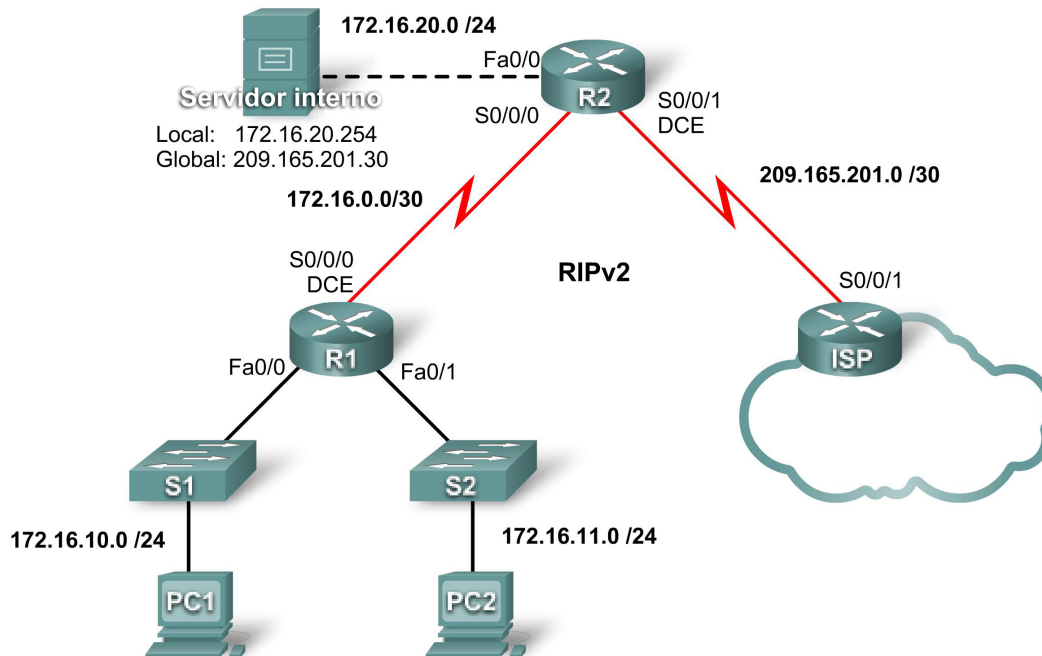


## Laboratório 7.4.3: Identificação e solução de problemas de DHCP e NAT

### Diagrama de topologia



### Tabela de endereçamento

| Dispositivo | Interface | Endereço IP   | Máscara de sub-rede |
|-------------|-----------|---------------|---------------------|
| R1          | S0/0/0    | 172.16.0.1    | 255.255.255.252     |
|             | Fa0/0     | 172.16.10.1   | 255.255.255.0       |
|             | Fa0/1     | 172.16.11.1   | 255.255.255.0       |
| R2          | S0/0/0    | 172.16.0.2    | 255.255.255.252     |
|             | S0/0/1    | 209.165.201.1 | 255.255.255.252     |
|             | Fa0/0     | 172.16.20.1   | 255.255.255.0       |
| ISP         | S0/0/1    | 209.165.201.2 | 255.255.255.252     |

### Objetivos de aprendizagem

Após concluir este laboratório, você será capaz de:

- Prepare a rede.
- Carregue roteadores com scripts.
- Localize e corrija todos os erros de rede.
- Documentar a rede corrigida.

## Cenário

Os roteadores, R1 e R2, da sua empresa foram configurados por um engenheiro de rede sem experiência. Vários erros na configuração resultaram em problemas de conectividade. Seu chefe lhe pediu para solucionar problemas, corrigir os erros de configuração e documentar seu trabalho. Com seus conhecimentos de DHCP, NAT e métodos de teste padrão, identifique e corrija os erros. Certifique-se de que todos os clientes tenham total conectividade. O ISP foi configurado corretamente.

Assegure-se de que a rede dê suporte ao seguinte:

1. O roteador R2 deve funcionar como o servidor DHCP para as redes 172.16.10.0/24 e 172.16.11.0/24 conectadas a R1.
2. Todos os PCs conectados a R1 devem receber um endereço IP na rede correta via DHCP.
3. O tráfego das redes locais R1 que entram pela interface Serial 0/0/0 em R2 e saem pela interface Serial 0/0/1 em R2 devem receber a tradução NAT com um conjunto de endereços fornecidos pelo ISP.
4. O servidor interno deve ser alcançável fora das redes utilizando o endereço IP 209.165.201.30 e dentro das redes utilizando o endereço 172.16.20.254

## Tarefa 1: Preparar a rede

**Etapas 1:** Cabear uma rede de maneira semelhante à presente no diagrama de topologia.

**Etapas 2:** Apagar todas as configurações existentes nos roteadores.

**Etapas 3:** Importar as configurações abaixo.

### R1

```
hostname R1
!
enable secret class
!
no ip domain lookup
!
interface FastEthernet0/0
 ip address 172.16.10.1 255.255.255.0
 ip helper-address 172.16.0.2
 no shutdown
!
interface FastEthernet0/1
 ip address 172.16.11.1 255.255.255.0
 no shutdown
!
interface Serial0/0/0
 ip address 172.16.0.1 255.255.255.252
 clock rate 125000
 no shutdown
!
router rip
 version 2
 network 172.16.0.0
 no auto-summary
!
banner motd $AUTHORIZED ACCESS ONLY$
```

```
!  
line con 0  
password cisco  
  logging synchronous  
  login  
line vty 0 4  
  password cisco  
  logging synchronous  
  login  
!  
end
```

## R2

```
hostname R2  
!  
enable secret class  
!  
ip dhcp excluded-address 172.16.10.1 172.16.10.3  
ip dhcp excluded-address 172.16.11.1 172.16.11.3  
!  
ip dhcp pool R1_LAN10  
  network 172.16.10.0 255.255.255.0  
  dns-server 172.16.20.254  
!  
ip dhcp pool R1_LAN11  
  network 172.16.11.0 255.255.255.0  
  dns-server 172.16.20.254  
!  
no ip domain lookup  
!  
interface FastEthernet0/0  
  ip address 172.16.20.1 255.255.255.0  
  ip nat inside  
  no shutdown  
!  
interface Serial0/0/0  
  ip address 172.16.0.2 255.255.255.252  
  no shutdown  
!  
interface Serial0/0/1  
  ip address 209.165.201.1 255.255.255.252  
  ip nat outside  
  clock rate 125000  
  no shutdown  
!  
router rip  
  version 2  
  network 172.16.0.0  
  default-information originate  
  no auto-summary  
!  
ip route 0.0.0.0 0.0.0.0 209.165.201.2  
!  
ip nat pool NAT_POOL 209.165.201.9 209.165.201.14 netmask 255.255.255.248  
ip nat inside source list NAT_ACL pool NATPOOL overload
```

```
!  
ip access-list standard NAT_ACL  
  permit 172.16.10.0 0.0.0.255  
!  
banner motd $AUTHORIZED ACCESS ONLY$  
!  
line con 0  
  password cisco  
  logging synchronous  
  login  
line vty 0 4  
  password cisco  
  logging synchronous  
  login  
!  
end
```

## ISP

```
hostname ISP  
!  
enable secret class  
!  
interface Serial0/0/1  
  ip address 209.165.201.2 255.255.255.252  
  no shutdown  
!  
ip route 0.0.0.0 0.0.0.0 Serial0/0/1  
!  
banner motd $AUTHORIZED ACCESS ONLY$  
!  
line con 0  
  password cisco  
  logging synchronous  
  login  
line vty 0 4  
  password cisco  
  logging synchronous  
  login  
!  
end
```

## Tarefa 2: Localizar e corrigir todos erros de rede

Quando a rede está configurada corretamente:

- PC1 e PC2 devem ser capazes de receber endereços IP do conjunto DHCP correto conforme evidenciado por `ipconfig` nos PCs. Além disso; `show ip dhcp bindings` em R2 agora deve mostrar ambos os PCs têm endereços IP recebidos.
- Pings de teste de PC1 e PC2 no ISP devem receber a tradução de sobrecarga NAT conforme evidenciado por um `show ip nat translations` em R2.
- Pings de teste no servidor interno para ISP devem receber a tradução NAT estática indicada na topologia. Utilize o comando `show ip nat translations` para verificar isso.
- Um ping no ISP no endereço global do servidor interno deve ter êxito.

- Pings de teste de ISP e R1 não devem receber a tradução NAT conforme evidenciado por um `show ip nat translations` or a `debug ip nat` em R2.

### Tarefa 3: Documentar as configurações do roteador

Em cada roteador, emita o comando **show run** e capture as configurações.

### Tarefa 4: Limpar

Apague as configurações e recarregue os roteadores. Desconecte e guarde o cabeamento. Para hosts PC normalmente conectados a outras redes, como a LAN escolar ou a Internet), reconecte o cabeamento apropriado e restaure as configurações TCP/IP.