Ainda conforme (Filippetti, 2008), o **Spanning Tree Protocol** (STP) é um protocolo que permite resolver problemas de loop em redes comutadas cuja topologia introduza ciclos nas ligações. O algoritmo Spanning Tree determina qual é o caminho mais eficiente entre cada segmento separado por bridges ou switches.

Caso ocorra um problema nesse caminho, o algoritmo recalculará entre os existentes, o novo caminho mais eficiente, habilitando-o automaticamente. O nome deriva do algoritmo spanning tree da teoria dos grafos.

O switch pode ter o estado das portas usando STP nos seguintes casos:

- **Bloqueio**
- **Escuta**
- **Aprendizado**
- **Encaminhamento**
- **Desativado**

Spanning tree
Spanning tree significa 'árvore de espalhamento', e é um conceito (estrutura) da Teoria dos Grafos em que cada nó consegue alcançar todos os outros. O STP faz uso desta árvore para que caminhos eficientes sejam criados.

Bloqueio
Apenas recebendo BPDUs.

Escuta

O switch processa BPDUs e espera por possíveis novas informações que podem fazê-lo voltar ao estado de Bloqueio.

Aprendizado
Quando a porta ainda está "aprendendo" e montando sua tabela de endereços de origem dos frames recebidos.

Encaminhamento
A porta envia e recebe dado. Operação normal. O STP continua monitorando por BPDUs que podem indicar que a porta deve retornar ao estado de bloqueio prevenindo um loop.

Desativado
Não está utilizando STP. O administrador de redes pode desabilitar a porta manualmente.

05

2.1 - O que o Spanning tree IEEE 802.1d faz?

Conforme o IEEE (www.ieee.org.br, acessado em 19 Out. 2011), o Protocolo Spanning Tree (STP) foi criado pela extinta DEC (Digital Equipment Corporation). O IEEE homologou posteriormente sua própria versão do protocolo, denominada IEEE 802.1d. A empresa CISCO utiliza o protocolo do IEEE.

O Spanning Tree Protocol (STP) é um protocolo de Camada 2 executado em pontes e switches. O principal objetivo do STP é garantir que você não crie loops quando tiver caminhos redundantes na rede.

O algoritmo spanning tree coloca cada porta de bridge/switch no estado **forwarding** (encaminhamento), ou no estado **blocking** (bloqueado).

Considera-se que todas as portas no estado forwarding estão na spanning tree atual. O conjunto de portas no estado forwarding cria um único caminho pelo qual os quadros são enviados entre os segmentos ethernet.

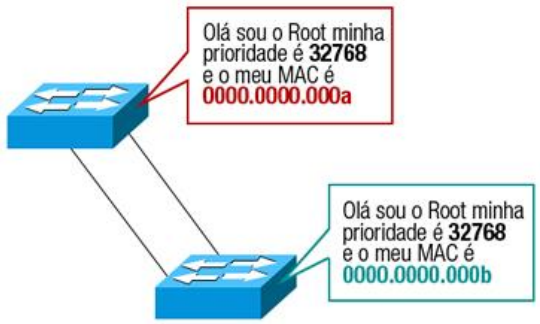
Segundo Filippetti (2008) o STP **desativa links redundantes** fazendo:

1. a eleição de um switch raiz (root bridge);
2. a nomeação das portas do switch raiz como portas designadas (designated ports);
3. a nomeação dos demais switches existentes chamados de não-raiz (non-root bridges);
4. no caso dos switches não-raiz, a porta com “menor custo” (determinada pela largura de banda do link em questão) é chamada de “porta-raíz”;
5. as demais portas dos switches não-raiz são chamadas de portas designadas.

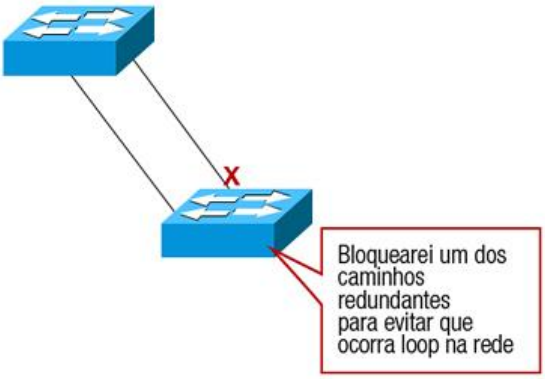
06

2.2 - Seleção de uma Root Bridge

Ainda conforme Filippetti (2008), um ID de um switch é usado para a escolha de ponte raiz da rede, além de determinar a porta raiz. Para determinar o switch raiz, as prioridades do mesmo e o endereço MAC são combinados. Se os dois switches tiverem o mesmo valor de prioridade, então o endereço MAC torna-se um critério de desempate para descobrir qual possui o menor ID. Geralmente a prioridade dos equipamentos vem configurada por default de **32.768**, desta forma, os endereços MAC dos equipamentos já entram em disputa para saber quem é o menor endereço MAC, para tornar-se o Root, isto é, a raiz da rede.



Após a eleição, se houver algum caminho redundante, o mesmo será bloqueado.



07

Switches e bridges rodando STP trocam informações por meio do **B**ridge **P**rotocol **D**ata **U**nits (BPDUs):

- A BPDU envia mensagem de configuração via “frame broadcast” com o ID de cada switch;
- O ID é utilizado na determinação do switch-raiz e da porta-raiz;
- O ID tem 8 bytes (valor de prioridade + MAC address do dispositivo);

- O valor default da prioridade de todos os dispositivos rodando STPvIEEE é “32.768”.

Se dois switches têm o mesmo valor de prioridade então o endereço MAC mais baixo é utilizado para a definição do switch-raiz.

As portas do switch ou bridge rodando STP podem estar em um dos quatro estados:

- **Blocking**
- **Listening**
- **Learning**
- **Forwarding**

Blocking
Porta não encaminha quadros.

Listening
Porta recebe e analisa os BPDUs para certificar-se que não ocorrerão loops na rede antes de começar o encaminhamento.

Learning
Registra os endereços dos *hardware*s conectados às interfaces e monta a tabela MAC.

Forwarding
Envia e recebe quadros.

08

Existe uma forma de selecionar a raiz, que é **redefinir a prioridade do switch**, pois quando você adquire um novo switch, você tem que ter alguma forma de torná-lo o switch raiz da rede.

Root Bridge é uma ponte que transmite continuamente a informação da topologia da rede a outras pontes, usando o protocolo spanning tree, a fim notificar a todas as pontes restantes da rede, quando as mudanças na topologia forem requeridas.

Isto significa que uma rede pode se reconfigurar sempre que uma ligação da rede (por exemplo, outra ponte) falha, assim um trajeto alternativo pode ser encontrado. A presença de uma ponte da raiz previne loops formados na rede. Deve ser situada centralmente na rede para fornecer o trajeto mais curto a outras ligações na rede. Ao contrário de outras pontes, a ponte da raiz envia sempre o excesso de frames para fora de suas portas.

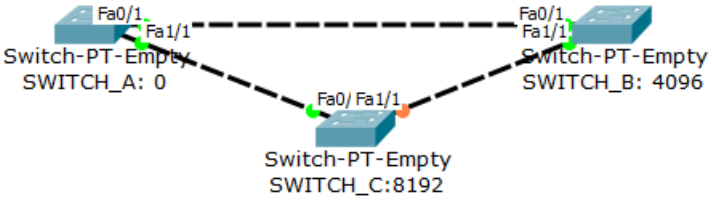
Cada rede deve ter somente uma ponte da raiz, e provavelmente, deverá ter o número mais baixo do ID da ponte.

Se desejar ajustar a probabilidade de seu switch para transformá-lo no switch raiz em sua rede Spanning-Tree você pode usar o seguinte comando:

```
SwitchB(config)# spanning-tree vlan 1 priority 4096
```

09

Observe a figura a seguir.



Spanning-Tree

Fonte: O Autor, 2015

Os números 0, 4096 e 8192 são as prioridades que estão definidas nos equipamentos. Desta forma o Switch A torna-se o switch raiz da rede (root bridge), mesmo que este possua um endereço MAC maior que o Switch B e Switch C.

Observe as configurações dos switches:

Configuração do Switch A

```
…. (relatório omitido)…..
spanning-tree extend system-id
spanning-tree vlan 1 priority 0
interface FastEthernet0/1
no ip address
interface FastEthernet1/1
no ip address
interface Vlan1
……
end
```

Configuração do Switch B

```
spanning-tree extend system-id
spanning-tree vlan 1 priority 4096
……
interface FastEthernet0/1
no ip address
interface FastEthernet1/1
no ip address
```

```
interface Vlan1
```

Configuração do Switch C

```
spanning-tree extend system-id
spanning-tree vlan 1 priority 8192
interface FastEthernet1/1
switchport mode access
no ip address
interface FastEthernet0/1
switchport mode access
no ip address
```

10

No momento em que se realiza cada um destes comandos, define-se a prioridade nos switches:

Switch_A(config)# spanning-tree vlan 1 priority 0

Switch_B(config)# spanning-tree vlan 1 priority 4096

Switch_C(config)# spanning-tree vlan 1 priority 8192

Observe os relatórios a seguir:

```
SWITCH A#SHOW SPANNING-TREE
VLAN0001
Spanning tree enabled protocol ieee
Root ID Priority 1
Address 0003.E4C3.6DB3
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Bridge ID Priority 1 (priority 0 sys-id-ext 1)
Address 0003.E4C3.6DB3
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 20
Interface Role Sts Cost Prio.Nbr Type
----------------------------------------------------------------------
Fa1/1 Desg FWD 19 128.2 P2p
Fa0/1 Desg FWD 19 128.1 P2p
SWITCH_A#
```

O SwitchA acabou tornando-se o switch raiz desta rede.

11

Devemos ter atenção aos valores permitidos para a definição do switch raiz, pois as prioridades são padronizadas no Cisco IOS do switch, não podendo assim, serem escolhidos valores diferentes destes:

```
SWITCH_B(config)#SPANNING-TREE VLAN 1 PRIORITY 2
% Bridge Priority must be in increments of 4096.
% Allowed values are:
0         4096   8192   12288 16384 20480 24576 28672
32768 36864 40960 45056 49152 53248 57344 61440
SWITCH_B(config)#
```

Usando o comando **show spanning-tree**, você pode analisar as prioridades definidas.

```
SWITCH_B#show spanning-tree
VLAN0001
Spanning tree enabled protocol ieee
Root ID Priority 1
Address 0003.E4C3.6DB3
Cost 19
Port 1(FastEthernet0/1)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Bridge ID Priority 4097 (priority 4096 sys-id-ext 1)
Address 000A.F326.C98C
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 20
Interface Role Sts Cost Prio.Nbr Type
---------------------------------------------------------------------
-
Fa0/1 Root FWD 19 128.1 P2p
Fa1/1 Desg FWD 19 128.2 P2p
SWITCH_B#
```

Use o comando **debug spanning-tree events** para fazer testes com as prioridades e verificar a escolha do melhor caminho.

Terminamos o processo do algoritmo Spanning-Tree. Veremos no próximo item como ocorre o processo das VLANs, como criar e como funciona uma VLAN.

12

3 - VLANs (Virtual Local Area Network) e VTP (Virtual Trunk Protocol)

3.1 - VLANs

Conforme Nascimento e Tavares (2012), nesta seção serão vistos os conceitos necessários e suficientes para a configuração de uma VLAN em uma rede de computadores.

Inicialmente, precisamos saber o que é uma VLAN.

Pode-se dizer que uma **VLAN** – Virtual LAN é um recurso disponível em switches cuja característica principal é a segmentação da rede. Uma VLAN é uma rede lógica que permite separar grupos de usuários e assim proporcionar uma melhoria no funcionamento da rede (desempenho, segurança, precisão).

Uma das aplicações da VLAN é no agrupamento de portas dos switches de acordo com os departamentos da empresa (Administrativo, Financeiro, Recursos Humanos, …). O agrupamento pode ser feito da forma mais adequada para cada caso. Regra geral, os usuários de mesmo perfil compartilham a mesma VLAN.

Ao criar uma VLAN você estará criando um domínio de broadcast (pacotes broadcast não são enviados de uma VLAN para outra). Por isso uma máquina na VLAN “A” não se comunicará com uma máquina na VLAN “B”. Para que haja comunicação entre hosts em VLANs diferentes é preciso que exista o roteamento entre as VLANs.

13

Vamos praticar?

Nada melhor que praticar para verificarmos o funcionamento de uma VLAN.

Primeiramente dispare o Packet Tracer instalado na sua máquina. Monte o cenário conforme figura a seguir:

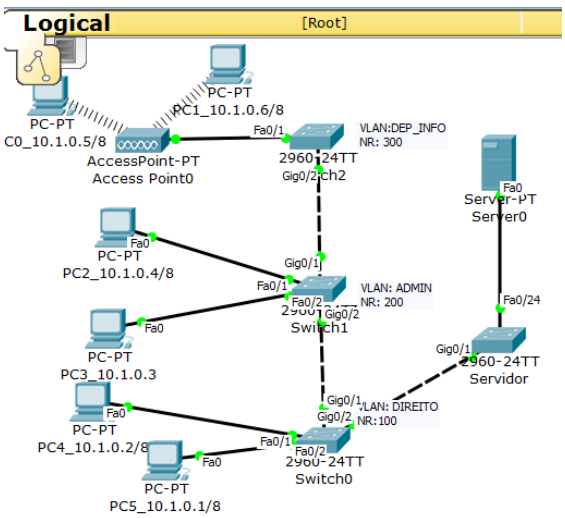


Figura 1.3: Criação de VLANs.
Fonte: O Autor, 2015.

configuração do switch servidor:

```
switch>en
switch#config t
enter configuration commands, one per line. end with cntl/z.
switch(config)#hostname servidor
servidor(config)#exit
servidor#wr
servidor#vlan database
servidor(vlan)#vtp server
device mode already vtp server.
servidor(vlan)#vtp domain projeto
changing vtp domain name from null to projeto
servidor(vlan)#exit
servidor#config t
servidor(config)#vlan 100
servidor(config-vlan)#name direito
servidor(config-vlan)#exit
servidor(config)#vlan 200
servidor(config-vlan)#name admin
servidor(config-vlan)#exit
servidor(config)#vlan 300
servidor(config-vlan)#name dep_info
servidor(config-vlan)#exit
servidor(config)#exit
servidor#
```

14

Configuração do switch client: neste caso, os comandos serão repetidos nos 3 switches 0, 1 e 2.

```
switch>enable
switch#vlan database
switch(vlan)#vtp client
switch(vlan)#vtp domain projeto
switch(vlan)#exit
switch#
```

O comando **show vlan no switch servidor** nos mostra:

```
servidor#show vlan
vlan name status ports
-------------------------------------------------------
1 default active fa0/1, fa0/2, fa0/3, fa0/4
fa0/5, fa0/6, fa0/7, fa0/8
fa0/9, fa0/10, fa0/11, fa0/12
fa0/13, fa0/14, fa0/15, fa0/16
fa0/17, fa0/18, fa0/19, fa0/20
fa0/21, fa0/22, fa0/23, gig0/2
100 direito active
200 admin active
```

```
300 dep_info active
1002 fddi-default act/unsup
1003 token-ring-default act/unsup
1004 fddinet-default act/unsup
1005 trnet-default act/unsup
(restante do relatório omitido)
------------------------------------------------------------------------
servidor#
```

O comando **show vlan no switch direito** nos mostra:

```
switch#show vlan
vlan name status ports
------------------------------------------------------------------------
1 default active fa0/3, fa0/4, fa0/5, fa0/6
fa0/7, fa0/8, fa0/9, fa0/10
fa0/11, fa0/12, fa0/13, fa0/14
fa0/15, fa0/16, fa0/17, fa0/18
fa0/19, fa0/20, fa0/21, fa0/22
fa0/23, fa0/24, gig0/1
100 direito active fa0/1, fa0/2
200 admin active
300 dep_info active
1002 fddi-default act/unsup
1003 token-ring-default act/unsup
1004 fddinet-default act/unsup
1005 trnet-default act/unsup
(restante do relatório omitido)
------------------------------------------------------------------------
```

15

Agora vamos configurar a porta trunk:

1- entre no modo de configuração global do switch0-Direito:
```
switch0# configure terminal
```

2- entre na interface que será trunk
```
switch0(config)# interface gig0/2
```

3- configure a porta como trunk
```
switch0(config-if)# switchport mode trunk
switch0(config-if)# end
switch0# wr
```

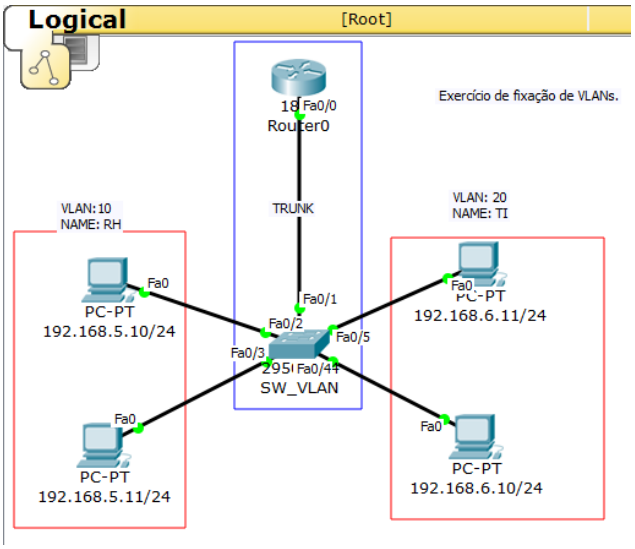
4- Repita os comandos para todas as portas trunk.

O comando “show run” mostra:

```
Switch#show run
.....................................
interface FastEthernet0/1
switchport access vlan 100
interface FastEthernet0/2
switchport access vlan 100
interface FastEthernet0/3
shutdown
.....................................
interface FastEthernet0/23
switchport mode trunk
interface FastEthernet0/24
interface GigabitEthernet0/1
switchport mode access
interface GigabitEthernet0/2
switchport mode trunk
.....................................
end
Switch#
```

16

Vamos a outro exemplo. Seja o cenário conforme figura a seguir:



Exemplo de VLANs
Fonte: O Autor, 2015

Configure os computadores conforme os IPs fornecidos, as VLANs 10 e 20, respectivamente RH e TI.

Configura as portas do switche conforme figura: fa0/1 modo trunk, fa0/2 e fa0/3 na vlan 10 do RH e as portas fa0/4 e fa0/5 na vlan 20 da TI.

Veja abaixo:

```
hostname sw_vlan
interface fastethernet0/1
switchport trunk allowed vlan 10,20
switchport mode trunk
interface fastethernet0/2
switchport access vlan 10
switchport mode access
interface fastethernet0/3
switchport access vlan 10
switchport mode access
interface fastethernet0/4
switchport access vlan 20
switchport mode access
interface fastethernet0/5
switchport access vlan 20
switchport mode access
```

17

O comando “show vlan brief” nos mostra:

```
sw_vlan#show vlan brief
vlan name status ports
----------------------------------------------------------
1 default active fa0/6, fa0/7, fa0/8, fa0/9
fa0/10, fa0/11, fa0/12, fa0/13
fa0/14, fa0/15, fa0/16, fa0/17
fa0/18, fa0/19, fa0/20, fa0/21
fa0/22, fa0/23, fa0/24, gig0/1
gig0/2
10 rh active fa0/2, fa0/3
20 ti active fa0/4, fa0/5
1002 fddi-default active
1003 token-ring-default active
1004 fddinet-default active
1005 trnet-default active
sw_vlan#
```

Observe que a porta fa0/2 está na VLAN 10 e que a porta fa0/4 está na VLAN 20, além disso, o switch está interligando duas redes diferentes, por meio do roteador “Router0”.

Para que os computadores se comuniquem, temos que configurar o Router0 para realizar o roteamento dessas VLANs, que estão em redes diferentes.

A porta fa0/1do Switch está ligada ao Router0 como Trunk, com isso a porta em modo Trunk consegue encaminhar o tráfego de outras VLANs.

18

Segue a configuração do modo trunk na porta do switch que o router está conectado.

```
switch(config)#inter f0/0
switch(config-if)#switchport mode trunk
switch(config-if)#switchport trunk allowed vlan 10
switch(config-if)#switchport trunk allowed vlan add 20
```

Vamos configurar as sub-interfaces e endereçamento IP no Router para que ele consiga rotear os pacotes entre as VLAN's.

```
Interface fastethernet0/0
no shutdown
exit
interface fastethernet0/0.1
encapsulation dot1q 1 native
ip address 192.168.1.1 255.255.255.0
interface fastethernet0/0.10
encapsulation dot1q 10
ip address 192.168.5.1 255.255.255.0
interface fastethernet0/0.20
encapsulation dot1q 20
ip address 192.168.6.1 255.255.255.0
r_vlan#
```

19

3.2 - O protocolo VTP (Virtual Trunk Protocol)

Segundo Filippetti (2008), este protocolo existe para gerenciar e manter a consistência de todas as VLANs configuradas em uma rede.

É necessário criar um servidor VTP. Todos devem utilizar a mesma identificação do domínio criado. O switch pode se encontrar em apenas um domínio de cada vez, logo um switch pode compartilhar informações do domínio VTP apenas com switches configurados dentro do mesmo domínio. As informações são repassadas pela porta tronco (trunk ports).

As **vantagens** de se utilizar o sistema VTP são:

1- permite que administradores adicionem, apaguem ou renomeiem VLANs com as alterações repassadas automaticamente propagadas para todos os switches pertencentes ao domíno VTP;
2- provê configuração de VLAN consistente entre todos os switches pertencentes a um mesmo

domínio;
3- permite que VLANs sejam truncadas através de redes mistas, como Ethernet para ATM ou FDDI;
4- mantém controle e monitoramento precisos sobre VLANs;
5- reporta VLANS adicionadas automaticamente para todos os switches pertencentes ao domínio;
6- permite a adição plug-and-play de VLANs.

20

3.3 - Como opera o VTP?

Ainda segundo Filippetti (2008), uma vez inseridos em um domínio VTP, switches podem ser configurados para interagir com as atualizações VTP propagadas de três formas distintas:

1 – servidor

Modo necessário para o switch criar, adicionar ou apagar VLANs em um domínio VTP. Mudanças de informações VTP também devem ser efetuadas nesse modo. Qualquer alteração sofrida por um switch é propagada para todo o domínio VTP.

2 – cliente

Nesse modo os switches recebem informações dos servidores VTP e enviam e recebem atualizações, mas não efetuam alterações. Nenhuma porta do cliente pode ser associada a uma nova VLAN antes de o servidor VTP notificar o cliente da existência dessa nova VLAN.

3 – transparente

Quando o switch não participa do domínio VTP, mas encaminha atualizações VTP por meio dos links configurados. Nesse modo um switch pode adicionar ou apagar VLANs, ele mantém a própria base, mas não a compartilha com os demais, apenas propaga as informações do servidor.

Com isso terminamos o primeiro módulo dedicado à recordação da infraestrutura necessária para a implementação dos protocolos de roteamento, conceitos que estudaremos no próximo módulo.

21

RESUMO

Como visto, a comutação (switching) na camada de enlace é baseada no endereço MAC da placa de rede do dispositivo para fazer a filtragem da rede.

O que torna a comutação na camada de enlace tão eficiente é a não modificação no pacote de dados, somente no quadro que a encapsula. Também é menos susceptível a erros.

Pode ser utilizada para testar conectividade entre grupos de trabalho e para a segmentação da rede (quebra do domínio de colisão). Ela aumenta a largura da banda disponível para cada usuário.

Recorde que a camada de enlace acomoda switches e bridges, porém existem diferenças importantes. Lembre-se dessas diferenças.

A figura a seguir ilustra o processo de aprendizagem do switch.

1 – a estação 1 quer se comunicar com a 6;

2 – a tabela MAC já se encontra formada;

3 – cada porta de conexão do switch tem o MAC de cada estação associada à mesma;

4 – a comunicação ocorre somente entre as estações interessadas.

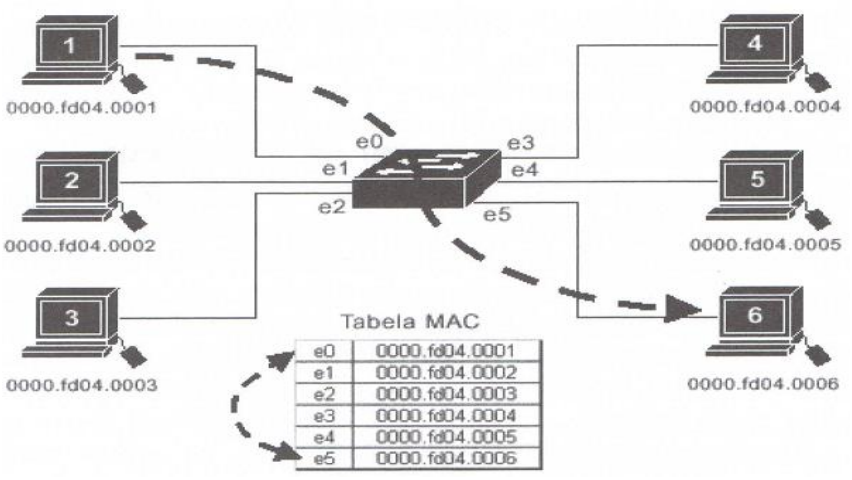


Figura 1.1: Comunicação ente rede comutada. Fonte: CCNA 4.1-Felippetti, 2008

Lembre-se, também, assim que o quadro chega à interface de um switch, o endereço do hardware de destino é comparado com a tabela MAC. Se o endereço de destino for conhecido e estiver presente na tabela então o frame é encaminhado apenas para a porta de saída associada àquele endereço (frame filtering).

22

Outro item importante é o Spanning Tree Protocol (STP), que permite resolver problemas de loop em redes comutadas cuja topologia introduza ciclos nas ligações. O algoritmo Spanning Tree determina qual é o caminho mais eficiente entre cada segmento separado por bridges ou switches. Caso ocorra um problema nesse caminho, o algoritmo recalculará entre os existentes, o novo caminho mais eficiente, habilitando-o automaticamente. O nome deriva do algoritmo spanning tree da teoria dos grafos.

Outro conceito importante é o da VLAN, que é um recurso disponível em switches cuja característica principal é a segmentação da rede. Uma VLAN é uma rede lógica que permite separar grupos de usuários e assim proporcionar uma melhoria no funcionamento da rede (desempenho, segurança, precisão). Uma das aplicações da VLAN é no agrupamento de portas dos switches de acordo com os departamentos da empresa (Administrativo, Financeiro, Recursos Humanos e outros).

E finalmente, o VTP (Virtual Trunk Protocol), que gerencia e mantém a consistência de todas as VLANs configuradas em uma rede.

As vantagens de se utilizar o sistema VTP são:

1 – permite que administradores adicionem, apaguem ou renomeiem VLANs com as alterações repassadas autometicamente propagadas para todos os switches pertencentes ao domíno VTP;

2 – provê configuração de VLAN consistente entre todos os switches pertencentes a um mesmo domínio;

3 – permite que VLANs sejam truncadas através de redes mistas, como Ethernet para ATM ou FDDI;

4 – mantém controle e monitoramento precisos sobre VLANs;

5 – reporta VLANS adicionadas automaticamente para todos os switches pertencentes ao domínio;

6 – permite a adição plug-and-play de VLANs.

UNIDADE 2 – SWITCHES, VLANS E ROTEAMENTO IP

MÓDULO 2 – ROTEAMENTO ESTÁTICO IP

01

1 - CONCEITO DE ROTEAMENTO IP

Conforme Filippetti (2008), antes de iniciar os conceitos de roteamento estático devemos saber que o Processo de Roteamento IP é um tópico pertinente a todos os roteadores e configurações que utilizam o protocolo IP.

O roteamento IP é um conjunto de regras que definem como dados originados em uma determinada sub-rede devem alcançar outra. Para partir de uma rede e alcançar outra, um roteador precisa fazer o direcionamento do pacote, analisar o seu cabeçalho e consultar sua **tabela de roteamento**.

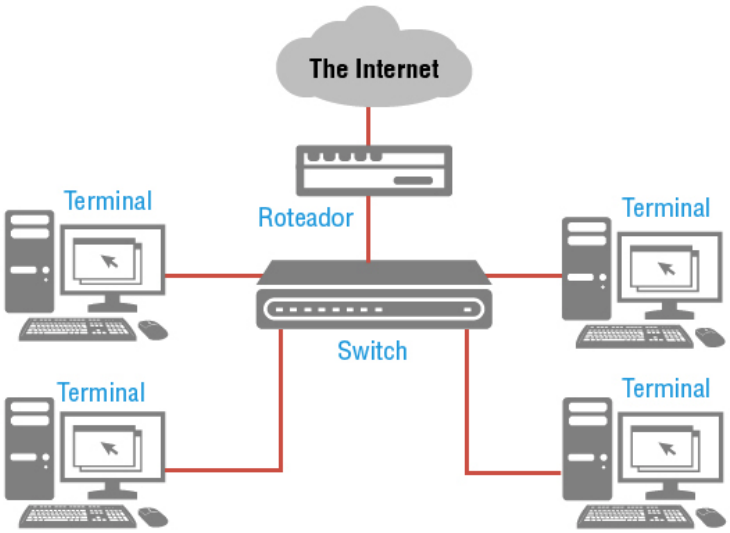
Sempre que sairmos de uma rede e entramos em outra, um roteador ou dispositivo equivalente estará por trás desse processo.

02

1.1 - O que são Roteadores?

Ainda conforme Filippetti (2008), roteadores são, na prática, dispositivos próprios ou computadores com uso específico. Isso porque os roteadores possuem processador, memória, ROM, RAM, memória NVRAM e Flash, as duas últimas atuando como dispositivos de armazenamento.

Podem-se usar computadores para executar a tarefa de roteadores, mas não com a mesma eficiência. Isto ocorre porque os roteadores possuem um processador projetado com instruções específicas para otimizar o processamento de pacotes com as informações necessárias e tomar as decisões de direcionamento, subordinados a um sistema operacional também específico.



03

No caso de um computador comum, por melhor que ele seja em vários aspectos, seu processador é projetado para executar um número bastante variado de instruções com diversos fins, subordinado a um sistema operacional com funções também bastante variadas.

Assim, roteadores são mais eficazes que computadores para essa tarefa, embora esses últimos possam ser utilizados, tal como ocorre em nosso dia a dia, particularmente em empresas de menor porte visando redução de investimentos em *hardware* de redes.

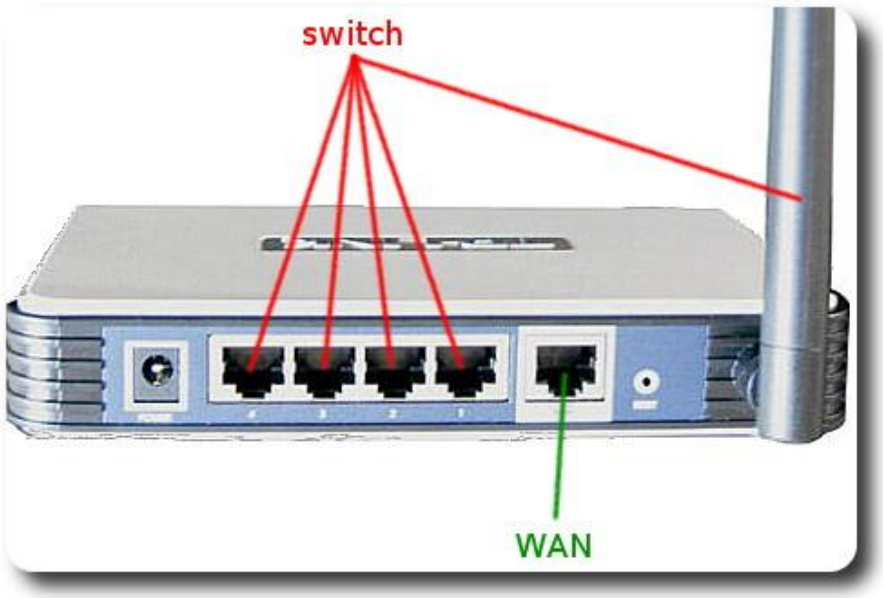
Fique Atento!

A capacidade de processamento e direcionamento de pacotes é um dos fatores que diferenciam marcas e modelos de roteadores e deve ser levada em conta, juntamente com seus recursos de *hardware* e sistema operacional, no momento da decisão de adquirir um equipamento que atenda aos requisitos presentes e futuros – dentro de cinco anos a partir de hoje, por exemplo – de tráfego na rede da organização.

04

Os roteadores wireless, muito comuns atualmente, em sua grande parte são produzidos para o mercado SoHo (*Small office Home office*, ou seja, pequenos escritórios e escritórios domésticos) e são uma combinação de roteador com switch.

A função principal dos mesmos é a mesma de um switch (comutação de pacotes). Esses equipamentos possuem uma entrada WAN (com endereço fornecido por uma operadora de banda larga) e de duas a quatro portas para encaminhamento de pacotes (switch) entre a rede externa (WAN) e a rede interna (LAN), além de oferecerem sinal de rádio para computadores com interface wireless Wi-Fi na rede local. Esses equipamentos não são o foco de nosso estudo nesta disciplina.



A função básica dos roteadores é direcionar pacotes com destino a redes locais e remotas, com diferentes endereços de rede e encaminhar esses pacotes entre a interface de entrada e a de saída.

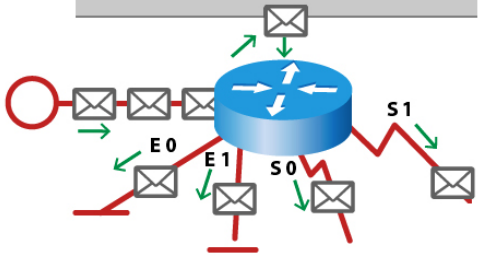
05

Conforme CCNA – Cisco Certified Network Associate-Study Guide (2005), roteadores não direcionam pacotes dentro de uma mesma rede ou sub-rede e, por essa razão, cada uma de suas interfaces – no mínimo duas – deve ter um “endereço válido de host” - já que se comportam como gateways da rede ou sub-rede à qual pertencem - diferentes entre si. Para executar essa tarefa eles constroem tabelas de roteamento, onde são armazenados os caminhos para que pacotes possam ser enviados a seus destinos finais.

Quando um pacote é recebido pelo roteador, ele analisa o endereço IP do pacote e procura a melhor correspondência entre este endereço de rede em sua **tabela de roteamento**.

Exemplo de uma tabela de Roteamento IP

Rede	Interface de Destino
172.16.100.0 / 24	Ethernet 0
172.16.200.0 / 24	Serial 1
172.17.0.0 / 16	Ethernet 0
172.18.10.0 / 24	Ethernet 0
172.18.20.0 / 24	Ethernet 1



A decisão de direcionamento é sempre tomada na camada 3 (rede) do modelo OSI, ou camada Internet no modelo TCP/IP. Assim roteadores acessam as camadas 1, 2 e 3 do modelo OSI e camadas de Acesso à Rede e Internet no modelo TCP/IP. Durante o roteamento os endereços de camada 2 (enlace) de origem e destino são das interfaces dos roteadores envolvidos no direcionamento, ou seja, a cada salto os endereços MAC de origem e destino são alterados, mas os endereços IP de origem e destino se mantém.

Isso corre porque o encapsulamento/desencapsulamento na camada 2 é refeito a cada salto, enquanto o processamento do pacote – encapsulamento/desencapsulamento na camada 3 - somente é feito para leitura do endereço IP de destino em busca da melhor rota. Quando o pacote chegar ao dispositivo de destino final, ocorrerá o processamento definitivo do pacote na camada 3.

Tabelas de roteamento
As tabelas de roteamento podem ser de dois tipos:

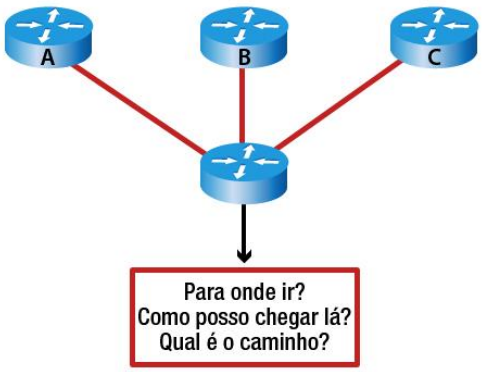
- **Dinâmica**: que se apoia em protocolos de roteamento do tipo RIP, OSPF e outros, com base em algoritmos, para escolher a melhor rota e seguem critérios denominados "métrica de roteamento".

Estática: é definida pelo administrador da rede, que utiliza comandos para adicionar cada rota manualmente, em cada roteador da rede. Este método somente é indicado para pequenas redes, onde existe um pequeno número de roteadores, com poucas rotas e rotas que não são alteradas frequentemente.

06

Segundo Filippetti (2008), ao direcionar o pacote para outro roteador, o novo endereço MAC deste novo quadro será da interface de saída e o MAC de destino será da interface de próximo salto, ou seja, no próximo roteador para onde será enviado o pacote que busca chegar a seu destino final.

A tabela de roteamento inclui ainda o endereço da interface de saída para encaminhar o pacote. Uma vez encontrada correspondência o roteador encapsula o pacote no quadro (frame) da camada de enlace da interface de saída e envia o pacote para seu destino.



Em muitos casos o próximo roteador ainda não é o destino final, mas provavelmente "conhece" um caminho para tanto, podendo essa operação se repetir diversas vezes, como é comum ocorrer na rede mundial.

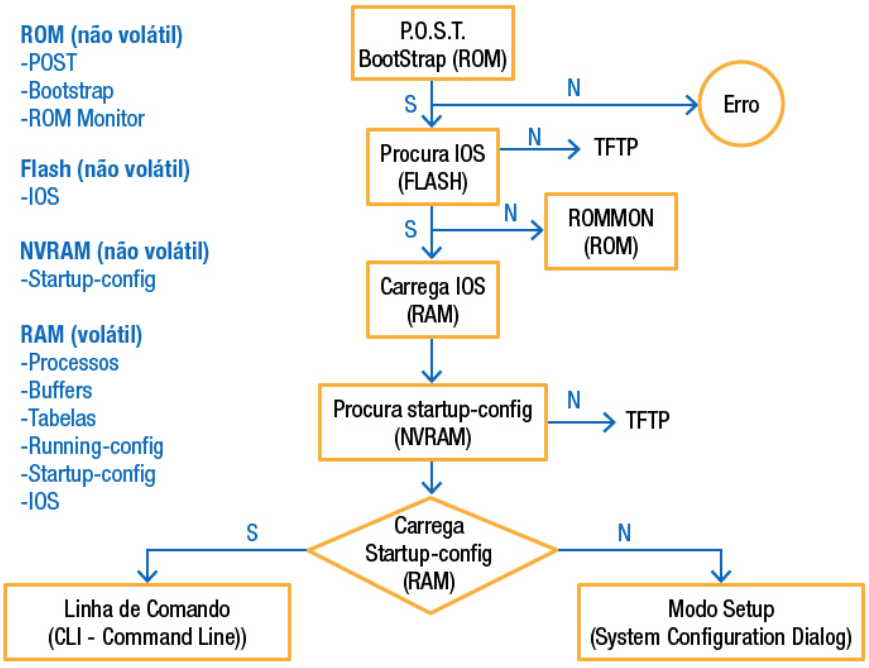
Para efetuar o roteamento de pacotes o roteador deve ter conhecimento de, no mínimo:

1) endereço de destino,
2) roteadores vizinhos,
3) rotas possíveis às redes remotas,
4) melhor rota para cada rede remota e
5) como manter e verificar informações relativas ao roteamento.

07

1.2 - Sequência de boot do roteador

Conforme CCNA – Cisco Certified Nework Associate–Study Guide (2005), como todo computador, os roteadores seguem uma sequência de boot, como mostra o fluxograma abaixo:



Boot do roteador
Fonte: CCNA, 2005

08

1.3 - Interfaces

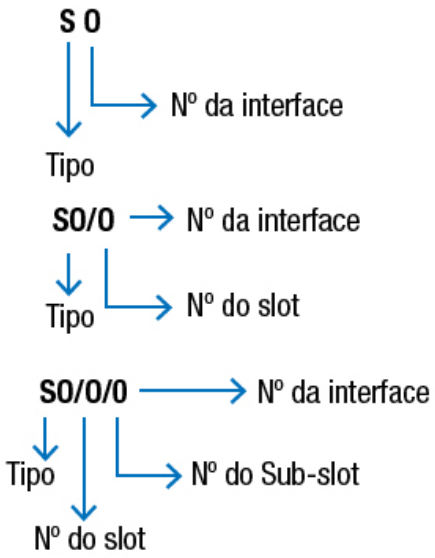
Ainda conforme o CCNA – Cisco Certified Nework Associate–Study Guide (2005), os roteadores podem ter dois tipos de interface:

- conectadas à **LAN** (Ethernet, Fast Ethernet, Gigabit, fibra óptica);
- conectadas à **WAN** (serial, ISDN, Frame Relay, ATM, FDDI).

Ao acessar um roteador para configurá-lo, utilizamos outras duas interfaces: **auxiliar** e **console**. Nem sempre o roteador terá uma interface Auxiliar (AUX), mas sempre disporá de uma interface de Console (CON). A interface AUX é utilizada para conexões remotas visando configurações, utilizando um modem com “conexão discada”. Já a porta CON é empregada para configurações do equipamento, utilizando-se um cabo rollover conectado a um computador próximo ao roteador (um notebook do administrador da rede, por exemplo). Ambas são portas padrão RJ-45.

Depois de configurado o roteador pela porta Console, também é possível fazer a manutenção e administração pelas interfaces citadas acima, usando TELNET ou o SSH. O SSH é o mais indicado por ser mais seguro permitindo criptografia, enquanto o TELNET envia texto plano e não permite criptografia.

As interfaces em roteadores podem ser identificadas e nominadas, conforme segue abaixo:



Identificação das Interfaces de um roteador.
Fonte: CCNA, 2005.

09

1.4 - Cabos usados em conexões Ethernet

Conforme o Help do Packet Tracer 6.2.0, para interligar os roteadores devemos ter para cada par de conexões cabos específicos. No caso de interfaces padrão Ethernet temos cabo direto (straight-through) e cabo cruzado (crossover).

Cabos diretos (*straight-through*) são usados entre conexões:	**Cabos cruzados** (*crossover*) são usados entre conexões:
• Switch a roteador • Switch a computador (ou similar) • Hub a computador (ou similar) • Hub a servidor	• Switch a switch • Computador a computador • Switch a hub • Hub a hub • Roteador a roteador • Roteador a servidor

10

1.5 - Comandos básicos para configuração de roteadores

Conforme Nascimento e Tavares (2012), a configuração dos roteadores é feita por meio do ambiente CLI (Command Line Interface). Os principais comandos são apresentados na tabela a seguir.

Alguns comandos de configuração dos roteadores CISCO.

Prompt	Descrição
Router>	Ambiente do modo de execução do usuário. Nesse modo o usuário pode visualizar informações sobre o roteador, mas não pode fazer alterações.
Router> enable	Para acessar o modo privilegiado.
Router#	Ambiente do modo "exec privilegiado". Esse modo suporta os comandos de debugging e de teste, exames detalhados do roteador, manipulação dos arquivos de configuração e acesso aos modos de configuração.
Modo Setup	Apresenta um dialogo interativo para uma configuração básica inicial.
Router(config)#	Modo de configuração global, utilizada para executar a configuração de um roteador.
Router(config-if)#	Modo de configuração de interface.
Router(config-line)#	Modo de configuração de Terminal Virtual.
Router#configure terminal	Acessa a configuração manual a partir do terminal de console.
Router> ?	Exibe os comandos disponíveis no ambiente de consulta para usuário normal.
Router# ?	Exibe os comandos disponíveis no ambiente de usuário privilegiado.
Router(config)# ?	Exibe os comandos disponíveis no ambiente de configuração global.

Fonte: Nascimento & Tavares, 2012.

Caso queira saber todos os comandos dos dispositivos switches e roteadores, observe os comandos das três últimas linhas da tabela acima citada.

11

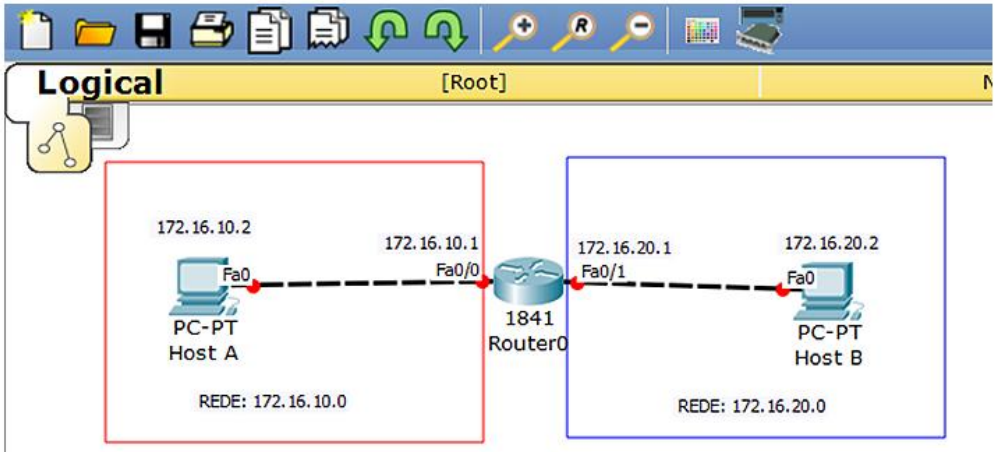
1.6 - Conceitos Importantes acerca do Roteamento IP

Conforme Filippetti (2008), o roteador "aprende" sobre as redes remotas por meio da comunicação com os roteadores vizinhos (roteamento dinâmico) ou por meio do administrador (roteamento estático). O roteador cria uma tabela de roteamento que descreve como encontrar tais redes remotas. Se um pacote é endereçado a uma rede cujo endereço não se encontra nessa tabela o pacote é descartado. Não há envio de mensagens de broadcast ou qualquer outro esquema utilizado para se descobrir tal rota.

Veremos como configurar os roteadores da rede sugerida para que suas tabelas incluam os endereços da redes remotas.

Os 3 modos diferentes de roteamento que podem ser utilizados são: estático, dinâmico (RIPv1, RIPv2, EIGRP, OSPF são aqueles que serão vistos nesta disciplina) e default.

Seja a figura do cenário abaixo:



Funcionamento do processo de roteamento IP.
Fonte: O Autor, 2015.

Acompanhe, a seguir, os passos para o roteamento.

12

Vamos ao passo a passo do roteamento.

Considere que o cenário esteja plenamente funcional (IPs, gateways dos hosts, portas dos roteadores- fa0/0 e fa0/1- devidamente configurados conforme dados da figura anterior). Veja que as redes estão diretamente conectadas ao roteador “Router 0”, portanto a tabela de roteamento já possui os endereços IPs de ambas as redes.

1- Da interface de comando (CLI) um usuário digita no host 172.16.10.2 o comando “ping 172.16.20.2”. Um pacote ICMP é então gerado no host A.

2- O protocolo IP trabalha em conjunto com o protocolo ARP para determinar qual rede o pacote é destinado. Determinado que o pacote é destinado a uma rede remota e não à local, ele é enviado para o roteador para que seja roteado para a rede de destino.

3- Para o host A enviar um pacote para o roteador, ele deve saber o endereço MAC da interface conectada à rede local (fa0/0). Para obter esse endereço, o host realiza uma pesquisa no ARP cachê.

4- Caso o endereço IP da interface fa0/0 não se encontre no ARP cachê, o host A emite uma mensagem de broadcast ARP, procurando identificar o endereço de hardware que corresponde ao endereço IP 172.16.10.1. Por isso que, normalmente, o primeiro “ping” expira (time out) e os outros quatro são bem sucedidos. Uma vez que o endereço seja armazenado no ARP cache do host, não mais ocorrem time outs.

5- A interface fa0/0 do roteador responde com o endereço MAC dele. O host A tem o necessário para transmitir o pacote para o roteador. A camada de rede passa o pacote gerado através da requisição ICMP (ICMP echo request = ping) para a camada de enlace juntamente com o endereço de hardware para onde o host A deseja enviar o pacote (interface fa0/0 do roteador). O pacote inclui o endereço IP da origem (source address), do destino (destination address) e o protocolo ICMP especificado no campo “protocolo” da camada de rede.

6- A camada de enlace gera um quadro que encapsula o pacote com informações de controle necessárias à sua transmissão pela rede local. Essas informações incluem os endereços MAC de origem, MAC do destino e o campo “type” que especifica qual protocolo de camada de rede está ativo (no caso o IP).

7- A camada de enlace do host A para o quadro gerado para a camada física que codifica os dados em 0s e 1s e os transmite por meio da interface local.

8- O sinal é captado pela interface FastEthernet 0/0 do roteador que sincroniza com o preâmbulo e efetua a extração do quadro. A interface realiza uma verificação (CRC) e compara o resultado obtido com o campo FCS, localizado no quadro, assegurando se a integridade do quadro foi mantida.

9- O endereço MAC do destino é verificado.

10- O protocolo IP verifica o endereço IP de destino do pacote recebido para certificar-se que o pacote é, de fato, destinado ao roteador. O roteador determina que o pacote é de uma rede diretamente conectada à interface fa0/1.

11- O roteador armazena o pacote no buffer da interface fa0/1. Ele gera um quadro para transmitir o pacote ao seu destino final. Primeiro ele verifica a tabela ARP para determinar se o endereço MAC de destino foi resolvido para o endereço IP em alguma comunicação anterior. Caso negativo, o roteador emite uma mensagem broadcast ARP pela interface fa0/1 para que o endereço 172.16.20.2 seja localizado.

12- O host B responde a essa mensagem com o endereço MAC da interface dele com a rede. O roteador possui, agora, todos os elementos para transmitir o pacote ao destino final. O quadro gerado pela interface fa0/1 do roteador possui o endereço MAC de destino (interface de rede instalada no host B). Mesmo que os endereços MACs do quadro mudem a cada interface que é atravessada, os endereços IPs de origem e de destino nunca são alterados, apenas alguns campos do cabeçalho do quadro sofre alterações.

13- O host B recebe o quadro e procede a checagem com o CRC. Caso não haja problemas o pacote é passado para a camada de rede responsável peal operação IP. O protocolo IP verifica o endereço IP de destino. Se coincidir com o IP do host B então analisa o campo protocolo do pacote para determinar qual o propósito do mesmo.

14- Determinada que o pacote é uma requisição ICMP, o host B gera um novo pacote ICMP com o endereço de destino sendo o IP do host A.

15- O processo reinicia no rumo oposto até atingir o host A, o seu destino final.

1.7 - Métrica

Conforme Nascimento e Tavares (2012), há casos em que um protocolo de roteamento aprende mais de uma rota para o mesmo destino. Para selecionar o melhor caminho, o protocolo de roteamento deve poder avaliar e diferenciar os caminhos disponíveis. A métrica é usada para essa finalidade.

Métrica é um valor usado por protocolos de roteamento para atribuir custos com a finalidade de alcançar redes remotas. A métrica é usada para determinar o melhor caminho quando houver vários caminhos para a mesma rede remota.

Cada protocolo de roteamento usa sua própria métrica. Por exemplo, o RIP usa a contagem de saltos, o OSPF usa a largura de banda. A contagem de saltos é a métrica mais fácil de visualizar. A contagem de saltos se refere ao número de roteadores que um pacote deve atravessar para alcançar a rede de destino.

A métrica usada em protocolos de roteamento IP pode ainda incluir:

- **Contagem de saltos;**
- **Largura de banda;**
- **Carga;**
- **Atraso;**
- **Confiabilidade;**
- **Custo.**

Contagem de saltos
É uma métrica simples que conta o número de roteadores que um pacote deve atravessar.

Largura de banda
Influencia a seleção do caminho ao escolher o caminho com a maior largura de banda.

Carga
Considera a utilização de tráfego de determinado link.

Atraso
Considera o tempo que um pacote leva para atravessar um caminho.

Confiabilidade
Avalia a probabilidade de uma falha de link, calculada a partir da contagem de erros de interface ou de falhas de link anteriores.

Custo
Um valor determinado pelo IOS ou pelo administrador de rede para indicar sua preferência por uma rota. O custo pode representar uma métrica, uma combinação de métricas ou uma política.

1.8 - Distância Administrativa

Conforme Filippetti (2008), a distância administrativa (AD, Administrative Distance) define a preferência de uma origem de roteamento. Cada origem de roteamento, incluindo protocolos de roteamento específicos, rotas estáticas e até mesmo redes diretamente conectadas, é priorizada na ordem da mais para a menos preferível usando um valor de distância administrativa.

A distância administrativa é um valor inteiro que varia de 0 a 255. Quanto menor o valor, melhor será a origem de rota. A melhor distância administrativa é zero (0). Somente uma rede diretamente conectada tem uma distância administrativa igual a zero (0). Uma rede cuja origem é uma rota estática tem AD igual a 1, enquanto redes com origem no protocolo RIP apresentam AD de 120 e, finalmente, redes com origem no protocolo OSPF têm como 110 o valor característico e único de sua distância administrativa. Veja tabela 2.2 abaixo listada.

Distâncias Administrativas

Protocolo	AD
Conectada	0
Estática	1
OSPF	110
RIP	120

Fonte: Nascimento &Tavares, 2012.

Observe o exemplo de um relatório abaixo listado. O mesmo foi obtido por meio do comando “show ip route” dado no ambiente do usuário privilegiado do roteador nomeado como R1 em um cenário hipotético submetido ao protocolo OSPF.

```
R1#show ip route
Codes: 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
Gateway of last resort is not set
172.20.0.0/16 is variably subnetted, 6 subnets, 4 masks
C 172.20.20.0/26 is directly connected, FastEthernet1/0
O 172.20.20.96/28 [110/65] via 172.20.20.122, 00:00:11, Serial0/1
C 172.20.20.120/30 is directly connected, Serial0/1
O 172.20.20.116/30 [110/128] via 172.20.20.122, 00:00:11, Serial0/1
C 172.20.20.112/30 is directly connected, Serial0/0
O 172.20.20.64/27 [110/65] via 172.20.20.114, 00:00:11, Serial0/0
```

Para analisar a tabela acima, observe que:

O – indica a rede alcançada pelo protocolo OSPF;

110 – indica a distância administrativa característica do protocolo OSPF;

65 – indica o custo do caminho para atingir a rede de destino.

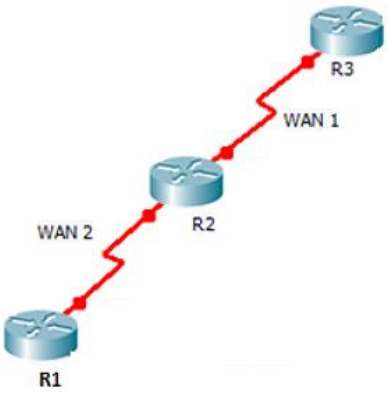
Ao analisar tabelas de roteamento, para a mesma topologia, compare as tabelas de roteamento para RIPv1, RIPv2 e OSPF. Observe com atenção especial como cada protocolo trata as sub-redes e a sumarização de rotas.

15

1.9 - Conceito de vizinhança

Conforme Filippetti (2008) e Nascimento e Tavares (20012), o conceito de vizinhança permite que os dispositivos conheçam melhor a topologia da rede da qual fazem parte.

No caso de roteadores, vizinhos são os dispositivos que compartilham o mesmo intervalo (faixa, range) de endereços IP.



Vizinhança entre roteadores
Fonte: O Autor, 2015.

Por exemplo, na figura acima, R1 e R2 são vizinhos compartilhando a rede WAN 2, assim como R2 e R3 compartilhando a rede WAN 1, mas R1 e R3 não são vizinhos, pois não compartilham nenhuma conexão de rede.

Para verificar os dispositivos vizinhos os roteadores, por meio de seus protocolos de roteamento, enviam mensagens específicas para processamento na camada de enlace dos dispositivos conectados em rede.

16

Os **anúncios periódicos de vizinhança** contêm informações importantes como marca do equipamento, modelo, endereços IP das interfaces e versão do sistema operacional.

Dizemos periódicos porque cada protocolo apresenta, por padrão (*default*), um período de tempo característico para o envio dos anúncios (*advertisements*).

Outra característica em comum aos dispositivos que trocam anúncios de vizinhança é a **possibilidade de desabilitar os anúncios de vizinhança** em interfaces específicas. Isto é muito útil quando temos uma interface de um roteador conectado à Internet, por exemplo, e não desejamos fornecer dados sobre esse equipamento para dispositivos não confiáveis.

Pessoas mal intencionadas poderiam usar estas informações para planejar e realizar ataques à rede da organização. Em casos nos quais uma interface esteja diretamente conectada a uma interface de um servidor, por exemplo, também é recomendável desabilitar o envio dos pacotes de vizinhança nesta interface. Isso se deve ao fato de o servidor não ler os anúncios e, portanto, não respondê-los. Deixar o serviço de anúncios de vizinhança habilitado nestes casos seria consumir banda desnecessariamente.

Ao serem enviados periodicamente, os anúncios periódicos de vizinhança, têm a importante função de informar alterações eventualmente ocorridas na rede, tais como:

- Falha de um link;

- Novo link;

- Perda de hardware (falha de um roteador);

- Alteração das configurações de um link (endereço IP, por exemplo).

Esses conceitos são suficientes para que possamos prosseguir. Veremos no próximo item os conceitos necessários para implementar o roteamento estático.

17

2. Roteamento Estático

Conforme Filippetti (2008), as rotas estáticas são definidas manualmente pelo administrador de redes. Da mesma forma, somente ele pode alterá-las ou desabilitá-las. As rotas estáticas são úteis em pequenas topologias, particularmente se tivermos apenas dois roteadores com uma interface cada a conectá-los, requerendo apenas uma única rota, embora possam ser utilizadas juntamente com rotas dinâmicas ou mesmo em topologias um pouco mais complexas.

Temos duas situações:

1) na primeira situação seria um desperdício de recursos configurar um protocolo de roteamento dinâmico em uma rede de topologia tão simples como a vista anteriormente;

2) na segunda situação, manter rotas de modo estático em topologias mais complexas e que sofrem alterações com frequência seria muito trabalhoso, resultando em maior probabilidade de erros humanos.

Cabe ao administrador de rede analisar e escolher a opção mais interessante.

O processo de roteamento IP é simples e não muda, independentemente do tamanho ou complexidade da rede.

Vantagens do roteamento estático	Desvantagens do roteamento estático
1. Redução do overhead na CPU do roteador. 2. Não utiliza largura de banda entre os roteadores. 3. Segurança, pois o administrador possui controle total do processo de roteamento.	1. Profundo conhecimento global da rede. 2. Adições e remoções de rotas de redes devem ser feitas manualmente. 3. Pouco viável para redes de grande porte, devido ao emprego de protocolos diversos.

18

2.1 - Criando uma rota estática

Segundo Nascimento e Tavares (2012), no roteamento estático nos preocuparemos somente com as redes remotas. As redes diretamente conectadas não precisam ser configuradas, pois o roteador já as conhece e, portanto, os respectivos caminhos para chegar até as mesmas.

A sintaxe do comando é:

`ip route [rede de destino] [máscara] [endereço do próximo ponto ou interface de saída] [distância administrativa] [permanente]`, onde:

1- **ip route**

Instrução que designa rota estática.

2- **rede de destino**

Endereço da rede a adicionar na tabela de roteamento.

3- **Máscara**

Máscara da rede de destino.

4- **endereço do próximo ponto**

Endereço do ponto que receberá o pacote e o enviará à rede de destino.

5- **interface de saída**

Utilizada no lugar do ip do próximo ponto. Utilizada somente para as interfaces seriais, para interfaces ethernet não funciona.

6- **distância administrativa**

O padrão é “1”. Se quiser pode mudar para qualquer valor de 1 a 254. O valor 255 torna a rede inalcançável. Sempre utilizaremos o padrão (default).

7- **Permanente**

Caso uma interface esteja desativada ou o roteador não possa se comunicar com o próximo ponto após um determinado período de tempo a rota é automaticamente descartada da tabela de roteamento. “Permanent” mantém sempre os dados da tabela de roteamento. Nós utilizaremos esse parâmetro sempre padrão (default).

19

Para criarmos uma rota estática para as redes remotas precisamos acessar o modo de configuração global e utilizar a seguinte sintaxe (o Router1, os IPs e máscaras foram atribuídos aleatoriamente):

```
Router1(config)#ip route 10.11.21.0 255.255.255.248 Fa 0/0
```

Onde:

- “ip route” é o comando para criar uma rota;
- “10.11.21.0 255.255.255.248” é o endereço IP e respectiva máscara da rede a ser alcançada (rede de destino);
- “Fa 0/0” é a interface de saída para chegar à rede de destino.

Podemos realizar a mesma tarefa de modo um pouco diferente:

```
Router1(config)#ip route 10.11.21.0 255.255.255.248 10.10.10.1
```

Onde:

- “ip route” é o comando para criar uma rota;
- “10.11.21.0 255.255.255.248” é o endereço IP e respectiva máscara da rede a ser alcançada (rede de destino);
- “10.10.10.1” é o endereço da interface de próximo salto.

As duas instruções (rotas) farão o mesmo trabalho, mas configurar rotas estáticas com interface de saída tem a vantagem de requisitar apenas uma pesquisa na tabela de roteamento em busca da interface de saída. No caso de usarmos endereço de próximo salto, será necessária uma segunda pesquisa para resolver o endereço de próximo salto.

Nos nossos exemplos desenvolvidos no Packet Tracer iremos utilizar a segunda opção por questão de hábito do professor.

Pronto!

É o suficiente para podermos partir para a implementação do protocolo de roteamento estático. No próximo item estudaremos a configuração do mesmo.

20

2.2 - Configuração do Roteamento Estático

Para a configuração do roteamento estático seguiremos o cenário fictício da figura a seguir. É uma rede um pouco mais complexa do que a vista anteriormente, no conceito de roteamento IP. Nele todas as redes têm máscara /24 ou 255.255.255.0.

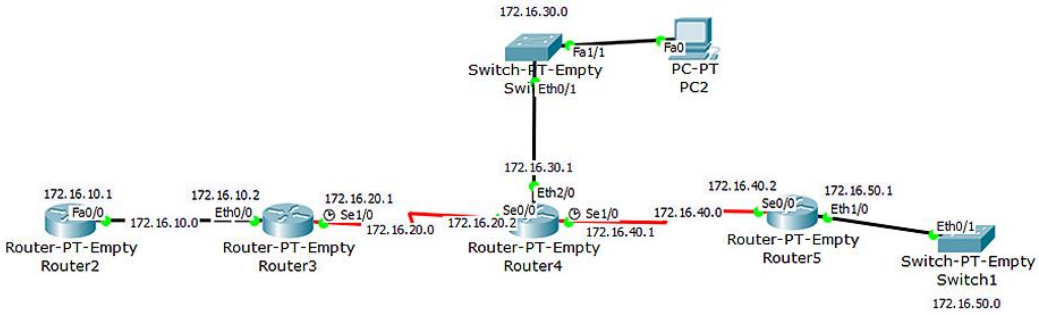


Figura 2.4: Rede mais complexa.
Fonte: O Autor, 2015.

Vamos fazer a configuração de cada um dos roteadores para o roteamento estático

```
Router 2:
Router>enable (entra no ambiente de usuário privilegiado)
Router#configure terminal (entra no ambiente de configuração global)
Router(config)#interface fa0/0 (entra na interface)
Router(config-if)#ip address 172.16.10.1 255.255.255.0 (atribuição de IP e msc)
Router(config-if)#no shut (para ativar a interface)
Router(config-if)#exit (para sair da interface e voltar ao ambiente de configuração
global)
Router(config)#ip route 172.16.20.0 255.255.255.0 172.16.10.2
Router(config)#ip route 172.16.30.0 255.255.255.0 172.16.10.2
Router(config)#ip route 172.16.40.0 255.255.255.0 172.16.10.2
Router(config)#ip route 172.16.50.0 255.255.255.0 172.16.10.2
Router(config)#end (término da configuração)
Router#wr (para salvar a configuração feita)
```

Observe:

1 – ip route é a instrução para o roteamento estático;
2 – 172.16.20.0 é a rede de destino considerada;
3 – 255.255.255.0 é a máscara da rede de destino considerada;
4 – 172.16.10.2 é o next hop, ou seja, o IP da porta de entrada para a rede de destino;

Pronto! Router 2 está configurado.

Como as configurações não mudam, vamos ao próximo roteador. Lembre-se: roteamento estático somente para as redes distantes (remotas).

Veja o roteador Router 3
Passemos ao roteador Router 4
Finalmente o Router 5

```
Router 3

Router 3
```

```
Router> enable
Router# configure terminal
Router(config)#interface eth0/0
Router(config-if)#ip address 172.16.10.2 255.255.255.0
Router(config-if)#no shut
Router(config-if)#exit
Router(config)#interface se1/0
Router(config-if)#ip address 172.16.20.1 255.255.255.0
Router(config-if)#no shut
Router(config-if)#exit
Router(config)#ip route 172.16.30.0 255.255.255.0 172.16.20.2
Router(config)#ip route 172.16.40.0 255.255.255.0 172.16.20.2
Router(config)#ip route 172.16.50.0 255.255.255.0 172.16.20.2
Router(config)#end
Router#wr

O Router 3 está pronto.
```

Router 4

```
Router> enable
Router# configure terminal
Router(config)#interface eth2/0
Router(config-if)#ip address 172.16.30.1 255.255.255.0
Router(config-if)#no shut
Router(config-if)#exit
Router(config)#interface se0/0
Router(config-if)#ip address 172.16.20.2 255.255.255.0
Router(config-if)#no shut
Router(config-if)#exit
Router(config)#interface se1/0
Router(config-if)#ip address 172.16.40.1 255.255.255.0
Router(config-if)#no shut
Router(config-if)#exit
Router(config)#
Router(config)#ip route 172.16.10.0 255.255.255.0 172.16.20.1
Router(config)#ip route 172.16.50.0 255.255.255.0 172.16.40.2
Router(config)#end
Router#wr

O Router 4 está pronto.
```

Router 5

```
Router> enable
Router# configure terminal
Router(config)#interface eth1/0
Router(config-if)#ip address 172.16.50.1 255.255.255.0
Router(config-if)#no shut
Router(config-if)#exit
```

```
Router(config)#interface se0/0
Router(config-if)#ip address 172.16.40.2 255.255.255.0
Router(config-if)#no shut
Router(config-if)#exit
Router(config)#
Router(config)#ip route 172.16.30.0 255.255.255.0 172.16.40.1
Router(config)#ip route 172.16.20.0 255.255.255.0 172.16.40.1
Router(config)#ip route 172.16.10.0 255.255.255.0 172.16.40.1
Router(config)#end
Router#wr

O Router 5 está pronto.
```

21

Assim terminamos a configuração do roteamento estático do cenário.

Para testar o cenário, vamos “pingar” todos com todos os dispositivos. Obtemos sucesso em todas as tentativas (como esperado). Vamos verificar as tabelas de roteamento do Router 4:

```
Router#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

172.16.0.0/24 is subnetted, 5 subnets
S 172.16.10.0 [1/0] via 172.16.20.1
C 172.16.20.0 is directly connected, Serial0/0
C 172.16.30.0 is directly connected, Ethernet2/0
C 172.16.40.0 is directly connected, Serial1/0
S 172.16.50.0 [1/0] via 172.16.40.2
Router#
```

Ao analisar as tabelas do roteamento podemos encontrar três tipos de rotas, dependendo da origem:

- Rede diretamente conectada;
- Rede remota;
- Rede inexistente.

Rede diretamente conectada
Endereço de rede cujo IP é de uma interface do próprio roteador. Caracterizada pelo “C” antes do IP da rede.

Rede remota

Endereço de rede cujo IP é de uma interface que pertence a outro roteador. Caracterizada pela letra “S” antes do IP da rede.

Rede inexistente
Quando um roteador recebe um pacote cujo endereço IP não consta de nenhuma das rotas existentes na tabela de roteamento, este pacote é descartado.

22

Conforme Filippetti (2008), algumas **premissas** são usadas para caracterizarmos as ações dos roteadores:

Regra 1: todos os roteadores tomam decisões sozinhos com base nas informações existentes na sua própria tabela de roteamento;

Regra 2: o fato de um roteador ter determinadas informações em sua tabela de roteamento, não significa que todos os roteadores tenham as mesmas informações;

Regra 3: as informações de roteamento sobre um caminho de uma rede para outra não fornecem informações de roteamento sobre o caminho inverso ou de retorno.

Vamos verificar as quatro tabelas de roteamento em conjunto, na sequência, Router 2, 3, 4 e 5:

Router 2: Gateway of last resort is not set 172.16.0.0/24 is subnetted, 5 subnets C 172.16.10.0 is directly connected, FastEthernet0/0 S 172.16.20.0 [1/0] via 172.16.10.2 S 172.16.30.0 [1/0] via 172.16.10.2 S 172.16.40.0 [1/0] via 172.16.10.2 S 172.16.50.0 [1/0] via 172.16.10.2 Router#	Router4: Gateway of last resort is not set 172.16.0.0/24 is subnetted, 5 subnets S 172.16.10.0 [1/0] via 172.16.20.1 C 172.16.20.0 is directly connected, Serial0/0 C 172.16.30.0 is directly connected, Ethernet2/0 C 172.16.40.0 is directly connected, Serial1/0 S 172.16.50.0 [1/0] via 172.16.40.2 Router#
Router 3: Gateway of last resort is not set 172.16.0.0/24 is subnetted, 5 subnets C 172.16.10.0 is directly connected, Ethernet0/0 C 172.16.20.0 is directly connected, Serial1/0 S 172.16.30.0 [1/0] via 172.16.20.2 S 172.16.40.0 [1/0] via 172.16.20.2 S 172.16.50.0 [1/0] via 172.16.20.2 Router	Router 5: Gateway of last resort is not set 172.16.0.0/24 is subnetted, 5 subnets S 172.16.10.0 [1/0] via 172.16.40.1 S 172.16.20.0 [1/0] via 172.16.40.1 S 172.16.30.0 [1/0] via 172.16.40.1 C 172.16.40.0 is directly connected, Serial0/0 C 172.16.50.0 is directly connected, Ethernet1/0 Router#

Observe que, apesar das rotas em todas as tabelas serem as mesmas, o modo como foram inseridas na tabela de roteamento difere de roteador para roteador. Algumas rotas foram configuradas estaticamente (S) enquanto outras diretamente conectadas (C). Esses conceitos são suficientes para que possamos configurar o roteamento estático.

23

3- RESUMO

Roteamentos são proporcionados pelos roteadores. Roteadores são dispositivos próprios ou computadores com uso específico. Isso porque os roteadores possuem processador, memória, ROM, RAM, memória NVRAM e Flash, as duas últimas atuando como dispositivos de armazenamento.

Os roteadores wireless, muito comuns atualmente, em sua grande parte são produzidos para o mercado SoHo (*Small office Home office*, ou seja, pequenos escritórios e escritórios domésticos) e são uma combinação de roteador com switch.

A função básica dos roteadores é direcionar pacotes com destino a redes locais e remotas, com diferentes endereços de rede e encaminhar esses pacotes entre a interface de entrada e a de saída. Roteadores não direcionam pacotes dentro de uma mesma rede ou sub-rede e, por essa razão, cada uma de suas interfaces – no mínimo duas – deve ter um “endereço válido de host” - já que se comportam como gateways da rede ou sub-rede à qual pertencem - diferentes entre si. Para executar essa tarefa eles constroem tabelas de roteamento, onde são armazenados os caminhos para que pacotes possam ser enviados a seus destinos finais.

O roteador “aprende” sobre as redes remotas por meio da comunicação com os roteadores vizinhos (roteamento dinâmico) ou por meio do administrador (roteamento estático). O roteador cria uma tabela de roteamento que descreve como encontrar tais redes remotas. Se um pacote é endereçado a uma rede cujo endereço não se encontra nessa tabela o pacote é descartado. Não há envio de mensagens de broadcast ou qualquer outro esquema utilizado para se descobrir tal rota.

24

As rotas estáticas são definidas manualmente pelo administrador de redes. Da mesma forma, somente ele pode alterá-las ou desabilitá-las. As rotas estáticas são úteis em pequenas topologias, particularmente se tivermos apenas dois roteadores com uma interface cada a conectá-los, requerendo apenas uma única rota, embora possam ser utilizadas juntamente com rotas dinâmicas ou mesmo em topologias um pouco mais complexas.

Temos duas situações:

1) na primeira situação seria um desperdício de recursos configurar um protocolo de roteamento dinâmico em uma rede de topologia tão simples como a vista anteriormente;

2) na segunda situação, manter rotas de modo estático em topologias mais complexas e que sofrem alterações com frequência seria muito trabalhoso, resultando em maior probabilidade de erros humanos.

No roteamento estático nos preocuparemos somente com as redes remotas. As redes diretamente conectadas não precisam ser configuradas, pois o roteador já as conhece e, portanto, os respectivos caminhos para chegar até as mesmas.

A sintaxe do comando é:

ip route [rede de destino] [máscara] [endereço do próximo ponto ou interface de saída] [distância administrativa] [permanente], onde:

1- **ip route**: instrução que designa rota estática;
2- **rede de destino**: endereço da rede a adicionar na tabela de roteamento;
3- **máscara**: máscara da rede de destino;
4- **endereço do próximo ponto**: endereço do ponto que receberá o pacote e o enviará à rede de destino;
5- **interface de saída**: utilizada no lugar do ip do próximo ponto. Utilizada somente para as interfaces seriais, para interfaces ethernet não funciona.
6- **distância administrativa**: o padrão é "1". Se quiser pode mudar para qualquer valor de 1 a 254. O valor 255 torna a rede inalcançável. Sempre utilizaremos o padrão (default);
7- **permanente**: caso uma interface esteja desativada ou o roteador não possa se comunicar com o próximo ponto após um determinado período de tempo a rota é automaticamente descartada da tabela de roteamento. "Permanent" mantém os dados da tabela sempre. Nós utilizaremos esse parâmetro sempre padrão (default).

UNIDADE 3 – SWITCHES, VLANS E ROTEAMENTO IP
MÓDULO 3 – ROTEAMENTO IP DINÂMICO RIPV1, RIPV2 E EIGRP (ENHANCED INTERIOR GATEWAY ROUTING PROTOCOL)

01

1 - PROTOCOLOS DE ROTEAMENTO DINÂMICO

Como vimos anteriormente, no roteamento estático as informações que um roteador precisa saber para poder encaminhar pacotes corretamente aos seus destinos são colocadas manualmente na tabela de rotas. Diferentemente, no roteamento dinâmico, os roteadores podem descobrir estas informações automaticamente e compartilhá-la com outros roteadores via **protocolos de roteamento dinâmicos**.

Um protocolo de roteamento dinâmico é uma linguagem que um roteador fala com outros roteadores a fim de compartilhar informações sobre alcançabilidade e estado das redes.

Conforme Filippetti (2008), os protocolos de roteamento dinâmico foram criados para facilitar a administração de redes cuja topologia é mais complexa, além de estar sujeita a alterações com certa frequência. Esses protocolos permitem que os roteadores troquem entre si informações sobre redes remotas (existente em outro roteador). Uma vez recebida nova informação ela é inserida na tabela do roteamento. Quando isto acontece dizemos que foi criada uma nova "entrada" na tabela de roteamento. De modo análogo, se uma rede ficar indisponível por qualquer motivo, uma rota pode ser desabilitada e ser retirada da tabela de roteamento.

Esse processo é dinâmico, ou seja, não depende da intervenção manual do administrador da rede e, por essa razão, esses protocolos são considerados protocolos de roteamento dinâmico.

Protocolos de roteamento dinâmico realizam algumas **tarefas características**, como:

a) detecção de redes remotas,

b) manutenção da tabela de roteamento,

c) escolha da melhor rota para as redes de destino e

d) localizar, quando necessário, nova rota para substituir outra que esteja inativa, momentaneamente ou definitivamente.

02

1.1 - Características dos protocolos de roteamento dinâmico

Conforme Boavida, Bernardes e Vapi, (2011), os protocolos de roteamento dinâmico podem ser comparados com base nas seguintes características:

- **Tempo de convergência;**
- **Escalabilidade;**
- **Classless (uso de VLSM) ou classful;**
- **Uso de recursos;**
- **Implantação e manutenção.**

1.2 - Operação do protocolo de roteamento do vetor de distância (distance vector)

Vetor de distância significa que as rotas são anunciadas como vetores de distância e direção. A distância é definida em termos de uma métrica como contagem de saltos.

A direção é fornecida simplesmente pela interface do roteador do próximo salto ou pela interface de saída neste roteador. Nesse caso, os roteadores não têm uma visão completa da topologia da rede.

Tempo de convergência
O tempo de convergência define a rapidez com que os roteadores da topologia de rede compartilham informações de roteamento e alcançam um estado de conhecimento consistente. Quanto mais rápida for a convergência, melhor será o protocolo. Os loops de roteamento podem ocorrer quando as tabelas de roteamento inconsistentes não são atualizadas devido a uma convergência lenta em uma rede variável.

Escalabilidade
A escalabilidade define o tamanho máximo que uma rede pode ter com base no protocolo de roteamento implantado. Quanto maior for a rede, mais escalável deverá ser o protocolo de roteamento.

Classless (uso de VLSM)
Os protocolos de roteamento classless incluem a máscara de sub-rede com o endereço de rede nas atualizações de roteamento. As redes atuais não são mais alocadas com base em classes e a máscara de sub-rede não pode ser determinada pelo valor do primeiro octeto. Os protocolos de roteamento classless são obrigatórios na maioria das redes atuais porque suportam VLSM, redes não contíguas e outros recursos que serão discutidos em capítulos posteriores.

Classfull
Os protocolos de roteamento classful não enviam informações sobre a máscara de sub-rede nas atualizações de roteamento. Os primeiros protocolos de roteamento, como o RIPv1, eram classful. Isso ocorria em uma época em que os endereços de rede eram alocados com base em classes: classe A, B ou C. O protocolo de roteamento não precisava incluir a máscara de sub-rede na atualização de roteamento porque a máscara de rede podia ser determinada com base no primeiro octeto do endereço de rede. Os protocolos de roteamento classful podem ser usados em algumas das redes atuais. No entanto, eles não incluem a máscara de sub-rede em suas tabelas e não podem ser usados em todas as situações. Os protocolos de roteamento classful não podem ser usados quando uma rede é colocada em sub-rede usando mais de uma máscara de sub-rede. Em outras palavras, os protocolos de roteamento classful não suportam VLSM e redes não contíguas.

Uso de recursos
O uso de recursos inclui os requisitos de um protocolo de roteamento como espaço de memória, utilização de CPU e utilização de largura de banda de link. Os requisitos de recursos mais altos precisam de hardware mais avançado para suportar a operação do protocolo de roteamento, além dos processos de encaminhamento de pacotes.

Implantação e manutenção
Implantação e manutenção descreve o nível de conhecimento necessário para que um administrador

de rede implante e mantenha a rede com base no protocolo de roteamento implantado.

03

1.3- Balanceamento de carga

Segundo Filippetti (2008), é possível que um roteador tenha “aprendido” (manualmente ou automaticamente) e mostre em sua tabela de roteamento mais de uma rota para o mesmo destino. Isto quer dizer que um roteador mostrará em sua tabela de roteamento uma única rede de destino, mas com mais de uma interface de saída, sendo uma para cada rota. Observe que isso pode ocorrer para diversas rotas, mas vamos analisar uma rede de destino apenas para compreendermos o processo.

Para tomar a decisão sobre qual a melhor rota para um destino específico, o roteador irá considerar as métricas de cada protocolo que originará a rota, escolhendo a métrica de menor custo, podendo, desde que configurado, realizar o balanceamento de carga de mesmo custo.

Esse processo é comum para redes locais. Também é possível realizar o balanceamento de carga de custos diferentes e, neste caso poderá ser configurado um balanceamento de carga de custo desigual, o que ocorre normalmente em redes WAN.

04

1.4- Convergência de redes

Segundo o CCNA – Cisco Certified Network Associate-Study Guide, o termo convergência de redes é empregado quando temos uma rede cujos roteadores têm suas tabelas consistentes, umas com as outras. Isso significa que todos os roteadores terão informações completas e precisas sobre a rede, sendo que uma rede é considerada completamente operante quando a convergência ocorre.

Os protocolos de roteamento apresentam como característica um tempo maior ou menor para promover a convergência da rede, ou seja, supondo que todos os equipamentos estejam desligados e sejam ligados para que carreguem suas configurações (sistema operacional), estes passam a trocar mensagens de atualização.

O tempo de convergência é o tempo para que os roteadores desta rede tenham suas tabelas consistentes.

O OSPF, por exemplo, promove a convergência mais rapidamente que o RIP, mas este assunto será tratado oportunamente.

05

2- ROTEAMENTO DINÂMICO RIPV1

Segundo o CCNA – Cisco Certified Network Associate-Study Guide, o RIP é um protocolo de roteamento classificado como **vetor de distância** (*distance vector*). Atualmente ele possui duas versões que trabalham com o IPv4. Nesta seção trataremos acerca da versão 1.

No roteamento dinâmico, temos as seguintes **vantagens** e **desvantagens**:

Vantagens	Desvantagens
•simplificar o gerenciamento da rede; •viabilizar a gestão de redes de grande porte.	•utilizar largura de banda nos links entre roteadores, coisa que o estático não faz; •requerer mais processamento pela CPU do roteador; •ter menor controle da internetwork.

O protocolo de roteamento dinâmico utiliza um modo automático para encontrar e atualizar as tabelas de roteamento. É mais simples que o roteamento estático, porém há o preço a pagar conforme citado nas desvantagens da utilização do mesmo.

Os protocolos a serem estudados são do tipo **IGP** (Interior Gateway Protocol), que trocam informações entre roteadores pertencentes a um mesmo **AS** (Autonomous System), que é uma coleção de redes sob um mesmo domínio administrativo.

06

Os **princípios** do protocolo RIP são os seguintes:

1- envia tabela de roteamento completa para todas as interfaces a cada 30 segundos;
2- utiliza a contagem de hops como métrica;
3- limita a contagem máxima de hops a 15, limitando o tamanho da rede. Os 15 saltos são consecutivos, em linha. Uma rede com mais de 15 roteadores pode utilizar o RIP desde que os mesmos não estejam na mesma linha (sequência).

A versão 1 do RIP é limitada em comparação com as redes atuais, na sua época de lançamento supria todas as necessidades. Ele se caracteriza por:

1) ser classfull;

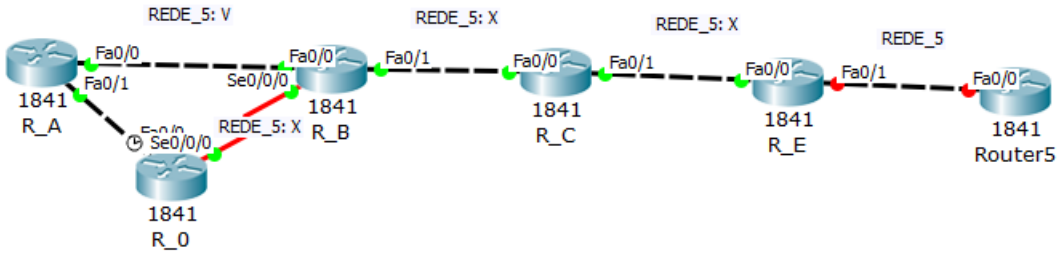
2) ter limite de 15 saltos e

3) utilizar pacotes broadcast.

Ele utiliza apenas a contagem de saltos (***hop count***) para determinar qual a melhor rota para uma rede remota. Ele pode balancear carga para até seis link de mesmo custo por meio do *round-robin load* balance.

07

Para nosso estudo, considere a figura a seguir.



Exemplo de um loop de Roteamento

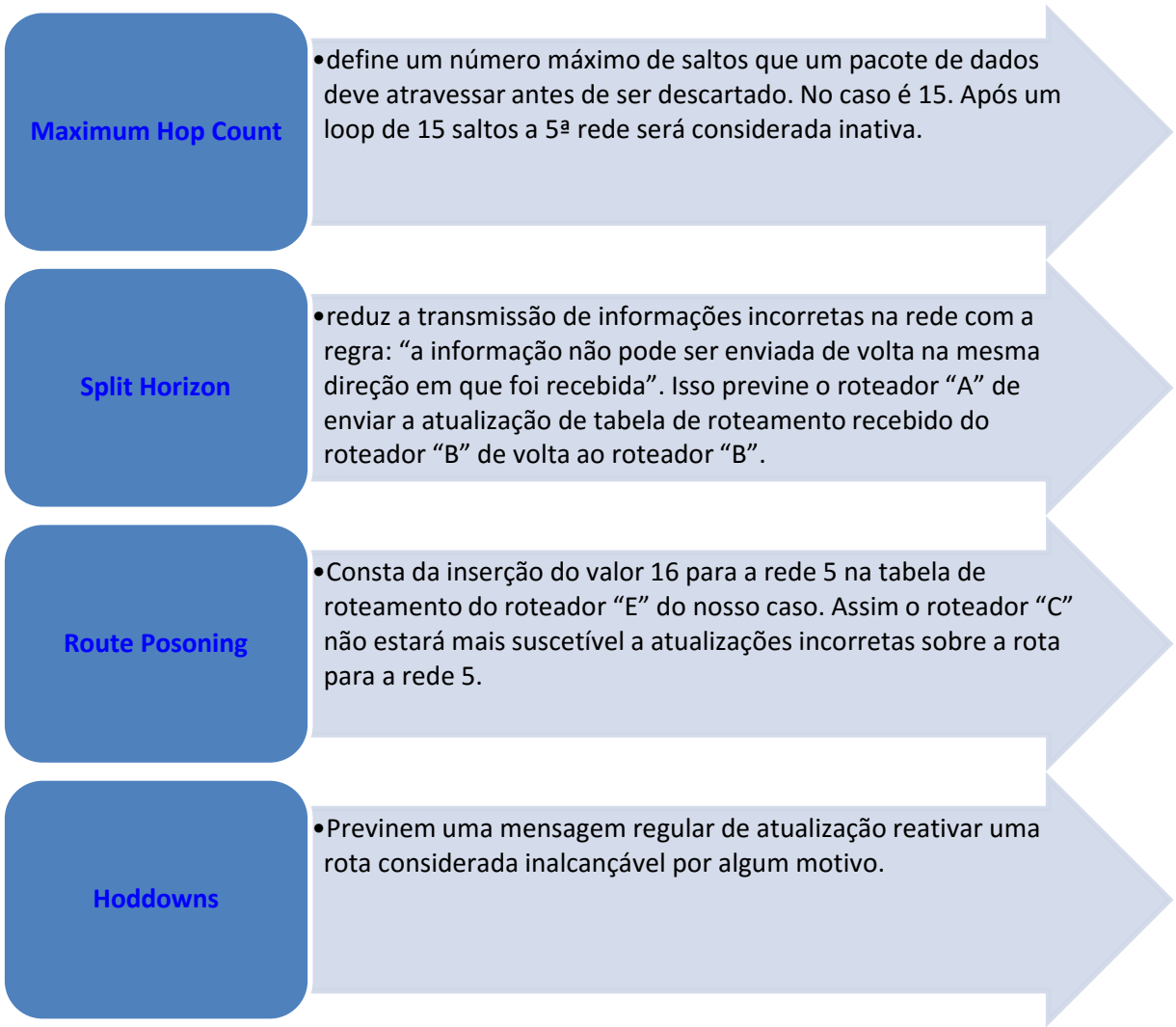
Fonte: O Autor, 2015

O RIP, sendo um protocolo distance vector, mantém registros de todas as mudanças ocorridas na rede através do broadcast periódico de atualizações de tabelas de roteamento para todas as interfaces ativas.

Na figura acima, por alguma razão, a interface para a rede 5 falha. Todos os roteadores sabem da rede 5 pelo roteador “E”. O roteador “A”, em suas tabelas, possui as rotas para a rede 5 por meio dos roteadores “B”, “C” e “E”. Quando a rede 5 falha, o roteador “E” avisa o roteador “C”. Isso faz com que o “C” pare de rotear pacotes para a rede 5 por meio do “E”. Porém os roteadores “A”, “B” e “D” ainda não sabem sobre a situação da rede 5, portanto, continuam enviando suas tabelas para atualização. Em consequência, há formação de um loop do pacote.

08

Para evitar essa questão, o RIP tem **mecanismos** que minimizam a ocorrência de loops de pacotes entre os roteadores quando estes não são atualizados simultaneamente. São eles:



09

3- ROTEAMENTO DINÂMICO RIPV2

Ainda, segundo o CCNA – Cisco Certified Network Associate-Study Guide, a versão 2 do RIP corrige algumas limitações da versão 1. Esta versão não é muito diferente da anterior. Continua sendo estritamente distance vector e segue utilizando a contagem de saltos como métrica. Essa versão continua enviando a tabela completa de roteamento periodicamente. A distância administrativa continua 120.

Vejamos as diferenças entre as versões:

	RIPv1	RIPv2
Tipo	Distance-Vector	Distance-Vector
Métrica	Nº Saltos (<=15)	Nº Saltos (<=15)
Anúncios	Classfull	Classless
VLSM	Não	Sim
Redes Descontínuas	Não	Sim
Autenticação	Não	Sim
Propagação	30 seg	30 seg
Tipo Propagação	broadcast	multicast
CIDR	Não	Sim
RFC	1058 E STD 58	1723
Dist Adm	120	120
Rotas por Pacote	25	25
Sumarização Auto	Sim	Sim
Sumarização Manual	Não	Sim
Convergência	Lenta	Rápida
Suporte Autenticação	Não	Sim

10

3.1- Configurações do RIPv1 ou RIPv2

```
rot(config)# router rip

r(config-r)# version 1 (version 2)

rot(config-rot)# network 172.16.0.0

...... todas diretamente conectadas ......

rot(config-rot)# passive-interface se0/0
```

```
rot(config)# ctr+z
```

Para se verificar as configurações do RIPv1 ou RIPv2 faça:

`# show ip route` (mostra toda a tabela de roteamento).

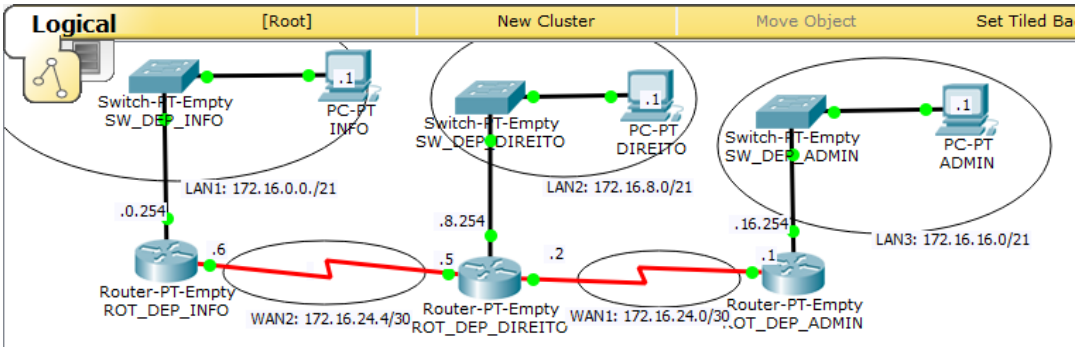
`# show ip route rip` (apresenta somente as rotas descobertas pelo RIP).

`# show ip rip database` (apresenta o conteúdo da base de dados privativa do RIP).

11

4- Roteamento dinâmico EIGRP - Enhanced Interior Gateway Routing Protocol

Seja o cenário da figura abaixo:



Cenário do Estudo de Caso
Fonte: O Autor, 2015

Partimos do princípio de que o cenário da figura satisfaça os requisitos abaixo listados.

a) a rede se encontra com o endereçamento IP realizado. Com os IPs dos terminais dos roteadores atribuídos.

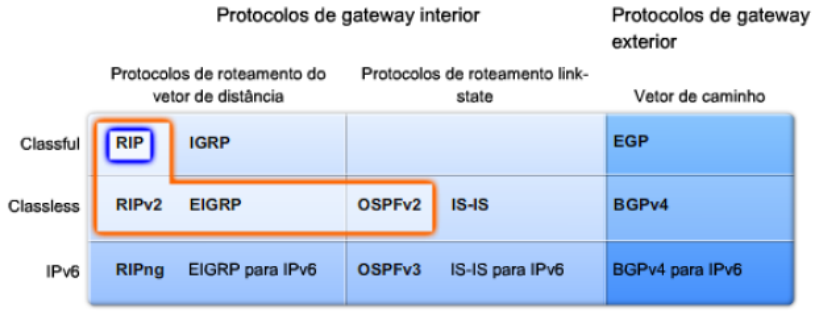
b) todos os roteadores com velocidade dos links de 2Megabps.

c) teste de "ping" de todos os vizinhos para todos os vizinhos esteja funcionando.

12

4.1- Informações gerais sobre o roteamento dinâmico EIGRP

Segundo a Cisco Network Academy:
1 - É um protocolo de roteamento do tipo Vetor Distância (Distance Vector) melhorado.



Mapas dos protocolocos RIP, EIGRP e OSPF
Fonte: Cisco Networking Academy, 2005.

a) Foi lançado em 1992 por meio do IPS 9.21.

b) Utiliza o algoritmo de atualização por difusão (DUAL - Diffuding Update Algorithm).

c) Não expira as entradas de roteamento nem utiliza atualizações periódicas.

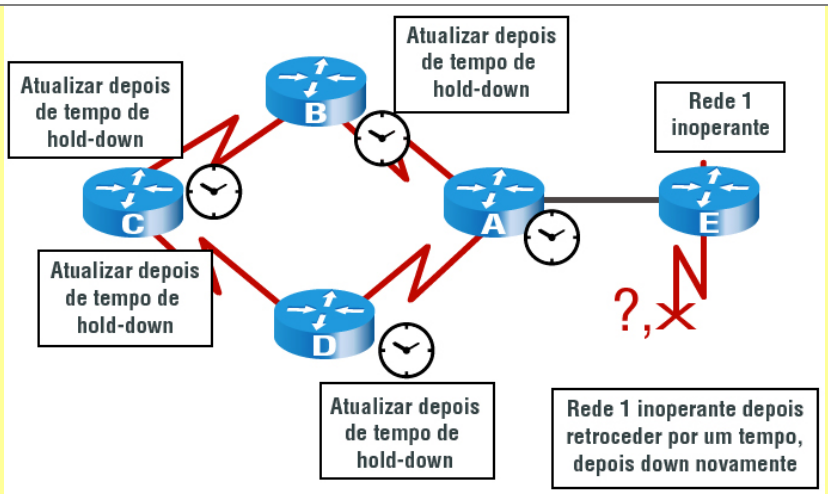
d) Mantém a tabela de roteamento, que inclui o melhor caminho e qualquer outro caminho de backup sem loop, separada da tabela de topologia.

e) A convergência é mais rápida devido à ausência de temporizadores holddown e um sistema de cálculo de rota coordenado.

Sem loop
Sem loop significa que o vizinho não possui uma rota até a rede dedestino que atravesse este roteador.

Temporizadores Holddown

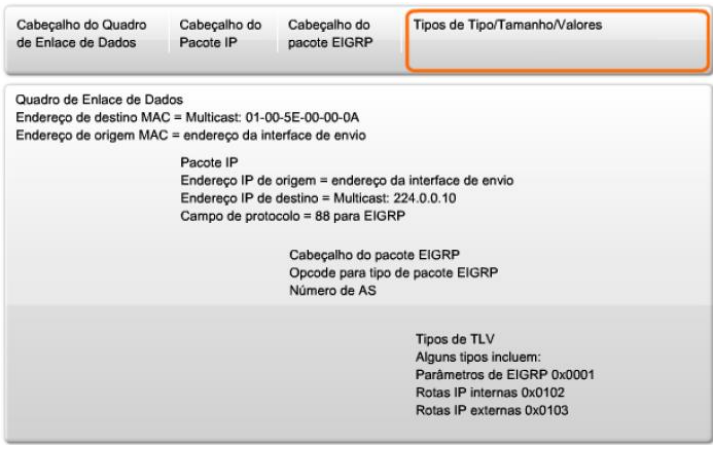
Você pode evitar um problema de contagem até o infinito usando temporizadores holddown, que funcionam da seguinte forma:



1) Quando um roteador recebe uma atualização de um vizinho, indicando que uma rede anteriormente acessível agora está inacessível, o roteador marca a rota como inacessível e inicia um temporizador holddown. Se, a qualquer momento antes do temporizador holddown expirar, uma atualização for recebida do mesmo vizinho indicando que a rede está novamente acessível, o roteador marca a rede como acessível e remove o temporizador holddown.
2) Se chegar uma atualização de um roteador vizinho diferente, com uma métrica melhor que a registrada originalmente na rede, o roteador marca a rede como acessível e remove o temporizador holddown.
3) Se, a qualquer momento antes do temporizador holddown expirar, uma atualização for recebida de um roteador vizinho diferente com uma métrica pior, a atualização será ignorada. Ignorar uma atualização com uma métrica pior quando um temporizador holddown está ativado concede mais tempo para que o conhecimento de uma alteração que cause perturbações seja propagado através de toda a rede.

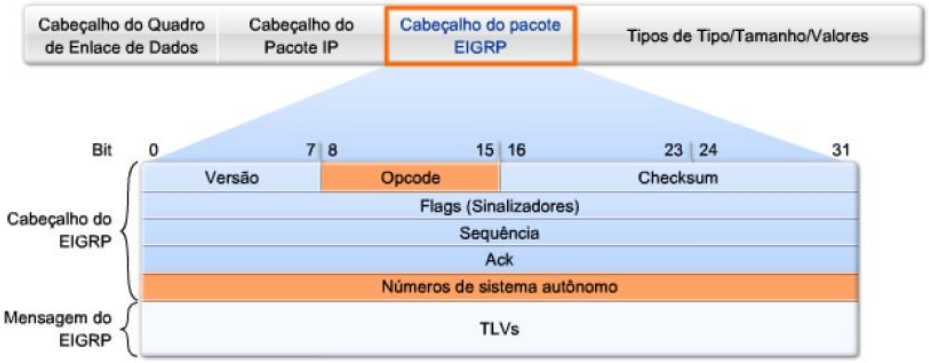
13

A mensagem EIGRP é encapsulada conforme a figura a seguir.



Encapsulamento EIGRP
Fonte: Cisco Networking Academy, 2005.

Toda mensagem do EIGRP inclui o cabeçalho. Os campos importantes que nos interessam são o campo "**opcode**" e o campo "**números de sistema autônomo**".



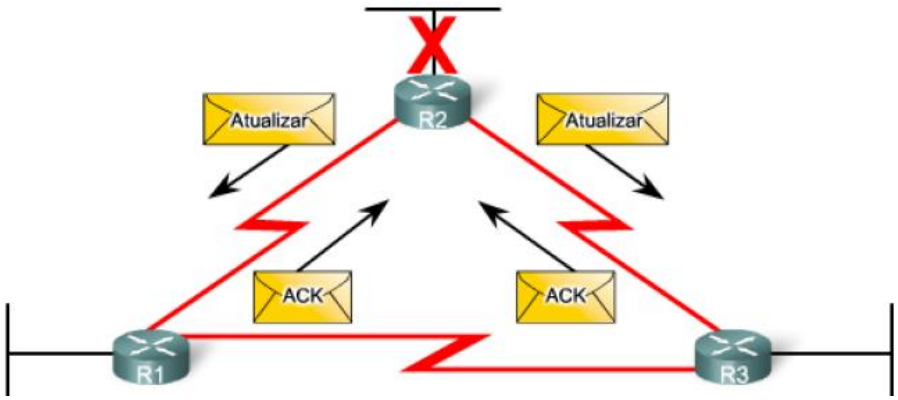
}**Encapsulamento EIGRP**

Fonte: Cisco Networking Academy, 2005.

14

O **opcode** especifica o tipo de pacote EIGRP:

Atualização: código 1. São pacotes utilizados para propagar informações de roteamento depois de uma alteração no pacote de confirmação (ACK). É enviado automaticamente quando o RTP (veja mais abaixo) confiável é utilizado.

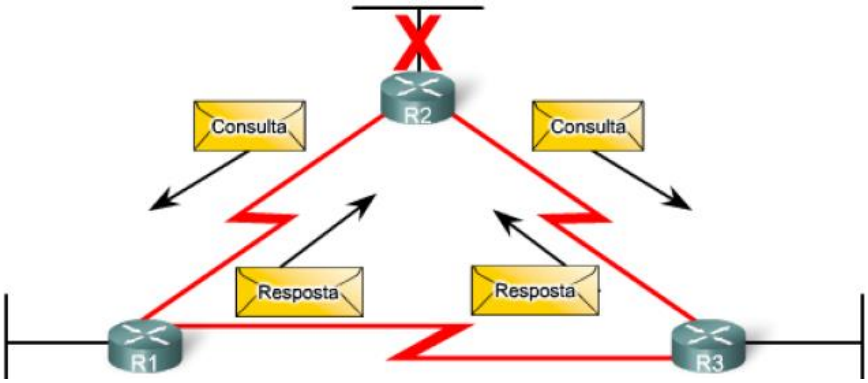


Pacotes de Atualização

Fonte: Cisco Networking Academy, 2005.

Consulta: código 3. É utilizado pelo DUAL ao procurar redes.

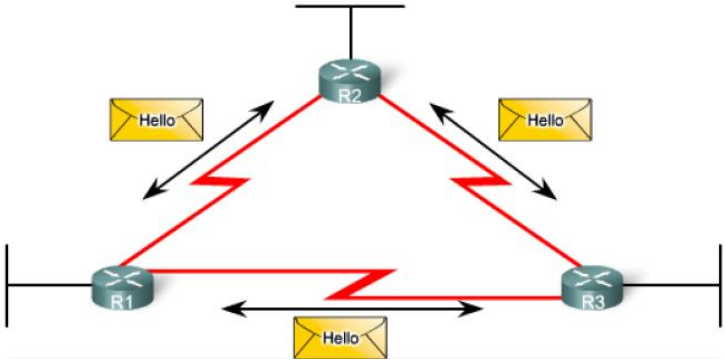
Resposta: código 4. É enviado automaticamente em resposta ao pacote de consulta.



Pacotes de Resposta

Fonte: Cisco Networking Academy, 2005.

Hello: código 5. São pacotes utilizados para detectar vizinhos e formar adjacências. Utiliza processo não confiável, portanto, nenhuma resposta é exigida do destino.



Pacotes Hello

Fonte: Cisco Networking Academy, 2005.

15

Intervalos de tempo do pacote "hello" e tempo de espera padrão do EIGRP: Irá depender da largura de banda utilizada.

- Se BW <= 1,544Mbps, link=multiponto ou Frame Relay então o intervalo de tempo hello padrão = 60 seg e o intervalo de tempo de espera padrão = 180 seg.
- Se BW > 1,544Mbps, link=Ethernet então o intervalo de tempo hello padrão = 5 seg e o intervalo de tempo de espera padrão = 15 seg.

OBS.: verifique que o tempo do intervalo hello padrão é 1/3 do de tempo de espera padrão em ambos os casos.

As atualizações do EIGRP podem ser parciais ou associadas:

Parciais	Associadas
•quando a atualização inclui somente informações sobre as alterações de rota.	•quando somente os roteadores afetados pela mudança receberão a atualização.

Frame relay
É um protocolo público de redes de longa distância. Funciona por chaveamento de pacotes que provê conectividade entre redes locais. Seu nome decorre do controle de quadros pela rede entre dois sites (ponto a ponto). Era originalmente parte de um padrão chamado de ISDN, que em tradução literal significa Rede Digital de Serviços Integrados. Será tratado por nós futuramente.

16

O campo parâmetros TLV (Tipo/Tamanho/Valor) inclui os pesos que o EIGRP utiliza para sua métrica composta. Por padrão, somente a largura de banda e o atraso são igualmente considerados, com k1=1 (largura de banda) e k3=1 (atraso), os demais valores são definidos como "0".

Mensagem EIGRP encapsulada
Fonte: Cisco Networking Academy, 2005.

Na figura acima os pesos k1 e k3 são, por padrão, definidos como iguais a “1”. O tempo de espera é o tempo máximo que o roteador deve esperar para o próximo “hello”.

No campo "Cabeçalho do Pacote IP" ficam as informações utilizadas para anunciar as rotas do eigrp dentro de um AS (Sistema Autônomo). Os campos que importam agora são: campos da métrica (largura de banda e atraso), campo de máscara de sub-rede (tamanho do prefixo que especifica o número de bits de rede na máscara de sub-rede) e o campo destino (endereço de destino da rota).

17

A largura de banda considerada é a **mais baixa largura de banda configurada** de qualquer interface ao longo da rota.

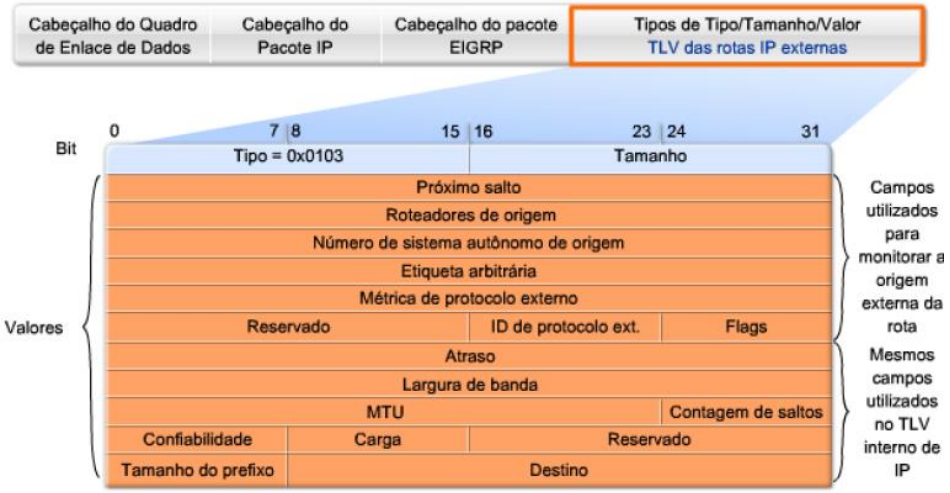
Mensagem EIGRP encapsulada
Fonte: Cisco Networking Academy, 2005.

O atraso é calculado como a soma de atrasos da origem para o destino em unidades de 10 microssegundos. Uma rota identificada por 0xFFFFFFFF é considerada inalcancável.

A mensagem de IP Externo é utilizada quando rotas externas são importadas para o processo de roteamento EIGRP.

18

No nosso caso, sempre importaremos ou redistribuiremos uma rota estática padrão para o EIGRP (veremos esse assunto oportunamente). O campo TLV de IP Externo inclui todos os campos utilizados pelo TVL de IP Interno.



Mensagem EIGRP encapsulada
Fonte: Cisco Networking Academy, 2005.

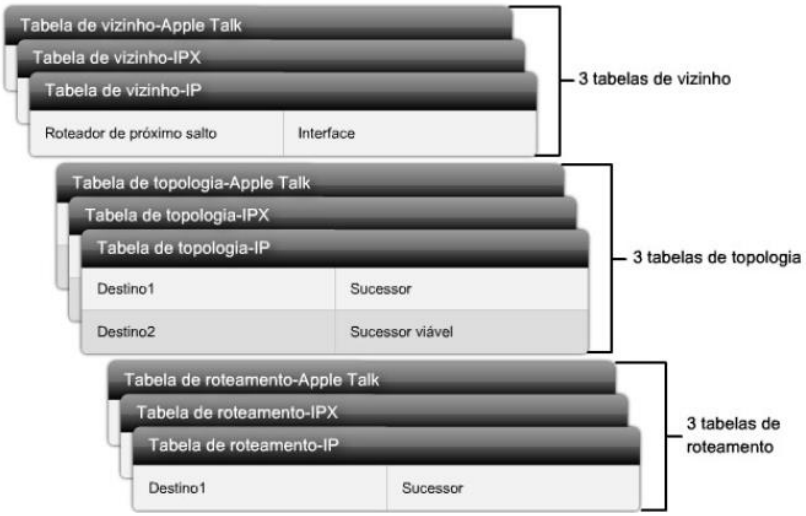
2 - O roteamento dinâmico EIGRP é considerado um híbrido (proprietário da Cisco) por ser uma versão melhorada do protocolo de roteamento vetor de distância da CISCO, o IGRP.

19

4.2- Características do roteamento dinâmico EIGRP

Ainda segundo a Cisco Network Academy:

4.2.1 - Fornece suporte a protocolos tais como o IP, IPX (novell) e Apple Talk, por meio dos módulos dependentes do protocolo (PDM- Protocol Dependent Modules). Os PDMs são responsáveis pelas tarefas de roteamento específicas para cada protocolo da camada de rede.



PDM do EIGRP

Fonte: Cisco Networking Academy, 2005.

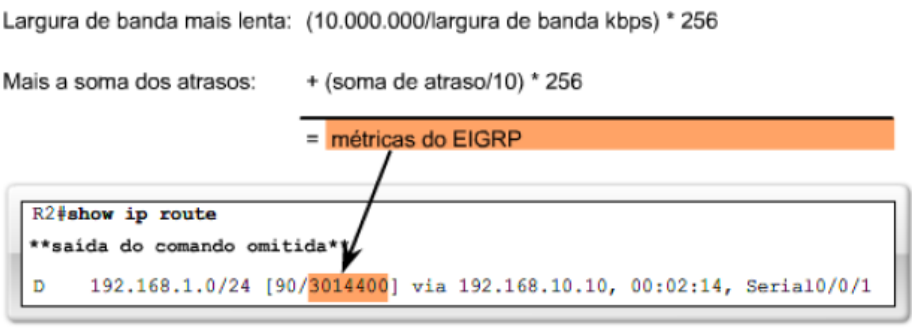
4.2.2 - A comunicação é feita via o protocolo Reliable Transport Protocol (RTP). É o protocolo utilizado pelo eigrp para a entrega e recebimento dos pacotes eigrp. Ele é independente da camada de rede, portanto não utiliza os serviços de UDP ou TCP porque o IPX (novell) e AppleTalk (Apple) não utilizam protocolos da pilha TCP/IP. Ele não utiliza a camada de redes do modelo OSI/TCP-IP. O RTP inclui entrega confiável e entrega não confiável de pacotes eigrp, semelhante ao TCP e ao UDP. Ele também envia pacotes unicast ou multcast. Os pacotes multcast do eigrp utilzam o endereço de multcast reservado 224.0.0.10 (lembra que o RIP utilizava o 224.0.0.1?).

20

4.2.3 - EIGRP não depende de protocolos roteados para funcionar.

4.2.4 - A métrica é obtida pela computação de cinco parâmetros: k1, k2, k3, k4 e k5 (Boa Leitura Do Ricardo Meira = Bandwidth, Load, Delay, Riability e MTU-Maximum Transmition Unit). Simplificadamente a métrica é obtida, por padrão, pela soma Bandwidth+delay.

4.2.5 - A largura de banda é calculada como: (10Megabits*256)/BW. É a velocidade do link mais lento do caminho até o destino.



Cálculo da métrica padrão do EIGRP.
Fonte: Cisco Networking Academy, 2005.

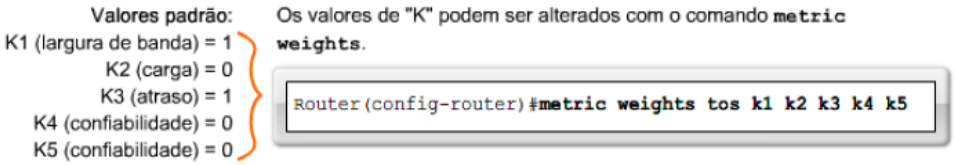
4.2.6 - O atraso (Delay) é medido em múltiplos de 10 microsegundos, com total de (soma dos atrasos/10)*256. É a soma dos atrasos de cada link do caminho até o destino.

4.2.7 - O caminho com menor valor é o escolhido para a tabela de roteamento.

4.2.8 - Esses parâmetros são observados nas interfaces por meio do comando "show interfaces".

21

4.2.9 - Para alterar os valores dos "ks" utilize o comando: "metric weights tos k1 k2 k3 k4 k5" dentro do ambiente de configuração do protocolo EIGRP.



Alterando os parâmetros da métrica padrão do EIGRP
Fonte: Cisco Networking Academy, 2005

A fórmula composta completa é:

Métrica={k1*BW+[(k2*BW)/(256-Load)]+k3*Delay}*[k5/(Reability+k4)]

Onde:

Se Kn=1, então é utilizado, senão kn=0.

Mneumônico para gravar de vez os cinco parâmetros: Boa Leitura Do Ricardo Meira (Bandwidth, Load, Delay, Riability, MTU)

Métrica Padrão = (k1*BW+k3*D)*256.

Se k1=1 e k3=1 então

Métrica Padrão = BW+D

22

Exemplo de cálculo de métrica eigrp considerando dois roteadores genéricos R2 e R3:

```
R2#show inter ser 0/0/1
Serial0/0/1 is up, line protocol is up
  Hardware is PowerQUICC Serial
  Internet address is 192.168.10.9/30
  MTU 1500 bytes, BW 1024 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set
***saída do comando omitida***

R3#show inter fa 0/0
FastEthernet0/0 is up, line protocol is up
  Hardware is AmdFE, address is 0002.b9ee.5ee0 (bia 0002.b9ee.5ee0)
  Internet address is 192.168.1.1/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
***saída do comando omitida***
```

Exemplo de cálculo da métrica padrão do EIGRP.

Fonte: Cisco Networking Academy, 2005

Da tabela anterior temos:

BW=(10.000.000/1024)*256=2.499.840

Delay = [(20.000/10)+(100/10)]*256= 514.560

23

Consultando a tabela de roteamento, temos na figura abaixo:

```
R2#show ip route
***saída do comando omitida***

Gateway of last resort is not set

     192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
D       192.168.10.0/24 is a summary, 00:00:15, Null0
D       192.168.10.4/30 [90/21024000] via 192.168.10.10, 00:00:15, Serial0/0/1
C       192.168.10.8/30 is directly connected, Serial0/0/1
     172.16.0.0/16 is variably subnetted, 4 subnets, 3 masks
D       172.16.0.0/16 is a summary, 00:00:15, Null0
D       172.16.1.0/24 [90/40514560] via 172.16.3.1, 00:00:15, Serial0/0/0
C       172.16.2.0/24 is directly connected, FastEthernet0/0
C       172.16.3.0/30 is directly connected, Serial0/0/0
     10.0.0.0/30 is subnetted, 1 subnets
C       10.1.1.0 is directly connected, Loopback1
D    192.168.1.0/24 [90/3014400] via 192.168.10.10, 00:00:15, Serial0/0/1
```

Tabela de roteamento padrão do EIGRP.

Fonte: Cisco Networking Academy, 2005

Métrica do EIGRP = BW+Delay = 2.499.840+514.560=3.014.400, tal como consta na tabela acima.

Por padrão, o EIGRP utiliza até 50 por cento da largura de banda de uma interface para informações de EIGRP. Isto impede que o processo do EIGRP utilize um link em excesso e que não libere largura de banda suficiente para o roteamento de tráfego normal. O comando ip bandwidth-percent eigrp pode ser utilizado para configurar o percentual de largura de banda que pode ser utilizado por EIGRP em uma interface, por exemplo:

```
R1(config)#interface serial 0/0/0
R1(config-if)#bandwidth 64
R1(config-if)#ip bandwidth-percent eigrp 1 50
```

Tabela de roteamento padrão do EIGRP.
Fonte: Cisco Networking Academy, 2005

24

Os intervalos Hello e os tempos de espera são configuráveis por interface e não precisam corresponder com outros roteadores de EIGRP para estabelecer adjacências.

```
R1(config)#int s0/0/0
R1(config-if)#ip hello-interval eigrp 1 60
R1(config-if)#ip hold-time eigrp 1 180
R1(config-if)#end

R2(config)#int s0/0/0
R2(config-if)#ip hello-interval eigrp 1 60
R2(config-if)#ip hold-time eigrp 1 180
R2(config-if)#end
```

Ajuste dos tempos “hello” e “hold-time” do EIGRP.
Fonte: Cisco Networking Academy, 2005

25

4.2.10 - As escolhas da melhor métrica e do melhor caminho são feitas por meio do DUAL (Diffusion Update Algorithm). Os conceitos envolvidos do DUAL são:

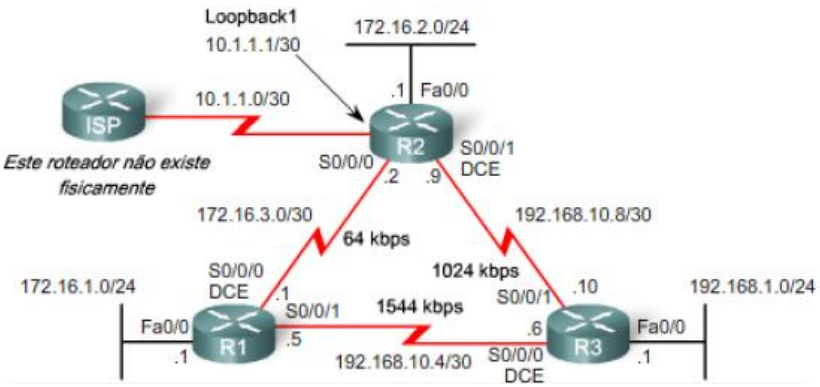
a) Feasible Distance (FD);

b) Reported Distance (RD);

c) Sucessor Route (SR);

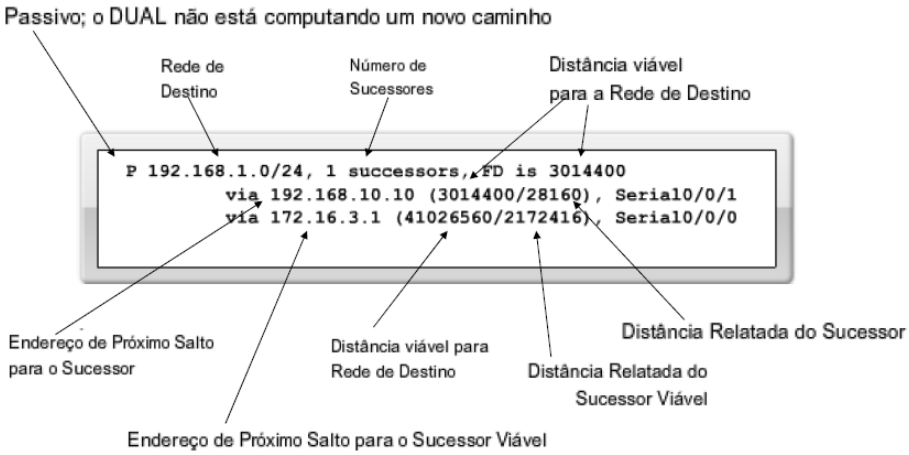
d) Feasible Sucessor (FS);

e) Feasible Condition (FC);



Ajuste dos tempos "hello" e "hold-time" do EIGRP.

Fonte: Cisco Networking Academy, 2005



Rotas para a rede 192.168.1.0/24.

Fonte: Cisco Networking Academy, 2005.

O DUAL mantém uma lista de rotas de backup determinadas como sem loop. Se a rota primária na tabela de roteamento falhar, a melhor rota de backup será adicionada imediatamente à tabela de roteamento.

Sucessor (roteador vizinho)

D 192.168.1.0/24 [90/**3014400**] via **192.168.10.10**, 00:00:31, Serial0/0/1

Distância viável (FD, Feasible distance) → é a métrica calculada mais baixa

Sucessor e Distância Viável para a rede 192.168.1.0/24.

Fonte: Cisco Networking Academy, 2005.

a) Feasible Distance (FD)
Distância até uma rede que é igual a métrica do vizinho até a rede + métrica até o vizinho, ou seja, FD = métrica do vizinho + métrica até o vizinho

b) Reported Distance (RD)
Distância anunciada por um roteador vizinho até um destino. Deve obedecer à regra RD < FD. Se RD > FD ocorre um loop de roteamento.

c) Sucessor Route (SR)
Rota ou caminho principal para um destino.

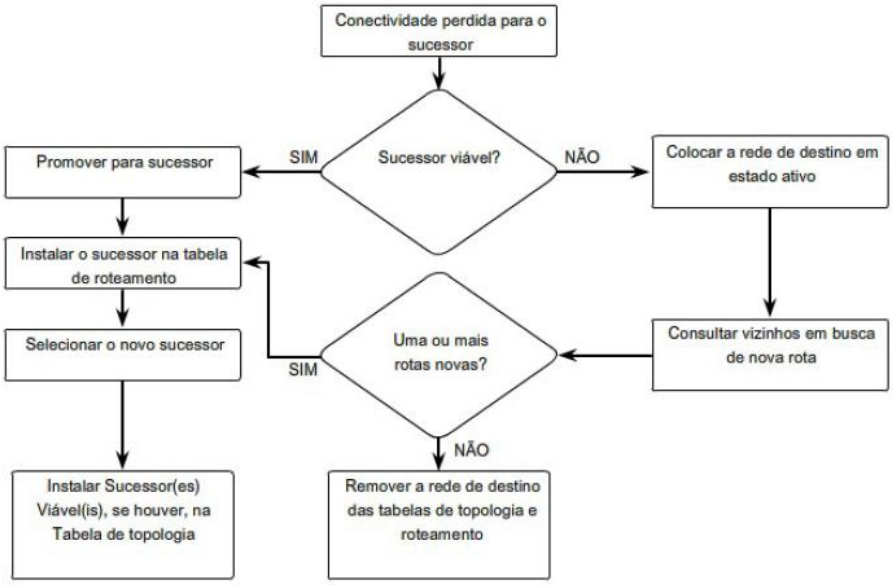
d) Feasible Sucessor (FS)
Possível rota ou caminho alternativo para um destino. É um vizinho que tem um caminho e backup sem loop para a mesma rede que o sucessor porque atende a condição de viabilidade (FC).

e) Feasible Condition (FC)
Ocorre quando um vizinho reporta uma RD menor que a FD (quando RD < FD), ou seja, quando a distância reportada para uma rede é menor que a distância viável do roteador para a mesma rede de destino.

26

4.2.11 - É um protocolo classless que suporta VLSM e CIRD

Máquina de Estado Finito do DUAL (FSM):



Fluxograma da FSM - Máquina de Estado Finito do DUAL.
Fonte: Cisco Networking Academy, 2005.

```
R2#debug eigrp fsm
EIGRP FSM Events/Actions debugging is on
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#int s0/0/1
R2(config-if)#shutdown
 ***saída do comando omitida***

DUAL: Find FS for dest 192.168.1.0/24. FD is 3014400, RD is 3014400
DUAL: 192.168.10.10 metric 4294967295/4294967295
DUAL: 172.16.3.1 metric 41026560/2172416 found Dmin is 41026560
DUAL: Removing dest 192.168.1.0/24, nexthop 192.168.10.10
DUAL: RT installed 192.168.1.0/24 via 172.16.3.1

R2(config-if)#end
R2#undebug all
All possible debugging has been turned off
```

Relatório da FSM do DUAL.
Fonte: Cisco Networking Academy, 2005.

27

4.2.12 - A Distância Administrativa (AD) é igual a 90.

4.2.13 - Permite a autenticação (assim como o OSPF) para troca de informações de roteamento. Também permite que os pacotes trafeguem criptografados.

4.2.14 - O EIGRP mantém 3 tabelas em sua base de dados:

a) Tabela de vizinhança: informações de todos os vizinhos conectados ao roteador.
b) Tabela de topologia: informações detalhadas da visão geral da rede e informações sobre a RD.
c) Tabela de informações gerais: contém as informações de todas as DF e as SR da rede.

4.2.15 - Para habilitar o EIGRP utilize o comando: router eigrp AS, onde AS é um número do intervalo 1 até 65.535. Embora o IOS Cisco referencie o parâmetro router eigrp como um "número de sistema autônomo", este parâmetro configura um processo do eigrp - uma instância de eigrp executada no roteador e não tem a ver com as configurações de AS em roteadores de ISP.

28

4.2.16 - Parâmetros de configuração: `network, passive-interface e auto-summary.`

A configuração básica é:

`#router eigrp 10`

`#network 172.16.0.0` (se rede classfull)

`#network 192.168.10.8 0.0.0.3` (se rede classless. A máscara 0.0.0.3 filtra as redes que devem ser divulgadas. Conhecida como **máscara coringa,** que é o complemento da máscara de rede).

`#auto-summary`

Neste exemplo:

a) o comando network em eigrp possui a mesma função que em outros protocolos de roteamento dinâmicos IGP.

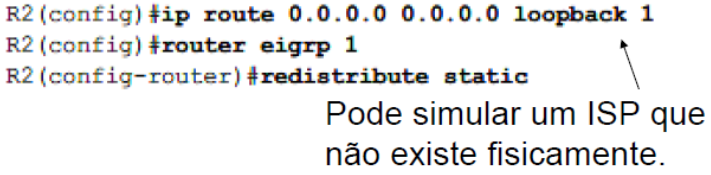
b) qualquer interface neste roteador que corresponda ao endereço de rede no comando network será habilitada para enviar e receber atualizações de eigrp.

c) esta rede e ou sub-rede serão incluídas nas atualizações de roteamento EIGRP.

29

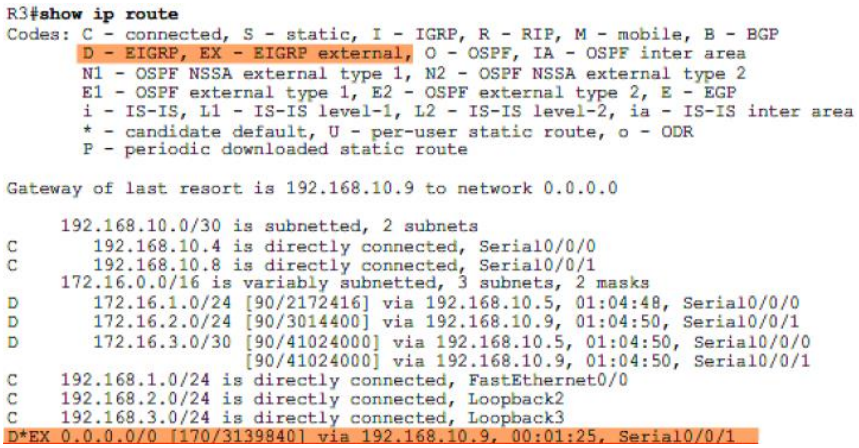
O EIGRP instala uma rota de sumarização "Null0" para cada rota primária. São descartados os pacotes que correspondem à rota de sumarização "Null0". Os anúncios de sumarização são feitos por interface, por exemplo: (config-if)# ip summary-address eigrp as-number network-address subnet-mask.

Rota padrão EIGRP:



Rota padrão do EIGRP.

Fonte: Cisco Networking Academy, 2005.



Rota padrão do EIGRP.

Fonte: Cisco Networking Academy, 2005.

d) cálculo da máscara coringa (é uma simples subtração da máscara da rede):
255.255.255.255 - 25.255.255.252 = 0.0.0.3

30

4.2.17 - Para testar a configuração faça:

a) **`show ip route`** (mostra a tabela de roteamento completa)

b) **`show ip eigrp route`** (mostra a tabela de roteamento montada pelo protocolo)

```
R3#show ip route
***saída do comando omitida***
Gateway of last resort is not set

     192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
D       192.168.10.0/24 is a summary, 00:03:11, Null0
C       192.168.10.4/30 is directly connected, Serial0/0/0
C       192.168.10.8/30 is directly connected, Serial0/0/1
D    172.16.0.0/16 [90/2172416] via 192.168.10.5, 00:03:23, Serial0/0/0
                   [90/2172416] via 192.168.10.9, 00:03:23, Serial0/0/1
C    192.168.1.0/24 is directly connected, FastEthernet0/0
```

Tabela de roteamento do EIGRP.

Fonte: Cisco Networking Academy, 2005.

Isto ocorre porque essas rotas são utilizadas apenas como anúncio. Não representam redes reais.

```
R2#show ip route
Gateway of last resort is not set

     192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
D       192.168.10.0/24 is a summary, 00:04:13, Null0
D       192.168.10.4/30 [90/2681856] via 192.168.10.10, 00:03:05, Serial0/0/1
C       192.168.10.8/30 is directly connected, Serial0/0/1
     172.16.0.0/16 is variably subnetted, 4 subnets, 3 masks
D       172.16.0.0/16 is a summary, 00:04:07, Null0
D       172.16.1.0/24 [90/2172416] via 172.16.3.1, 00:11:11, Serial0/0/0
C       172.16.2.0/24 is directly connected, FastEthernet0/0
C       172.16.3.0/30 is directly connected, Serial0/0/0
     10.0.0.0/30 is subnetted, 1 subnets
C       10.1.1.0 is directly connected, Loopback1
D    192.168.1.0/24 [90/2172416] via 192.168.10.10, 00:02:54, Serial0/0/1
```

Rota de Sumarização Null0 do EIGRP.

Fonte: Cisco Networking Academy, 2005.

31

c) **`show ip protocols`** (mostra as informações do protocolo utilizado)

```
R1#show ip protocols
Routing Protocol is "eigrp 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
```

Métrica composta do EIGRP.

Fonte: Cisco Networking Academy, 2005.

d) **`show ip EIGRP interfaces`** (mostra as interfaces envolvidas no processo EIGRP)

Considere os dados listados a seguir:

Meio	Atraso
100 M ATM	100 µseg
FastEthernet	100 µseg
FDDI	100 µseg
1 HSSI	20.000 µseg
16 M Token Ring	630 µseg
Ethernet	1.000 µseg
T1 (padrão Serial)	20.000 µseg
512 K	20.000 µseg
DSO	20.000 µseg
56 K	20.000 µseg

MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, reliability 255/255, txload 1/255, rxload 1/255.

O comando: `(config-if)#bandwidth` kilobits modifica a métrica padrão de 1544 do roteador.

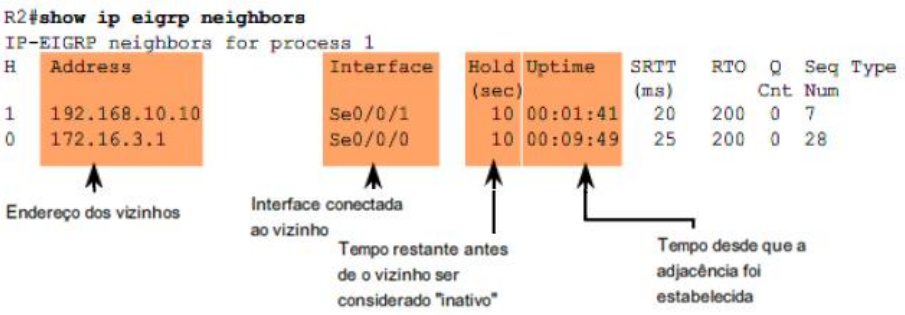
Na fórmula acima:

`reliability 255/255` é o valor da confiabilidade. Quanto maior confiabilidade, melhor.

`txload 1/255, rxload 1/255` são os valores de carga. Quanto menos carga, melhor.

32

e) **show ip eigrp neighbors** (mostra os vizinhos do envolvidos no processo eigrp)



Vizinhos do roteador R2

Fonte: Cisco Networking Academy, 2005.

f) **show ip eigrp topology** (mostra as entradas da tabela de topologia no processo eigrp)

```
R2#show ip eigrp topology 192.168.1.0
IP-EIGRP topology entry for 192.168.1.0/24
  State is Passive, Query origin flag is 1, 1 Successor(s), FD is 3014400
  Routing Descriptor Blocks:
  192.168.10.10 (Serial0/0/1), from 192.168.10.10, Send flag is 0x0
      Composite metric is (3014400/28160), Route is Internal
      Vector metric:
        Minimum bandwidth is 1024 Kbit
        Total delay is 20100 microseconds
        Reliability is 255/255
        Load is 1/255
        Minimum MTU is 1500
        Hop count is 1
  172.16.3.1 (Serial0/0/0), from 172.16.3.1, Send flag is 0x0
      Composite metric is (41026560/2172416), Route is Internal
      Vector metric:
        Minimum bandwidth is 64 Kbit
        Total delay is 40100 microseconds
        Reliability is 255/255
        Load is 1/255
        Minimum MTU is 1500
        Hop count is 2
```

Topologia da rede.

Fonte: Cisco Networking Academy, 2005.

g) **show ip eigrp traffic** (mostra o tráfego de pacotes geridos pelo processo eigrp)

33

RESUMO

Neste módulo foram apresentados os protocolos de roteamento dinâmico RIPv1 e RIPv2 e o EIGRP, proprietário da CISCO.

Os protocolos de roteamento dinâmico foram criados para facilitar a administração de redes cuja topologia é mais complexa, além de estar sujeita a alterações com certa frequência. Esses protocolos permitem que os roteadores troquem entre si informações sobre redes remotas (existente em outro roteador). Uma vez recebida nova informação ela é inserida na tabela do roteamento. Quando isto acontece dizemos que foi criada uma nova “entrada” na tabela de roteamento. De modo análogo, se

uma rede ficar indisponível por qualquer motivo, uma rota pode ser desabilitada e ser retirada da tabela de roteamento.

Esse processo é dinâmico, ou seja, não depende da intervenção manual do administrador da rede e, por essa razão, esses protocolos são considerados protocolos de roteamento dinâmico.

Protocolos de roteamento dinâmico realizam algumas tarefas características, como: 1) detecção de redes remotas, 2) manutenção da tabela de roteamento, 3) escolha da melhor rota para as redes de destino e 4) localizar, quando necessário, nova rota para substituir outra que esteja inativa, momentaneamente ou definitivamente.

Os protocolos de roteamento dinâmico podem ser comparados com base nas seguintes características: 1) Tempo de convergência, 2) Classless (uso de VLSM), 3) Uso de recursos; 4) a Implantação e manutenção.

Outro conceito importante é o vetor de distância, ou seja, as rotas são anunciadas como vetores de distância e direção. A distância é definida em termos de uma métrica como contagem de saltos. A direção é fornecida simplesmente pela interface do roteador do próximo salto ou pela interface de saída neste roteador.

34

O RIP é um protocolo de roteamento classificado como Vetor de Distância. Atualmente ele possui 2 versões que trabalham com o IPv4 que simplifica o gerenciamento da rede e viabiliza a gestão de redes de grande porte. Por outro lado, temos as desvantagens de: 1) utilizar largura de banda nos links entre roteadores, coisa que o estático não faz; 2) requerer mais processamento pela CPU do roteador e 3) ter menor controle da internetwork.

Utiliza os princípios abaixo listados:

1- envia tabela de roteamento completa para todas as interfaces a cada 30 segundos;

2- utiliza a contagem de hops como métrica;

3- limita a contagem máxima de hops a 15, limitando o tamanho da rede. Os 15 saltos são consecutivos, em linha. Uma rede com mais de 15 roteadores pode utilizar o RIP desde que os mesmos não estejam na mesma linha (sequência).

Routing Protocol é um protocolo de roteamento do vetor de distância classless que foi lançado em 1992 pela Cisco Systems. O EIGRP é protocolo de roteamento proprietário da Cisco e um aprimoramento de outro protocolo proprietário da Cisco, o Protocolo de roteamento de gateway interior (IGRP, Interior Gateway Routing Protocol). O IGRP é um protocolo de roteamento do vetor de distância classful que já não é mais suportado pela Cisco. O EIGRP utiliza o código-fonte de "D" para DUAL na tabela de roteamento. O EIGRP possui uma distância administrativa padrão de 90 para rotas internas e 170 para rotas importadas de uma fonte externa, como as rotas padrão.

O EIGRP utilizou PDMs (Módulos dependentes do protocolo) conferindo-lhe a capacidade de suportar protocolos de camada 3 diferentes incluindo IP, IPX e AppleTalk. O EIGRP utiliza o Protocolo de transporte confiável (RTP, Reliable Transport Protocol) como o protocolo da camada de transporte para a entrega de pacotes EIGRP. O EIGRP utiliza entrega confiável para atualizações, consultas e respostas do EIGRP e utiliza entrega não confiável para hellos e confirmações do EIGRP. RTP confiável significa que uma confirmação do EIGRP deve ser devolvida. Antes de as atualizações de EIGRP serem enviadas, um roteador deverá detectar primeiro seus vizinhos. Isto é feito com pacotes hello do EIGRP.

35

Ao centro do EIGRP está o Algoritmo de atualização por difusão (DUAL, Diffusing Update Algorithm). A máquina de estado finito do DUAL é utilizada para determinar o melhor caminho e caminhos de backup em potencial para cada rede de destino.

O sucessor é um roteador vizinho que é utilizado para encaminhar pacotes utilizando a rota de menor custo para a rede de destino. Distância viável (FD, Feasible Distance) é a métrica mais baixa calculada para alcançar a rede de destino através do sucessor. Um sucessor viável (FS, Feasible Successor) é um vizinho que tem um caminho de backup sem loop para a mesma rede que o sucessor e que também atende a condição de viabilidade. A condição de viabilidade (FC, Feasibility Condition) é atingida quando a distância reportada (RD, Reported Distance) de um vizinho para uma rede for menor que a distância viável do roteador para a mesma rede de destino. A distância reportada é simplesmente uma distância viável do vizinho EIGRP para a rede de destino.

O comando `network` é semelhante ao utilizado com o RIP. A rede é o endereço de rede classful das interfaces diretamente conectadas no roteador. Uma máscara curinga é um parâmetro opcional que pode ser utilizado para incluir somente interfaces específicas. Existem diversos modos de propagar uma rota padrão estática com o EIGRP. O comando `redistribute static` no modo de roteador do EIGRP é um método comum.

É definido nas camadas Física (Camada 1) e de Enlace (Camada 2), interconecta duas ou mais LANs e usa técnica de multiplexação e o campo de CRC do frame para detectar erros na transmissão. Para maximizar a largura de banda, não os corrige, passando esta tarefa para as camadas superiores.

UNIDADE 3 – SWITCHES, VLANS E ROTEAMENTO IP
MÓDULO 4 – ROTEAMENTO DINÂMICO OSPF, FRAME-RELAY E REDISTRIBUIÇÃO DE ROTEAMENTO.

01

1 - ROTEAMENTO DINÂMICO OSPF

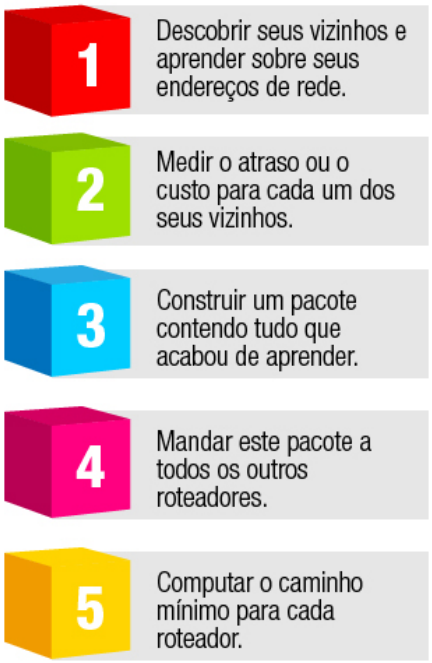
Conforme o CCNA – Cisco Certified Network Associate-Study Guide e Filippetti (2008), o protocolo OSPF (Open Shortest Path First) é um protocolo IGP (Interior Gateway Protocol), projetado para uso intra-AS (Sistema Autônomo).

O protocolo OSPF é definido pela RFC 2328 e foi desenvolvido para atender às necessidades da comunidade Internet que demandavam um protocolo IGP eficiente, não proprietário e interoperável com outros protocolos de roteamento.

OSPF baseia-se na tecnologia "link-state", diferente e bem mais avançada que a tecnologia utilizada em protocolos vetoriais, como o RIP, que utiliza o algoritmo Bellman-Ford para cálculo da melhor rota.

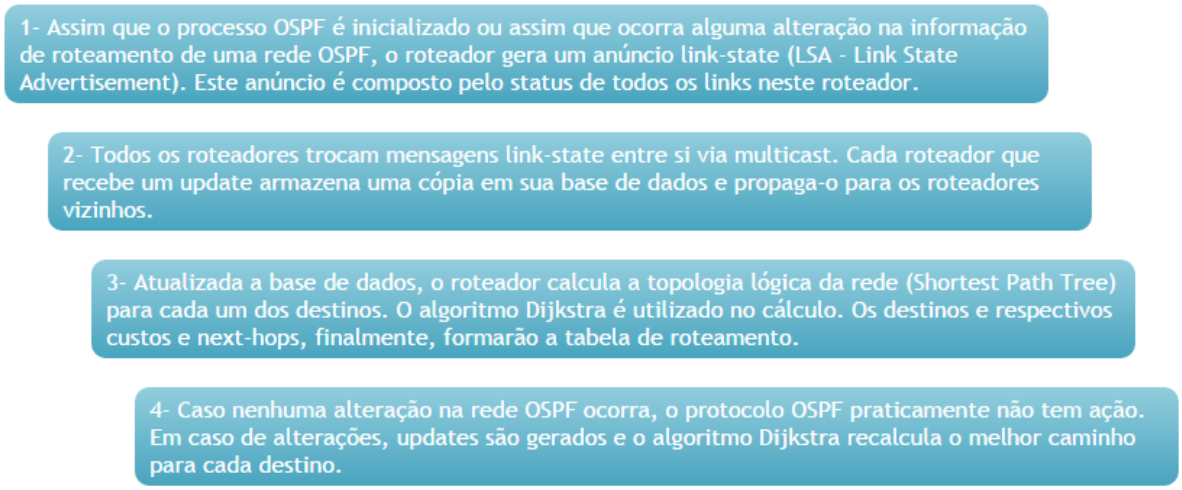
Dizer que OSPF é um protocolo classificado como link-state significa que o protocolo utiliza um algoritmo baseado no estado da ligação para tomada de decisões sobre qual o melhor caminho a ser tomado.

Apenas para relembrar, a ideia por trás de **roteamento link-state** é simples e pode ser apresentada em cinco passos:



Bellman-Ford
O algoritmo de Bellman-Ford resolve o problema do caminho mais curto de única origem para o caso mais geral. Diferentemente do algoritmo de Dijkstra, o algoritmo de Bellman-Ford não impõe nenhuma restrição sobre o sinal do peso das arestas, o que o torna uma solução mais genérica.

A operação do algoritmo utilizado pelo OSPF - chamado de algoritmo de Dijkstra – pode ser resumida como:



OSPF consome mais CPU que protocolos mais simples, como o RIP, exatamente pelos cálculos que ele realiza.

1.1 – OSPF x RIP

Conforme Filippetti (2008), o protocolo RIP possui características que limitam sua aplicação em redes complexas. O protocolo OSPF resolve todas as limitações. Observe a comparação:

Protocolo RIP	Protocolo OSPF
1. Limite de 15 saltos (roteadores) até a rede destino.	1. Não existe limite de saltos com OSPF.
2. RIP não oferece suporte a VLSM.	2. OSPF suporta VLSM.
3. RIP não suporta autenticação.	3. OSPF utiliza anúncios multicast, e as atualizações apenas são disparadas quando existe alguma alteração na rede (anúncios incrementais).
4. RIP adota o procedimento de enviar broadcasts periódicos contendo a totalidade da tabela de roteamento para a rede. Em redes de grande porte e nas WAN, isso gera um consumo excessivo de largura de banda e causa problemas mais sérios.	4. Redes OSPF convergem mais eficientemente do que redes RIP.
5. O processo lento e ineficiente de convergência de uma rede.	5. OSPF permite um meio mais eficaz de balanceamento de carga.
6. RIP baseia-se na contagem de saltos para definição da melhor rota.	6. OSPF permite a implementação de hierarquia às redes, por meio das áreas. Isso facilita o planejamento da rede, assim como tarefas de agregação e sumarização de rotas.
7. Redes baseadas no protocolo RIP são planas. Não existe o conceito de fronteiras ou áreas. RIP não é compatível com redes classless e com conceitos de agregação e sumarização de redes. As limitações de não suporte a VLSM, autenticação e anúncios multicast foram amenizadas com a introdução da versão 2 do protocolo RIP (RIPv2), entretanto, o restante das limitações permaneceram inalteradas.	7. OSPF permite a transferência e marcações de rotas externas, injetadas em um AS (Sistema Autônomo). Isso permite rastrear rotas injetadas por protocolos EGP, como o BGP.

O OSPF também apresenta desvantagens:

1) É mais complexo de ser planejado, configurado e suportado, em comparação com o RIP.

2) Os processos OSPF consomem mais CPU que processos RIP, uma vez que o algoritmo e a estrutura utilizados pelo OSPF são muito mais complexos.

Essas desvantagens são compensadas pela qualidade e pelas funcionalidades proporcionadas por ele às conexões.

1.2 - O Algoritmo SPF

Conforme Filippetti (2008) e Nascimento e Tavares, como já dissemos, em uma rede OSPF o melhor caminho (o mais curto) é calculado aplicando-se o algoritmo Dijkstra. O algoritmo coloca o roteador na raiz da topologia e calcula o melhor caminho para um destino baseando-se no custo cumulativo até o destino em questão. Cada roteador na rede terá uma visão única da topologia lógica, ainda que todos os roteadores utilizem a mesma base de dados link-state (link-state database).

Algumas terminologias são pertinentes para nosso estudo, conforme veremos a seguir.

a) Custo

O custo, métrica de uma interface OSPF, é uma indicação do overhead necessário para o envio de

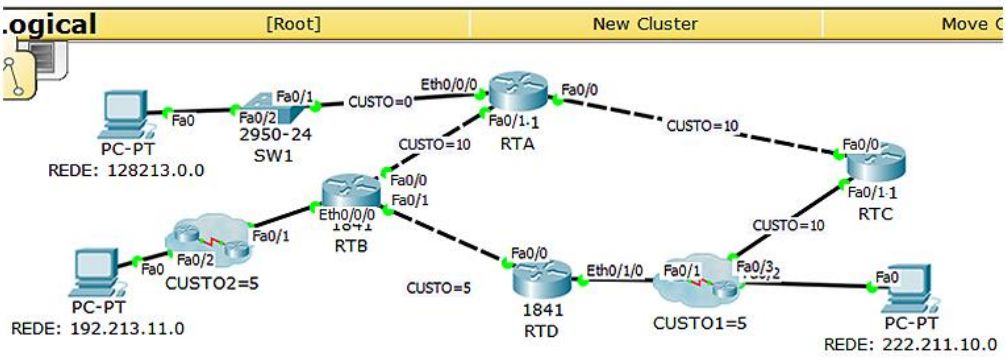
pacotes através desta interface. O custo de uma interface é inversamente proporcional à largura de banda desta interface, ou seja, uma largura de banda maior indica um custo menor.

Uma largura de banda maior indica um custo menor. Por exemplo, se a interface é fastethernet (100Mb) então o Custo = 100.000.000/Banda (bps). Por este motivo, é importante a correta configuração do parâmetro Bandwidth em interfaces rodando OSPF.

b) Árvore (topologia) de caminho mais curto (SP Tree)

Observe a topologia ilustrada na figura abaixo. Observe a diferença entre a topologia física e a topologia lógica gerada pelo algoritmo, considerando-se os custos associados a cada interface. O roteador RTA é raiz da topologia.

No exemplo ilustrado, o custo do roteador RTA para a rede 222.211.10.0 pode ser 20 (10+5+5), se considerarmos o caminho via roteador RTB e RTD ou, também, 20 (10+10), se considerarmos o caminho via RTC. Em caso de caminhos com igual custo, OSPF balanceia a carga (para até 6 caminhos, na implementação do OSPF segundo a Cisco).



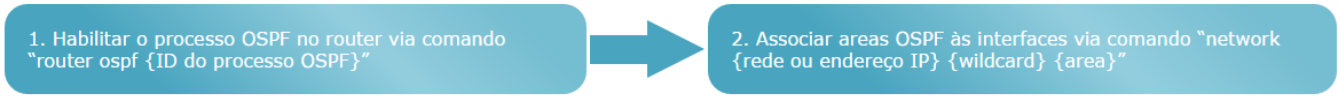
Caminho mais curto
Fonte: O Autor, 2015

c) Roteadores de fronteira (Área ou Borda)

Conforme Filippetti (2008) e Nascimento e Tavares (2012), o OSPF utiliza multicast para propagar os anúncios pela rede. O conceito de áreas foi criado para criar fronteiras de propagação destes anúncios. A propagação de “updates” e o cálculo da topologia pelo algoritmo Dijkstra são restritos à área. Todos os roteadores em uma mesma área terão a mesma base de dados topológica. Roteadores que pertencem a mais de uma área terão as bases de dados de cada área a qual pertencem. Este é o caso dos roteadores de fronteira, como os ABRs (Area Border Routers) e os ASBRs (Autonomous System Border Routers).

1.3 - Configuração do OSPF em um router Cisco

Conforme o CCNA – Cisco Certified Network Associate-Study Guide, a **configuração** do protocolo OSPF em routers Cisco é realizada em dois passos:



O ID do processo OSPF não precisa ser o mesmo em roteadores distintos e vários processos OSPF podem ser executados em um mesmo router. Procedimento este não recomendado, já que cada instância consome grandes porções de CPU e memória. Um bom projetista não utilizaria mais de um processo OSPF em um mesmo router.

O parâmetro "network", diferentemente do que ocorre na configuração de outros protocolos de roteamento, no OSPF, indica quais interfaces participarão do processo e quais as áreas OSPF a que pertencem. Esta é uma particularidade do protocolo. Devemos nos lembrar que, em uma rede OSPF, a fronteira é o link, e este é definido pela interface.

Mas por que os parâmetros de sumarização, em redes OSPF, devem ser configurados na interface?

Resposta: devido às áreas. O ID da área é definido por um número inteiro compreendido entre 0 e 4.294.967.295, e também pode assumir a forma de um endereço IP (ex.: área 0 = 0.0.0.0).

1.4 - Autenticação OSPF

OSPF permite a autenticação de pacotes de forma que routers participam de domínios de roteamento baseados em senhas pré-definidas. Por default, OSPF não utiliza esquemas de autenticação.

Basicamente, existem dois métodos de autenticação que podem ser utilizados:

1) Autenticação Simples

Chaves são configuradas por área OSPF. Routers em uma mesma área que desejem participar do processo de roteamento devem ser configurados com a mesma chave. A desvantagem deste método é que as chaves são trocadas pela rede, e podem ser facilmente interceptadas.

Exemplo

2) Autenticação Forte (MD5)

Uma chave e uma senha são configurados em cada router. O router usa um algoritmo baseado no pacote OSPF, na chave e no ID da chave para gerar um “message digest”, que é inserido no pacote. Este método permite a troca de senha sem a interrupção da comunicação.

Exemplo

Exemplo Autenticação Simples

Exemplo:

```
interface Ethernet0
ip address 10.10.10.10 255.255.255.0
ip ospf authentication-key minha senha

router ospf 10
network 10.10.0.0 0.0.255.255 area 0
area 0 authentication
```

Link Autenticação Forte

Exemplo:

```
interface Ethernet0
ip address 10.10.10.10 255.255.255.0
ip ospf message-digest-key 10 md5 my password

router ospf 10
network 10.10.0.0 0.0.255.255 area 0
area 0 authentication message-digest
```

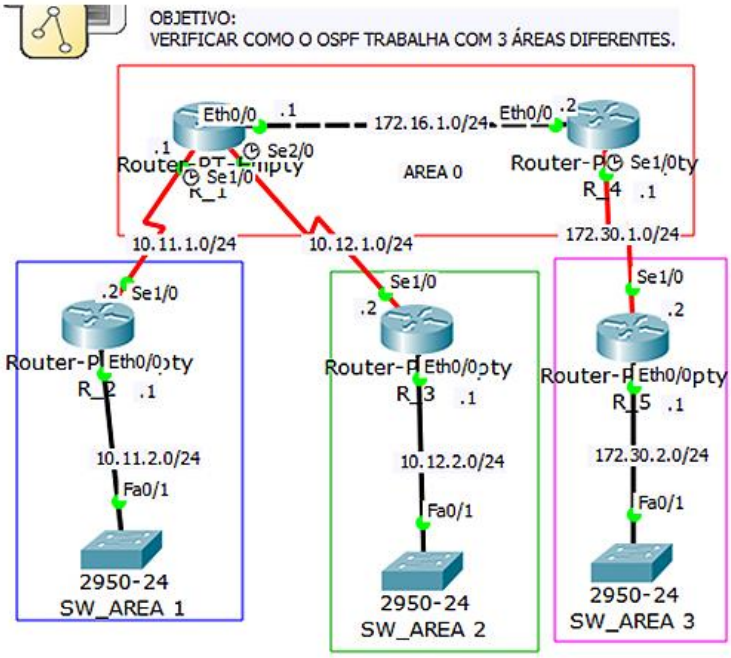
1.5 - OSPF Multi-Área

Segundo Filippetti (2008), o protocolo OSPF possui algumas restrições quando mais de uma área é configurada. Se apenas uma área existir, esta área será SEMPRE a área “0”, chamada de **backbone area**. Quando existem múltiplas áreas, uma destas áreas deve ser a área “0”. Uma das boas práticas ao se desenhar redes com o protocolo OSPF é começar pela área “0” e expandir a rede criando outras áreas (ou segmentando a área “0”).

A área “0” deve ser o centro lógico da rede, ou seja, todas as outras áreas devem ter uma conexão física com o backbone (área “0”). O OSPF aguarda que todas as áreas encaminhem informações de roteamento para o backbone, e este, se encarregará de disseminar estas informações para as outras áreas. Em situações nas quais não é possível estabelecer uma conexão direta com a área “0”, um link virtual (virtual link) deverá ser estabelecido. O link virtual OSPF funciona como uma “VPN” que integra uma área, não conectada diretamente ao backbone, por meio de uma área diretamente conectada a ele.

Informações sobre rotas que são geradas e utilizadas dentro de uma mesma área são chamadas de “intra-area routes” e são precedidas pela letra “O” na tabela de roteamento. Rotas que são originadas em outras áreas são chamadas de “inter-area routes”, ou “summary-routes”. Estas são precedidas por “O IA”, na tabela de roteamento. Rotas originadas por outros protocolos de roteamento e redistribuídas em uma rede OSPF são conhecidas por “external-routes”. Estas são precedidas pelas letras “O E1” ou “O E2”, na tabela de roteamento.

Quando temos múltiplas rotas para um mesmo destino, o critério de desempate em uma rede OSPF obedece a seguinte ordem: intra-area, inter-area, external E1, external E2.

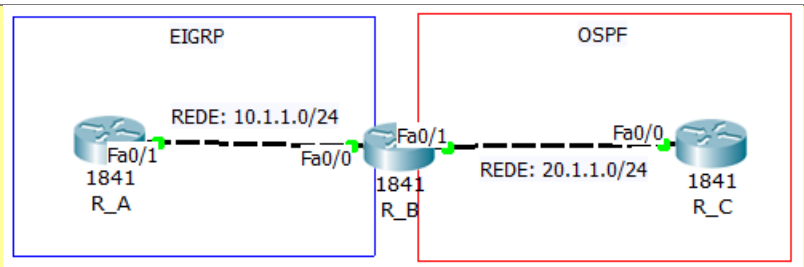


OSPF em áreas diferentes.
Fonte: O Autor, 2015.

Área diretamente conectada

Rotas Diretamente Conectadas

Redistribuir redes que estão diretamente conectadas em um protocolo de roteamento não é uma prática comum e por essa razão não é exibido em nenhum exemplo. Porém, é importante saber que pode ser feito, tanto direta quanto indiretamente. Para distribuir rotas diretamente conectadas utilize o comando *redistribute connected.* Você também deve definir a métrica para este caso. Você também pode redistribuir rotas indiretamente conectadas nos protocolos de roteamento, conforme o exemplo:



Cenário para redistribuição de rotas.
Fonte: O Autor, 2015

Neste exemplo, o roteador B tem duas interfaces Fast Ethernet. A interface FastEthernet 0/0 está na rede 10.1.1.0/24 e a FastThernet 0/1 está na rede 20.1.1.0/24. O roteador B está rodando EIGRP com o roteador A e OSPF com o roteador C. O roteador B está redistribuindo as rotas dos processos EIGRP e OSPF. A configuração a seguir é referente ao roteador B:

Router B

```
interface FastEthernet0/0
ip  address 10.1.1.4 255.255.255.0
interface FastEthernet0/1
ip  address 20.1.1.4 255.255.255.0
router eigrp 7
redistribute ospf 7 metric 10000 100 255 1 1500
network 10.1.1.0 0.0.0.255
auto-summary
no eigrp  log-neighbor-changes
router ospf 7
log-adjacency-changes
redistribute eigrp 7 subnets
network 20.1.1.0   0.0.0.255 area 0
```

Observe a tabela de roteamento do Router B:

```
routerB#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 - periodicdownloaded static route
Gateway of last resort is not set
         20.0.0.0/24 is subnetted, 1 subnets
C       20.1.1.0 is directly connected, FastEthernet0/1
         10.0.0.0/24 is subnetted, 1 subnets
C       10.1.1.0 is directly connected, FastEthernet0/0
```

Em relação à configuração e à tabela de roteamento acima, podemos dizer:

1) As redes em questão estão na tabela de roteamento do roteador B como diretamente conectadas.
2) A rede 10.1.1.0/24 faz parte do processo EIGRP e a rede 20.1.1.0/24 faz parte do processo OSPF.
3) Router B está redistribuindo as rotas entre o EIGRP e o OSPF.

Abaixo estão as tabelas de roteamento dos roteadores A e C:

```
routerA#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, * - candidate default
       U - per-user static route, o - ODR
Gateway of last resort is not set
            10.0.0.0/24 is subnetted, 1 subnets
C          10.1.1.0 is directly connected, FastEthernet0
            20.0.0.0/24 is subnetted, 1 subnets
D EX    20.1.1.0 [170/284160] via 10.1.1.4, 00:07:26, FastEthernet0

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 - periodicdownloaded static route
Gateway of last resort is not set
            20.0.0.0/24 is subnetted, 1 subnets
C          20.1.1.0 is directly connected, FastEthernet1
O E2    10.1.1.0 [110/20] via 20.1.1.4, 00:07:32, FastEthernet1
```

O roteador A tem aprendido sobre a rede 20.1.1.0/24 via EIGRP, que é exibida como uma rota externa, porque esta rede foi redistribuída do OSPF para o EIGRP. O roteador C tem aprendido sobre a rede 10.1.1.0/24 via OSPF como uma rota externa, porque esta rede foi redistribuída do EIGRP para o OSPF. Ainda que o roteador B não esteja redistribuindo redes diretamente conectadas, ele anuncia a rede 10.1.1.0/24 pois esta faz parte do processo EIGRP que é redistribuída para o OSPF. De forma similar, o roteador B anuncia a rede 20.1.1.0/24, pois esta faz parte do processo OSPF que é redistribuída para o EIGRP.

1.6 – Vizinhos e Adjacências

Conforme Filippetti (2008) e Nascimento e Tavares (2012), routers que compartilham um mesmo segmento tornam-se neighbors (vizinhos) neste segmento. O estabelecimento de uma relação de vizinhança ocorre por meio da mensagem “Hello”. Routers tornam-se vizinhos assim que conseguem se enxergar como vizinho no pacote Hello do router vizinho. Desta forma, uma comunicação nas duas vias é garantida. É importante ressaltar que a negociação de vizinhança utiliza apenas o endereço IP primário da interface. Se a mesma estiver configurada com endereços secundários, estes não serão utilizados no processo. Se endereços secundários forem configurados, estes devem pertencer à mesma área OSPF do endereço primário.

Dois routers não estabelecem uma relação de vizinhança até que os seguintes pontos sejam verificados:

- **Area-ID;**
- **Autenticação;**
- **Hello e "Dead Intervals";**
- **"Stub Area Flag";**
- **MTU Size.**

Area-ID
Para dois routers que possuem interfaces em um mesmo segmento, estas interfaces devem pertencer à mesma área OSPF, pertencer à mesma sub-rede e possuir a mesma máscara de rede.

Autenticação
Se autenticação estiver sendo utilizada, routers vizinhos devem trocar a mesma senha em um dado segmento.

Hello e "Dead Intervals"
Routers OSPF trocam mensagens "Hello" em cada segmento. O Keepalive HELLO configurado deve ser consistente em um mesmo segmento. O "Dead Interval" é o intervalo de tempo entre o último pacote HELLO recebido e o router considerar o neighbor como "down". Este intervalo deve ser o mesmo em um mesmo segmento OSPF. Os comandos para configuração destes intervalos nas interfaces são: "ip ospf hello-interval seconds" e "ip ospf dead-interval seconds"

Stub Area Flag
Dois routers devem possuir o mesmo valor no campo "Stub Area Flag", no pacote Hello, para serem vizinhos. Tenha em mente que a definição de áreas "STUB" afeta a relação de vizinhança entre os routers.

MTU Size
Se os valores das interfaces MTU Size forem diferentes em cada ponta, a adjacência não será formada. Se por algum motivo existir a necessidade de estabelecer a adjacência mantendo-se MTUs distintas em cada ponta, o comando "ip ospf mtu-ignore" configurado em cada interface envolvida no processo resolve o problema.

O processo de formação de **adjacências** ocorre após a definição das relações de vizinhança.

Routers adjacentes são aqueles que trocaram pacotes HELLO e iniciaram o processo de sincronismo da base de dados.

1.7 - Roteador DR (Designed Router) e BDR (Backup Designed Router)

Segundo Filippetti (2008), isso ocorre no caso de termos mais de um roteador na área “0”, tal como da figura anterior, R_1 e R_4 estão na área “0”. Neste caso o protocolo elege o roteador que irá transmitir aos demais roteadores da rede os pacotes de atualização, consulta e hello.

A eleição do router DR é feita pelo pacote HELLO. Pacotes HELLO são trocados entre os routers via multicast, em cada segmento. O router que tiver o maior OID (OSPF ID) em um segmento é eleito o DR para aquele segmento. O mesmo processo é realizado para a eleição do BDR. Em caso de empate, o router com maior RID (Router ID) vence a disputa.

Para reduzir a quantidade de informação trocada em um dado segmento, OSPF elege um router para ser o router designado (Designated Router - DR) e outro para assumir o papel de backup dele (Backup Designated Router - BDR) em cada segmento multi-acesso (como segmentos Ethernet, por exemplo). O princípio é criar um ponto central na rede multi-acesso para troca de informações.

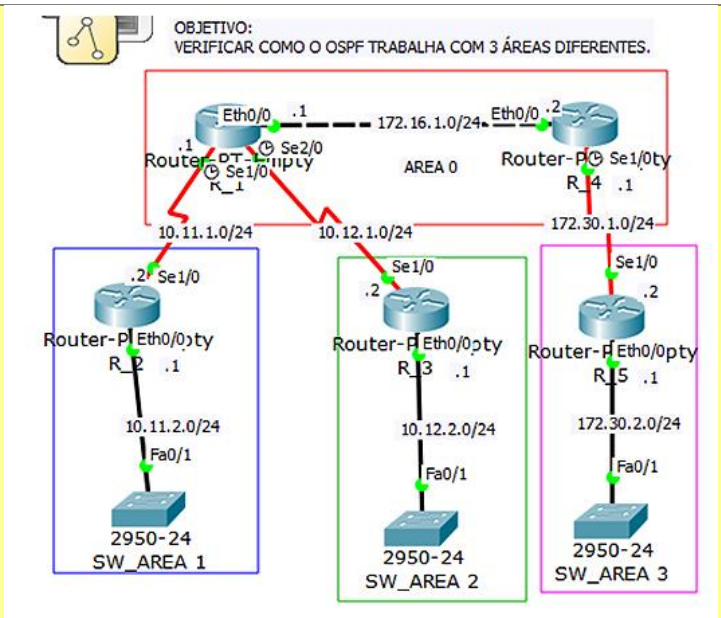
A prioridade default para uma interface OSPF é 1. Este valor pode ser alterado pelo comando: “ip ospf priority“. Uma prioridade “0” significa que a interface em questão não será considerada no processo de eleição do DR/BDR.

O RID é definido pelo maior endereço IP configurado no router. Entretanto, se interfaces Loopbacks existirem, o RID é definido pelo maior IP configurado em uma interface Loopback. É interessante utilizar Loopbacks para definição do RID, pois com elas é possível “garantir” que este endereço IP se manterá, e não será trocado em uma eventual alteração na rede.

O comando “show ip ospf interface” é uma forma rápida de verificar se todas as interfaces encontram-se configuradas nas áreas em que deveriam.

Um ponto importante a ser lembrado é que a ordem em que os comandos são digitados no router é muito importante. Por exemplo, se o comando “network 203.250.0.0 0.0.255.255 area 0.0.0.0” for digitado ANTES do comando “network 203.250.13.41 0.0.0.0 area 1”, todas as interfaces seriam colocadas na área 0 (0.0.0.0), o que é incorreto, já que desejamos que a loopback (203.250.13.41) seja colocada na área 1.

Exemplos de comandos SHOW



loopbacks

Interface de loopback

Algumas vezes é utilizada a interface “lookback” que é uma interface de software, ou seja, virtual, significando que não é física, é apenas lógica e pode ser usada em diversas situações quando, por exemplo, não podemos ou não desejamos instalar interfaces extras em roteadores. Esta interface ficará sempre “up”, por isso é aconselhável utilizá-la como interface de gerenciamento, evitando interfaces de LAN ou WAN. Ela aceita endereço IP, responde ao comando “ping” e a rede da qual faz parte será divulgada na tabela de roteamento.

Exemplos de comandos show

```
RTB#show ip ospf interface e0
Ethernet0 is up, line protocol is up
Internet Address 203.250.14.3 255.255.255.0, Area 0.0.0.0
Process ID 10, Router ID 203.250.12.1, Network Type BROADCAST, Cost: 10
Transmit Delay is 1 sec, State DROTHER, Priority 1
Designated Router (ID) 203.250.15.1, Interface address 203.250.14.2
Backup Designated router (ID) 203.250.13.41, Interface address
203.250.14.1
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 0:00:03
Neighbor Count is 3, Adjacent neighbor count is 2
Adjacent with neighbor 203.250.15.1 (Designated Router)
Adjacent with neighbor 203.250.13.41 (Backup Designated Router)

RTD#show ip ospf neighbor
Neighbor ID Pri State Dead Time Address Interface
```

```
203.250.12.1 1 2WAY/DROTHER 0:00:37 203.250.14.3 Ethernet0
203.250.15.1 1 FULL/DR 0:00:36 203.250.14.2 Ethernet0
203.250.13.41 1 FULL/BDR 0:00:34 203.250.14.1 Ethernet0
```

2. ROTEAMENTO DINÂMICO FRAME RELAY

Conforme a Cisco Network Academy (2005), as redes e os equipamentos de computação dos dias atuais, devido às características da celeridade, precisam trabalhar a velocidades muito mais altas e transferir dados em grande quantidade.

O Frame Relay é uma tecnologia de comunicação de dados de alta velocidade. Combina as funcionalidades de multiplexação estatística e compartilhamento de portas do X25 com as características de alta velocidade e baixo atraso (delay) dos circuitos TDM (clique aqui para ver as diferenças). É um serviço de pacotes que organiza as informações em pacotes de dados com endereço de destino definido.

Apesar de ser um protocolo relativamente antigo, o Frame Relay (FR) é ainda muito utilizado na área de telecomunicações. Por suas características de qualidade e por existir no Brasil uma rede legada com grande capilaridade, o Frame Relay está presente na composição de diversos serviços de Telecom, em geral, como uma opção de acesso a redes de dados corporativas ou à Internet.

De uma forma genérica, pode-se dizer que a tecnologia Frame Relay implementa mecanismos para o envio de informações por comutação de pacotes, sejam elas provenientes de serviços de dados como de voz. A forma de envio é feita por “frames” (ou quadros), onde cada frame tem um “endereço” que define o destino de entrega da informação.

O FR é definido nas camadas Física (Camada 1) e de Enlace (Camada 2), interconecta duas ou mais LANs.

Antigo

Entre 1980 - início de 1990: o Bell Labs (EUA) desenvolvia a tecnologia ISDN tendo o protocolo Frame Relay como parte do conjunto. Entretanto, devido a suas características, o protocolo foi desmembrado e evoluiu como um serviço de rede independente, com padrões e recomendações elaborados por órgão internacionais de Telecomunicações.

Clique aqui

Comparação entre os circuitos TDM, o protocolo X25 e o Frame Relay

	TDM	X25	Frame Relay
Multiplexação em Tempo	sim	não	não
Multiplexação Estatística (Circuito Virtual)	não	sim	sim
Compartilha portas	não	Sim	sim
Alta velocidade (por $)	sim	Não	sim
Atraso (delay)	muito baixo	Alto	baixo

Fonte: Acesso à Internet, 2015

Comutação

Aprendemos que roteadores direcionam pacotes para outros roteadores em redes diferentes. Além disso, outra função básica de um roteador é encaminhar os pacotes entre interfaces de entrada e saída.

Suponhamos que o roteador R1 possua a interface Fa 0/0 configurado com o IP 172.16.0.1 /28, aonde chega um pacote e outra interface Se 0/0/0 cujo IP é 172.16.0.17 /28, por onde sairá o pacote. Respectivamente as redes envolvidas são 172.16.0.0 /24 e 172.16.0.16 /24, ou seja, sub-redes diferentes no mesmo roteador.

Para direcionar os pacotes entre as duas interfaces, vamos supor que existe uma rota apropriada. Nesse caso o roteador usará o recurso da comutação de pacotes. Assim, para o pacote "atravessar" o roteador seguindo da interface de entrada até a interface de saída é necessário realizar a comutação de pacotes IP.

Existe a possibilidade da interface de entrada apresentar tecnologia diferente da interface de saída. No exemplo acima a interface Fa 0/0 é uma interface FastEthernet, enquanto a Se 0/0/0 é uma interface serial. Cada uma delas opera com quadros (frames) diferentes em função das tecnologias características de cada link. Interfaces FastEthernet usam encapsulamento Ethernet, enquanto a Se 0/0/0 pode estar usando um link PPP. Por essa razão dizemos que a principal função da comutação em roteadores é encapsular pacotes no tipo apropriado do quadro de enlace (camada 2) característico do protocolo de camada 2 da interface de saída.

2.2 – Características e benefícios do Frame Relay

Segundo a Cisco Network Academy (2005), como é derivado do antigo X25, o FR usa a mesma tecnologia de comutação de pacotes, porém, de modo mais eficiente. Em consequência, a rede se torna mais rápida, mais simples e mais barata de manter.

O Frame Relay surgiu para **amenizar problemas de comunicação** que outros protocolos não conseguiam, tais como velocidades mais altas, eficiência em altas larguras de banda, particularmente

para surtos de tráfego, otimização dos dispositivos de rede para a redução do processamento dos protocolos e a necessidade de contar LANs e WANs.

Podemos destacar algumas razões que tornam o Frame Relay uma versão **mais eficiente e eficaz** do antigo X25. São elas:

1) não realiza detecção de erros, o que resulta em um processamento significativamente menor que o X.25;
2) é independente de protocolo (ele aceita dados de diferentes protocolos).
3) os dados são encapsulados pelo equipamento Frame Relay, não pela rede.
4) os dispositivos (roteadores, DSU-Data Service Unit/CSU-Communication Service Unit) conectados em uma rede Frame Relay é que são responsáveis pela correção de erros e pelo formato do frame;
5) o tempo de processamento é minimizado para que a transmissão dos dados seja muito mais rápida e eficiente.
6) o Frame Relay é totalmente digital, o que reduz a chance de erros e oferece taxas de transmissão excelentes. O Frame Relay opera tipicamente de 64 até 2048 Mbps.

Como o processamento dos pacotes no Frame Relay é rápido, ele é ideal para as **redes complexas** de hoje.

Alguns **benefícios** de sua utilização:

1) múltiplas conexões lógicas podem ser transmitidas em uma única conexão física, reduzindo os custos de comunicação.
2) pela redução do processamento necessária, consegue-se um maior desempenho e tempo de resposta;
3) o Frame Relay usa um protocolo de rede simples, os equipamentos só precisam de pequenas modificações de software ou hardware, em consequência, não há necessidade de grandes recursos financeiros para a atualização do sistema. Como exemplo de uma aplicação que utiliza o Frame Relay temos o VOFR, ou voz sobre Frame Relay.
4) como o Frame Relay é independente de protocolo, ele pode processar tráfego a partir de protocolos como IP, IPX da Novell e SNA. O Frame Relay é a escolha ideal para a conexão de WANs (Redes de Área Extensa), as quais têm alto volume de tráfego em surtos imprevisíveis. Essas aplicações, tipicamente incluem transferência de dados, CAD/CAM e aplicações cliente-servidor.
5) oferece vantagens para a interconexão de WANs. No passado, a instalação de WANs requeria o uso linhas privativas (LPs) ou comutação de circuitos baseados em linhas privativas. No Frame Relay, não é necessário instalar linhas privativas dedicadas para se fazer uma conexão WAN-WAN, o que reduz os custos.

2.3 - Que tecnologia é utilizada?

Usa técnica de multiplexação e o campo de CRC do frame para detectar erros na transmissão. Para maximizar a largura de banda, não os corrige, passando esta tarefa para as camadas superiores.

Frame Relay provê uma comunicação entre dispositivos DTEs através de dispositivos DCEs. Por operar na camada 2, qualquer informação de camada de rede (IP, IPX, AppleTalk), é totalmente irrelevante para ele.

Essa tecnologia é utilizada em todas as redes ao redor do mundo para interligar aplicações do tipo LAN, SNA, internet e voz.

Como funciona?

Frame Relay funciona como propagador de informações através de uma rede de dados. Divide essas informações em frames (quadros) ou packets (pacotes). Cada frame carrega um endereço, usado pelos equipamentos da rede para determinar o seu destino. É um chaveamento de pacotes, por isso permite uma grande variedade de aplicações.

A tecnologia Frame Relay é baseada no uso de Circuitos Virtuais (VCs). Um VC é um circuito de dados virtual bidirecional configurado entre duas portas quaisquer da rede, funciona como um circuito dedicado. Existem dois tipos de VCs:

a) Permanent Virtual Circuit (PVC)
b) Switched Virtual Circuit (SVC)

O PVC oferece o ganho relativo ao uso estatístico de banda do Frame Relay enquanto o SVC propicia a conectividade entre quaisquer pontos de origem e destino.

a) Permanent Virtual Circuit (PVC)

Permanent Virtual Circuit (PVC)

Ele é configurado pelo operador na rede através do sistema de Gerência de Rede, como sendo uma conexão permanente entre 2 pontos. Seu encaminhamento através dos equipamentos da rede pode ser alterado ao longo do tempo devido a falhas ou reconfigurações de rotas, porém as portas de cada extremidade são mantidas fixas e de acordo com a configuração inicial.

b) Switched Virtual Circuit (SVC)

Switched Virtual Circuit (SVC)

O SVC também foi padronizado para o Frame Relay desde o princípio. Ele é disponibilizado na rede de forma automática, sem intervenção do operador, como um circuito virtual, para atender as aplicações de Voz que estabelecem novas conexões a cada chamada. O estabelecimento de uma chamada usando o protocolo de sinalização do SVC (ITU-T Q933) é comparável ao uso normal de telefone, onde a aplicação de usuário especifica um número de destinatário para completar a chamada, e o SVC é

estabelecido entre as portas de origem e destino.

O estabelecimento de SVCs na rede é mais complexo que os PVCs, embora seja transparente para o usuário final. As conexões devem ser estabelecidas de forma dinâmica na rede, atendendo as solicitações de destino e banda das diversas aplicações de usuários, e devem ser acompanhadas e cobradas de acordo com o serviço fornecido.

2.5 – Composição do Sistema Frame Relay:

Ainda conforme a Cisco Network Academy (2005), uma rede Frame Relay é composta por:

1- Equipamentos de usuários (PCs, estações de trabalho, servidores, computadores de grande porte) e suas respectivas aplicações;

2- Equipamentos de acesso com interface Frame Relay (Bridges, Roteadores de Acesso, Dispositivos de Acesso Frame Relay - FRAD);

3- Equipamentos de rede (switches, roteadores de rede, equipamentos de transmissão com canais E1 ou T1).

A conversão dos dados para o protocolo Frame Relay é feita pelos equipamentos de acesso. Os frames gerados são enviados aos equipamentos de rede, que transportam esses frames até o seu destino, usando os procedimentos de chaveamento ou roteamento próprios do protocolo.

O que preciso para começar?

Inicialmente há necessidade de:

1) um provedor de serviços Frame Relay, normalmente uma companhia telefônica;
2) uma assinatura de uma taxa de informações assegurada (CIR), por exemplo, 64 kbps. Isso significa que a companhia garantirá que os dados trafegarão pelo PVC (Private Virtual Circuit) nessa taxa. Dependendo do tráfego da rede e do tipo de linha adquirido, por exemplo, 2 Megabps fracionado a 128 kbps, poder-se-á conseguir taxas de transmissão mais altas para surtos de 2 segundos. Em horas de pico (congestionamento de tráfego) a taxa poderá voltar para, não menos, de 64 kbps.
3) do equipamento Frame Relay. Como o Frame Relay não faz conversão de protocolos nem detecção/correção de erros, os dispositivos do usuário final precisam ser inteligentes. Alguns dos equipamentos Frame Relay são os FRADs (Frame Relay Assembler/Disassembler), roteadores, bridges e switches de frame.

2.6 - Operação de comunicação Frame Relay

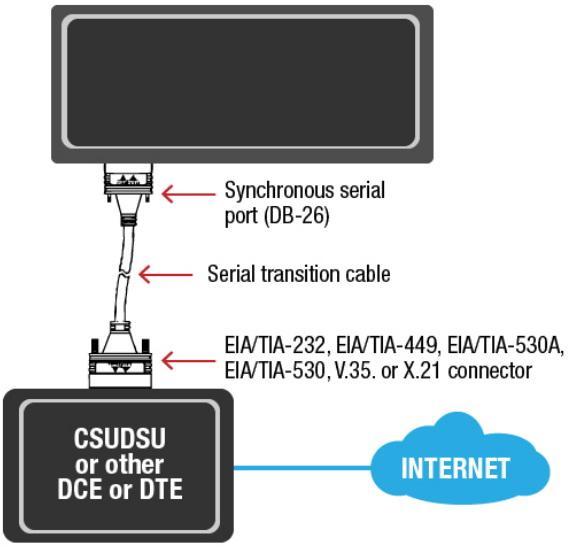
1º) O Host envia um frame com o endereço MAC de destino ao router.

2º) O Router descarta o frame e analisa o endereço IP de destino, analisa na sua tabela de roteamento e envia o pacote pela interface apropriada. (se a rota não for encontrada e não tiver uma rota padrão-gateway of last resort- o pacote será descartado).

3º) O pacote será encapsulado em um frame Frame Relay, e será enviado para a rede Frame Relay, contendo o número DLCI-Data Link Connection Identifier- da interface serial (O DLCI identifica o PVC) para os routers e switches da operadora participante Frame Relay.

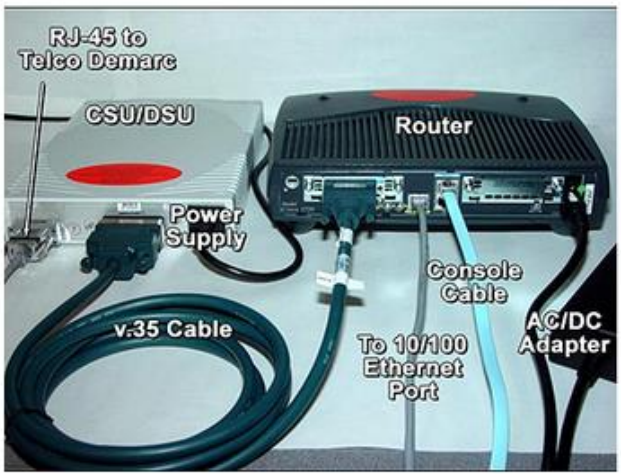
4º) O dispositivo CSU-Communication Service Unit/DSU-Data Service Unit- recebe o sinal digital, codifica na "linguagem" Frame Relay e repassa para o PSE.

5º) O CSU/DSU é conectado ao demarc por meio de uma tomada RJ-45.



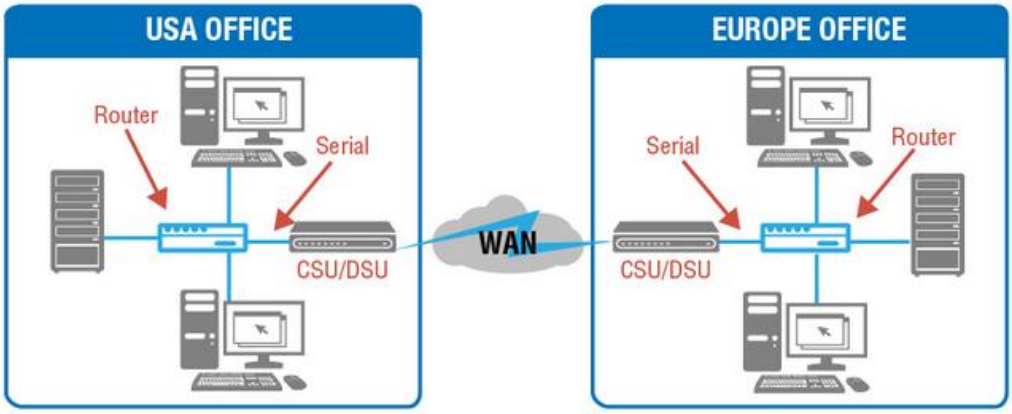
Equipamento CSU/DSU.

Fonte: Acesso à Internet, 2015.



Equipamento demarc.

Fonte: Acesso à Internet, 2015.



Exemplo de ligação entre redes.
Fonte: Acesso à Internet, 2015.

6º) O Demarc é conectado ao loop local, que é conectado ao CO (Central Office). O loop local se conecta ao CO por par trançado ou fibra ótica.

7º) O CO recebe o frame e envia para a "nuvem" Frame Relay. O endereço IP destino e o numero DLCI são analisados.

8º) Alcançando o switching office mais próximo, o frame é enviado através do loop local. O frame é recebido pelo demarc e encaminhado para o CSU/DSU. O Router recebe o frame e o envia para a rede local.

2.7 - Vantagens e Restrições do Frame Relay

Vantagens do FR	Restrições do FR
1. Custo de propriedade reduzido (equipamentos mais simples); 2. Padrões estáveis e largamente utilizados, possibilita a implementação de plataformas abertas e plug-and-play; 3. Overhead reduzido, combinado com alta confiabilidade; 4. Redes escaláveis, flexíveis e com procedimentos de recuperação bem definidos; 5. Interoperabilidade com outros protocolos e aplicações, tais como ATM e TCP/IP.	1. Os equipamentos de usuário devem utilizar aplicações com protocolos inteligentes, que controlem o fluxo das informações enviadas e recebidas; 2. A rede de transporte deve ser virtualmente a prova de falhas.

2.8 - Estrutura do Quadro do Frame Relay

Ainda conforme a Cisco Network Academy (2005),o protocolo do Frame Relay utiliza um frame com estrutura comum e bastante simplificada, conforme demonstram as figuras abaixo e a descrição a seguir:

Estrutura do frame

FLAG	CABEÇALHO	INFORMAÇÃO DE USUÁRIO	FCS	FLAG

Estrutura do frame.
Fonte: Acesso à Internet, 2015.

Estrutura do cabeçalho

Byte 1								Byte 2							
DLCI						C/R	EA	DLCI				FE CN	BE CN	DE	EA
8	7	6	5	4	3	2	1	8	7	6	5	4	3	2	1

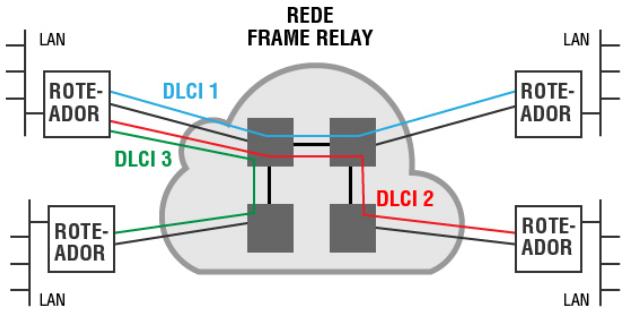
Estrutura do cabeçalho.
Fonte: Acesso à Internet, 2015.

A tabela a seguir descreve resumidamente os campos da estrutura e do cabeçalho.

Flags	Indicam o início e o fim de cada frame.
Cabeçalho	Carrega as informações de controle do protocolo. É composto por 2 bytes com as seguintes informações: DLCI (Data Link Connection Identifier), com 10 bits, representa o número (endereço) designado para o destinatário de um PVC dentro de um canal de usuário, e tem significado local apenas para a porta de origem (vide figura abaixo); C/R (Command / Response), com 1 bit, é usado pela aplicação usuária; FECN (Foward Explicit Congestion Notification), com 1 bit, é usado pela rede para informar um equipamento receptor de informações que procedimentos de prevenção de congestionamento devem ser iniciados; BECN (Backward Explicit Congestion Notification), com 1 bit, é usado pela rede para informar um equipamento transmissor de informações que procedimentos de prevenção de congestionamento devem ser iniciados; DE (Discard Eligibility Indicator), com 1 bit, indica se o frame pode ser preferencialmente descartado em caso de congestionamento na rede; EA (Extension Bit), com 2 bits, é usado para indicar que o cabeçalho tem mais de 2 bytes, em caso especiais;
Informação de usuário	Contém as informações da aplicação usuária a serem transportadas através da rede Frame Relay.
FCS	O FCS (Frame Check Sequence) representa o CRC padrão de 16 bits usado pelo protocolo Frame Relay para detectar erros existentes entre o Flag de início do frame e o próprio FCS, e pode ser usado apenas para frames com até 4096 bytes.

Descrição do cabeçalho do Frame Relay

A figura a seguir exemplifica DLCIs configurados a partir de uma mesma porta para vários destinatários em locais distintos da rede.



Estrutura do cabeçalho.
Fonte: Acesso à Internet, 2015.

FECN
Quando a rede frame relay identifica um congestionamento na “nuvem”, o switch ativa o bit FECN no cabeçalho do pacote frame relay. Isso informará ao DCE destino que a rota recém atravessada pelo pacote em questão encontra- e congestionada.

BECN (Backward Explicit Congestion Notification)
Quando o switch detecta um congestionamento na rede, ele envia um pacote para o router de origem, para diminuir o fluxo de pacotes.

DE
Quando um router Frame Relay detecta congestionamento na rede, ele ativa o bit DE no cabeçalho do pacote frame relay, (de 0 para 1). Se o switch frame relay estiver congestionado, ele vai descartar todos os pacotes com o bit ativado (bit 1).

2.9 - Frame Relay em redes Cisco

Ainda conforme a Cisco Network Academy (2005), para configurar Frame Relay em routers Cisco especificar o encapsulamento:

```
Router(config)#interface serial0/0 | encapsulation frame-relay [ietf - cisco]
```

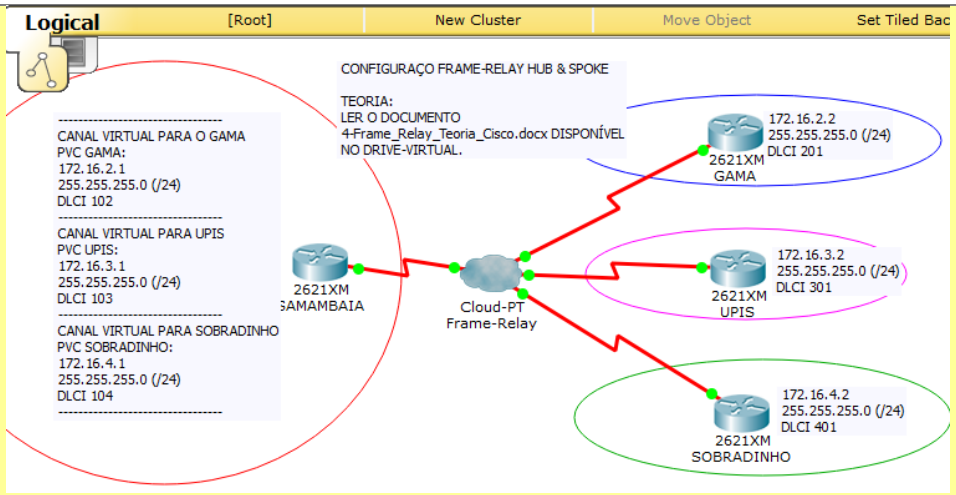
Observação: se nada for especificado após o *encapsulation,* será escolhido o modo de encapsulamento default *cisco* (que só é funcional com routers Cisco).

Veja aqui um exemplo de configuração do Frame Relay.

Link páginas amarelas

Configuração do Frame Relay: exemplo resolvido

Seja o cenário abaixo:



Configuração do Frame Relay.
Fonte: O Autor, 2015.

Cenário: conectar 4 sites (filiais) entre si por meio do frame-relay cada filial faz parte de uma sub-rede. Os endereços virtuais (dlci) foram fornecidos pela empresa de telecomunicações.

Aplique a configuração dos roteadores com os dados abaixo:

1) gama: pvc gama; IP: 172.16.2.1/24; dlci 102.
2) upis: pvc upis; IP: 172.16.3.1/24; dlci 103.
3) sobradinho: pvc sobradinho; IP:172.16.4.1/24; dlci 104

Roteador gama:

```
router(config)# hostname gama
gama(config)# int se0/0
gama(config-if)# encap frame-relay ietf
gama(config-if)# frame-relay lmi-type cisco
gama(config-if)# ip add 172.16.2.2 255.255.255.0
gama(config-if)# frame-relay interface-dlci 201
gama(config-if)# no shut
gama(config-if)# end
gama#wr
```

Repita os passos acima para cada um dos roteadores upis e sobradinho, com seus respectivos parêmetros.

A questão é: como interligar os 3 sítios (gama, upis e sobradinho) a samambaia se tenho somente uma interface serial (se0)?

A resposta é: utilizar o artifício da sub-interface. Repare nos avisos ao lado do sítio samambaia: os pvc, ips, mscs e dlcis.

Então, no roteador samambaia faça:

```
(config)# int se0/0
(config-if)# encap frame-relay ietf
(config-if)# frame-relay lmi-type cisco
(config-if)# no shut
(config-if)# int se0/0.102 point-to-point
(config-subif)# ip add 172.16.2.1 255.255.255.0
(config-subif)# frame-relay interface-dlci 102
(config-subif)#exit
(config-if)# int se0/0.103 point-to-point
(config-subif)# ip add 172.16.3.1 255.255.255.0
(config-subif)# frame-relay interface-dlci 103
(config-subif)# exit
(config-if)# int se0/0.104 point-to-point
(config-subif)# ip add 172.16.4.1 255.255.255.0
(config-subif)# frame-relay interface-dlci 104
(config-subif)#exit
(config-if)# exit
(config)#wr
```

Repita os passos aos demais roteadores.

Configurou todos os roteadores?

Testou a conectividade entre os 3 e samambaia?

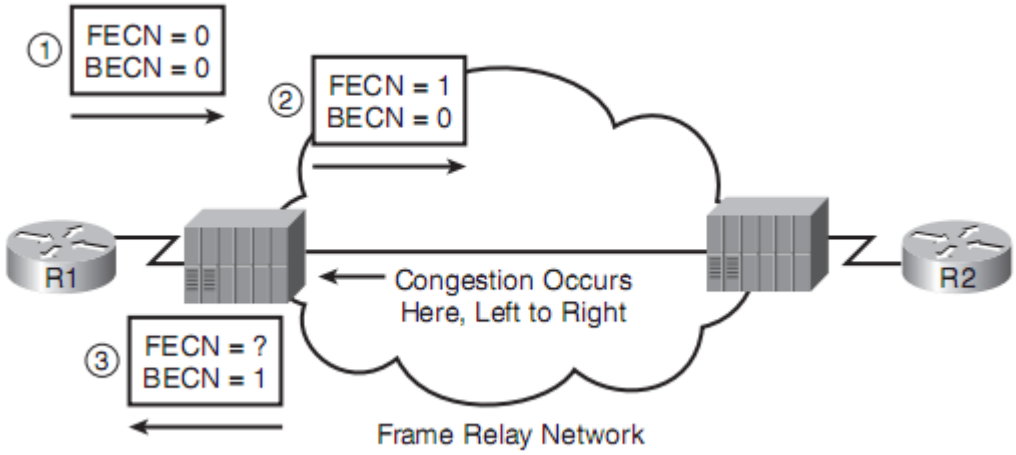
Se obteve “sucesso” então a rede está funcional com cada um "falando" com samambaia.

O que ocorre entre os três roteadores?
Veja que a comunicação falha. Solução: configure o roteamento entre eles. Use o estático ou um dos dinâmicos que já aprendeu. Se utilizar o RIP então:

> enable
router rip
#version 2
network 172.16.0.0 (sabe explicar o por que?)
end
#wr

2.10 - Fluxo das informações

O fluxo básico das informações em uma rede Frame Relay é descrito a seguir por meio da figura.



Fluxo das informações FR.

Fonte: Acesso à Internet, 2015.

1º) As informações são enviadas através da rede Frame Relay usando o DLCI, que especifica o destinatário do frame.

2º) Se a rede tiver algum problema ao processar o frame devido às falhas ou ao congestionamento nas linhas de dados, os frames são simplesmente descartados.

3º) A rede Frame Relay não executa a correção de erros, pois ela considera que o protocolo da aplicação de usuário executa a recuperação de falhas através da solicitação de retransmissão dos frames perdidos.

4º) A recuperação de falhas executada pelo protocolo da aplicação, embora confiável, apresenta como resultado o aumento do atraso (delay), do processamento de frames e do uso de banda, o que torna imprescindível que a rede minimize o descarte de frames.

5º) A rede Frame Relay requer circuitos da rede de transmissão com baixas taxas de erros e falhas para apresentar boa eficiência.

Em redes de transmissão de boa qualidade, o congestionamento é de longe a causa mais frequente de descarte de frames, demandando da rede Frame Relay a habilidade de evitar e reagir rapidamente ao congestionamento como forma de determinar a sua eficiência.

2.11 - Especificações e Normas Frame Relay

Existem dois órgãos internacionais que padronizam o Frame Relay: ANSI e ITU-T. Cada órgão publica as normas com uma numeração diferente:

Especificação: **Service Description** – ANSI T1.606 ou I233

Especificação: **Core Aspects** – ANSI T1.618 ou Q922 (Anexo A)

Especificação: **Access Signaling** – ANSI T1.617 ou Q933

2.11 - Principais conceitos e configuração do Frame Relay

Frame Relay (FR) para redes WANs.

1. é um protocolo de tráfego de pacotes em nível da camada de enlace disponibilizado pelas operadoras de serviço de telefonia (antiga BrasilTelecom).
2. utiliza enlaces virtuais PVC-Permanent Virtual Circuit.
3. compõe-se de nós de comutação (switches FR) que encaminham pacotes FRAD (frame relay assembler/disassembler) implementados em roteadores.
4. padrão industrial, como protocolo de comunicação da camada de enlace que usa circuitos virtuais.
5. usa encapsulamento HLDLC (High Level Data Link Control) nos roteadores.
6. amplamente utilizado, originou-se do protocolo x25.
7. utiliza pacotes de tamanho variável para a transferência dos mesmos de maneira mais eficiente e flexível.
8. a maioria das companhias telefônicas disponibiliza o FR a 56 kbps.
9. dispositivos fr: dte (do lado do cliente representado pelo roteador de borda) e o dce (da cia telefônica, a nossa núvem que vamos configurar, representado pelo equipamento CSU/DSU - Comunnication Service Unit/Data Service Unit).
10. a comunicação física normalmente é feita por uma conexão serial (RS-232). É a nossa conexão DCE sincronizada (a do relógio).
11. FR fornece comunicação da camada de enlace orientada a conexão (tal como o telefone). Existe uma comunicação definida entre cada par de dispositivos e ela é associada a um identificador de conexão (circuito virtual FR).
12. os circuitos virtuais fornecem um caminho bidirecional de um DTE a outro e são identificados pelo DLCI (Data Link Connection Identifier).

13. os circuitos virtuais são multiplexados (vários canais em um único canal físico) para a transmissão através da rede. Podem ser: circuitos virtuais comutados (SVCs) ou circuitos virtuais permanentes (PVCs) que utilizaremos.

14. LMI - Local Management Interface: a) cisco (cisco + 3 outras empresas); b) ansi (american national standard institute) e c) ietf - q933a - itu-t q933 anexo a.

15. como configurar o FR?

a) o roteador cliente (você) é o DTE;

b) definir o FR camada 2 na serial correspondente:

#config t.

#int se0/0

#encapsulation frame-relay ietf

c) configurar o formato do protocolo de gestão do fr (lmi):

#frame-relay lmi-type ansi

#no shutdown

#end

#wr

16. para verificação do FR faça:

a) show interface serial0/0

b) show frame-relay pvc

c) show frame-relay map

por exemplo:

r_econo:

int se0/1/0

encapsulation frame-relay

frame-relay interface-dlci 50

exit

ip route

192.168.2.0 255.255.255.0 10.0.0.20

r_info:

int se0/1/0

encapsulation frame-relay

frame-relay interface-dlci 50

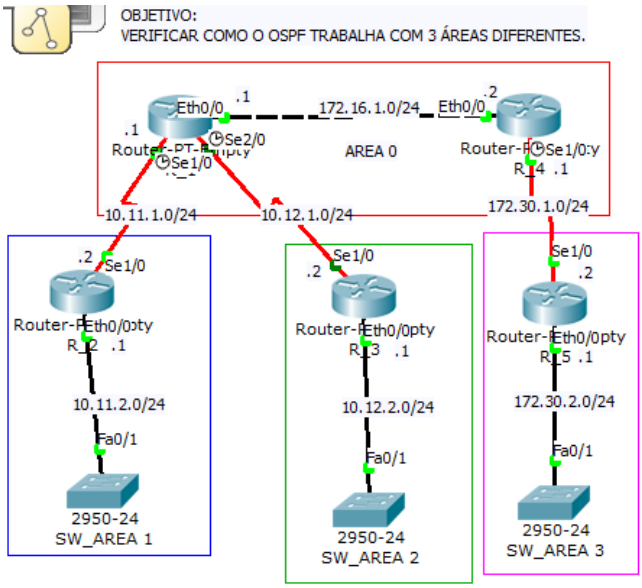
exit

ip route

192.168.1.0 255.255.255.0 10.0.0.10

a) **Configuração do protocolo OSPF, Área 0, 1, 2 e 3.**

Objetivo: Configurar os roteadores da topologia dada com o protocolo OSPF de tal maneira que torne a rede totalmente funcional.



Configuração OSPF em áreas diferentes.

Fonte: O Autor, 2015.

Tarefas:

1º) monte a topologia no packet tracer.

2º) execute o plano de endereçamento ip.

3º) configure os roteadores conforme mostrado.

4º) simule no packet tracer.

5º) em cada um dos roteadores, execute os comandos:

5.1) show ip route;

5.2) show ip ospf neighbor;

5.3) show ip ospf int;

6º) pesquise na internet o significado:

6.1) resultado de show ip route:

- C

- O

- O IA

6.2) resultado de show ip ospf neighbor:

-neighbor

-pri

-state

Configurações:

Em cada interface de cada roteador:

- ative a interface.

- atribua IP/Msc com o comando <IP> <Msc> da rede à qual pertence a interface.

Em cada roteador:

- configure o protocolo com o comando router ospf 100.

- publique a rede com o comando network <rede> <wildcard> area 0

(este comando deve ser repetido tantas vezes quantas forem as interfaces que ligam áreas diferentes).

Exemplos:

CONFIG R1

CONFIG R4

CONFIG R1:

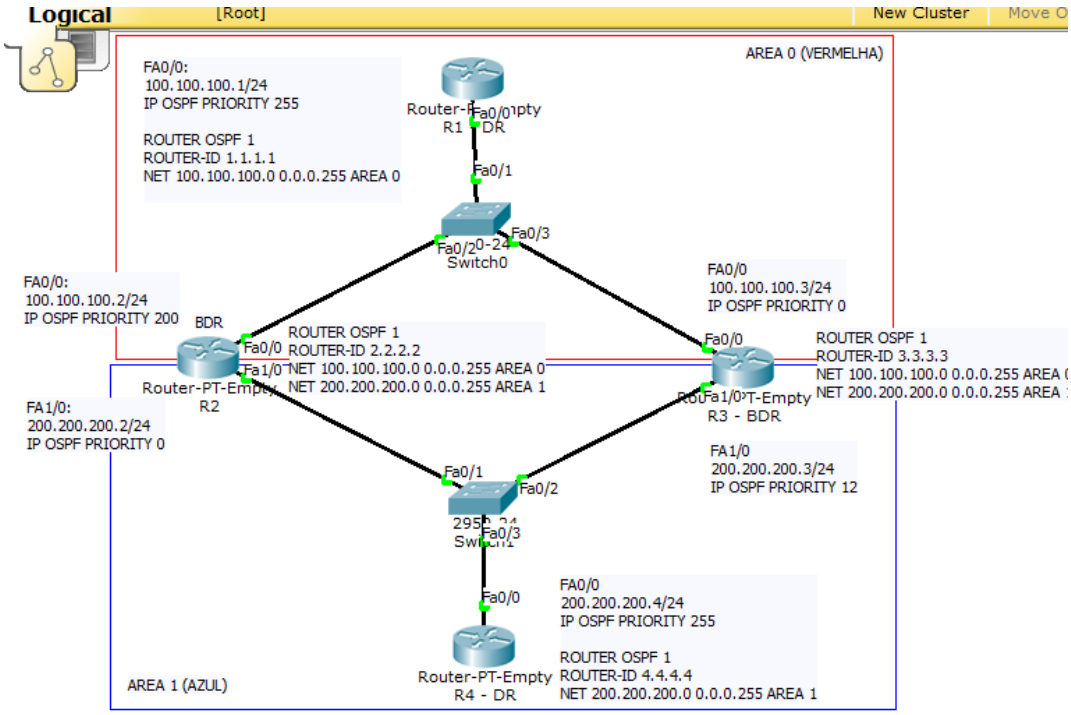
```
interface Ethernet0/0
ip address 172.16.1.1 255.255.255.0
interface Serial2/0
ip address 10.12.1.1 255.255.255.0
interface serial1/0
ip address 10.11.1.1 255.255.255.0
router ospf 100
network 172.16.1.0 0.0.0.255 area 0
network 10.11.0.0 0.0.255.255 area 1
network 10.12.0.0 0.0.255.255 area 2
```

CONFIG R4:

```
interface Ethernet0/0
ip address 172.16.1.2 255.255.255.0
interface Serial1/0
ip address 172.30.1.1 255.255.255.0
router ospf 100
network 172.16.1.0 0.0.0.255 area 0
network 172.30.0.0 0.0.255.255 area 3
```

2.14 - Exemplo resolvido de eleição do roteador DR e BDR

Seja o cenário da figura abaixo, com quatro roteadores (R1, R2, R3 e R4) conectados em 2 redes broadcast distintas: R1, R2 e R3 em uma rede e R2, R3 e R4 em outra rede. Todos os roteadores deverão usar OSPF sendo a rede broadcast do R1, R2 e R3 a área 0 e a outra rede a área 1.



Eleição do Roteador DR e BDR.

Fonte: Acesso à Internet, 2015.

Para a área 0 o R1 deverá ser o Designated Router (DR) e o R2 deverá ser o BDR. O R3 deverá ser DROTHER.

Para a área 1 o R4 deverá ser o Designated Router (DR) e o R3 deverá ser o BDR. O R2 deverá ser DROTHER.

3– Exemplos de Configurações dos Roteadores

Exemplo 1: roteamento OSPF

Configurar o roteamento OSPF pelo comando “router ospf processo”, onde o processo é um número do processo OSPF.

O roteador também possui um router ID único que geralmente é a interface loopback ou então o maior endereço IP do roteador. Para adicionar interfaces deve-se usar o comando “network área”. Um roteador pode ter interfaces em áreas distintas, define-se cada área pelo comando network. Para definir a prioridade de um roteador ser DR ou BDR em uma rede OSPF, usa-se o comando “ip ospf priority n” na interface broadcast onde o “n” é um valor de prioridade onde quanto maior, melhor. Se usarmos o “0” o

roteador nunca se elegerá como DR ou BDR. Nos roteadores eleitos a serem DR deve-se utilizar o valor 16 (máximo), nos roteadores BDR foi utilizado o 12 e para o DROTHER utilizado “0”.

Comandos importantes de verificação

```
R4# sh ip ospf neighbor
```

```
R1# show ip ospf interface
```

Configuração

R1	**R3**
interface FastEthernet0/0 no shut ip address 100.100.100.1 255.255.255.0 exit ip ospf priority 255 router ospf 1 router-id 1.1.1.1 network 100.100.100.0 0.0.0.255 area 0	interface FastEthernet0/0 no shut ip address 100.100.100.3 255.255.255.0 ip ospf priority 0 interface FastEthernet1/0 no shut ip address 200.200.200.3 255.255.255.0 ip ospf priority 200 router ospf 1 router-id 3.3.3.3 network 100.100.100.0 0.0.0.255 area 0 network 200.200.200.0 0.0.0.255 area 1
R2	**R4**
interface FastEthernet0/0 no shut ip address 100.100.100.2 255.255.255.0 ip ospf priority 200 exit	interface FastEthernet0/0 no shut ip address 200.200.200.4 255.255.255.0 ip ospf priority 255 router ospf 1

interface FastEthernet1/0 no shut ip address 200.200.200.2 255.255.255.0 ip ospf priority 0 router ospf 1 router-id 2.2.2.2 network 100.100.100.0 0.0.0.255 area 0 network 200.200.200.0 0.0.0.255 area 1	router-id 4.4.4.4 network 200.200.200.0 0.0.0.255 area 1

Siglas

DR: roteador designado.

BDR: roteador designado de backup.

DROther: não dr e não bdr.

Verificações

```
show ip ospf neighbor.

R1#show ip ospf neighbor

R2#show ip ospf neighbor

R3#show ip ospf neighbor

R4#show ip ospf neighbor
```

Relatórios dos comandos "**Show ip ospf interface**" dos roteadores R1 e R2.

```
R1#show ip ospf interface

R2#show ip ospf interface
```

```
R1#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
2.2.2.2           0   FULL/DROTHER    00:00:30    100.100.100.2   FastEthernet0/
0
3.3.3.3           0   FULL/DROTHER    00:00:30    100.100.100.3   FastEthernet0/
0
R1#
```

```
R2#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
1.1.1.1         255   FULL/DR         00:00:30    100.100.100.1   FastEthernet0/
0
3.3.3.3           0   2WAY/DROTHER    00:00:30    100.100.100.3   FastEthernet0/
0
4.4.4.4         255   FULL/DR         00:00:30    200.200.200.4   FastEthernet1/
0
3.3.3.3         200   FULL/BDR        00:00:30    200.200.200.3   FastEthernet1/
0
R2#
```

```
R3#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
2.2.2.2           0   2WAY/DROTHER    00:00:39    100.100.100.2   FastEthernet0/
0
1.1.1.1         255   FULL/DR         00:00:39    100.100.100.1   FastEthernet0/
0
2.2.2.2           1   FULL/DROTHER    00:00:39    200.200.200.2   FastEthernet1/
0
4.4.4.4         255   FULL/DR         00:00:39    200.200.200.4   FastEthernet1/
0
R3#
```

```
R4#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
3.3.3.3         200   FULL/BDR        00:00:31    200.200.200.3   FastEthernet0/
0
2.2.2.2           1   FULL/DROTHER    00:00:31    200.200.200.2   FastEthernet0/
0
R4#
```

```
R4#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
3.3.3.3         200   FULL/BDR        00:00:31    200.200.200.3   FastEthernet0/
0
2.2.2.2           1   FULL/DROTHER    00:00:31    200.200.200.2   FastEthernet0/
0
R4#
```

Relatório do comando "Show ip ospf interface" do roteador R1.

```
R1#show ip ospf interface
FastEthernet0/0 is up, line protocol is up
  Internet address is 100.100.100.1/24, Area 0
  Process ID 1, Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 255
  Designated Router (ID) 1.1.1.1, Interface address 100.100.100.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:00
  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 2, Adjacent neighbor count is 2
    Adjacent with neighbor 2.2.2.2
    Adjacent with neighbor 3.3.3.3
  Suppress hello for 0 neighbor(s)
R1#
```

Relatório do comando "Show ip ospf interface" do roteador R2.

```
R2#show ip ospf interface
FastEthernet0/0 is up, line protocol is up
  Internet address is 100.100.100.2/24, Area 0
  Process ID 1, Router ID 2.2.2.2, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DROTHER, Priority 0
  Designated Router (ID) 1.1.1.1, Interface address 100.100.100.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:00
  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 2, Adjacent neighbor count is 1
    Adjacent with neighbor 1.1.1.1  (Designated Router)
  Suppress hello for 0 neighbor(s)
FastEthernet1/0 is up, line protocol is up
  Internet address is 200.200.200.2/24, Area 1
  Process ID 1, Router ID 2.2.2.2, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DROTHER, Priority 1
  Designated Router (ID) 4.4.4.4, Interface address 200.200.200.4
  Backup Designated Router (ID) 3.3.3.3, Interface address 200.200.200.3
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:00
  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 2, Adjacent neighbor count is 2
    Adjacent with neighbor 4.4.4.4  (Designated Router)
    Adjacent with neighbor 3.3.3.3  (Backup Designated Router)
  Suppress hello for 0 neighbor(s)
R2#
```

Exemplo 2: Configuração de Roteamento Frame Relay

Funcionamento dos DLCIs em uma rede Frame Relay

Configuração de um número DLCI para se associar a uma interface:

Router (config-if)# frame relay interface-dlci 16

Mapeamento IP x DCLI

Router(config)# int s0

Router(config-if)# encap frame

Router(config-if)#int s0.16 multipoint

Router(config-if)#no frame-relay inverse-arp

Router (config-if)#ip address 172.16.30.1 255.255.255.0

Router (config-if)#frame-relay map ip 172.16.30.17 17 broadcast

Router (config-if)#frame-relay map ip 172.16.30.18 18 broadcast

Router (config-if)#frame-relay map ip 172.16.30.19 19 broadcast

4. REDISTRIBUIÇÃO DE ROTEAMENTOS

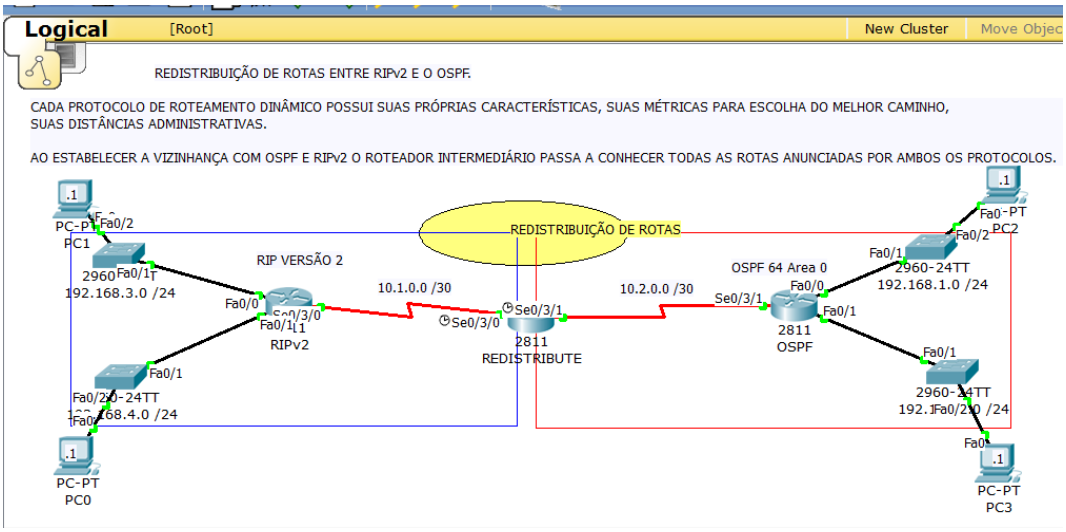
O uso de um protocolo de roteamento para anunciar rotas que são aprendidas por outro protocolo de roteamento, rotas estáticas ou rotas diretamente conectadas, é chamado de **redistribuição de rotas**.

Conforme Brito (2012), o ideal é ter apenas um protocolo de roteamento em toda a rede, porém muitas vezes isso não é possível devido a inúmeros fatores, como por exemplo, a fusão de empresas, múltiplos departamentos gerenciados por vários administradores de rede, ambientes com equipamentos de diversos fabricantes e etc. Por esses motivos ter múltiplos protocolos de roteamento é geralmente comum e muitas vezes faz-se necessário redistribuir as rotas aprendidas por um ou outro protocolo.

As diferenças nas características dos protocolos de roteamento, como métricas, distâncias administrativas, se são classful ou classless podem afetar a redistribuição. Essas diferenças devem ser levadas em consideração para ter sucesso nas redistribuições de rotas.

Ao redistribuir informações de rotas de um protocolo para outro, lembre-se que as métricas de cada protocolo desempenham um papel importante na redistribuição. Cada protocolo usa diferentes métricas. Por exemplo, As métricas do RIP são baseadas em contagem de saltos, mas EIGRP usam uma composição de métricas baseadas em largura de banda (Bandwidth), carga (Load), atraso (Delay), confiabilidade (Reliability) e MTU (Maximum Transmission Unit), porém bandwidth e delay são os únicos utilizados por padrão. O mneumônico “Boa Leitura Do Ricardo Meira” nos ajuda a lembrar desses parâmetros.

Ao redistribuir rotas é necessário definir a métrica legível ao protocolo que irá receber essas rotas. Existem dois métodos para definir métricas no processo de redistribuição. Vamos admitir o cenário a seguir.



Cenário para redistribuição de rotas.
Fonte: O Autor, 2015

Ativação do protocolo RIPv2:

```
router rip
version 2
network 10.0.0.0
network 192.168.3.0
network 192.168.4.0
no auto-summary
```

Ativação do protocol OSPF com número do processo igual a 64.

```
router ospf 64
network 192.168.1.0 0.0.0.255 area 0
network 192.168.2.0 0.0.0.255 area 0
network 10.2.0.0 0.0.0.3 area 0
```

Redistribuição dos protocolos. Inicialmente com o OSPF:

```
router ospf 64
redistribute rip subnets
network 10.2.0.0 0.0.0.3 area 0
```

Agora a redistribuição do protocolo RIPv2:

```
router rip
version 2
redistribute ospf 64 metric 10
network 10.0.0.0
no auto-summary
```

Note que na configuração do rip há necessidade de definir o tipo da métrica e designá-la às sub-redes (característica do rip), ou utilize uma métrica padrão para todas as redistribuições (usando o comando ***default-metric,*** isto diminui o trabalho, porque elimina a necessidade de definir cada métrica separadamente):

```
router rip
version 2
redistribute static
redistribute ospf 1
default-metric 1
```

4.1 - Distância Administrativa

Se o roteador está rodando mais de um protocolo de roteamento e aprende uma nova rota para o mesmo destino usando dois protocolos de roteamento, então qual rota deve ser eleita a melhor rota? Cada protocolo usa sua própria métrica para determinar a melhor rota. Não é possível comparar rotas com diferentes tipos de métricas. A **distância administrativa** resolve esse problema.

Distâncias administrativas são atribuídas às rotas de origem de modo que a rota de origem preferida será escolhida como melhor caminho.

Distância administrativa ajuda na seleção de rotas entre os diferentes protocolos de roteamento, mas pode causar problemas para a redistribuição.

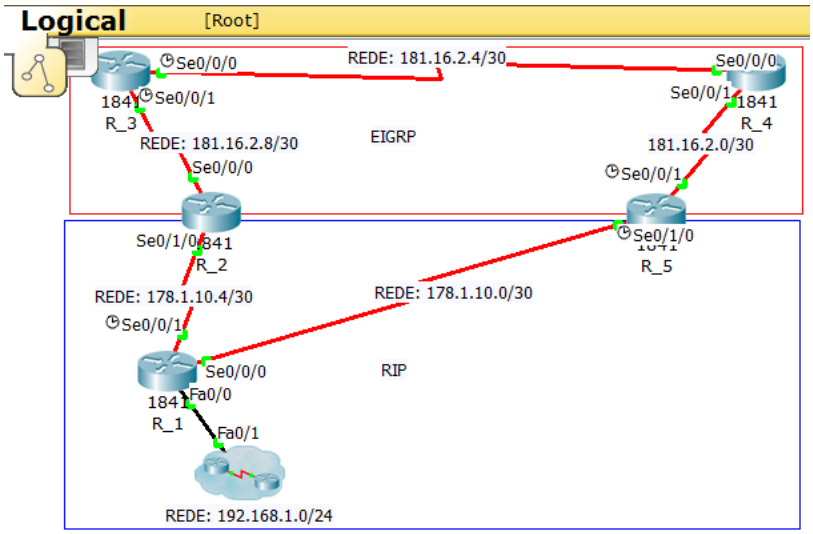
Estes **problemas** podem ser:

1) na forma de loop de roteamento;

2) problemas de convergência e

3) rotas ineficientes.

Veja abaixo uma topologia com a descrição de um possível problema.



Cenário para redistribuição de rotas.
Fonte: O Autor, 2015

Na topologia acima, se R1 está rodando RIP e R2 e R5 estão rodando RIP e EIGRP e redistribuindo RIP no EIGRP, então existe um problema em potencial. Por exemplo, R2 e R5 aprendem sobre a rede 192.168.1.0 através de R1 usando RIP. Este conhecimento é redistribuído no EIGRP. R2 aprende sobre a rede 192.168.1.0 através de R3. R5 aprende sobre esta rede a partir de R4 usando EIGRP. EIGRP tem um valor menor de distância administrativa que RIP (100 x 120); Por este motivo, as rotas EIGRP são as utilizadas na tabela de roteamento. Agora existe um potencial loop roteamento. Mesmo que haja qualquer mecanismo para ajudar a rede a ficar livre de loops entrarem em ação, ainda há um problema de convergência.

Se R2 e R5 estão também redistribuindo EIGRP no RIP (também conhecido como redistribuição mútua) e a rede 192.168.1.0 não estiver diretamente conectada a R1 (R1 está aprendendo de outro roteador acima dele), então existe o problema de R1 aprender sobre a rede 192.168.1.0 de R2 e R5 com uma melhor métrica que a original.

O mecanismo de redistribuição de rotas é proprietário nos roteadores Cisco. As regras para redistribuição em um roteador Cisco ditam que a rota redistribuída esteja presente na tabela de roteamento. Não é suficiente que a rota esteja presente na tabela de topologia ou na “database”. Rotas com uma menor distância administrativa (AD) sempre são instaladas na tabela de roteamento.

Por exemplo, se uma rota estática for redistribuída no EIGRP em R5, e o EIGRP consequentemente redistribuiu no RIP no mesmo roteador (R5), a rota estática não é redistribuída no RIP porque isto nunca esteve na tabela de roteamento do EIGRP. Isto é devido ao fato que rotas estáticas tem uma AD de 1 e rotas EIGRP terem AD de 90 e a rota estática estar instalada na tabela de roteamento. Para redistribuir a

rota estática no EIGRP em R5, é obrigatória a utilização do comando ***redistribute static*** nas configurações de roteamento do RIP (***router rip***).

Rota estática padrão

A rota estática padrão é aquela que enviará todos os pacotes por determinada interface de saída. Usamos este recurso quando nenhuma outra rota na tabela de roteamento corresponder ao endereço IP de destino ou quando um roteador tem somente outro roteador a ele conectado. Essa topologia é denominada rede raiz ou rede *stub*.

Para configurar uma rede estática padrão basta digitar no modo de configuração global:

Router1(config)#ip route 0.0.0.0 0.0.0.0 [interface de saída]

Em função do endereço e máscara compostos por zeros, esta rota também é chamada "*quad-zero*".

Há dois métodos de receber uma rota conectada.

1. uma interface é configurada com um endereço de IP e máscara, a sub-rede correspondente é considerada uma rota conectada.
2. uma rota estática é configurada com apenas uma interface de saída e não um IP de um vizinho (***next-hop***), isto é considerada uma rota estática.

Exemplo:

```
Router#conf t

Router(config)#ip route 10.0.77.0 255.255.255.0 ethernet 0/0

Router(config)#end

Router#show ip route static

10.0.0.0/24 is subnetted, 1 subnets

S 10.0.77.0 is directly connected, Ethernet0/0
```

Um comando ***network*** configurado no EIGRP, RIP ou que inclui (ou "cobre") qualquer um desses tipos de rotas conectadas inclui a sub-rede para anúncio.

Por exemplo, se uma interface tem o IP 10.0.23.1, máscara 255.255.255.0 e se a sub-rede 10.0.23.0/24 é uma rota conectada então será anunciada por um desses protocolos de roteamento quando o comando ***network*** for configurado conforme a seguir:

```
router rip | igrp # | eigrp #

network 10.0.0.0
```

Esta rota estática 10.0.77.0/24 é também anunciada por este protocolo de roteamento, porque é uma rota conectada e está “coberta” pelo segmento de rede.

4.3 - Sintaxe do Protocolo de Redistribuição: Exemplo

Conforme a Cisco Network Academy (2005), esta saída exemplo de comando exibe uma redistribuição no roteador configurado com o protocolo `EIGRP de rota estática, OSPF, RIP e IS-IS.`

```
Router igrp/eigrp1

network 131.108.0.0

redistribute static

redistribute ospf 1

redistribute rip

redistribute isis

default-metric 10000 100 255 1 1500
```

EIGRP precisam de cinco métricas quando redistribuem outros protocolos: Bandwidth, Load, Delay, Reliability e MTU, respectivamente. Veja um exemplo das métricas do IRGP.

Múltiplos processos do IGRP e do EIGRP podem rodar no mesmo roteador, com redistribuição de rotas entre eles. Por exemplo, IGRP1 e IGRP2 podem rodar no mesmo roteador. Porém, rodar dois processos de um protocolo no mesmo roteador é raramente necessário e pode consumir muito processador e muita memória.

A redistribuição de IGRP/EIGRP em outro processo IGRP/EIGRP não requer nenhuma conversão de métrica, não existe a necessidade de definir as métricas ou de utilizar o comando ***default-metric*** na redistribuição.

Uma redistribuição de rota estática recebe preferência sobre uma rota sumarizada porque a distância administrativa das rotas estáticas é 1 enquanto que a distância administrativa das rotas EIGRP sumarizadas é 5. Isto acontece quando uma rota estática é redistribuída com o uso do ***redistribite static*** sob o processo EIGRP e o processo EIGRP tem a rota padrão.

Exemplo

Metric:	**Value**
Bandwidth:	Kbps; 10000 para Ethernet
Delay:	Em 10µseg; para Ethernet é 100x10 microseg = 1ms
Reliability:	255 = 100% de confiabilidade
Load:	Carga efetiva numérica de 0 a 255 (255 =100% de carga)
MTU:	Menor MTU da rota; Para Ethernet = 1500 bytes

4.4 – Redistribuição do protocolo OSPF: exemplo

A saída dos comandos abaixo exibe a redistribuição de rotas estáticas, RIP, IGRP, EIGRP e IS-IS no processo OSPF.

router ospf 1

network 131.108.0.0 0.0.255.255 area 0

redistribute static metric 200 subnets

redistribute rip metric 200 subnets

redistribute igrp 1 metric 100 subnets

redistribute eigrp 1 metric 100 subnets

redistribute isis metric 10 subnets

A métrica do OSPF é um valor de custo baseado no cálculo: "10^8/ bandwidth do link em bits/seg.". Por exemplo, o custo OSPF para um link Ethernet é 10, pois, $10^8/10^7 = 10$.

Se a métrica não for especificada no OSPF, ele a define com o padrão 20 para todos os protocolos, exceto rotas BGP que tem métrica 1.

Se trabalhar com uma rede dividida em sub-redes, há que se utilizar o comando ***subnet*** para redistribuir no OSFP. Sem esse comando o OSPF irá redistribuir somente a maior rede.

É possível executar mais que um processo OSPF em um mesmo roteador. Porém, como dito acima, executar mais de um processo do mesmo protocolo é raramente necessário e pode consumir muita memória e processamento.

Não há necessidade de definir métrica alguma ou usar o comando ***default-metric*** quando redistribuir um processo OSPF a outro processo OSPF.

4.5 - Redistribuição do protocolo RIP: exemplo

Conforme Brito (2012), os comandos referidos abaixo se destinam tanto ao RIPv1 quanto ao RIPv2.

A saída abaixo exibe redistribuição das rotas estáticas, IGRP, EIGRP, OSPF, e IS-IS no protocolo RIP.

router rip

network 131.108.0.0

redistribute static

redistribute igrp 1

redistribute eigrp 1

redistribute ospf 1

redistribute isis

default-metric 1

A métrica do RIP é composta de contagens de saltos e o valor máximo válido da métrica é 15. Qualquer valor acima de 15 é considerado infinito, pode-se usar o valor 16 para descrever uma métrica inalcançável no RIP. Quando se distribui um protocolo no RIP a Cisco recomenda que você use uma métrica baixa como 1. Uma métrica alta como 10, limita o RIP ainda mais. Se você define a métrica 10 para redistribuir as rotas no RIP essas rotas somente poderão ser anunciadas para os próximos 5 saltos seguintes, ponto em que a métrica excede 15 saltos. Por definição, com a métrica 1 você habilita a rota a dar o número máximo de saltos possíveis em um domínio RIP. Mas, isto aumenta a possibilidade de acontecer loop de roteamento caso existam múltiplos pontos de redistribuição e um roteador aprenda sobre a rede com uma métrica melhor que o ponto de distribuição original, como explicado anteriormente. Portanto, deve-se garantir que a métrica não seja muito alta, para que esta seja anunciada para todos os roteadores, nem muito baixa, levando a loop de roteamento quando há múltiplos pontos de redistribuição.

Resumo

O protocolo OSPF (Open Shortest Path First) é um protocolo IGP (Interior Gateway Protocol), projetado para uso intra-AS (Sistema Autônomo). É definido pela RFC 2328.

O protocolo OSPF foi desenvolvido para atender às necessidades da comunidade Internet que demandavam um protocolo IGP eficiente, não proprietário e Interoperável com outros protocolos de roteamento.

OSPF baseia-se na tecnologia “link-state”, diferente e bem mais avançada que a tecnologia utilizada em protocolos vetoriais, como o RIP, que utiliza o algoritmo Bellman-Ford para cálculo da melhor rota.

Em uma rede OSPF o melhor caminho (o mais curto) é calculado aplicando-se o algoritmo Dijkstra. O algoritmo coloca o roteador na raiz da topologia e calcula o melhor caminho para um destino baseando-se no custo cumulativo até o destino em questão. Cada roteador na rede terá uma visão única da topologia lógica, ainda que todos os roteadores utilizem a mesma base de dados link-state (link-state database).

O custo, métrica de uma interface OSPF, é uma indicação do overhead necessário para o envio de pacotes através desta interface. O custo de uma interface é inversamente proporcional à largura de banda desta interface. Uma largura de banda maior indica um custo menor. Por exemplo, se a interface é fastethernet (100Mb) então o Custo = 100.000.000/Banda (bps). Por este motivo, é importante a correta configuração do parâmetro Bandwidth em interfaces rodando OSPF.

Quanto à tecnologia Frame Relay, é uma tecnologia de comunicação de dados de alta velocidade. Combina as funcionalidades de multiplexação estatística e compartilhamento de portas do X25 com as características de alta velocidade e baixo atraso (delay) dos circuitos TDM. É um serviço de pacotes que organiza as informações em pacotes de dados com endereço de destino definido.

É definido nas camadas Física (Camada 1) e de Enlace (Camada 2), interconecta duas ou mais LANs.

Usa técnica de multiplexação e o campo de CRC do frame para detectar erros na transmissão. Para maximizar a largura de banda, não os corrige, passando esta tarefa para as camadas superiores.

Frame Relay provê uma comunicação entre dispositivos DTEs através de dispositivos DCEs. Por operar na camada 2, qualquer informação de camada de rede (IP, IPX, AppleTalk), é totalmente irrelevante para ele.

Usa o artifício do PVC (Permanent Virtual Circuit). Criado o circuito virtual os dispositivos se enxergam como se estivessem conectados diretamente. Esses circuitos são conexões lógicas criadas por dispositivos DTEs através de uma rede *packet-switched* e identificadas por um *DLCI (Data Link Connection Identifier)* similar ao MAC Address nas redes Ethernet. Existe outra derivação dos PVC, o *SVC (Switched Virtual Connection)* que são circuitos baseados em pacotes, não criando assim um circuito virtual permanente.

Funciona como propagador de informações através de uma rede de dados. Divide essas informações em frames (quadros) ou packets (pacotes). Cada frame carrega um endereço, usado pelos equipamentos da rede para determinar o seu destino. É um chaveamento de pacotes, por isso permite uma grande variedade de aplicações.

Finalmente, quanto à Redistribuição de Roteamentos, podemos dizer que para redistribuir rotas é necessário definir a métrica legível ao protocolo que irá receber essas rotas. As regras para redistribuição em um roteador Cisco ditam que a rota redistribuída esteja presente na tabela de roteamento.

Ao redistribuir informações de rotas, de um protocolo para outro, cada protocolo desempenha um papel importante na redistribuição. Cada um usa diferentes métricas. As métricas do RIP são baseadas em contagem de saltos, mas IGRP e EIGRP usam uma composição de métricas baseadas em largura de banda (Bandwidth), carga (Load), atraso (Delay), confiabilidade (Reliability) e MTU (Maximum Transmission Unit), porém bandwidth e delay são os únicos utilizados por padrão. O mneumônico “Boa Leitura Do Ricardo Meira” nos ajuda a lembrar desses parâmetros.

Ao redistribuir rotas é necessário definir a métrica legível ao protocolo que irá receber essas rotas. Existem dois métodos para definir métricas no processo de redistribuição.

Não é suficiente que a rota esteja presente na tabela de topologia ou na “database”. Rotas com uma menor distância administrativa (AD) sempre são instaladas na tabela de roteamento. Por exemplo, se uma rota estática for redistribuída no em R5, e o IGRP consequentemente redistribuiu no RIP no mesmo roteador (R5), a rota estática não é redistribuída no RIP porque isto nunca esteve na tabela de roteamento do IGRP. Isto é devido ao fato que rotas estáticas tem uma AD de 1 e rotas IGRP terem AD de 100 e a rota estática estar instalada na tabela de roteamento. Para redistribuir a rota estática no IGRP em R5, é obrigatória a utilização do comando ***redistribute static*** nas configurações de roteamento do RIP (***router rip***).

O comportamento padrão para os protocolos de roteamento dinâmico RIP, IGRP e EIGRP é de anunciar as rotas diretamente conectadas quando um seguimento de rede sob um protocolo de roteamento inclui a interface conectada da sub-rede.