[MikrotikBrasil]
Routers & Wireless Systems

Implementação de IPV6 no Mikrotik

MUM – Brasil 2010
Salvador BA
Wardner Maia

Introdução

Nome: Wardner Maia

→ Engenheiro Eletricista modalidade Eletrotécnica/Eletrônica/Telecomunicações

→ Provedor de Internet desde 1995

→Ministra treinamentos em rádio frequencia desde 2002 e em Mikrotik desde 2006

→Certificações Mikrotik:

Trainer (2007) – Riga, Latvia
MTCWE, MTCRE (2008) – Krakow, Poland
MTCUME, MTCTE (2009) – Praga, Czech Republik
MTCINE (2010) – Vroklaw, Poland

Introdução

MD Brasil – TI & Telecom

→ Operadora de Serviços de Comunicação Multimídia e Serviços de Valor Adicionado

→ Distribuidora oficial de Hardware e Software Mikrotik

→ Integradora e fabricante de equipamentos com produtos homologados na Anatel.

→ Parceira da Mikrotik em treinamentos

www.mikrotikbrasil.com.br / www.mdbrasil.com.br

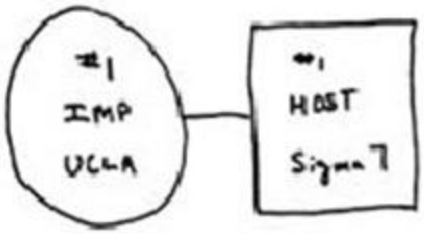
Agenda

- → Porque IPV6, agora
- → Princípios básicos do protocolo IPV6
- → Técnicas para coexistencia e transição
- → Endereçamento e roteamento no IPV6
- → Roteamento estático e dinâmico – RIPng, OSPFv3 e BGP
- → Segurança no IPV6 – IPV6 Firewall
- → IPV6 em ação no mundo real

Porquê IPV6, agora

Porque IPV6 ?

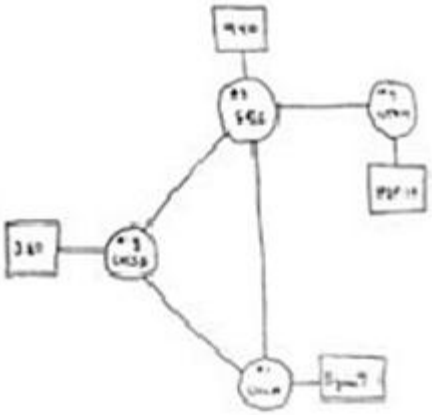
A Internet não foi concebida para ser a grande rede que é hoje



THE ARPA NETWORK

SEPT 1969

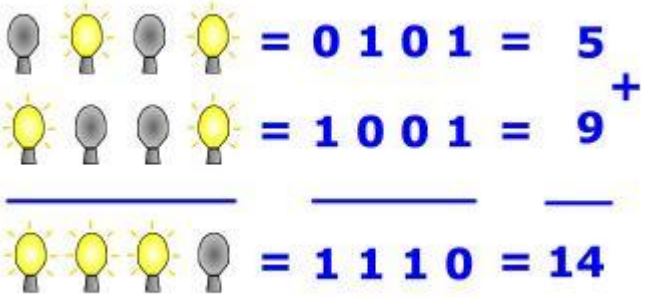
1 NODE



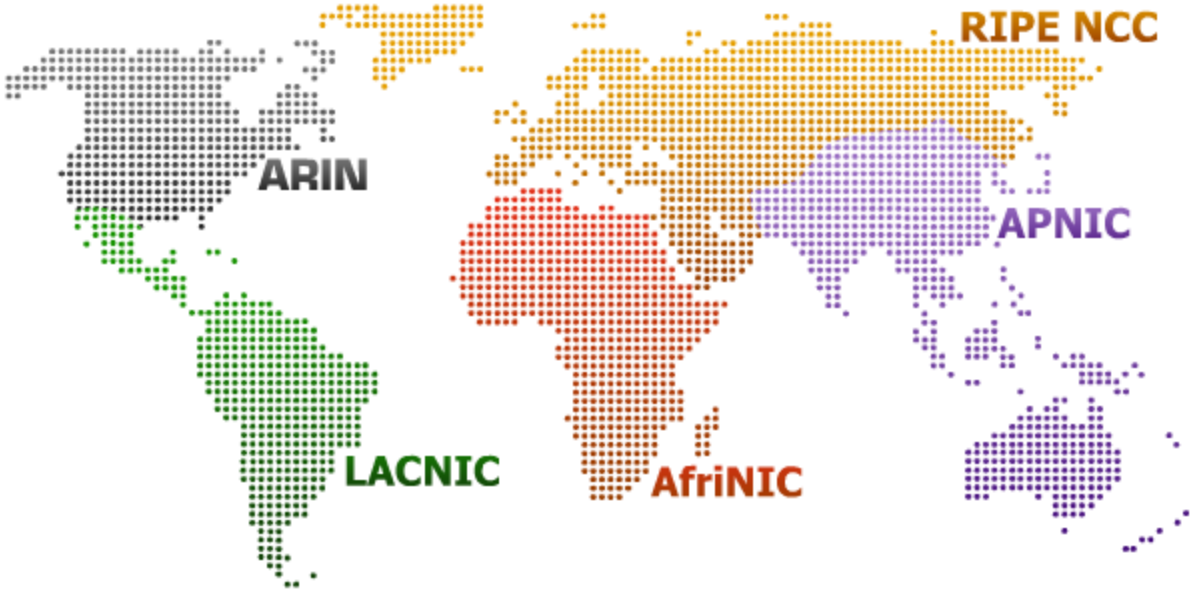
THE ARPA NETWORK

DEC 1969

4 NODES



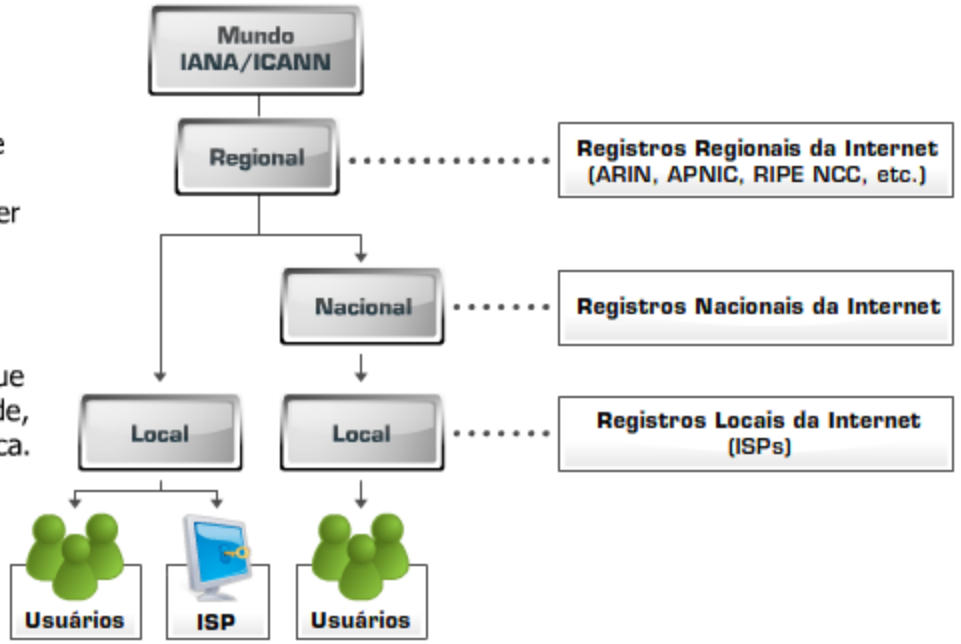
Distribuição do IPV6
Entidades de governança da Internet



Distribuição dos recursos de numeração

Para evitar a utilização de endereços IP duplicados, sua distribuição tem de ser controlada.

Hoje, isso é feito por um conjunto de entidades, que dividem a responsabilidade, numa estrutura hierárquica.



Porque IPV6 ?

- → O IPV4 possui um espaço total de 2^{32} = ~ 4,3 bilhões de endereços IP
- → Grande parte desse espaço já foi distribuida, sendo que menos de 5% encontra-se hoje disponível para novas distribuições
- → Com o esgotamento do IPV4, a consequência natural será um aumento de custos dos serviços de Internet, beneficiando os atuais detentores dos blocos de IPV4.
- → No Brasil, as grandes Teles (com raríssimas excessões) mostram-se bastante apáticas com relação à implantação do IPV6. Fala-se até em implementar NAT em larga escala (LSNAT)

Porque IPV6 ?

Além da absoluta necessidade pelo esgotamento do IPV4, podem ser citados outros motivadores interessantes como:

→ Expansão das redes

→ Qualidade de serviço

→ Mobilidade

→ Internet “das coisas”

Razões históricas para o esgotamento do IPV4

→ Em 1983 a Internet era composta de 100 computadores apenas e a política de distribuição de endereços baseava-se em uma visão não comercial da Internet. A divisão do espaço era feita em “classes”:

Classe	# Bits de rede	# Bits de Hosts	Range Decimal
Class A	8 bits	24 bits	1-126
Class B	16 bits	16 bits	128-191
Class C	24 bits	8 bits	192-223

→ 126 redes “Classe A” que podiam ter até 16,777,214 hosts cada.

→ 16,384 redes “Classe B” que podiam ter até 65,534 hosts cada

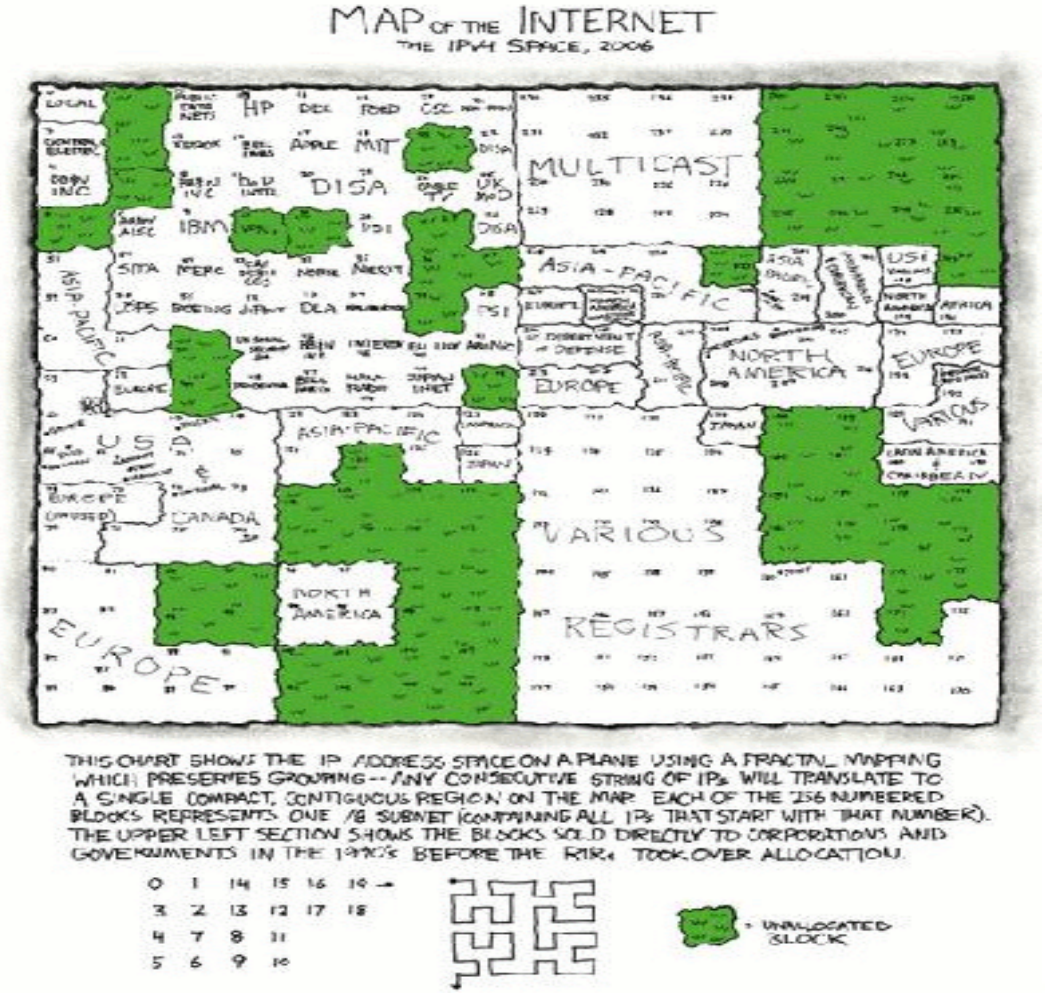
→ 2 milhões de redes “Classe C” que podiam ter até 254 hosts cada.

Razões históricas para o esgotamento do IPV4

→ Divisão do espaço IPV4 em 2006 (disponível no site da IANA)

→ Corporações como a HP, GE, DEC, MIT, DISA, Apple, AT&T, IBM, USPS, receberam seus /8

→ Hoje, mais de 50% do espaço disponível está alocado para os EUA.



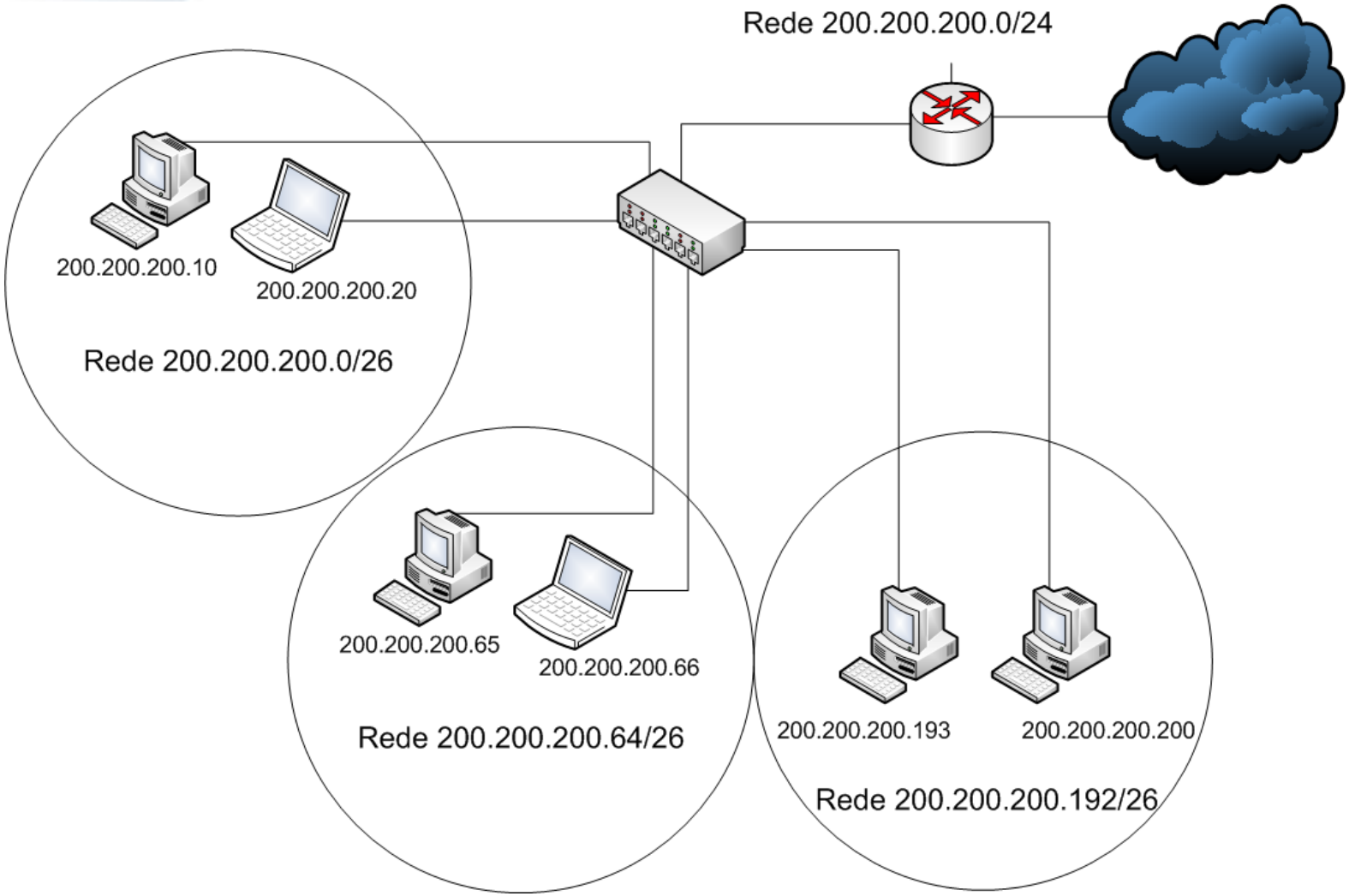
Correndo atrás do prejuízo !

Com as previsões de abertura comercial da Internet, já em 1990 começaram os estudos para evitar o esgotamento dos recursos de numeração, pois mantendo o corrente esquema ainda na década de 90 o IPV4 estaria esgotado.

Algumas técnicas foram utilizadas:

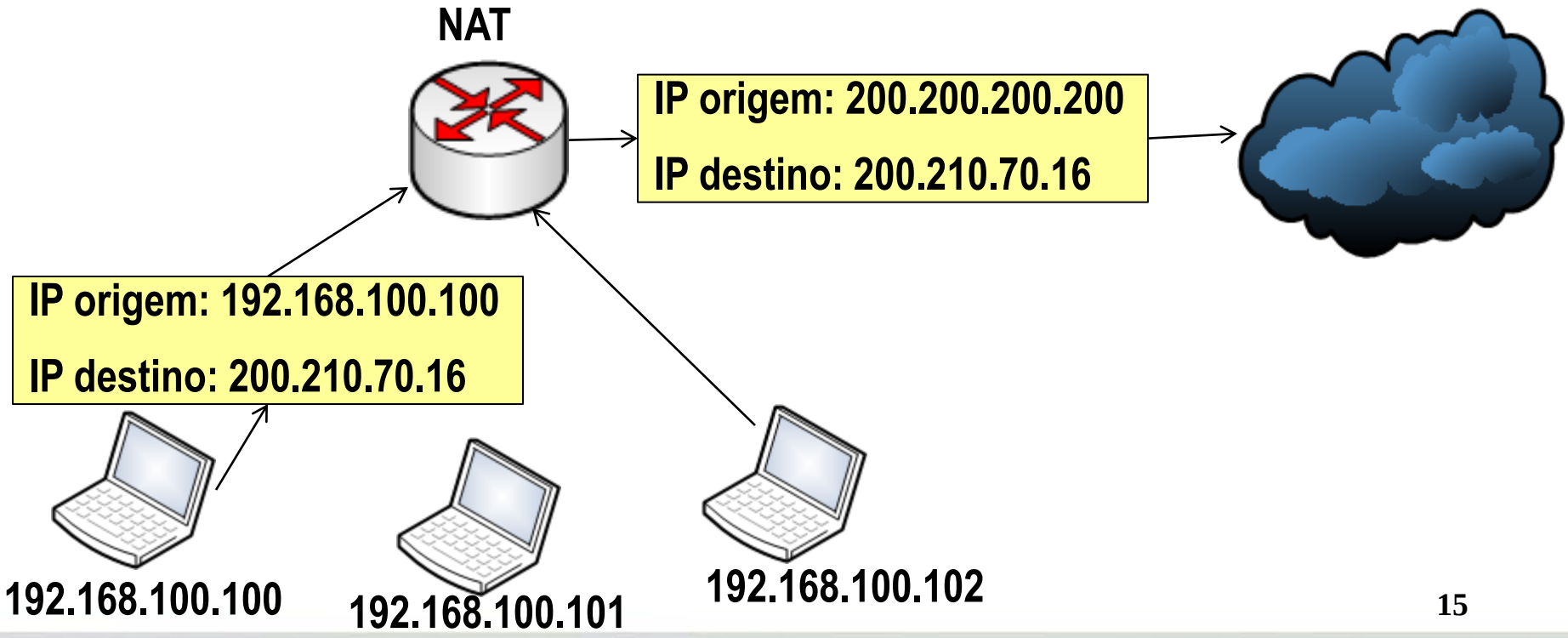
- → Final do esquema de Classes com a adoção do CIDR (Classless Inter Domain Routing) – RFC 4632
- → DHCP (Dynamic Host Configuration Protocol) – RFC 2131
- → NAT (Network Address Translation) – RFC 3022 + Endereços Privados – RFC 1918

Uso do CIDR


Rede 200.200.200.0/24
200.200.200.10
200.200.200.20
Rede 200.200.200.0/26
200.200.200.65
200.200.200.66
Rede 200.200.200.64/26
200.200.200.193
200.200.200.200
Rede 200.200.200.192/26

Uso do NAT

Exemplo: Um computador da rede interna 192.168.100.100 acessando www.mikrotikbrasil.com.br (200.210.70.16) através do roteador que tem IP público 200.200.200.200.



Princípios básicos do IPV6

IPV6

As medidas paliativas como NAT, DHCP e CIDR proporcionaram uma sobrevida do IPV4 até os dias de hoje, tempo no qual foram discutidas várias propostas de soluções.

Finalmente em 1988 a RFC 2460 definiu o IPV6:

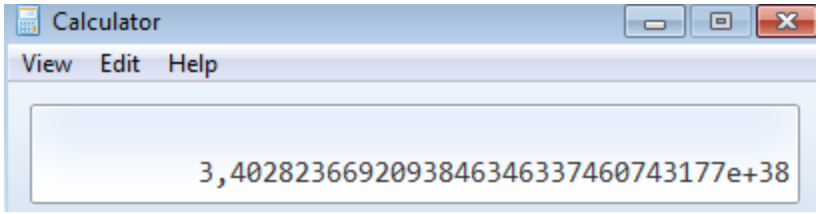
- → 128 bits para endereçamento
- → Cabeçalho base simplificado
- → Cabeçalhos de extensão
- → Identificação do fluxo de dados (QoS)
- → Mecanismos de IPSec incorporados ao protocolo
- → Realiza a fragmentação e remontagem dos pacotes somente na origem e destino
- → Não requer NAT – todas conexões são fim-a-fim
- → Mecanismos que facilitam a configuração de redes

Espaço de endereçamento no IPV6

IPV4

2^{32} = 2,3 milhões de endereços

IPV6



2^{128} = 56 octilhões de endereços por ser humano na terra !

Principais mudanças em relação ao IPV4

1) Quantidade de endereços:
Arquitetura fim a fim sem NAT facilitando a rastreabilidade da rede e aplicações como antes impossibilitadas.

2) Modificação do cabeçalho:
Cabeçalho mais simples e eficiente com 40 bytes fixos e previsão de cabeçalhos de extensão.

3) Segurança com IPSec:
Com o suporte a IPSec mandatório, administradores poderão assegurar a autenticidade, privacidade e integridade de dados de suas redes.

Principais mudanças em relação ao IPV4

4) Mecanismos de QoS:
Identificação do fluxo de dados no cabeçalho permitirá implementação mais eficaz de políticas de QoS.

5) ICMP modificado:
Mais eficaz, permitindo a autoconfiguração, descoberta de vizinhança e gerenciamento eficaz de grupos multicast.

6) Fragmentação feita somente na origem:
Mais agilidade e menor carga no processamento dos pacotes nos roteadores intermediários.

7) Mobilidade:
Suporte à mobilidade integrado ao protocolo irá facilitar aplicações de roaming e nomádicas.

Representação do IPV6

IPV4 (4 x 8 bits)
11000000 10101000 000000001 000000001
192 168 1 1

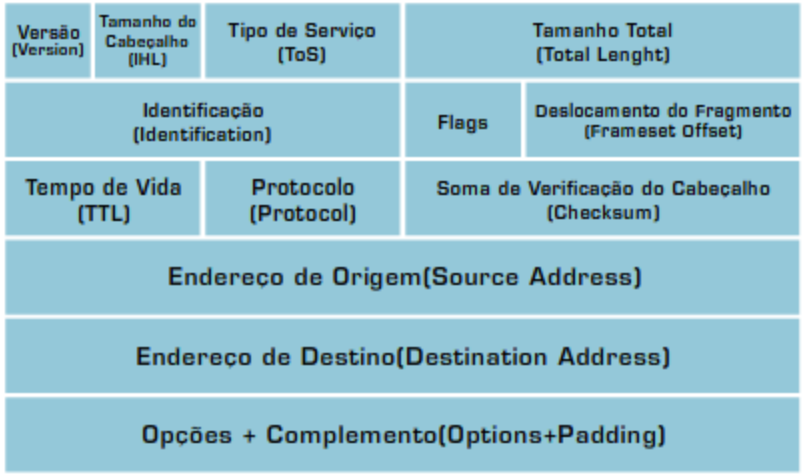
IPV6 (8 x 16 bits)
0010000000000001 0000010001110000 0001111100001001 0000000100110001
0000000000000000 0000000000000000 0000000000000000 0000000000001001

2001:**0**470:1f09:0131:**0000:0000:0000:000**9

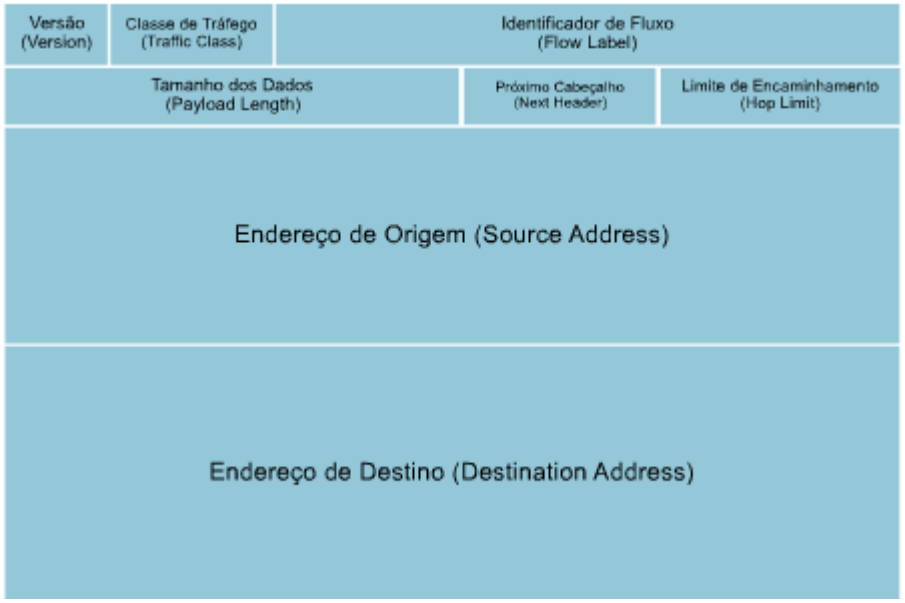
2001:470:1f09:131:**0:0:0**:9

2001:470:1f09:131**::**9

Cabeçalhos IPV4 / IPV6



12 campos fixos podendo ou não conter dados. Tamanho pode variar de 20 a 60 bytes.



Tamaho fixo de 40 bytes podendo ter cabeçalhos de extensão

Endereçamento no IPV6

Unicast (um para um)
Identifica uma única interface de forma que um pacote enviado a um endereço unicast é entregue a uma única interface

Anycast (um para um-de-muitos)
Identifica um conjunto de interfaces. Um pacote encaminhado a um endereço unicast é entregue à interface pertencente a esse conjunto mais próxima da origem (da perspectiva dos protocolos de roteamento)

Multicast (um para muitos)
Tambem refere-se a um conjunto de interfaces mas no entanto um pacote enviado a um endereço multicast é entregue a todas as interfaces associadas a esse endereço.

Tipos de endereços

→ Endereços de Link-local (fe80::/64)

Endereços auto configuráveis, utilizados para comunicação entre interfaces no mesmo enlace, não roteáveis for a do enlace.

→ Unicast Global:

Equivalentes aos IP's públicos do IPV4

→ Aplicações especiais

- → Não especificado ::/128 – equivalente a 0.0.0.0 do IPV4
- → loopback ::1/128) – equivalente ao 127.0.0.1
- → Túneis 6to4 – 2002::/16

etc.

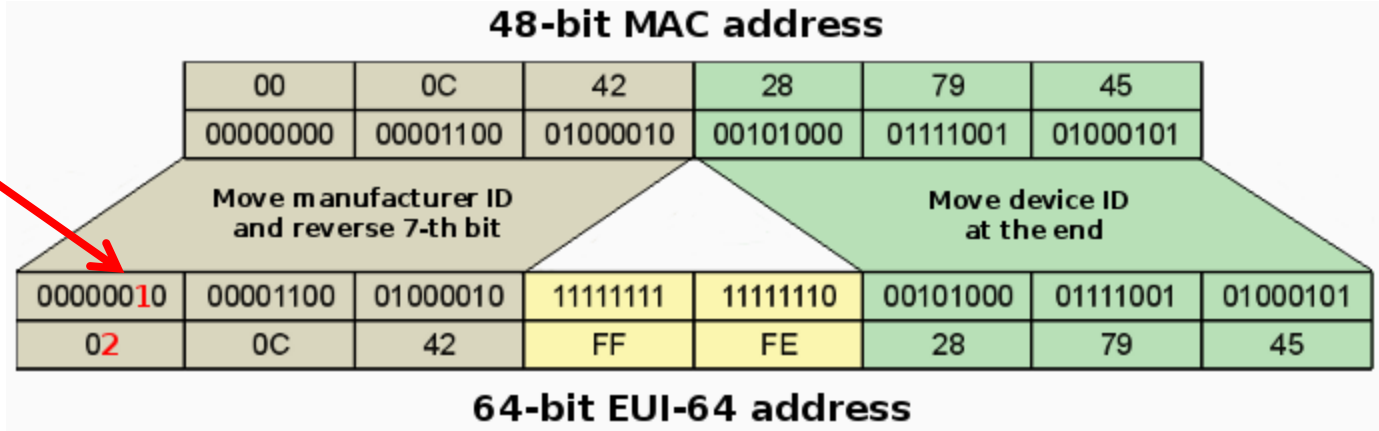
Autoconfiguração

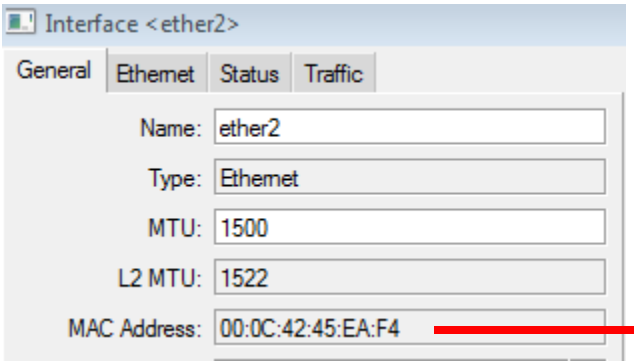
O IPV6 possui um mecanismo de autoconfiguração dos nós que pode funcionar das seguintes formas:

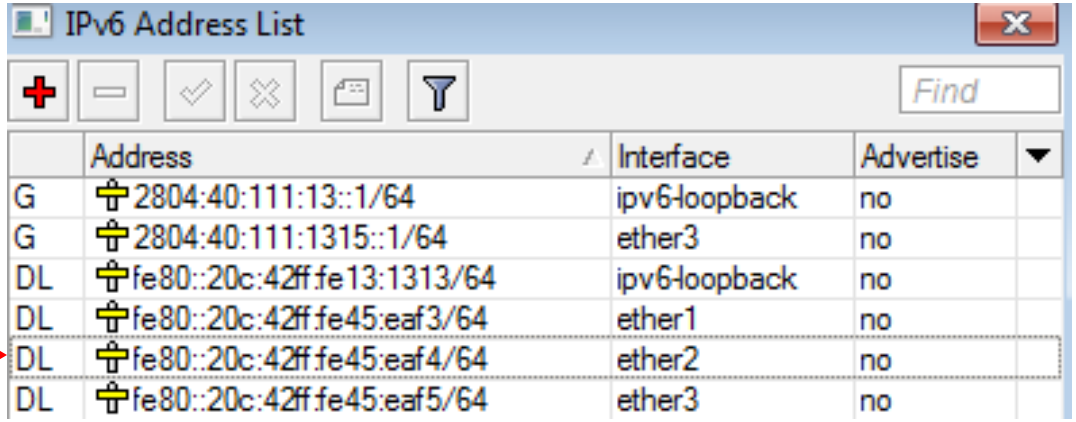
→ Configuração Stateless
Os nós se autoconfiguram utilizando o protocolo de descoberta de vizinhança (Neighbor Discovery – ND) baseado no ICMPv6

→ Configuração Statefull
É necessária a existencia de um servidor de DHCPv6 para a configuração dos nós.

Formação de endereços locais



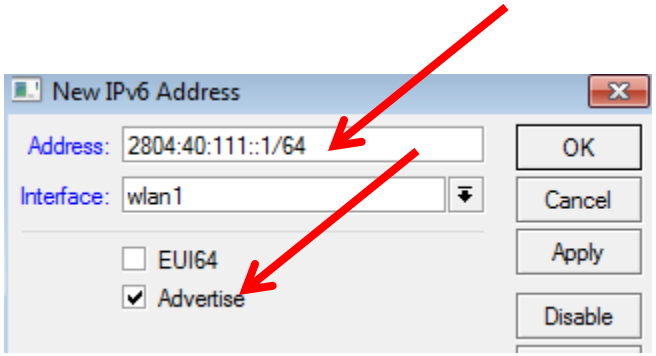




00:0C:42:45:EA:F4 → FE80::20C:42**FF:FE**45:EAF4/64

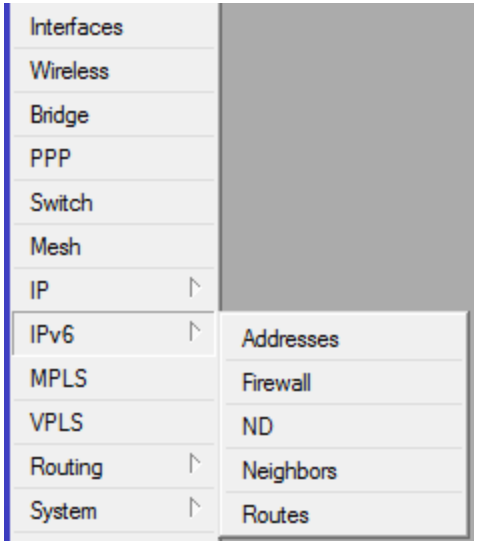
Configuração Stateless utilizando o Mikrotik

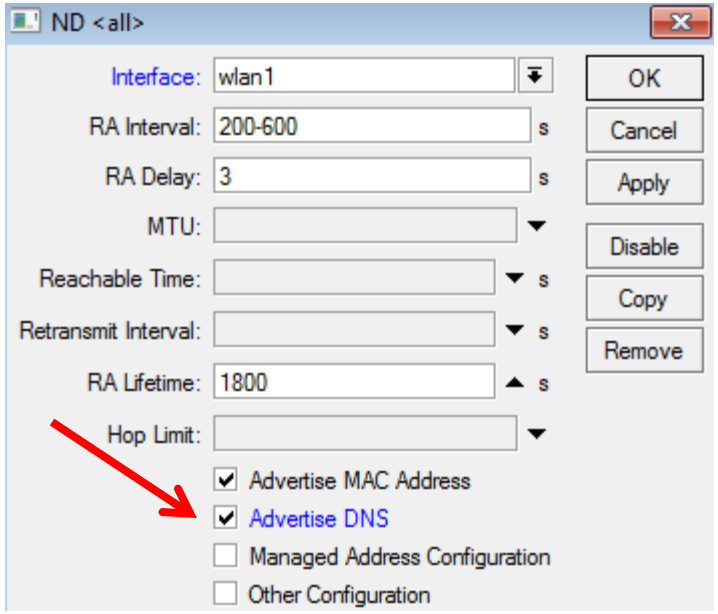
1 – Configurar um endereço IPV6 golbal na Interface onde os clientes estão conectados, mantendo o advertise habilitado



Configuração Stateless utilizando o Mikrotik

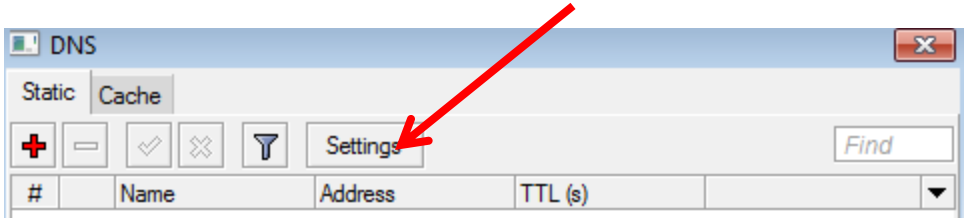
2 – Configurar o Neighbor Discovery na interface dos clientes (ou em all), habilitando o anúncio de DNS

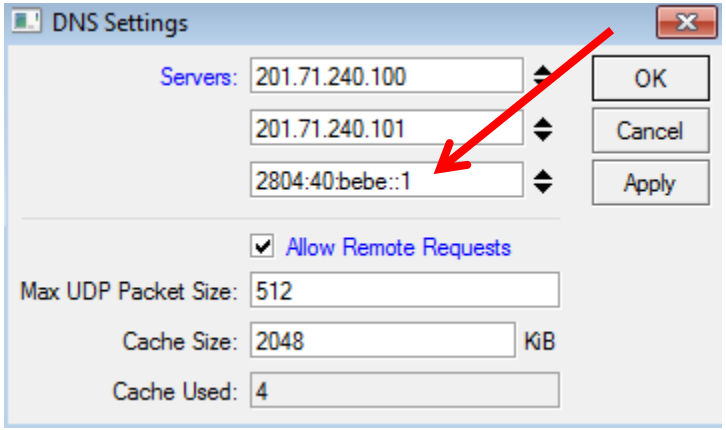




Configuração Stateless utilizando o Mikrotik

3 – Configurar o DNS em /ip dns settings





Fragmentação no IPV6

→ No IPV4

Roteadores fragmentam os pacotes de acordo com a MTU do próximo enlace.

→ No IPV6

Através do protocolo PMTUD (Path MTU discovery), a fragmentação é negociada inicialmente entre a origem e o destino somente

Isso tem o objetivo de diminuir a carga de processamento de roteadores intermediários e melhorar a performance do tráfego

O PMTUD trabalha com base no ICMPv6 que envia mensagens de “packet too big”, sempre que o pacote excede a MTU do próximo salto.

IPV4 → IPV6

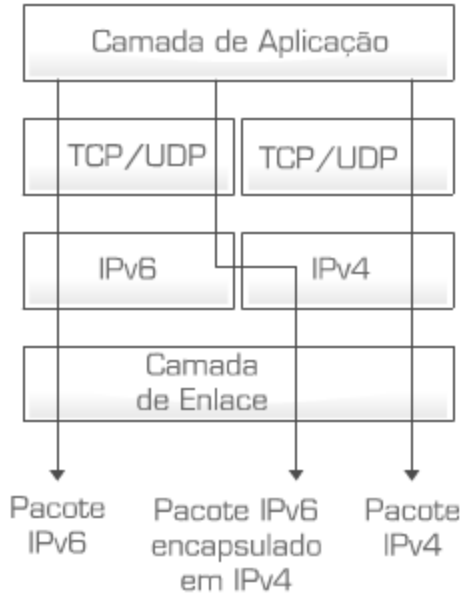
Coexistência e Transição

IPV4 → IPV6

Várias técnicas são utilizadas. Podemos resumi-las em 3 grupos:

- → Pilha Dupla (Dual Stack), quando convivem no mesmo dispositivo e redes, tanto IPV4 como IPV6
- → Técnicas de tunelamento, transportando IPV6 sobre estruturas somente IPV4
- → Técnicas de tradução, permitindo que dispositivos somente IPV6 falem com dispositivos somente IPV4.

IPV4 → IPV6
Transição utilizando pilha dupla

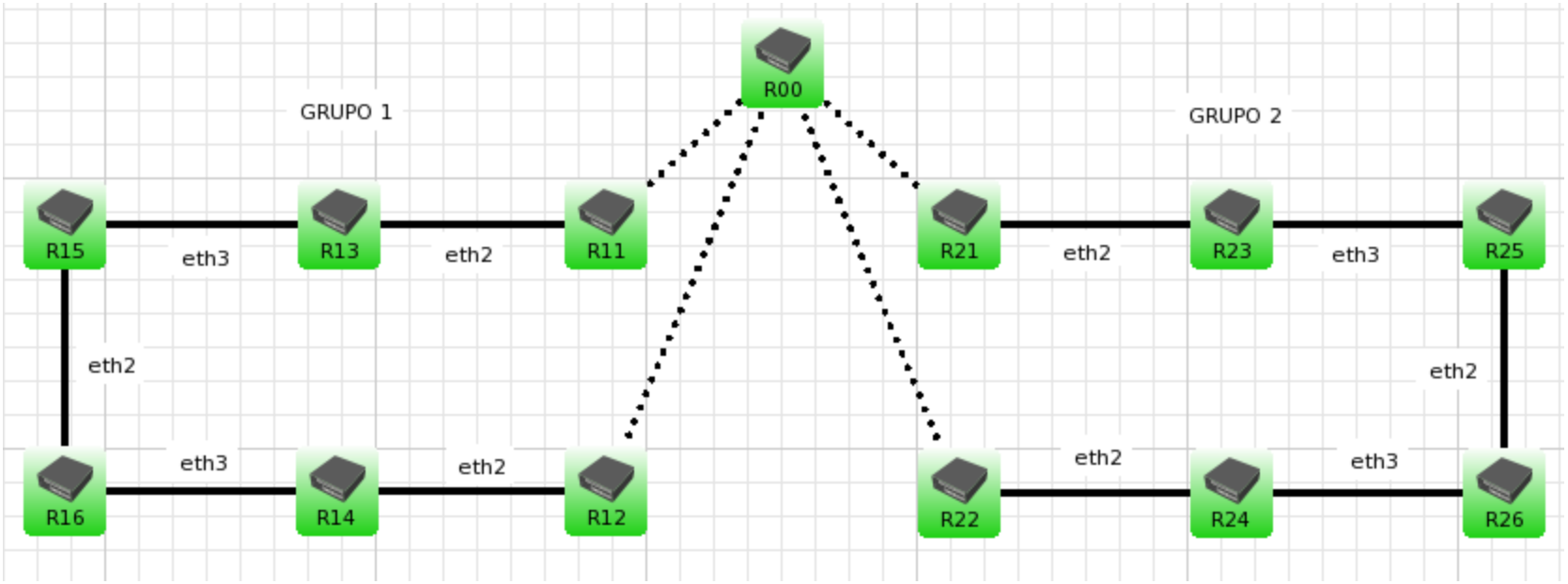


- → Inserir o suporte a IPV6 paulatinamente sem descontinuar a estrutura IPV4
- → As aplicações precisam escolher o protocolo em que irão trabalhar. Exemplo, o DNS quando quando tem um record AAAA e A, responde de acordo com o pacote que iniciou a consulta.

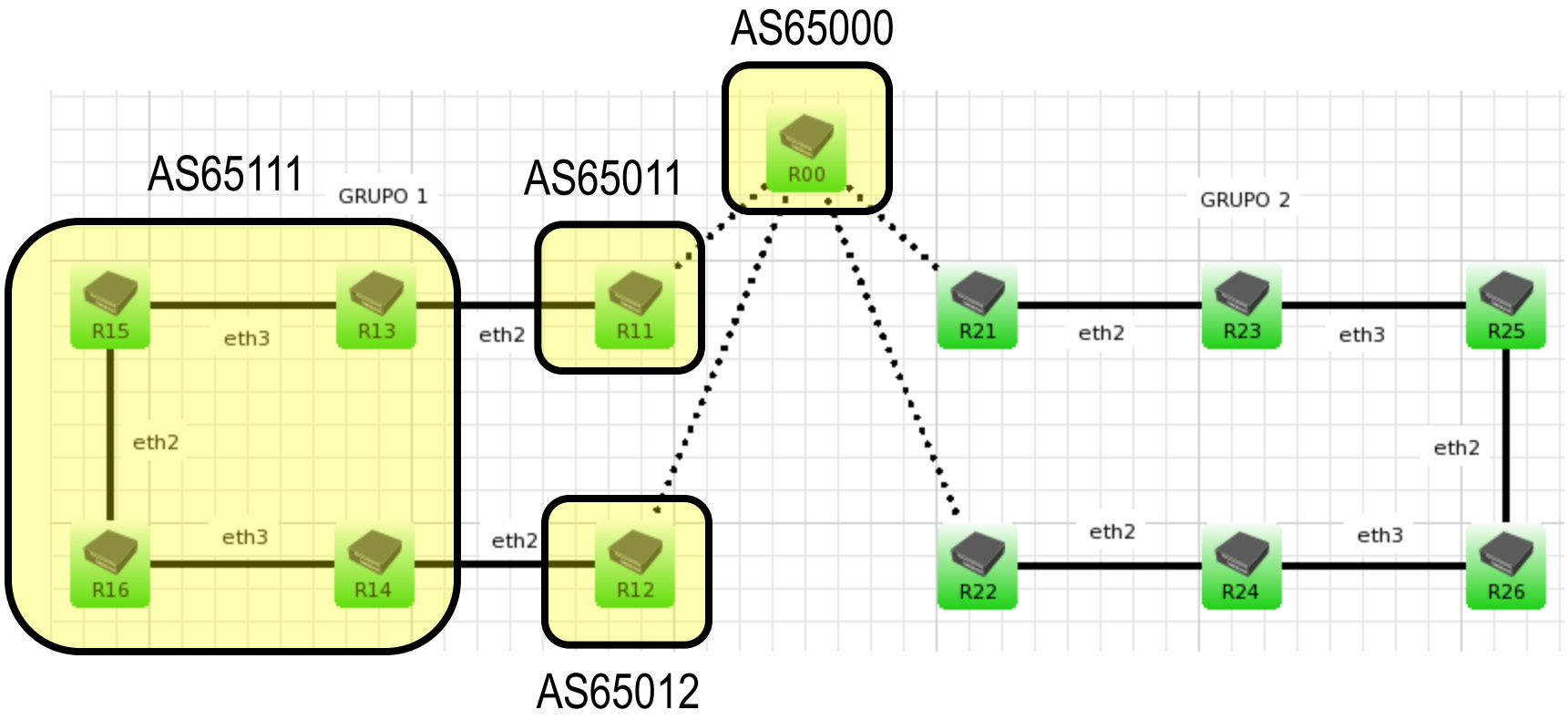
Endereçamento e Roteamento no IPV6

Endereçamento e roteamento no IPV6

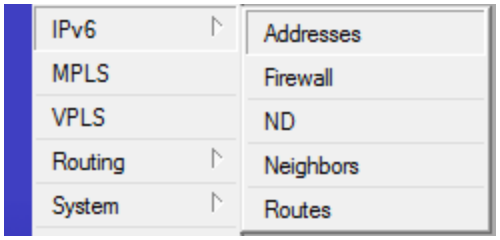
Q

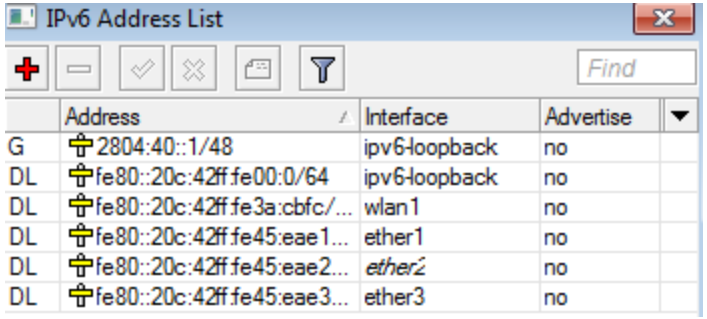


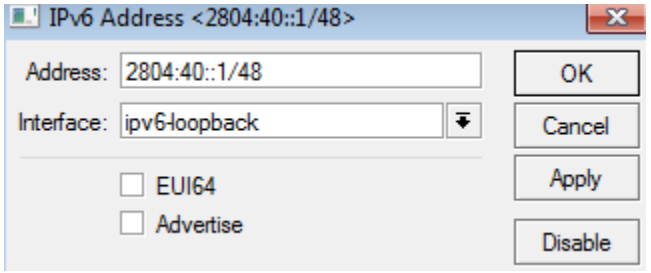
Endereçamento e roteamento no IPV6

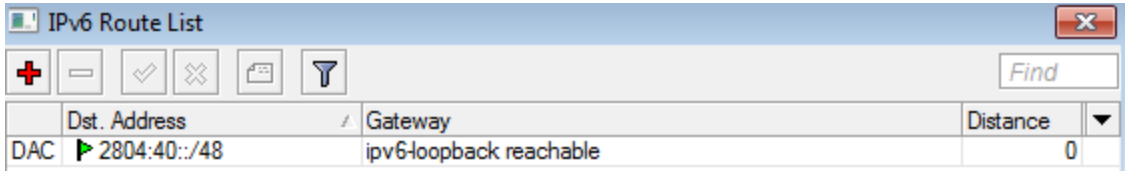


Endereçamento e Roteamento estático



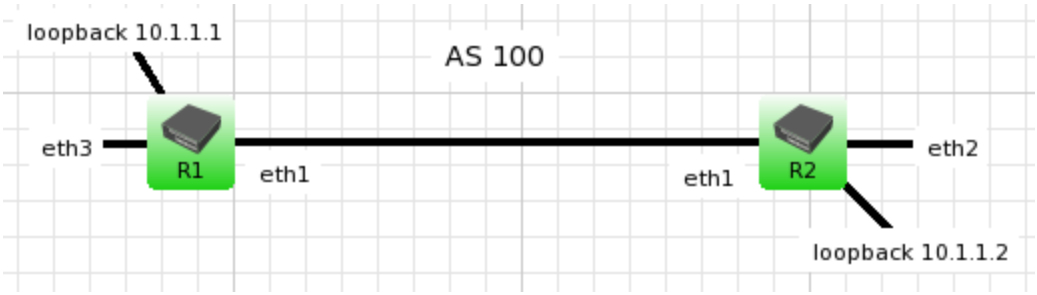


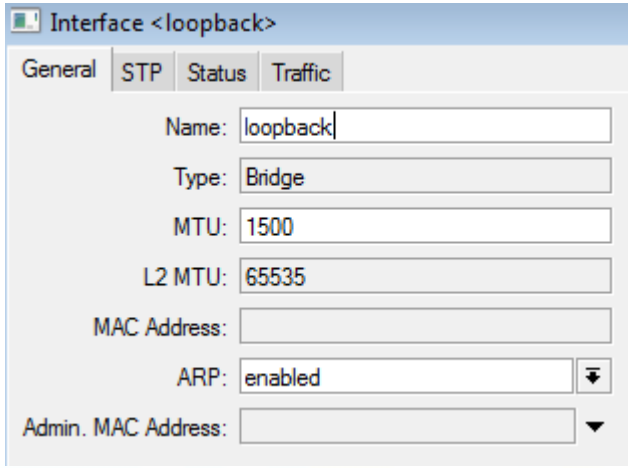


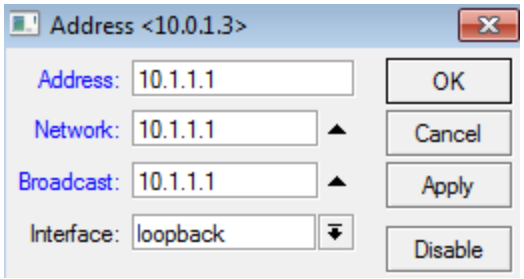


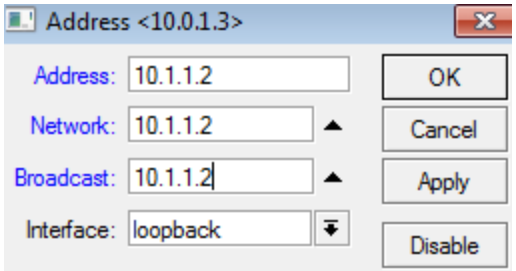
Configuração de Endereços de Loopback no IPV4

Endereços de Loopback eliminam a dependencia da interface física para efetuar a conexão TCP. Utilizada com frequência em roteamento dinâmico.



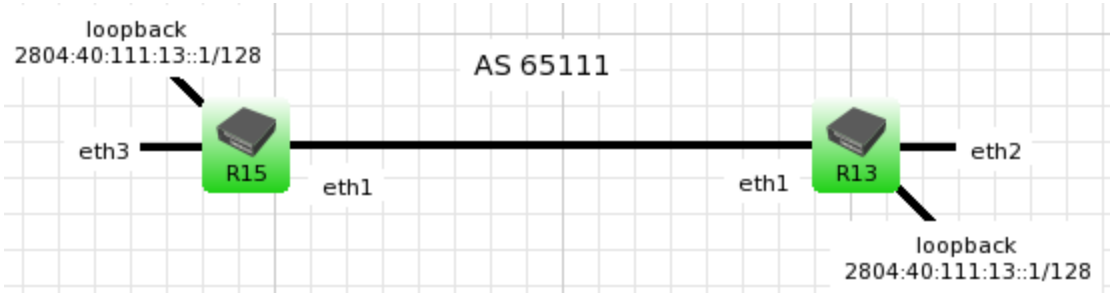


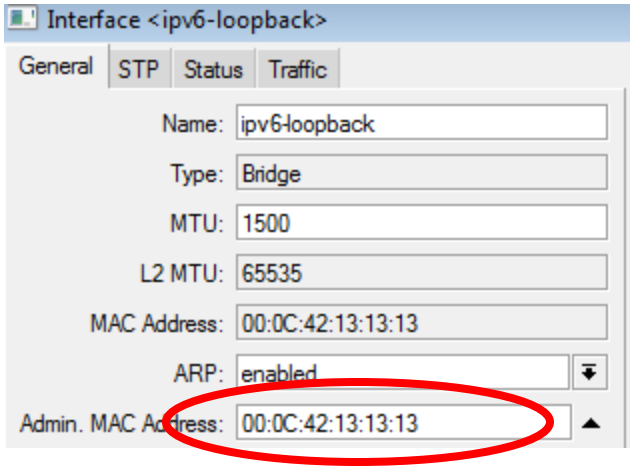


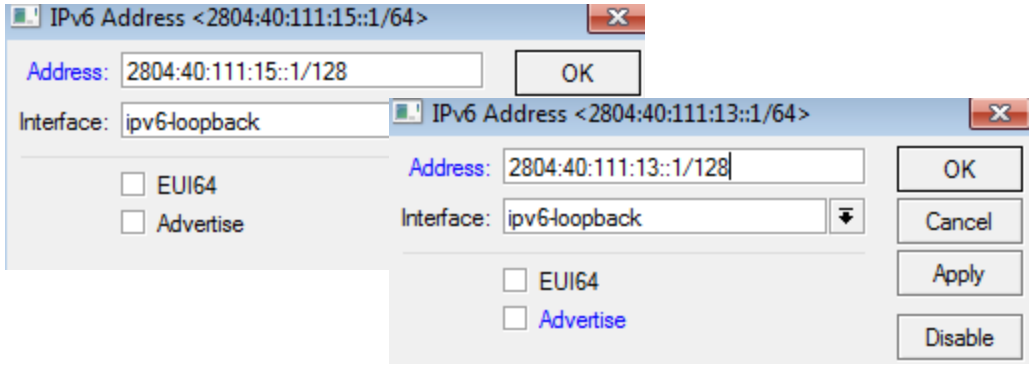


Configuração de Endereços de Loopback no IPV6

No IPV6 os endereços são formados a partir dos MAC addresses. Como a Bridge não tem um, o método anterior falhará. Solução – usar Admin MAC

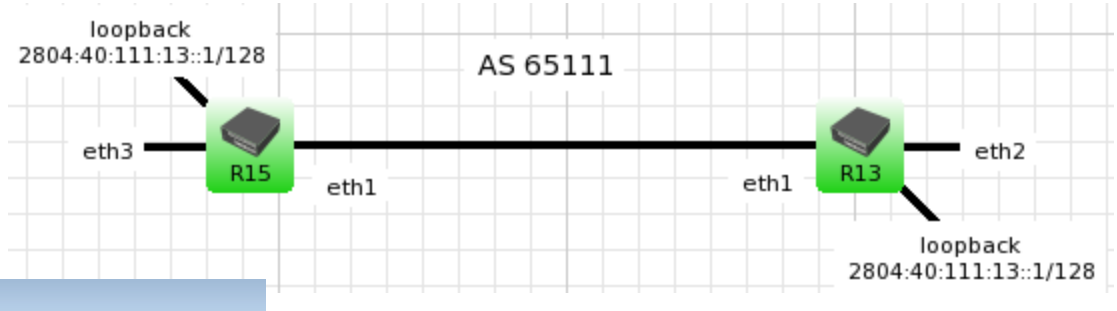


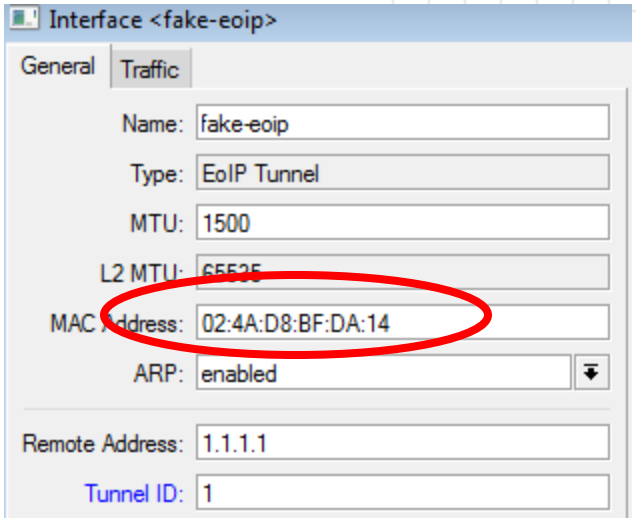


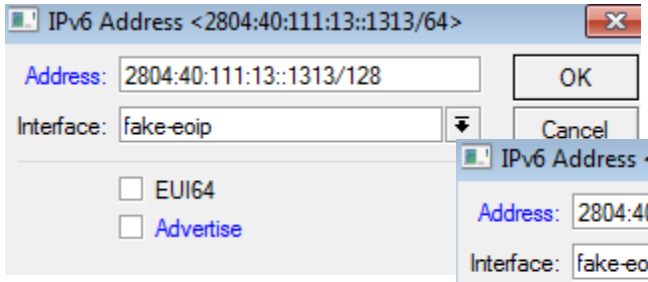


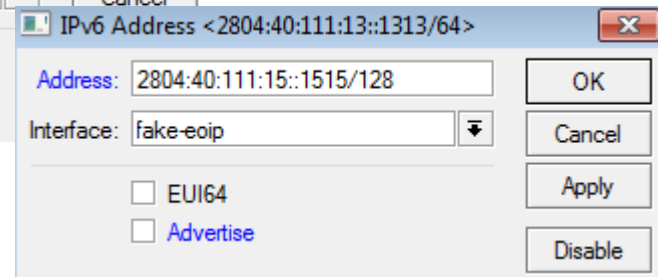
Configuração de Endereços de Loopback no IPV6

Como solução alternativa pode-se criar um túnel EoIP falso que cria uma interface com um MAC automático.

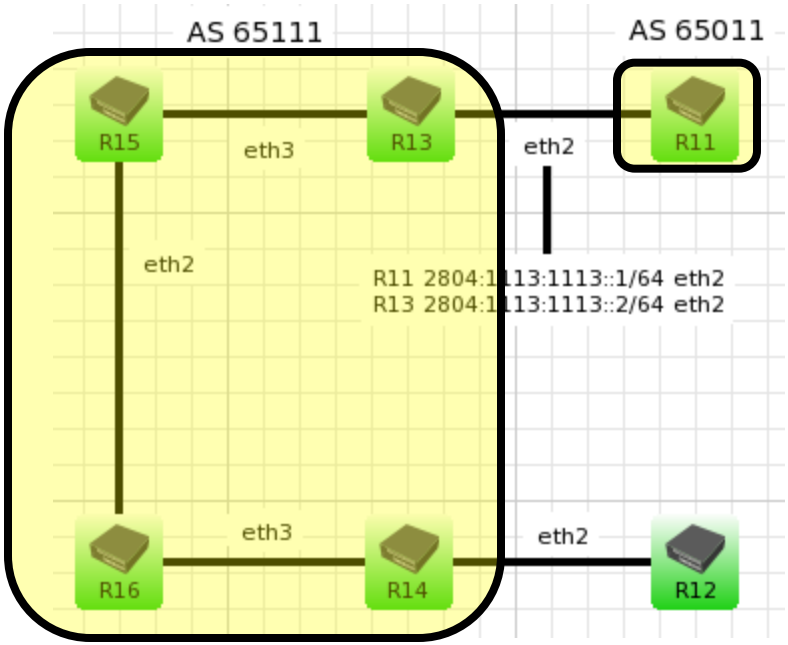




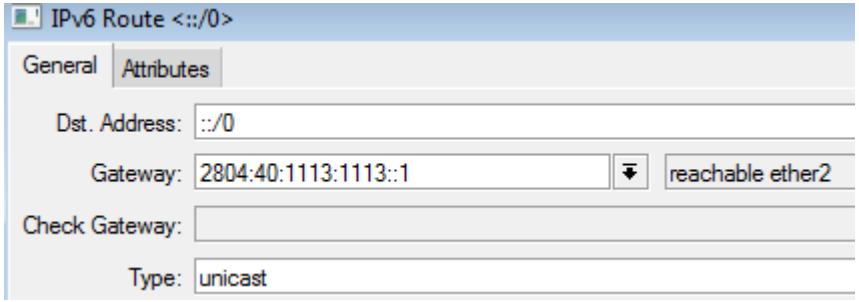




Endereçamento e roteamento no IPV6
Rota default

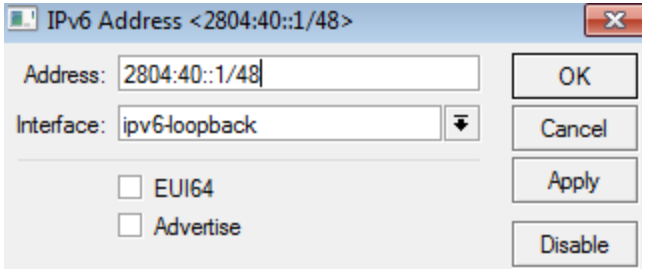


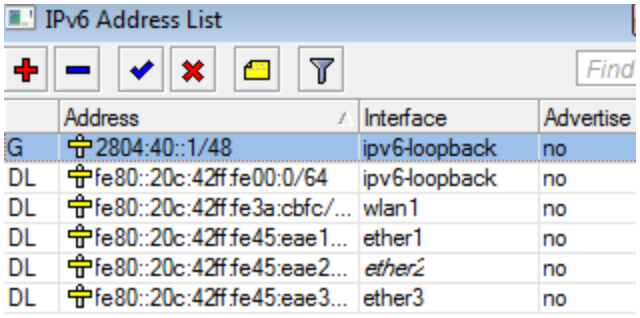
Rota default de 13 para 11



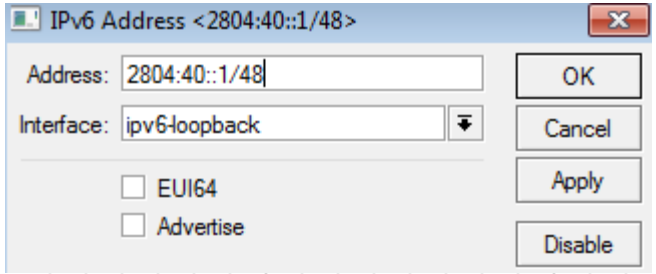
Endereçamento e roteamento no IPV6

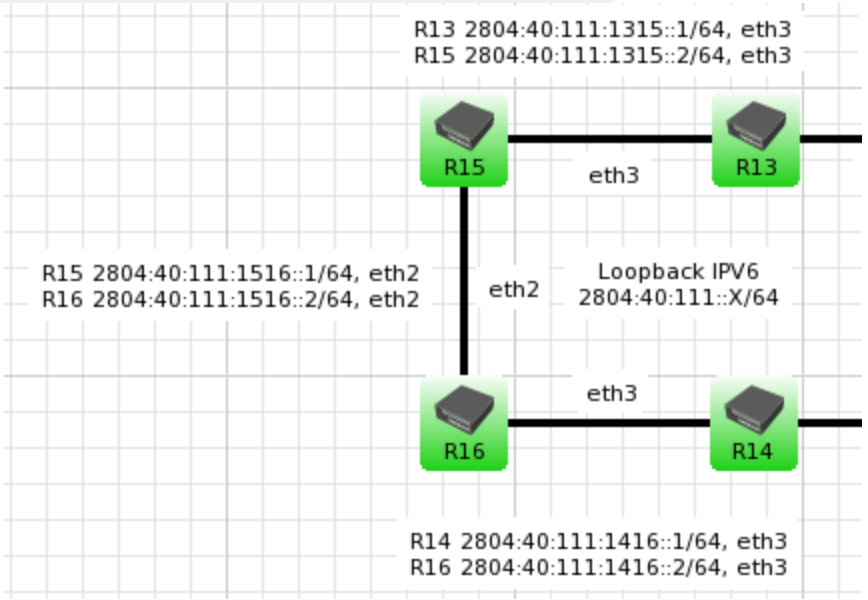
Configurações em R00





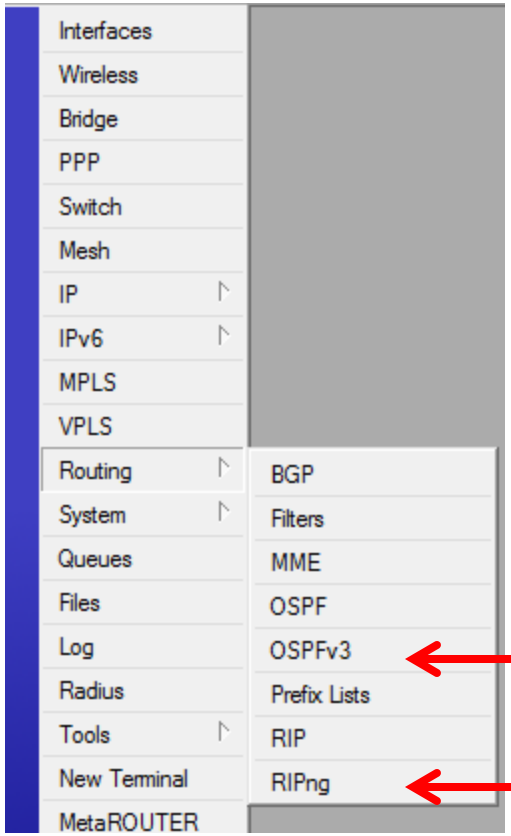
Configurações em R11





Roteamento dinâmico no IPV6

Roteamento dinâmico no IPV6
IGP

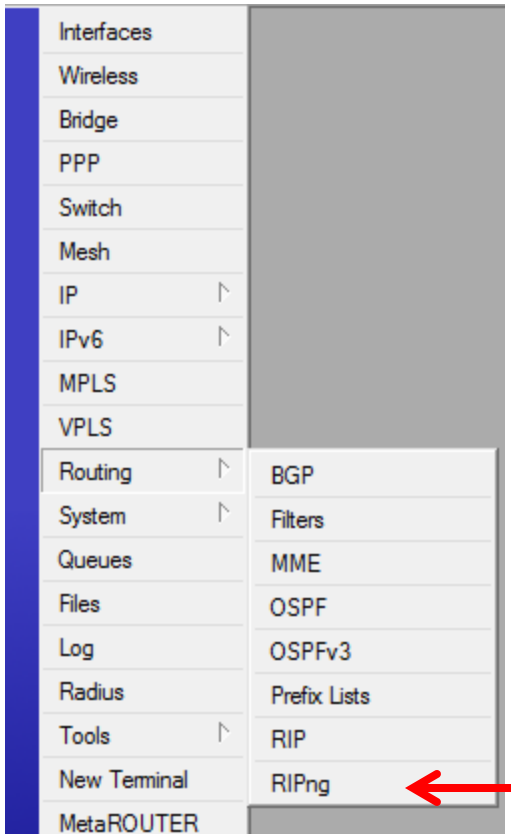


O Mikrotik suporta dois protocolos de roteamento interno:

→ RIP “New Generation” (RIPng)

→ OSPFv3

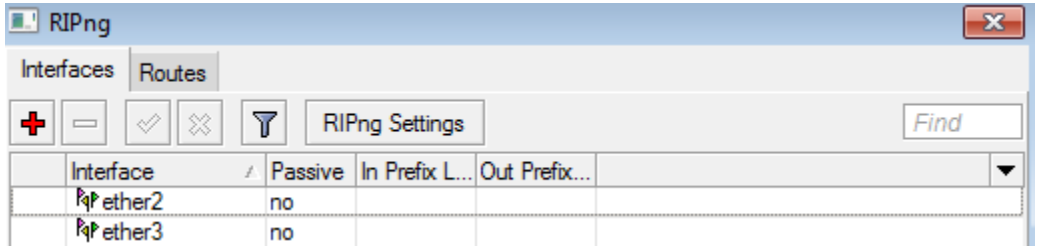
Roteamento dinâmico no IPV6
RIPng



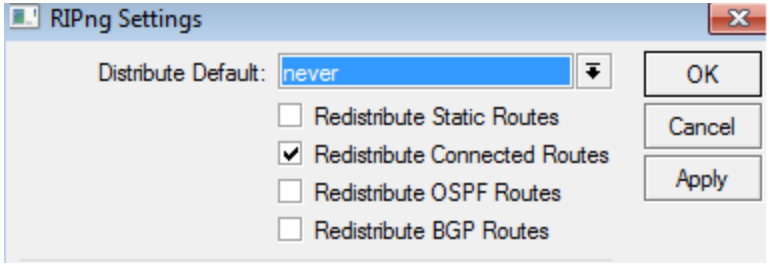
- → Baseado no RIPv2 e RFC 2080
- → Utiliza o algorítimo de Bellman-Ford, sendo um protocolo do tipo “distance vector”.
- → Limitado a 15 saltos
- → Utiliza o grupo de Multicast ff02::9 (todos Roteadores RIP) como destino para as mensagens de update.

Roteamento dinâmico no IPV6
RIPng

→ Configura-se selecionando as interfaces em que o RIPng irá rodar

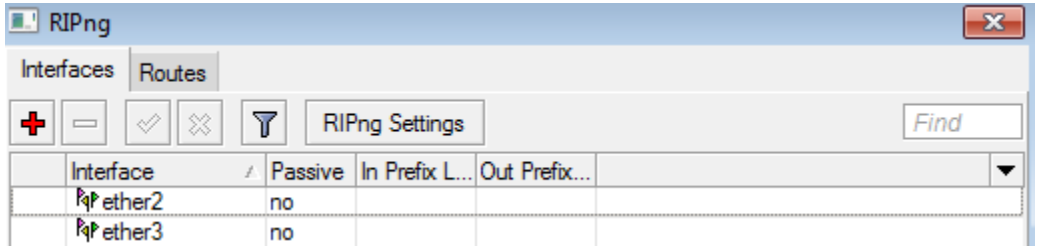


→ Redes não podem ser arbitradas para as publicações, podendo no entanto serem publicadas rotas conectadas e estáticas

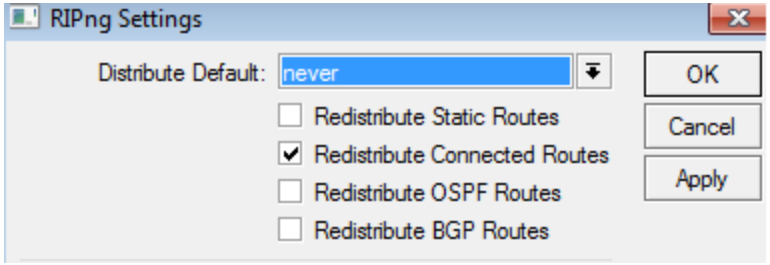


Roteamento dinâmico no IPV6
RIPng

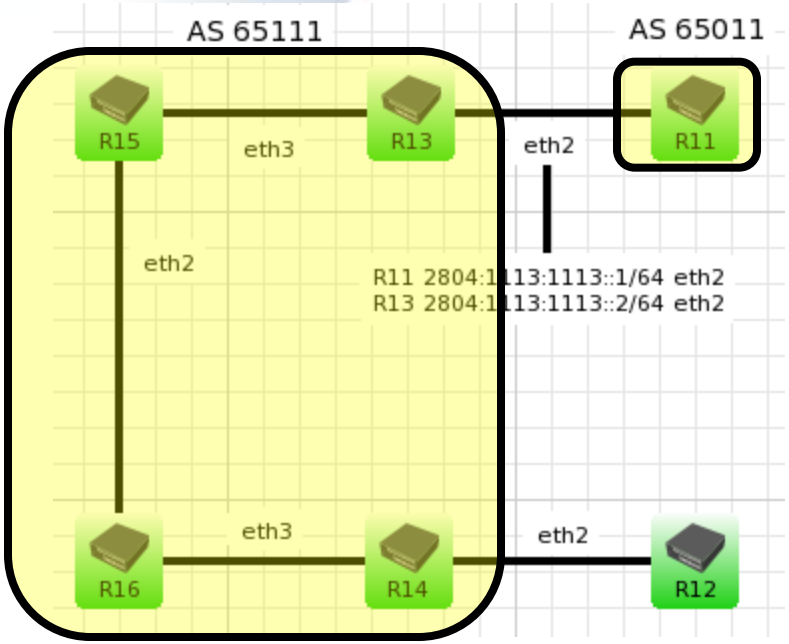
→ Configura-se selecionando as interfaces em que o RIPng irá rodar



→ Redes não podem ser arbitradas para as publicações, podendo no entanto serem publicadas rotas conectadas e estáticas



Roteamento IPV6 com RIPng

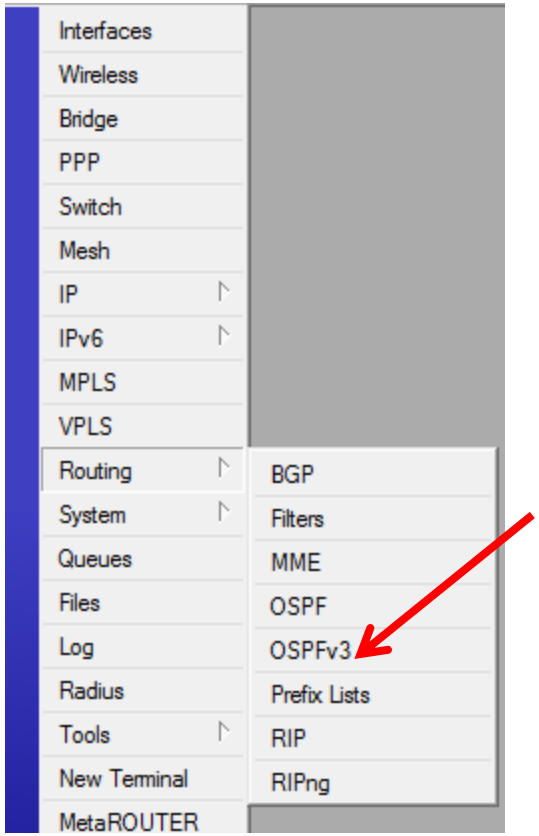


Rotas obtidas em R15

IPv6 Route List

	Dst. Address	Gateway	Distance
DAr	2804:40:111:13::/64	fe80::20c:42ff:fe45:eaf5%ether3 reachable	120
DAr	2804:40:111:14::/64	fe80::20c:42ff:fe0e:d8ee%ether2 reachable	120
DAC	2804:40:111:15::/64	ipv6-loopback reachable	0
DAC	2804:40:111:1315::/64	ether3 reachable	0
DAr	2804:40:111:1416::/64	fe80::20c:42ff:fe0e:d8ee%ether2 reachable	120
DAC	2804:40:111:1516::/64	ether2 reachable	0
DAr	2804:40:1113:1113::/64	fe80::20c:42ff:fe45:eaf5%ether3 reachable	120
DAr	2804:111:16::/64	fe80::20c:42ff:fe0e:d8ee%ether2 reachable	120

Roteamento dinâmico no IPV6
OSPFv3

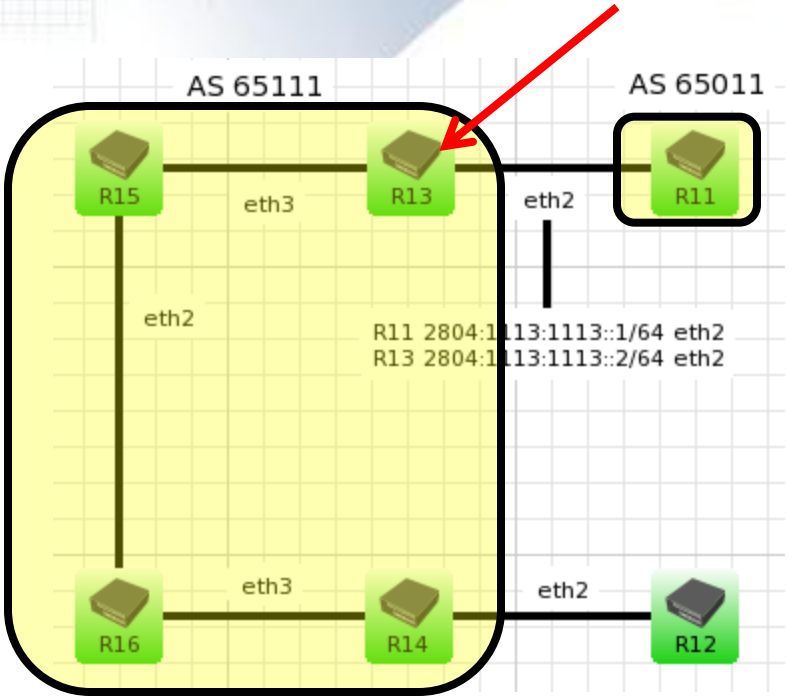


O protocolo OSPF utilizado no IPV4 (V2) precisou de várias modificações para suportar o IPV6, dando origem ao OSPFv3 (RFC 2740)

Os mesmos princípios utilizados no OSPFv2, como LSA's, flooding, utilização do algorítimo de Djkstra, etc foram mantidos. Porém o OSPFv3 possue varias melhorias em relação ao seu sucessor.

A principal diferença de configuração é que no OSPFv3 não há mais configurações de redes e sim de interfaces, que passam a ser mandatórias.

Roteamento dinâmico no IPV6
OSPFv3



Configurações em R13

OSPFv3

Interfaces | Instances | Areas | Area Ranges | Virtual Links | Neighbors | NBMA Neighbors | LSA | Routes | ...

Area	Interface	Cost	Priority	Network Type	Instance	Neig...	State
backbone	ether3	10	1	default	default	1	backup
backbone	ipv6-loopback	10	1	default	default	0	designated router

OSPFv3

Interfaces | Instances | Areas | Area Ranges | Virtual Links | Neighbors | NBMA Neighbors | LSA | Routes | ...

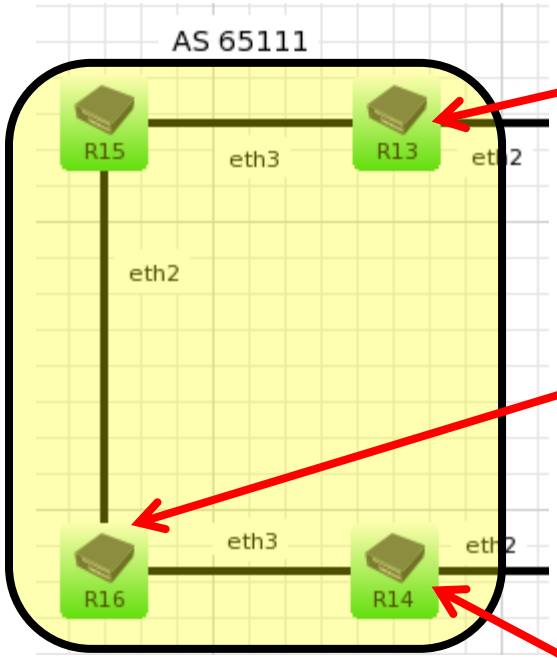
Name	Router ID	Running
default	0.0.0.13	yes

OSPFv3

Instances | Areas | Area Ranges | Virtual Links | Neighbors | NBMA Neighbors | LSA | Routes | AS Border Routers | ...

Instance	Area Name	Area ID	Type	Default C...	Interfac...	Active I...	Neighb...
default	backbone	0.0.0.0	default		2	2	1

Roteamento dinâmico no IPV6 - OSPFv3



IPv6 Route List

OSPF | is | yes | Filter | Find

	Dst. Address	Gateway	Distance
DAo	2804:40:111:15::/64	fe80::20c:42ff:fe45:c128%ether3 reachable	110
DAo	2804:40:111:16::/64	fe80::20c:42ff:fe45:c128%ether3 reachable	110
DAo	2804:40:111:1416::/64	fe80::20c:42ff:fe45:c128%ether3 reachable	110
DAo	2804:40:111:1516::/64	fe80::20c:42ff:fe45:c128%ether3 reachable	110

IPv6 Route List

OSPF | is | yes | Filter | Find

	Dst. Address	Gateway	Distance
DAo	::/0	fe80::20c:42ff:fe45:c127%ether2 reachable	110
DAo	2804:40:111:13::/64	fe80::20c:42ff:fe45:c127%ether2 reachable	110
DAo	2804:40:111:15::/64	fe80::20c:42ff:fe45:c127%ether2 reachable	110
DAo	2804:40:111:1315::/64	fe80::20c:42ff:fe45:c127%ether2 reachable	110

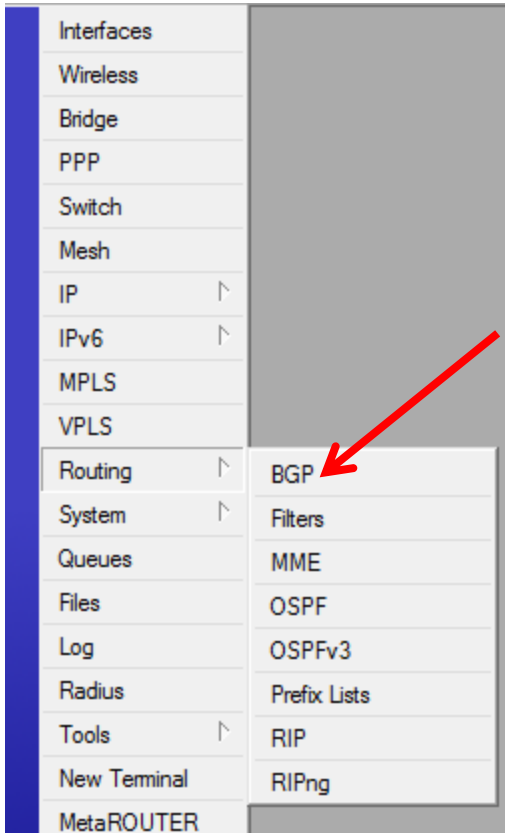
IPv6 Route List

OSPF | is | yes | Filter | Find

	Dst. Address	Gateway	Distance
DAo	::/0	fe80::20c:42ff:fe0e:d8ef%ether3 reachable	110
DAo	2804:40:111:13::/64	fe80::20c:42ff:fe0e:d8ef%ether3 reachable	110
DAo	2804:40:111:15::/64	fe80::20c:42ff:fe0e:d8ef%ether3 reachable	110
DAo	2804:40:111:16::/64	fe80::20c:42ff:fe0e:d8ef%ether3 reachable	110
DAo	2804:40:111:1315::/64	fe80::20c:42ff:fe0e:d8ef%ether3 reachable	110
DAo	2804:40:111:1516::/64	fe80::20c:42ff:fe0e:d8ef%ether3 reachable	110

Rotas OSPF resultantes

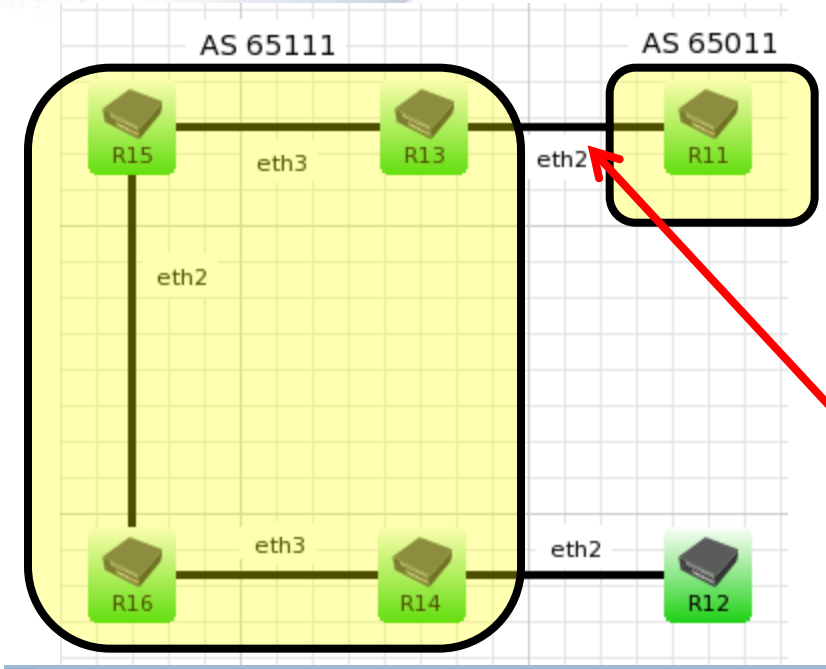
Roteamento externo no IPV6
BGP



O protocolo BGP permite a propagação de múltiplas famílias de endereços (adress families) e não houve a necessidade do desenvolvimento de um novo protocolo de roteamento externo.

Para ativar a propagação de prefixos IPV6 sobre um peer IPV4, basta que a implementação do BGP tenha suporte a multiprotocolos, no caso IPV6, e habilitar o mesmo no peer.

Roteamento externo no IPV6
BGP



BGP

Instances | VRFs | Peers | Networks | Aggregates | VPN4 Routes | Advertisements

Name	AS	Router ID	Out Filter	Confeder...	Confeder..
default	65011	10.0.1.1			

BGP

Instances | VRFs | Peers | Networks | Aggregates | VPN4 Routes | Advertisements

Refresh | Refresh All | Resend | Reser

Name	Insta...	Remote Address	Remote ...	Remote ID	State
peer11-00	default	172.16.0.254	65000	10.0.0.0	established
peer11-13	default	192.168.1.2	65111	10.0.1.3	established

BGP

Instances | VRFs | Peers | Networks | Aggregates | VPN4 Routes | Advertisements

Peer	Prefix	Nexthop	AS Path	Origin
peer11-00	10.1.0.0/16	172.16.0.11	65111	igp
peer11-00	10.11.11.0/24	172.16.0.11		igp
peer11-13	10.22.22.0/24	192.168.1.1	65000,65022	igp
peer11-13	10.12.12.0/24	192.168.1.1	65000,65012	igp
peer11-13	10.2.0.0/16	192.168.1.1	65000,65021,...	igp
peer11-13	10.21.21.0/24	192.168.1.1	65000,65021	igp
peer11-13	10.100.100.0...	192.168.1.1	65000	igp
peer11-13	2804:40:11::/...	2804:40:1113...		igp
peer11-13	10.11.11.0/24	192.168.1.1		igp

BGP Peer <peer11-13>

General | Advanced | Status

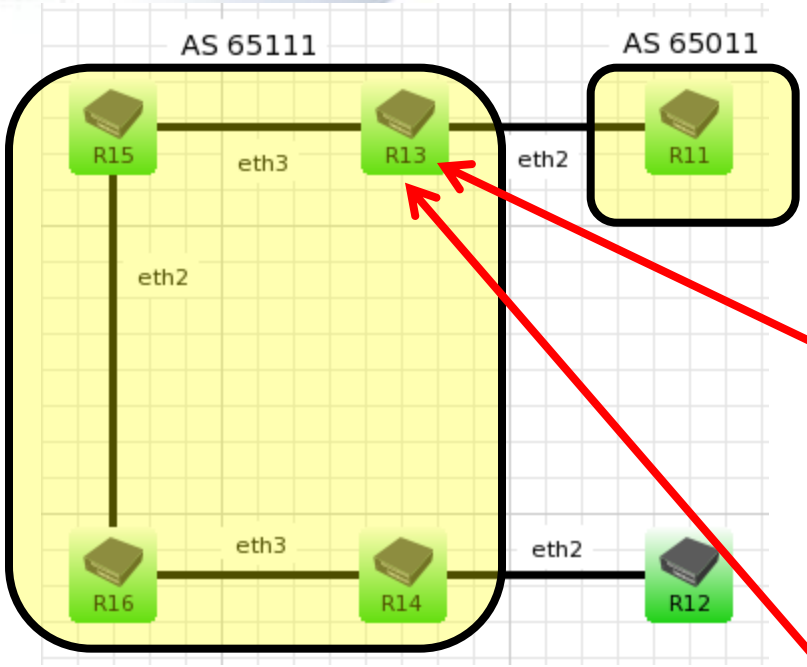
Address Families: ☑ ip ☑ ipv6 ☐ l2vpn ☐ vpn4 ☐ l2vpn-cisco

BGP

Instances | VRFs | Peers | Networks | Aggregates | VPN4 Routes | Advertisements

Network	Synchroni...
10.11.11.0/24	no
2804:40:11::/48	no

Roteamento externo no IPV6 BGP



Route List

Routes | Nexthops | Rules | VRF

BGP | is | yes

	Dst. Address	Gateway	Distance
DAb	10.1.0.0/16	10.0.1.4 recursive via 192.168.1.6 ether3	200
DAb	10.2.0.0/16	192.168.1.1 reachable ether2	20
Db	10.2.0.0/16	10.0.1.4 recursive via 192.168.1.6 ether3	200
DAb	10.11.11.0/24	192.168.1.1 reachable ether2	20
Db	10.12.12.0/24	192.168.1.1 reachable ether2	20
DAb	10.12.12.0/24	10.0.1.4 recursive via 192.168.1.6 ether3	200
DAb	10.21.21.0/24	192.168.1.1 reachable ether2	20
Db	10.21.21.0/24	10.0.1.4 recursive via 192.168.1.6 ether3	200
DAb	10.22.22.0/24	192.168.1.1 reachable ether2	20
Db	10.22.22.0/24	10.0.1.4 recursive via 192.168.1.6 ether3	200
DAb	10.100.100.0/...	192.168.1.1 reachable ether2	20
Db	10.100.100.0/...	10.0.1.4 recursive via 192.168.1.6 ether3	200

IPv6 Route List

Find

	Dst. Address	Gateway	Distance
AS	::/0	2804:40:1113:1113::1 reachable ether2	1
DAb	2804:40:11::/48	fe80::20c:42ff:fe47:2aa%ether2 reachable	20
DAC	2804:40:111:13::/64	ipv6-loopback reachable	0
DAo	2804:40:111:15::/64	fe80::20c:42ff:fe45:c128%ether3 reachable	110
DAo	2804:40:111:16::/64	fe80::20c:42ff:fe45:c128%ether3 reachable	110
DAC	2804:40:111:1315::/64	ether3 reachable	0
DAo	2804:40:111:1416::/64	fe80::20c:42ff:fe45:c128%ether3 reachable	110
DAo	2804:40:111:1516::/64	fe80::20c:42ff:fe45:c128%ether3 reachable	110
DAC	2804:40:1113:1113::/64	ether2 reachable	0

Rota externa recebida do peer eBGP (R11)

Segurança no IPV6

Mitos e “Meias verdades” sobre segurança em IPV6

→ Como não existe NAT no IPV6, o usuário está mais exposto.

→ IPV6 é seguro pois o IPSec é mandatório

→ Devido ao grande tamanho do espaço IPV6, um ataque de port scan é infrutífero

Considerações sobre segurança em IPV6

Pode-se a analisar a segurança em IPV6 em relação ao IPV4 sob vários aspectos diferentes:

- → Aquisição de dados para ataques
- → Acesso não autorizado
- → Spoofing de IP
- → Ataques a DHCP e ARP
- → Ataques de amplificação baseados em broadcasts (Smurf attack)
- → Sequestro de rotas
- → Propagação de vírus, e malwares
- → Ataques a mecanismos de tradução

Segurança no IPV6
Aquisição de dados

Esse geralmente é o processo em que se inicia a maioria dos ataques. O atacante silenciosamente procura obter o máximo de informações acerca da rede do atacado.

→ No IPV4

- Ping sweeps – ping, tracroute, firewalk

- Port Scans – nmap

- Scans de vulnerabilidades de serviços - nessus

Segurança no IPV6
Aquisição de dados

→ Considerações quanto ao IPV6

- ping sweep e port scans mais difíceis de se implementar

- novos endereços de multicast expõe certos alvos facilmente, como todos ós nós (FF02::1) , todos roteadores (FF05::2), servidores DHCP (FF05::5)

- Novas técnicas para scanning como coletar em logs de dns's, ataques de dicionário com base em endereços fáceis de memorização como 2804:40:café:dado::1

-

Segurança no IPV6
Acesso não autorizado

→ No IPV4

Controlado básicamente por ACL's

Técnicas como o "door knock" (bater a porta) podem ser utilizadas para dinamicamente permitir acessos externos

→ No IPV6

O mesmo para IPV4

Suporte a IPSec pode tornar as coisas mais fáceis e seguras.

Segurança no IPV6
Aquisição de dados

→ Boas práticas:

- Filtrar endereços IPV6 de uso interno nos roteadores de borda.

- Usar endereços estáticos não obvios para sistemas críticos.

- Filtrar serviços não necessários no Firewall.

- Filtrar seletivamente o ICMPv6

-

Segurança no IPV6
Spoofing de IP

Consiste na troca dos reais endereços IP de origem que pode ocorrer por aplicativos mal feitos ou por atividade maliciosa.

Para as conexões entrantes, somente o controle de BOGON's pode auxiliar. Pode-se evitar que usuários de sua rede façam spoofing.

→ No IPV4

Uma boa prática para provedores de última milha é negar a saida todos os endereços que não sejam de sua própria rede

→ No IPV6

O mesmo, porém lembrando que a parte destinada aos hosts tem um espaço de endereçamento infinitamente maior

Segurança no IPV6
Ataques a DHCP e ARP

Ataques a DHCP e ARP spoofing em redes IPV4 são muito fáceis de serem feitos e muito eficientes. Ver apresentação http://mum.mikrotik.com/presentations/PL10/maia.pdf

No IPV6, semelhantes técnicas podem ser utilizadas para ataque as redes, sendo que:

→ NO IPV6 o ARP não existe mas o mecanismo de descoberta de vizinhos é semelhante e não tem autenticação

→ O mecanismo de autoconfiguração stateless trabalha de forma análogo a um DHCPv4 e pode ser explorado da mesma forma.

Segurança no IPV6
Ataques a DHCP e ARP

Felizmente existem mecanismos para assegurar esses serviços (longe no entanto de estarem disponíveis nos produtos atualmente existentes)

→ SEND (Secure Neighbor Discovery) – descoberta de vizinhos de forma segura (RFC 3972)

→ DHCPv6 com autenticação

OBS: Em redes de provedores de acesso é possivel segregar os tráfego entre clientes utilizando técnicas de filtros de camada 2, evitando assim os ataques acima citados.
Para tanto ver: http://mum.mikrotik.com/presentations/PL10/maia.pdf

Segurança no IPV6
Ataques de amplificação de broadcast

Um antigo e conhecido ataque no IPV4 é o ataque de amplificação de Broadcast, conhecido como “Smurf Attack”. Consiste em mandar para um endereço de broadcast um pacote ICMP de “echo request” com o endereço de origem spoofado para o endereço da vítima. Todos os hosts da rede respondem para a vítima causando um ataque de DoS.

Esse método foi usado no passado e teve sua mitigação relativamente simples com a modificação dos kernels de sistemas operacionais impedindo que endereços de broadcast propaguem pacotes de broadcast diretamente. Esse “bug” não existe no Mikrotik e na maioria dos sistemas modernos.

Segurança no IPV6
Ataques de amplificação de broadcast

No IPV6 não existe endereço de Broadcast mas no entanto vários outros novos foram criados para o Multicast

Assim é possivel que um ataque semelhante ao ataque “Smurf”, enviando mensagens para os nós terminais da rede com IP de origem spoofado com endereços de Multicast

→ Mitigação desse possível ataque:

Filtrar descartando, todos os pacotes que contenham endereços de Multicast como endereço de origem.

Segurança no IPV6
Ataques a protocolos de roteamento

Esses ataques procuram redirecionar tráfego ou causar problemas de roteamento ou mesmo negação de serviço com a injeção de rotas falsas, envio de updates constantes para causar flood, etc.

→ BGP: O protocolo BGP utilizado é o mesmo, sendo que o IPV6 é uma família de endereços suportada e não há qualquer diferença de comportamento com relação a segurança no BGP a não ser a questão de autenticação e de TTL (ver apresentação de BGP no dia de amanhã)

→ OSPFv3 e RIPng: Os mecanismos de autenticação existentens nos antecessores OSPFv2 e RIP, foram retirados e a segurança deve-se basear em IPSec*

* Ainda não suportado no Mikrotik

Segurança no IPV6
Ataques a protocolos de roteamento

Esses ataques procuram redirecionar tráfego ou causar problemas de roteamento ou mesmo negação de serviço com a injeção de rotas falsas, envio de updates constantes para causar flood, etc.

→ BGP: O protocolo BGP utilizado é o mesmo, sendo que o IPV6 é uma família de endereços suportada e não há qualquer diferença de comportamento com relação a segurança no BGP a não ser a questão de autenticação e de TTL (ver apresentação de BGP no dia de amanhã)

→ OSPFv3 e RIPng: Os mecanismos de autenticação existentens nos antecessores OSPFv2 e RIP, foram retirados e a segurança deve-se basear em IPSec*

* Ainda não suportado no Mikrotik

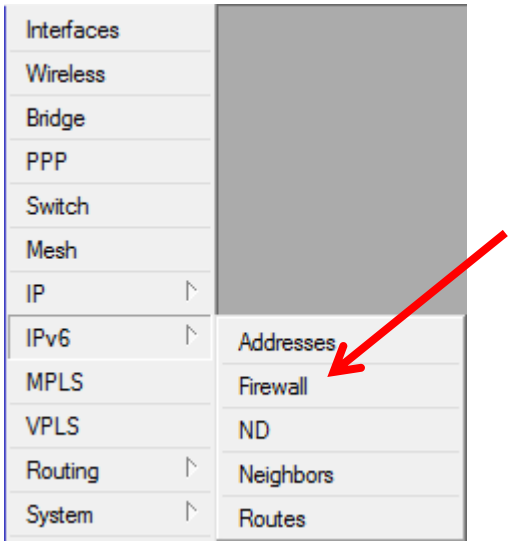
Segurança no IPV6
Vírus e malwares

Não há significativas mudanças nos males causados por vírus com o uso de um protocolo ou outro.

No entanto vírus que dependem de escaneamento de hosts expostos tendem a não mais existir, dado o grande espaço de numeração do IPV6

→ As regras de bloqueio de portas conhecidas de vírus utilizadas para o IPV4 podem ser utilizadas em Firewalls IPV6.

Firewall IPV6 no Mikrotik RouterOS



Princípios Básicos de Proteção

→Proteção do próprio roteador
- → tratamento das conexões e eliminação de tráfego prejudicial/inútil
- → permitir somente os serviços necessários no próprio roteador
- → prevenir e controlar ataques e acesso não autorizado ao roteador

→Proteção da rede interna
- → tratamento das conexões e eliminação de tráfego prejudicial/inútil
- → permitir somente os serviços necessários nos clientes
- → prevenir e controlar ataques e acesso não autorizado em clientes.

Regras de Firewall
Filtrando tráfego prejudicial/inútil

Filtros de portas de vírus

→Bloqueia portas mais populares utilizadas por vírus TCP e UDP 445 e 137-139

→No momento existem algumas centenas Trojans ativos e menos de 50 tipos de vírus ativos

→ No site da Mikrotik há uma lista com as portas e protocolos que utilizam esses vírus.

→Baixar lista de vírus Mikrotik e fazer as regras de acordo

Firewall
Proteções de ataques DoS

→O Principal objetivo do ataque de DoS é o consumo de recursos como CPU ou largura de banda.

→Usualmente o roteador é inundado com requisições de conexões TCP/SYN causando a resposta de TCP/SYN-ACK e a espera do pacote de TCP/ACK

→Normalmente não é intencional e é causada por vírus em clientes

→Todos IP's com mais de 10 conexões com o roteador podem ser considerados atacantes .

Firewall
Proteções de ataques DoS

Ataques DoS - cont

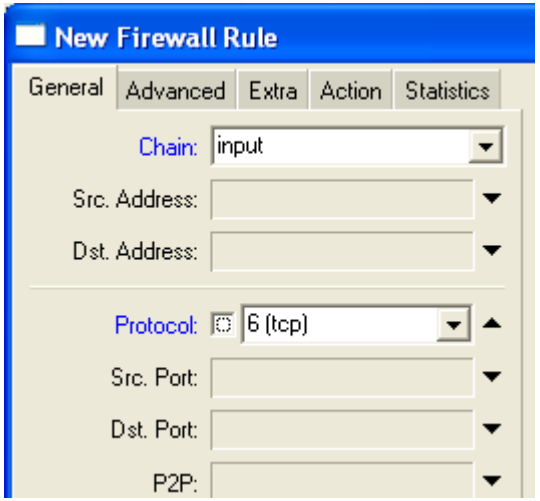
→Se simplesmente descartarmos as conexões, permitiremos que o atacante crie uma nova conexão.

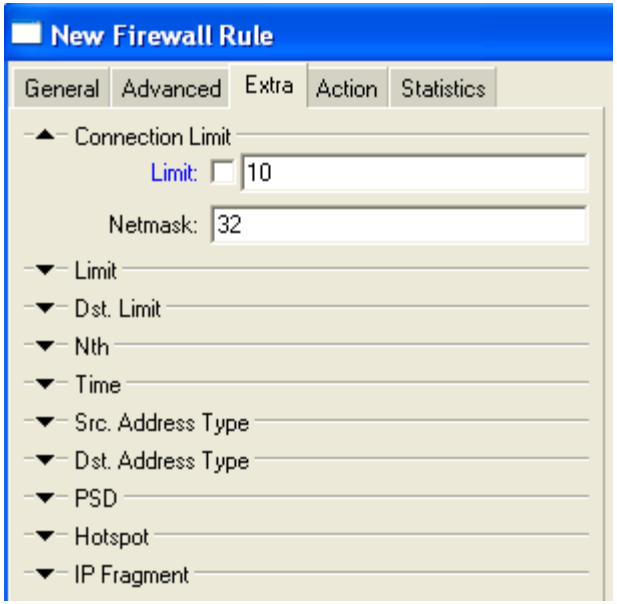
→A proteção pode ser implementada em dois estágios:

→ Detecção – criando uma lista dos atacantes DoS com base em connection limit

→Supressão – aplicando restrições aos que forem detectados.

Firewall
Proteções de ataques DoS

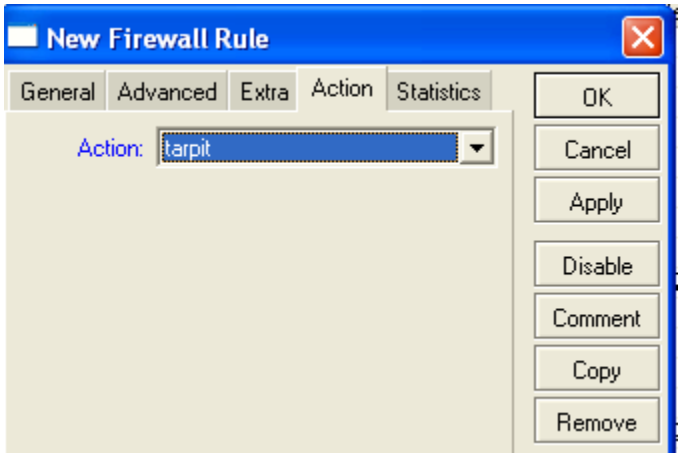




Firewall
Proteções de ataques DoS

- → Com a ação tarpit aceitamos a conexão e a fechamos, não deixando no entanto o atacante trafegar.

- → Esta regra deve ser colocada antes da regra de detecção ou então a address list vai reeescreve-la todo o tempo.

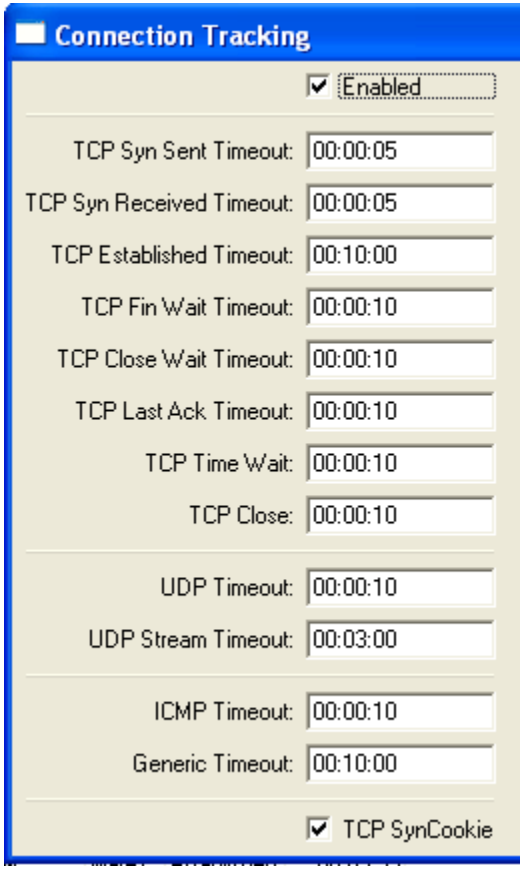


Firewall
Proteções de ataques

dDOS

→Ataques de dDos (dDoS) são bastante parecidos com os de DoS, porém partem de um grande número de hosts infectados

→A única medida que podemos tomar é habilitar a opção TCP syn cookie no connection tracking do Firewall



Regras de Firewall
Controle de ICMP

O Internet Control Message Protocol (ICMP) é basicamente uma ferramenta para diagnóstico da rede e alguns tipos de ICMP obrigatoriamente devem ser liberados.

No IPV4 boas práticas indicam a manutenção de pelo menos 5 tipos de ICMP (type:code), que são:

- PING – Mensagens 0:0 e 8:0
- TRACEROUTE – Mensagens 11:0 e 3:3
- PMTUD – Path MTU discovery – mensagem 3:4

Os outros tipos de ICMP normalmente podem ser bloqueados sem qualquer efeito danoso à rede

Regras de Firewall
Controle de ICMP

O Internet Control Message Protocol (ICMP) é basicamente uma ferramenta para diagnóstico da rede e alguns tipos de ICMP obrigatoriamente devem ser liberados.

No IPV4 boas práticas indicam a manutenção de pelo menos 5 tipos de ICMP (type:code), que são:

- PING – Mensagens 0:0 e 8:0
- TRACEROUTE – Mensagens 11:0 e 3:3
- PMTUD – Path MTU discovery – mensagem 3:4

Os outros tipos de ICMP normalmente podem ser bloqueados sem qualquer efeito danoso à rede

Regras de Firewal - Controle de ICMP

Equivalentes do IPV4 no IPV6

ICMPv6 Type 1 Code 0 – No route to destination

ICMPv6 Type 3 - Time exceeded

ICMPv6 Type 128 and Type 129 - Echo request and echo reply

Novas mensagens potencialmente requeridas no IPV6:

ICMPv6 Type 2 - Packet too big – requerido pelo PMTUD

ICMPv6 Type 4 - Parameter problem

ICMP Type 130-132 - Multicast listener messages

ICMPv6 Type 133/134 – Router solicitation and router advertisement

ICMPv6 Type 135/136 – Neighbor solicitation and neighbor advertisement.

Filtrando tráfego indesejável

IP's Bogons:

→ No IPV4

Ainda que restem poucos endereços IPV4 (menos de 5%), aqueles não alocados podem ser empregados para ataques quando o atacante quer ocultar seu endereço.

→ No IPV6

O grande espaço de endereçamento do IPV6 torna a necessidade de controle de BOGONS ainda mais crítica.

Controlando BOGONS

O Site abaixo mantem listas e serviços para controle de BOGONS

http://www.team-cymru.org/Services/Bogons/

Listas podem ser obtidas:

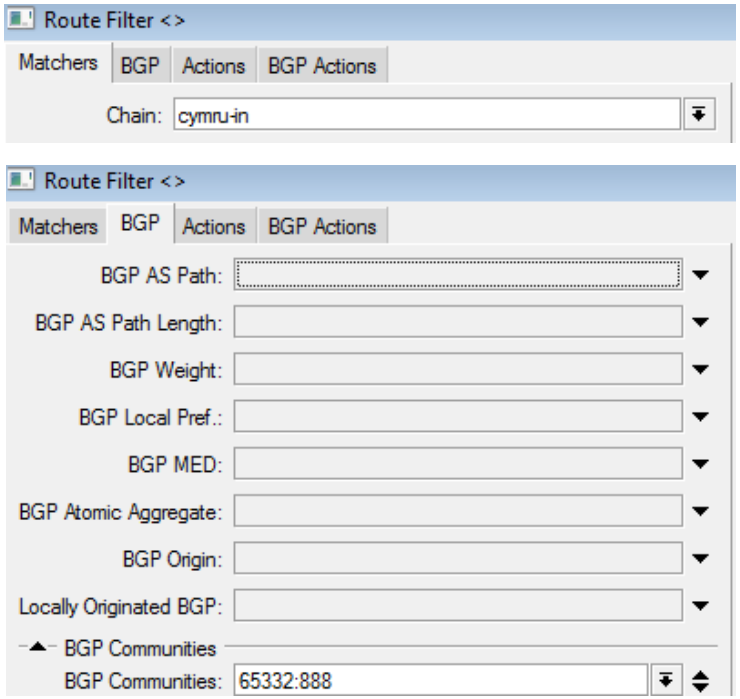
→ pelo próprio site

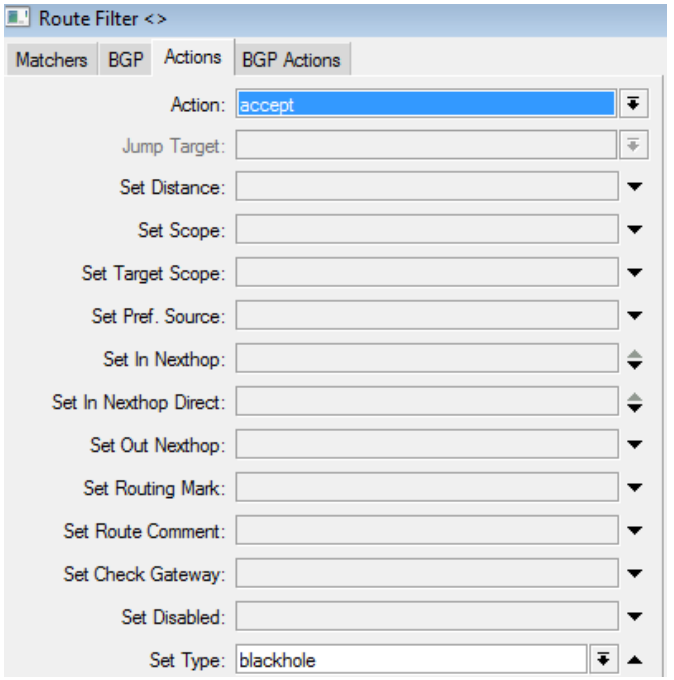
→ por email

→ automáricamente fazendo um peer BGP com a cymru

Filtro automático de Full Bogons via BGP (não é firewall)

Marcando as rotas entrantes do peer com o Cymru como blackhole

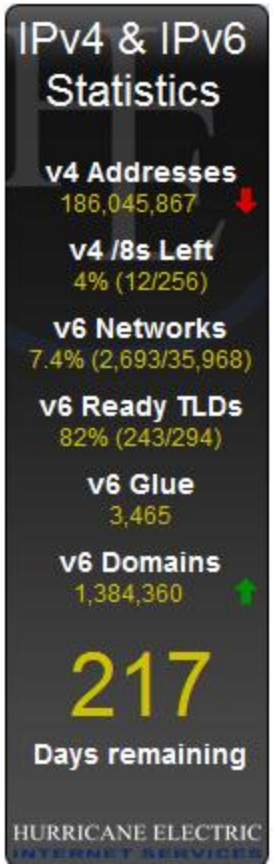




Implementação de IPV6 no Mikrotik

IPV6

Como começar ???



Como começar

Para quem não tem conectividade nativa IPV6 uma boa solução é começar por um túnel IPV4-IPV6. Como sugestão a empresa abaixo oferece essa conectividade sem custo.

HURRICANE ELECTRIC
INTERNET SERVICES

Internet Backbone and Colocation Provider

Hurricane Electric

Free IPv6 Certifications!

http://ipv6.he.net/certification

www.tunnelbroker.net
www.he.net

Como começar

São oferecidos dois tipos de túnel:

→ Túneis regulares

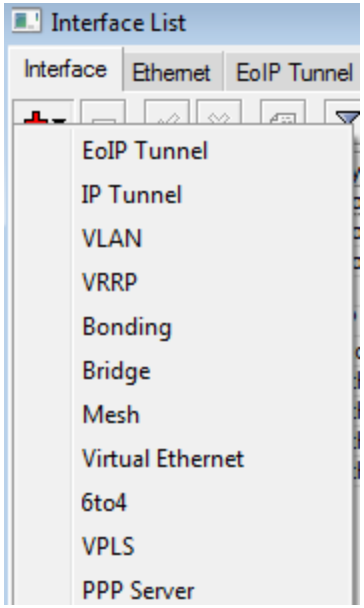
Úteis para quem ainda não tem AS ou se tem ainda não tem seu bloco próprio de IPV6

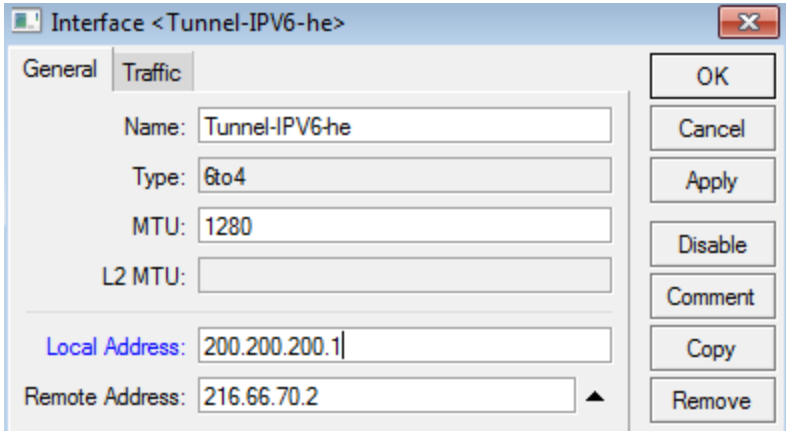
→ Túneis BGP

Quem tem AS e bloco IPV6 designado mas não tem conectividade nativa IPV6 pode anunciar seu bloco pela HE sem qualquer custo. Nesse caso será pedida uma carta de confirmação para conferencia da titularidade do AS.

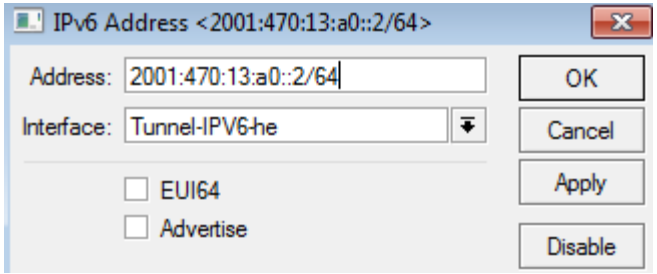
Configurações no Mikrotik

1 – Criar a interface 6to4 utilizando o seu endereço IPV4 e o remoto fornecido pela HE



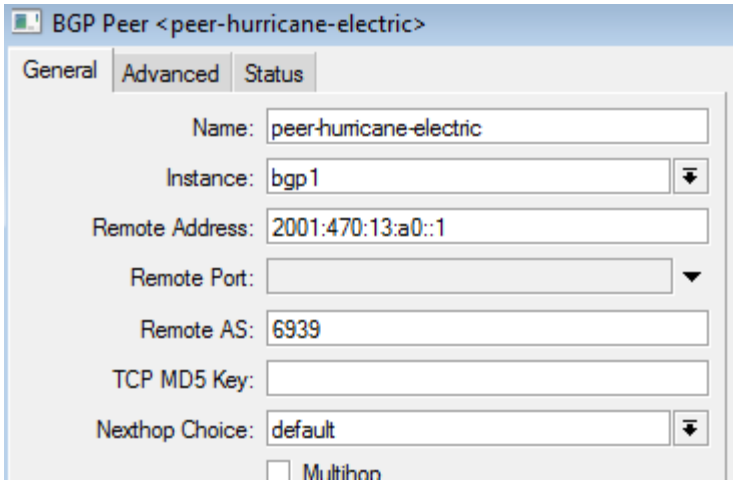


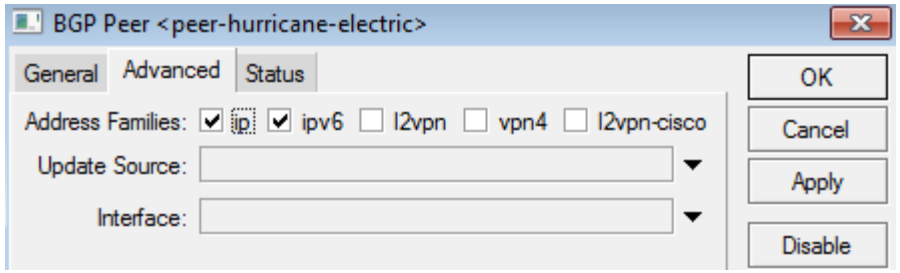
2 – Configurar o endereço IPV6 fornecido pela HE na interface criada

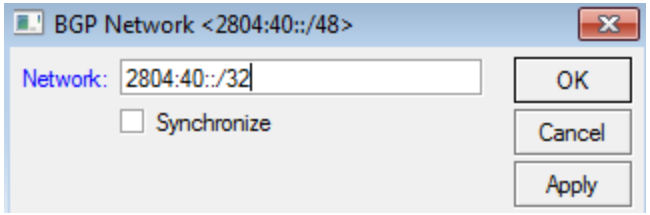


Configurações no Mikrotik

3 – Fazer o Peer com a HE habilitando o MBGP com address family IPV6 e publicar o bloco de IPV6 pertencente ao provedor.







IPV6 Como começar

Principais desafios:

→ Falta de conectividade nativa. Túneis podem ser um bom começo para o aprendizado do IPV6 mas terão suas limitações quando em produção

→ Falta de suporte nos equipamentos dos clientes.

→ Quebra do paradigma interno nas empresas. Investimento em planejamento, treinamentos e equipamentos.

IPV6 Como começar

Estratégias para os pequenos e médios provedores

- → Começar a exigir equipamentos com suporte a IPV6
- → Quem ainda não tem, correr atrás do seu AS
- → Procurar formas de se conectar a um PTT
- → Iniciar o estudo e implementação, ontem !

Obrigado !

Wardner Maia – maia@mikrotikbrasil.com.br