Treinamento MikroTik MTCNA Online

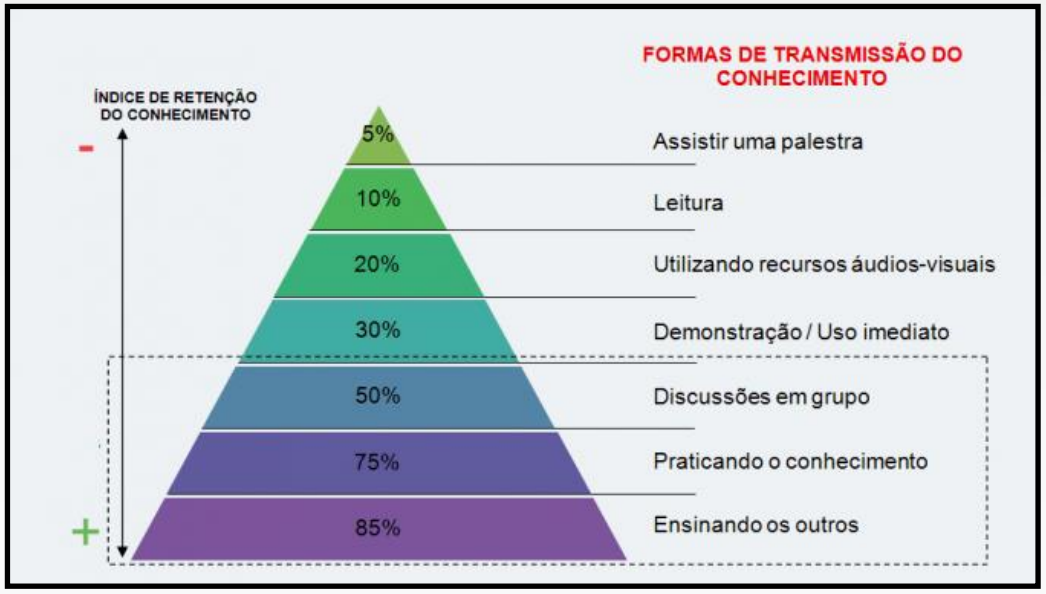
RouterOS v7

Redes Brasil

Importante

Redes Brasil

- **Aprendizado:** Busque absorver conceitos.
- **Pratique**: Faça todos os laboratórios propostos.

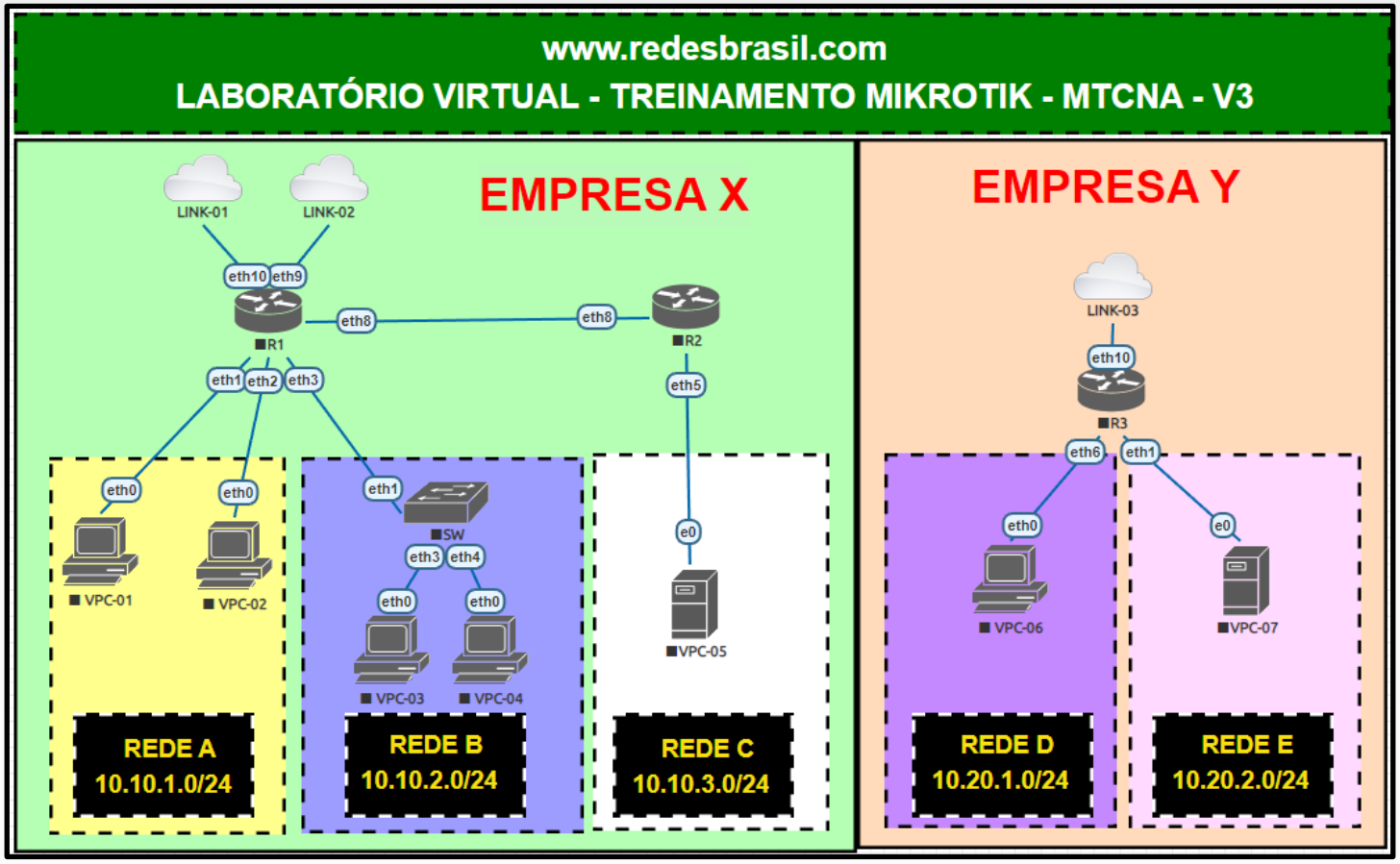


- Essa pirâmide foi elaborada por meio de estudos da National Training Laboratories (NTL).

Fique tranquilo !!!

Redes Brasil

Vamos praticar muito.



Curso oficial ?

- Poderá ser oficial;
- Prova somente presencial;
- Recertificação poderá ser Online;

Objetivos do curso

- Tonar o aluno apto prestar o exame de certificação;
- Tornar o aluno apto a configurar com eficiência os equipamentos da MikroTik;

Prova de certificação

- 25 questões;
- Prova em Inglês;
- 1 hora de duração (média 2,4 minutos por questão);
- Nota igual ou superior a 60% para ser aprovado;
- Nota igual ou superior a 75% para passar na primeira etapa para consultor official.
- Pode consultar roteador, anotações e sites da MikroTik.
- Pode usar tradutor.
- Faça o teste de exemplo no site da MikroTik. https://mikrotik.com/client/testExample

Certificado

- Todos o alunos irão receber o certificado de participação por e-mail.

CERTIFICADO

Certificamos que **Ademir** [redacted] participou do treinamento oficial MTCIPv6E (MikroTik Certified IPv6 Engineer), ministrado pela empresa Redes Brasil na cidade de Goiânia - GO, nos dias 24 e 25 de Julho de 2017 na modalidade presencial, cumprindo uma carga horária de 16 horas.

Francisco Neto
MikroTik Training Partner

Redes Brasil

MikroTik

CRB2017IPv6E041

- Alunos que fizerem a prova de certificação e tiverem nota igual ou maior que 60% receberão o certificado da MikroTik que será gerado dentro do próprio site do fabricante.

MikroTik

Francisco Ribeiro de Souza Neto

having successfully completed the appropriate training and certification requirements, is hereby recognised as a MikroTik Certified Network Associate

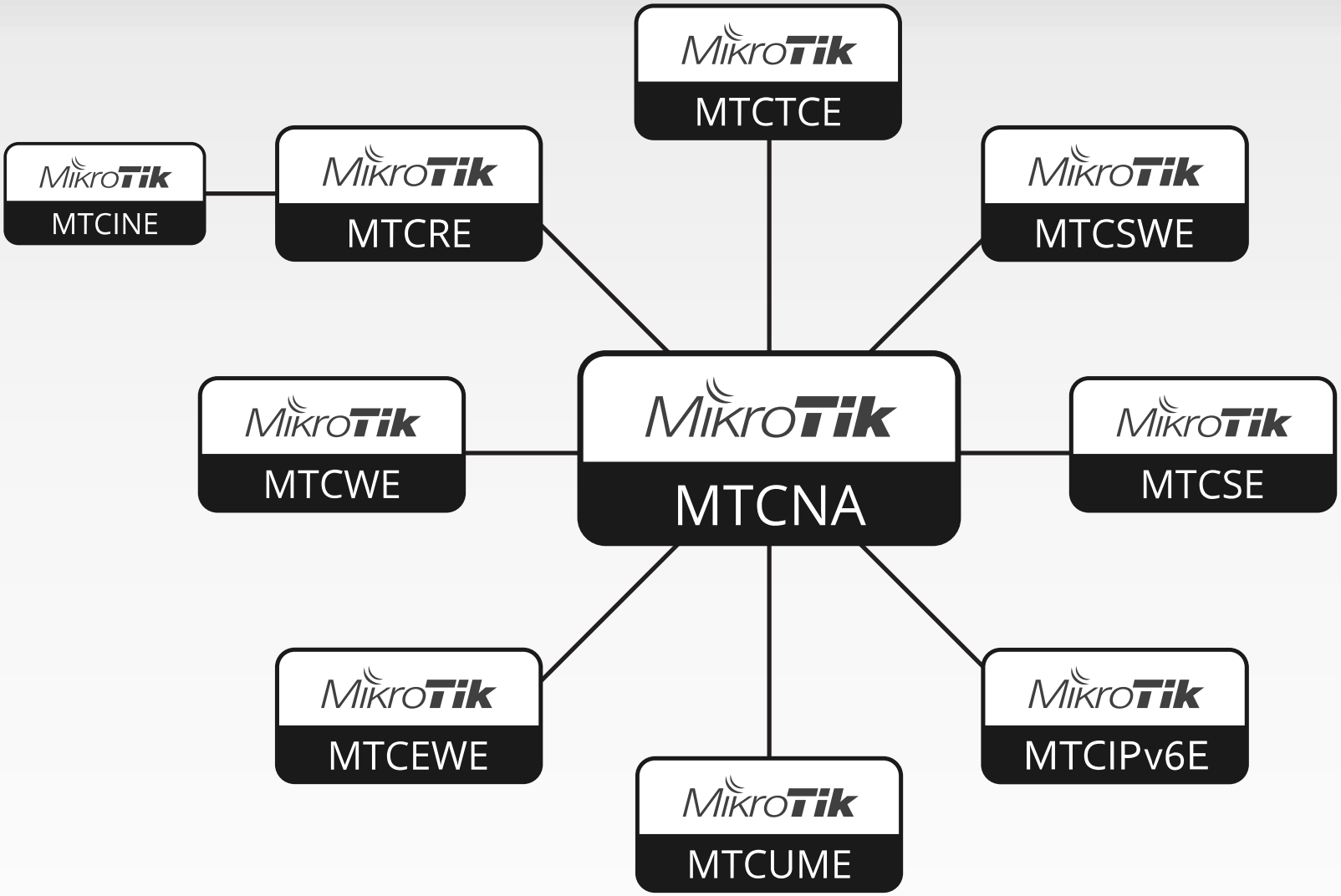
MTCNA

MikroTik

2204NA1773
2022-04-20

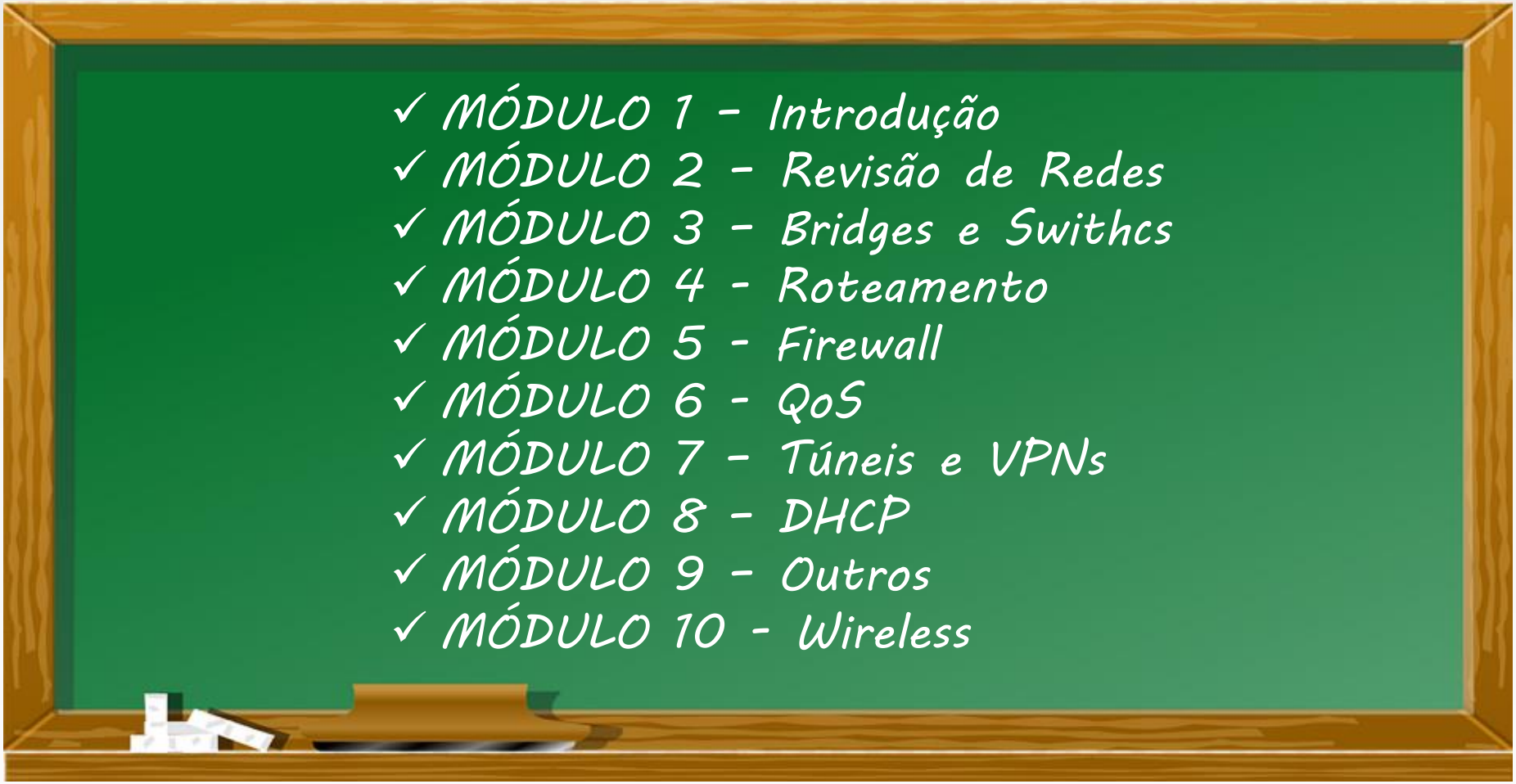
Valid for three years since issue.
Validate the authenticity of this document at mikrotik.com/certificates.
Issued by Mikrotīkls SIA, office address Brivibas gatve 214i, Riga, Latvia.

Certificações da MikroTik



Versão 6 x Versão 7

Módulos do Treinamento



MÓDULO 1 - INTRODUÇÃO

MÓDULO 1 - Introdução

- ✓ 1.1 - Oque é o RouterOS;
- ✓ 1.2 - Hardware - RouterBoards, CCRs, CRS, CSSs e Outros;
- ✓ 1.3 - Configuração inicial;
- ✓ 1.4 - Atualização do RouterOS e Firmware;
- ✓ 1.5 - Instalando um pacote adicional;
- ✓ 1.6 - Métodos de acesso;
- ✓ 1.7 - Usuários e grupos de acesso ao roteador;
- ✓ 1.8 - Tipos de backups;
- ✓ 1.9 - Reset de equipamentos;
- ✓ 1.10 - Reinstalação com Netinstall;
- ✓ 1.11 - Tipos de licença;
- ✓ 1.12 - Fonte de informações MikroTik;
- ✓ 1.13 - Modo seguro

MÓDULO 1.1
Oque é o RouterOS

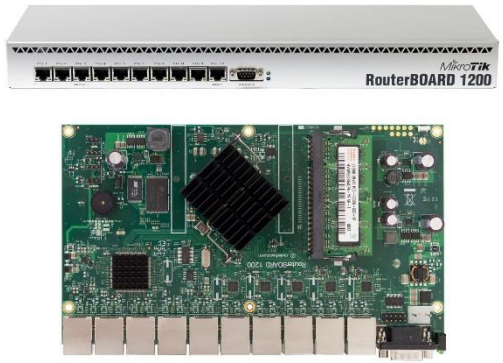
MikroTik/RouterBoard/RouterOS

Redes Brasil

MikroTik

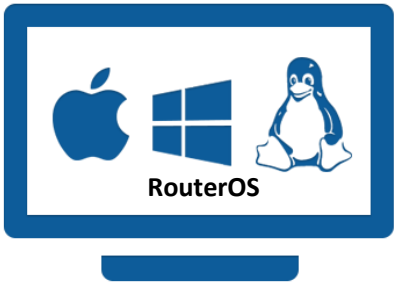
Empresa

RouterBoard



Hardware

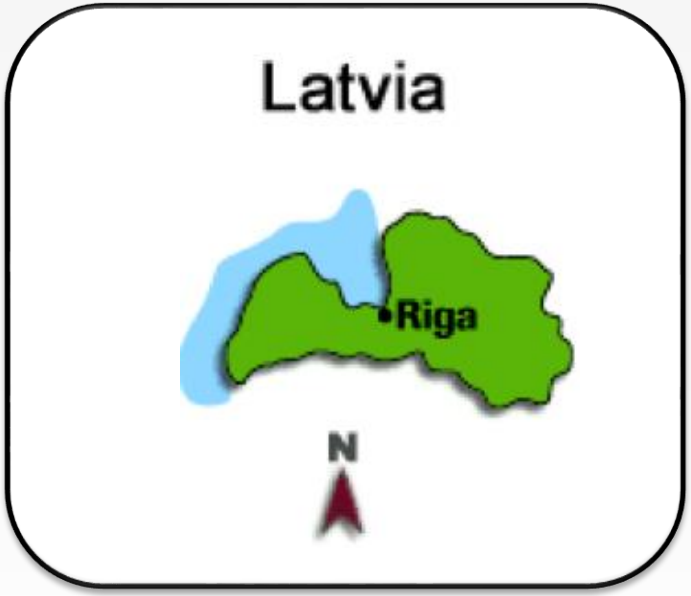
RouterOS



Software/ SO

MikroTik

- Criada em 1996
- Sediada na capital da Letónia, Riga.
- Desenvolve software e hardware focado no mercado de redes de computadores.



Oque é o RouterOS?

- RouterOS é o software desenvolvido pela MikroTik.
- Comumente utilizado em RouterBoards, mas também pode ser instalado em um servidor ou até mesmo virtualizado.
- É um sistema operacional baseado em Linux que pode facilmente controlar redes de pequeno, médio e grande porte.
- O sistema ganhou destaque muito grande nos últimos anos por alguns motivos que veremos logo a seguir.

Oque é o RouterOS?

- O RouterOS possui várias funcionalidades, abaixo segue algumas:

  - Roteador simples
  - Controlador de banda
  - Firewall simples e avançado (camada 2,3 e 7)
  - Controlador de conteúdo
  - Access point (wireless) com vários recursos
  - Hotspot com varias opções
  - Sniff de rede (Analisador de pacotes e conexões)
  - Balanceador de links
  - Failover
  - Concentrador de VPN
  - Roteador avançado utilizando protocolos de roteamento dinâmico (OSPF,BGP,RIP e MPLS)
  - Firewall de IDS (intrusion detection system/Sistema de detecção de intrusão)
  - QoS (Quality of service/Qualidade de serviço)
  - Gerenciador de conexões wireless de alto desempenho
  - Outros

Onde posso rodar o RouterOS?

Redes Brasil

Equipamentos MikroTik

RouterOS v7

ARM
Main package
Extra packages
ARM64
Main package
Extra packages
MIPSBE
Main package
Extra packages
MMIPS
Main package
Extra packages
SMIPS
Main package
Extra packages

Servidor físico

X86
Main package
Extra packages
CD Image
Install image

Máquina Virtual

Cloud Hosted Router

Images
Main package
VHDX image
VMDK image
VDI image
VirtualPC image
OVA template
Raw disk image

MÓDULO 1.2 - HARDWARE

Conhecendo o Hardware da MikroTik

Redes Brasil

RouterBoards

CCRs

Swtichs

Wireless Outdoor

Wireless Indoor

Outros

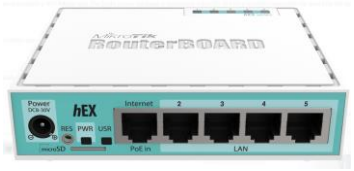
Oque são RouterBoards ?

- Hardware criado pela MikroTik desde 2002;
- Atende desde usuários domésticos até grandes empresas;
- Hardware relativamente barato se comparado com outros fabricantes;

Alguns modelos de RouterBoards?

HAP – RB941
Residencial - Baixo custo
Com Wi-Fi

HEX Lite – RB750r2
SOHO - Baixo custo



HEX – RB750Gr3
Baixo custo

RB 450Gx4
Sem case e sem fonte

RB 2011 CPU 600Mhz

RB 1100AHx4 CPU Quad-core 1,4Ghz

RB 3011 CPU Dual-core 1,4Ghz

RB 1100AHx4 Dude Edition SSD 60GB

RB 4011 CPU Quad-core 1,4Ghz

RB 5009 CPU Quad-core 1,4Ghz

CCRs da linha 1000

CCR 1009

9 núcleos de processamento

CCR 1016

16 núcleos de processamento

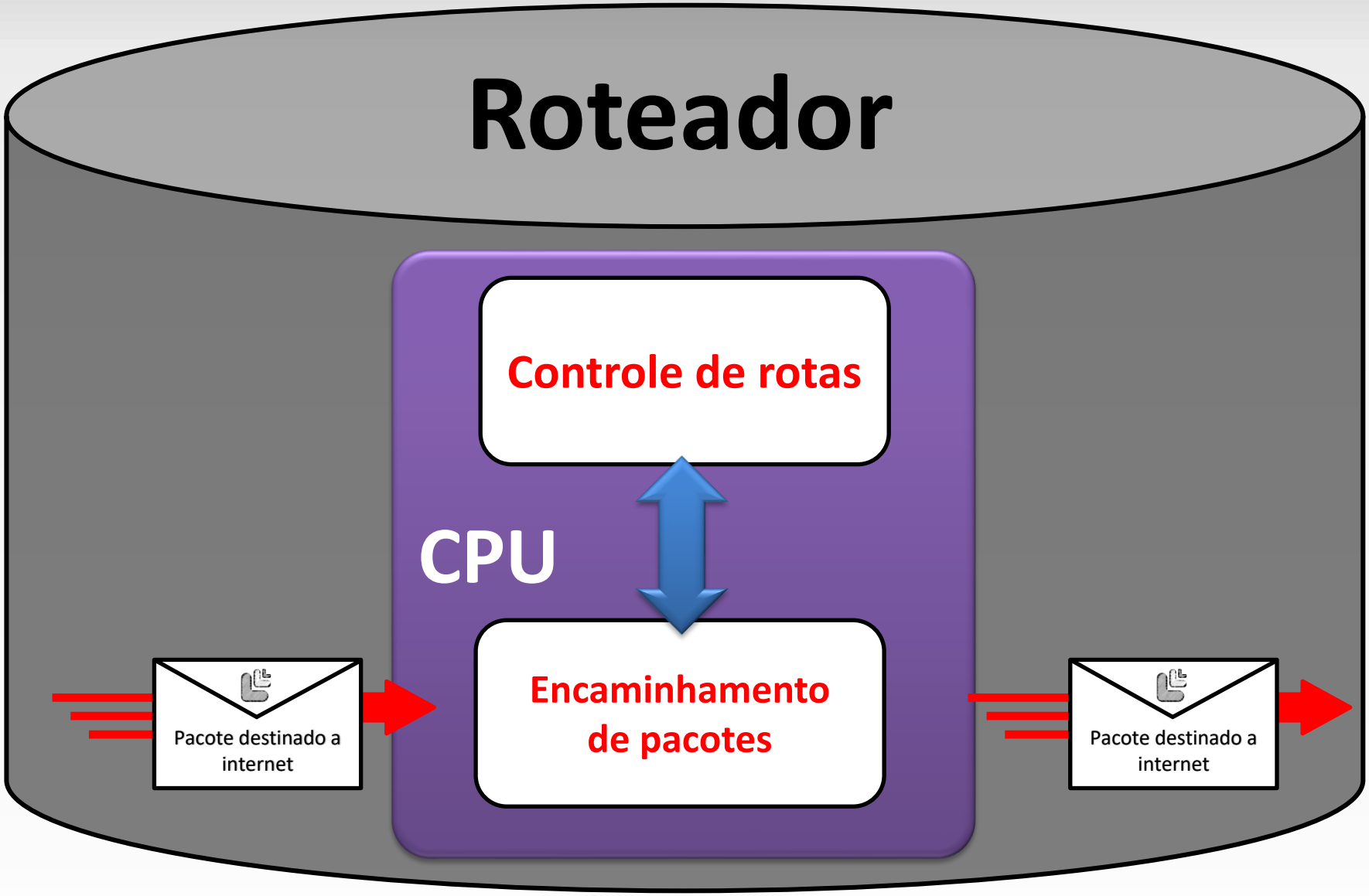
CCR 1036

36 núcleos de processamento

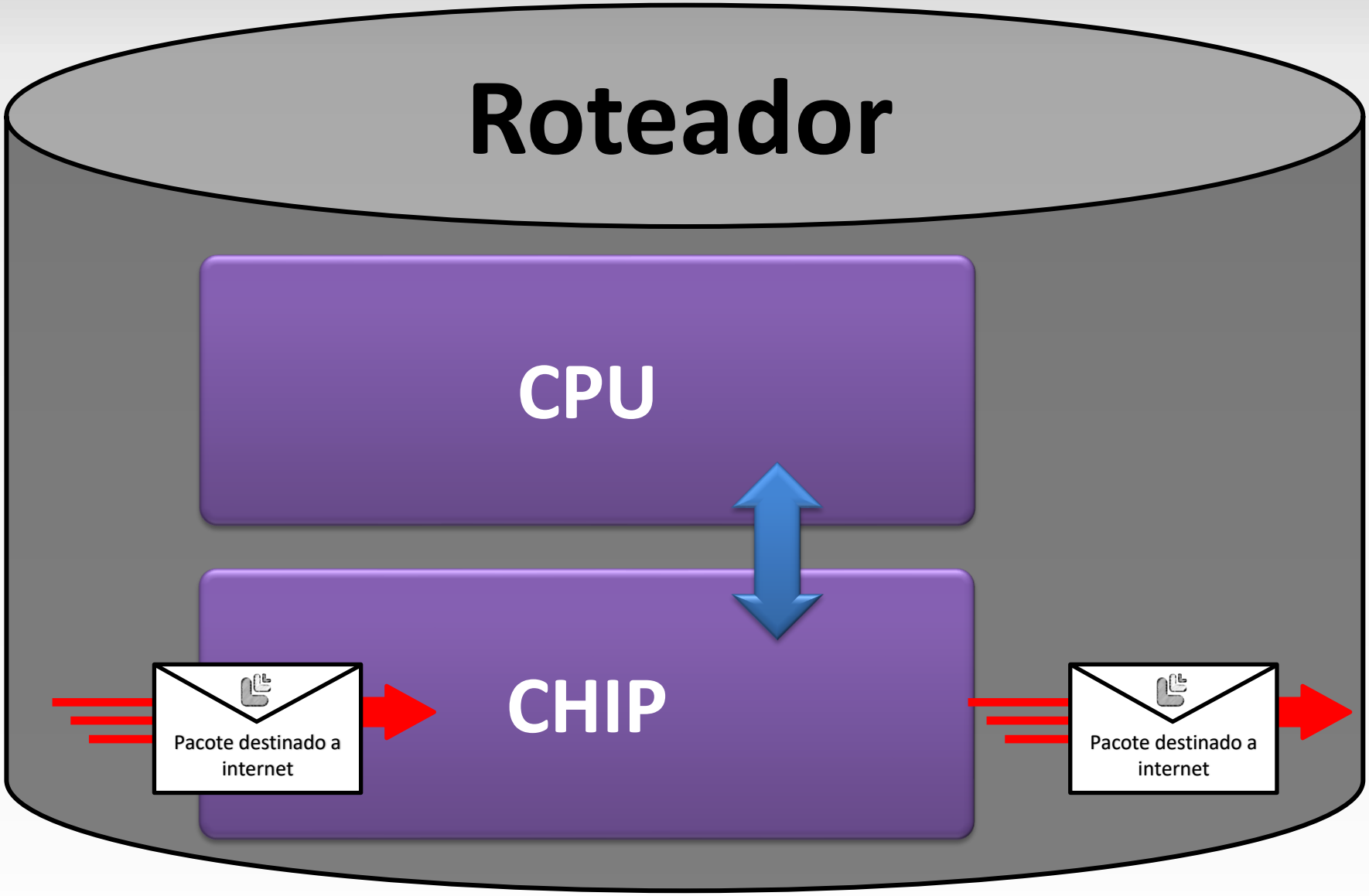
CCR 1072

72 núcleos de processamento

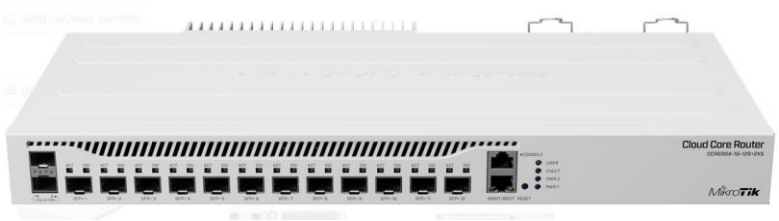
Soft Router



Separação de CPU e Chip

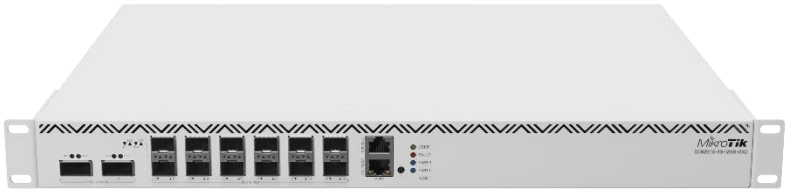


CCRs da linha 2000

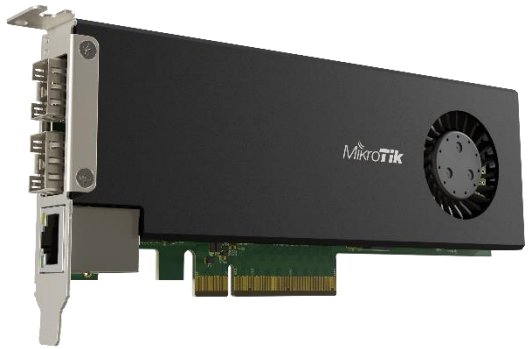


CCR 2004

CCR 2116



CCR 2216

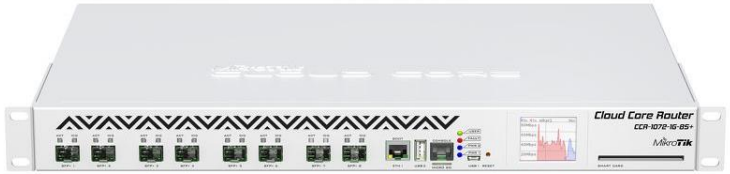


CCR2004-1G-2XS-PCIe

Roteadores vs Switchs

Redes Brasil

Roteador

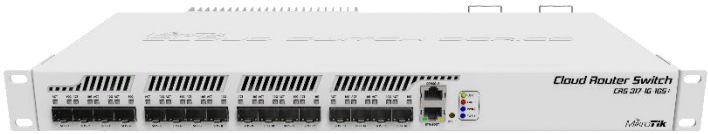


CCR 1072

8 interfaces de 10G
72 CPUs
Tráfego máximo com pacotes de 64 bytes = 48Gbps

3350,00 dólares

Switch



CRS 317

16 interfaces de 10G
2 CPUs
Tráfego máximo com pacotes de 64 bytes = 120Gbps

439,00 dólares

Swtichs CRS e CSS

Redes Brasil

CRS 326

Roda RouterOS

24 interfaces 1G
2 interfaces 10G

209,00 dólares

CSS 326

Roda SwOS

24 interfaces 1G
2 interfaces 10G

159,00 dólares

CRS 1xx e 2xx vs CRS 3xx e 5xx

CRS 125

Difícil de configurar
Poucos recursos no offload

24 interfaces ethernets 1G
1 interfaces fibra 1G

189,00 dólares

CRS 326

Fácil de configurar
Muitos recursos no offload

24 interfaces ethernets 1G
2 interfaces fibra 10G

199,00 dólares

Resumo

RouterBoard

Roteador

RouterOS

Vários modelos

CCR

Roteador

RouterOS

Alto tráfego

CSS

Switch

SwOS

\+ Barato que CRSs

Configuração simples

Somente camada 2

Poucos recursos

CRS 1xx e 2xx

Switch

RouterOS

\+ Baratos que CRSs 3xx e 5xx

Configuração complicada

Poucos recursos no offload

CRS 3xx e 5xx

Switch

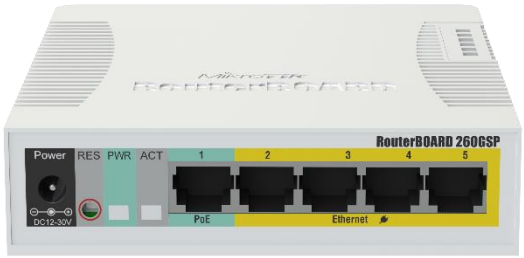
RouterOS

\+ Caros que CRSs 1xx e 2xx

Configuração simples

Muitos recursos no offload

Alguns modelos de Swtichs CSS



CSS 106 (RB 260)

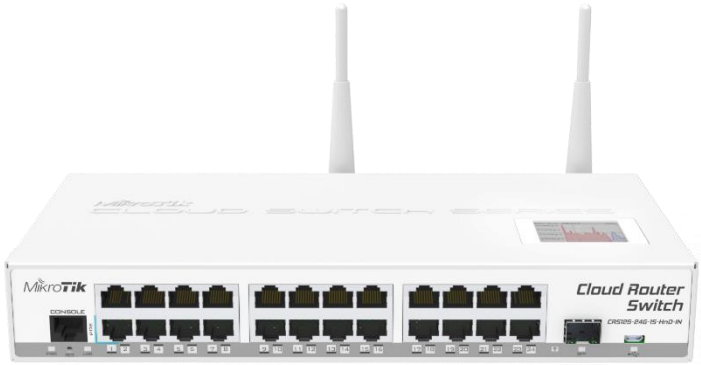
CSS 326

CSS 610 (netPower)

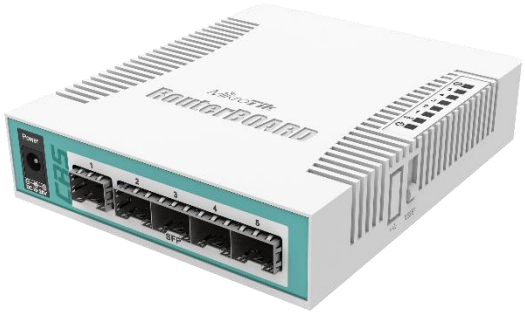
CSS 610

Alguns modelos de Swtichs CRS 1xx e 2xx

CRS 109



CRS 125



CRS 106

CRS 212

Alguns modelos de Swtichs CRS 3xx e 5xx

Redes Brasil

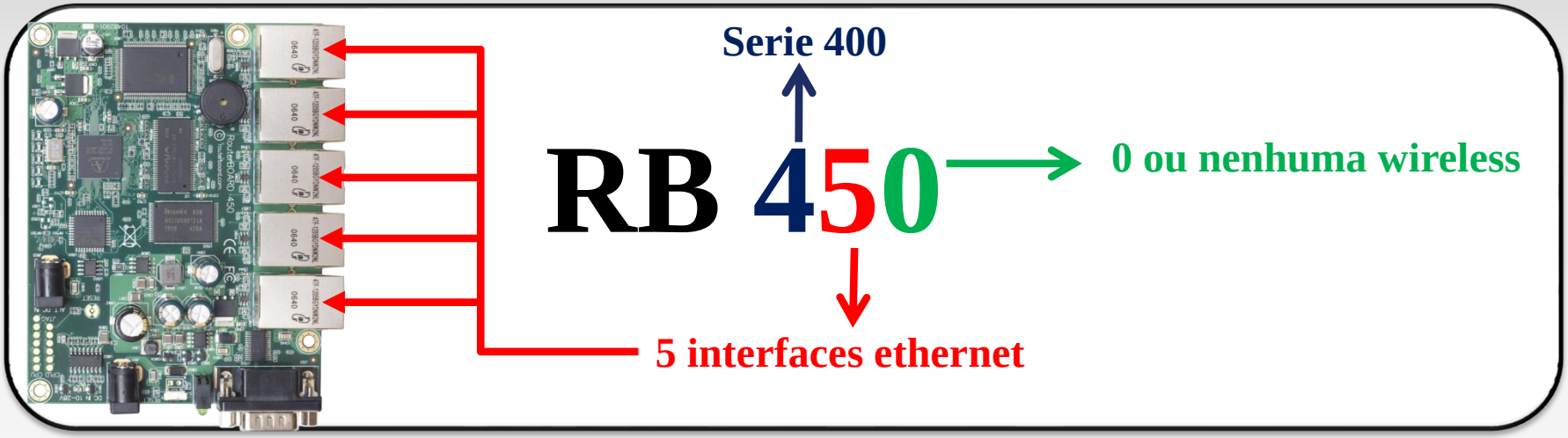
CRS 305

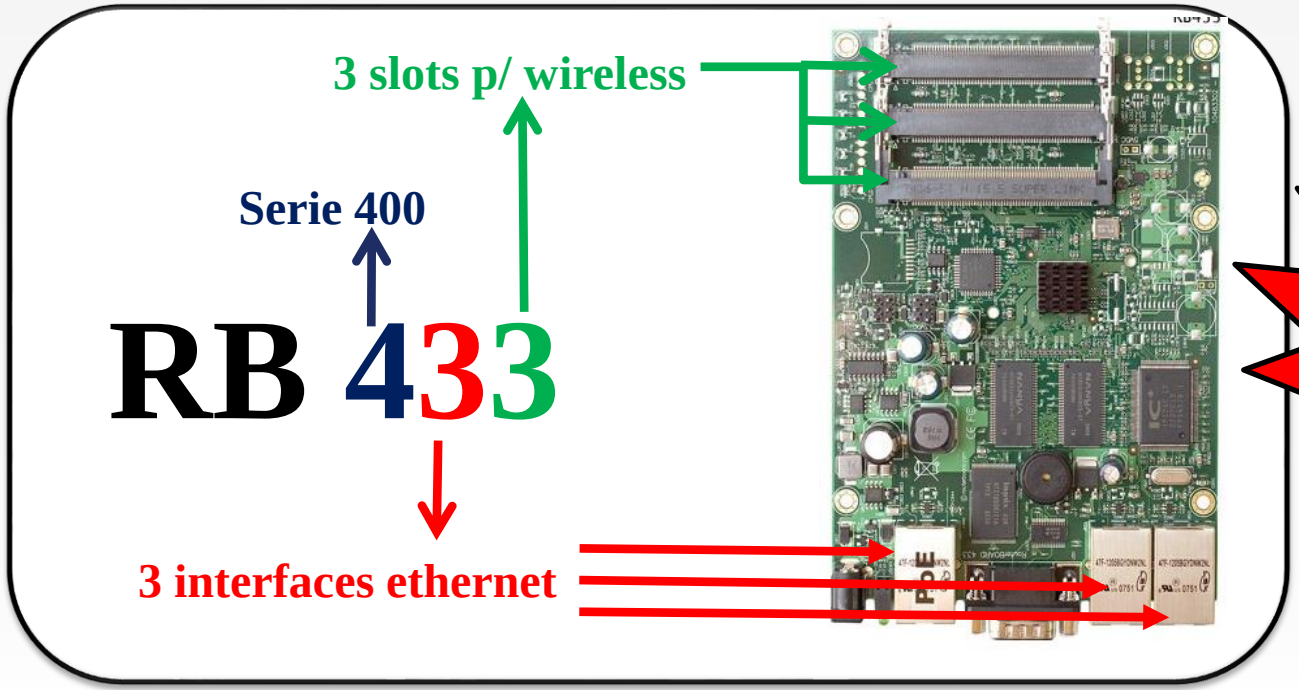
CRS 317

CRS 354

CRS 518

Nomenclatura das RouterBoards





Lógica de nomenclatura válida somente para RouterBoards com modelos especificados por 3 números.

Nomenclatura Geral

Tipo de case
- (not used) - main type of enclosure for a product
- **RM** - rack-mount enclosure
- **IN** - indoor enclosure
- **EM** - extended memory
- **LM** - light memory
- **BE** - black edition case
- **TC** - Tower (vertical) case
- **OUT** - outdoor enclosure

Banda
- **5** - 5Ghz
- **2** - 2.4Ghz
- **52** - dual band 5Ghz and 2.4Ghz

Número de chains
- (not used) - single chain
- **D** - dual chain
- **T** - triple chain

Potencia do rádio
- (not used) - "Normal" - <23dBm at 6Mbps 802.11a; <24dBm at 6Mbps 802.11g
- **H** - "High" - 23-24dBm at 6Mbps 802.11a; 24-27dBm at 6Mbps 802.11g
- **HP** - "High Power" - 25-26dBm 6Mbps 802.11a; 28-29dBm at 6Mbps 802.11g
- **SHP** - "Super High Power" - 27+dBm at 6Mbps 802.11a; 30+dBm at 6Mbps 802.11g

Protocolo
- (not used) - 802.11a/b/g support
- **n** - for cards with 802.11n support
- **ac** - for cards with 802.11ac support

Tipo de conector
- (not used) – modelo com somente uma opçãp
- **MMCX** - MMCX connector type
- **u.FL** - u.FL connector type

https://help.mikrotik.com/docs/display/ROS/Product+Naming

Outros equipamentos e acessórios

Wireless Outdoor

Wireless Indoor

Outros

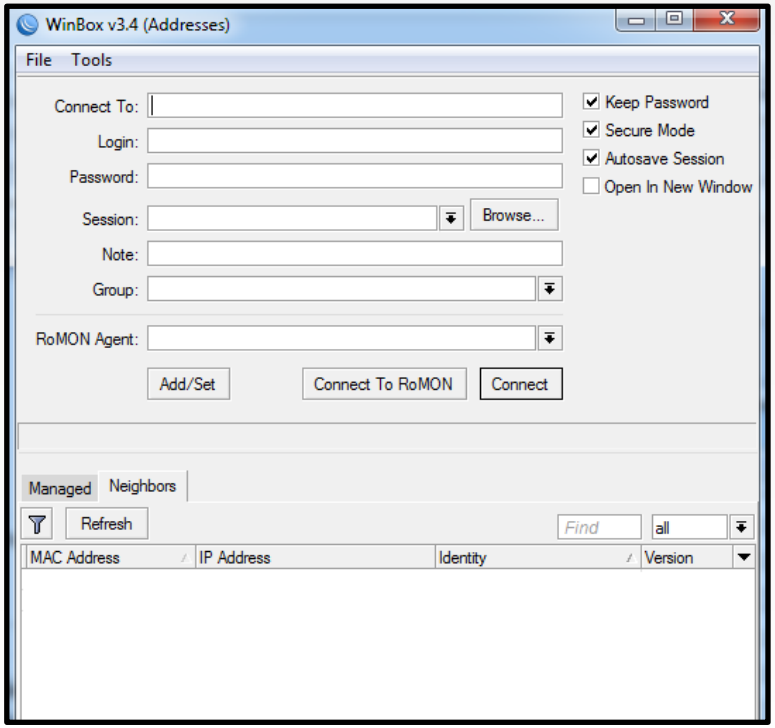
MÓDULO 1·3
Configuração inicial

Primeiro acesso com Winbox

- Existem diversas maneira de acessar o RouterOS sendo o Winbox a mais utilizada.

- Winbox pode ser usado para acessar o RouterOS via endereço MAC ou IP.

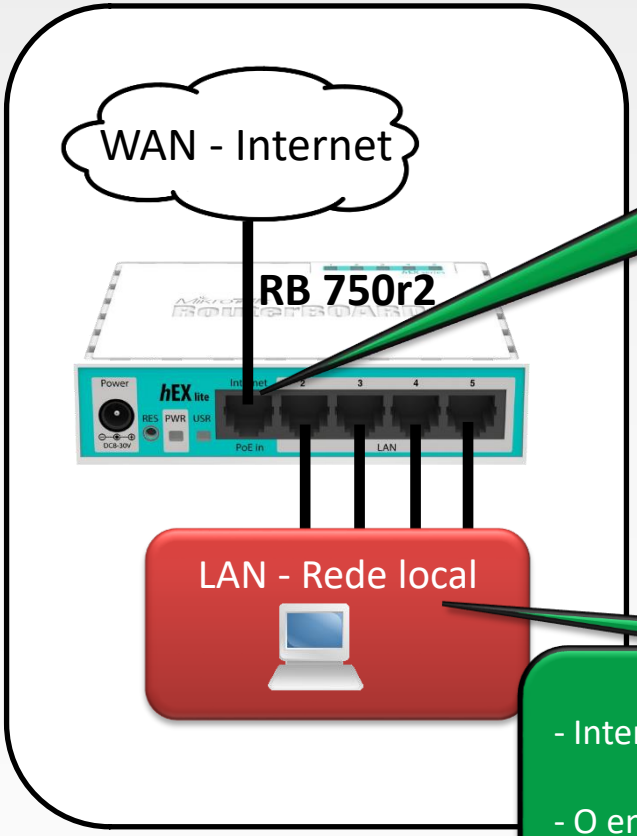
- Winbox é um aplicativo para Windows e caso precise usar em Linux ou MacOS será necessário usar emuladores como Wine ou CrossOver.



Configuração de fábrica

Redes Brasil

Interface 1
- DHCP-Client rodando.
- Regras de firewall bloqueando o acesso.



Em resumo!!

Os roteadores vem com configurações focadas para uso residencial.

Para uso empresarial é recomendado sempre limpar essas configurações.

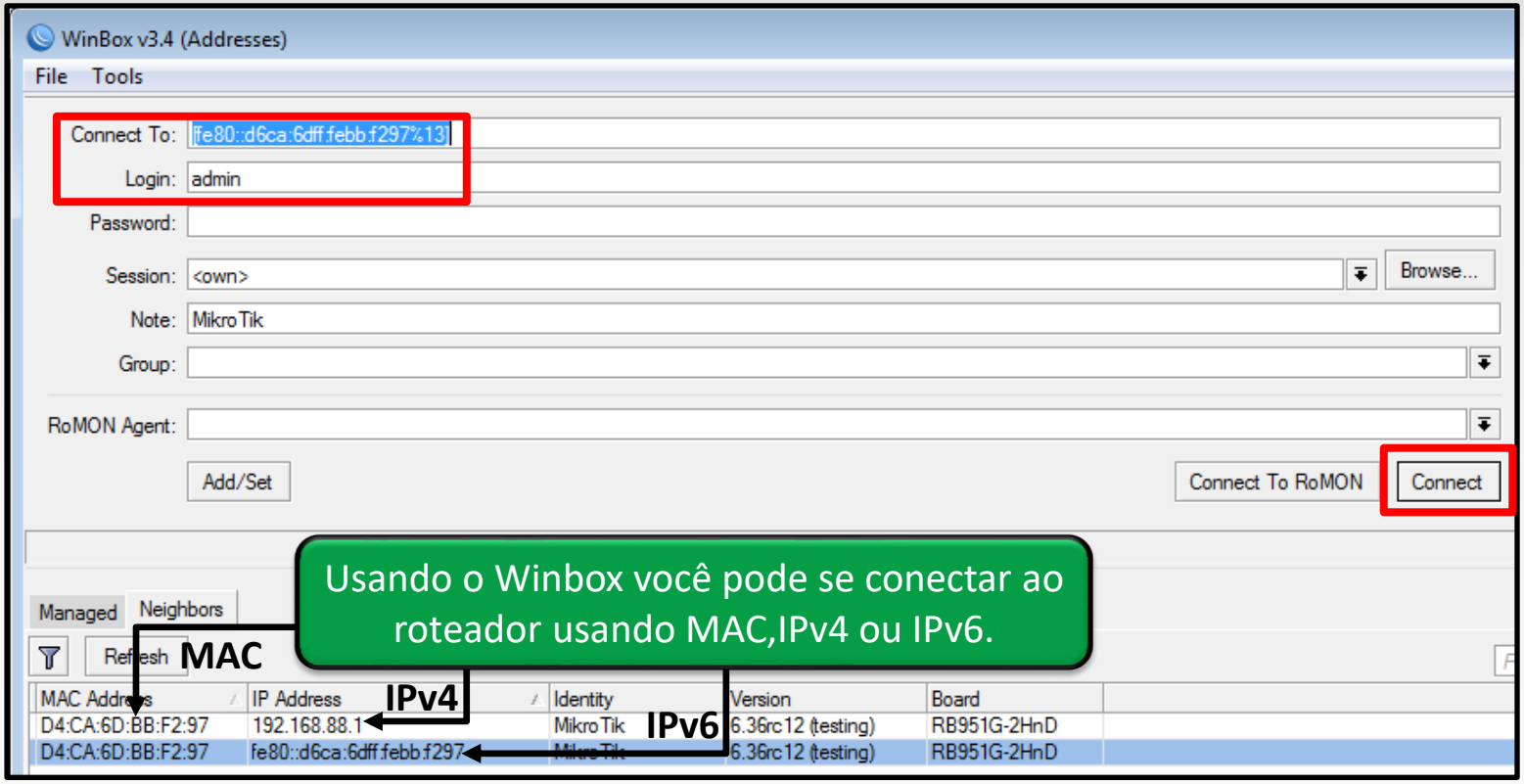
Interface 2,3,4 e 5
- Interligadas no mesmo domínio de broadcast através de uma bridge.
- O endereço 192.168.88.1/24 foi atribuído a essa bridge.
- Um DHCP-Server rodando nessa bridge.

Exemplo de configuração de fábrica

- Todos os roteadores vem com uma configuração de fábrica.
- Na maioria dos casos essa configuração tem a interface ether1 designada para comunicação WAN e o restantes das interfaces designadas para rede LAN.
- Você pode conferir mais detalhes sobre a configuração de fabrica de cada equipamento acesso o link abaixo:

  http://wiki.mikrotik.com/wiki/Manual:Default_Configurations

Primeiro acesso

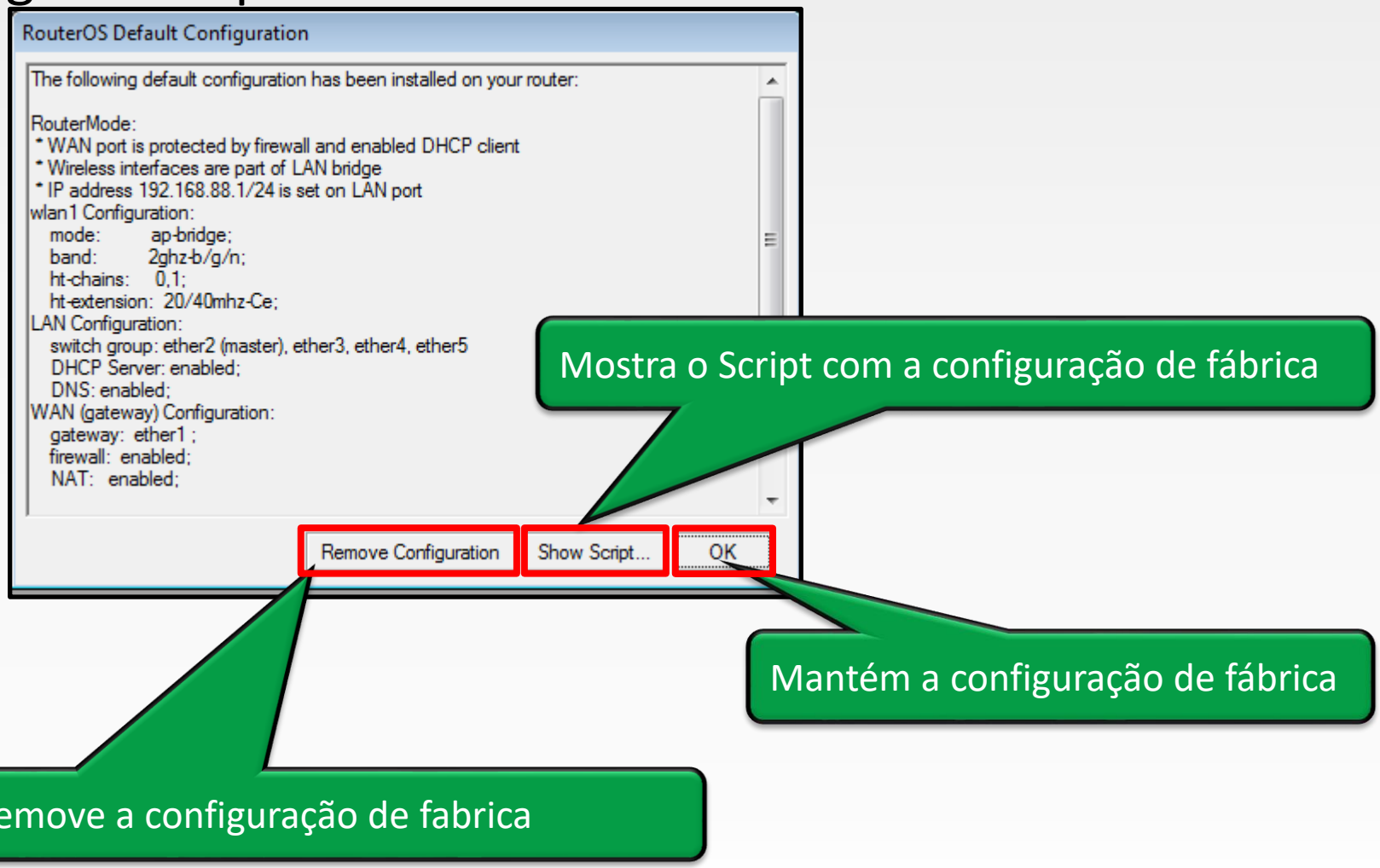


- Ligue seu computador ao roteador
- Abra o winbox clique na aba Neighbors
- Clique no endereço MAC ou IP.
- No campo Login coloque “admin”.
- No campo Password deixe em branco.
- Clique em connect.

Primeiro acesso

Redes Brasil

- Se esse for o primeiro acesso ao roteador a seguinte imagem irá aparecer.



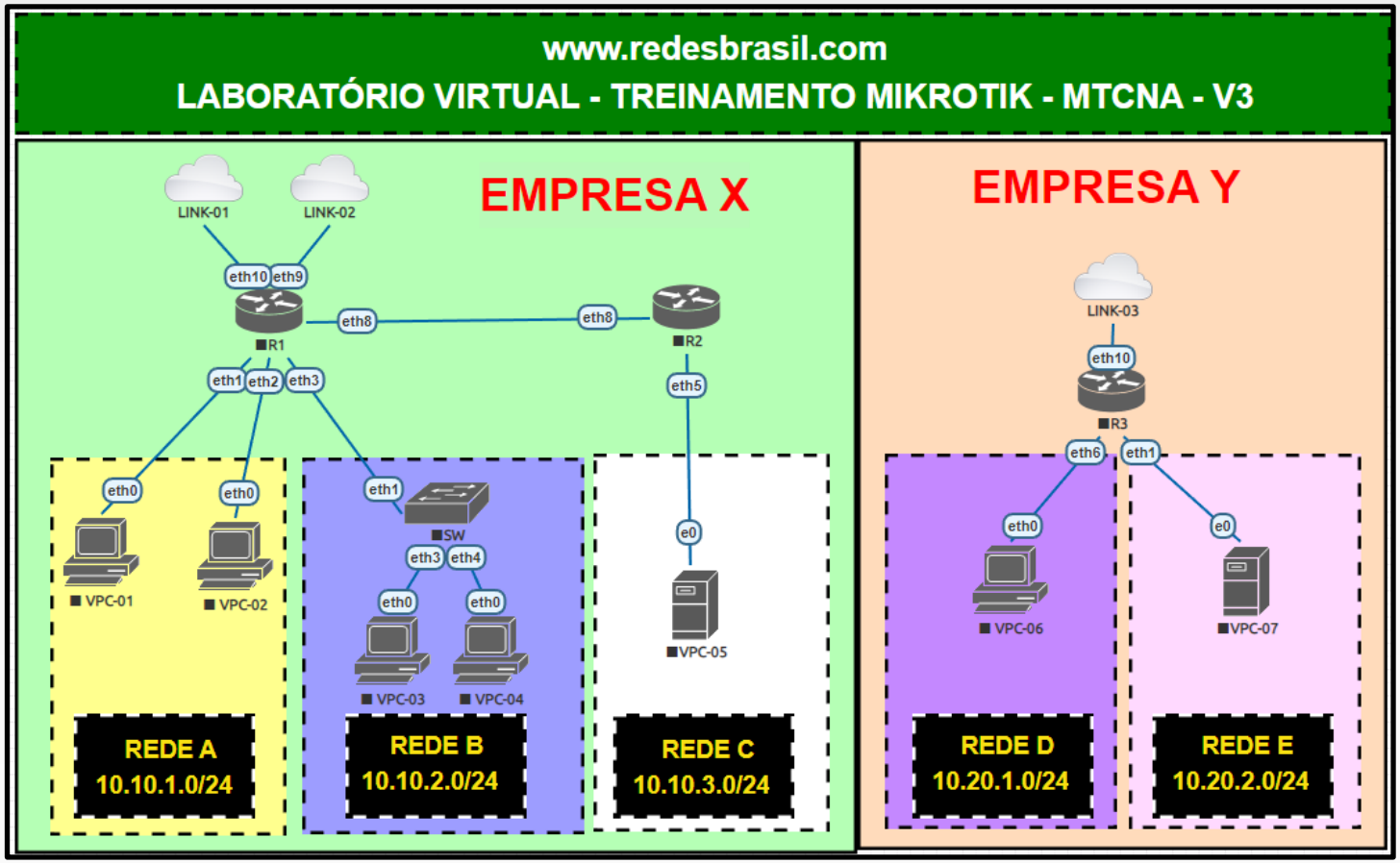
Resumo

1. No primeiro acesso nunca use a interface 1 devido aos bloqueios de acesso que vem de fábrica para essa interface.

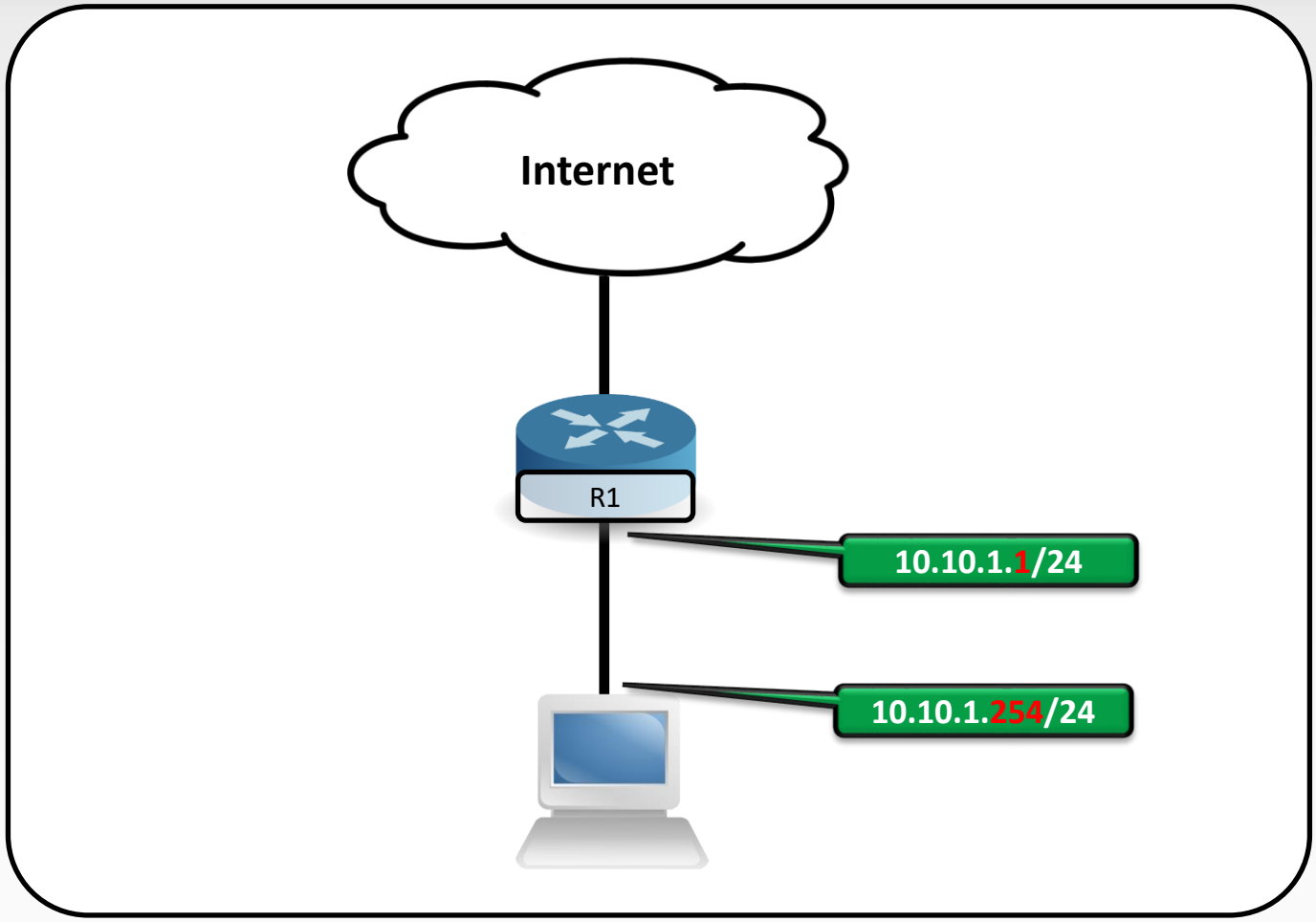
2. Sempre limpe as configurações de fábrica antes de iniciar suas configurações.

3. Caso o acesso via MAC ficar caindo, tente se conectar ao roteador via IPv6 (se disponível) e/ou deixe habilitada somente a interface que se liga ao roteador (desabilite todas as outras).

Diagrama da rede



Topologia simplificada



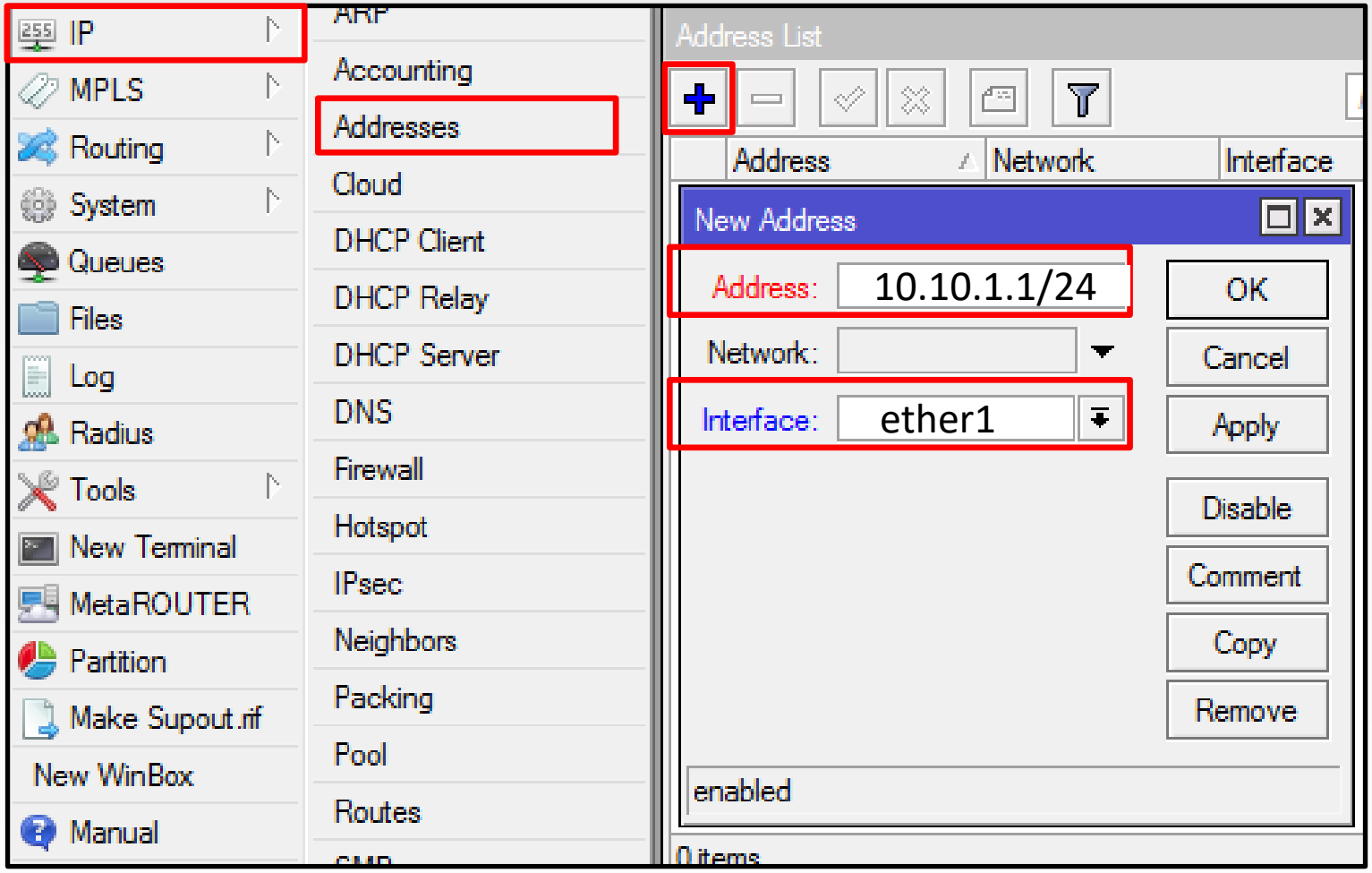
Passo a passo da configuração inicial

1. Configurar IP na interface;
2. Configurar DHCP server;
3. Renomear o Roteador e as interfaces;
4. Configurar IP de WAN;
5. Configurar Rota Default;
6. Configurar DNS no roteador;
7. Configurar NAT;

Configurando IP na interface de LAN

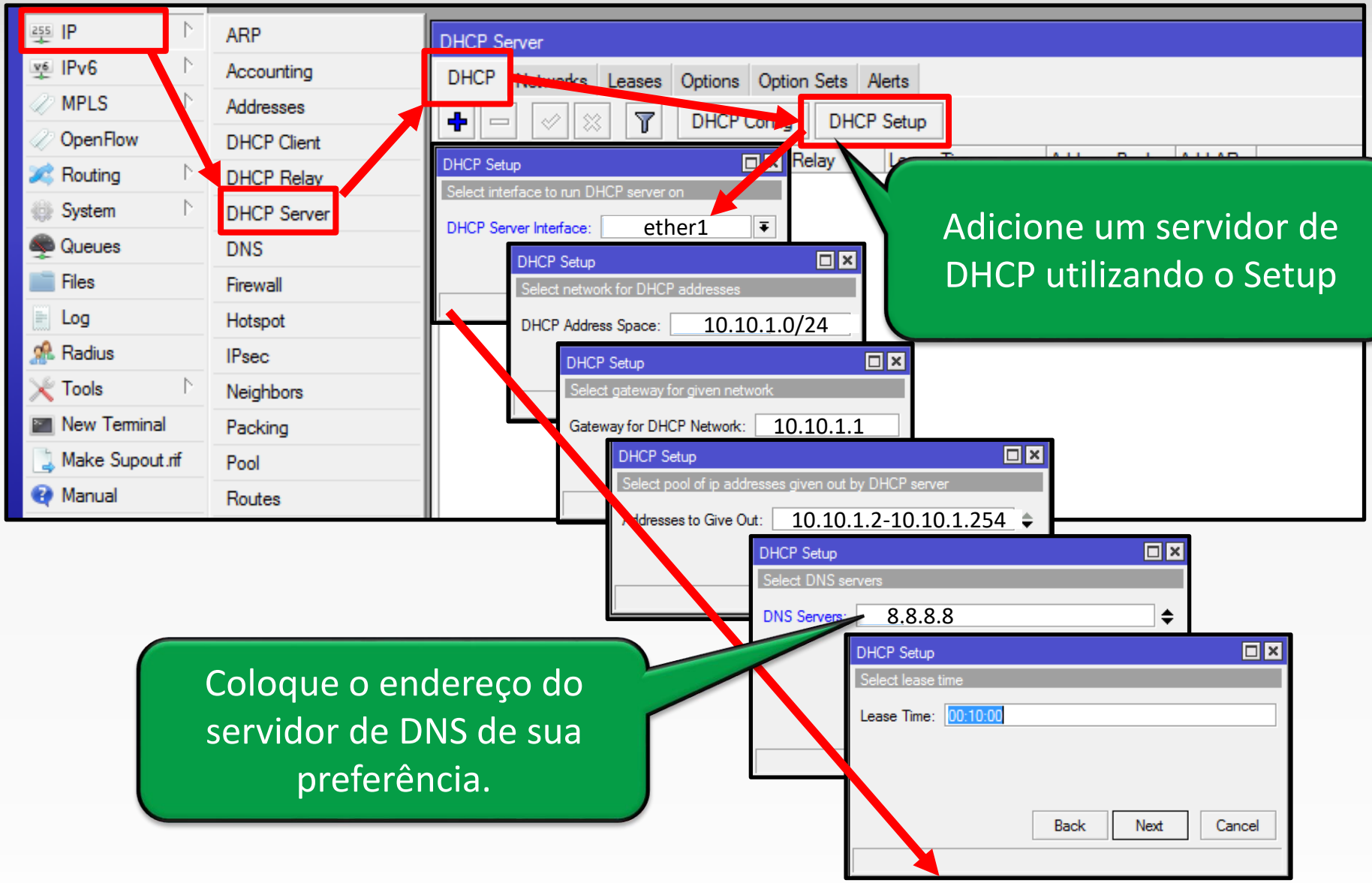
Redes Brasil

- Adicione os IP na interface de LAN

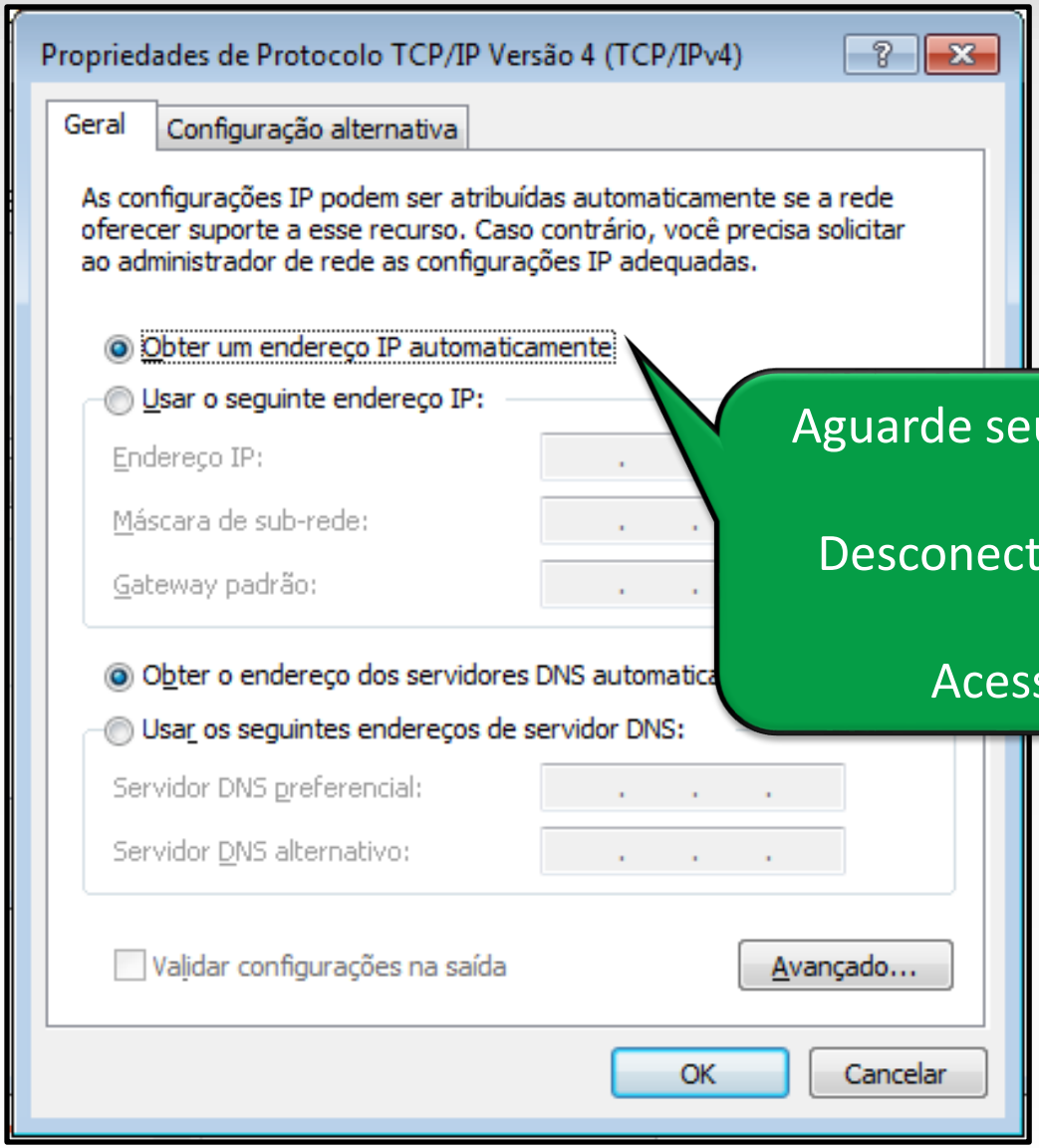


Configurando DHCP Server

Redes Brasil



DHCP Cliente

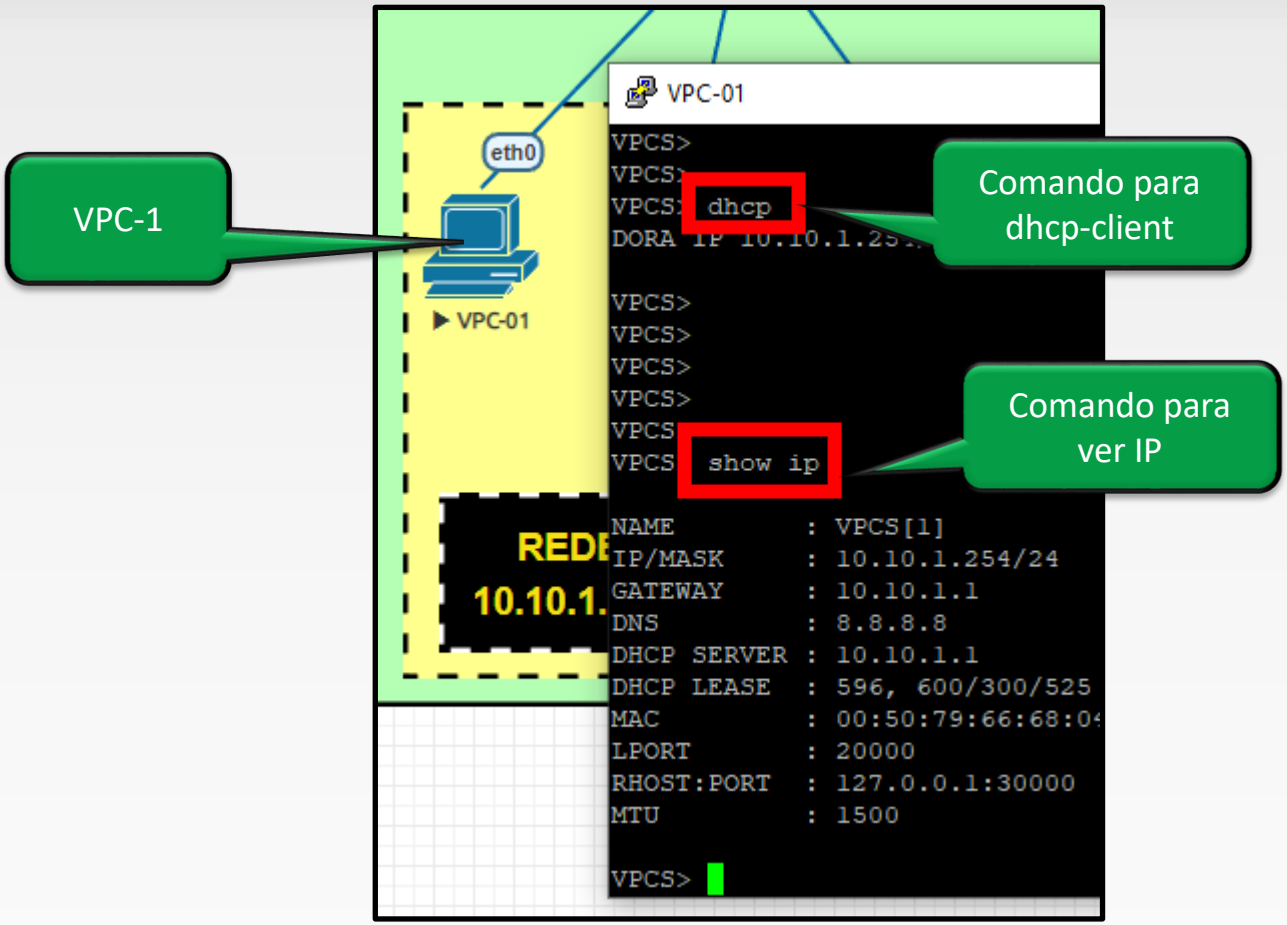


Aguarde seu PC pegar IP do roteador.

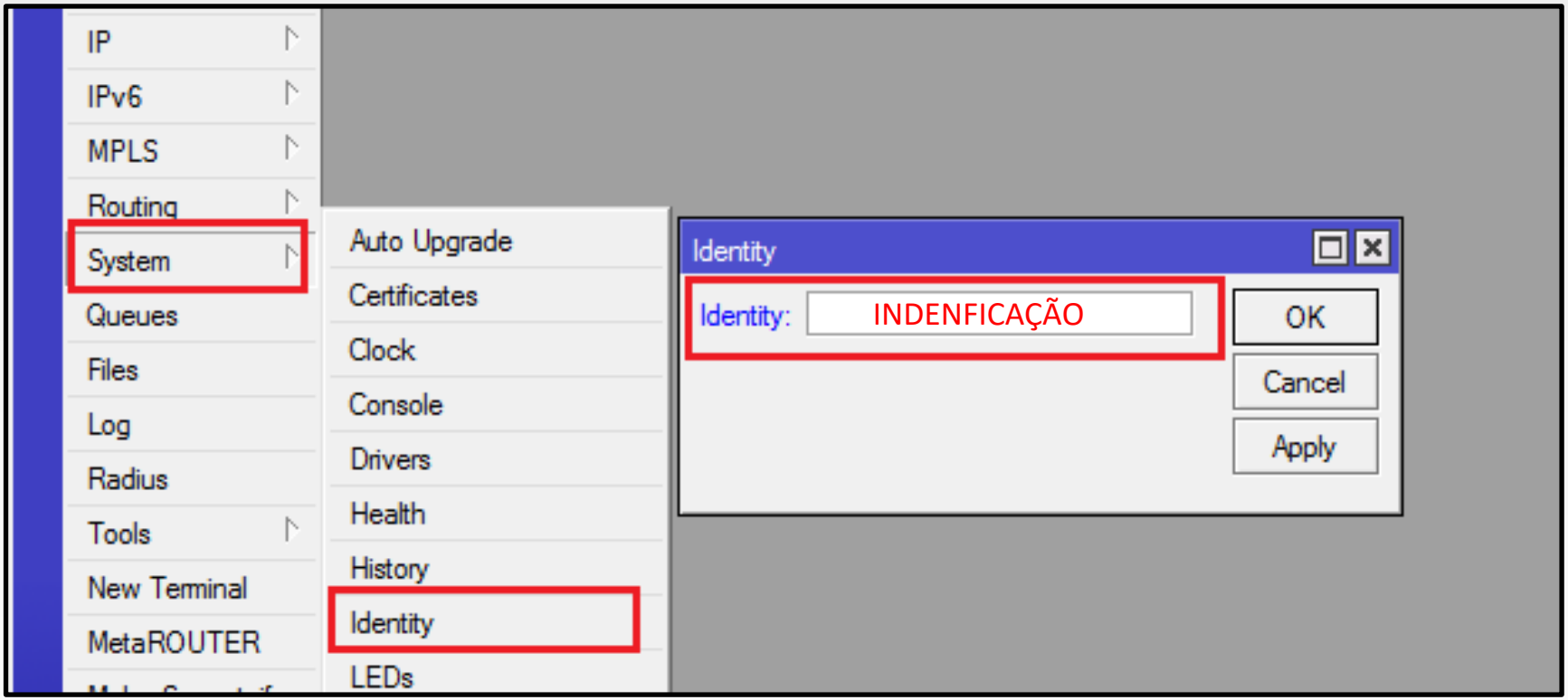
Desconecte-se do Winbox via MAC

Acesse o roteador via IP.

DHCP Cliente

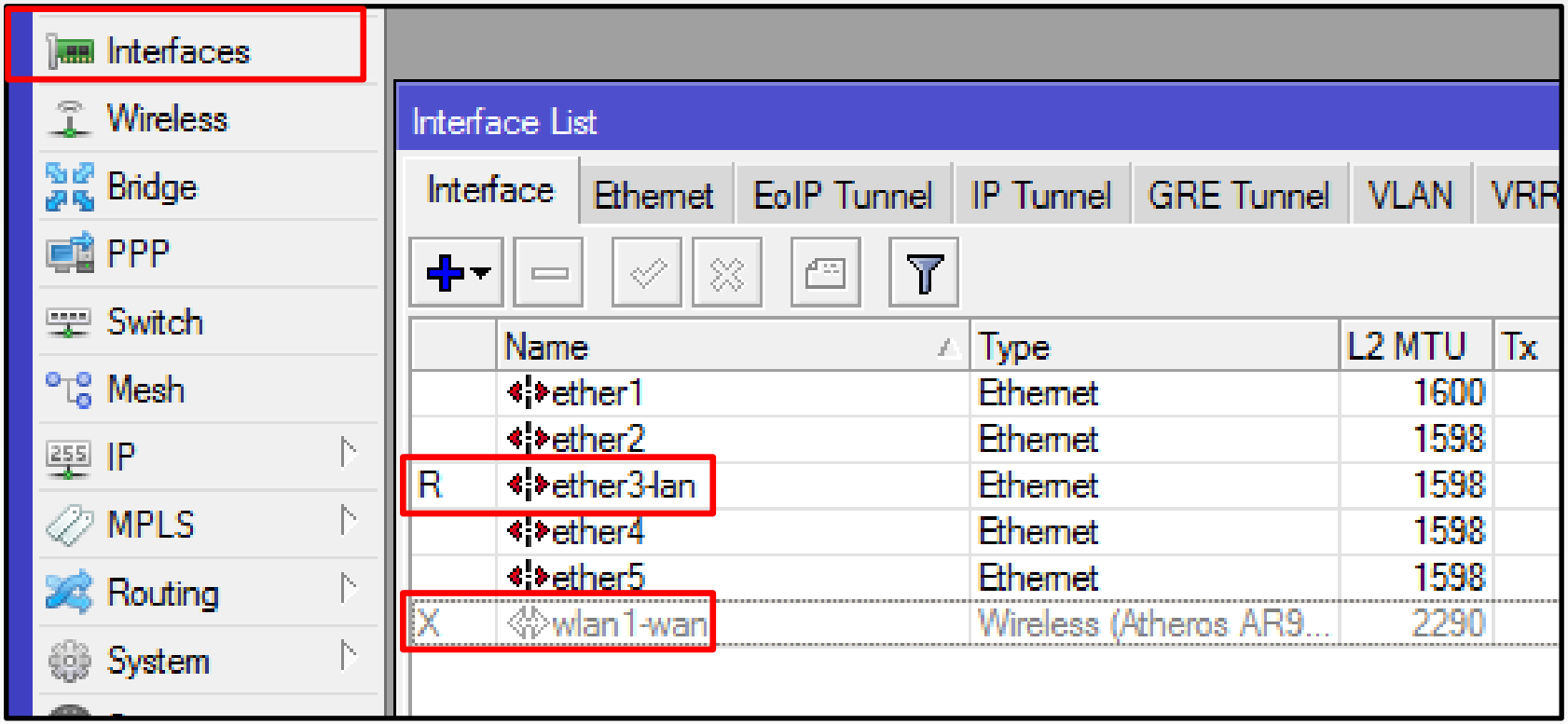


Identificando seu roteador



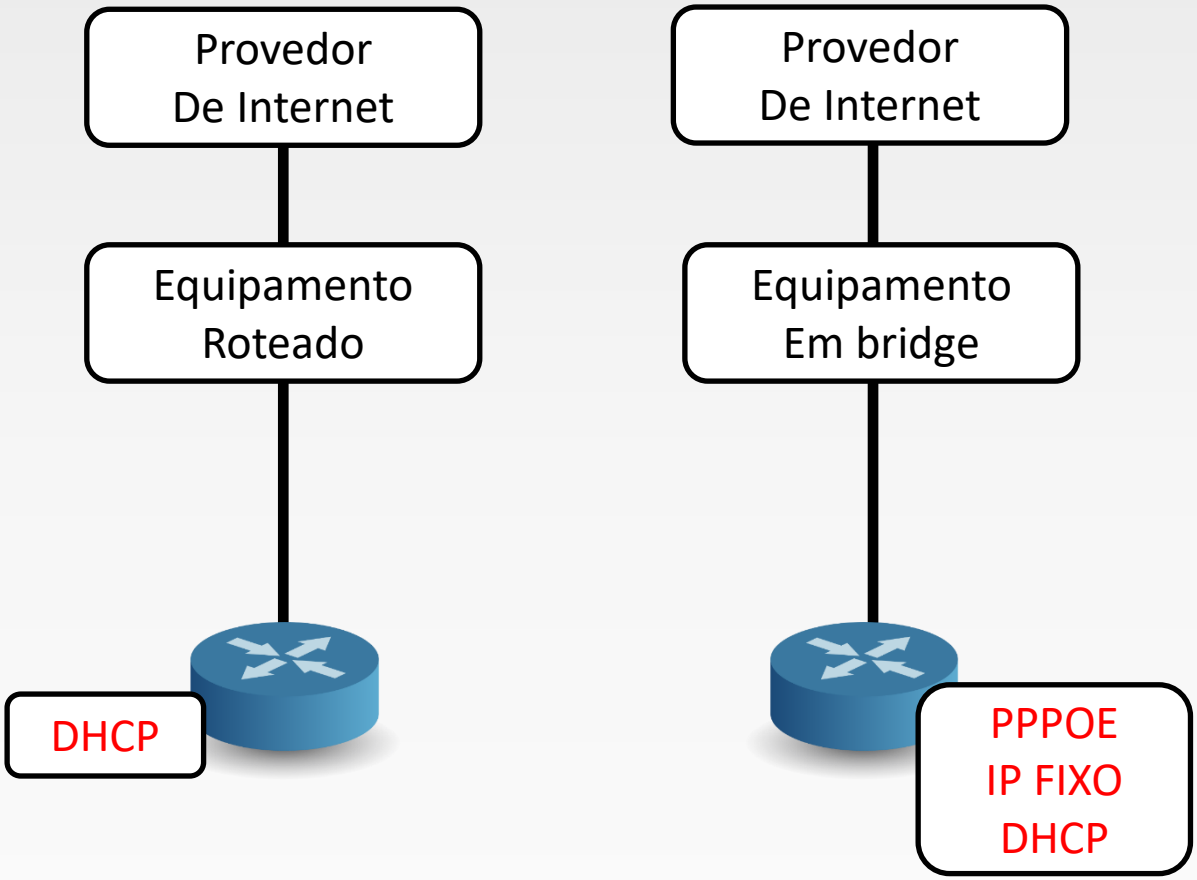
Renomeando suas interfaces

- Renomeie suas interface conforme a imagem abaixo.

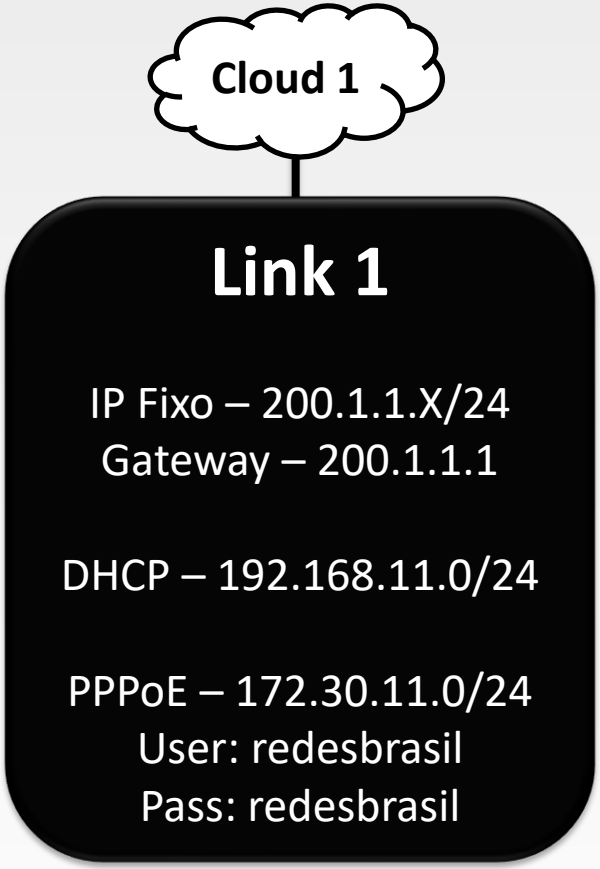


Equipamentos CPE

Link de Internet

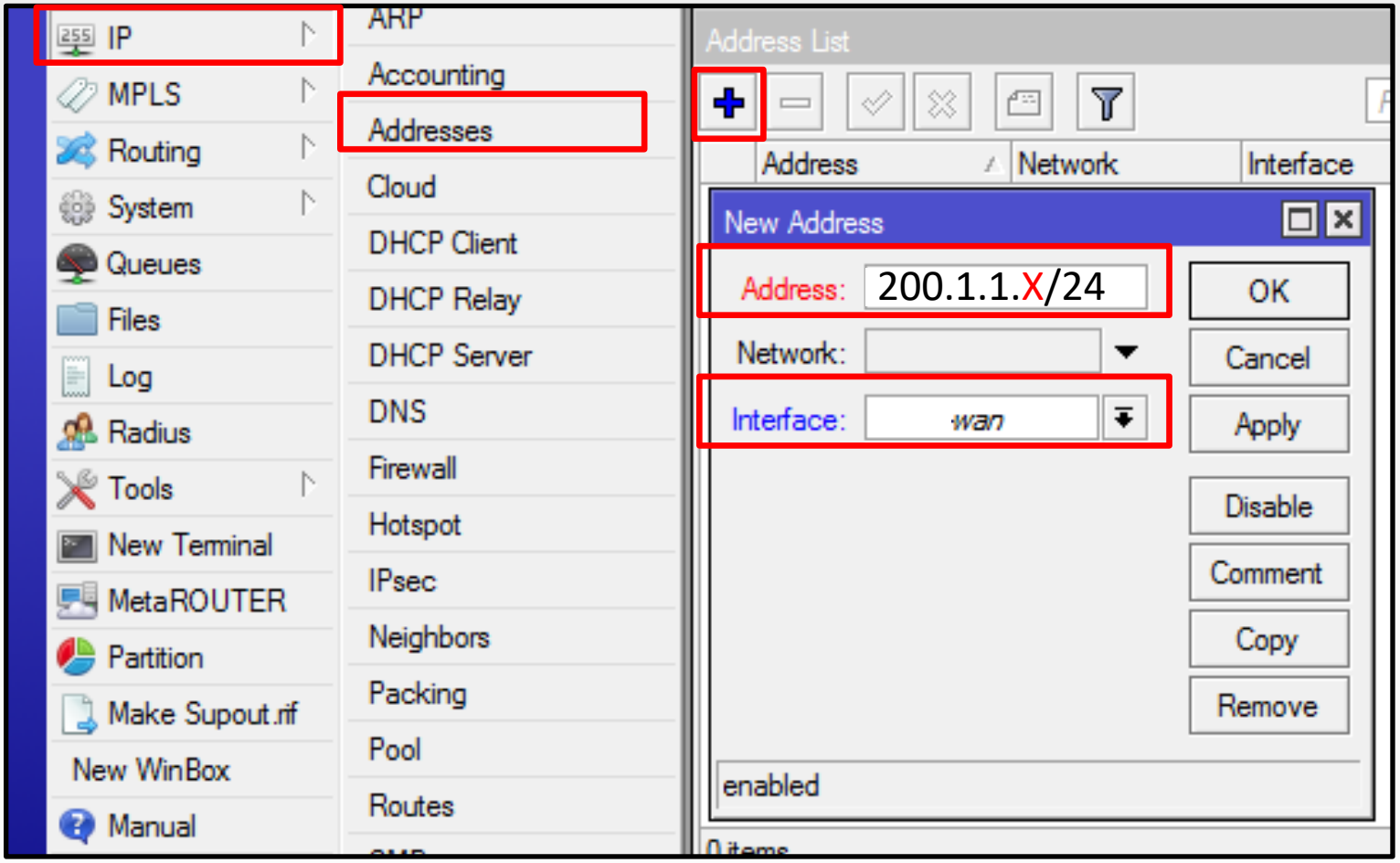


Recendo o Link de Internet



Configurando IP na interface de WAN

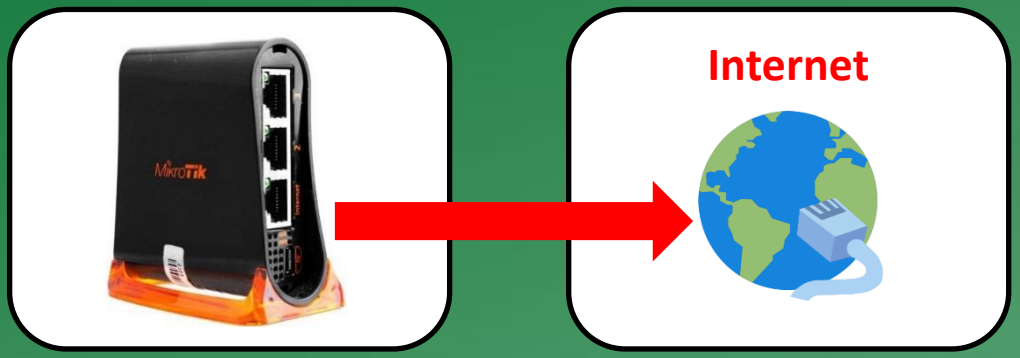
- Adicione os IP na interface de WAN



Teste de conectividade

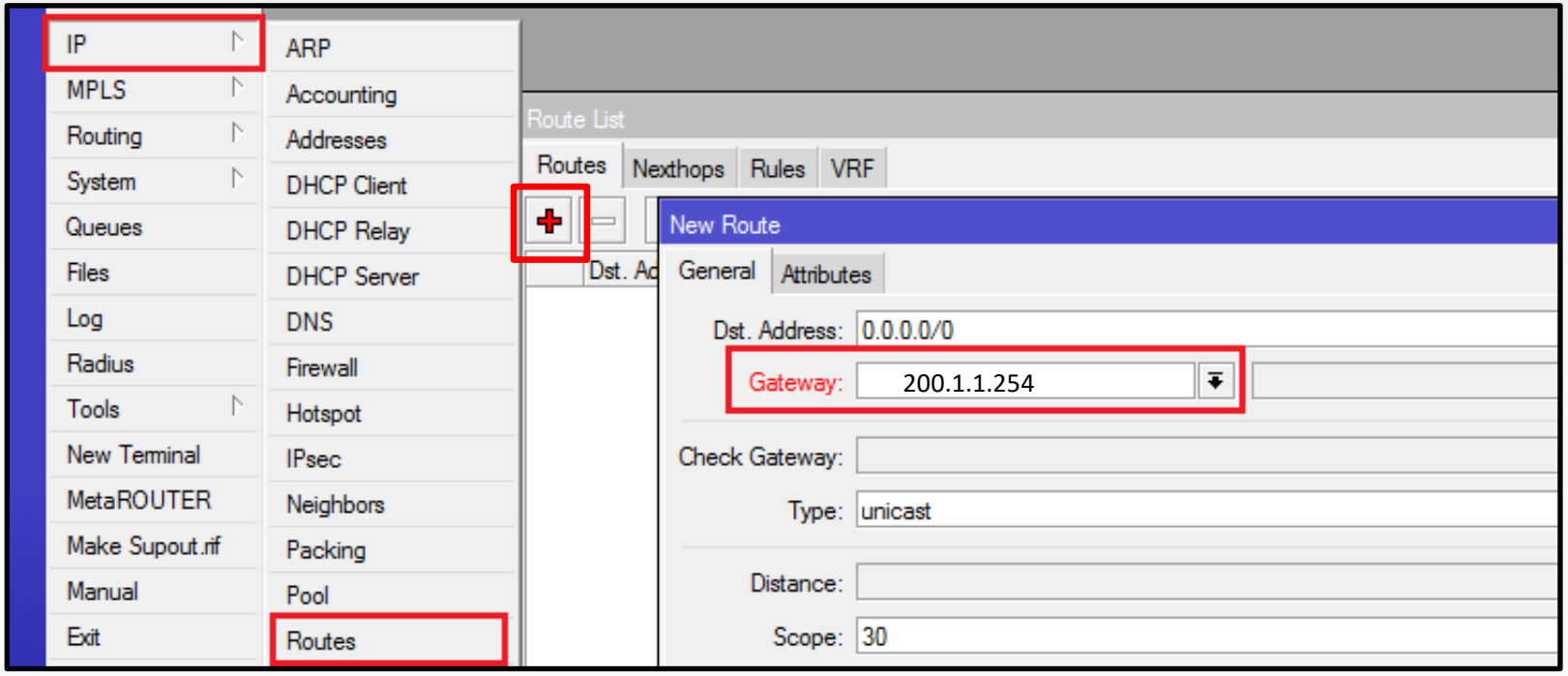
Redes Brasil

1) Pingar a partir da Routerboard o seguinte IP: **200.1.1.254**
2) Pingar a partir da Routerboard o seguinte IP: **8.8.8.8**



Configurando rota default

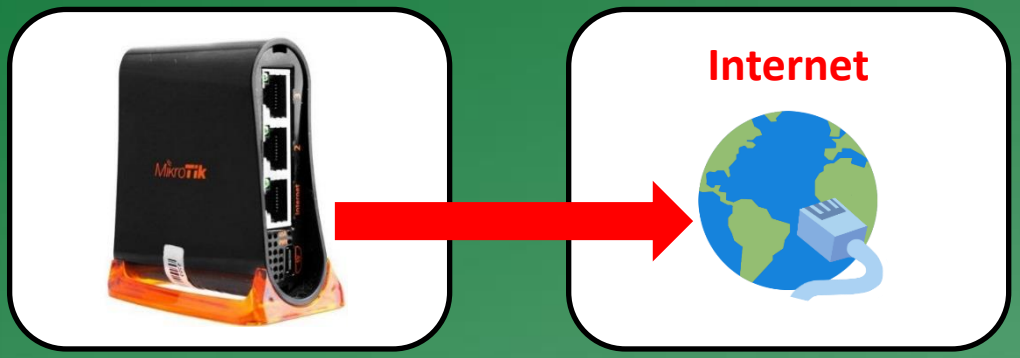
- Adicione a rota padrão



Teste de conectividade

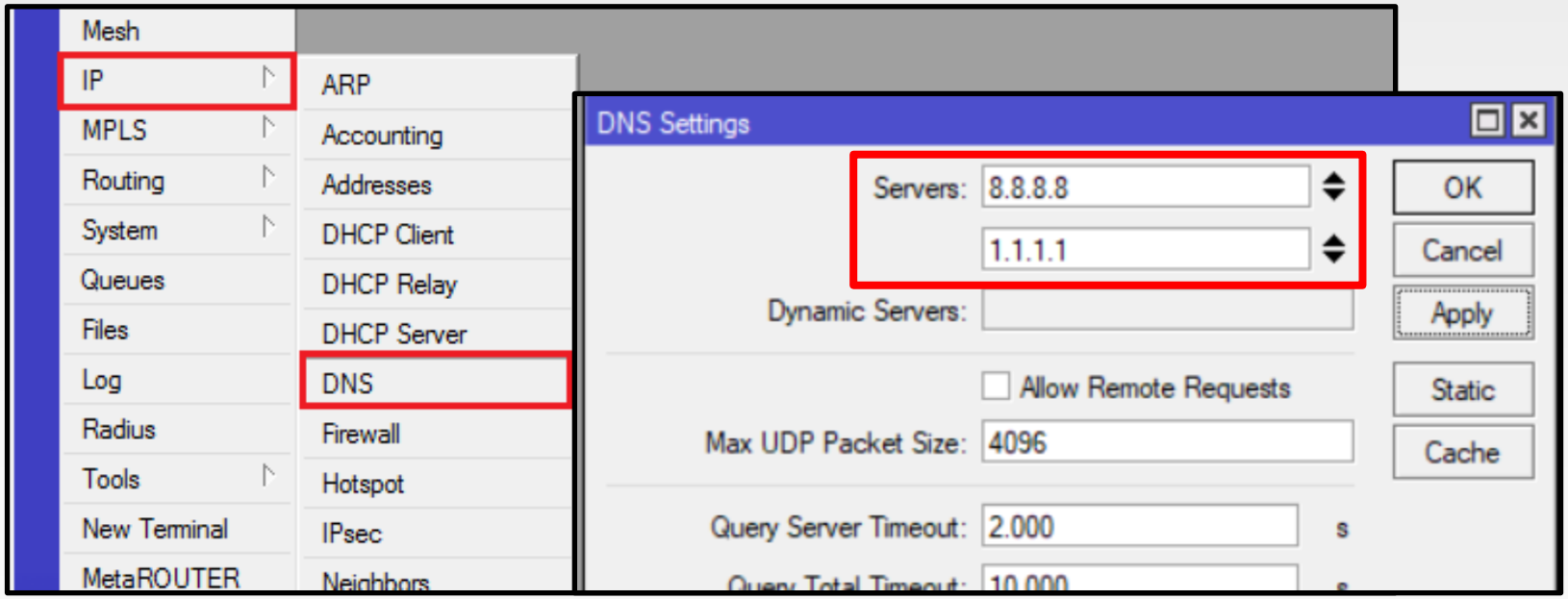
1) Pingar a partir da Routerboard o seguinte IP: **8.8.8.8**

2) Pingar a partir da Routerboard o domínio: **google.com**



Configurando DNS

- Adicione o servidor DNS



- Teste novamente o ping para: **google.com**

- Quando você checa a opção “Alow remote requests”, você está habilitando seu router como um servidor de DNS.

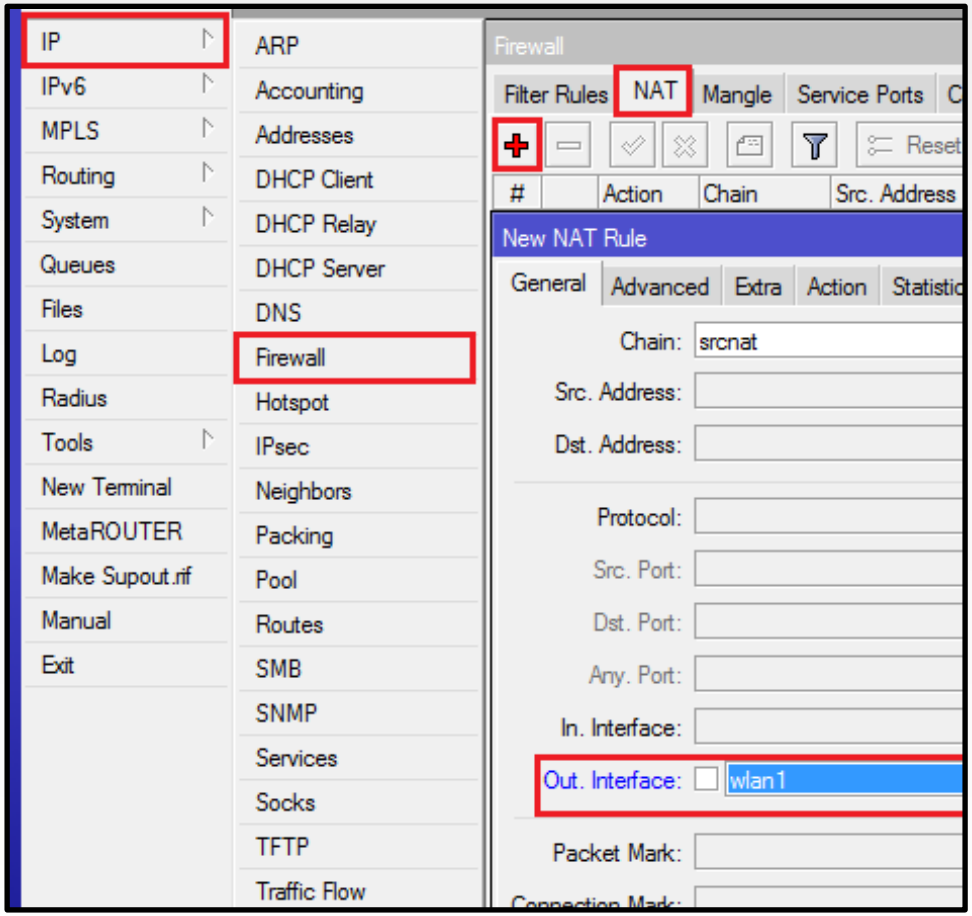
Teste de conectividade

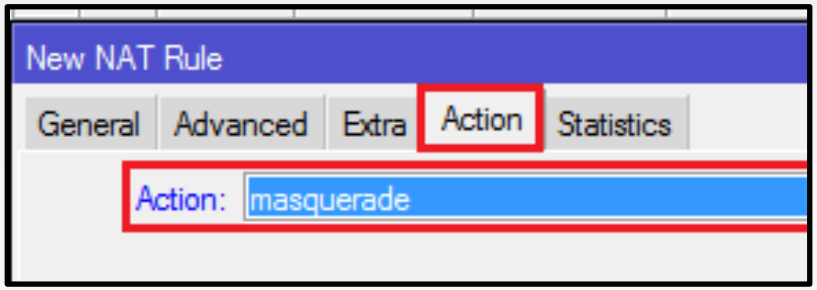
1) Pingar a partir de seu PC o seguinte IP: **8.8.8.8**

2) Pingar a partir de seu PC o domínio: **google.com**

Regra de mascaramento

- Adicionar uma regra de NAT, mascarando as requisições que saem pela interface wlan1.





LAB 1 – Configuração inicial

LAB 1

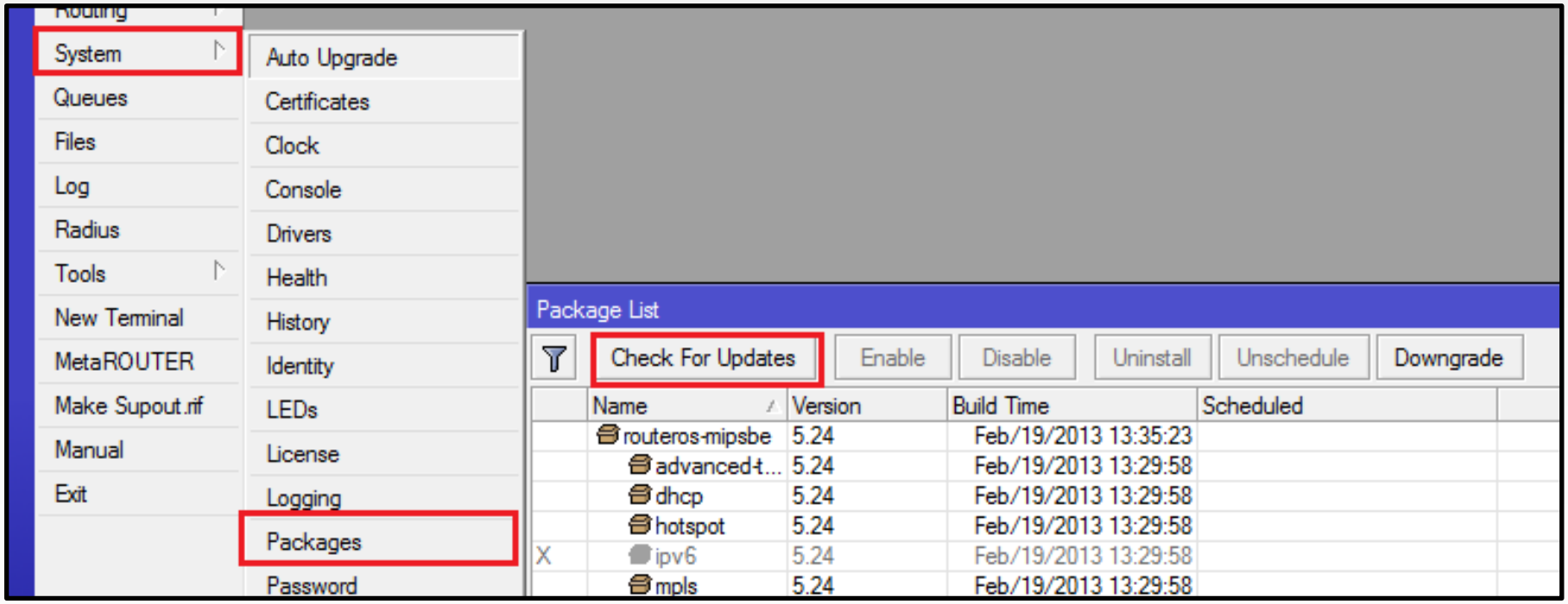
- Olhando o passo a passo abaixo faça a configuração inicial

1. Configurar IP na interface;
2. Configurar DHCP server;
3. Renomear o Roteador e as interfaces;
4. Configurar IP de WAN;
5. Configurar Rota Default;
6. Configurar DNS no roteador;
7. Configurar NAT;

MÓDULO 1.4 – Atualização

Atualizando o RouterOS

- Certifique se que o RouterOS tem conectividade com a internet e já resolve nomes (DNS funcionando).



E ai qual versão instalar ?

Redes Brasil

Donwgrade do RouterOS

- Baixe o arquivo para arquitetura correta;
- Faça upload;
- Execute os comandos abaixo.

  /system/package/downgrade

LAB 2 – Downgrade e Upgrade

LAB 2

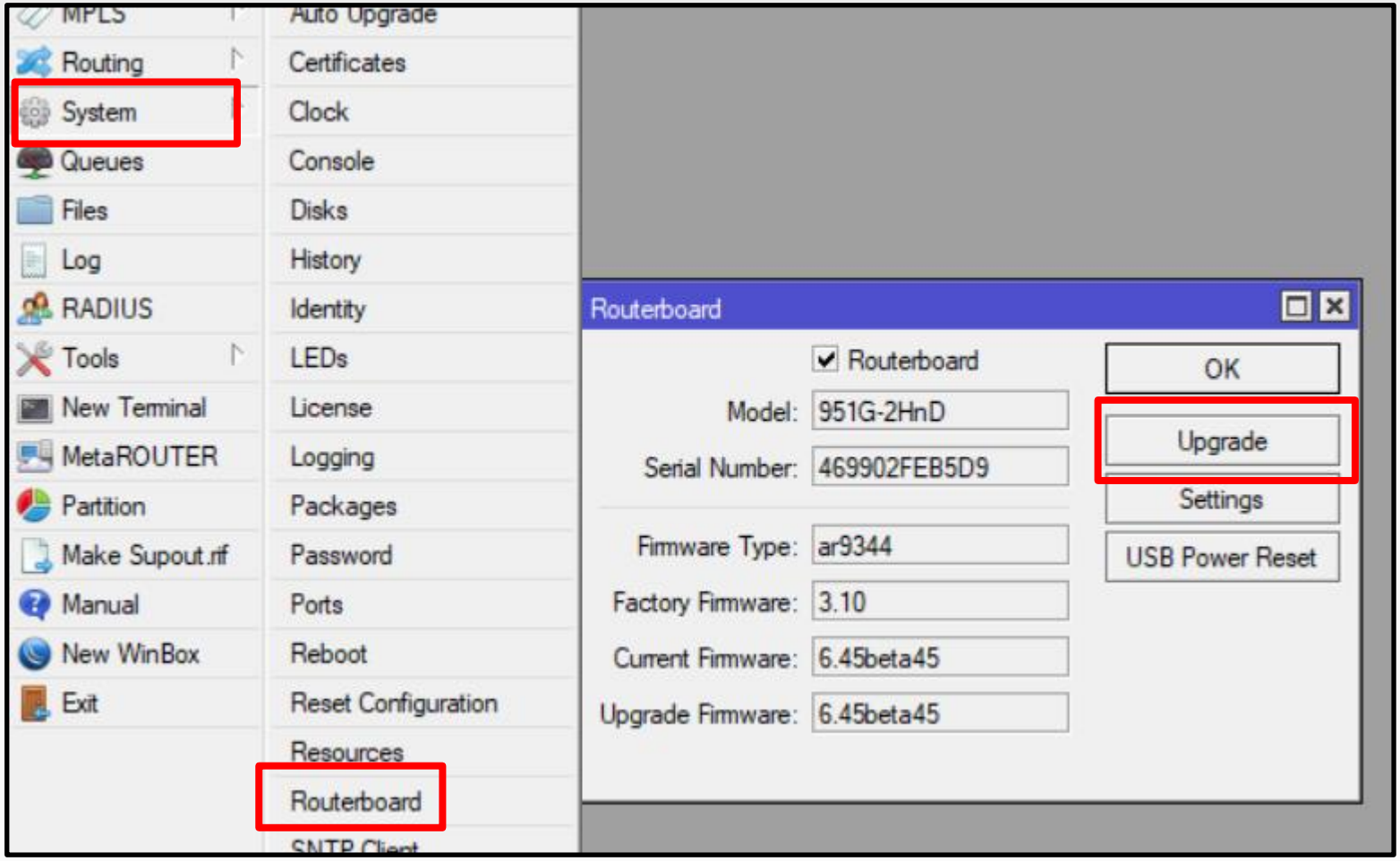
- Faça downgrade de R1 para a versão 7.5 e depois faça Upgrade para a versão mais recente no canal stable.

Quando devo atualizar ?

1. Você vai colocar o roteador em produção ?
2. Resolve um problema que precisa resolver ?
3. Corrige uma falha de segurança que você está exposto ?
4. Traz novos recursos que você precisa ?
5. Traz melhorias de performance que irão fazer diferença para sua rede ?

Upgrade de firmware

- Para fazer upgrade de firmware clique em:

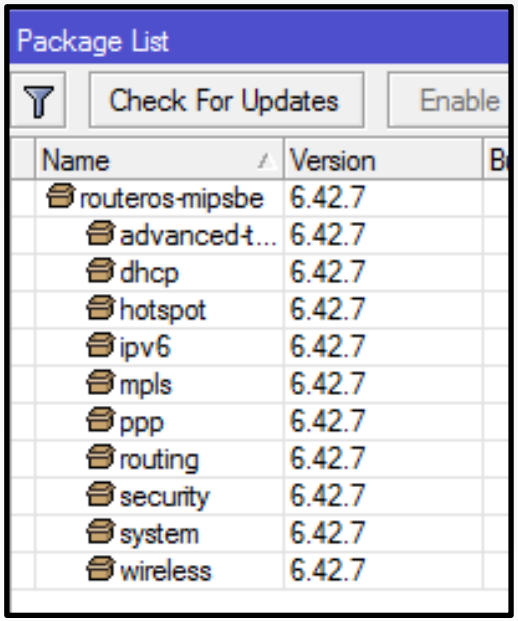


MÓDULO 1.5 – Pacotes adicionais

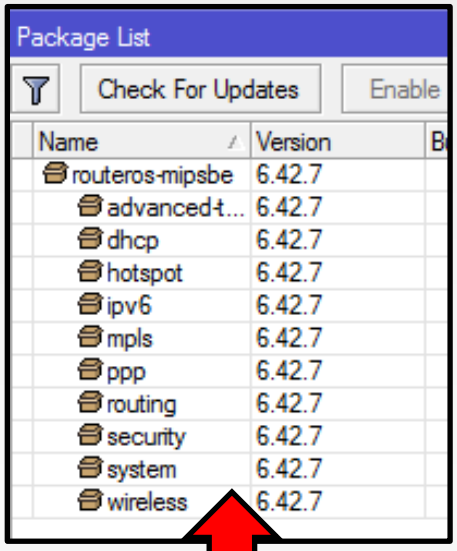
Adicionando novos pacotes

- É possível adicionar pacotes adicionais durante ou após a instalação do RouterOS.

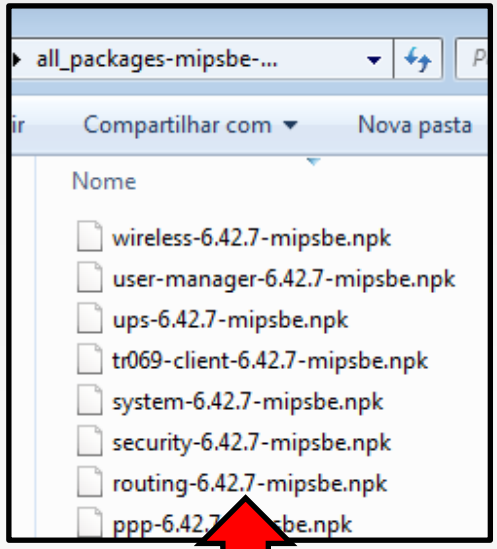
- Para adicionar após a instalação basta fazer o seguinte.
  - Fazer o download dos pacotes respeitando a arquitetura do processador e a versão atual do RouterOS.
  - Arrastar os arquivos para raiz de Files
  - Efetuar o reboot do roteador.



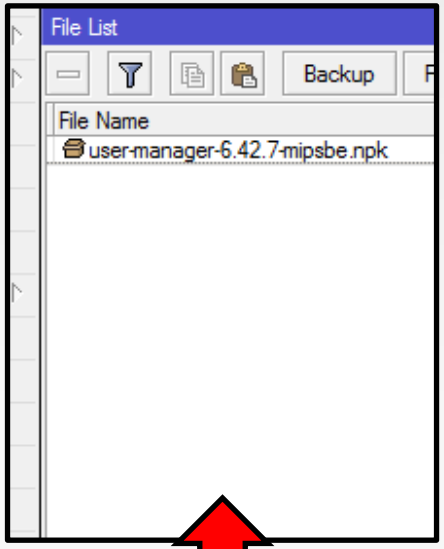
Adicionando novos pacotes



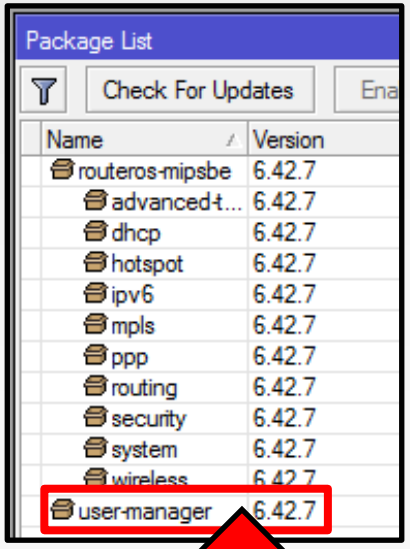
Pacotes instalados no roteador.



Pacotes baixados e extraídos no PC.



Pacote de User Manager enviado para o roteador.

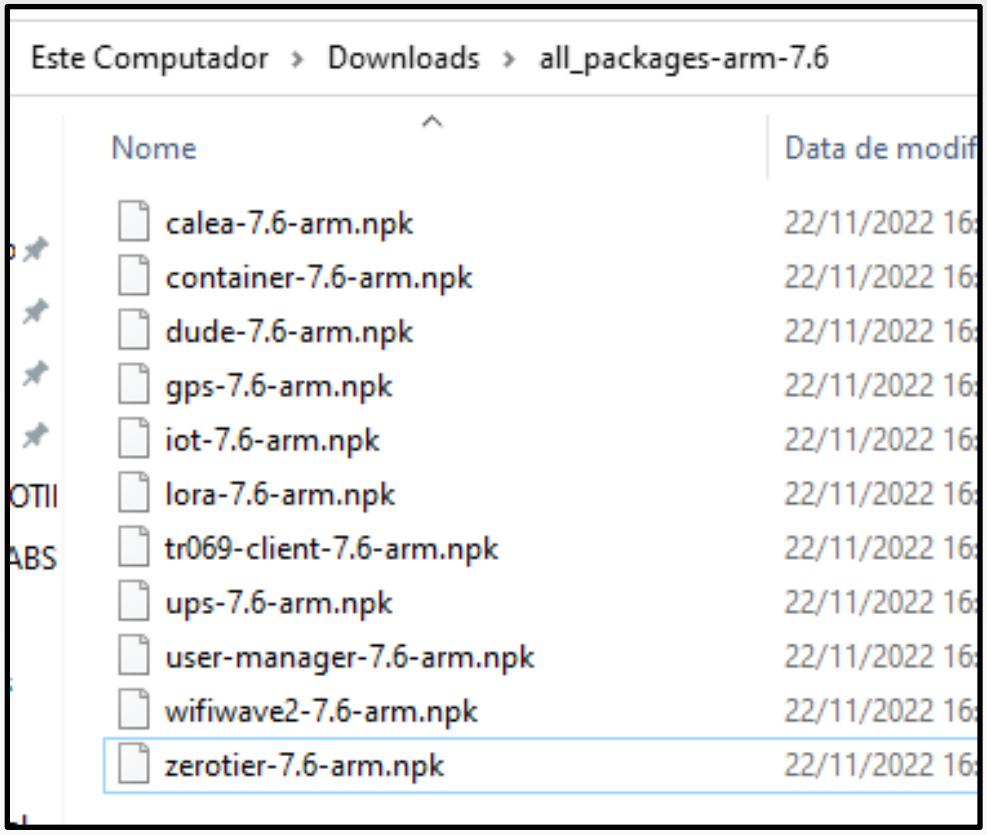


Após reboot o pacote foi instalado.

https://mikrotik.com/download

Pacotes adicionais

- Calea
- Container
- Dude
- GPS
- IOT
- LORA
- TR069
- UPS
- User Manager
- Wifiwave2
- ZeroTier



LAB 3 – Instalação de pacotes

LAB 3

- Faça a instalação do pacote do Dude;

MÓDULO 1.6 – Métodos de acesso

Métodos de acesso

- O RouterOS pode ser acessado via:

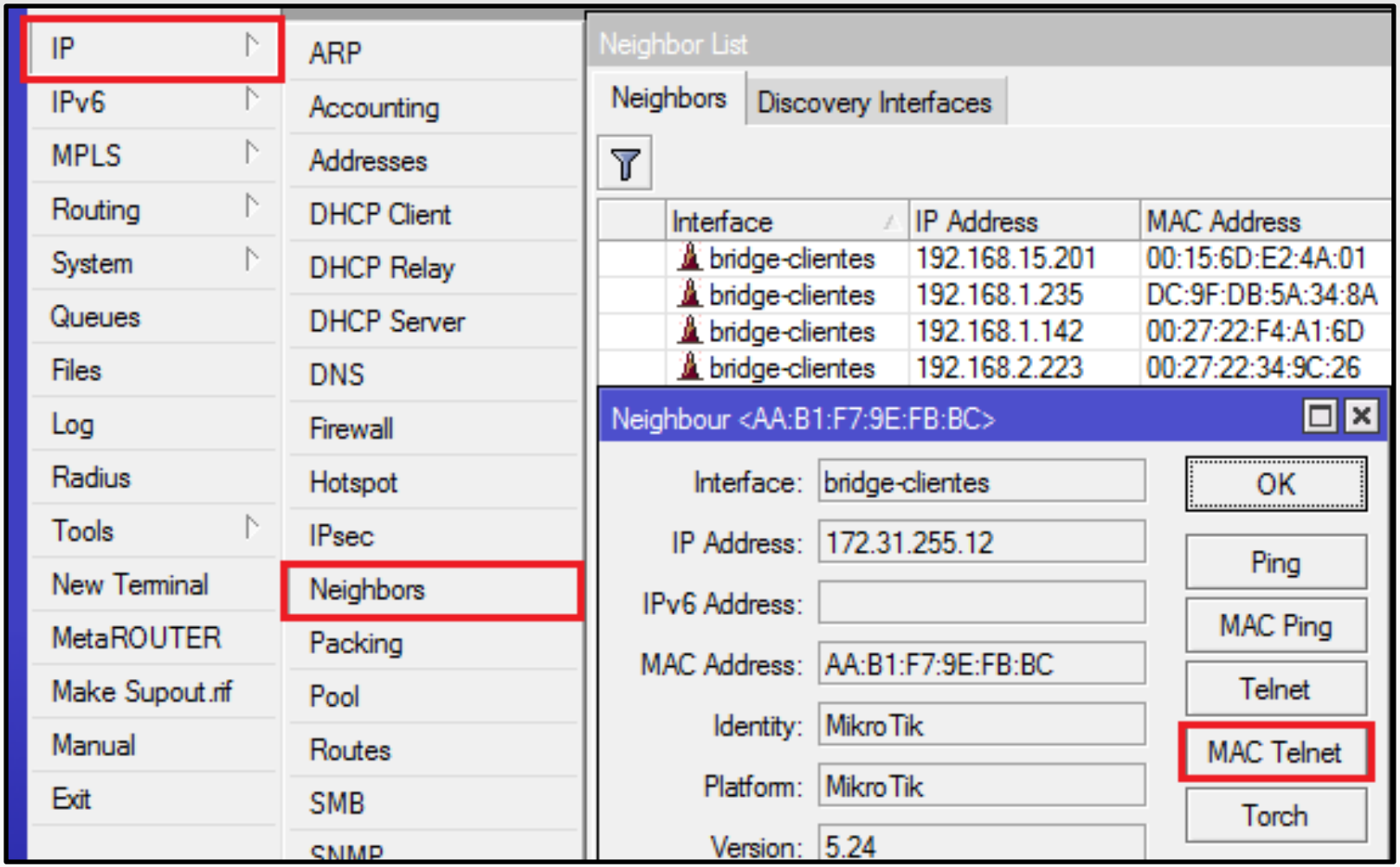
  - Winbox via MAC
  - Winbox via IP
  - Winbox via RoMON
  - Telnet via MAC
  - Telnet via IP
  - SSH
  - HTTP
  - HTTPS
  - API
  - FTP
  - Cabo console (caso roteador possua porta console)
  - Teclado e monitor (caso tenha instalado em um PC).

Primeiro acesso ao roteador

- Se o seu roteador não possui endereço de IP (v4 ou v6), poderá ser gerenciado via.
  - Mac-winbox
  - Mac-telnet
  - Teclado e monitor (caso tenha instalado em um PC).
  - Cabo console (caso roteador possua porta console)

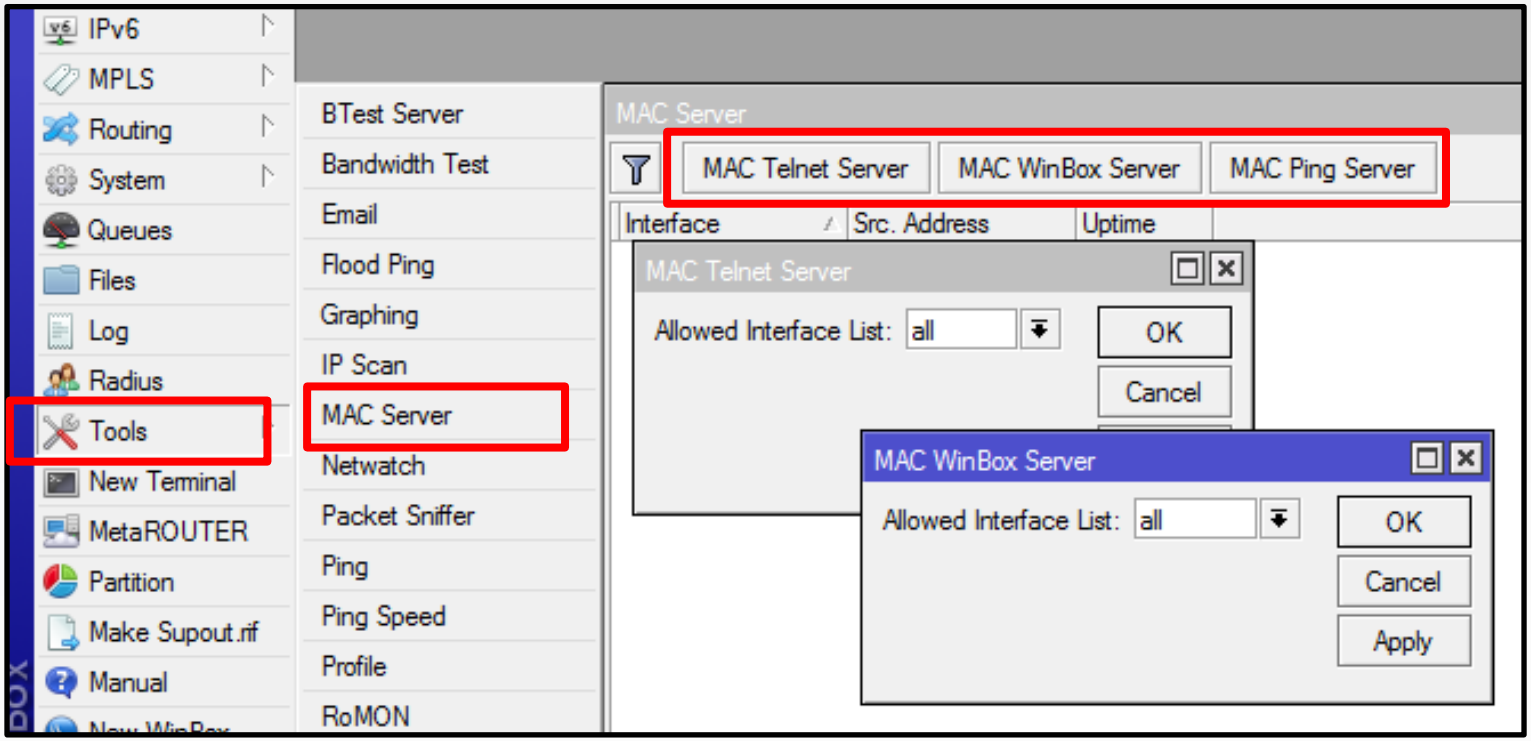
- Se o seu roteador está com pacote de IPv6 habilitado ele poderá ser gerenciado também a partir do endereço de link-local que é gerado de forma automática.

MAC-Telnet



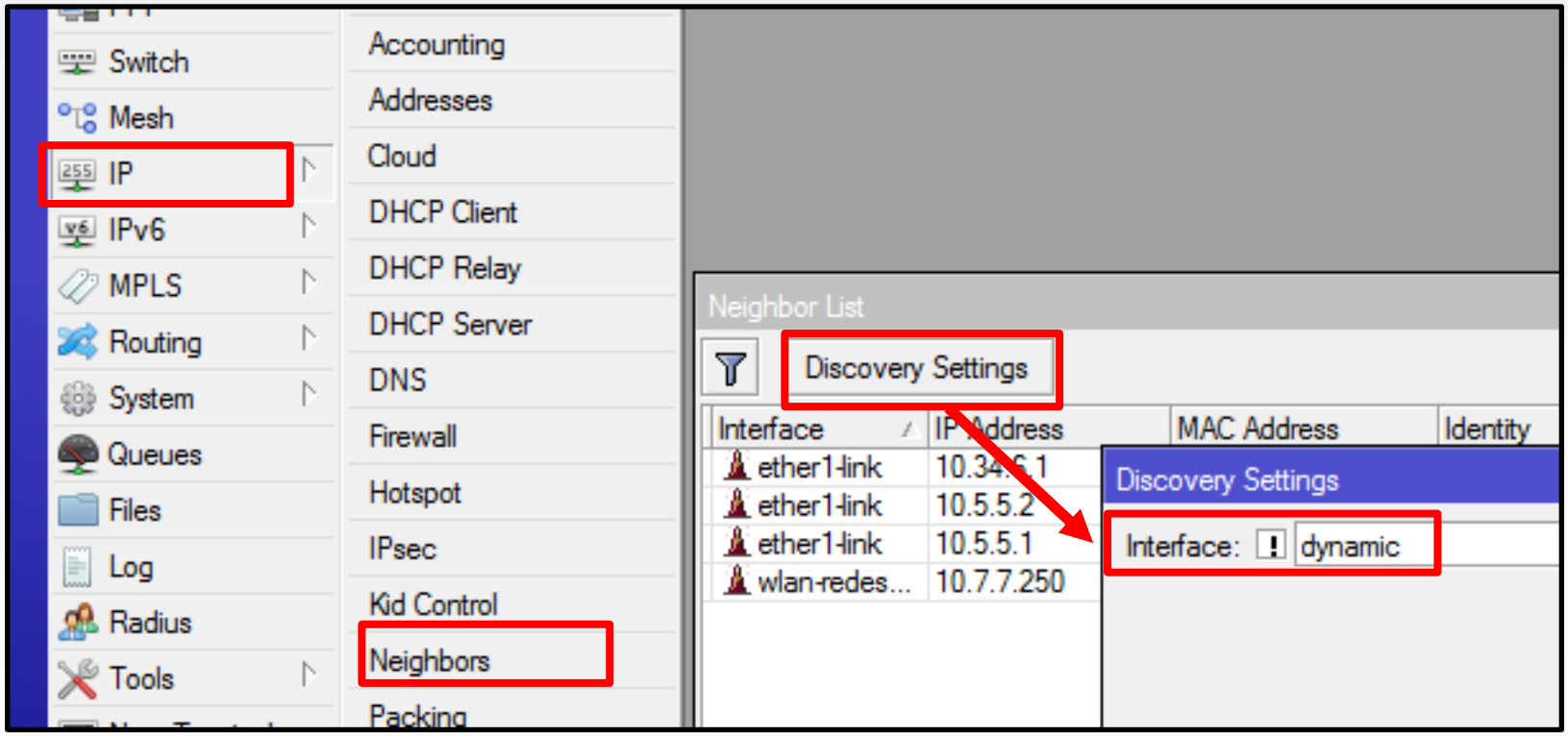
Acesso via MAC

- O acesso via MAC address é possível porque o RouterOS possui um MAC server.
- Esse função vem habitada por padrão e pode ser desabilitada.



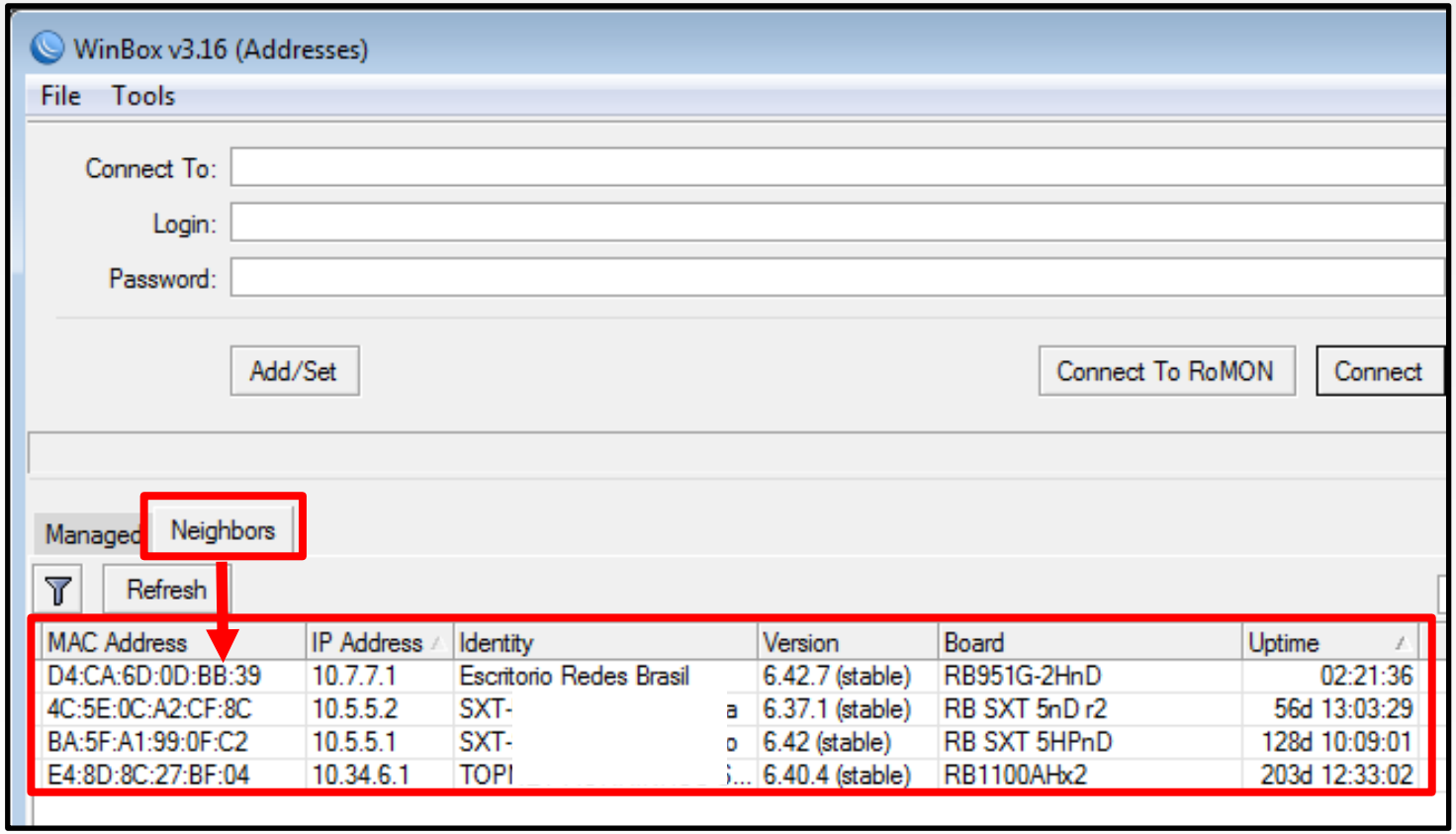
MNDP

- MikroTik Neighbor Discovery protocol
- Protocolo para descoberta de vizinhos.



MNDP

- Winbox utiliza o MNDP para encontrar os dispositivos da MikroTik na descoberta de vizinhos.



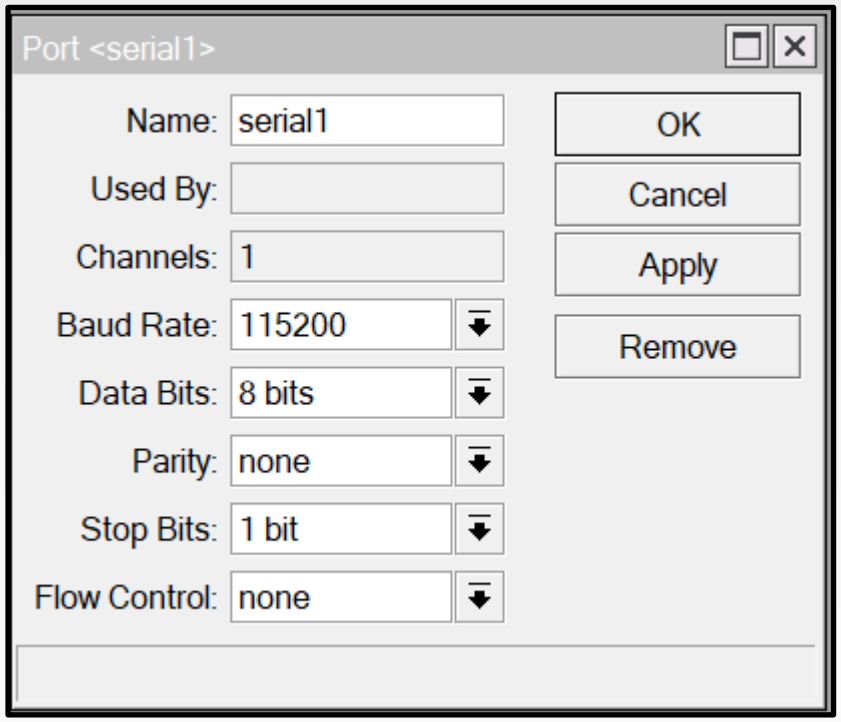
LAB 4 – Acessos via MAC

LAB 4

1. Desabilite o acesso via MAC telnet do R2 na interface que se comunica com R1 e tente fazer o acesso.
2. Desabilite o MNDP na interface do R2 que se comunica com o PC local e faça o Discovery via Winbox no PC para testar se funcionou.

Acesso via cabo console

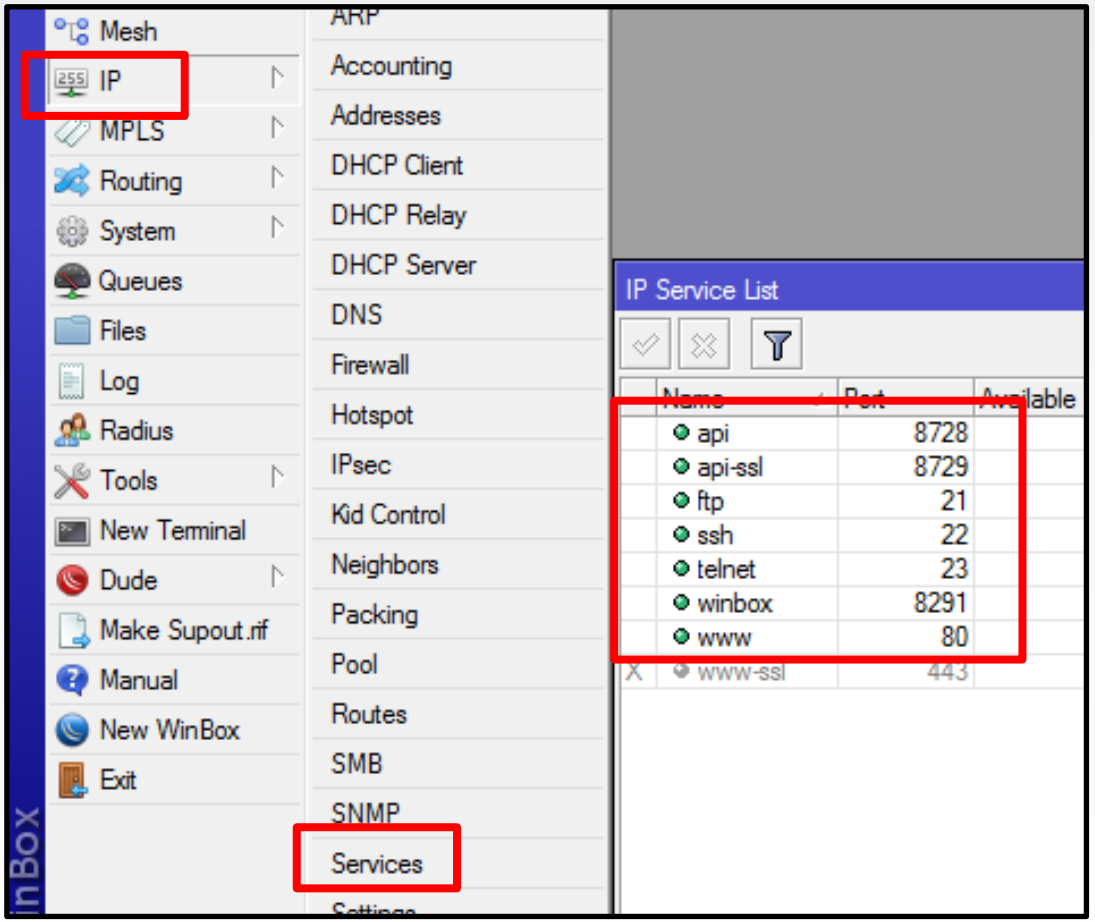
Acesso via cabo console



Outros modos de acesso

- Após configurar um endereço de IP no RouterOS existem outros modos de acesso.

  - API
  - SSH
  - FTP
  - Telnet
  - Web



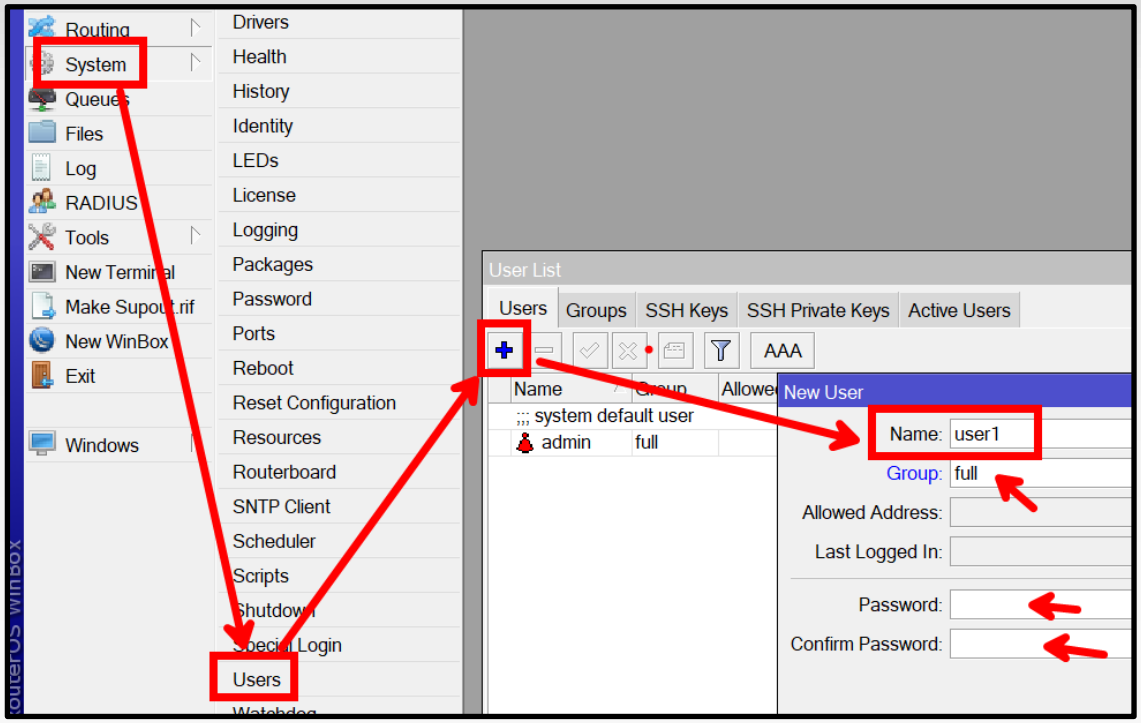
LAB 5 – Desabilitando serviços

LAB 5

1. Acesse o R2 e configure IP na interface que se comunica com o PC;
2. Crie o DHCP Server;
3. Faça o Linux pegar IP;
4. Faça testes de acessos com os serviços de FTP, Telnet, SSH, Winbox e WWW.
5. Troque as portas e tente acessar novamente;
6. Desabilite os serviços que você não usa.

MÓDULO 1.7 – Usuários e Grupos

Criando novo usuário

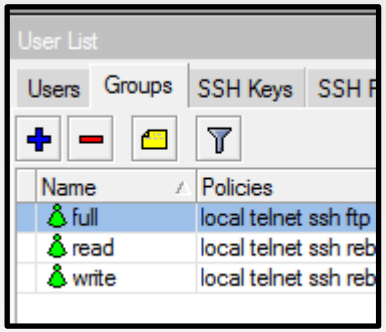


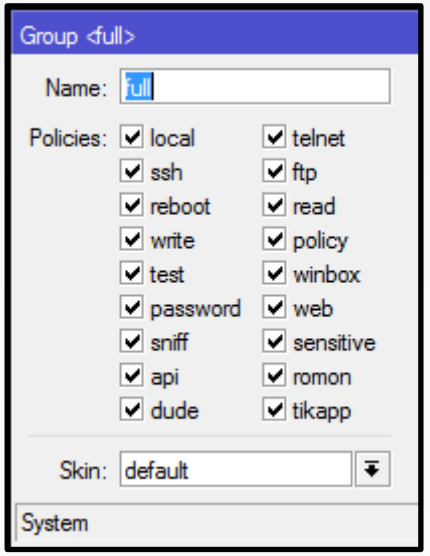
1. Crie um novo usuário com senha ;
2. Apague o usuário admin.

Usuário e grupos

Redes Brasil

- É possível criar novos usuário e grupos de usuários;
- Por padrão o RouterOS vem com usuário admin e sem senha;
- Por padrão existem 3 grupos:
  - **full** = Tem acesso completo no roteador com todas as permissões liberadas;
  - **read** = Tem acesso somente de leitura (não consegue criar nem alterar nada e também não possui acesso FTP);
  - **write** = Tem acesso a ler, criar e alterar configurações dentro do roteador, porém não tem permissão de criar, alterar e remover outros usuários e grupo de usuários (também não possui acesso FTP).
- Utilizando grupos personalizados podemos restringir acesso a alguns serviços.
- Via acesso web (webfig) podemos desenhar um Skin e liberar acesso somente partes especificas dentro do roteador.





Como usar Skin

1. Criar o Skin via web;

2. Criar um novo grupo de usuário e selecionar o Skin criado;

3. Criar um usuário e selecionar o grupo criado;

LAB 6 – Criando novo usuário

LAB 6

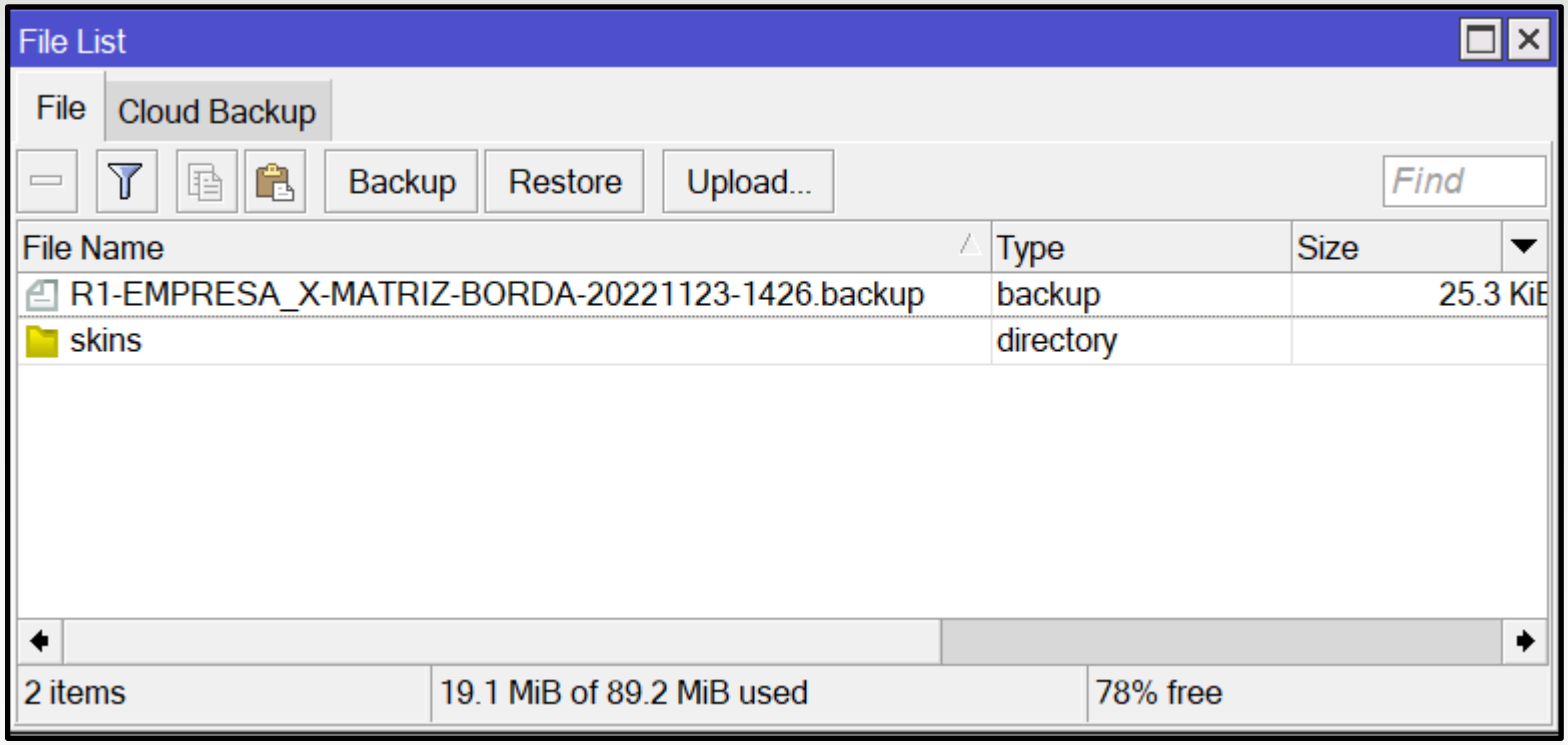
1. Acesse R2 via web;
2. Desenhe um Skin a sua escolha;
3. Crie um grupo que faça uso do Skin criado;
4. Crie um novo usuário e selecione o grupo criado no passo anterior;
5. Faça login via winbox e via web com esse novo usuário.

MÓDULO 1.8 - Backups

Diferença entre os dois backups

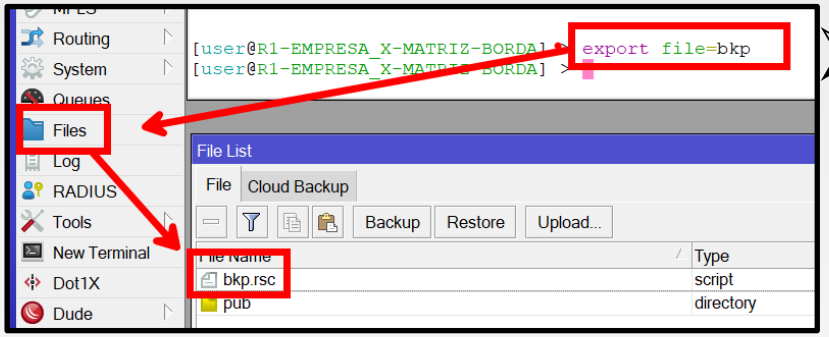
	Backup comum	Comando export
Criptografado	X	
Permite colocar senha	X	
Carrega usuários de acesso ao router	X	
Carrega usuários PPP, hotspot e outros	X	X
Possível editar		X
Compatível com hardware diferente		X
Possibilidade de exportar e importar por partes		X

Backup comum (binário)



- Observe que o arquivo gerado recebe o identificação do router mais as informações de data e hora.

Localizando e editando backup



- Após o comando “export file=bkp ” será gerado um arquivos no menu files.

```
bkp.rsc - Bloco de Notas
Arquivo  Editar  Formatar  Exibir  Ajuda
# nov/23/2022 16:13:34 by RouterOS 7.6
# software id =
#
/interface ethernet
set [ find default-name=ether1 ] name=ether1-rede-a
set [ find default-name=ether4 ] name=ether4-rede-b
set [ find default-name=ether10 ] name=ether10-link1
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/ip pool
add name=dhcp_pool0 ranges=10.10.1.2-10.10.1.254
/ip dhcp-server
add address-pool=dhcp_pool0 interface=ether1-rede-a name=dhcp1
/port
set 0 name=serial0
/ip address
add address=10.10.1.1/24 interface=ether1-rede-a network=10.10.1.0
add address=200.1.1.158/24 interface=ether10-link1 network=200.1.1.0
/ip dhcp-server network
add address=10.10.1.0/24 dns-server=10.10.1.1 gateway=10.10.1.1
```

- Após transferir o arquivo para sua maquina ele poderá ser editado pelo bloco de notas.

Enviando Backup via E-mail OutLook


```
:g email "seu_email_aqui"
:g senha "sua_senha_aqui"

/tool e-mail
set address=smtp-mail.outlook.com from=$email port=587 tls=starttls user=$email
password=$senha

/system scheduler
add disabled=no interval=1m name=BACKUP-VIA-EMAIL on-event=":g RouterName [/sy\
    stem identity get name]\r\
    \n\r\
    \n/export file=\"\$RouterName\"\r\
    \n\r\
    \n:delay 10\r\
    \n\r\
    \n/tool/e-mail/send to=\$email file=\$RouterName subject=\"BACKUP \$RouterN\
    ame\"" \
    start-date=nov/30/2022 start-time=02:10:00
```

Enviando Backup via FTP


```
/system scheduler
add interval=1d name=BACKUP-VIA-FTP on-event=":g server \"10.10.254.1\"\t\t\r\
   \n:g user \"usuario-ftp\"\r\
   \n:g pass \"senha-ftp\"\r\
   \n:g port \"21\"\r\
   \n\r\
   \n\r\
   \n:g RouterName [/system identity get name]\r\
   \n\r\
   \n/export file=\"\$RouterName\"\r\
   \n:delay 2\r\
   \n/tool fetch upload=yes mode=ftp address=\$server user=\$user
password=\$p\
   ass src-path=(\"/\$RouterName\".\".rsc\") dst-path=(\"/\$RouterName\".\".rs\
   c\") port=\$port\r\
   \n" \
   start-date=nov/30/2022 start-time=14:16:41
```

Enviando Backup por Telegram

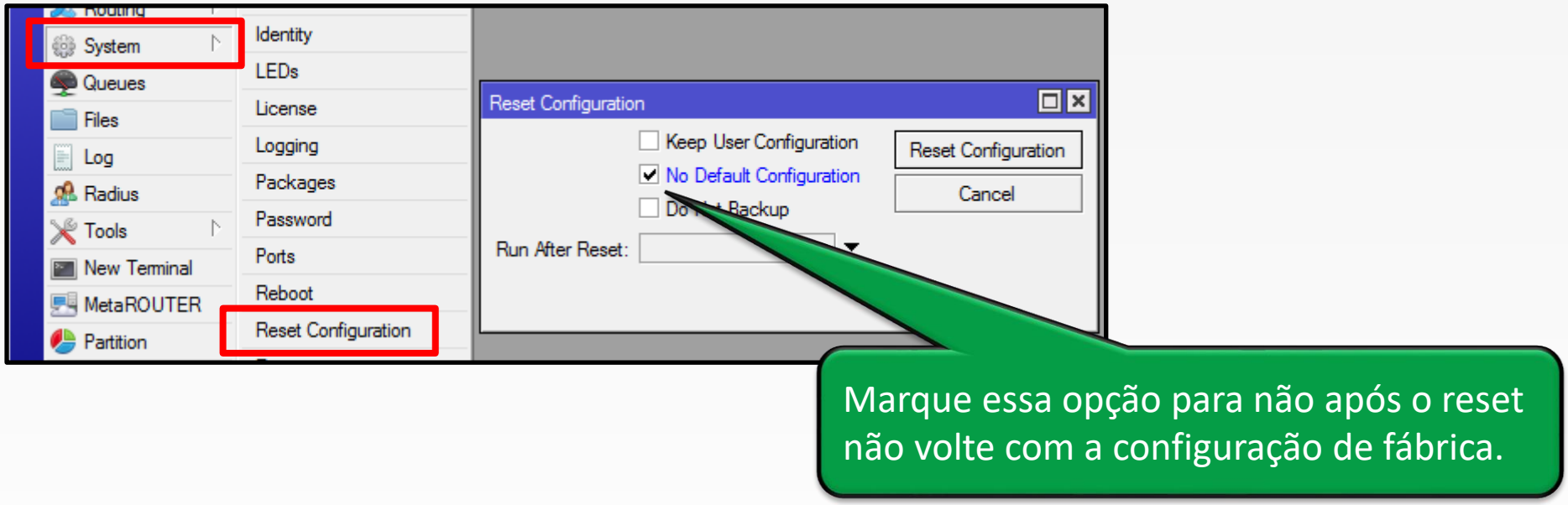
Clique no link e fale com o Bot.

https://t.me/RedesBrasilBackups_bot

MÓDULO 1.9 – Reset de equipamentos

Resetando seu roteador

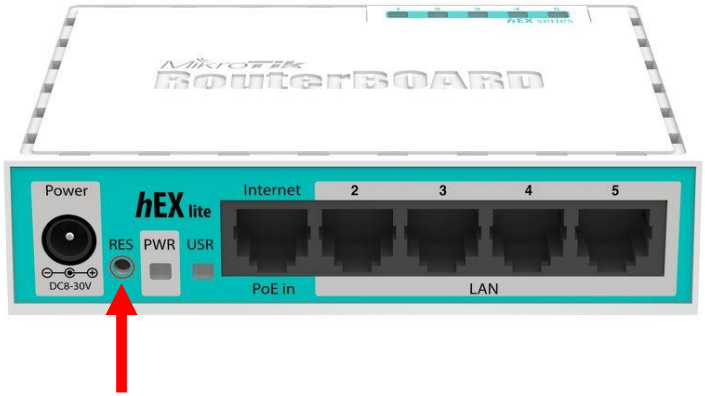
- Se não for o primeiro acesso siga a imagem abaixo para efetuar o reset.



Resetando seu roteador

Redes Brasil

- Se você não possui as credenciais de acesso ao roteador o reset deverá ser feito usando o botão de reset.



Atenção

Para resetar o equipamento:

1. **Desligue o cabo de alimentação do equipamento.**
2. **Pressione o botão de reset e mantenha pressionado.**
3. **Ligue o cabo de alimentação;**
4. **Após ligar o cabo de alimentação conte 5 segundos se solte o botão de reset.**

Funções do Botão de Reset

- O botão de reset tem pelo menos 4 funções acionadas da seguinte forma.
  - Desligue a alimentação do equipamento.
  - Ligue o equipamento com botão de reset pressionado.
  - Solte o botão de reset observando a tabela abaixo

Função	Tempo
Ativar backup RouterBOOT	3 segundos
Reset do equipamento	5 segundos
Ativar modo Caps	10 segundos
Reinstalação via Netinstall	15 ou mais segundos

https://help.mikrotik.com/docs/display/ROS/Reset+Button

Proteção de RouterBoot

Cuidado, risco de perder seu roteador

- Comando para ativar

/system/routerboard/settings/set protected-routerboot=enabled

- Comando para fazer a formtação completa

/system/routerboard/settings set reformat-hold-button=50 reformat-hold-button-max=60

https://help.mikrotik.com/docs/display/ROS/RouterBOARD#RouterBOARD-Protectedbootloader

MÓDULO 1.10 – Instalação e Reinstalação do RouterOS

Instalação do RouterOS

- Assim como qualquer sistema operacional o RouterOS precisa ser instalado(em routerboards já vem instalado por padrão) , as principais maneiras de instalar o ROS são:

  - Via CD (Baixar a ISO x86)
  - Via rede utilizando o Netinstall
  - Importando o disco em ambientes virtuais (CHR)

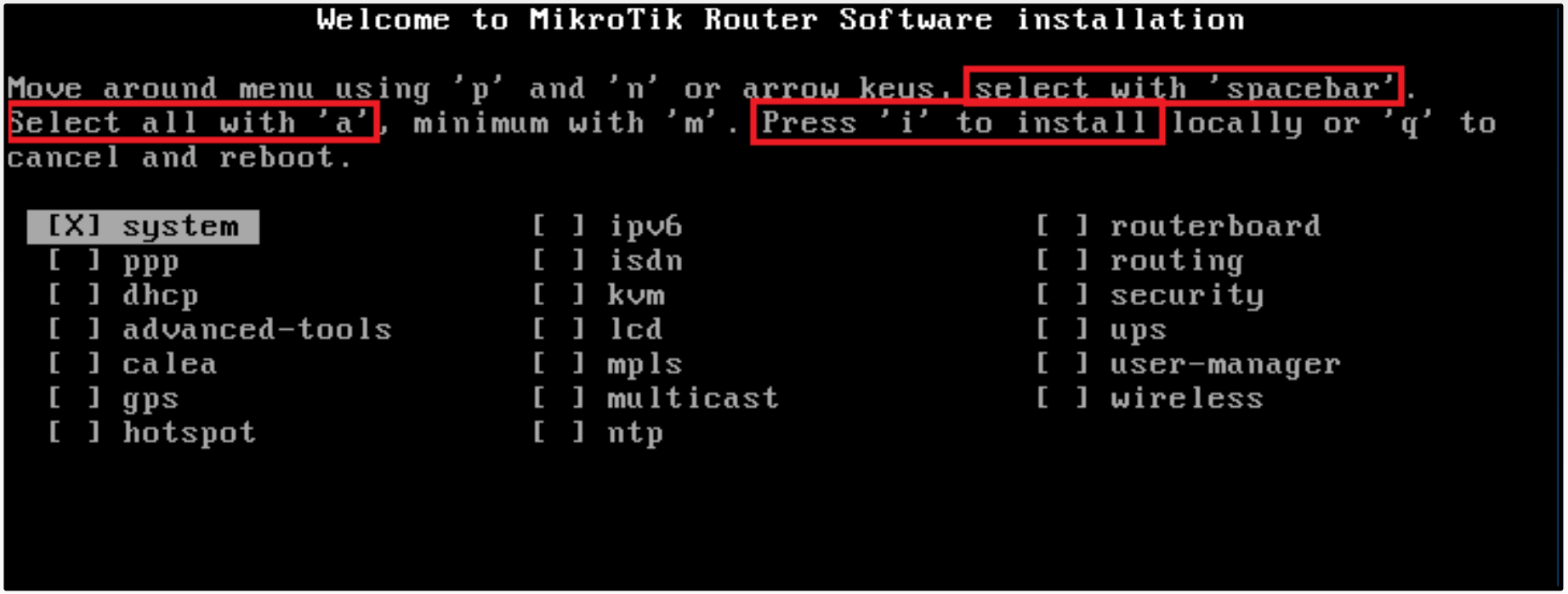
https://www.mikrotik.com/download

Oque é o CHR ?

https://help.mikrotik.com/docs/pages/viewpage.action?pageId=18350234

Instalando pela ISO

- Em caso de você estar utilizando uma maquina física grave a ISO em um CD e ajuste a sequencia de boot para CD/DVD.



Instalando via Netinstall em routerboards

- Faça download do Netinstall;
- Faça download do pacote que deseja usar;
- Configure IP estático no PC;
- Ajuste as configurações do Netinstall;
- Altere sequencia de inicialização para a RouterBoard fazer o boot via ethernet;
- Faça a formatação pelo Netinstall.

https://help.mikrotik.com/docs/display/ROS/Netinstall

Possíveis problemas com Netinstall

- O Netinstall precisa ser aberto como administrador;
- Firewall do Windows;
- Deixar mais de uma interface ativa;
- É necessário configurar gateway na configuração de rede do PC;
- Alterar configuração de rede com Netintall em execução.

MÓDULO 1.11 - Licenças

Níveis de licença

- Todo equipamento da MikroTik já vem com uma licença.
- O nível de licença padrão de cada equipamento geralmente é compatível com o nível de hardware que o equipamento possui.
- A formatação com outras ferramentas muda o software-id causa a perda da licença.
- Na tabela abaixo temos mais detalhes de como a licença fica vinculada.

Tipo de instalação	Licença vinculada a
RouterBoard	HDD, NAND
x86	MBR
CHR	MBR e UUID

https://help.mikrotik.com/docs/display/ROS/RouterOS+license+keys

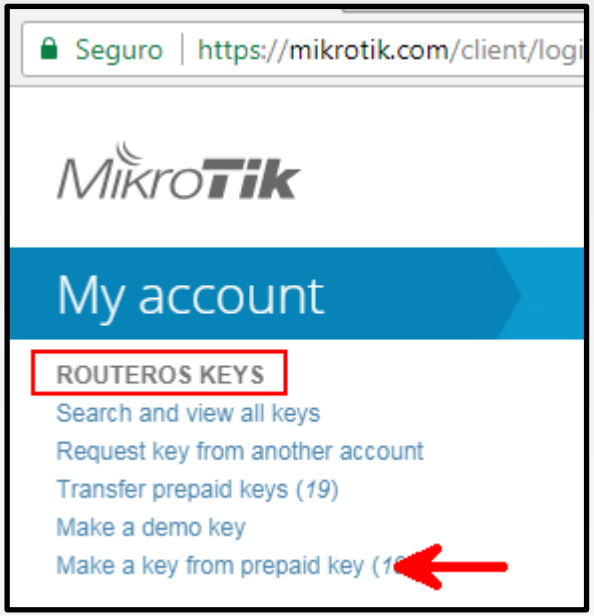
Níveis de licença para RouterBoards e x86

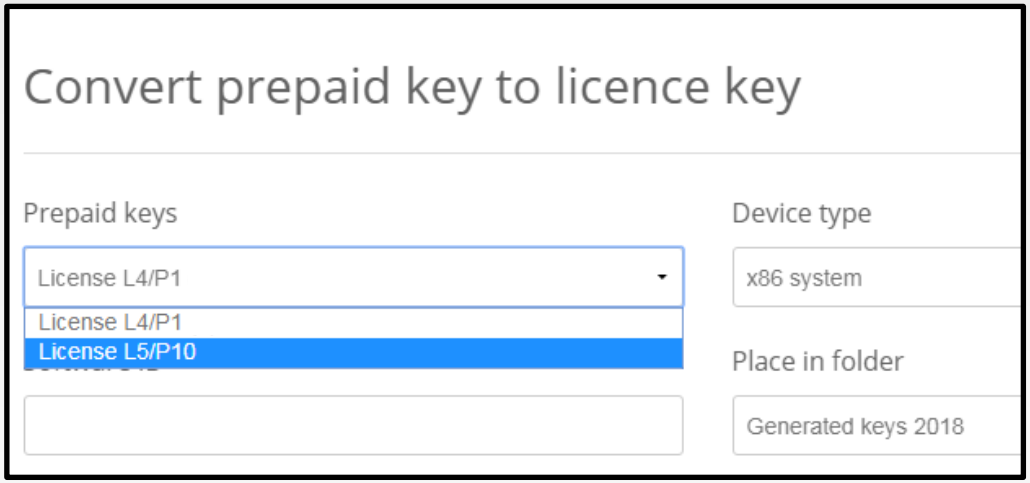
Level number	0 (Trial mode)	1 (Free Demo)	3 (WISP CPE)	4 (WISP)	5 (WISP)	6 (Controller)
Price	no key	registration required	not for sale	$45	$95	$250
Wireless AP mode (PtM)	24h trial	-	no	yes	yes	yes
PPPoE tunnels	24h trial	1	200	200	500	unlimited
PPTP tunnels	24h trial	1	200	200	500	unlimited
L2TP tunnels	24h trial	1	200	200	500	unlimited
OVPN tunnels	24h trial	1	200	200	unlimited	unlimited
EoIP tunnels	24h trial	1	unlimited	unlimited	unlimited	unlimited
VLAN interfaces	24h trial	1	unlimited	unlimited	unlimited	unlimited
Queue rules	24h trial	1	unlimited	unlimited	unlimited	unlimited
HotSpot active users	24h trial	1	1	200	500	unlimited
User manager active sessions	24h trial	1	10	20	50	Unlimited

Níveis de licença para o CHR

Licença	Limite de velocidade	Preço
Free	1Mbit	FREE
P1	1Gbit	$45
P10	10Gbit	$95
P-Unlimited	Unlimited	$250

Correspondência de licenças





Preço	RouterBoard e x86	CHR
$45	Level 4	P1
$95	Level 5	P10
$250	Level 6	P-Unlimited

MÓDULO 1.12 – Fontes de Informações

Fontes de informações MikroTik

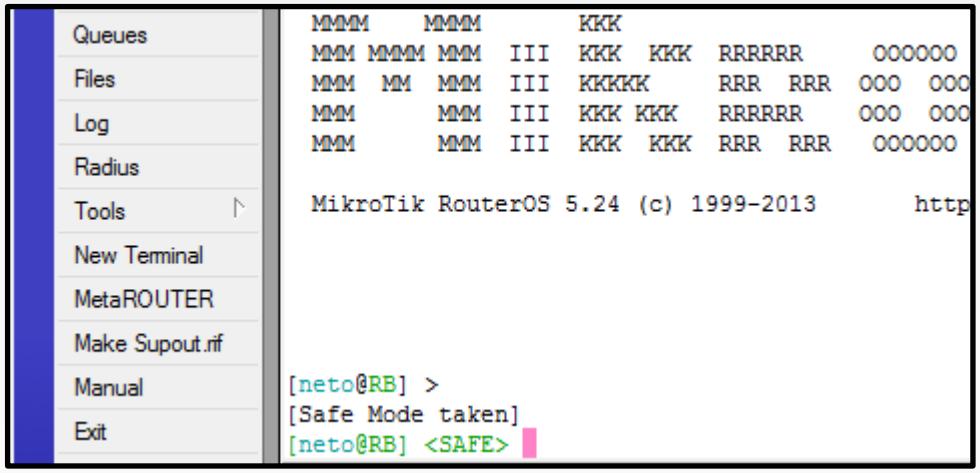
- Ticket – https://help.mikrotik.com/servicedesk/servicedesk/customer/user/login?destination=portals
- Fórum – https://forum.mikrotik.com
- Wiki Antiga – https://wiki.mikrotik.com
- Wiki Nova – https://help.mikrotik.com/docs/
- MUM – https://mum.mikrotik.com
- Distribuidores – https://mikrotik.com/buy
- Consultores – https://mikrotik.com/consultants

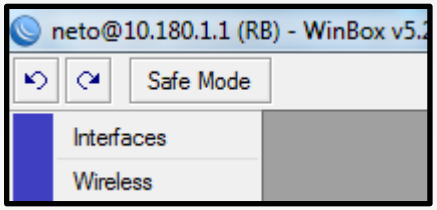
- E-mail de suporte – support@mikrotik.com
- Arquivo de Supout.rif

MÓDULO 1.13 - Modo Seguro

Modo seguro

- O MikroTik permite o acesso ao sistema através do “modo seguro”. Este modo permite desfazer as configurações modificadas caso a sessão seja perdida de forma automática. Para habilitar o modo seguro pressione “CTRL+X” ou na parte superior clique em Safe Mode.





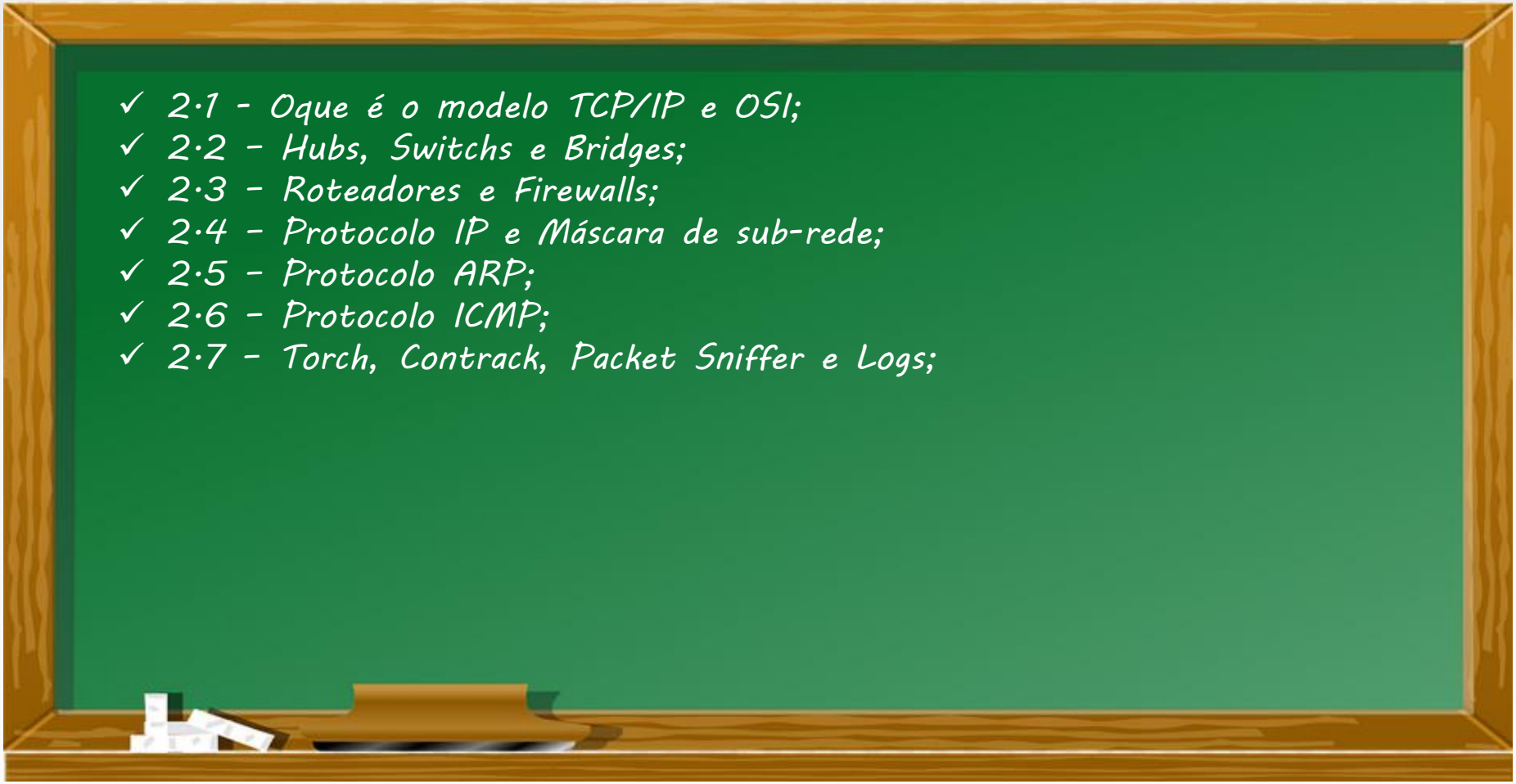
Modo seguro

- Se um usuário entra em modo seguro, quando já há um nesse modo, a seguinte mensagem será dada: "Hijacking Safe Mode from someone – unroll/release/
  - u: desfaz todas as configurações anteriores feitas em modo seguro e põe a presente sessão em modo seguro
  - d: deixa tudo como está
  - r: mantém as configurações no modo seguro e põe a sessão em modo seguro. O outro usuário receberá a seguinte mensagem:

"Safe Mode Released by another user"

MÓDULO 2 – Revisão de Redes

MÓDULO 2 - Revisão de Redes



MÓDULO 2.1 - Oque é o modelo TCP/IP e OSI;

Um pouco de historia

- 1962 – Primeiras comunicações em rede.
- 1965 – Primeira comunicação WAN.
- 1969 – Desenvolvido o TCP.
- 1978 – Vários padrões de comunicação.
- 1981 – Inicio de discussões sobre padronizações.
- 1984 – Chegada do modelo OSI

Siglas
ISO - International Organization for Standardization
OSI - Open Systems Interconnection

Modelos de comunicação

https://www.redesbrasil.com/modelo-tcp-ip-4-ou-5-camadasp/

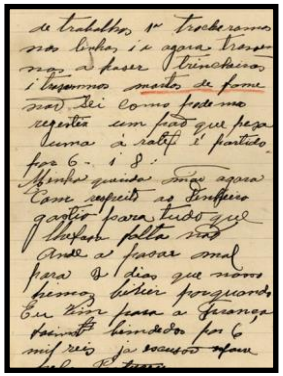
Pacotes de dados

- Existem várias tecnologias e protocolos para transmissão de dados entre 2 dispositivos;
- Quando se fala de internet a maior parte dos dados são transmitidos via IP;
- Os dados quebrados em pequenos pedaços e por fim transmitidos através de pacotes.

Carta vs Pacote

Redes Brasil

Carta



Remetente
Nome: Francisco Neto

End: Goiânia/GO,
Rua 10, N°501

Destinatário
Nome: João da Silva

End: Fortaleza/CE,
Rua 20, N°456

Pacote

Origem

Porta: 6423
IP: 10.10.254.1
MAC: 50:9E:00:01:00:07

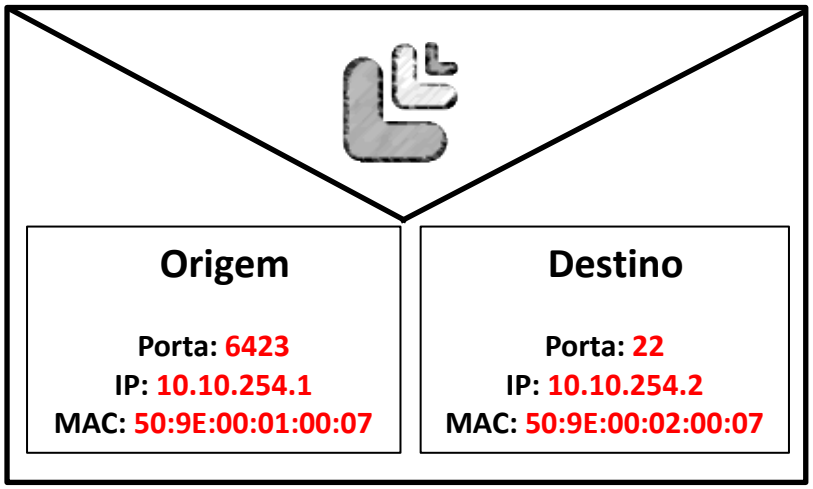
Destino

Porta: 22
IP: 10.10.254.2
MAC: 50:9E:00:02:00:07

Português vs Inglês

Redes Brasil

Pacote



Dst. MAC Address

Src. Address:

Protocol:

Src. Port:

Dst. Address:

Dst. Port:

Src. MAC Address:

Português vs Inglês

Redes Brasil

Pacote

Origem	Destino
Porta: 6423 IP: 10.10.254.1 MAC: 50:9E:00:01:00:07	Porta: 22 IP: 10.10.254.2 MAC: 50:9E:00:02:00:07

Packet

Source (SRC)	Destination (DST)
Port: 6423 Address: 10.10.254.1 MAC: 50:9E:00:01:00:07	Port: 22 Address: 10.10.254.2 MAC: 50:9E:00:02:00:07

Transporte de dados

- Quais são as principais informações usadas para transporte de dados?

	Origem = Source = SRC	Destino = Destination = DST
4	**Port**	**Port**
3	**IP / Address**	**IP / Address**
2	**MAC**	**MAC**

Um pouco mais sobre o modelo OSI

Os dados são gerados por aplicativos e repassados para camada de aplicação, e a partir de então serão **encapsulados** camada por camada até chegar a camada física onde serão transformados em sinais (elétricos ,luminosos etc...)

Dados

Aplicação

Transporte

Rede

Enlace

Física

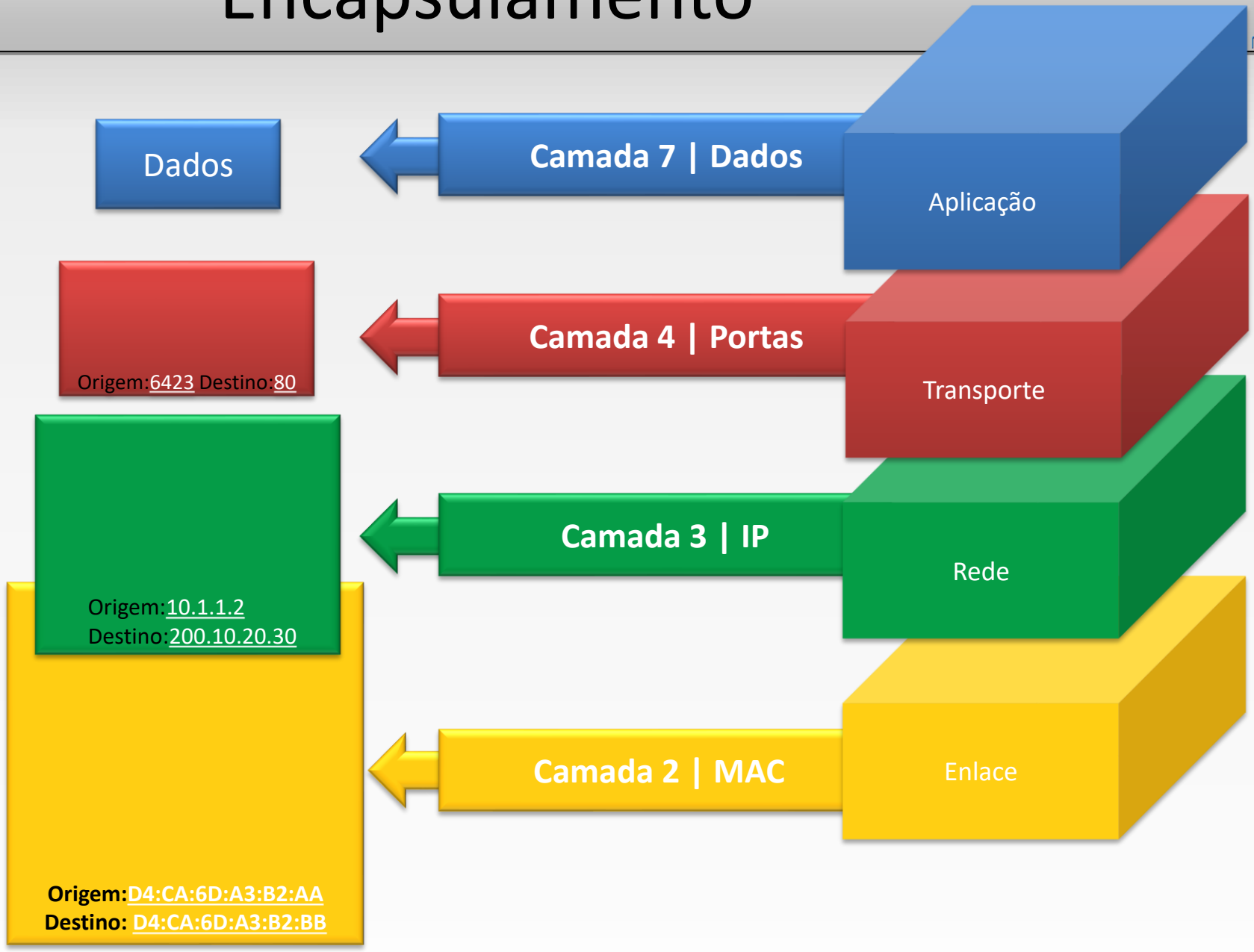
Cabeçalho possui porta (TCP/UDP) de origem e destino

Cabeçalho possui IP de origem e destino

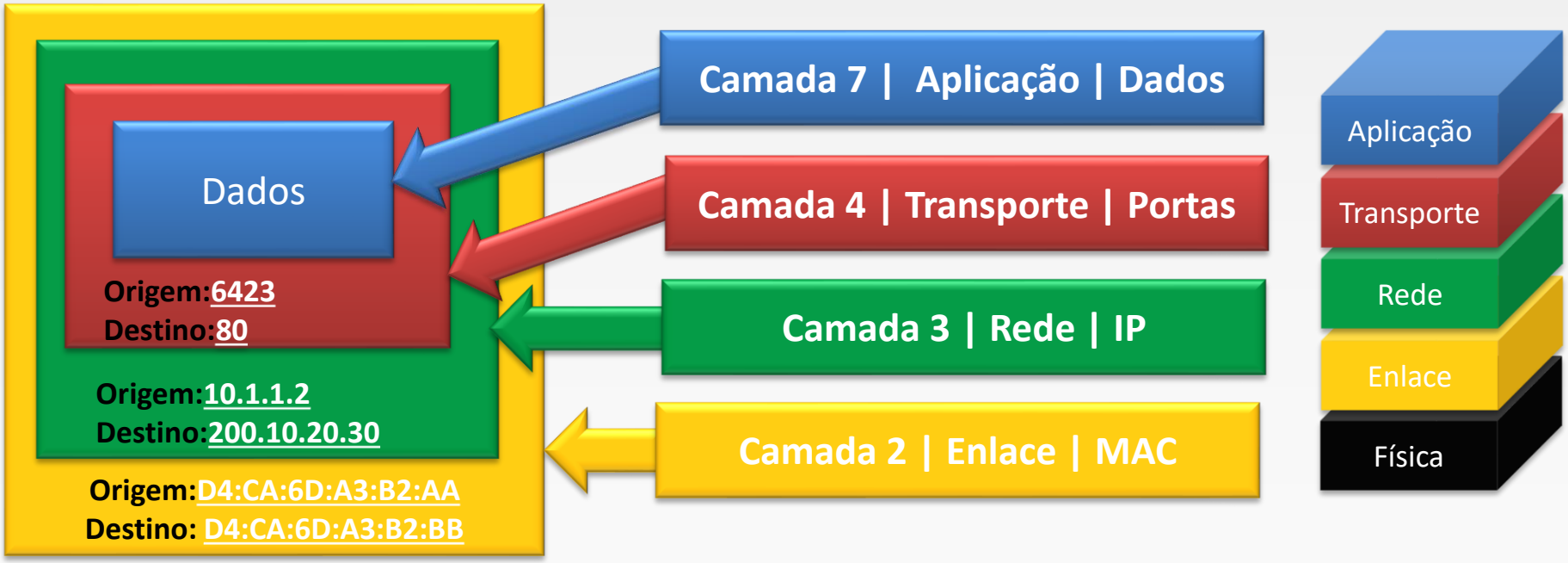
Cabeçalho possui MAC de origem e destino

0110110010100100001

Encapsulamento



Encapsulamento

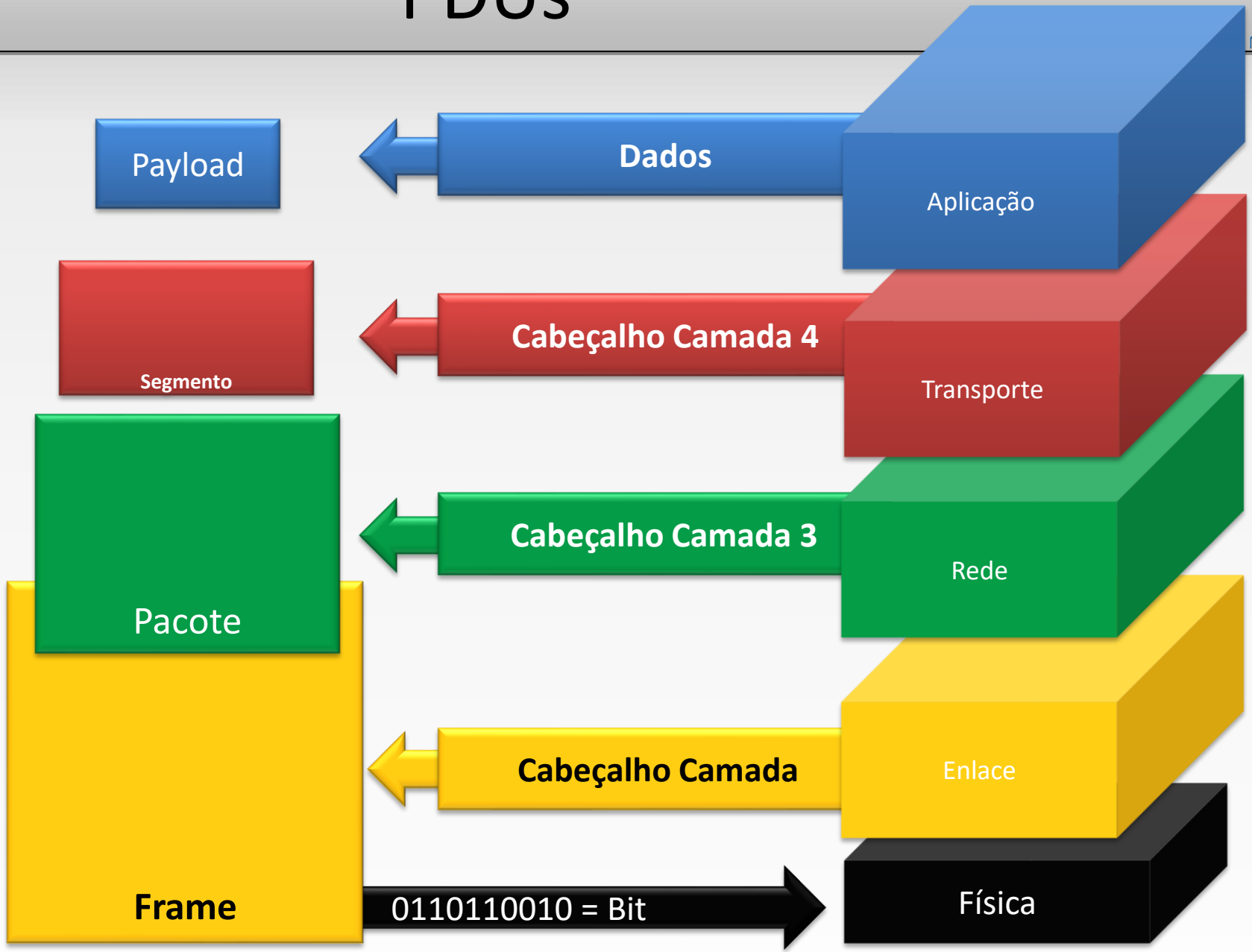


PDU - Protocol data unit

- **Protocol data unit** ou em português **Unidade de dados de protocolo** em telecomunicações descreve um bloco de dados que é transmitido entre duas instâncias da mesma camada.

Camada	PDU
4 - Camada de transporte	Segmento
3 - Camada de rede	Pacote
2 - Camada de enlace	Frame (quadro)
1 - Camada física	Bit

PDUs


Payload
Dados
Aplicação
Segmento
Cabeçalho Camada 4
Transporte
Pacote
Cabeçalho Camada 3
Rede
Cabeçalho Camada
Enlace
Frame
0110110010 = Bit
Física

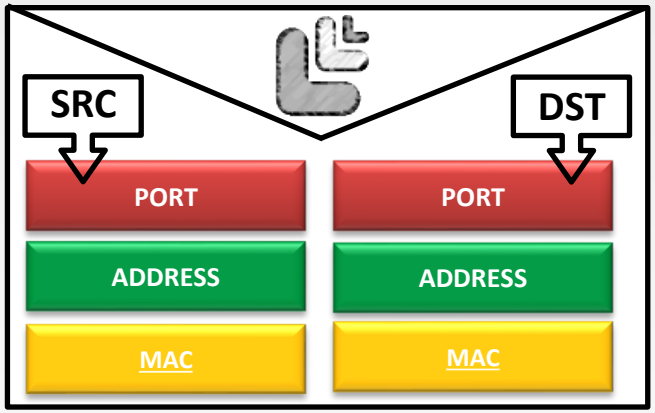
MÓDULO 2.2 – Hubs, Switchs e Bridges;

1 - Camada física

- A camada física fornece os requisitos para transportar pelo meio físico os bits que formam o frame da camada 2.

- O objetivo da camada física é criar o sinal elétrico, óptico ou eletromagnético que representa os bits em cada frame.

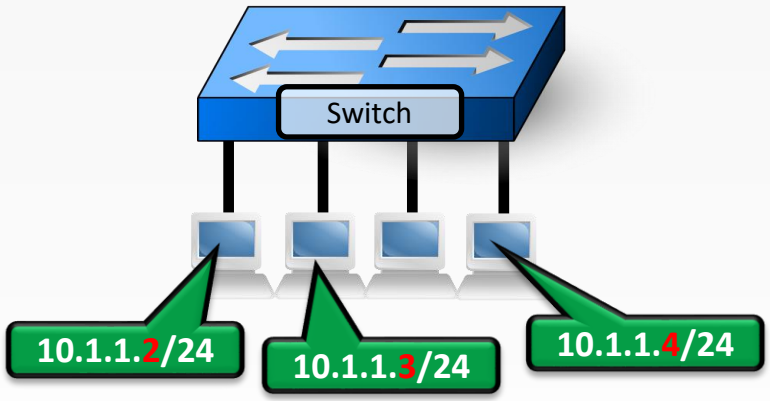
O Hub



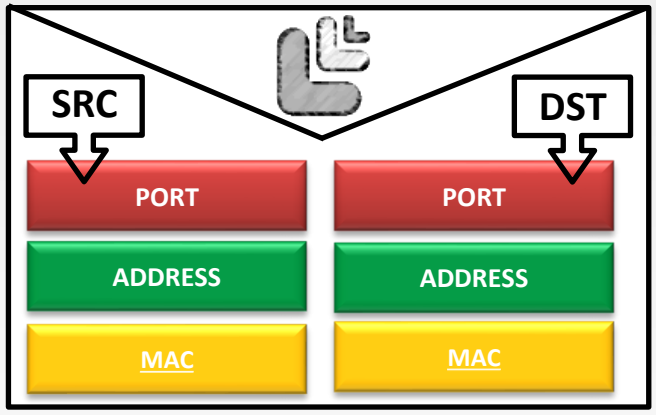
Só consegue entender bits

2 - Camada de enlace

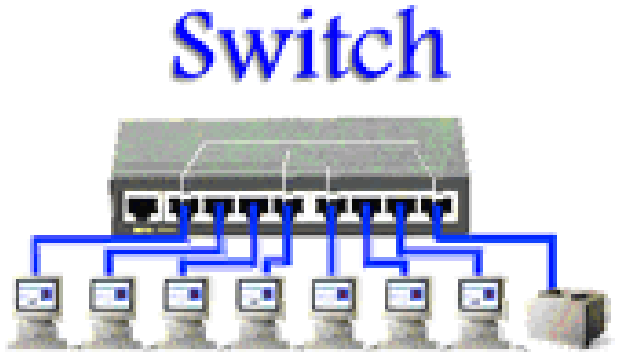
- Camada responsável pelo endereçamento físico, controle de acesso ao meio e correções de erros da camada 1.
- Endereçamento físico se faz pelos endereços MAC (Controle de Acesso ao Meio) que são únicos no mundo e que são atribuídos as interfaces dos dispositivos de rede.
- Exemplos de MAC Address: 50:9E:00:01:00:01 – 11:22:33:44:55:66 – AA:BB:CC:DD:EE:FF
- Switchs, bridges trabalham em camada 2 e **NÃO** separam domínios de broadcast.
- PPPoE, DHCP, ARP e outros protocolos se propagam pelo domínio de broadcast.



O Switch



Toma decisões baseadas no endereço MAC



Bridge

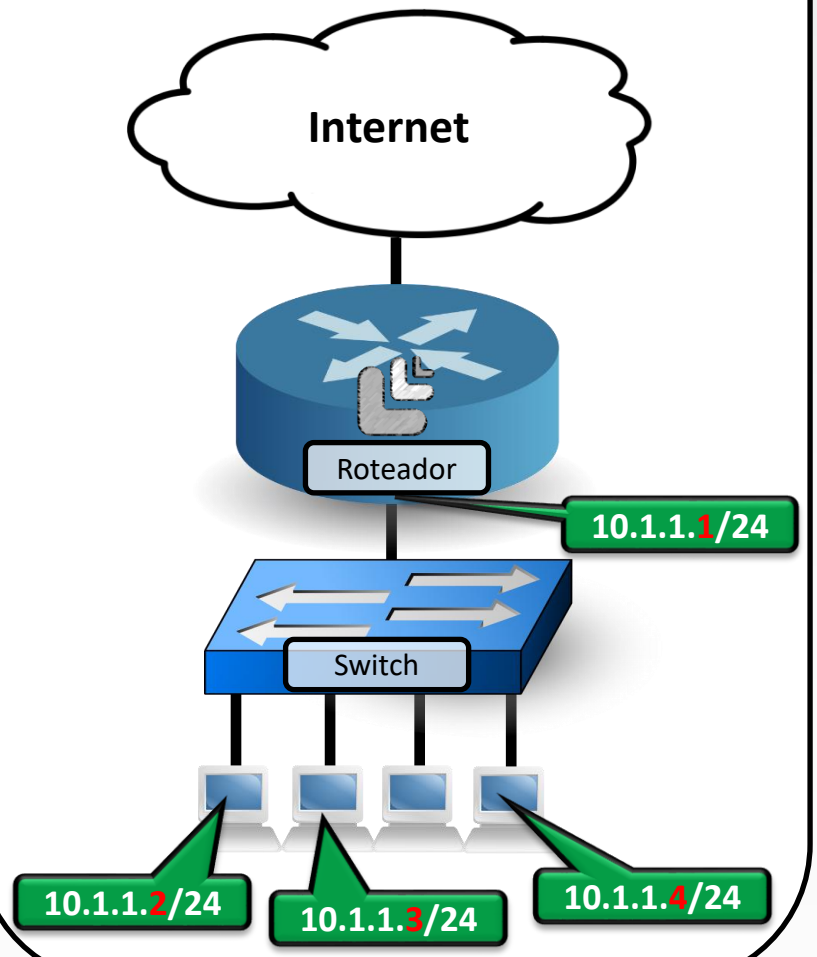
Bridge | Ports | Port Extensions | VLANs | MSTIs | Port MST Overrides | Filters | NAT | Hosts

	MAC Address	On Interface
DE	FE:49:43:68:5B:E8	ether8-proxmox-...
DL	E6:CC:A1:2A:18:07	loopback
DE	DC:2C:6E:3C:2A:18	ether5-link_oi
DL	CA:FD:AE:36:DC:D5	bridge-servidores
DE	BA:72:D7:E7:F6:2F	ether8-proxmox-...
DE	B6:79:0D:CF:B6:64	ether8-proxmox-...
DE	B6:79:0D:CF:B6:03	ether8-proxmox-...
DL	B2:F6:3B:C5:33:36	bridge-link_oi
DE	7E:F5:12:B7:A9:6E	ether8-proxmox-...
DE	7C:D9:A0:02:83:2E	ether5-link_oi

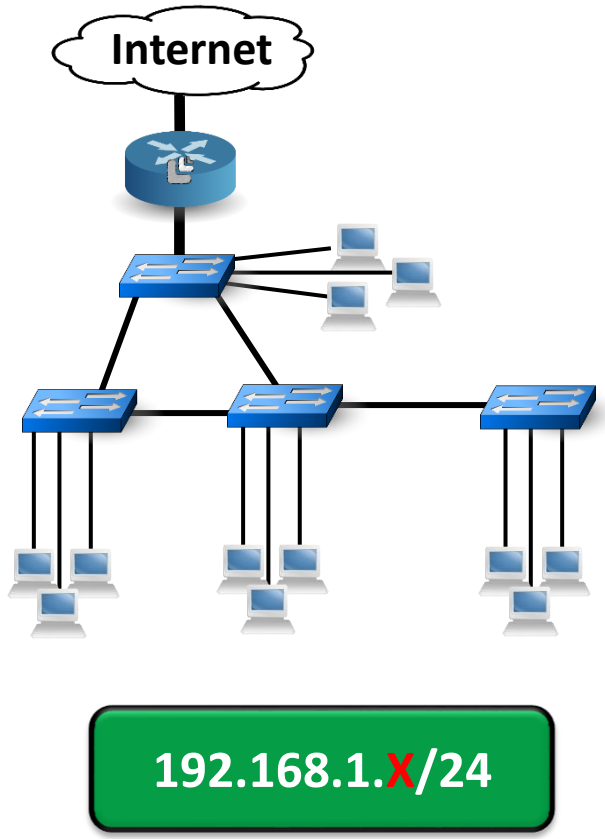
Cenários onde se aplicam switches

Redes Brasil

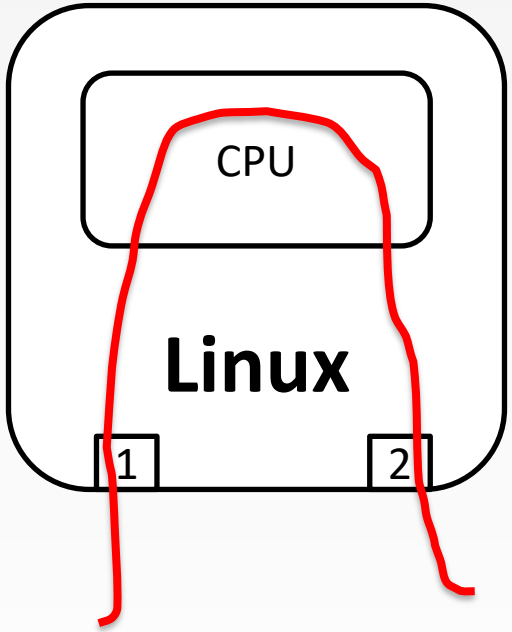
Cenário 1



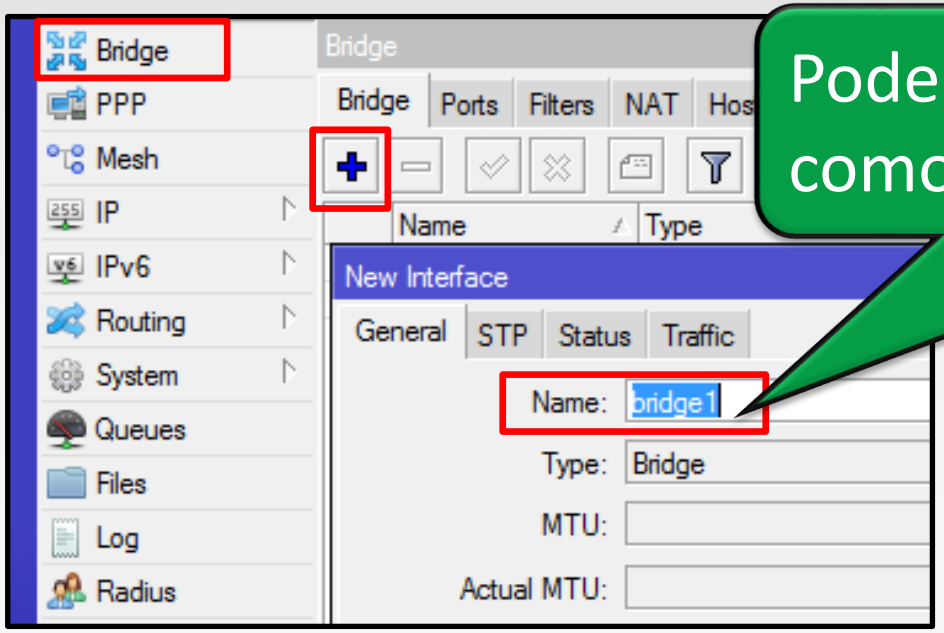
Cenário 2



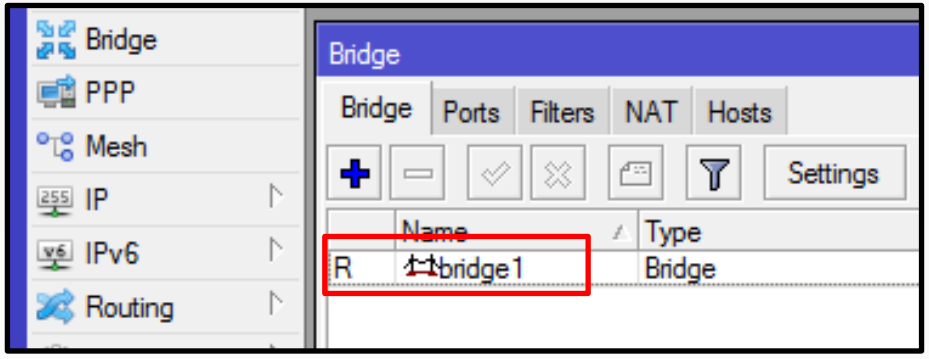
Oque é uma Bridge ?



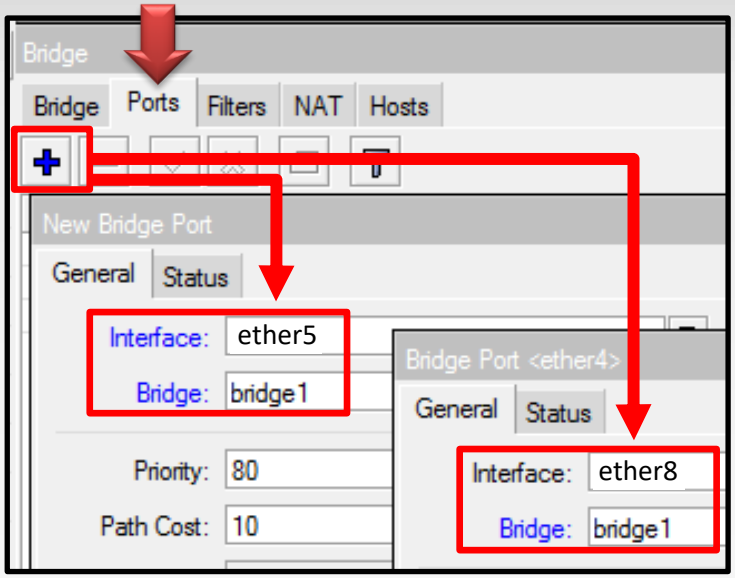
Criando uma bridge



Podemos resumir uma bridge como um switch virtual.



Adicionando interfaces na bridge

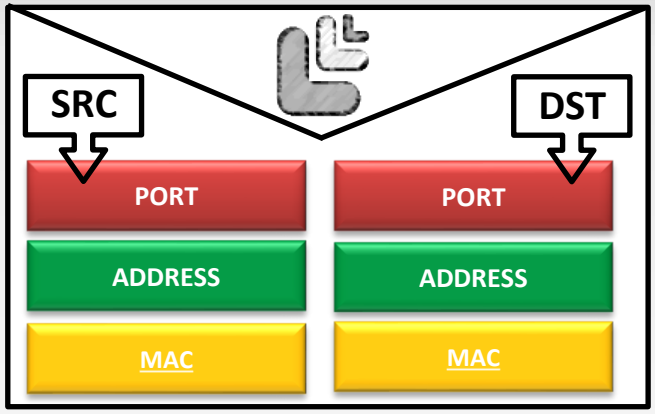


MÓDULO 2.3 – Roteadores e Firewalls

3 - Camada de rede

- Responsável pelo endereçamento lógico dos pacotes;
- Roteadores trabalham em camada 3 e separam domínios de broadcast;
- Determinam que rota os pacotes irão seguir para atingir o destino;
- PPPoE, DHCP, ARP e outros protocolos **NÃO** através de roteadores.

O Roteador



Toma decisões baseadas no endereço de IP

Route List

Active | is | yes

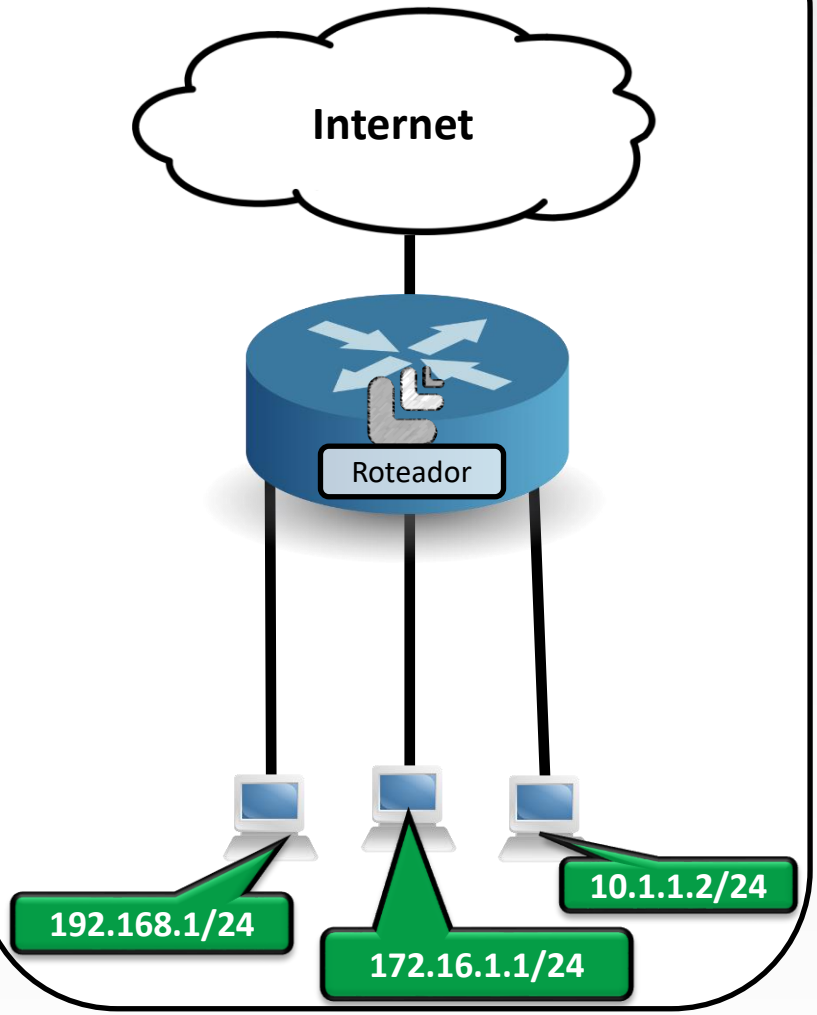
Routing Table | contains | main

	Dst. Address	Gateway	Distance
AS	0.0.0.0/0	pppoe-link-topnet	1
DAo	10.0.0.0/9	172.16.100.1%ether3-ptp-smart_layer	110
DAo	10.7.7.0/24	172.16.100.1%ether3-ptp-smart_layer	110
DAC	10.7.8.0/24	bridge-servidores	0
DAo	10.7.9.0/24	172.16.100.1%ether3-ptp-smart_layer	110
DAo	10.7.10.0/24	172.16.100.1%ether3-ptp-smart_layer	110
DAC	10.7.101.0/24	vlan101-lab1-comunidade	0
DAC	10.7.102.0/24	vlan102-lab2-comunidade	0
DAC	10.7.103.0/24	vlan103-lab3-comunidade	0
DAC	10.8.8.0/24	bridge-rede-local	0

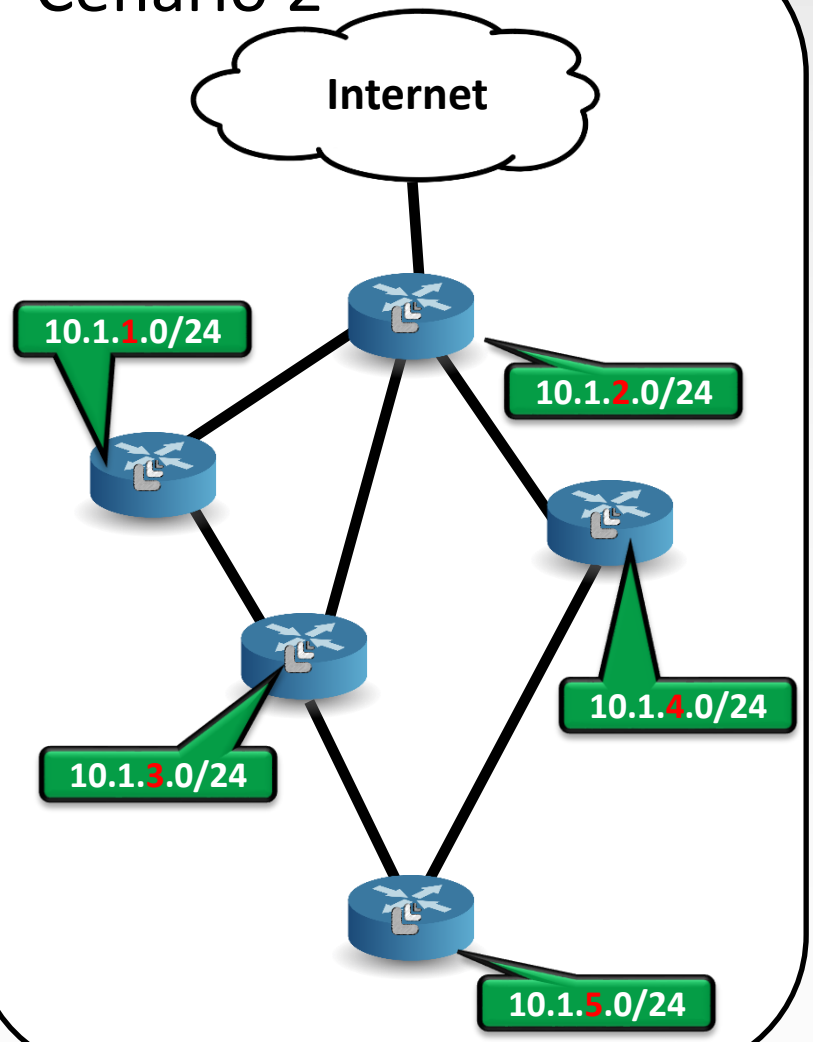
Cenários onde se aplicam roteadores

Redes Brasil

Cenário 1



Cenário 2



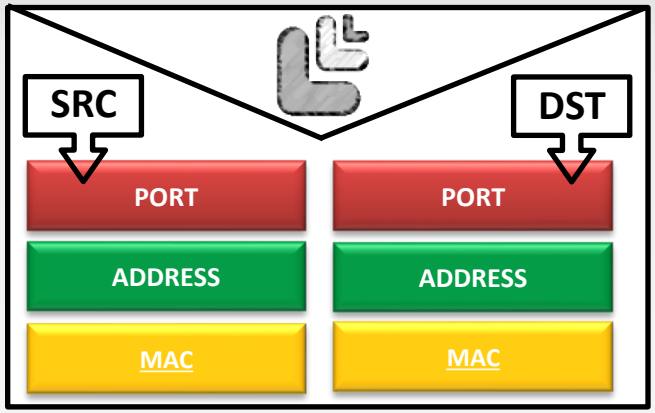
4 - Camada de transporte

- No host de origem essa camada é responsável por pegar os dados das camadas superiores e dividir em pacotes para que sejam transmitidos.

- No host de destino, pega os pacotes recebidos da camada de rede, remonta os dados originais e os envia para a camada superior.

- Alguns protocolos da camada 4 são: TCP, UDP, RTP

O Firewall



Toma decisões baseadas informações de várias camadas incluindo a camada 4

Firewall

Filter Rules | NAT | Mangle | Raw | Service Ports | Connections | Address Lists | Layer7 Protocols

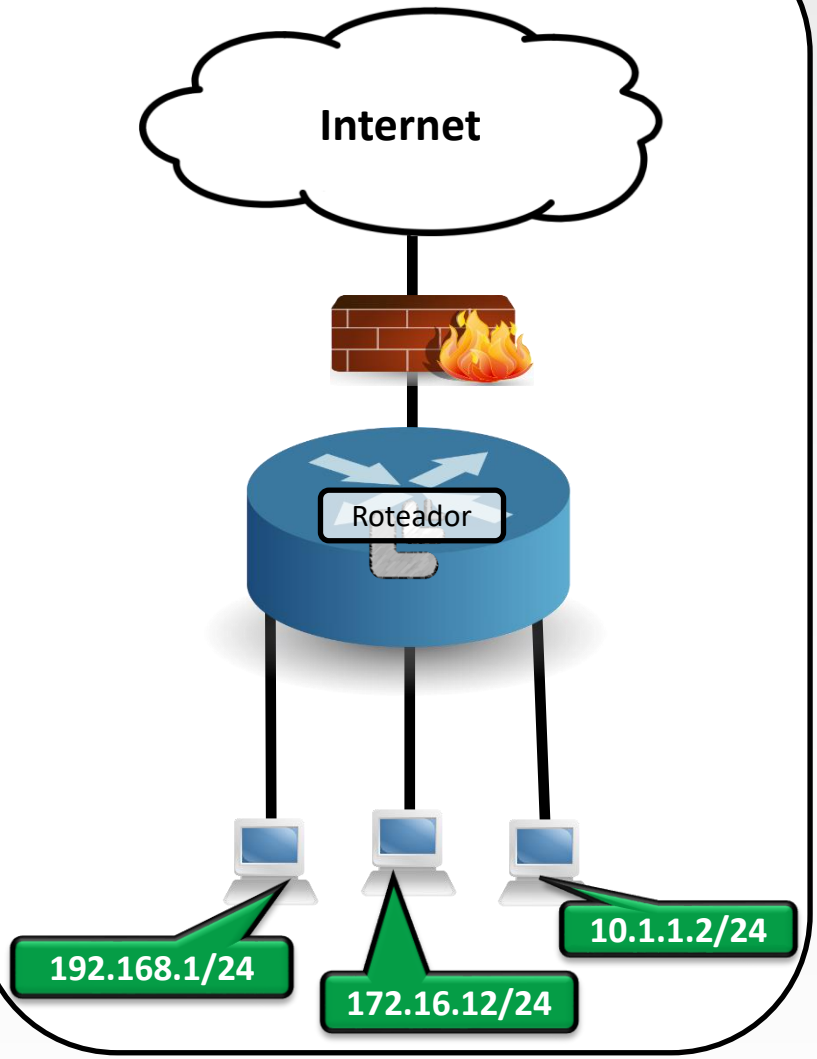
Reset Counters | Reset All Counters | Find

#	Action	Chain	Src. Ad...	Dst. Addre...	Proto...	Dst. Port	In. Interf...	Out. In...	Packets	Comment
0	acc...	input							10 193	ACEITA CONEXOES ESTABELECIDAS ...
1	acc...	input							355	ACEITA LISTA REDE-SUPORTE
2	acc...	input			1 (ic...				159	ACEITA PACOTES ICMP
3	drop	input			1 (ic...				0	DROP ICMP
4	acc...	input			17 (u...	1701,450...			1	ACEITA L2TP
5	acc...	input			6 (tcp)	63780			0	ACEITA SSTP
6	add ...	input			6 (tcp)	1224			0	PEGA IP PARA LISTA PRE-REDE-SUPO...
7	add ...	input			6 (tcp)	2412			0	PEGA IP PARA LISTA REDE-SUPORTE
8	acc...	input			17 (u...	53			0	ACEITA DNS PARA REDE LOCAL
9	acc...	input			89 (o...				0	ACEITA OSPF
10	drop	input							1 427	DROP GERAL
11	acc...	forward							16 939	ACEITA TUDO DA REDE DE SUPORTE
12	drop	forward		45.70.147....	6 (tcp)	22			13	DROP ACESSO A PORTA 22 DOS SER...
13	drop	forward		45.70.147....	6 (tcp)	80			2	DROPA ACESSO A PORTA 80 DO SER...

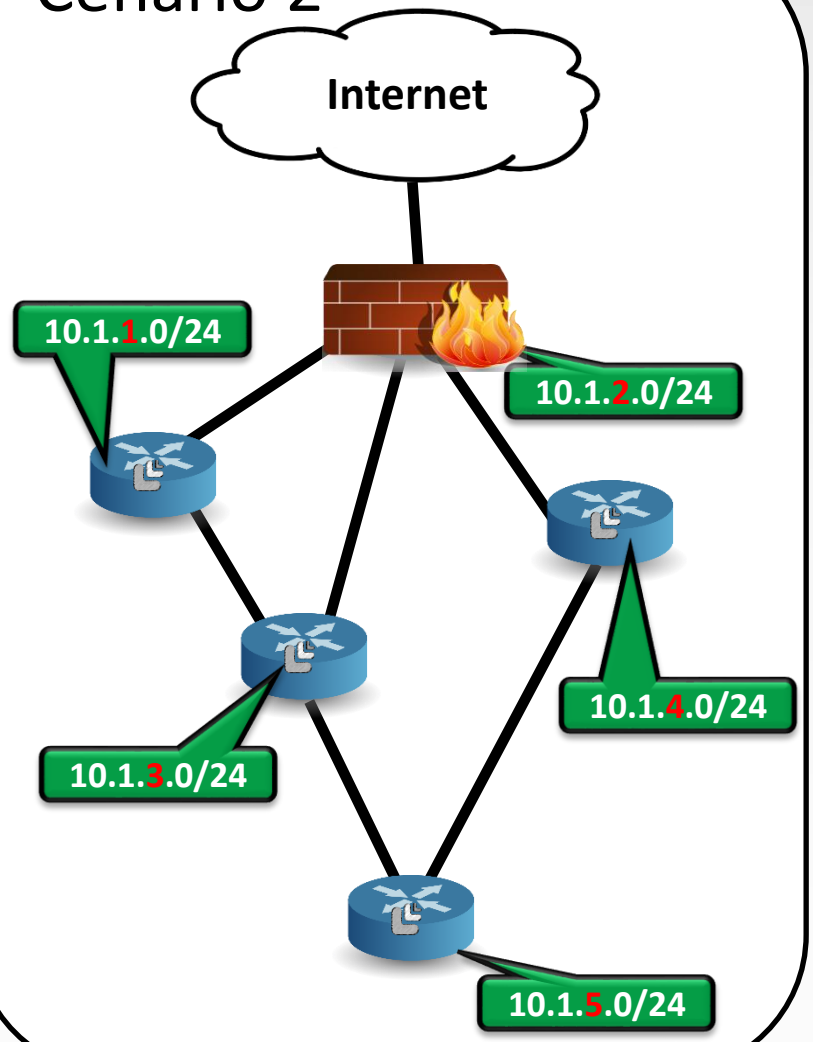
Cenários onde se aplicam firewalls

Redes Brasil

Cenário 1



Cenário 2



7 - Camada de aplicação

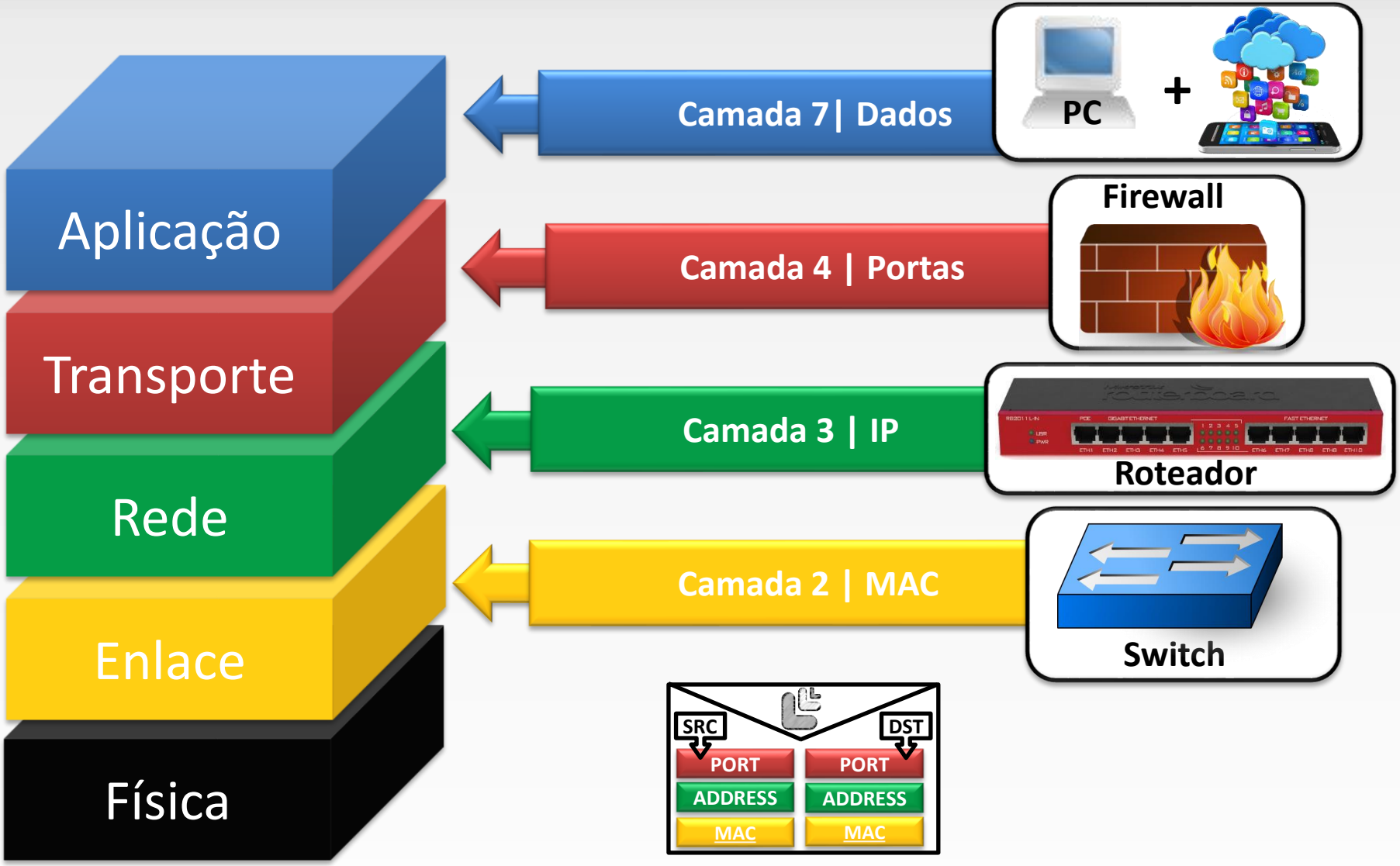
- Muitos confundem aplicação com aplicativo.
- Usuário interagem com o aplicativo e o aplicativo interage com protocolos da camada de aplicação(HTTP, SMTP, FTP, SSH, Telnet ...).

Aplicativos

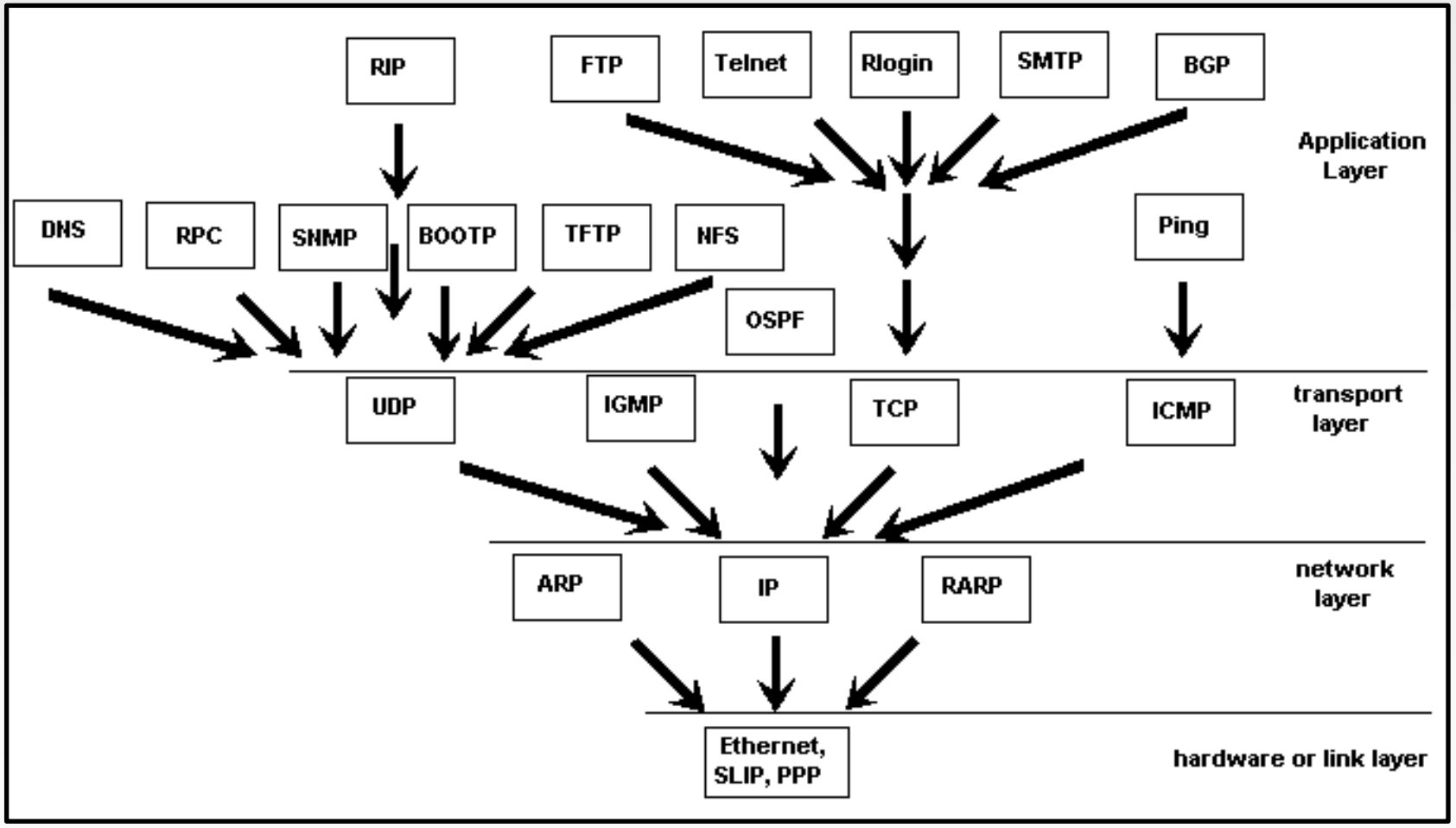
Protocolos da camada de aplicação

HTTP
HTTPS
DNS
SMTP

O datagrama


Aplicação
Transporte
Rede
Enlace
Física
Camada 7| Dados
PC
+
Camada 4 | Portas
Firewall
Camada 3 | IP
Roteador
Camada 2 | MAC
Switch
SRC
DST
PORT
PORT
ADDRESS
ADDRESS
MAC
MAC

Protocolos


RIP
FTP
Telnet
Rlogin
SMTP
BGP
Application Layer
DNS
RPC
SNMP
BOOTP
TFTP
NFS
Ping
OSPF
UDP
IGMP
TCP
ICMP
transport layer
ARP
IP
RARP
network layer
Ethernet, SLIP, PPP
hardware or link layer

MÓDULO 2.4 - Protocolo IP e Máscara de sub-rede;

Endereço IP

- É o endereço lógico de um dispositivo de rede;
- Atualmente possui duas versão, IPv4 e IPv6;
- A principal diferença entre eles é quantidade de IPs disponíveis;
  - IPv4 (32 bits) = 4 Bilhões de IPs
  - IPv6 (128 bits) = 340 Undecilhões de IPs

IPv4

- Endereço IPv4 é um numero de 32 bits divido em 4 partes (4 octetos) separados por pontos.

- Exemplos de endereço IP:
  - 200.200.0.1
  - 10.0.0.5
  - 192.168.50.188

10.1.1.256 – Atenção isso não é um IP válido

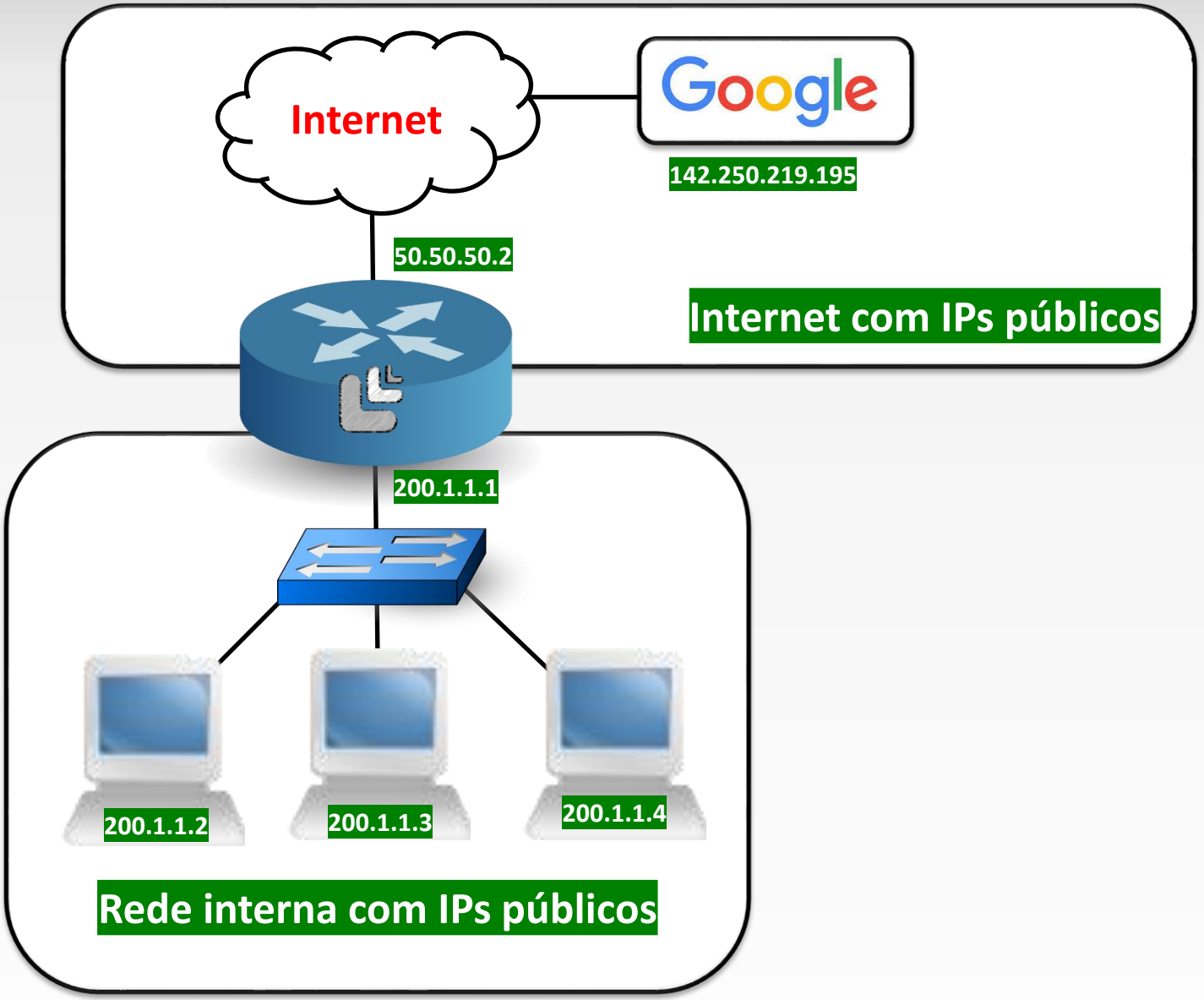
IPs públicos pra todo mundo !!!

- A internet foi pensada para que qualquer dispositivo pudesse se comunicar com outro dispositivo sem nenhum tipo de tradução ou alteração no pacote.

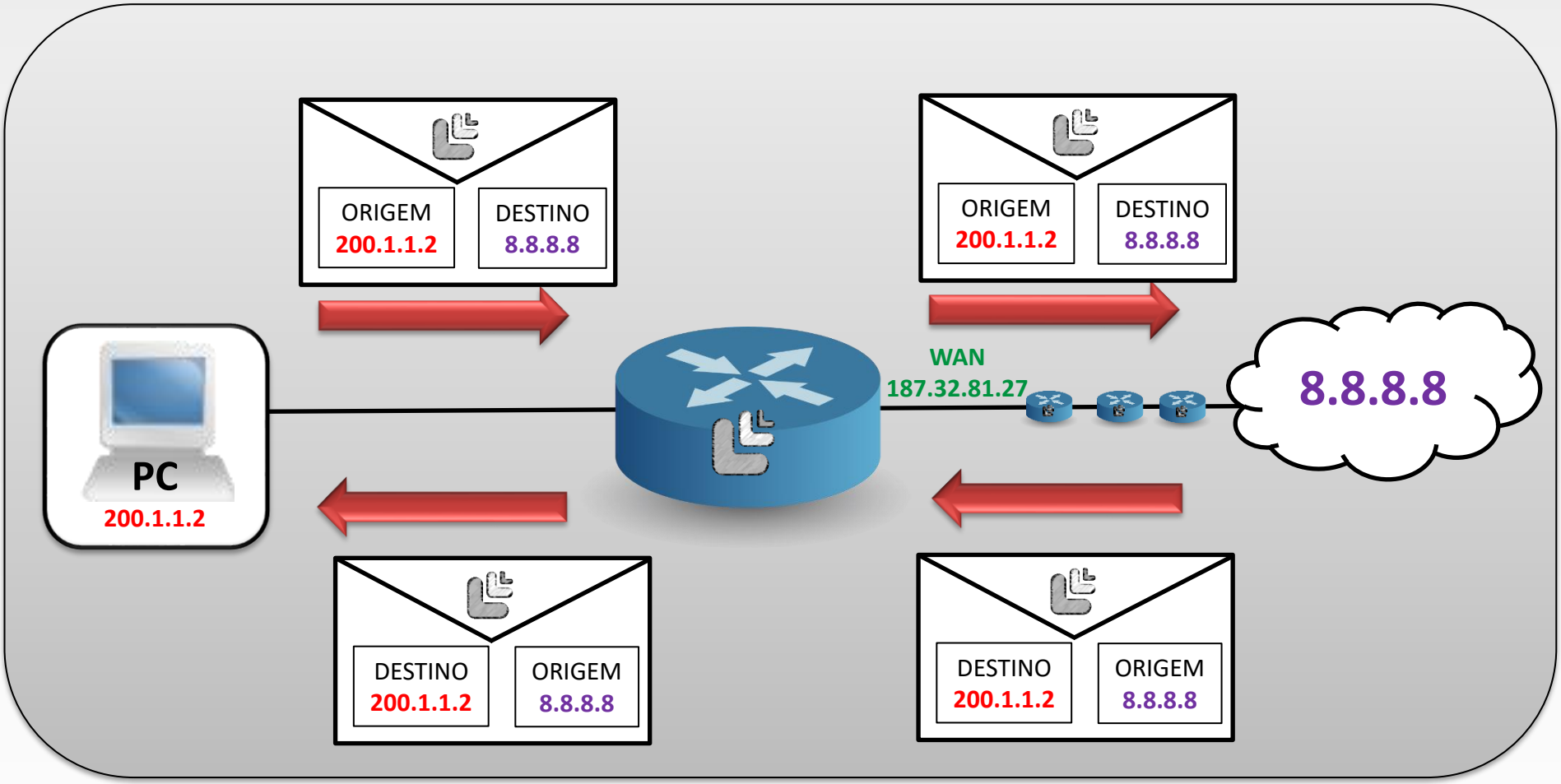
- Não existiam IPs privados;

- Todos os dispositivos recebiam IPs públicos.

Dispositivos com IPs públicos



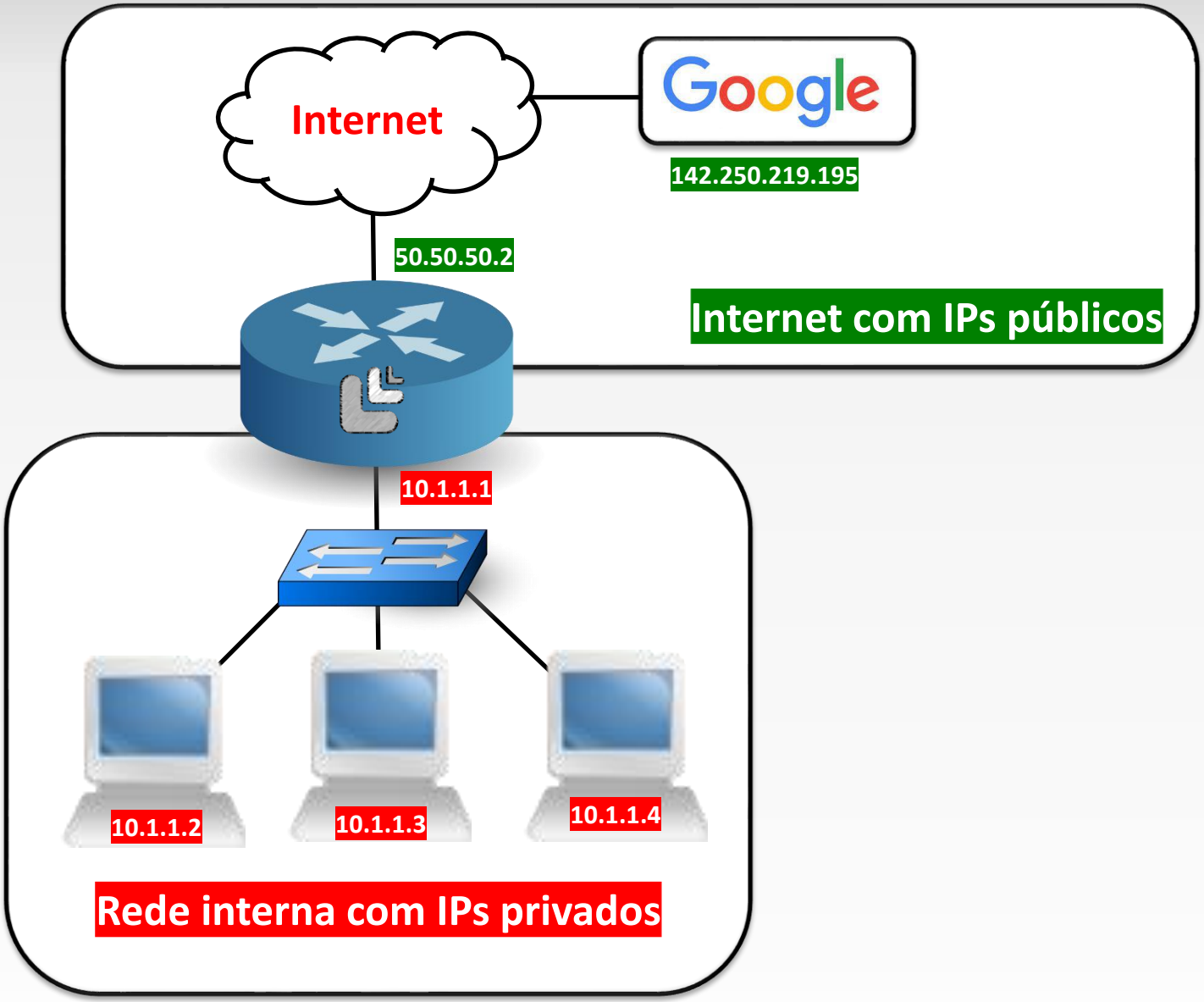
Rede LAN com IPs públicos



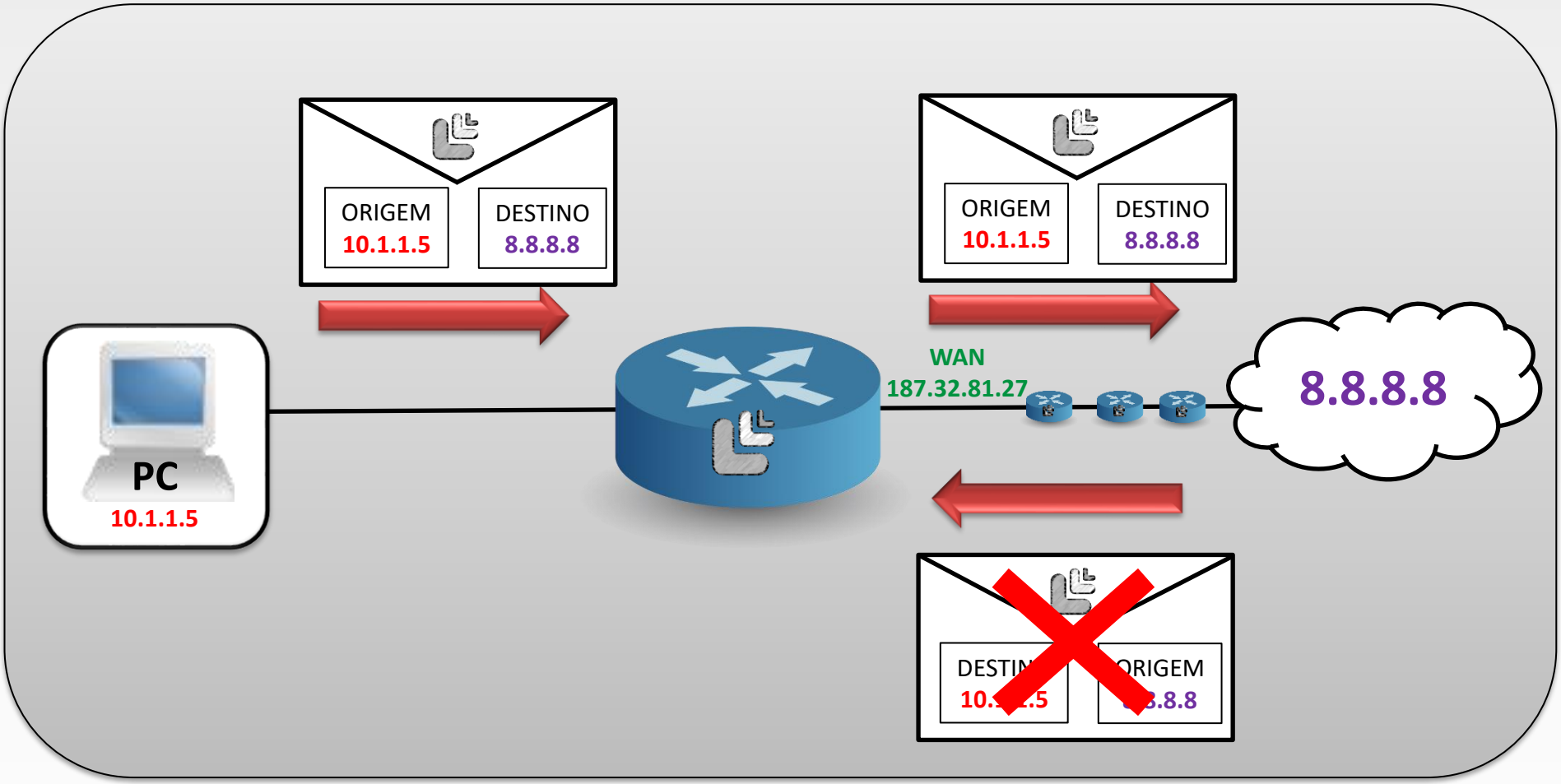
NAT e IPs privados

- Na década 90 perceberam que o IPv4 não iria comportar todo o crescimento da internet;
- O NAT foi criado como técnica paliativa para resolver o problema do escassez do IPv4;
- Foi definido na RFC 3022;
- Os prefixos abaixo foram definidos na RFC 1918 e são normalmente usados em redes que fazem uso de NAT;
  - 10.0.0.0/8
  - 192.168.0.0/16
  - 172.16.0.0/12
- O usuário final que antes recebia um bloco de IPs públicos passa a receber somente 1 IP público.

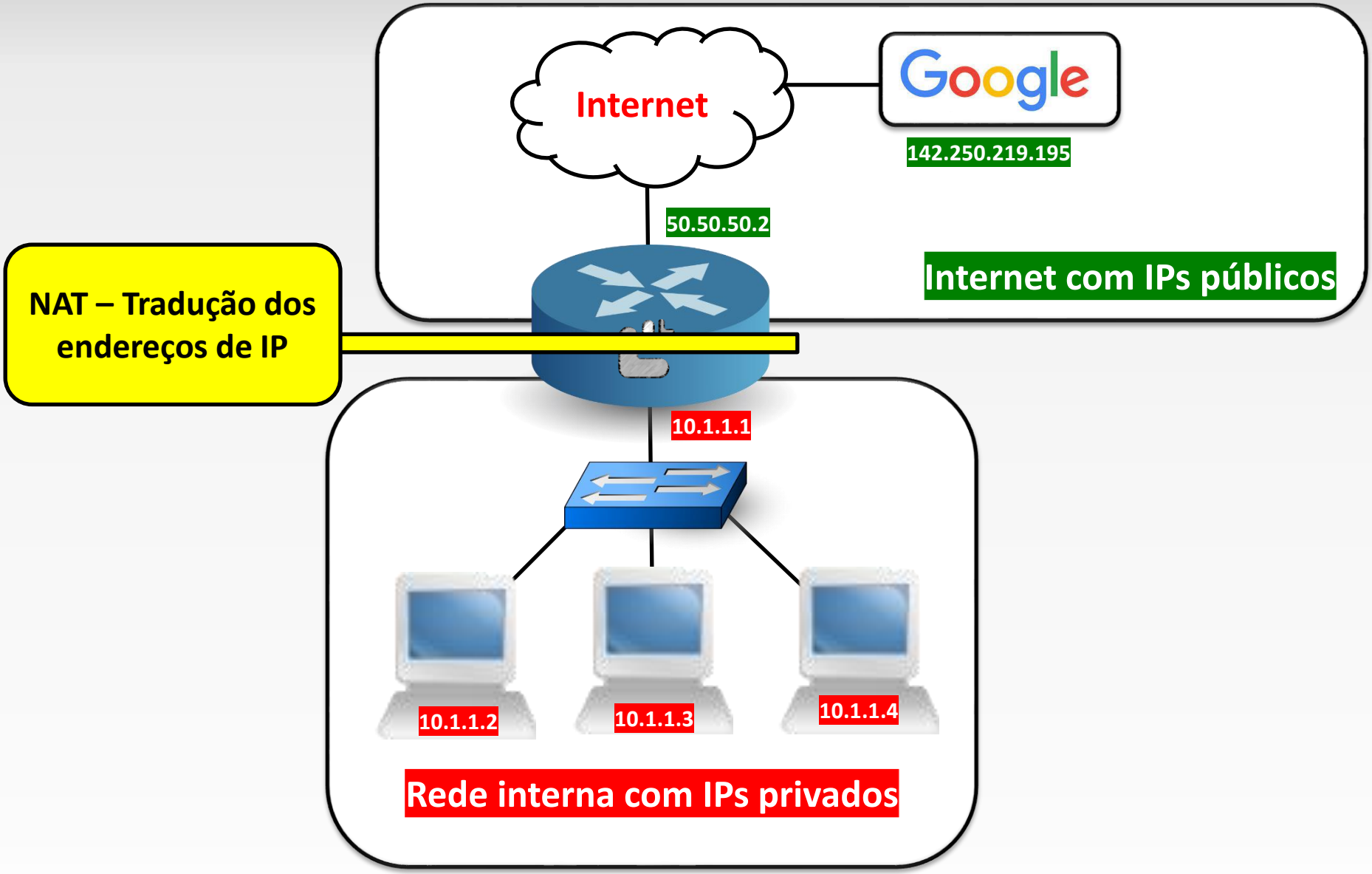
IPs privados



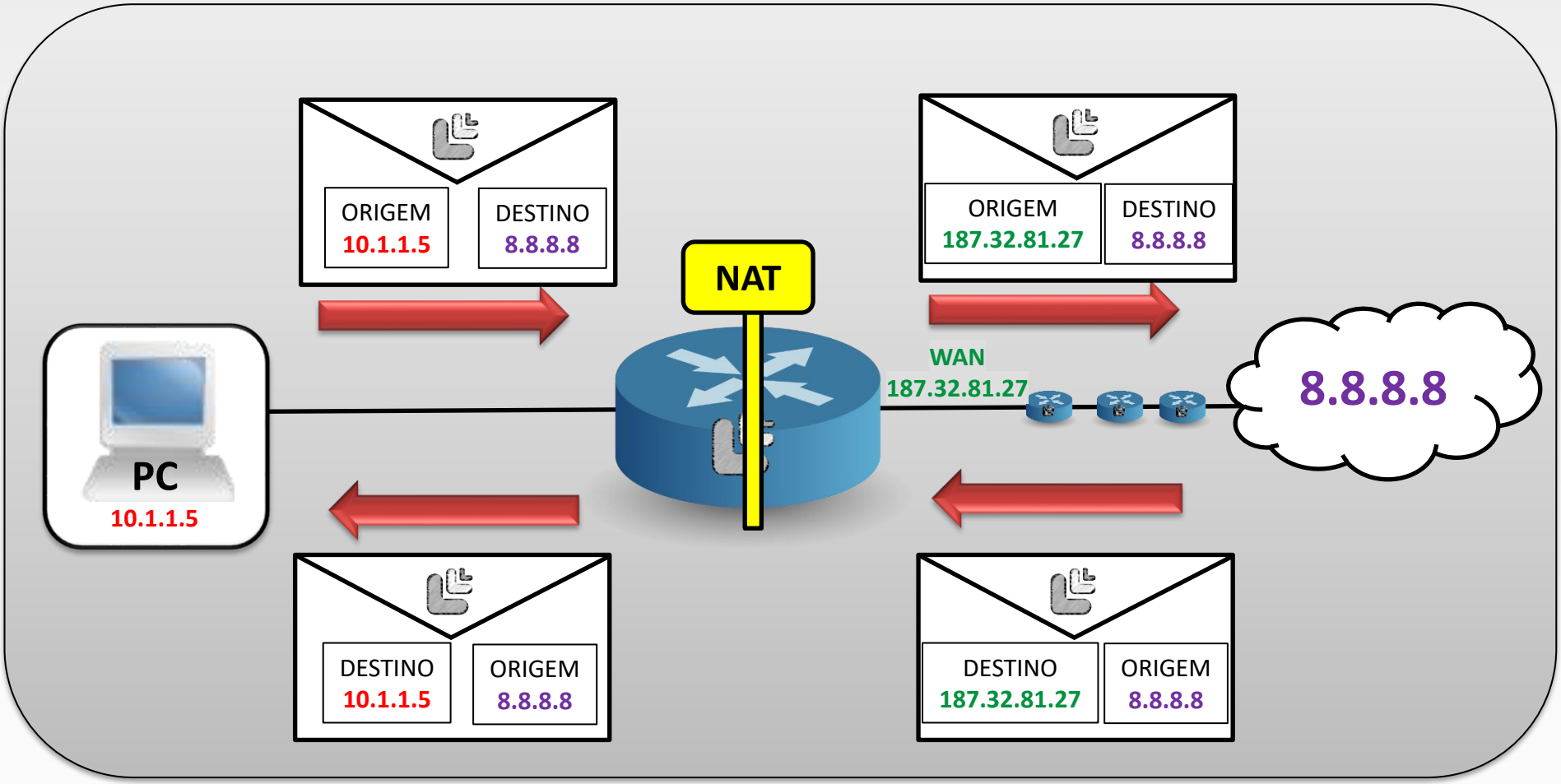
Endereços privados sem uso de NAT



O NAT



NAT


ORIGEM
10.1.1.5
DESTINO
8.8.8.8
NAT
ORIGEM
187.32.81.27
DESTINO
8.8.8.8
WAN
187.32.81.27
8.8.8.8
PC
10.1.1.5
DESTINO
10.1.1.5
ORIGEM
8.8.8.8
DESTINO
187.32.81.27
ORIGEM
8.8.8.8

IP Público vs IP Privado

Endereços Privados

REDE	RESERVADA PARA	DOCUMENTAÇÃO
10.0.0.0/8	Private-Use Networks	RFC 1918
172.16.0.0/12	Private-Use Networks	RFC 1918
192.168.0.0/16	Private-Use Networks	RFC 1918

Utilizado somente na rede interna.
Podem se repetir em diferentes residências e empresas.

Endereços Públicos

200.1.1.2
195.147.178
50.4.2.78
20.10.5.7
11.40.8.9
1.1.1.1
2.8.9.7
220.8.7.4

Globalmente alcançável, portanto deve ser único.

Endereços reservados

Endereços reservados

REDE	RESERVADA PARA	DOCUMENTAÇÃO
0.0.0.0/8	This Network	RFC 1122, Section 3.2.1.3
10.0.0.0/8	Private-Use Networks	RFC 1918
127.0.0.0/8	Loopback	RFC 1122, Section 3.2.1.3
169.254.0.0/16	Link Local	RFC 3927
172.16.0.0/12	Private-Use Networks	RFC 1918
192.0.0.0/24	IETF Protocol Assignments	RFC 5736
192.0.2.0/24	TEST-NET-1	RFC 5737
192.88.99.0/24	6to4 Relay Anycast	RFC 3068
192.168.0.0/16	Private-Use Networks	RFC 1918
198.18.0.0/15	Network Interconnect	
198.51.100.0/24	TEST-NET-2	RFC 5737
203.0.113.0/24	TEST-NET-3	RFC 5737
224.0.0.0/4	Multicast	RFC 3171
240.0.0.0/4	Reserved for Future Use	RFC 1112, Section 4
255.255.255.255/32	Limited Broadcast	RFC 919, Section7
100.64.0.0/10	CGNAT	RFC 6598

IPs Público, Privados e Reservados

IPs Reservados

0.0.0.0/8
100.64.0.0/10
127.0.0.0/8
169.254.0.0/16
192.0.0.0/24
192.0.2.0/24
192.88.99.0/24
198.18.0.0/15
198.51.100.0/24
203.0.113.0/24
224.0.0.0/4
233.252.0.0/24
240.0.0.0/4
255.255.255.255/32

IPs Privados

10.0.0.0/8
192.168.0.0/16
172.16.0.0/12

IPs Públicos

Todo restante

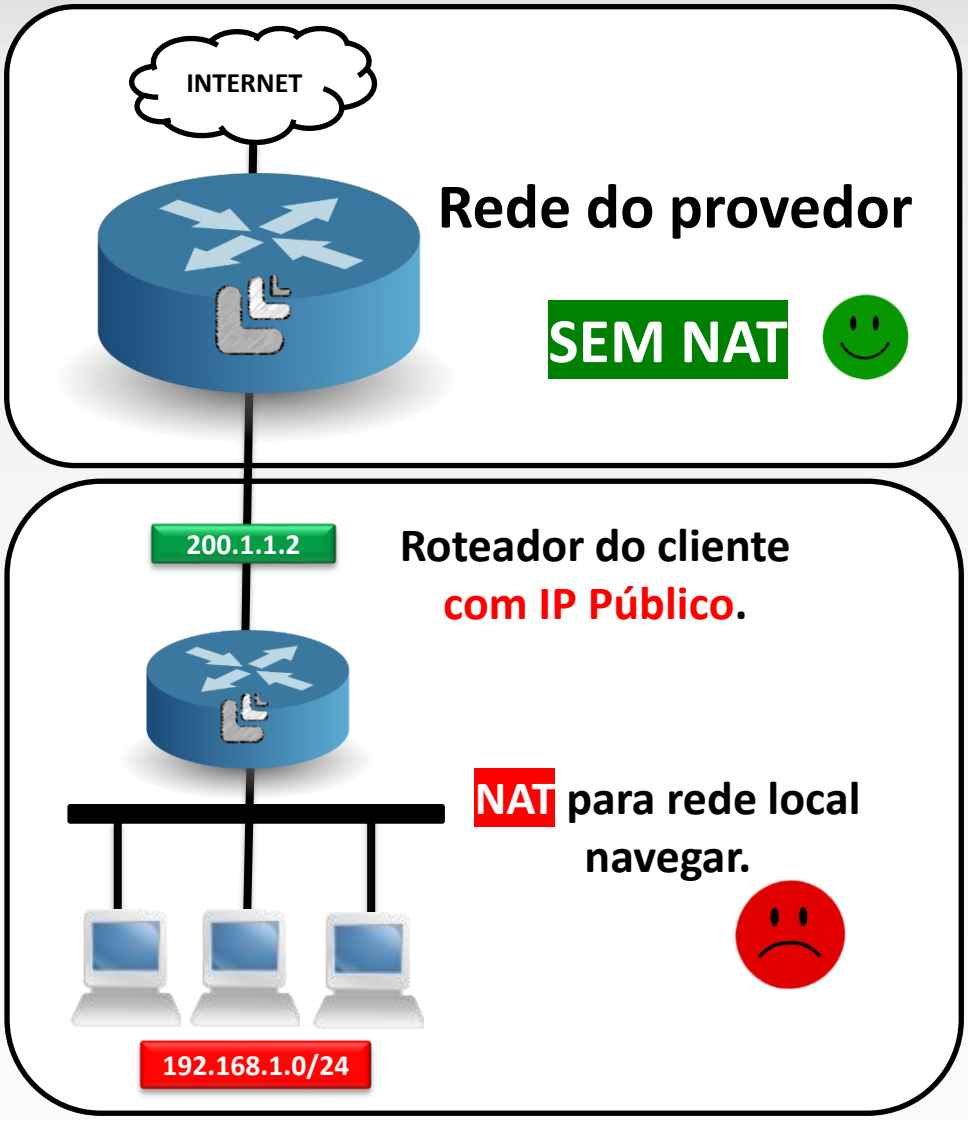
Exemplos abaixo

200.10.16.247
150.20.33.50
50.50.8.8
1.1.1.1
8.8.8.8
11.12.89.78

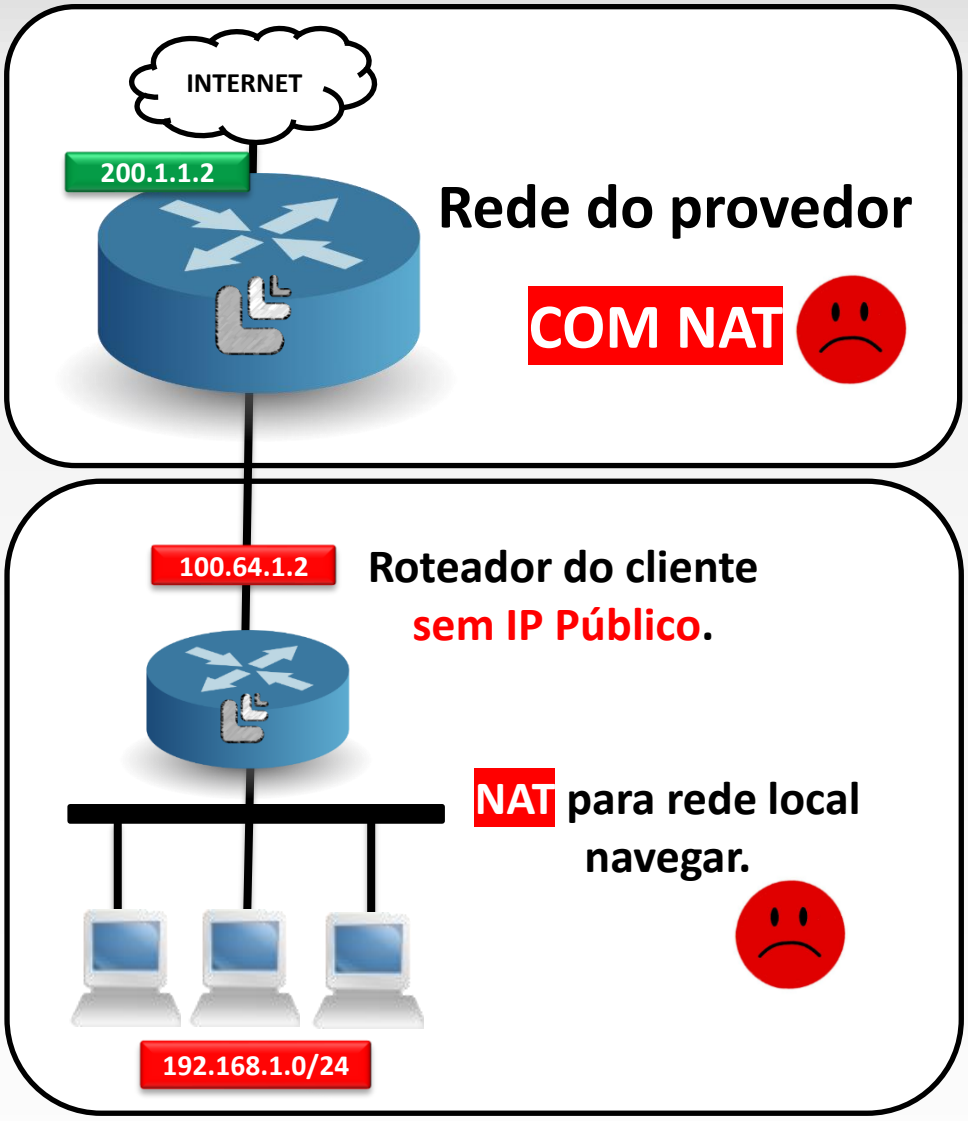
CGNAT

- O NAT ajudou e a internet continuo crescendo e muito;
- Apesar do IPv6 ter sido criado ainda na década de 90 até hoje sua adoção ainda é lenta;
- E mesmo entregando somente 1 IP público para cada usuário final o IPv4 começou a se esgotar novamente;
- E mais uma vez para que a internet continuasse crescendo entra em ação novamente o famoso NAT.
- Mas dessa vez ele é feito dentro do provedor de acesso a Internet e ganhou o nome de CGNAT.

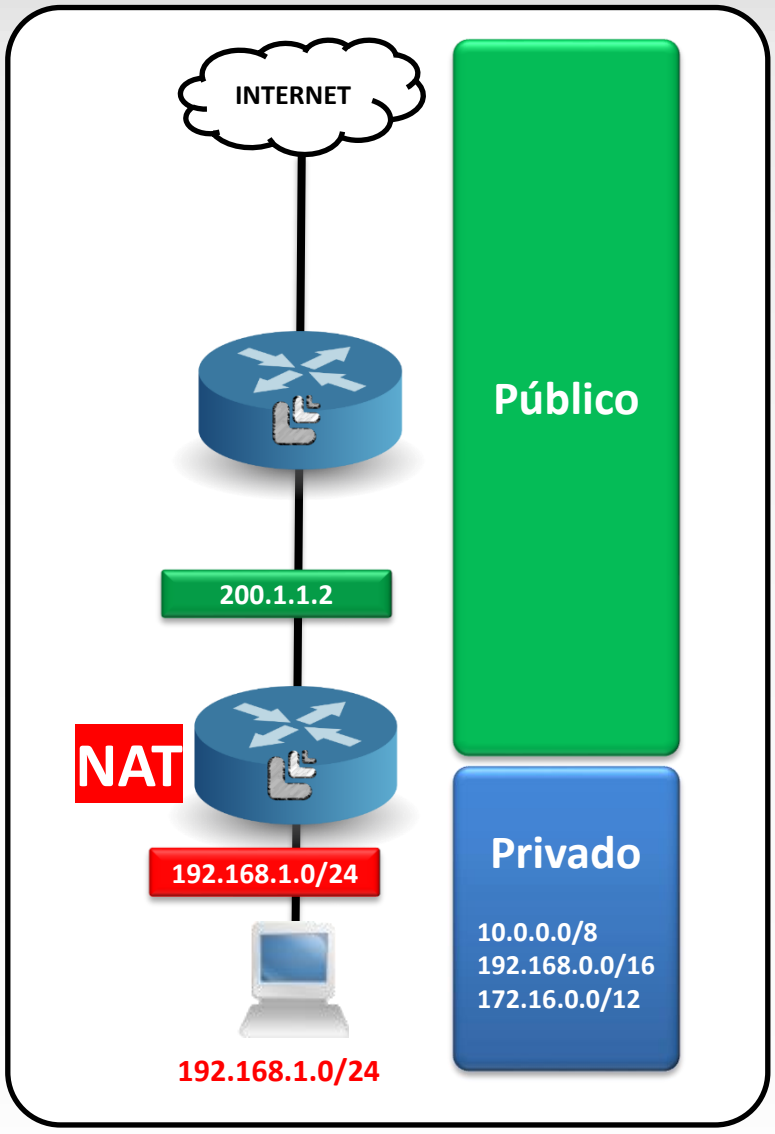
Rede com um NAT

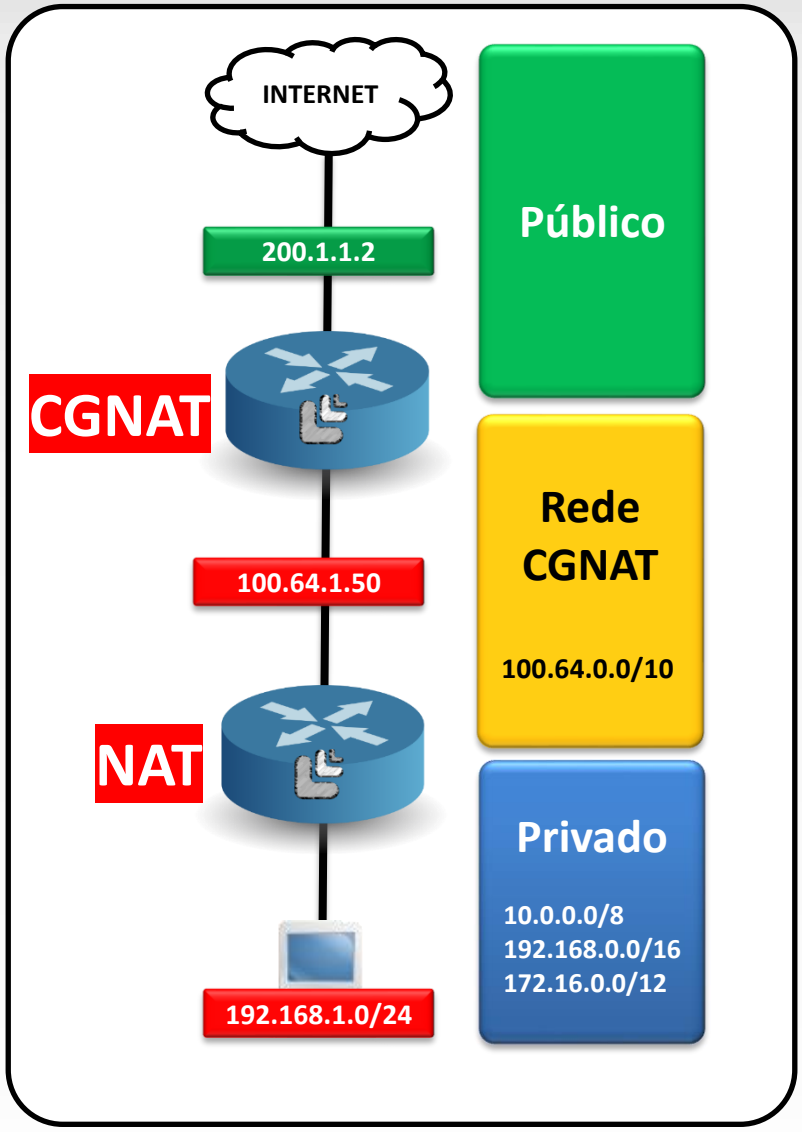


Rede com dois NATs

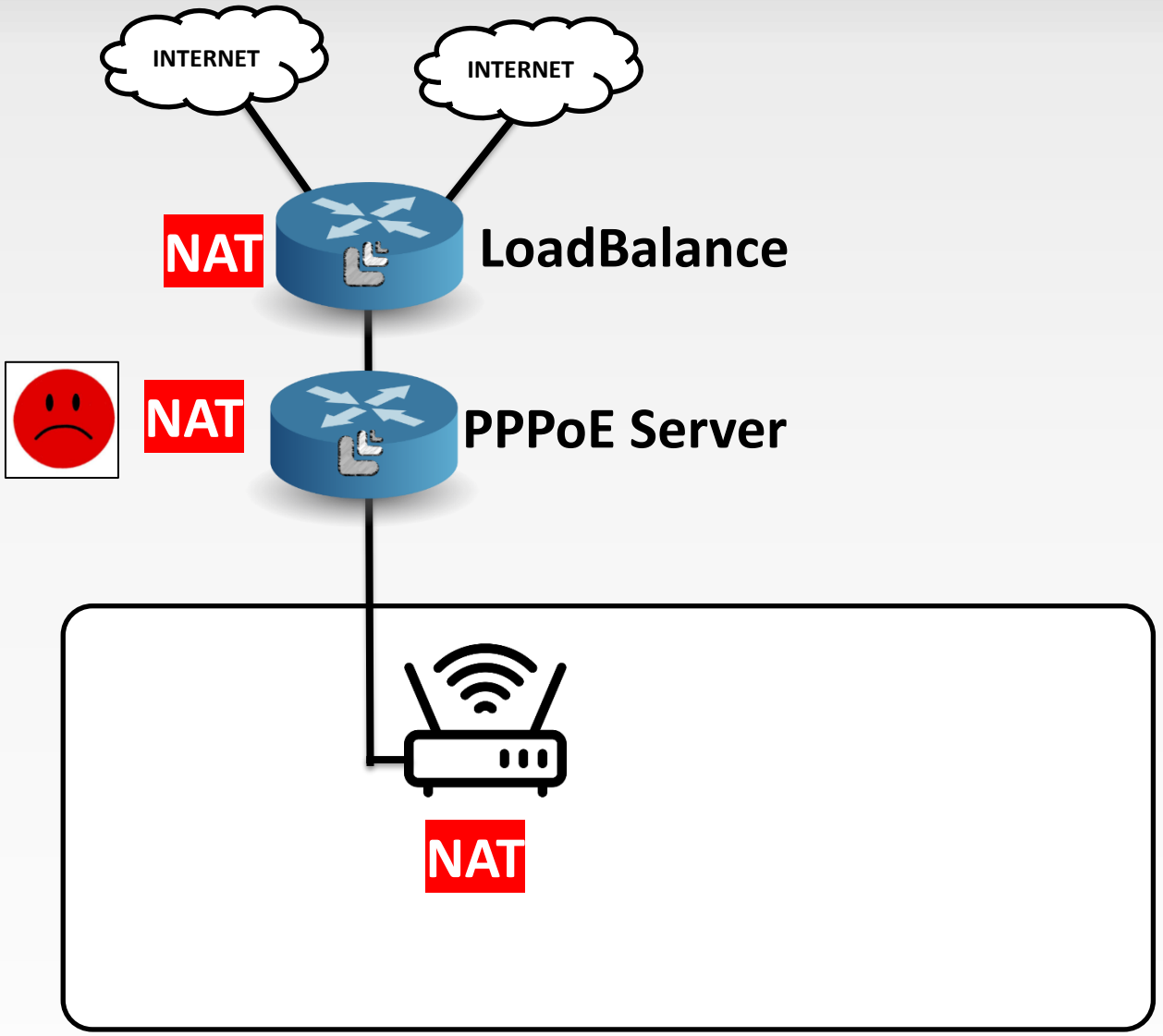


NAT vs CGNAT

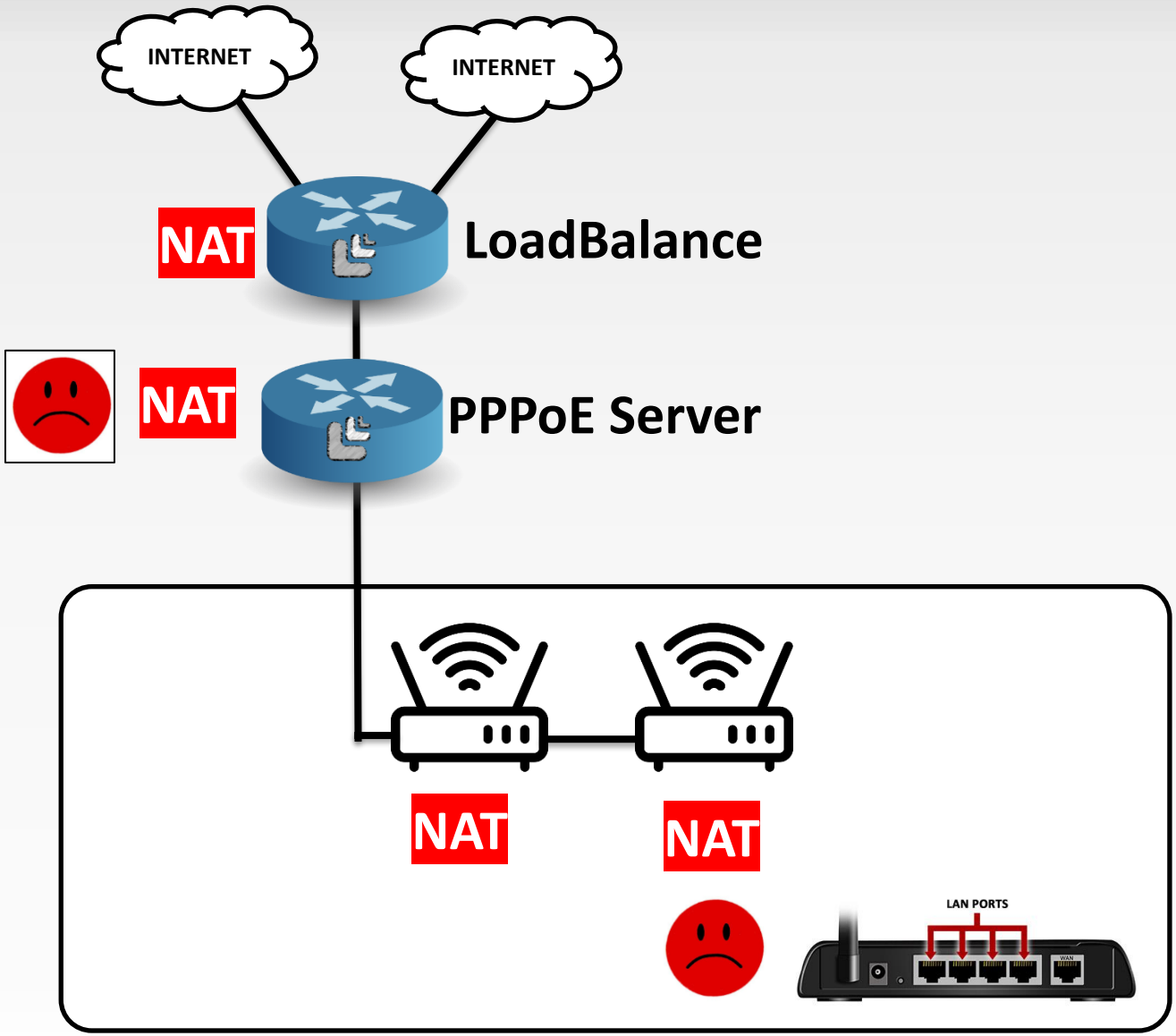

INTERNET
Público
200.1.1.2
NAT
Privado
192.168.1.0/24
10.0.0.0/8
192.168.0.0/16
172.16.0.0/12
192.168.1.0/24


INTERNET
Público
200.1.1.2
CGNAT
Rede
CGNAT
100.64.0.0/10
100.64.1.50
NAT
Privado
10.0.0.0/8
192.168.0.0/16
172.16.0.0/12
192.168.1.0/24

Erros comum com relação a NAT



Erros comum com relação a NAT

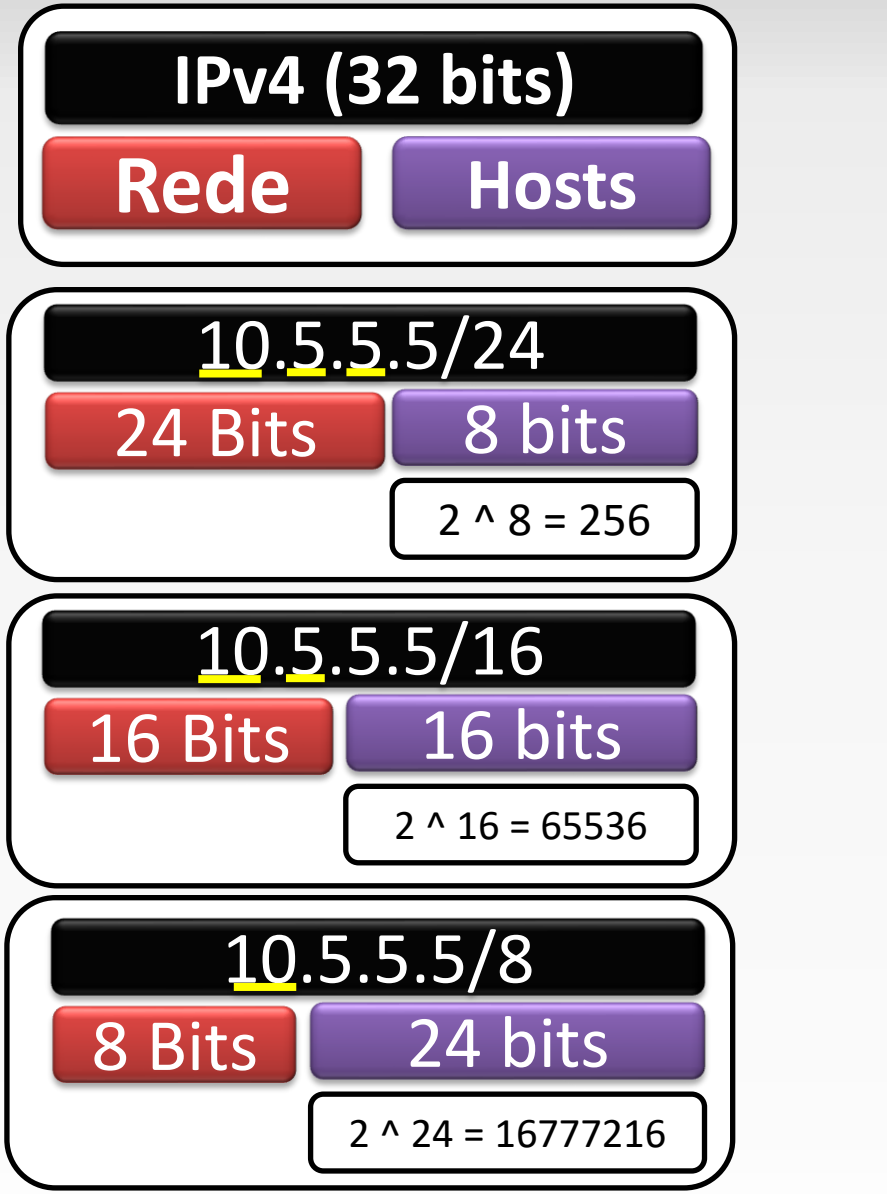


Máscara de sub-rede

- A máscara de sub-rede determina o tamanho de uma rede;
- Na maioria das vezes que você vai configurar um endereço de IP a máscara de sub-rede vai ser exigida ou automaticamente preenchida.
- Normalmente é escrita em dois formatos, vajamos alguns exemplos.

Notação decimal	Notação CIDR	QT de IPs
255.255.255.0	/24	256
255.255.255.252	/30	4
255.0.0.0	/8	16777216
255.255.255.255	/32	1
255.255.252.0	/22	1024
255.255.0.0	/16	65536

Divisão lógica do IP



Quanto IPs tem ?

Redes Brasil

CIDR	QT de IPs
/32	1
/31	2
/30	4
/29	8
/28	16
/27	32
/26	64
/25	128
/24	256
/23	512
/22	1024
/21	2048
/20	4096

https://www.site24x7.com/tools/ipv4-subnetcalculator.html

End. de Rede e Broadcast

- O endereço de REDE é o primeiro IP da sub rede;
- O endereço de BROADCAST é o último IP da sub rede;
- Esses endereços(Rede e broadcast) são reservados e não podem ser usados.

IP e Mask	End. de Rede	End. de Broadcast
10.1.1.5/24	10.1.1.0	10.1.1.255
10.1.1.11/28	10.1.1.0	10.1.1.15
10.1.1.33/30	10.1.1.32	10.1.1.35
10.5.14.0/16	10.5.0.0	10.5.255.255
10.20.30.40/8	10.0.0.0	10.255.255.255

Quanto IPs utilizáveis tem ?

-2

CIDR	QT de IPs	IPs utilizáveis
/32	1	1
/31	2	0 *
/30	4	2
/29	8	6
/28	16	14
/27	32	30
/26	64	62
/25	128	126
/24	256	254
/23	512	510
/22	1024	1022
/21	2048	2046
/20	4096	4094

Onde começa e onde termina ?

IP e Mask	End. de Rede	End. de Broadcast	Range utilizável
10.1.1.5/24	10.1.1.0	10.1.1.255	10.1.1.1 – 10.1.1.254
10.1.1.11/28	10.1.1.0	10.1.1.15	10.1.1.1 – 10.1.1.14
10.1.1.33/30	10.1.1.32	10.1.1.35	10.1.1.33 – 10.1.1.34
10.1.2.255/22	10.1.0.0	10.1.3.255	10.1.0.1 – 10.1.3.254
10.5.14.0/16	10.5.0.0	10.5.255.255	10.5.0.1 – 10.5.255.254
10.20.30.40/8	10.0.0.0	10.255.255.255	10.0.0.1 – 10.255.255.254

Resumo sobre IPs

- IP público vs IP privado;
- IP utilizável vs IP não utilizável;
- IP válido vs IP inválido.

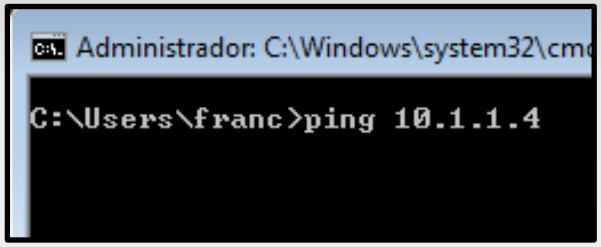
MÓDULO 2.5 - Protocolo ARP

Protocolos - ARP

- ARP – Address resolution protocol (protocolo de resolução de endereços).

- Como o próprio nome sugere esse protocolo consegue resolver(encontrar) o endereço MAC através do endereço de IP e após feito isto o coloca em uma tabela.

Funcionamento do ARP



3 - Qual é o MAC do PC que está com IP 10.1.1.4 ?

10.1.1.10

Switch

10.1.1.2

10.1.1.3

10.1.1.4

1- Tenho que gerar o pacote de PING.

2 - Quais informações eu já tenho ?

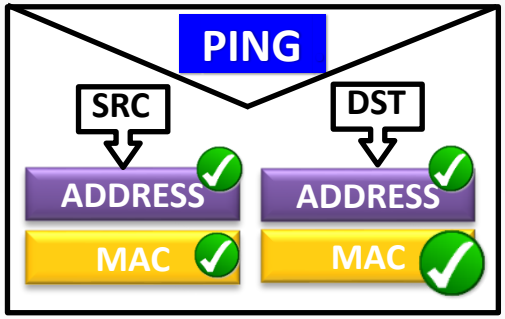
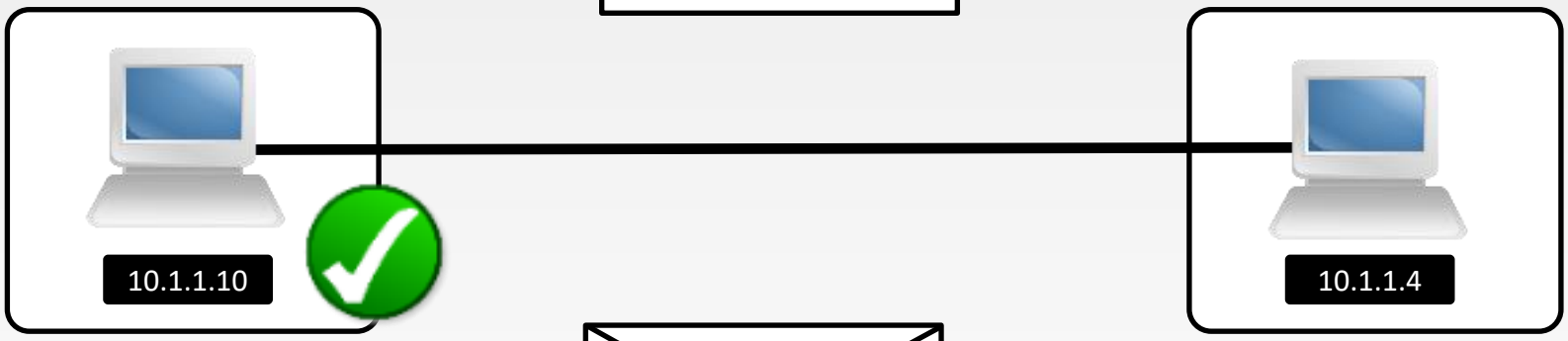


Tabela ARP

IP	MAC
10.1.1.4	E4:8D:8C:04:D5:CC

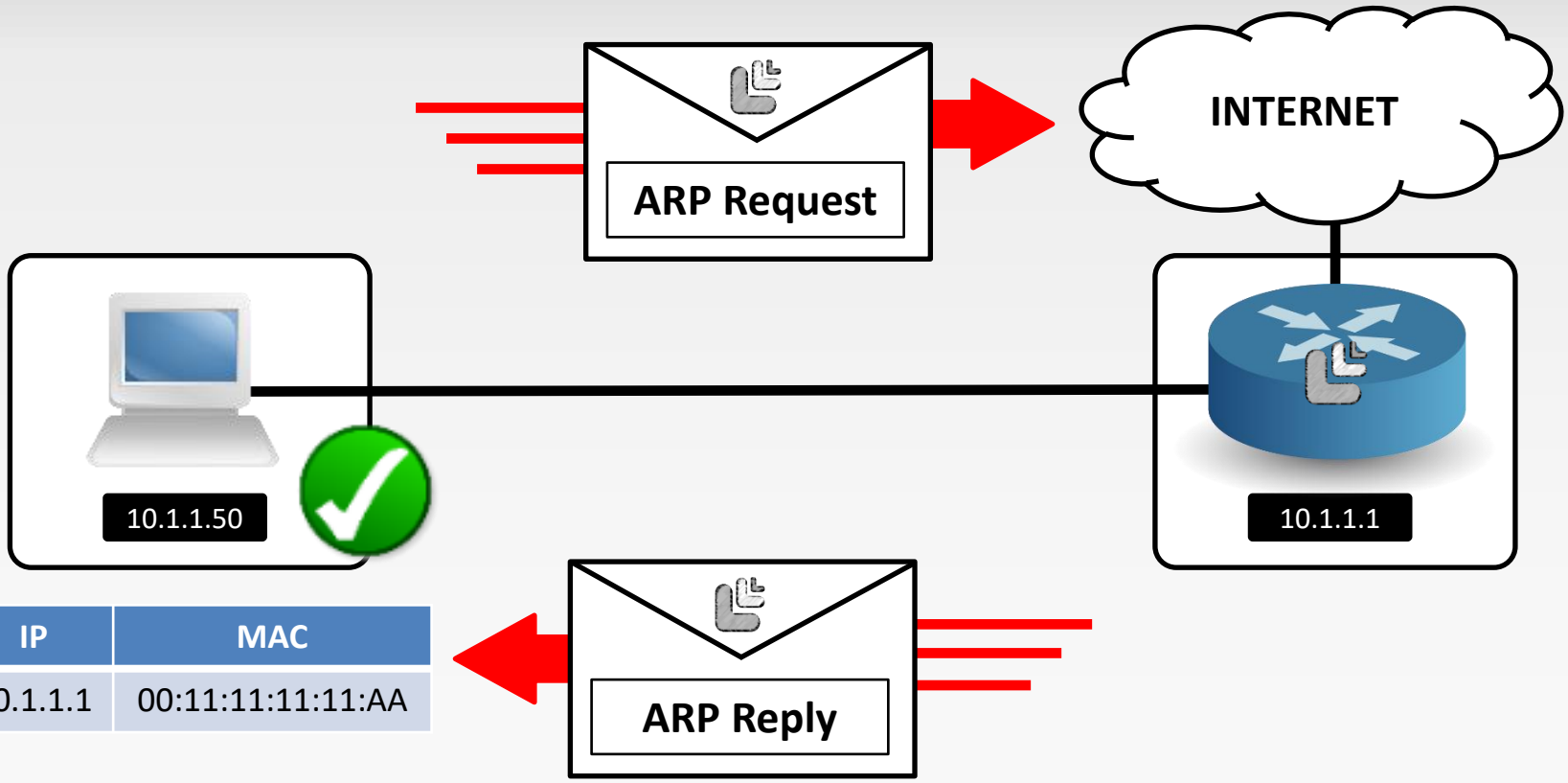
4 - Meu MAC é E4:8D:8C:04:D5:CC

PC para PC



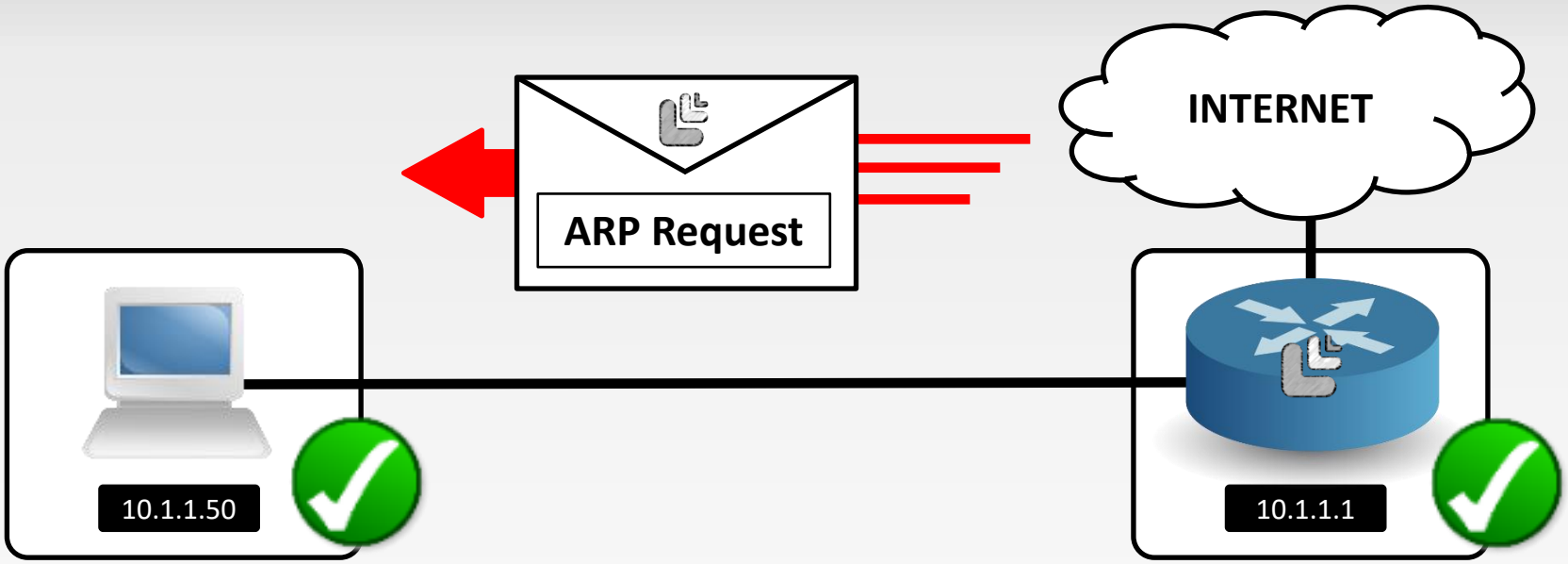
IP	MAC
10.1.1.1	00:11:11:11:11:AA

PC para roteador



IP	MAC
10.1.1.1	00:11:11:11:11:AA

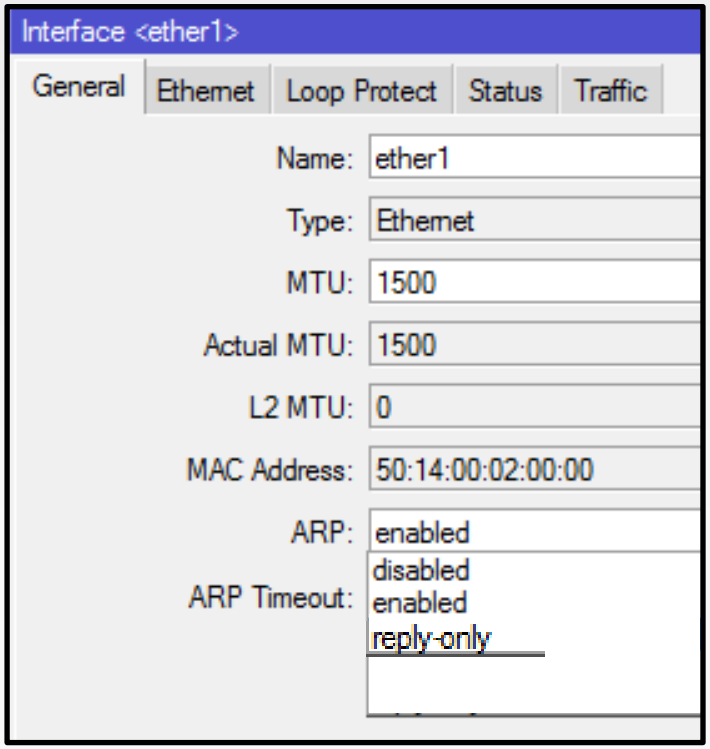
Roteador para PC



IP	MAC
10.1.1.1	00:11:11:11:11:AA

IP	MAC
10.1.1.50	00:11:11:11:11:BB

Modos do ARP



enable: Faz requisições de ARP
Responde requisições ARP

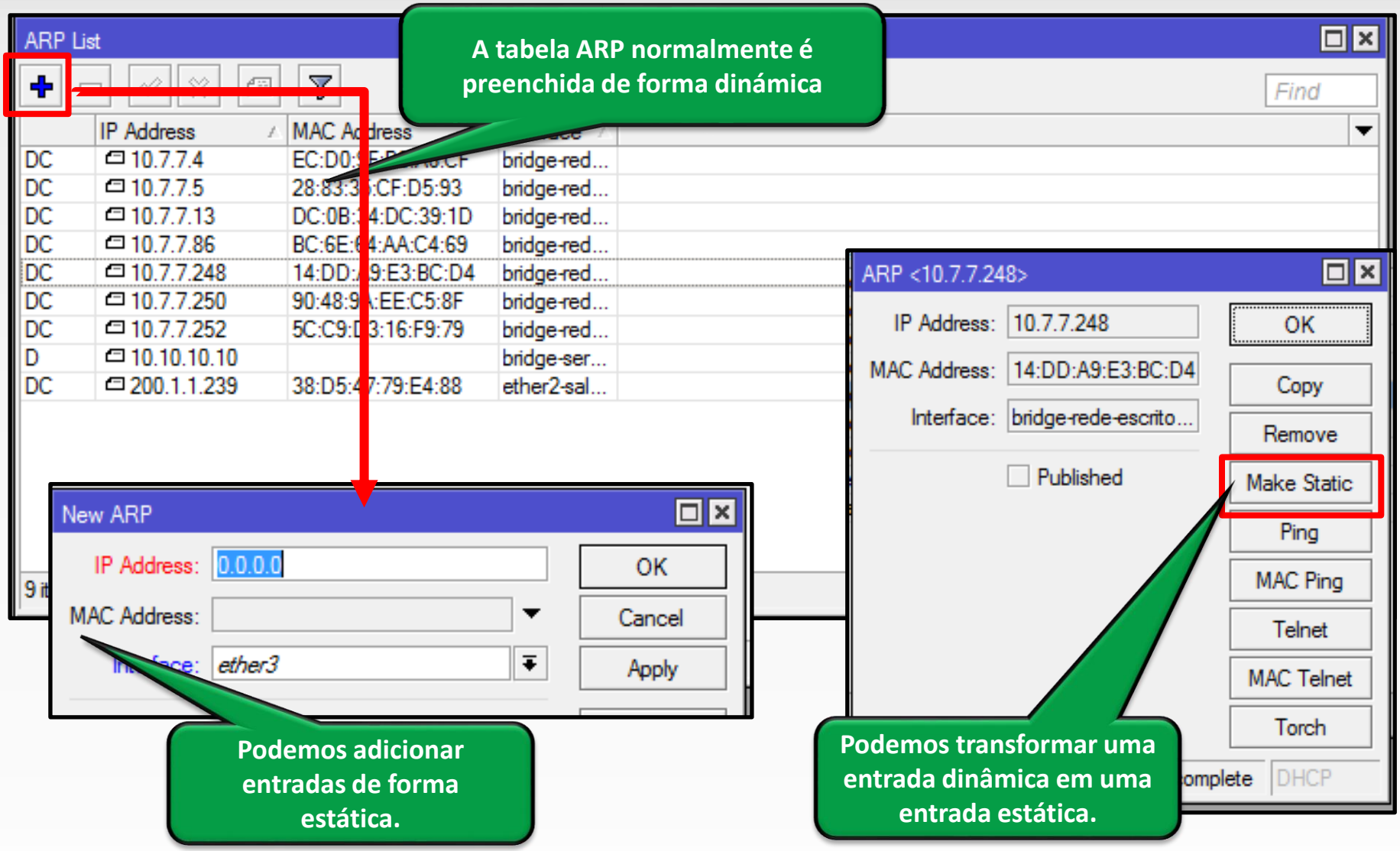
reply-only: Não faz requisições de ARP
Responde requisições ARP

disable: Não faz requisições de ARP
Não responde requisições ARP

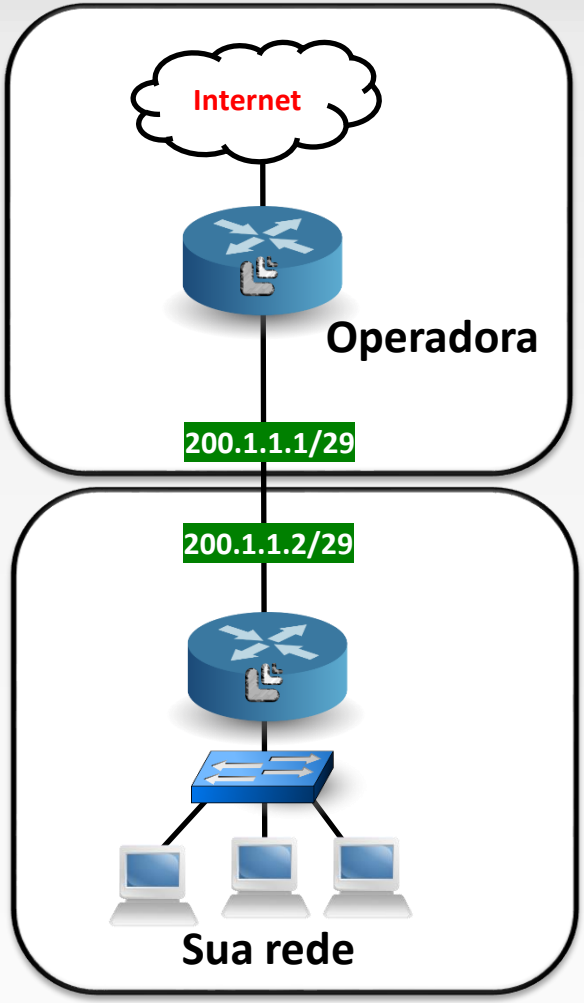
IP duplicado

- Criar uma entrada estática na tabela ARP pode ser muito útil em casos onde temos hosts com IPs duplicados na rede;
- Normalmente o acesso remoto a esses dispositivos fica comprometido;
- Com a entrada estática na tabela ARP podemos acessar e forçar o acesso a um dos dispositivos e logo na sequencia fazer a alteração do endereço de IP.

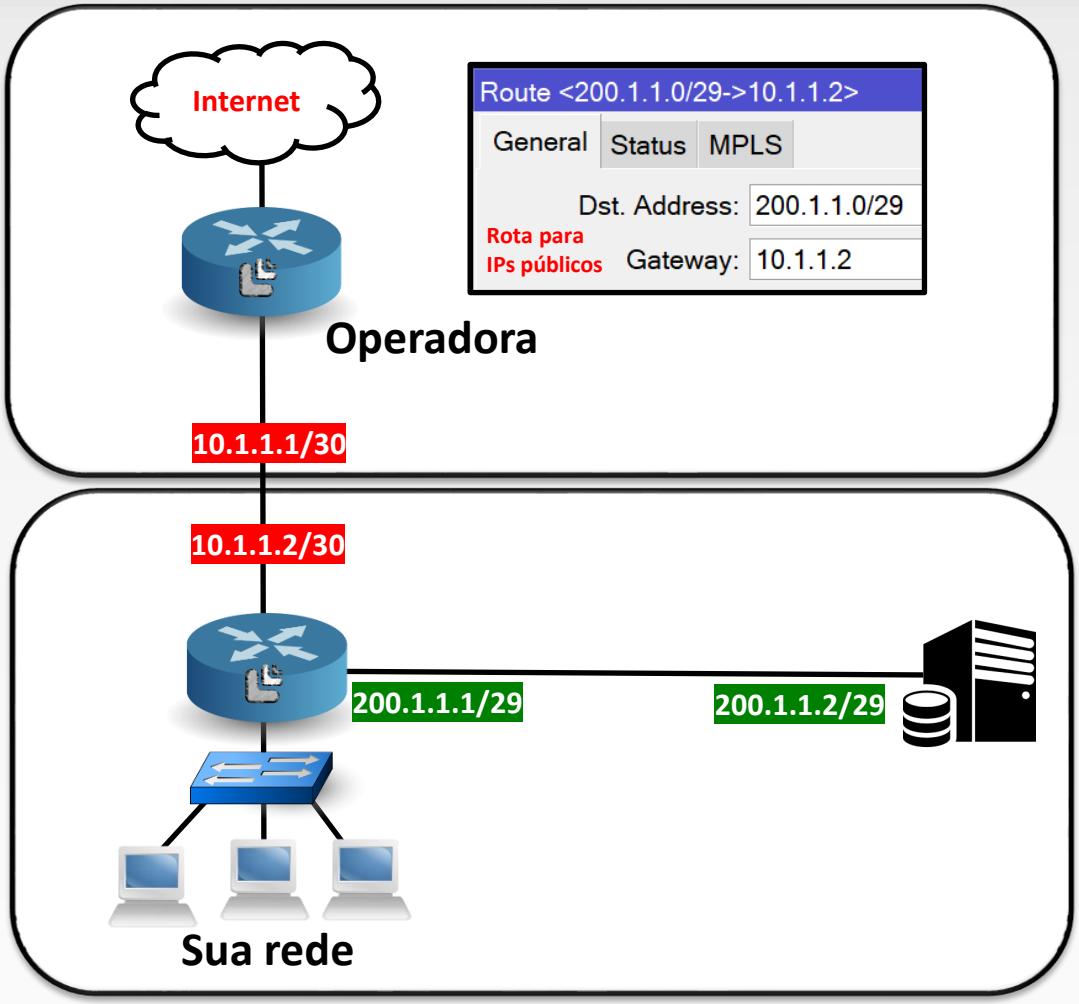
Tabela ARP


A tabela ARP normalmente é preenchida de forma dinâmica
ARP List
Find
IP Address
MAC Address
DC 10.7.7.4 EC:D0:... bridge-red...
DC 10.7.7.5 28:83:3...:CF:D5:93 bridge-red...
DC 10.7.7.13 DC:0B:...4:DC:39:1D bridge-red...
DC 10.7.7.86 BC:6E:...4:AA:C4:69 bridge-red...
DC 10.7.7.248 14:DD:...9:E3:BC:D4 bridge-red...
DC 10.7.7.250 90:48:9...:EE:C5:8F bridge-red...
DC 10.7.7.252 5C:C9:D...3:16:F9:79 bridge-red...
D 10.10.10.10 bridge-ser...
DC 200.1.1.239 38:D5:...7:79:E4:88 ether2-sal...
New ARP
IP Address: 0.0.0.0
MAC Address:
Interface: ether3
OK
Cancel
Apply
ARP <10.7.7.248>
IP Address: 10.7.7.248
MAC Address: 14:DD:A9:E3:BC:D4
Interface: bridge-rede-escrito...
Published
OK
Copy
Remove
Make Static
Ping
MAC Ping
Telnet
MAC Telnet
Torch
DHCP
Podemos adicionar entradas de forma estática.
Podemos transformar uma entrada dinâmica em uma entrada estática.

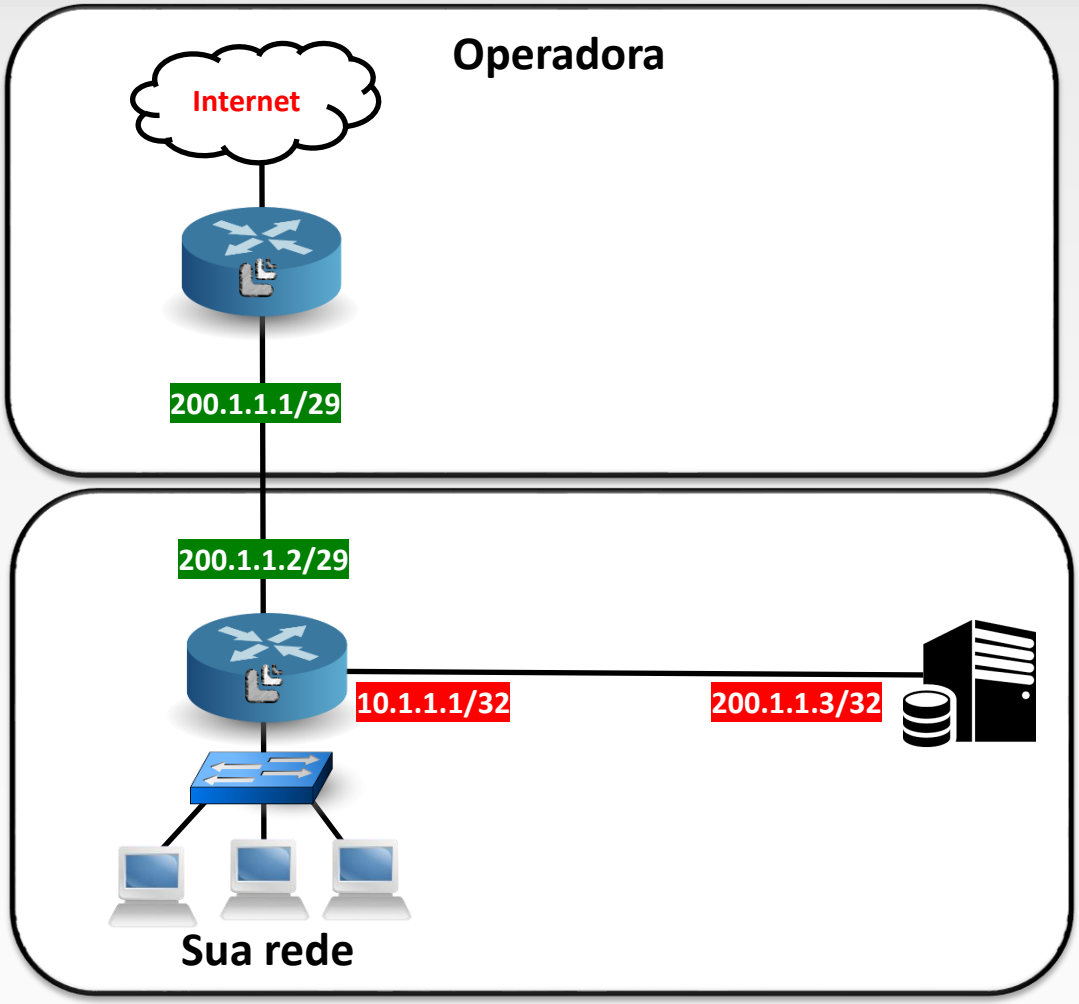
IP público recebido na WAN



IP público roteado



Usando IP público na LAN mesmo recebendo na WAN



MÓDULO 2.6 - TCP vs UDP

Protocolos de transporte

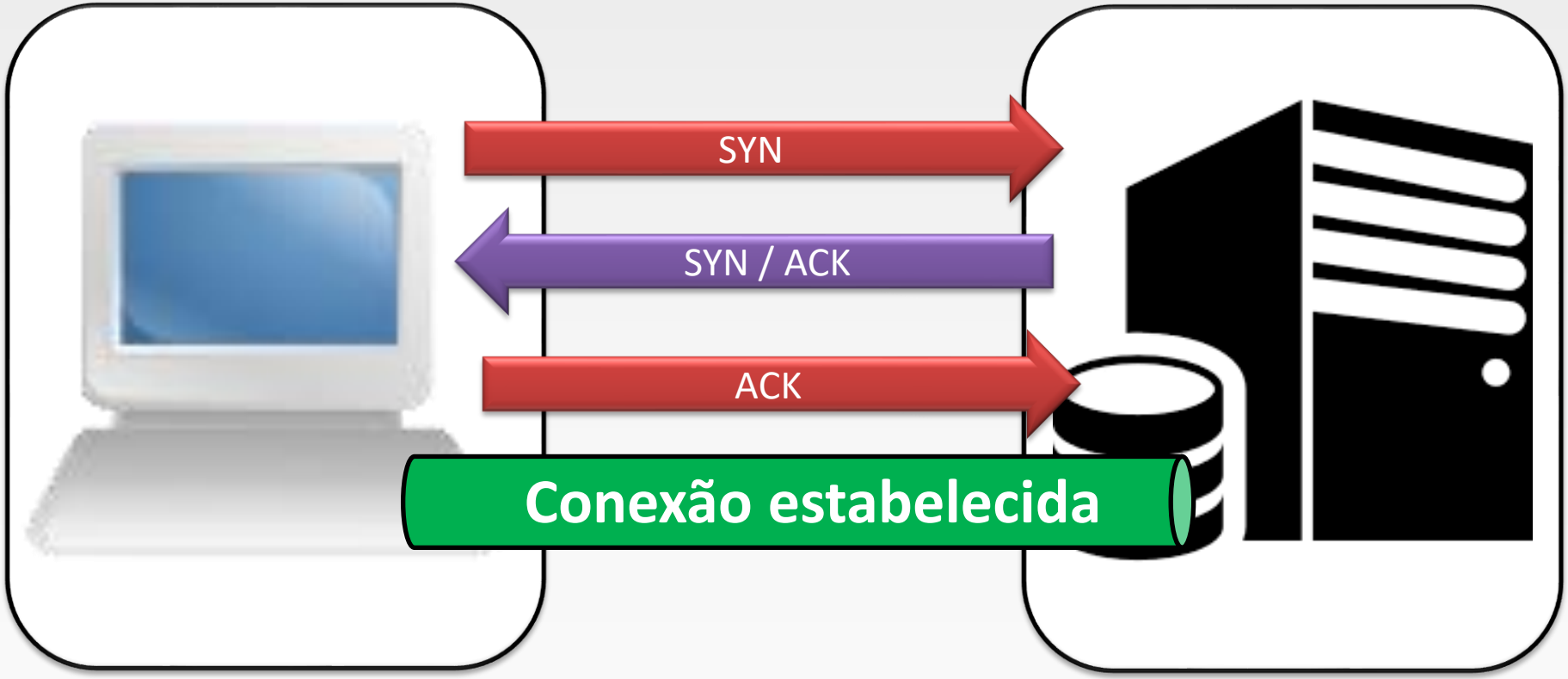
- Tanto o TCP quanto o UDP são protocolos da camada de transporte;
- Vários protocolos de camadas superiores fazem uso do TCP e UDP;
- Um único host pode ter vários serviços usando o TCP ou até mesmo o UDP;
- Cada serviço precisa estar associado uma porta (1 a 65536, porta 0 existe, mas tem uso reservado)

https://arxiv.org/pdf/2201.00142.pdf

Protocolos - UDP / TCP

UDP	TCP
Não é orientado a conexão; nenhuma sessão é estabelecida entre os hosts	Orientado por conexão; uma sessão é estabelecida entre os hosts.
O UDP não garante ou confirma a entrega nem sequencia os dados	O TCP garante a entrega usando confirmações e entrega sequenciada dos dados.
É mais rápido	O TCP é mais lento
Baixa sobrecarga	Maior sobrecarga
Menor latência	Maior latência
Menor overhead (8 bytes)	Maior overhead (20 bytes)

TCP - Three-Way Handshake



Protocolos que usam TCP e UDP

TCP	UDP
• DNS • HTTP • HTTPS • SSH • TELNET • FTP • WINBOX • BGP	• DNS • SNMP • NTP • DHCP • TFTP • RIP • L2TP

MÓDULO 2.7 – Protocolo ICMP

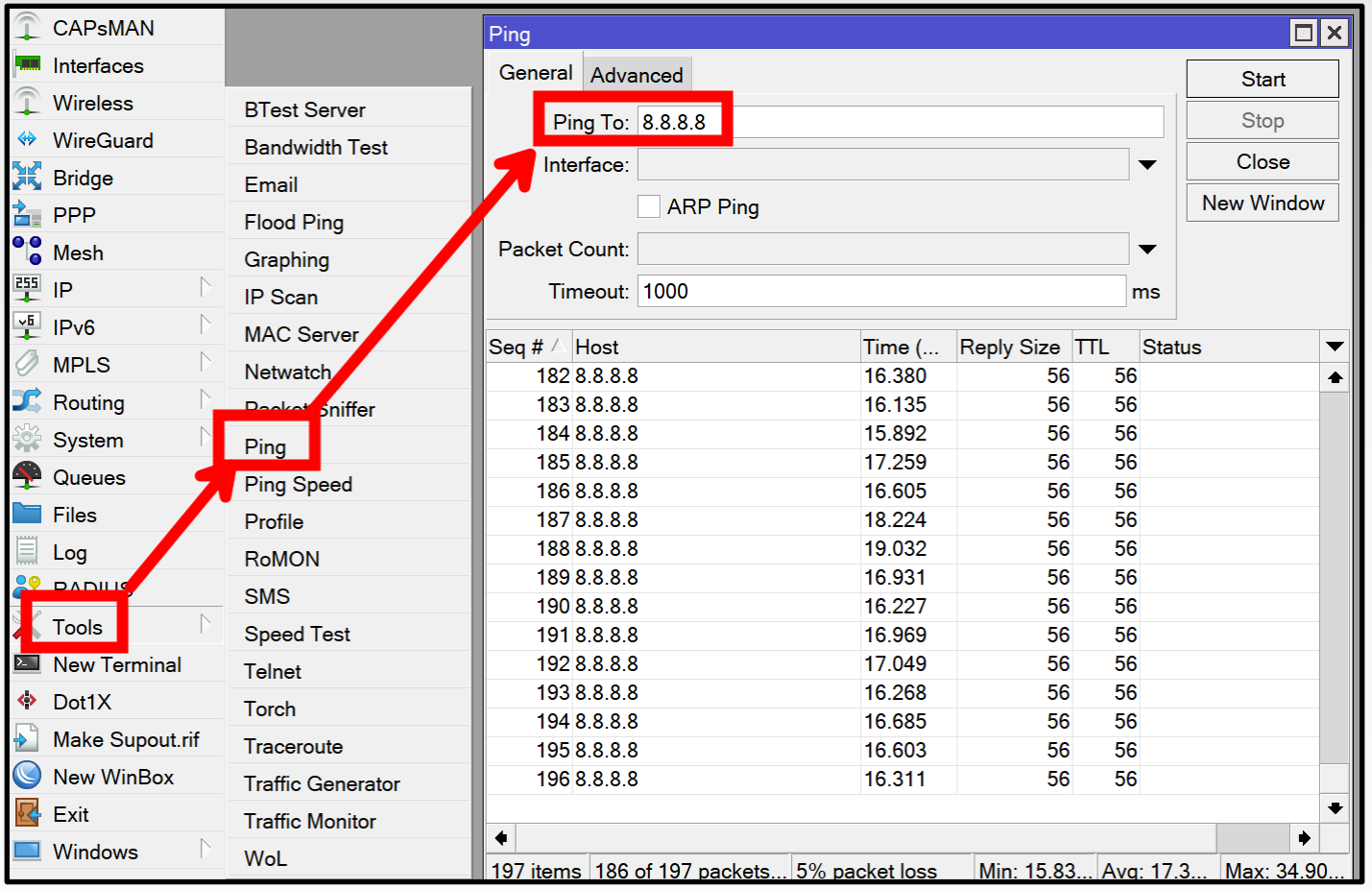
Protocolos - ICMP

- Internet Control Message Protocol ou protocolo de mensagens de controle da Internet é usado para relatar erros e trocar informações de status e controle.

- Diferente do TCP e UDP esse protocolo não implementa portas e para diferenciar uma mensagem de outra utiliza dois campos chamados de tipo e código.

ICMP Type	Code	Description
0	0	eco reply (to ping)
3	0	destination network unreachable
3	1	destination host unreachable
3	2	destination protocol unreachable
3	7	destination host unknown
8	0	eco request
10	0	router discovery
11	0	TTL expired

PING

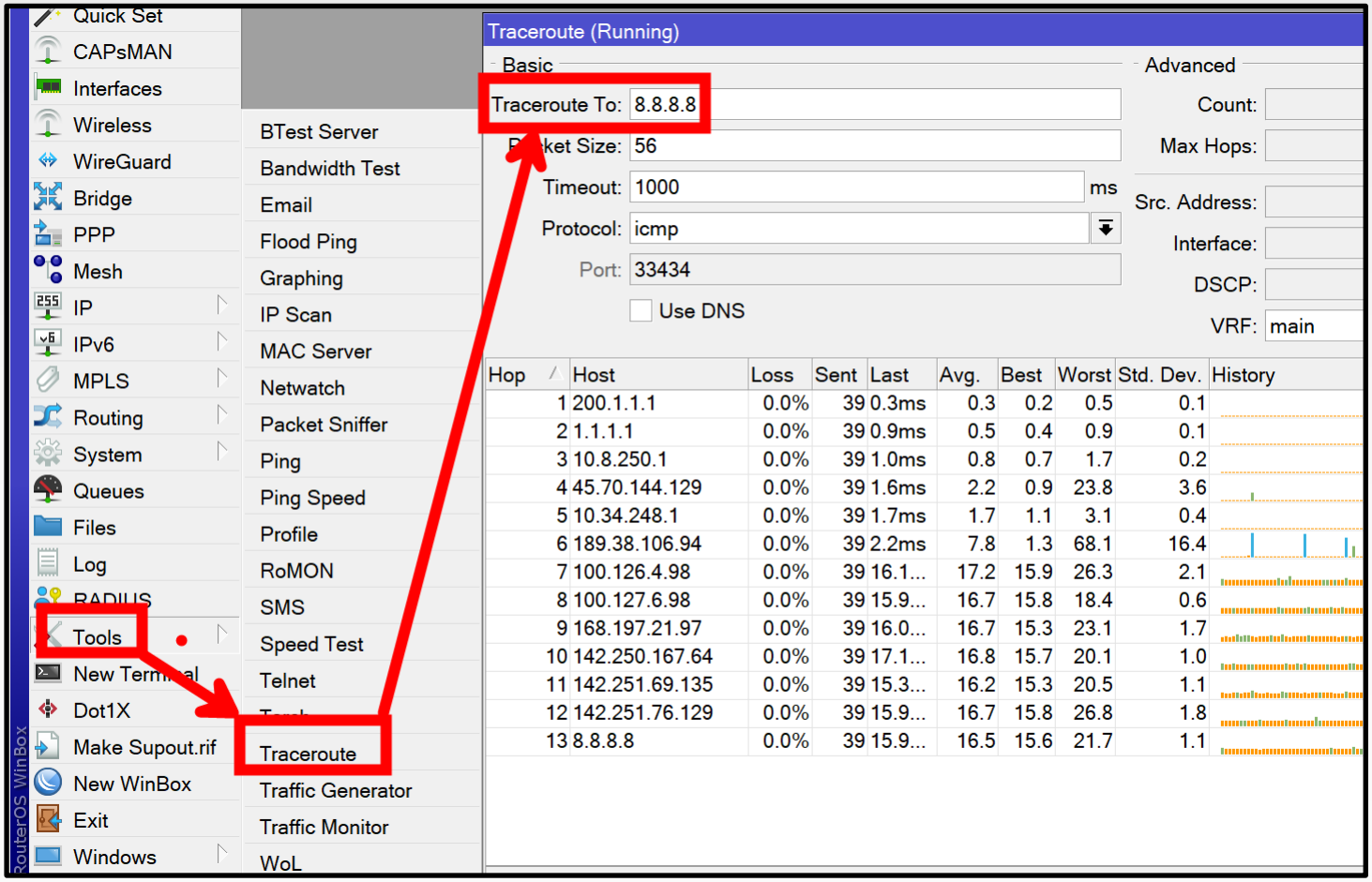

CAPsMAN
Interfaces
Wireless
WireGuard
Bridge
PPP
Mesh
IP
IPv6
MPLS
Routing
System
Queues
Files
Log
Tools
New Terminal
Dot1X
Make Supout.rif
New WinBox
Exit
Windows
BTest Server
Bandwidth Test
Email
Flood Ping
Graphing
IP Scan
MAC Server
Netwatch
Ping
Ping Speed
Profile
RoMON
SMS
Speed Test
Telnet
Torch
Traceroute
Traffic Generator
Traffic Monitor
WoL
Ping
General
Advanced
Start
Stop
Close
New Window
Ping To: 8.8.8.8
Interface:
ARP Ping
Packet Count:
Timeout: 1000
ms
Seq # / Host Time (... Reply Size TTL Status
182 8.8.8.8 16.380 56 56
183 8.8.8.8 16.135 56 56
184 8.8.8.8 15.892 56 56
185 8.8.8.8 17.259 56 56
186 8.8.8.8 16.605 56 56
187 8.8.8.8 18.224 56 56
188 8.8.8.8 19.032 56 56
189 8.8.8.8 16.931 56 56
190 8.8.8.8 16.227 56 56
191 8.8.8.8 16.969 56 56
192 8.8.8.8 17.049 56 56
193 8.8.8.8 16.268 56 56
194 8.8.8.8 16.685 56 56
195 8.8.8.8 16.603 56 56
196 8.8.8.8 16.311 56 56
197 items
186 of 197 packets...
5% packet loss
Min: 15.83...
Avg: 17.3...
Max: 34.90...

Um pouco mais sobre o PING

Redes Brasil

- Status (UP/Down);
- Latência;
- Perda de pacotes;
- Teste de Fragmentação;
- Teste de roteamento na ponta remota;
- Teste de Spoofing;
- Testar tabelas de roteamento separadas.

Traceroute


Quick Set
CAPsMAN
Interfaces
Wireless
WireGuard
Bridge
PPP
Mesh
IP
IPv6
MPLS
Routing
System
Queues
Files
Log
RADIUS
Tools
New Terminal
Dot1X
Make Supout.rif
New WinBox
Exit
Windows
RouterOS WinBox
BTest Server
Bandwidth Test
Email
Flood Ping
Graphing
IP Scan
MAC Server
Netwatch
Packet Sniffer
Ping
Ping Speed
Profile
RoMON
SMS
Speed Test
Telnet
Traceroute
Traffic Generator
Traffic Monitor
WoL
Traceroute (Running)
Basic
Traceroute To: 8.8.8.8
Packet Size: 56
Timeout: 1000 ms
Protocol: icmp
Port: 33434
Use DNS
Advanced
Count:
Max Hops:
Src. Address:
Interface:
DSCP:
VRF: main
Hop Host Loss Sent Last Avg. Best Worst Std. Dev. History
1 200.1.1.1 0.0% 39 0.3ms 0.3 0.2 0.5 0.1
2 1.1.1.1 0.0% 39 0.9ms 0.5 0.4 0.9 0.1
3 10.8.250.1 0.0% 39 1.0ms 0.8 0.7 1.7 0.2
4 45.70.144.129 0.0% 39 1.6ms 2.2 0.9 23.8 3.6
5 10.34.248.1 0.0% 39 1.7ms 1.7 1.1 3.1 0.4
6 189.38.106.94 0.0% 39 2.2ms 7.8 1.3 68.1 16.4
7 100.126.4.98 0.0% 39 16.1... 17.2 15.9 26.3 2.1
8 100.127.6.98 0.0% 39 15.9... 16.7 15.8 18.4 0.6
9 168.197.21.97 0.0% 39 16.0... 16.7 15.3 23.1 1.7
10 142.250.167.64 0.0% 39 17.1... 16.8 15.7 20.1 1.0
11 142.251.69.135 0.0% 39 15.3... 16.2 15.3 20.5 1.1
12 142.251.76.129 0.0% 39 15.9... 16.7 15.8 26.8 1.8
13 8.8.8.8 0.0% 39 15.9... 16.5 15.6 21.7 1.1

MÓDULO 2.8 - Torch, Contrack, Packet Sniffer e Logs;

Ferramentas de análise

- **Torch:** Ferramenta de análise de conexões em tempo real (por interface);
- **Packet Sniffer:** Ferramenta para captura de pacotes, podendo salvar a captura em um arquivo para análise mais detalhada;
- **Logs:** Podemos usar a ação log do firewall para gerar informações uteis para diagnosticar problemas que estejam ou não relacionados com o firewall;
- **Contrack:** Se estiver ativa, ele pode monitorar conexões destinadas e que passam pelo roteador com detalhes importantes como por exemplo traduções feitas pelo NAT.

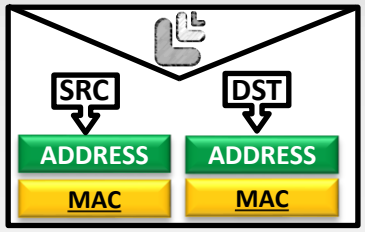
MÓDULO 3 - Bridges e Swtichs

MÓDULO 3 – Bridges e Swtichs

- ✓ 3.1 – Funcionamento de um Swtich;
- ✓ 3.2 – Bridge vs Swtich;

MÓDULO 3.1 – Funcionamento de um Swtich

Como o switch funciona



MAC	INTERFACE
AA:BB:CC:DD:EE:11	ether1
AA:BB:CC:DD:EE:44	ether4
AA:BB:CC:DD:EE:33	ether3
AA:BB:CC:DD:EE:22	ether2

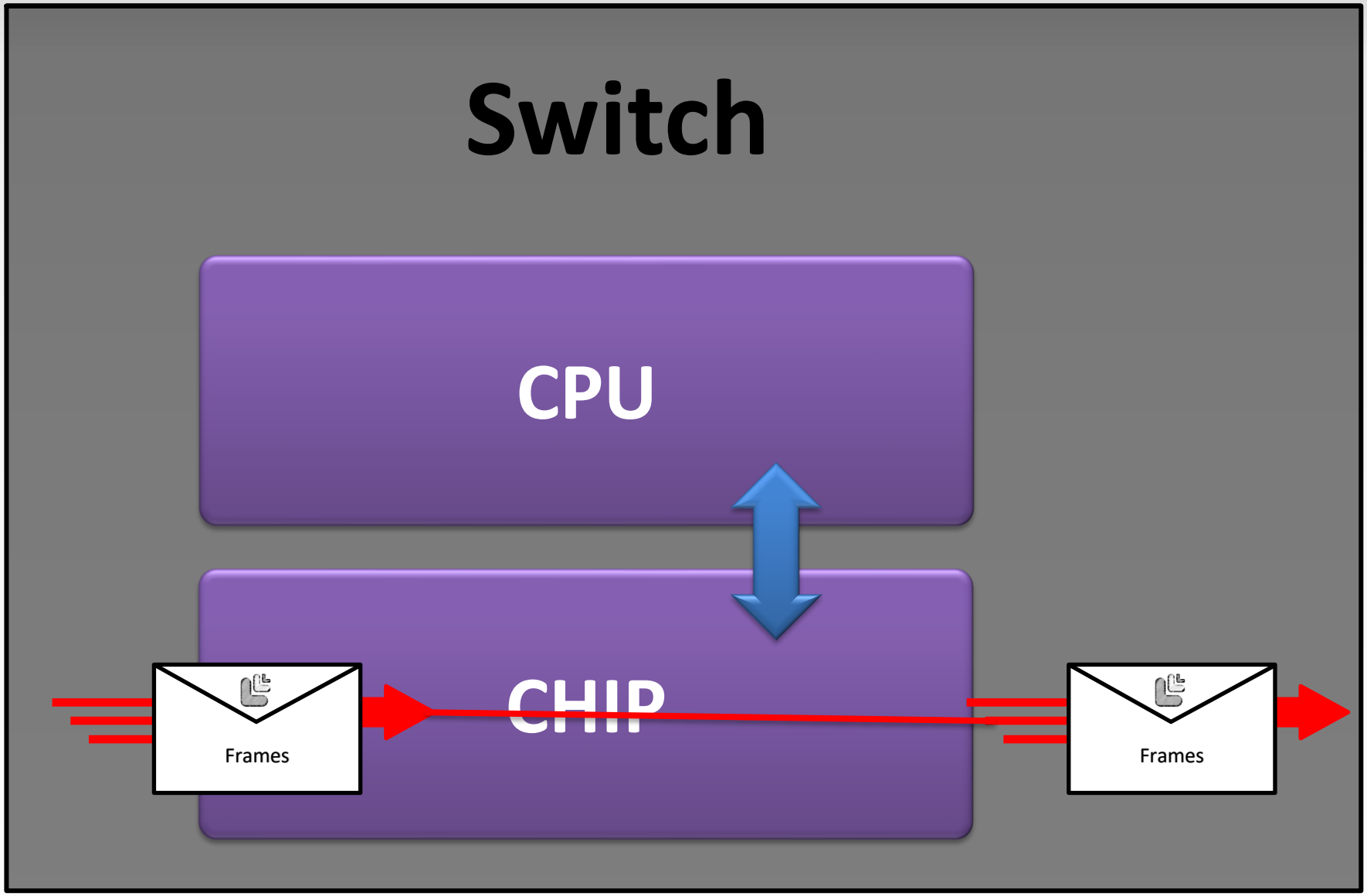
MÓDULO 3·2 – Bridge vs Swtich

Bridge vs Switch

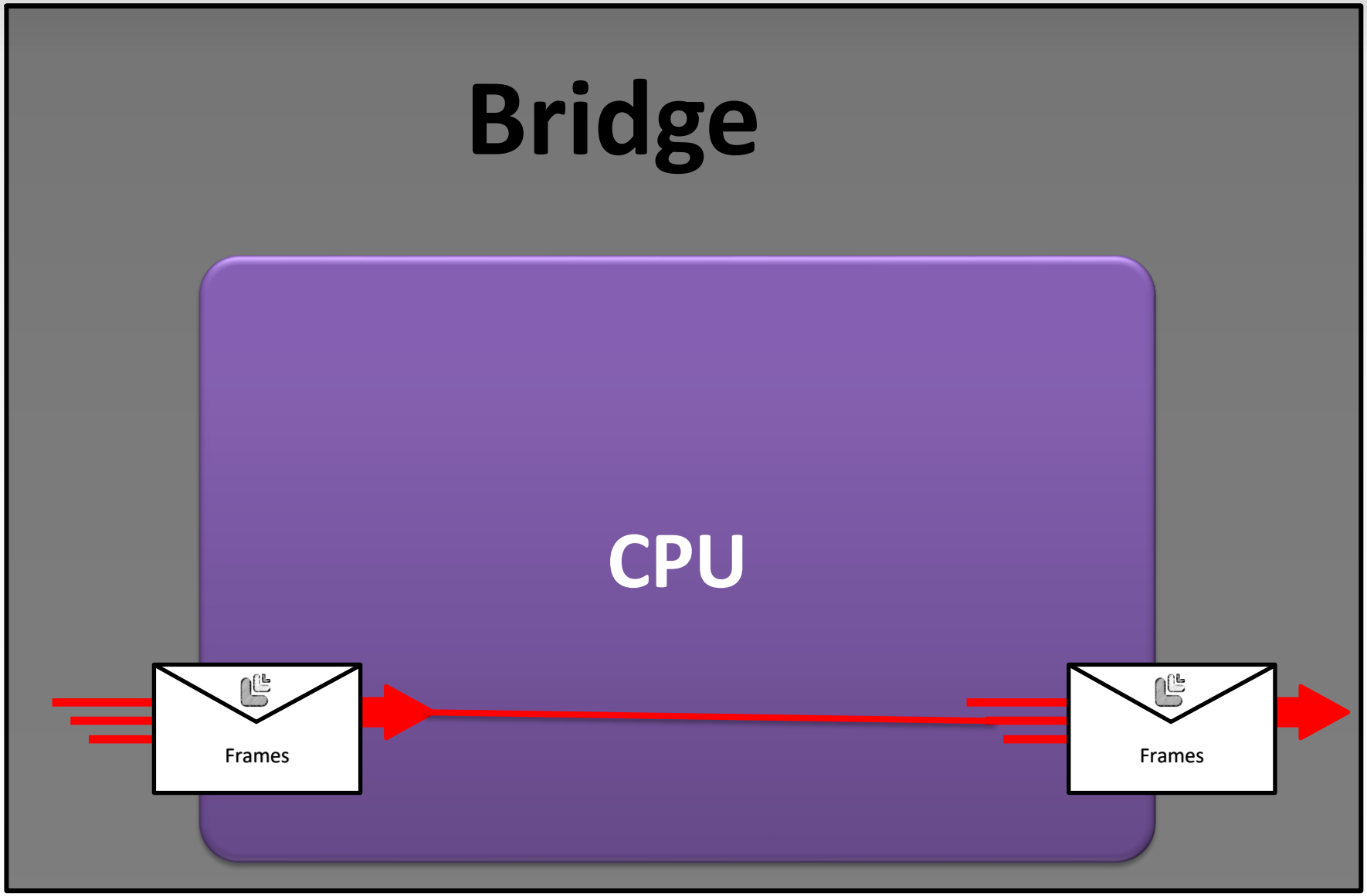
- Uma bridge tem o funcionamento igual ao de um switch porém a comutação dos frames são feitas via Software/CPU.

- O switch faz a comutação dos frames via CHIP.

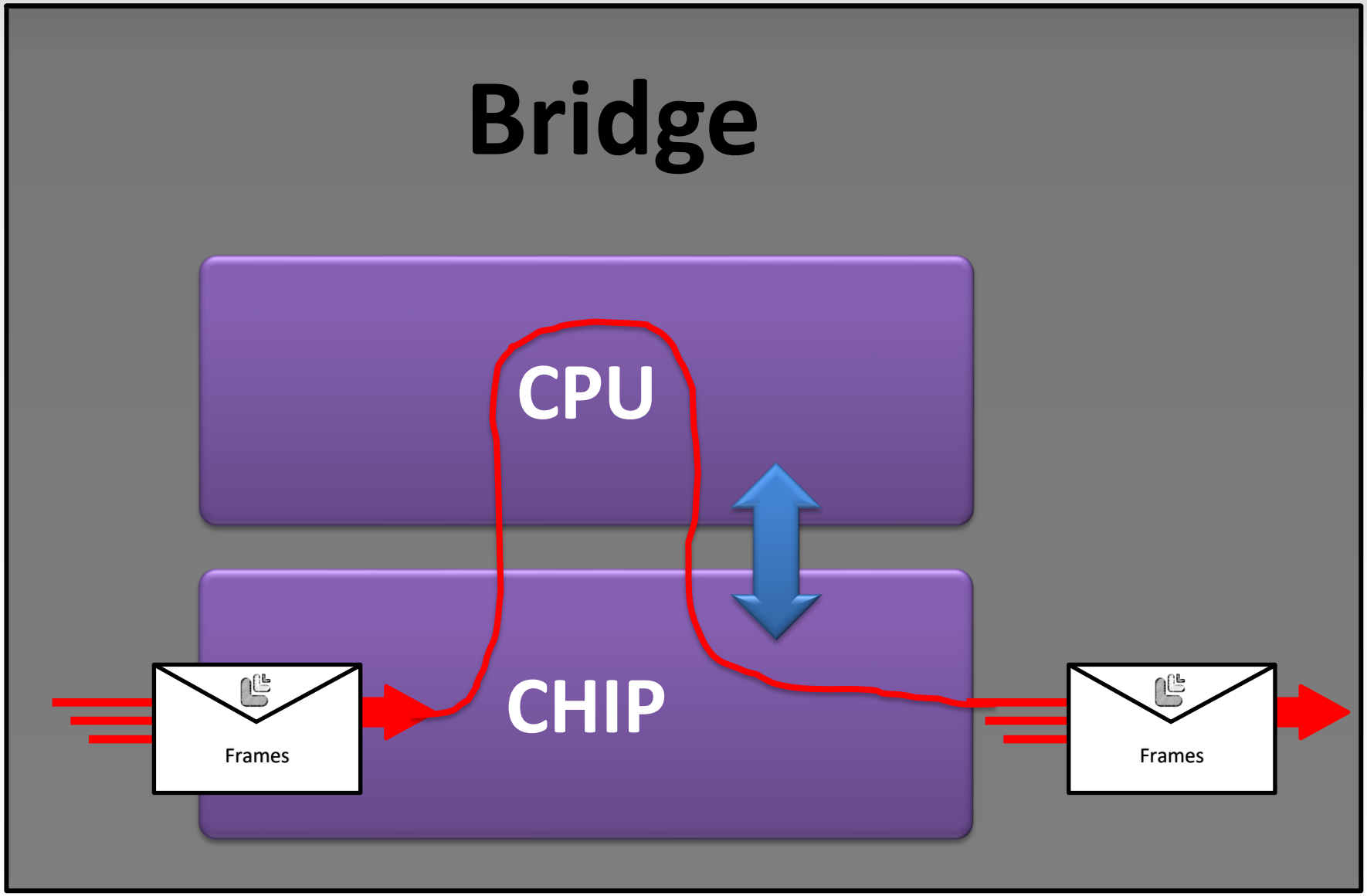
Bridge vs Switch



Bridge vs Switch



Bridge vs Switch



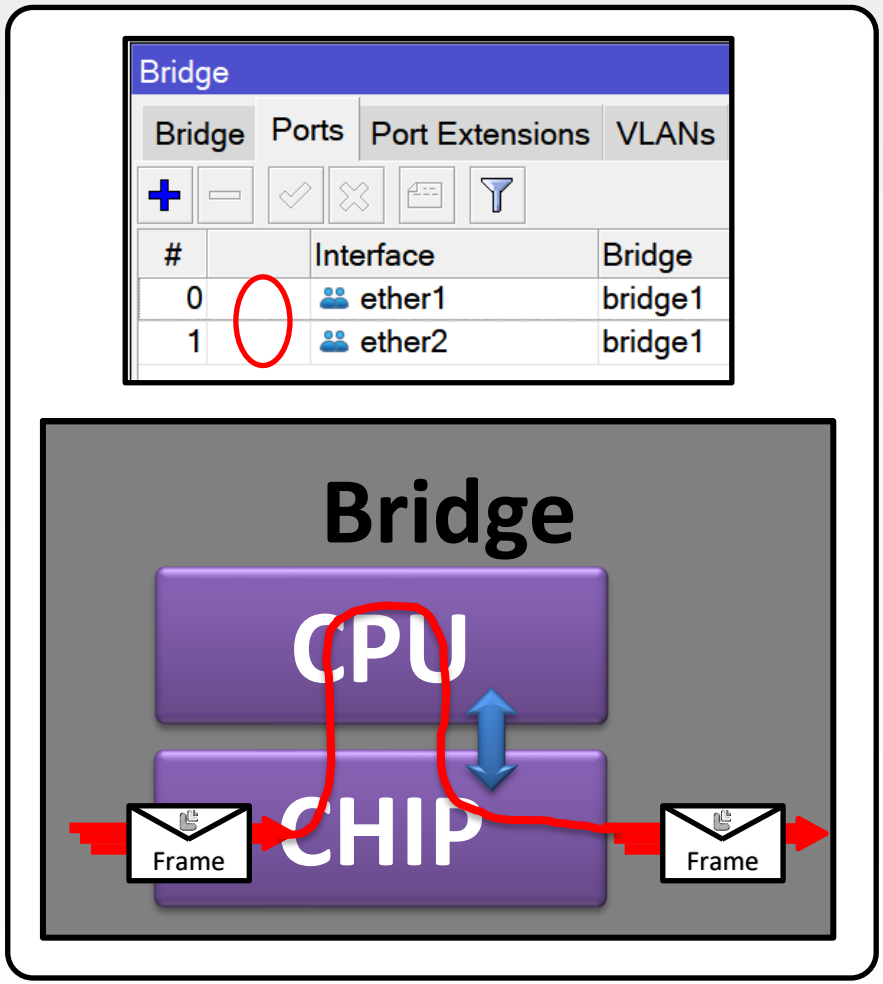
Bridge vs Switch

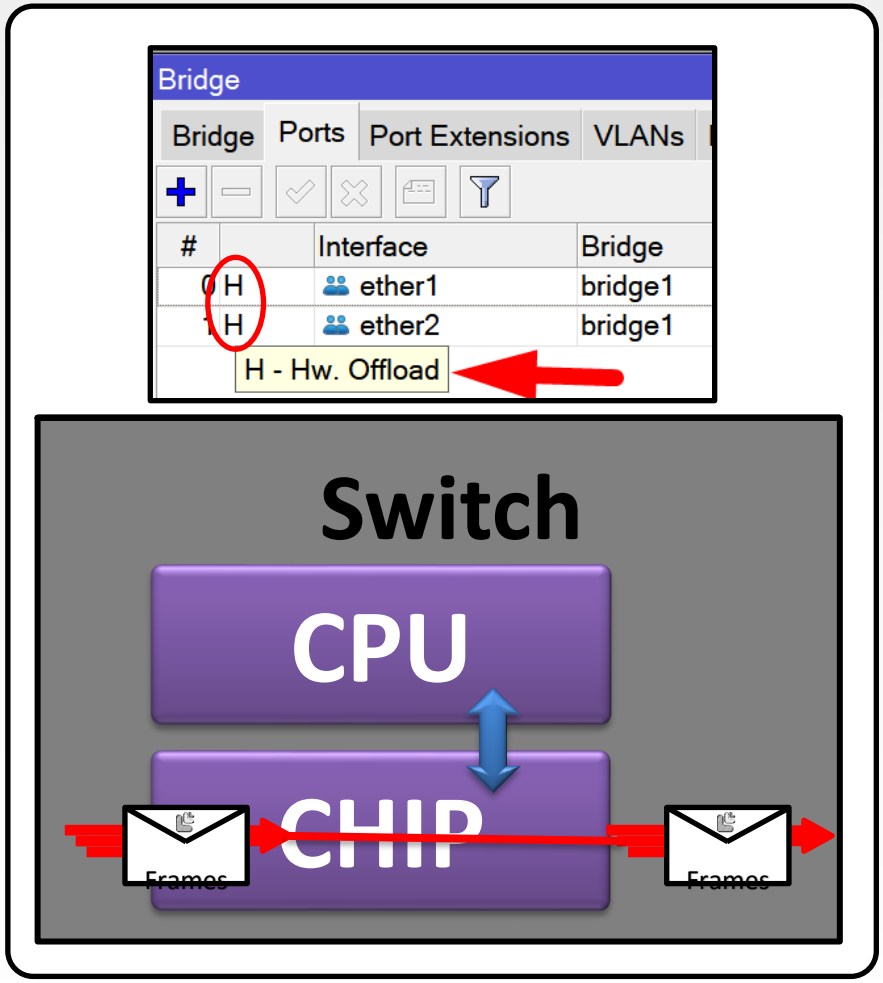
- No RouterOS para usar tanto a função de Bridge quanto a função de Switch precisamos criar uma bridge.

Bridge vs Switch

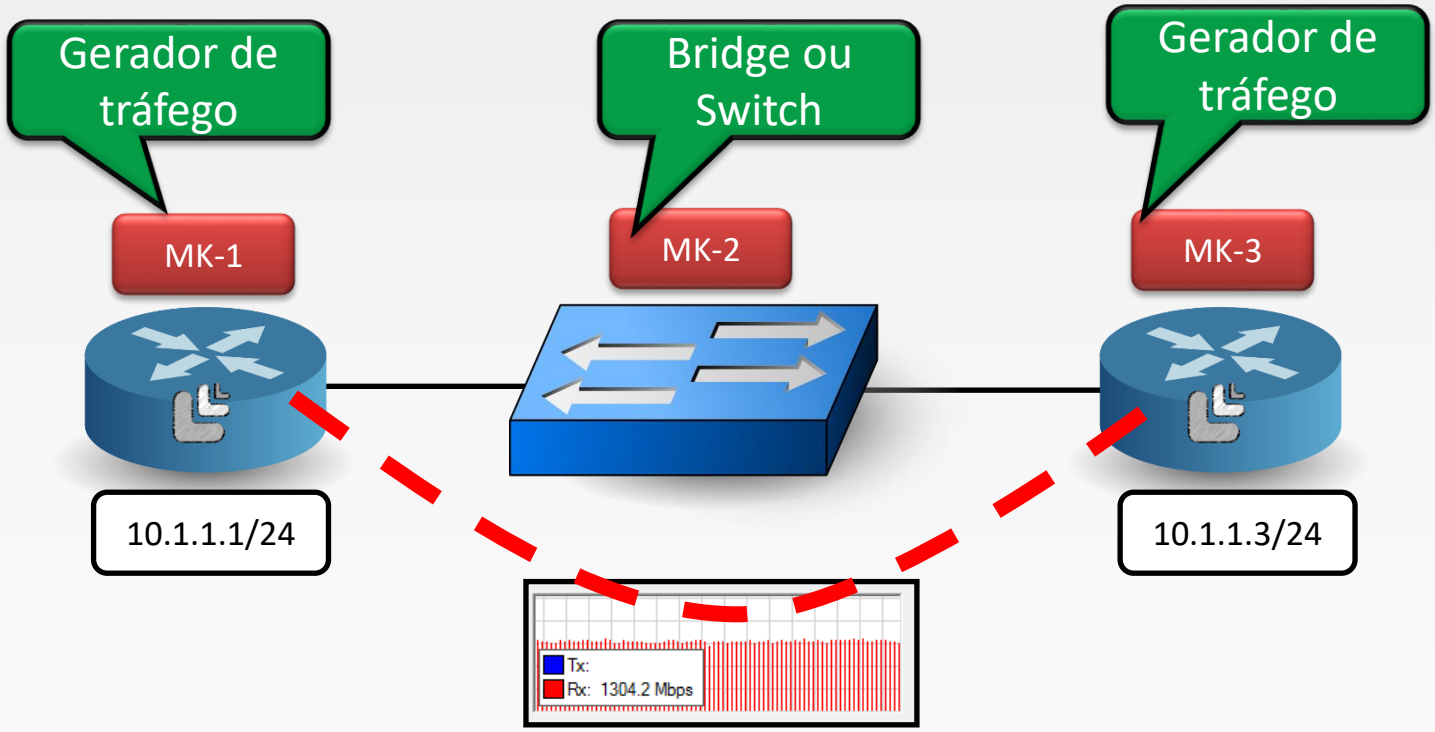
Redes Brasil

- No final das contas para saber se você está usando bridge ou switch você precisa olhar se está com Hardware Offload ativo.





Testes de bancada Bridge e Switch

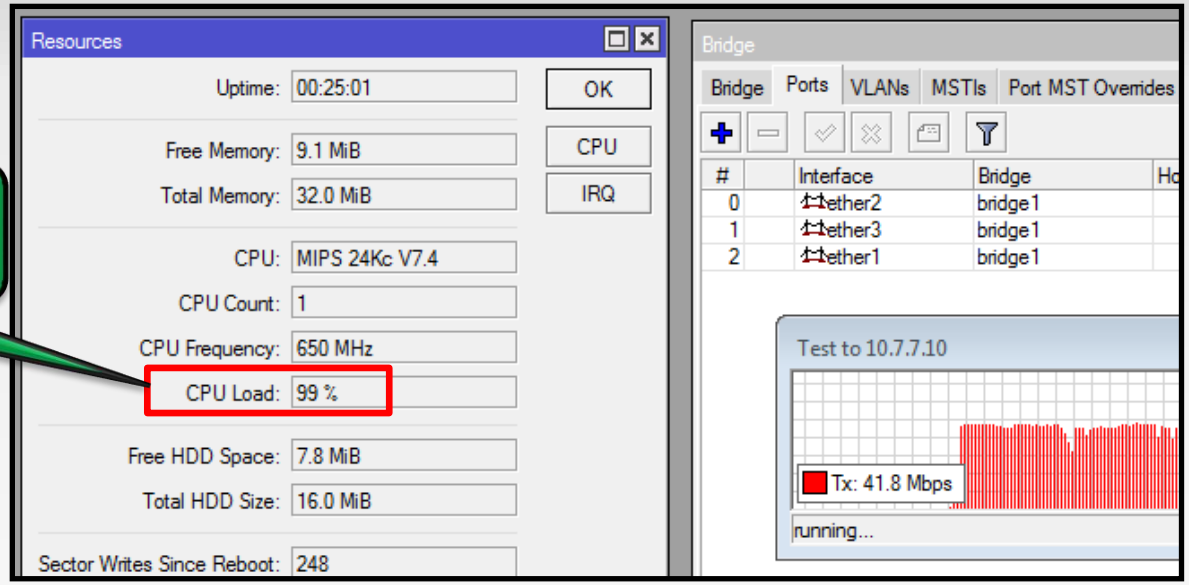


Vídeo com teste de desempenho https://www.youtube.com/watch?v=tNEhExMOJyw

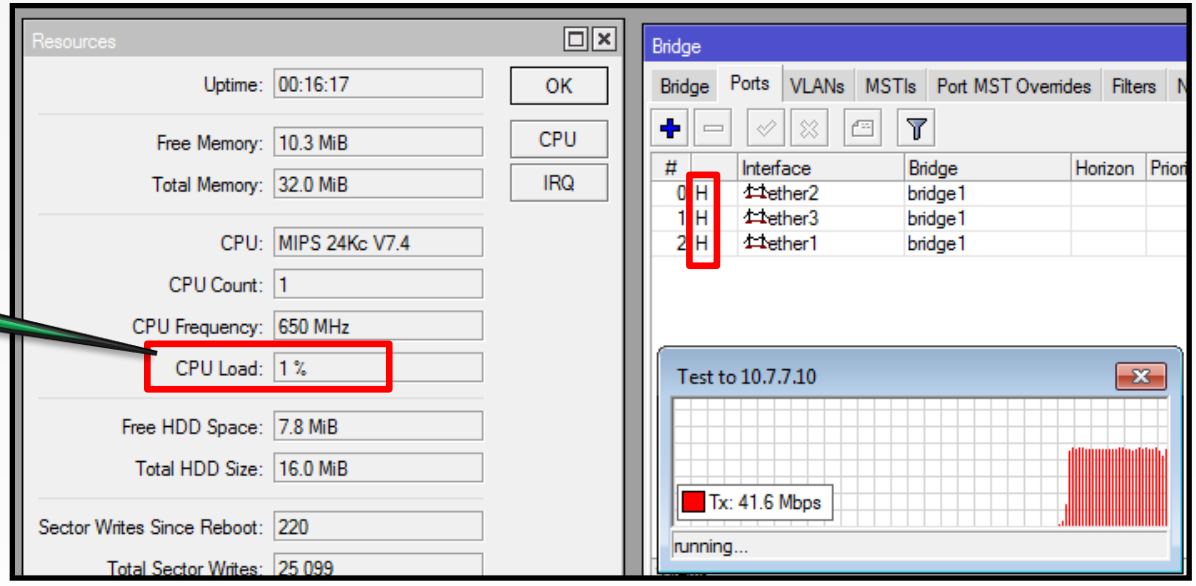
Desempenho

Redes Brasil

Sem hardware-offload

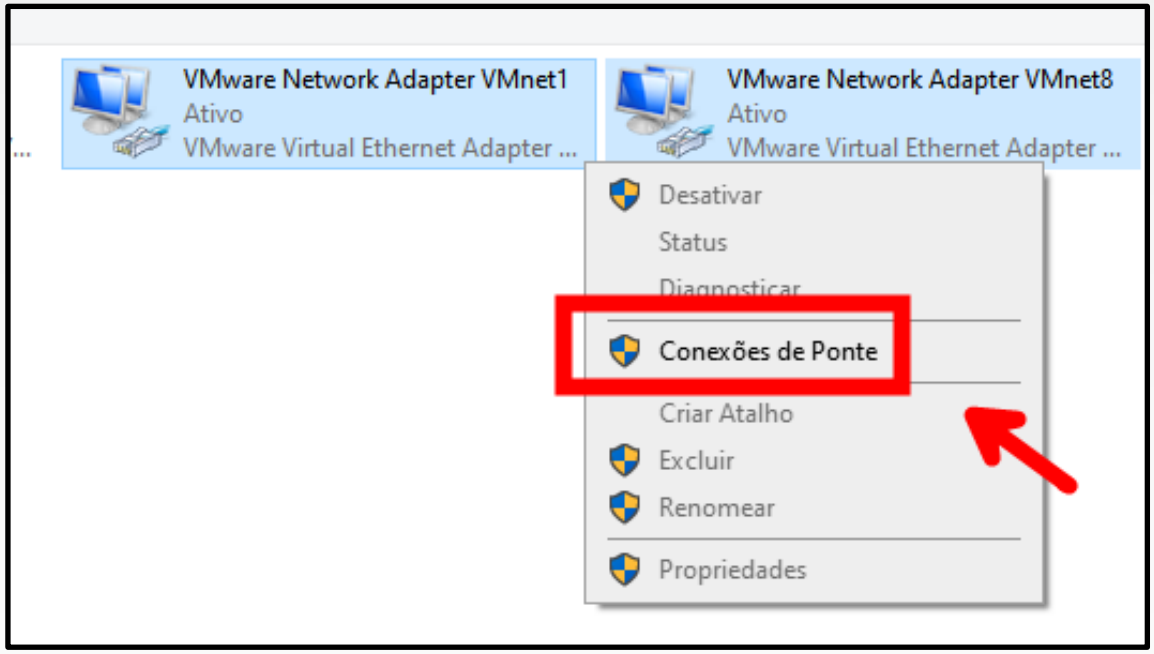


Com hardware-offload

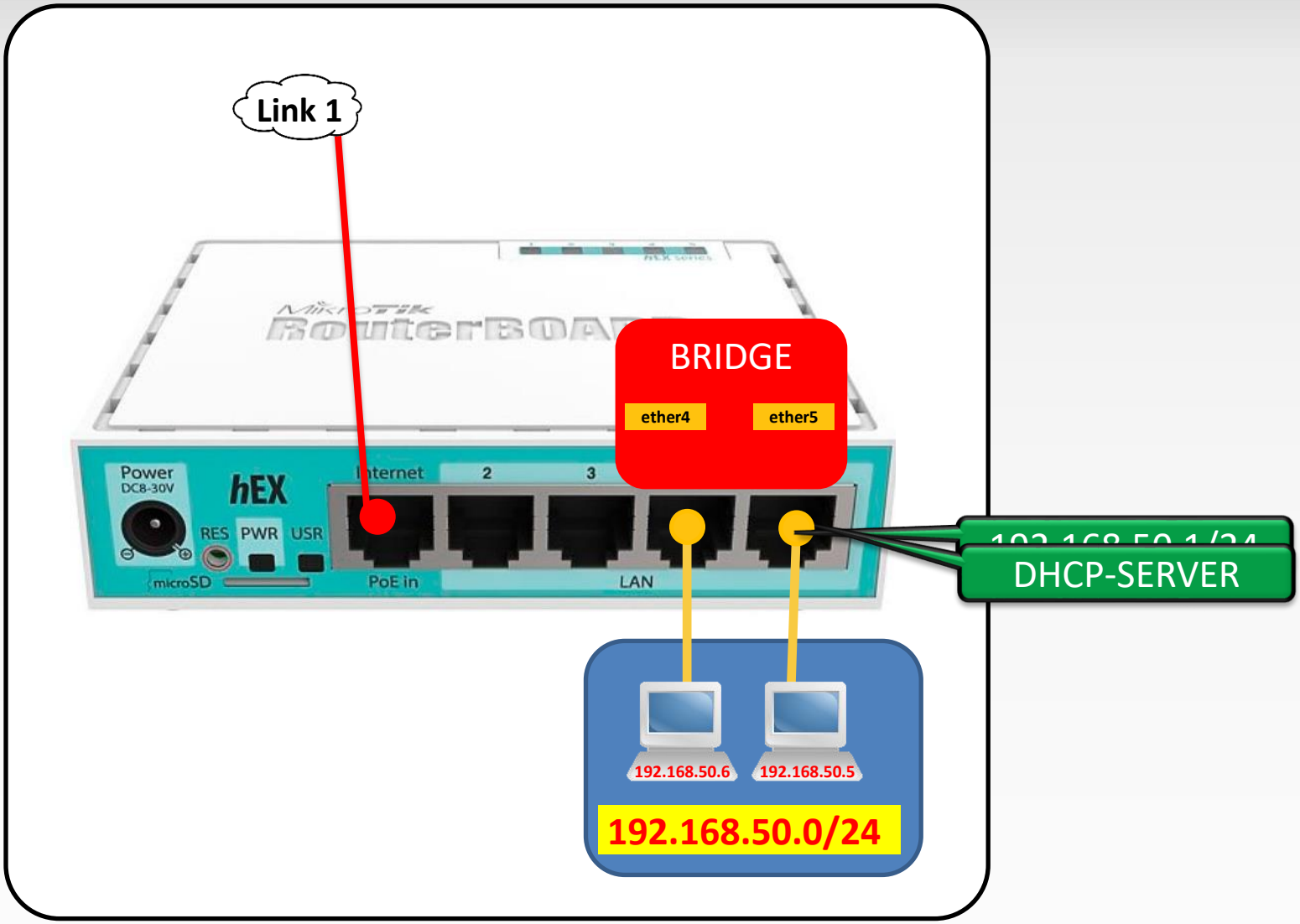


Exemplos de uso somente de Bridge

- CCR da série 1000;
- CHR;
- Windows;
- Linux.



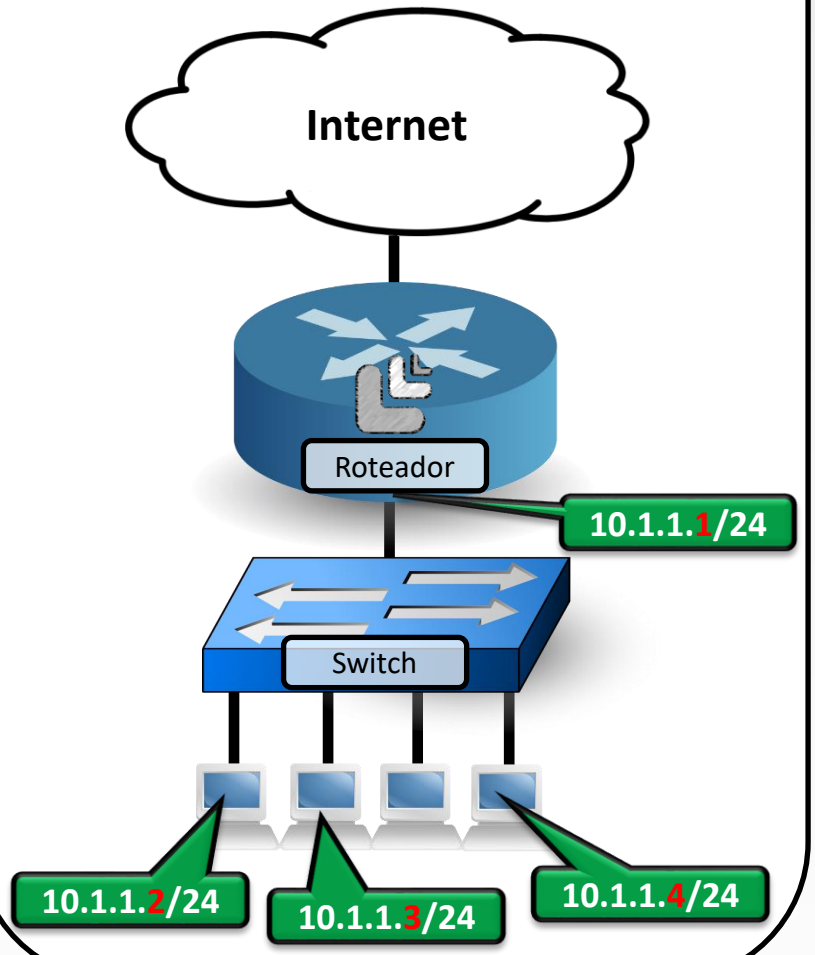
Bridge


Link 1
BRIDGE
ether4
ether5
Power
DC8-30V
hEX
RES
PWR
USR
microSD
Internet
2
3
PoE in
LAN
DHCP-SERVER
192.168.50.6
192.168.50.5
192.168.50.0/24

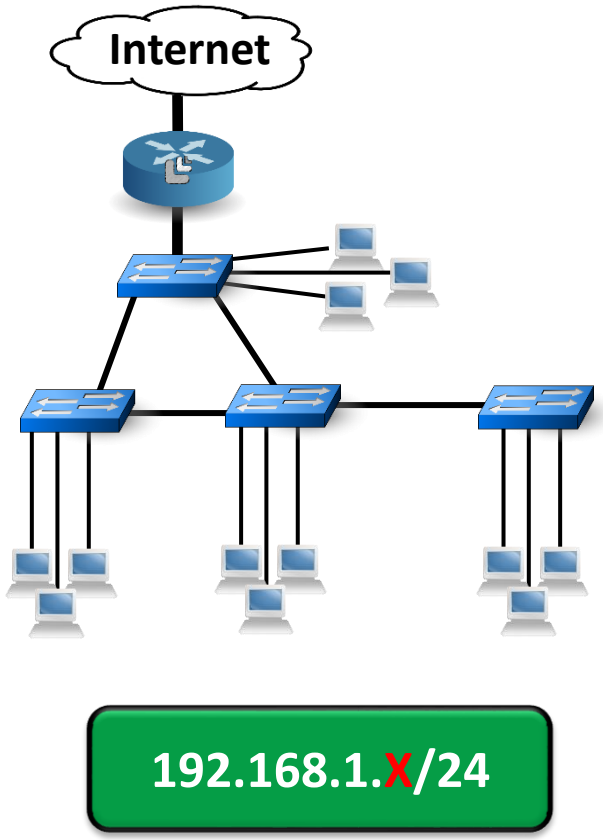
Cenários onde se aplicam switches

Redes Brasil

Cenário 1



Cenário 2



MÓDULO 4 - Roteamento

MÓDULO 4 - Roteamento

- ✓ 4.1 - Oque é, e quando preciso de roteamento;
- ✓ 4.2 - Quando o roteador é realmente necessário?
- ✓ 4.3 - Rota default;
- ✓ 4.4 - Rotas estáticas;
- ✓ 4.5 - ECMP,Check-gateway e Distância;
- ✓ 4.6 - Extras sobre roteamento.

MÓDULO 4.1 – Oque é e quando preciso de roteamento

O que é roteamento

- Roteamento é o processo selecionar o caminho por onde serão **enviados** ou **encaminhados** os pacotes rede;

- Todo host precisa de roteamento para **enviar** seus pacotes;

- Um roteador utiliza o processo de roteamento para **encaminhar** pacotes entre redes distintas.

Rota diretamente conectada

- Sempre que você adiciona um endereço de IP a uma interface, automaticamente irá surgir uma rota diretamente conectada;

- Essa rota informa ao host que para alcançar aquela determinada sub-rede é necessário enviar pacotes através da interface que o IP foi atribuído;

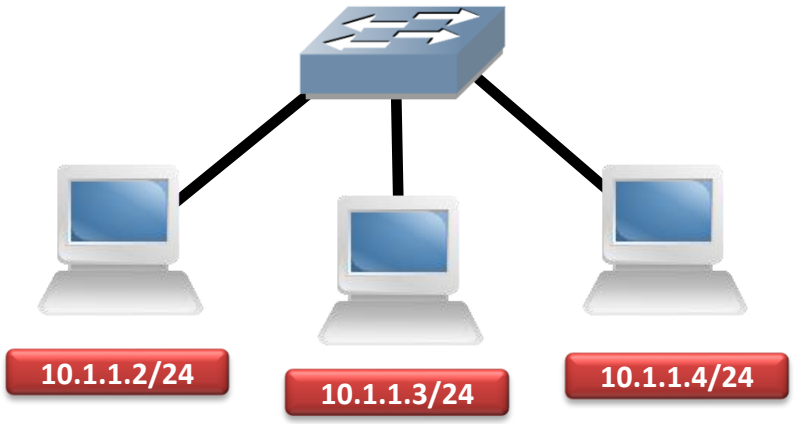
MÓDULO 4.2 – Quando o roteador é realmente necessário ?

Quando preciso de um roteador ?

Redes Brasil

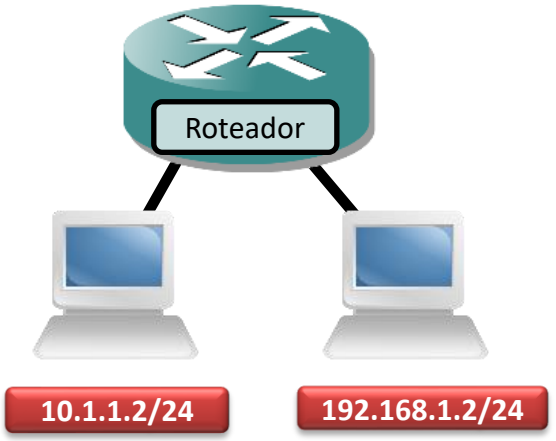
Hosts na mesma sub-rede

Não precisam de um roteador



Hosts em diferentes sub-redes

Precisam de um roteador

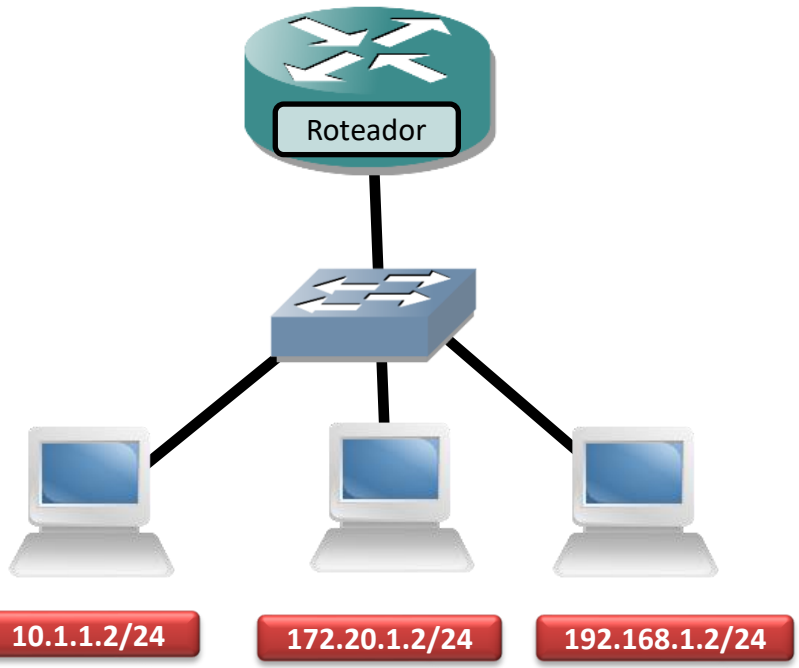


Quando preciso de um roteador ?

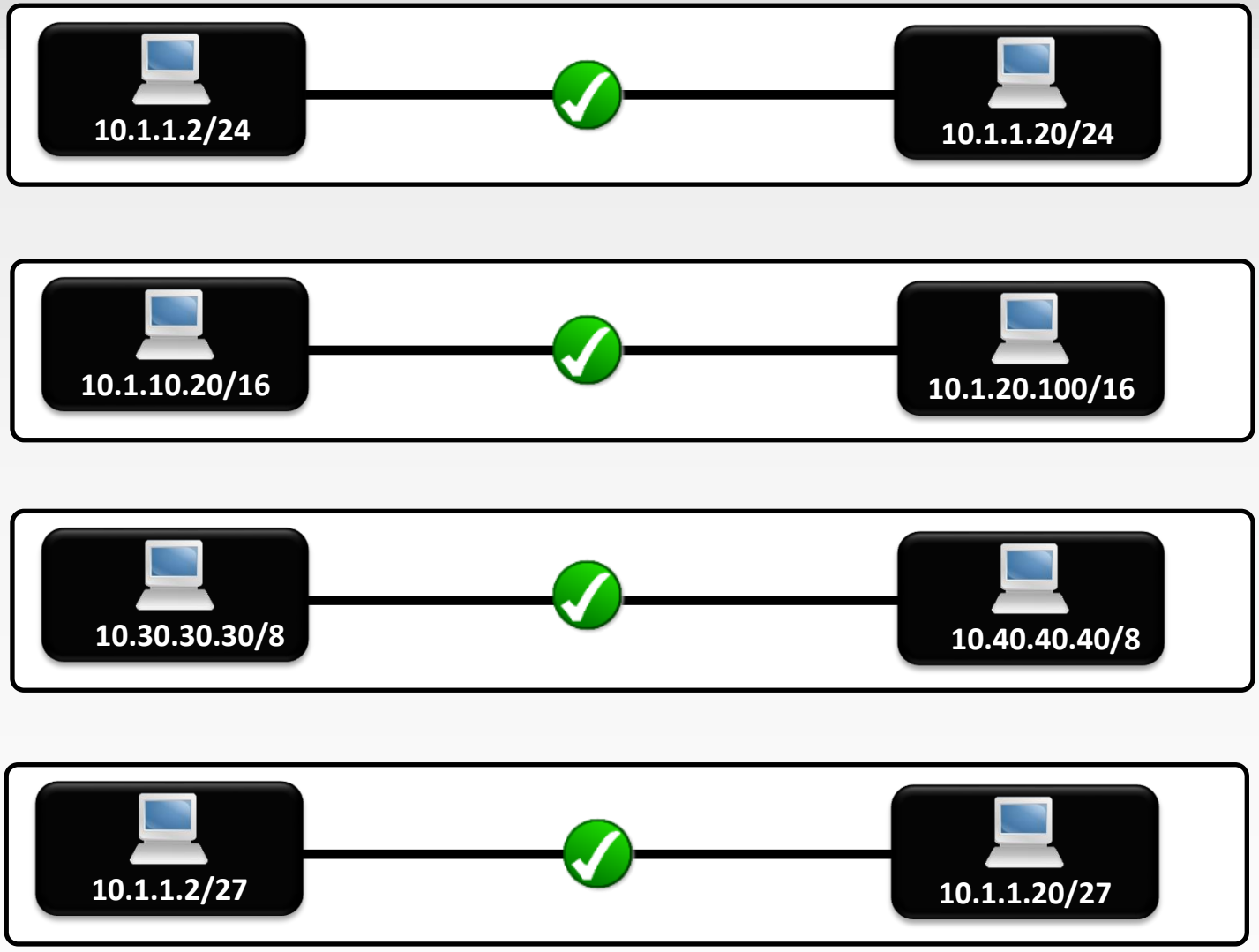
Redes Brasil

Hosts em diferentes sub-redes

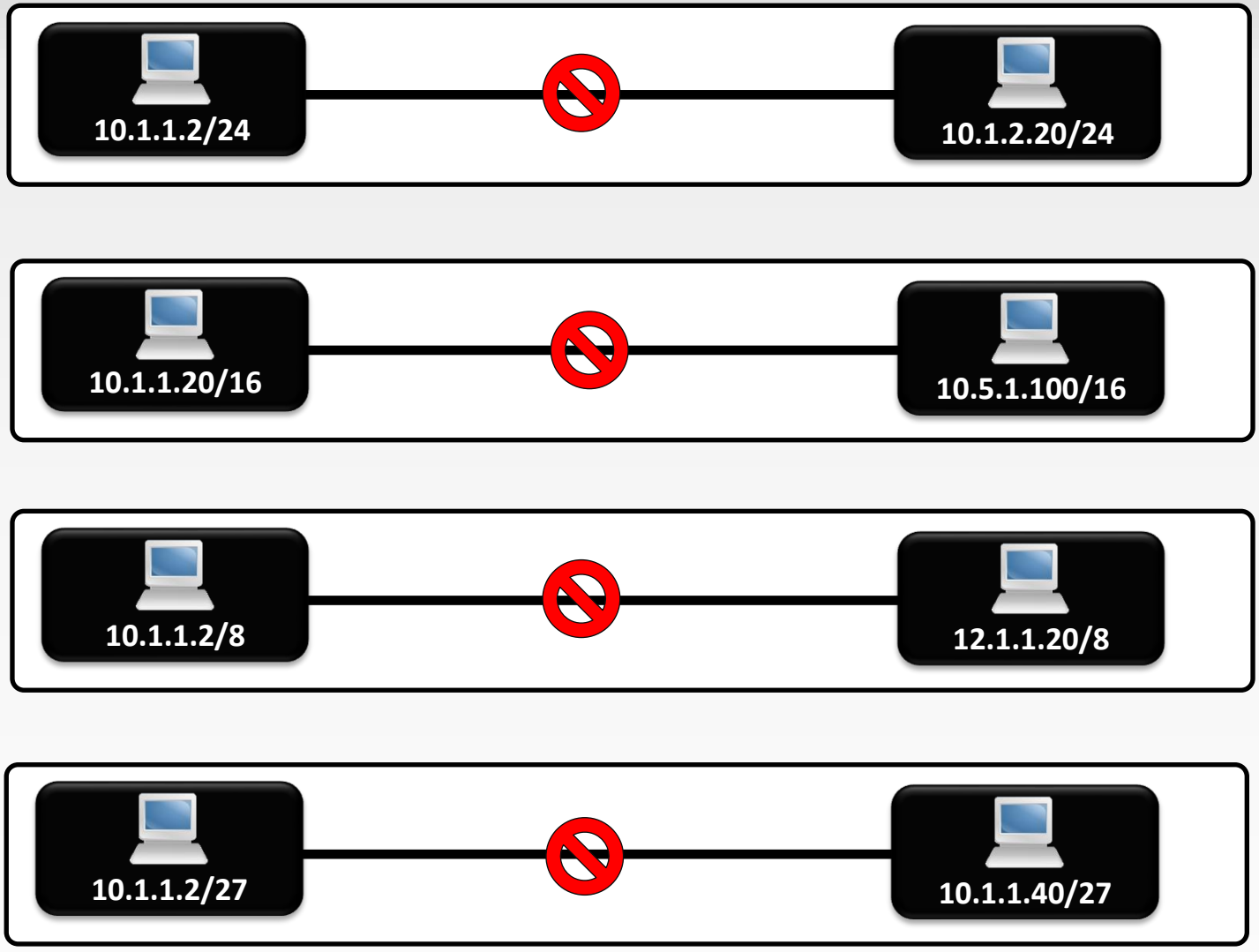
Precisam de um roteador



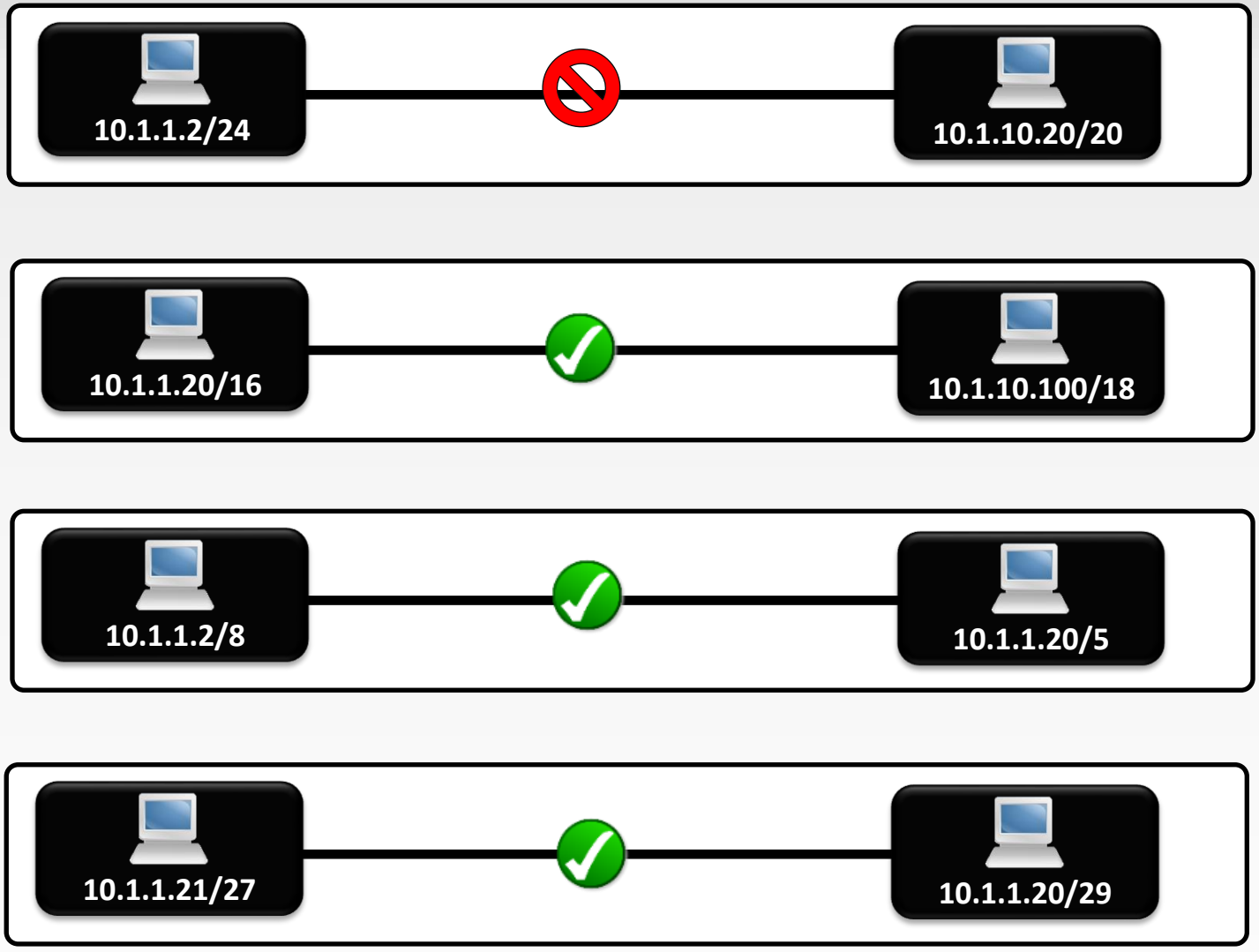
Como saber se dois hosts estão na mesma sub-rede?



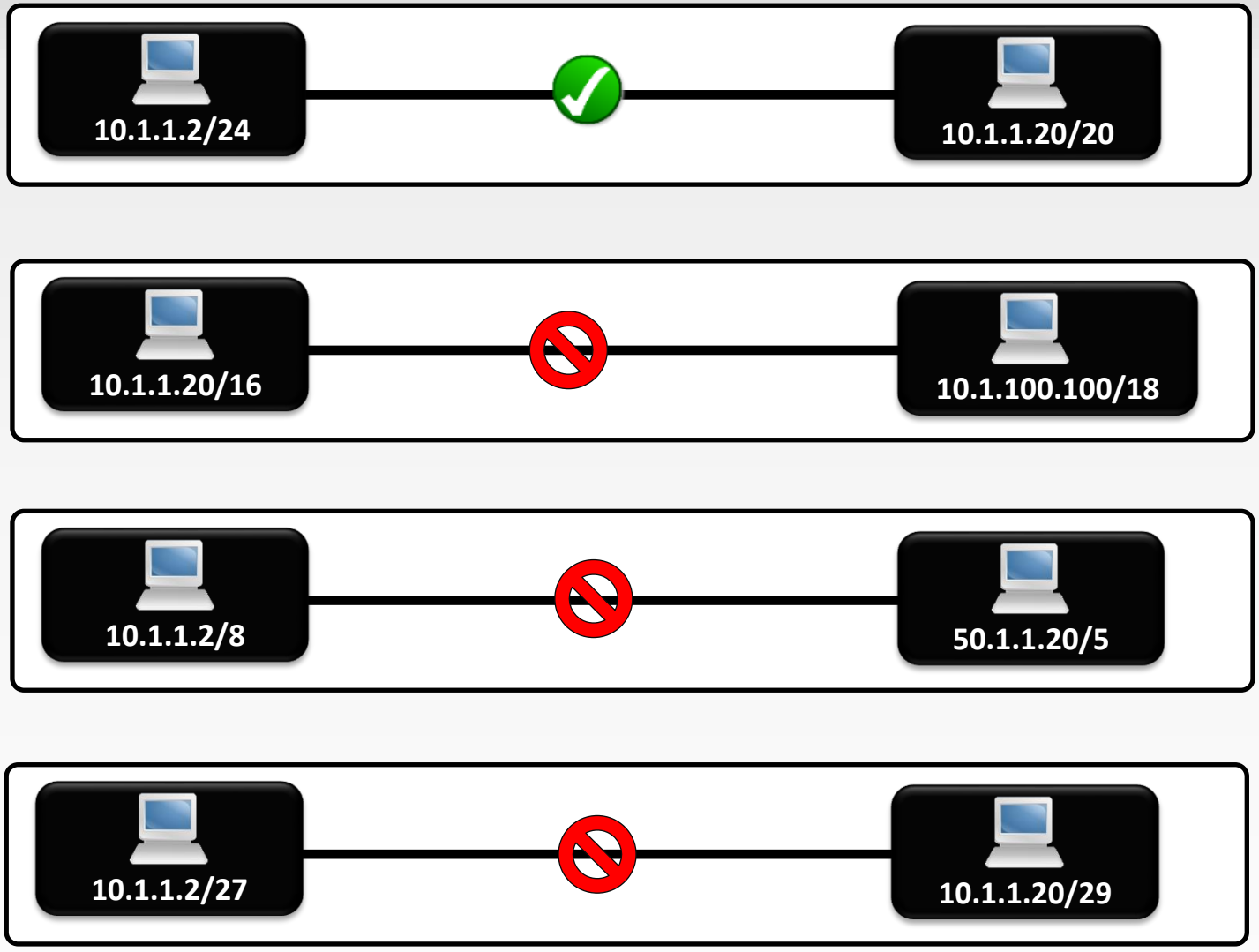
Como saber se dois hosts estão na mesma sub-rede?



Como saber se dois hosts estão na mesma sub-rede?



Como saber se dois hosts estão na mesma sub-rede?



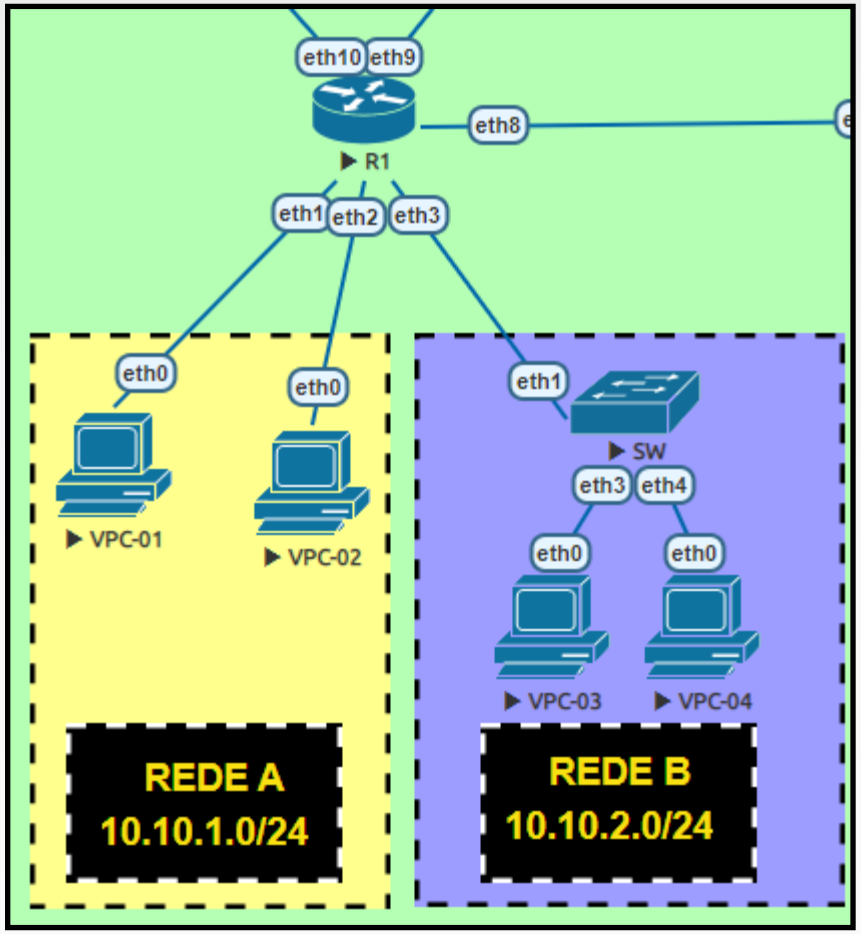
MÓDULO 4.3 - Rota default

Rota default

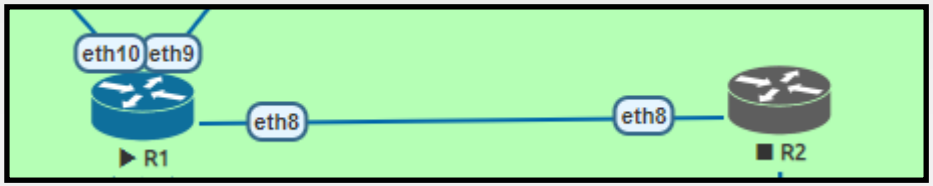
- Rota default é utilizada para enviar pacotes para todos os destinos que não possuírem rotas mais especificas;

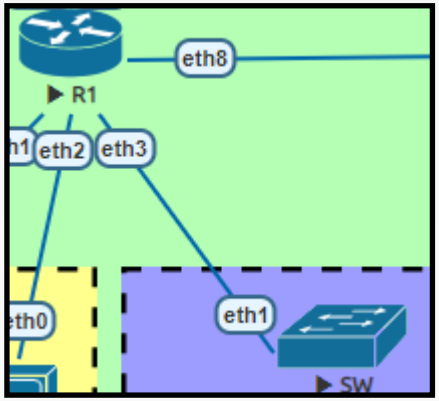
- Normalmente ao fazer a configuração de rede em um dispositivo e informar o gateway, o dispositivo irá criar a famosa rota default;

Duas redes ligadas ao mesmo roteador



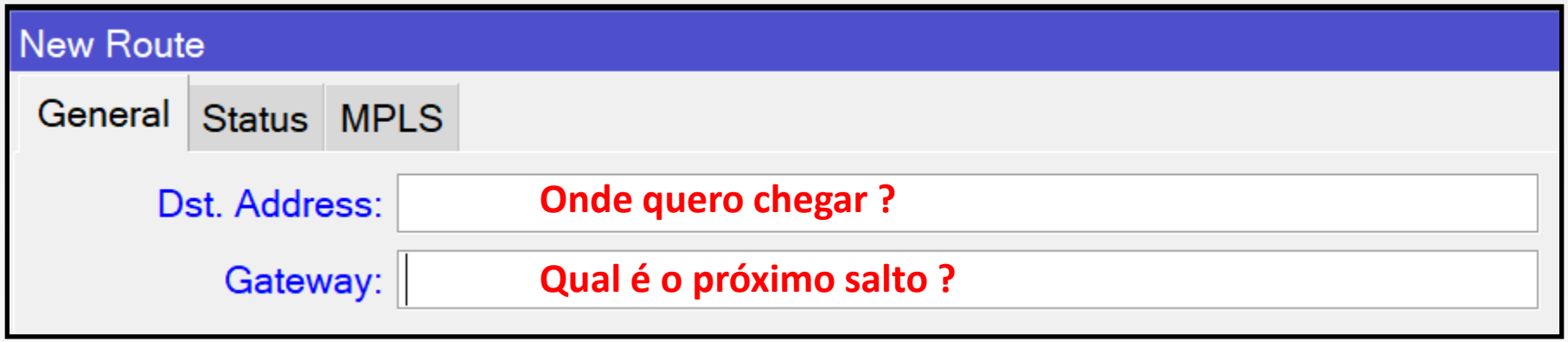
Problemas por falta de gateway



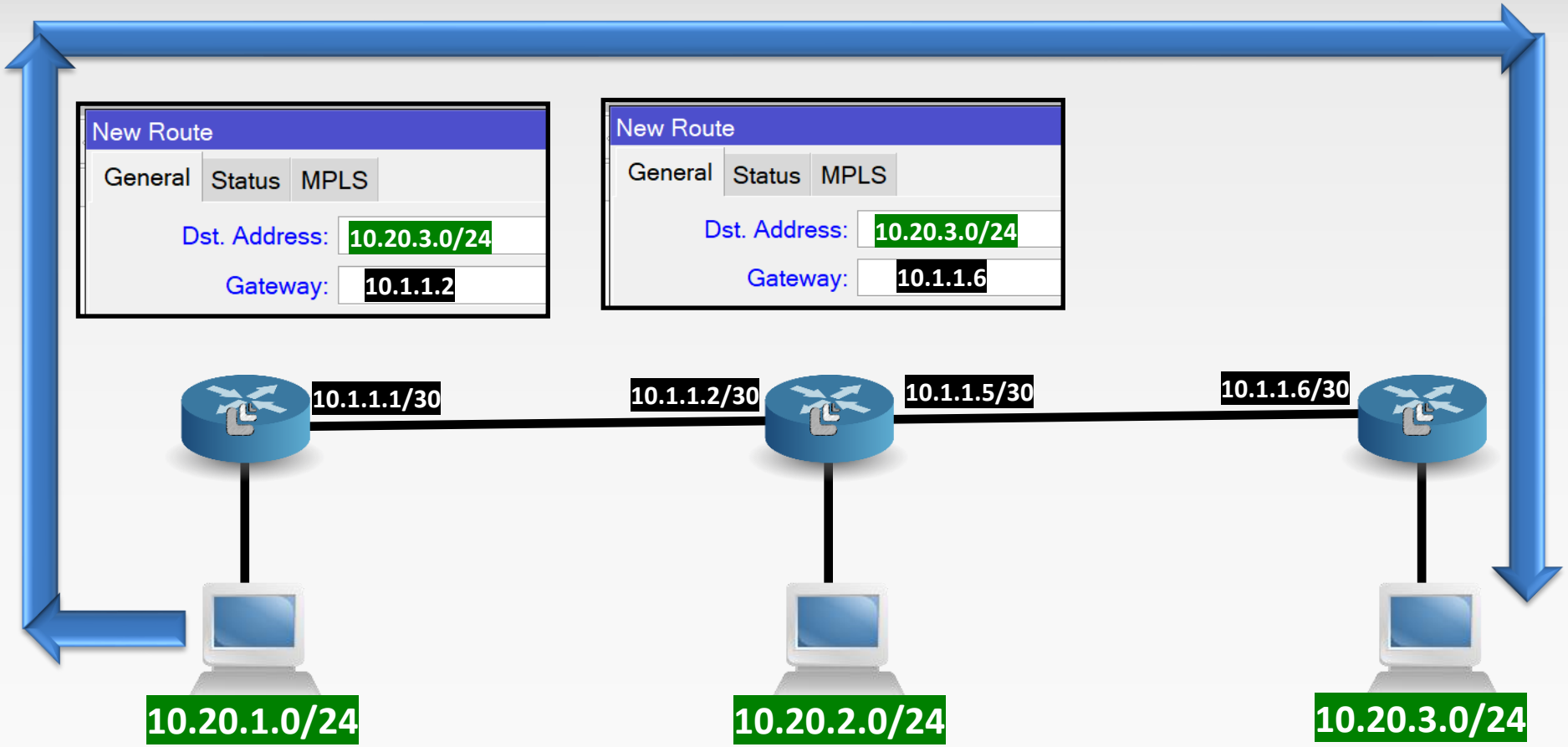


MÓDULO 4.4 - Rotas estáticas

Criando rotas estáticas



Rotas estáticas



Padrão para criar rotas

MikroTik
/ip route add dst-address=10.10.10.0/24 gateway=172.16.1.1

Cisco
ip route 10.10.10.0 255.255.255.0 172.16.1.1

Hauwei
ip route-static 10.10.10.0 255.255.255.0 172.16.1.1

Juniper
set routing-options set static route 10.10.10.0/24 next-hop 172.16.1.1

Linux
ip route add 10.10.10.0/24 via 172.16.1.1

Windows
route ADD 10.10.10.0 MASK 255.255.255.0 172.16.1.1

Como o roteador escolhe a melhor rota ?

- Para decidir qual é o melhor caminho para alcançar um determinado destino o processo de roteamento irá consultar a tabela de roteamento por inteira;

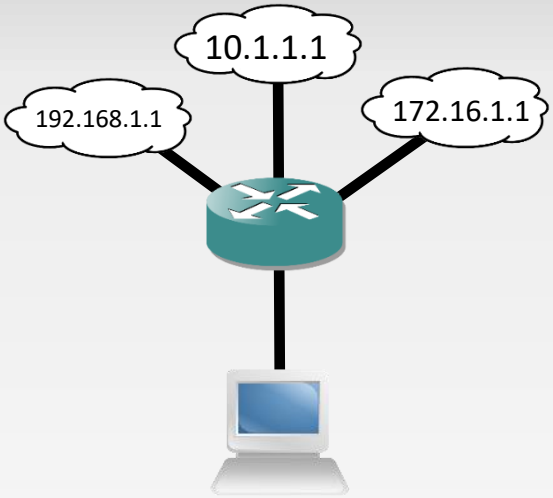
- Se o roteador encontrar mais de uma rota para o destino solicitado ele sempre irá utilizar a **rota mais especifica**;

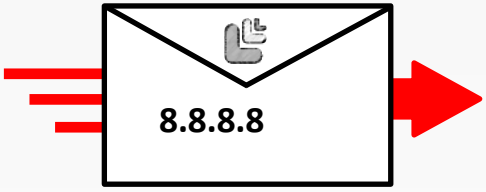
  - A rota defult será utilizada sempre que não houver uma rota mais especifica para o destino.

Tabela de rotas

Dst. Address	Gateway
0.0.0.0/0	192.168.1.1
8.0.0.0/8	10.172.6.1
8.8.0.0/16	10.172.5.1

Desempate na tabela de roteamento



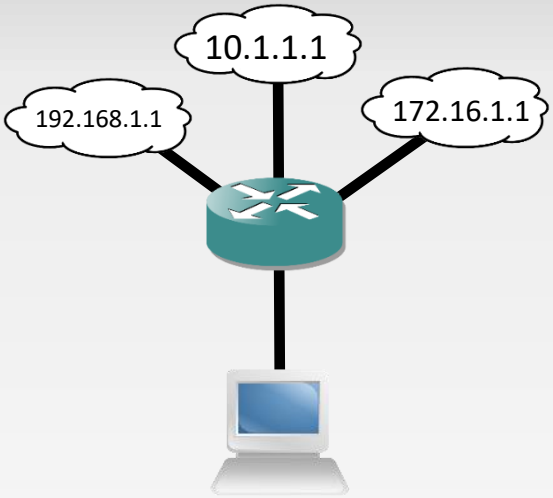


Route List

Routes | Nexthops | Rules | VRF

	Dst. Address	Gateway	Distance
AS	0.0.0.0/0	10.1.1.1 reachable ether1	1
AS	8.8.0.0/16	172.16.1.1 reachable ether3	1
AS	8.8.8.0/24	192.168.1.1 reachable ether2	1

Desempate na tabela de roteamento

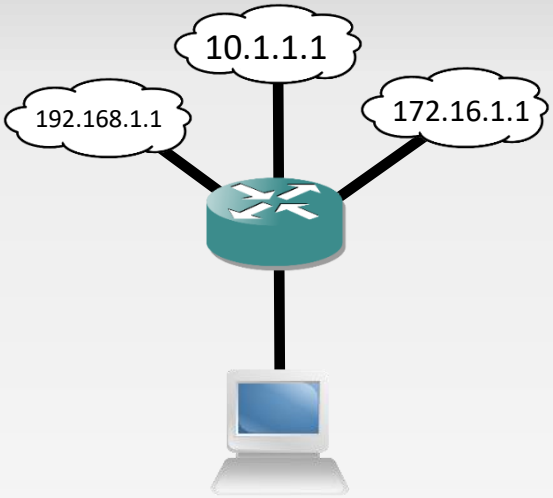


Route List

Routes | Nexthops | Rules | VRF

	Dst. Address	Gateway	Distance
AS	0.0.0.0/0	10.1.1.1 reachable ether1	1
AS	8.8.0.0/16	172.16.1.1 reachable ether3	1
AS	8.8.8.0/24	192.168.1.1 reachable ether2	1

Desempate na tabela de roteamento



Route List

Routes | Nexthops | Rules | VRF

	Dst. Address	Gateway	Distance
AS	0.0.0.0/0	10.1.1.1 reachable ether1	1
AS	10.5.50.0/24	192.168.1.1 reachable ether2	1
AS	10.10.10.0/24	172.16.1.1 reachable ether3	1

Desempate na tabela de roteamento

AS	0.0.0.0/0	200.1.1.1
AS	192.168.50.0/27	10.10.1.100
AS	192.168.50.0/28	10.10.1.150
AS	192.168.50.0/29	10.10.1.200

AS	0.0.0.0/0	200.1.1.1
AS	192.168.50.0/27	10.10.1.100
AS	192.168.50.0/28	10.10.1.150
AS	192.168.50.0/29	10.10.1.200

Entendendo roteamento

DST ADDRESS	GATEWAY
10.20.1.0/24	ether1
10.1.1.0/30	ether2
10.20.2.254	10.1.1.2

DST ADDRESS	GATEWAY
10.20.2.0/24	ether1
10.1.1.0/30	ether2
10.20.1.254	10.1.1.1

Entendendo roteamento

DST ADDRESS	GATEWAY
10.20.1.0/24	ether1
10.1.1.0/30	ether2
10.20.2.0/24	10.1.1.2

DST ADDRESS	GATEWAY
10.20.2.0/24	ether1
10.1.1.0/30	ether2
10.20.1.254	10.1.1.1

Entendendo roteamento

DST ADDRESS	GATEWAY
10.20.1.0/24	ether1
10.1.1.0/30	ether2
10.20.2.0/24	10.1.1.2

DST ADDRESS	GATEWAY
10.20.2.0/24	ether1
10.1.1.0/30	ether2
10.20.1.0/24	10.1.1.1

MÓDULO 4.5 – ECMP, Check Gateway e Distância

ECMP

- Quando duas ou mais rotas apontam para o mesmo destino ou seja, o IP ou rede especificada no Dst. Address é o mesmo, o roteador irá fazer uma espécie de balanceamento de conexões entre as rotas;

- Esse processo é chamados de ECMP (Equal cost multi path);

Distância

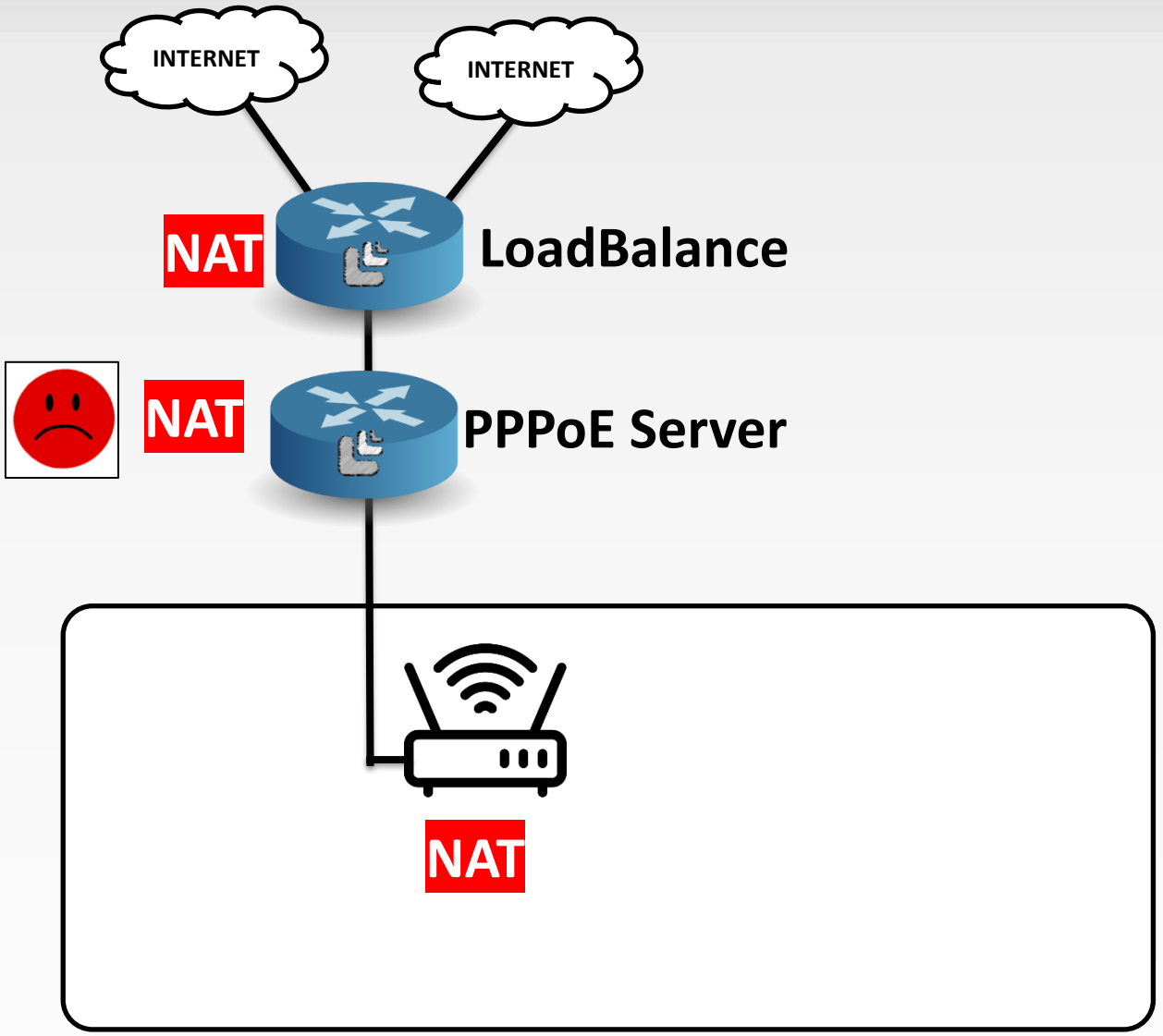
- Quando duas rotas apontam para o mesmo destino ou seja, o IP ou rede especificada no Dst. Address é o mesmo, somente o primeiro critério para desempate de roteamento não vai ser suficiente para que o roteador escolha somente uma das rotas;
- Para ocorrer o desempate precisamos usar o campo distance;
- Quanto menor a distância maior será a prioridade da rota;
- Ao configurar um rota estática o valor padrão é 1;
- Esse campo pode ser alterado para o valores entre 1 e 255.

Check-gateway

- A funcionalidade Check-gateway irá verificar se o gateway é alcançável através de ICMP ou ARP.
- A checagem ocorre a cada 10 segundos.
- Se após duas tentativas seguidas o gateway não responder, ele é considerado inalcançável.
- Após receber uma resposta o gateway novamente é considerado alcançável.

MÓDULO 4.6 – Extras sobre roteamento

Roteamento para eliminar NAT desnecessário



Tipos de rotas

Terminal <3>

```
[user@R1-EMPRESA_X-MATRIZ-BORDA] > ip/route/print detail
Flags: D - dynamic; X - disabled, I - inactive, A - active;
c - connect, s - static, r - rip, b - bgp, o - ospf, d - dhcp, v - vpn, m - modem, y - copy; H - hw-offloaded;
+ - ecmp
```

/ip/route/print detail

D - dynamic
X - disabled
I - inactive
A - active
c - connect
s - static
r - rip
b - bgp
o – ospf
d – dhcp
v - vpn
m - modem
y - copy
H - hw-offloaded
+ - ecmp

Routing Fantazy

Terminal <4>

```
[user@R1-EMPRESA_X-MATRIZ-BORDA] > routing/fantasy/add
```

/routing fantasy

add count=10 dst-address=0.0.0.0/0 gateway=10.1.1.0/30 prefix-length=0-32