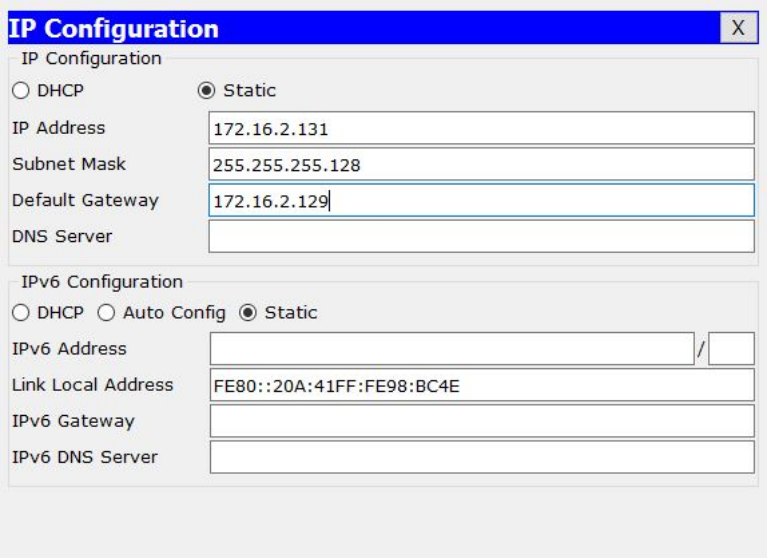
06

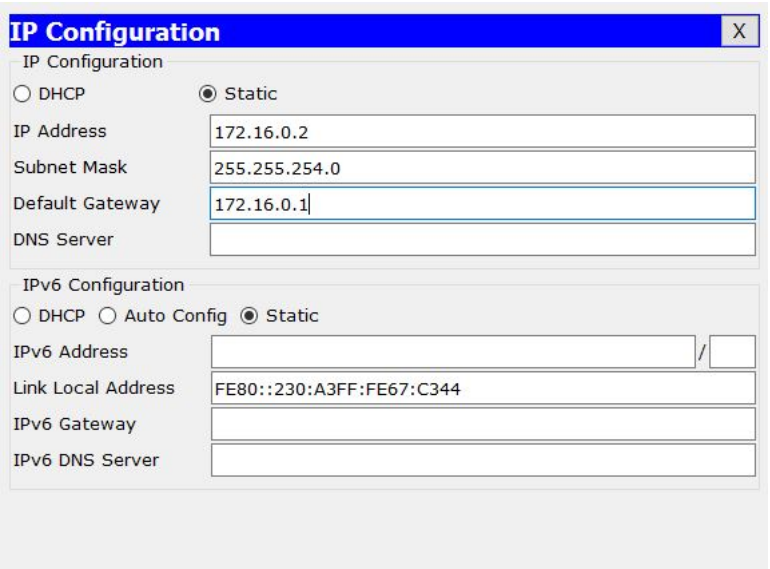
# Mãos à obra: Criando listas de acesso

Os diretores da Mutillidae informaram que somente o gerente de finanças e o gerente de vendas devem ter acesso ao servidor, os demais funcionários do setor de vendas e finanças não devem ter acesso. Devemos para isso criar a lista de acesso.

- Os endereços IP alocados pelo DHCP podem ser renovados em horas ou alguns dias. Dessa forma, como queremos dar acesso somente ao gerente de vendas e ao gerente de finanças, é importante que os endereços IP desses usuários não sejam alterados o que comprometeria nossa lista de acesso. Vamos então, configurar tais endereços IP estaticamente nos dois computadores e assim garantimos que eles não serão renovados.
- Clique no computador do gerente de finanças e insira o endereço IP 172.16.2.131, máscara 255.255.255.128 e default-gateway 172.16.2.129. Devemos ter o seguinte resultado:




- Devemos realizar essa mesma configuração para o computador do gerente de vendas colocamos estaticamente o endereço IP 172.16.0.2, máscara 255.255.254.0 e gateway 172.16.0.1. Teremos o seguinte resultado:




- Clique no roteador e vá até a aba CLI
- Entre na parte privilegiada digitando **enable** e posteriormente entre na parte de configuração digitando **configure terminal**. Como configuramos esses endereços estaticamente devemos removê-lo dos pools DHCP para não serem

alocado assim para nenhum outro usuário.

- Digite **ip dhcp excluded-address 172.16.0.2**
- Na sequência, digite **ip dhcp excluded-address 172.16.2.131**

Devemos criar agora a lista de acesso permitindo somente que o computador do gerente de vendas e do gerente de finanças acessem o servidor.

- O primeiro passo é criar essa lista de acesso, digitamos: **ip access-list extended SERVIDOR-GERENTES**
- Devemos criar essas políticas de acesso permitindo primeiramente o acesso do computador do gerente de finanças, digitamos **permit tcp 172.16.2.131 0.0.0.0 172.16.3.2 0.0.0.0**
- Na sequência permitimos o acesso do gerente de vendas, digitamos: **permit tcp 172.16.0.2 0.0.0.0 172.16.3.2 0.0.0.0**
- Em seguida, devemos negar o acesso dos demais funcionários do setor de vendas e finanças, para negar acesso aos demais funcionários de finanças, digitamos: **deny tcp 172.16.2.0 0.0.0.255 172.16.3.2 0.0.0.0** e na sequência negamos o acesso para todos os demais funcionários de vendas ** deny tcp 172.16.0.0 0.0.0.255 172.16.3.2 0.0.0.0**
- Por fim, devemos permitir todas as demais comunicações, digitamos: **permit ip any any**
- Devemos agora informar que essa política de acesso deve ser implementada nas sub-interfaces de finanças e vendas no sentido de entrada. Saímos da configuração da lista de acesso digitando **exit** e na sequência entramos na sub-interface da Vlan de vendas (por exemplo: **interface FastEthernet 0/0.1**). Para fazermos essa associação com a lista de acesso, digitamos: **ip access-group SERVIDOR-GERENTES in**
- Agora saímos da parte de configuração sub-interface da Vlan de vendas, digitando **exit** e na sequência entramos na sub-interface do setor de finanças (por exemplo: **interface FastEthernet 0/0.2**) e fazemos a associação com a lista de acesso digitando: **ip access-group SERVIDOR-GERENTES in**

Vá aos computadores, na aba dos Web Browsers e tente acessar o servidor. Qual é o resultado?