
# Virando a chave para IPv6

## Como um bom planejamento pode tornar sua rede mais eficiente e segura

MUM Brasil

Foz do Iguaçú

Novembro/2019

# Introdução

**Wardner Maia**

Engenheiro – Eletrotécnica e Eletrônica com especialização em Telecomunicações;

Provedor de Acesso à Internet desde 1995;

Treinamentos para ISPs desde 2002, Trainer Mikrotik #021;

Diretor técnico da MD Brasil IT & Telecom;

Diretor do LACNIC.

# Sobre o que

# é essa apresentação?

# Sobre o que é essa apresentação?

**Mais uma falando de:**

**- escassêz do IPv4?**

**- importância do IPv6?**

**- blá, blá, blá????**

md brasil
TI&TELECOM

# SIM!

# Certamente!

# Europa distribui seu último /22

**25/12/2019!**

The Register®
Biting the hand that feeds IT

DEVOPS BUSINESS PERSONAL TECH SCIENCE E

Data Centre ▸ Networks

## We are absolutely, definitively, completely and utterly out of IPv4 addresses, warns RIPE

So will you all please move to IPv6? World: Nope.

By Kieren McCarthy in San Francisco 25 Nov 2019 at 22:31 186 SHARE ▼


RIPE NCC
RIPE NETWORK COORDINATION CENTRE

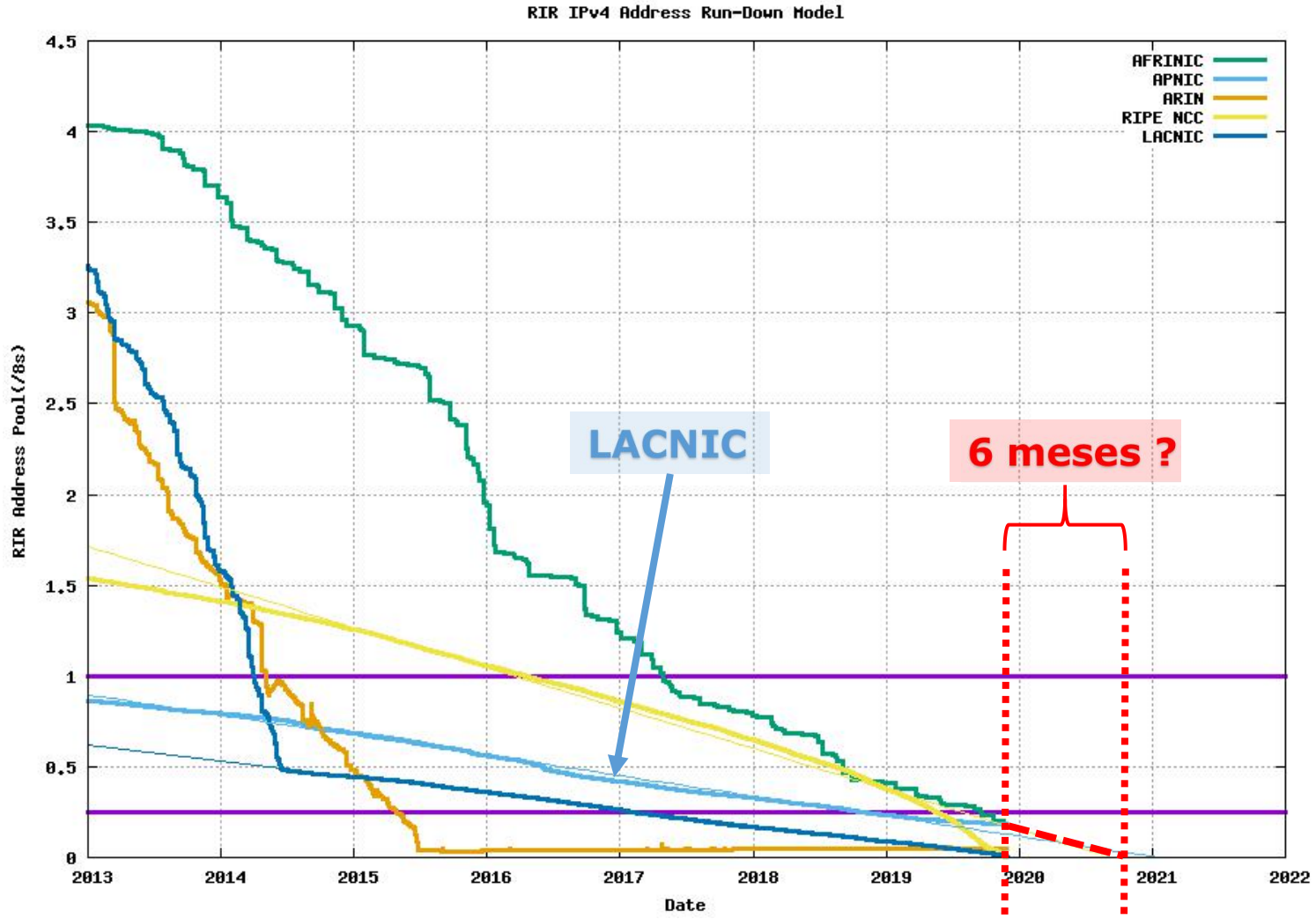
## The RIPE NCC has run out of IPv4 Addresses

**Today, at 15:35 (UTC+1) on 25 November 2019, we made our final /22 IPv4 allocation from the last remaining addresses in our available pool. We have now run out of IPv4 addresses.**

Our announcement will not come as a surprise for network operators - IPv4 run-out has long been anticipated and planned for by the RIPE community. In fact, it is due to the community's responsible stewardship of these resources that we have been able to provide many thousands of new networks in our service region with /22 allocations after we reached our last /8 in 2012.

# Evolução do IPv4

https://ipv4.potaroo.net/



# O que foi feito na região de LACNIC?

- As políticas de distribuição de IPs trouxeram o estoque até os dias de hoje (restam apenas ~6 meses);

- Treinamentos em IPv6 desde 2005;

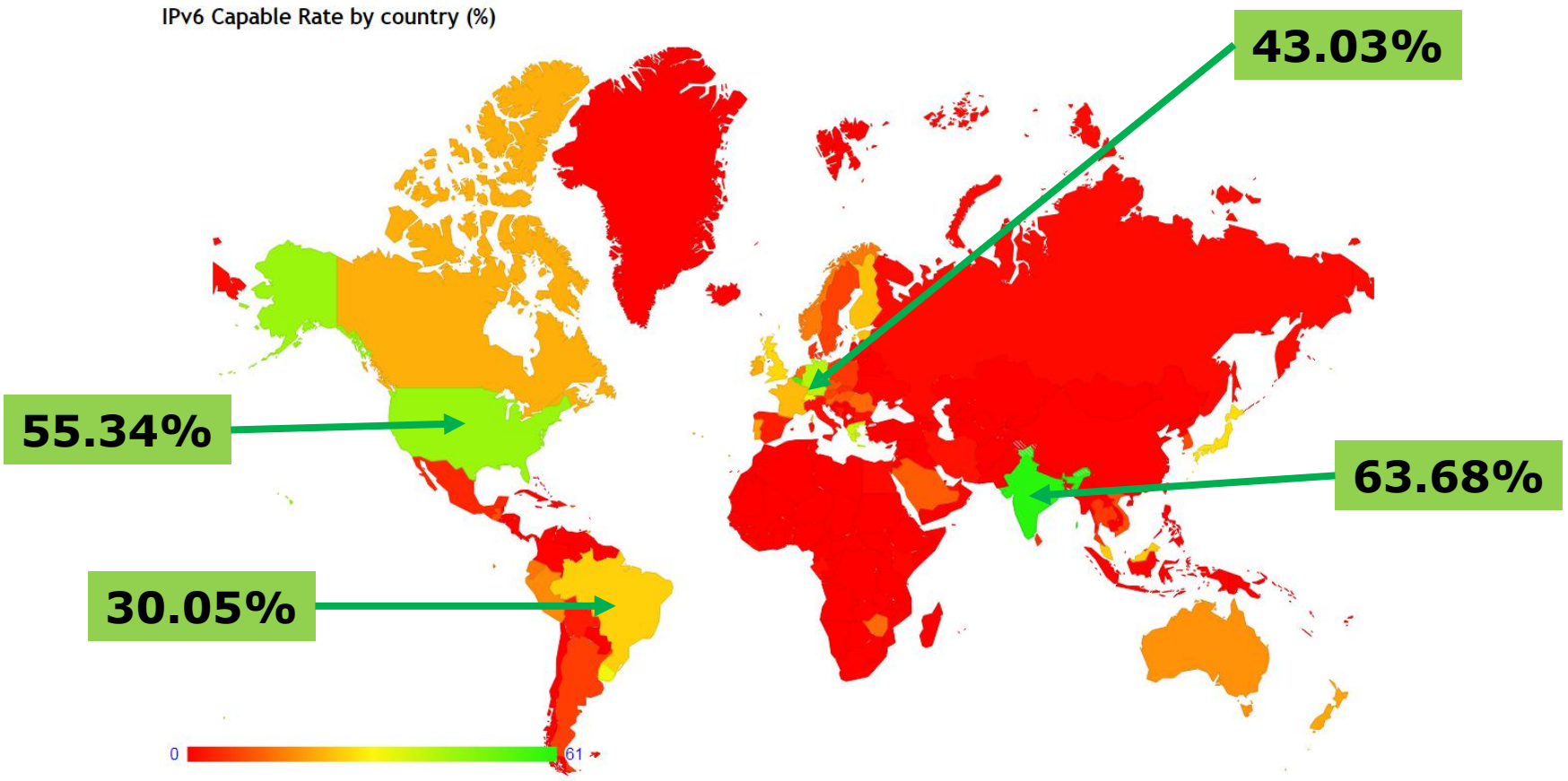
- Cursos online de IPv6 com nais de 10 mil capacitados;

- Maior porcentagem de associados com IPv6 atribuído (+96%);

- É a que mais anuncia IPv6 (+45%);

- Porcentagem de adoção de quase 10% abaixo da média global.

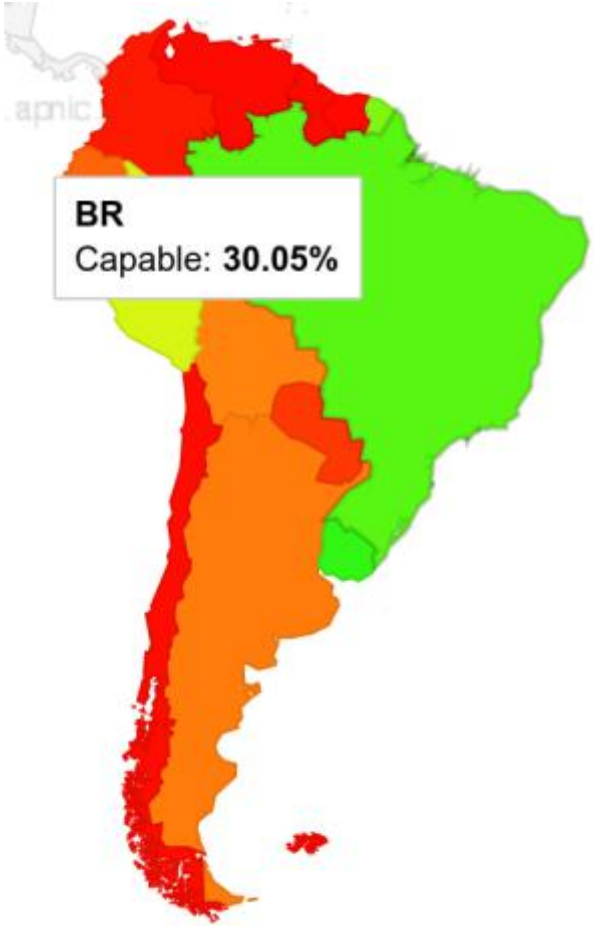
# Adoção do IPv6 (visto pelo APNIC)




https://stats.labs.apnic.net/ipv6

estado em 27 de novembro de 2019

# Situação no Brasil




| ASN | AS Name | IPv6 Capable | IPv6 Preferred | Samples |
|---|---|---|---|---|
| AS[redacted] | | 59.43% | 59.18% | 31,699 |
| AS[redacted] | | 57.30% | 48.59% | 14,898 |
| AS[redacted] | | 50.52% | 50.24% | 14,350 |
| AS[redacted] | | 85.64% | 85.40% | 12,998 |
| AS[redacted] | | 66.04% | 65.60% | 12,039 |

- Crescimento do IPv6 puxado pelas grandes operadoras.

- Em quanto colaboram para os 30% de adoção os provedores regionais?

# Porque a baixa adesão ao IPv6 pelos ISPs regionais?

# Porque a baixa adesão dos ISPs regionais?

Principais desculpas:

- Nosso fornecedor de link não nos fornece IPv6

- Os equipamentos que utilizamos não suportam IPv6

- O IPv6 ainda não “pegou”. Tem muito conteúdo que só acessa em IPv4

- Temos outra prioridade. Depois de fazermos xxxx, vamos pensar nisso;

- Não sabemos por onde começar

# Porque a baixa adesão dos ISPs regionais?

Principais desculpas:

~~- Nosso fornecedor de link não nos fornece IPv6~~

- Os equipamentos que utilizamos não suportam IPv6

- O IPv6 ainda não “pegou”. Tem muito conteúdo que só acessa em IPv4

- Temos outra prioridade. Depois de fazermos xxxx, vamos pensar nisso;

- Não sabemos por onde começar

# Porque a baixa adesão dos ISPs regionais?

Principais desculpas:

~~- Nosso fornecedor de link não nos fornece IPv6~~

~~- Os equipamentos que utilizamos não suportam IPv6~~

- O IPv6 ainda não “pegou”. Tem muito conteúdo que só acessa em IPv4

- Temos outra prioridade. Depois de fazermos xxxx, vamos pensar nisso;

- Não sabemos por onde começar

# Porque a baixa adesão dos ISPs regionais?

Principais desculpas:

~~- Nosso fornecedor de link não nos fornece IPv6~~

~~- Os equipamentos que utilizamos não suportam IPv6~~

~~- O IPv6 ainda não "pegou". Tem muito conteúdo que só acessa em IPv4~~

- Temos outra prioridade. Depois de fazermos xxxx, vamos pensar nisso;

- Não sabemos por onde começar

# Porque a baixa adesão dos ISPs regionais?

Principais desculpas:

~~- Nosso fornecedor de link não nos fornece IPv6~~

~~- Os equipamentos que utilizamos não suportam IPv6~~

~~- O IPv6 ainda não "pegou". Tem muito conteúdo que só acessa em IPv4~~

~~- Temos outra prioridade. Depois de fazermos xxxx, vamos pensar nisso;~~

- Não sabemos por onde começar

# Porque a baixa adesão dos ISPs regionais?

Principais desculpas:

~~- Nosso fornecedor de link não nos fornece IPv6~~

~~- Os equipamentos que utilizamos não suportam IPv6~~

~~- O IPv6 ainda não "pegou". Tem muito conteúdo que só acessa em IPv4~~

~~- Temos outra prioridade. Depois de fazermos xxxx, vamos pensar nisso;~~

- Não sabemos por onde começar

# Porque a baixa adesão dos ISPs regionais?

Razões reais:

- Não percepção da importância competitiva negativa que pode em breve representar a não adoção do IPv6

- Medo do desconhecido - um ingrediente a mais para administrar.

- Despreparo do pessoal de help desk

**- Não saber por onde começar - Dificuldades com relação ao planejamento.**

# IPv4 x IPv6

# Em que momento estamos?

# IPv4 x IPv6
# Em que momento estamos?

**Paradigma da Escassêz x Abundância**

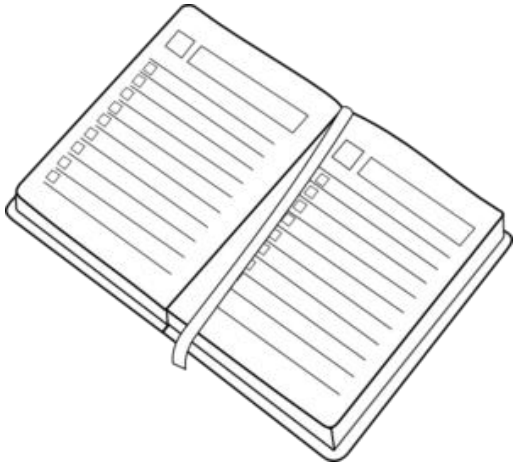
**IPv4:**

- Precisamos nos preparar para melhorar o que já estamos fazendo há tempos - **administrar a escassêz!**

**IPv6:**

- Precisamos nos preparar para tirar o que há de melhor no IPv6 - **desfrutar da abundância!**

# Agenda



Introdução ✓

Administrando a escassêz do IPv4

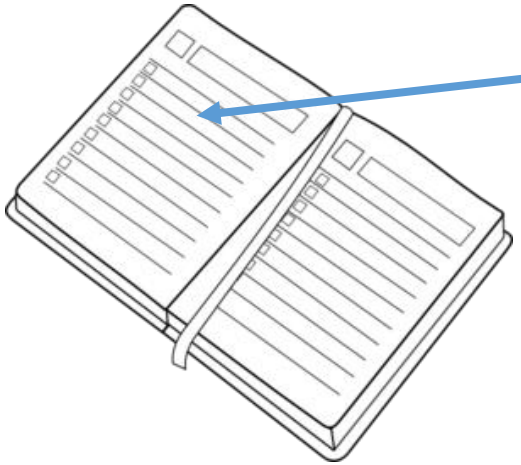
Desfrutando da abundância do IPv6

Impactos na segurança da rede

Planejamento da infraestrutura

Efetivando com RouterOS

# Agenda



Introdução ✓

**Administrando a escassêz do IPv4**

Desfrutando da abundância do IPv6

Impactos na segurança da rede

Planejamento da infraestrutura

Efetivando com RouterOS

# Soluções para compartilhamento de endereços

Dual-Stack Lite [DS-Lite]

NAT64 [RFC6145] [RFC6146];

Address+Port (A+P) proposals [A+P] [PORT-RANGE]

Stateless Address Mapping [SAM]

**Carrier Grade NAT (CGN) or Large Scale NAT (LSN) [LSN-REQS]**

# NAT, CGNAT
# NAT 444

# Implementações e problemas relacionados

# Rastreabilidade com CGNAT

disruptive.asia

HOME | NEWS | VIEWS | FEATURES | OFF THE WIRE | VIDEOS | EVENTS | D

## Here's why it's getting harder for law enforcement to find you via your IP address

March 10, 2017 · Don Sambandaraksa · Views · 0

Credit: VectorShots / Shutterstock.com

EUROPOL — ABOUT EUROPOL | ACTIVITIES & SERVICES | CRIME AREAS & TRENDS | PARTNERS & AGREEMENTS | CAREERS & PROCUREMENT

HOME › NEWSROOM › ARE YOU SHARING THE SAME IP ADDRESS AS A CRIMINAL? LAW ENFORCEMENT CALL FOR THE END OF CARRIER GRADE NAT (CGN) TO INCREASE ACCOUN...

## ARE YOU SHARING THE SAME IP ADDRESS AS A CRIMINAL? LAW ENFORCEMENT CALL FOR THE END OF CARRIER GRADE NAT (CGN) TO INCREASE ACCOUNTABILITY ONLINE

17 October 2017

IEEE Xplore® Digital Library — Institutional Sign In

Browse | My Settings | Get Help | Subscribe

All — Enter keywords or short phrases (searches metadata only by default)

Browse Journals & Magazines > IEEE Security & Privacy > Volume: 15 Issue: 5

## Availability of Required Data to Support Criminal Investigations Involving Large-Scale IP Address–Sharing Technologies

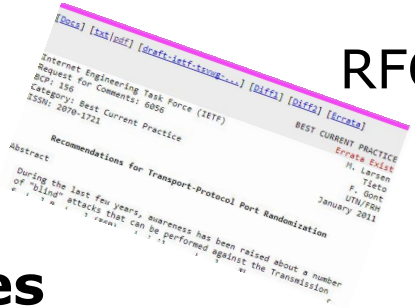
Sign In or Purchase to View Full Text

87 Full Text Views

# Argumentos Técnicos

# RFC 6302

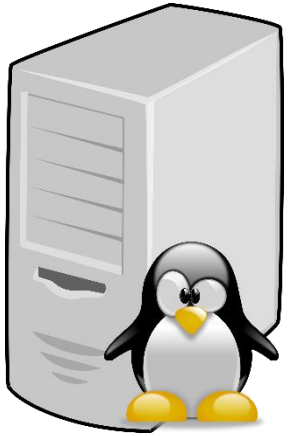
# Recomendações para logging




RFC 6302

**Considerações para servidores**

*"In the wake of IPv4 exhaustion and deployment of IP address sharing techniques, this document recommends that Internet-facing servers* ***log port number*** *and accurate timestamps in addition to the incoming IP address."*



# Recomendações para Logging

RFC 6302

**Considerações para ISPs**

*"ISP deploying IP address sharing techniques should also deploy a corresponding logging architecture to maintain records of the relation between a customer's identity and* ***IP/port resources*** *utilized."*

# Fundamentos legais no Brasil

## Relatório final do GT-IPv6

**5.1 – Implicações do GC-NAT44 na quebra de sigilo de dados telemáticos**

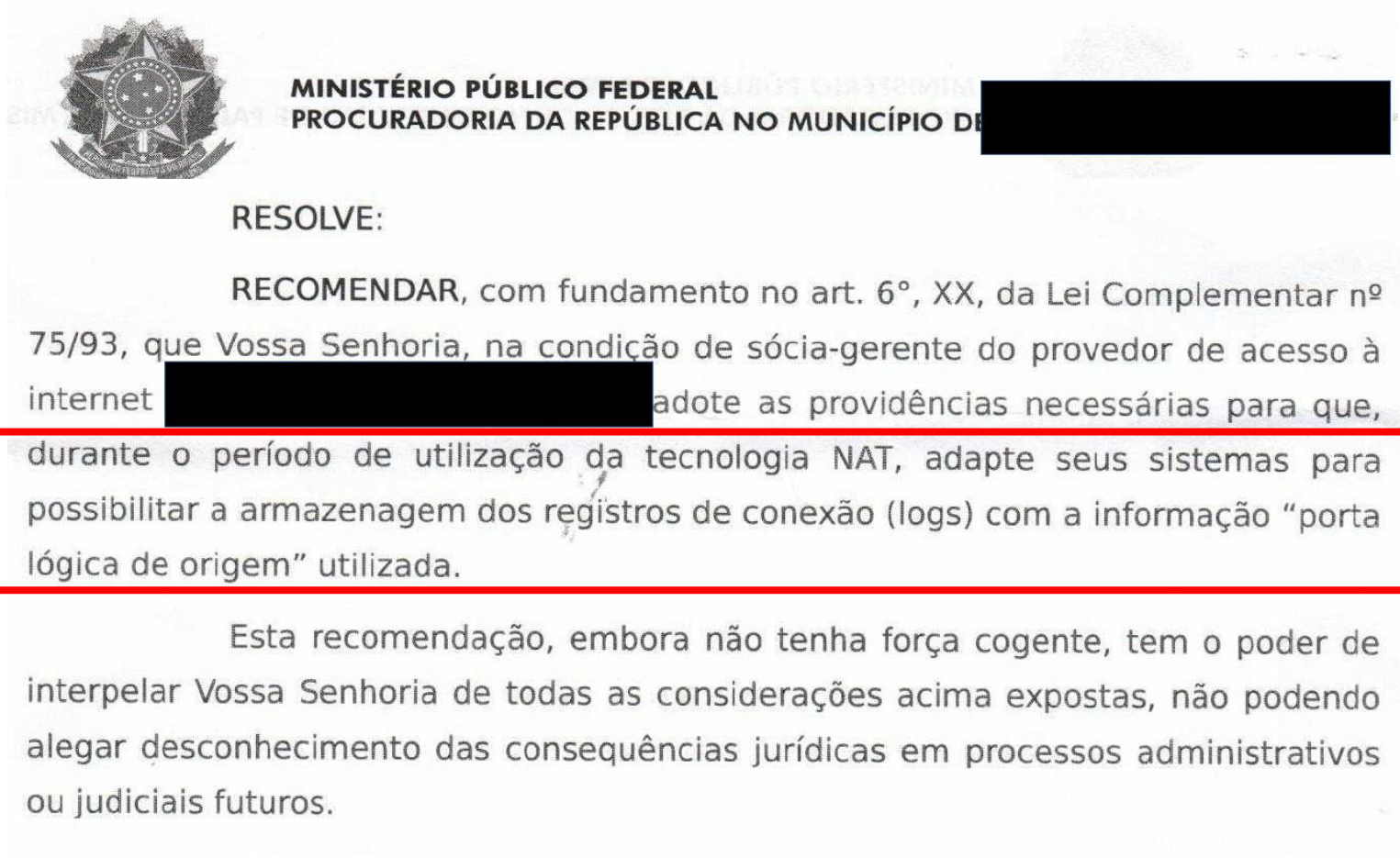
Tanto no Grupo de Trabalho do NIC.br como no Grupo de Trabalho da ANATEL foi intensamente discutida a questão da identificação unívoca de um determinado usuário que faz uso de um endereço IP compartilhado. Em ambos os Grupos de Trabalho foi consenso que a única forma das prestadoras fornecerem o nome do usuário que faz uso de um IP compartilhado em um determinado instante seria com a informação da "porta lógica de origem da conexão" que estava sendo utilizada durante a conexão. Dessa forma, os provedores de aplicação devem fornecer não somente o IP de origem utilizado para usufruto do serviço que ele presta, mas também a "porta lógica de origem".

Em uma Conexão à Internet, para cada sessão aberta pelo usuário, é utilizada uma "porta lógica" para sua comunicação com outras redes e equipamentos. Assim, mesmo quando dois usuários fazem o uso compartilhado de um mesmo IPv4, eles usarão portas distintas para a sua comunicação.

Será com base na informação da "porta lógica de origem" que as identificações judiciais para fins de quebra de sigilo e interceptação legal continuarão sendo possíveis de serem realizadas de forma unívoca. Portanto, torna-se necessário que na solicitação de quebra de sigilo seja informada, além dos atributos atuais (endereço IP de origem, data, hora e fuso da conexão), a porta de origem da comunicação.

# Fundamentos legais

## Solicitações do MP Federal para provedores de acesso



MINISTÉRIO PÚBLICO FEDERAL
PROCURADORIA DA REPÚBLICA NO MUNICÍPIO DE [redacted]

RESOLVE:

RECOMENDAR, com fundamento no art. 6°, XX, da Lei Complementar nº 75/93, que Vossa Senhoria, na condição de sócia-gerente do provedor de acesso à internet [redacted] adote as providências necessárias para que, durante o período de utilização da tecnologia NAT, adapte seus sistemas para possibilitar a armazenagem dos registros de conexão (logs) com a informação "porta lógica de origem" utilizada.

Esta recomendação, embora não tenha força cogente, tem o poder de interpelar Vossa Senhoria de todas as considerações acima expostas, não podendo alegar desconhecimento das consequências jurídicas em processos administrativos ou judiciais futuros.

# Qual é o tamanho desses logs?

# Logs para ISPs

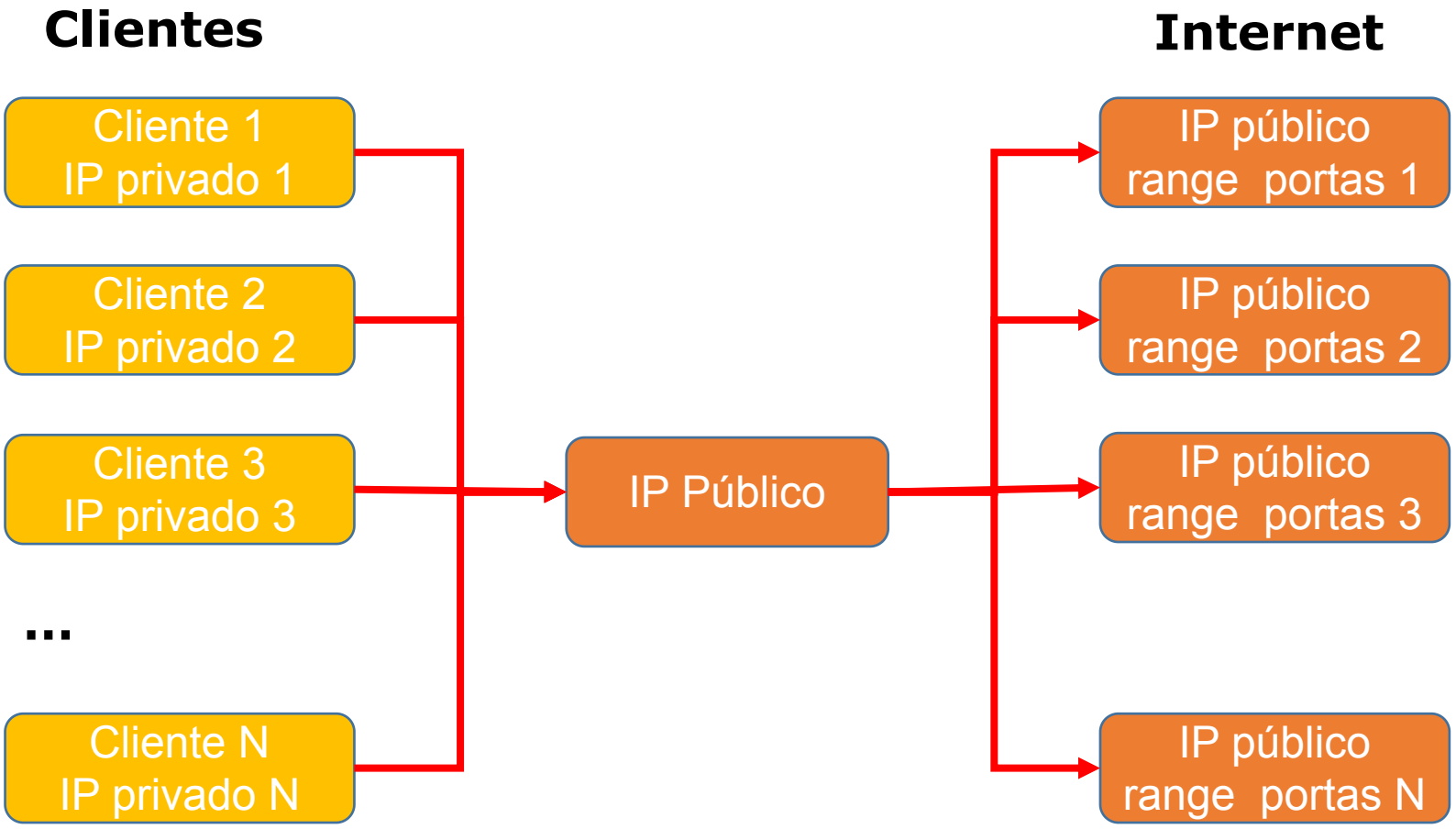
Logar toda atividade dos usuários com a porta de origem seria muito custoso de recursos e espaço. Contudo, a RFC 6269 sugere a alocação de grupos pré definidos de portas:

*RFC 6269 (Issues with IP Address Sharing)*

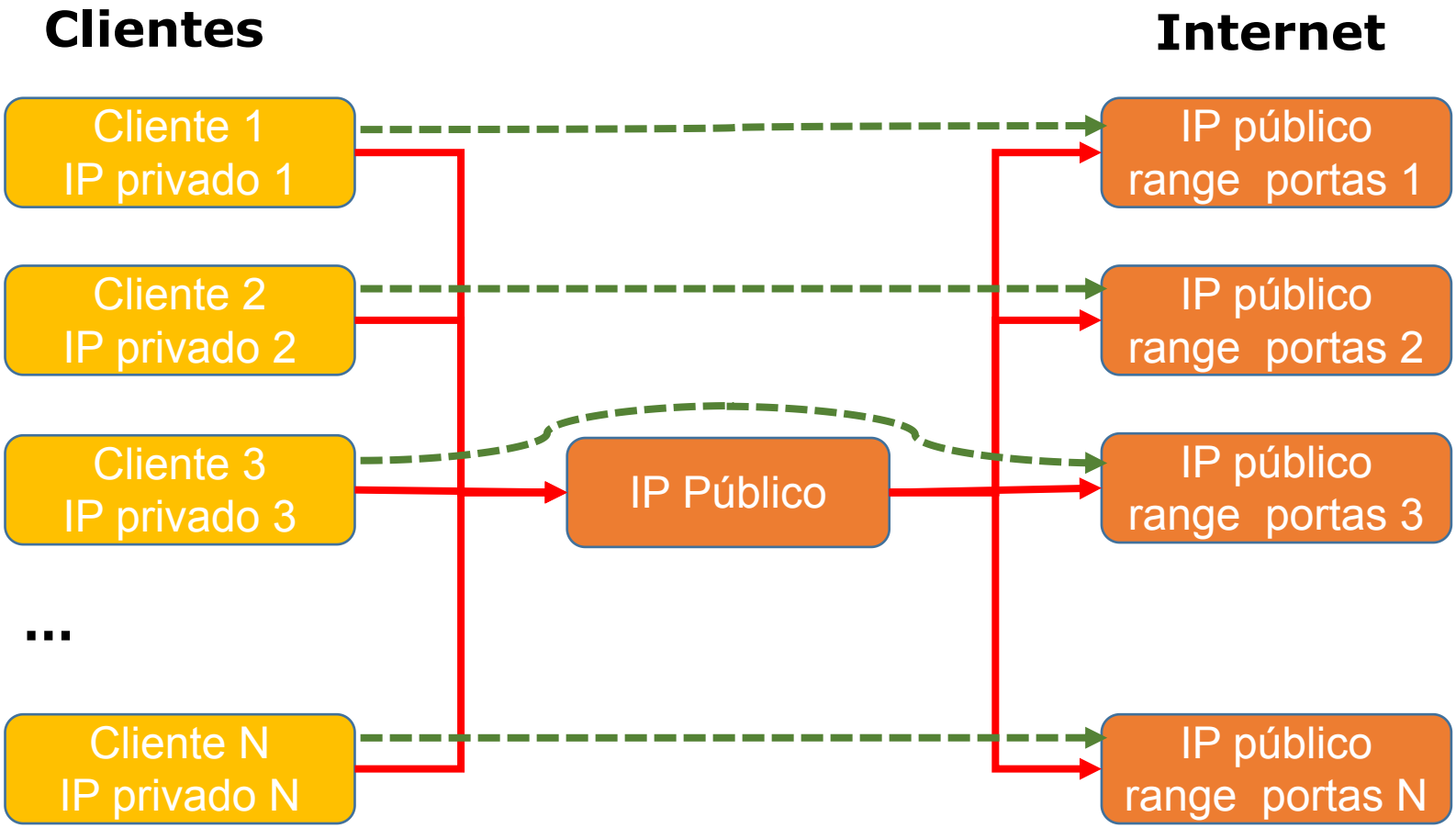
*"Address sharing solutions may mitigate these issues to some extent by **pre-allocating groups of ports.** Then only the allocation of the group needs to be recorded, and not the creation of every session binding within that group."*

Desta forma não são necessários logs, mas sim a implementação de um esquema fixo e a documentação desse esquema.

# Implementação no ISP



# Implementação no ISP



# Quais portas?

# Quais portas?

Portas IANA

- Well-Known Ports: from 0 through 1023;
- Registered Ports: from 1024 through 49151;
- Dynamic and/or Private Ports: from 49152 through 65535.

# Quais portas?

Podemos utilizar as portas **registradas**?

Embora o termo “portas registradas” possam sugerir algum tipo de restrição, a RFC 4787 deixa claro que o uso destas portas para essa finalidade é permitido:

*"mapping a source port to a source port that is already registered is unlikely to have any bad effects".*

*Assim, temos um total de 64511 (1024-65535) portas para utilização no CGNAT*

# Quantas portas por cliente?

# Número de portas e TCP Time-wait

Após o fechamento de uma conexão TCP, esta entra no estado TIME-WAIT (tipicamente de 4 minutos);

O objetivo é evitar conexões duplicadas em caso de sobreposição de conexões TCP velhas e novas devido a repetição de número de sequencia TCP;

O delay do TIME-WAIT tem por objetivo dar tempo suficiente para que as conexões "morram" antes de reabri-las

Isso implica em uma reserva maior de portas que o número real de conexões necessárias.

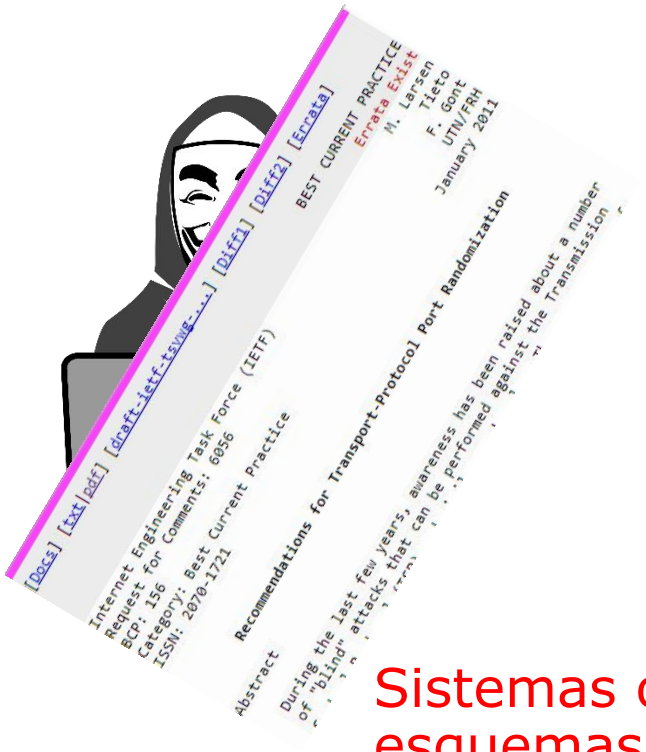
# Número de portas e segurança

Existem diversos tipos de ataques “cegos” contra o protocolo TCP e similares.

Consequências possíveis: redução do throughput, conexões quebradas e ou dados corrompidos;

Esses ataques se baseiam na possibilidade de saber (ou adivinhar) 5 parâmetros (Protocolo, endereço de origem, endereço de destino, porta de origem e porta de destino)

# Número de portas e segurança




RFC 6056

Recomendações para randomização de portas em protocolos de transporte

O range de portas dinâmicas definido pela IANA é a faixa de 49152-65535, e é utilizada para a seleção de portas efêmeras

Sistemas operacionais usualmente implementam esquemas de randomização de portas. Quanto mais portas disponíveis por usuário, mais eficiente pode ser a randomização.

# Quantas portas por usuário?

Dependendo do tipo de conexão, teremos diferentes necessidades. Ex. para clientes móveis de um Hotspot poucas portas podem ser suficientes, diferentemente de banda larga fixa com FTTH quando vários dispositivos irão compartilhar as portas;

Quanto maior o número de portas reservarmos por usuário, menor probabilidade de futuros problemas;

A questão que temos que responder é:

Quantas vezes nosso espaço IPv4 deve ser multiplicado para atender nossas futuras necessidades?

# Planejamento de IPv4 em tempos de esgotamento...

# Cenário hipotético

**Quadro atual:**

- Pequeno ISP em região com 200 mil habitantes
- 50 mil domicílios
- atualmente com 1 mil clientes

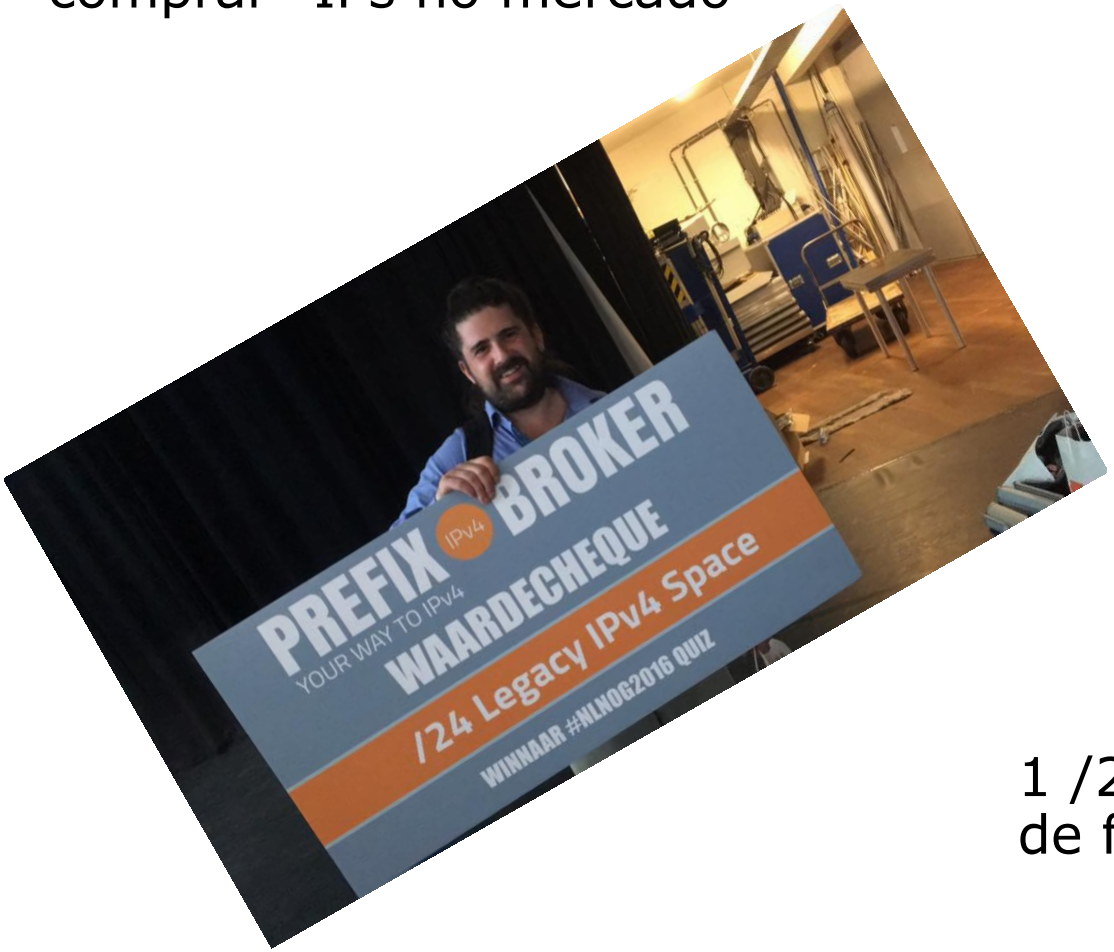
**Previsão de crescimento nos próximos 3 anos**

- Quer crescer atingindo 50% de penetração (25 mil clientes)

Provedor tem somente 1 bloco /22 (1024 IPs) de IPv4!

# Como crescer sem IPs?

**Alternativa 1** - Localizar um IP Broker e "comprar" IPs no mercado




Um /20 recém negociado no Brasil custou a "bagatela" de US$ 70.000,00

~R$300.000,00

1 /20 = Quantos Km de fibras ópticas?

# Como crescer sem IPs?

**Fazendo CGNAT:**

Para fazer frente as necessidades futuras o ISP terá de fazer CGNAT com a "taxa de compartilhamento" de 1:25

Número de portas por assinante:

Considerando 64511 portas, o número será:

- 64511 / 25 ~= 2580 portas por assinante

assinante 1: 1.024 - 3.604

assinante 2: 3.605 - 6.185

…

assinante 25k: 65.285 – 65.535

# Como crescer sem IPs?

**Alternativa 2** - Comprar uma caixa "mágica" que você liga na tomada e multiplica seus IPs!

Algumas caixinhas mágicas custam ~R$ 50K

Ah, e você precisa de duas pois quem tem uma não tem nenhuma! (R$ 100k)

Quantos Km de fibra você compra com R$ 100K?

# Como crescer com poucos IPs (e gastando pouco)

# Como crescer sem IPs? (e gastando pouco)

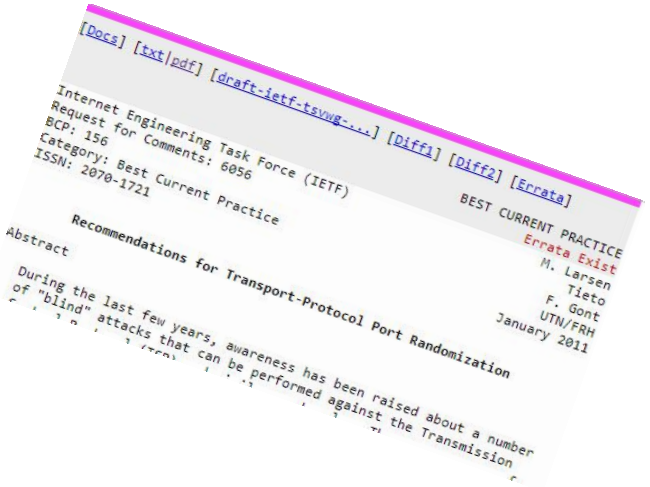
**Alternativa 3** - Estudar um pouco, seguir as RFCs e configurar seu próprio CGNAT com RouterOS ou Linux


**Economize e construa redes de fibra.**

**Sua rede vale o mesmo que de quem comprou IPs ou caixas mágicas!**

# Como implementar o CGNAT

**RFC 6598**


[Docs] [txt|pdf] [draft-ietf-tsvwg-...] [Diff1] [Diff2] [Errata]

Internet Engineering Task Force (IETF)
Request for Comments: 6056
BCP: 156
Category: Best Current Practice
ISSN: 2070-1721

BEST CURRENT PRACTICE
Errata Exist
M. Larsen
Tieto
F. Gont
UTN/FRH
January 2011

Recommendations for Transport-Protocol Port Randomization

Abstract

During the last few years, awareness has been raised about a number of "blind" attacks that can be performed against the Transmission

O espaço reservado para o CGNAT ou NAT 444, de acordo com a RFC 6598 é 100.64.0.0/10

Primeira alternativa, NAT for cada endereço IP:

https://wiki.mikrotik.com/wiki/Manual:IP/Firewall/NAT

# Script para CGNAT (Wiki Mikrotik)

```
:global sqrt do={
  :for i from=0 to=$1 do={
    :if (i * i > $1) do={ :return ($i - 1) }
  }
}

:global addNatRules do={
  /ip firewall nat add chain=srcnat action=jump jump-target=xxx \
    src-address="$($srcStart)-$($srcStart + $count - 1)"

  :local x [$sqrt $count]
  :local y $x
  :if ($x * $x = $count) do={ :set y ($x + 1) }
  :for i from=0 to=$x do={
    /ip firewall nat add chain=xxx action=jump jump-target="xxx-$($i)" \
      src-address="$($srcStart + ($x * $i))-$($srcStart + ($x * ($i + 1) - 1))"
  }
```

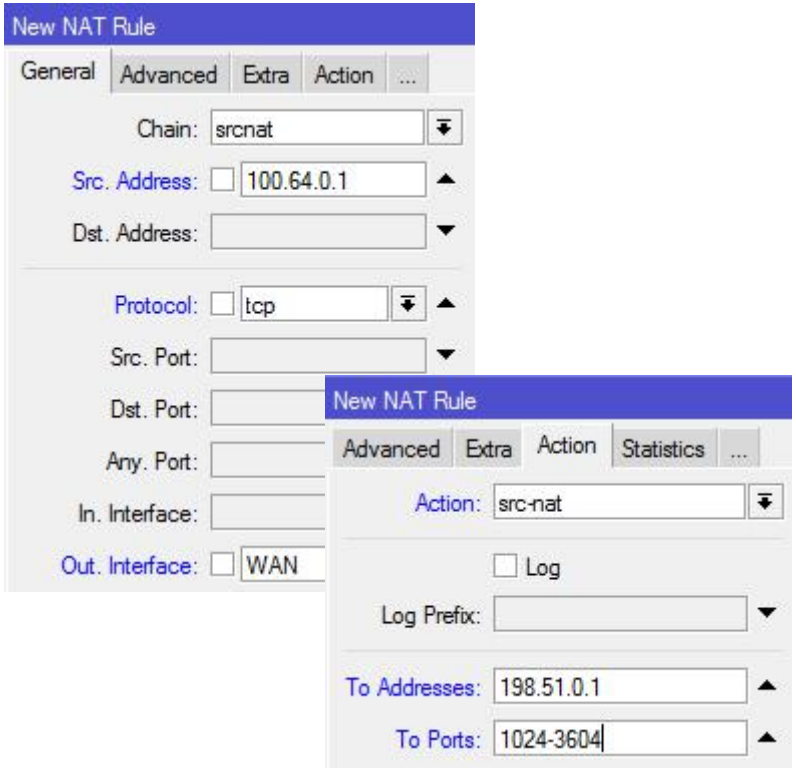
# Script para CGNAT

```
  :for i from=0 to=($count - 1) do={
    :local prange "$($portStart + ($i * $portsPerAddr))-$($portStart + (($i + 1) * $portsPerAddr) - 1)"
    /ip firewall nat add chain="xxx-$($i / $x)" action=src-nat protocol=tcp src-address=($srcStart + $i) \
     to-address=$toAddr to-ports=$prange
    /ip firewall nat add chain="xxx-$($i / $x)" action=src-nat protocol=udp src-address=($srcStart + $i) \
     to-address=$toAddr to-ports=$prange
  }
}
```

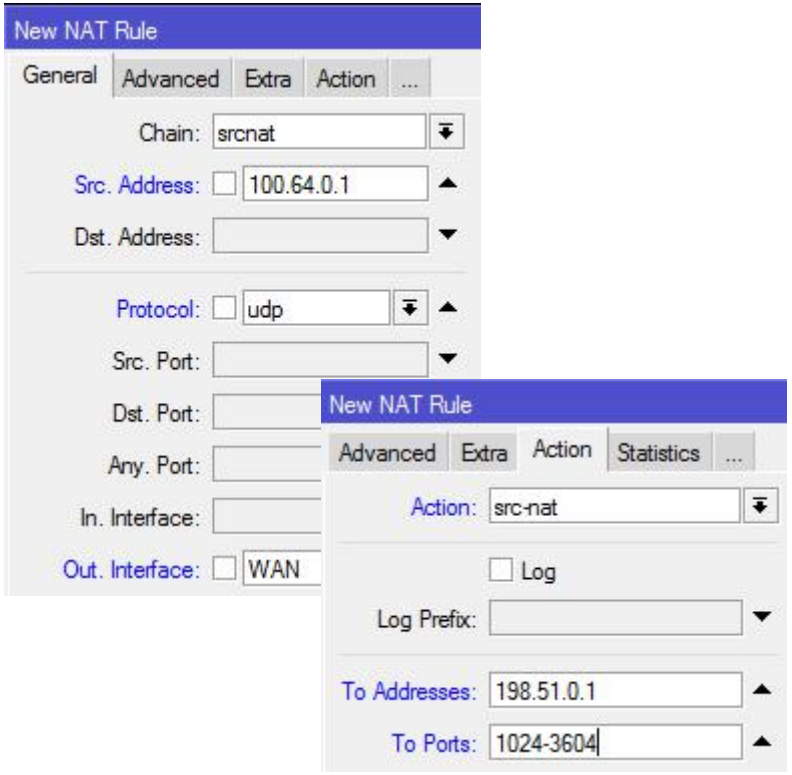
# CGNAT

Basicamente são criadas 3 regras de NAT por endereço IP:

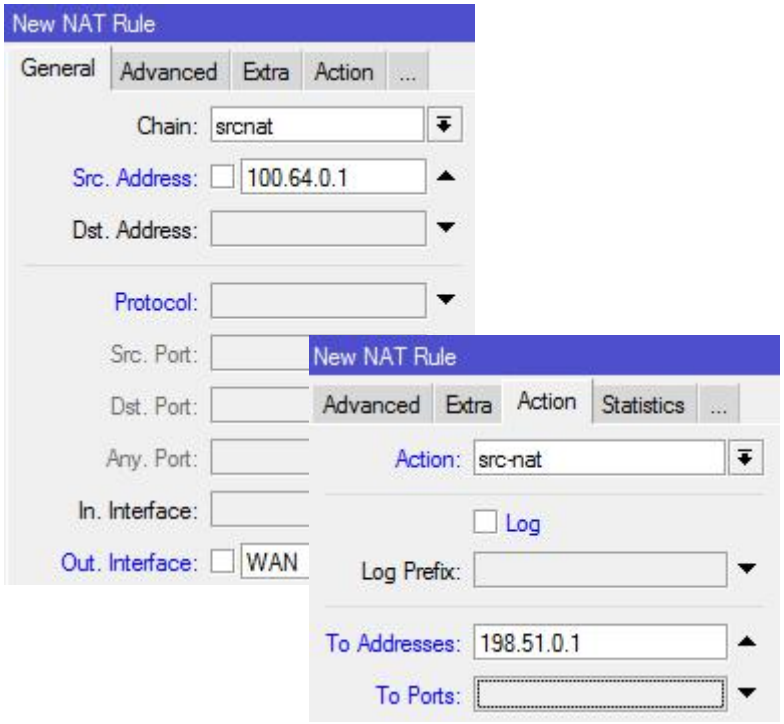
## Protocolo TCP




## Protocolo UDP



Outros protocolos (não orientados a porta)




**Para uma taxa de compartilhamento de 1:25, teremos um total de:**

**3 x 25 = 75K regras!**

# Implementando o CGNAT

Com essa implementação teríamos 3 x 25 x 100 = 75k regras!

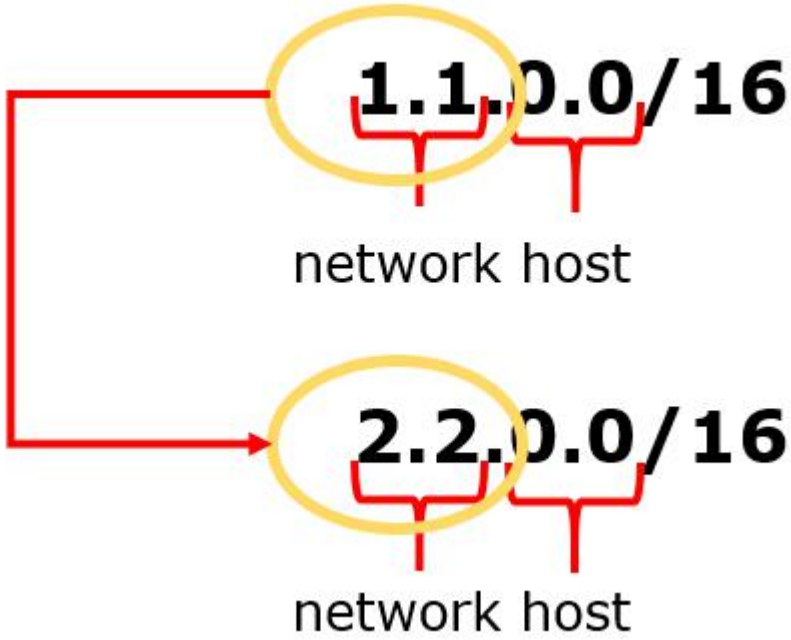
Felizmente, tanto Linux como RouterOS possuem uma funcionalidade que torna as coisas mais melhores: “netmap”

Netmap foi inicialmente implementado no iptables do Linux em um patch chamado “patch-o-matic”, que foi portado para o RouterOS.

# Como funciona o Netmap

# Como funciona o Netmap

Netmap é uma implementação de NAT de origem ou de destino no qual apenas a parte da rede de um IP é "nateada". A parte do host permanece intacta.Ex. mapear a rede 1.1.0.0/16 na 2.2.0.0/16



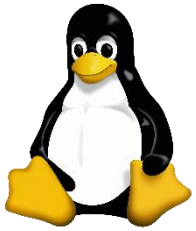

O endereço IP:
**1.1.X.Y**

será traduzido para:

**2.2.X.Y**

# Utilização de Netmap

**No Linux**



iptables -t nat -A POSTROUTING -s 1.1.1.0/24 -j NETMAP --to 2.2.2.0/24

**No RouterOS**

/ip firewall nat

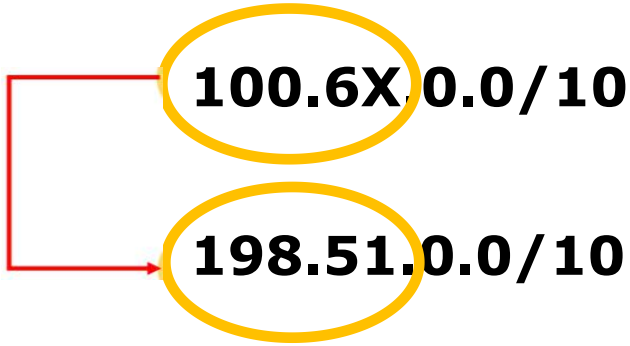
add action=netmap chain=srcnat protocol=udp src-address=1.1.1.0/24 to-addresses=2.2.2.0/24

add action=netmap chain=srcnat protocol=udp src-address=1.1.1.0/24 to-addresses=2.2.2.0/24

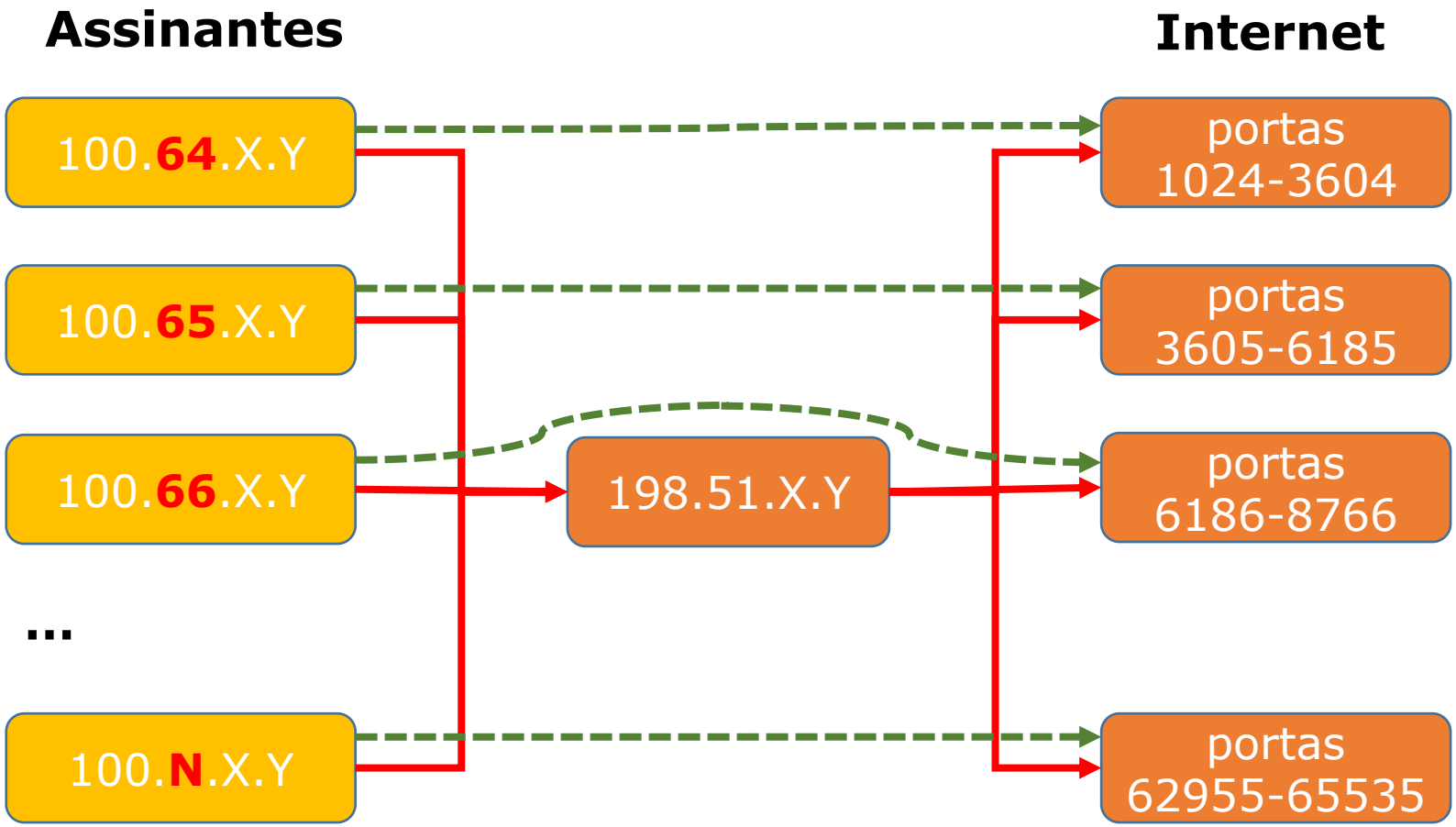
# Using Netmap

Netmap faz um NAT 1:1, onde a parte do host é mantido e apenas a parte de rede é modificada.

Em nosso caso iremos utilizar o seguinte esquema:

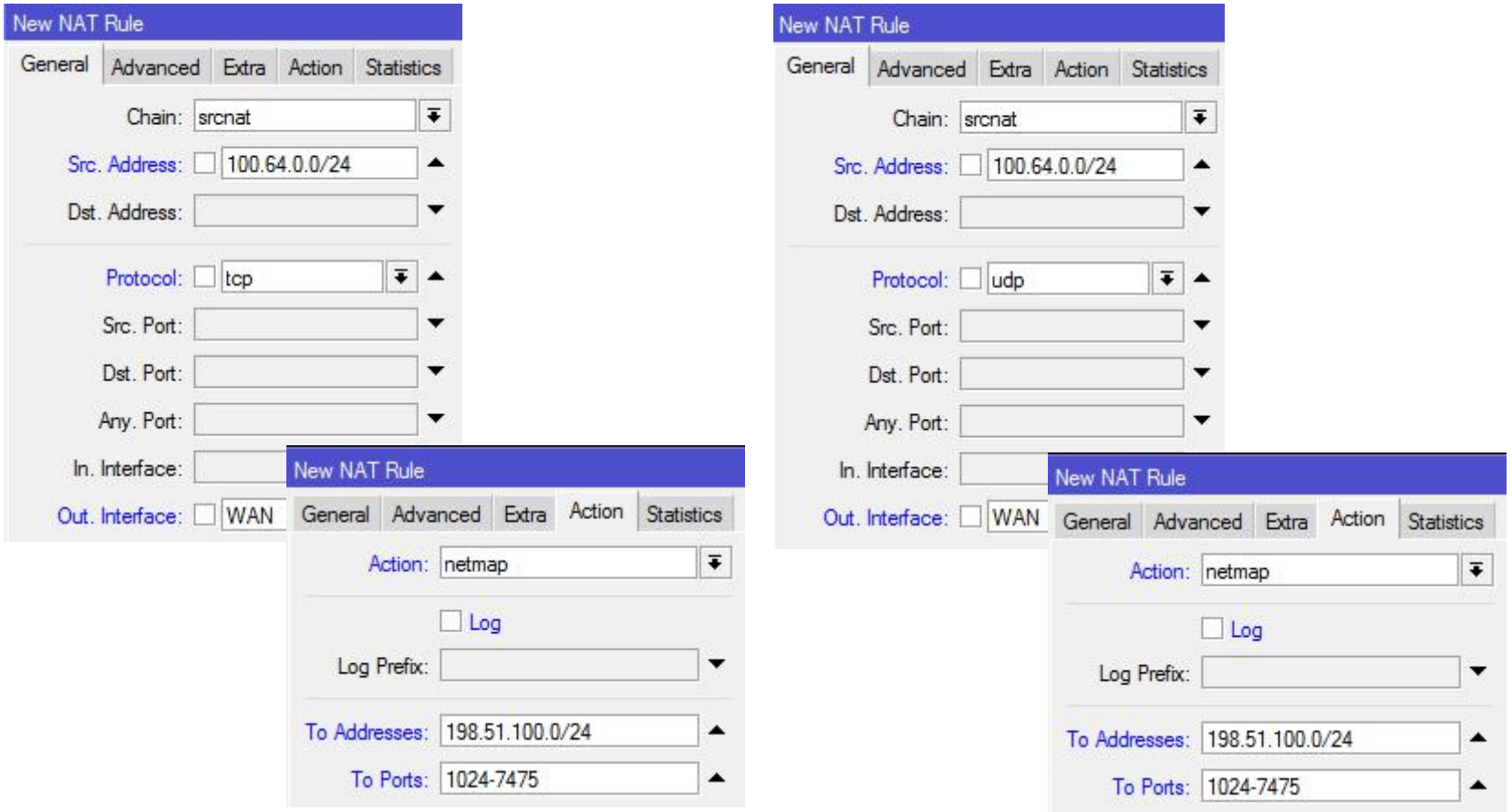


# Utilizando Netmap



# Utilizando Netmap

## Regras típicas de Netmap:



# Using Netmap

A quantidade de regras vai depender apenas da **taxa de compartilhamento.** Se temos uma taxa de 1:N, serão necessárias:

- N regras para TCP
- N regras para UDP
- 1 regra para protocolos não orientados a porta

Independentemente do tamanho da rede sempre serão:

**2N+1 regras!**

Nosso ISP hipotético teria 51 regras ao invés de 75K.

# Exemplo de implementação no RouterOS

# Utilização de Netmap

Utilizando uma taxa de compartilhamento mais "comportada" de 1:7

Teremos:

- 7 regras para TCP
- 7 regras para UDP e
- 1 regra para outros protocolos

- Total 15 regras.

Utilizaremos um esquema bem simples para tornar bem intuitiva a distribuição.

# Planejamento do CGNAT

**Prefixo "publico" alocado para o cliente:**

- 198.51.0.0/22* (198.51.0.0 – 198.51.3.255)

**Divisão de portas proposta**

1) 1024 - 9999 – (Faixa 0);
2) 10000 – 19999 – (Faixa 1);
3) 20000 – 29999 – (Faixa 2);
4) 30000 – 39999 – (Faixa 3);
5) 40000 – 49999 – (Faixa 4);
6) 50000 – 59999 – (Faixa 5);
7) 60000 – 65535 – (Faixa 6).

* O prefixo utilizado nesta apostila não é de fato uma das reservadas para documentação (RFC 5737).

# Planejamento do CGNAT

**Prefixo reservado para CGNAT (RFC 6598):**

- 100.64.0.0/10
- Range 100.64.0.0 – 100.127.255.255

**Divisão do range proposta:**

- 100.10**X.Y.Z** onde:

X = Faixa do Range de portas (0 a 6 no nosso caso)

Y = Terceiro octeto do IP público compartilhado

Z = Quarto octeto do IP público compartilhado

# CGNAT Planning

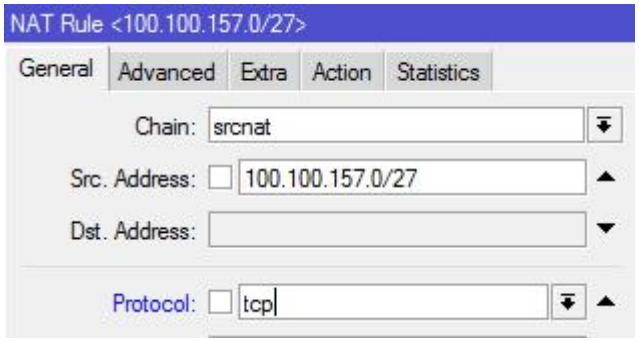
Supondo um POP com o range 198.51.2.64/27

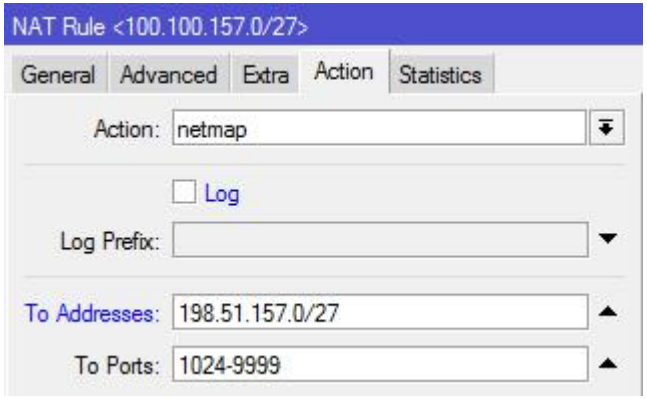
Por exemplo o IP 198.51.2.70 será compartilhado com 7 assinantes:

| Subscriber | CGNAT IP | Public IP | Port Range |
|---|---|---|---|
| subscriber 1 | 100.**100**.2.70 | 198.51.2.70 | **1024-9999** |
| subscriber 2 | 100.**101**.2.70 | 198.51.2.70 | **10000-19999** |
| subscriber 3 | 100.**102**.2.70 | 198.51.2.70 | **20000-29999** |
| subscriber 4 | 100.**103**.2.70 | 198.51.2.70 | **30000-39999** |
| subscriber 5 | 100.**104**.2.70 | 198.51.2.70 | **40000-49999** |
| subscriber 6 | 100.**105**.2.70 | 198.51.2.70 | **50000-59999** |
| subscriber 7 | 100.**106**.2.70 | 198.51.2.70 | **60000-69999** |

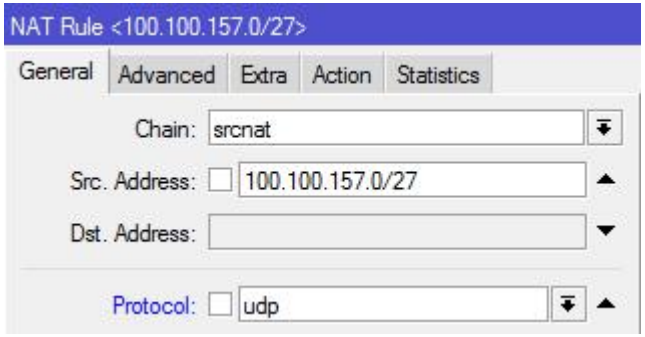
# Implementação no RouterOS

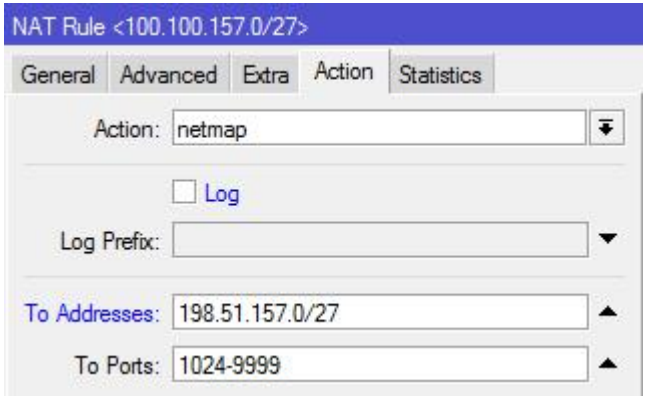
## TCP




## UDP



# Implementação no RouterOS

**Protocolo TCP**

/ip firewall nat

add action=netmap chain=srcnat out-interface=wlan1 protocol=tcp src-address=100.100.X.0/27 to-addresses=198.51.X.0/27 to-ports=1024-9999

add action=netmap chain=srcnat out-interface=wlan1 protocol=tcp src-address=100.101.X.0/27 to-addresses=198.51.X.0/27 to-ports=10000-19999

add action=netmap chain=srcnat out-interface=wlan1 protocol=tcp src-address=100.102.X.0/27 to-addresses=198.51.X.0/27 to-ports=20000-29999

add action=netmap chain=srcnat out-interface=wlan1 protocol=tcp src-address=100.103.X.0/27 to-addresses=198.51.X.0/27 to-ports=30000-39999

add action=netmap chain=srcnat out-interface=wlan1 protocol=tcp src-address=100.104.X.0/27 to-addresses=198.51.X.0/27 to-ports=40000-49999

add action=netmap chain=srcnat out-interface=wlan1 protocol=tcp src-address=100.105.X.0/27 to-addresses=198.51.X.0/27 to-ports=50000-59999

add action=netmap chain=srcnat out-interface=wlan1 protocol=tcp src-address=100.106.X.0/27 to-addresses=198.51.X.0/27 to-ports=60000-65535

# Implementação no RouterOS

**Protocolo UDP**

/ip firewall nat

add action=netmap chain=srcnat out-interface=wlan1 protocol=udp src-address=100.100.X.0/27 to-addresses=198.51.X.0/27 to-ports=1024-9999

add action=netmap chain=srcnat out-interface=wlan1 protocol=udp src-address=100.101.X.0/27 to-addresses=198.51.X.0/27 to-ports=10000-19999

add action=netmap chain=srcnat out-interface=wlan1 protocol=udp src-address=100.102.X.0/27 to-addresses=198.51.X.0/27 to-ports=20000-29999

add action=netmap chain=srcnat out-interface=wlan1 protocol=udp src-address=100.103.X.0/27 to-addresses=198.51.X.0/27 to-ports=30000-39999

add action=netmap chain=srcnat out-interface=wlan1 protocol=udp src-address=100.104.X.0/27 to-addresses=198.51.X.0/27 to-ports=40000-49999

add action=netmap chain=srcnat out-interface=wlan1 protocol=udp src-address=100.105.X.0/27 to-addresses=198.51.X.0/27 to-ports=50000-59999

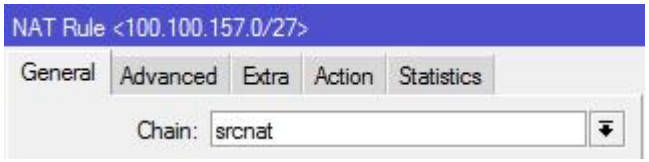
add action=netmap chain=srcnat out-interface=wlan1 protocol=udp src-address=100.106.X.0/27 to-addresses=198.51.X.0/27 to-ports=60000-65535

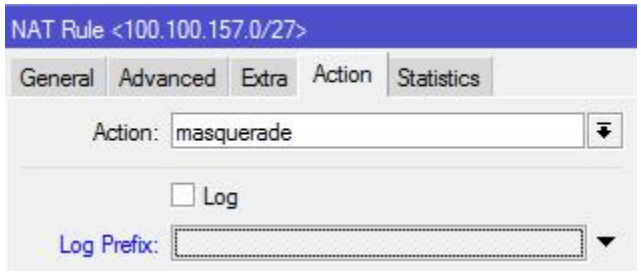
# Implementação no RouterOS

**Tráfego não orientado a portas**

/ip firewall nat

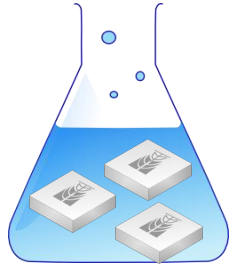
add action=masquerade src-address=100.100.X.0/27 chain=srcnat out-interface=wlan1



# CGNAT

1024 – 9999 – 100.100;
10000 – 19999 – 100.101;
20000 – 29999 – 100.102;
30000 – 39999 – 100.103;
40000 – 49999 – 100.104;
50000 – 59999 – 100.105;
60000 – 65535 – 100.106;

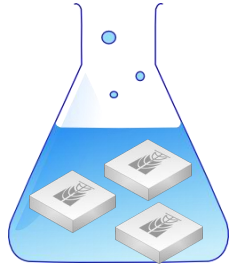


Com base no planejamento sugerido, identificamos facilmente o cliente que esteja por detrás do conjunto IP/porta:

- 198.51.2.145, porta 4045 -

# CGNAT

1024 – 9999 – 100.100;
10000 – 19999 – 100.101;
20000 – 29999 – 100.102;
30000 – 39999 – 100.103;
40000 – 49999 – 100.104;
50000 – 59999 – 100.105;
60000 – 65535 – 100.106;

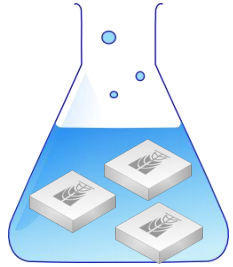


Com base no planejamento sugerido, identificamos facilmente o cliente que esteja por detrás do conjunto IP/porta:

- 198.51.2.145, porta 4045 - **100.100.2.145**

# CGNAT

1024 – 9999 – 100.100;
10000 – 19999 – 100.101;
20000 – 29999 – 100.102;
30000 – 39999 – 100.103;
40000 – 49999 – 100.104;
50000 – 59999 – 100.105;
60000 – 65535 – 100.106;

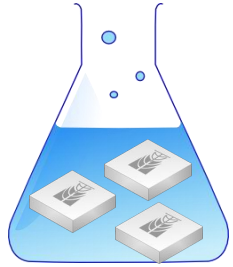


Com base no planejamento sugerido, identificamos facilmente o cliente que esteja por detrás do conjunto IP/porta:

- 198.51.2.145, porta 4045 - **100.100.2.145**
- 198.51.0.27, porta 50045 -

# CGNAT

1024 – 9999 – 100.100;
10000 – 19999 – 100.101;
20000 – 29999 – 100.102;
30000 – 39999 – 100.103;
40000 – 49999 – 100.104;
50000 – 59999 – 100.105;
60000 – 65535 – 100.106;

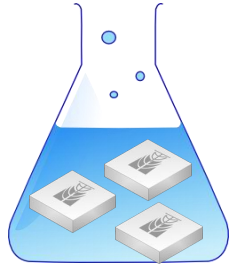


Com base no planejamento sugerido, identificamos facilmente o cliente que esteja por detrás do conjunto IP/porta:

- 198.51.2.145, porta 4045 - **100.100.2.145**
- 198.51.0.27, porta 50045 - **100.105.0.27**

# CGNAT

1024 – 9999 – 100.100;
10000 – 19999 – 100.101;
20000 – 29999 – 100.102;
30000 – 39999 – 100.103;
40000 – 49999 – 100.104;
50000 – 59999 – 100.105;
60000 – 65535 – 100.106;

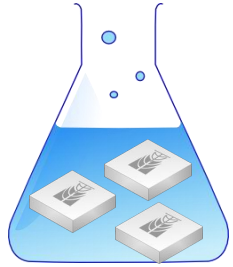


Com base no planejamento sugerido, identificamos facilmente o cliente que esteja por detrás do conjunto IP/porta:

- 198.51.2.145, porta 4045 - **100.100.2.145**
- 198.51.0.27, porta 50045 - **100.105.0.27**
- 198.51.3.66, porta 13016 -

# CGNAT

1024 – 9999 – 100.100;
10000 – 19999 – 100.101;
20000 – 29999 – 100.102;
30000 – 39999 – 100.103;
40000 – 49999 – 100.104;
50000 – 59999 – 100.105;
60000 – 65535 – 100.106;

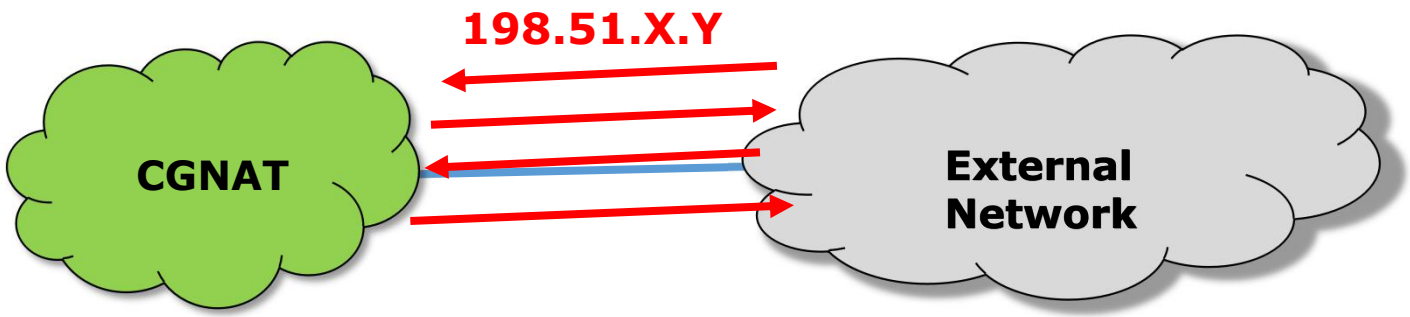


Com base no planejamento sugerido, identificamos facilmente o cliente que esteja por detrás do conjunto IP/porta:

- 198.51.2.145, porta 4045 - **100.100.2.145**
- 198.51.0.27, porta 50045 - **100.105.0.27**
- 198.51.3.66, porta 13016 - **100.101.3.66**

# Netmap e “loops estáticos”

Com essa implementação, qualquer pacote originado fora da rede e destinado para um IP público utilizado pelo CGNAT não terá rotas internas, causando um loop estático




Exemplo, um ping originado na Internet e destinado ao IP 198.51.X.Y chegará ao concentrador e será enviado de volta ao último roteador, que enviará para concentrador de novo, etc, etc.

# Netmap e “loops estáticos”

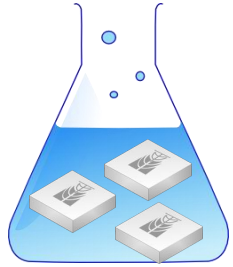
Soluções possíveis:

- Regra de dst-nat apontando para um IP configurado no concentrador ou para um IP de blackhole;

- Todos endereços IP públicos configurados em uma interface de loopback do concentrador;

- Simplesmente uma rota de blackhole para a grade inteira que estiver sendo roteada para o concentrador.

# Considerações sobre topologias de redes



Autenticações distribuídas:

- Regras de netmap nos concentradores

Autenticação concentrada:

- Regras de netmap no concentrador

Não importa a forma como você trabalha, a aplicação da técnica será a mesma.

# Redirecionamento de portas

Necessário mais um nível de direcionamento no CGNAT

Conjunto de regras pré definidas auxilia na administração.

Exemplo, os Usuários 100.64.X.Y e 100.65.X.Y querem direcionamento para porta 80

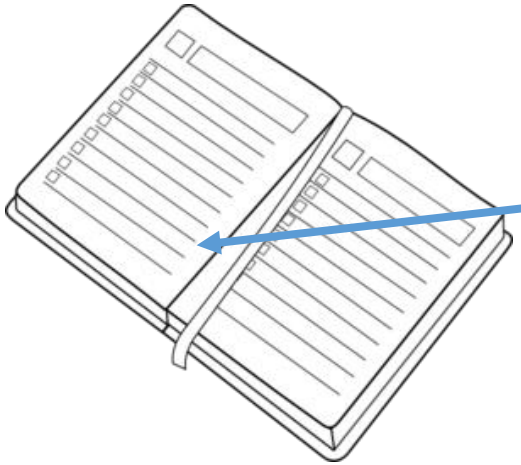
| IP/porta externa | IP do CGNAT | IP interno cliente |
|---|---|---|
| 198.51.X.Y:80**64** | 100.**64**.X.Y:80 | 192.168.1.180 |
| 198.51.X.Y:80**65** | 100.**65**.X.Y:80 | 192.168.1.180 |

Informar ao cliente

Pré configurar no CGNAT

Pré configurar na CPE

# Agenda



Introdução ✓

Administrando a escassêz do IPv4 ✓

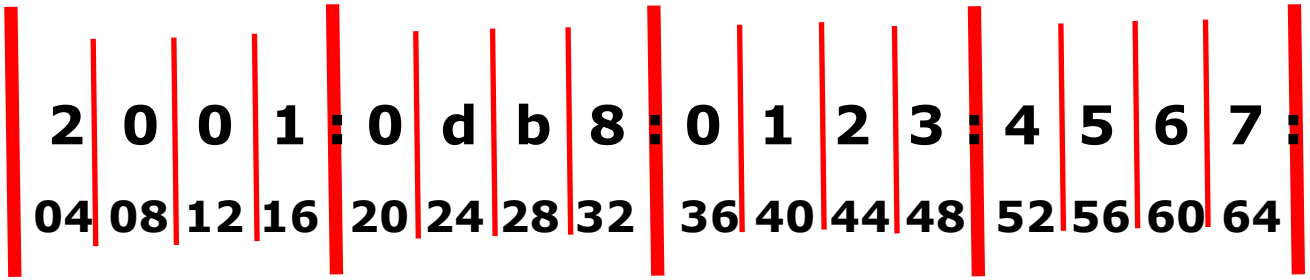
**Desfrutando da abundância do IPv6**

Impactos na segurança da rede

Planejamento da infraestrutura

Implementação com RouterOS

# Planejando o IPv6
# Considerações

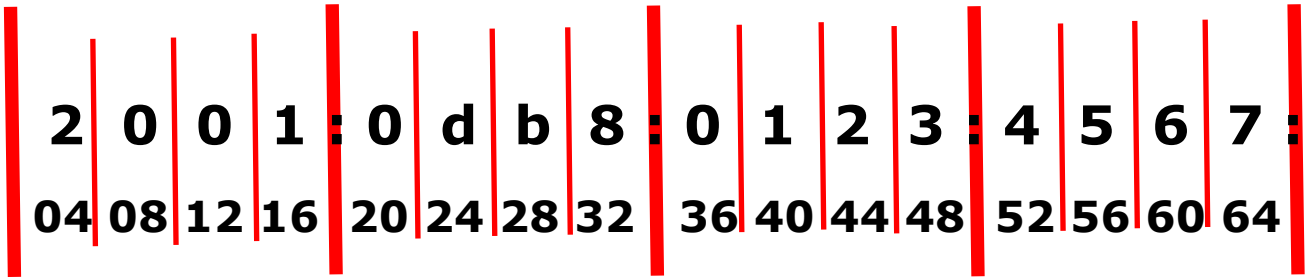



- Alocação mínima para ISPs é /32

- Maior Prefixo permitido anunciar no BGP é /48

- Alocação mínima para funcionamento do SLAAC é um /64

# Planejando o IPv6
# Considerações



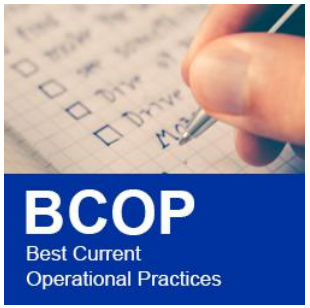

- Tamanho de prefixo recomendado para clientes (RFC6177):
  - /56 para clientes residenciais
  - /48 para clientes corporativos

/56 - 256 /64 sub redes

/48 - 65536 /64 sub redes

# Planejando o IPv6

RIPE BCOP (Doc. 690 – Outubro/2017) recomenda a alocação de /48 também para usuários domésticos!




/48 para todos?

Qual é a lógica do RIPE?

Esgotar o IPv6? 

# /48 para todos?

Por 10 anos a recomendação já foi de /48 para todos!

A RFC 3177 (2001), anterior à 6177 (2011) já preconizava o uso de /48 para usuários domésticos e residenciais:

*RFC3177*

*"….*

*In particular, we recommend:*

*- Home network subscribers, connecting through on-demand or always-on connections should receive a /48.*

*- Small and large enterprises should receive a /48.*

*- Very large subscribers could receive a /47 or slightly shorter prefix, or multiple /48's.*

*…"*

# /48 para todos?

Em 2011 A RFC 6177 revisou o entendimento, sem no entanto dar muitas razões para tanto:

*RFC6177*

*"….*

*While the /48 recommendation does simplify address space management for end sites, it has also been widely criticized as being wasteful*

*…*

*While it seems likely that the size of a typical home network will grow over the next few decades, it is hard to argue that home sites will make use of 65K subnets within the foreseeable future.*

*…"*

# /48 para todos?

Os operadores na região do RIPE retomam em 2017 a discussão, argumentando:

*"...*

*4.2.1. /48 for everybody*

*This is probably the most practical way to assign IPv6 prefixes to end customer CPE devices. In this case everyone has a /48 prefix and advanced end-users are less likely to make mistakes when addressing their networks and devices, resulting in much less call-centre time to sort out problems. It also has the advantage of sharing the same prefix size as ULAs and some transition mechanisms, so this facilitates a direct mapping of existing customer addressing plans to the delegated prefix.*

*..."*

# /48 para todos?

A BCOP 690 não "condena" a política da RFC6177, pontuando no entanto que tal diferenciação teriam razões muito mais comerciais que técnicas.

*"...*

*4.2.2. /48 for business customers and /56 for residential customers*

*Some operators decide to give a /48 prefix to their business customers and a /56 to their residential customers.* ***This rationale is understood to be mainly coming from sales and marketing departments where they wish to create some distinction in services between different types of customer.*** *This method can be considered as pragmatic, future-proof and has nearly no downsides, the same as the "/48 for everyone" approach.*

*..."*

# /48 para todos?

Em seguida aponta algumas razões para a preferência para o /48 para todos e alternativamente recomenda pelo menos a reserva de um /48

"...

An alternative is to reserve a /48 for residential customers, but actually assign them just the first /56. If subsequently required, they can then be upgraded to the required prefix size without the need to renumber, or the spare prefixes can be used for new customers if it is not possible to obtain a new allocation from your RIR (which should not happen according to current IPv6 policies)

..."

# Mas, meu bloco é suficiente para esse “desperdício” todo?

# Planejando a distribuição

Questões:

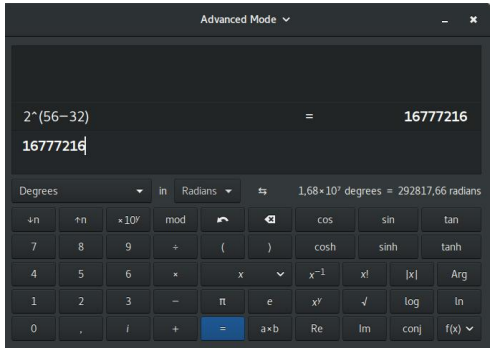
1) Quantos clientes /56 podemos alocar em um /32?

2) Quantos clientes /48 podemos alocar em um /32?

# Planejando a distribuição

Questões:

1) Quantos clientes /56 podemos alocar em um /32?



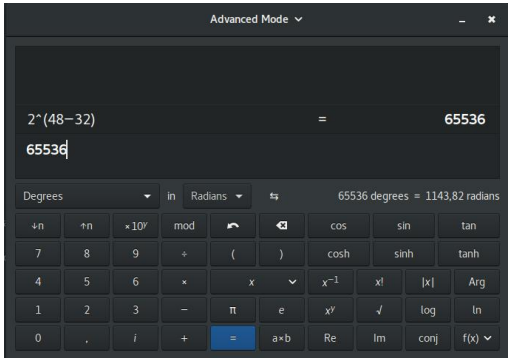

**2 ^ (56 – 32) = 16.777.216**

Um pouquinho mais de 16 milhões de clientes!

# Planejando a distribuição

Questões:

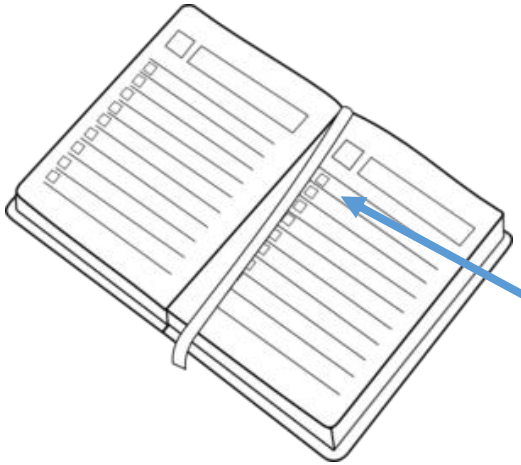
1) Quantos clientes /48 podemos alocar em um /32?




**2 ^ (48 – 32) = 65.536**

Satisfeito com 65 mil clientes?

# Agenda



- Introdução ✓
- Administrando a escassêz do IPv4 ✓
- Desfrutando da abundância do IPv6 ✓
- **Impactos na segurança da rede**
- Planejamento da infraestrutura
- Efetivando com RouterOS

# Impactos na segurança da rede

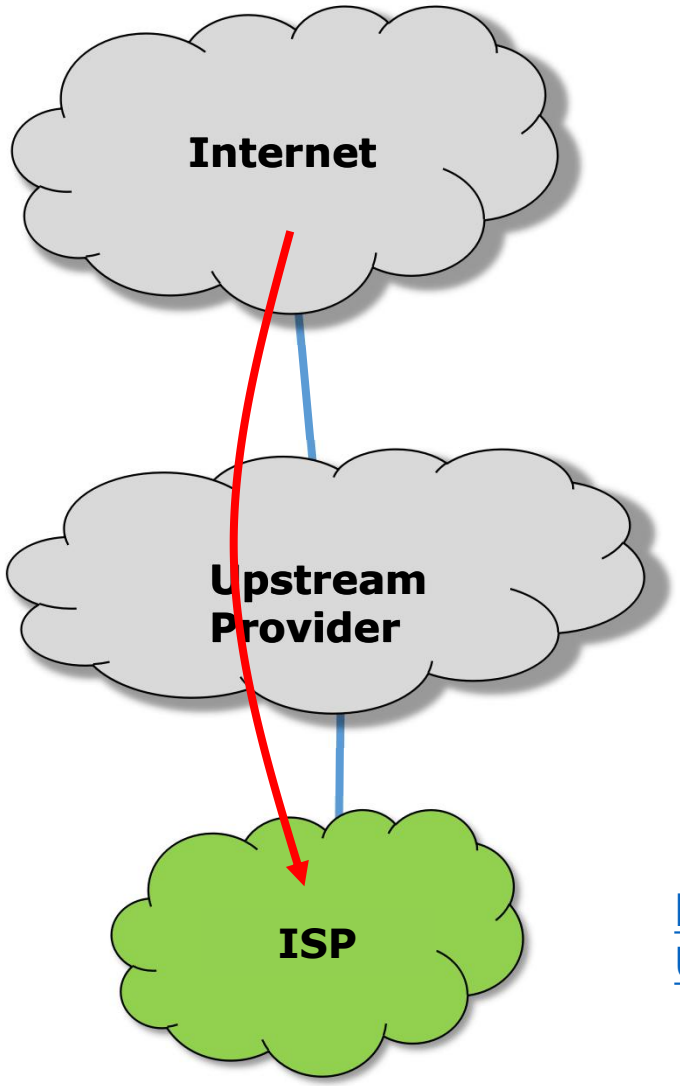
Uma outra boa razão não mencionada na BCOP 690 está relacionada à segurança.

Técnicas de mitigação de ataques DDoS volumétricos podem ser facilitadas e melhoradas no caso de:

RTBH – Blackhole disparada remotamente

Mitigação na nuvem por um provedor de mitigação

# RTBH em IPv4

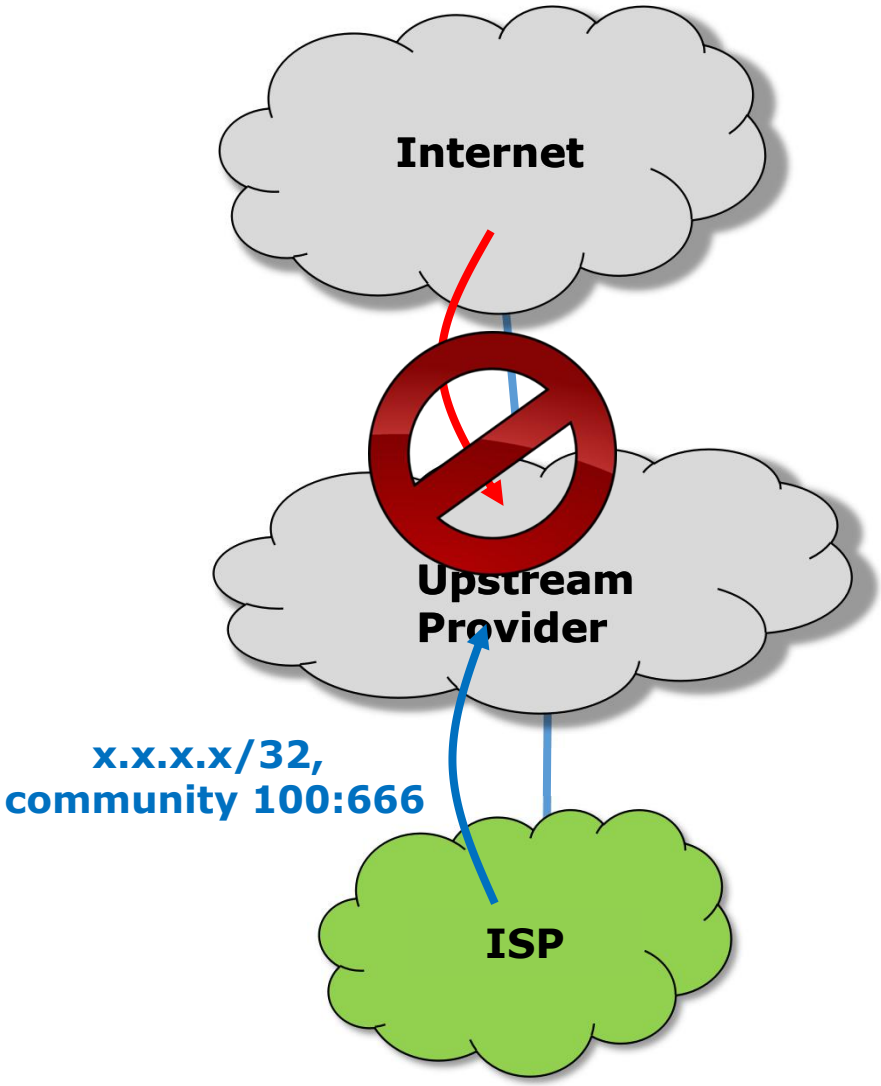



O ISP está sofrendo um ataque volumétrico destinado a um determinado IPv4 /32;

O provedor de Upstream possui política de communities que coloca em blackhole um IP /32 quando anunciado com a community ex. 100:666);

http://mum.mikrotik.com/presentations/EU16/presentation_2960_1456752556.pdf

# RTBH em IPv4

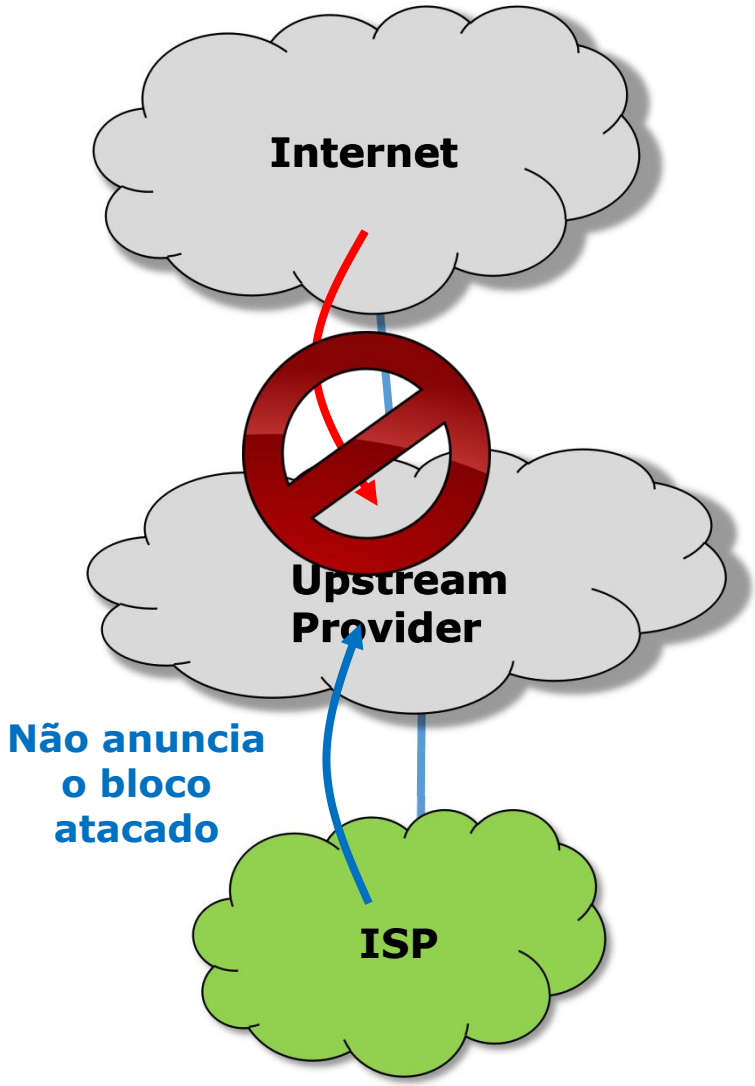



O ISP anuncia o /32 com a community 100:6666 em questão;

O provedor de Upstream coloca o IP /32 em blackhole;

A comunicação do mundo externo com o IP /32 é perdida e o ataque volumétrico cessa;

# RTBH em IPv6

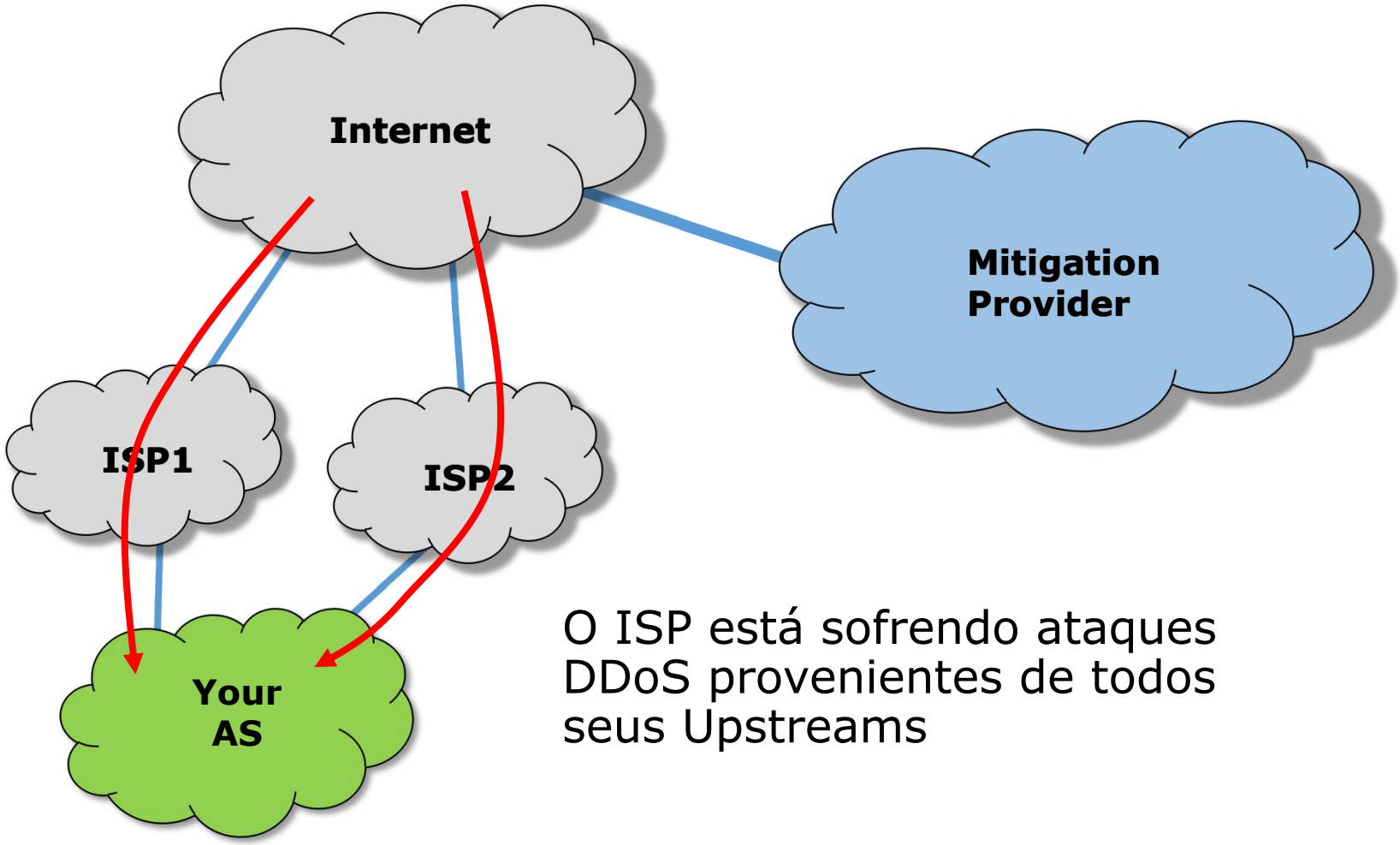



A mesma técnica pode funcionar com o IPv6. A diferença é que quando se trata do IPv4 o upstream necessariamente tem de ter a política de community.

Se O ISP distribui IPv6 /48, ele simplesmente parte os anúncios em vários e **não anuncia o bloco atacado.**

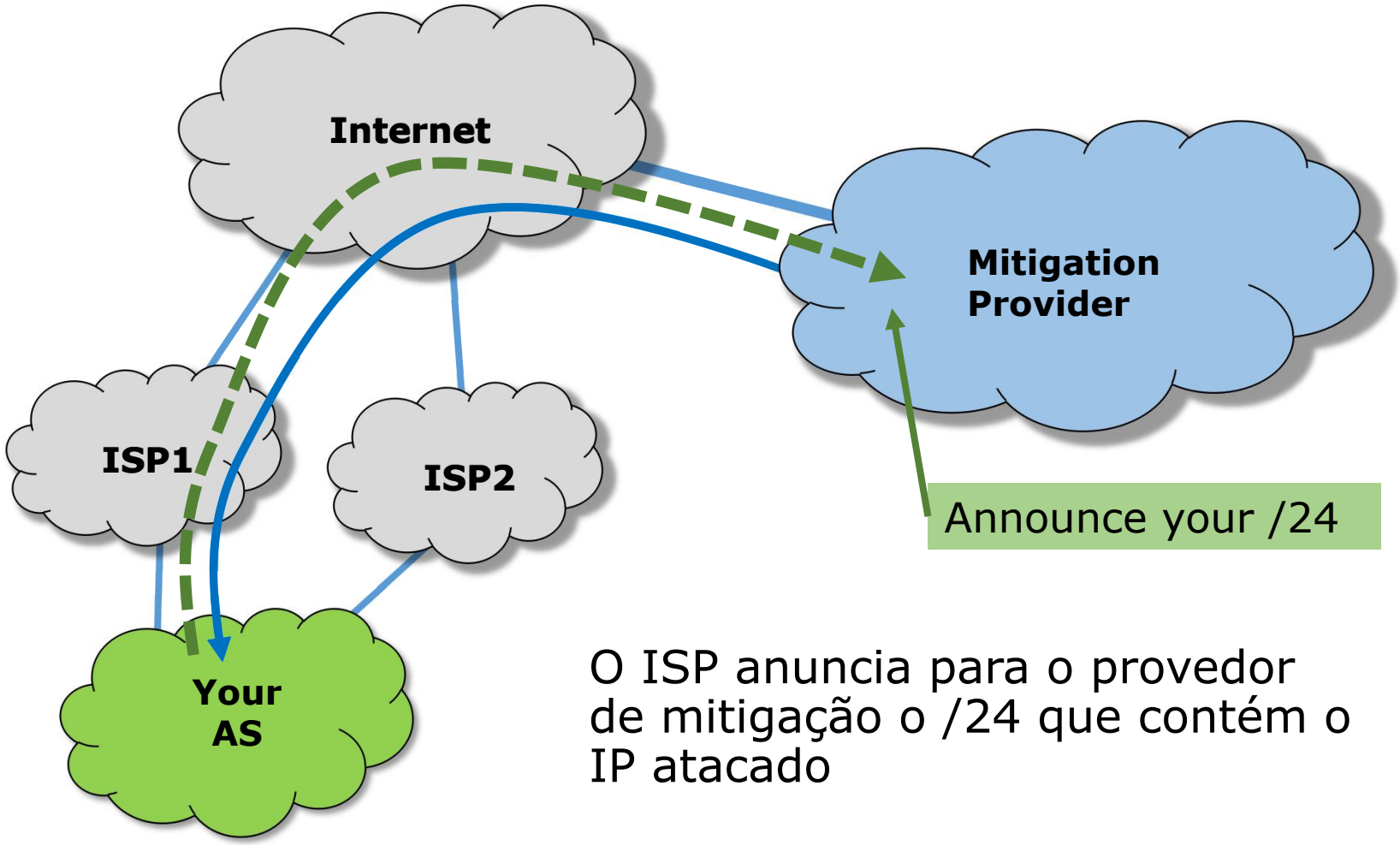
O ataque cessará independentemente da ação do Usptream!

# Mitigação na nuvem em IPv4



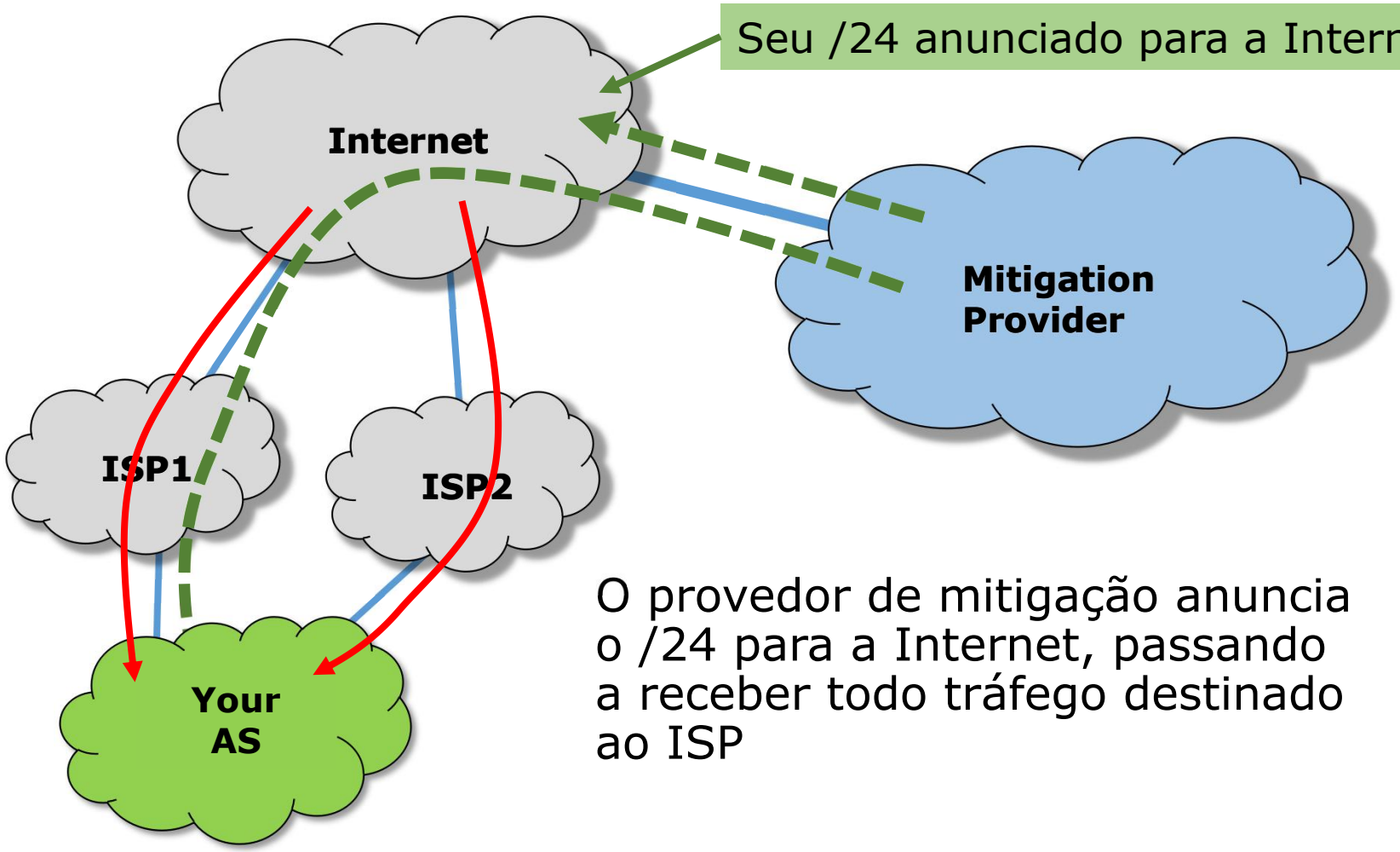

O ISP está sofrendo ataques DDoS provenientes de todos seus Upstreams

# Mitigação na nuvem em IPv4



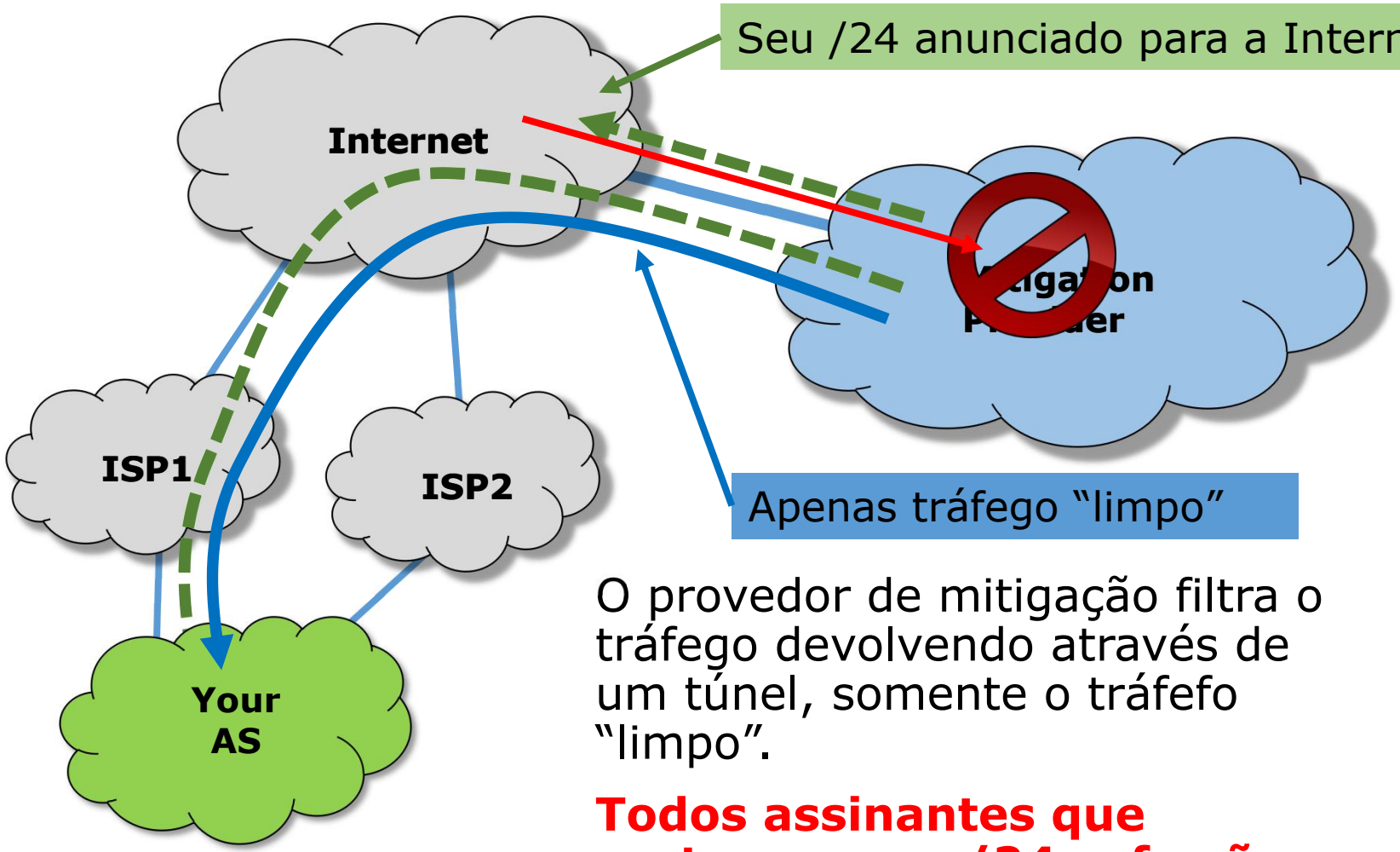

O ISP anuncia para o provedor de mitigação o /24 que contém o IP atacado

# Mitigação na nuvem em IPv4




O provedor de mitigação anuncia o /24 para a Internet, passando a receber todo tráfego destinado ao ISP

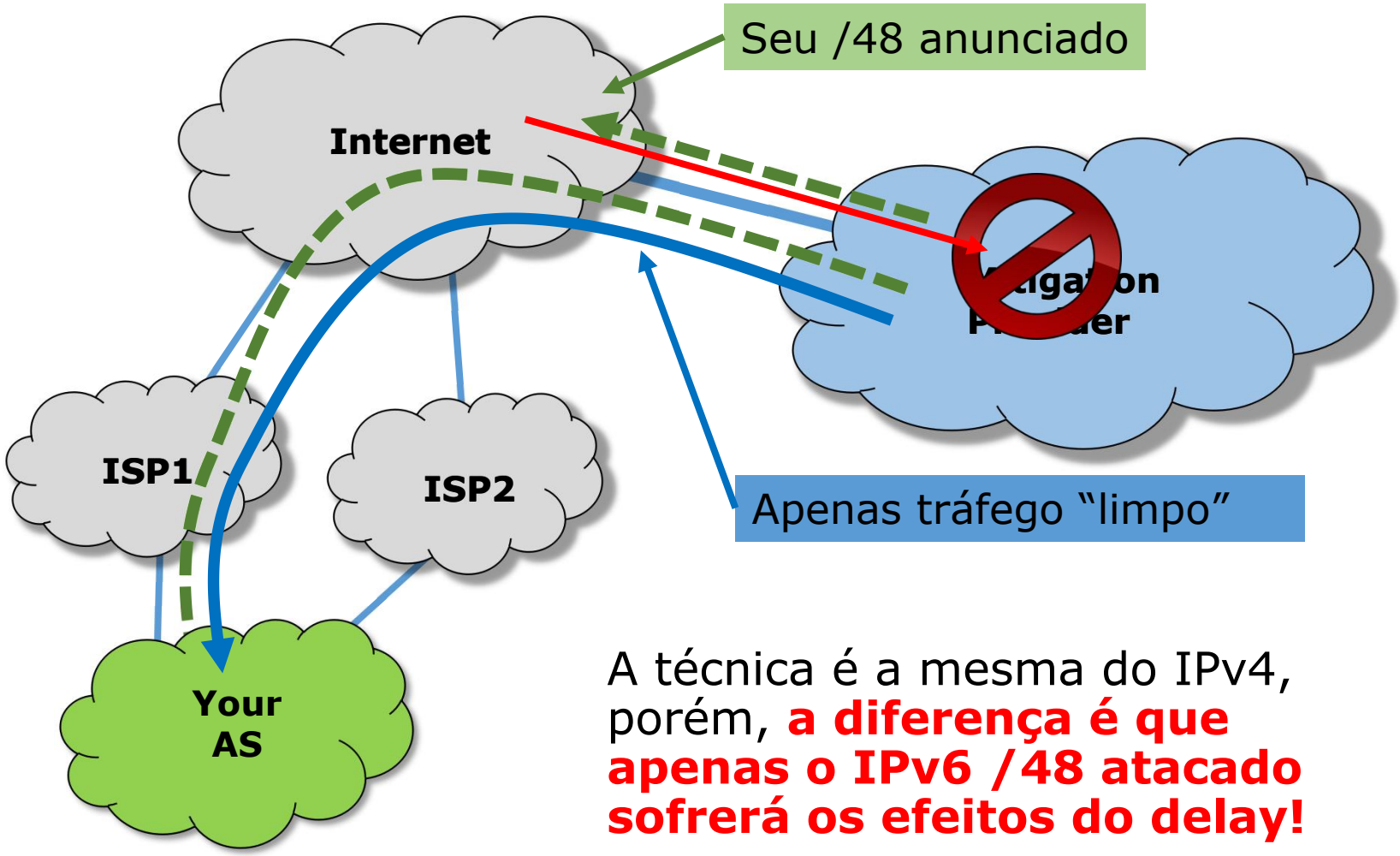
# Mitigação na nuvem em IPv4




O provedor de mitigação filtra o tráfego devolvendo através de um túnel, somente o tráfefo “limpo”.

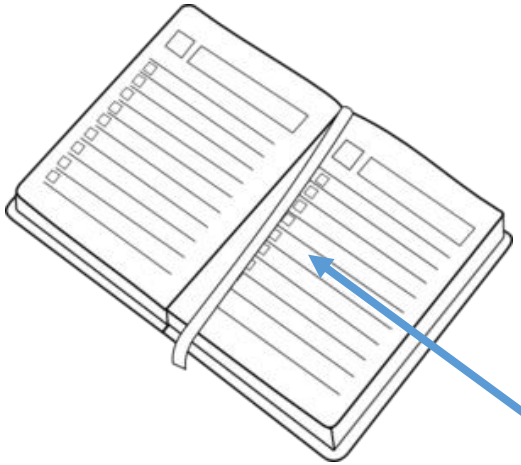
**Todos assinantes que pertencem ao /24 sofrerão um delay natural do túnel.**

# Mitigação na nuvem em IPv6




A técnica é a mesma do IPv4, porém, **a diferença é que apenas o IPv6 /48 atacado sofrerá os efeitos do delay!**

# Agenda



Introdução ✓

Administrando a escassêz do IPv4 ✓

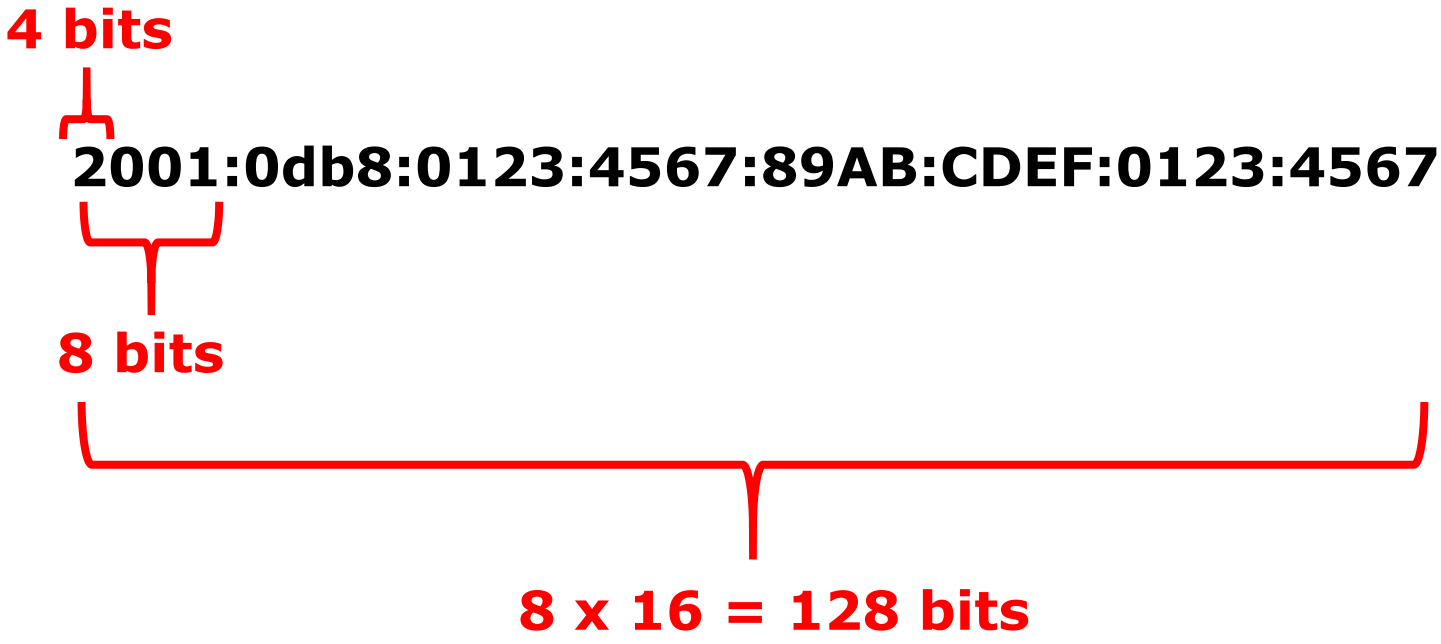
Desfrutando da abundância do IPv6 ✓

Impactos na segurança da rede ✓

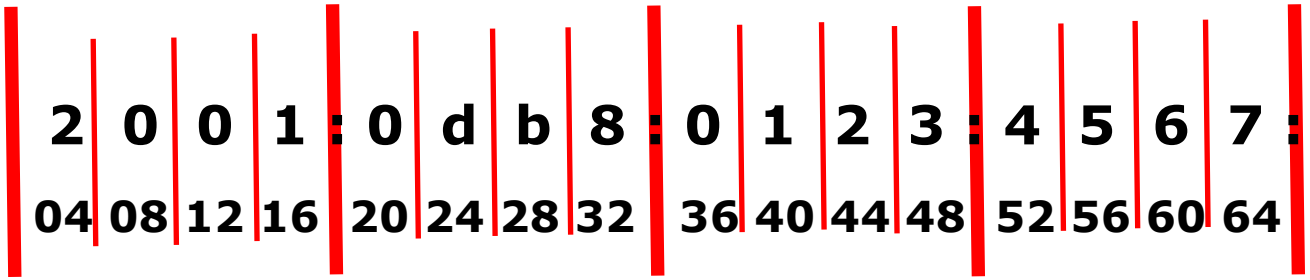
**Planejamento da infraestrutura**

Implementação com RouterOS

# Anatomia do IPv6



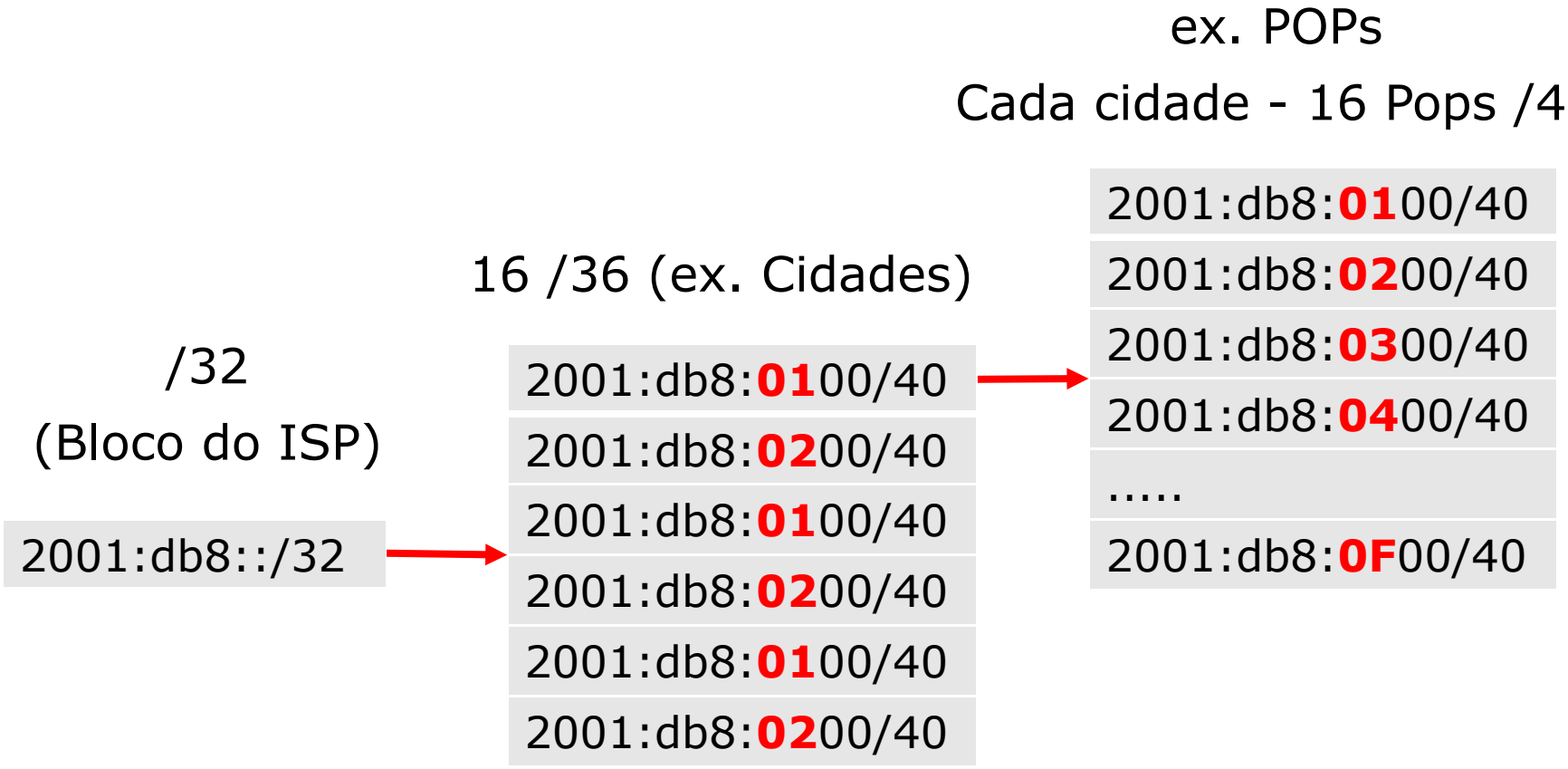
# Planejamento




Considerando a “anatomia” do IPv6, é interessante planejar a distribuição com saltos de 4 bits.

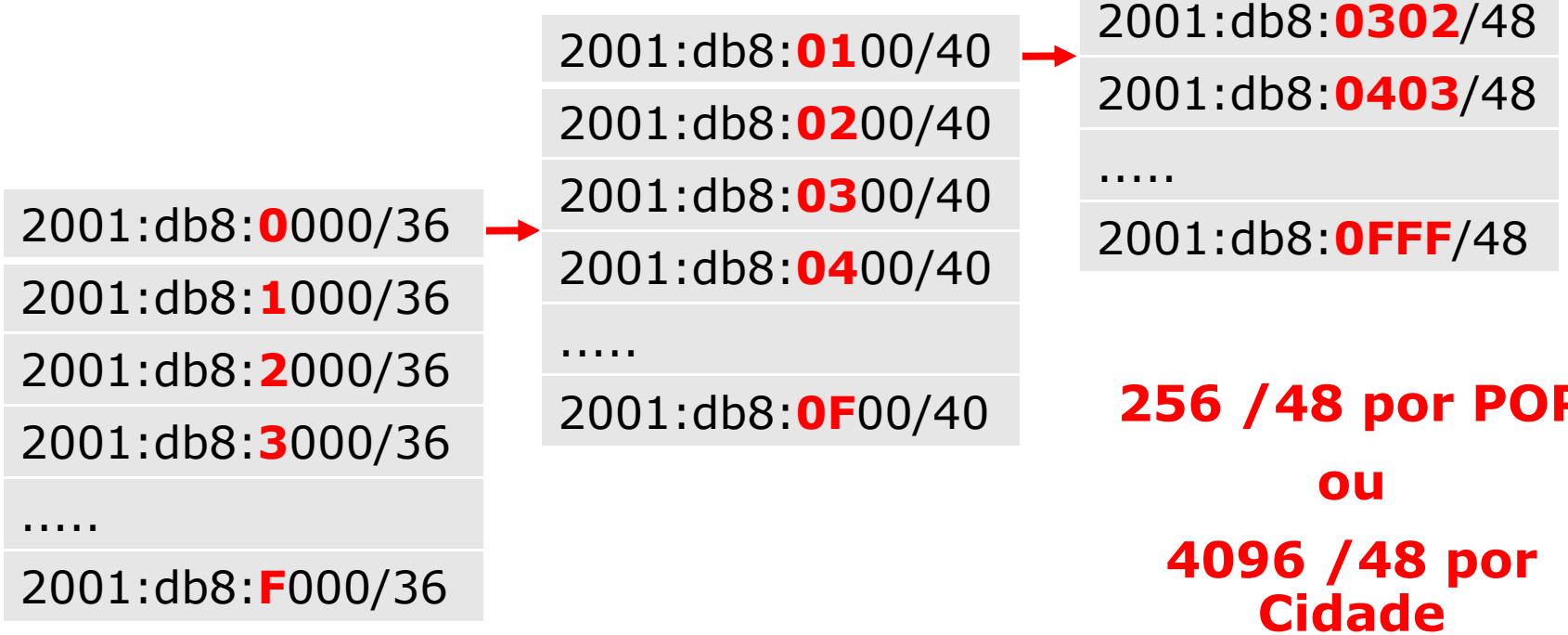
Isso tornará nossa distribuição mais “limpa”, fácil de entender e evitar futuras confusões

# Planejamento



# Planejamento

A alocação de /48 para todos irá tornar o planejamento muito mais simples e de fácil entendimento



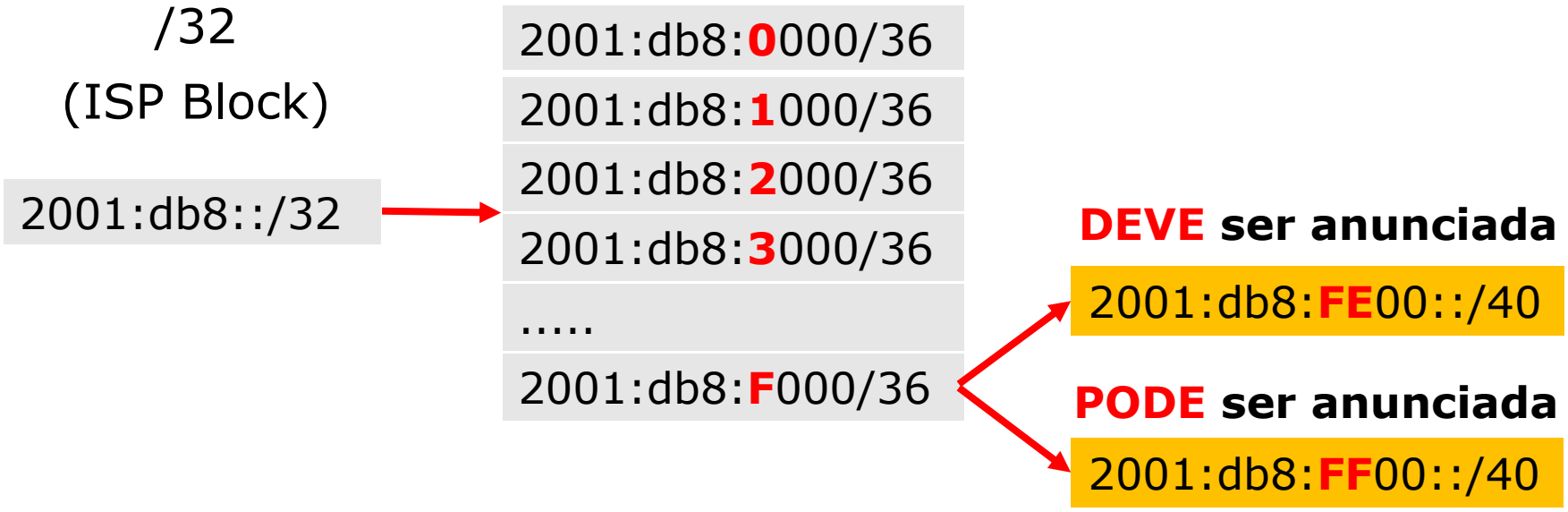

**256 /48 por POP**

**ou**

**4096 /48 por Cidade**

# Planejamento
# Endereços de Infraestrutura

Considere reservar uma parte do último /36 para infraestrutura e dividir em partes que necessariamente devem ser anunciadas e aquelas que não necessáriamente precisam ser anuciadas



# Continuando BCOP 690

# Endereços Fixos ou Dinâmicos?

# Endereços dinâmicos ou persistentes?

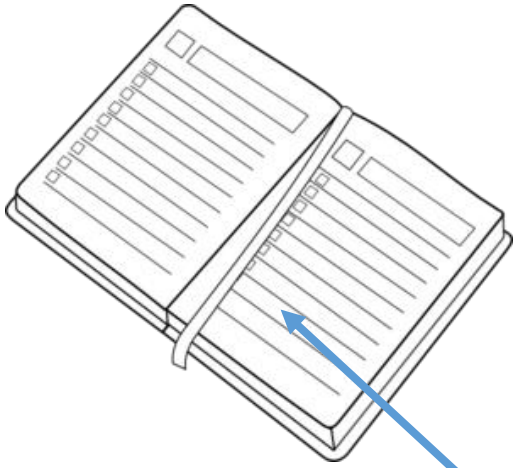
Alguns problemas relacionados a endereços dinâmicos:

- Logs / accounting para rastreamento;
- Problemas relacionados a serviços em clientes
- Problemas relacionados a queda de energia

Recomendação da BCOP 690:

- Usar endereços fixos (permanentes)
- Se, por alguma razão (comercial por exemplo) não quiser dar fixo, configurar um grande lifetime para a conexão;

# Agenda

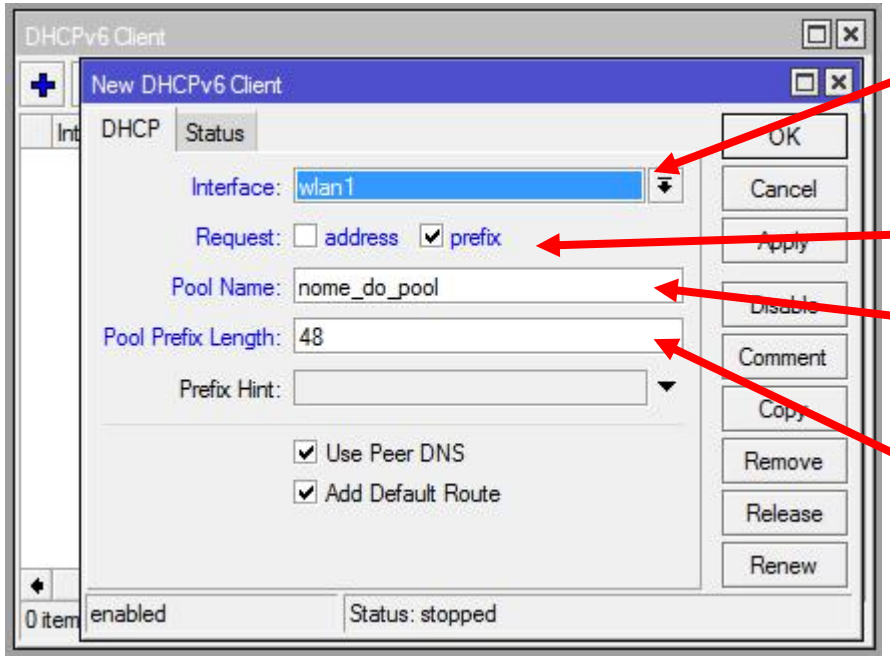


- Introdução ✓
- Administrando a escassêz do IPv4 ✓
- Desfrutando da abundância do IPv6 ✓
- Impactos na segurança da rede ✓
- Planejamento da infraestrutura ✓
- **Implementação com RouterOS**

# Suporte a PPP and DHCPv6 no RouterOS

# Cliente DHCPv6

O cliente DHCPv6 PD obtém prefixos de um servidor DHCPv6 PD, e pode subdividi-lo entre os clientes inserindo uma rota para o servidor DHCPv6.




Interface onde o cliente vai rodar

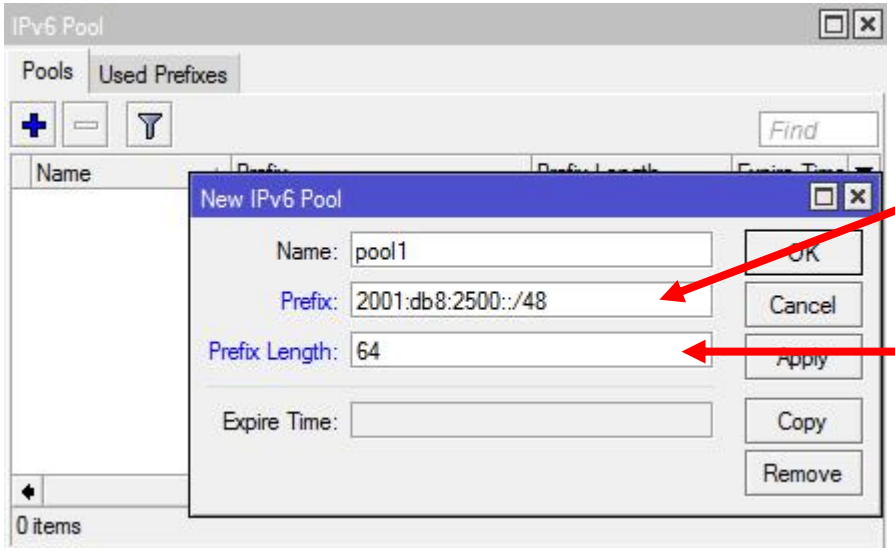
Para requisitar um prefixo

Pool interno que irá ser criado

Tamanho do prefixo

# IPv6 Pool

O pool IPv6 define uma faixa de endereços para uso futuro que estará disponível para SLAAC, DHCPv6 e servidores PPP




Prefixo alocado ao roteador

Bitmask para repartir o prefixo Ex. para SLAAC

# Suporte ao PPP

Alocação dinâmica (não recomendada)

Configurando um pool no concentrador e distribuindo os prefixos via PPP;

Como não há suporte a accounting, para a rastreabilidade é necessário alguma técnica adicional, com um script “on-logon” and “on-logout” e o envio a um servidor de Logs remoto;

# Suporte a PPP
# Distribuição Persistente

Para a distribuição de IPv6 em caráter fixo (persistente) através de RADIUS vários fabricantes suportam atributo "Delegated-IPv6-Prefix"

Até a data da elaboração deste trabalho não há suporte no RouterOS para o atributo "Delegated-IPv6-Prefix" para PPP.

Thread aberta no Forum da Mikrotik em 2014 e até hoje com pedidos de solução:

https://forum.mikrotik.com/viewtopic.php?t=89443

# Suporte a PPP
# Distribuição persistente

É possível porém fazer uma distribuição em caráter persistente, utilizando o RouterOS + RADIUS, com alguns “ajustes”

- O RouterOS suporta o atributo proprietário “Mikrotik-Delegated-IPv6-Pool”, que é uma string que pode ser associada ao cliente

- Torna-se necessário o pré cadastro de todos os pools para todos clientes em todos os concentradores

- Uma vez que um cliente se conecte via PPP, o RADIUS enviará a string correspondente àquele cliente e, havendo o prefixo cadastrado com aquela string será atribuída ao cliente.

# Conclusões

# Conclusões

As técnicas para CGNAT com baixo custo e boa performance aqui abordadas podem desempenhar um papel importante nessa fase de transição. Entretanto CGNAT não é algo sustentável a longo prazo. Lembre-se que as portas também são finitas!

IPv6 é totalmente diferente de IPv4 e por isso não devemos usar os mesmo conceitos e paradigmas de planejamento. Devemos “aproveitar” da abundancia do IPv6

Para aqueles que ainda não iniciaram a implementação de IPv6, não esperem os “45’ do segundo tempo”. Já estamos no segundo tempo da prorrogação.

# Leitura mínima recomendada para quem vai implementar

# Referencias

**BCOP 690**

Best Current Operational Practice for Operators: IPv6 prefix assignment for end-users - persistent vs non-persistent, and what size to choose

https://www.ripe.net/publications/docs/ripe-690

**BCOP 631**

IPv6 Troubleshooting for Residential ISP Helpdesks

https://www.ripe.net/publications/docs/ripe-631

# Obrigado!