



INSTITUTO FEDERAL

Norte de Minas Gerais

Campus Januária

Admin. Serviços de Redes

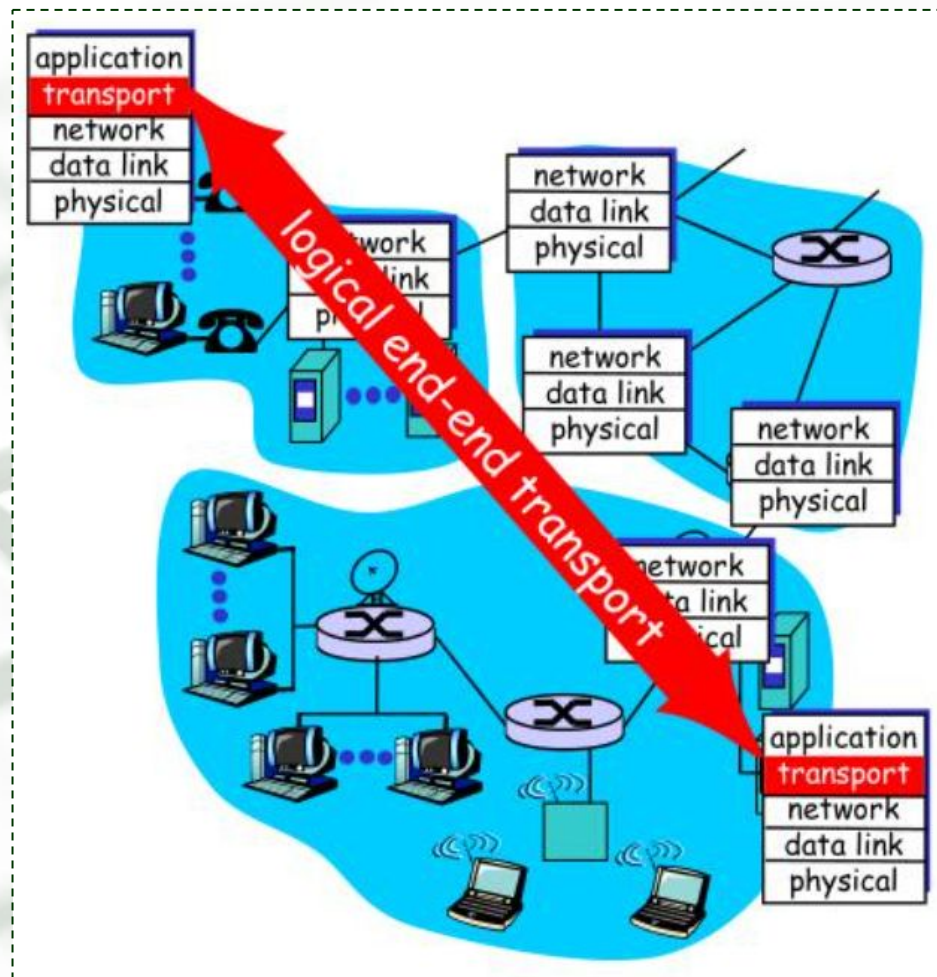
- NAT / CGNAT -



TCP / IP

A **Conectividade fim-a-fim** sempre foi uma premissa fundamental da **Arquitetura TCP/IP**.

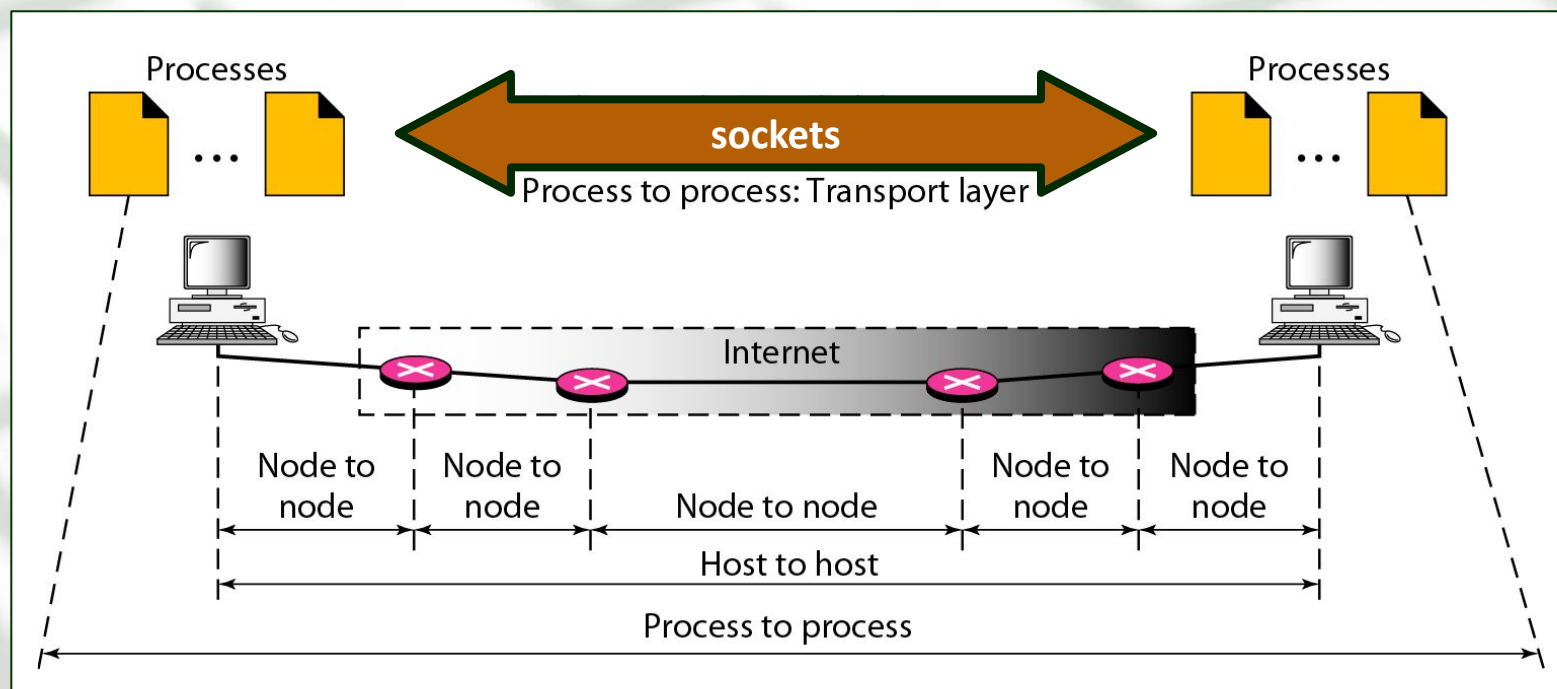
Isso significa dizer que **qualquer nó da rede pode estabelecer conexão, de ponta a ponta, com qualquer outro nó.**





TCP / IP

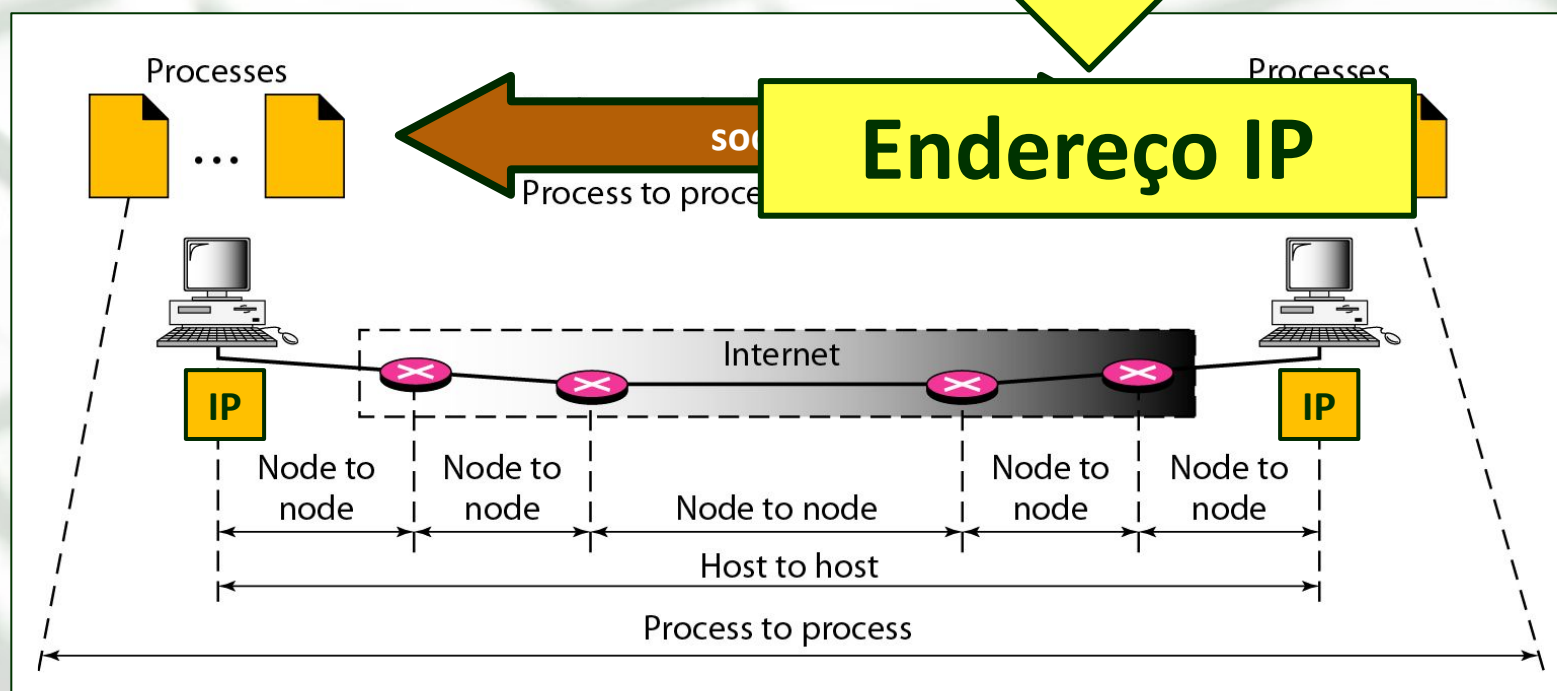
- Contudo, para que isso funcione, é necessário que **cada host possua um endereço globalmente único**, para que possa ser localizado pelos pares na rede...





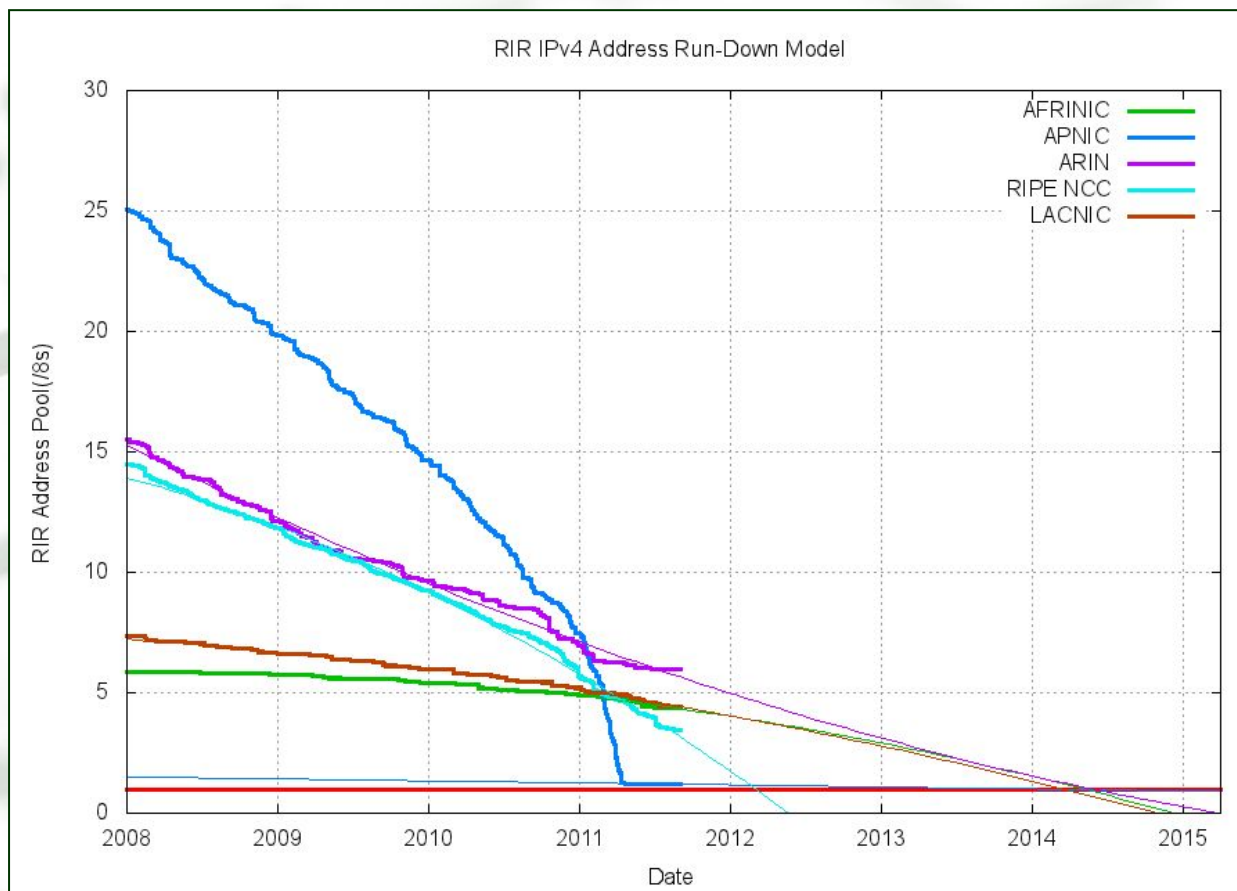
TCP / IP

- Contudo, para que isso funcione, é necessário que **cada host possua um endereço globalmente único**, para que possa ser localizado pelos pares na rede...





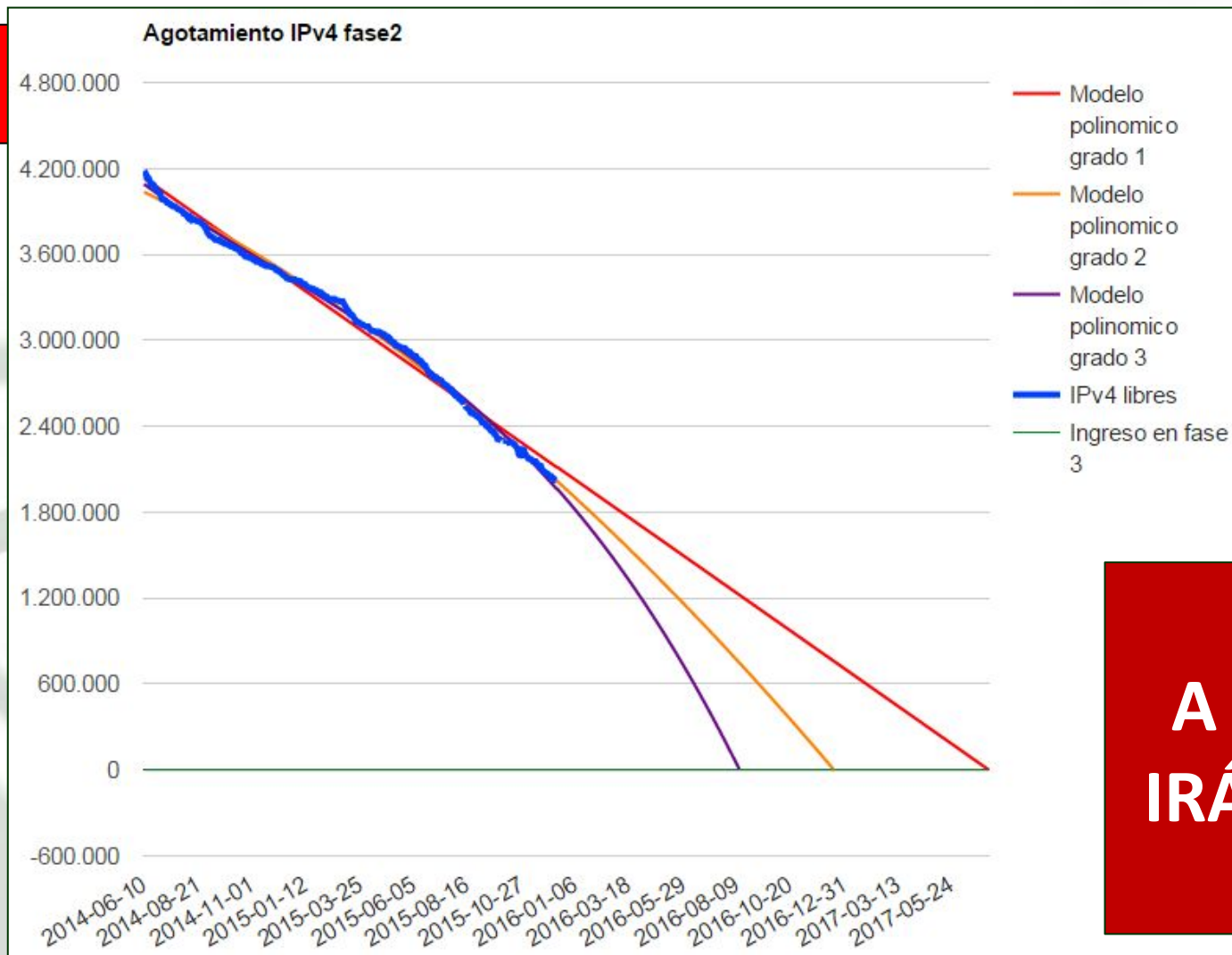
OS ENDEREÇOS IP IRÃO SE ESGOTAR!





INSTITUTO FEDERAL
Norte de Minas Gerais
Campus Januária

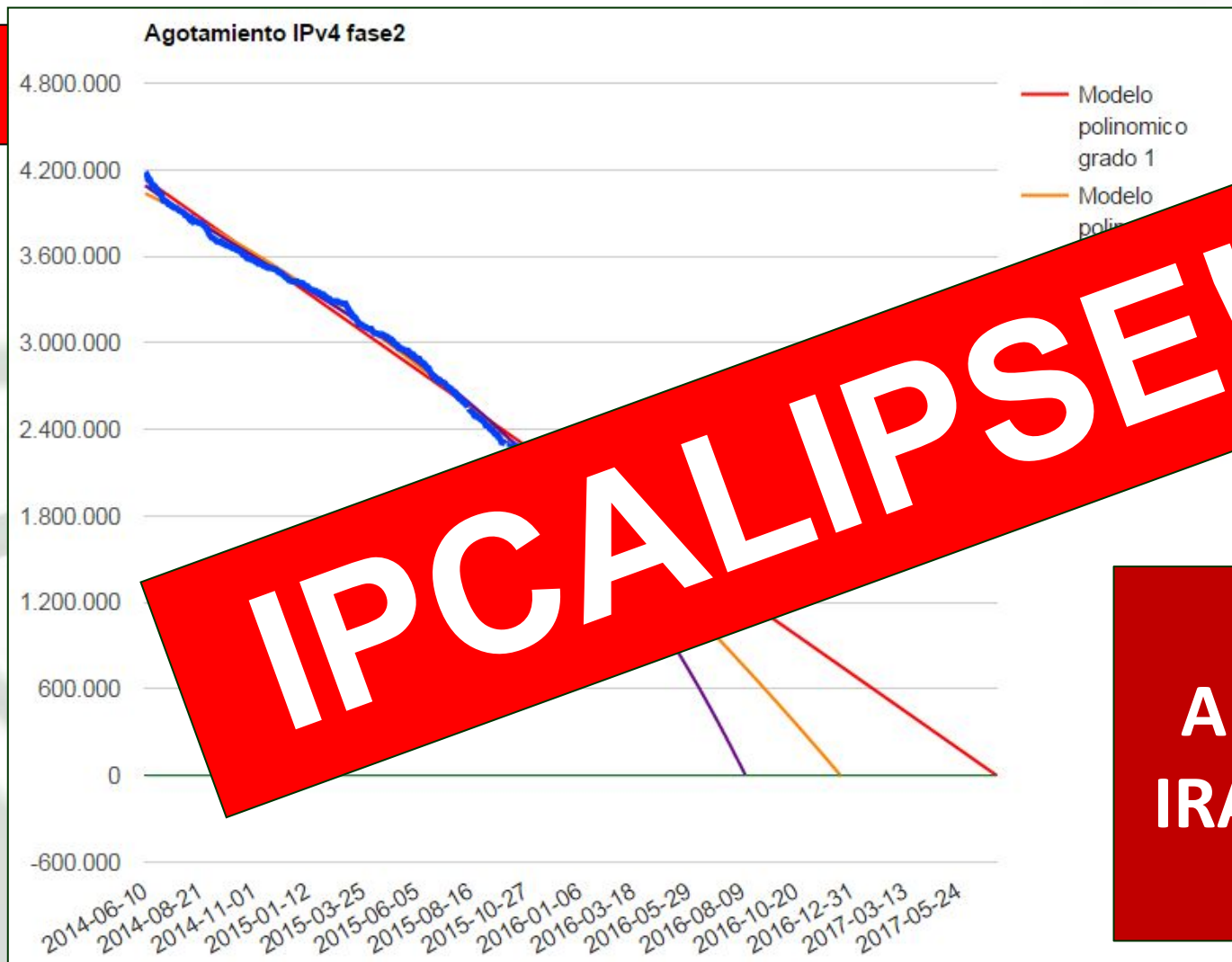
TCP / IP



**A INTERNET
IRÁ ACABAR!**



TCP / IP

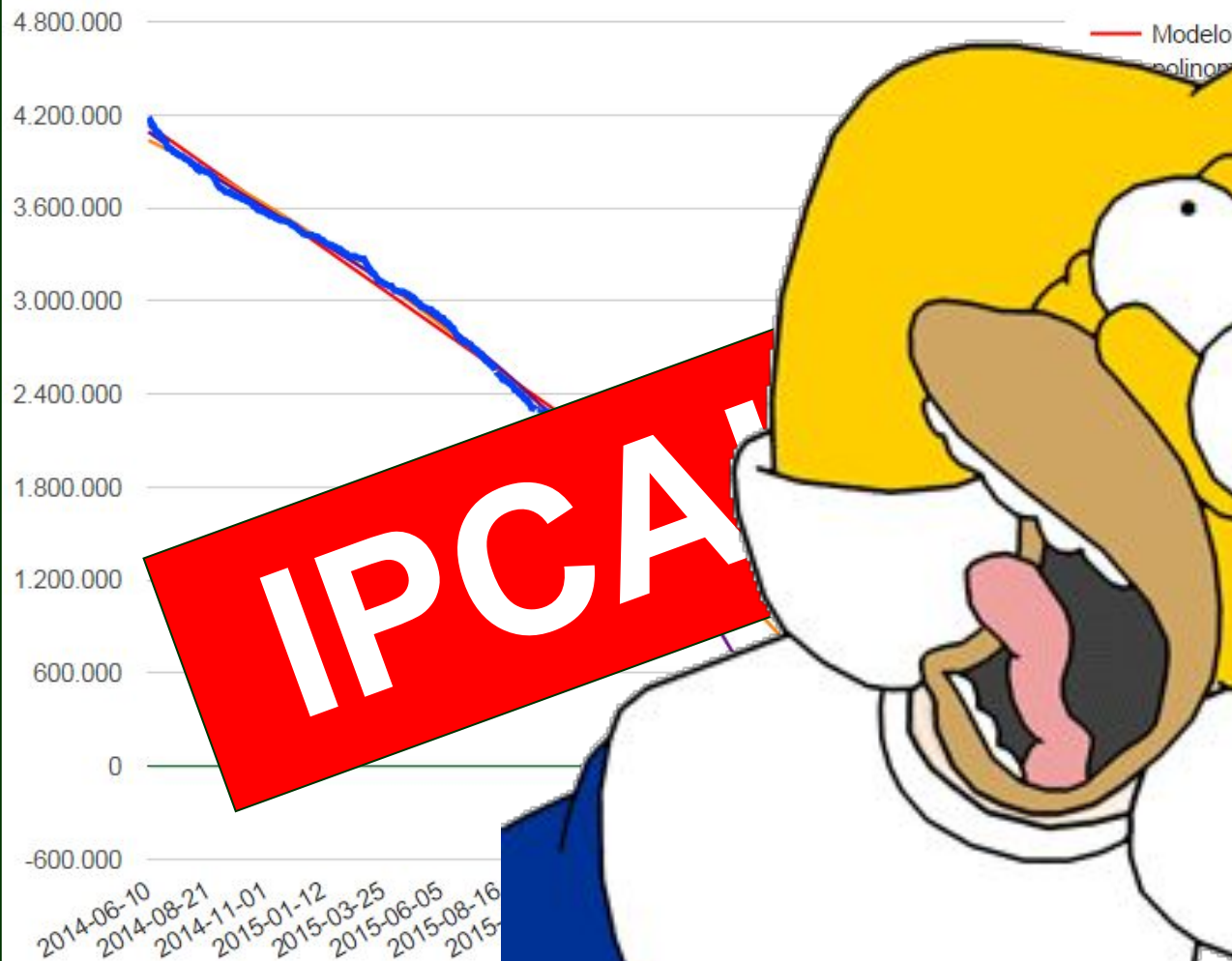


**A INTERNET
IRÁ ACABAR!**



TCP / IP

Agotamiento IPv4 fase2





TCP / IP

CALMA...

Nada que uma boa GAMBIARRA não resolva...





NAT

CALMA...

Nada que uma boa **GAMBIARRA** não resolva...



NAT



NAT / RFC 1918

- Na década de 90, a **RFC 1918** estabeleceu que 03 faixas de rede IPv4 **não seriam mais roteáveis na Internet**.
- Essas faixas, denominadas faixas de **Rede Privada**, seriam utilizadas apenas para **endereçar hosts internos às redes locais**, sejam domésticas ou empresariais...

RFC 1918

Address Allocation for Private Internets

February 1996

3. Private Address Space

The Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of the IP address space for private internets:

| | | | |
|-------------|---|-----------------|---------------------|
| 10.0.0.0 | - | 10.255.255.255 | (10/8 prefix) |
| 172.16.0.0 | - | 172.31.255.255 | (172.16/12 prefix) |
| 192.168.0.0 | - | 192.168.255.255 | (192.168/16 prefix) |



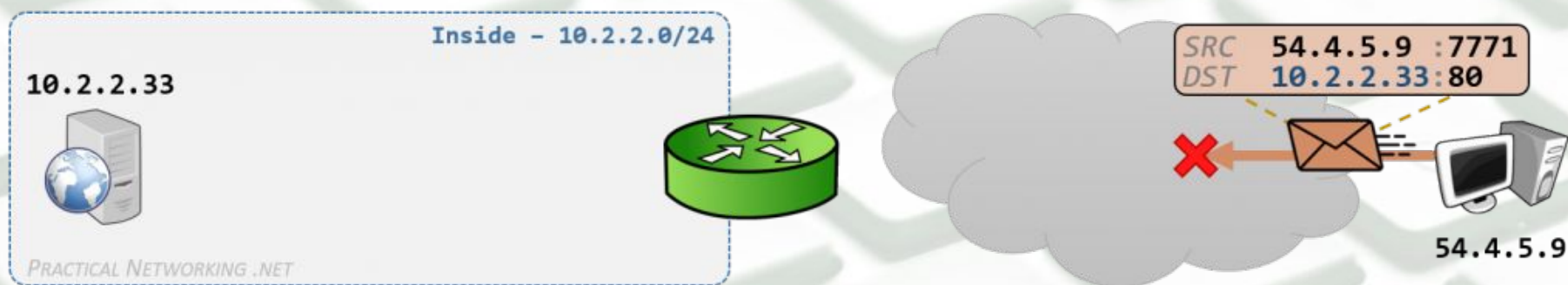
NAT / RFC 1918

- Com essa técnica, os inúmeros hosts das redes LANs não necessitam mais consumir endereços globalmente únicos da Internet (chamados **Endereços Públicos**).
- As diversas redes LANs podem **usar a mesma faixa de rede**, por exemplo, 192.168.10.0/24, **sem que uma interfira no funcionamento das outras**, afinal, eram redes apenas de âmbito local.
- Mas isso gerou um problema para a interconexão de redes...



NAT / RFC 1918

- Como responder à uma requisição de um cliente em rede privada?
- Como acessar um serviço provido em uma rede privada?

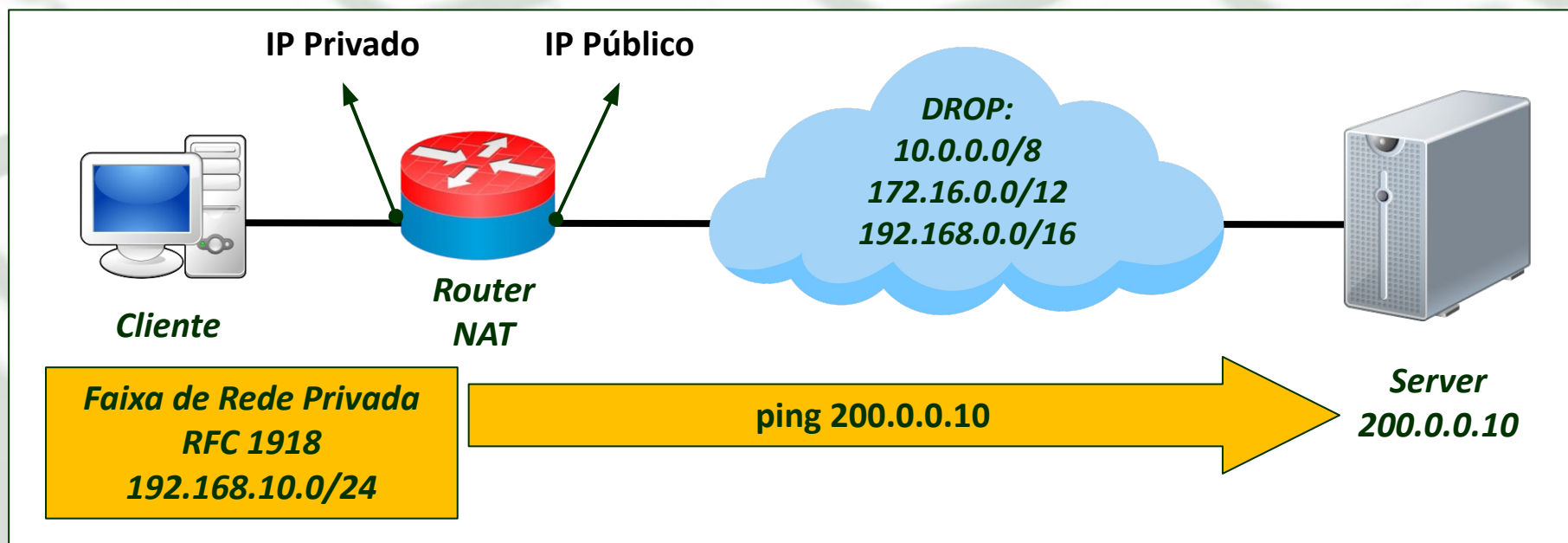


SOLUÇÃO: os hosts locais devem compartilhar um endereço globalmente válido (endereço público).



NAT / RFC 1918

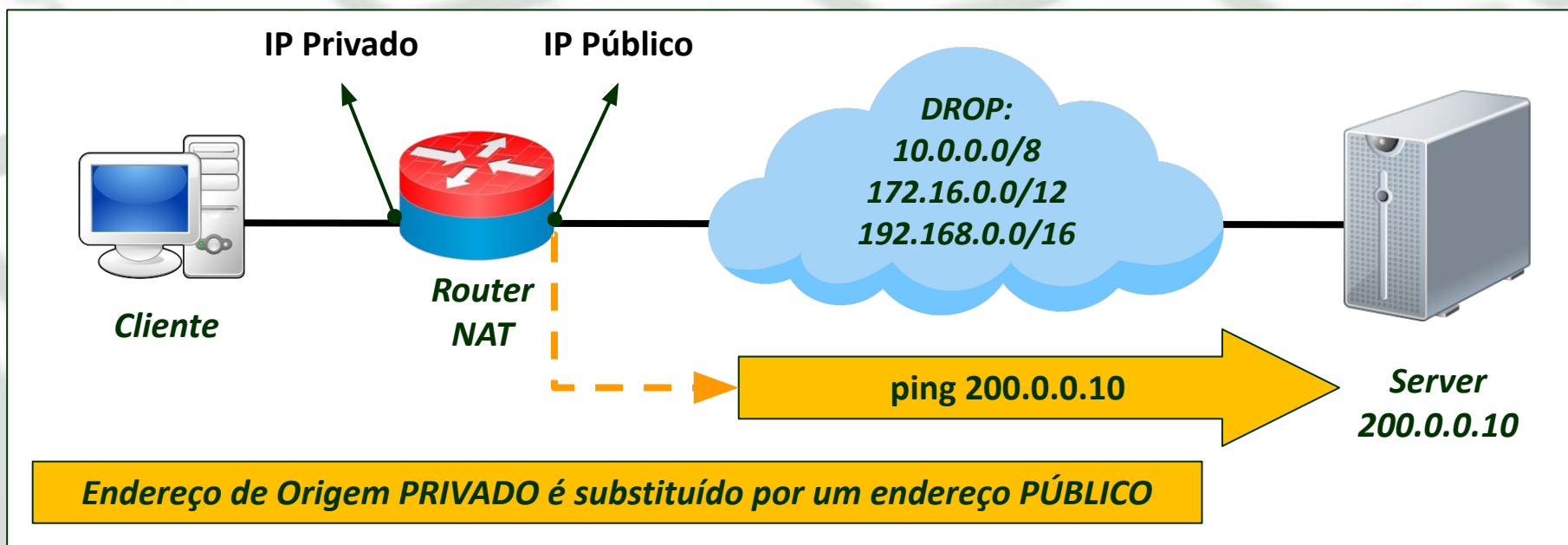
- No mundo real, provedores não propagam pacotes cujo IP de origem ou destino são das faixas definidas pela RFC 1918.
- A comunicação abaixo só é possível após a configuração de um NAT, geralmente realizado no **gateway** das bordas da rede.





NAT / RFC 1918

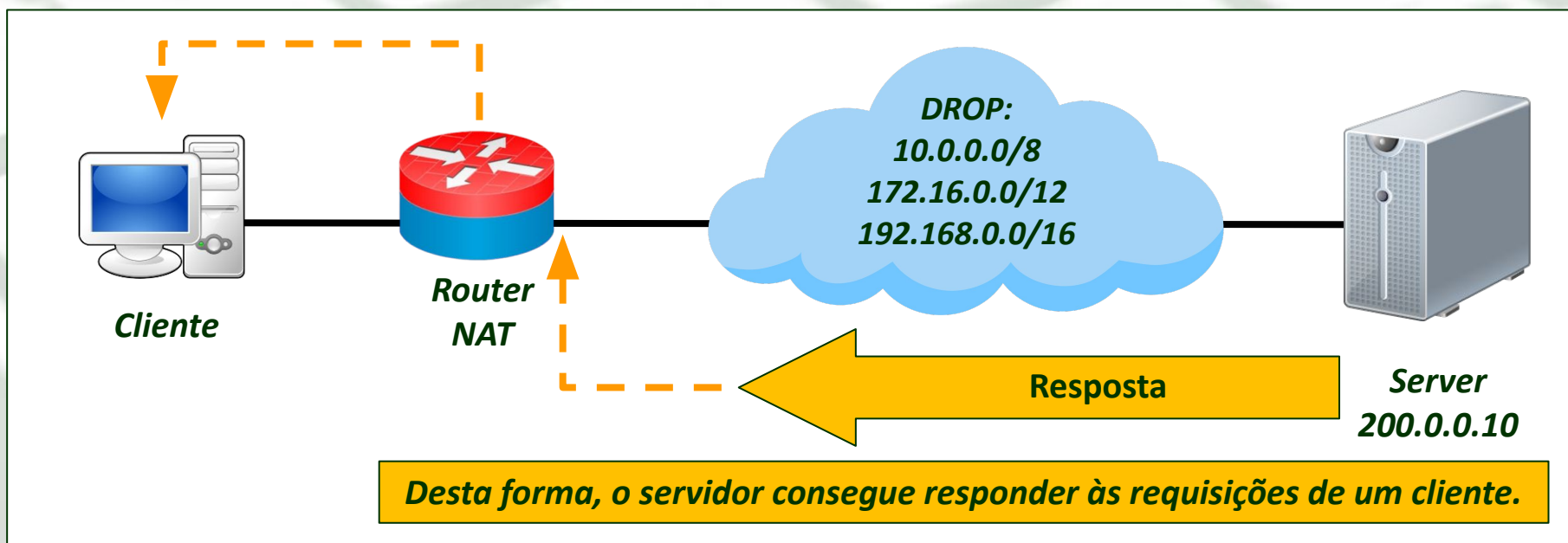
- No mundo real, provedores não propagam pacotes cujo IP de origem ou destino são das faixas definidas pela RFC 1918.
- A comunicação abaixo só é possível após a configuração de um NAT, geralmente realizado no **gateway** das bordas da rede.





NAT / RFC 1918

- No mundo real, provedores não propagam pacotes cujo IP de origem ou destino são das faixas definidas pela RFC 1918.
- A comunicação abaixo só é possível após a configuração de um NAT, geralmente realizado no **gateway** das bordas da rede.

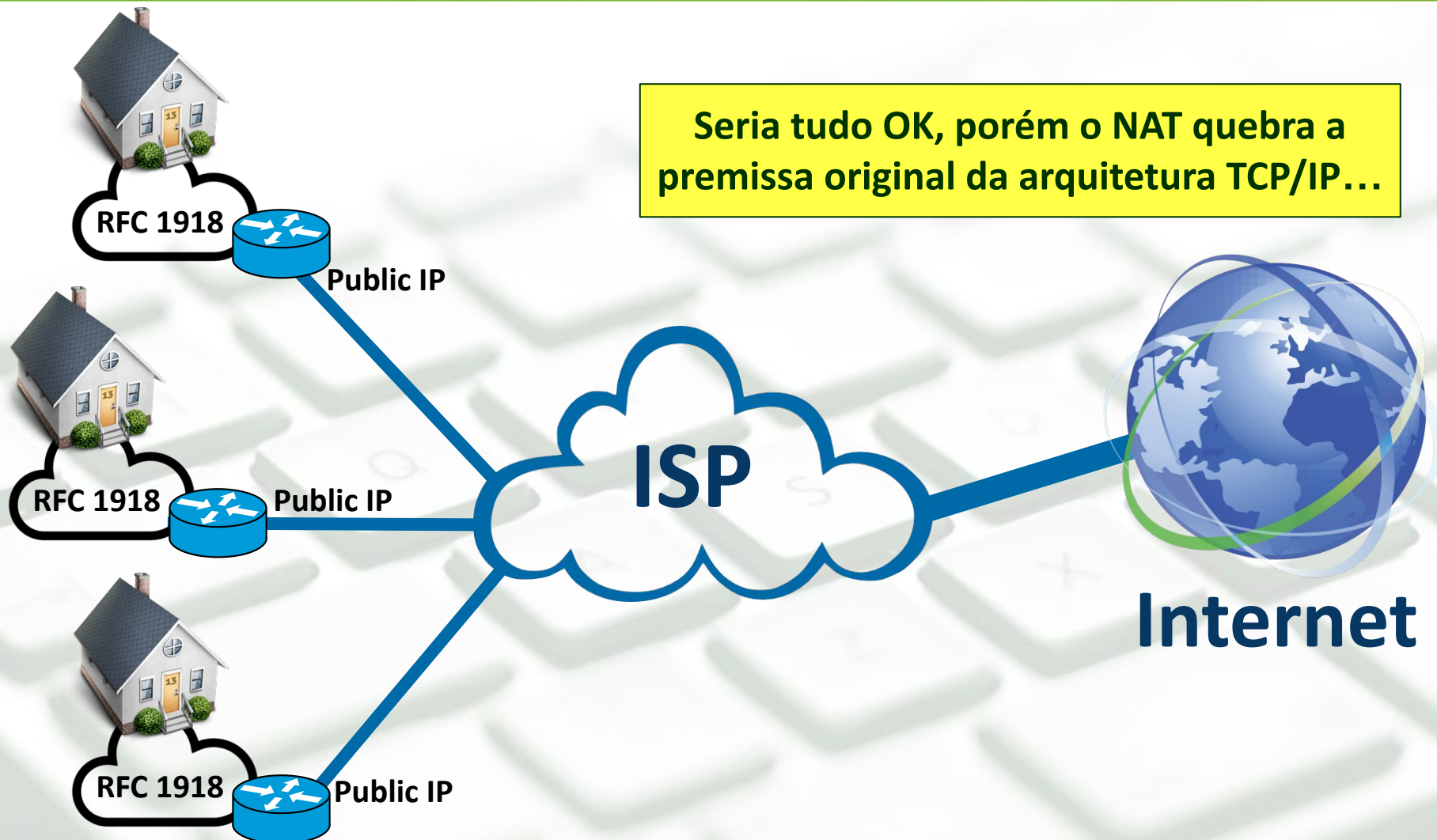




INSTITUTO FEDERAL
Norte de Minas Gerais
Campus Januária

NAT / RFC 1918

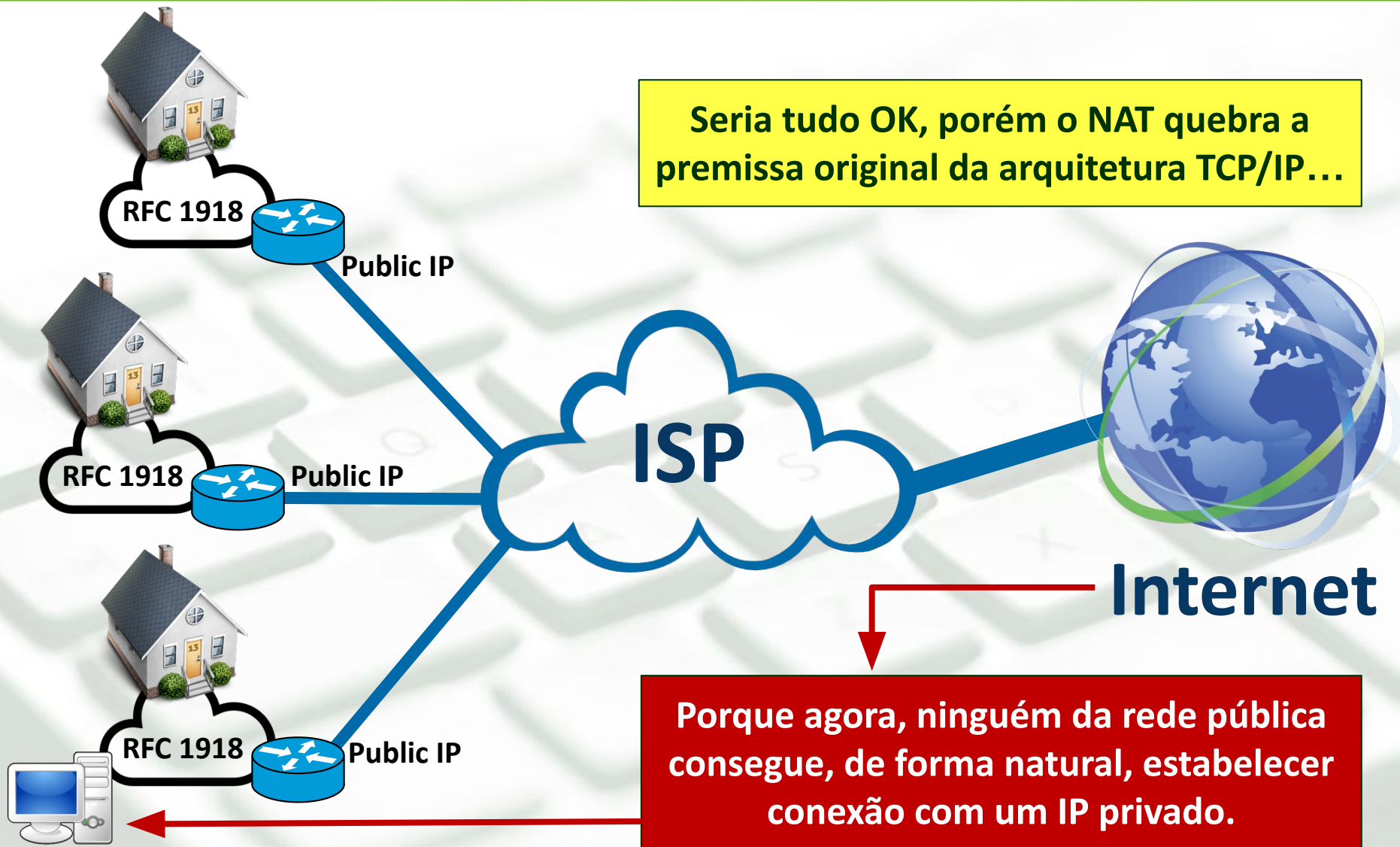
Seria tudo OK, porém o NAT quebra a premissa original da arquitetura TCP/IP...





NAT / RFC 1918

Seria tudo OK, porém o NAT quebra a premissa original da arquitetura TCP/IP...

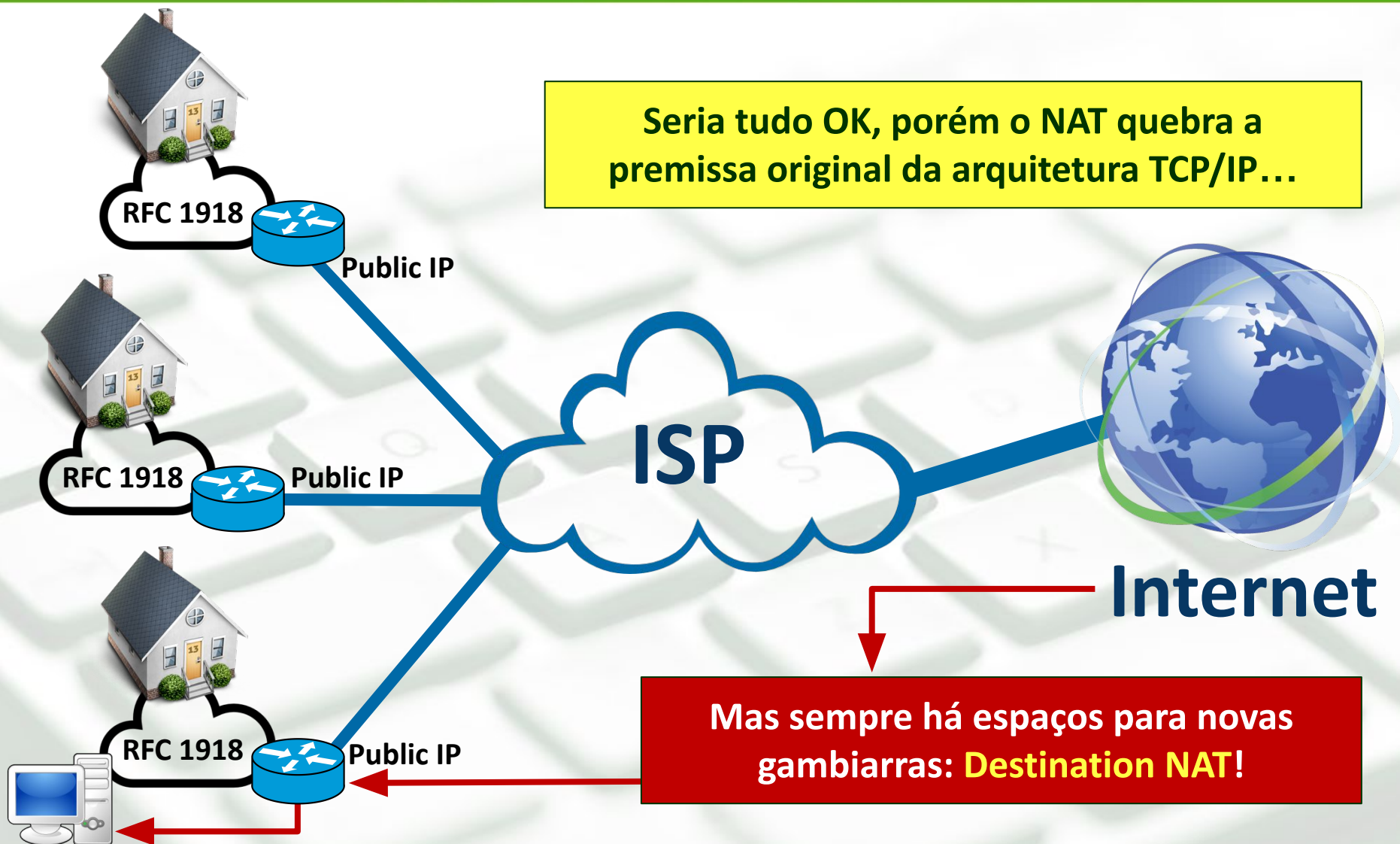


Porque agora, ninguém da rede pública consegue, de forma natural, estabelecer conexão com um IP privado.



NAT / RFC 1918

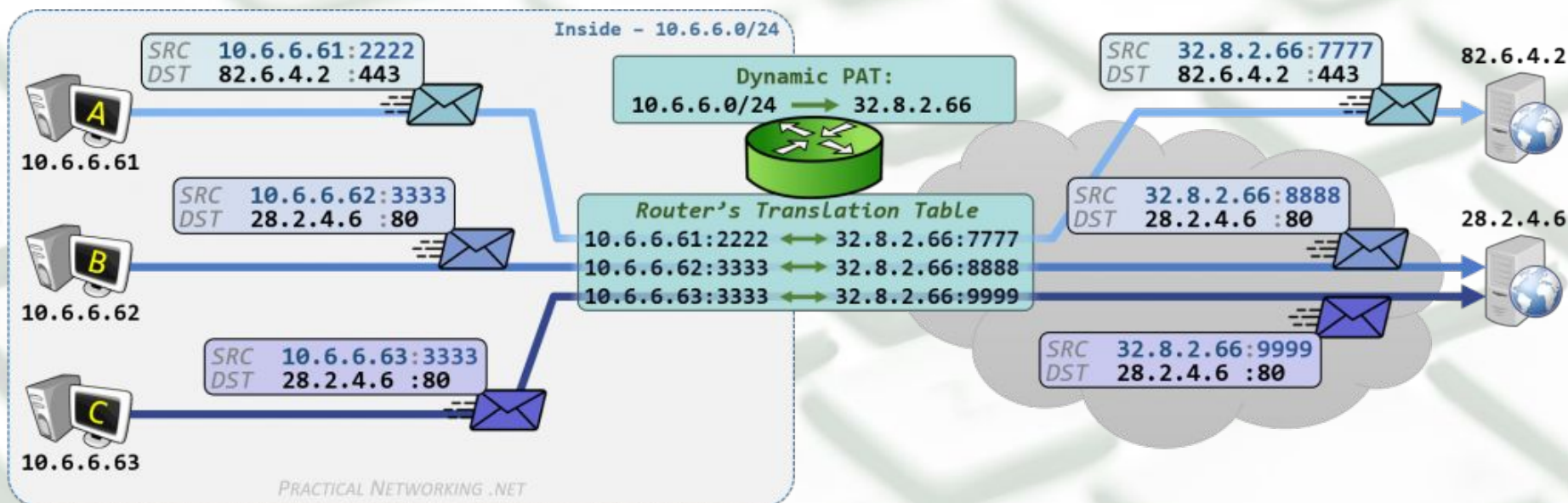
Seria tudo OK, porém o NAT quebra a premissa original da arquitetura TCP/IP...





NAT / RFC 1918

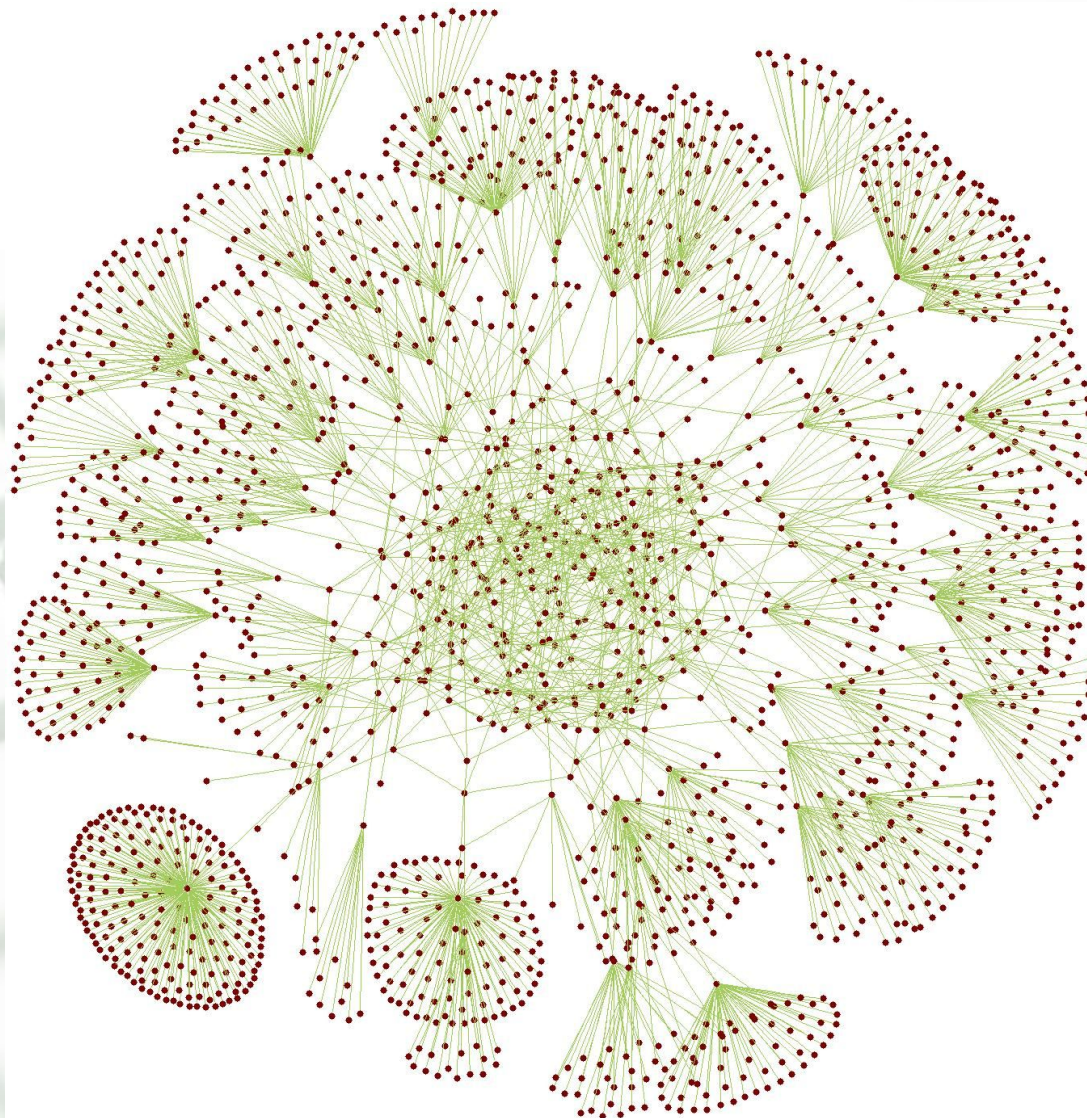
E ainda impõe overheads no processo de comunicação...





INSTITUTO FEDERAL
Norte de Minas Gerais
Campus Januária

Mas não há nada ruim que...





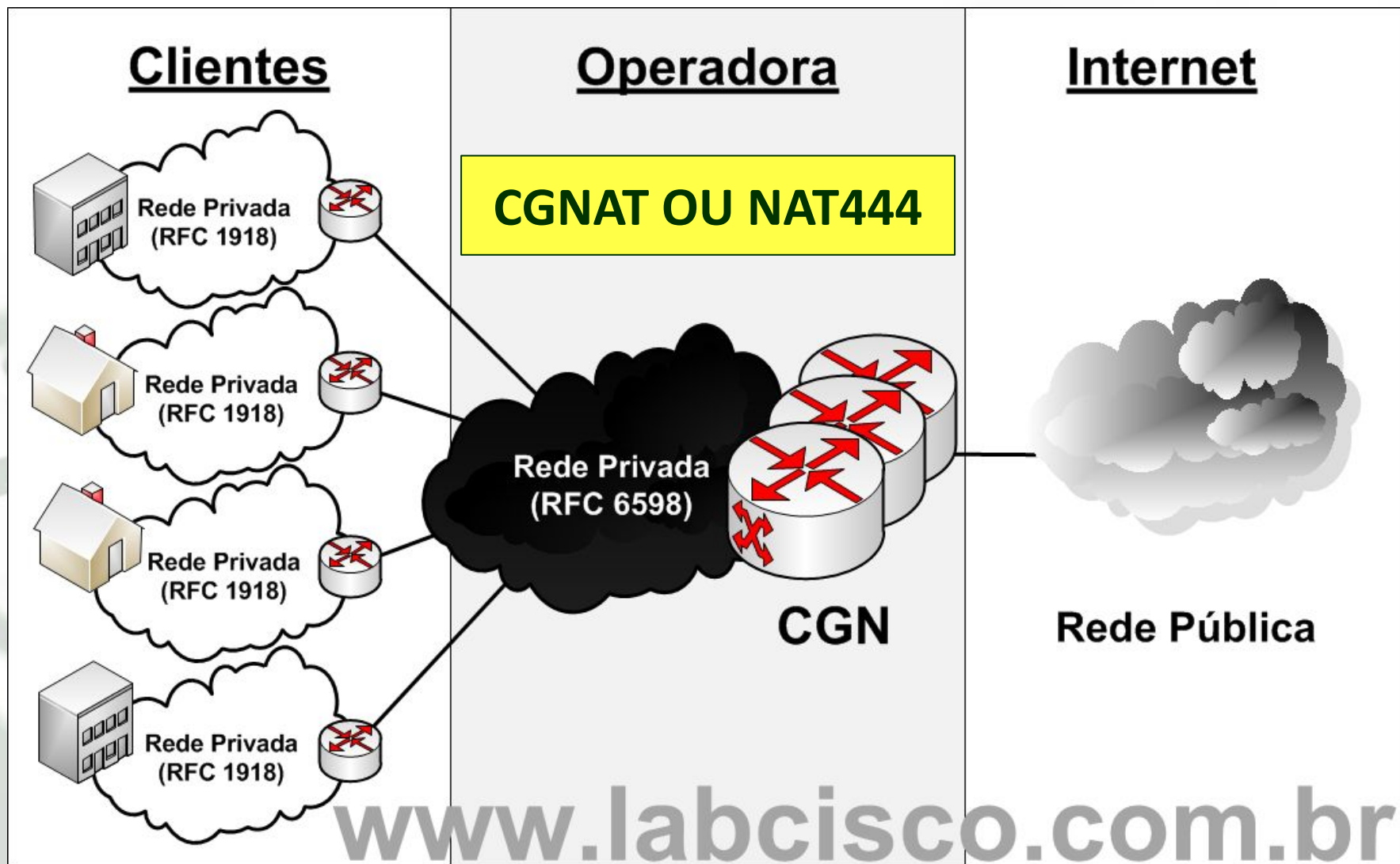
CGNAT / RFC 6598

- Com o número crescente de assinantes de planos de Internet, além do sucesso do 3G/4G, cada vez era maior a **escassez de endereços IP públicos** para que os provedores conseguissem atender seus clientes.
- Em 2012 a IANA estabeleceu uma **nova faixa de endereços privados**, para serem utilizados exclusivamente por provedores (**RFC 6598**).
- Essa nova faixa é a **100.64.0.0/10**

AGORA É NECESSÁRIO FAZER NAT DO NAT... TAMBÉM CHAMADO CGNAT

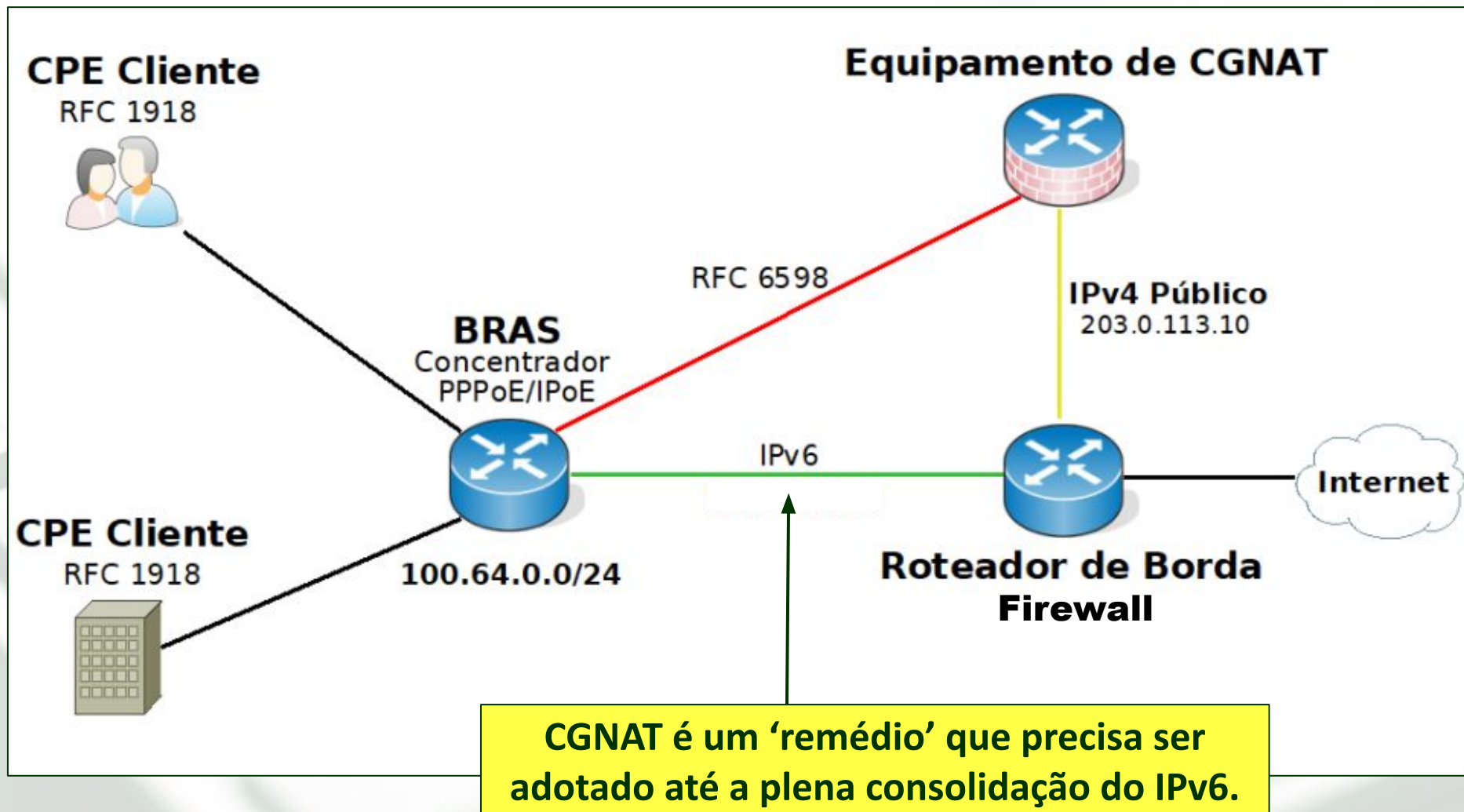


CGNAT / RFC 6598





CGNAT / RFC 6598





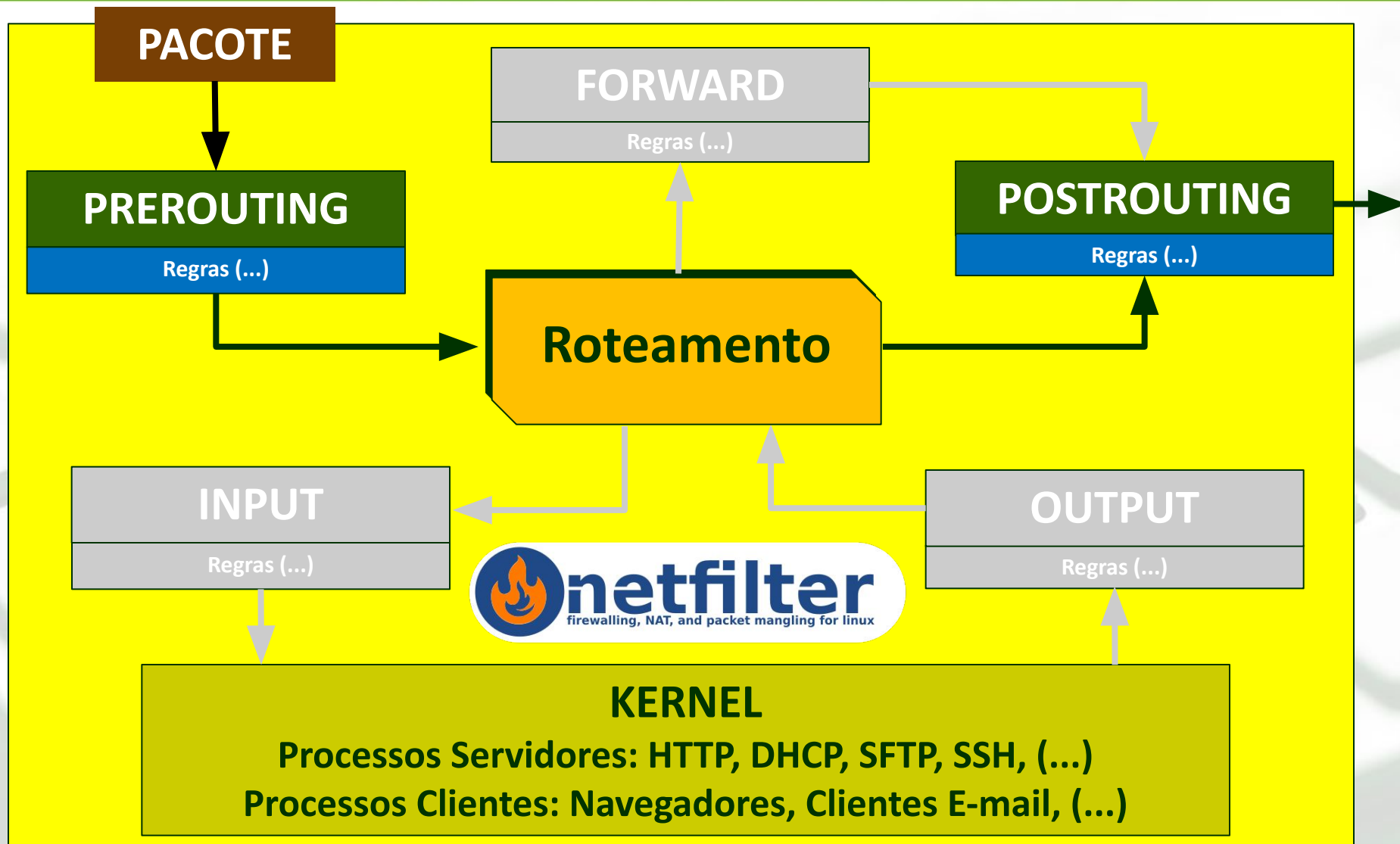
Atividade

- Assista a esse vídeo...
- Leia essa matéria...
- Estude esse conteúdo...





NAT IPtables





■ SNAT (*Source NAT*) com IPTables:

■ Método 1

■ Tradução para endereço *Estático*...

```
# iptables -t nat -A POSTROUTING -o eth1 -j SNAT --to 1.2.3.4
```

└─ Interface de acesso à Internet

■ Método 2

■ Tradução para endereço *Dinâmico*...

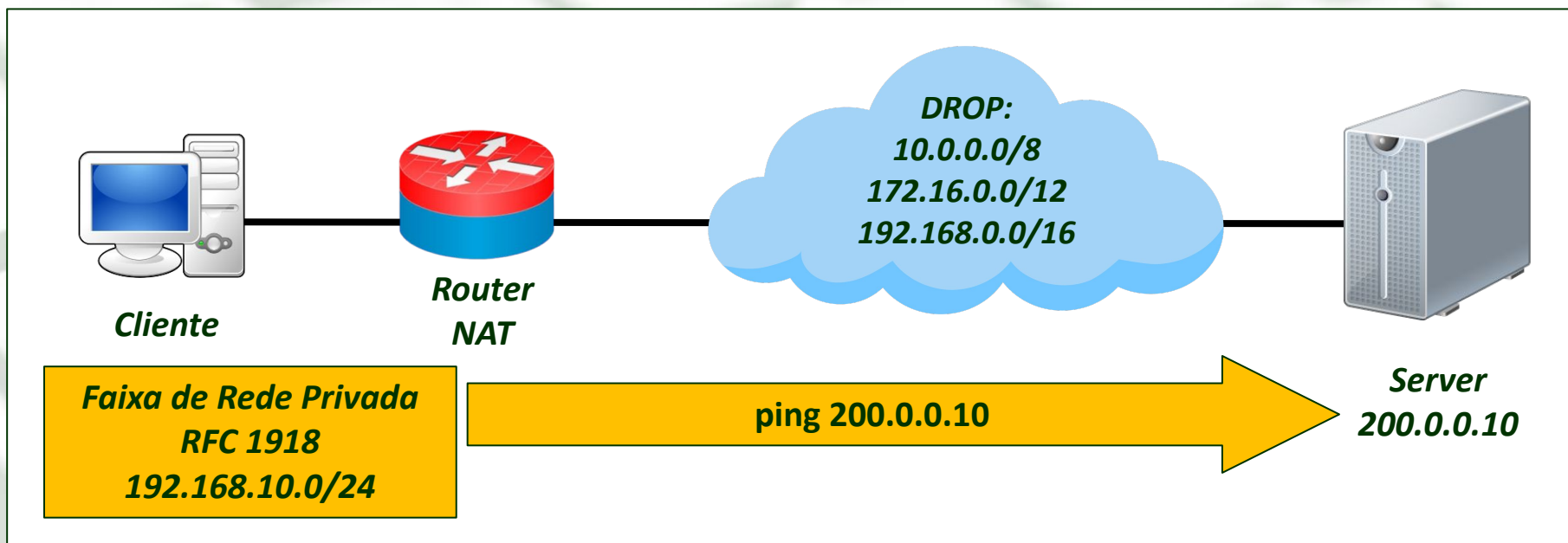
■ Técnica de Mascaramento (*Masquerading*)

```
# iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE
```



Laboratório 13-1

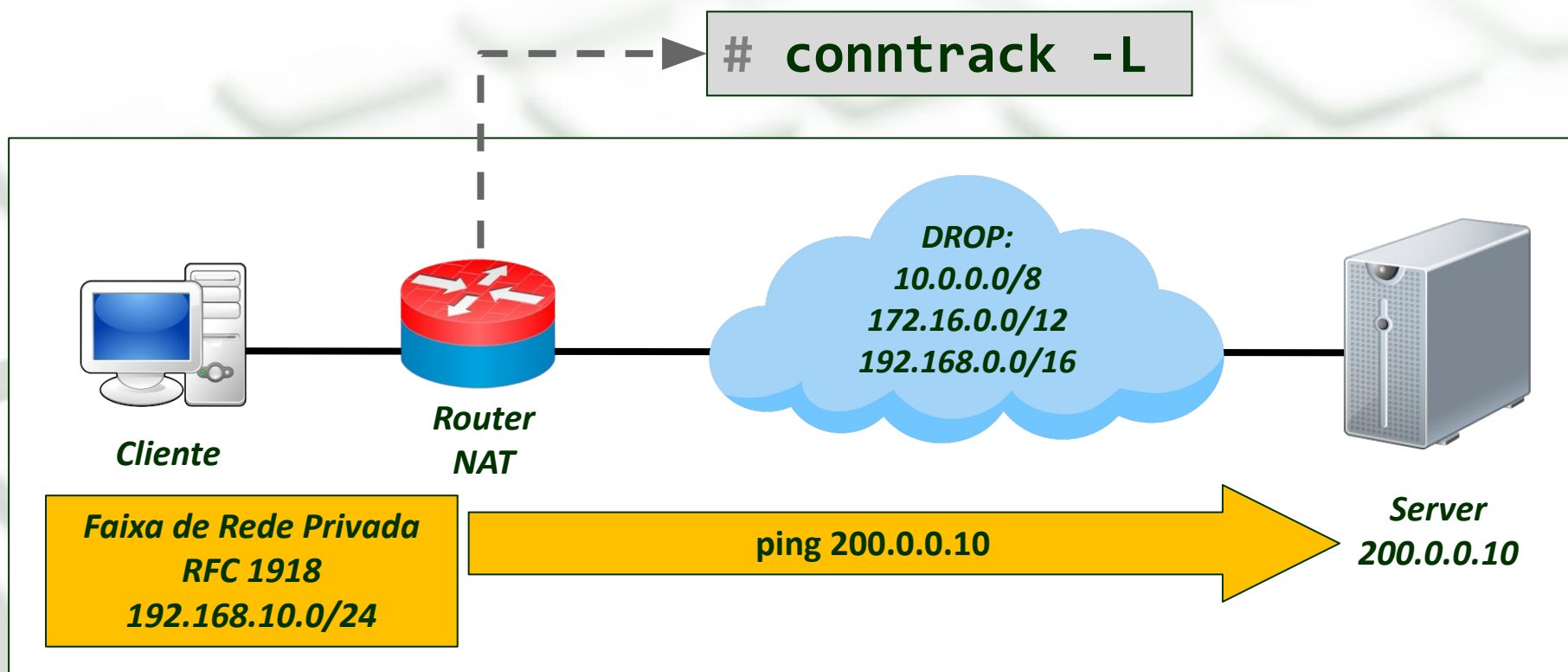
- Implemente o laboratório e verifique o funcionamento do NAT usando o **TCPDUMP**.





Laboratório 13-1

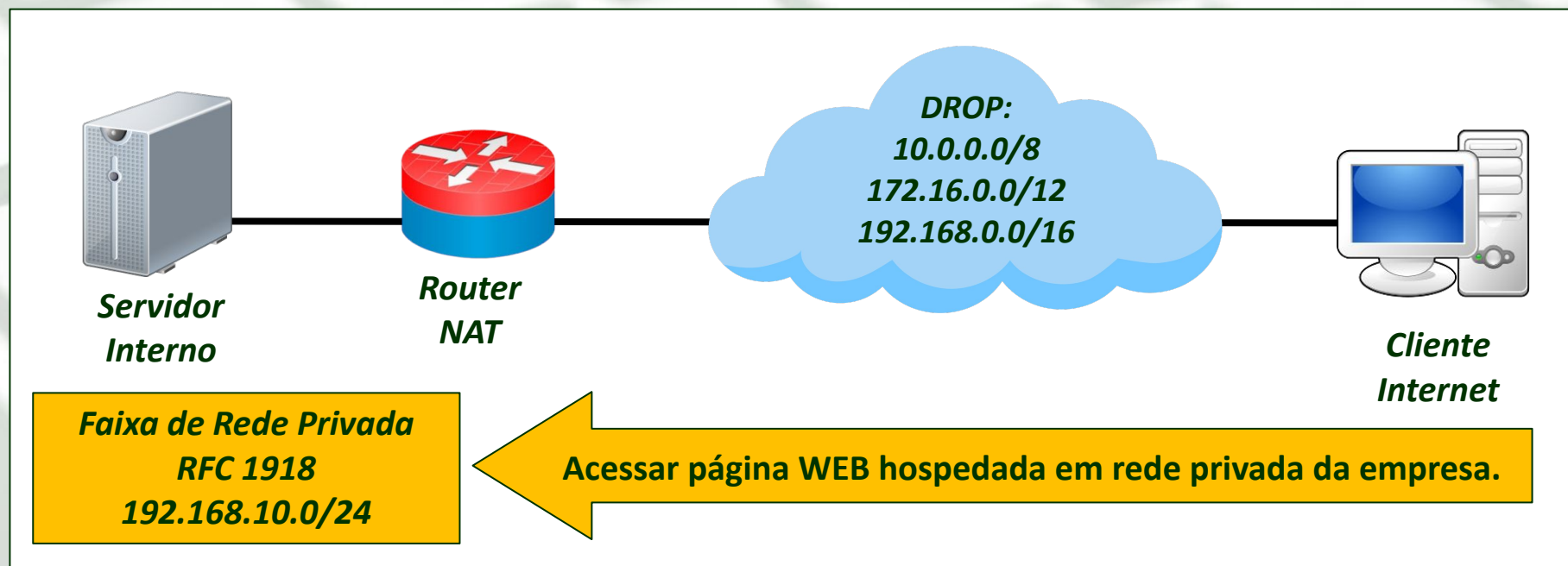
- Utilitário **conntrack**. Execute e analise o retorno...





DNAT

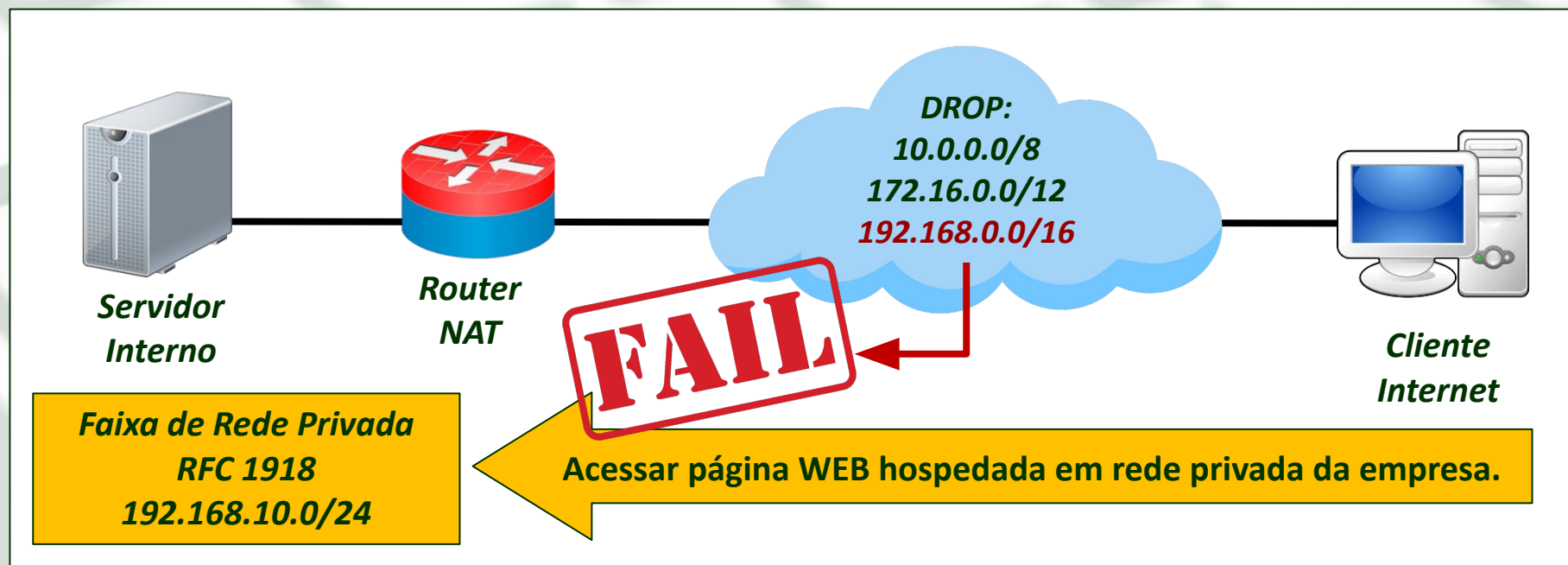
- **Perceba:** O mesmo problema de se tentar acessar a rede pública a partir de uma rede privada, acontece quando **um host na rede pública necessita acessar algum serviço dentro de uma rede privada.**





DNAT

- **Perceba:** O mesmo problema de se tentar acessar a rede pública a partir de uma rede privada, acontece quando **um host na rede pública necessita acessar algum serviço dentro de uma rede privada.**

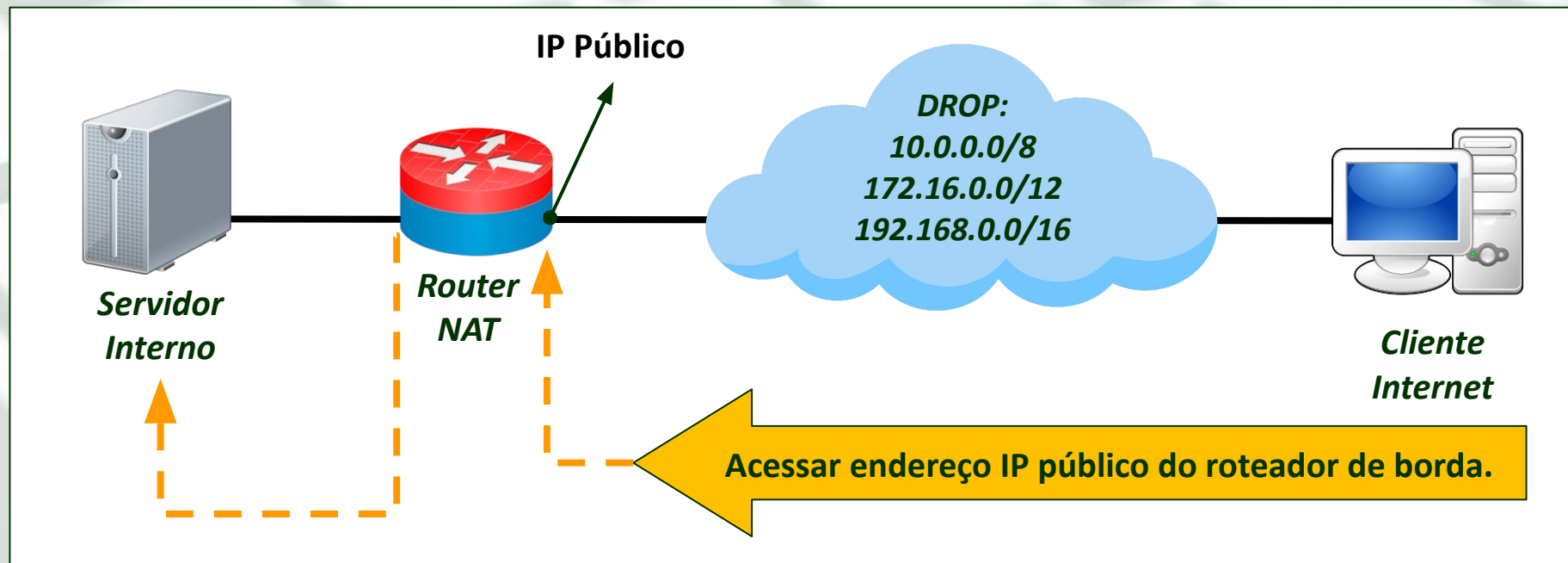




DNAT

■ Solução...

- Configurar Router para realizar Destination NAT.





■ DNAT com IPTables:

- A tradução (conversão) do endereço de destino deve acontecer **antes** que o *router* processe o roteamento do pacote.
- Chain **PREROUTING**.

```
# iptables -t nat -A PREROUTING -i eth1 -j DNAT --to 192.168.10.1
```

└─ Interface com Endereço Público

Nesta regra, todo pacote recebido pela interface eth1 será encaminhado para o endereço 192.168.10.1



DNAT

- Encaminhar apenas protocolos e aplicações específicas:

```
# iptables -t nat -A PREROUTING -i eth1 -p tcp --dport 80 -j  
DNAT --to 192.168.10.1
```

Redirecionar apenas tráfego WEB.

- Redirecionamento de portas:

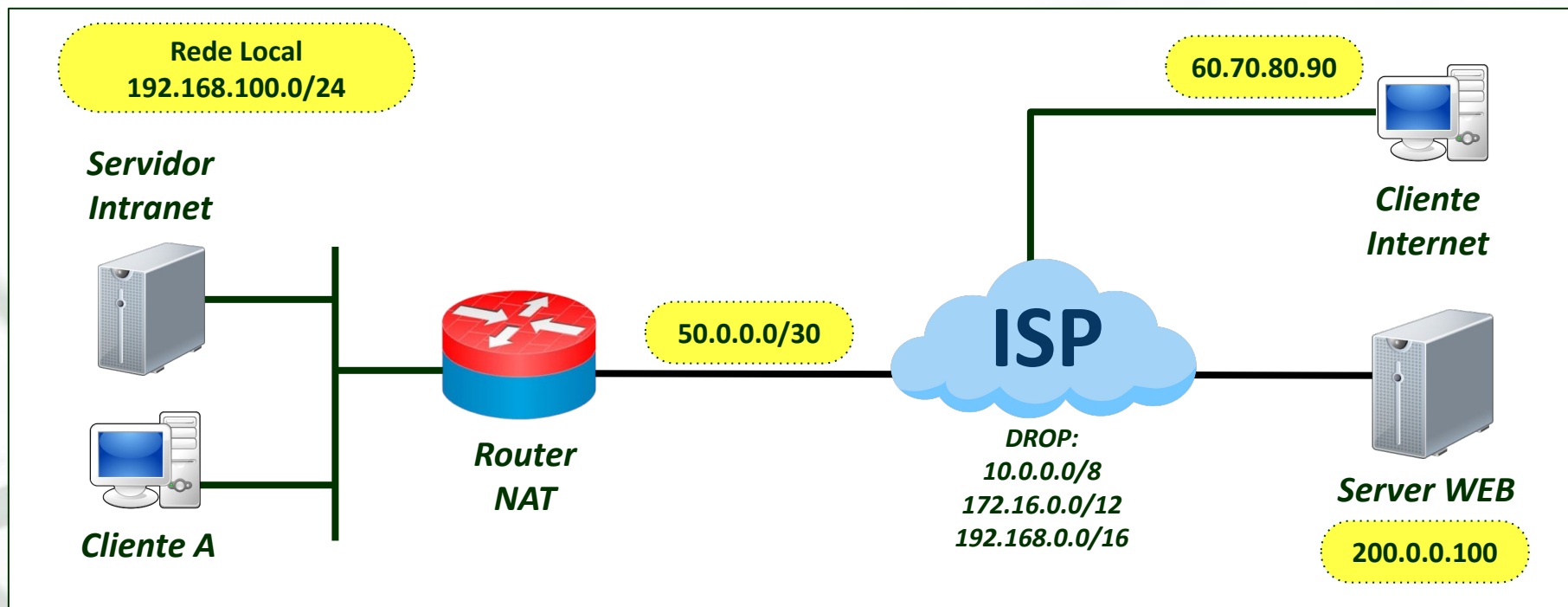
```
# iptables -t nat -A PREROUTING -i eth1 -p tcp -j DNAT --to  
192.168.10.1:3128
```

*Todo tráfego com destino para porta 80 é redirecionado para a
porta 3128 do IP 192.168.10.1.*

*Regra útil para implementar um **proxy transparente**.*



Laboratório 13-2



- “ISP” deve dropar pctes de/para todas as faixas de redes privadas.
- “Cliente A” deve acessar página WEB do “Server Web”.
- “Cliente Internet” deve poder acessar via SSH o “Servidor Intranet”.
- “Router NAT” permite acesso SSH apenas da sua rede privada.



Zonas Desmilitarizadas

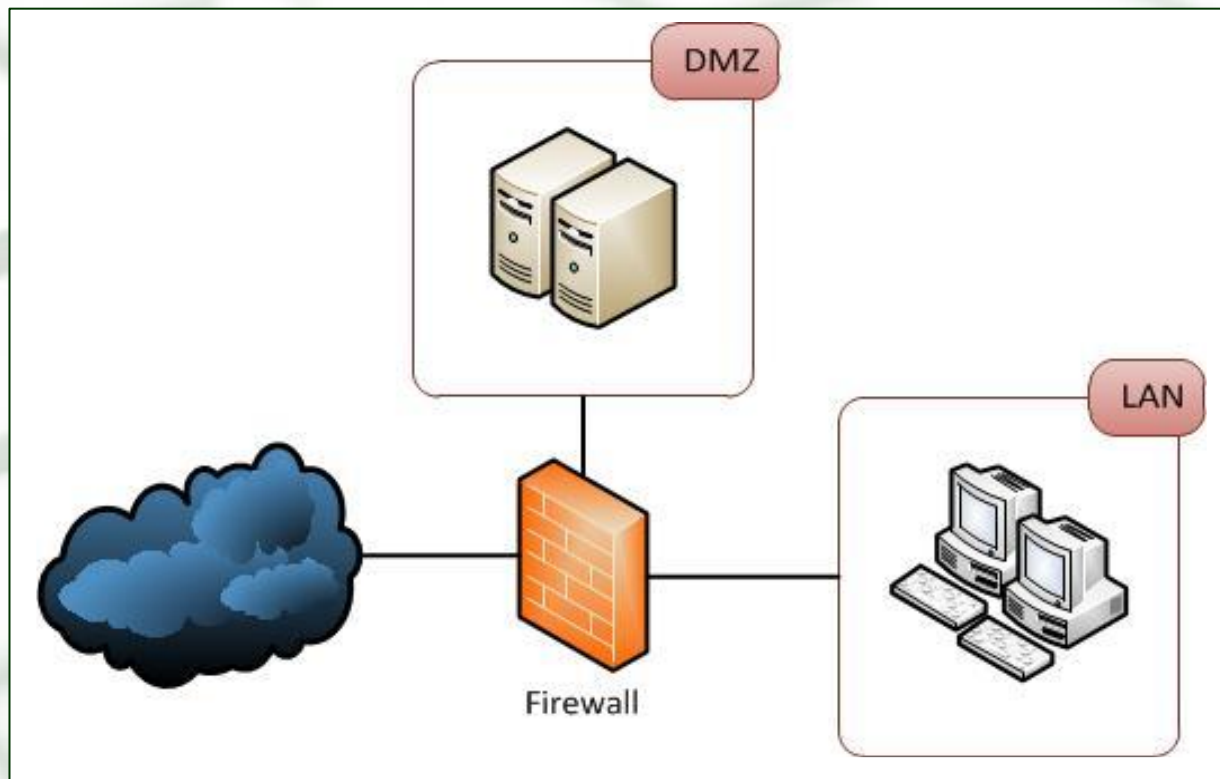
- Uma **Zona Desmilitarizada (DMZ)** também conhecida por **Rede de Perímetro** é uma Sub-Rede organizacional que mantém serviços disponíveis para acesso universal.
- A correta configuração dessa **zona intermediária**, entre a rede pública e a rede privada, é fundamental para preservar a política de segurança da informação das organizações.



DMZ

■ Arquiteturas de DMZ

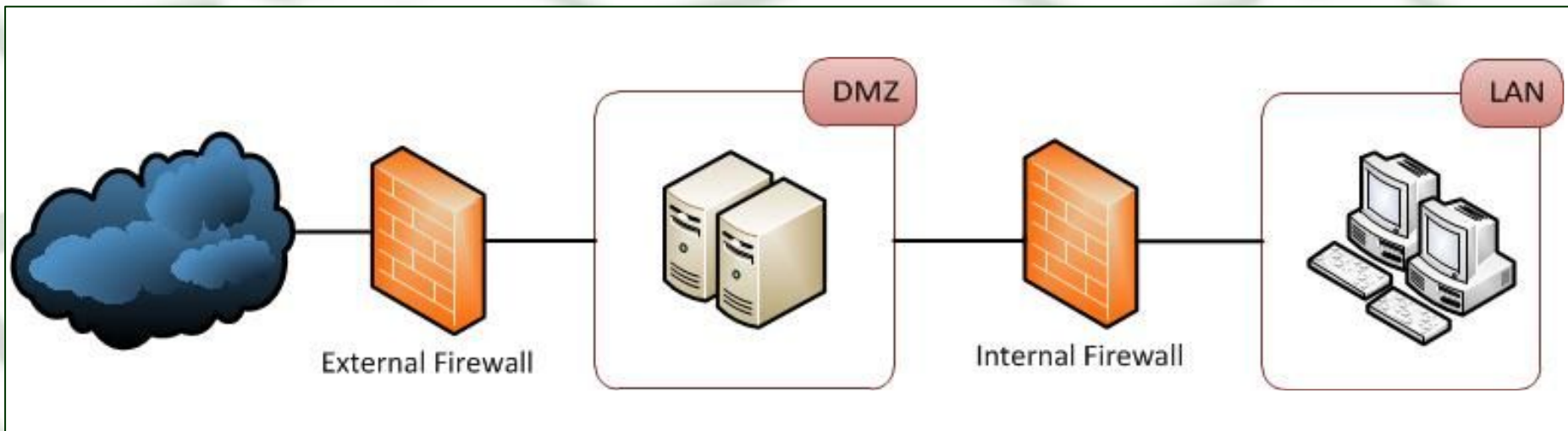
- *Three-Pronged Firewall ou single firewall*





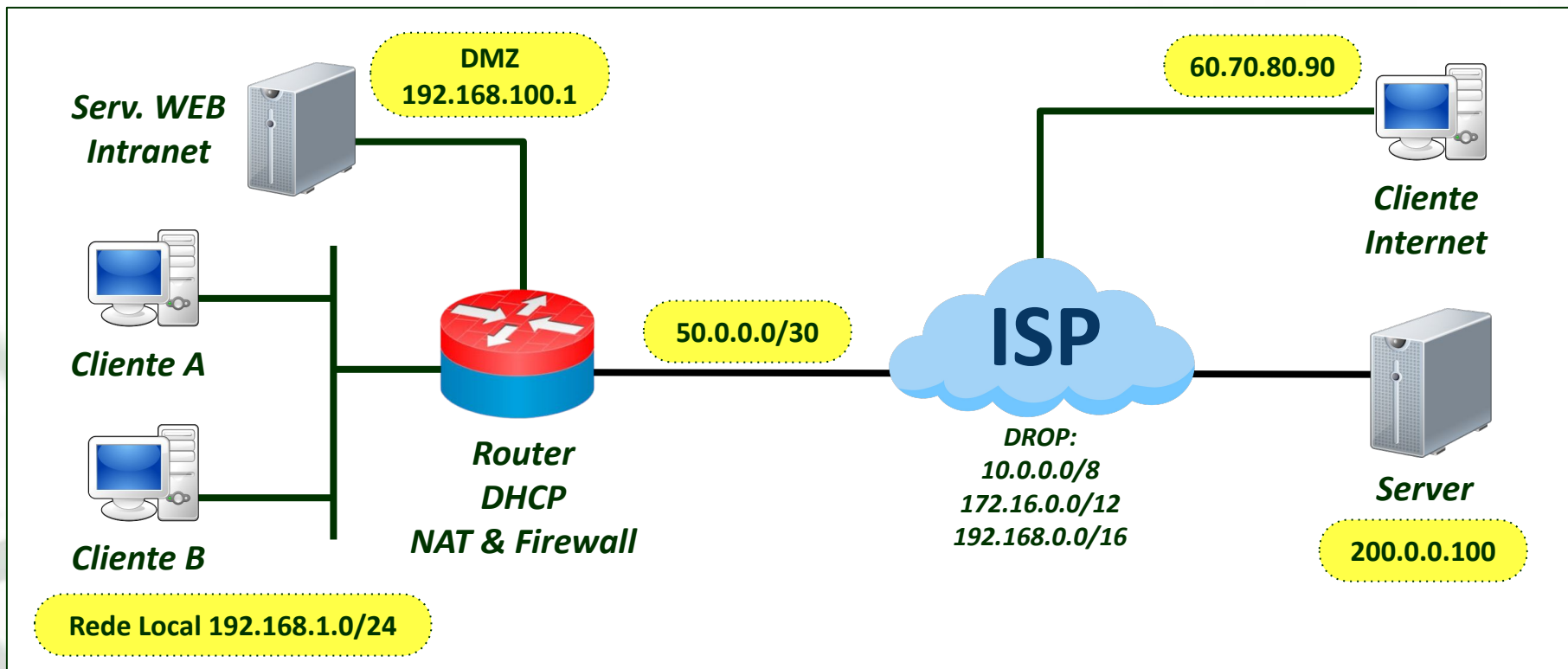
DMZ

- **Arquiteturas de DMZ**
 - *Multiple Firewall DMZ*





Laboratório 13-3



Política Restritiva para o "Firewall" - "ISP" dropa faixas de redes privadas.

"Clientes" podem Acessar Serviços HTTP, HTTPS e SSH do "Server" no mundo.

"Cliente Internet" pode estabelecer VPN com Router (Serviço na Porta 1194).

SSH do "Router" disponível apenas para "Clientes da Rede Local".

SSH do "Servidor Intranet" disponível para acesso de qualquer lugar (privado ou público).

HTTP e HTTPS do "Servidor Intranet" Liberados para Qualquer tipo de Acesso.

Ah...e claro, o DHCP deve funcionar 😊



Seminário Individual

- **DNS e DDNS**

Arquitetura de Servidores DNS

Funcionamento Protocolo DNS

DNS vs. DDNS

*Vídeo
Introdutório*





Referências

- **Guia Foca GNU/Linux.**

Disponível em <http://www.guiafoca.org/>

- **Documentação NetFilter.**

Disponível em <http://www.netfilter.org/documentation/>

- **Blog LabCisco**

Disponível em

<http://labcisco.blogspot.com/2014/09/cgnat-na-transicao-ipv6-solucao-ou-vilao.html>

- **Prof. Ph.D. Edgard Jamhour**

Disponível em <https://www.ppgia.pucpr.br/~jamhour/Pessoal/Graduacao/Ciencia/Teoria/>

- **Fernando Frediani**

Disponível em <https://ftp.registro.br/pub/gter/gter47/03-CGNAT-Bem-feito.pdf>

- **MORIMOTO, Carlos E; Servidores Linux - Guia Prático.**