Capacitação IPv6.br

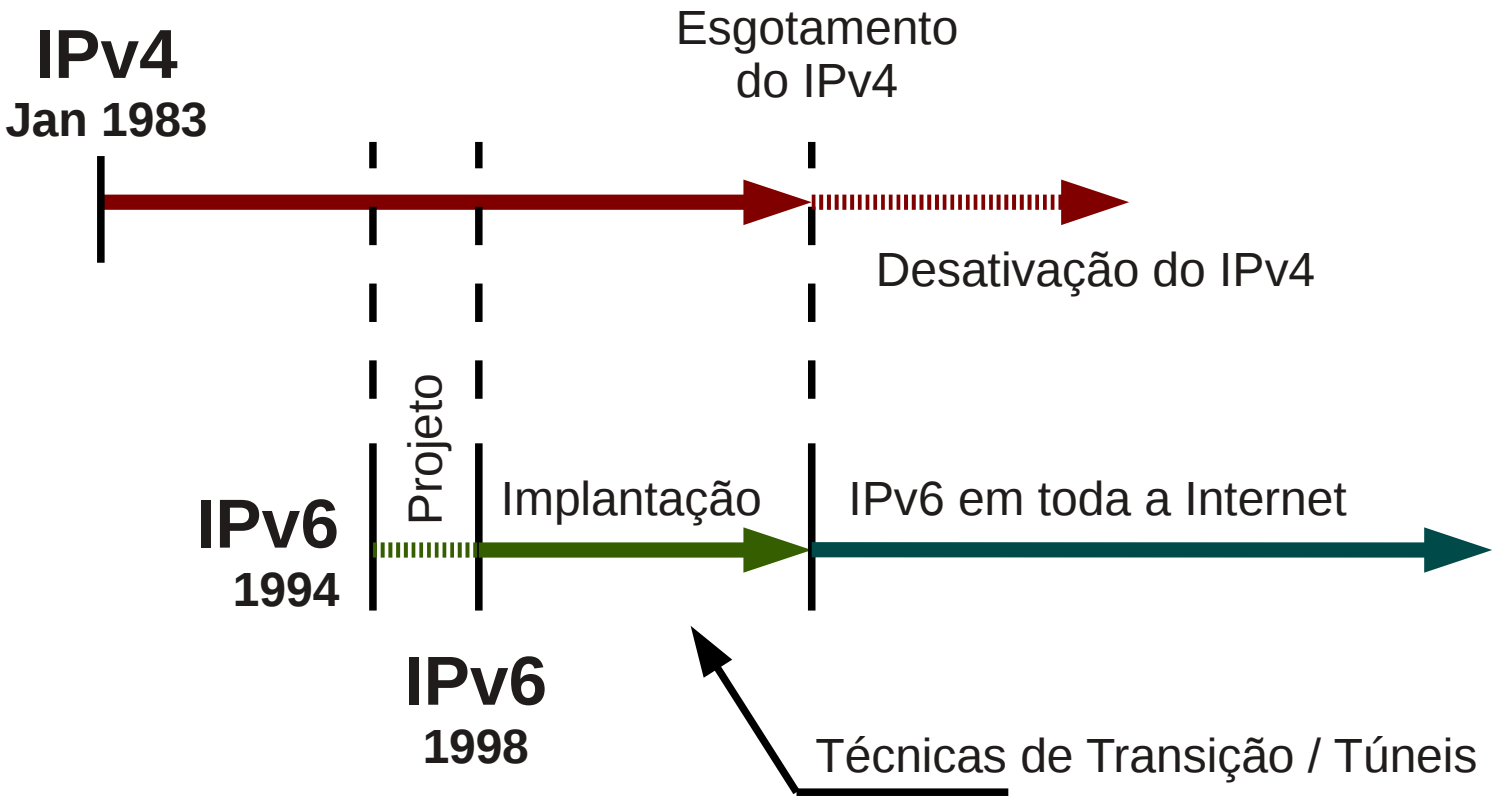
Técnicas de Transição

Agenda

- Introdução
- Classificação das Técnicas
- Pilha Dupla
- 6in4 e 6over4
- GRE
- Tunnel Brokers
- DS-Lite e DS-Lite + A+P
- IVI, dIVI e dIVI-pd
- NAT64 e DNS64
- 464XLAT
- 4rd
- 6PE e 6VPE
- 6rd
- 6to4
- Teredo
- ISATAP
- A+P
- NAT444
- Considerações Finais

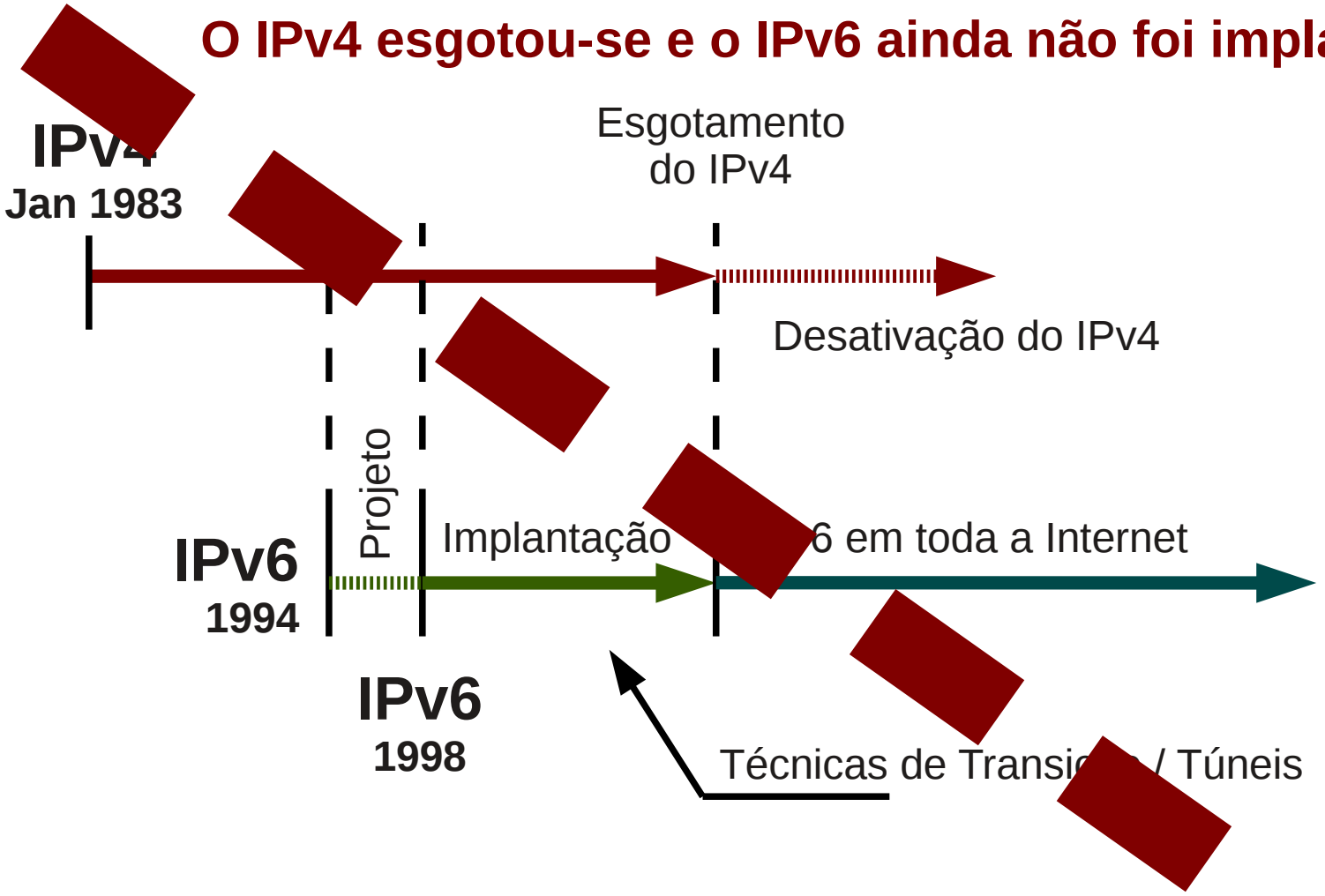
Introdução

Introdução

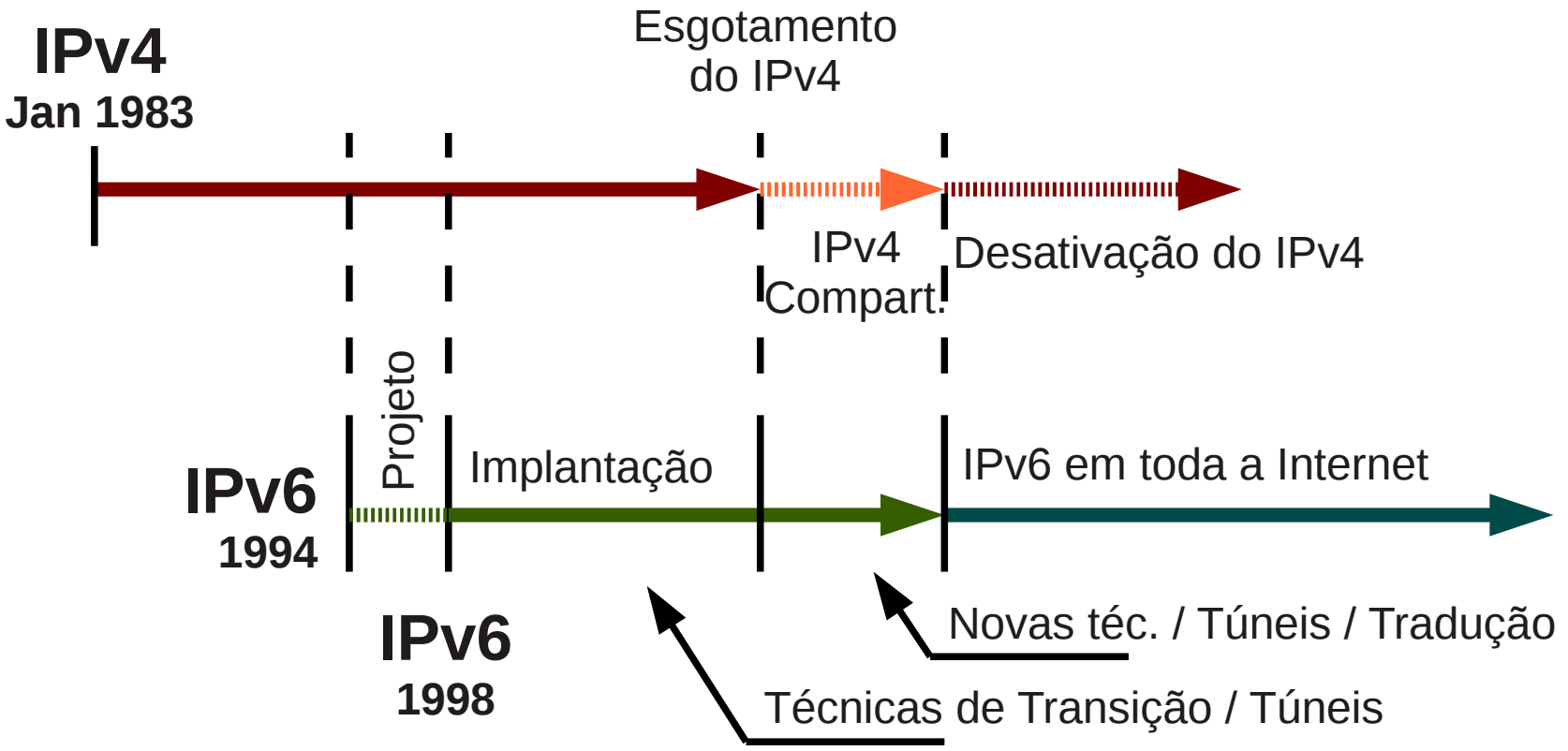

IPv4
Jan 1983
Esgotamento
do IPv4
Desativação do IPv4
IPv6
1994
Projeto
Implantação
IPv6 em toda a Internet
IPv6
1998
Técnicas de Transição / Túneis

Introdução

Isso não aconteceu assim
O IPv4 esgotou-se e o IPv6 ainda não foi implantado



Introdução

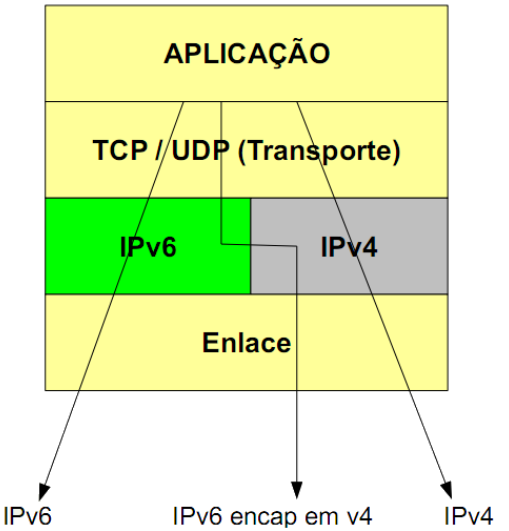


E agora, como proceder?

- IPv6 é necessário
- IPv4 não pode ser descartado agora
- Como implementar os dois em curto prazo?

Pilha Dupla

- IPv6 + IPv4 em todos os nós
- Se a consulta DNS retorna:
  - **A**: a aplicação usa IPv4
  - **AAAA**: a aplicação usa IPv6
  - **AAAA** e **A**: a aplicação tenta primeiro o IPv6, se falhar, tenta o IPv4
  - **AAAA** e **A**: a aplicação com **happy eyeballs** tenta IPv6 e IPv4 simultaneamente, o mais rápido é usado

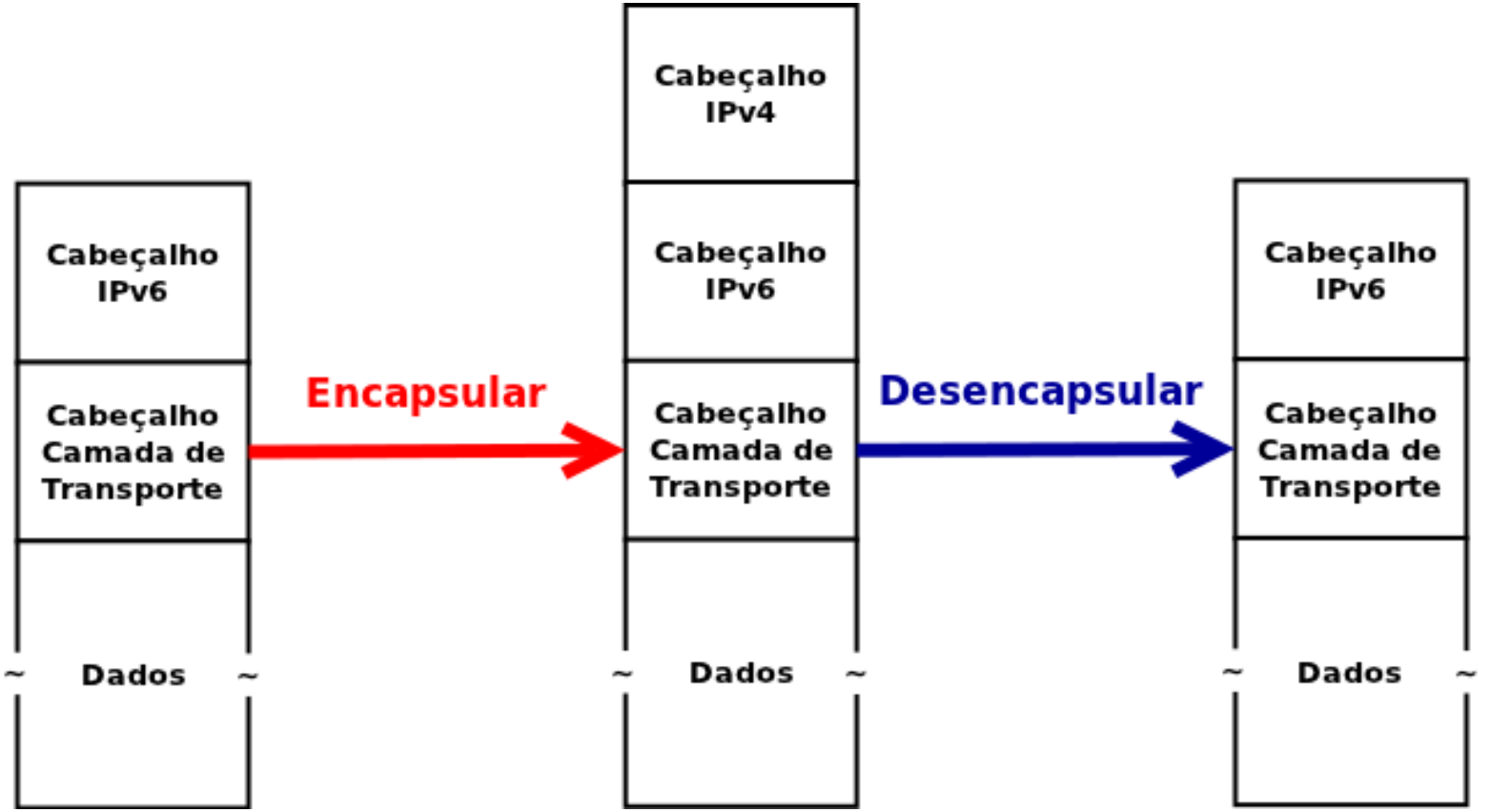


- Tenho IPv6
- Computador destino na Internet tem IPv6
- Mas meu provedor somente oferece IPv4
- Como eu consigo fazer esta comunicação em IPv6?

Utilizar túneis

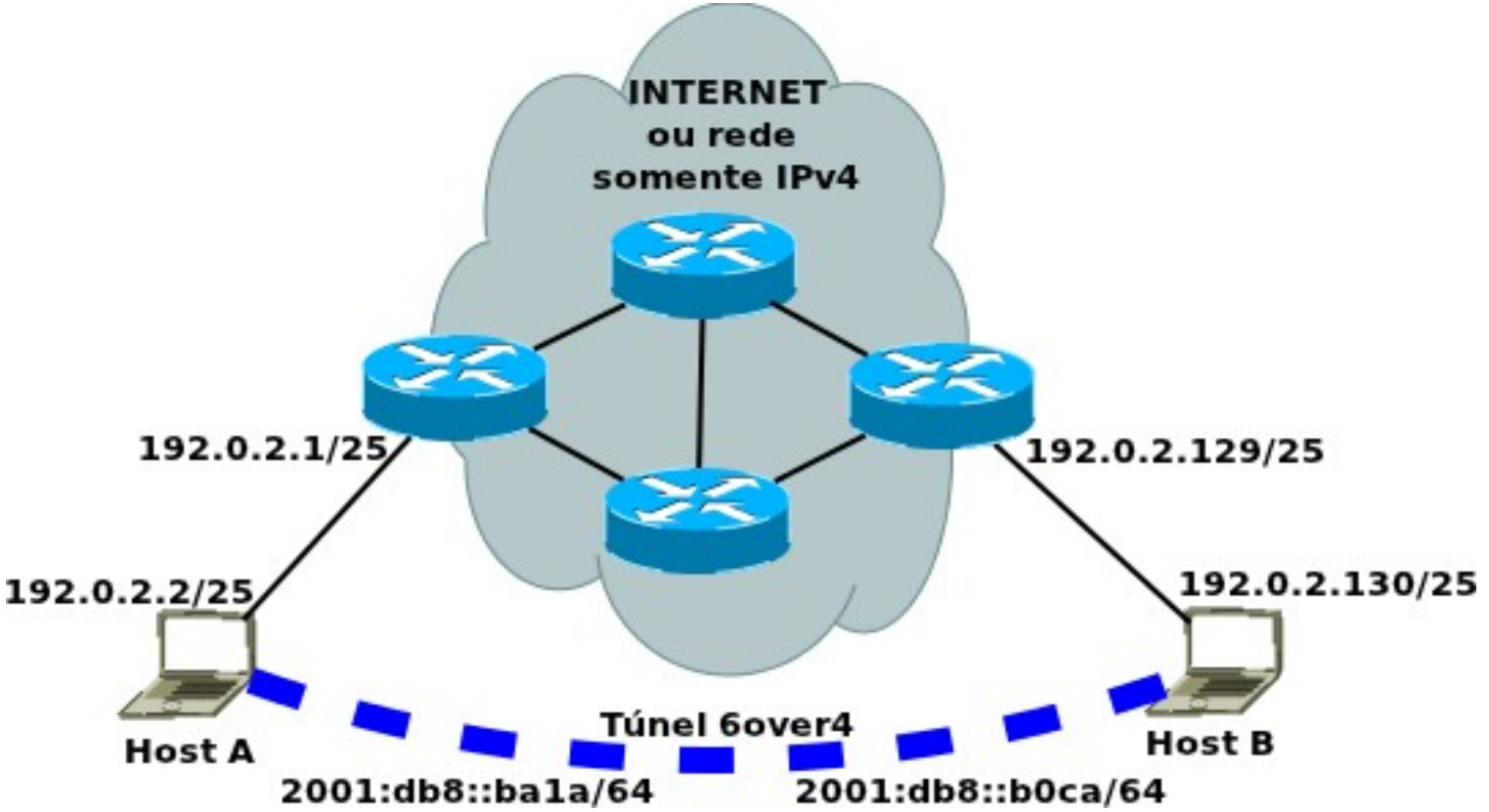
- Colocar todo o pacote IPv6 dentro de um pacote IPv4

6in4



- Técnica de encapsulamento do IPv6 diretamente dentro do pacote IPv4 – **RFC 4213**
- Tipo 41 (0x29) no campo cabeçalho: protocolo 41

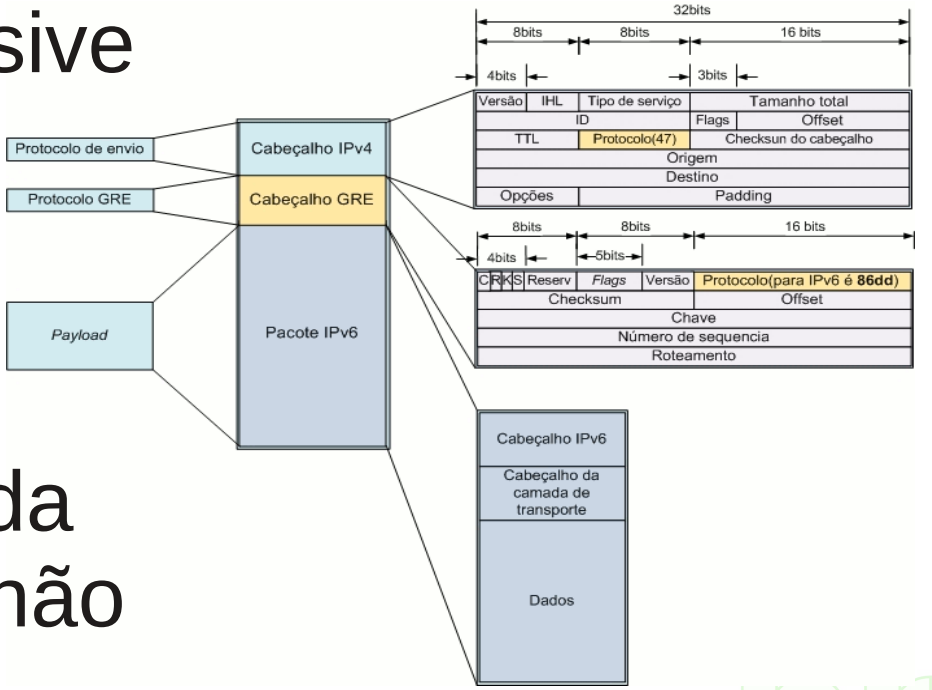
6over4



- Túnel configurado manualmente, usando o encapsulamento 6in4
- Pode ser usado para contornar partes da rede, ou Internet, que não suportam IPv6

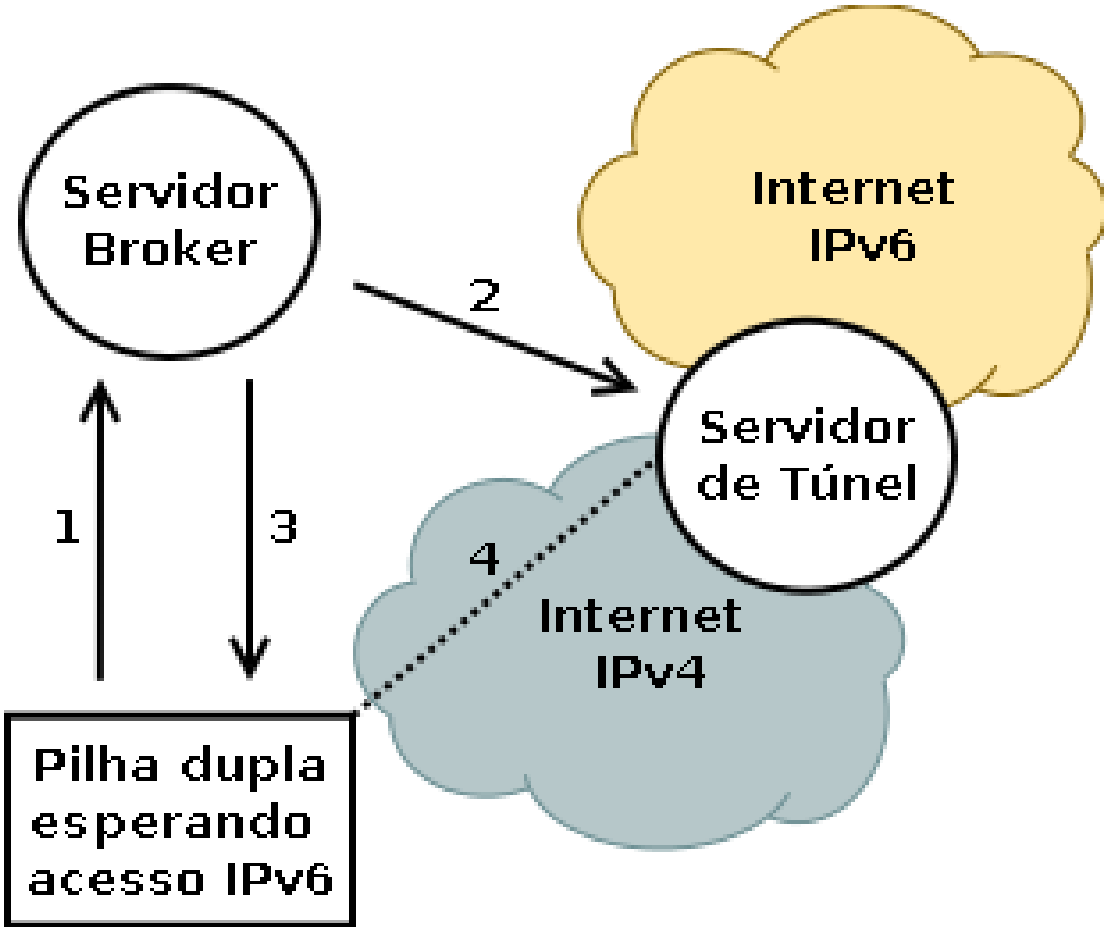
GRE

- Técnica de encapsulamento genérica, definida na **RFC 2784**, pode ser usada para transportar diversos protocolos, inclusive IPv6 e IPv4.
- Configuração manual
- Mesmos casos de uso do 6over4: contornar partes da rede, ou da Internet, que não suportam o protocolo.



Laboratório 6over4 e GRE

Tunnel Brokers



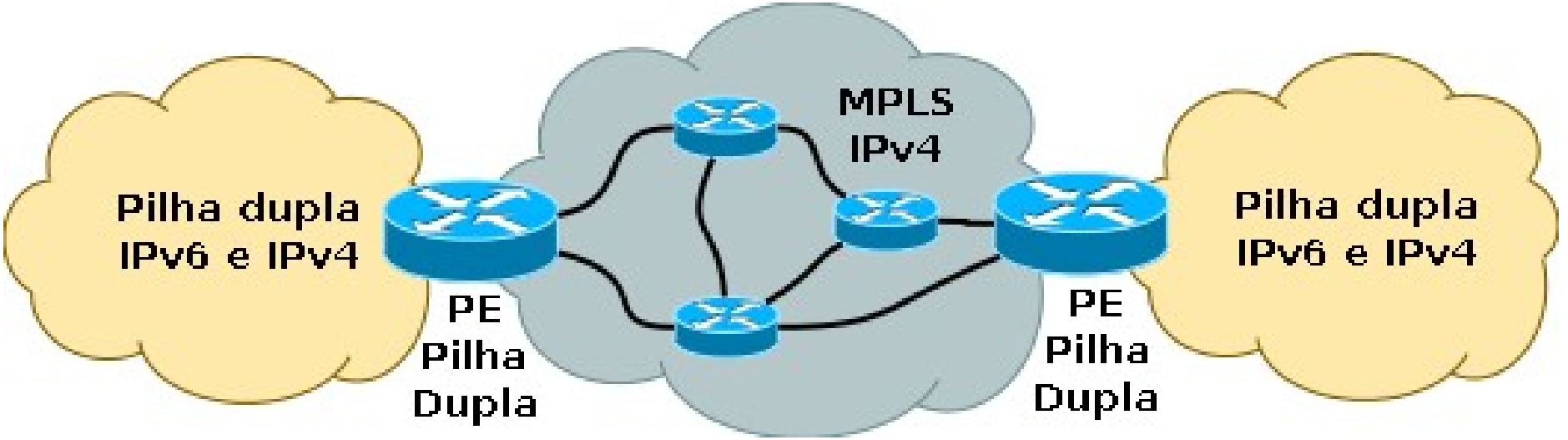
Tunnel Brokers

- Podem usar diversas técnicas de encapsulamento e protocolos de comunicação: 6in4, UDP, AYIYA, TSP, etc.
- A implantação de um serviço de Tunnel Broker não é trivial, pois não existem softwares abertos para a função de Servidor Broker
- http://tunnelbroker.net - Hurricane Electric – recomendado para Sistemas Autônomos, é possível estabelecer sessões BGP e anunciar seu próprio bloco.
- http://sixxs.net - PoP da Algar Telecom no Brasil – pode-se obter redes /64 e /48 para testes – ótimo desempenho.

6PE e 6VPE

- RFCs 4798 e 4659
- Comunicação IPv6 por meio de um core MPLS IPv4, usando LSPs (Label Switch Paths)
- 6PE – apenas tabela global de roteamento
- 6VPE – tabelas de roteamento separadas logicamente
- Permite que o provedor utilize a infraestrutura IPv4 já existente para facilitar a implantação do IPv6

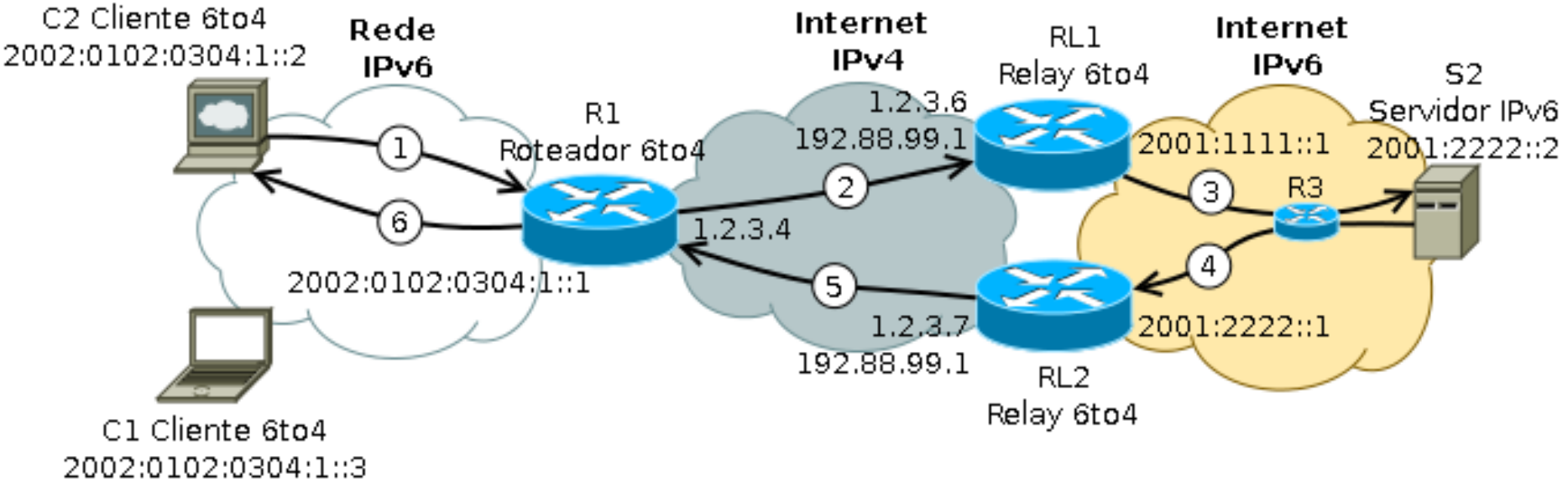
6PE e 6VPE



6to4

- O 6to4 (RFC 3056) é uma das técnicas de transição mais antigas e serviu de base para o 6rd
- Originalmente, seu objetivo era obter conectividade IPv6 por meio de túneis automáticos 6in4
- Provavelmente trouxe mais problemas para a implantação do IPv6 na Internet, do que benefícios
- Vários sistemas operacionais, em especial o Windows, utilizam essa técnica automaticamente

6to4


C2 Cliente 6to4
2002:0102:0304:1::2
Rede
IPv6
1
6
R1
Roteador 6to4
2002:0102:0304:1::1
C1 Cliente 6to4
2002:0102:0304:1::3
Internet
IPv4
1.2.3.6
192.88.99.1
2
1.2.3.4
5
1.2.3.7
192.88.99.1
RL1
Relay 6to4
RL2
Relay 6to4
Internet
IPv6
2001:1111::1
3
R3
4
2001:2222::1
S2
Servidor IPv6
2001:2222::2

6to4

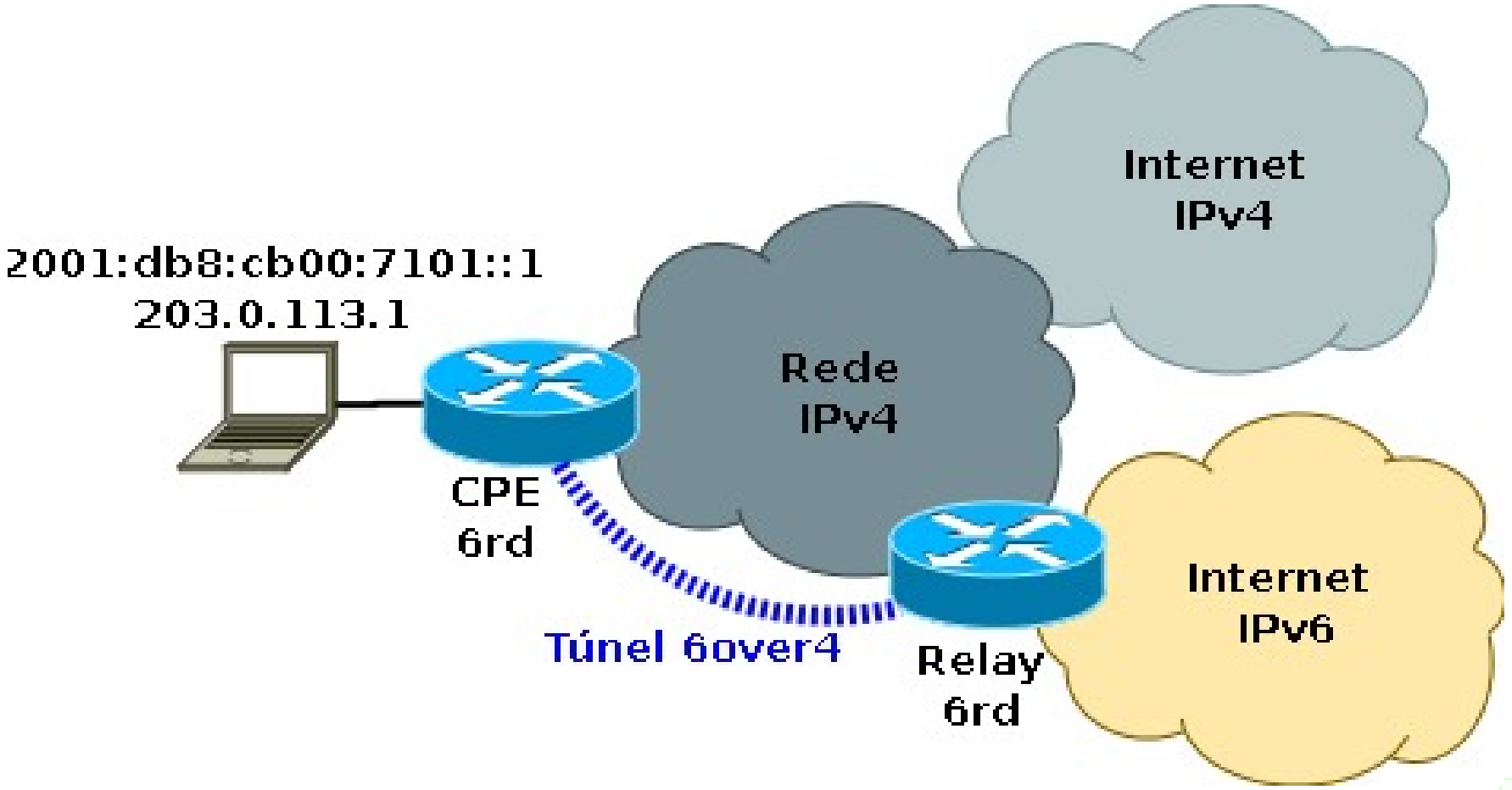
- Os endereços usam o prefixo **2002:wwxx:yyzz::/48**, onde wwxx:yyzz é o endereço IPv4 do roteador 6to4.
- Os relays usam o endereço anycast **192.88.99.1**
- Em redes pilhas dupla, com servidores IPv6 é recomendável instalar um relay 6to4 para que as respostas às requisições de clientes 6to4 saiam já encapsuladas da rede
- Em redes corporativas, pode-se bloquear os túneis 6to4 bloqueando-se o protocolo 41
- Pode-se também desativar os túneis 6to4 no Windows
- Laboratório disponível no CD ou Website

Laboratório 6to4

6rd

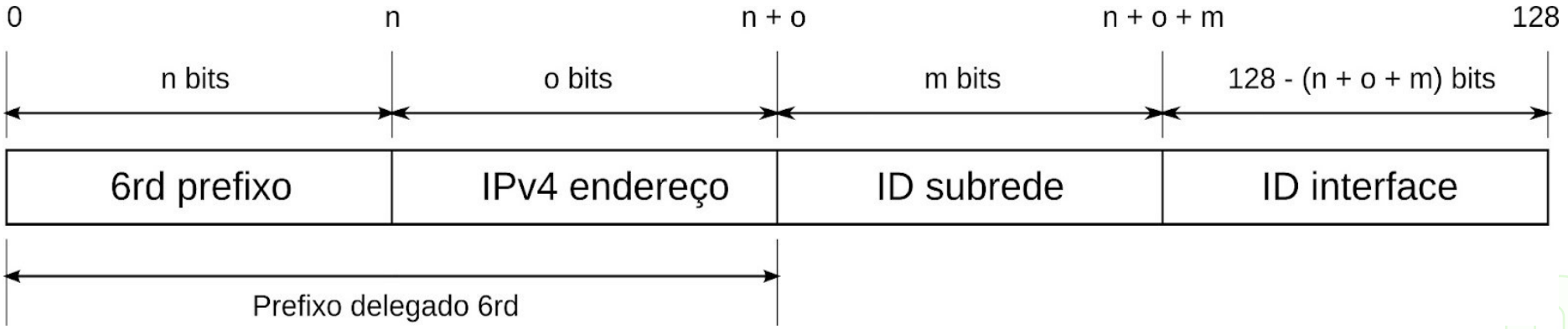
- O 6rd (rapid deployment) é uma técnica para facilitar a implantação do IPv6 entre o provedor e o usuário, sobre uma rede já existente IPv4
- Provedor Free, na França
- RFC 5569
- Baseado no 6to4

6rd


Internet
IPv4
2001:db8:cb00:7101::1
203.0.113.1
Rede
IPv4
CPE
6rd
Túnel 6over4
Relay
6rd
Internet
IPv6

6rd

- Formato do endereço IPv6
  - Normalmente n=32, o=32, m=0
  - Pode-se aumentar n, mas significa entregar prefixos mais longos do que /64 para os usuários, quebrando a SLAAC.
  - Pode-se omitir o prefixo de rede IPv4, diminuindo o. Por exemplo, para um prefixo 198.51.0.0/16, os bits que representam 198.51 poderiam ser omitidos.

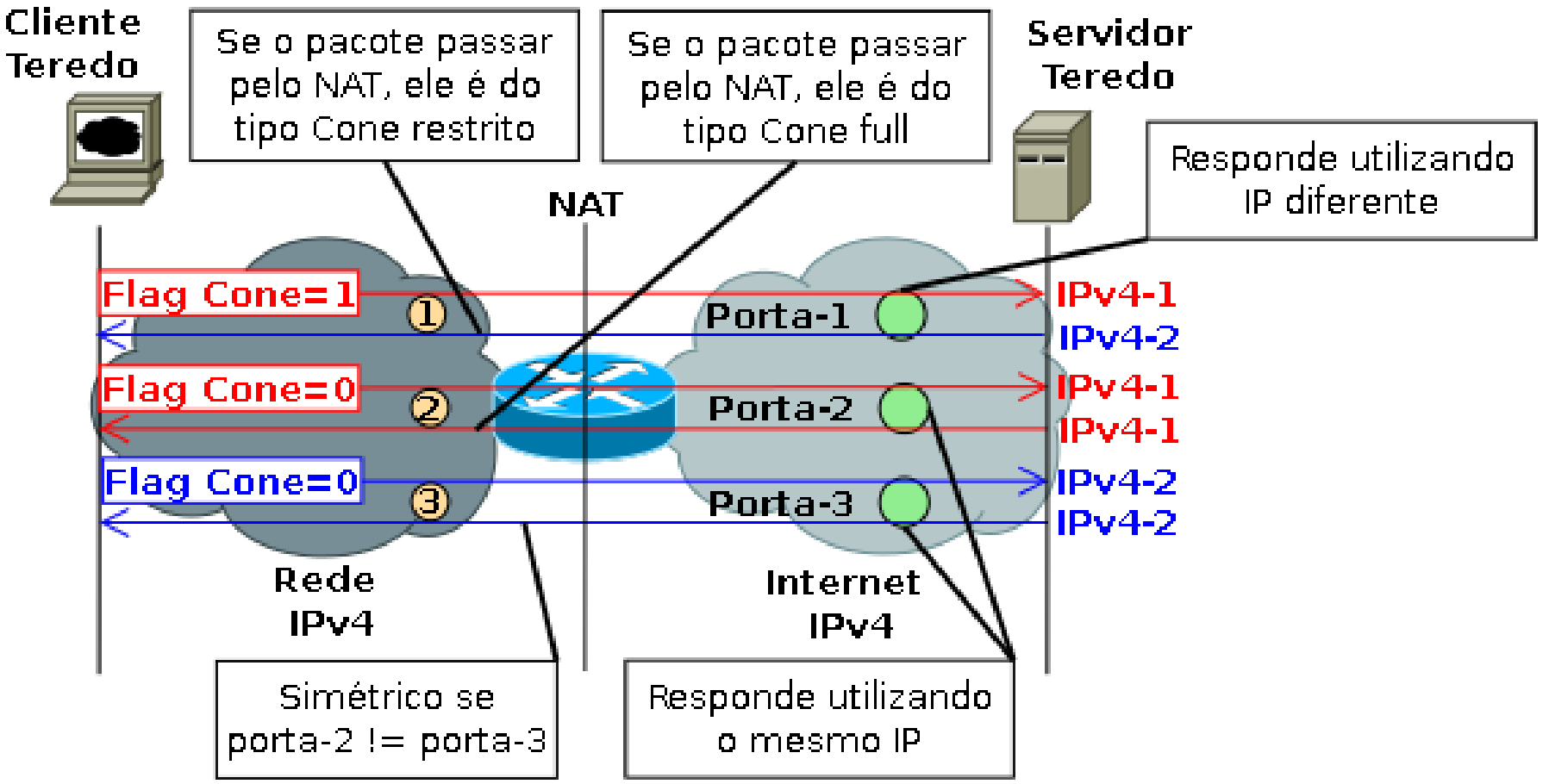


6rd

- Implementações
  - Linux kernel 2.6.33 ou superior
  - Cisco, Juniper, etc
- Pode ser útil para provedores que administram remotamente o CPE
- Não é uma técnica para ser usada para novos usuários, já que se baseia numa rede nativa IPv4, e não IPv6, mas pode ser útil para a base existente de usuários
- Laboratório disponível no CD ou Website

Laboratório 6rd

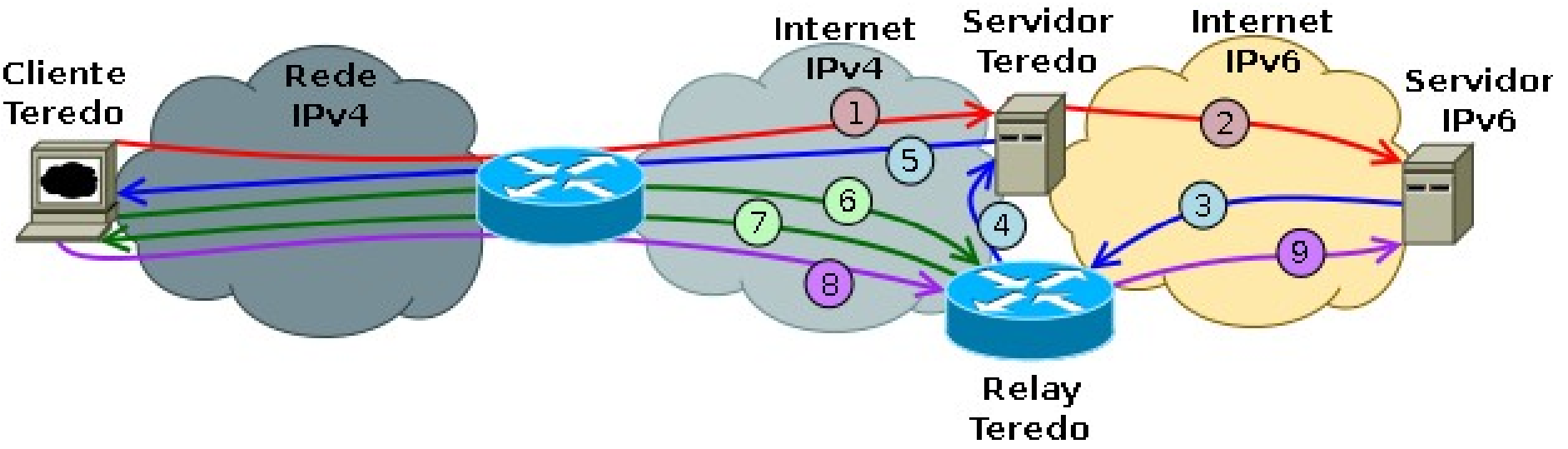
Teredo



Teredo

- O Teredo (**RFC 4380**) foi criado com o mesmo objetivo do 6to4, mas usa encapsulamento UDP, o que permite seu funcionamento com NAT IPv4
- Usa o prefixo 2001:0000::/32
- O Windows o implementa de forma automática.
- Pode ser bloqueado numa rede corporativa, bloqueando-se a comunicação na porta UDP 3544, ou desativando-o no Windows.

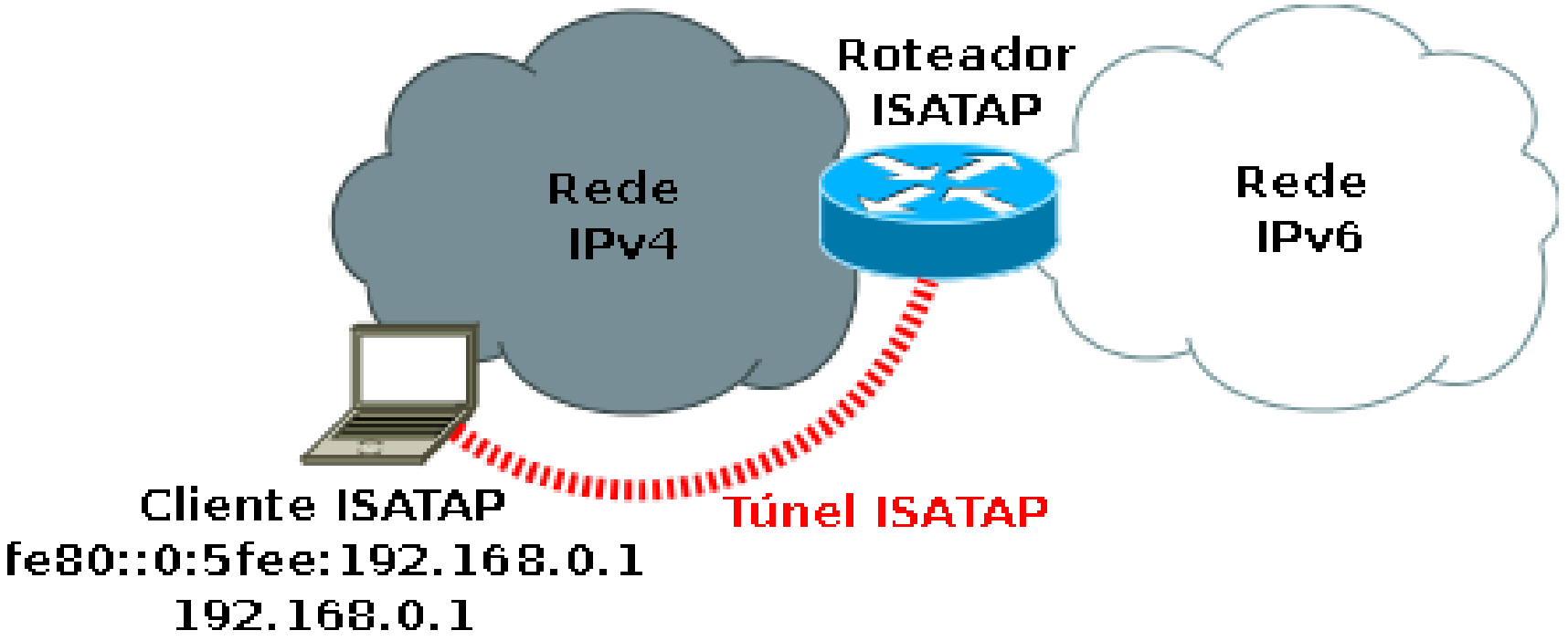
Teredo



ISATAP

- O ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) (RFC 5214) é um túnel automático IPv6 sobre IPv4 para ser usado dentro das corporações
- Não funciona através da Internet
- Baseado no protocolo 41

ISATAP



- Tenho IPv4
- Computador destino na Internet tem IPv4
- Mas meu provedor somente oferece IPv6
- Como eu consigo fazer esta comunicação em IPv4?

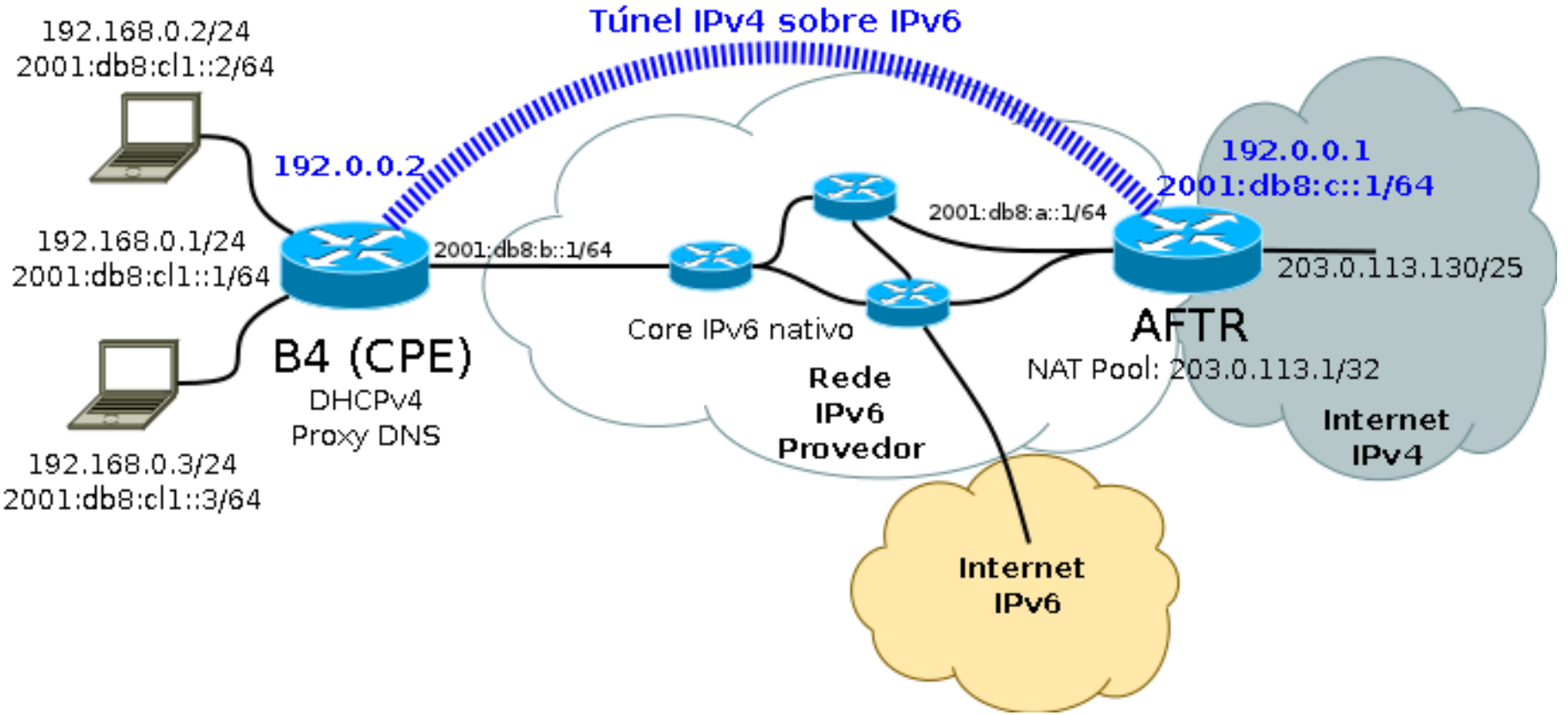
Utilizar túneis

- Colocar todo o pacote IPv4 dentro de um pacote IPv6

DS-Lite e DS-Lite com A+P

- Técnicas usadas na seguinte situação:
  - Entre provedores e seus usuários
  - Não há IPv4 disponíveis, é preciso preservá-los, compartilhando-os
  - Usuários trabalham com IPv6 nativo
- RFC 6333
- AFTR: http://www.isc.org/software/aftr
  - Desenvolvido pelo ISC por solicitação da Comcast

DS-Lite



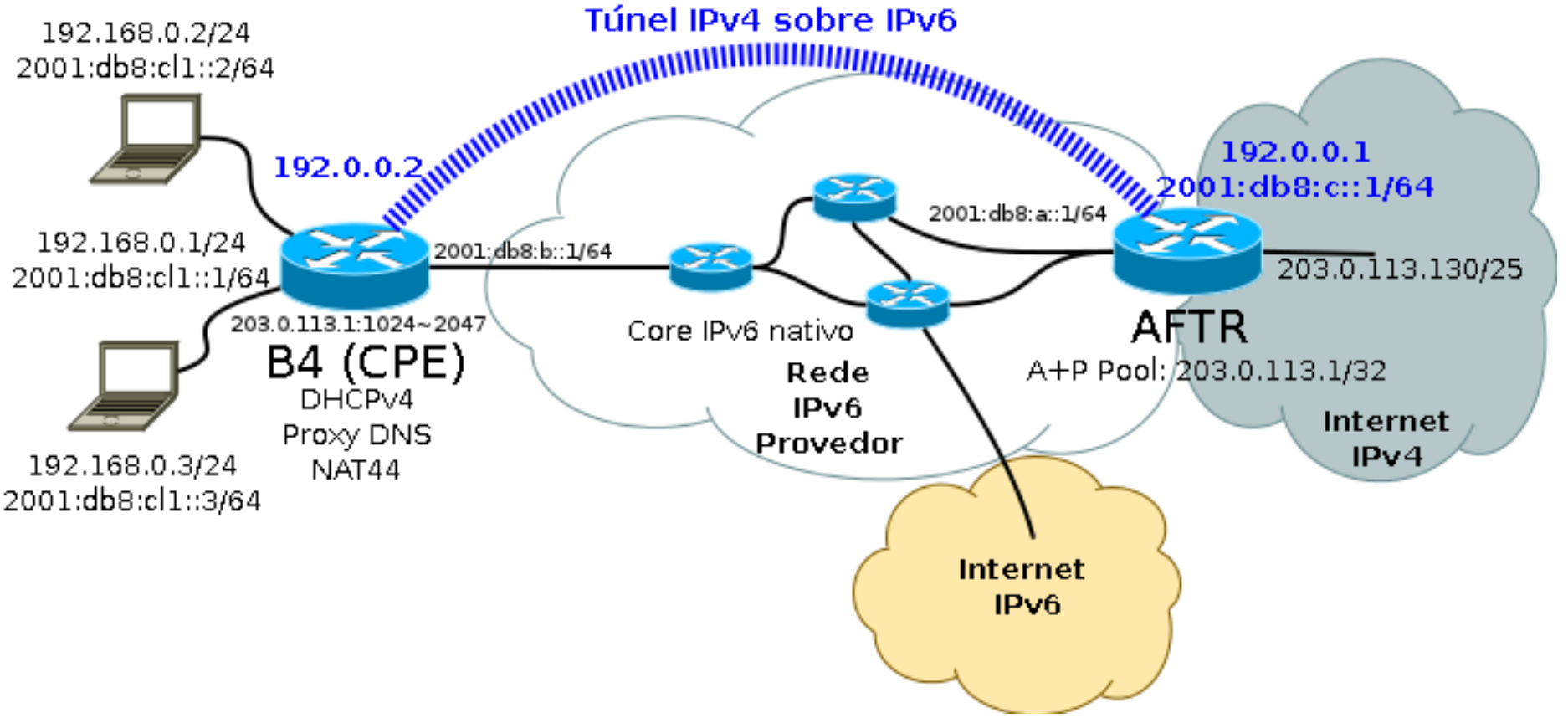
DS-Lite

- B4 = Basic Bridge BroadBand
  - IPv6 nativo
  - Deve suportar túneis 4in6 (Linux / OpenWRT)
  - DHCPv4 (para atribuição dos endereços v4 RFC 1918 aos hosts)
  - Proxy DNS (faz as consultas via IPv6, evitando a tradução)
- AFTR = Address Family Transition Router
  - CGN – NAT44
  - Um só NAT, não é NAT 444, faz a tradução para cada um dos dispositivos do usuário, já que o CPE opera como bridge
- Endereços na faixa 192.0.0.0/29 nos túneis: não gasta blocos IPv4 na infraestrutura do provedor.

DS-Lite com A+P

- Similar ao DS-Lite, mas usa A+P
  - Compartilhamento de endereços (A – Address), com restrição de portas (P – Portas).
- Stateless
- O usuário recebe um IPv4 válido, mesmo com algumas restrições
- NAT44 no CPE, obedecendo a restrição de portas
  - Hosts não precisam conhecer o A+P

DS-Lite com A+P

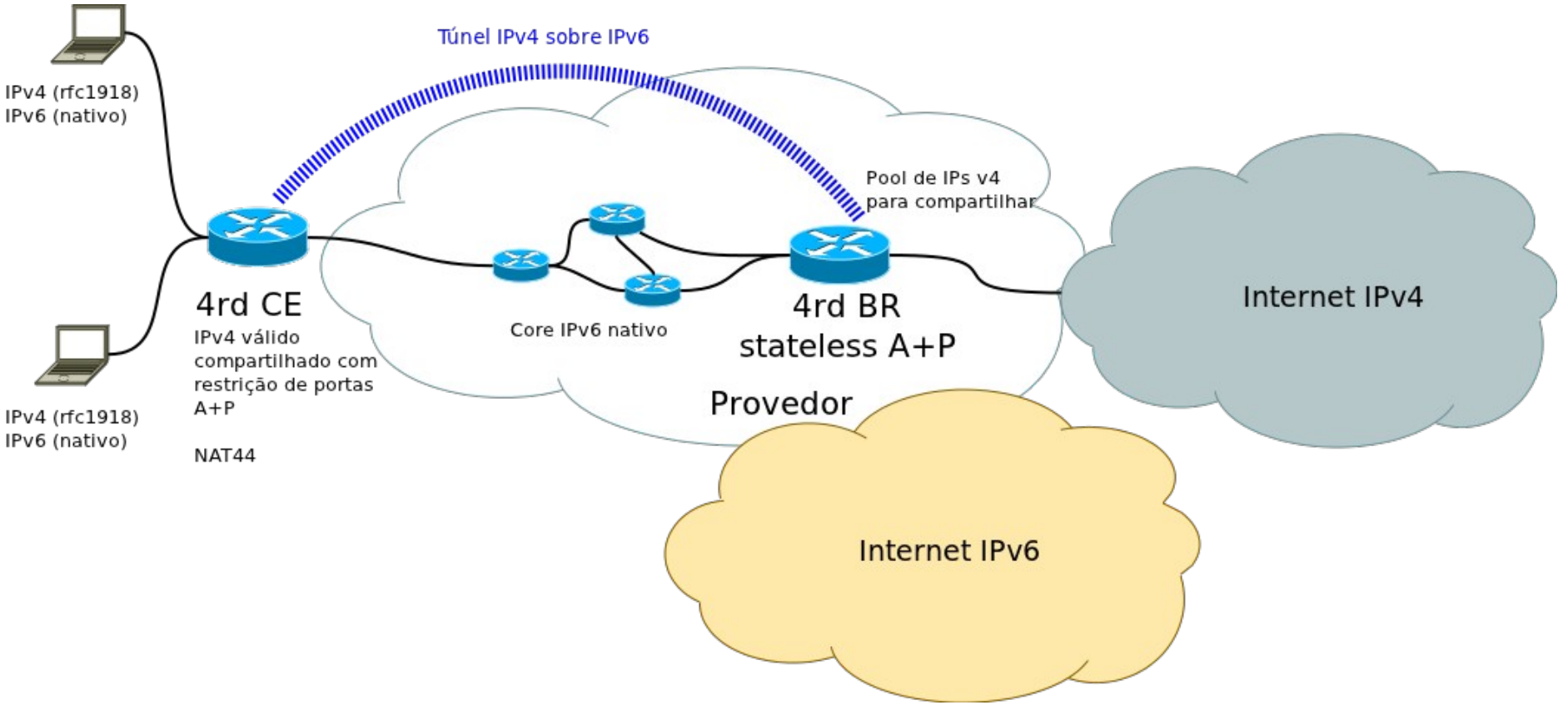


Laboratório DSLite

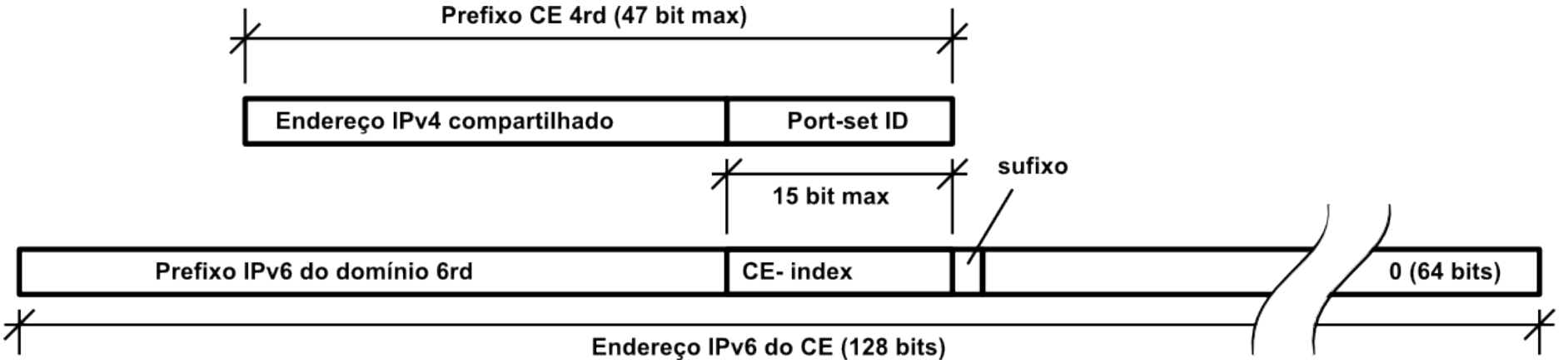
4rd

- O 4rd (draft-despres-intarea-4rd-01) é uma técnica muito similar ao DS-Lite com A+P
  - Usa túneis 4in6 para fornecer IPs v4 compartilhados para usuários somente IPv6
  - Usa compartilhamento de endereços com restrição de portas (A+P)
- O endereço IPv4 e parâmetros de compartilhamento são mapeados no endereço IPv6

4rd


Túnel IPv4 sobre IPv6
IPv4 (rfc1918)
IPv6 (nativo)
IPv4 (rfc1918)
IPv6 (nativo)
4rd CE
IPv4 válido
compartilhado com
restrição de portas
A+P
NAT44
Core IPv6 nativo
Pool de IPs v4
para compartilhar
4rd BR
stateless A+P
Provedor
Internet IPv4
Internet IPv6

4rd



Blocos de portas:

1o. bloco: 0001 + port-set-ID (n=1 a 12 bits) + sufixo (que varia de 0 a 12-n)
2o. bloco: 001 + port-set-ID (n=1 a 13 bits) + sufixo (que varia de 0 a 13-n)
3o. bloco: 01 + port-set-ID (n=1 a 14 bits) + sufixo (que varia de 0 a 14-n)
4o. bloco: 1 + port-set-ID (n=1 a 15 bits) + sufixo (que varia de 0 a 15-n)

4rd

tamanho do port set (bits)	qtd de ID's (CPEs)	Head=0001 1o. bloco	Head=001 2o. bloco	Head=01 3o. bloco	Head=1 4o. bloco	total de portas	portas não utilizadas
1	2	2048	4096	8192	16384	30720	4096
2	4	1024	2048	4096	8192	15360	4096
3	8	512	1024	2048	4096	7680	4096
4	16	256	512	1024	2048	3840	4096
5	32	128	256	512	1024	1920	4096
6	64	64	128	256	512	960	4096
7	128	32	64	128	256	480	4096
8	256	16	32	64	128	240	4096
9	512	8	16	32	64	120	4096
10	1024	4	8	16	32	60	4096
11	2048	2	4	8	16	30	4096
12	4096	1	2	4	8	15	4096
13	8192	-	1	2	4	7	8192
14	16384	-	-	1	2	3	16384
15	32768	-	-	-	1	1	32768

4rd

- Implementação baseada em vyatta que pode ser usada para testes: http://bougaidenpa.org/masakazu/archives/176
- Produtos da linha SEIL do provedor japonês IIJ também implementam o protocolo.
- O desenvolvimento do 4rd deve ser acompanhado com atenção:
  - Funciona em redes somente IPv6
  - Stateless
  - Conectividade fim a fim
  - Quando necessário o uso de técnicas stateful, isso é feito no lado do cliente (NAT44 obedecendo à restrição de portas)

- Somente tenho IPv6
- Computador destino na Internet somente tem IPv4
- Como eu consigo fazer esta comunicação?

Utilizar Tradução

- Fazer equivalência entre campos IPv6 com campos IPv4 na mudança de uma rede para outra

RFC 6145

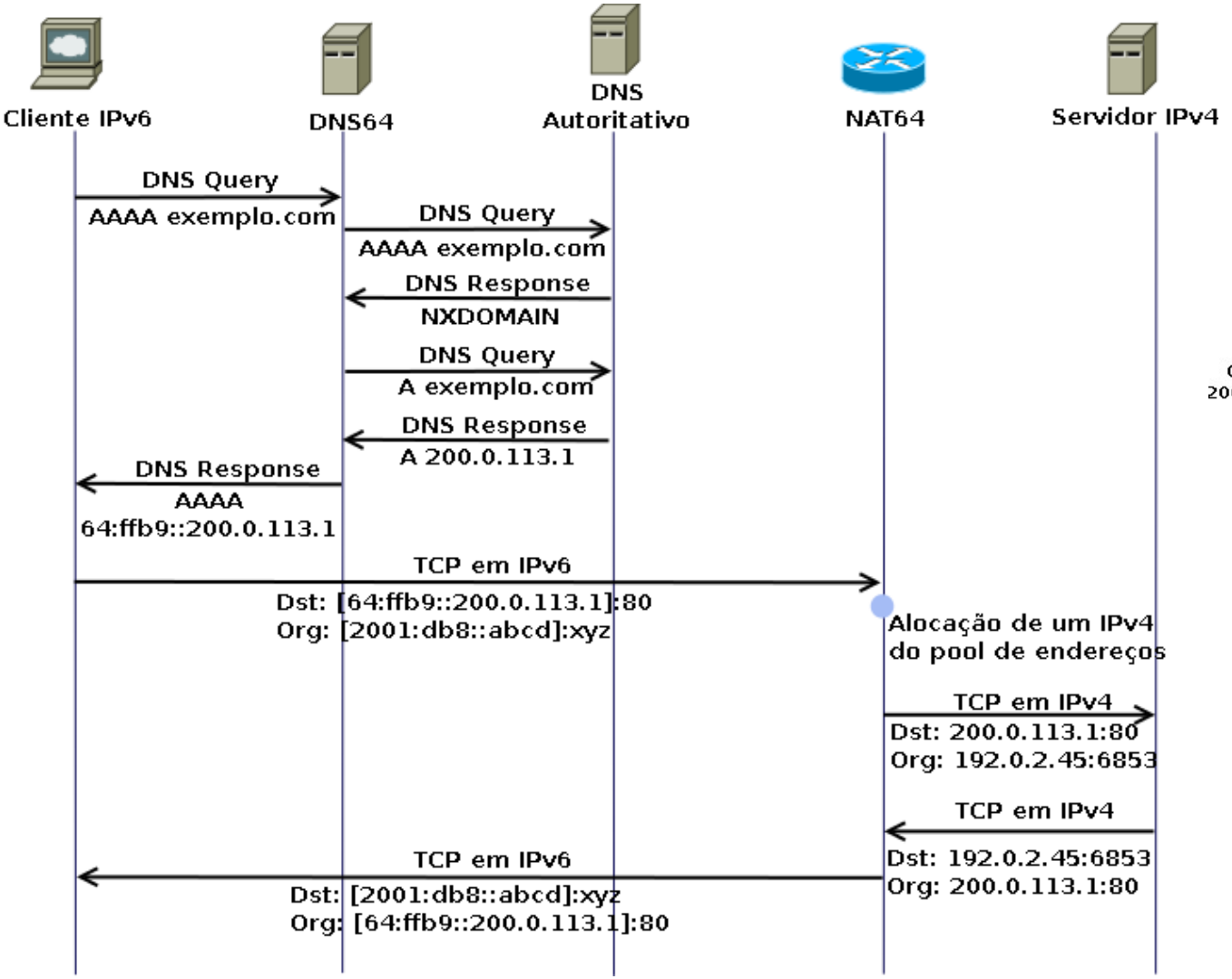
Campo IPv6	Cabeçalho IPv4 Traduzido
Versão (0x6)	Versão (0x4)
Classe de Tráfico	Tipo de Serviço
Etiqueta de Fluxo	(descartado)
Tamanho do Payload	Tamanho Total = Tamanho do Payload + 20
Próximo Cabeçalho	Protocolo
Limite de Nós	Tempo de Vida
Endereço de Origem	Aplicar mapeamento
Endereço de Destino	Aplicar mapeamento
----	IHL = 5
----	CRC do Cabeçalho Recalculado

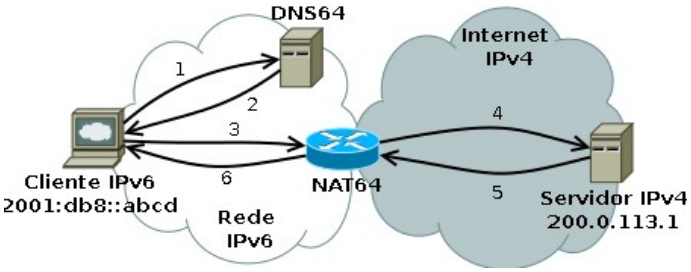
RFC 6145

Campo IPv4	Tradução para IPv6
Versão (0x4)	Versão (0x6)
IHL	(descartado)
Tipo de Serviço	Classe de Tráfico
Tamanho Total	Tamanho do Payload = Tamanho Total - IHL * 4
Identificação	(descartado)
Flags	(descartado)
Offset	(descartado)
Tempo de vida	Limite de Nós
Protocolo	Próximo Cabeçalho
CRC do Cabeçalho	(descartado)
Endereço de Origem	Aplicar mapeamento
Endereço de Destino	Aplicar mapeamento
Opções	(descartado)

- Endereços IPv4 são escassos
- Como atribuir um IPv4 quando fizer a tradução?
- Se tivesse falando de redes IPv4 com endereçamento privado para acessar a Internet teríamos algo similar?

NAT64 e DNS64



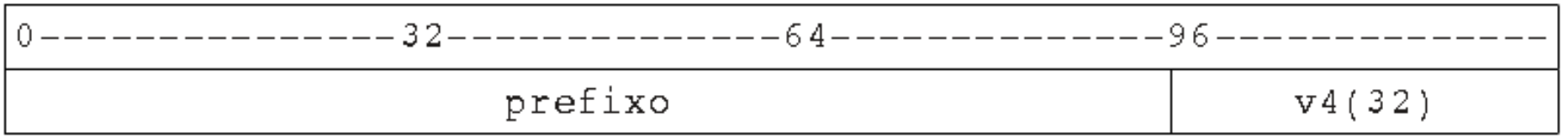


NAT64 e DNS64

- Caso de uso similar ao do DS-Lite:
  - Entre provedores e seus usuários
  - Não há IPv4 disponíveis, é preciso preservá-los, compartilhando-os
  - Usuários trabalham com IPv6 nativo
    - Não recebem um IPv4, nem mesmo privado
    - A comunicação com hosts v4 é feita por meio de tradução
- NAT64 e DNS64 são técnicas independentes que operam em conjunto

NAT64

- Definido na **RFC 6146**
- Tradução stateful de pacotes IPv6 em IPv4
- Prefixo bem conhecido: **64:ff9b::/96**
- Linux, Windows, Cisco, Juniper, A10, F5, etc.




```
ex.: IPv4 = 203.0.113.1
     IPv6 convertido = 64:ff9b::203.0.113.1
```

DNS64

- Técnica auxiliar ao NAT64
- RFC 6147
- Funciona como um DNS recursivo, para os hosts, mas:
  - Se não há resposta AAAA, converte a resposta A em uma resposta AAAA, convertendo o endereço usando a mesma regra (e prefixo) do NAT64
- BIND ou Totd

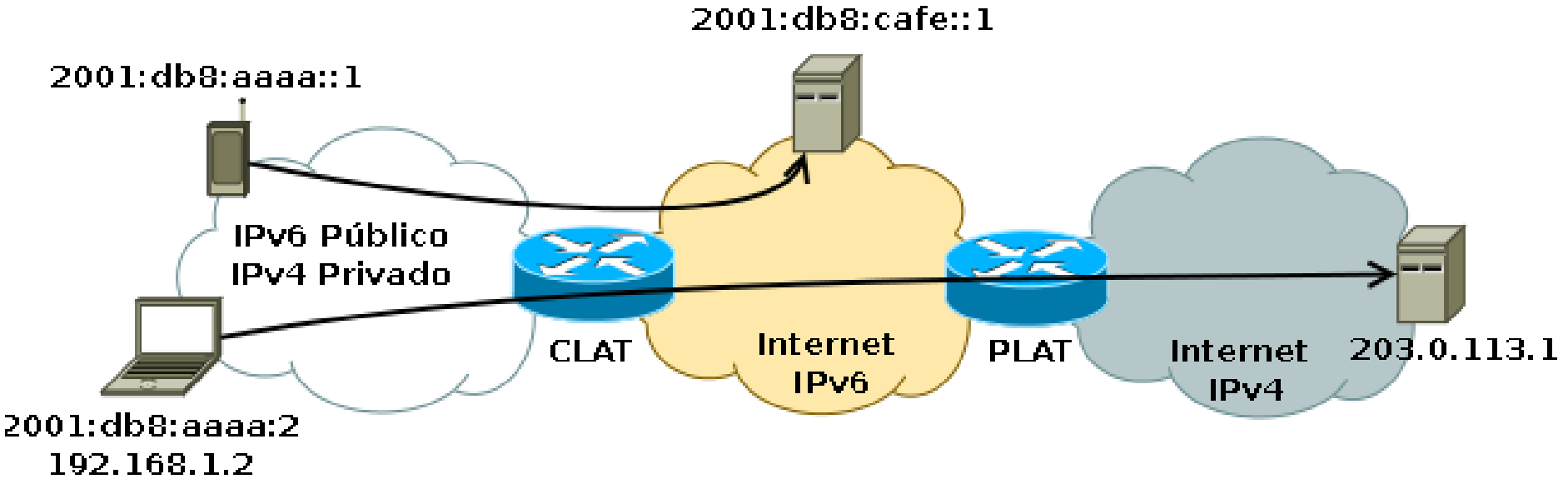
NAT64 e DNS64

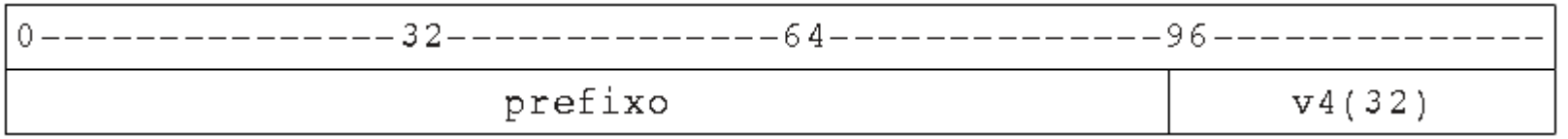
- Computadores trabalham apenas com IPv6
  - Alguns softwares, não preparados ainda para o IPv6, podem não funcionar
- Tradução de endereços
  - Algumas aplicações, que carregam IPs em sua forma literal no protocolo, na camada de aplicação, não funcionarão. Ex.: ftp em modo ativo, sip.

Laboratório NAT64

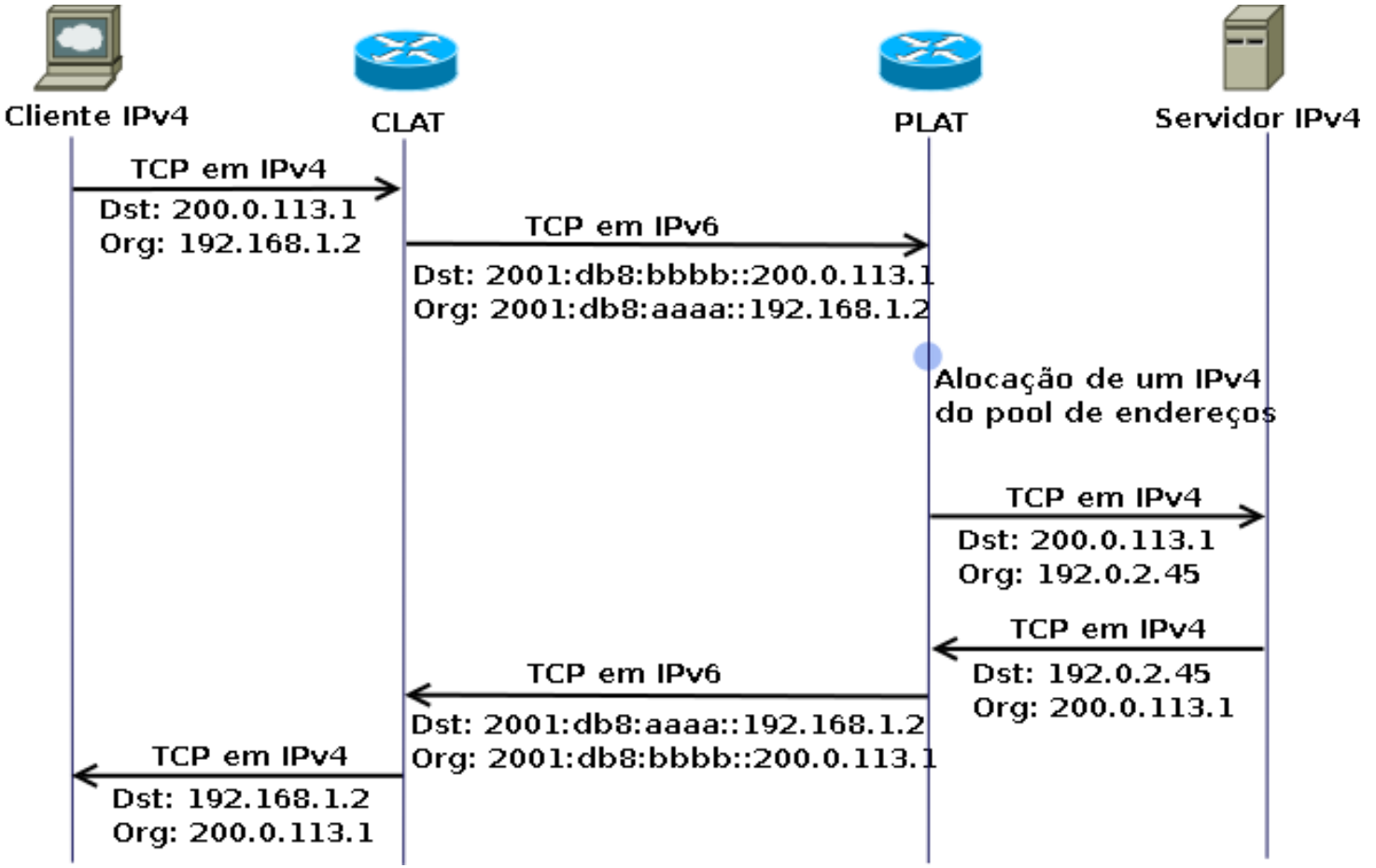
- NAT64 e DNS64 não oferecem IPv4, quebrando algumas aplicações
- É possível atribuir um IPv4, mesmo que privado, aos usuários?

464XLAT





464XLAT



464XLAT

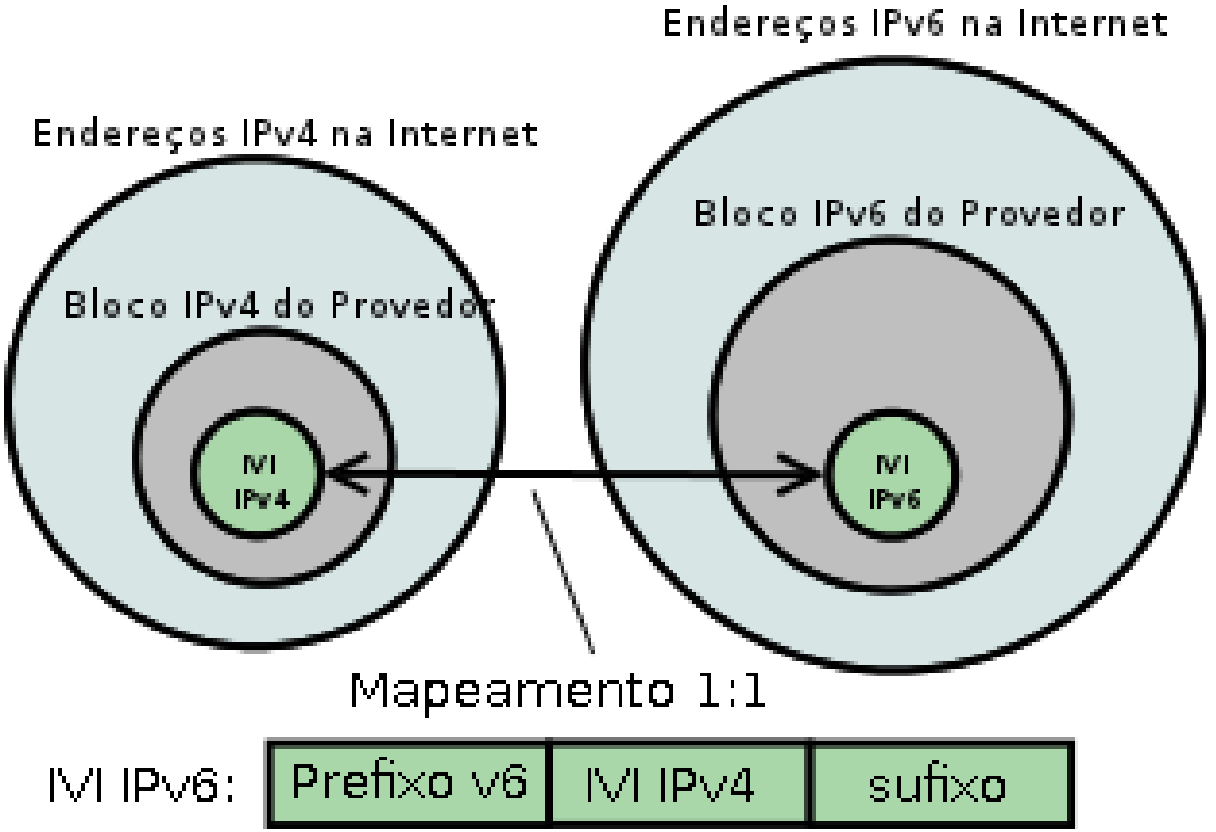
- Solução que usa dupla tradução, similar ao dIVI ou dIVI-pd
- draft-ietf-v6ops-464xlat-01
- Não é realmente uma técnica nova, mas uma aplicação de duas técnicas já conhecidas em conjunto:
  - O NAT64, no lado do provedor – PLAT (provider side translator) – RFC 6146
  - Um tradutor stateless, semelhante ao IVI, no lado do cliente, mas que usa endereços privados (RFC1918), e não públicos – CLAT (customer side translator) – RFC 6145

464XLAT

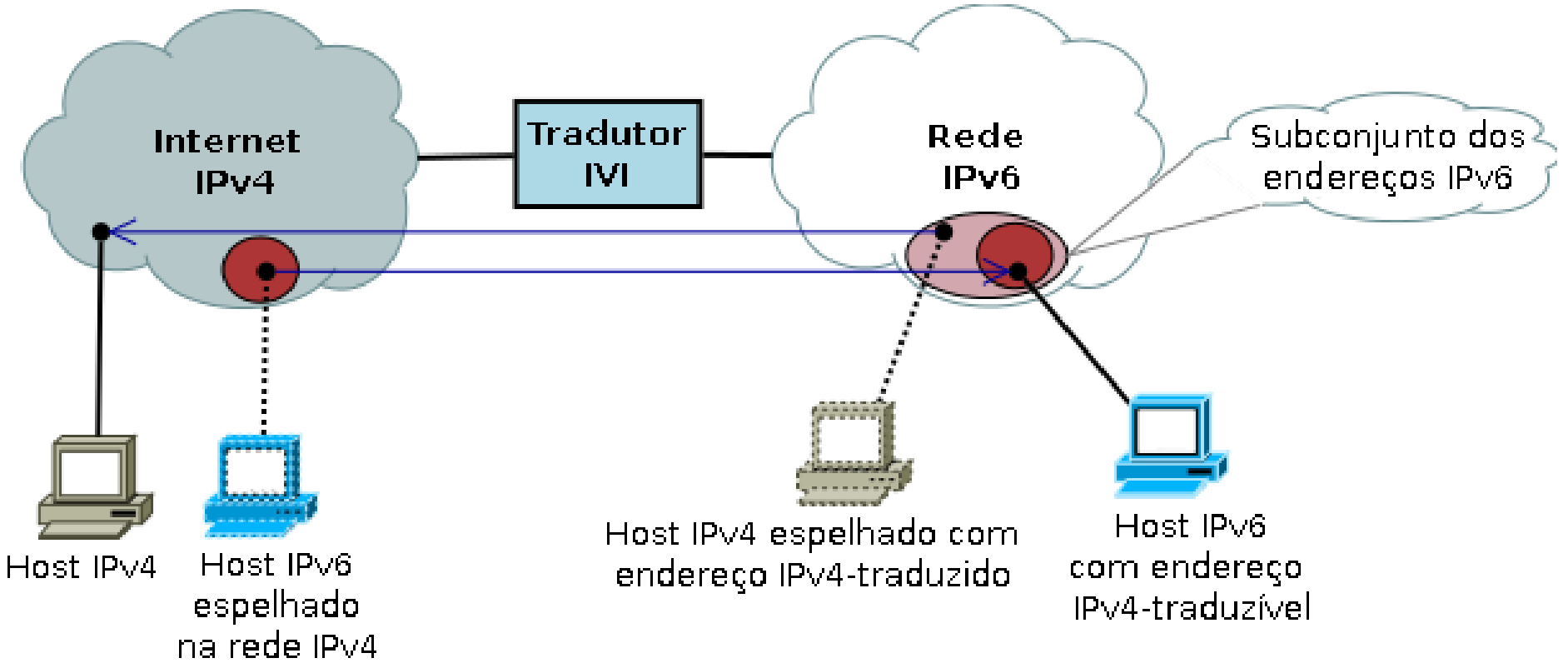
- CLAT
  - Android: http://code.google.com/p/android-clat
  - http://www.ivi2.org/IVI
- PLAT: NAT64 (diversas opções)
- Testes realizados pela T-Mobile e pelo Ponto de Troca de Tráfego japonês JPIX
- Não é a solução ideal:
  - Não aceita conexões entrantes (para o v4)
  - Stateful do lado do provedor
- Pode ser implantada em larga escala em pouco tempo, pois seus componentes básicos já estão relativamente maduros

- É possível fazer uma tradução sem guardar o histórico?
- Existem mais IPv6 do que IPv4, como fazer um mapeamento 1:1?

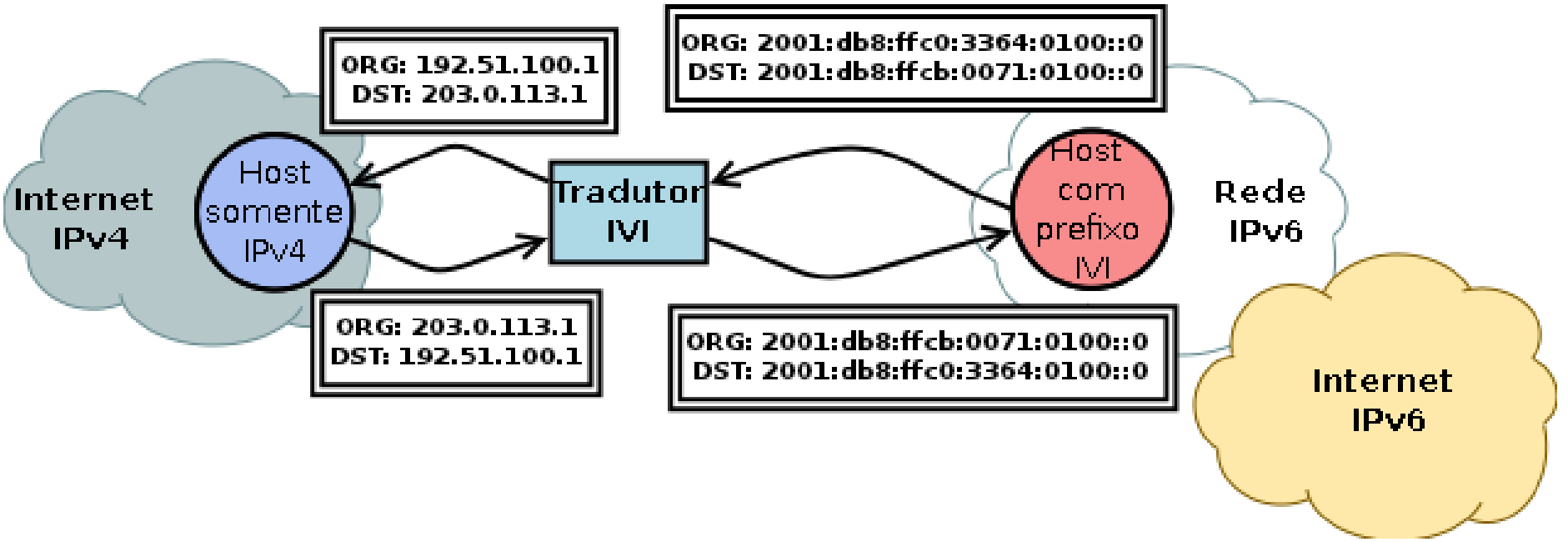
IVI


Endereços IPv6 na Internet
Endereços IPv4 na Internet
Bloco IPv6 do Provedor
Bloco IPv4 do Provedor
IVI
IPv4
IVI
IPv6
Mapeamento 1:1
IVI IPv6:
Prefixo v6
IVI IPv4
sufixo

IVI


Internet
IPv4
Tradutor
IVI
Rede
IPv6
Subconjunto dos
endereços IPv6
Host IPv4
Host IPv6
espelhado
na rede IPv4
Host IPv4 espelhado com
endereço IPv4-traduzido
Host IPv6
com endereço
IPv4-traduzível

IVI



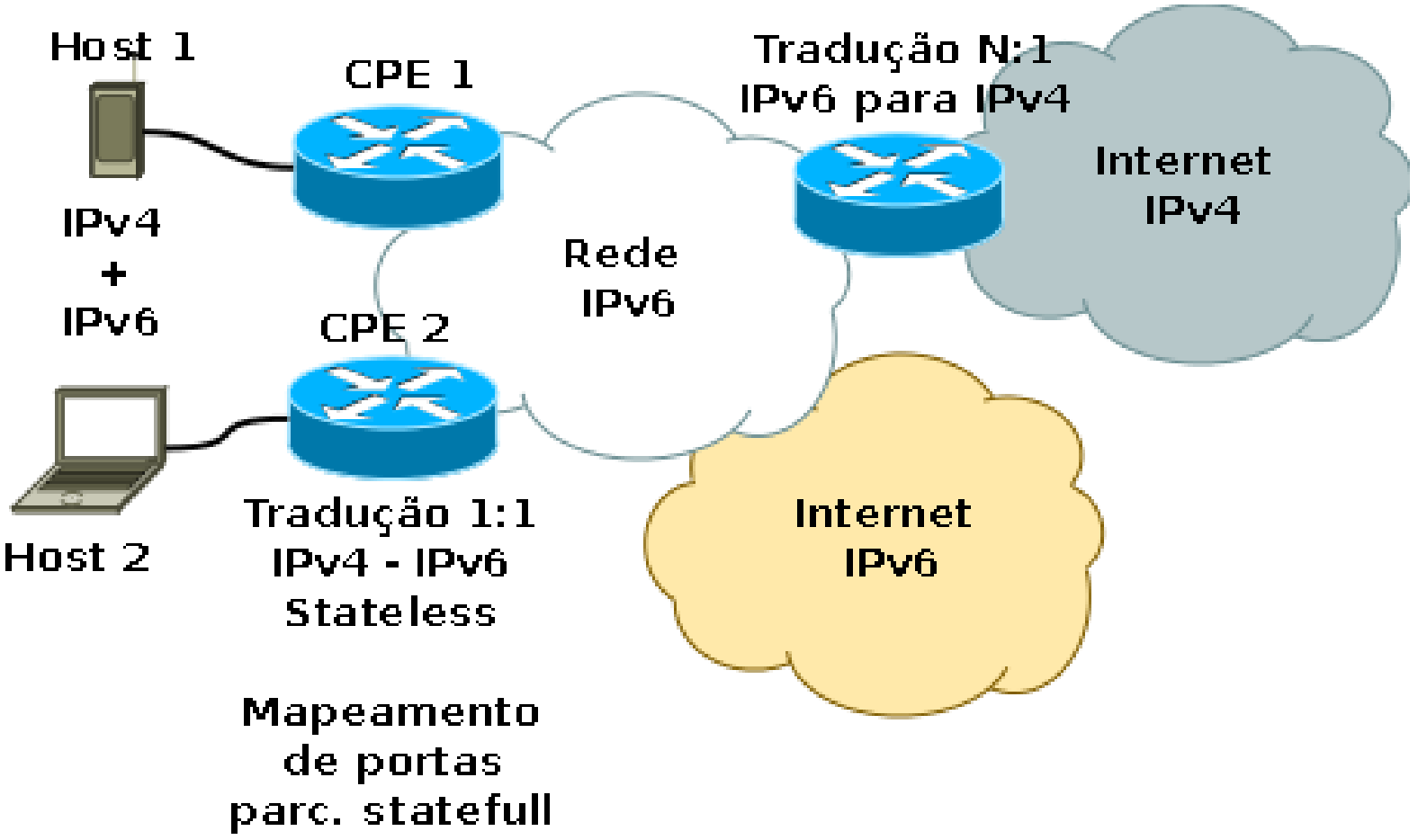
A tradução dos cabeçalhos é feita da mesma forma que no NAT64, conforme a **RFC 6145**

IVI

- IVI = IV (4 em romano) + VI (6 em romano)
- Como o IVI não trata do esgotamento do IPv4, e exige um mapeamento 1:1, é mais adequado para servidores IPv6, do que para estações de trabalho em geral.
- O IVI foi desenvolvido para que servidores somente IPv6 da CERNET2 (Rede Acadêmica Chinesa), pudessem ser acessados da Internet IPv4
- **RFC 6219**
- Há uma implementação aberta do IVI para Linux, que pode ser usada para testes: http://www.ivi2.org/IVI/

- É possível expandir a tradução para que uma maior quantidade de usuários possa ser atendida?
- Compartilhar a tradução é possível?

dIVI e dIVI-pd



dIVI e dIVI-pd

- O dIVI (draft-xli-behave-divi-04) e o dIVI-pd (draft-xli-behave-divi-pd-01) são técnicas que usam dupla tradução para fornecer endereços IPv4 compartilhados, com restrição de portas, a hosts somente IPv6.
- No dIVI é possível entregar apenas 1 endereço IPv6, e um endereço IPv4, para um dado CPE, enquanto no dIVI-pd é possível delegar um prefixo.

dIVI

- No CPE pode haver dois tipos de tradução
  - Totalmente stateless, mas nesse caso os hosts devem obedecer, por algum outro meio, a restrição de portas
  - Parcialmente stateless, quando o CPE realiza a tradução das portas e guarda o estado relativo a isso
- O dIVI é adequado para dispositivos móveis, quando 1 endereço IPv4 e 1 endereço IPv6 normalmente são suficientes

dIVI-pd

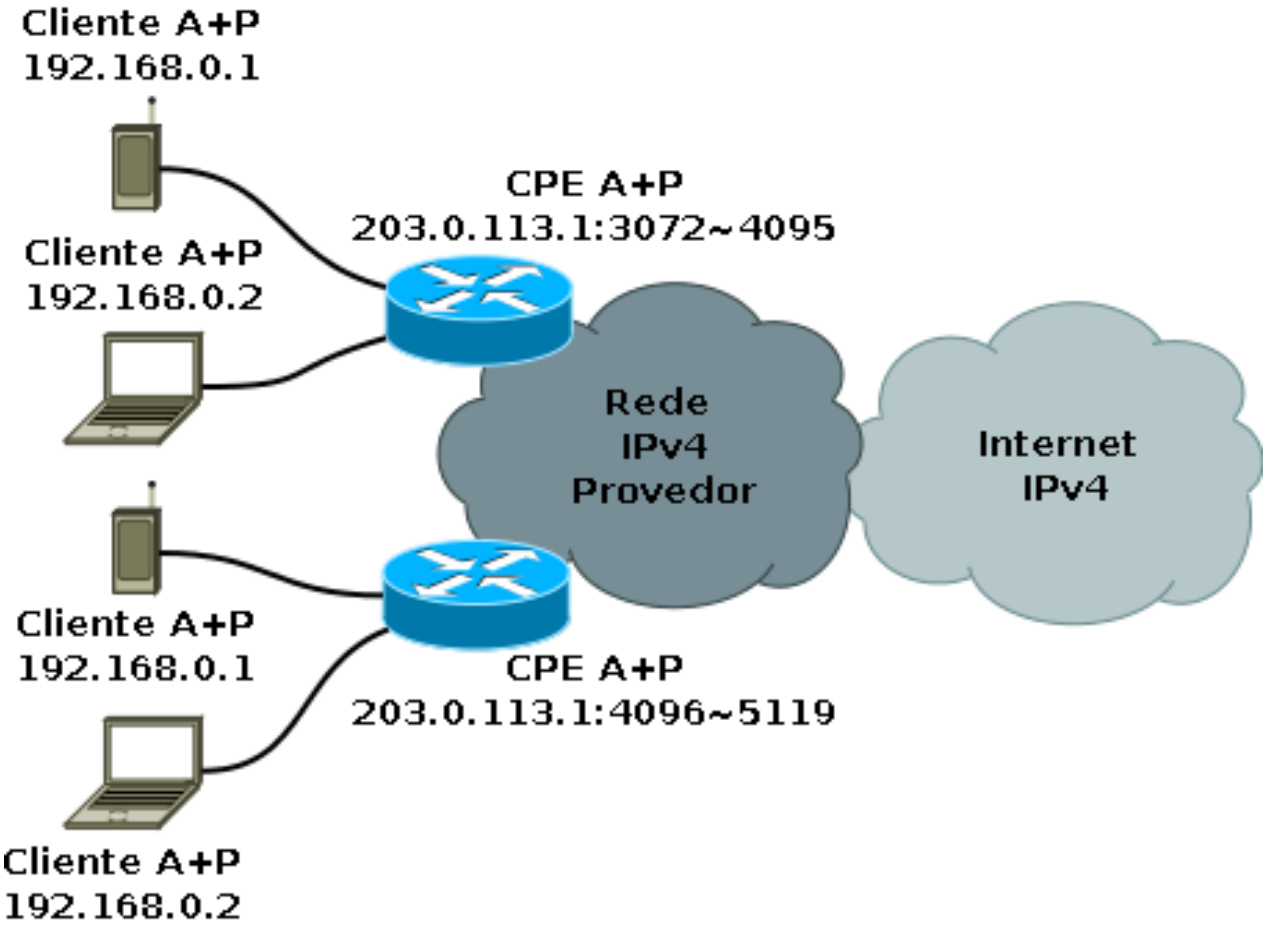
- No dIVI-pd cada CPE recebe:
  - Um prefixo IPv6, que pode ser distribuído para os diversos hosts via SLAAC
  - Um endereço IPv4, com portas restritas, que pode ser compartilhado entre diversos hosts, se o CPE realizar a função de NAT44 e DHCPv4

dIVI e dIVI-pd

- Soluções praticamente ideais:
  - Funcionam sobre redes somente v6
  - Stateless
  - Conectividade fim a fim
  - Não necessitam de DNS64 ou ALG
  - Quando necessário usar técnicas stateful (mapeamento de portas ou NAT44) isso é feito no lado do usuário
  - A tradução N:1 implementada no provedor pode ser usada também com DNS64 e eventualmente ALGs para clientes somente IPv6

- Os IPv4 estão acabando por aqui e já acabaram em outros lugares
- Distribuição em massa de IPv6 ou de técnicas de transição ainda não é realidade
- Existe algo que possa ser feito para dar sobrevida ao IPv4?

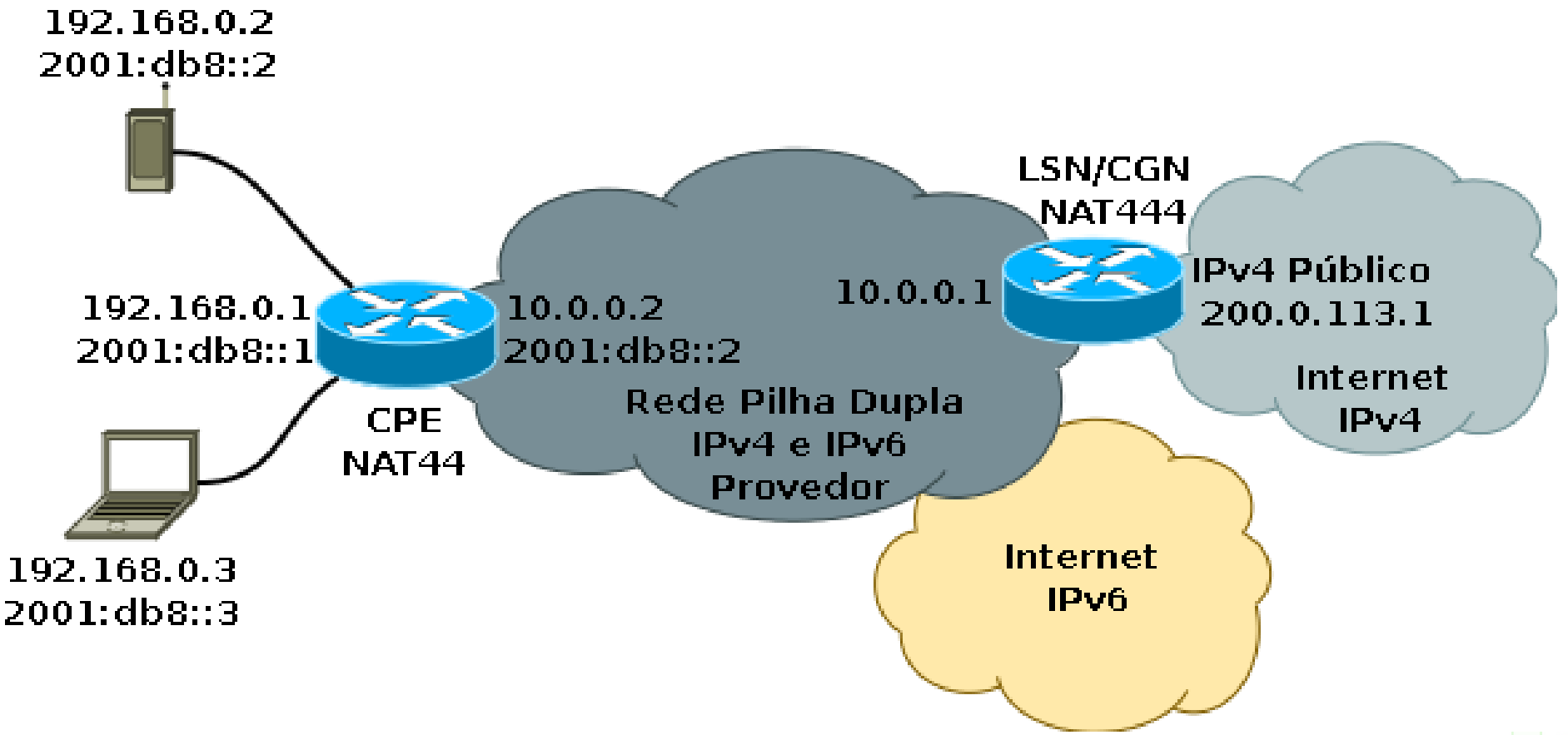
A+P


Cliente A+P
192.168.0.1
Cliente A+P
192.168.0.2
CPE A+P
203.0.113.1:3072~4095
Rede
IPv4
Provedor
Internet
IPv4
Cliente A+P
192.168.0.1
CPE A+P
203.0.113.1:4096~5119
Cliente A+P
192.168.0.2

A+P

- O A+P (RFC 6346) não é uma técnica de transição para IPv6, mas uma forma de preservar os endereços IPv4
- Pode ser usada em conjunto com a implantação nativa do IPv6
- O A+P consiste em compartilhar o mesmo IPv4 para diversos usuários, restringindo as faixas de portas que cada um deles pode usar
- O A+P é menos nocivo à arquitetura da Internet do que o NAT

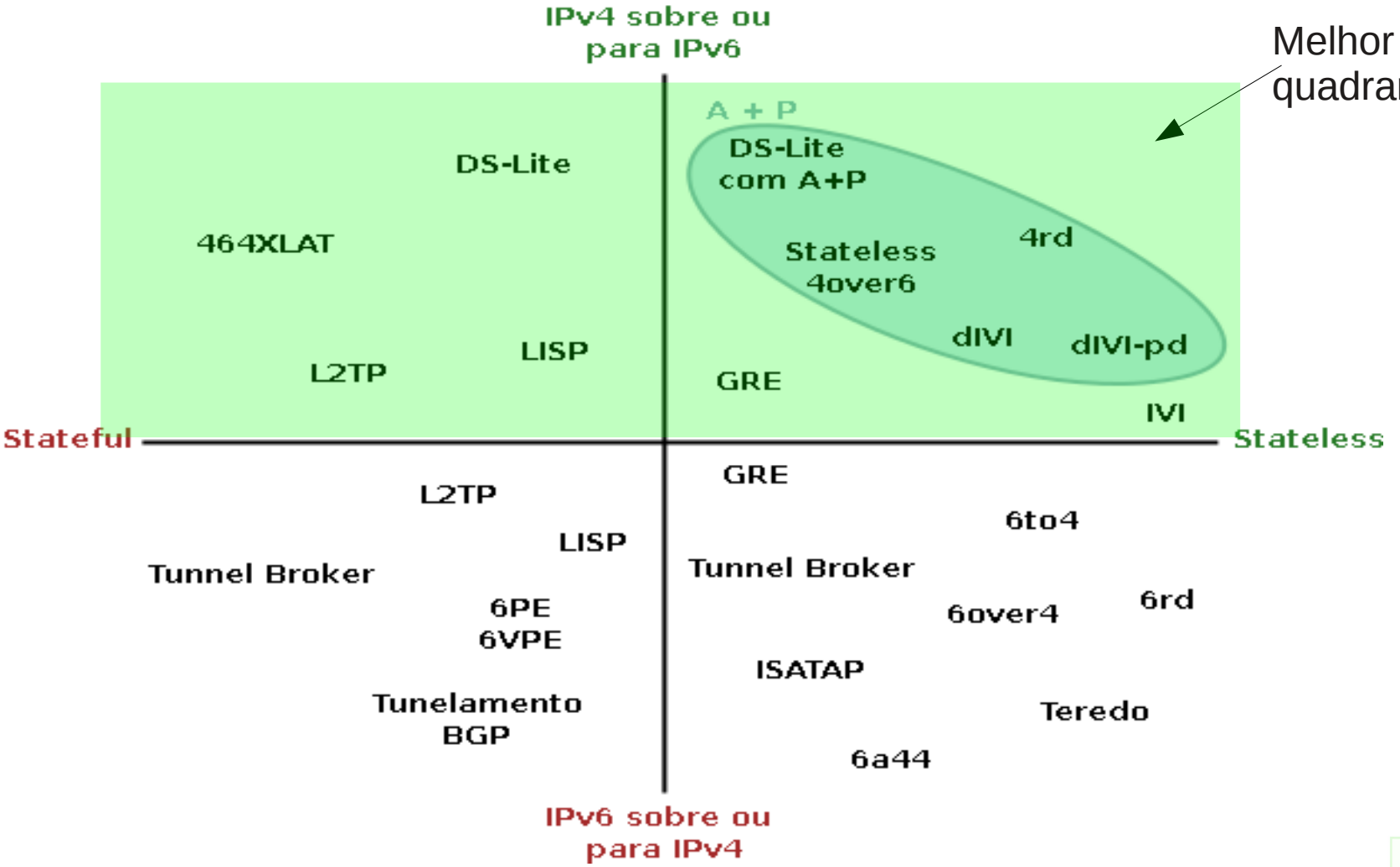
NAT444



NAT444

- O NAT444 (draft-shirasaki-nat444-05) não é uma técnica de transição para o IPv6, mas uma forma de prolongar a vida útil do IPv4, por meio do compartilhamento
- O NAT444 pode ser usado, contudo, em conjunto com a implantação do IPv6
- O NAT444 implica na utilização de dois NATs, um no provedor, outro no usuário, e quebra a conectividade fim a fim, e potencialmente diversas aplicações
- Existe uma proposta para reservar-se um bloco IPv4 específico para o NAT444: draft-weil-shared-transition-space-request-15

Classificação das Técnicas



Classificação das Técnicas

- Critérios de escolha
  - IPv6 nativo nos usuários
  - Stateless em detrimento de stateful
  - Evitar técnicas para prolongar a vida do IPv4, sem a adoção concomitante do IPv6
  - Adequação à rede onde será implantada
  - Maturidade e opções de implantação

Classificação das Técnicas

- Pilha Dupla
  - Técnica padrão, adequada para enquanto ainda houver IPs versão 4 disponíveis
- Túneis
  - Pacotes IPv4 encapsulados em IPv6, ou vice-versa
- Tradução
  - Pacotes IPv4 traduzidos para IPv6, e vice-versa
- ALG (Application Layer Gateway)
  - Gateways que lidam com aplicações específicas

Classificação das Técnicas

- Stateful
  - É necessário manter informações de estado, como tabelas com endereços e portas.
- Stateless
  - Não é necessário manter estado, cada pacote é processado de forma independente, de acordo com uma regra ou algorítmo.
- **Stateless** é preferível a Stateful.
  - Escala melhor
  - É mais barato, do ponto de vista computacional e financeiro.

Considerações finais

- Deve-se usar pilha dupla, se não houver falta de endereços IPv4
- A Internet caminha para ser somente IPv6, deve-se preferir técnicas que usem IPv6 nativo
- Deve-se evitar duplo NAT IPv4, o NAT444
  - Técnicas com dupla tradução e túneis IPv4 sobre IPv6 evitam a necessidade do duplo NAT, para compartilhar o IPv4
- Stateless preferível a stateful
- Caso stateful seja necessário, que seja preferivelmente do lado do usuário, e não do provedor

Laboratório NAT64

Contatos

- Equipe do CEPTRO, NIC.br
  - ipv6@nic.br
- Coordenador do IPv6.br
  - Antonio M. Moreiras

    moreiras@nic.br

    Inoc-dba: 22548*amm

Backup

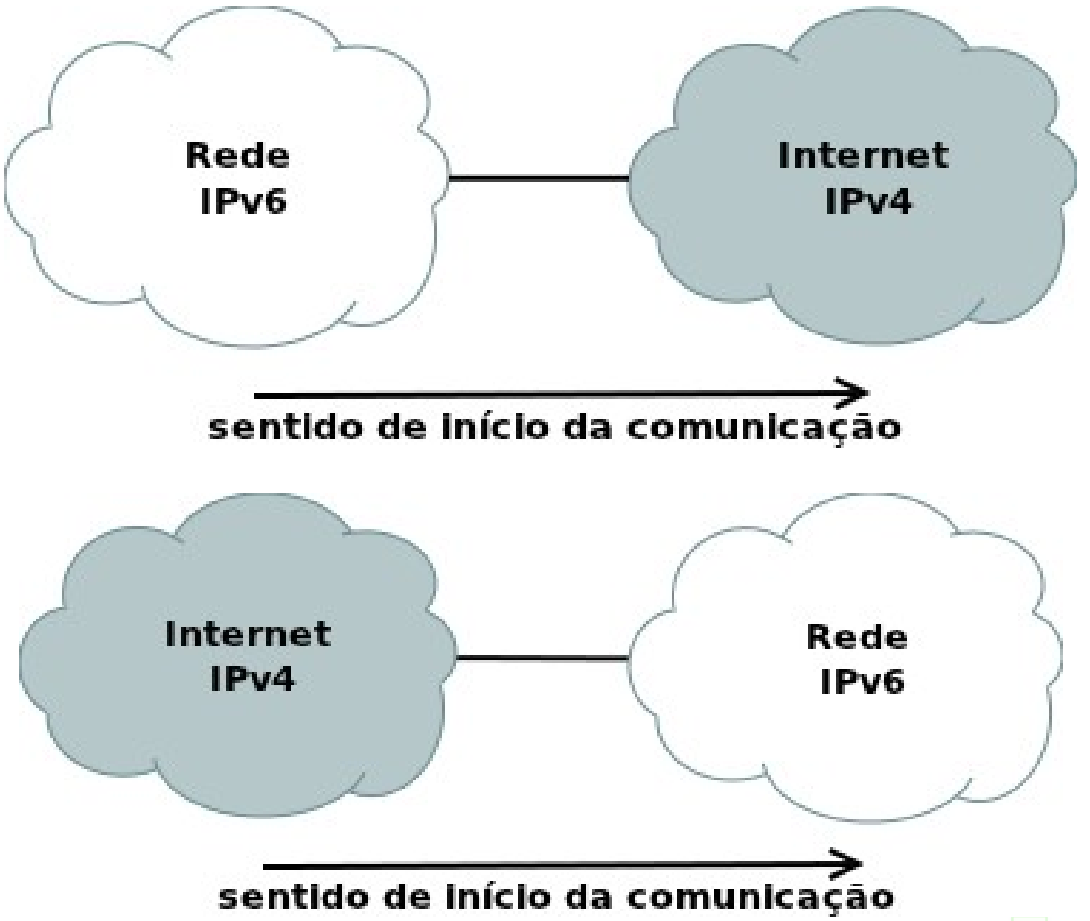
- Detalhamento dos cenários

Cenários

- Mostram as diferentes situações em que há necessidade de redes IPv6 e IPv4 coexistirem e interoperarem
- Generalização e extensão dos cenários apresentados na **RFC 6144**

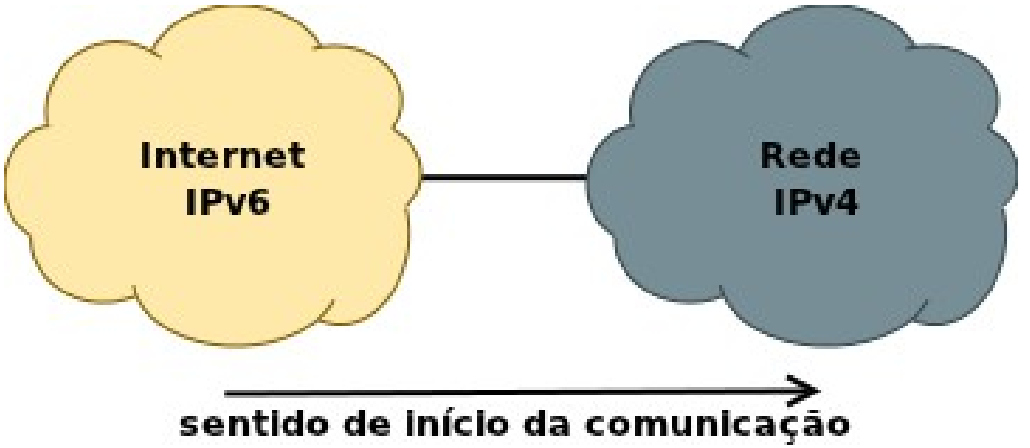
Cenários 1 e 2

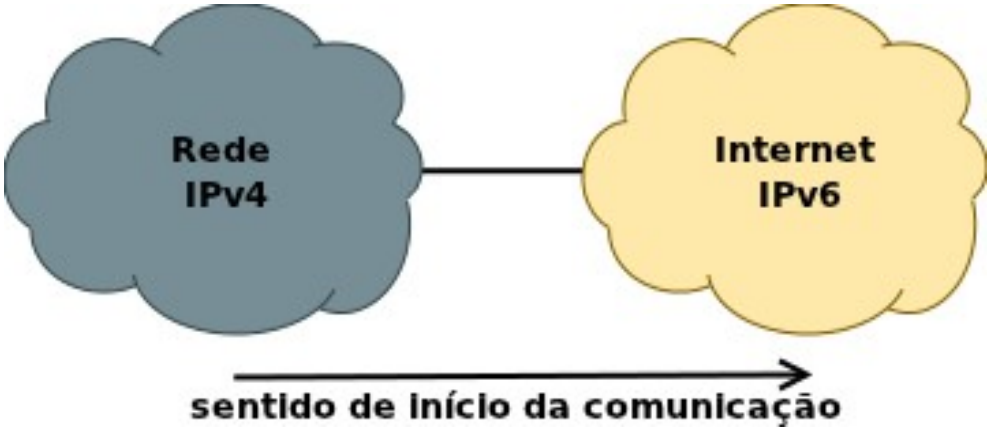
- O cenário 1 representa uma rede com falta de endereços v4, ou uma rede nova, somente v6.
  - Soluções simples, stateless ou stateful.
- O cenário 2, onde há serviços na rede, é mais complexo.
  - Mapeamento 1:1 frequentemente não pode ser feito.
  - Soluções normalmente stateful.
  - Stateless pode ser possível se o mapeamento puder ser feito parcialmente.



Cenários 3 e 4

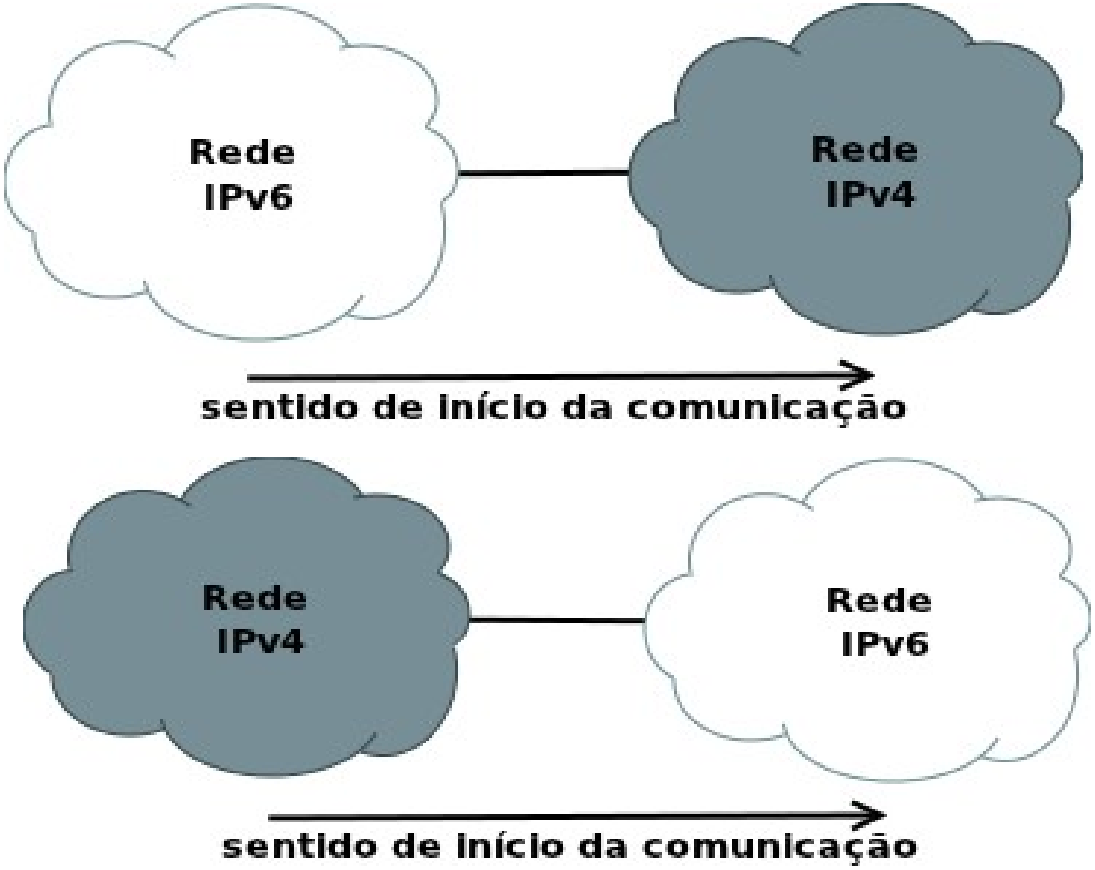
- O cenário 3 representa, tipicamente, uma rede legada IPv4 que tem de responder a requisições da Internet v6.
  - Soluções stateful.
- O cenário 4 pode ser encontrado num estágio avançado da migração, onde usuários IPv4 têm de acessar serviços somente IPv6 na Internet.
  - Sem solução de tradução na própria rede.





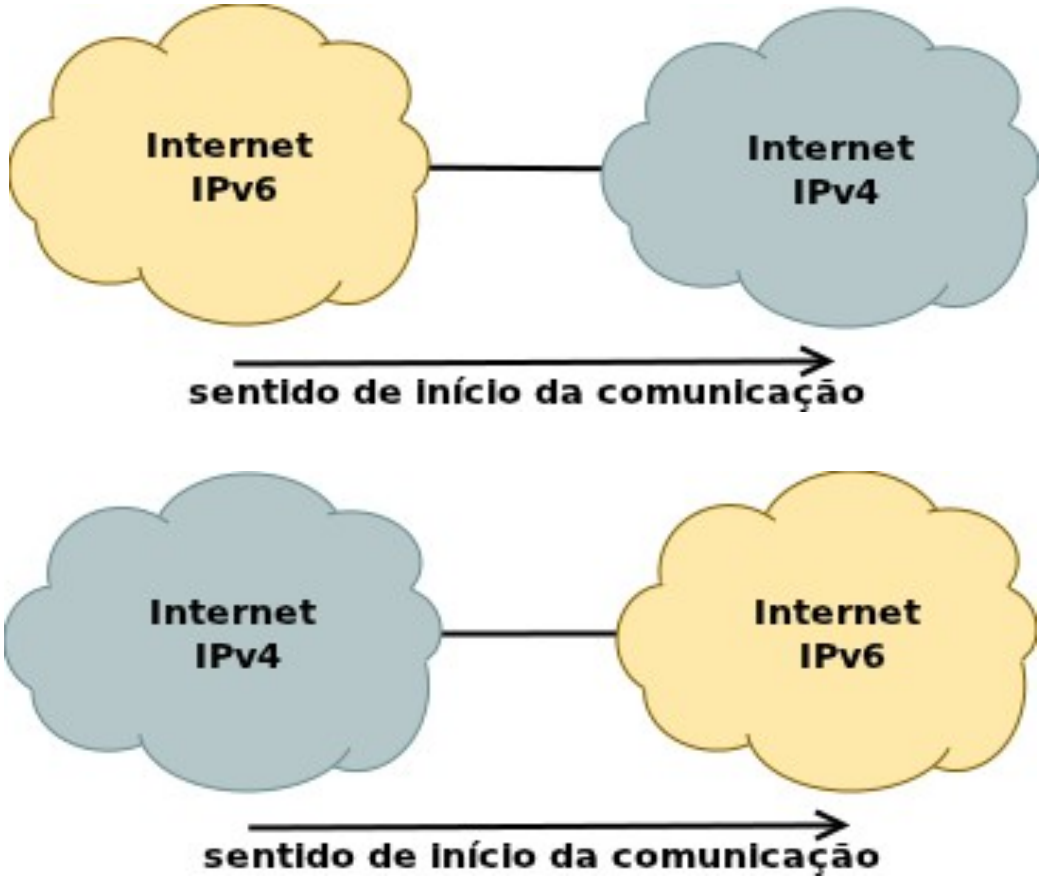
Cenários 5 e 6

- Similares os cenários 1 e 2.
- O cenário 5 representa uma rede com falta de endereços v4, ou uma rede nova, somente v6.
  - Soluções simples, stateless ou stateful.
- O cenário 6, onde há serviços na rede, é mais complexo.
  - Mapeamento 1:1 frequentemente não pode ser feito.
  - Soluções normalmente stateful.
  - Stateless pode ser possível se o mapeamento puder ser feito parcialmente.



Cenários 7 e 8

- Os cenários 7 e 8 representam uma situação ideal, onde qualquer dispositivo na Internet IPv6 poderia comunicar-se com qualquer outro na Internet IPv4, e vice-versa.
- Solução improvável.



Cenários 9 e 10

- Os cenários 9 e 10 representam situações onde é necessário fazer duas redes IPv6 comunicarem-se através da Internet IPv4, ou duas redes IPv4 comunicarem-se através da Internet IPv6.
  - Soluções de tunelamento.