Problemas e soluções reais em prover Alta Disponibilidade com OSPF, MPLS, BGP e VRF.

Palestrante: Lacier Dias

Introdução

Nome: Lacier Dias

- ✓ Formado em Segurança da Informação
- ✓ Pós-Graduado em Segurança de Rede de Computadores
- ✓ MBA em Gerenciamento de Projetos – FGV

- ✓ Treinamentos e Certificações:
  - ➢ IPV6
  - ➢ MikroTik Consultant, MTCNA, MTCWE, MTCUME, MTCRE e MTCINE.
  - ➢ Microsoft Certified Professional
  - ➢ ITIL, Cobit
  - ➢ BSC (Balanced Scorecard)
  - ➢ ISO 27001 e 27002
  - ➢ Motorola, Proxim e Alvarion
  - ➢ Allied Telesis, Cisco e Juniper
  - ➢ Hughes Networks

Objetivos da Apresentação

- ✓ Apresentar como foi migrar grandes redes em produção em bridge total ou parcial para roteamento dinâmico.
- ✓ Abordar como podemos fazer isso de maneira pouco traumática.
- ✓ Apresentar cases reais de migração com baixo impacto aos clientes.
- ✓ Mostrar o ambiente pós migração.

Alta Disponibilidade

- Um sistema de alta disponibilidade é um sistema resistente a falhas.

- Abordaremos:
  - A rede
  - Humana

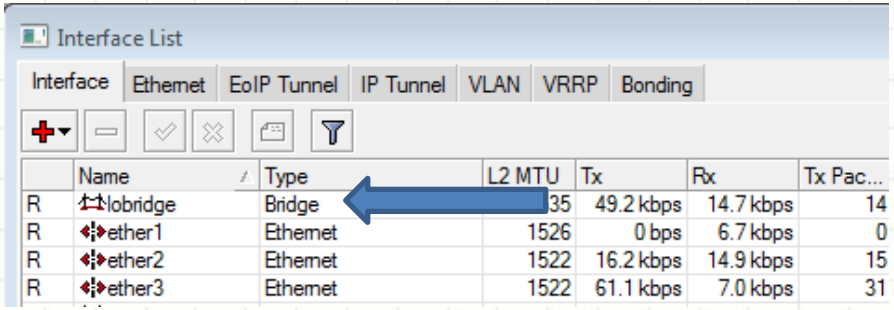
OSPF, MPLS, BGP e VRF

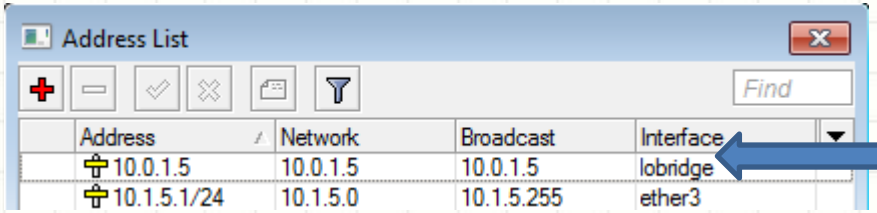
- Quais benefícios e impacto do uso destes protocolos????

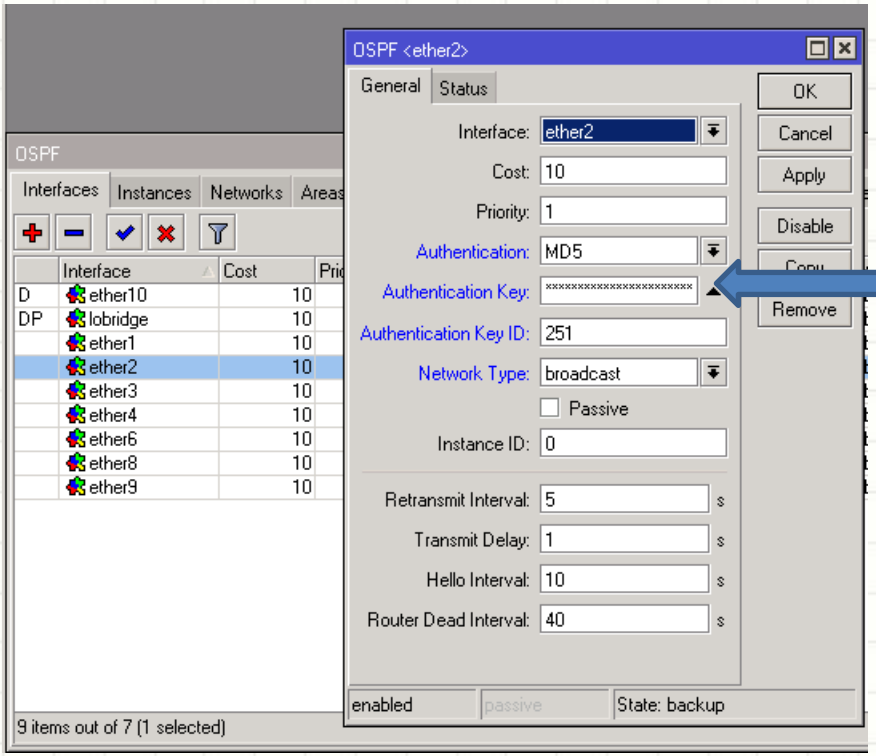
OSPF

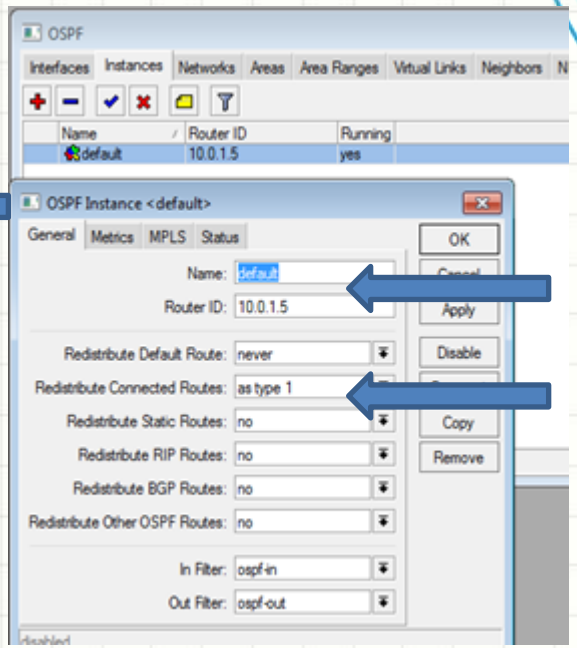
- **Vantagens:**
  - O OSPF é um protocolo especialmente projetado para o ambiente TCP/IP para ser usado internamente ao AS.
  - Publicação de Tabelas: Link State Routing Protocol e a busca pelo menor caminho.
  - Algoritmo Shortest Path First - SPF.
  - Simples de configurar no Mikrotik.
- **Problema mais comum:**
  - Configurações inseguras.

OSPF

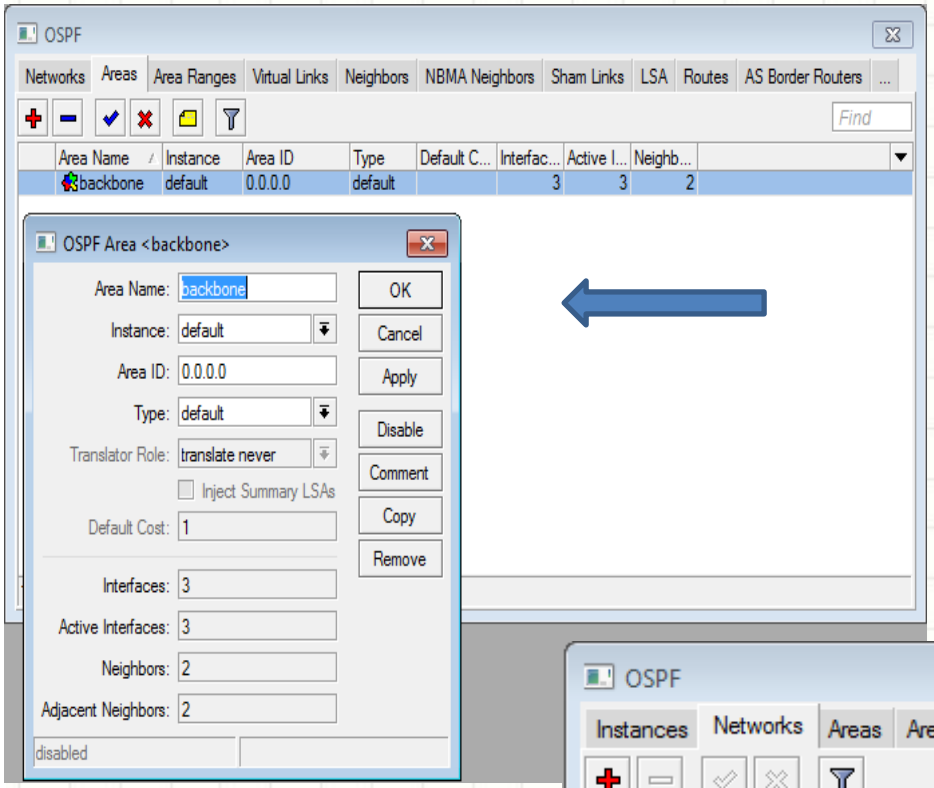

Interface List
Interface
Ethernet
EoIP Tunnel
IP Tunnel
VLAN
VRRP
Bonding
Name
Type
L2 MTU
Tx
Rx
Tx Pac...
R lobridge Bridge 35 49.2 kbps 14.7 kbps 14
R ether1 Ethernet 1526 0 bps 6.7 kbps 0
R ether2 Ethernet 1522 16.2 kbps 14.9 kbps 15
R ether3 Ethernet 1522 61.1 kbps 7.0 kbps 31

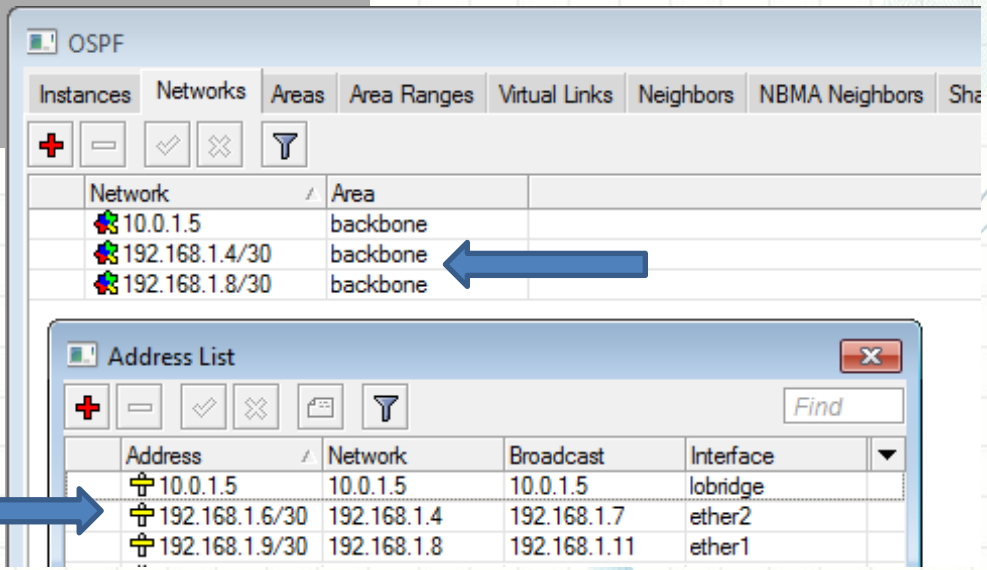

Address List
Find
Address
Network
Broadcast
Interface
10.0.1.5 10.0.1.5 10.0.1.5 lobridge
10.1.5.1/24 10.1.5.0 10.1.5.255 ether3


OSPF
Interfaces
Instances
Networks
Areas
Interface
Cost
D ether10 10
DP lobridge 10
ether1 10
ether2 10
ether3 10
ether4 10
ether6 10
ether8 10
ether9 10
9 items out of 7 (1 selected)
OSPF <ether2>
General
Status
OK
Cancel
Apply
Disable
Copy
Remove
Interface: ether2
Cost: 10
Priority: 1
Authentication: MD5
Authentication Key: ••••••••••••••••••••••••
Authentication Key ID: 251
Network Type: broadcast
Passive
Instance ID: 0
Retransmit Interval: 5 s
Transmit Delay: 1 s
Hello Interval: 10 s
Router Dead Interval: 40 s
enabled
passive
State: backup


OSPF
Interfaces
Instances
Networks
Areas
Area Ranges
Virtual Links
Neighbors
Name
Router ID
Running
default 10.0.1.5 yes
OSPF Instance <default>
General
Metrics
MPLS
Status
OK
Apply
Disable
Copy
Remove
Name: default
Router ID: 10.0.1.5
Redistribute Default Route: never
Redistribute Connected Routes: as type 1
Redistribute Static Routes: no
Redistribute RIP Routes: no
Redistribute BGP Routes: no
Redistribute Other OSPF Routes: no
In Filter: ospf-in
Out Filter: ospf-out

OSPF


OSPF
Networks
Areas
Area Ranges
Virtual Links
Neighbors
NBMA Neighbors
Sham Links
LSA
Routes
AS Border Routers
...
Find
Area Name
Instance
Area ID
Type
Default C...
Interfac...
Active I...
Neighb...
backbone
default
0.0.0.0
default
3
3
2
OSPF Area <backbone>
Area Name: backbone
Instance: default
Area ID: 0.0.0.0
Type: default
Translator Role: translate never
Inject Summary LSAs
Default Cost: 1
Interfaces: 3
Active Interfaces: 3
Neighbors: 2
Adjacent Neighbors: 2
disabled
OK
Cancel
Apply
Disable
Comment
Copy
Remove


OSPF
Instances
Networks
Areas
Area Ranges
Virtual Links
Neighbors
NBMA Neighbors
Sha
Network
Area
10.0.1.5
backbone
192.168.1.4/30
backbone
192.168.1.8/30
backbone
Address List
Find
Address
Network
Broadcast
Interface
10.0.1.5
10.0.1.5
10.0.1.5
lobridge
192.168.1.6/30
192.168.1.4
192.168.1.7
ether2
192.168.1.9/30
192.168.1.8
192.168.1.11
ether1

MPLS

❖ Multi Protocol Label Switching é um mecanismo de transporte que foi padronizado através da RFC-3031 e opera numa camada OSI intermediária às definições tradicionais do Layer 2 (Enlace) e Layer 3 (Rede), por isso que se tornou recorrente ser referido como um protocolo de "Layer 2,5".

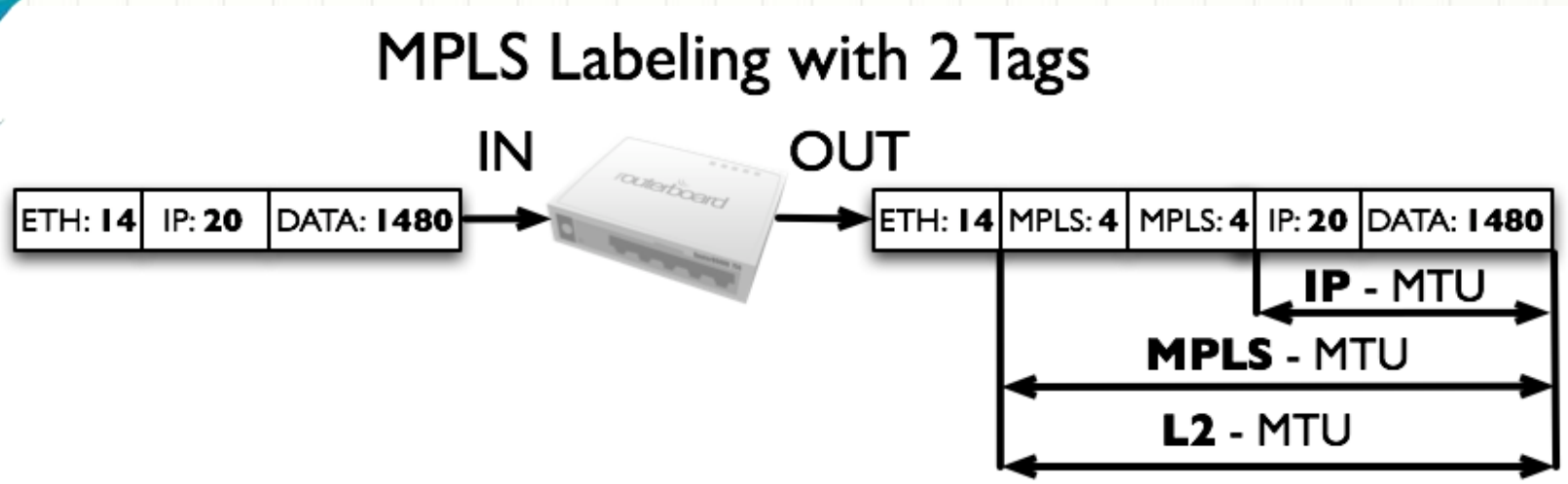
✓ **Vantagens**

- ➢ Melhor desempenho no encaminhamento de pacotes;
- ➢ Criação de caminhos (Label Switching Paths) entre os roteadores;
- ➢ Possibilidade de associar requisitos de QoS, baseados nos rótulos carregados pelos pacotes.

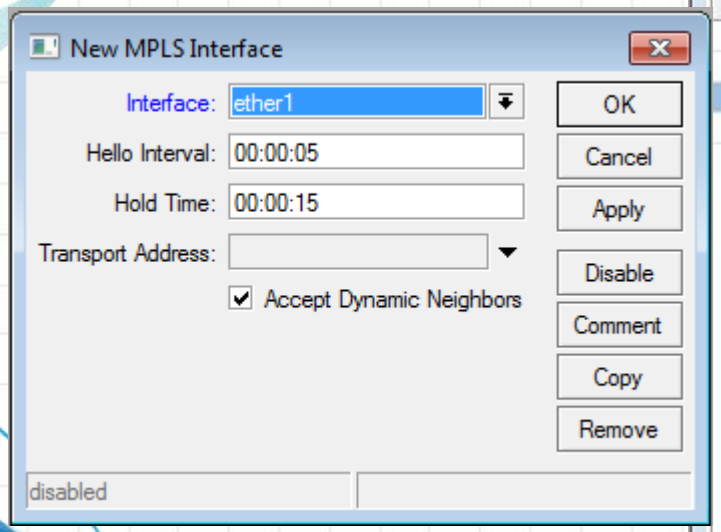
✓ **Desvantagens**

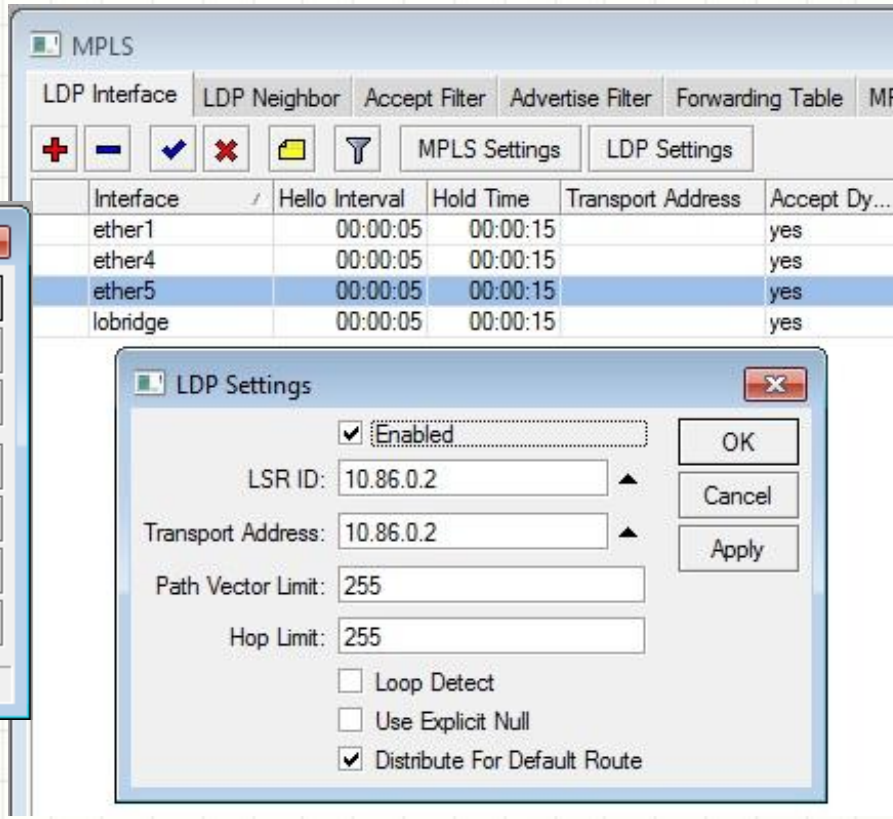
- ➢ Problemas graves com a alteração do MTU.

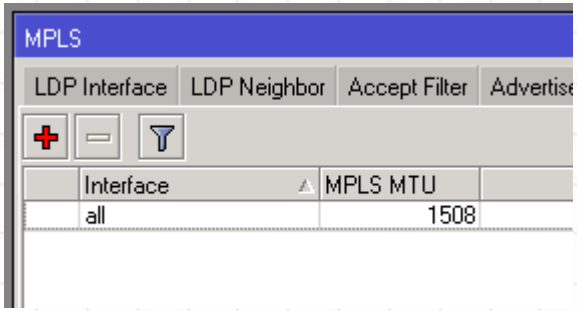
MPLS


MPLS Labeling with 2 Tags
IN
OUT
ETH: 14
IP: 20
DATA: 1480
routerboard
ETH: 14
MPLS: 4
MPLS: 4
IP: 20
DATA: 1480
IP - MTU
MPLS - MTU
L2 - MTU

MPLS


New MPLS Interface
Interface: ether1
Hello Interval: 00:00:05
Hold Time: 00:00:15
Transport Address:
Accept Dynamic Neighbors
OK
Cancel
Apply
Disable
Comment
Copy
Remove
disabled

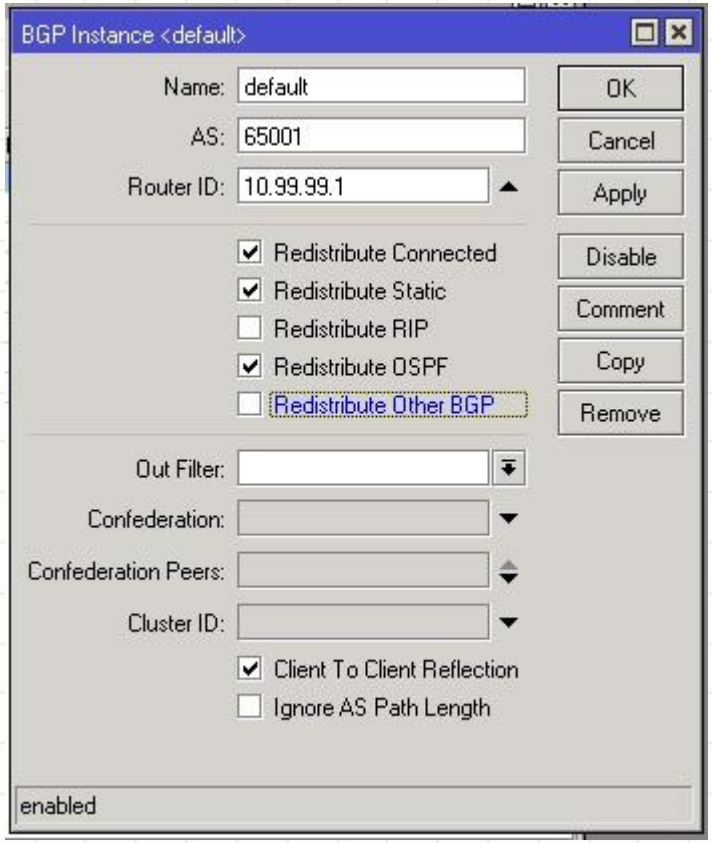

MPLS
LDP Interface
LDP Neighbor
Accept Filter
Advertise Filter
Forwarding Table
MPLS Settings
LDP Settings
Interface
Hello Interval
Hold Time
Transport Address
Accept Dy...
ether1 00:00:05 00:00:15 yes
ether4 00:00:05 00:00:15 yes
ether5 00:00:05 00:00:15 yes
lobridge 00:00:05 00:00:15 yes
LDP Settings
Enabled
LSR ID: 10.86.0.2
Transport Address: 10.86.0.2
Path Vector Limit: 255
Hop Limit: 255
Loop Detect
Use Explicit Null
Distribute For Default Route
OK
Cancel
Apply

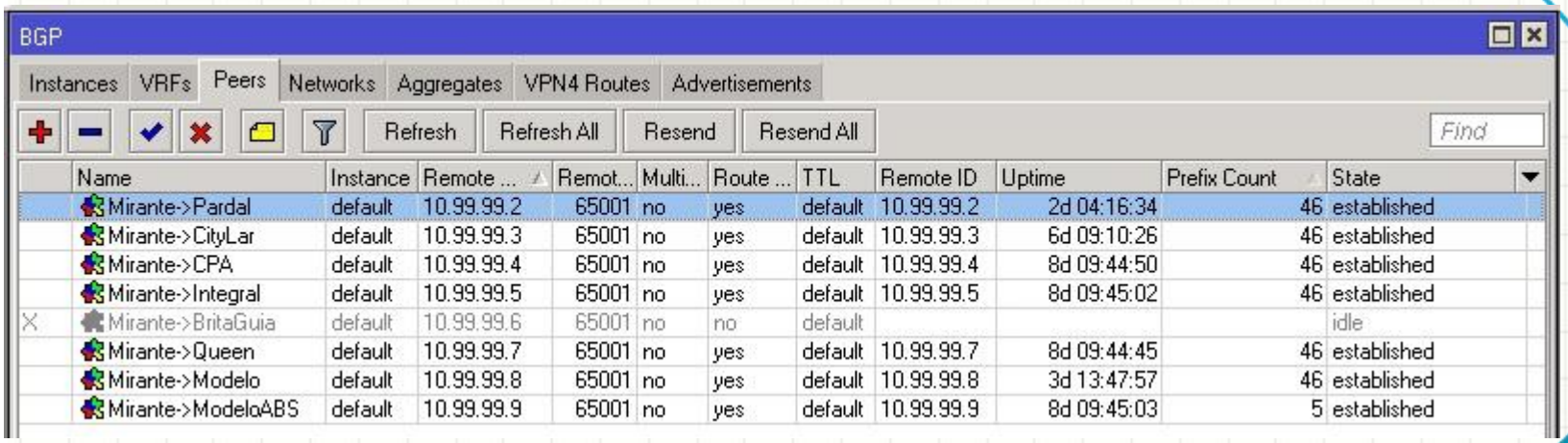

MPLS
LDP Interface
LDP Neighbor
Accept Filter
Interface
MPLS MTU
all 1508

BGP

- **Vantagens:**
  - O BGP - foi projetado para evitar loops de roteamento em topologias arbitrarias, o mais serio problema de seu antecessor, o EGP (Exterior Gateway Protocol).
  - A função primária de um sistema BGP é trocar informação de acesso à rede, inclusive informação sobre a lista das trajetórias dos ASs, com outros sistemas BGP.
- **Problema:**
  - Configurações requer atenção e conhecimento.

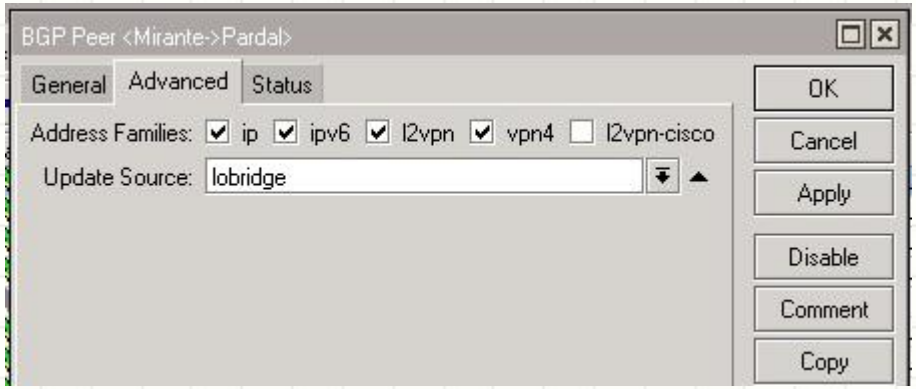
iBGP

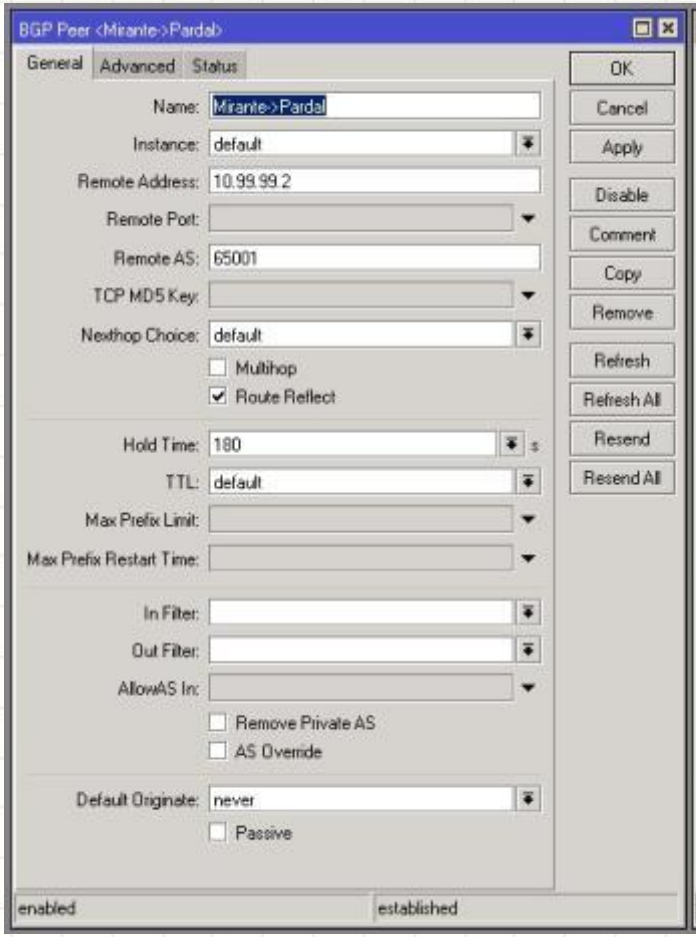


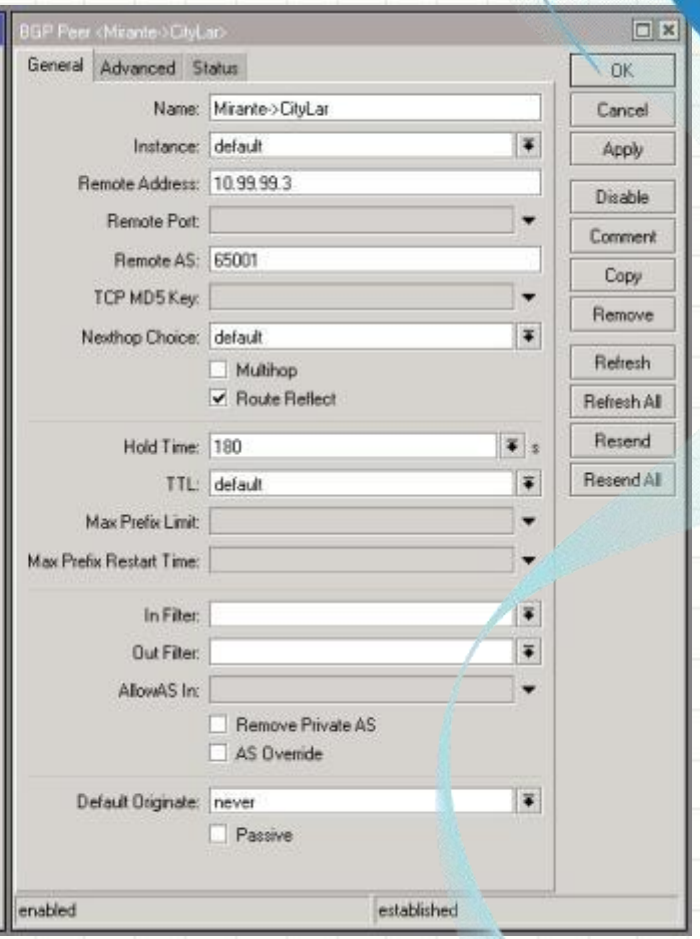


Name	Instance	Remote ...	Remot...	Multi...	Route ...	TTL	Remote ID	Uptime	Prefix Count	State
Mirante->Pardal	default	10.99.99.2	65001	no	yes	default	10.99.99.2	2d 04:16:34	46	established
Mirante->CityLar	default	10.99.99.3	65001	no	yes	default	10.99.99.3	6d 09:10:26	46	established
Mirante->CPA	default	10.99.99.4	65001	no	yes	default	10.99.99.4	8d 09:44:50	46	established
Mirante->Integral	default	10.99.99.5	65001	no	yes	default	10.99.99.5	8d 09:45:02	46	established
Mirante->BritaGuia	default	10.99.99.6	65001	no	no	default				idle
Mirante->Queen	default	10.99.99.7	65001	no	yes	default	10.99.99.7	8d 09:44:45	46	established
Mirante->Modelo	default	10.99.99.8	65001	no	yes	default	10.99.99.8	3d 13:47:57	46	established
Mirante->ModeloABS	default	10.99.99.9	65001	no	yes	default	10.99.99.9	8d 09:45:03	5	established

iBGP


BGP Peer <Mirante->Pardal>
General
Advanced
Status
OK
Cancel
Apply
Disable
Comment
Copy
Address Families: ip ipv6 l2vpn vpn4 l2vpn-cisco
Update Source: lobridge


BGP Peer <Mirante->Pardal>
General
Advanced
Status
OK
Cancel
Apply
Disable
Comment
Copy
Remove
Refresh
Refresh All
Resend
Resend All
Name: Mirante->Pardal
Instance: default
Remote Address: 10.99.99.2
Remote Port:
Remote AS: 65001
TCP MD5 Key:
Nexthop Choice: default
Multihop
Route Reflect
Hold Time: 180 s
TTL: default
Max Prefix Limit:
Max Prefix Restart Time:
In Filter:
Out Filter:
AllowAS In:
Remove Private AS
AS Override
Default Originate: never
Passive
enabled
established


BGP Peer <Mirante->CityLar>
General
Advanced
Status
OK
Cancel
Apply
Disable
Comment
Copy
Remove
Refresh
Refresh All
Resend
Resend All
Name: Mirante->CityLar
Instance: default
Remote Address: 10.99.99.3
Remote Port:
Remote AS: 65001
TCP MD5 Key:
Nexthop Choice: default
Multihop
Route Reflect
Hold Time: 180 s
TTL: default
Max Prefix Limit:
Max Prefix Restart Time:
In Filter:
Out Filter:
AllowAS In:
Remove Private AS
AS Override
Default Originate: never
Passive
enabled
established

VRF

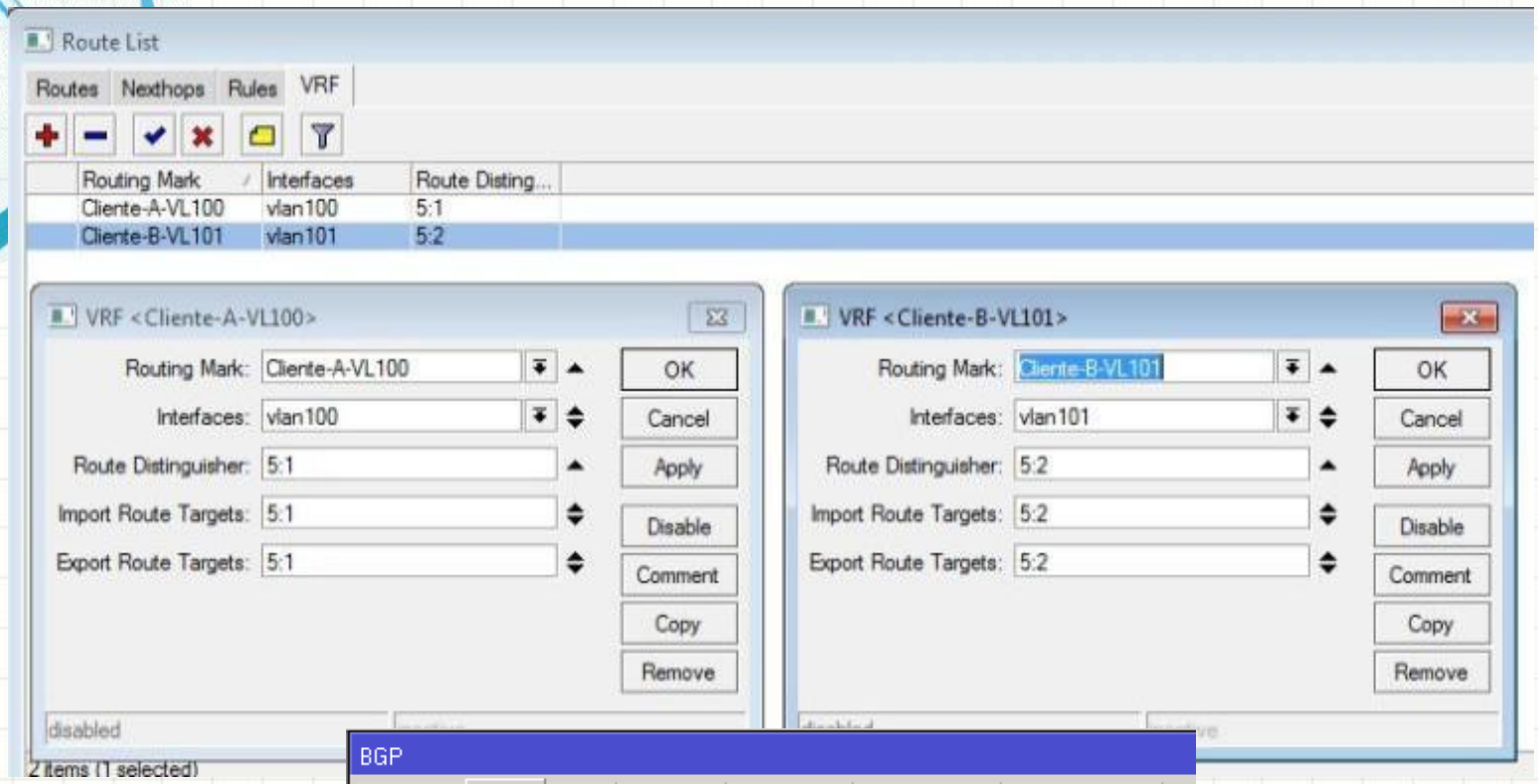
Vantagens

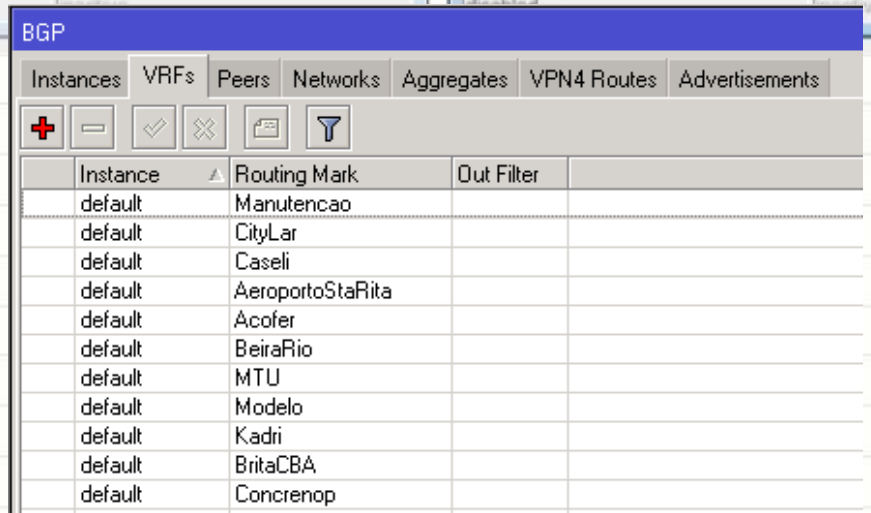
- Virtual Routing and Forwarding, em redes de computadores baseadas em IP, roteamento virtual e Transmissão (VRF) é uma tecnologia que permite que várias instâncias de uma tabela de roteamento possam coexistir dentro do mesmo roteador ao mesmo tempo.
- Segmentação sem alto consumo de processamento;

✓ **Desvantagens**

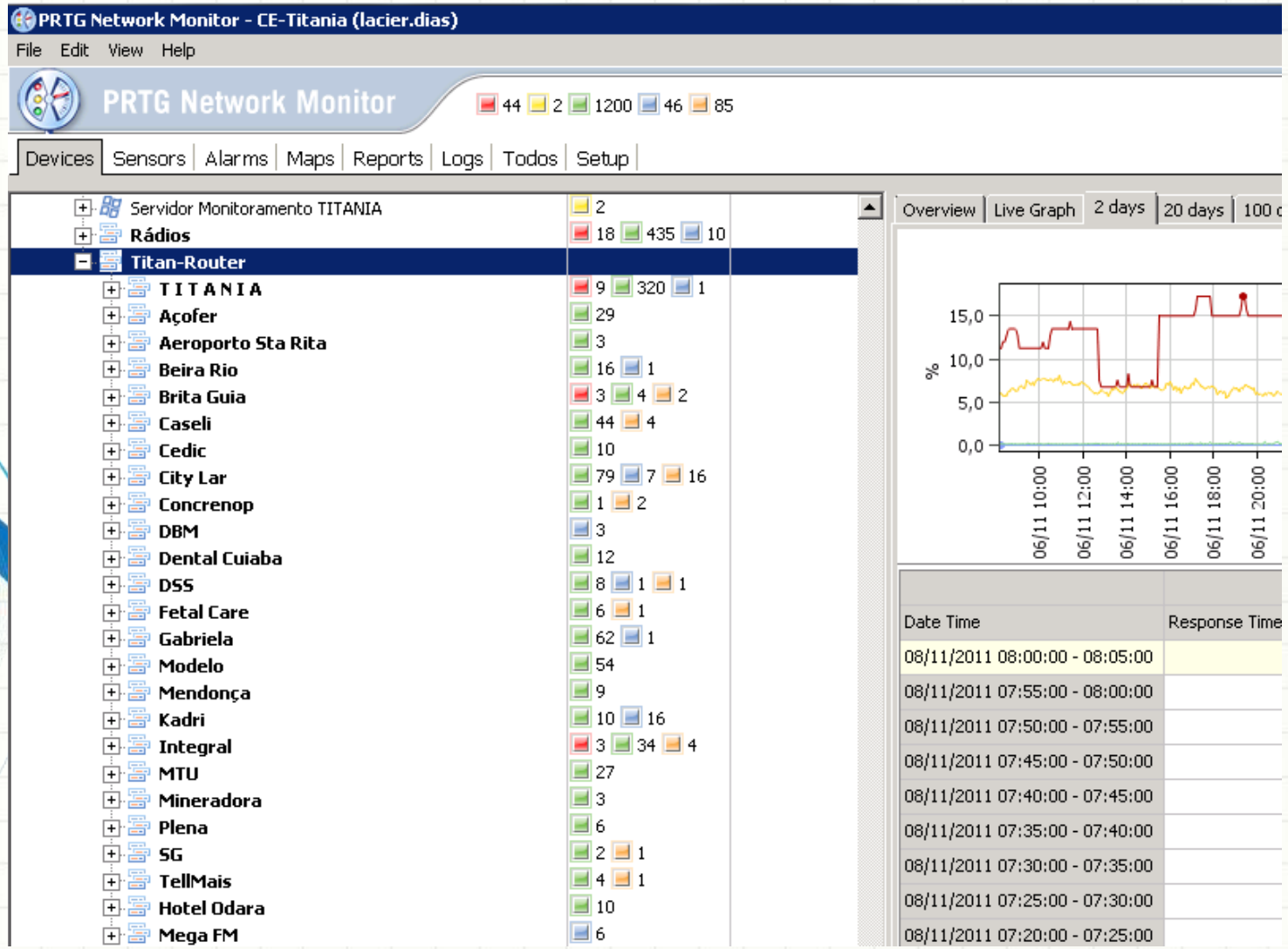
- Configurações requer atenção e conhecimento.

VRF

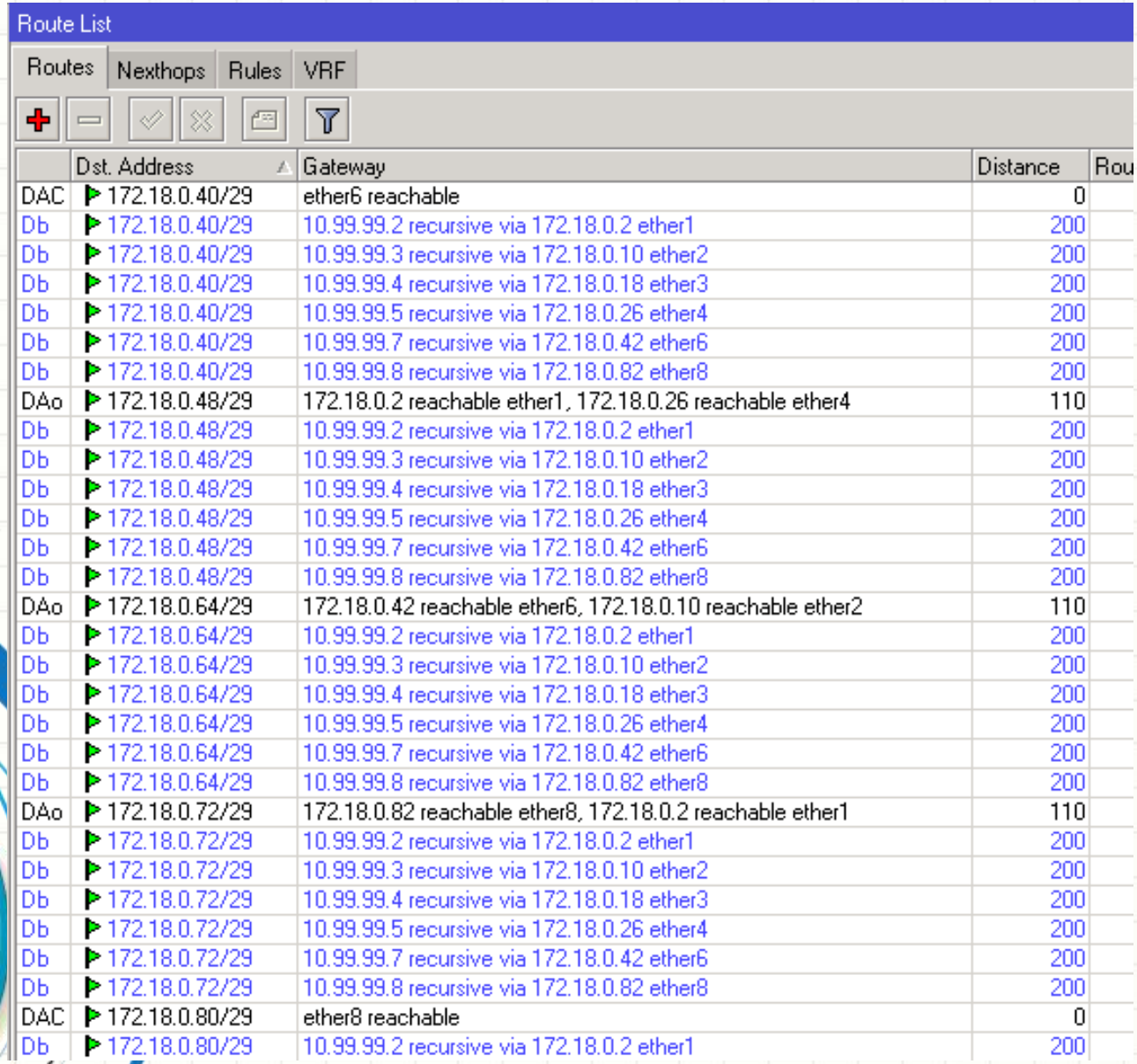

Route List
Routes
Nexthops
Rules
VRF
Routing Mark
Interfaces
Route Disting...
Cliente-A-VL100
vlan100
5:1
Cliente-B-VL101
vlan101
5:2
VRF <Cliente-A-VL100>
Routing Mark: Cliente-A-VL100
Interfaces: vlan100
Route Distinguisher: 5:1
Import Route Targets: 5:1
Export Route Targets: 5:1
OK
Cancel
Apply
Disable
Comment
Copy
Remove
disabled
VRF <Cliente-B-VL101>
Routing Mark: Cliente-B-VL101
Interfaces: vlan101
Route Distinguisher: 5:2
Import Route Targets: 5:2
Export Route Targets: 5:2
OK
Cancel
Apply
Disable
Comment
Copy
Remove
2 items (1 selected)


BGP
Instances
VRFs
Peers
Networks
Aggregates
VPN4 Routes
Advertisements
Instance
Routing Mark
Out Filter
default Manutencao
default CityLar
default Caseli
default AeroportoStaRita
default Acofer
default BeiraRio
default MTU
default Modelo
default Kadri
default BritaCBA
default Concrenop

MONITORAMENTO

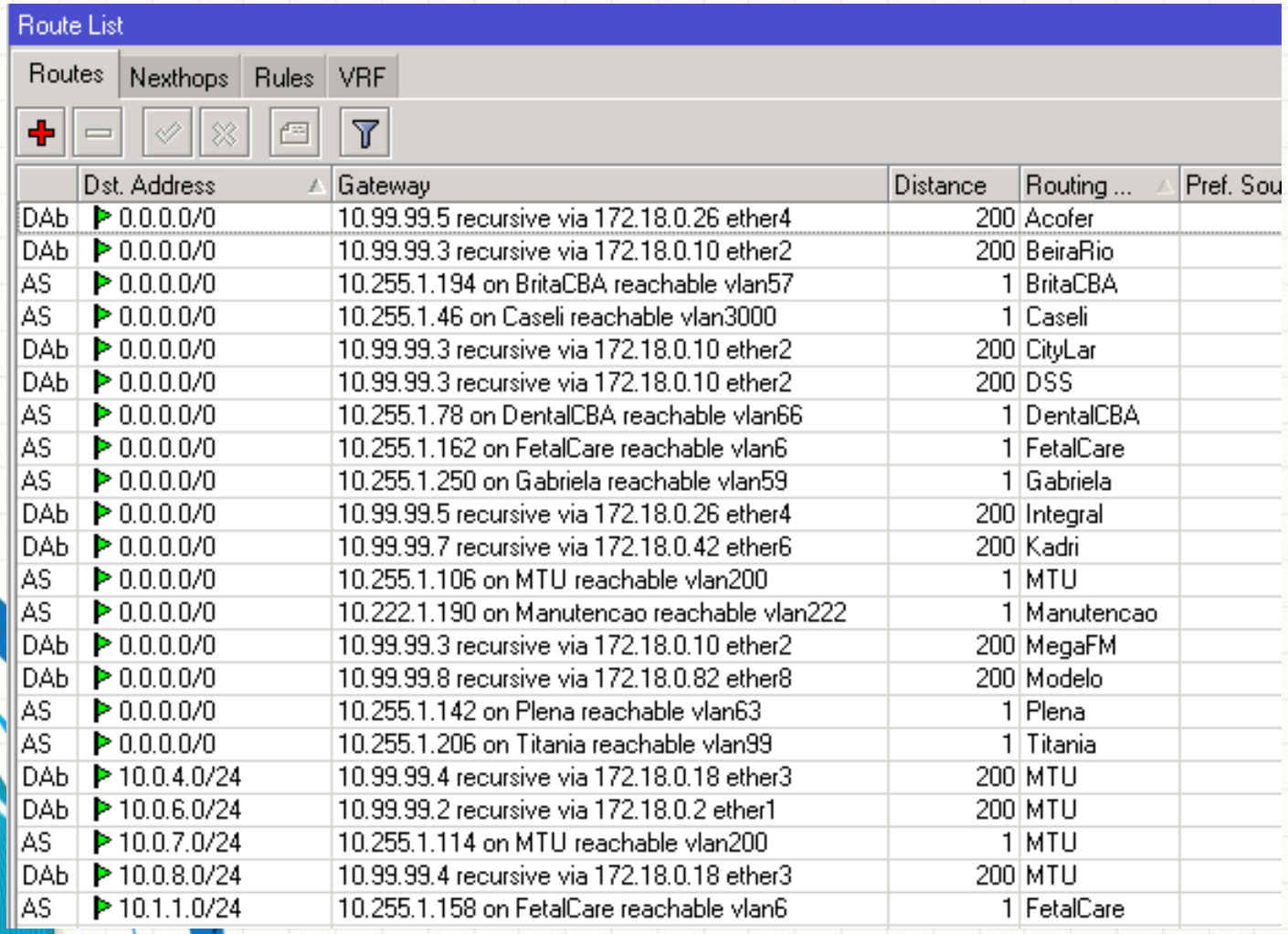


RESULTADO FINAL



	Dst. Address	Gateway	Distance	Rou
DAC	172.18.0.40/29	ether6 reachable	0	
Db	172.18.0.40/29	10.99.99.2 recursive via 172.18.0.2 ether1	200	
Db	172.18.0.40/29	10.99.99.3 recursive via 172.18.0.10 ether2	200	
Db	172.18.0.40/29	10.99.99.4 recursive via 172.18.0.18 ether3	200	
Db	172.18.0.40/29	10.99.99.5 recursive via 172.18.0.26 ether4	200	
Db	172.18.0.40/29	10.99.99.7 recursive via 172.18.0.42 ether6	200	
Db	172.18.0.40/29	10.99.99.8 recursive via 172.18.0.82 ether8	200	
DAo	172.18.0.48/29	172.18.0.2 reachable ether1, 172.18.0.26 reachable ether4	110	
Db	172.18.0.48/29	10.99.99.2 recursive via 172.18.0.2 ether1	200	
Db	172.18.0.48/29	10.99.99.3 recursive via 172.18.0.10 ether2	200	
Db	172.18.0.48/29	10.99.99.4 recursive via 172.18.0.18 ether3	200	
Db	172.18.0.48/29	10.99.99.5 recursive via 172.18.0.26 ether4	200	
Db	172.18.0.48/29	10.99.99.7 recursive via 172.18.0.42 ether6	200	
Db	172.18.0.48/29	10.99.99.8 recursive via 172.18.0.82 ether8	200	
DAo	172.18.0.64/29	172.18.0.42 reachable ether6, 172.18.0.10 reachable ether2	110	
Db	172.18.0.64/29	10.99.99.2 recursive via 172.18.0.2 ether1	200	
Db	172.18.0.64/29	10.99.99.3 recursive via 172.18.0.10 ether2	200	
Db	172.18.0.64/29	10.99.99.4 recursive via 172.18.0.18 ether3	200	
Db	172.18.0.64/29	10.99.99.5 recursive via 172.18.0.26 ether4	200	
Db	172.18.0.64/29	10.99.99.7 recursive via 172.18.0.42 ether6	200	
Db	172.18.0.64/29	10.99.99.8 recursive via 172.18.0.82 ether8	200	
DAo	172.18.0.72/29	172.18.0.82 reachable ether8, 172.18.0.2 reachable ether1	110	
Db	172.18.0.72/29	10.99.99.2 recursive via 172.18.0.2 ether1	200	
Db	172.18.0.72/29	10.99.99.3 recursive via 172.18.0.10 ether2	200	
Db	172.18.0.72/29	10.99.99.4 recursive via 172.18.0.18 ether3	200	
Db	172.18.0.72/29	10.99.99.5 recursive via 172.18.0.26 ether4	200	
Db	172.18.0.72/29	10.99.99.7 recursive via 172.18.0.42 ether6	200	
Db	172.18.0.72/29	10.99.99.8 recursive via 172.18.0.82 ether8	200	
DAC	172.18.0.80/29	ether8 reachable	0	
Db	172.18.0.80/29	10.99.99.2 recursive via 172.18.0.2 ether1	200	

RESULTADO FINAL



	Dst. Address	Gateway	Distance	Routing ...	Pref. Sou
DAb	0.0.0.0/0	10.99.99.5 recursive via 172.18.0.26 ether4	200	Acofer	
DAb	0.0.0.0/0	10.99.99.3 recursive via 172.18.0.10 ether2	200	BeiraRio	
AS	0.0.0.0/0	10.255.1.194 on BritaCBA reachable vlan57	1	BritaCBA	
AS	0.0.0.0/0	10.255.1.46 on Caseli reachable vlan3000	1	Caseli	
DAb	0.0.0.0/0	10.99.99.3 recursive via 172.18.0.10 ether2	200	CityLar	
DAb	0.0.0.0/0	10.99.99.3 recursive via 172.18.0.10 ether2	200	DSS	
AS	0.0.0.0/0	10.255.1.78 on DentalCBA reachable vlan66	1	DentalCBA	
AS	0.0.0.0/0	10.255.1.162 on FetalCare reachable vlan6	1	FetalCare	
AS	0.0.0.0/0	10.255.1.250 on Gabriela reachable vlan59	1	Gabriela	
DAb	0.0.0.0/0	10.99.99.5 recursive via 172.18.0.26 ether4	200	Integral	
DAb	0.0.0.0/0	10.99.99.7 recursive via 172.18.0.42 ether6	200	Kadri	
AS	0.0.0.0/0	10.255.1.106 on MTU reachable vlan200	1	MTU	
AS	0.0.0.0/0	10.222.1.190 on Manutencao reachable vlan222	1	Manutencao	
DAb	0.0.0.0/0	10.99.99.3 recursive via 172.18.0.10 ether2	200	MegaFM	
DAb	0.0.0.0/0	10.99.99.8 recursive via 172.18.0.82 ether8	200	Modelo	
AS	0.0.0.0/0	10.255.1.142 on Plena reachable vlan63	1	Plena	
AS	0.0.0.0/0	10.255.1.206 on Titania reachable vlan99	1	Titania	
DAb	10.0.4.0/24	10.99.99.4 recursive via 172.18.0.18 ether3	200	MTU	
DAb	10.0.6.0/24	10.99.99.2 recursive via 172.18.0.2 ether1	200	MTU	
AS	10.0.7.0/24	10.255.1.114 on MTU reachable vlan200	1	MTU	
DAb	10.0.8.0/24	10.99.99.4 recursive via 172.18.0.18 ether3	200	MTU	
AS	10.1.1.0/24	10.255.1.158 on FetalCare reachable vlan6	1	FetalCare	

Planejamento da Migração

1. Treinamento
   - 1 semana
2. Planejamento
   - 3 semanas
3. Teste e Homologação
   - 2 semanas
4. Migração
   - 1 dia
5. Ajuste fino
   - 2 dias

Conclusão

Sucesso da migração depende do planejamento.

Não importa o tamanho da sua rede.

PERGUNTAS??????

AGRADECIMENTOS

Obrigado!!!

LACIER DIAS

LACIER@TITANIA.COM.BR

MSN: LACIER_DIAS@HOTMAIL.COM

SKYPE: LACIER.DIAS

(65) 9968-5684