

# Projeto Integrado em Redes de Computadores



Cruzeiro do Sul Virtual  
Educação a distância



# Material Teórico



**Projeto – Fase 4 – Configuração de VLANs e do DHCP**

**Responsável pelo Conteúdo:**

Prof. Dr. Vagner da Silva

**Revisão Textual:**

Prof.<sup>a</sup> Esp. Kelciane da Rocha Campos





- LAN Virtual – VLAN;
- DHCP (*Dynamic Host Configuration Protocol*).



### OBJETIVOS DE APRENDIZADO

- Entender como a segmentação da rede LAN usando VLANs pode trazer benefícios para aumentar a produtividade pelo melhor desempenho da rede;
- Conhecer como um roteador pode ser configurado com o serviço DHCP para oferecer endereços IPv4 para a rede LAN, bem como entender os benefícios relacionados ao controle dinâmico desses endereços.





# Orientações de estudo

Para que o conteúdo desta Disciplina seja bem aproveitado e haja maior aplicabilidade na sua formação acadêmica e atuação profissional, siga algumas recomendações básicas:



## Assim:

- ✓ Organize seus estudos de maneira que passem a fazer parte da sua rotina. Por exemplo, você poderá determinar um dia e horário fixos como seu “momento do estudo”;
- ✓ Procure se alimentar e se hidratar quando for estudar; lembre-se de que uma alimentação saudável pode proporcionar melhor aproveitamento do estudo;
- ✓ No material de cada Unidade, há leituras indicadas e, entre elas, artigos científicos, livros, vídeos e sites para aprofundar os conhecimentos adquiridos ao longo da Unidade. Além disso, você também encontrará sugestões de conteúdo extra no item **Material Complementar**, que ampliarão sua interpretação e auxiliarão no pleno entendimento dos temas abordados;
- ✓ Após o contato com o conteúdo proposto, participe dos debates mediados em fóruns de discussão, pois irão auxiliar a verificar o quanto você absorveu de conhecimento, além de propiciar o contato com seus colegas e tutores, o que se apresenta como rico espaço de troca de ideias e de aprendizagem.

## LAN Virtual – VLAN

Aplicar as melhores técnicas em configurações de equipamentos oferece benefícios como a melhoria de desempenho de tráfego e, consequentemente, possibilita a melhoria da produtividade dos colaboradores de uma empresa. Uma das técnicas aplicadas para melhorar o desempenho da rede é a segmentação da rede LAN, isso segmenta o domínio de *broadcast*, evitando que a rede tenha um mau comportamento.

Ao se focar na segmentação da rede LAN, as atenções são voltadas para a camada dois do modelo OSI. É nessa camada que o *switch* faz os controles de envios de quadros e é nesse equipamento que se estabelecem configurações para a segmentação da rede LAN.

Essa segmentação da rede LAN pode ser feita por uma técnica identificada por VLANs. As VLANs são redes criadas virtualmente e são configuradas em *switches*, elas fornecem segmentação e permitem flexibilidade organizacional, pois uma rede virtual pode agrupar máquinas que estão em espaços geograficamente diferentes da empresa.

O *switch* aceita a configuração de várias VLANs e cada uma delas é considerada uma rede lógica separada. Por essa característica, um quadro que tenha como destino uma outra VLAN deverá ser enviado para um *gateway* (roteador ou *switch* de layer 3) para ser roteado na rede.

As VLANs devem seguir um critério de criação e devem ser definidas no projeto, geralmente elas são criadas considerando-se grupos que estejam no mesmo departamento, projeto ou seções. Além desses agrupamentos, é possível, em alguns casos, segmentar a rede por características de tráfego.

Com as VLANs, é possível implementar políticas de acesso e segurança, considerando-se os grupos segmentados. Cada porta do *switch* pode ser vinculada a apenas uma VLAN e podem ser criadas várias VLANs em um *switch*. Cada VLAN criada tem um endereço de rede diferente para ela, portanto deve-se considerar um projeto com endereçamento hierárquico para compor essas VLANs criadas.

Por padrão, todas as portas do *switch* da fabricante CISCO estão atribuídas à VLAN 1, por esse motivo todas as portas se comunicam com as outras portas do *switch*. A partir do momento que outras VLANs são criadas, as portas associadas a essas outras VLANs não irão se comunicar, pois as máquinas vinculadas a essas portas terão endereço IPv4 de outra rede.

Vamos configurar VLANs na topologia apresentada na Figura 1.

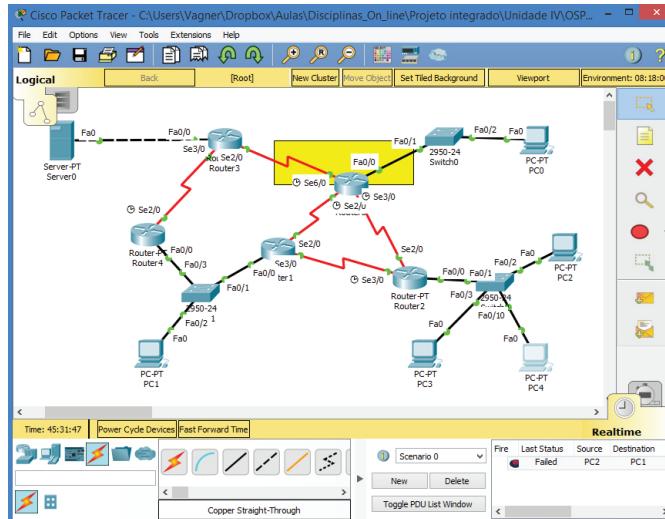


Figura 1 – Topologia para configuração da VLAN

Fonte: Acervo do Conteudista

Utilizaremos o *switch 2* para configuração da VLAN. Como pode ser observado, temos três máquinas conectadas ao *switch 2*. Será usado o PC 3 (conectado a *fast 0/3* do *switch*) e o PC 4 (conectado a *fast 0/10* do *switch*).

Iremos criar duas VLANs e configuraremos o *switch* e as máquinas conforme o Quadro 1.

Quadro 1 – Configuração do *Switch 2* e PCs

| Equipamento | Porta   | VLAN | Endereço rede | Máscara         |
|-------------|---------|------|---------------|-----------------|
| Switch 2    | 0/3     | 10   | -----         | -----           |
|             | 0/10    | 20   | -----         | -----           |
| PC3         | VLAN 10 |      | 192.168.3.3   | 255.255.255.128 |
| PC4         | VLAN 20 |      | 192.168.3.130 | 255.255.255.128 |

Para criar as VLANs, entre no modo de configuração de linha de comando do *switch 2* e execute os comandos a seguir.

```

Switch>enable
Switch#configure terminal
Switch(config)#vlan 10
Switch(config-vlan)#name contabilidade
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#name engenharia
Switch(config-vlan)#end
  
```

Após executar os comandos para configuração das VLANs, elas já estarão disponíveis para vincular as portas do *switch* a cada VLAN. A Figura 2 apresenta as informações das VLANs que estão configuradas no *switch* 2.

| VLAN Name               | Status | Ports   |
|-------------------------|--------|---|
| 1 default               | active | Fa0/1, Fa0/2, Fa0/3, Fa0/4<br>Fa0/5, Fa0/6, Fa0/7, Fa0/8<br>Fa0/9, Fa0/10, Fa0/11, Fa0/12<br>Fa0/13, Fa0/14, Fa0/15, Fa0/16<br>Fa0/17, Fa0/18, Fa0/19, Fa0/20<br>Fa0/21, Fa0/22, Fa0/23, Fa0/24 |
| 10 contabilidade        | active |   |
| 20 engenharia           | active |   |
| 1002 fddi-default       | active |   |
| 1003 token-ring-default | active |   |
| 1004 fddinet-default    | active |   |
| 1005 trnet-default      | active |   |

| VLAN | Type | SAID   | MTU  | Parent | RingNo | BridgeNo | Stp | BrdgMode | Trans1 | Trans2 |
|------|------|--------|------|--------|--------|----------|-----|----------|--------|--------|
| 1    | enet | 100001 | 1500 | -      | -      | -        | -   | 0        | 0      | 0      |
| 10   | enet | 100010 | 1500 | -      | -      | -        | -   | 0        | 0      | 0      |
| 20   | enet | 100020 | 1500 | -      | -      | -        | -   | 0        | 0      | 0      |
| 1002 | fddi | 101002 | 1500 | -      | -      | -        | -   | 0        | 0      | 0      |

Figura 2 – Lista das VLANs do *switch* 2

Fonte: Acervo do Conteudista

Como pode ser observado na Figura 2, há disponível a VLAN 1, considerada a VLAN padrão, todas as portas dos *switches* estão vinculadas a ela. Pode-se notar também as duas VLANs criadas, a VLAN 10 (contabilidade) e a VLAN 20 (engenharia), sem nenhuma porta associada a elas.

O próximo passo é associar as portas às VLANs 10 e 20, conforme definido no quadro 1. O PC 3 será vinculado à VLAN 10 e o PC 4 ficará na VLAN 20. Execute os comandos abaixo para vincular as portas às VLANs.

```

Switch#configure terminal

Switch(config)#interface fastEthernet 0/3

Switch(config-if)#switchport mode access

Switch(config-if)#switchport access vlan 10

Switch(config-if)#exit

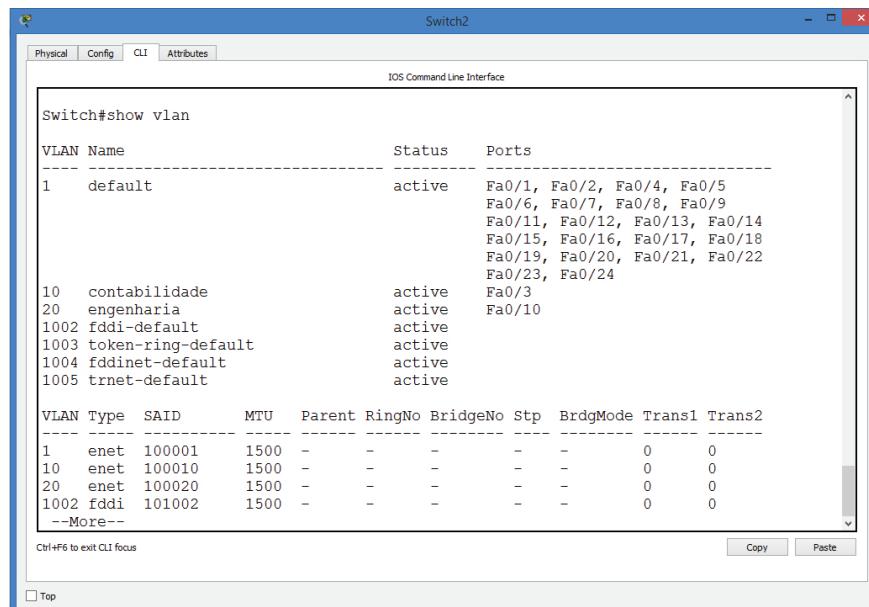
Switch(config)#interface fastEthernet 0/10

Switch(config-if)#switchport mode access

Switch(config-if)#switchport access vlan 20

```

Após aplicar os comandos para vincular as portas às VLANs, observa-se que essas portas deixaram de ser vinculadas à VLAN 1 e estão vinculadas às VLANs criadas. A Figura 3 apresenta como está a configuração.



```

Switch#show vlan

VLAN Name          Status    Ports
---- -- --
1    default        active   Fa0/1, Fa0/2, Fa0/4, Fa0/5
                           Fa0/6, Fa0/7, Fa0/8, Fa0/9
                           Fa0/11, Fa0/12, Fa0/13, Fa0/14
                           Fa0/15, Fa0/16, Fa0/17, Fa0/18
                           Fa0/19, Fa0/20, Fa0/21, Fa0/22
                           Fa0/23, Fa0/24
10   contabilidade  active   Fa0/3
20   engenharia     active   Fa0/10
1002 fddi-default  active
1003 token-ring-default
1004 fddinet-default
1005 trnet-default  active

VLAN Type      SAID      MTU      Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- -- --
1   enet       100001    1500     -       -       -       -       0       0
10  enet       100010    1500     -       -       -       -       0       0
20  enet       100020    1500     -       -       -       -       0       0
1002 fddi      101002    1500     -       -       -       -       0       0
--More--

```

Figura 3 – Lista de VLANs e portas associadas

Fonte: Acervo do Conteudista

Como o PC 3 está conectado à porta *fast 0/3* e a porta *fast 0/3* foi vinculada à VLAN 10, então o PC 3 pertence à VLAN 10. O mesmo raciocínio é aplicado para o PC 4.

Temos que configurar os PCs, cada um deles em uma rede diferente, conforme definido no Quadro 1. Para configurar o PC 3, selecione-o e na aba “*Desktop*” selecione “*IP Configuration*”. A Figura 4 apresenta como ficará a configuração do PC 3.

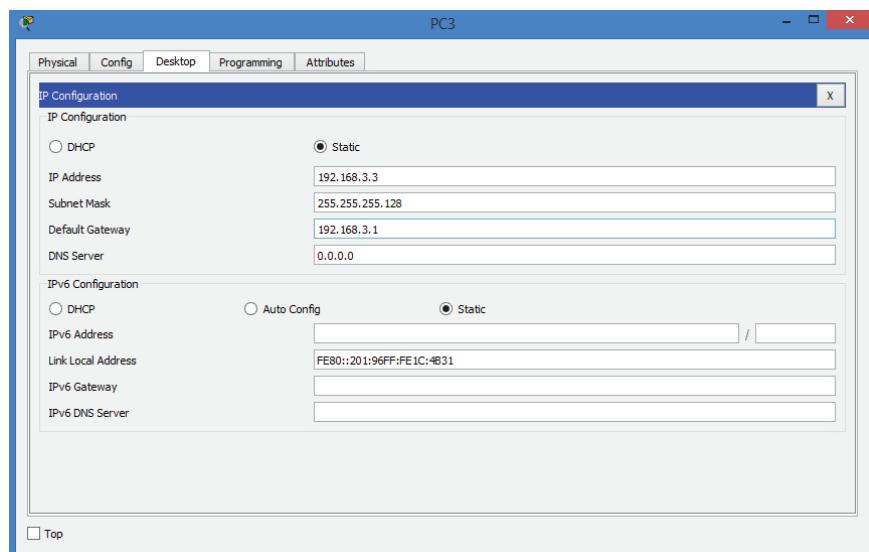


Figura 4 – Configuração do endereço IP do PC 3

Fonte: Acervo do Conteudista

Faça a configuração do PC 4 observando o endereço e máscara, conforme definido no Quadro 1. A Figura 5 apresenta a configuração do PC 4.

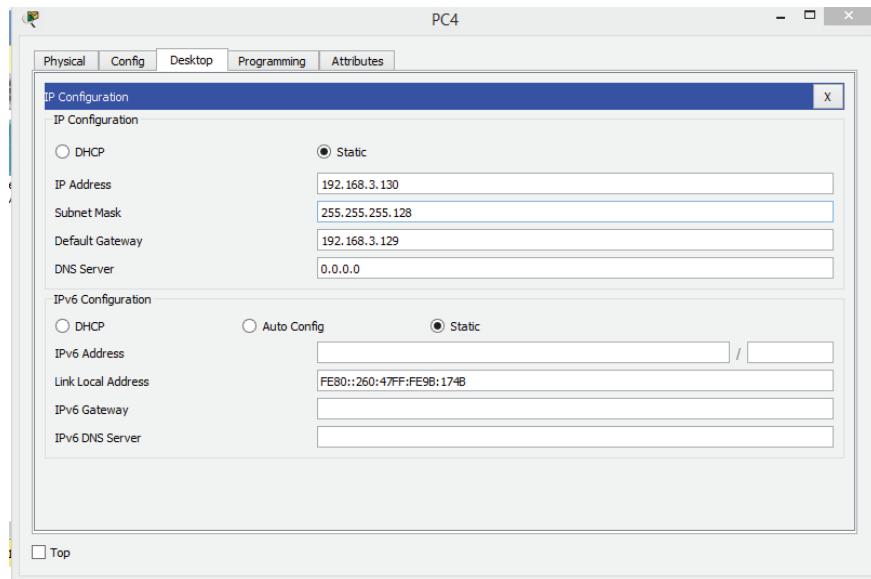


Figura 5 – Configuração do endereço IP do PC 4

Fonte: Acervo do Conteudista

A configuração definida até este ponto do processo não permite a comunicação entre as máquinas, pois elas, embora estejam no mesmo switch, estão configuradas com endereços de redes diferentes, um para cada VLAN. A Figura 6 apresenta o comando “ping” executado no PC 3, tentando alcançar o PC 4.

```
Physical Config Desktop Programming Attributes
Command Prompt
Ping statistics for 192.168.3.130:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 192.168.3.130

Pinging 192.168.3.130 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.3.130:
  Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>
```

Figura 6 – Testando conectividade

Fonte: Acervo do Conteudista

Até essa etapa da configuração, somente as portas vinculadas na mesma VLAN com máquinas configuradas com endereços IPs na mesma rede irão se comunicar. Resumindo, somente as máquinas que estão configuradas na mesma VLAN irão se comunicar.

Para permitir que máquinas configuradas em diferentes VLANs se comuniquem, é necessário configurar um *gateway* que tem a capacidade de rotear pacotes. Na topologia apresentada, o roteador 2 será usado para rotear pacotes e permitir a comunicação entre as VLANs 10 e 20.

Quando o tráfego de pacotes de uma VLAN tem que alcançar outros destinos que não sejam uma máquina configurada em sua própria VLAN, esse tráfego deve seguir por outros dispositivos, como *switch* de *layer 3* ou roteador. Nesse caso, haverá no mínimo uma porta ligada a outro dispositivo. Nessa topologia, a porta *fast 0/1* do *switch* está conectada à porta *fast 0/0* do roteador e ela será usada como meio de transporte de todo tráfego para todas as VLANs que tiverem pacotes para trafegar fora de seus domínios.

Para permitir que várias VLANs tenham seus pacotes trafegando para outras redes, temos que configurar um tronco, um caminho que permitirá que quadros das VLANs possam trafegar por ele. O tronco deve ser configurado nas duas pontas, nesse caso a interface *fast 0/1* do *switch* e na interface *fast 0/0* do roteador.

No roteador, além de configurar a interface *fast 0/0* para o tronco, temos que configurar também sub-interfaces, uma para cada VLAN criada. Vamos configurar um tronco no *switch*, entre na configuração de linha de comando e execute os comandos a seguir.

```
Switch>enable
Switch#configure terminal
Switch(config)#interface fastethernet 0/1
Switch(config-if)#switchport mode trunk
```

A configuração baseia-se em entrar na interface que se tornará um tronco e aplicar os comandos definindo-a como tronco. Agora precisamos entrar na configuração de linha de comando do roteador 2 e aplicar os comandos a seguir para configurá-lo.

```
Router>enable
Router#configure terminal
Router(config)#interface fastethernet 0/0
Router(config-if)#no ip address
Router(config-if)#interface fastethernet 0/0.1
Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip address 192.168.3.1 255.255.255.128
```

```

Router(config-subif)#exit
Router(config)#interface fastethernet 0/0
Router(config-if)#interface fastethernet 0/0.2
Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#ip address 192.168.3.129 255.255.255.128
Router(config-subif)#end

```

O Quadro 2 apresenta os comandos para a configuração do roteador.

Quadro 2 – Principais comandos para a configuração do roteador

| Comando   | Descrição  |
|---|--|
| Router(config-if)#no ip address                             | Aplicado para apagar qualquer endereço IP configurado na interface (nesse caso, <i>fastethernet 0/0</i> )  |
| Router(config-if)#interface fastethernet 0/0.1              | Cria dentro da interface 0/0 uma sub-interface com identificação 0/0.1   |
| Router(config-subif)#encapsulation dot1Q 10                 | Utilizado para encapsular esta sub-interface como tronco. O protocolo para tronco é o dot1.q. Nesse comando é vinculada à essa sub interface a VLAN criada, nesse caso a VLAN 10 |
| Router(config-subif)#ip address 192.168.3.1 255.255.255.128 | Atribui endereço IP à subinterface criada  |

Após aplicarmos os comandos para criação da sub-interface, devemos configurá-la para um tronco pelo comando *Router(config-subif)#encapsulation dot1Q 10*, em que dot1.q é o protocolo para torná-la um tronco e o valor 10 é a vinculação dessa sub-interface à VLAN 10, e permitimos que os pacotes da VLAN 10 sejam roteados. A mesma configuração deve ser feita para a VLAN 20.

Após a configuração, os pacotes já devem ser roteados, e as máquinas pertencentes a VLANs diferentes, e consequentemente a redes diferentes, já podem alcançar uma a outra. A Figura 7 apresenta o teste de conectividade entre as duas VLANs.

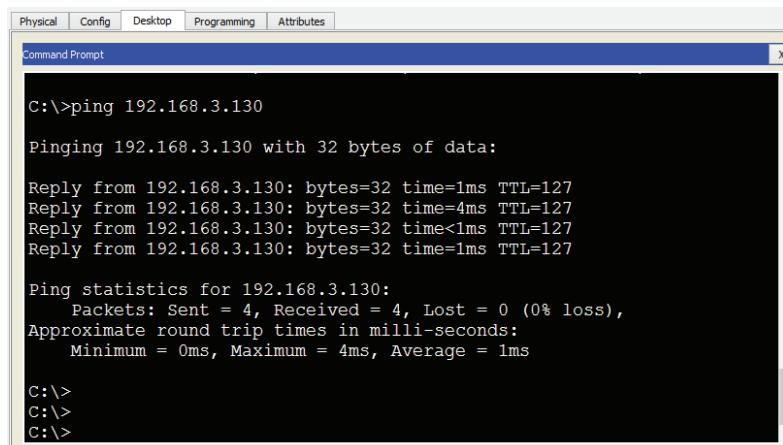
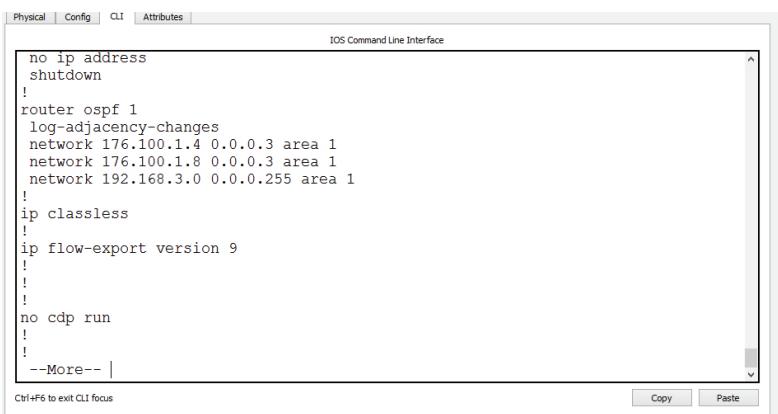


Figura 7 – Testando conectividade

Fonte: Acervo do Conteudista

Para que os pacotes tenham como destino a *internet*, um protocolo de roteamento dinâmico ou então um roteamento padrão deve ser configurado. Nessa simulação, o protocolo de roteamento dinâmico OSPF foi configurado. A Figura 8 apresenta parte da configuração do roteador.

Como pode ser observado, está sendo divulgada a rede *network 192.168.3.0 0.0.0.255 area1 1*, esta rede é a rota resumida ou super rede para as redes 192.168.3.0 255.255.255.128 e 192.168.3.128 255.255.255.128.



```

Physical | Config | CLI | Attributes | 
IOS Command Line Interface
no ip address
shutdown
!
router ospf 1
log-adjacency-changes
network 176.100.1.4 0.0.0.3 area 1
network 176.100.1.8 0.0.0.3 area 1
network 192.168.3.0 0.0.0.255 area 1
!
ip classless
!
ip flow-export version 9
!
!
no cdp run
!
!--More-- |
Ctrl+F6 to exit CLI focus
Copy Paste

```

Figura 8 – Comando *show running-config*

Fonte: Acervo do Conteudista

A definição de quantas e como serão criadas as VLANs faz parte do projeto de redes. Elas devem ser bem planejadas para oferecer o melhor desempenho da rede. Segmentar as redes VLAN por departamento é, muitas vezes, uma boa prática para configuração de redes, no entanto, se o departamento tiver muitas máquinas configuradas, é interessante pensar em dividi-las em outras VLANs.

## DHCP (*Dynamic Host Configuration Protocol*)

O DHCP é um protocolo desenvolvido para fornecer informações como endereços IP's, máscara de sub-rede, *gateway* e endereço do servidor DNS às máquinas clientes de uma rede, para que possam ser configurados de forma dinâmica.

Ao utilizar uma máquina como servidor DHCP, o trabalho de gerenciamento de uma rede se torna mais fácil e confiável, pois não é necessária a configuração manual dos endereços e outras informações que estão sendo usadas nas máquinas.

A máquina configurada como DHCP gerencia a alocação de endereços IPs, respondendo às solicitações dos clientes que necessitam de endereços IPs para se comunicarem pela rede.

As máquinas clientes recebem a alocação das informações do servidor por um determinado tempo definido pela configuração no próprio servidor. Quando o tempo da alocação expira, o cliente precisa solicitar outro endereço, que, na maioria das vezes, será o mesmo que estava alugado.

Na configuração do servidor, o administrador define a faixa de endereços que será oferecida e por quanto tempo eles permanecerão nas máquinas. Nesses servidores, é possível vincular os endereços MAC das máquinas que receberão endereços IPs fixos, esses são os casos dos servidores ou outros equipamentos que exigem endereços fixos.

Após a configuração do servidor DHCP, uma série de mensagens é trocada entre a máquina cliente e a máquina configurada como servidor para que o endereço IP seja alocado de forma correta.

Vamos usar a mesma topologia já usada nesta aula para configurar o roteador como um servidor DHCP.

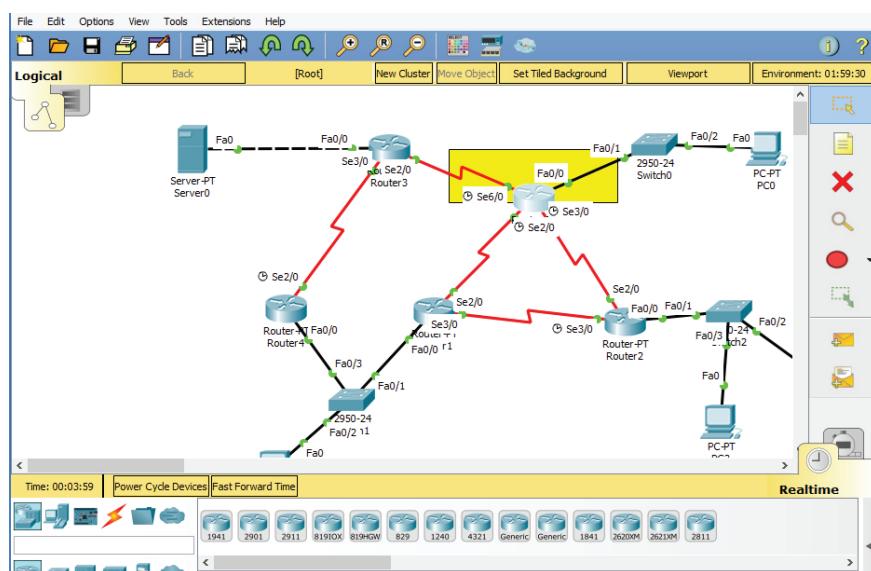


Figura 9 – Topologia para configuração do DHCP

Fonte: Acervo do Conteudista

Entre na configuração de linha de comando do roteador e execute os comandos a seguir para ele oferecer o serviço de DHCP.

```
Router>enable
Router#configure terminal
Router(config)#ip dhcp pool CONTAS
Router(dhcp-config)#network 192.168.1.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.1.1
```

Com essas configurações efetuadas, o roteador já está apto a conceder endereços IPs para as máquinas que estão na rede e configuradas para receber endereço automaticamente.

Vamos inserir mais uma máquina na rede e configurá-la para receber endereço do servidor DHCP. Insira mais uma máquina e não a conecte no *switch* ainda. Abra a janela de configuração deste PC e abra a aba “Config”. Selecione a opção DHCP. A Figura 10 apresenta a janela para configuração do endereço IP.

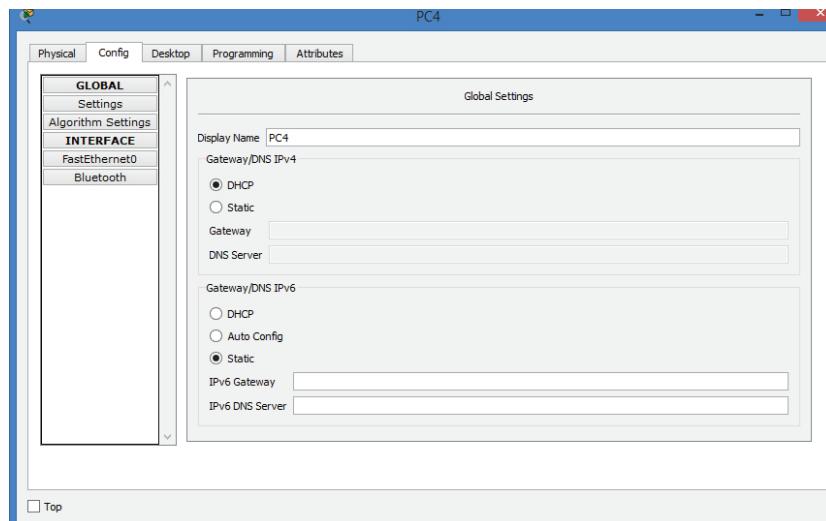


Figura 10 – Configuração do PC

Fonte: Acervo do Conteudista

Selecionando a opção “DCHP”, estamos configurando o PC para obter endereço IP automaticamente. Ao ligar o computador ou então ao conectá-lo no *switch*, ele irá solicitar um endereço IP e outras informações via *broadcast* para a máquina que estiver com o serviço DHCP.

Nesse caso, o roteador responderá à solicitação, informando os dados que foram configurados. Para verificar a configuração estabelecida no computador, abra a janela de configuração e abra a aba “Config”, e as informações de configuração no roteador serão estabelecidas. A Figura 11 apresenta as informações configuradas no PC.

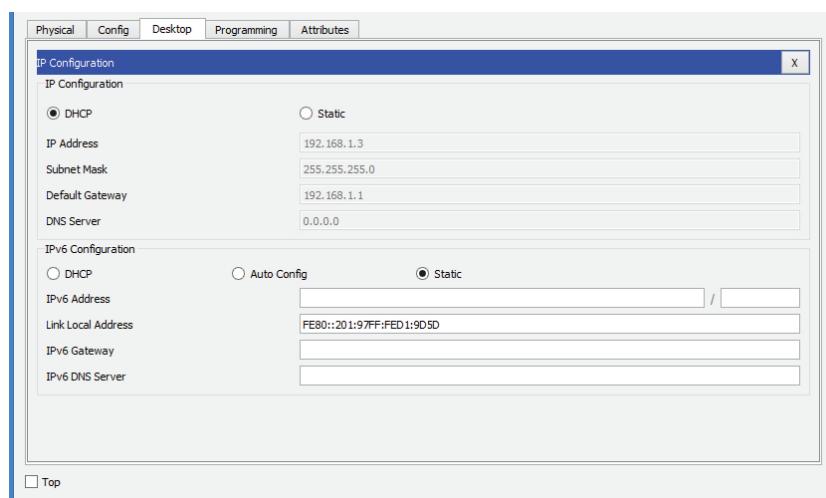


Figura 11 – Informações configuradas no PC

Fonte: Acervo do Conteudista

Alguns endereços IPs que estão configurados para serem alocados podem ser destinados a servidores ou outras máquinas que precisam ter seus endereços fixos, ou seja, devem ser configuradas com os mesmos endereços. Há também situações como a que está ocorrendo nessa configuração, em que o roteador já tem configurado um endereço IP fixo e esse não pode ser oferecido pelo motivo de possíveis conflitos.

Para esses casos, temos como solicitar ao servidor DHCP, nessa simulação, o roteador, para não oferecer esse endereço que já está sendo usado. Para isso, devemos informar na configuração DHCP que sejam excluídos os endereços que não serão ofertados. Execute os comandos a seguir para excluir o endereço que não poderá ser ofertado.

```
Router>enable  
Router#configure terminal  
Router(config)#ip dhcp excluded-address 192.168.1.1
```

Com esse comando, o endereço IP 192.168.1.1 não será ofertado pelo DHCP, pois este já está sendo usado na interface *fastethernet* do roteador. Para verificar os endereços alocados, aplique o comando indicado na Figura 12 e verá o endereço 192.168.1.3 já alocado para o endereço MAC indicado.

| IP address  | Client-ID/<br>Hardware address | Lease expiration | Type |
|-------------|--------------------------------|------------------|------|
| 192.168.1.3 | 0001.97D1.9D5D                 | --               |      |

Figura 12 – Informações configuradas no PC

Fonte: Acervo do Conteudista

Caso queira configurar mais endereços que não serão alocados - por exemplo, endereços do 1 ao 50 não sendo concedidos, utilize o comando a seguir.

```
Router(config)#ip dhcp excluded-address 192.168.1.1    192.168.1.50
```

É possível estabelecer outras configurações, como endereço do servidor DNS e o tempo em que será feita a concessão dos endereços solicitados. Para configurar o DNS, execute o comando abaixo.

```
Router(dhcp-config)#dns-server 192.168.1.1
```

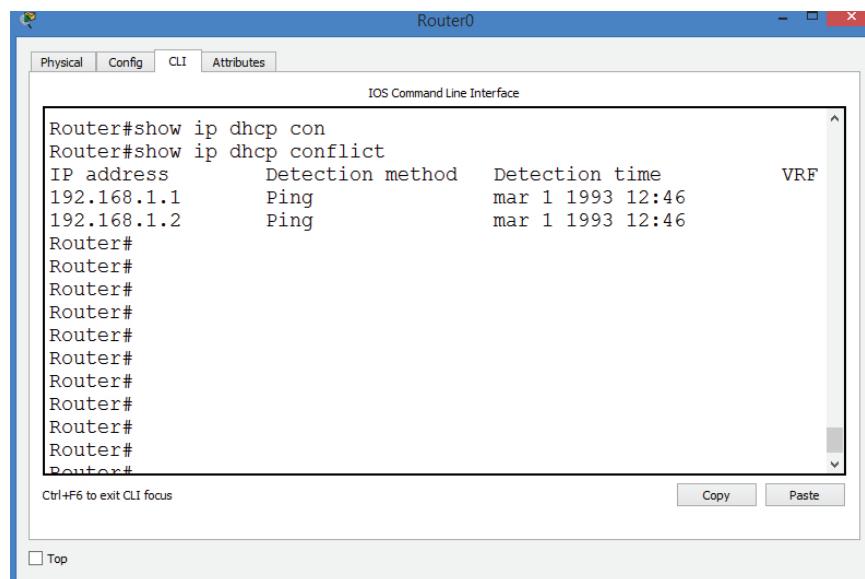
Para configurar o nome do servidor de domínio e permitir que o servidor DHCP forneça essa informação para as máquinas, execute o comando a seguir.

```
Router(dhcp-config)#default-name GRUPO
```

O *packet tracer* não comporta o comando para definir o tempo de concessão, pois se isso fosse possível o seguinte comando seria aplicado para reservar o endereço por sete dias.

```
Router(dhcp-config)#lease 7
```

O servidor DHCP pode verificar se há conflitos de endereços na rede. Para verificar esta inconsistência, execute o comando da Figura 13.



```
Router#show ip dhcp conflict
IP address Detection method Detection time VRF
192.168.1.1 Ping mar 1 1993 12:46
192.168.1.2 Ping mar 1 1993 12:46
```

Figura 13 – Comando para encontrar conflitos de endereços IPs

Fonte: Acervo do Conteudista

Embora seja possível configurar DHCP em roteadores, este procedimento deve ser evitado, pois como boa prática em projeto de redes, o roteador deve ficar com sua principal operação, que é a de rotear pacotes, principalmente se for o roteador de borda da empresa.

É conveniente distribuir as atividades para outros equipamentos de redes, assim pode-se contribuir para o melhor desempenho da rede de computadores. Geralmente, utiliza-se para servidores DHCP um servidor já configurado com outros serviços na rede, ele pode oferecer este tipo de serviço, deixando o roteador para a sua principal função, que é a de rotear pacotes.

O servidor DHCP pode ser também configurado para fornecer endereços IPv6; portanto, para essa nova versão de IP é possível usar um servidor DHCP. Isso facilitará ainda mais o controle dos endereços na rede, pois um endereço IPv6 é bem maior e mais trabalhoso de controlar e configurar que um endereço IPv4.

# Material Complementar

## Indicações para saber mais sobre os assuntos abordados nesta Unidade:

### Sites

#### **Criando vlan de Ethernet em Catalyst Switches**

Veja no *link* a seguir mais comandos para complementação da configuração de VLANs.

<http://bit.ly/2ZhFhP>

#### **Exemplo de truncamento ISL e 802.1Q entre Switches de configuração fixa Catalyst da camada 2 e Switches CatOS**

O conceito de tronco é necessário para a configuração das VLANs. Leia o texto disponibilizado no *link*.

<http://bit.ly/2vZgqz2>

#### **Configurando dinamicamente as opções do servidor de DHCP**

Veja mais sobre servidores DHCP.

<http://bit.ly/2vWP8cz>

#### **DHCPv6 usando o exemplo de configuração da característica da delegação do prefixo**

No *link* a seguir você irá aprender a configurar IPv6.

<http://bit.ly/2vZqyYy>

## Referências

CHAPPELL, L.; FARKAS, D. **Diagnosticando redes: Cisco InternetWork Troubleshooting.** São Paulo: Pearson Education do Brasil, 2002.

MATTHEW H. B. **Projeto de Interconexão de redes: Cisco InternetWork Design.** São Paulo: Pearson Education do Brasil, 2003.





**Cruzeiro do Sul**  
Educacional