

# Camada de Rede: NAT+DHCP+DNAT

Trabalho 02 (2024.2)

Universidade de Brasília

Fundamentos de Redes de Computadores - Professor Tiago Alves

## Alunos

Matrícula	Aluno
19/0104821	Daniel Rocha Oliveira
18/0108011	Guilherme Brito Vilas Boas
20/0043536	Silas Neres de Souza

## Visão Geral

### Sistema Operacional

- Sistema Operacional: Open BSD
- Justificativa: Sistema operacional utilizado pelo professor durante suas aulas. Apesar das dificuldades, visando uma maior nota no trabalho, optamos por usar o Open BSD para a confecção do trabalho 2.

## Introdução

Este documento descreve o processo de criação de uma rede local (LAN) utilizando um computador inutilizado com OpenBSD como roteador e firewall, com a configuração de DHCP, NAT e DNAT.

## Visão Geral da Topologia e Configuração Inicial

A topologia de rede a ser criada será a seguinte:

```
[ comp1 ] ---- udav0 [ OpenBSD ] re0 --- [ internet ]
```

## Configuração da interface externa

O OpenBSD está configurado para obter o endereço IP da rede externa (LDS) via DHCP. Para isso, edite o arquivo /etc/hostname.re0:

```
echo 'inet autoconf' > /etc/hostname.re0
```

Esta configuração permite que o OpenBSD obtenha o endereço IP, gateway e servidores DNS automaticamente ao inicializar a interface.

## Configuração da interface interna

Para configurar o IP estático da interface LAN, precisamos editar o arquivo `/etc/hostname.udav0`.

O IP 172.24.0.1 será atribuído à interface, com máscara de sub-rede /16 e sem gateway configurado:

```
echo 'inet 172.24.0.1 255.255.0.0 NONE' > /etc/hostname.udav0
```

---

## Permissão de encaminhamento de pacotes entre as interfaces

Por padrão, o OpenBSD, como a maioria dos sistemas operacionais, não encaminha pacotes entre interfaces de rede. Isso é feito para garantir a segurança e evitar que o sistema atue como roteador sem ser explicitamente configurado para isso.

Para permitir o roteamento entre as interfaces, precisamos habilitar o encaminhamento de pacotes IPv4:

```
sysctl net.inet.ip.forwarding=1  
echo 'net.inet.ip.forwarding=1' >> /etc/sysctl.conf
```

## Configuração DHCP

O DHCP (Dynamic Host Configuration Protocol) é um protocolo utilizado para atribuir endereços IP e outras configurações de rede (como o gateway e servidores DNS) automaticamente aos dispositivos na rede.

Para configurar o serviço DHCP, precisamos editar o arquivo `/etc/dhcpd.conf`, definindo o escopo da rede, o servidor DNS e o gateway. Também será fixado o endereço IP para a "Máquina 1" (`maq_teste`) (172.24.0.15).

```
subnet 172.24.0.0 netmask 255.255.0.0 {  
    option domain-name-servers 192.168.133.1;  
    option routers 172.24.0.1;  
    range 172.24.0.10 172.24.255.254;  
    host maq_teste {  
        fixed-address 172.24.0.15;  
        hardware ethernet <endereco_mac_maquina_teste>;  
    }  
}
```

A configuração do arquivo `/etc/dhcpd.conf` no servidor DHCP define a rede 172.24.0.0/16, atribuindo endereços IP no intervalo 172.24.0.10 a 172.24.255.254 para os dispositivos da rede interna. O servidor DNS é configurado para 192.168.133.1, e o gateway padrão é definido como 172.24.0.1, o IP da interface LAN do roteador OpenBSD. Além disso, a "Máquina 1" recebe um IP fixo (172.24.0.15) com base no seu endereço MAC, garantindo que essa máquina tenha sempre o mesmo IP ao se conectar à rede.

Após a configuração, precisamos iniciar o serviço DHCP com os comandos:

```
rcctl enable dhcpd  
rcctl start dhcpd
```

As leases DHCP atribuídas podem ser verificadas no arquivo `/var/db/dhcpd.leases`:

```
cat /var/db/dhcpd.leases
```

Após a configuração, a máquina teste conectada à LAN deve receber o IP fixado (172.24.0.15) e ser capaz de se comunicar com o roteador recém configurado.

Para testes:

- Podemos verificar se a máquina teste recebeu o IP definido pela configuração do DHCP, com `ifconfig`.
- Podemos verificar a existência de uma rota entre a máquina local e o roteador com o comando:

```
ping 172. 24. 0. 1
```

## Configuração de NAT (Network Address Translation)

NAT (Network Address Translation) é uma técnica que traduz endereços de rede, permitindo que uma rede privada use endereços IP internos. O NAT é normalmente implementado em roteadores, que são dispositivos que conectam redes. Ele funciona substituindo o endereço IP de origem por um endereço IP público do roteador, quando um dispositivo da rede privada envia dados para a rede pública.

Para configurar o NAT, iremos utilizar PF (O PF é um filtro de pacotes com estado licenciado BSD, uma peça central de software para firewall).

Para configurar esse filtro de pacotes, devemos editar o arquivo `/etc/pf.conf` para configurar as regras de NAT:

```
Definição da interface externa (WAN) e interna (LAN)
ext_if="re0" # Interface de rede externa conectada à WAN
int_if="udav0" # Interface de rede interna conectada à LAN
```

Regras de NAT (Network Address Translation)

```
match out on $ext_if inet from $int_if:network to any nat-to ($ext_if)
# Tradução de endereço de origem (NAT) para pacotes saindo da rede interna para a
externa,
# usando o IP da interface externa
pass in on $int_if from $int_if:network to any keep state
# Permite pacotes de entrada na interface interna (LAN), mantendo o estado das
conexões
pass out on $ext_if from any to any keep state
# Permite pacotes de saída da interface externa (WAN), mantendo o estado das conexões
```

Aplique as regras de NAT com o comando:

```
pfctl -f /etc/pf.conf
```

Essas regras permitem que as máquinas na rede LAN (172.24.X.X) acessem a Internet, fazendo NAT através da interface `re0`.

Para testes:

- Verificar conectividade com o roteador externo (DNS ou gateway)
  - Execute o comando `ping` para verificar se a rede interna consegue alcançar o roteador do laboratório ou a rede externa.

```
ping 192. 168. 133. 1
```

- Testar acesso à Internet
  - o Execute o comando curl para verificar se é possível acessar a Internet a partir de um dispositivo na rede interna. O exemplo abaixo tenta acessar a página inicial do Google.

```
curl www.google.com
```

## Configuração de DNAT (Destination Network Address Translation)

DNAT (Destination Network Address Translation), comumente utilizado em port forwarding, é uma técnica de NAT onde o endereço de destino dos pacotes de rede é alterado. Essa técnica é frequentemente usada para redirecionar o tráfego de uma porta específica em um IP público para um IP interno em uma rede privada. Por exemplo, quando um pacote chega em um roteador na porta 80 de seu IP público, o roteador pode redirecionar esse tráfego para um servidor interno na rede local (LAN) que está ouvindo na mesma porta.

Para redirecionar o tráfego da porta 80 da interface externa (re0) para a máquina de teste na porta 8080, adicionamos a seguinte regra de DNAT no arquivo /etc/pf.conf:

```
pass in on $ext_if inetproto tcp from any to ($ext_if) port 80 rdr-to 172.24.0.15 port 8080
```

- Esta regra redireciona o tráfego TCP destinado à porta 80 para o IP 172.24.0.15 na porta 8080.
- Para testar a configuração do DNAT, podemos preparar o seguinte SETUP:
- No roteador, inicie um servidor de escuta na porta 80:

```
nc -l 80
```

- Na máquina de teste (conectada na rede interna), inicie um servidor de escuta na porta 8080:

```
nc -l 8080
```

Na máquina externa (no laboratório), use o comando telnet para testar a conexão:

```
telnet <IP que re0 recebeu> 80
```

O tráfego da porta 80 será redirecionado para a máquina de teste na porta 8080.

## Limitações Conhecidas

Pouca disponibilidade de máquinas físicas para configuração e testes.

Limitações físicas no adaptador de rede, mal contato e pouca disponibilidade para muitos alunos o que leva necessitar da compra.

Configuração do IP estático é sensível ao MAC da máquina de teste, logo, sempre que há mudança no MAC é necessário mudar as configurações.

## Referências

OpenBSD PF - Getting Started - Disponível em: <https://www.openbsd.org/faq/pf/config.html>

OpenBSD FAQ - Networking - Disponível em: <https://www.openbsd.org/faq/faq6.html>

OpenBSD PF - Building a Router - Disponível em: <https://www.openbsd.org/faq/pf/example1.html>

Materiais de Aula disponibilizados pelo Professor - Disponível no Moodle da Disciplina