

Treinamento

MTCRE



Instrutor



Redes Brasil

Leonardo Vieira

"leomikrotik"

- 27 Anos experiência com redes e TI.
- Em 2009 iniciei com MikroTik
- Contract TI / Contract Cloud / Redes Brasil
- Palestrante MUM – Brasil
- Treinamentos Oficiais MikroTik



[Facebook.com/Leonardo.mikrotik](https://www.facebook.com/Leonardo.mikrotik)

[linkedin.com/in/albuquerqueleonardo/](https://www.linkedin.com/in/albuquerqueleonardo/)



@leomikrotik



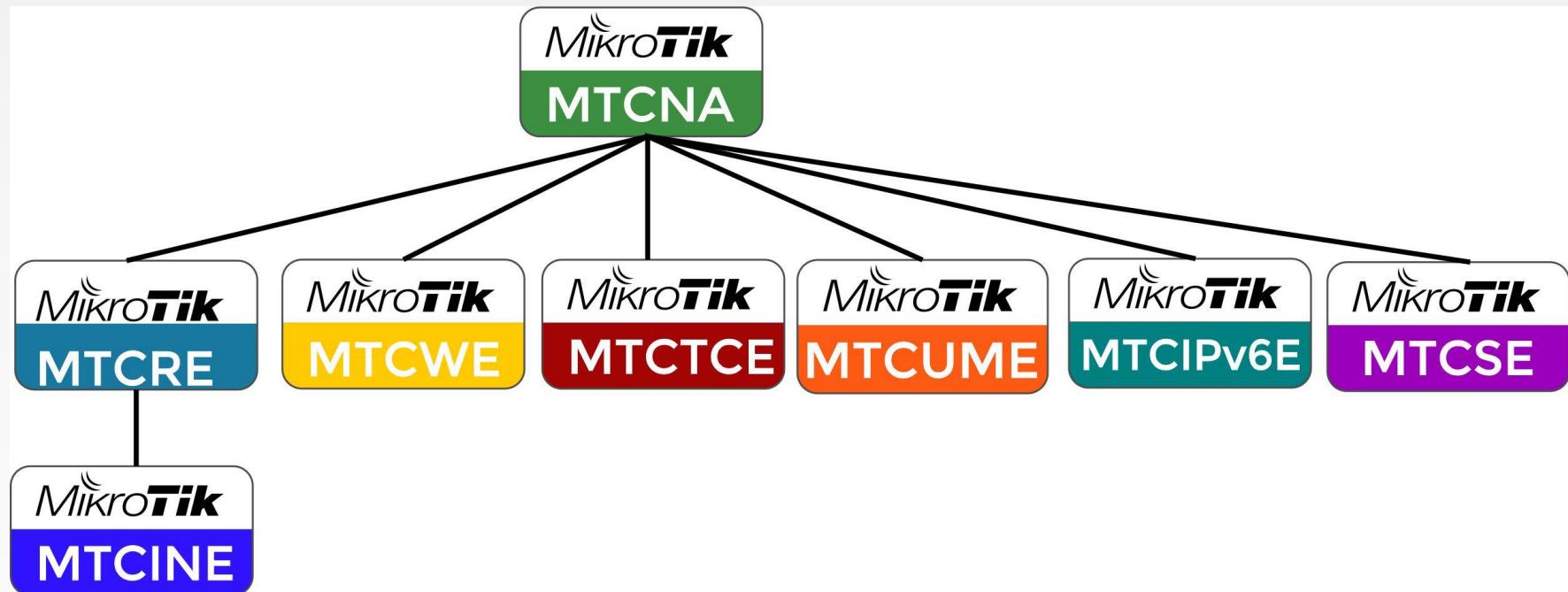
youtube.com/leomikrotik



facebook.com/contractti/



Certificações



Cronograma

Redes Brasil

- Treinamento das 09:00hs às 18:00hs
- Almoço as 12:00hs – 1:30 hora de duração
- Coffe break as 15:30hs



Tópicos do treinamento

- Vantagens e desvantagens de uma rede em bridge.
- Entendo como funcionada roteamento.
- Como planejar uma rede roteada.
- Roteamento estático X OSPF
- Implementando OSPF
- OSPF avançado
- Túneis,VPNs e considerações finais.

Importante

- **Curso oficial:** Proibido ser filmado ou gravado.
- **Celular:** Desligado ou em modo silencioso.
- **Perguntas:** Sempre bem vindas.
- **Internet:** Evite o uso inapropriado.
- **Aprendizado:** Busque absorver conceitos.

- **Evite conversas paralelas.**



Apresente-se a turma

- Diga seu nome.
- Com que trabalha.
- Seu conhecimento sobre o RouterOS.
- Seu conhecimento com redes.



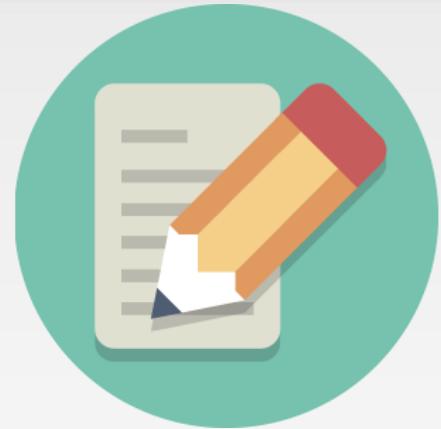
Objetivos do curso

- Abordar todos os tópicos necessários para o exame de certificação MTCRE.
- Prover um visão geral sobre roteamento e túneis.
- Fazer uma abordagem simples e objetiva de como planejar e implementar uma rede roteada com foco em segurança e performance.



Prova de certificação - MTCRE

- 25 questões;
- Prova em Inglês;
- 1 hora de duração (média 2,4 minutos por questão);
- Nota igual ou superior a 60% para ser aprovado.
- Pode consultar roteador, anotações e sites da MikroTik.
- Pode usar tradutor.
- É necessário ter o feito e passado no MTCNA anteriormente;



Certificado



Redes Brasil

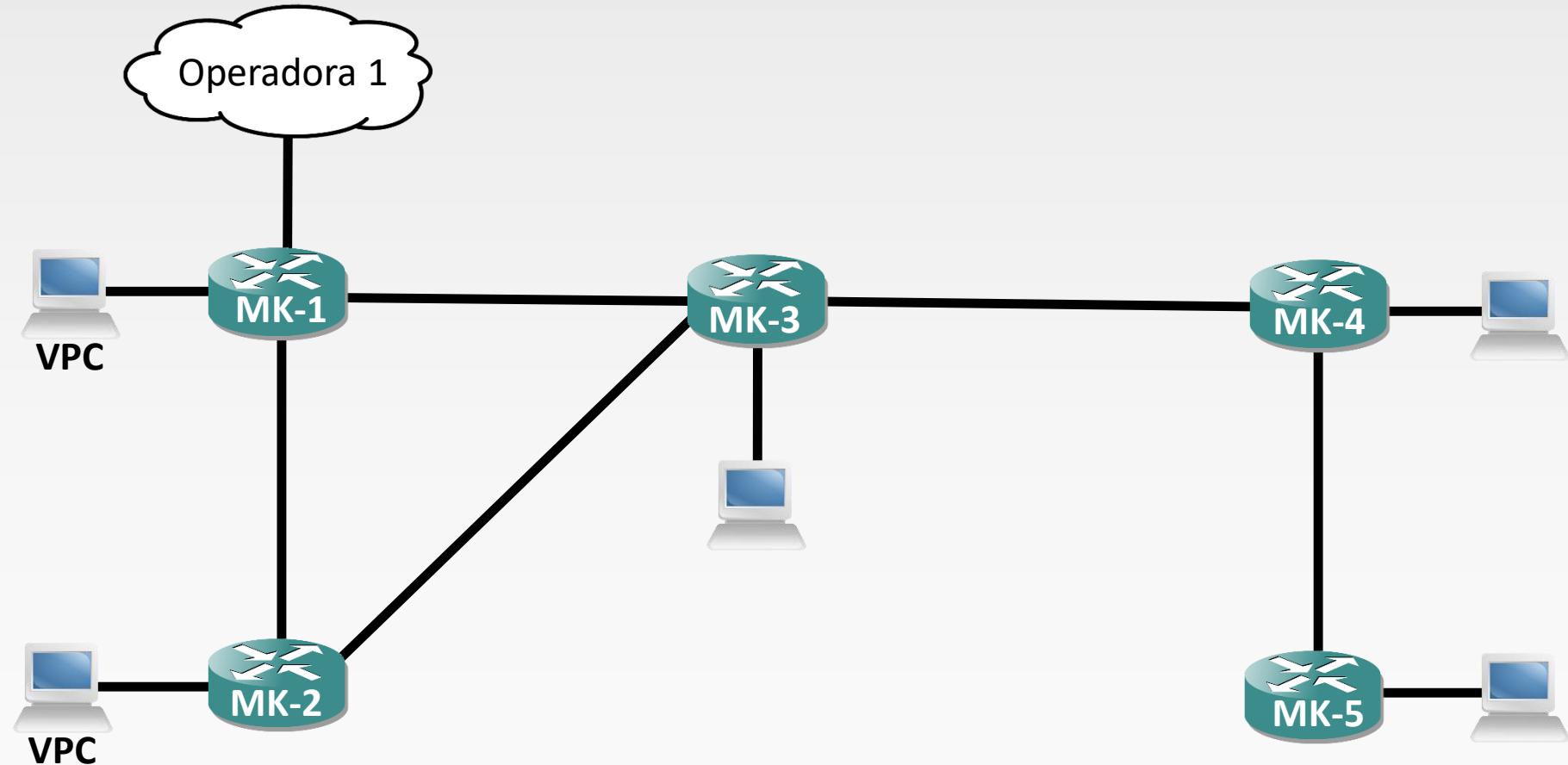
- Todos os alunos irão receber o certificado de participação por e-mail.
- Aluno que fizerem a prova de certificação e tiverem nota igual ou maior que 60% receberão o certificado da MikroTik que será gerado dentro do próprio site do fabricante.





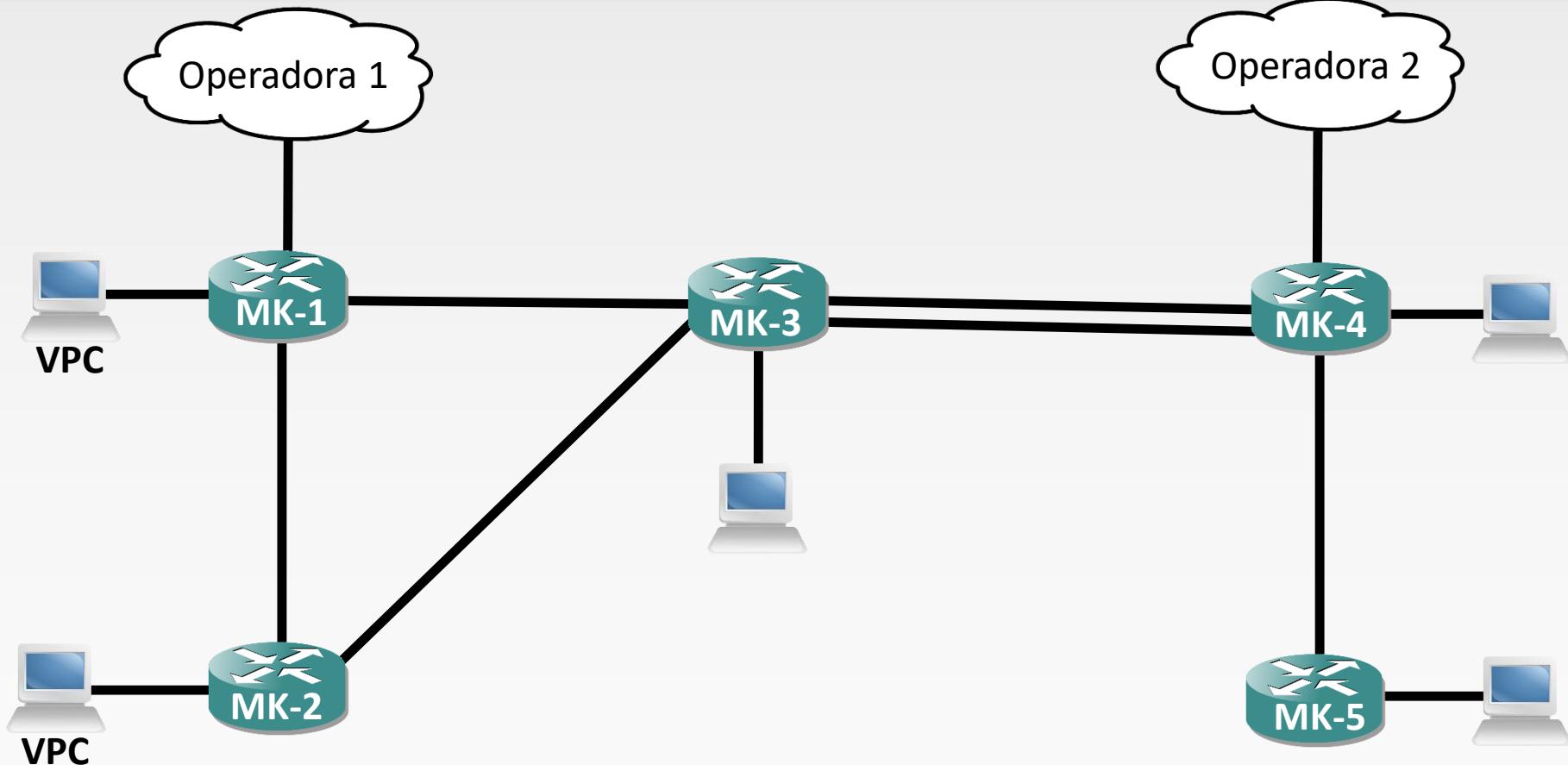
Topologia da rede em bridge

➤ Lembre-se de seu número X



Topologia da rede roteada

➤ Lembre-se de seu número X





Acessando os roteadores



WinBox v3.12 (Addresses)

File Tools

Connect To: 10.7.7.4 Keep Password
 Secure Mode
 Autosave Session
 Open In New Window

Login: admin
Password:
Session: <own>
Note:
Group:

RoMON Agent: 10.7.7.4

Add/Set Connect To RoMON Connect

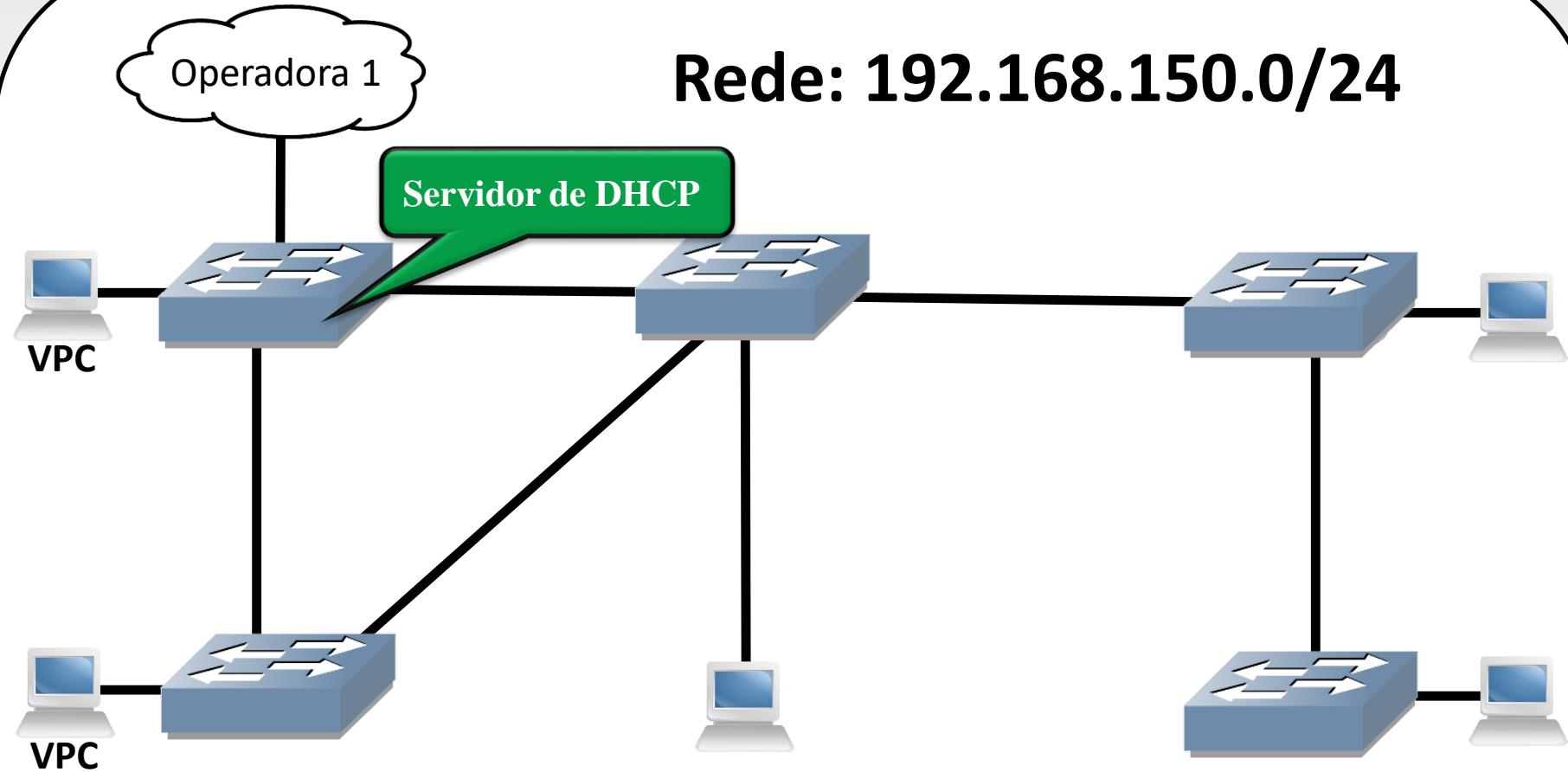
Managed RoMON Neighbors

Address C. H. P. ... Identity Ve... Board

50:0F:0E:42:00:01	2.	1	5...	MK-02 - Aluno_15	6....	CHR
50:0F:0E:43:00:00	2.	1	5...	MK-03 - Aluno_15	6....	CHR
50:0F:0E:44:00:01	4.	2	5...	MK-04 - Aluno_15	6....	CHR
50:0F:0E:45:00:00	6.	3	5...	MK-05 - Aluno_15	6....	CHR

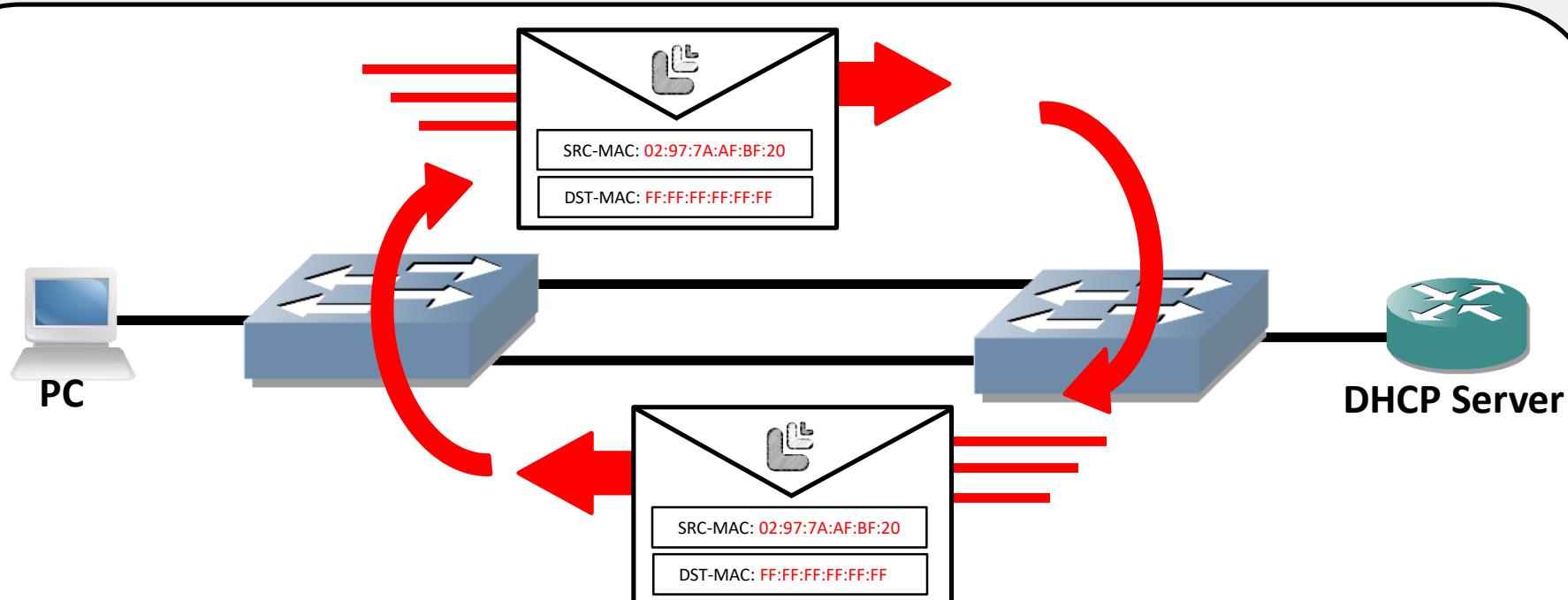


Topologia da rede em bridge



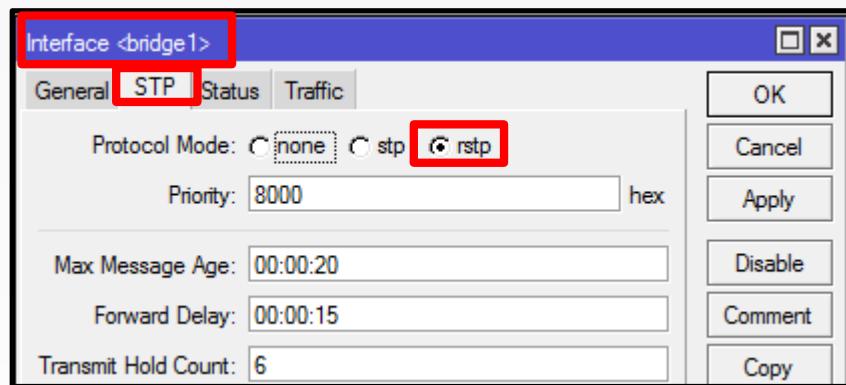
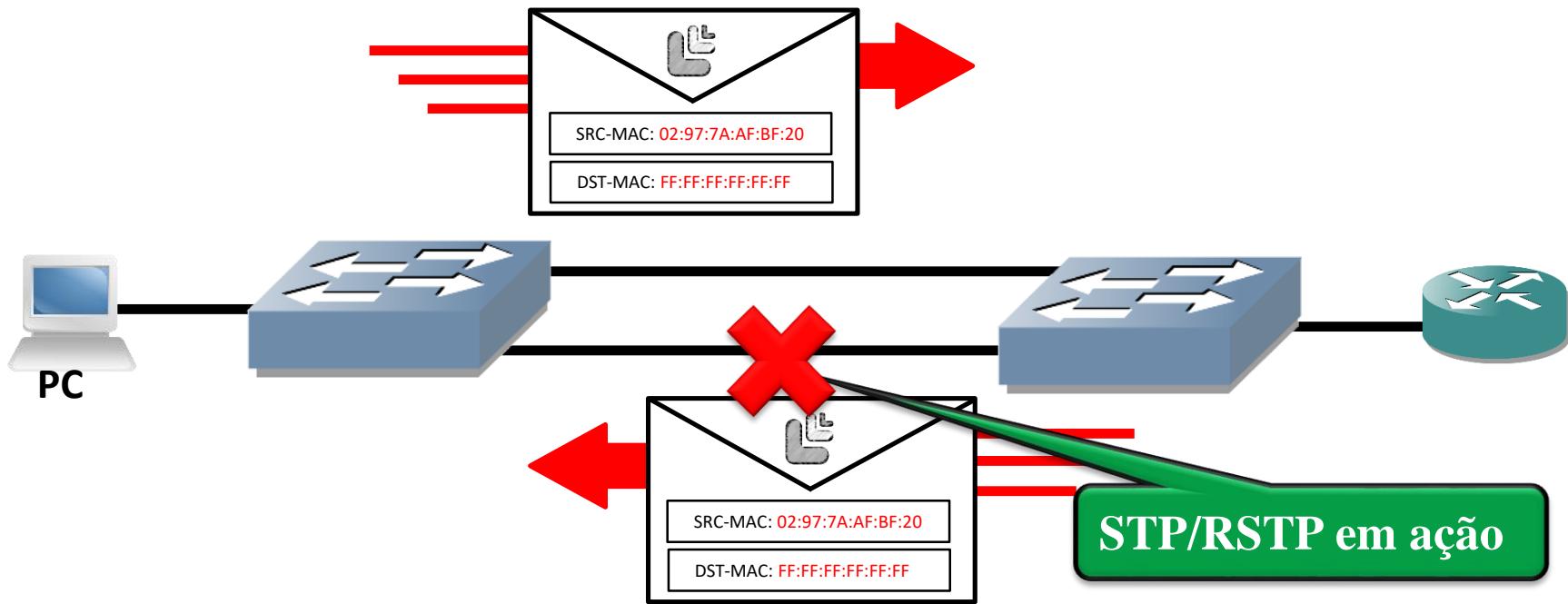
[Vídeo sobre a diferença entre bridges e switchs](#)

Loop de camada 2

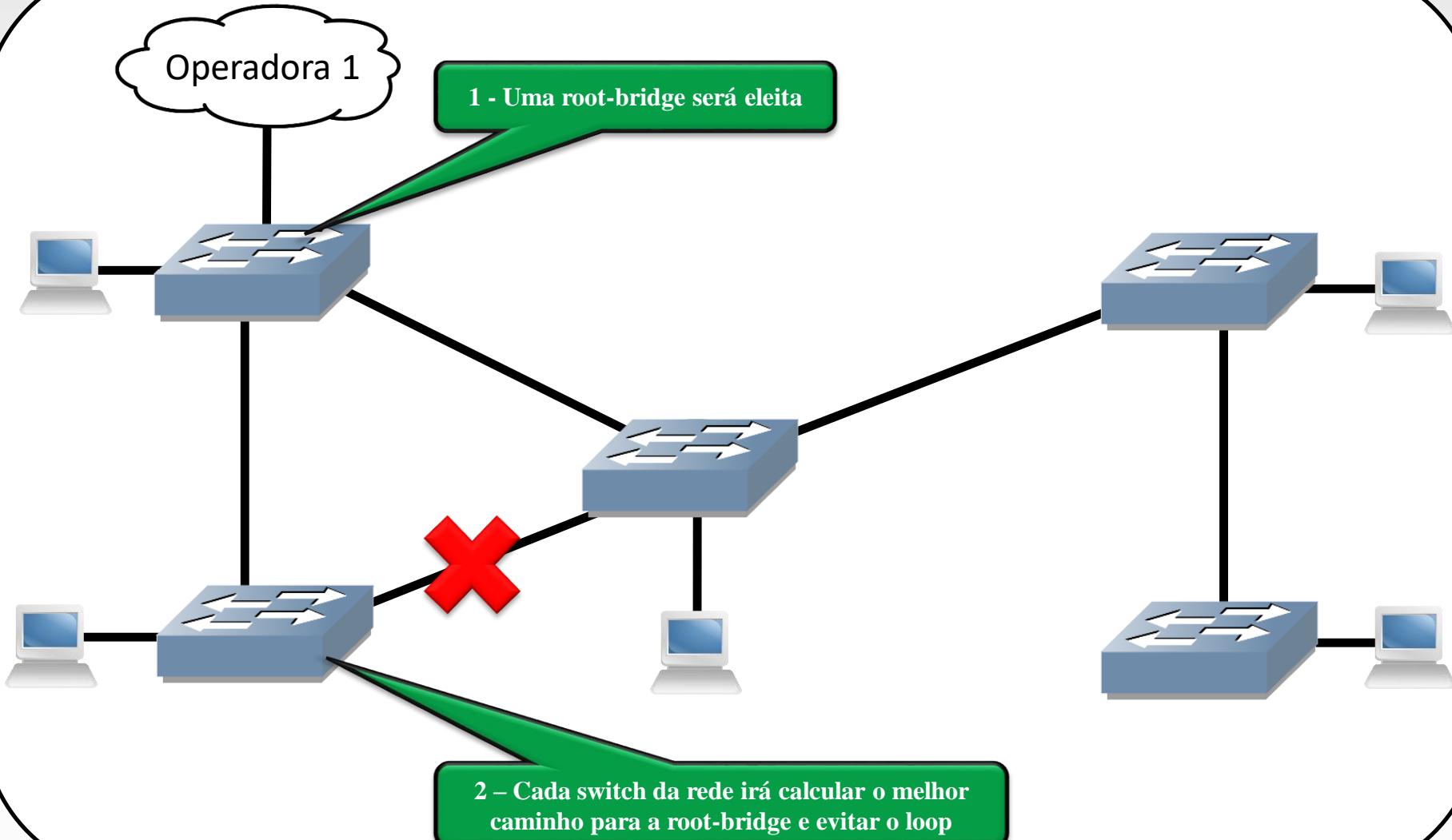




Como evitar loop de camada 2 ?



Funcionamento do STP



Eleição da root-bridge



Redes Brasil

The screenshot shows the Winbox interface for managing a bridge. On the left, a sidebar lists various network protocols: PPP, Mesh, IP, IPv6, MPLS, Routing, System, Queues, and Files. The 'Bridge' icon is selected and highlighted with a red box. The main window has tabs for 'Bridge', 'Ports', 'Filters', 'NAT', and 'Hosts'. The 'Bridge' tab is active. Below it, a sub-dialog titled 'Interface <bridge1>' shows the 'General' tab selected. Under 'Protocol Mode', the 'rstp' radio button is selected. The 'Priority' field is set to '8000' and is also highlighted with a red box. Other tabs in this dialog include 'STP', 'Status', and 'Traffic'. At the bottom right of the sub-dialog are 'OK', 'Cancel', and 'Apply' buttons.

O switch com menor priority será eleito a root-bridge

The screenshot shows the Winbox interface for managing a bridge. The 'Bridge' icon in the sidebar is highlighted with a red box. The main window has tabs for 'Bridge', 'Ports', 'Filters', 'NAT', and 'Hosts'. The 'Bridge' tab is active. Below it, a sub-dialog titled 'Interface <bridge1>' shows the 'General' tab selected. Under 'Root Bridge', the 'Root Bridge' checkbox is checked. The 'Root Bridge ID' field is set to '0x8000.00:00:AB:89:A4:09' and is highlighted with a red box. Other tabs in this dialog include 'STP', 'Status', and 'Traffic'. At the bottom right of the sub-dialog are 'OK', 'Cancel', 'Apply', 'Disable', 'Comment', and 'Copy' buttons. The 'Bridge' table at the top shows one entry for 'bridge1' with a priority of 65535 and a transmission rate of 63.8 kbps. The 'Neighbor List' table at the bottom shows four entries for switches MK-5, MK-4, MK-3, and MK-2, each with a MAC address and an identity column.

IP Address	MAC Address	Identity	Platform
10.40.40.5	00:00:AB:89:A4:09	MK-5	MikroTik
10.40.40.4	00:00:AB:8F:9E:09	MK-4	MikroTik
10.40.40.3	00:00:AB:94:9E:09	MK-3	MikroTik
10.40.40.2	00:00:AB:FE:82:09	MK-2	MikroTik

Em caso de empate do campo priority o switch com menor mac-address será eleito a root-bridge.

Eleição da root-bridge

No RouterOS, é possível definir qualquer valor para a prioridade entre 0 e 65535.

O padrão IEEE 802.1W informa que a prioridade deve ser de 4096 em 4096.

Para evitar problemas de incompatibilidade, recomenda-se usar somente estas prioridades HEX:
0, 4096, 8192, 12288, 16384, 20480, 24576, 28672,
32768, 36864, 40960, 45056, 49152, 53248, 57344,
61440

STP x RSTP

STP – Spanning Tree Protocol

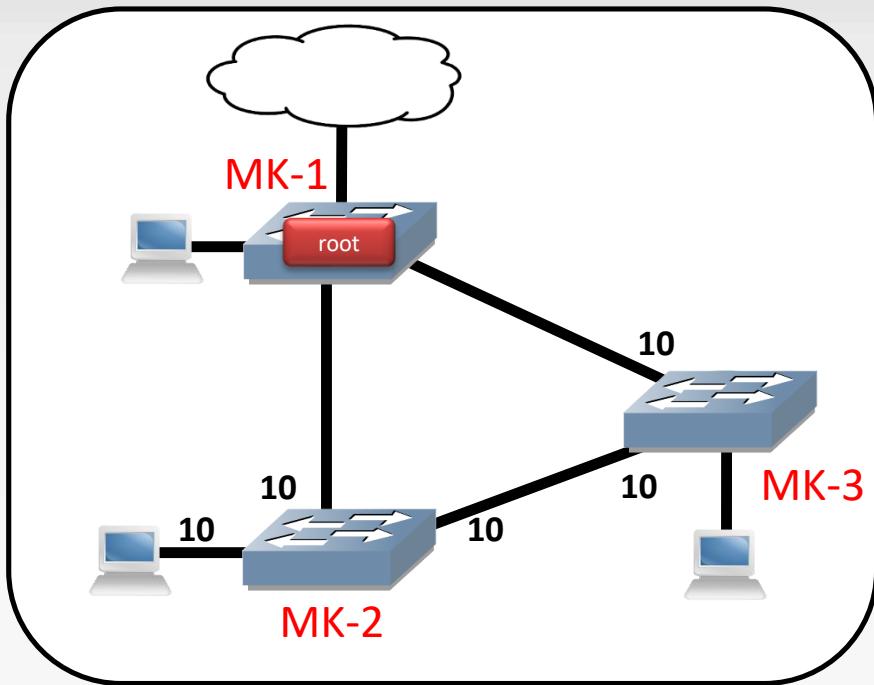
leva 50 seg para responder a mudança
de topologia da rede.

RSTP – Rapid Spanning Tree Protocol

mais rápido para convergência após a mudança
de topologia da rede. Menos de 10 seg.



Laboratório de STP

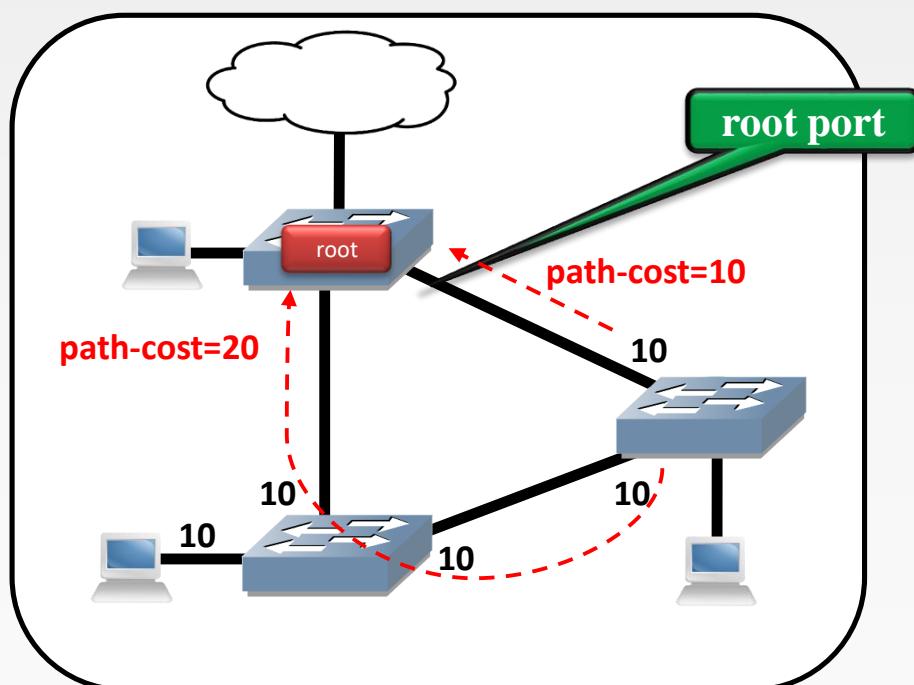
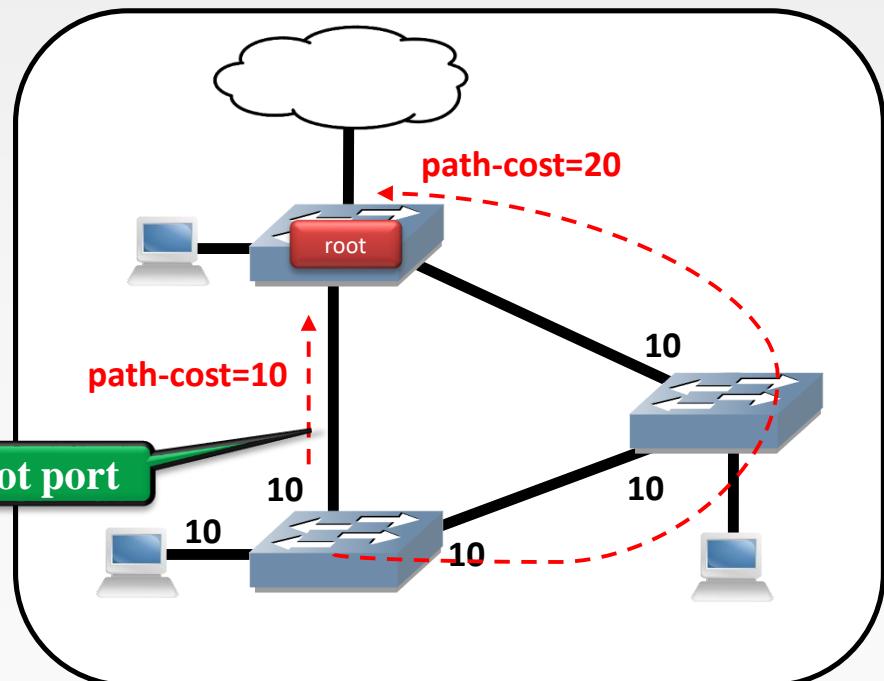


MK-1

Objetivo

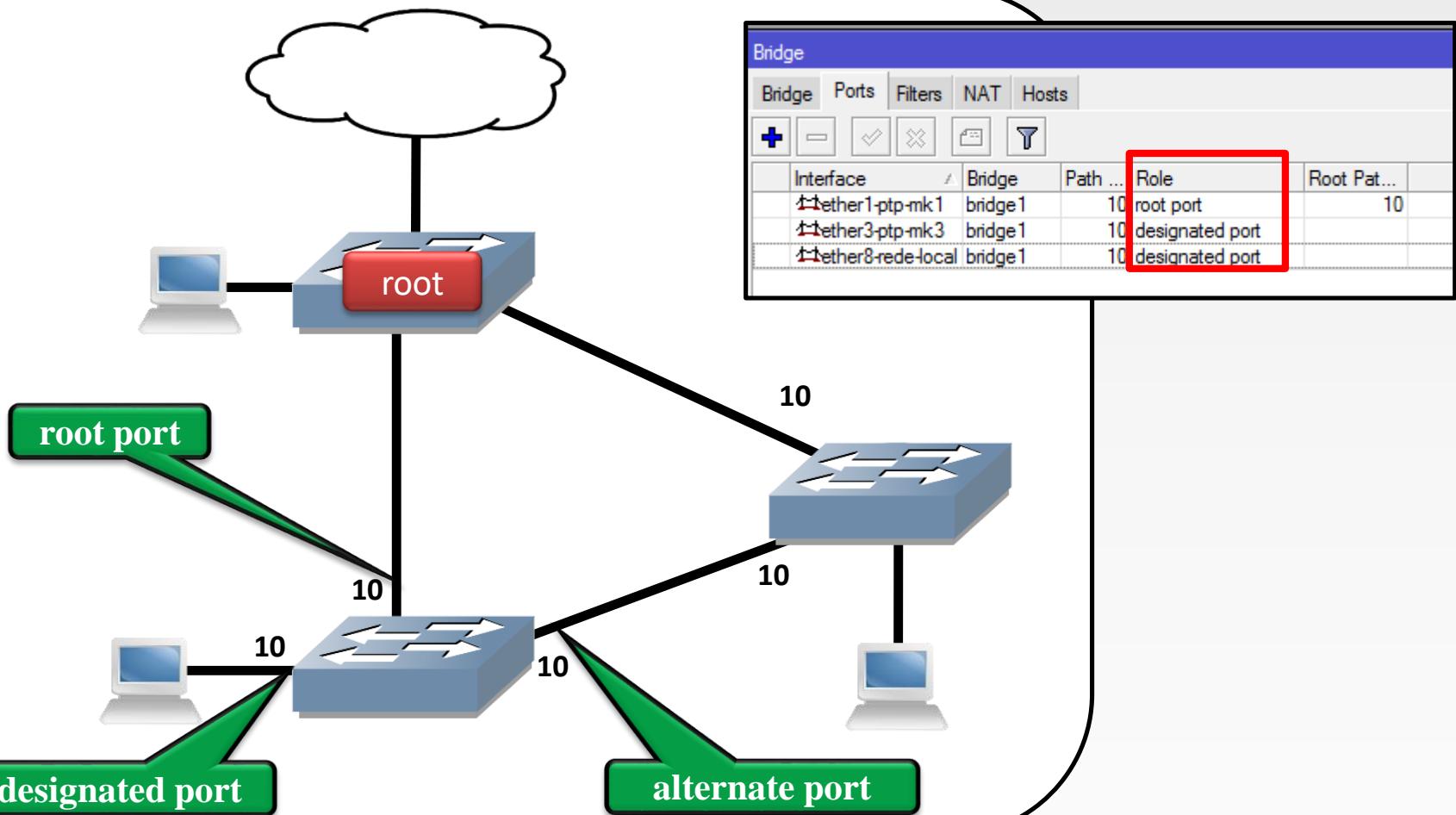
- 1 – Verifique qual equipamento foi eleito root-bridge da rede.
- 2 – Faça com que o MK-1 seja eleito como root-bridge.

Escolha da root port



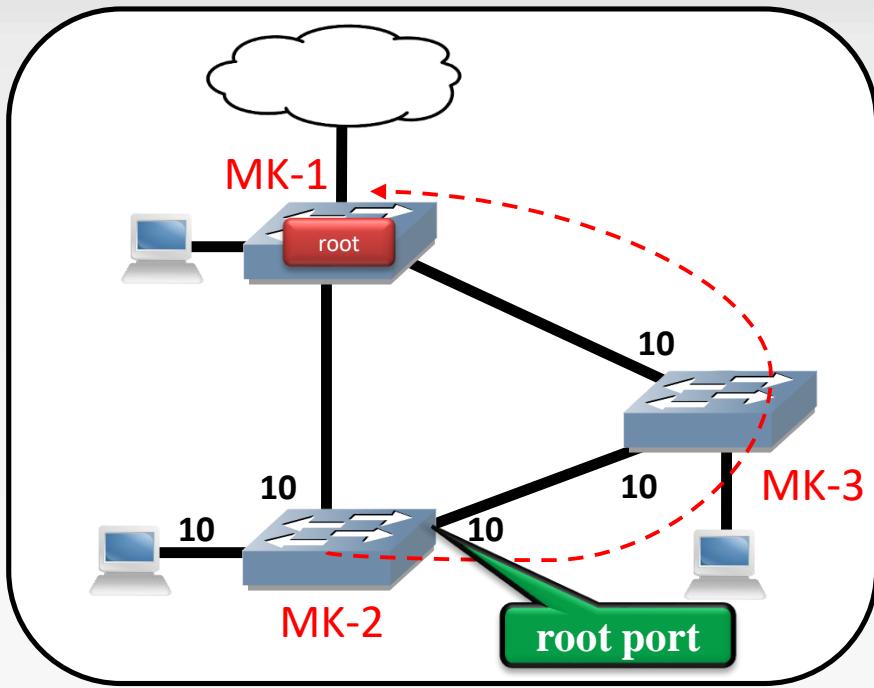
Status das portas no MK-2

Redes Brasil



Laboratório de STP

Redes Brasil



Objetivo

- 1 – Verifique qual é o caminho principal de MK-2 para MK-1.
- 2 – Altere as configurações para que o caminho principal fique como a imagem acima.

Observações do ambiente em bridge

- Todos os hosts ficarão no mesmo domínio de broadcast, logo estão na mesma rede.
- Caso não utilize filtros de bridge um host poderá “enxergar” todos os hosts da rede.
- A rede será mais vulnerável a ataques e erros.
- Comprometimento de redundância caso tenha mais de uma um ponto de interconexão com operadoras.

Planejamento de rede

Redes Brasil

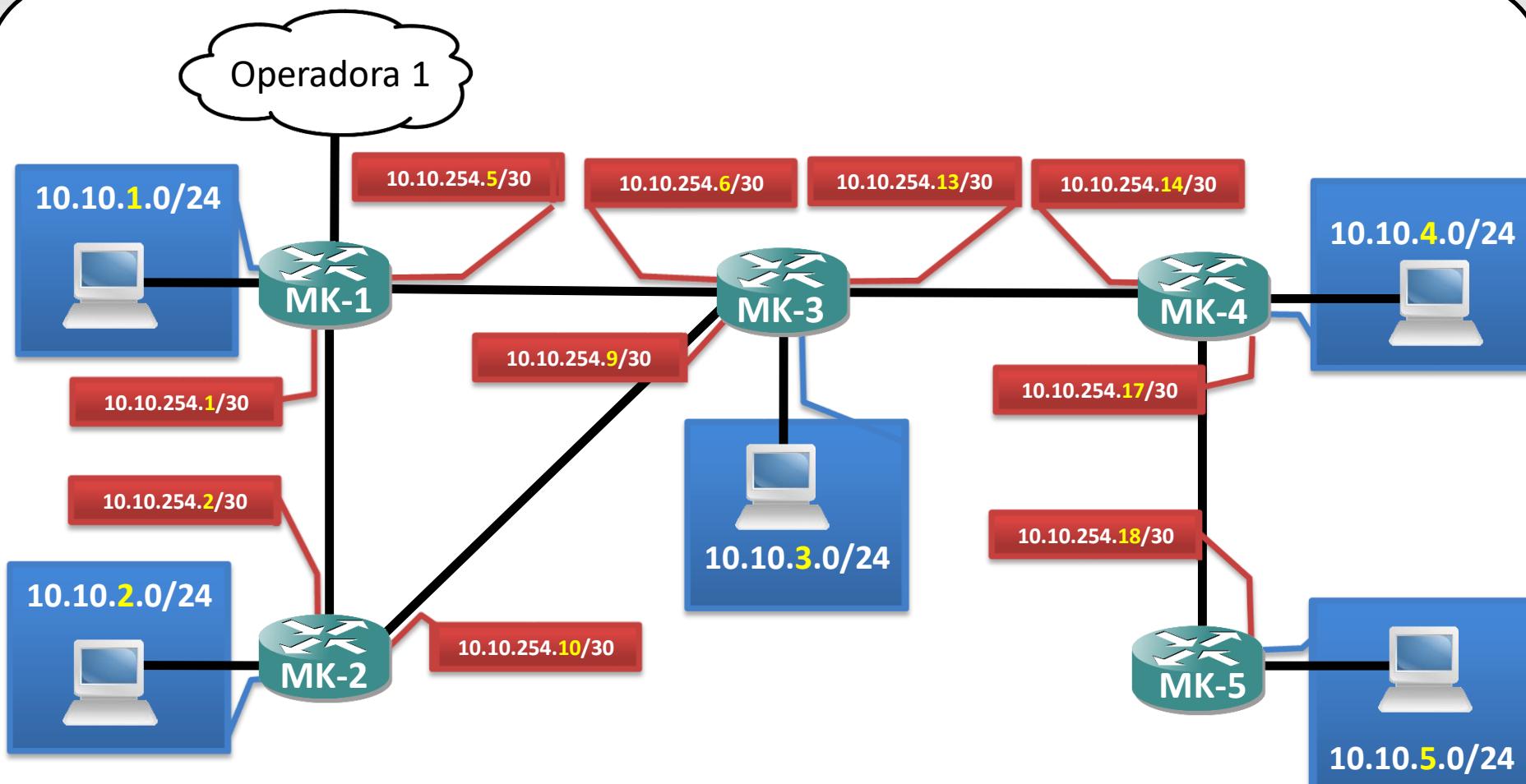
O que devo planejar?

Loopbacks

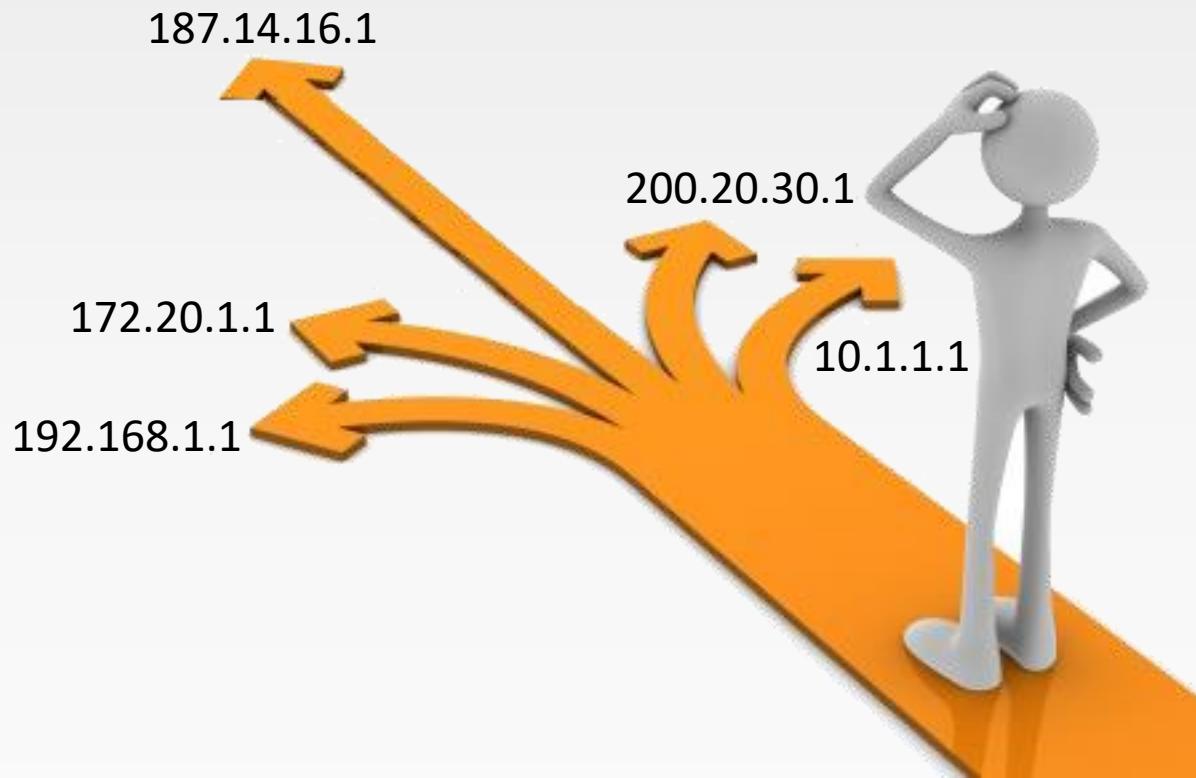
PTPs

Cientes finais

Endereçamento para rede roteada



Roteamento



Roteamento

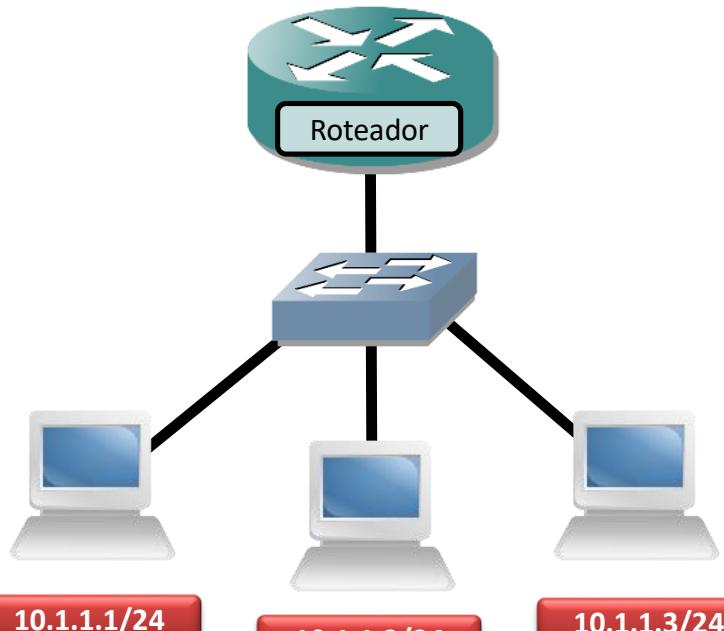
➤ O Mikrotik suporta:

- **Roteamento estático:** As rotas são criadas pelo usuário através de inserções pré-definidas em função da topologia da rede.
- **Roteamento dinâmico:** As rotas são geradas automaticamente através de um protocolo de roteamento dinâmico ou de algum agregado de endereço IP.



Quando o processo roteamento é utilizado?

Comunicação direta
Não precisa de rotas



Comunicação roteada
Precisa de rotas

192.168.1.1/24



Roteador



10.1.1.1/24

10.1.1.2/24



Roteador



10.1.1.1/24

- O processo de roteamento é utilizado quando host em sub-redes diferentes precisam se comunicar.

Introdução a roteamento

- Quais são as principais informações em um pacote para que ocorra comunicação entre dois hosts?

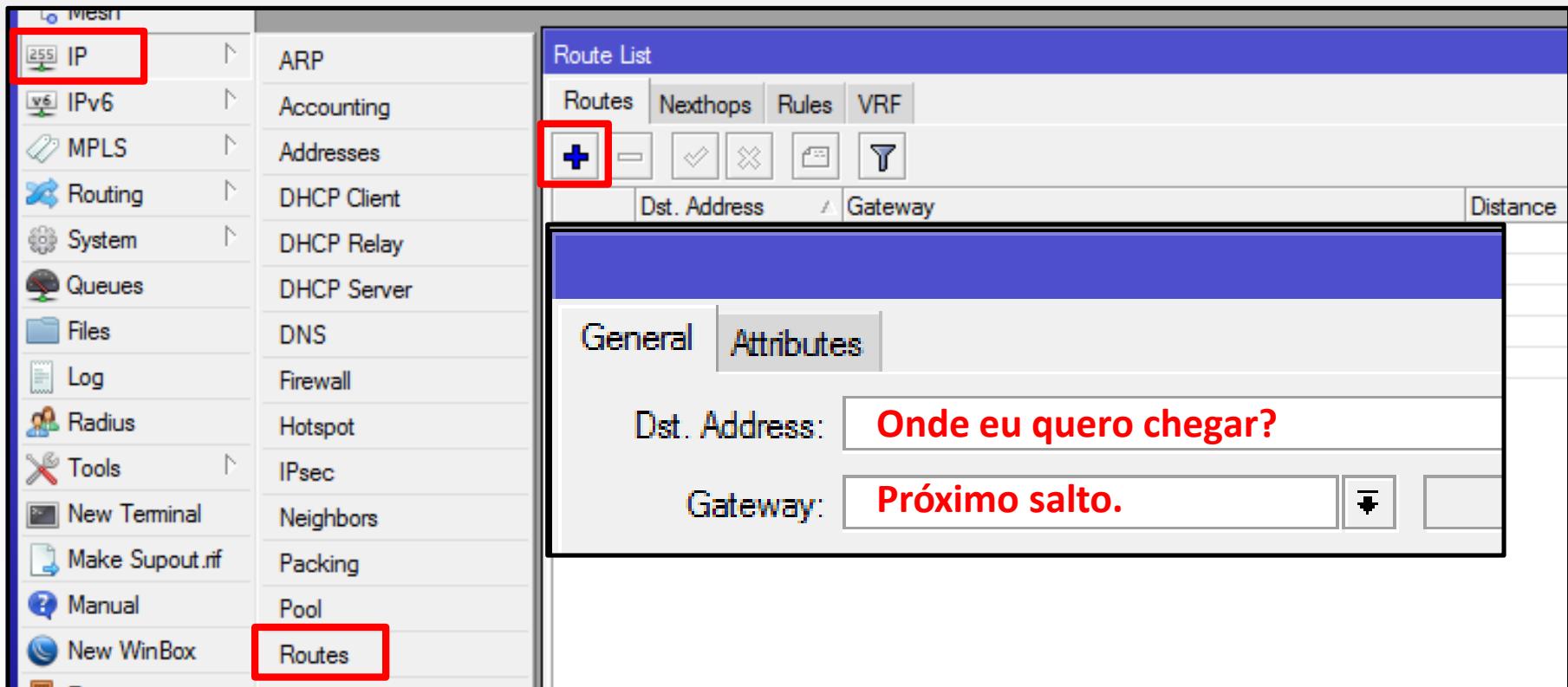
Origem = Source = SRC		Destino = Destination = DST	
4	Ports		Ports
3	IP		IP
2	MAC		MAC

- Qual/quais dessas informações o roteador usa por padrão para determinar a rota de encaminhamento de pacotes?



Principais campos de uma rota

- Os dois principais campos de uma rota são:
 - **Dst. Address** = Rede ou IP de destino
 - **Gateway** = IP ou interface que será utilizado como gateway.



Como alcançar a rede 1 e 2 a partir de MK-3?

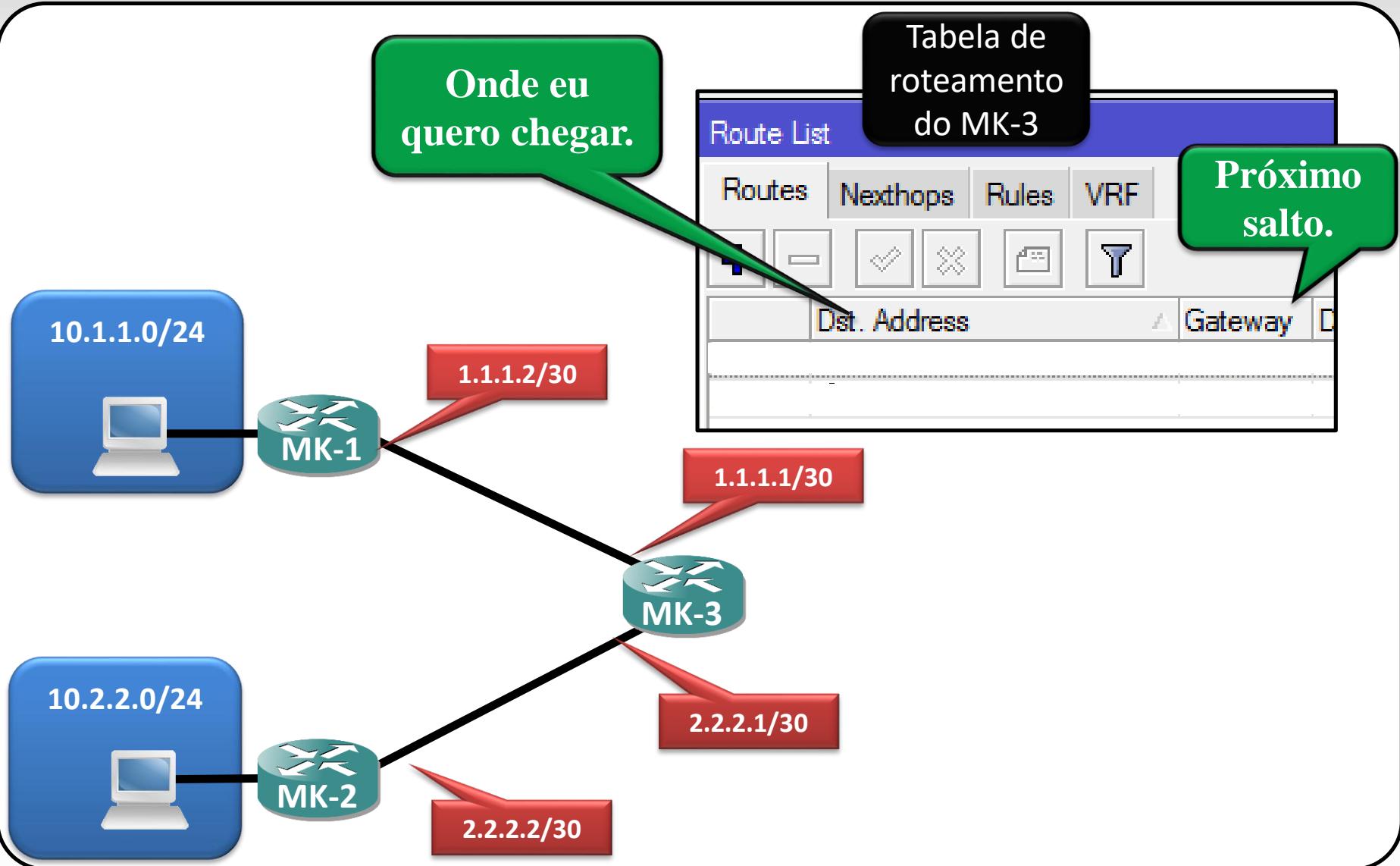
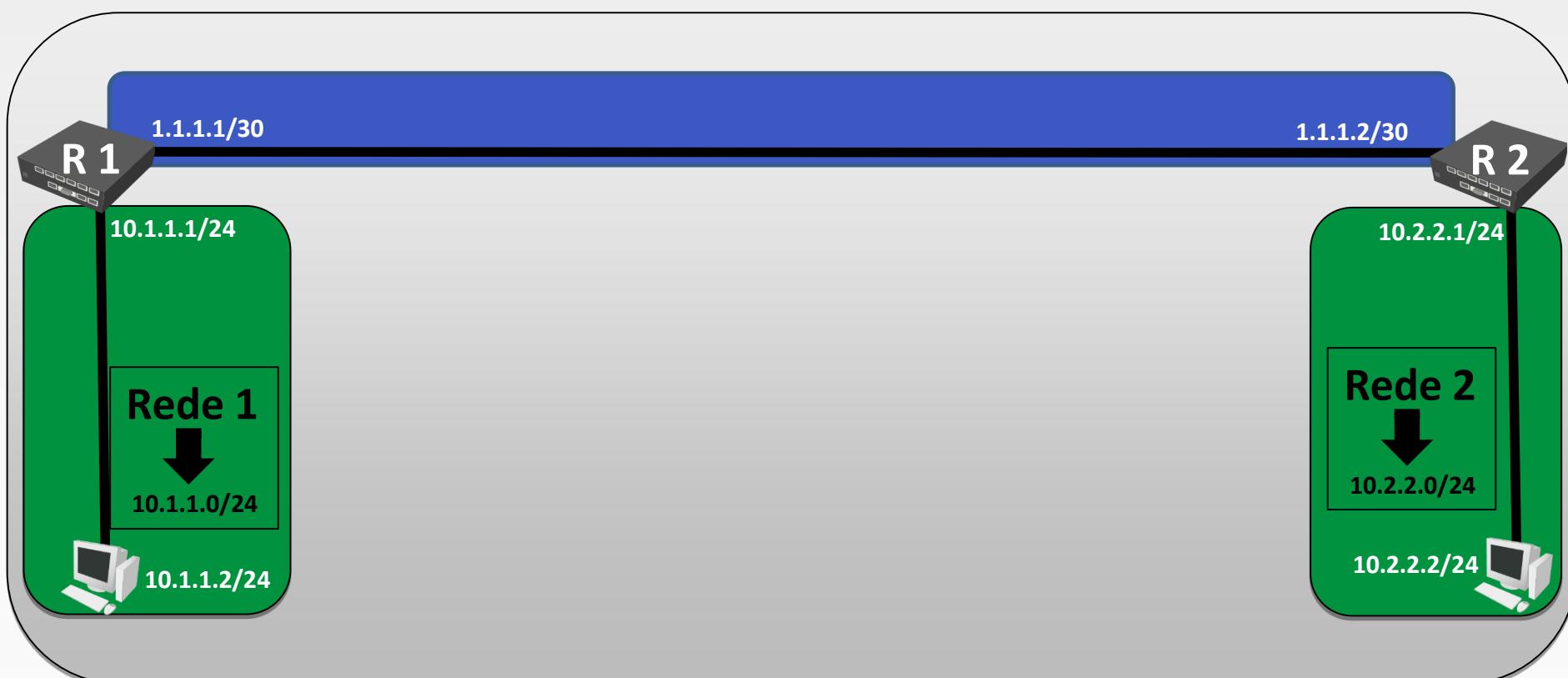


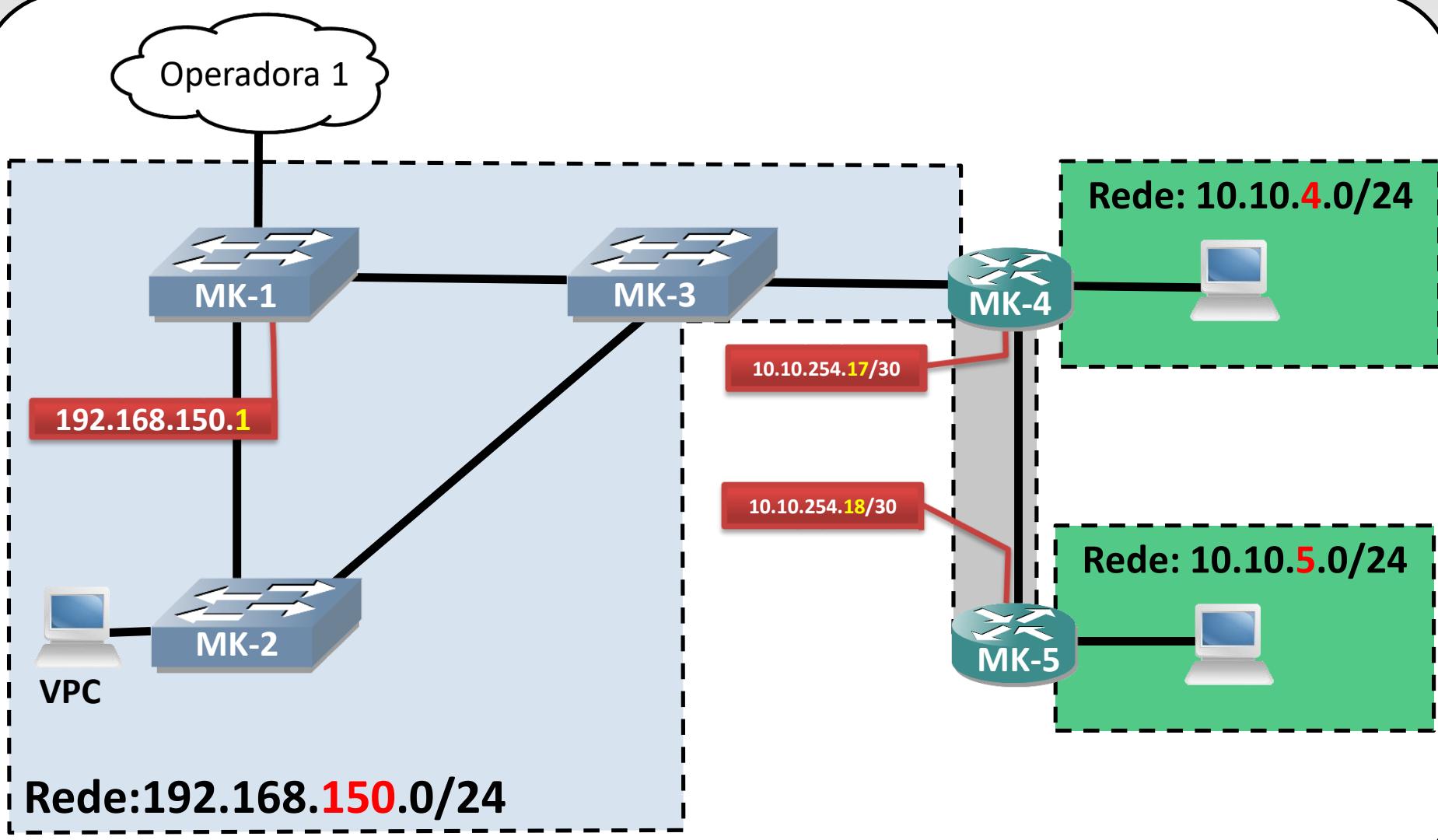
Diagrama simples para roteamento

Redes Brasil



Topologia do LAB

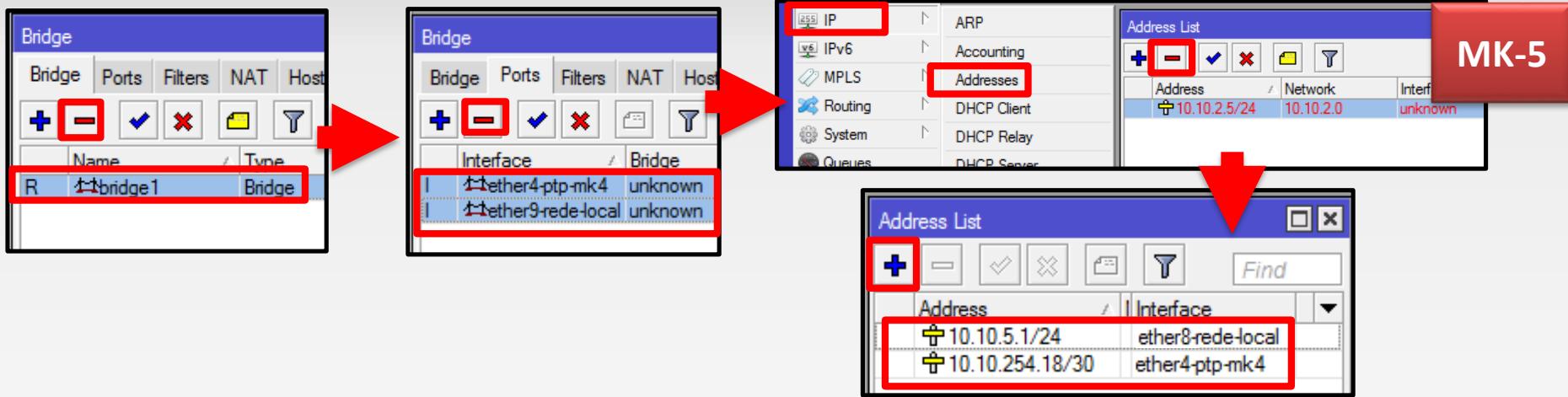
Redes Brasil



Segmentando a rede 5



Redes Brasil



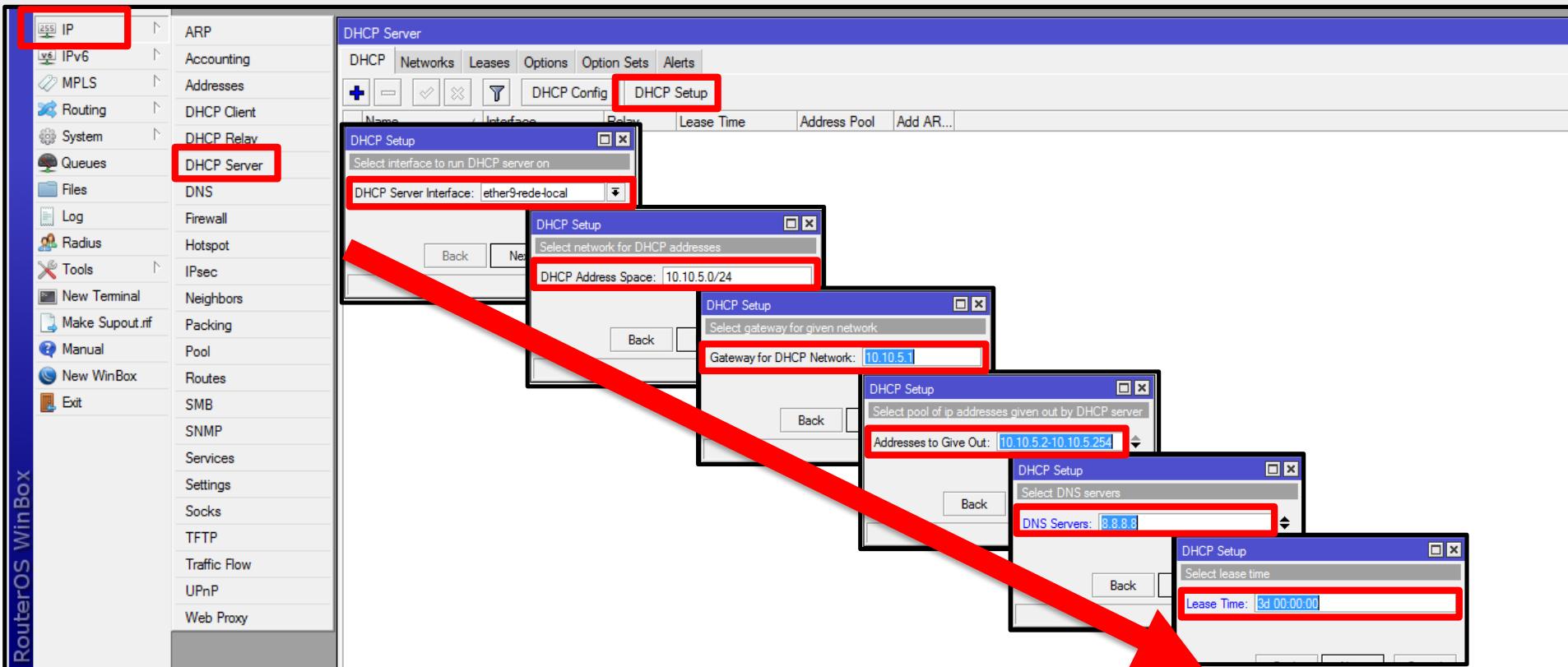
Descrição do LAB

1. Remova a bridge e as interfaces que foram adicionadas nessa bridge.
2. Remova o endereço de IP que estava associado a bridge.
3. Adicione o endereço 10.10.5.1/24 na **ether8**.
4. Crie um servidor de DHCP para **ether8**.
5. Adicione o endereço 10.10.254.18/30 na **ether4**.
6. Abra o PC-5 e digite o comando DHCP para renovar a informações de rede.



Criando um servidor de DHCP

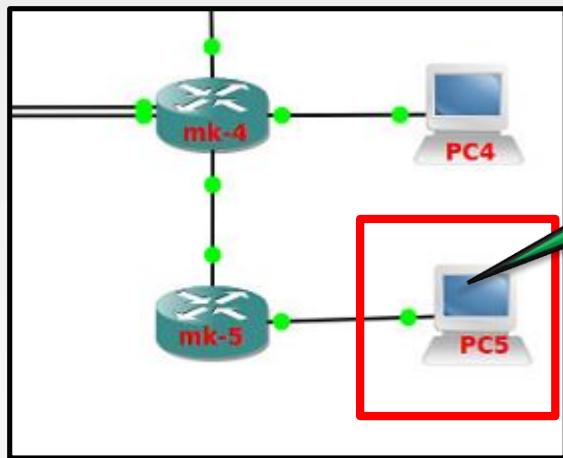
MK-5



Renovando IP do servidor de DHCP



Redes Brasil



1 - Clique duplo
no PC 5

A terminal window titled "PC5" showing a command-line interface. The window has a menu bar with "Arquivo", "Editar", "Ver", and "Pesquisar". The main area displays the following text:
1. PC5
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is [] .
VPCS> **dhcpc**
DORA IP 10.10.5.254/24 GW 10.10.5.1

A red rectangular box highlights the command "dhcpc" at the bottom of the terminal window. A green arrow points from this red box to a green speech bubble containing the text "2 - Digite o comando
dhcpc".

2 - Digite o comando
dhcpc



Segmentando a rede 4

The screenshot shows four windows from the Winbox interface:

- Bridge**: Shows a bridge named "bridge1" selected. The "Add" button (+) is highlighted.
- Bridge**: Shows the "bridge1" bridge with three interfaces: "ether3-ptp-mk3", "ether5-ptp-mk5", and "ether9-rede-local". The "Delete" button (-) is highlighted.
- IP**: Shows the IP address list. The "Address" column has two entries: "10.10.2.4/24" and "10.10.2.0". The "Delete" button (-) is highlighted.
- Address List**: Shows the detailed view of the IP address "10.10.2.4/24" assigned to "ether8-rede-local". The "Delete" button (-) is highlighted.

A red arrow points from the first window to the second. Another red arrow points from the third window to the fourth. A red box labeled "MK-4" is in the top right corner.

Descrição do LAB

1. Remova a bridge e as interfaces que foram adicionadas nessa bridge.
2. Remova o endereço de IP que estava associado a bridge.
3. Adicione o endereço 10.10.4.1/24 na **ether8**.
4. Adicione o endereço 10.10.254.17/30 na **ether5**.
5. Crie um servidor de DHCP para ether8.
6. Abra o PC-4 e digite o comando DHCP para renovar a informações de rede.



Teste de comunicação

```
.. PC5
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^]'.

VPCS> ping 10.10.4.254

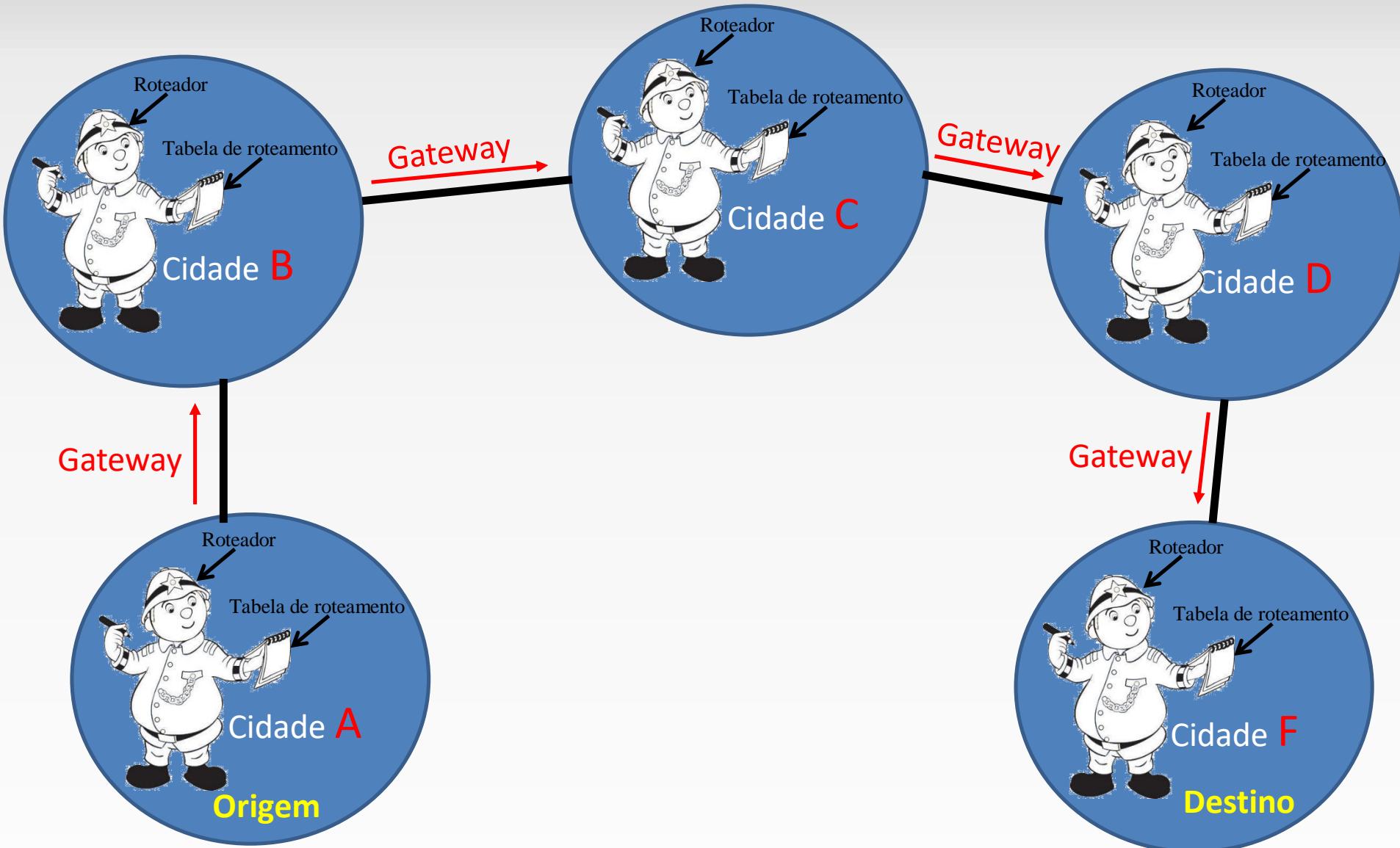
84 bytes from 10.10.4.254 icmp_seq=1 ttl=62 time=4.526 ms
84 bytes from 10.10.4.254 icmp_seq=2 ttl=62 time=1.884 ms
84 bytes from 10.10.4.254 icmp_seq=3 ttl=62 time=2.221 ms
84 bytes from 10.10.4.254 icmp_seq=4 ttl=62 time=1.892 ms
84 bytes from 10.10.4.254 icmp_seq=5 ttl=62 time=1.923 ms

VPCS>
```

1 - Faça o teste de PING do PC5 para o PC4 conforme a imagem.

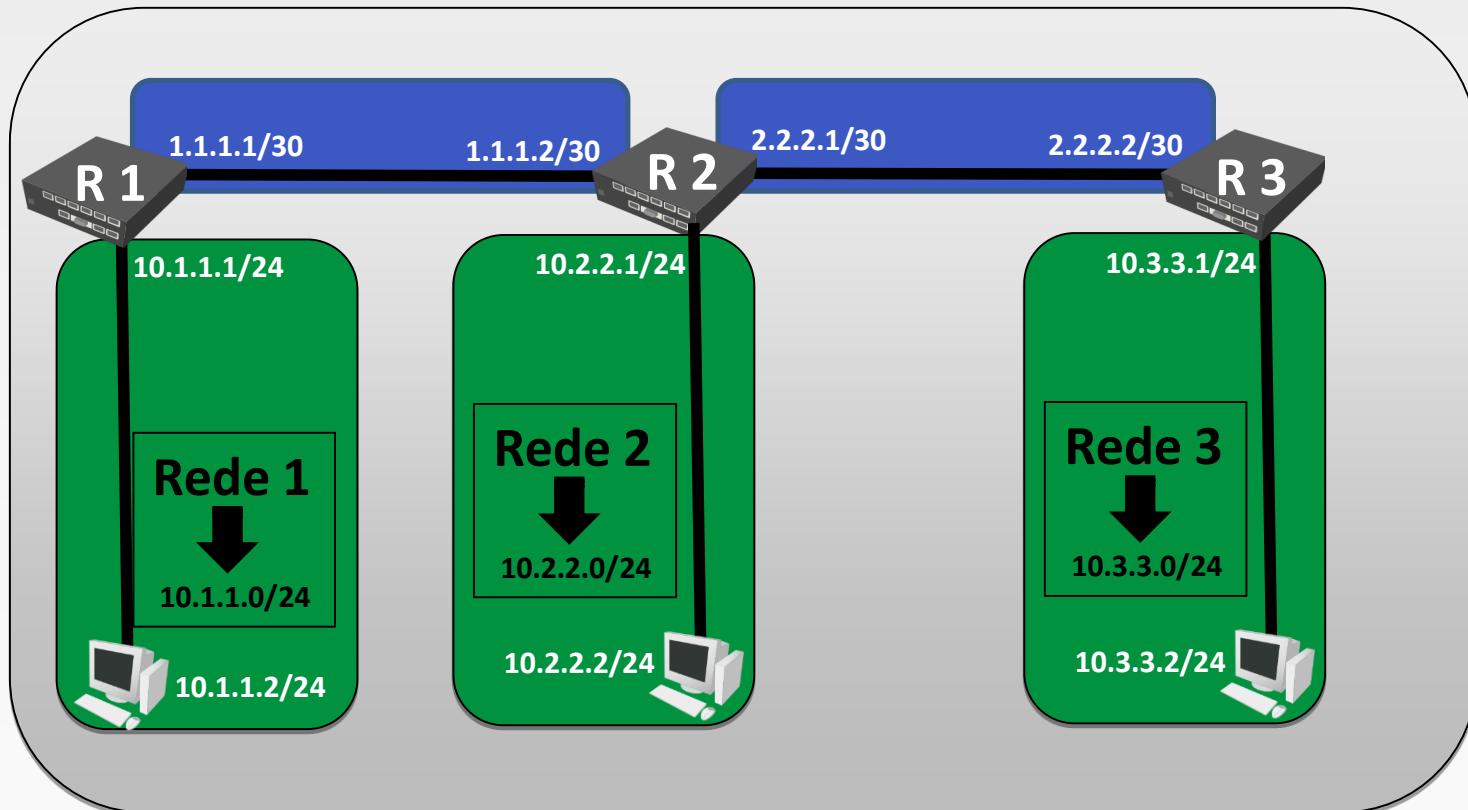
2 – Caso não obtiver êxito com as solicitações de PING faça os ajustes necessários.

Analogia do processo de roteamento

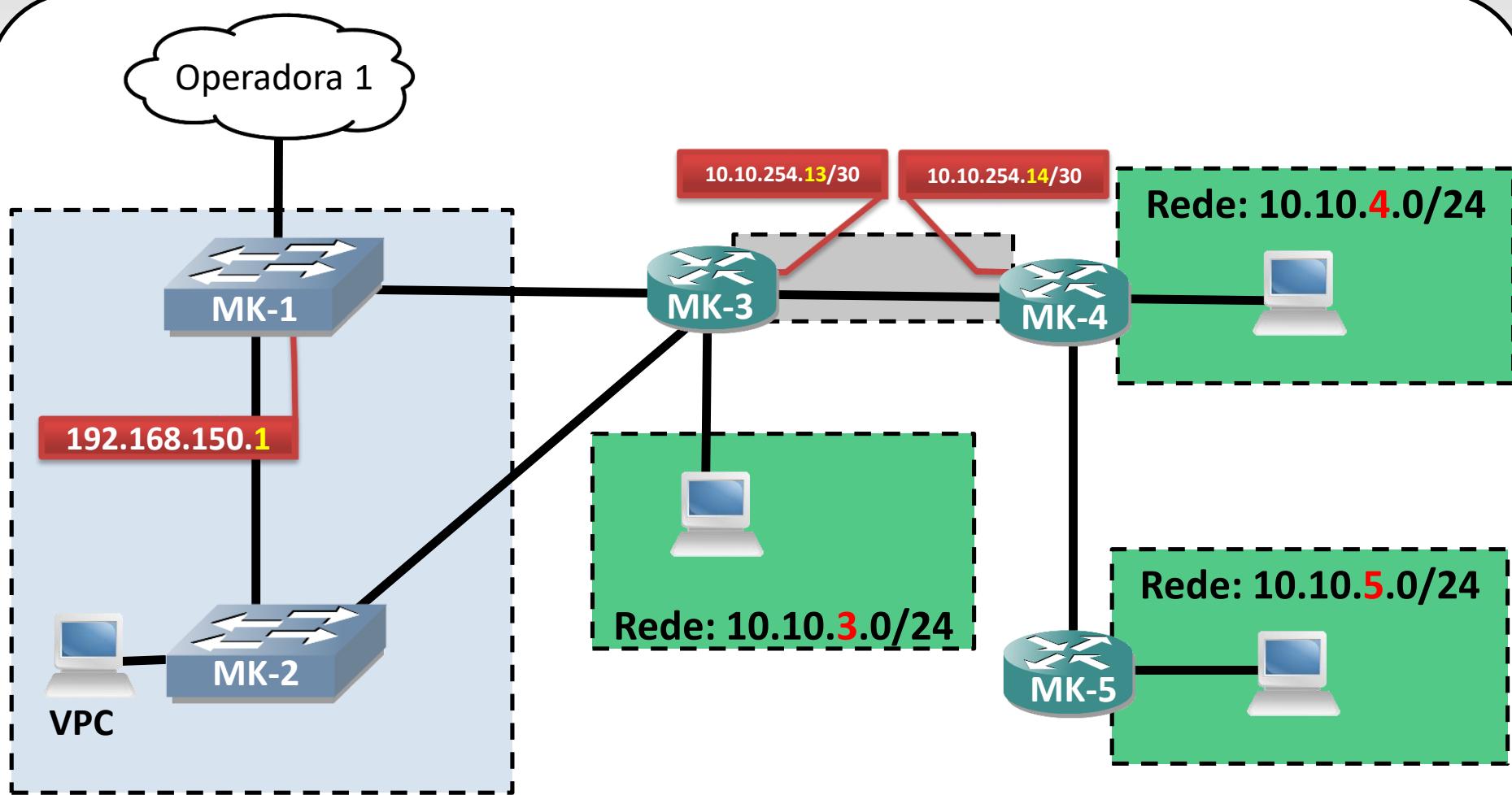




Exemplo 2 de roteamento

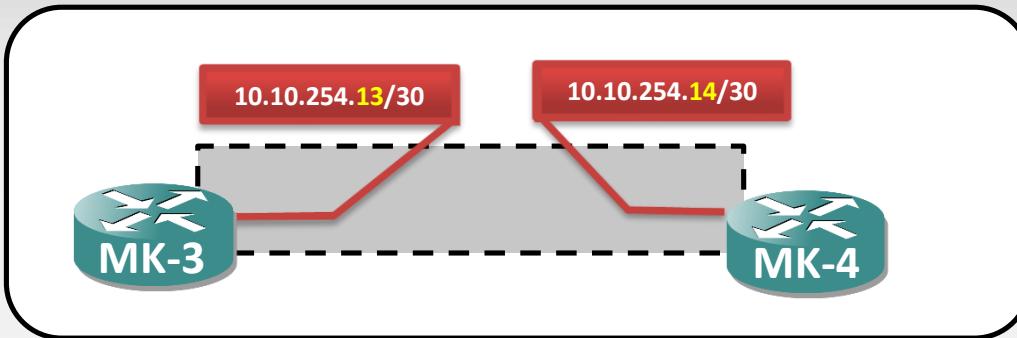


Segmentando a rede 3





Segmentando a rede 3



MK-3

Descrição do LAB

1. Remova a bridge e as interfaces que foram adicionadas nessa bridge.
2. Remova o endereço de IP que estava associado a bridge.
3. Adicione o endereço 10.10.3.1/24 na **ether8**.
4. Adicione o endereço 10.10.254.13/30 na **ether4**.
5. Crie um servidor de DHCP para ether8.
6. Abra o PC-3 e digite o comando DHCP para renovar a informações de rede.

Não esqueça de colocar o IP 10.10.254.14/30 na ether3 do MK-4.



Teste de comunicação

1 - Faça o teste de PING do PC3 para o PC4 e PC5.



```
.. PC3
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^]'.

VPCS> ping 10.10.4.254

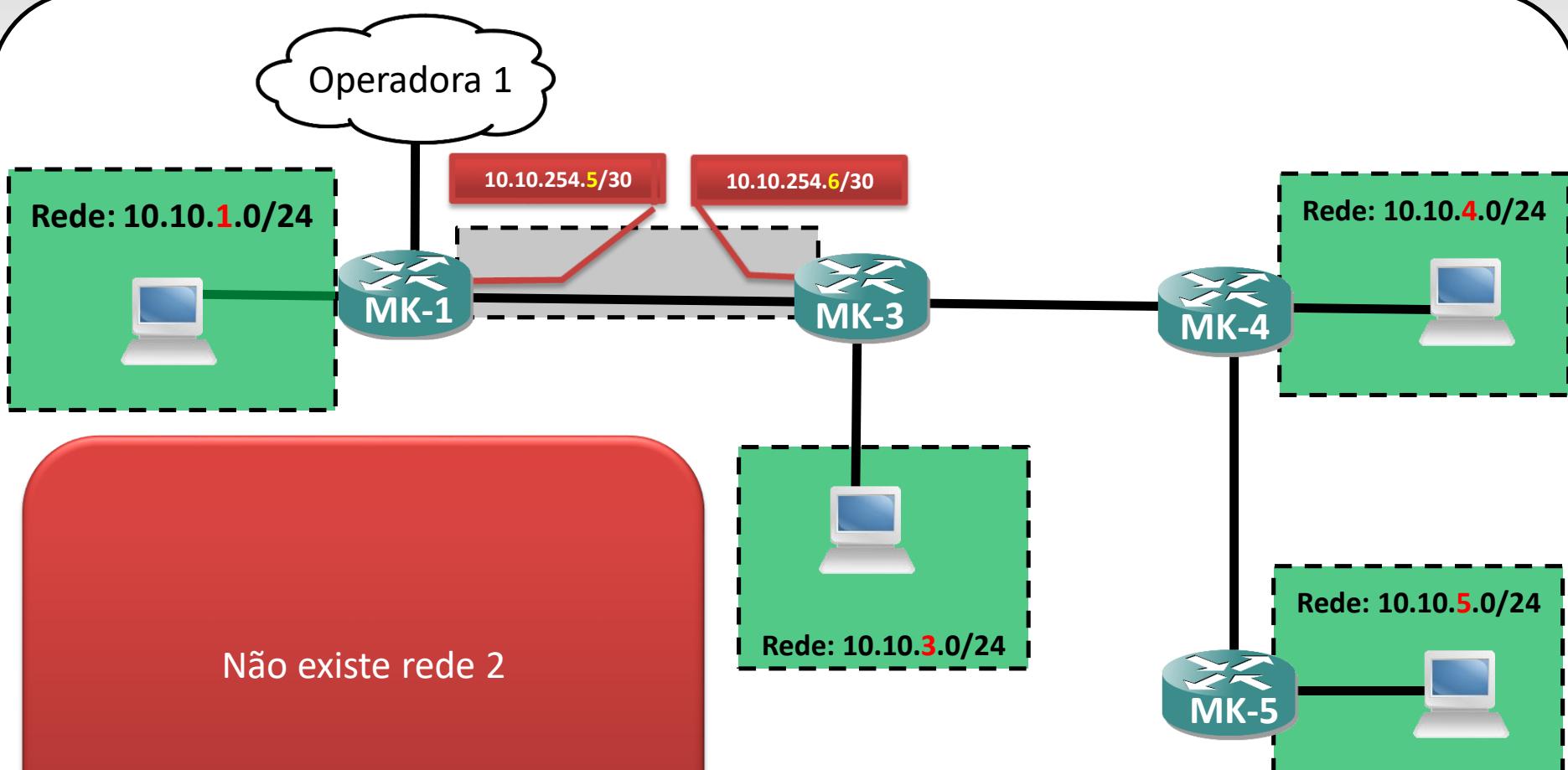
84 bytes from 10.10.4.254 icmp_seq=1 ttl=62 time=3.888 ms
84 bytes from 10.10.4.254 icmp_seq=2 ttl=62 time=1.863 ms
84 bytes from 10.10.4.254 icmp_seq=3 ttl=62 time=1.941 ms
84 bytes from 10.10.4.254 icmp_seq=4 ttl=62 time=1.781 ms
84 bytes from 10.10.4.254 icmp_seq=5 ttl=62 time=2.128 ms

VPCS> ping 10.10.5.254

84 bytes from 10.10.5.254 icmp_seq=1 ttl=61 time=5.744 ms
84 bytes from 10.10.5.254 icmp_seq=2 ttl=61 time=2.780 ms
84 bytes from 10.10.5.254 icmp_seq=3 ttl=61 time=2.791 ms
84 bytes from 10.10.5.254 icmp_seq=4 ttl=61 time=2.731 ms
84 bytes from 10.10.5.254 icmp_seq=5 ttl=61 time=2.627 ms
```

2 – Caso não obtiver êxito com as solicitações de PING faça os ajustes necessários.

Segmentando a rede 1





TTL

- TTL é o limite máximo de saltos que um pacote pode dar até ser descartado;
- No RouterOS o valor padrão do TTL é 64 e cada roteador decrementa este valor em 1 antes de passá-lo adiante;
- O menu Firewall Mangle pode ser usado para manipular este parâmetro;
- Se um roteador recebe um pacote com TTL=1 esse pacote só poderá ser destinado ao próprio roteador.
- O roteador não passa adiante pacotes que chegarem com TTL=1;





Alterando o TTL

Traceroute (Running)

Traceroute To: 8.8.8.8

Packet Size: 56

Timeout: 1000

Protocol: icmp

Port: 33434

Use DNS

Count:

Max Hops:

Src. Address: **Antes**

Interface:

DSCP:

Routing Table:

Hop	/	Host	Loss
1	/	10.172.254.25	0
2	/	10.172.80.100	0
3	/	179.185.128.254	0
4	/	177.205.10.193	0
5	/	177.205.9.109	0
6	/	179.185.131.1	0
7	/	177.99.249.70	0
8	/	187.115.214.182	0
9	/	72.14.198.181	0
10	/	209.85.245.163	0
11	/	8.8.8.8	0

Regra no Firewall Mangle

Mangle Rule <>

General Advanced Extra Action Statistics

Chain: **forward**

Src. Address: []

Dst. Address: []

Protocol: 1 (icmp)

Src. Port: []

Dst. Port: []

Any. Port: []

Action: change TTL

Log

Log Prefix: []

- TTL Action -

change increment decrement

New TTL: **100**

Traceroute (Running)

Traceroute To: 8.8.8.8

Packet Size: 56

Timeout: 1000

Protocol: icmp

Port: 33434

Use DNS

Count:

Max Hops:

Src. Address: **Depois**

Interface:

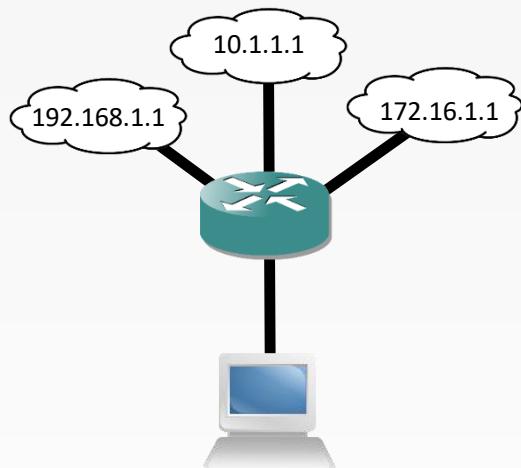
DSCP:

Routing Table:

Hop	/	Host	Loss
1	/	10.172.254.25	0
2	/	8.8.8.8	0

Funcionamento padrão (nexthop-lookup)

- O roteador executa uma tarefa chamada “**nexthop-lookup**” (pesquisa de próximo salto) para cada pacote que passa por ele.
- Lembrando que essa busca sempre será feita varrendo todas as entradas da FIB.

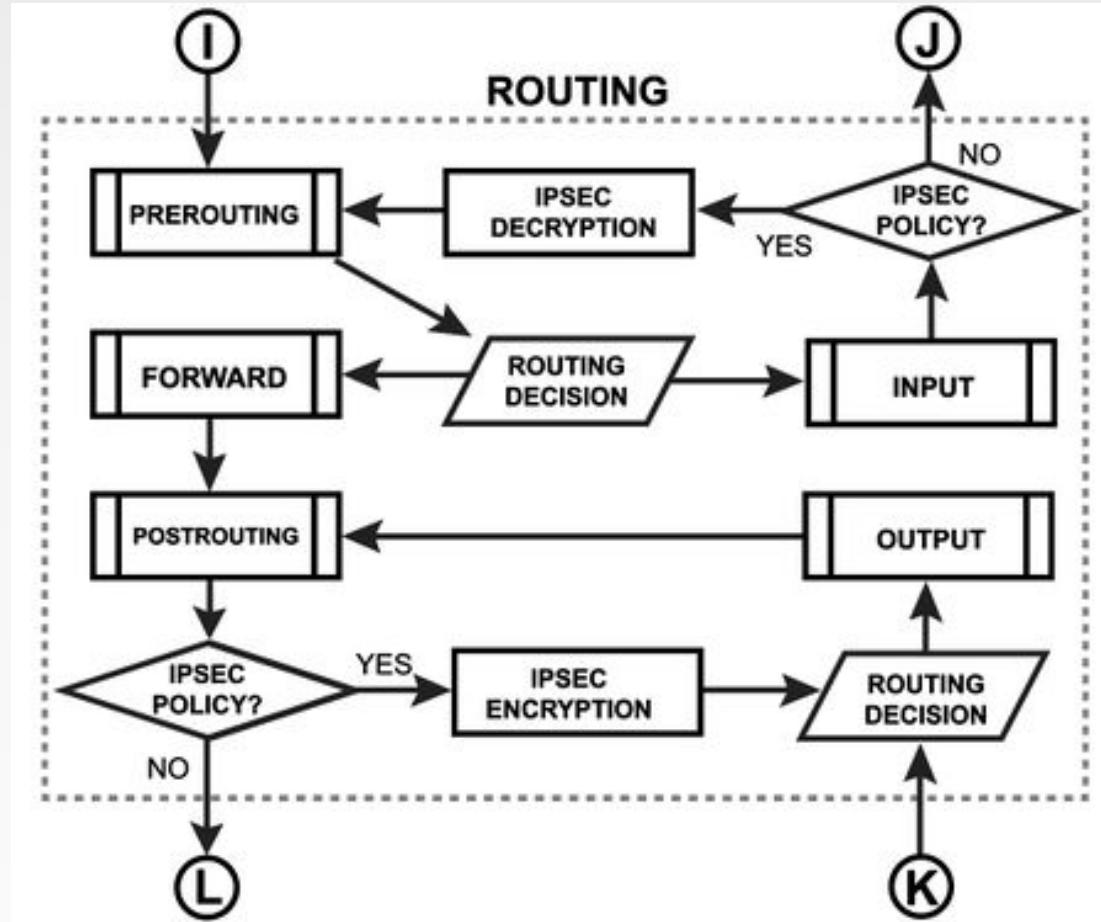


Marca de Roteamento

- Podemos usar o Firewall Mangle para realizar marcas de roteamento.
- Limite de marcas 251
- Todas rotas sem marcas são mantidas na tabela MAIN



Diagrama de Roteamento

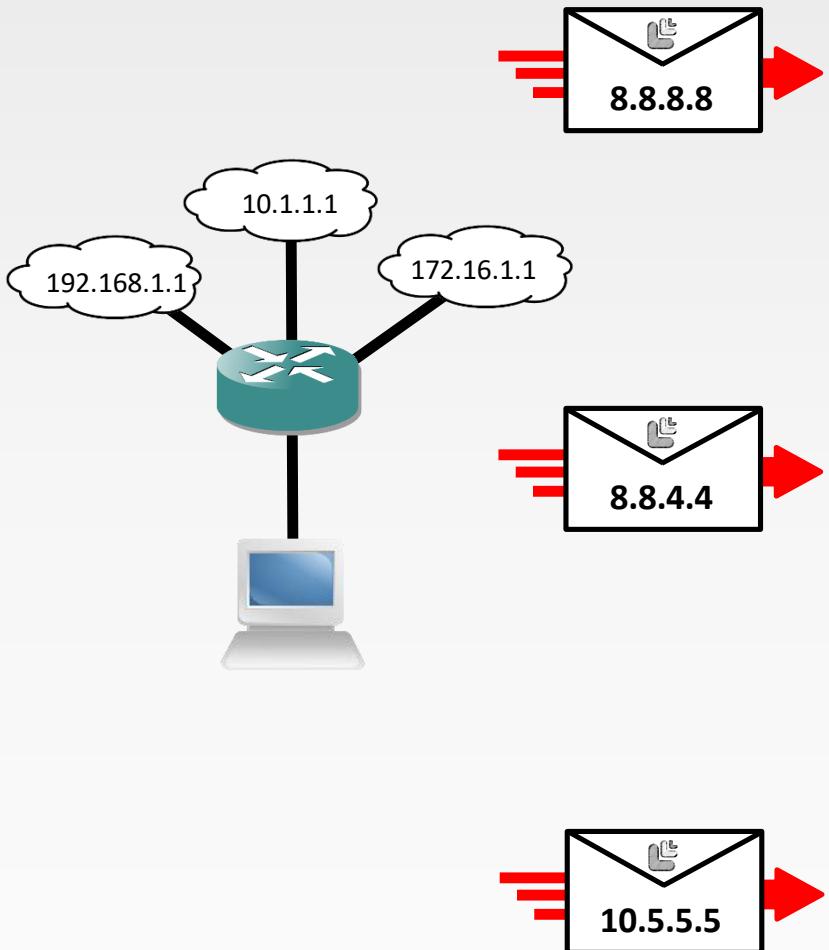


Fonte: https://wiki.mikrotik.com/wiki/Manual:Packet_Flow

Funcionamento padrão (nexthop-lookup)



Redes Brasil



Route List			
	Dst. Address	Gateway	Distance
AS	► 0.0.0.0/0	10.1.1.1 reachable ether1	1
AS	► 8.8.0.0/16	172.16.1.1 reachable ether3	1
AS	► 8.8.8.0/24	192.168.1.1 reachable ether2	1

Route List			
	Dst. Address	Gateway	Distance
AS	► 0.0.0.0/0	10.1.1.1 reachable ether1	1
AS	► 8.8.0.0/16	172.16.1.1 reachable ether3	1
AS	► 8.8.8.0/24	192.168.1.1 reachable ether2	1

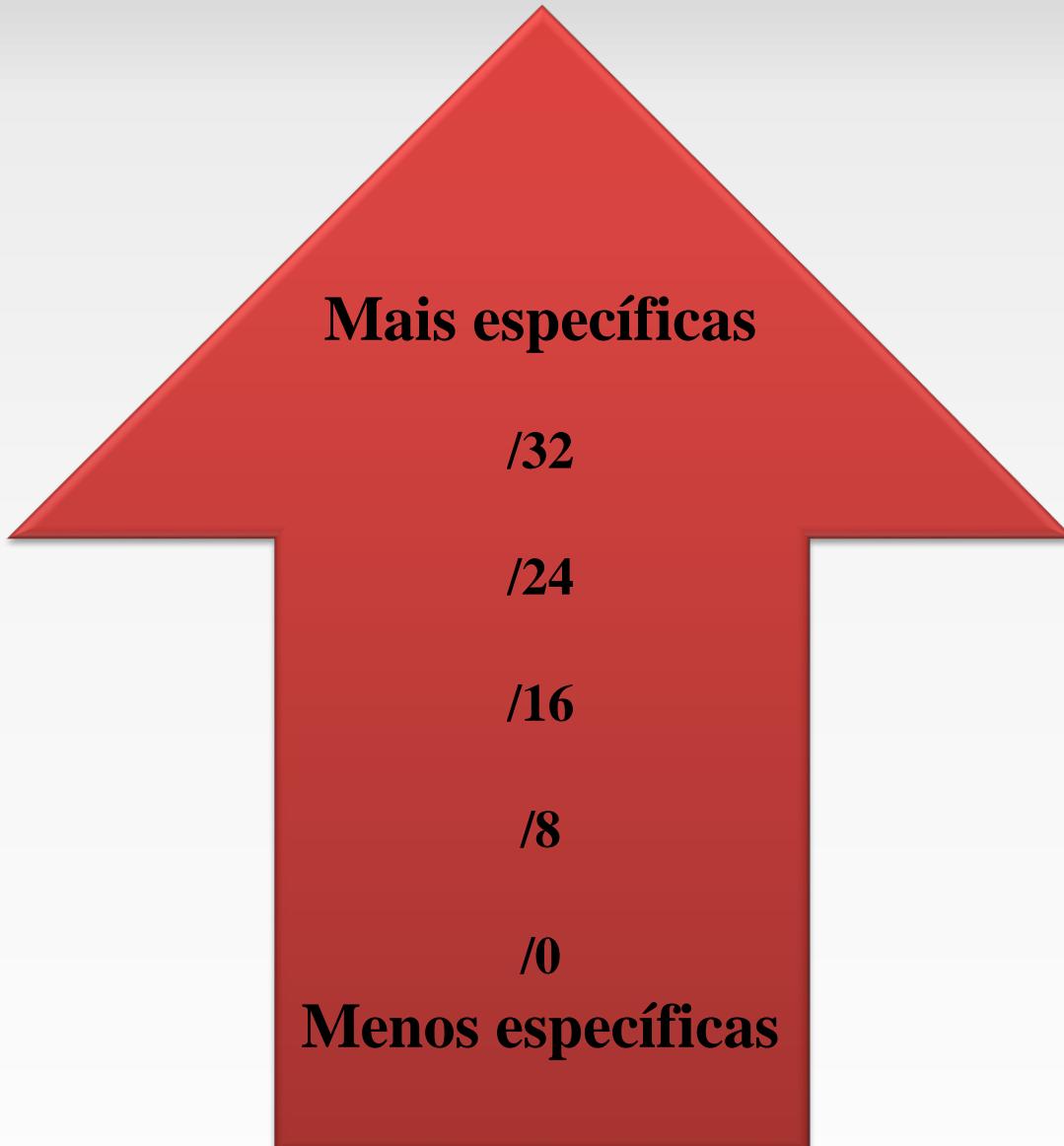
Route List			
	Dst. Address	Gateway	Distance
AS	► 0.0.0.0/0	10.1.1.1 reachable ether1	1
AS	► 10.5.50.0/24	192.168.1.1 reachable ether2	1
AS	► 10.10.10.0/24	172.16.1.1 reachable ether3	1

Escolha da melhor rota

- Para cada novo encaminhamento o roteador faz uma leitura completa da tabela de rotas.
- Se o roteador encontrar mais de uma rota para o mesmo **destino** ele irá utilizar a rota **mais específica**.
- A **rota default** será utilizada somente se **não houver** uma rota para o determinado destino.

Rota mais específicas

Redes Brasil

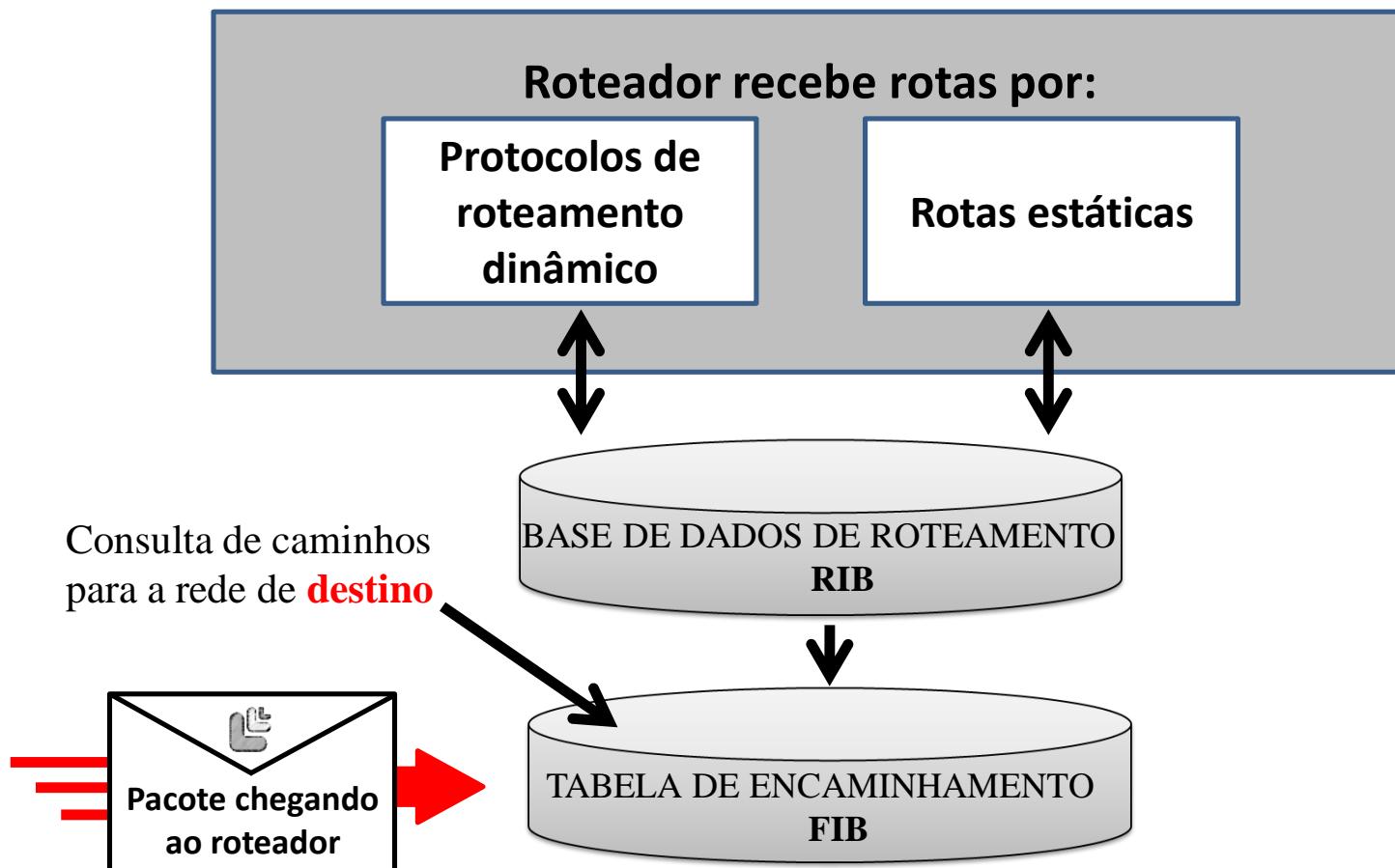


Funcionamento básico de um Roteador



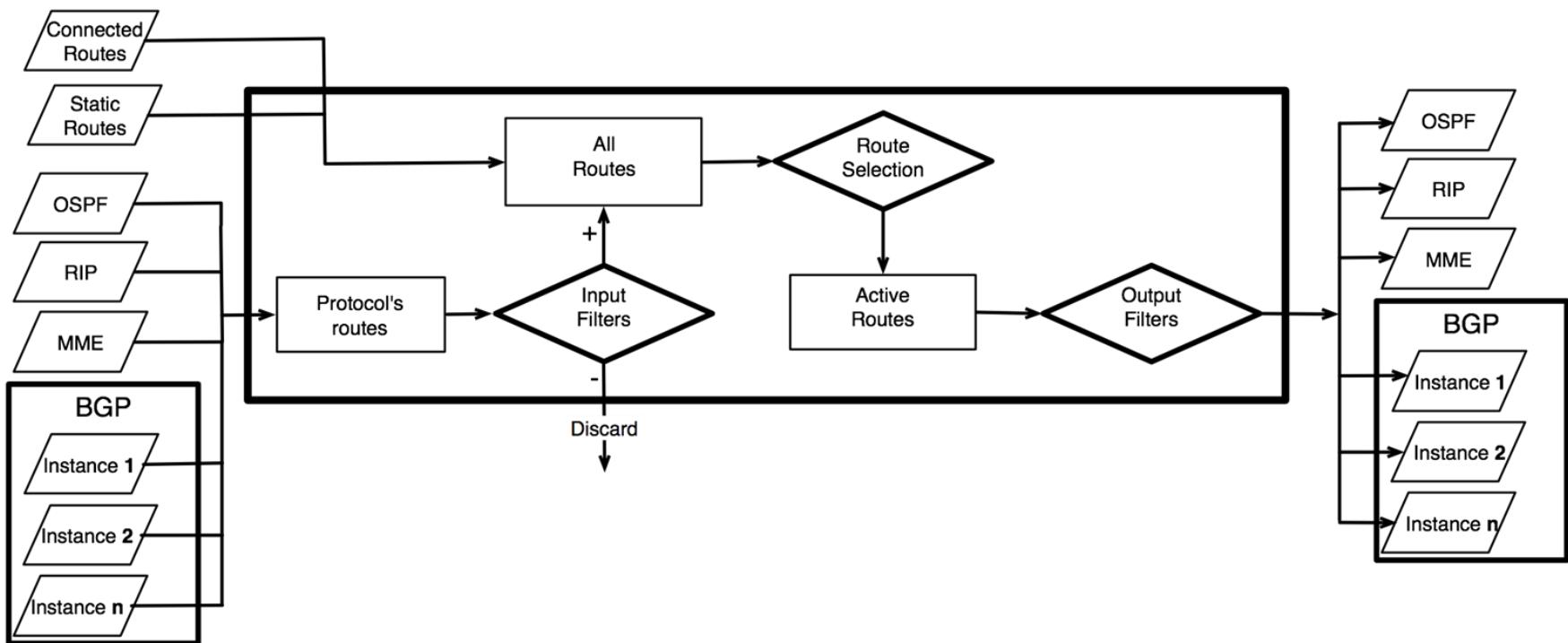
Redes Brasil

Roteador



Funcionamento básico de um Roteador

Redes Brasil



Fundamentos de roteamento

Routing Information Base (RIB)

- A **RIB** é o local onde ~~todas as informações~~ a respeito do roteamento IP estão armazenadas. A RIB é única em cada roteador e compartilhada com protocolos.
- Uma rota é inserida na RIB, sempre que um protocolo aprende uma nova rota.
- O RouterOS mantém as rotas agrupadas em tabelas separadas pelas marcas de roteamento (routing marks). E, em alguns casos, as métricas (distâncias) associado a este roteador.
- Todas as rotas sem marcas de roteamento são mantidas na tabela “main” (principal). É importante entender que RIB não é utilizada para o encaminhamento de pacotes e não é anunciada para o restante das redes as quais o roteador está conectado.

Fundamentos de roteamento

Forwarding Information Base (FIB)

- A **FIB** é a base de dados que contém uma cópia das informações necessárias para o encaminhamento dos pacotes relacionando as redes às respectivas interfaces.
- A FIB contém todas as rotas que podem potencialmente serem anunciadas aos roteadores vizinhos pelos protocolos de roteamento dinâmico.
- Por padrão no RouterOS todas as rotas ativas estão na *main-table* que pode ser visualizada em /ip route, inclusive com os detalhes inseridos pelos rotocolos de roteamento dinâmico.

Tipos de rotas

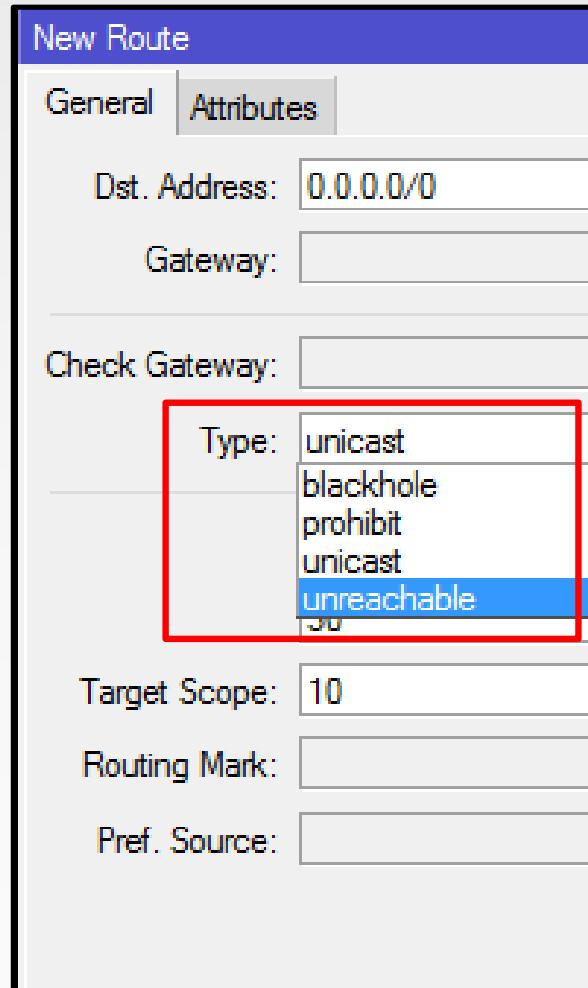
Flag/Sigla	Significado da sigla	Tipo de rota
A	Active	Rota ativa
C	Connected	Rota diretamente conectada
S	Static	Rota estática
D	Dynamic	Rota dinâmica
B	Blackhole	Rota do tipo buraco negro
U	Unreachable	Rota inalcançável
P	Prohibit	Rota do tipo proibida
o	OSPF	Rota aprendida via OSPF
b	BGP	Rota aprendida via BGP
r	RIP	Rota aprendida via RIP
m	MME	Rota aprendida via MME

```
/ip route print
```

Flags: X - disabled, A - active, D - dynamic, C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme, B - blackhole, U - unreachable, P - prohibit

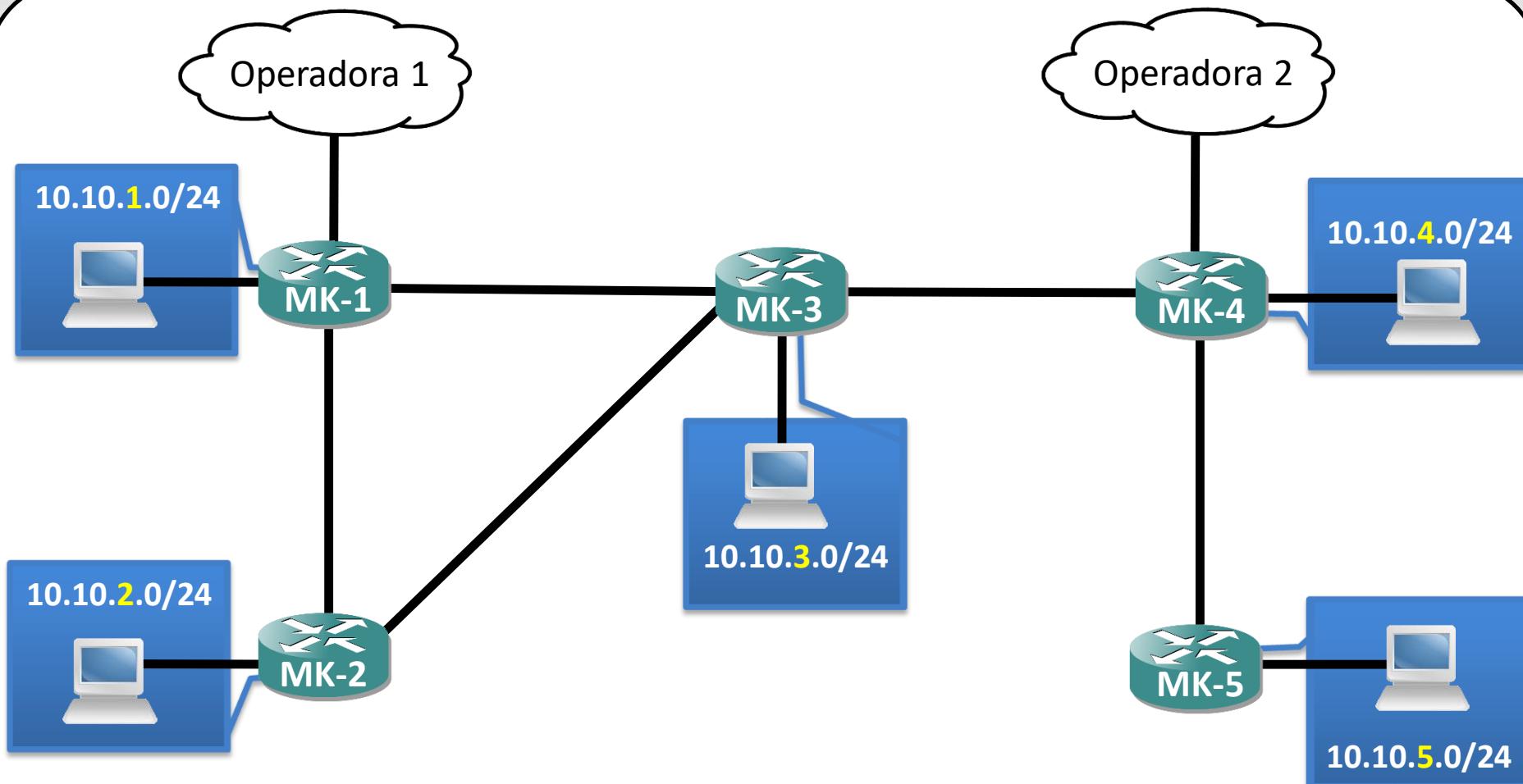
Campo Type

- **Blackhole:** Descarta o pacote silenciosamente.
- **Unreachable:** Descarta o pacote e envia uma notificação via ICMP para o host de origem (“host unreachable” type 3 code 1).
- **Prohibit:** Descarta o pacote e envia uma notificação via ICMP para o host de origem (“communication administratively prohibited” type 3 code 13).



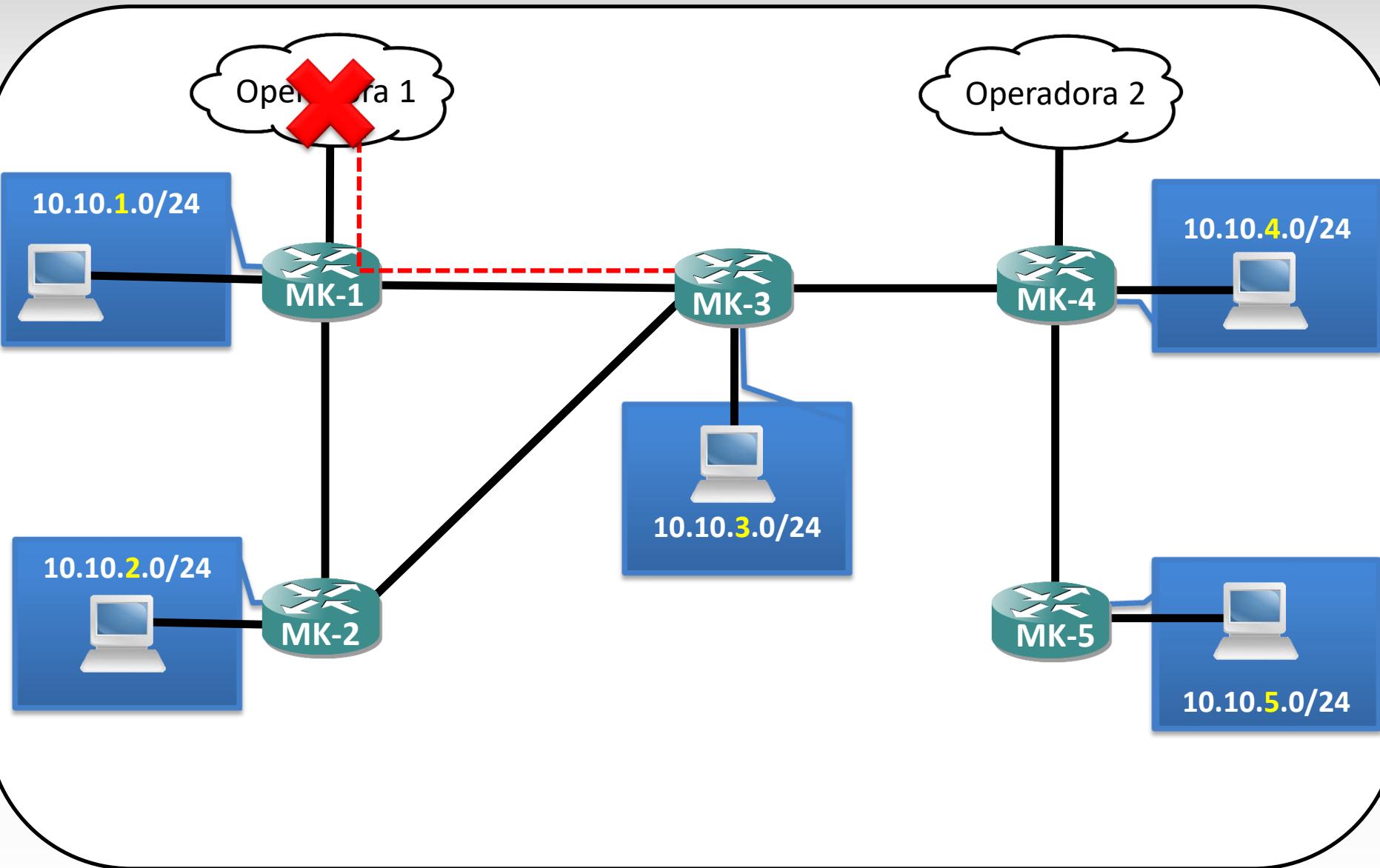
Ativando a segunda operadora

Redes Brasil

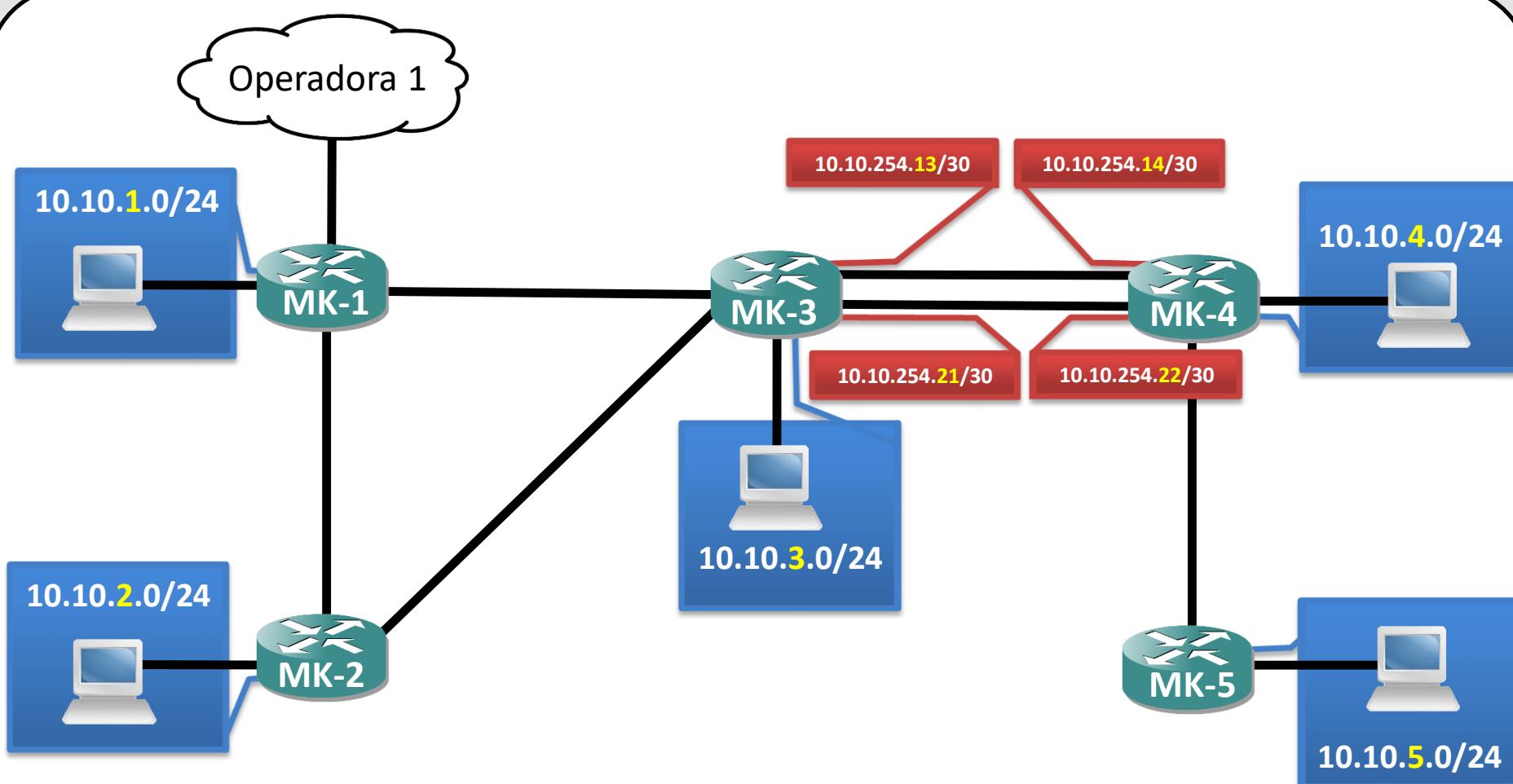




Dificuldades do roteamento estático

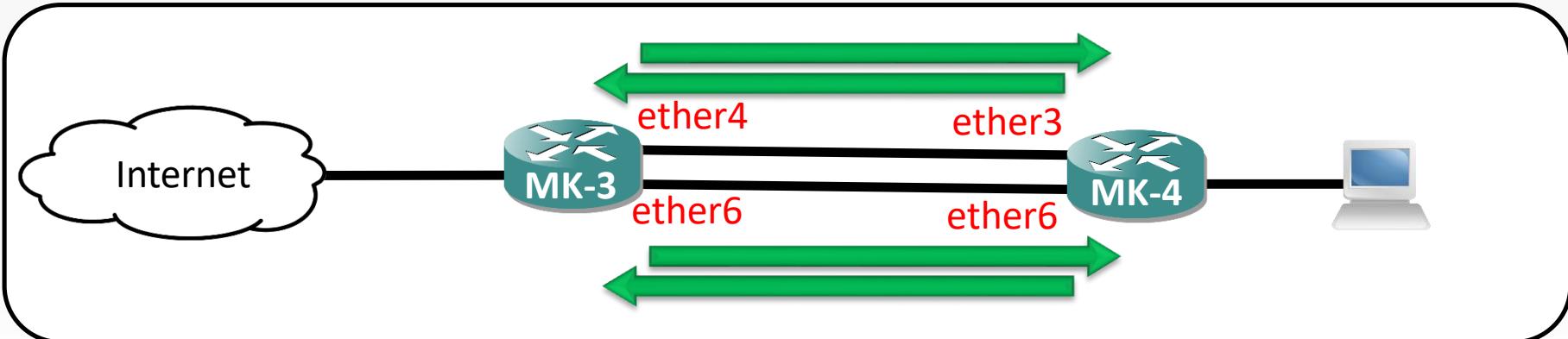
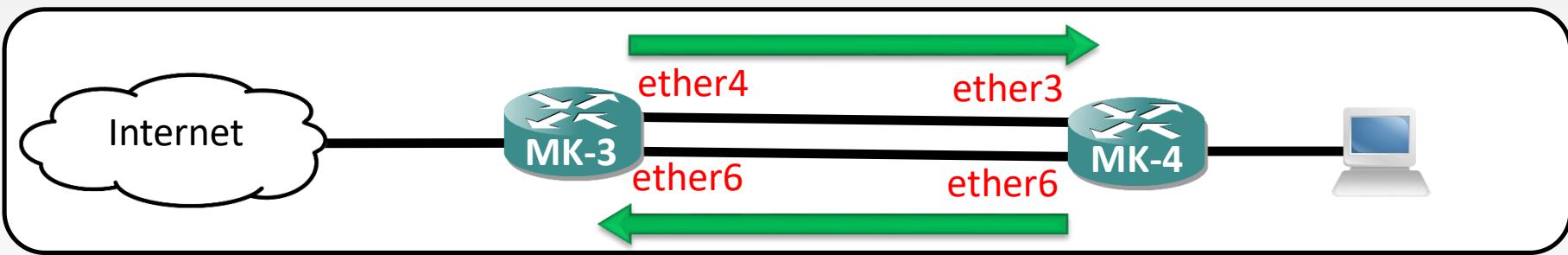
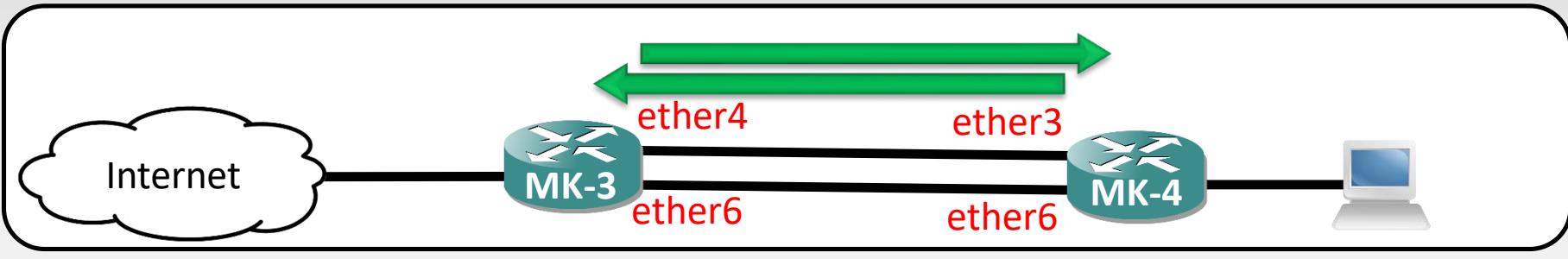


Ativando segunda rota entre MK-3 e MK-4



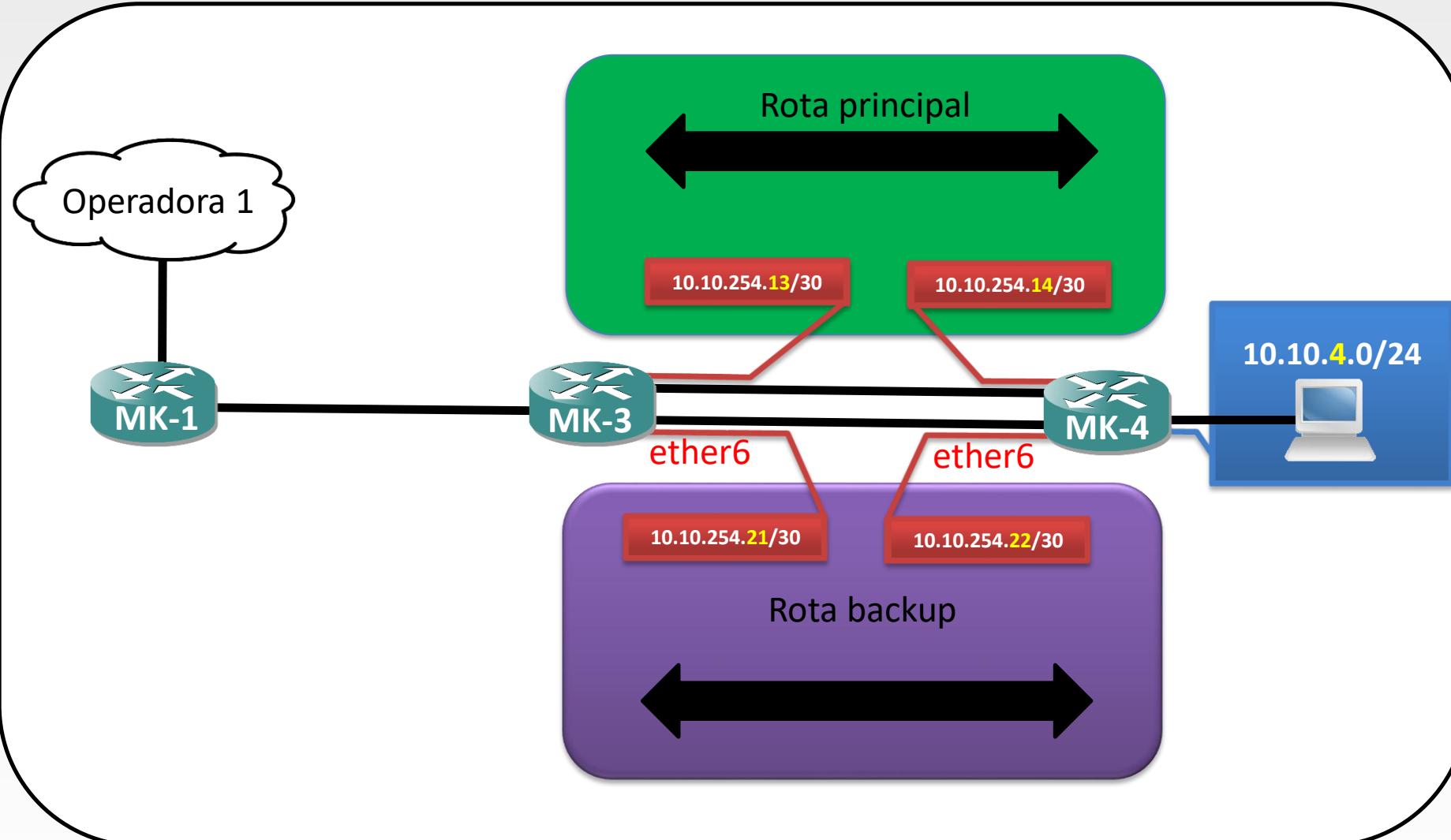


Algumas opções com duas rotas





Definindo rota principal e backup

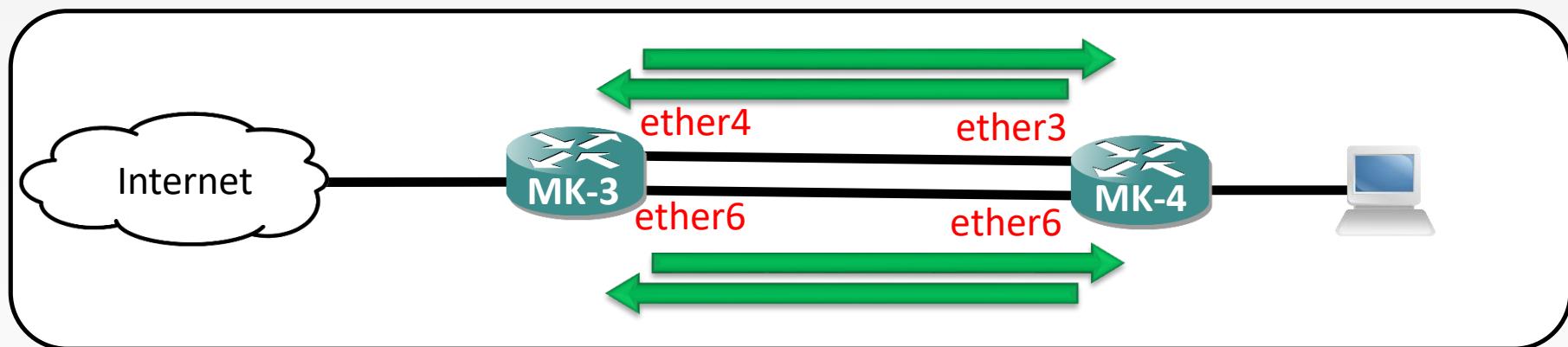


Check-gateway

- A funcionalidade Check-gateway irá verificar se o gateway é alcançável através de ICMP ou ARP.
- A checagem ocorre a cada 10 segundos.
- Se após duas tentativas seguidas o gateway não responder, ele é considerado inalcançável.
- Após receber uma resposta o gateway novamente é considerado alcançável.
- A funcionalidade de check-gateway não entra em funcionamento quando é utilizado em rotas ECMP.

ECMP – Equal cost multi path

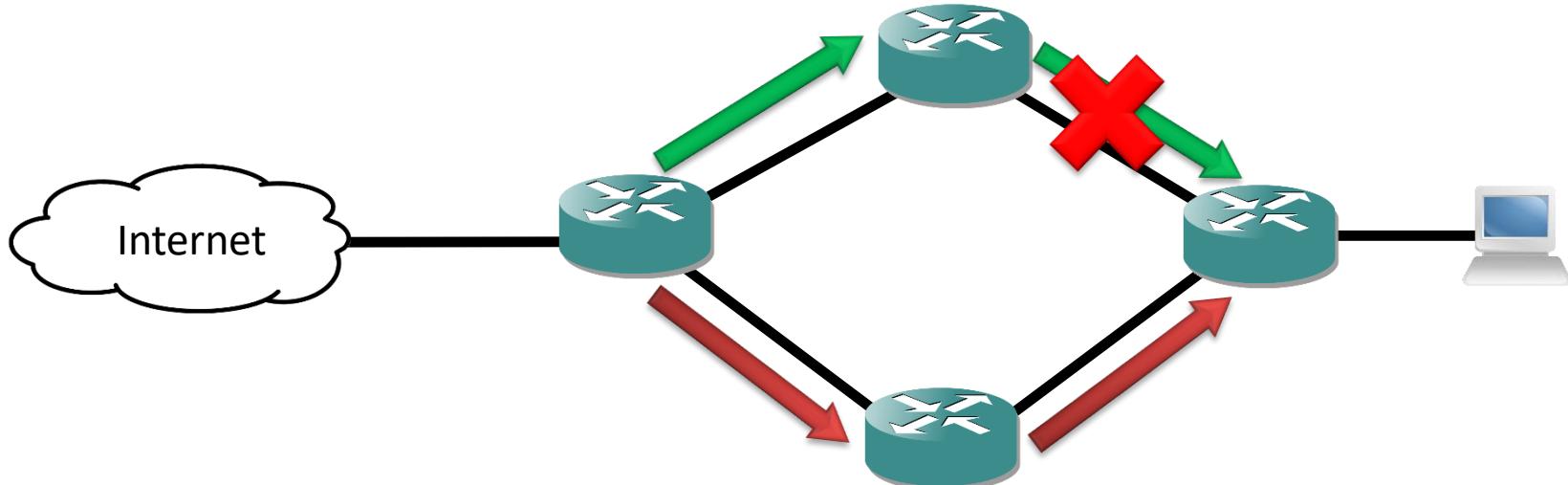
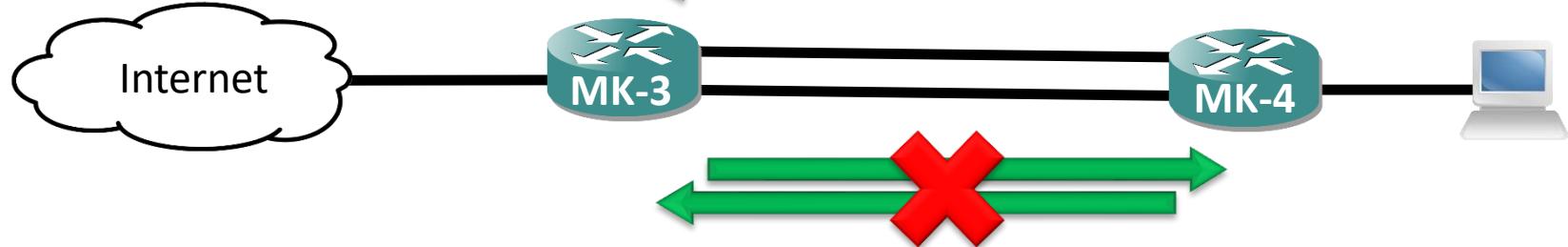
- O roteador nesse caso terá 2 gateways e estará fazendo um balanceamento de carga simples entre os 2 Links utilizando ECMP.



Redundância x rotas estáticas

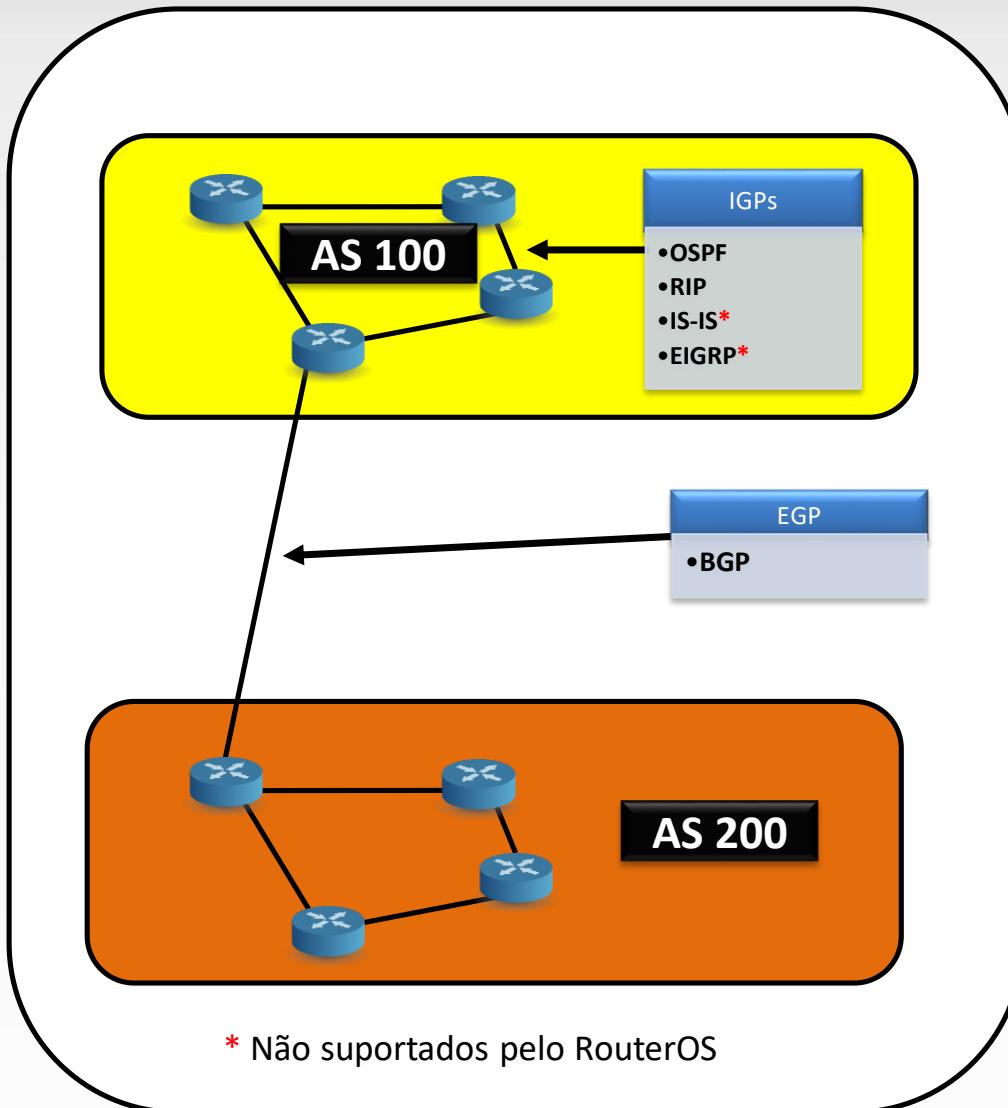
Redes Brasil

ECMP





Roteamento dinâmico



Roteamento dinâmico

- O MikroTik suporta os seguintes protocolos:
 - RIP versão 1 e 2;
 - OSPF versão 2 e 3;
 - BGP versão 4.
- O uso de protocolos de roteamento dinâmico permite implementar redundância e balanceamento de links de forma automática e é uma forma de se fazer uma rede semelhante as redes conhecidas como Mesh, porém de forma estática.

Roteamento dinâmico - BGP

- O protocolo BGP é destinado a fazer comunicação entre AS(Autonomos System) diferentes, podendo ser considerado como o coração da internet.
- O BGP mantém uma tabela de “prefixos” de rotas contendo informações para se encontrar determinadas redes entre os AS's.
- A versão corrente do BGP no Mikrotik é a 4, especificada na RFC 1771.

OSPF

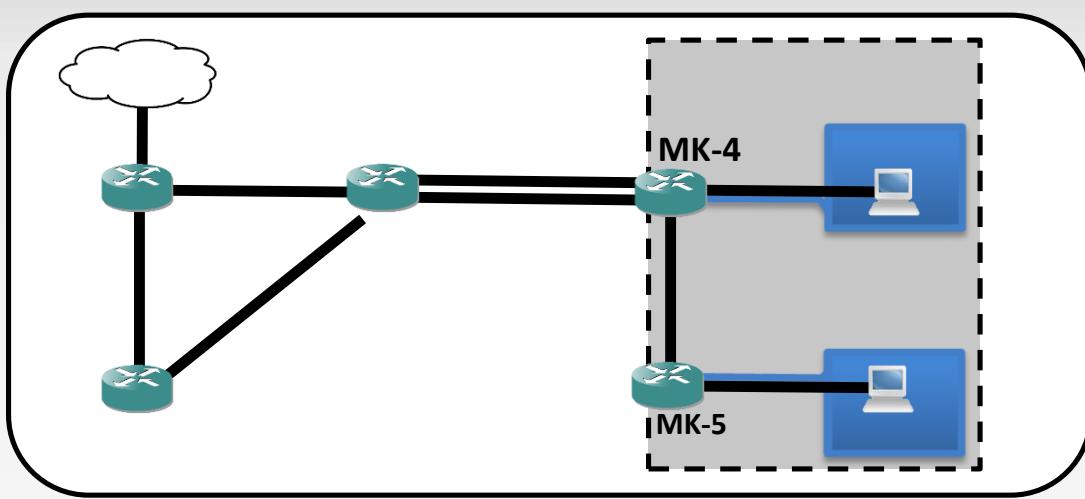
- O protocolo OSPF utiliza o **estado do link** e o **algoritmo de Dijkstra** para construir e calcular o menor caminho para todos destinos conhecidos na rede.
- Os roteadores OSPF utilizam o protocolo IP 89 para comunicação entre si.
- O OSPF distribui informações de roteamento entre roteadores pertencentes ao mesmo AS.
- O OSPF é um protocolo para uso como IGP.
- As rotas aprendidas via protocolo OSPF por padrão tem distância igual a 110.

Distâncias padrões

Protocolo	Distancia
connected	0
static	1
eBGP	20
OSPF	110
RIP	120
MME	130
iBGP	200

LAB – OSPF básico

Redes Brasil



Descrição do LAB

1. Altere a distância das rotas estáticas para um valor maior que 110 de forma que as rotas aprendidas via OSPF tenham prioridade.
2. Para que o protocolo OSPF funcione, precisamos realizar um **único procedimento** que é adicionar as redes ([/routing ospf network](#))
3. Verifique a tabela de vizinhos do OSPF ([/routing ospf neighbor](#)).
4. Verifique as novas rotas aprendidas via OSPF.



Ativando OSPF entre MK-4 e MK-5

Operadora 1

MK-1

MK-2

MK-3

MK-4

MK-5

10.10.4.0/24

10.10.5.0/24

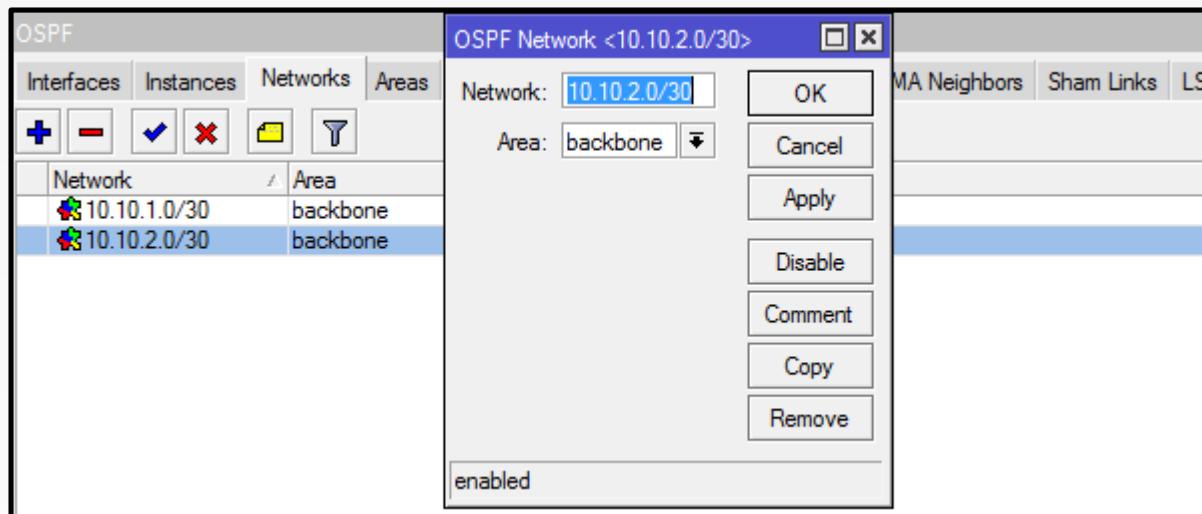
Ativando OSPF



Networks (redes) OSPF

➤ Ao adicionar uma rede em **/routing ospf network** o roteador fará o seguinte:

1. Ativará OSPF nas interfaces que tem um endereço de IP que estiver no range da rede adicionada.
2. Enviará a rede adicionada para os outros roteadores.



Ativando OSPF em toda a rede

Redes Brasil

MK-1

MK-3

MK-4

Operadora 1

MK-1

MK-3

MK-4

OSPF

Não existe rede 2

MK-5

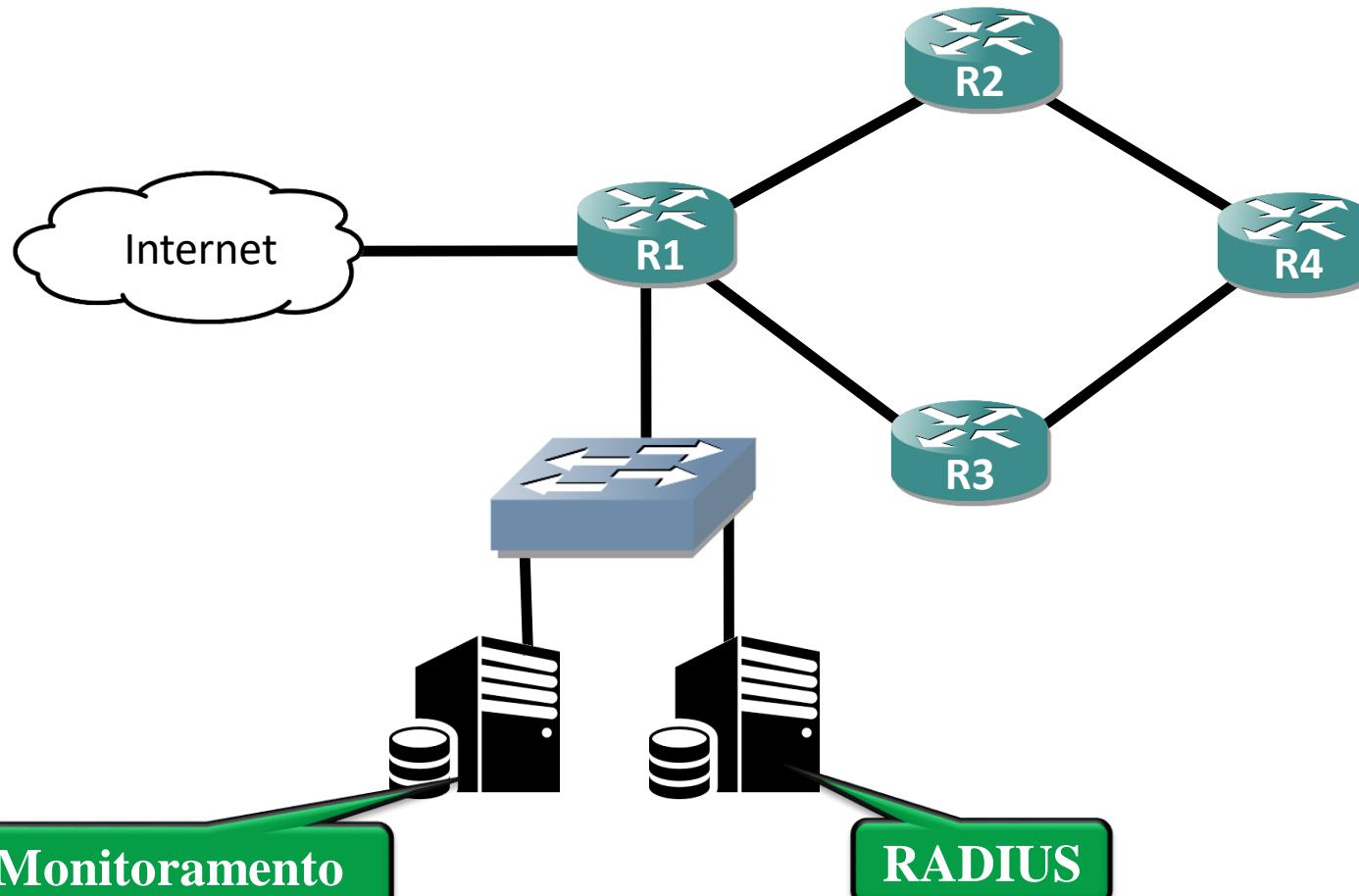
Neighbor (vizinhos) OSPF

- Os roteadores OSPF encontrados estão listados na aba Neighbours (vizinhos);
- Após a conexão ser estabelecida cada um irá apresentar um status operacional conforme descrito abaixo:
 - **Full:** Base de dados completamente sincronizada;
 - **2-way:** Comunicação bi-direcional estabelecida;
 - **Down,Attempt,Init,Loading,ExStart,Exchange:** Não finalizou a sincronização completamente.

OSPF						
Interfaces	Instances	Networks	Areas	Area Ranges	Virtual Links	Neighbors
<input type="button" value="Filter"/>						NBM
Instance	Router ID	Address	Interface	State Changes	State	
default	10.172.255.5	10.172.47.4	ether003...	13	Full	
default	10.172.255.8	10.172.200.7	ether009...	13	Full	
default	10.172.255.1	10.172.32.1	ether002...	5	Full	

Interface de loopback

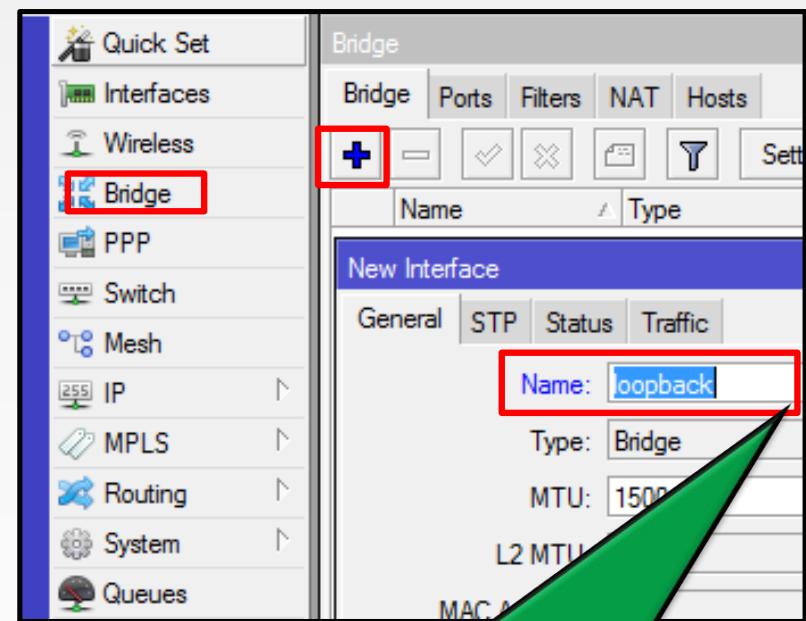
- Qual endereço de IP utilizar para monitoramento, RADIUS e acesso ?



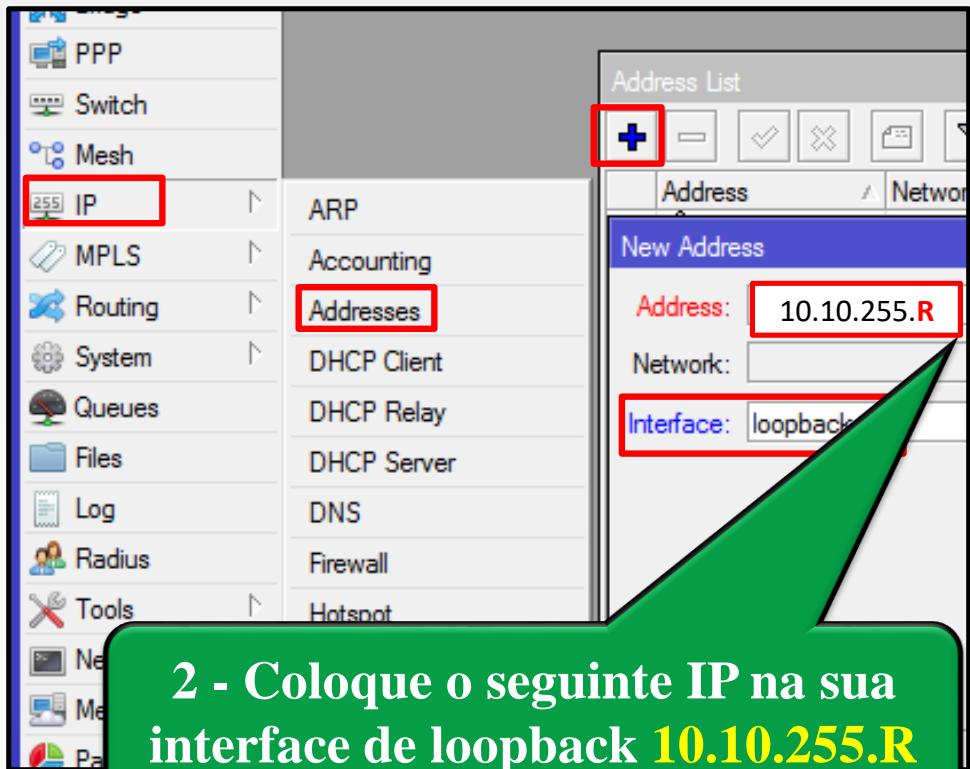
Interface de loopback

- Interface de loopback é uma interface virtual (por exemplo uma bridge) que nunca estará como status “down”.

Todos
roteadores



1 - Adicione a bridge e altere o nome para “loopback”



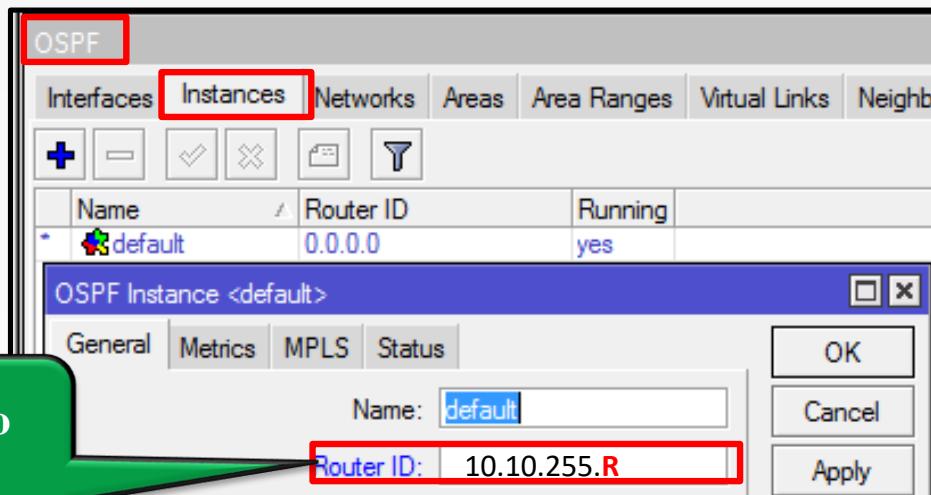
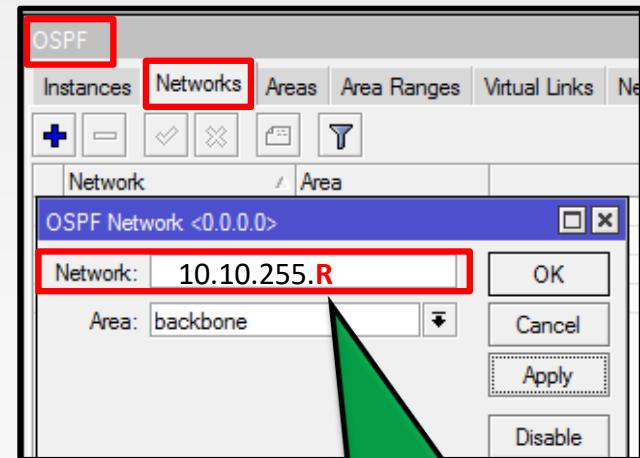
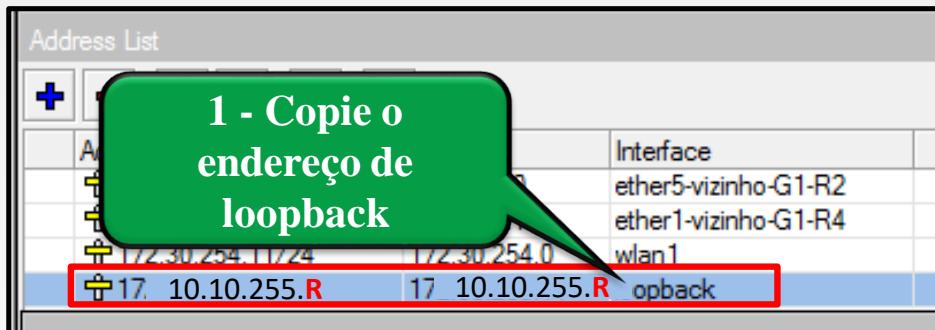
2 - Coloque o seguinte IP na sua interface de loopback **10.10.255.R**



Router ID e loopback

- Cada roteador precisa ser identificado na rede com um ID único, caso esse ID não for especificado manualmente o roteador usará o **menor IP ativo** que existir em sua “IP list”.
- É uma boa prática utilizar o endereço de loopback como RouterID
- Para ter acesso ao roteador pelo IP de loopback é necessário adicionar o endereço em OSPF - Networks

**Todos
roteadores**



OSPF – Hello e Ded Interval

- **Hello** Responsável pela descoberta e de routers vizinhos
 - São enviados a cada 10s
- **Dead Interval** – Tempo de espera até considerar o roteador vizinho morto.
- **Hello e Dead Intervals** tem que ser o mesmo valor entre os roteadores caso contrario não formará adjacência.
- **Restrasmit Interval** – Tempo que aguardará a confirmação do recebimento de LSA.

OSPF – States

- **Down** – Não recebeu nenhum pacote hello.
- **Attempt** – Apenas para redes NBMA, nenhuma informação nova foi recebida.
- **Init** – O Router não recebeu no pacote hello seu RouterID
- **2-Way** – Comunicação Bi-direcional estabelecida neste ponto ocorre a eleição de DR e BDR.
- **Ex-Start** – Definem uma sequencia para iniciar a transmissão de informações. O Router com ID mais alto é quem incia.
- **Exchange** – Trocam pacotes de descrição do banco de dados
- **Loading** – São trocado as informações states link.
- **FULL** – Adjacencia ok com DR e BDR ou Point to Point.



OSPF Instance

- **Router ID:** Geralmente o IP do roteador. Caso não seja especificado o roteador usará o menor IP que exista na interface.
- **Redistribute Default Route:**
 - **Never:** nunca distribui rota padrão.
 - **If installed (as type 1):** Envia com métrica 1 se tiver sido instalada como rota estática, DHCP ou PPP (*BGP).
 - **If installed (as type 2):** Envia com métrica 2 se tiver sido instalada como rota estática, DHCP ou PPP (*BGP).
 - **Always (as type 1):** Sempre, com métrica 1.
 - **Always (as type 2):** Sempre, com métrica 2.
- **Redistribute Connected Routes:** O roteador irá distribuir todas as rotas estejam diretamente conectadas a ele.
- **Redistribute Static Routes:** Caso habilitado, distribui as rotas cadastradas de forma estática em /ip routes.
- **Redistribute RIP Routes:** Caso habilitado, redistribui as rotas aprendidas por RIP.
- **Redistribute BGP Routes:** Caso habilitado, redistribui as rotas aprendidas por BGP.
- Na aba “Metrics” é possível modificar as métricas que serão exportadas as diversas rotas

OSPF Instance <default>

General	Metrics	MPLS	Status
Name: default			
Router ID: 10.10.255.R			
Redistribute Default Route: never			
Redistribute Connected Routes: no			
Redistribute Static Routes: no			
Redistribute RIP Routes: no			
Redistribute BGP Routes: no			
Redistribute Other OSPF Routes: no			

OSPF Instance <default>

General	Metrics	MPLS	Status
Default Route Metric: 1			OK
Connected Routes Metric: 20			Cancel
Static Routes Metric: 20			Apply
RIP Routes Metric: 20			Disable
BGP Routes Metric:			Comment
Other OSPF Routes Metric:			Copy
			Remove

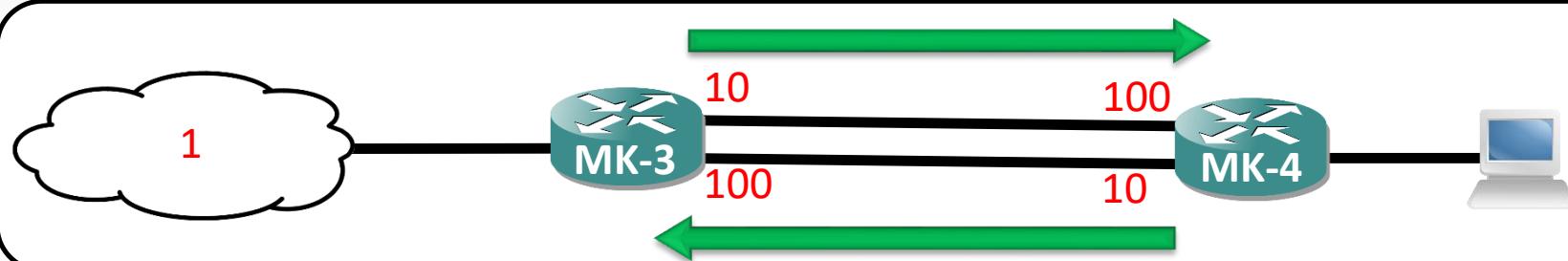
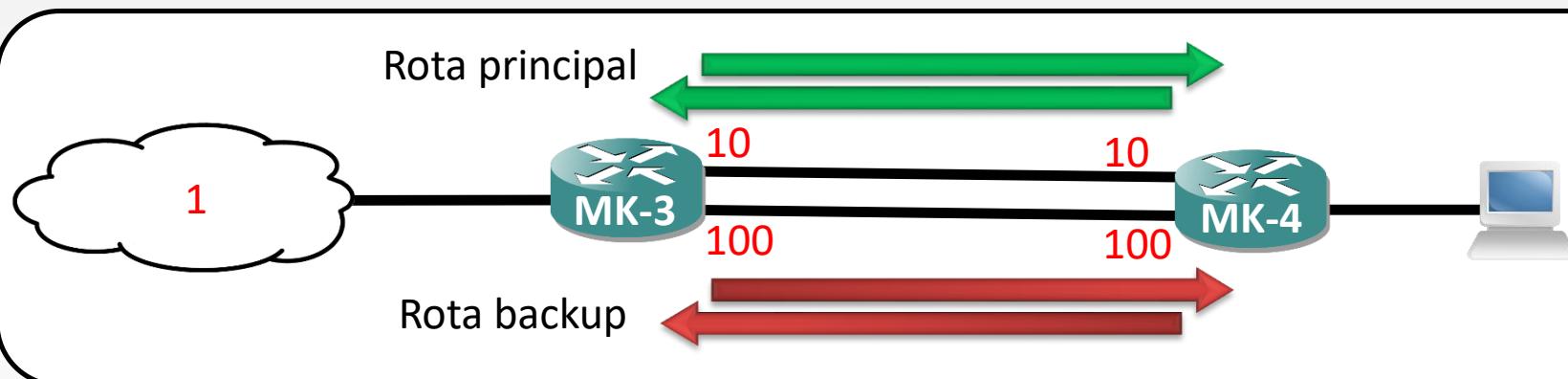
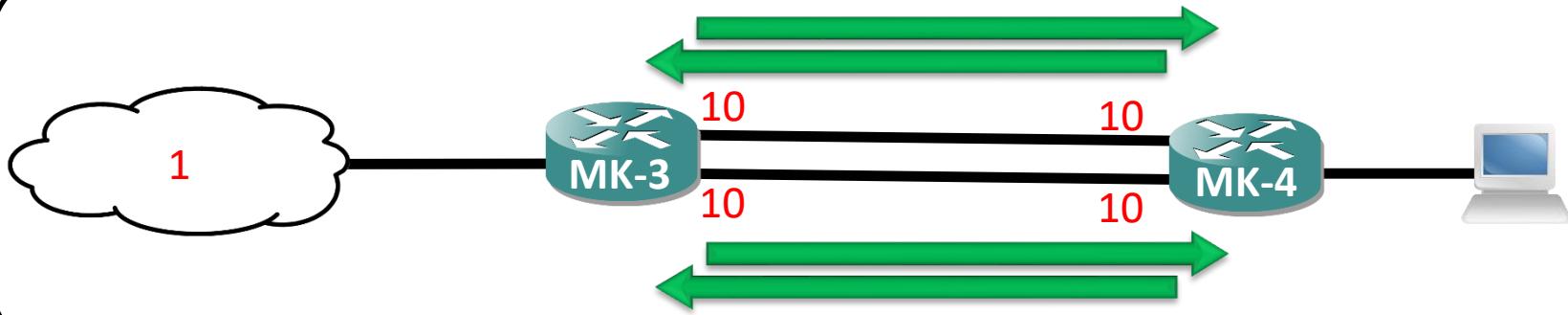
OSPF – Custo de interfaces

- Por padrão todas interfaces tem custo 10.
- Para alterar este padrão você deve adicionar interfaces de forma manual.
- Escolha o tipo de rede correta para todas interfaces OSPF.

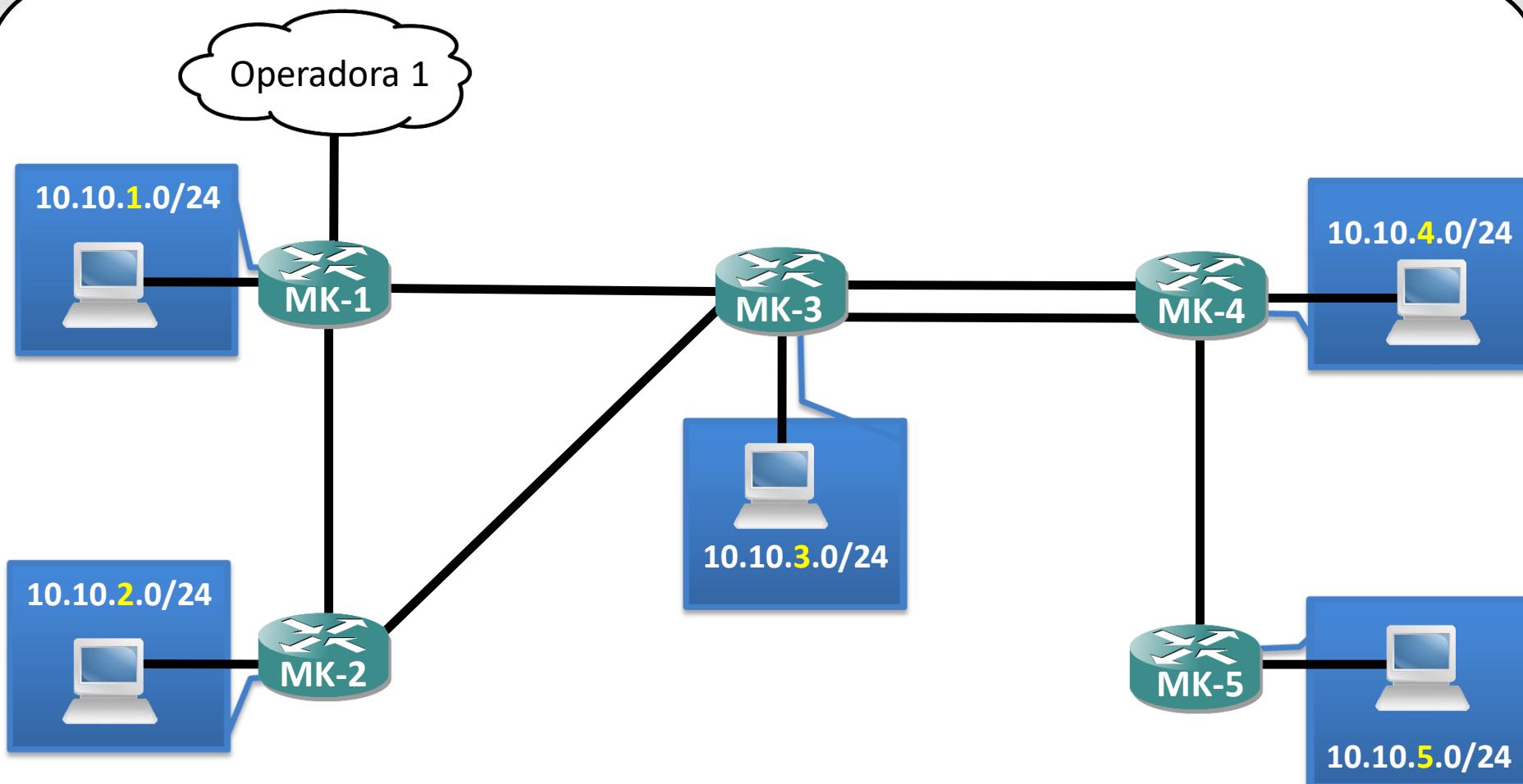
- Verifique rotas ECMP em sua tabela de roteamento.
- Atribua custos necessários para que o link backup só seja usado caso outros links falhem.
- Verifique a redundância da rede OSPF.

Manipulando custos

Redes Brasil

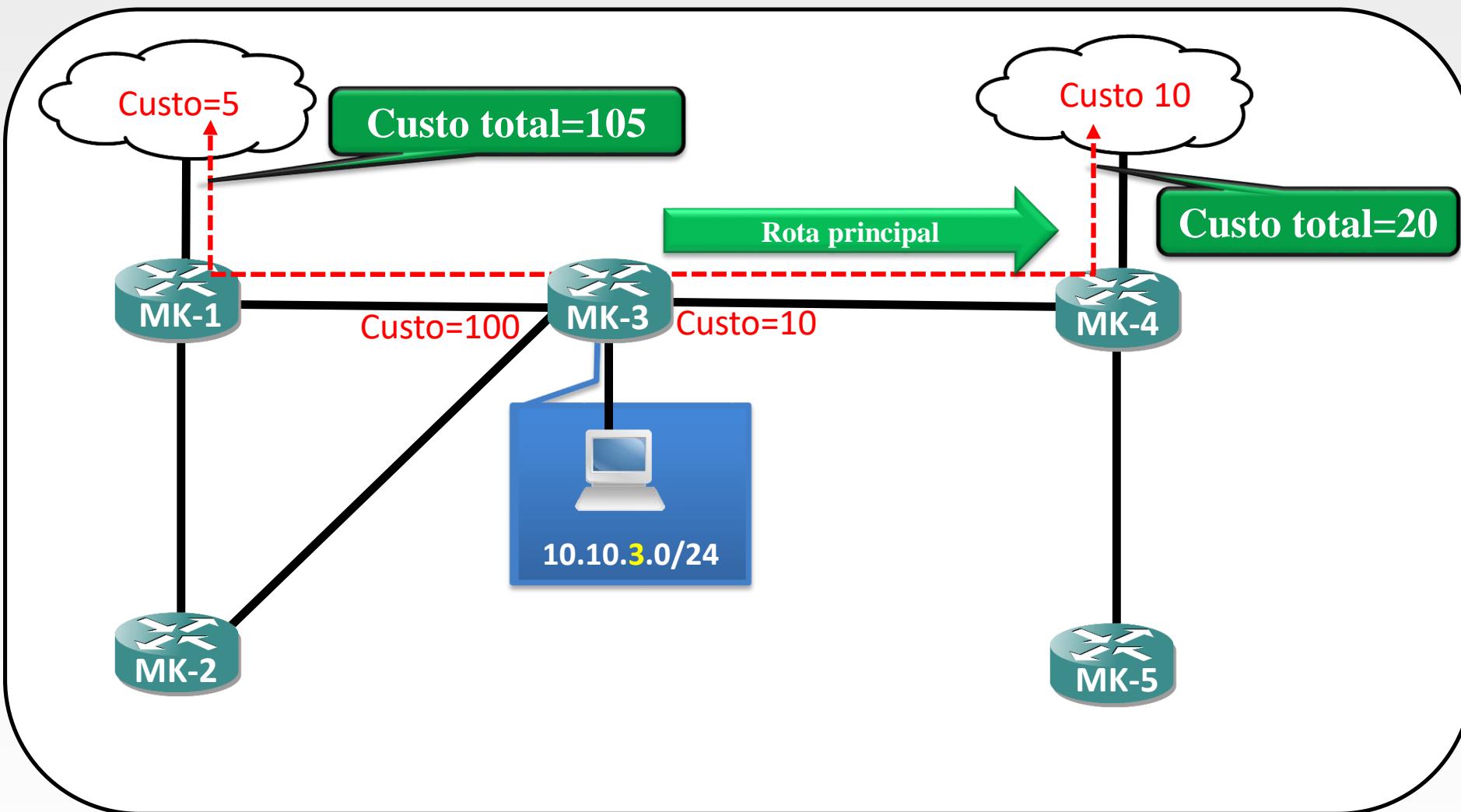


Manipulando custos



Métrica tipo 1

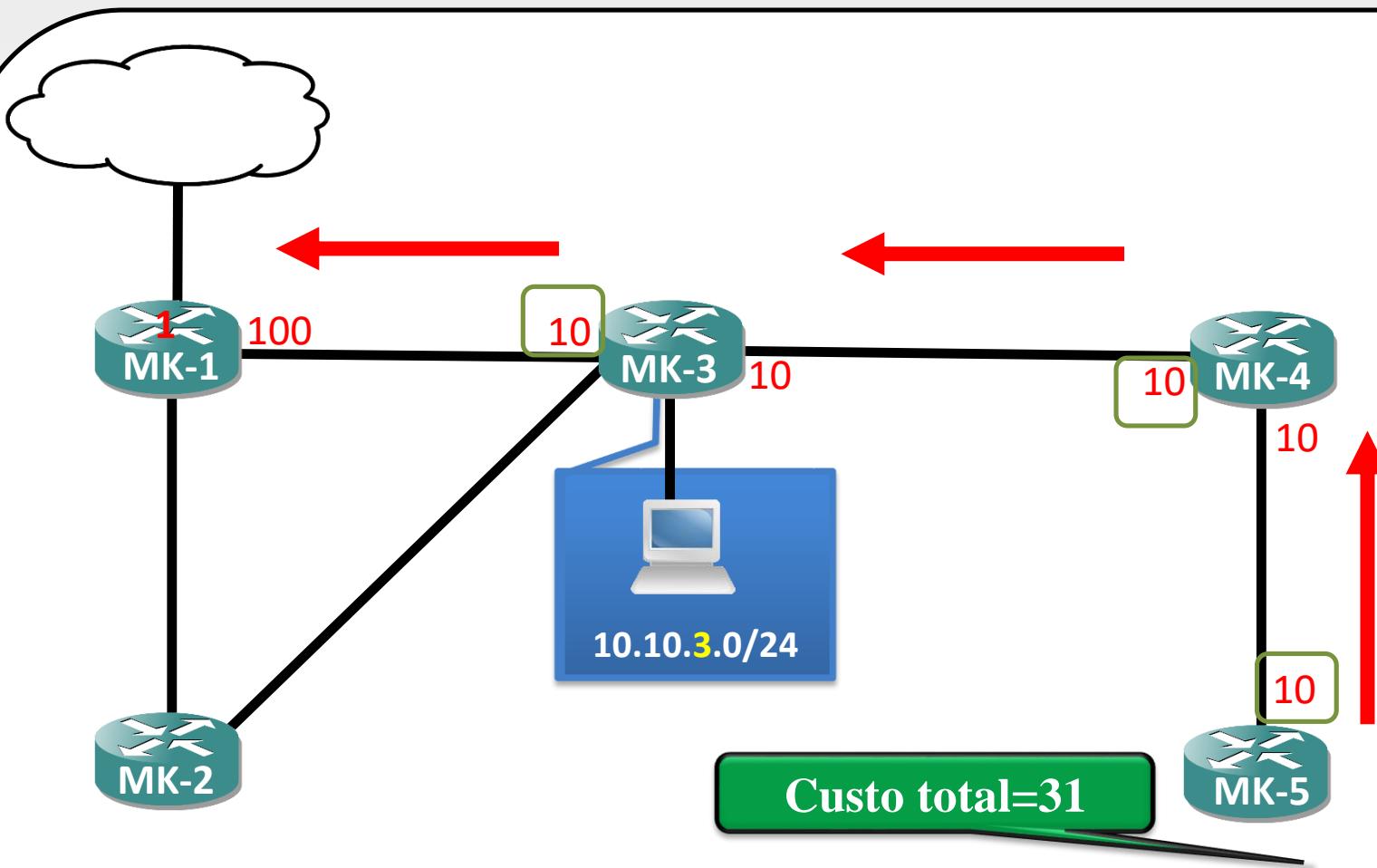
- Métrica do tipo 1 soma o custo externo com o custo interno.





Métrica tipo 1 – Rota Default

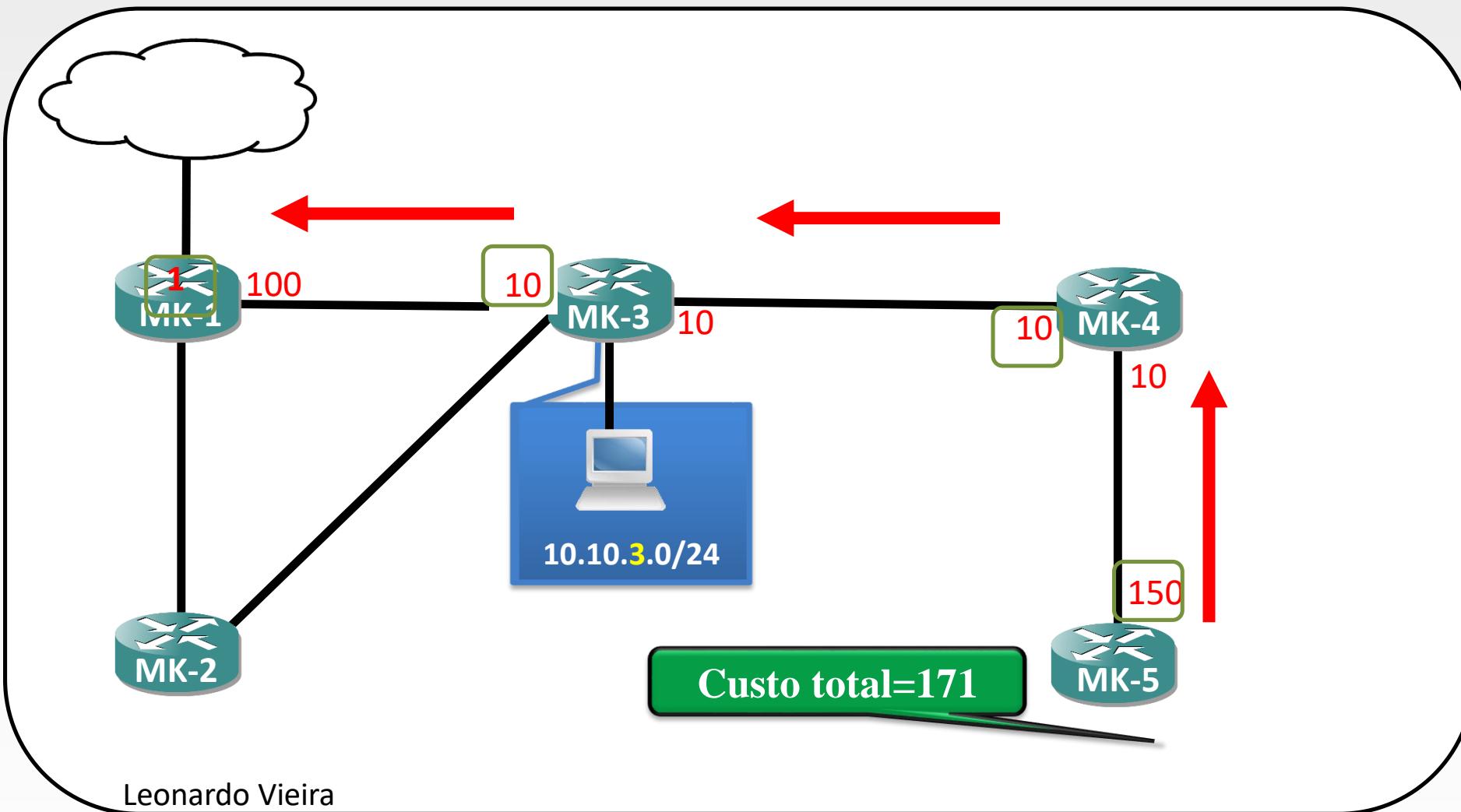
- Métrica do tipo 1 soma o custo externo com o custo interno.





Métrica tipo 1 – Rota Default

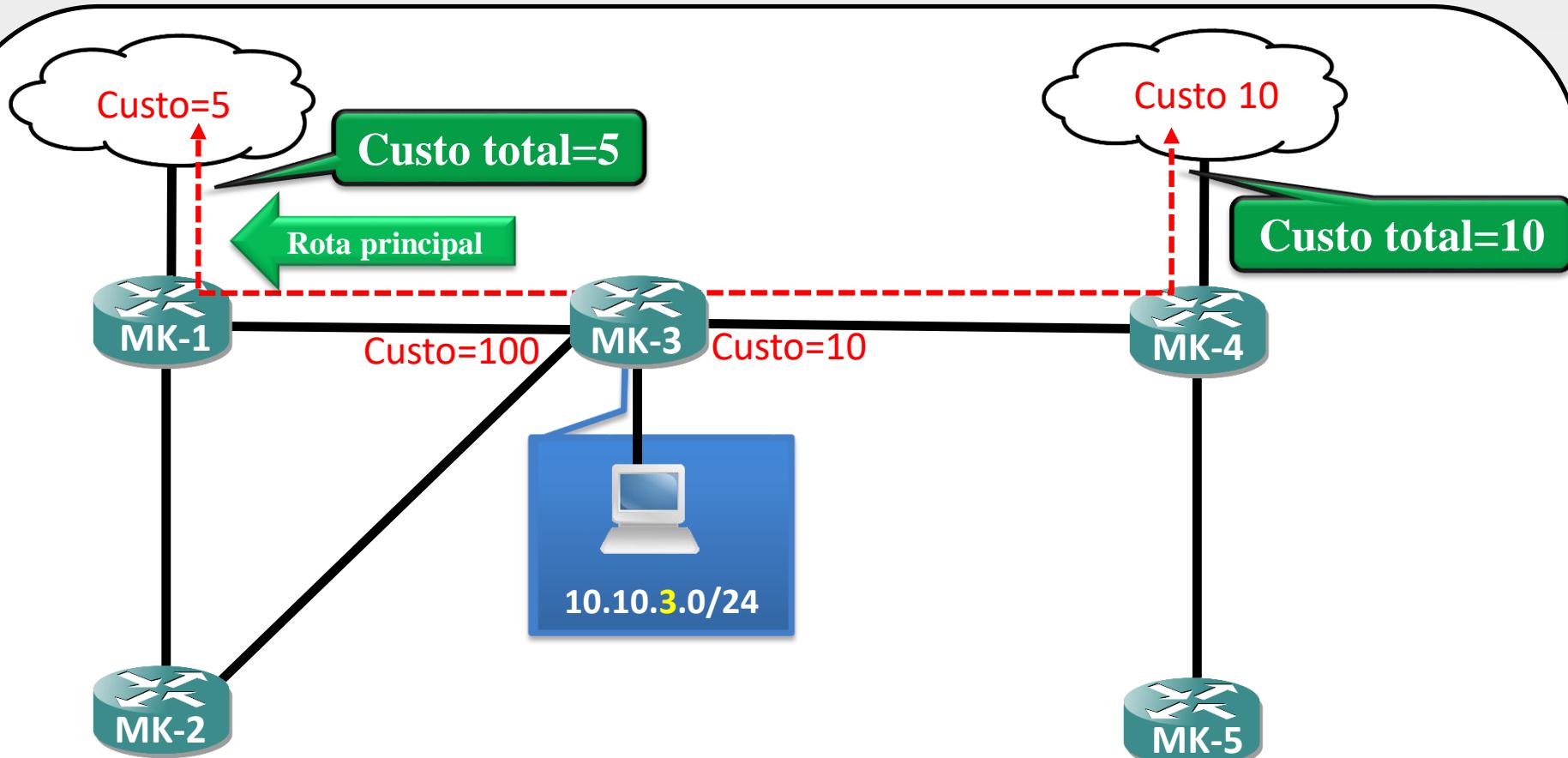
- Métrica do tipo 1 soma o custo externo com o custo interno.





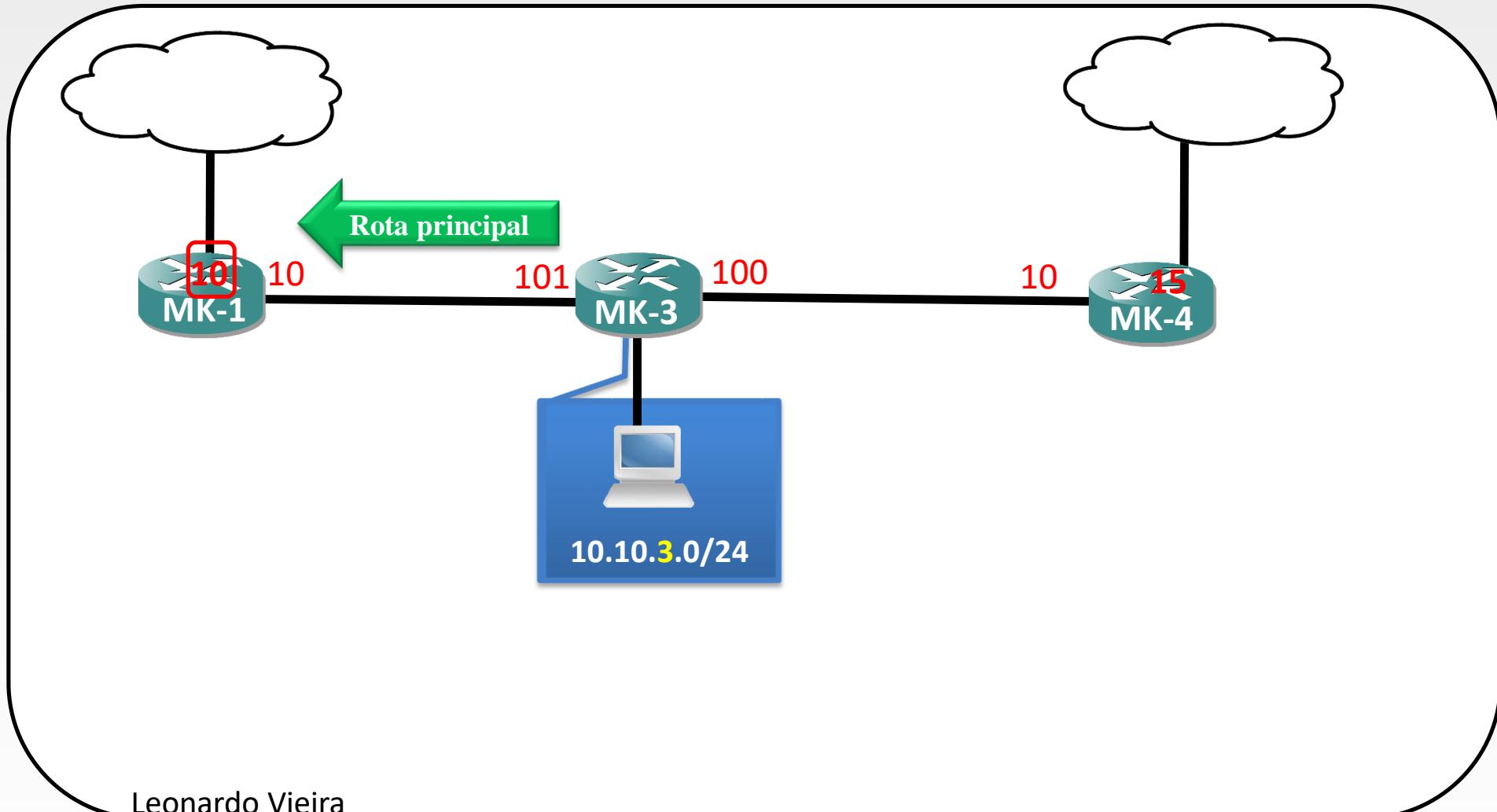
Métrica tipo 2

- Métrica do tipo 2 usa somente o custo externo.



Métrica tipo 2- Rota Default

- Métrica do tipo 2 usa somente o custo externo.





Métrica Rota Externa

OSPF

Interfaces Instances Networks Areas Area Ranges Virtual Links Neighbors NBMA Neighbors

OSPF Instance <default>

General Metrics MPLS Status

Default Route Metric: 1

Connected Routes Metric: 20

Static Routes Metric: 20

RIP Routes Metric: 20

BGP Routes Metric:

Other OSPF Routes Metric:

OK Cancel Apply Disable Comment Copy Remove

1 item (1 selected)

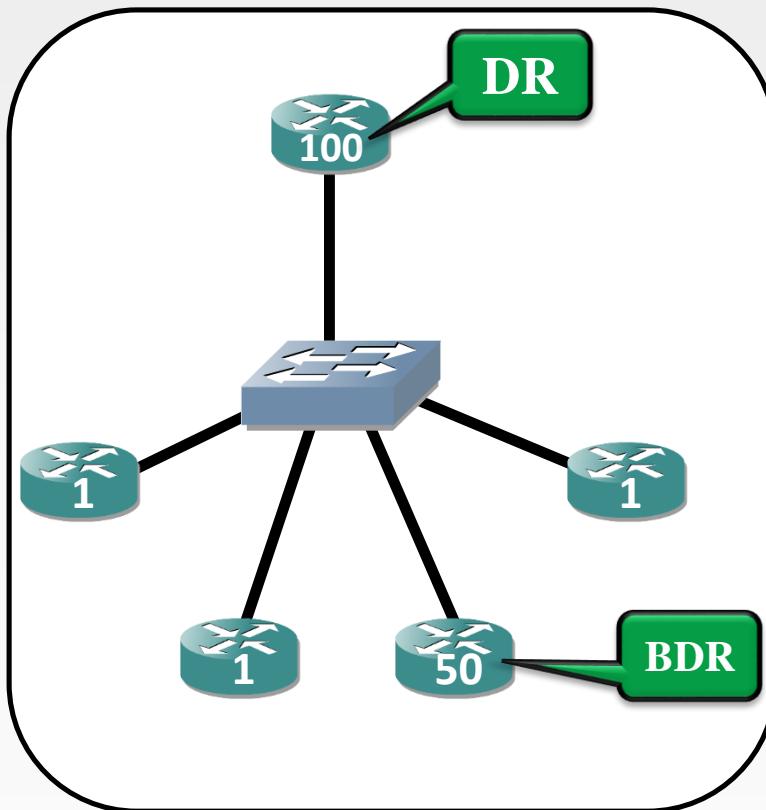
enabled default

The screenshot shows a network configuration interface for OSPF. On the left, there's a tree view with 'Interfaces' selected. In the center, a dialog box for 'OSPF Instance <default>' is open, specifically on the 'Metrics' tab. This tab contains fields for various route types: Default Route Metric (set to 1), Connected Routes Metric (set to 20), Static Routes Metric (set to 20), RIP Routes Metric (set to 20), BGP Routes Metric (empty), and Other OSPF Routes Metric (empty). The dialog also includes tabs for General, MPLS, and Status, and buttons for OK, Cancel, Apply, Disable, Comment, Copy, and Remove. At the bottom of the dialog, it says '1 item (1 selected)'. At the very bottom of the interface, there are buttons for 'enabled' and 'default'.



Designated router OSPF

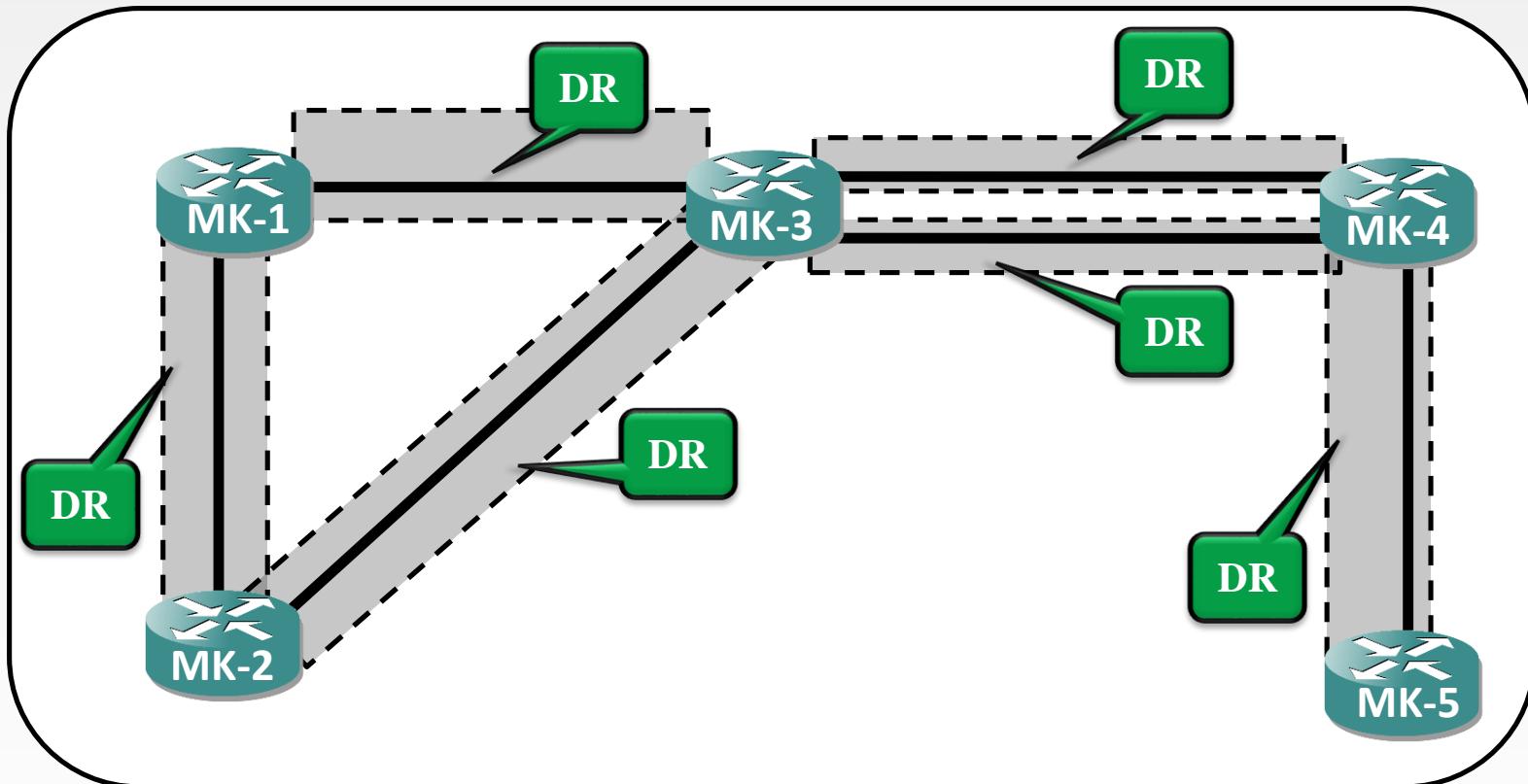
- Para reduzir o tráfego OSPF em redes **broadcast** e **NBMA** (Non-Broadcast Multiple Access), uma única fonte para atualização de rotas é criado (os roteadores designados(DR)).
- Um DR mantém uma tabela completa da topologia da rede e envia atualizações para os demais roteadores.
- O roteador com **maior prioridade** será eleito como DR.
- Também será eleito roteadores backup BDR.
- Roteadores com prioridade 0 nunca serão DR ou BDR.
- Caso a prioridade for igual em todos os roteadores, o DR será eleito usando o **maior** valor especificado no routerID





Quantos DRs tem minha rede?

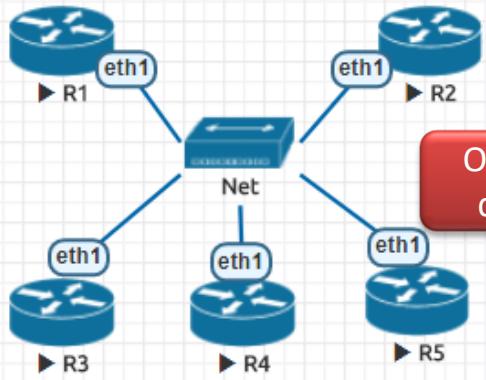
- A eleição de DR e BDR acontece em todas as redes do tipo broadcast e NBMA



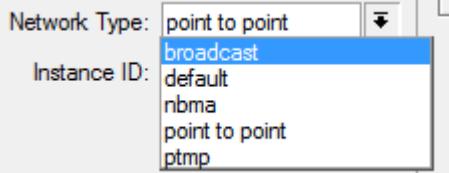


Tipos de rede

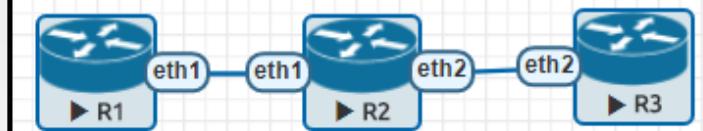
Broadcast



Ocorre eleição de DR e BDR

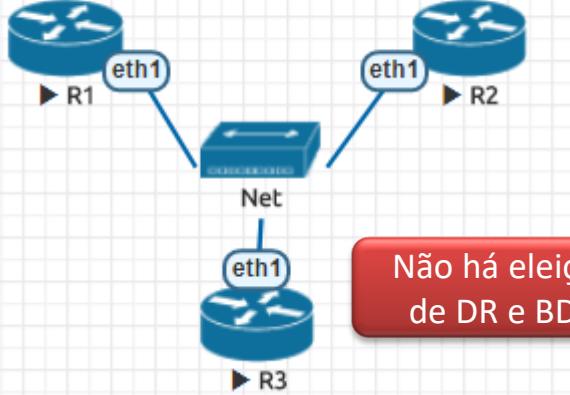


Point to point



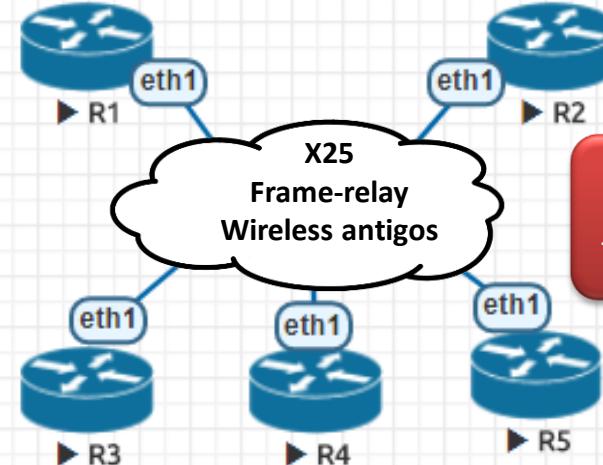
Não há eleição de DR e BDR

PTMP – Point to multipoint



Não há eleição de DR e BDR

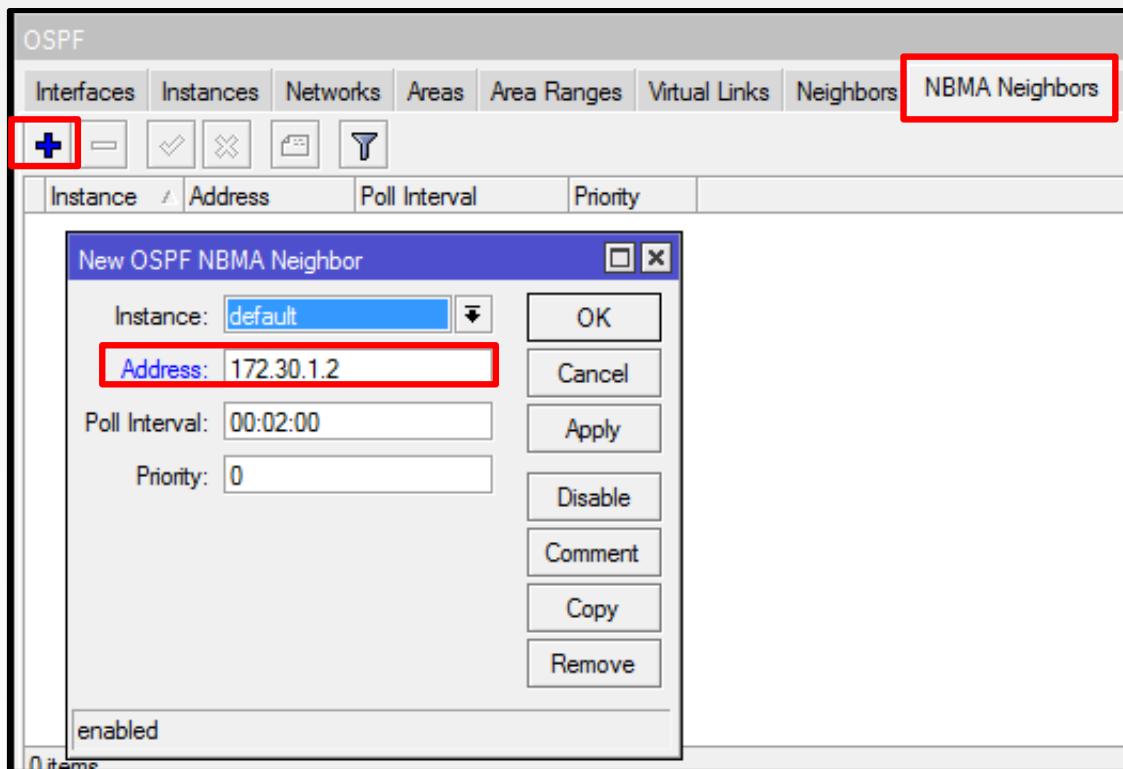
NBMA - Nonbroadcast multiaccess



- Utiliza endereços de unicast
- Ocorre eleição de DR e BDR.

NBMA Neighbors

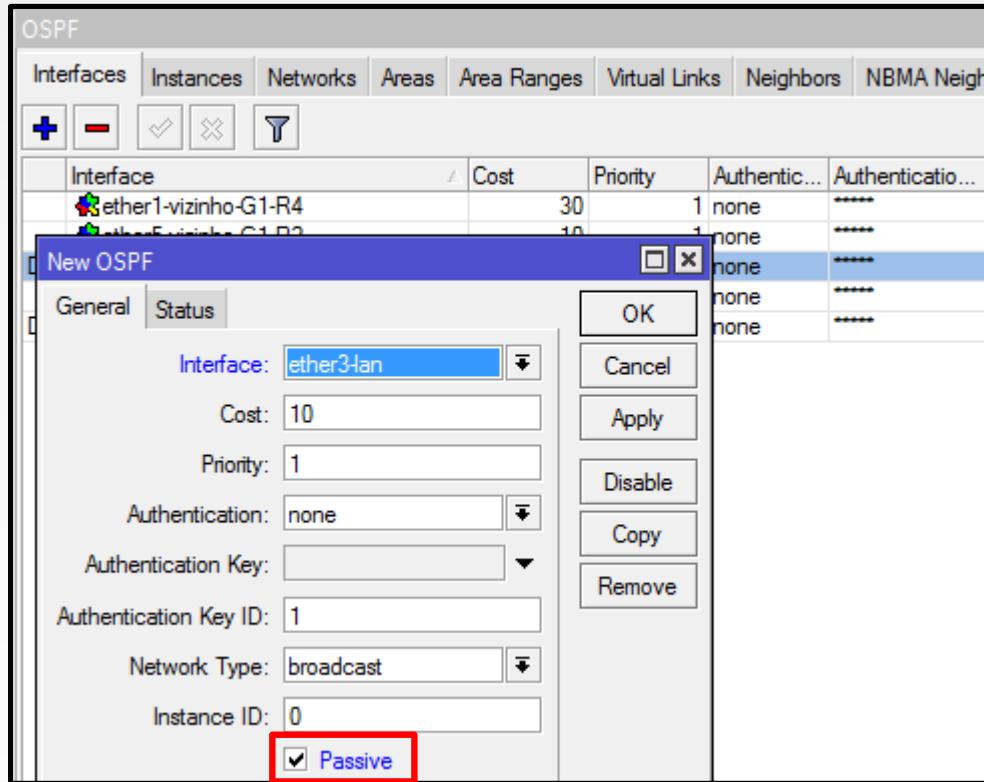
- Em redes não-broadcast “ex: Frame Relay” é necessário especificar os neighbors manualmente.
- A prioridade determina a chance do router ser eleito DR.





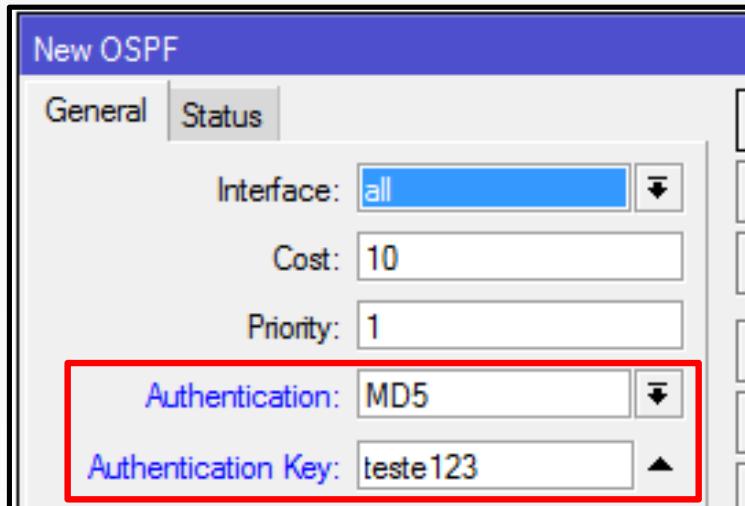
Interface Passiva

- O modo passivo permite desativar as mensagens de “Hello” enviadas pelo protocolo OSPF as interfaces dos clientes (desativa OSPF na interface).
- Portanto ativar este recurso é sinônimo de segurança.



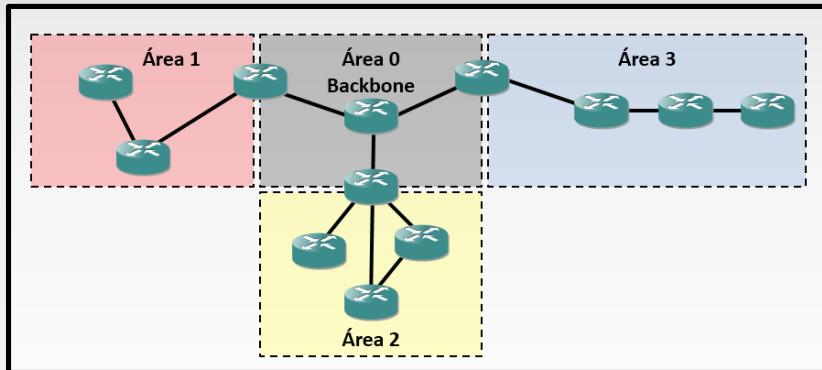
OSPF autenticação

- O MikroTik suporta os seguintes métodos de autenticação.
 - **None**: Não utiliza método de autenticação.
 - **Simples**: Autenticação em texto plano.
 - **MD5**: Autenticação com encriptação md5.





Áreas OSPF

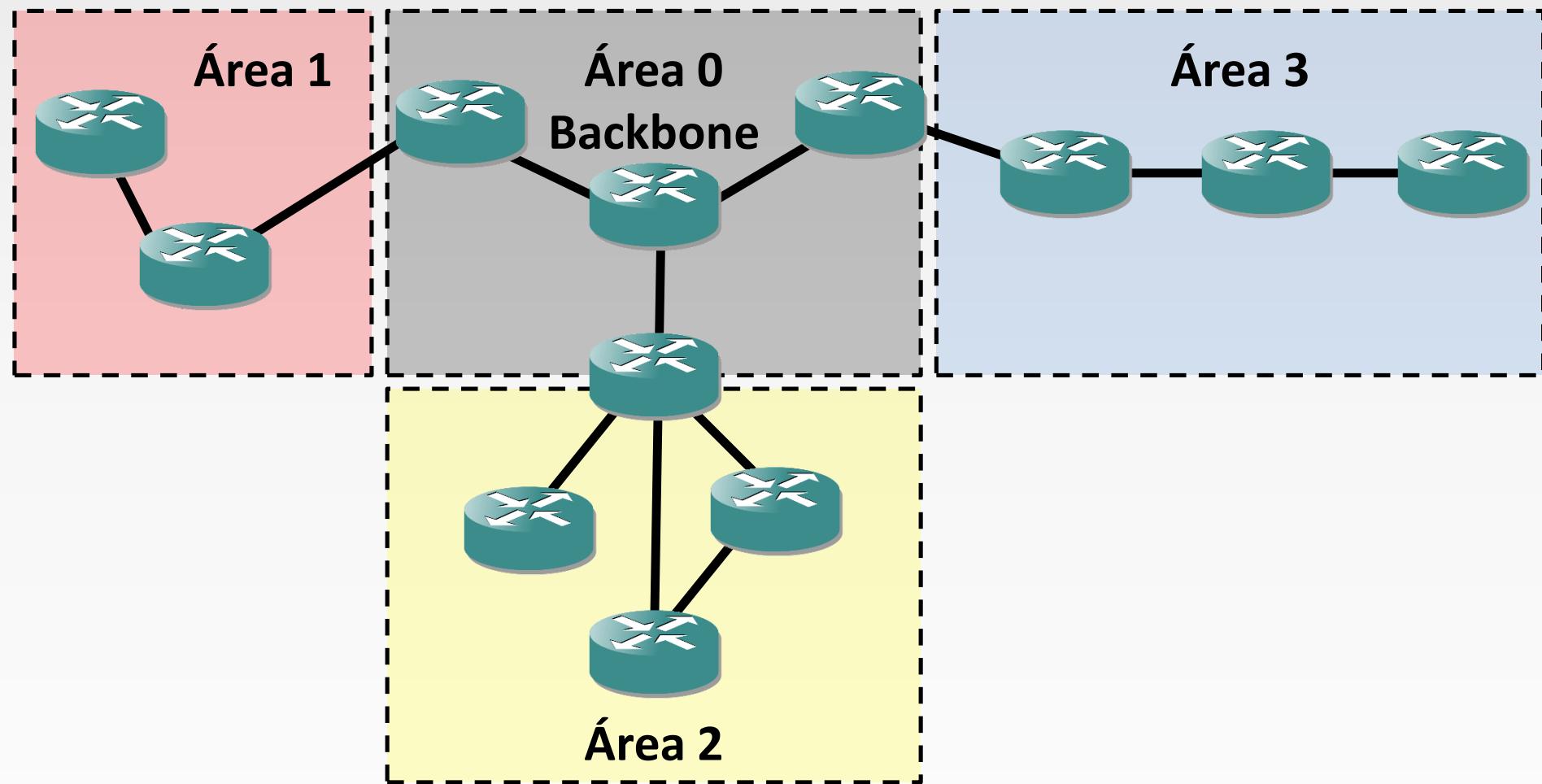


- A criação de áreas permite você agrupar uma coleção de roteadores (indicado nunca ultrapassar 50 roteadores por área).
- A estrutura de uma área não é visível para outras áreas.
- Cada área executa uma cópia única do algoritmo de roteamento.
- As áreas OSPF são identificadas por um número de 32 bits(0.0.0.0 – 255.255.255.255).
- Esses números devem ser únicos para o AS.

Área de backbone

- A área backbone é o coração da rede OSPF. Ela possui o ID (0.0.0.0) e deve sempre existir.
- A backbone é responsável por redistribuir informações de roteamento entre as demais áreas.
- As demais áreas devem sempre estar conectadas a uma área backbone de forma direta ou indireta(utilizando virtual link).

Exemplo de AS e várias áreas

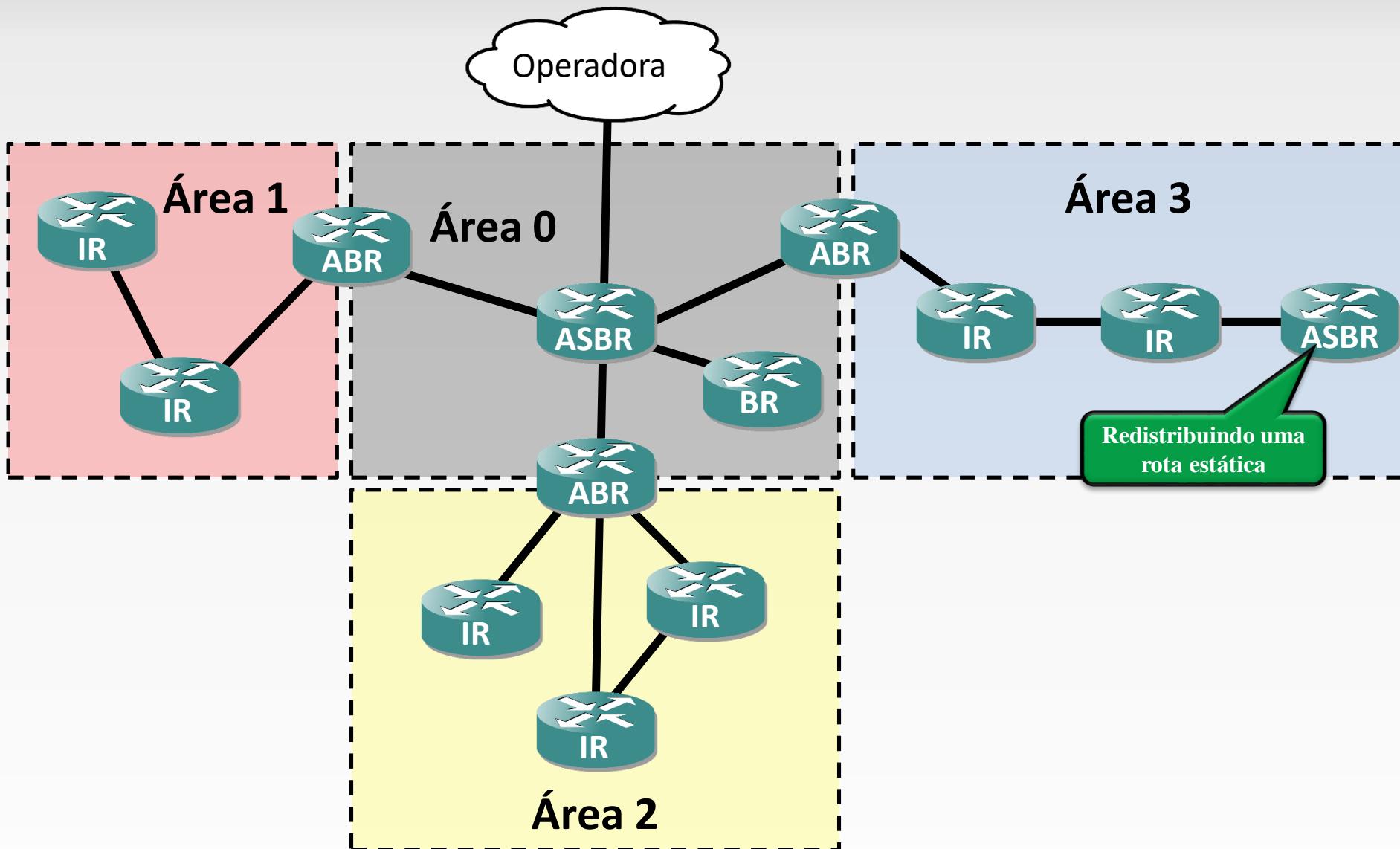


Tipos de roteadores no OSPF

- Tipos de roteadores em OSPF são:
 - Roteadores de borda Autonomous System (**ASBR**).
 - São roteadores que redistribuem rotas externas ao AS.
 - Roteadores de backbone (**BR**).
 - Roteadores internos a uma área (**IR**).
 - Roteadores de borda de área (**ABR**).
 - OS ABRs devem ficar entre duas áreas e devem tocar a área 0.



Tipos de roteadores no OSPF

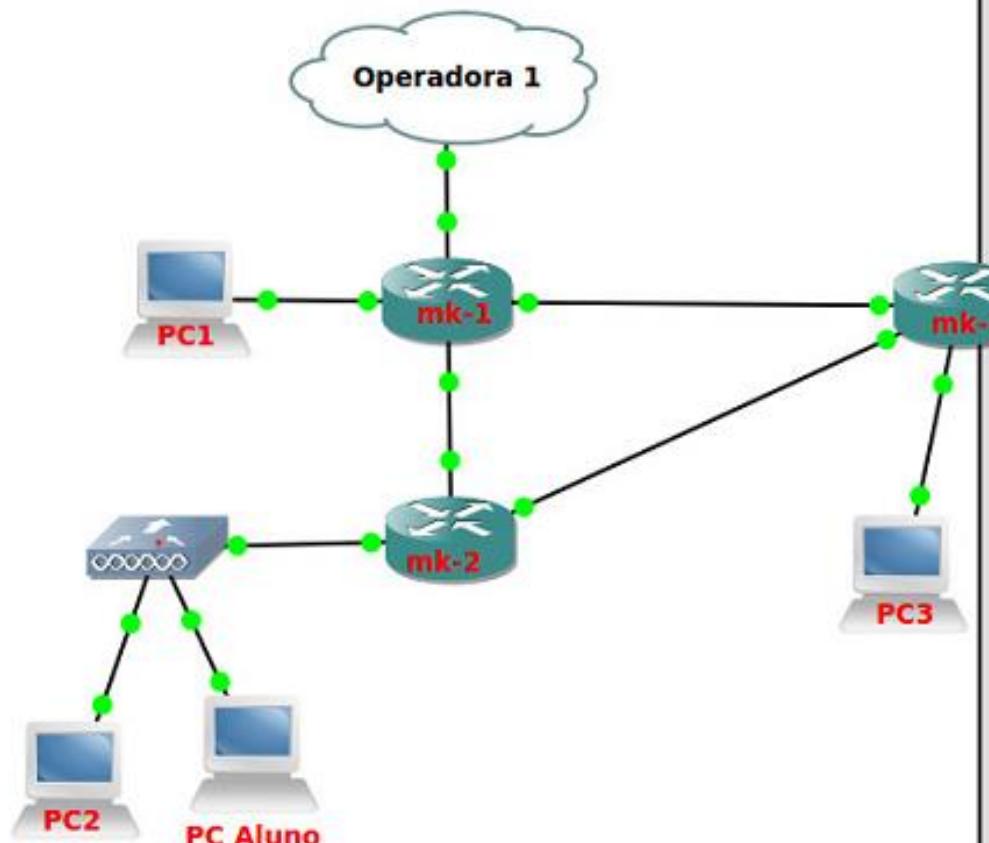


Implementando áreas no OSPF

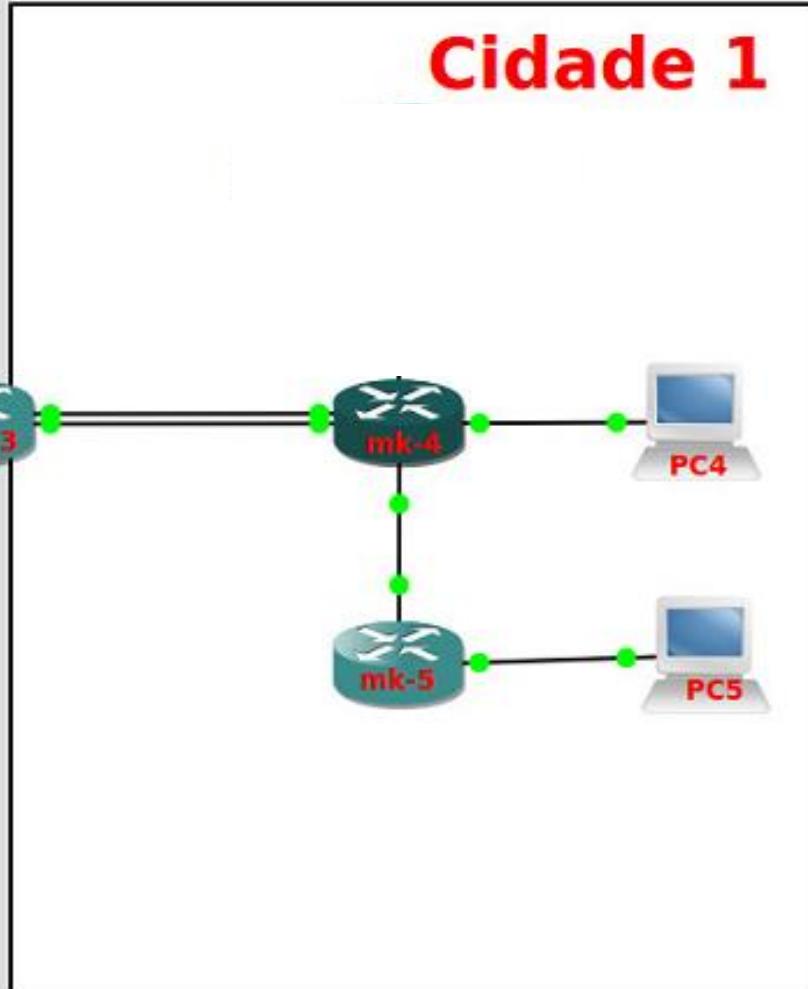


Redes Brasil

Cidade 0



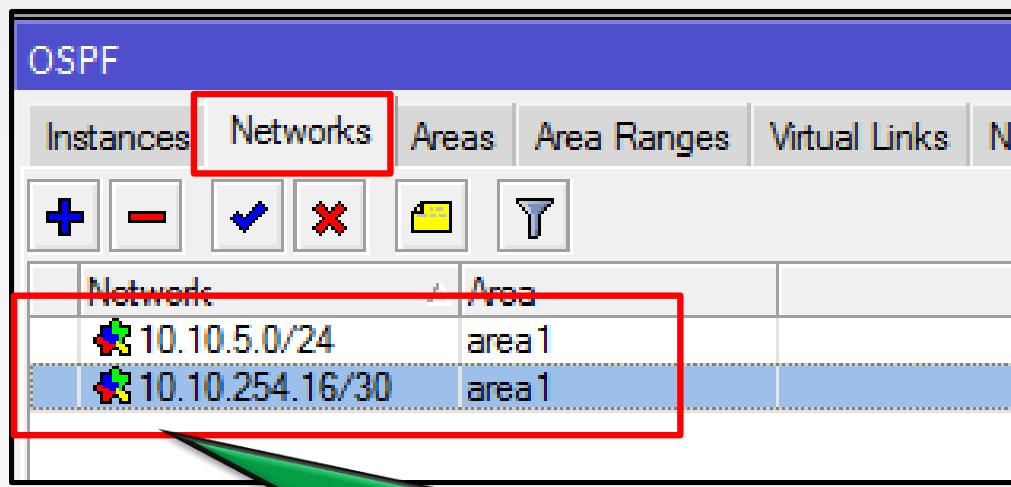
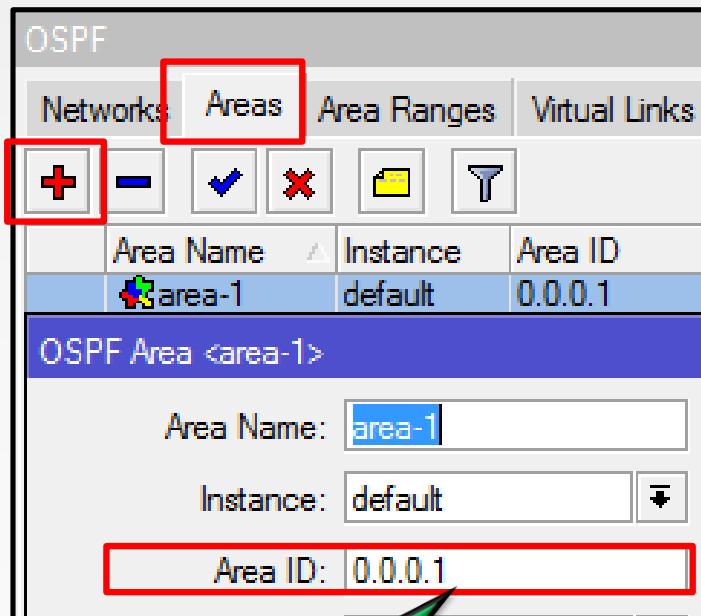
Cidade 1



Implementando áreas no OSPF

- Exemplo de configuração do roteador MK-5

MK-3 MK-4 MK-5

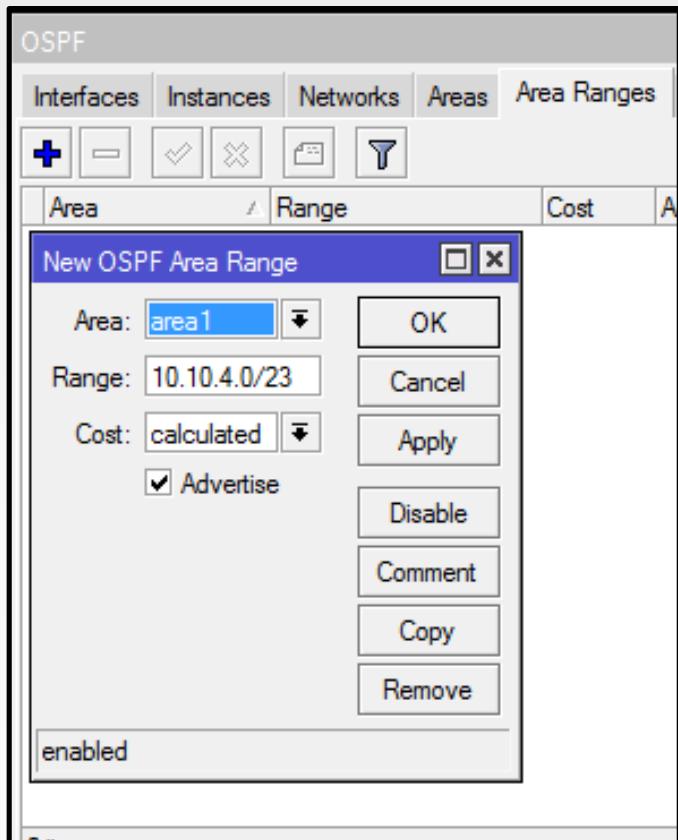


1 - Crie a área1

2 - Altere as redes do OSPF para funcionar nas áreas corretas de acordo com a imagem anterior



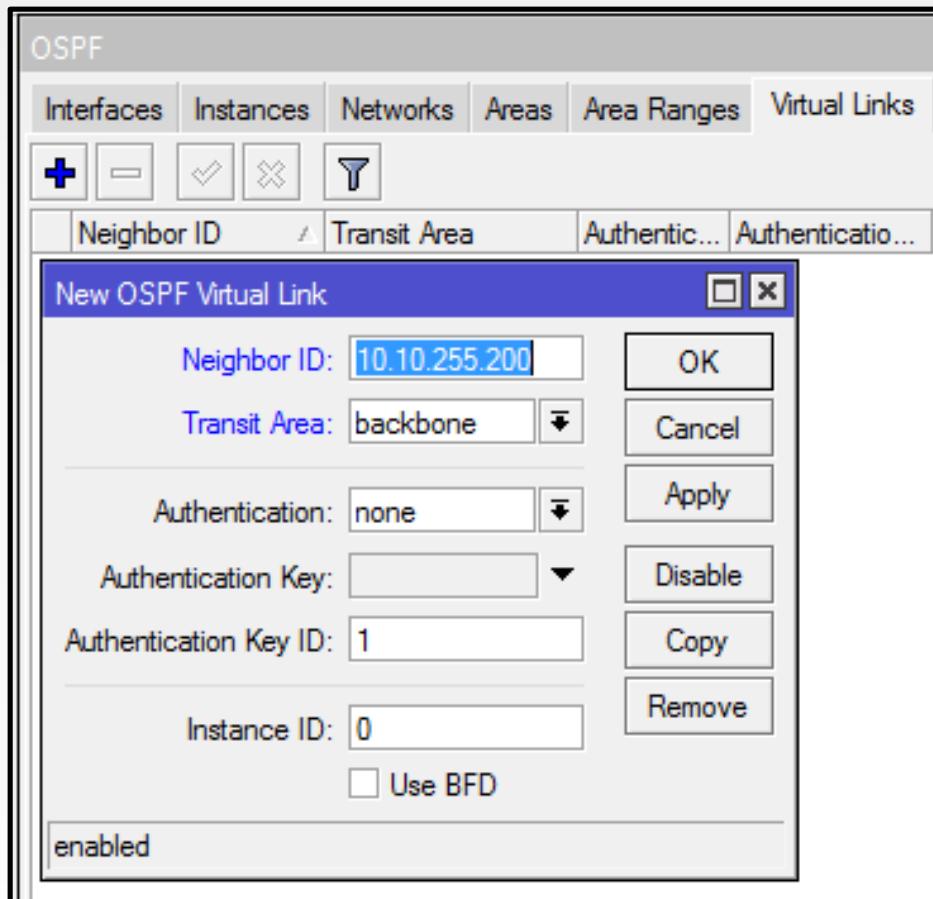
Agregação de áreas



- Utilizado para agregar uma range de redes em uma única rota.
- É feita sempre nos roteadores de borda de área (**ABRs**).
- É possível atribuir um custo para essas rotas agregadas.
- Ao criar uma agregação lembre-se de especificar a qual área aquele prefixo pertence.

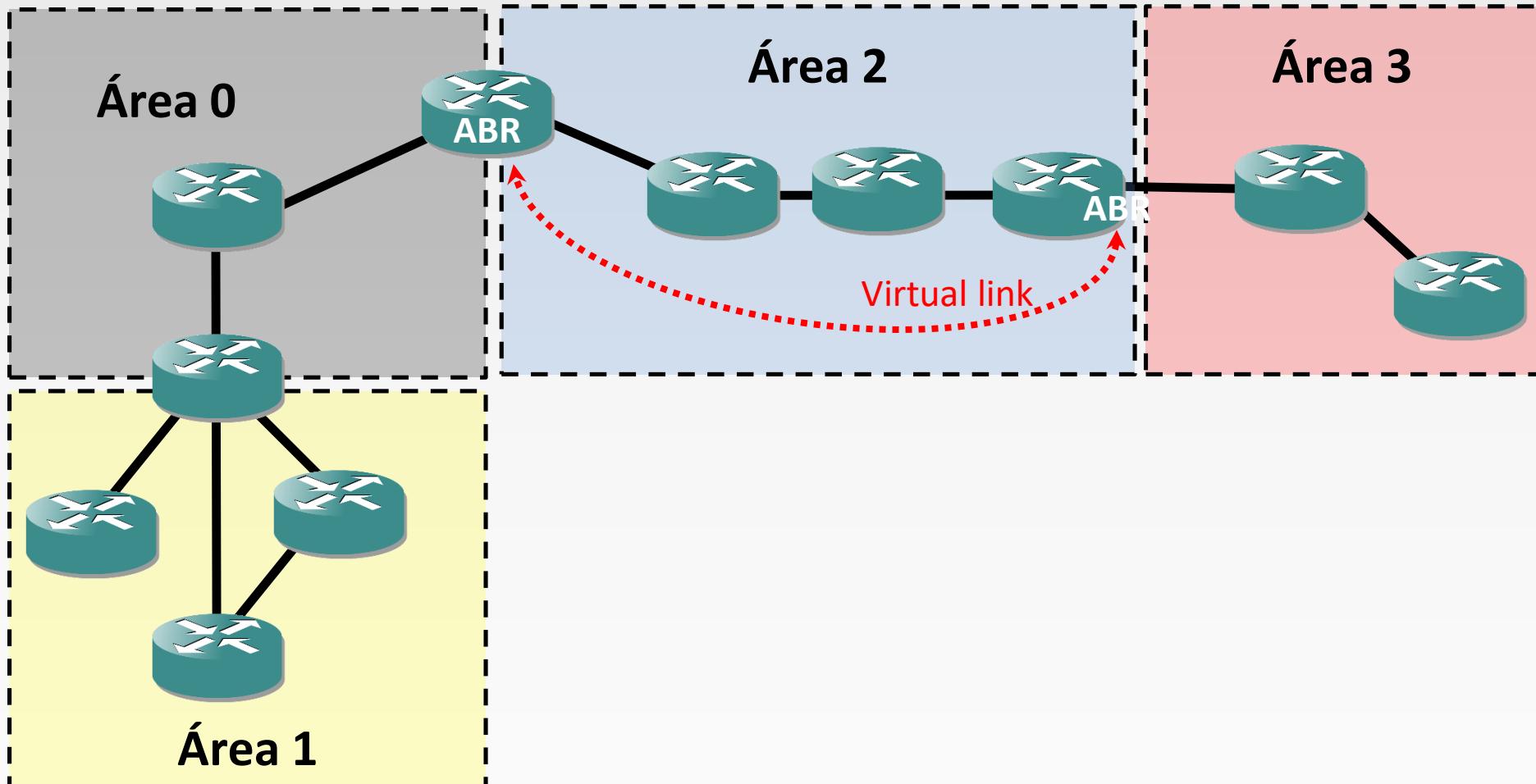
Virtual Link

- Utilizado conectar áreas remotas ao backbone através de áreas não-backbone;



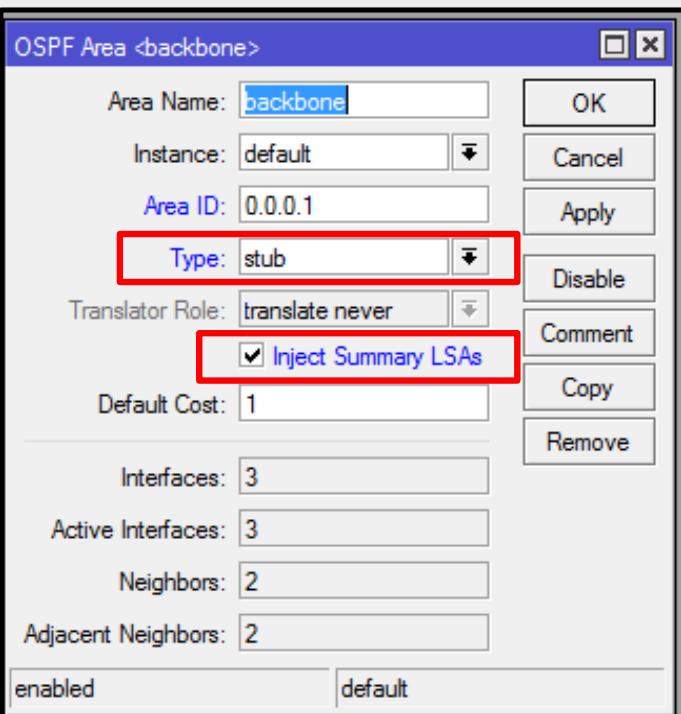
Virtual Link

Redes Brasil





Área Stub

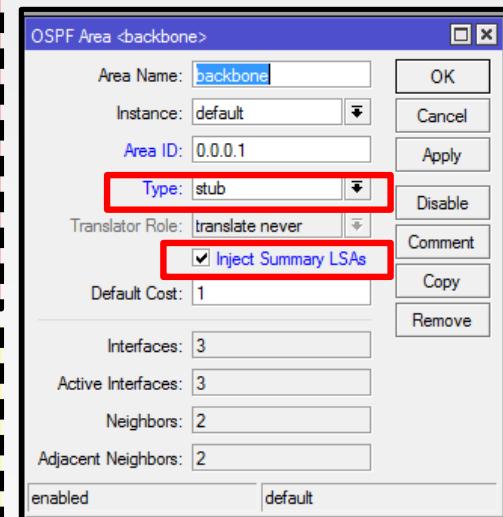
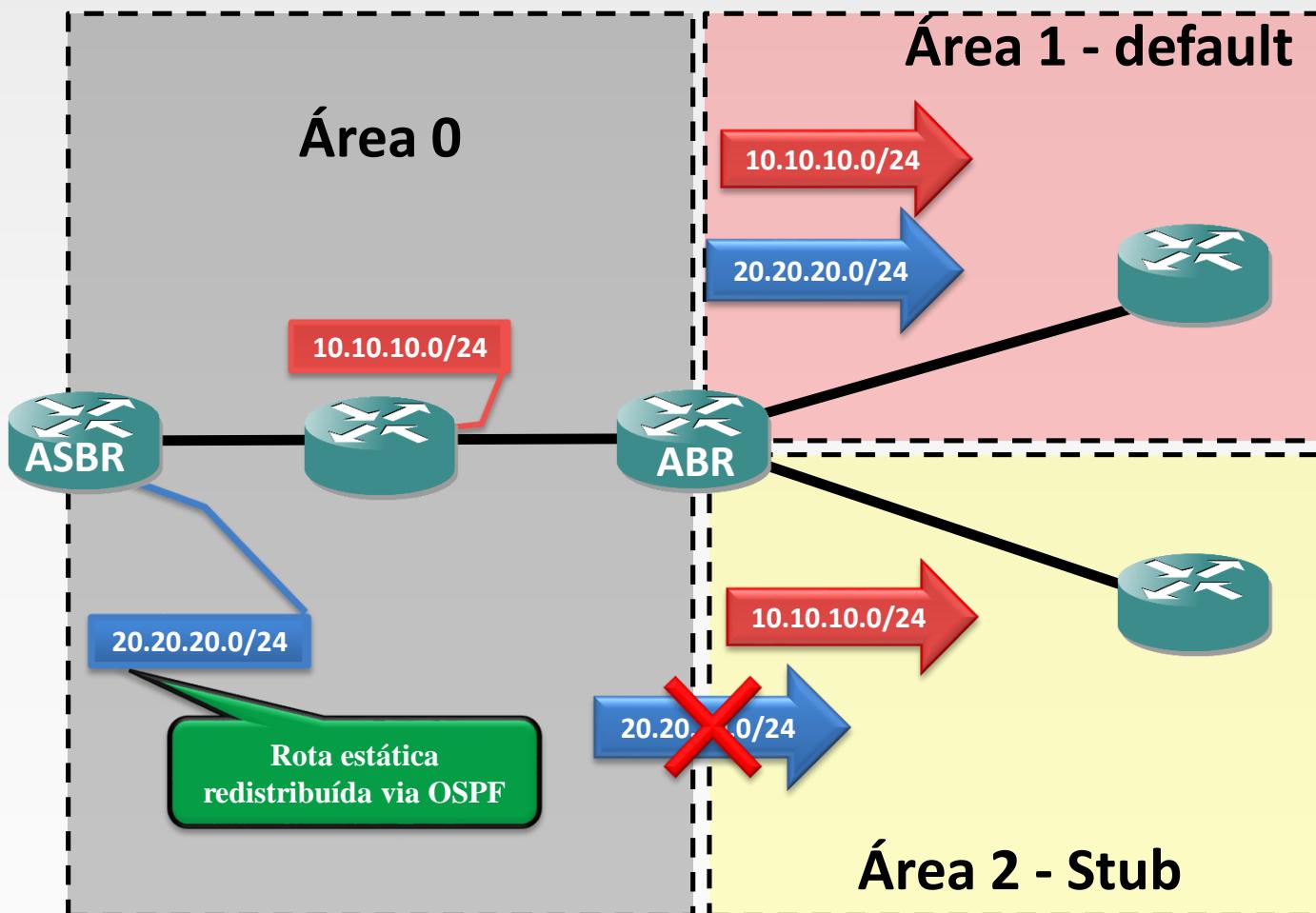


- Uma área Stub é uma área que não recebe rotas de AS externos;
- Tipicamente todas rotas para os AS externos são substituídas por uma rota padrão. Esta rota será criada automaticamente por distribuição do ABR;
- A opção “Inject Summary LSA” permite especificar se os sumários de LSA da área de backbone ou outras áreas serão reconhecidos pela área stub;
- Habilite esta opção somente no ABR;
- O custo padrão dessa área é 1;

Área Stub

Redes Brasil

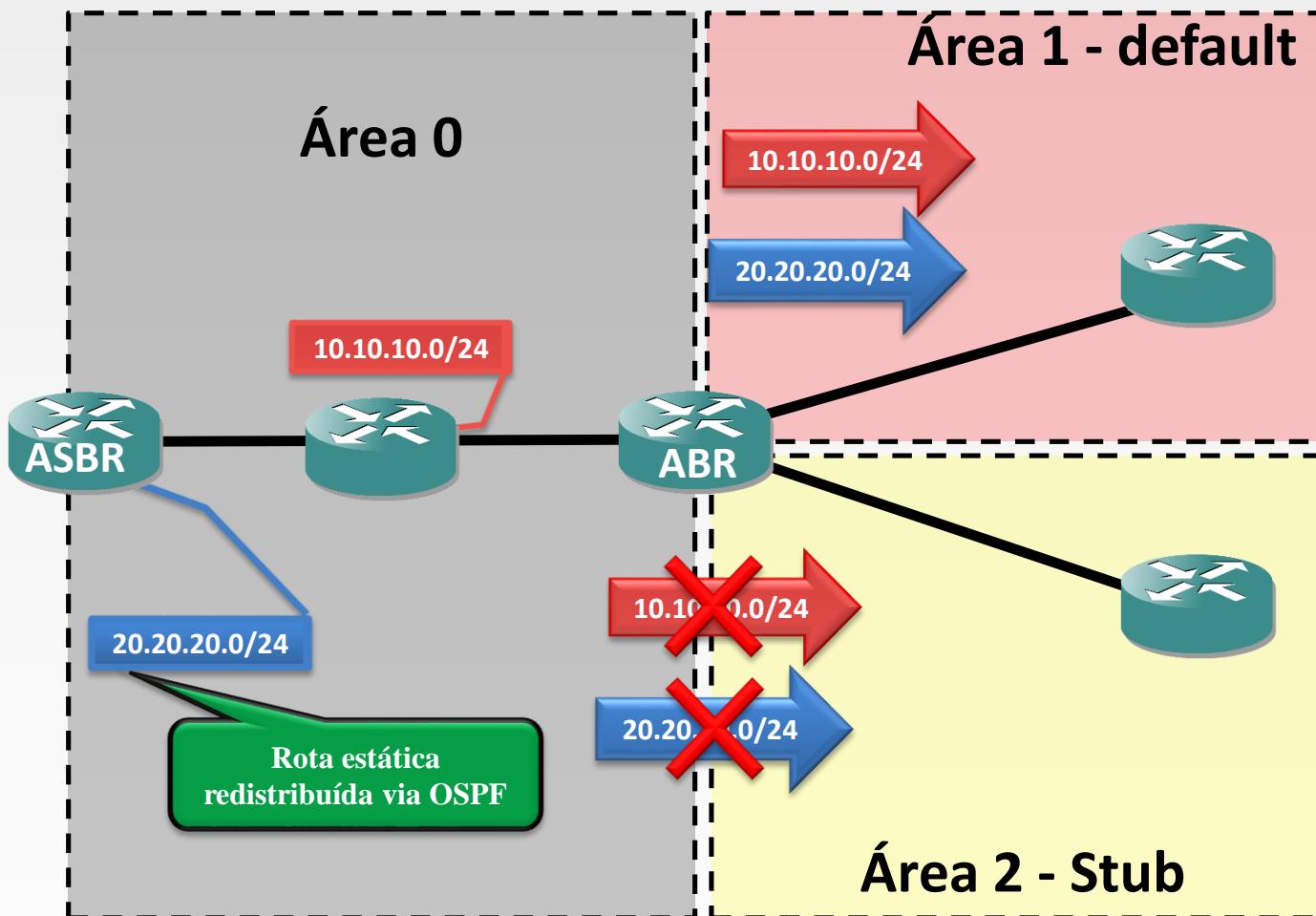
- Não recebe, nem transporta rotas externas.





Área Totally Stub

- Não recebe, nem transporta rotas externas.
- Não recebe rotas de outras áreas.



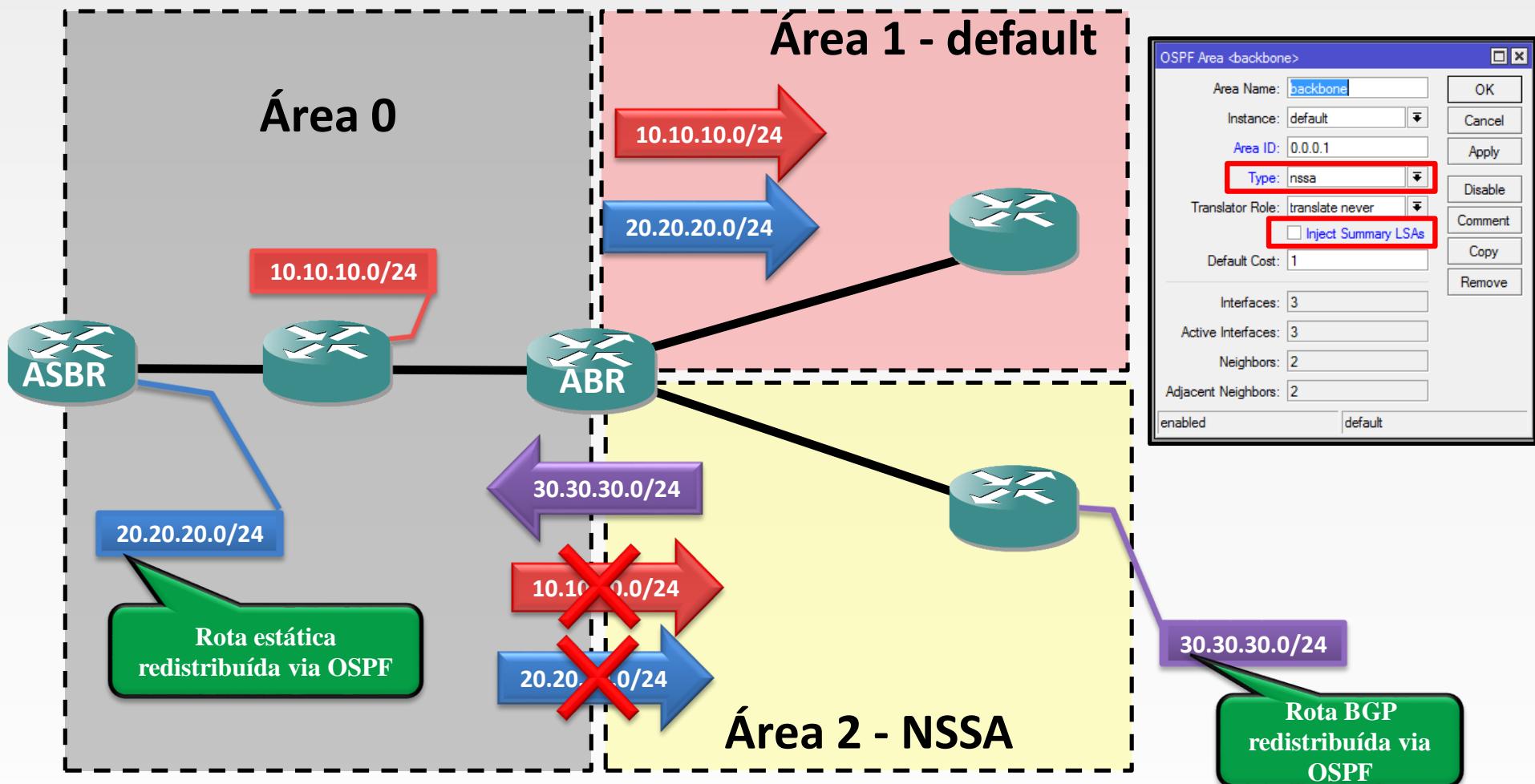
Área NSSA

- Um área NSSA é um tipo de **área stub que tem** capacidade de injetar transparentemente rotas para o backbone;
- **Translator role** – Esta opção permite controlar que ABR da área NSSA irá atuar como repetidor do ASBR para a área de backbone:
 - Translate-always: roteador sempre será usado como tradutor. “ABR”
 - Translate-candidate: ospf elege um dos roteadores ABR candidatos para fazer as traduções.

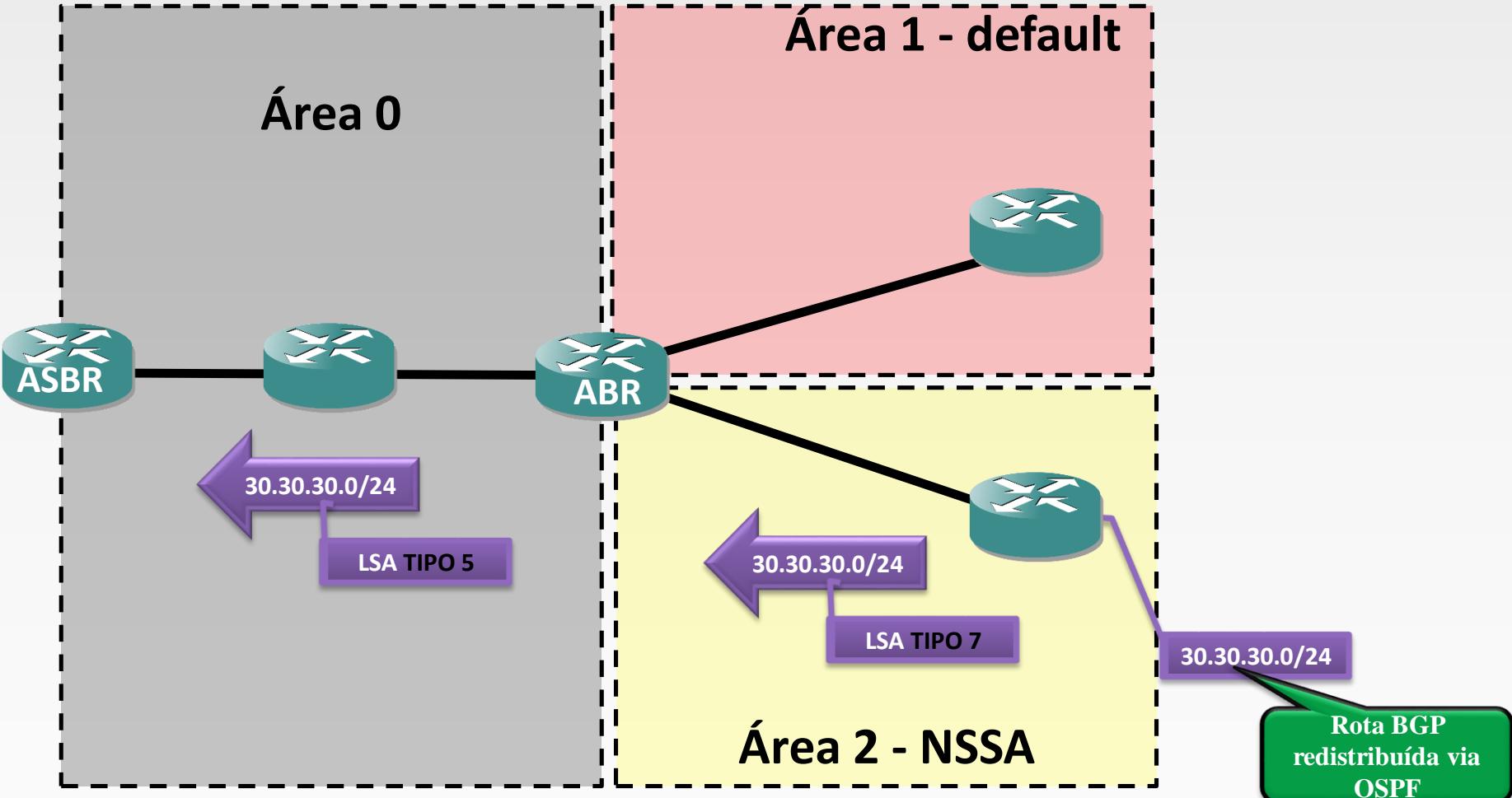
Área NSSA



- Tem as mesmas características de áreas STUB e Totally STUB com a particularidade de poder transportar rotas externas ao AS.



LSA tipo 5 e tipo 7



Link State Advertisement, pacote de dados contém informações de estado de link e roteamento, que são compartilhadas entre os vizinhos do OSPF.



LSA – Link State Advertisement

➤ **Tipo 1 Router**

Há um para cada roteador da área, e não ultrapassa a área.

➤ **Tipo 2 Network**

É gerado pelo DR e circula apenas dentro da área, não atravessa o ABR

➤ **Tipo 3 Summary Network**

É gerado pelo ABR e descreve o número da rede e a máscara, e por default não são summarizadas. E não é envidado para as áreas STUB e NSSA

➤ **Tipo 4 Summary ASBR**

É gerado pelo ABR apenas quando existe um ASBR dentro da área e informa uma rota para que todos possam chegar até o ASBR.

➤ **Tipo 5 AS External**

Usado para transportar redes de outro AS e não são enviados para áreas STUB e NSSA

➤ **Tipo 7**

São gerados em áreas NSSA pelo ASBR e o ABR (caso configurado converte em LSA do tipo 5 para outras áreas)

LSA – MK-5

Redes Brasil

OSPF						
Neighbors	NBMA Neighbors	Sham Links	LSA	Routes	AS Border Routers	Area Border Routers
T						
Instance	Area	Type	ID	Originator	Age (s)	
summary network						
default	area1	summary	10.10.254.4	10.10.254.6	128	
summary asbr						
default	area1	summary	10.10.254.5	10.10.254.6	77	
router						
default	area1	router	10.10.254.14	10.10.254.14	33	
default	area1	router	10.10.254.18	10.10.254.18	31	
default	area1	router	10.10.254.6	10.10.254.6	84	
network						
default	area1	network	10.10.254.17	10.10.254.14	33	
default	area1	network	10.10.254.14	10.10.254.14	83	
as external						
		as external	0.0.0.0	10.10.254.5	138	
8 items						

LSA Type 3

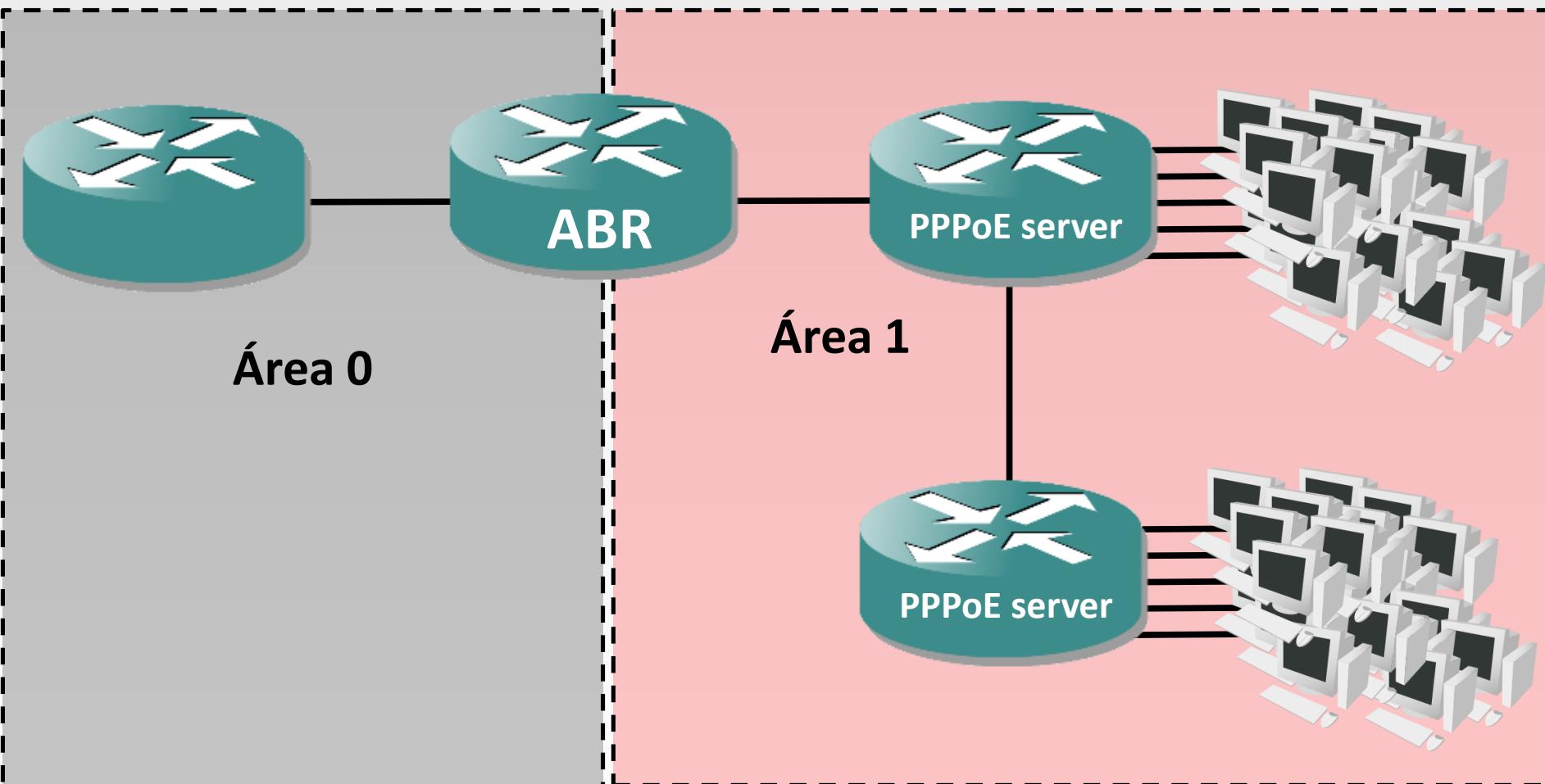
LSA Type 4

LSA Type 1

LSA Type 2

LSA Type 5

Problemas com túneis



Filtros de Roteamento

➤ É possível criar um filtro de rotas para evitar que todas rotas /32 se espalhem pela rede OSPF;

Para isto é necessário você ter uma rota agregada para esta rede túneis:

- Uma boa forma de ser fazer isso é atribuindo o endereço da rede utilizada pelos túneis na interface do concentrador.



Filtros OSPF

New Route Filter

Matchers	BGP	Actions	BGP Actions
Chain: <input type="text" value="ospf-in"/>			
Prefix: <input type="text"/>			
Prefix Length: <input type="text" value="32"/>			
Match Chain: <input type="text"/>			
Protocol: <input type="text"/>			
Distance: <input type="text"/>			
Scope: <input type="text"/>			
Target Scope: <input type="text"/>			
Pref. Source: <input type="text"/>			
Routing Mark: <input type="text"/>			
Route Comment: <input type="text"/>			
Route Tag: <input type="text"/>			
Route Targets: <input type="text"/>			
<input type="checkbox"/> Invert Route Targets			
Site Of Origin: <input type="text"/>			

OK Cancel Apply Disable Comment Copy Remove

New Route Filter

Matchers	BGP	Actions	BGP Actions
Action: <input type="text" value="discard"/>			
Jump Target: <input type="text"/>			
Set Distance: <input type="text"/>			
Set Scope: <input type="text"/>			
Set Target Scope: <input type="text"/>			
Set Pref. Source: <input type="text"/>			
Set In Nexthop: <input type="text"/>			
Set In Nexthop Direct: <input type="text"/>			
Set Out Nexthop: <input type="text"/>			
Set Routing Mark: <input type="text"/>			
Set Route Comment: <input type="text"/>			
Set Check Gateway: <input type="text"/>			
Set Disabled: <input type="text"/>			
Get Type: <input type="text"/>			

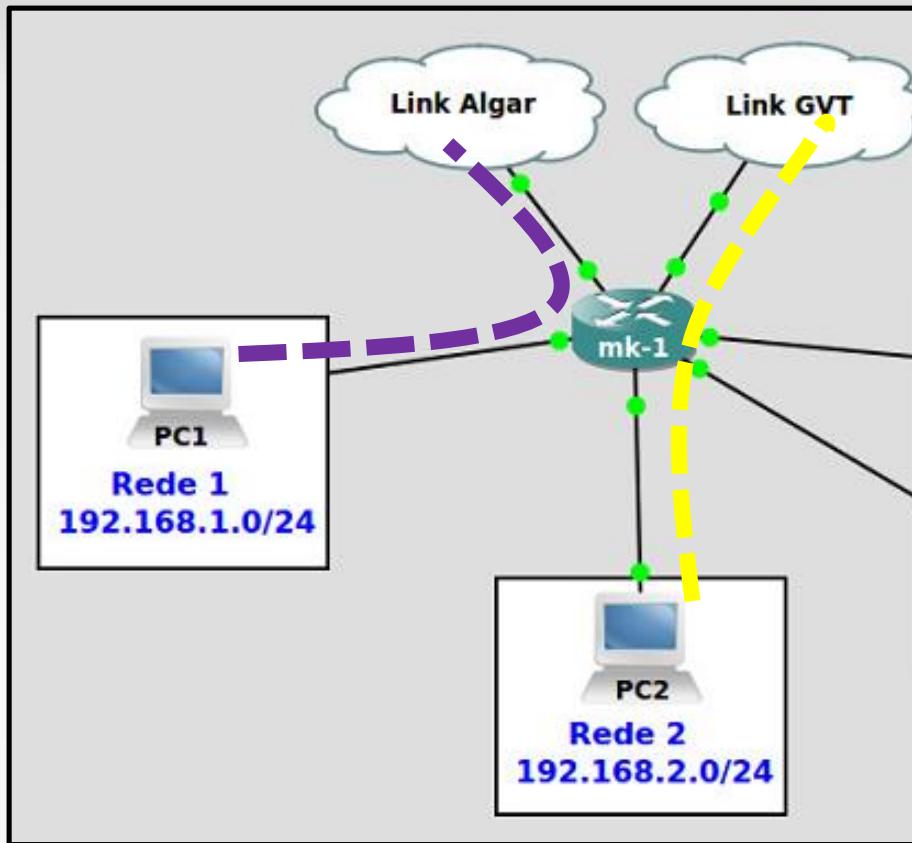
OK Cancel Apply Disable Comment Copy Remove

Resumo OSPF

- **Para segurança da rede OSPF:**
 - Use chaves de autenticação;
 - Use a maior prioridade(255) para os DR;
 - Use interfaces passiva para rede dos usuários/clientes.
- **Para aumentar a performance da rede OSPF:**
 - Use o tipo correto de área;
 - Use o tipo correto de rede para as áreas;
 - Use agregação de áreas sempre que possível;
 - Use filtros de roteamento sempre que necessário.
- **Utilize sempre como boa prática a interface loopback**

Balanceamento simples e eficiente

Redes Brasil



Objetivo

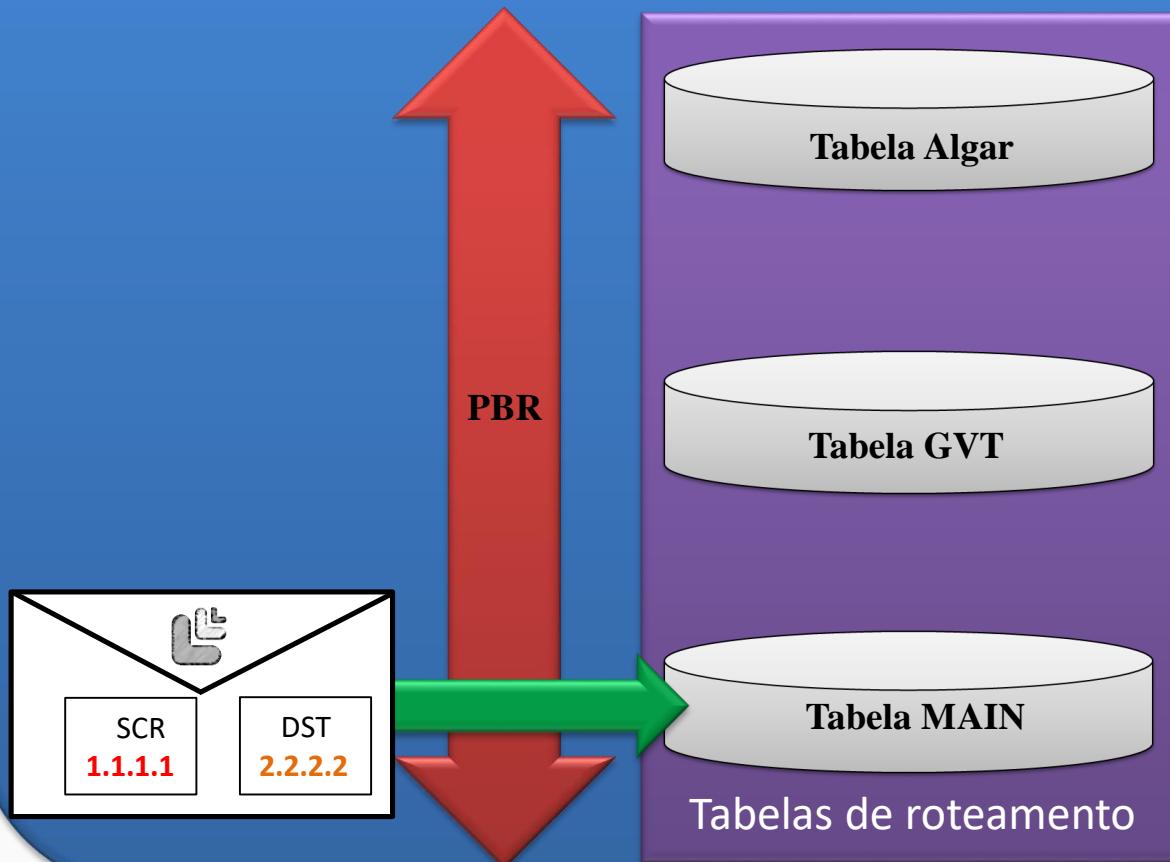
1. Forçar a rede 1 (192.168.1.0/24) navegar na internet pelo link da Algar
2. Forçar a rede 2 (192.168.2.0/24) navegar na internet pelo link da GVT
3. Sem usar regras de firewall
4. A rede 1 deverá continuar se comunicando com a rede 2

Tabela de roteamento virtual



Redes Brasil

Roteador



- Qual informação o roteador utiliza por padrão, para determinar o gateway antes de fazer encaminhamento de pacotes?

Criando novas tabelas de roteamento



Redes Brasil

The screenshot shows a network configuration interface with a sidebar and a main route list window.

Sidebar:

- IP (selected, highlighted with a red box)
- IPv6
- MPLS
- OpenFlow
- Routing
- System
- Queues
- Files
- Log
- Radius
- Tools
- New Terminal
- Make Supout.rif
- Manual
- Exit

Main Window:

Route List: Shows two routes created:

- Route <0.0.0.0/0>** (General tab selected)
 - Dst. Address: 0.0.0.0/0
 - Gateway: 10.10.10.1 (highlighted with a red box)
 - Check Gateway: [empty]
 - Type: unicast
 - Distance: 1
 - Scope: 30
 - Target Scope: 10
 - Routing Mark: roteamento-link-gvt (highlighted with a red box)
 - Pref. Source: [empty]
- Route <0.0.0.0/0>** (General tab selected)
 - Dst. Address: 0.0.0.0/0
 - Gateway: discador-algar (highlighted with a red box)
 - Check Gateway: [empty]
 - Type: unicast
 - Distance: 1
 - Scope: 30
 - Target Scope: 10
 - Routing Mark: roteamento-link-algar (highlighted with a red box)
 - Pref. Source: [empty]

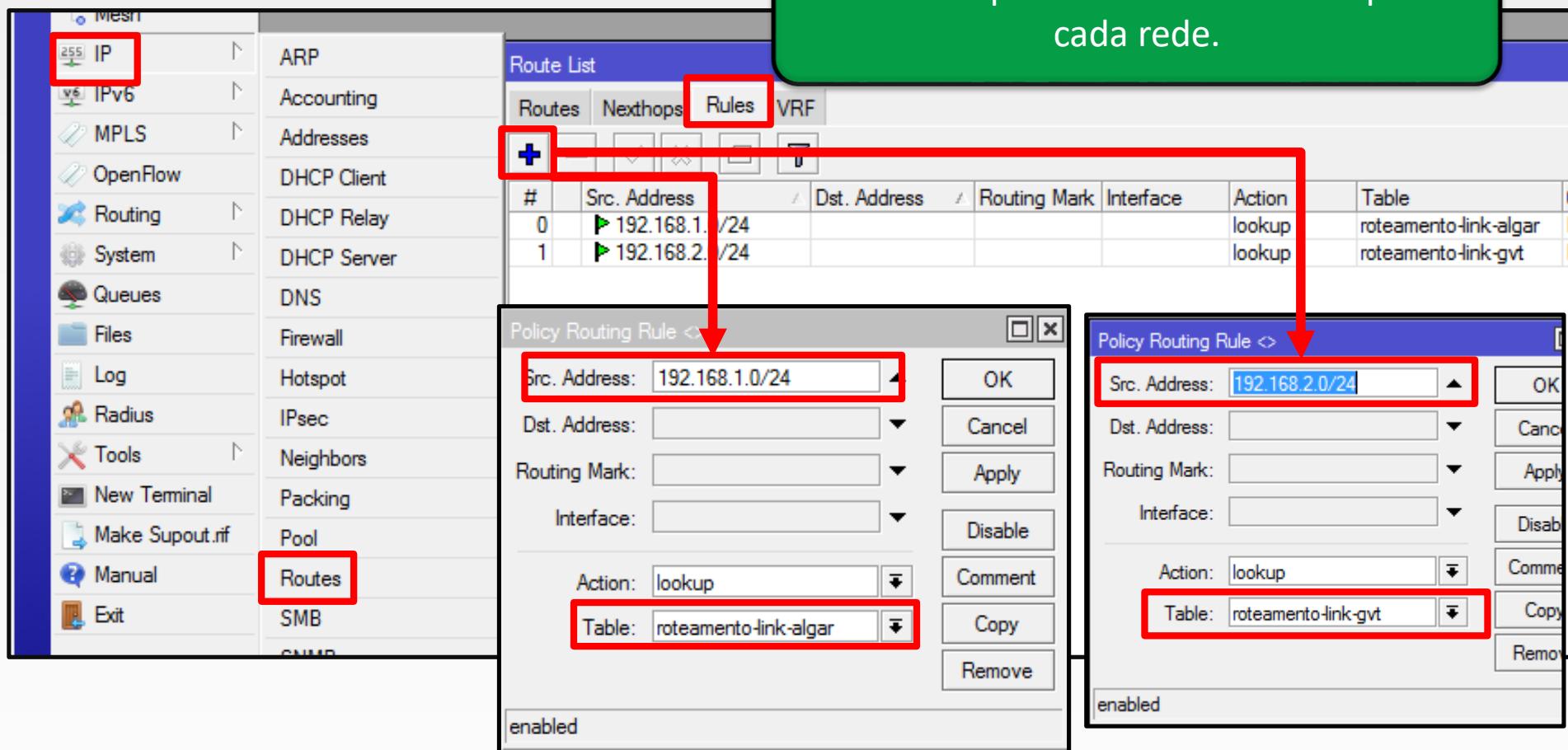
Bottom Callout:

Crie uma nova tabela de roteamento para cada link, conforme a imagem

Criando políticas de roteamento (PBR)

Redes Brasil

Crie uma política de roteamento para cada rede.



The screenshot shows the Winbox interface for managing routing policies. On the left, the navigation menu is visible with 'IP' selected. In the center, the 'Route List' window is open, showing two existing rules:

#	Src. Address	Dest. Address	Routing Mark	Interface	Action	Table
0	► 192.168.1.0/24				lookup	roteamento-link-algar
1	► 192.168.2.0/24				lookup	roteamento-link-gvt

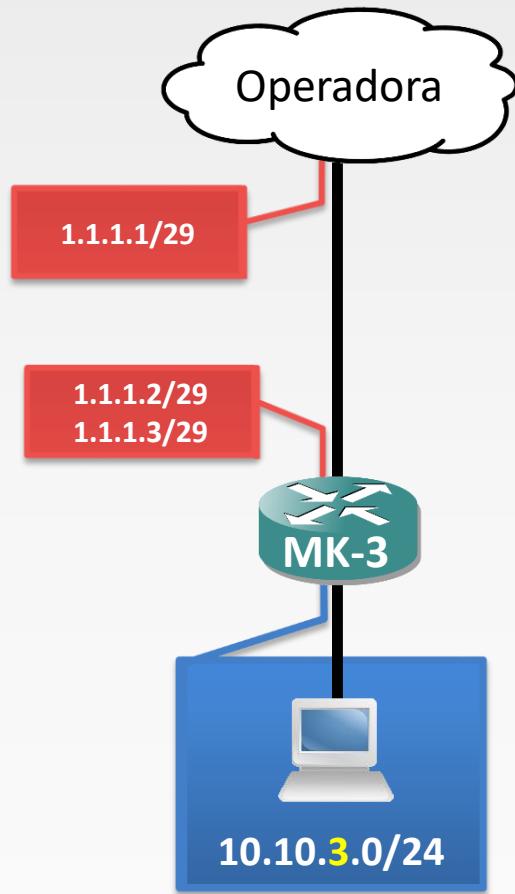
A green callout box on the right says 'Crie uma política de roteamento para cada rede.' (Create a routing policy for each network). Two new 'Policy Routing Rule' dialog boxes are shown, each with a red arrow pointing to it from the callout:

- Rule 1 (Left):** Src. Address: 192.168.1.0/24, Action: lookup, Table: roteamento-link-algar
- Rule 2 (Right):** Src. Address: 192.168.2.0/24, Action: lookup, Table: roteamento-link-gvt

The bottom status bar indicates 'enabled'.



Campo de Pref. Source



The screenshot shows a routing configuration window. In the top section, titled "Address List", there is a table:

Address	Network	Interface
1.1.1.3/24	1.1.1.0	ether1-link
1.1.1.2/24	1.1.1.0	ether1-link

In the bottom section, titled "New Route", the "Pref. Source" field is highlighted with a red box and contains the value **1.1.1.3**.

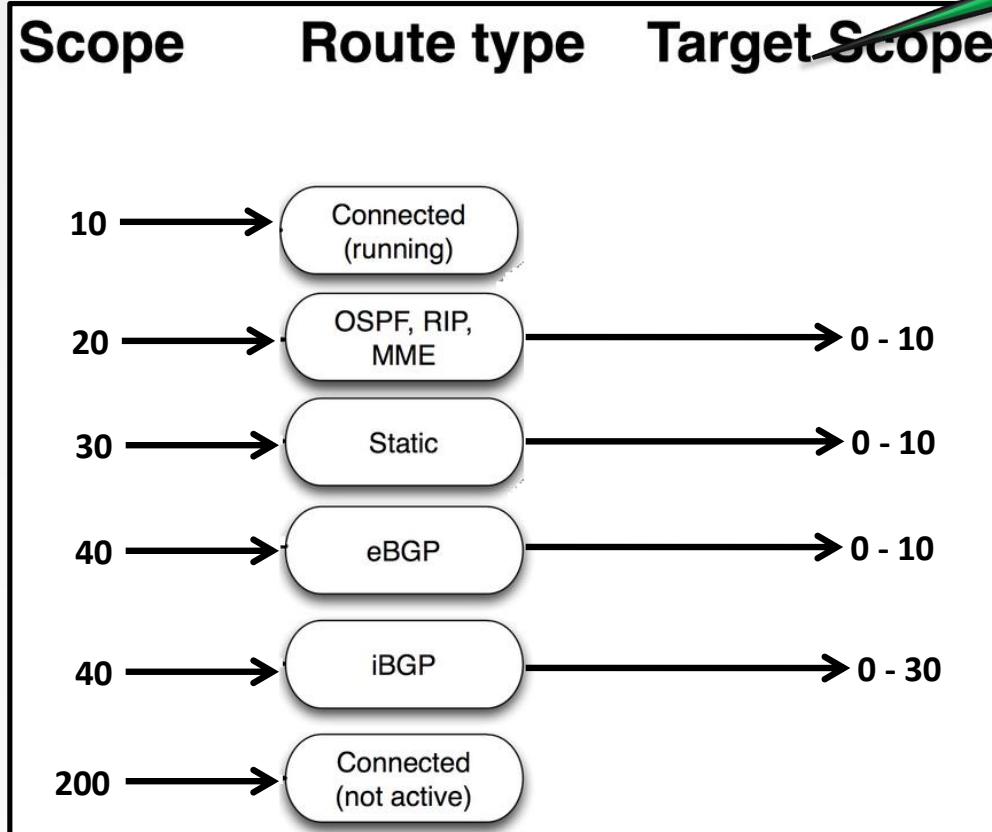
2 IPs em uma mesma interface

Especifique aqui o IP que deseja força utilização

Scope e Target Scope (roteamento recursivo)

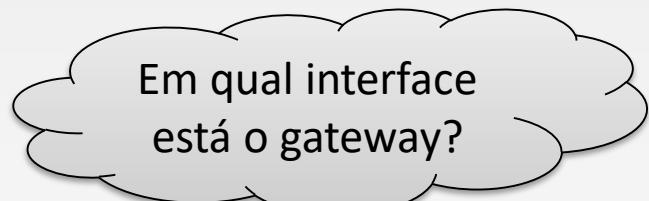
Redes Brasil

Encontre o gateway em
rotas com SCOPE entre

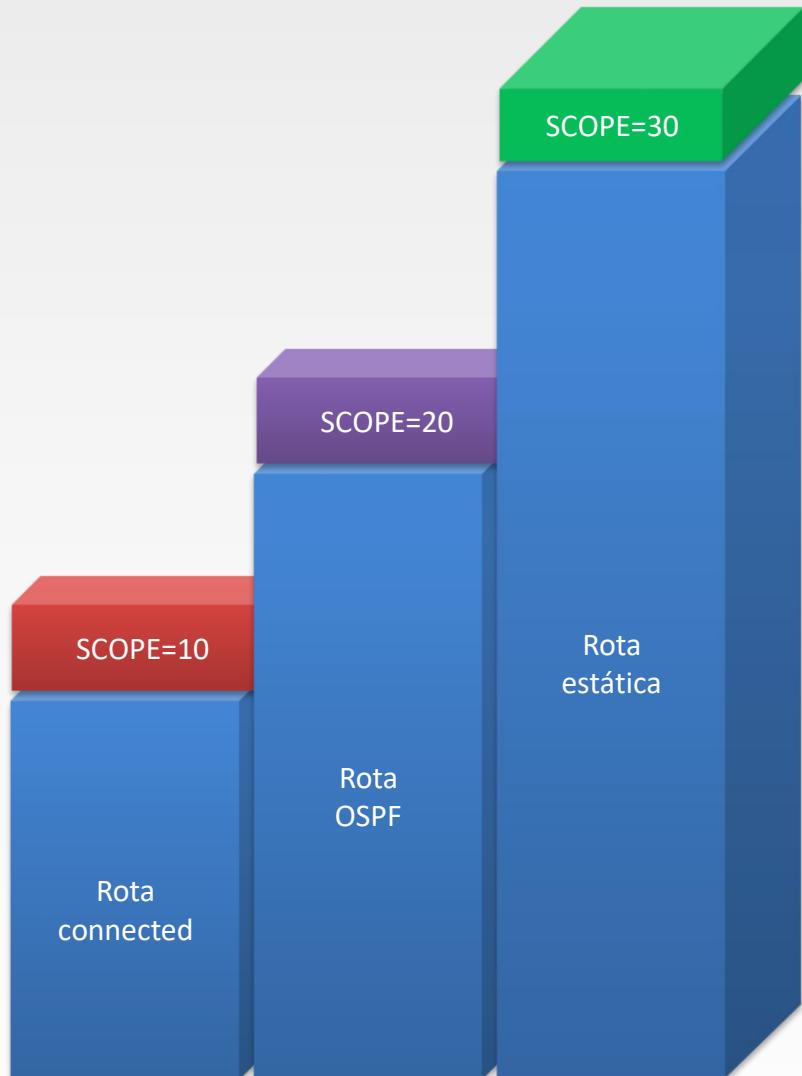


Scope e Target Scope (roteamento recursivo)

Redes Brasil



MEU TARGET SCOPE=10





Scope e Target Scope (roteamento recursivo)

Route List

Routes | Nexthops | Rules | VRF

Route List (Original):

	Dst. Address	Gateway	Distance	Scope	Target Scope
S	0.0.0.0/0	8.8.8 unreachable	5	30	10
AS	8.8.8.8	172.25.255.1 reachable bridge-rede-local	1	30	10
DAC	172.25.100.0/...	bridge-rede-local reachable	0	10	10
DAC	172.25.255.0/...	bridge-rede-local reachable	0	10	10

Não consegue achar o gateway pois o mesmo não está diretamente conectado.

Route List

Routes | Nexthops | Rules | VRF

Route List (After Change):

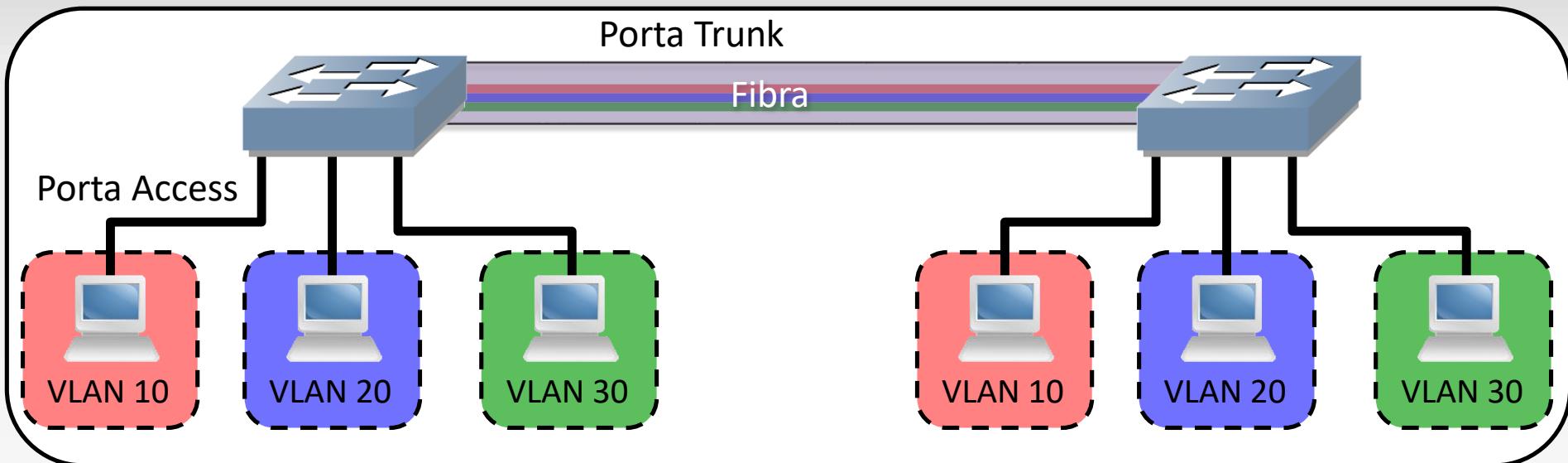
	Dst. Address	Gateway	Distance	Scope	Target Scope
AS	0.0.0.0/0	8.8.8 recursive via 172.25.255.1 bridg...	5	30	31
AS	8.8.8.8	172.25.255.1 reachable bridge-rede-local	1	30	10
DAC	172.25.100.0/...	bridge-rede-local reachable	0	10	10
DAC	172.25.255.0/...	bridge-rede-local reachable	0	10	10

Após alterar o campo Target Scope a rota consegue encontrar o gateway através de outra rota estática.

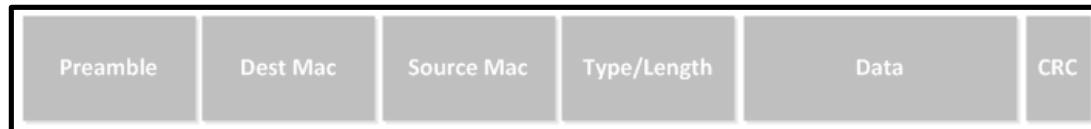
VLAN

- Uma rede local virtual, normalmente denominada de VLAN, é uma rede logicamente independente.
- Várias VLANs podem coexistir em um mesmo switch, de forma a dividir uma rede local (física) em mais de uma rede (virtual), criando domínios de broadcast separados.
- VLANs são definidas pelo padrão IEEE 802.1Q.
- Quando utilizamos o recurso de VLAN é inserido um novo campo de 4 bytes no cabeçalho de camada 2.
- 12 bits desse novo campo são usados para fazer a identificação da VLAN (por isso podemos ter até 4096 diferentes VLANs)

Portas e cabeçalho de VLANs



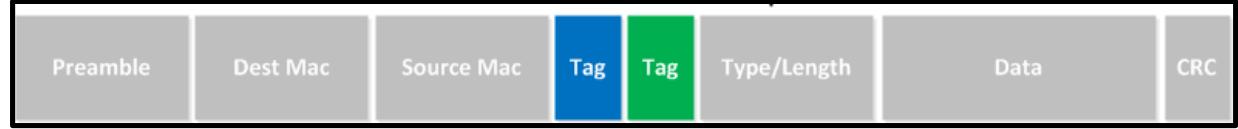
Frame original



802.1q



q-in-q ou 802.1ad





Implementação de VLAN

10.10.40.1/24

VLAN 40

BRIDGE

VLAN 40

BRIDGE

ether8



MK-1

MK-3

MK-4

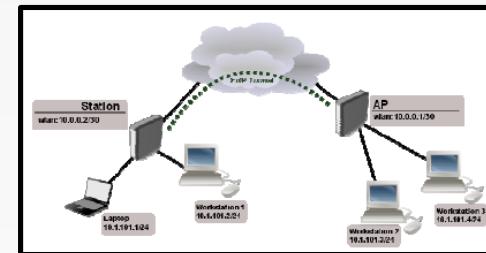
10.10.40.254/24

Informações

1. Se a interface de saída for uma VLAN uma TAG será inserida no frame.
2. Se a interface de saída **não** for uma **VLAN** não será inserida a TAG.
3. Bridge podem ser usadas para retirar a TAG de VLANs.

Túneis EoIP

- EoIP(Ethernet over IP) é um protocolo proprietário Mikrotik para encapsulamento de todo tipo de tráfego sobre o protocolo IP.
- EoIP é um túnel de camada 2 que por padrão não implementa segurança. Para implementar segurança você pode fazer uso de IPSec.
- Quando habilitada a função de Bridge dos roteadores que estão interligados através de um túnel EoIP, todo o tráfego é passado de uma lado para o outro de forma transparente mesmo roteado pela internet e por vários protocolos.
- O protocolo EoIP possibilita:
 - Interligação em bridge de LANs remotas através da internet.
 - Interligação em bridge de LANs através de túneis criptografados.
- A interface criada pelo túnel EoIP suporta todas funcionalidades de uma interface ethernet. Endereços IP e outros túneis podem ser configurados na interface EoIP. O protocolo EoIP encapsula frames ethernet através do protocolo GRE.

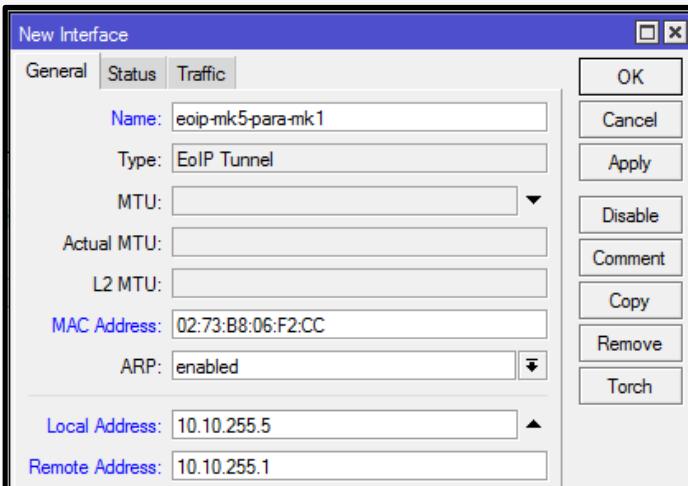
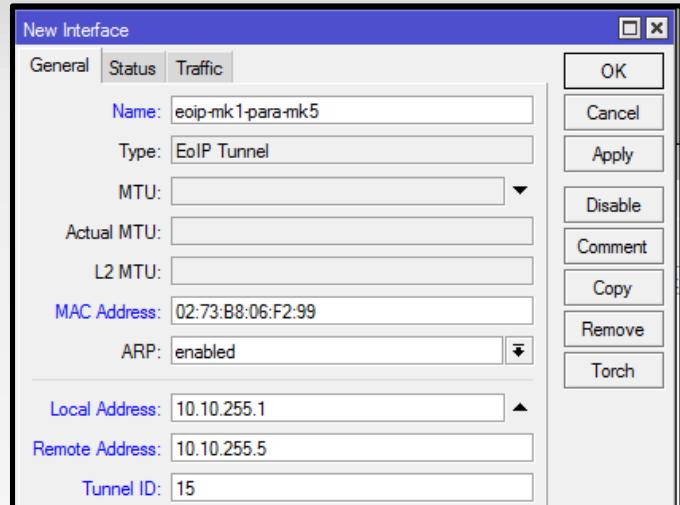


Túneis EOIP



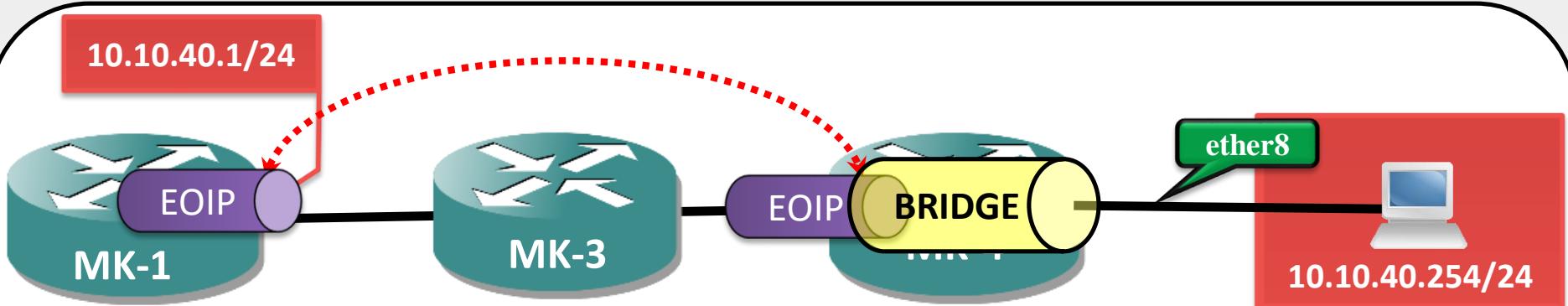
Redes Brasil

- Criando um túnel EoIP entre as redes por trás dos roteadores 10.0.0.1 e 22.63.11.6.
- Os MACs devem ser diferentes e estar entre o rage: 00-00-5E-80-00-00 e 00-00-5E-FF-FF-FF, pois são endereços reservados para essa aplicação.
- O MTU deve ser deixado em 1500 para evitar fragmentação.
- O túnel ID deve ser igual para ambos.



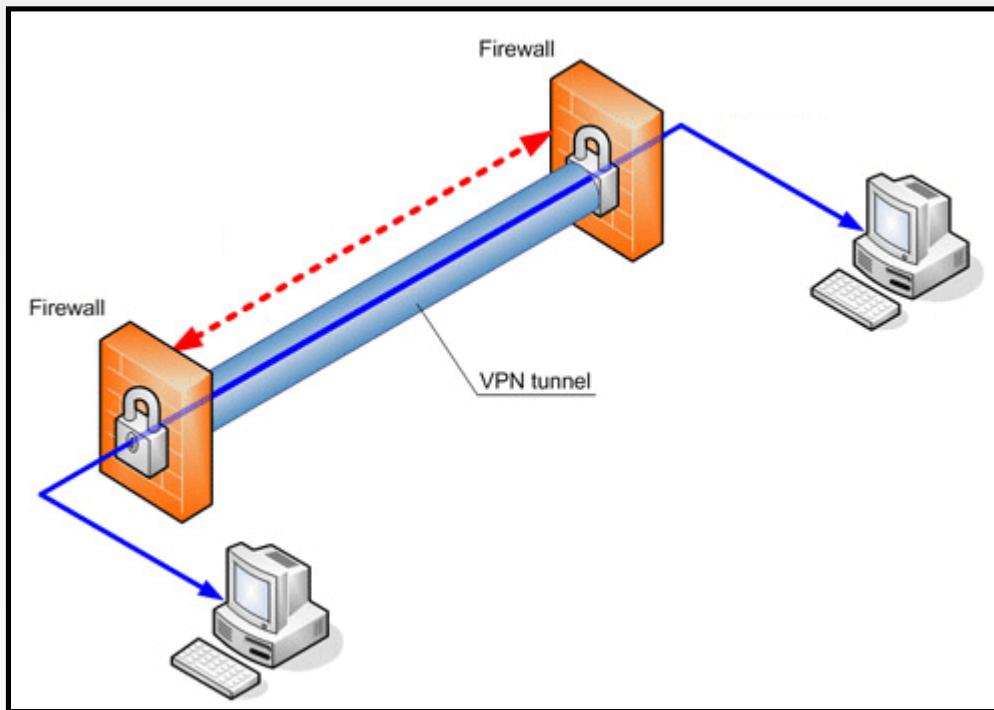
Implementação de EOIP

Redes Brasil



Túneis e VPN

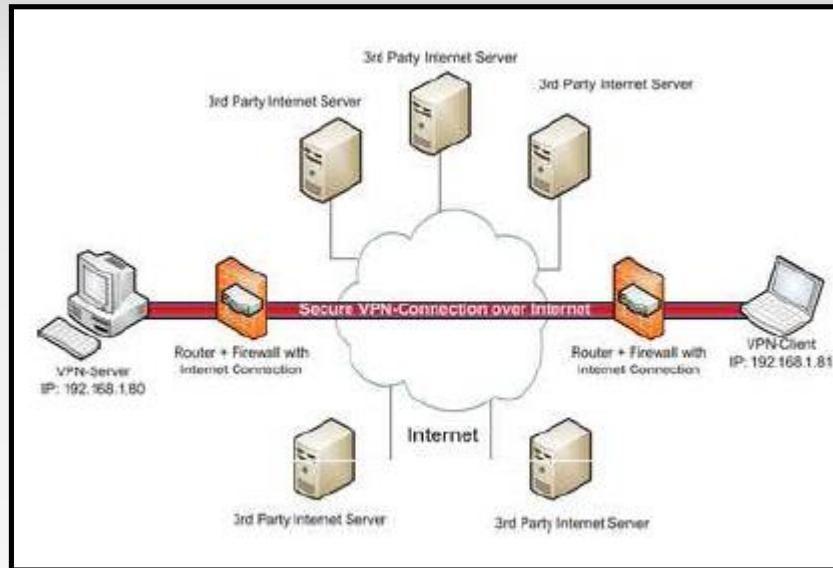
Redes Brasil





VPN

- Uma Rede Privada Virtual é uma rede de comunicações privada normalmente utilizada por uma empresa ou conjunto de empresas e/ou instituições, construídas em cima de uma rede pública. O tráfego de dados é levado pela rede pública utilizando protocolos padrão, não necessariamente seguros.
- VPNs seguras usam protocolos de criptografia por tunelamento que fornecem confidencialidade, autenticação e integridade necessárias para garantir a privacidade das comunicações requeridas. Quando adequadamente implementados, estes protocolos podem assegurar comunicações seguras através de redes inseguras.



VPN

- As principais características da VPN são:
 - Promover acesso seguro sobre meios físicos públicos como a internet por exemplo.
 - Promover acesso seguro sobre linhas dedicadas, wireless, etc...
 - Promover acesso seguro a serviços em ambiente corporativo de correio, impressoras, etc...
 - Fazer com que o usuário, na prática, se torne parte da rede corporativa remota recebendo IPs desta e perfis de segurança definidos.
 - A base da formação das VPNs é o tunelamento entre dois pontos, porém tunelamento não é sinônimo de VPN.

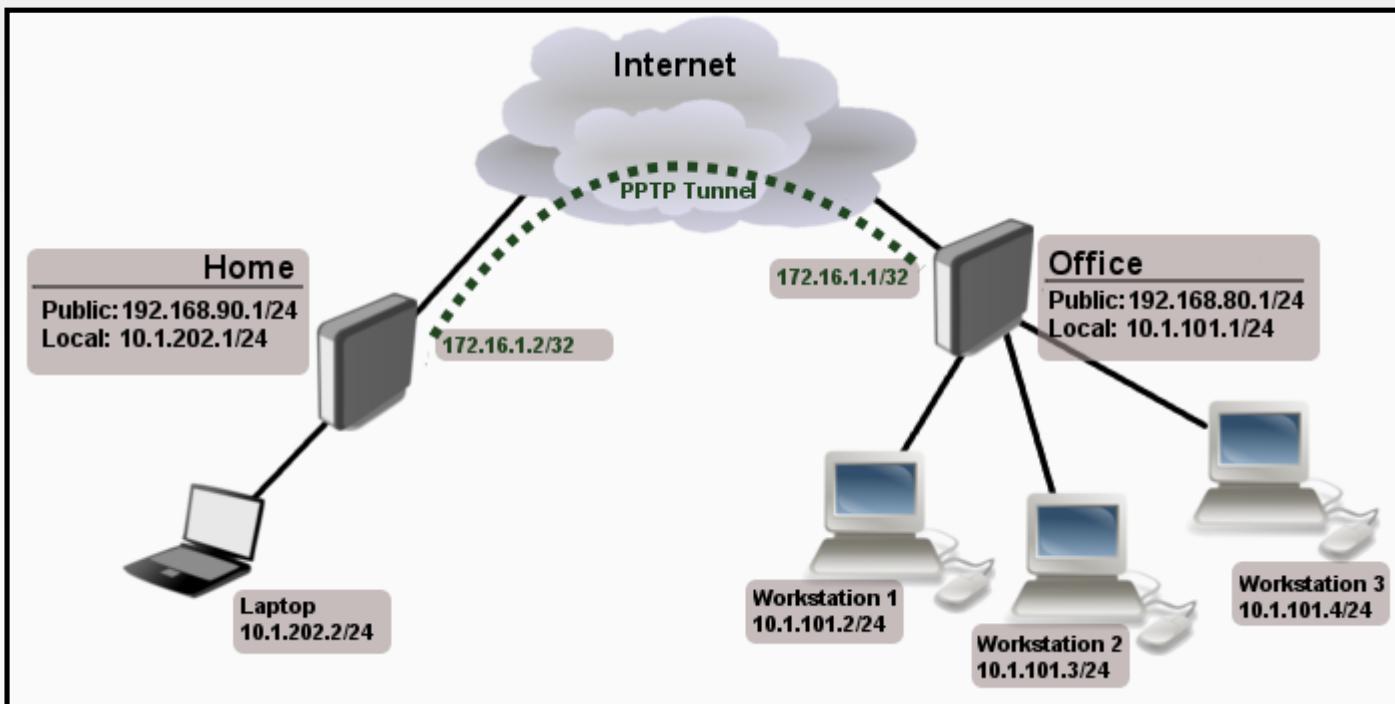


Tunelamento

- A definição de tunelamento é a capacidade de criar túneis entre dois hosts por onde trafegam dados.
- O MikroTik implementa diversos tipos de tunelamento, podendo ser tanto servidor como cliente desses protocolos:
 - PPP (Point to Point Protocol)
 - PPPoE (Point to Point Protocol over Ethernet)
 - PPTP (Point to Point Tunneling Protocol)
 - L2TP (Layer 2 Tunneling Protocol)
 - OVPN (Open Virtual Private Network)
 - IPSec (IP Security)
 - Túneis IPIP
 - Túneis EoIP
 - Túneis VPLS
 - Túneis TE
 - Túneis GRE

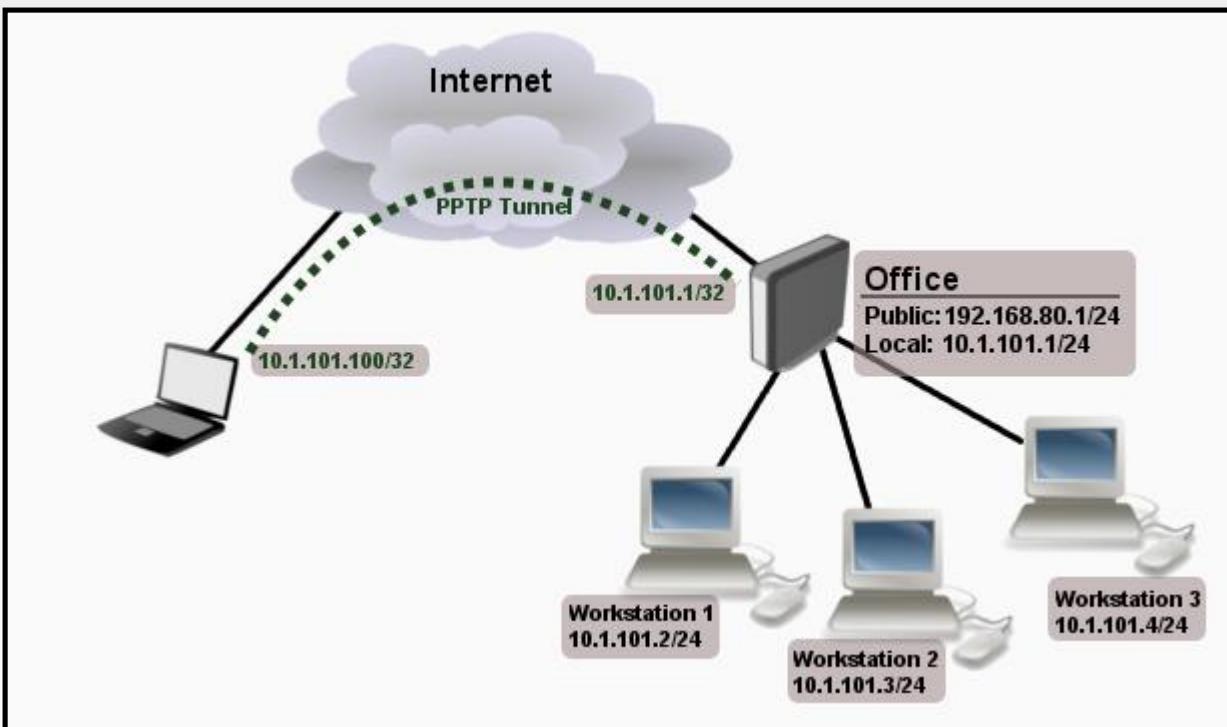


Site-to-site





Conexão remota



Endereçamento ponto a ponto /32



Redes Brasil

- Geralmente usado em túneis
- Pode ser usado para economia de IPs.

Router 1

Address <1.1.1.1>

Address:	1.1.1.1	OK
Network:	2.2.2.2	Cancel
Interface:	wlan1	Apply
Disable		
Comment		
Copy		
Remove		
enabled		

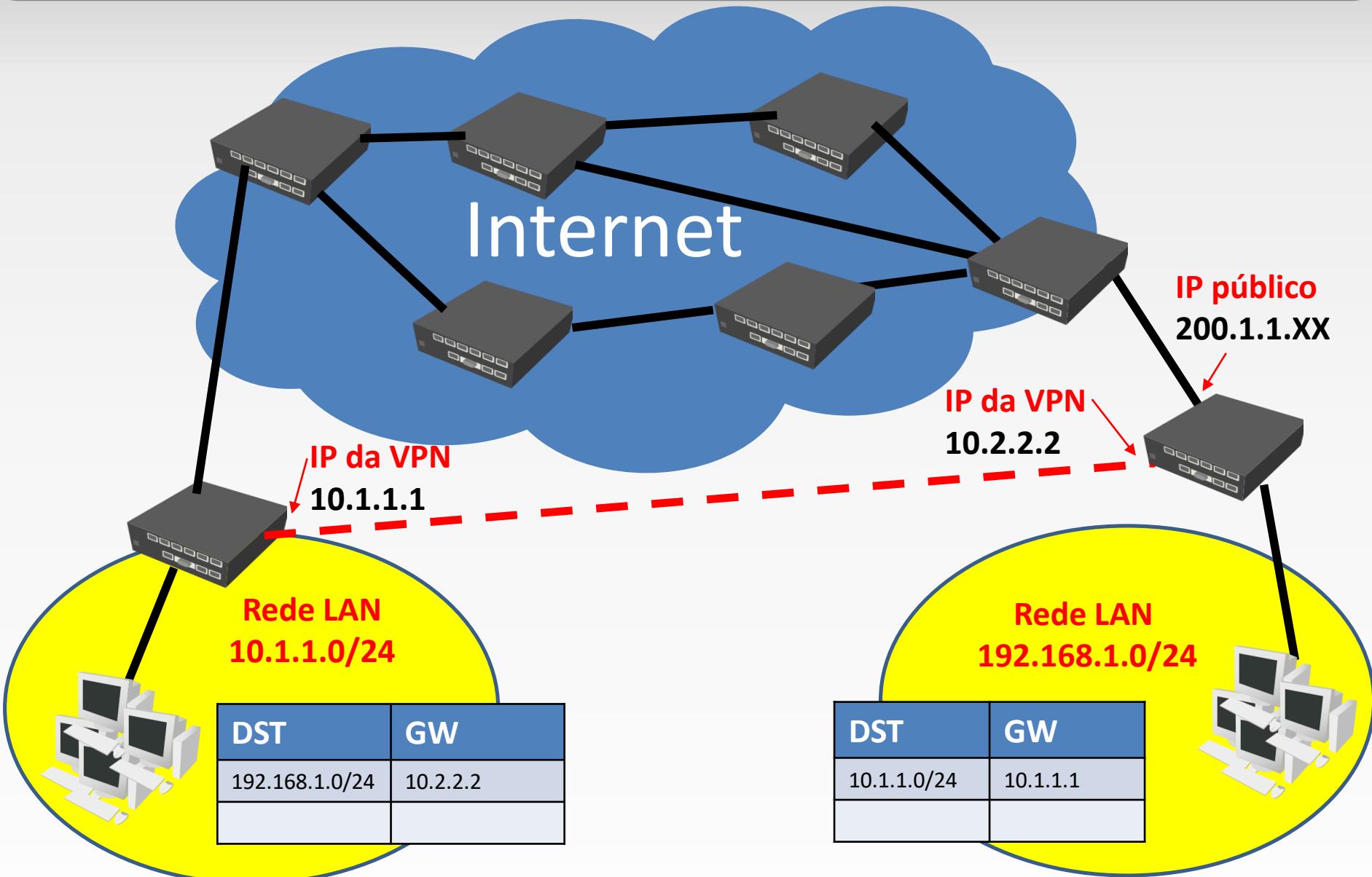
Router 2

New Address

Address:	2.2.2.2	OK
Network:	1.1.1.1	Cancel
Interface:	wlan1	Apply
Disable		
Comment		
Copy		
Remove		
enabled		

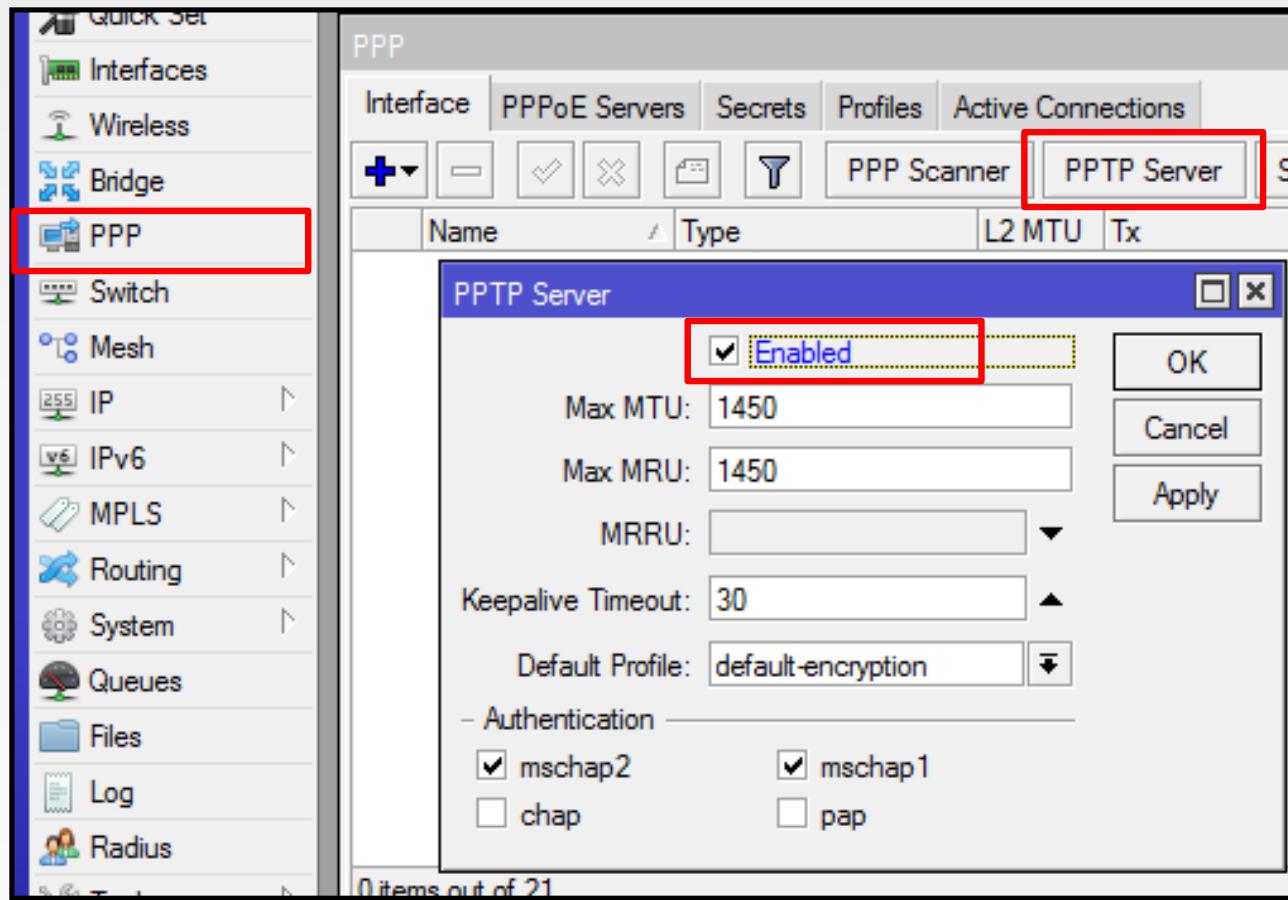
Diagrama de VPN

Redes Brasil





Ativando PPTP server





Criando o usuário para o PPTP Client

The screenshot shows the Winbox interface for configuration. On the left, a sidebar lists various network components: Quick Set, Interfaces, Wireless, Bridge, PPP (highlighted with a red box), Switch, Mesh, IP, IPv6, MPLS, Routing, System, Queues, Files, and Log. The main window is titled 'PPP' and contains tabs for Interface, PPPoE Servers, Secrets (highlighted with a red box), Profiles, and Active Connections. Below the tabs is a toolbar with icons for creating (+), deleting (-), selecting (checkmark), deleting (X), saving (disk), and running (play). A sub-header 'PPP Authentication&Accounting' is present. The central area is titled 'New PPP Secret' and contains fields for Name (set to 'teste'), Password (set to 'teste'), Service (set to 'any'), Caller ID (empty), Profile (set to 'default'), Local Address (set to '10.1.1.1'), and Remote Address (set to '10.2.2.2').

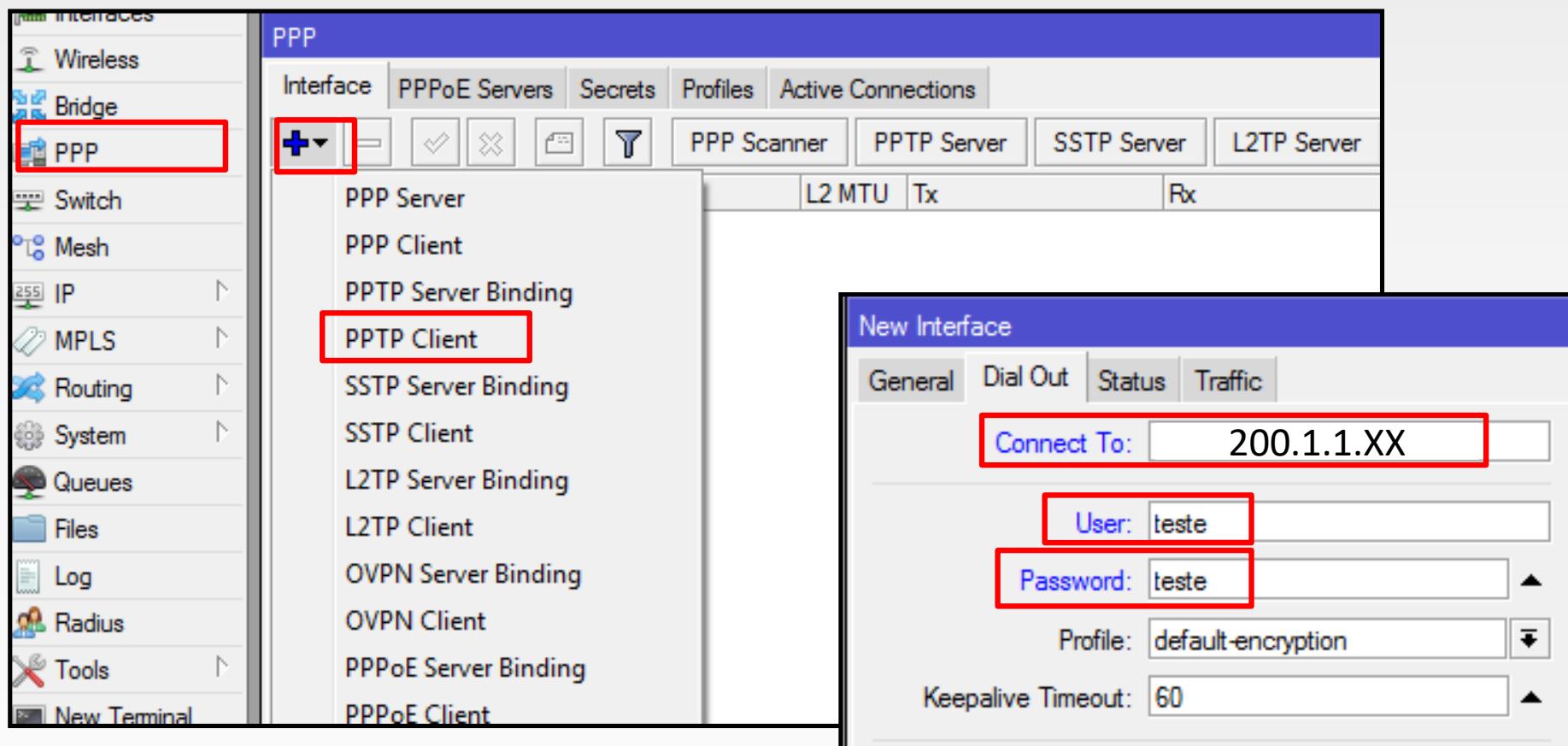
Usuário e senha que serão
usando para o cliente de VPN
se autenticar.

IP que será atribuído
localmente quando o usuário
“teste” se conectar.

IP que será atribuído no
cliente **remoto** ao se conectar
usando o usuário “teste”.

Criando o PPTP Client

Redes Brasil



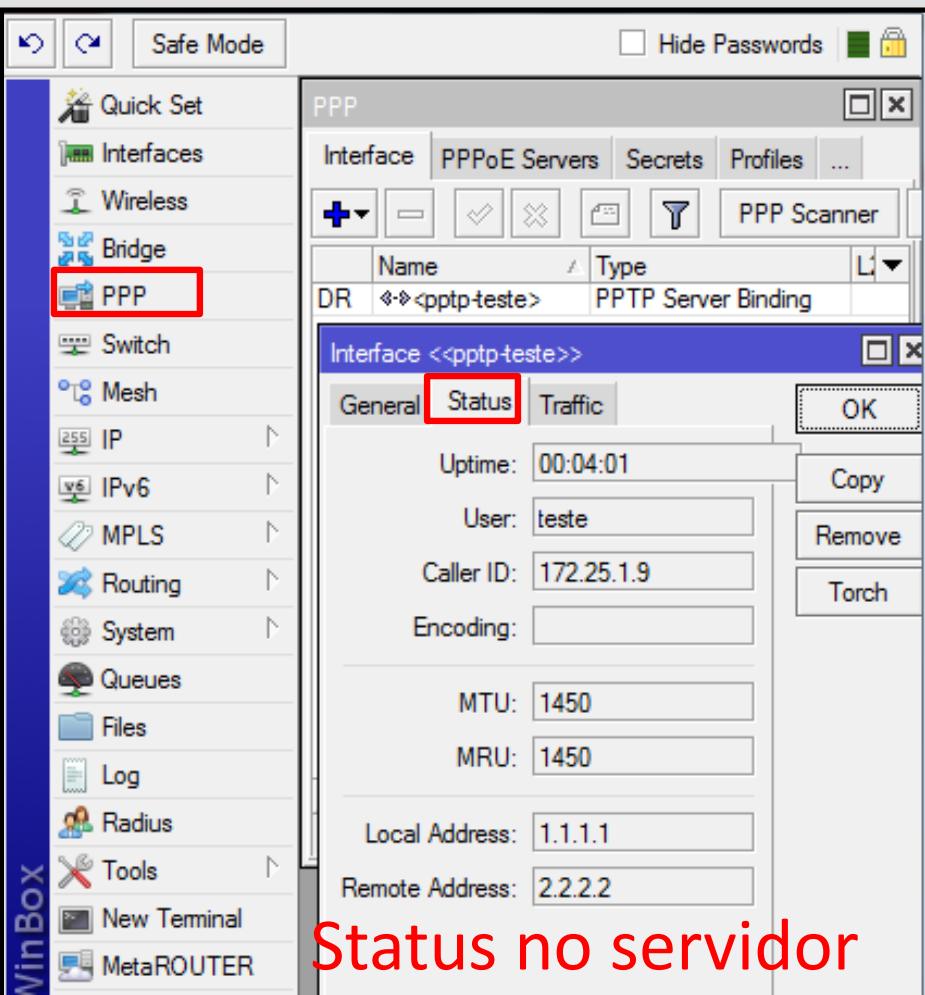
The screenshot shows the Winbox interface for managing network interfaces. On the left, a sidebar lists various interface types: Wireless, Bridge, PPP, Switch, Mesh, IP, MPLS, Routing, System, Queues, Files, Log, Radius, Tools, and New Terminal. The PPP option is selected and highlighted with a red box.

The main window title is "PPP" and contains tabs for Interface, PPPoE Servers, Secrets, Profiles, and Active Connections. The "Interface" tab is active. Below the tabs is a toolbar with icons for creating (+), deleting (-), and managing interfaces. The interface list includes: PPP Server, PPP Client, PPTP Server Binding, **PPTP Client**, SSTP Server Binding, SSTP Client, L2TP Server Binding, L2TP Client, OVPN Server Binding, OVPN Client, PPPoE Server Binding, and PPPoE Client. The "PPTP Client" item is also highlighted with a red box.

A modal dialog titled "New Interface" is open on the right, specifically for the "Dial Out" tab. It contains fields for "Connect To:" (set to 200.1.1.XX), "User:" (set to teste), "Password:" (set to teste), "Profile:" (set to default-encryption), and "Keepalive Timeout:" (set to 60).

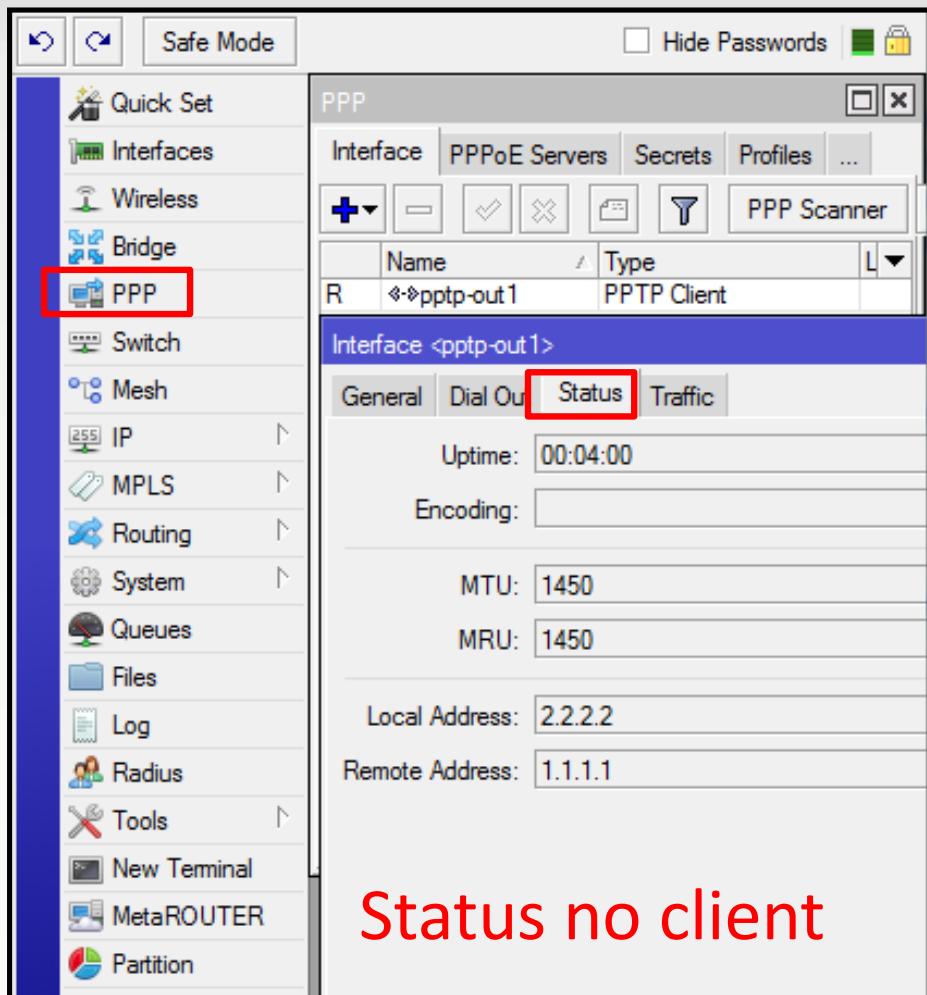
Acompanhando o Status

Redes Brasil



This screenshot shows the WinBox interface for monitoring PPP connections. On the left, the navigation bar includes options like Quick Set, Interfaces, Wireless, Bridge, and PPP. The PPP option is highlighted with a red box. In the main window, the 'PPP' tab is selected under the 'Interface' tab. A table lists a connection named 'DR <> <pptp-teste>' of type 'PPTP Server Binding'. Below this, a detailed status window for 'Interface <> <pptp-teste>' is open, also with its 'Status' tab highlighted by a red box. The status window displays various parameters: Uptime (00:04:01), User (teste), Caller ID (172.25.1.9), Encoding (empty), MTU (1450), MRU (1450), Local Address (1.1.1.1), and Remote Address (2.2.2.2).

Status no servidor



This screenshot shows the WinBox interface for monitoring PPP connections. The navigation bar and tabs are identical to the previous screenshot. The 'PPP' tab is selected under the 'Interface' tab. A table lists a connection named 'R <> <pptp-out1>' of type 'PPTP Client'. Below this, a detailed status window for 'Interface <> <pptp-out1>' is open, with its 'Status' tab highlighted by a red box. The status window displays parameters: Uptime (00:04:00), Encoding (empty), MTU (1450), MRU (1450), Local Address (2.2.2.2), and Remote Address (1.1.1.1).

Status no cliente



Criando as rotas

The image shows two screenshots of a network configuration interface, likely from a Cisco-like router or switch, demonstrating the creation of routes and their status.

Left Screenshot (Server Side):

- Left Panel:** Shows navigation links: IP (selected), ARP, Accounting, Addresses, DHCP Client, DHCP Relay, DHCP Server, DNS, Firewall, Hotspot, IPsec, Neighbors, Packing, Pool, Make Supout.rif, and Routes.
- Middle Panel:** Shows the "Route List" with tabs for Routes, Nexthops, Rules, and VRF. A red box highlights the "+" button to add a new route. The "New Route" dialog has tabs for General and Attributes. The "General" tab shows "Dst. Address: 10.1.2.0/24" and "Gateway: 2.2.2.2". A red box highlights the "Gateway" field. Below it are fields for "Check Gateway:", "Type: unicast", "Distance:", and "Score: 30".
- Text Label:** "Rota no servidor" (Route on the server) is overlaid on the middle panel.
- Right Screenshot (Client Side):**
- Left Panel:** Similar navigation links: IP (selected), ARP, Accounting, Addresses, DHCP Client, DHCP Relay, System, Queues, Files, Log, Radius, Tools, New Terminal, MetaROUTER, Partition, Make Supout.rif, and Routes.
- Middle Panel:** Shows the "Route List" with tabs for Routes, Nexthops, Rules, and VRF. A red box highlights the "+" button to add a new route. The "New Route" dialog has tabs for General and Attributes. The "General" tab shows "Dst. Address: 10.1.1.0/24" and "Gateway: 1.1.1.1". A red box highlights the "Gateway" field. Below it are fields for "Check Gateway:", "Type: unicast", "Distance:", and "Score: 30".
- Text Label:** "Rota no cliente" (Route on the client) is overlaid on the middle panel.

This screenshot shows the "Tunnels" configuration page on the server side.

Left Panel: Shows navigation links: Queues, Files, Log, Radius, Tools, New Terminal, MetaROUTER, and Partition.

Middle Panel: Shows tunnel parameters: MTU: 1450, MRU: 1450, Local Address: 1.1.1.1, and Remote Address: 2.2.2.2.

Text Label: "Status no servidor" (Status on the server) is overlaid on the middle panel.

This screenshot shows the "Tunnels" configuration page on the client side.

Left Panel: Shows navigation links: Log, Radius, Tools, New Terminal, MetaROUTER, and Partition.

Middle Panel: Shows tunnel parameters: Local Address: 2.2.2.2, and Remote Address: 1.1.1.1.

Text Label: "Status no cliente" (Status on the client) is overlaid on the middle panel.

Campos PPPoE

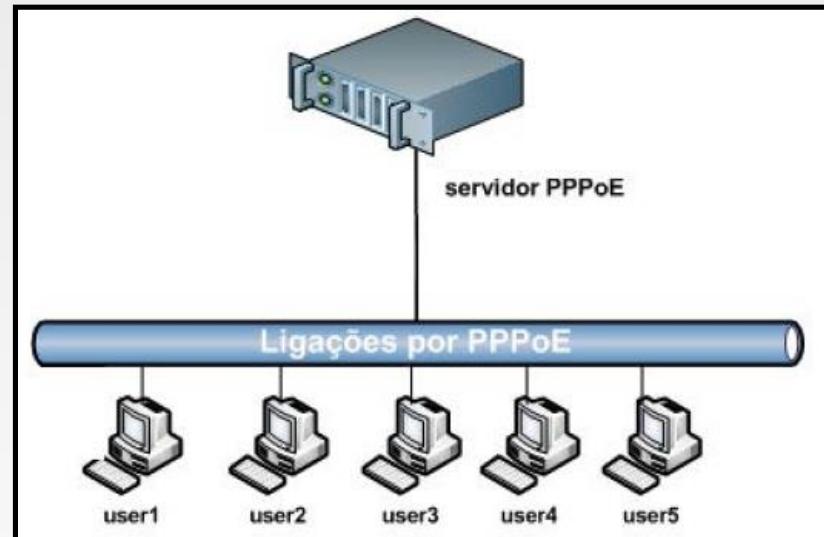
- **MTU/MRU:** Unidade máximas de transmissão/ recepção em bytes. Normalmente o padrão ethernet permite 1500 bytes. Em serviços PPP que precisam encapsular os pacotes, deve-se definir valores menores para evitar fragmentação.
- **Keepalive Timeout:** Define o período de tempo em segundos após o qual o roteador começa a mandar pacotes de keepalive por segundo. Se nenhuma resposta é recebida pelo período de 2 vezes o definido em keepalive timeout o cliente é considerado desconectado.
- **Authentication:** As formas de autenticação permitidas são:
 - **Pap:** Usuário e senha em texto plano sem criptografia.
 - **Chap:** Usuário e senha com criptografia.
 - **Mschap1:** Versão chap da Microsoft conf. RFC 2433
 - **Mschap2:** Versão chap da Microsoft conf. RFC 2759

PPPoE – Cliente e Servidor

- PPPoE é uma adaptação do PPP para funcionar em redes ethernet. Pelo fato da rede ethernet não ser ponto a ponto, o cabeçalho PPPoE inclui informações sobre o remetente e o destinatário, desperdiçando mais banda. Cerca de 2% a mais.
- Muito usado para autenticação de clientes com base em Login e Senha. O PPPoE estabelece sessão e realiza autenticação com o provedor de acesso a internet.
- O cliente não tem IP configurado, o qual é atribuído pelo Servidor PPPoE(concentrador) normalmente operando em conjunto com um servidor Radius. No MikroTik não é obrigatório o uso de Radius pois o mesmo permite criação e gerenciamento de usuários e senhas em uma tabela local.
- PPPoE por padrão não é criptografado. O método MPPE pode ser usado desde que o cliente suporte este método.

PPPoE – Cliente e Servidor

- O cliente descobre o servidor através do protocolo pppoe discovery que tem o nome do serviço a ser utilizado.
- Precisa estar no mesmo barramento físico ou os dispositivos passarem pra frente as requisições PPPoE usando pppoe relay.
- No MikroTik o valor padrão do Keepalive Timeout é 10, e funcionará bem na maioria dos casos. Se configurarmos pra zero, o servidor não desconectará os clientes até que os mesmos solicitem ou o servidor for reiniciado.



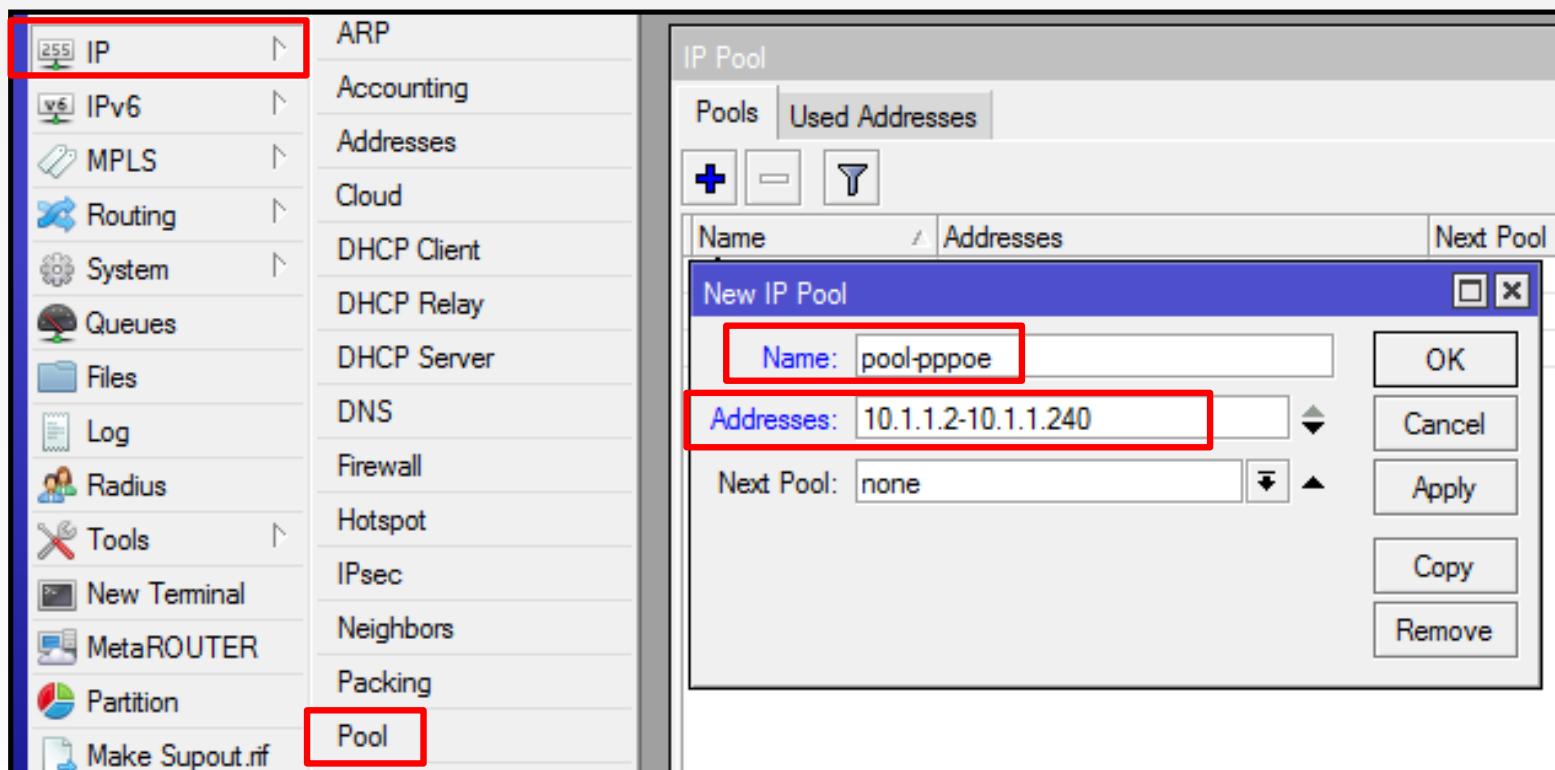
Passos para criar o PPPoE server

- 1) Criar o Pool
- 2) Criar o servidor de PPPoE
- 3) Ajustar ou criar um novo perfil
- 4) Criar usuários



Criando um Pool

- Esses são os endereços que serão entregues ao clientes que se conectarem no servidor de PPPoE.
- Para fins de organização iremos reservar o primeiro IP utilizável para usarmos em nosso roteador (no nosso caso o 10.1.1.1).
- Também iremos fazer uma reserva de endereço para cliente que por ventura precisarem de IP fixo (no nosso caso do 10.1.1.241 até o 10.1.1.254)

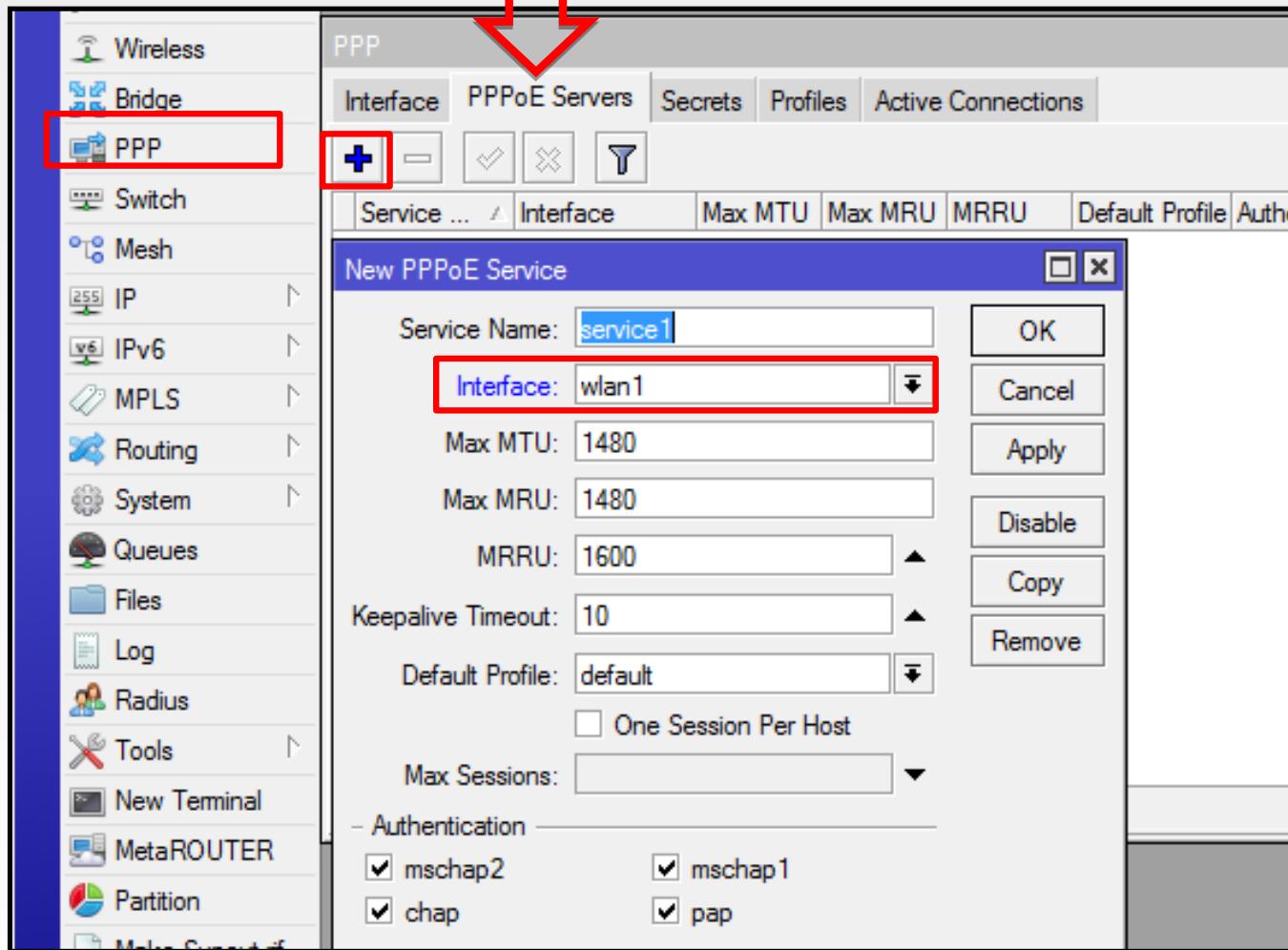


Criando o PPPoE server

Redes Brasil

Service Name = Nome que os clientes vão procurar (pppoe-discovery).

Interface = Interface onde o servidor pppoe vai escutar.





Criando um novo perfil

- **Name** = Nome de identificação do perfil
- **Local Address** = Endereço que será utilizado no servidor de PPPoE
- **Remote Address** = Endereços que serão entregues ao clientes que se conectarem(nesse caso selecionamos o pool previamente criado).

The screenshot shows a network configuration interface with a sidebar on the left and a main panel on the right.

Left Sidebar:

- Wireless
- Bridge
- PPP** (highlighted with a red box)
- Switch
- Mesh
- IP
- IPv6
- MPLS
- Routing
- System

Main Panel:

The main panel has a header with tabs: Interface, PPPoE Servers, Secrets, **Profiles**, and Active Connections. The Profiles tab is selected.

Below the header are four buttons: a blue plus sign (+), a minus sign (-), a folder icon, and a magnifying glass icon.

A table below the buttons lists profiles. The first profile is highlighted with a blue bar and labeled "PPP Profile <perfil-300k>".

Name	Local Address	Remote Address	Bridge
Perfil-300k	10.1.1.1	pool-pppoe	

The "Perfil-300k" row has four tabs: General, Protocols, Limits, and Queue. The General tab is selected.

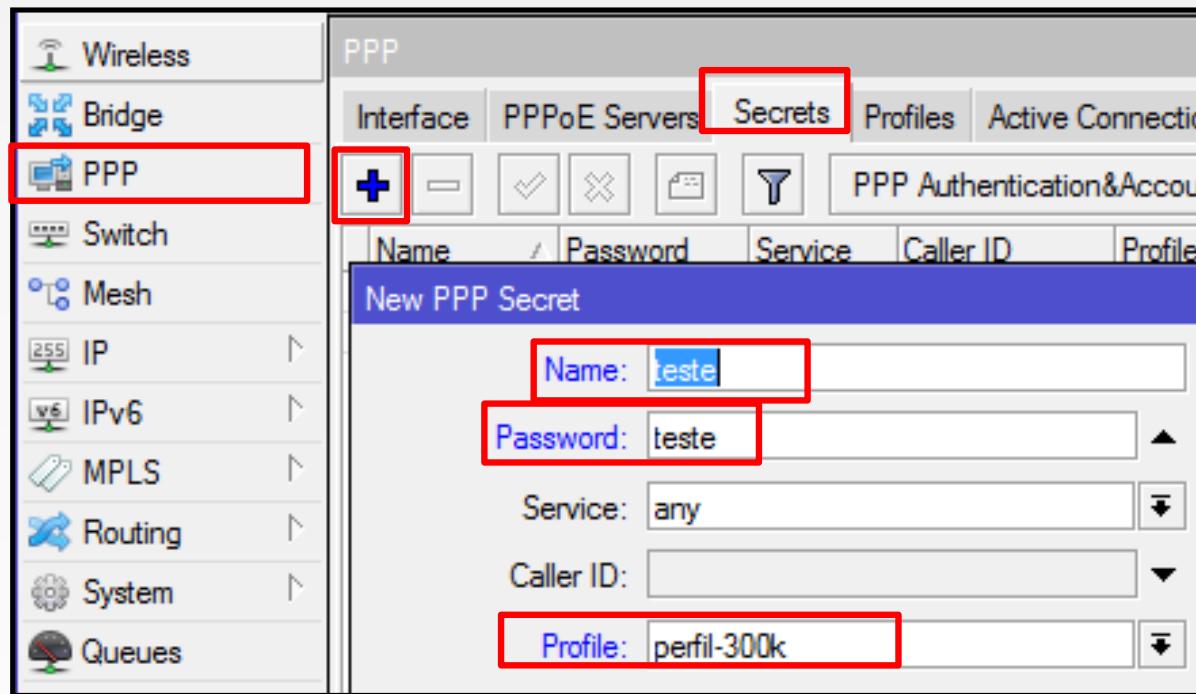
Fields in the General tab are highlighted with red boxes:

- Name: perfil-300k
- Local Address: 10.1.1.1
- Remote Address: pool-pppoe



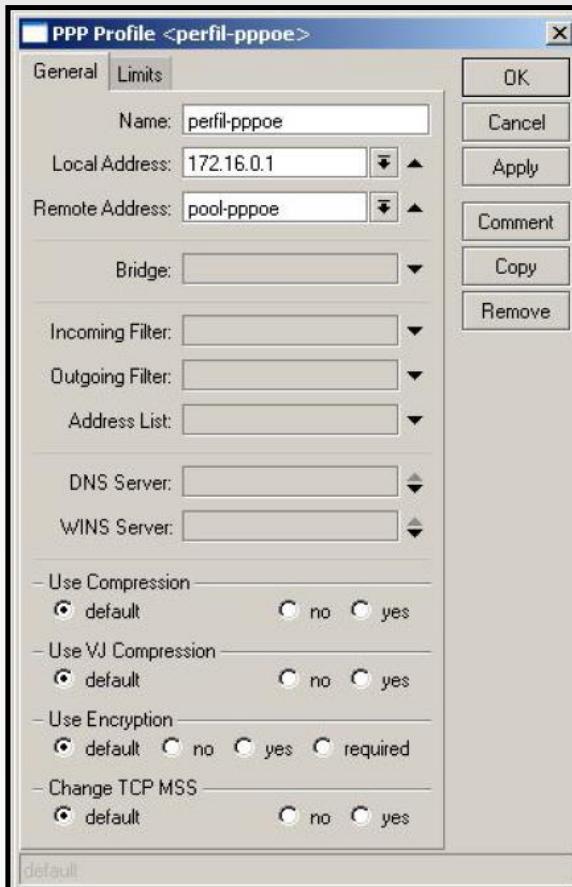
Criando um usuário

- Adicione um usuário e senha
- Obs.: Caso queira verificar o MAC-Address, adicione em Caller ID. Esta opção não é obrigatória, mas é um parâmetro a mais para segurança.





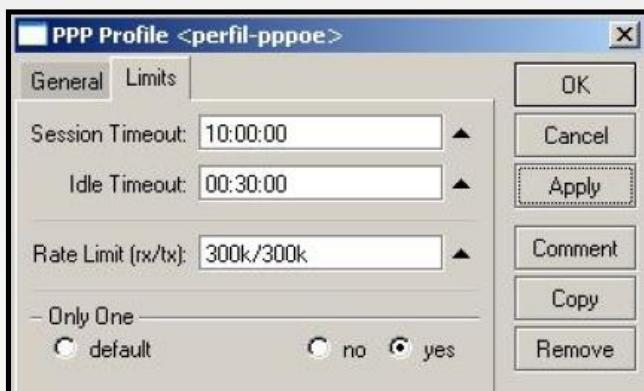
Mais sobre perfis



- Bridge: Bridge para associar ao perfil
- Incoming/Outgoing Filter: Nome do canal do firewall para pacotes entrando/saindo.
- Address List: Lista de endereços IP para associar ao perfil.
- DNS Server: Configuração dos servidores DNS a atribuir aos clientes.
- Use Compression/Encryption/Change TCP MSS: caso estejam em default, vão associar ao valor que está configurado no perfil default-profile.



Mais sobre perfis



- Session Timeout: Duração máxima de uma sessão PPPoE.
- Idle Timeout: Período de ociosidade na transmissão de uma sessão. Se não houver tráfego IP dentro do período configurado, a sessão é terminada.
- Rate Limit: Limitação da velocidade na forma rx-rate/tx-rate. Pode ser usado também na forma rx-rate/tx-rate rx-burst-rate/tx-burstrate rx-burst-threshold/tx-burst-threshold burst-time priority rx-rate-min/tx-rate-min.
- Only One: Permite apenas uma sessão para o mesmo usuário.



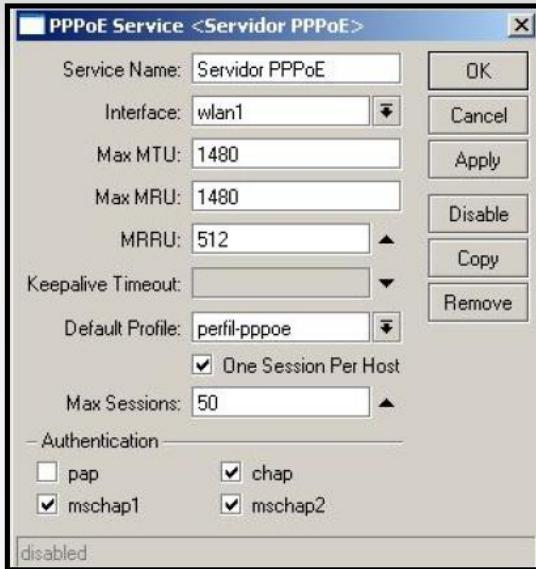
Mais sobre o database



- Service: Especifica o serviço disponível para este cliente em particular.
- Caller ID: MAC Address do cliente.
- Local/Remote Address: Endereço IP Local (servidor) e remote(cliente) que poderão ser atribuídos a um cliente em particular.
- Limits Bytes IN/Out: Quantidade em bytes que o cliente pode trafegar por sessão PPPoE.
- Routes: Rotas que são criadas do lado do servidor para esse cliente específico. Várias rotas podem ser adicionadas separadas por vírgula.
Dst-address gateway metric



Mais sobre o PPPoE Server

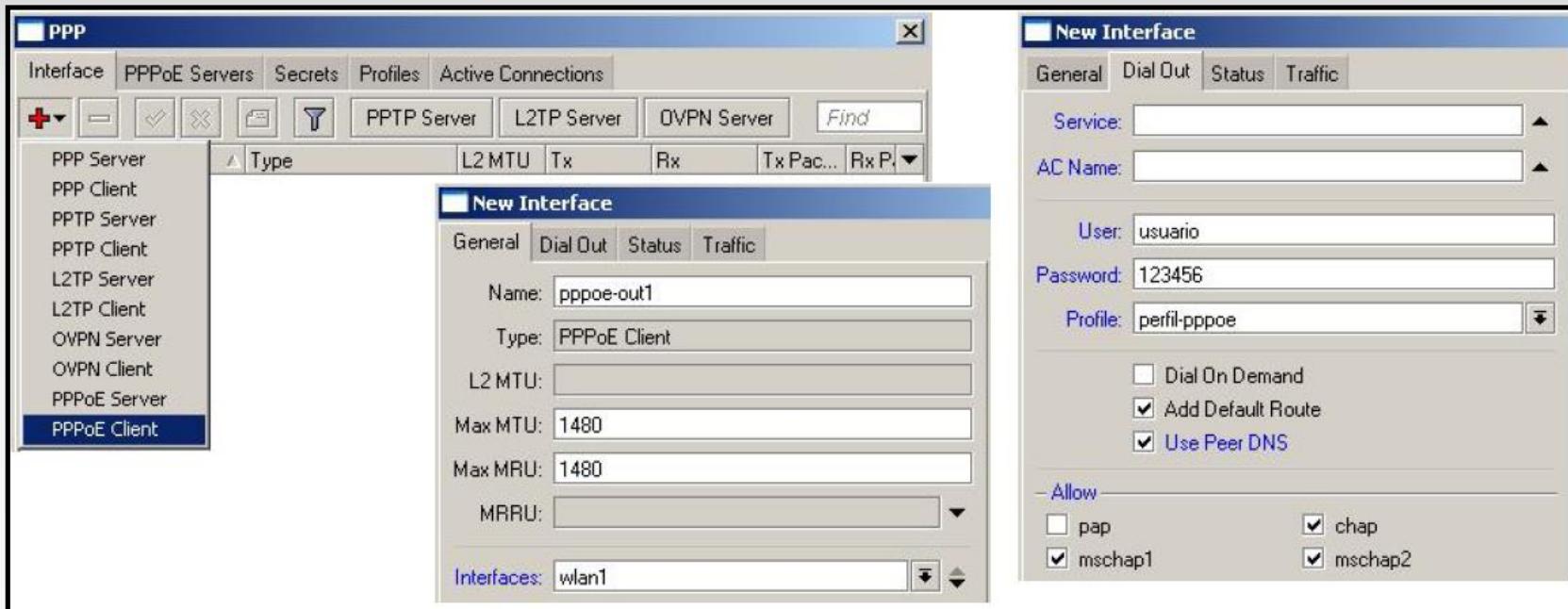


O concentrador PPPoE do MikroTik suporta múltiplos servidores para cada interface com diferentes nomes de serviço. Além do nome do serviço, o nome do concentrador de acesso pode ser usado pelos clientes para identificar o acesso em que se deve registrar. O nome do concentrador é a identidade do roteador. O valor de MTU/MRU inicialmente recomendado para o PPPoE é 1480 bytes. Em uma rede sem fio, o servidor PPPoE pode ser configurado no AP. Para clientes MikroTik, a interface de rádio pode ser configurada com a MTU em 1600 bytes e a MTU da interface PPPoE em 1500 bytes.

Isto otimiza a transmissão de pacotes e evita problemas associados a MTU menor que 1500 bytes. A opção One Session Per Host permite somente uma sessão por host(MAC Address). Por fim, Max Sessions define o número máximo de sessões que o concentrador suportará.



Configurando o PPPoE Client



- AC Name:** Nome do concentrador. Deixando em branco conecta em qualquer um.
- Service:** Nome do serviço designado no servidor PPPoE.
- Dial On Demand:** Disca sempre que é gerado tráfego de saída.
- Add Default Route:** Adiciona um rota padrão(default).
- User Peer DNS:** Usa o DNS do servidor PPPoE.

Perguntas ?

Redes Brasil

