

Projeto Integrado em Redes de Computadores



Cruzeiro do Sul Virtual
Educação a distância

Material Teórico



Projeto – Fase 3 – Configuração NAT, HSRP e ACLs

Responsável pelo Conteúdo:

Prof. Dr. Vagner da Silva

Revisão Textual:

Prof.^a Esp. Kelciane da Rocha Campos



- NAT (*Network Address Translation* – Tradução de Endereço de Redes);
- HSRP;
- ACL (*Access Control List* – Lista de Controle de Acesso).



OBJETIVOS DE APRENDIZADO

- Entender como usar a técnica que prolonga o uso do endereçamento IPv4, bem como implementar no simulador a tradução de endereço de rede;
- Conhecer como oferecer redundância na rede para propiciar disponibilidade de *link* e equipamento de borda, permitindo maior tempo de uso dessa rede;
- Entender como configurar segurança de rede pela aplicação de filtro de pacotes nos sentidos interno para externo e externo para interno.



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.

NAT (*Network Address Translation* – Tradução de Endereço de Redes)

No desenvolvimento do endereço IPv4, não se pensou na dimensão que a rede de computadores poderia alcançar. Ele, então, foi especificado em um total de 32 bits, agrupados em quatro conjuntos de oito bits para representar o endereçamento das máquinas.

Com essa especificação e vinculado a uma máscara de rede, é possível endereçar, aproximadamente, 4 bilhões de equipamentos na rede. Essa quantidade era considerada adequada na época do seu desenvolvimento.

Com o decorrer do tempo, observou-se uma demanda crescente por endereços IPv4, devido à quantidade de máquinas sendo configuradas na rede, e percebeu-se que alguma providência deveria ser tomada para evitar o esgotamento de endereços IPv4.

Algumas técnicas foram estudadas e elaboradas, dentre elas temos: VLSM, NAT e a que se considera definitiva: o desenvolvimento de uma nova versão de endereçamento, especificado como IPv6.

O NAT tem como objetivo traduzir endereços privativos para endereços públicos. Os endereços privativos podem e devem ser configurados na rede LAN das empresas, eles não são roteáveis; portanto, devem ser traduzidos para endereços públicos, ou seja, endereços que serão reconhecidos na *internet*.

Os endereços privativos estão definidos na especificação do IPv4, conforme apresentado no Quadro 1.

Quadro 1 – Endereços privativos

Faixa de endereço	Classe
10.0.0.0 - 10.255.255.255	A
172.16.0.0 - 172.31.255.255	B
192.168.0.0 - 192.168.255.255	C

As empresas podem, livremente, desenvolver um planejamento de endereçamento IPv4, considerando uma dessas faixas de endereços, e obter um endereço público, formalmente, para que seja configurado na interface serial que está conectada a equipamentos do provedor de acesso.

O endereço IP privativo deve ser traduzido para o endereço público ao fazer um acesso externo à rede da empresa, somente assim serão estabelecidas conexões com servidores que estão pela *internet*.

Qualquer empresa poderá usar a faixa de endereço privativo que considere necessária e não precisa se preocupar se outra empresa está usando a mesma faixa, pois o que não pode ser igual é o endereço público.

Há algumas formas de configuração NAT, dentre elas temos a configuração estática, em que um endereço privativo é mapeado para um endereço público. Esse tipo de configuração é mais adequado para as situações em que a empresa tem, em sua rede interna, configurados servidores que devem ser acessados da rede externa.

O Quadro 2 vinculado à Figura 1 demonstra o NAT estático.

Quadro 2 – NAT estático

Endereço privativo	Endereço público
192.168.1.1	200.100.100.1
192.168.1.2	200.100.100.10
192.168.1.3	200.100.100.20

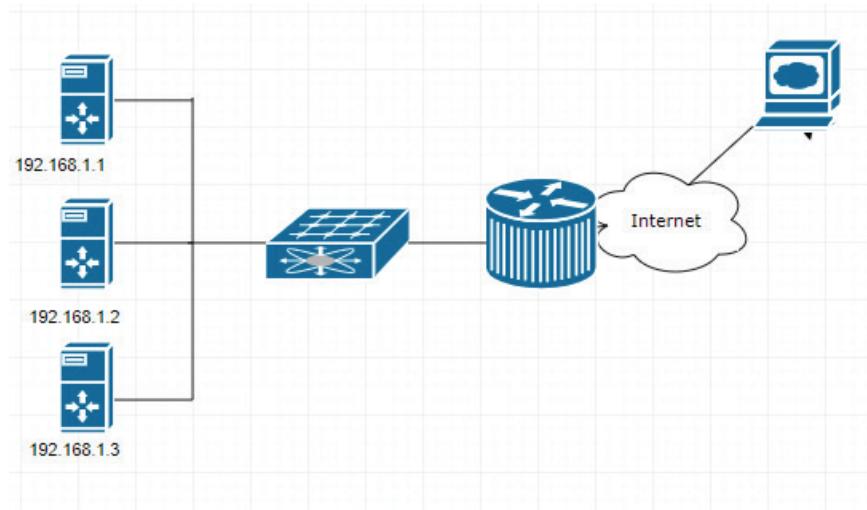


Figura 1 – NAT estático

Fonte: Acervo do Conteudista

A outra forma de configuração refere-se ao NAT dinâmico, ele usa um *pool* de endereços públicos para oferecer às requisições feitas internamente. Ainda oferece uma limitação ao exigir endereços públicos suficientemente disponíveis para satisfazer a quantidade total de sessões simultâneas de usuário.

Quadro 3 – NAT dinâmico

Endereço privativo	Endereço público
192.168.1.1	200.100.100.1
192.168.1.2	200.100.100.10
Disponível	200.100.100.20
Disponível	200.100.100.30
Disponível	200.100.100.40

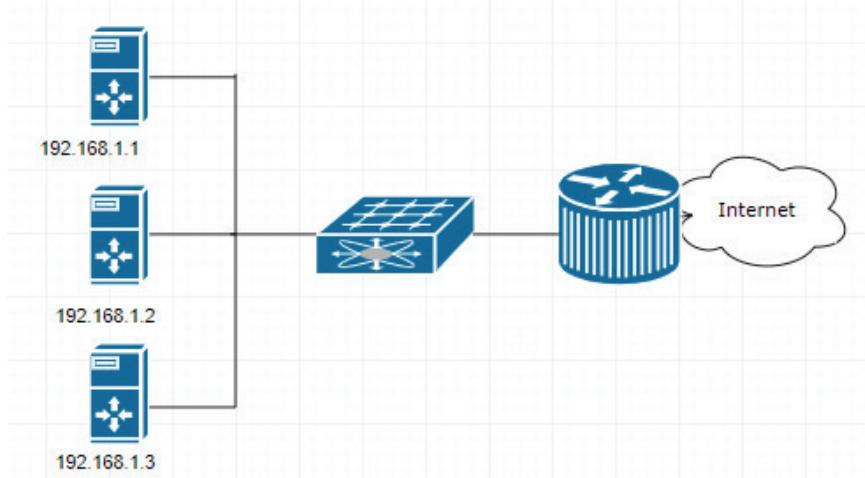


Figura 2 – NAT dinâmico

Fonte: Acervo do Conteudista

A outra forma de configurar o NAT, e a mais adequada para as empresas em geral, utiliza o número da porta e endereço IP de destino para mapear os pacotes internos para acesso externo.

Também conhecida como PAT, mapeia endereços privados em um único endereço público, para isso usa a porta de origem e endereço IP de destino, para manter um controle e conseguir identificar qual máquina internamente fez a requisição.

Vamos configurar o PAT usando o *packet tracer*, considerando a topologia apresentada na Figura 3.

Temos que inserir mais uma interface WAN no roteador 0 para simular uma conexão com o provedor de acesso, pois as duas disponíveis nesse roteador já estão sendo usadas. Para inserir essa interface, selecione o roteador 0 e a janela da Figura 3 será apresentada.

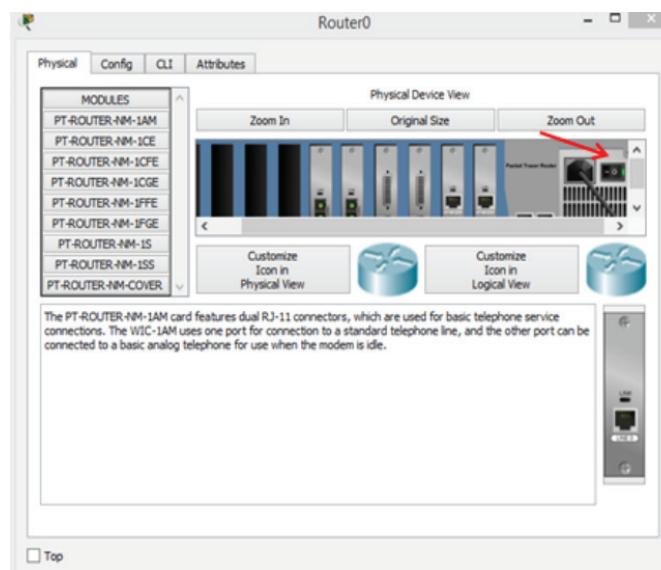


Figura 3 – Janela para inserir interface

Fonte: Acervo do Conteudista

Observe que na aba “Physical” aparece as interfaces que estão disponíveis para esse modelo de roteador. Para inserir uma interface, você deve desligar o roteador, a seta vermelha apresentada na Figura 4 mostra o botão “liga/desliga”. Selecione esse botão com o mouse e o roteador será desligado.

Com o roteador desligado, escolha no menu direito a interface WAM “PT-RPU-TER-NM-1S”. Selecione a interface e arraste-a para o local indicado apresentado com a seta vermelha da Figura 4.

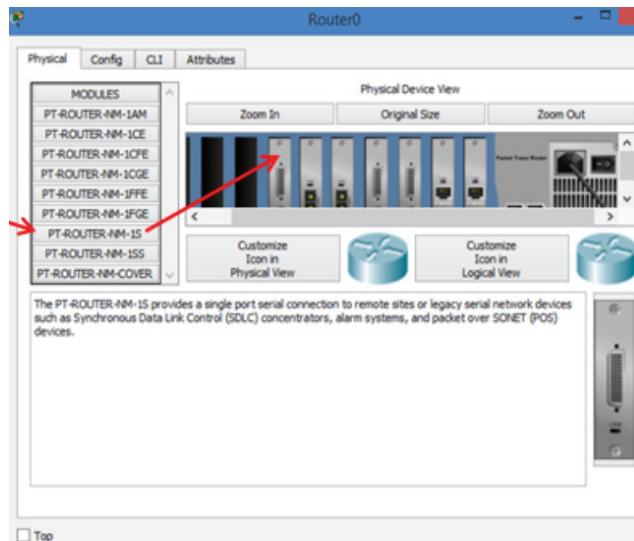


Figura 4 – Escolha da interface

Fonte: Acervo do Conteudista

Agora ligue o roteador, selecionando o botão “liga/desliga”, e a interface estará pronta para ser conectada e configurada. A interface foi inserida na posição 6/0, usaremos essa identificação da interface para configurá-la.

Para conectar o roteador 0 ao roteador 3, selecione o *link* de conexões e após selecione o *link* serial, conforme apresentado na figura 5. Selecione o roteador 6 e escolha a serial 6/0, depois selecione o roteador 3 e escolha a serial 2/0.

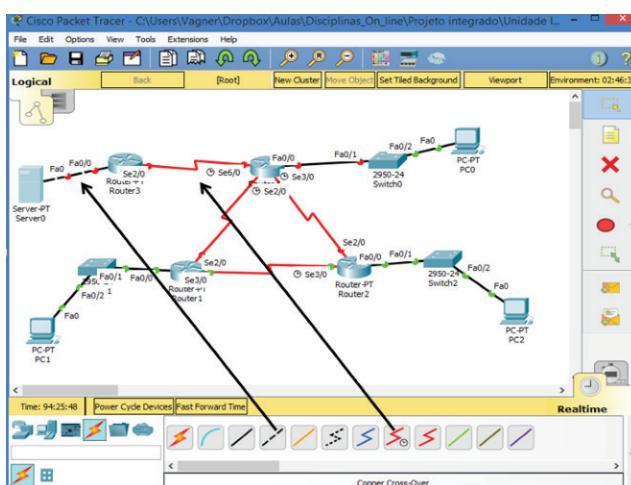


Figura 5 – Conexão com o roteador

Fonte: Acervo do Conteudista

Logo após, conecte a *fastethernet* 0 do servidor e a *fastethernet* 0/0 do roteador usando um cabo “*Copper Cross-Over*”, conforme indicado na Figura 5.

Configure as interfaces dos roteadores e servidor conforme o Quadro 4.

Quadro 4 – Endereços e interfaces para configuração

Equipamento	Interface	Endereço IP	Máscara
Roteador 0	Serial 6/0	202.68.3.1	255.255.255.252
Roteador 3	Serial 2/0	202.68.3.2	255.255.255.252
	fast 0/0	172.32.1.1	255.255.255.0
Servidor 0	fastethernet	172.32.1.2	255.255.255.0

Para configurar a interface 6 do roteador 0, execute os seguintes comandos.

```
Router>enable
Router#configure terminal
Router(config)#interface serial 6/0
Router(config-if)#ip address 202.68.3.1 255.255.255.252
Router(config-if)#clock rate 64000
Router(config-if)#no shutdown
```

Após configurar a interface, a rede deve ser divulgada, execute os comandos abaixo para divulgação da rede.

```
Router(config-if)#exit
Router(config)#router ospf 1
Router(config-router)#network 202.68.3.0 0.0.0.3 area 1
```

Vamos considerar, conforme Figura 6, que o roteador 0 é o roteador de saída e entrada de dados de uma empresa, ou seja, o roteador de borda. Sendo assim, iremos configurar esse roteador para que ele faça a tradução de endereço IP privativo (192.168.1.0/24) pertencente à LAN, para endereço público (202.60.3.1/30) pertencente à WAN.

Na Figura 6, o retângulo amarelo mostra as duas interfaces que serão configuradas para tradução de endereço.

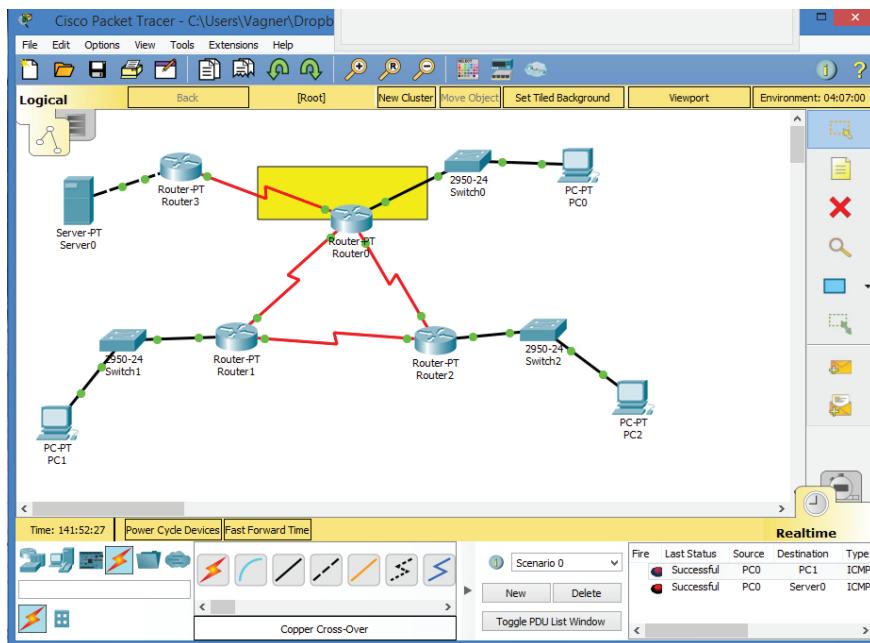


Figura 6 – Interfaces que irão traduzir

Fonte: Acervo do Conteudista

Para configurar o NAT, execute os seguintes comandos no roteador 0.

```
Router>enable
```

```
Router#configure terminal
```

```
Router(config)#ip nat inside source list 1 interface serial 6/0 overload
```

```
Router(config)#access-list 1 permit any
```

```
Router(config)#interface fastEthernet 0/0
```

```
Router(config-if)#ip nat inside
```

```
Router(config-if)#exit
```

```
Router(config)#interface serial 6/0
```

```
Router(config-if)#ip nat outside
```

Com os comandos executados, o NAT foi configurado. O quadro 5 descreve a função de cada um dos comandos.

Quadro 5 – Descrição dos comandos

Comando	Descrição
Router>enable	Muda do modo usuário para o modo privilegiado
Router#configure terminal	Muda do modo privilegiado para o modo de configuração global

Comando	Descrição	
Router(config)#ip nat inside source list 1 interface serial 6/0 overload		Configura o NAT por portas (PAT)
<i>list 1</i>		Lista de acesso 1 (ACL)
<i>Interface serial 6/0</i>		Interface que será traduzida
<i>overload</i>		Ativa a tradução de portas
Router(config)#access-list 1 permit any	Configura lista de acesso para permitir o tráfego de pacotes	
Router(config)#interface fastEthernet 0/0	Entra no modo de configuração da interface fastEthernet 0/0	
Router(config-if)#ip nat inside	Configura a fastEthernet como interna no processo de tradução	
Router(config-if)#exit	Sai do modo de configuração da interface	
Router(config)#interface serial 6/0	Entra no modo de configuração da interface serial 0/0	
Router(config-if)#ip nat outside	Configura a serial como externa no processo de tradução	

Para verificar se a tradução está funcionando, entre no *prompt* de comando do PC0 e execute um *ping* para o servidor (172.32.1.2).

Logo após, entre na CLI do roteador 0 e execute o comando apresentado na Figura 7.

```

Router#
Router#show ip nat translations
Proto Inside global     Inside local      Outside local      Outside global
icmp 202.68.3.1:4      192.168.1.2:4    172.32.1.2:4      172.32.1.2:4
icmp 202.68.3.1:5      192.168.1.2:5    172.32.1.2:5      172.32.1.2:5
icmp 202.68.3.1:6      192.168.1.2:6    172.32.1.2:6      172.32.1.2:6
icmp 202.68.3.1:7      192.168.1.2:7    172.32.1.2:7      172.32.1.2:7

Router#
Router#
Router#
Router#
Ctrl+F6 to exit CLI focus

```

Figura 7 – Comando para verificar tradução

Fonte: Acervo do Conteudista

Como pode ser observado na Figura 7, o endereço local (192.168.1.1) foi traduzido para o endereço externo (202.68.3.1).

HSRP

Muitas empresas têm como requisito o acesso externo, seja para se conectar à matriz ou então para utilizar serviços ou outros recursos disponíveis remotamente. Quando a empresa se enquadra nessa característica, é necessário planejar a rede de forma a fornecer disponibilidade aos serviços e, consequentemente, aos dados.

O requisito disponibilidade nos direciona a implementar redundância de equipamentos e outros recursos de redes para manter todos os serviços disponíveis a maior parte do tempo possível. Em projeto de redes, o projetista deve avaliar a necessidade do requisito disponibilidade e decidir como isso será feito.

Uma das formas de obter disponibilidade da rede em quase cem por cento do tempo passa pela configuração do HSRP (*Hot Standby Router Protocol*). Ele garante o tráfego caso o *gateway*, nesse caso um roteador, venha a falhar por algum problema.

Para permitir redundância usando o HSRP, dois ou mais roteadores de borda (roteadores com conexão externa à rede da empresa) devem ser configurados. Um será considerado o roteador ativo, ele será eleito e responsável por encaminhar os pacotes que os *hosts* enviam. O outro será o *standby* e irá assumir as responsabilidades do roteador ativo caso ele falhe.

Ao configurar roteadores em um grupo HSRP, o roteador com prioridade mais alta será o roteador ativo; caso a prioridade seja a mesma, o roteador com maior endereço IP será o roteador ativo.

Embora não seja classificado como protocolo de roteamento dinâmico, o HSRP envia mensagens entre os roteadores para verificar suas atividades. A seguir a descrição de algumas considerações importantes sobre o HSRP.

Mensagens *Hello* – contêm todas as mensagens para o funcionamento do HSRP, como autenticação, versão, *timers* etc.

Processo de eleição – primeiro critério para eleger o roteador ativo será a prioridade, os roteadores já são, por padrão, configurados com prioridade 100, podendo ser alterada entre 0 e 255. A segunda prioridade será o maior endereço IP.

HSRP *Timers* – o padrão usado na troca do *Hello timers* é de 3 segundos, ou seja, esse é o tempo usado para verificar se o roteador está operando. O *Hold Timers* tem seu tempo definido em 10 segundos. É aconselhável definir um *hold timer* três vezes maior que o *Hello*. Na prática, se em três *Hello* o roteador ativo não responder, então pode-se ativar a troca, automaticamente, para que o *standby* assuma a responsabilidade.

Preempt – comando usado para permitir que um roteador com maior prioridade que entrar na rede HSRP assuma como roteador ativo. Se esse comando não for definido na configuração, então o roteador com maior prioridade entrando na rede HSRP não assumirá a responsabilidade pela troca de mensagens.

Endereço Virtual – o HSRP usa endereço MAC e IP virtual na configuração.

Vamos implementar redundância em uma rede e configurar o HSRP para fornecer disponibilidade. Para isso, insira um roteador “Router-PT” na topologia que estamos usando. A Figura 8 apresenta a topologia utilizada.

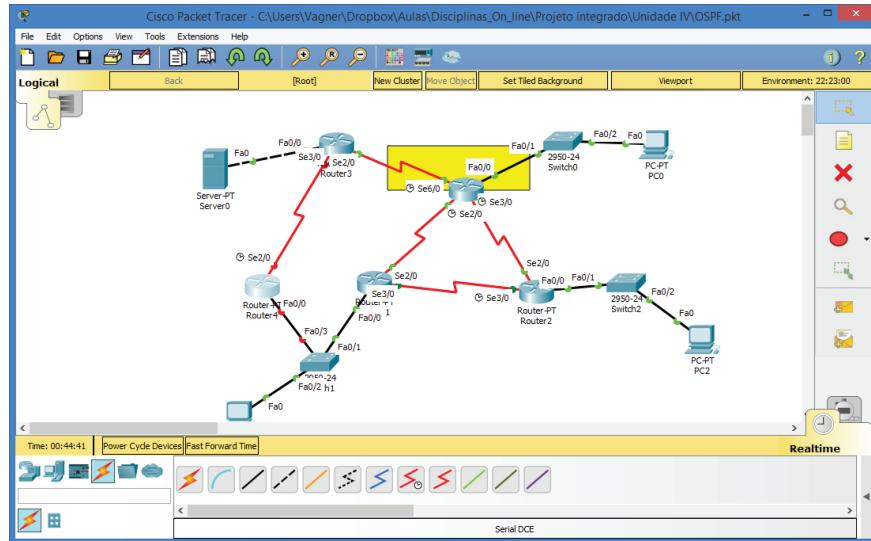


Figura 8 – Topologia para configuração do HSRP

Fonte: Acervo do Conteudista

Configure as interfaces do roteador 3 e roteador 4 conforme Quadro 6.

Quadro 6

Equipamento	Interface	Endereço IP	Máscara
Roteador 4	Serial 2/0	205.104.1.1	255.255.255.252
	Fast 0/0	192.168.2.5	255.255.255.0
Roteador 3	Serial 3/0	205.104.1.2	255.255.255.252

Os comandos a seguir deverão ser executados para configurar a interface e divulgar a rede com o protocolo OSPF no roteador 4. Para executá-los, entre na configuração de linha de comando no roteador 4.

```

Router>enable
Router#configure terminal
Router(config)#interface fastethernet 0/0
Router(config-if)#ip address 192.168.2.5 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface serial 2/0
Router(config-if)#ip address 205.104.1.1 255.255.255.252
Router(config-if)#clock rate 64000
Router(config-if)#no shutdown
Router(config-if)#exit

```

```
Router(config)#router ospf 1
Router(config-router)#network 205.104.1.0 0.0.0.3 area 1
Router(config-router)#network 192.168.2.0 0.0.0.255 area 1
```

Para configurar o roteador 3, execute os seguintes comandos na linha de comando.

```
Router>enable
Router#configure terminal
Router(config)#interface serial 3/0
Router(config-if)#ip address 205.104.1.2 255.255.255.252
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config-router)#network 205.104.1.0 0.0.0.3 area 1
```

Com as configurações dos roteadores 3 e 4 já feitas, podemos aplicar os comandos no roteador 4 para configurar o HSRP e viabilizar a disponibilidade. Ao observar a topologia, você poderá notar que estamos simulando uma empresa com dois roteadores de borda, sendo eles o roteador 1 e o roteador 4. Eles estão com suas respectivas *fastethernet* conectadas ao *switch 1* e cada um deles simulando uma conexão diferente com a *internet*.

Agora já podemos configurar os roteadores 1 e 4 para oferecer redundância na rede LAN à qual os dois estão conectados.

No roteador 1, iremos configurá-lo para ser o roteador ativo. Execute, na interface *fastethernet 0/0* do roteador 1, os comandos a seguir.

```
Router(config-if)#standby 1 ip 192.168.2.100
Router(config-if)#standby 1 priority 150
```

No roteador 4, execute o comando a seguir.

```
Router(config-if)#standby 1 ip 192.168.2.100
```

Configure, conforme Figura 9, o *default gateway* do computador PC1 para o endereço IP virtual 192.168.2.100.

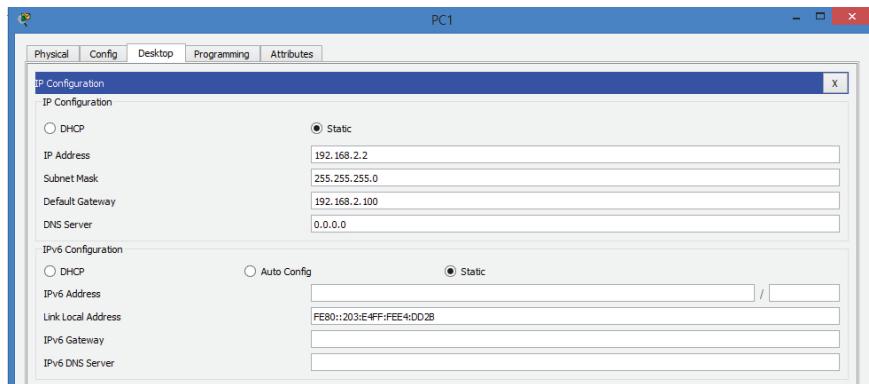


Figura 9 – Configuração da interface do PC1

Fonte: Acervo do Conteudista

Com a aplicação de todos os comandos citados anteriormente, o HSRP estará configurado. Sendo assim, podemos efetuar o teste de conectividade. Entre no PC1 e execute um “ping” para o servidor. Conforme poderá observar, os pacotes chegarão ao servidor. A Figura 10 apresenta o resultado do comando “ping” no servidor.

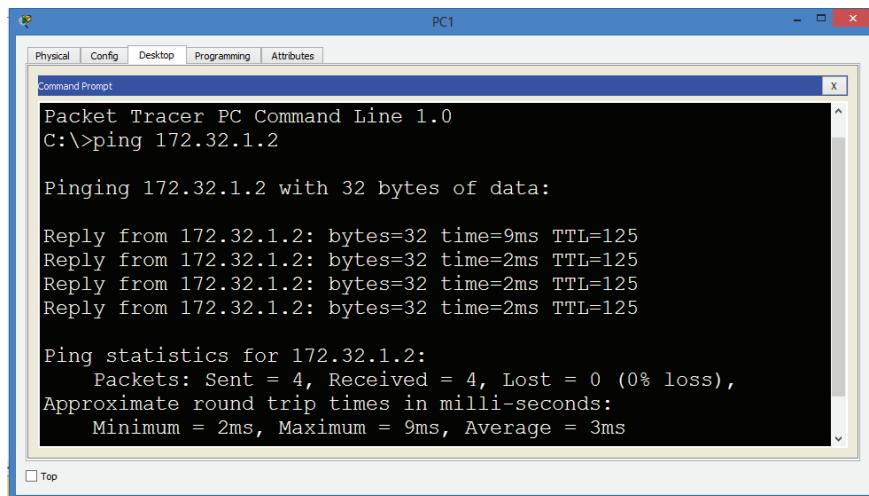


Figura 10 – Teste de conectividade com o servidor 0

Para verificar se a redundância está mesmo funcionando, desative a interface *fastethernet 0/0* do roteador 1 executando o comando a seguir.

```
Router(config-if)#shutdown
```

Lembre-se de que o do roteador 1 foi definido como ativo na configuração HSRP pela execução do comando *standby priority 150*, ou seja, no grupo HSRP ele é o de maior prioridade. A Figura 11 apresenta a interface *fast 0/0* desativada.

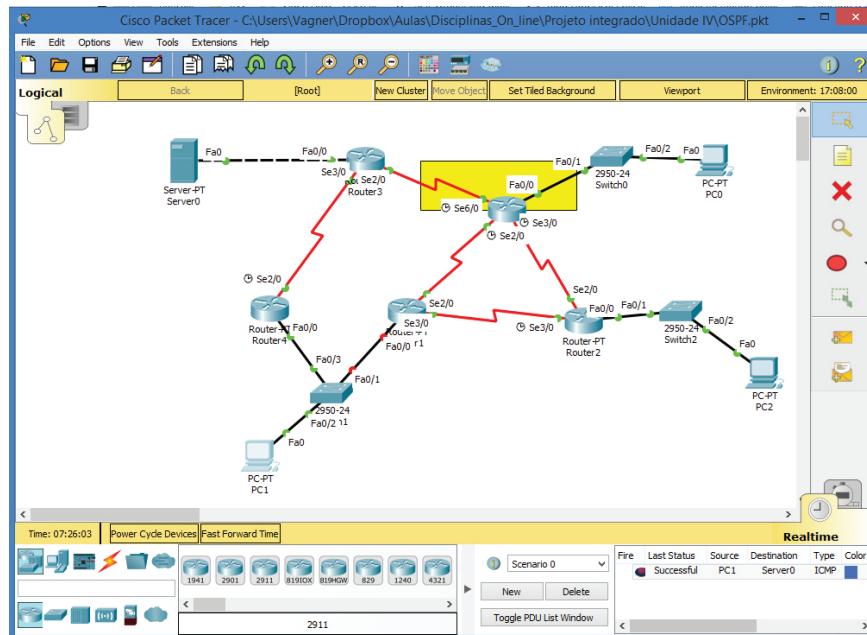
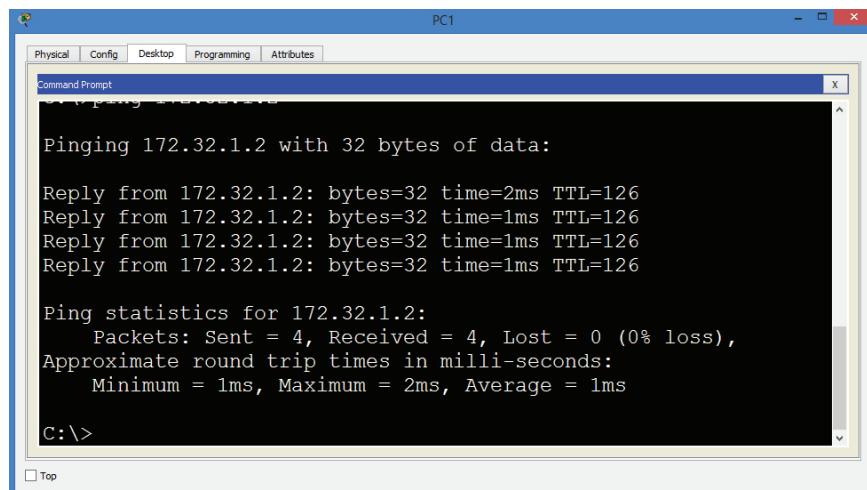


Figura 11 – Interface *FastEthernet 0/0* desativada

Fonte: Acervo do Conteudista

Agora, faça novamente o teste de conectividade e irá observar que os pacotes ainda estão sendo respondidos pelo servidor 0. A Figura 12 apresenta o resultado do comando “ping” com a interface *fastethernet* do roteador 1 desabilitada.



```
Pinging 172.32.1.2 with 32 bytes of data:
Reply from 172.32.1.2: bytes=32 time=2ms TTL=126
Reply from 172.32.1.2: bytes=32 time=1ms TTL=126
Reply from 172.32.1.2: bytes=32 time=1ms TTL=126
Reply from 172.32.1.2: bytes=32 time=1ms TTL=126

Ping statistics for 172.32.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\>
```

Figura 12 – Teste de conectividade do PC1

Fonte: Acervo do Conteudista

ACL (Access Control List – Lista de Controle de Acesso)

As listas de controle de acesso permitem o filtro de pacotes na rede, esse filtro pode ser feito tanto no sentido da rede interna para rede externa (*Proxy*), como também da rede externa para a rede interna (*Firewall*).

Esse filtro de pacotes auxilia na segurança da empresa e pode ser configurado nos roteadores de borda, permitindo acesso apenas aos pacotes que satisfaçam as regras configuradas nas Listas de Controle de Acesso.

Nos roteadores CISCO, podem ser configurados dois tipos de ACL: uma padrão, em que as regras são consideradas apenas para o endereço IP de origem, e outra estendida, em que vários outros campos e pacotes podem ser considerados nas listas de acesso.

Em cada lista de acesso, podemos configurar uma série de regras e podemos ter várias listas de acesso, cada uma com suas regras previamente definidas. As regras devem ser inseridas de forma lógica para se ter o efeito desejado, os pacotes são analisados considerando-se a ordem em que as regras foram inseridas e na primeira ocorrência que satisfaça uma das regras, os pacotes são negados ou permitidos.

Configurar as regras na lista de controle de acesso não faz com que elas sejam executadas. Além da configuração das regras, a lista de controle de acesso deve ser vinculada a uma interface e ainda indicar em que direção ela será considerada, se na direção de saída (*out*) da interface ou na direção de entrada (*in*) da interface.

Vamos utilizar a topologia já configurada para implementar uma lista de controle de acesso no roteador 2. A primeira regra que iremos inserir irá negar qualquer pacote gerado no PC2 para a rede externa, ou seja, esse computador só poderá se comunicar em sua rede LAN.

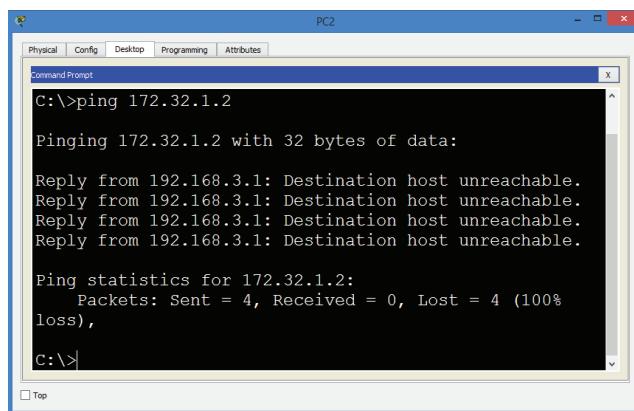
Entre no modo de configuração de linha no roteador 2 e vamos criar uma lista de controle de acesso padrão. Para isso, execute os comandos a seguir no roteador 2.

```
Router>enable  
Router#configure terminal  
Router(config)#access-list 1 deny 192.168.3.2  
Router(config)#access-list 1 permit any  
Router(config)#interface fastEthernet 0/0  
Router(config-if)#ip access-group 1 in
```

A lista de acesso criada está dentro da faixa numérica de uma ACL padrão (*access-list 1*), esse tipo de ACL considera apenas o endereço de origem para aplicar a regra. A primeira regra da ACL 1 nega os pacotes que têm o endereço IP de origem como 192.168.3.2 (*access-list 1 deny 192.168.3.2*), nessa mesma ACL foi colocada uma regra para permitir todos os outros pacotes (*access-list 1 permit any*).

Ao configurar uma ACL, o roteador implicitamente configura a negação de todos os outros pacotes que trafegam pela rede, esse é o motivo para inserir uma regra com a permissão para que todos os outros pacotes trafeguem normalmente (*access-list 1 permit any*). Caso não seja inserida a regra para permitir o tráfego de outros pacotes, eles serão descartados.

Teste a conectividade gerando pacotes do PC2 para qualquer outro computador que está remotamente. A Figura 13 apresenta o resultado do teste.



```
C:\>ping 172.32.1.2

Pinging 172.32.1.2 with 32 bytes of data:

Reply from 192.168.3.1: Destination host unreachable.

Ping statistics for 172.32.1.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
    c:\>
```

Figura 13 – Teste de conectividade do PC2

Fonte: Acervo do Conteudista

Como pode ser observado na Figura 13, não há comunicação, ou seja, a regra está funcionando. Para comprovar que somente o PC2 não pode trafegar com seus pacotes para a rede externa, insira mais um computador PC3 na topologia. A Figura 14 apresenta a topologia com o PC3 inserido.

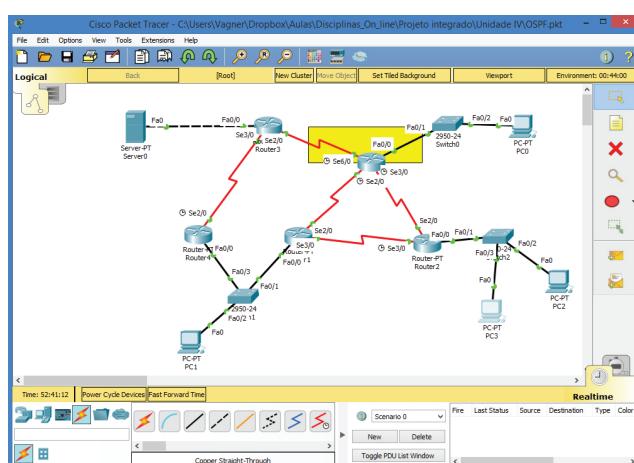
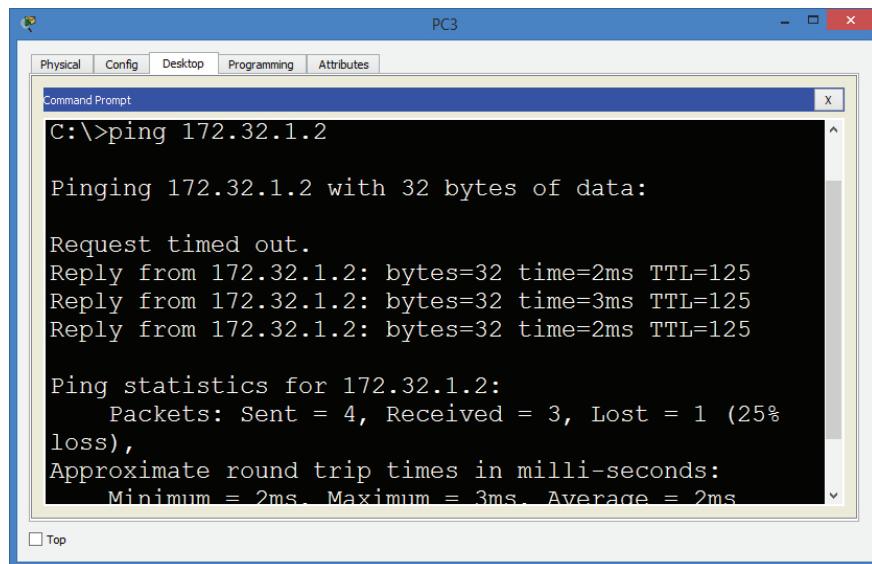


Figura 14 – PC3 inserido na topologia

Fonte: Acervo do Conteudista

Configure o PC3 com o endereço 192.168.3.3, máscara 255.255.255.0 e *default gateway* 192.168.3.1. Após a configuração, faça o teste de conectividade conforme Figura 15.



The screenshot shows a Windows Command Prompt window titled "PC3". The window has tabs at the top: Physical, Config, Desktop, Programming, and Attributes. The "Config" tab is selected. Inside the window, the command "ping 172.32.1.2" is entered, followed by its execution output:

```
C:\>ping 172.32.1.2

Pinging 172.32.1.2 with 32 bytes of data:

Request timed out.
Reply from 172.32.1.2: bytes=32 time=2ms TTL=125
Reply from 172.32.1.2: bytes=32 time=3ms TTL=125
Reply from 172.32.1.2: bytes=32 time=2ms TTL=125

Ping statistics for 172.32.1.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 3ms, Average = 2ms
```

Figura 15 – Teste de conectividade com o PC3

Fonte: Acervo do Conteudista

Como pode ser observado, o PC3 consegue alcançar o servidor 0 e o PC2, pela regra estabelecida, não consegue alcançá-lo.

É possível configurar várias outras regras em uma ACL, no entanto cabe uma observação em relação a projeto: é desejável que os roteadores de borda sejam configurados para dar vazão aos pacotes que cheguem até ele; sendo assim, as listas de controle de acesso devem ser evitadas nesses roteadores.

Atualmente, é mais adequado implementar um *firewall* entre o roteador de borda e a rede interna da empresa e deixar que o roteador de borda fique com a responsabilidade e tenha características para manter o tráfego na rede.

Material Complementar

Indicações para saber mais sobre os assuntos abordados nesta Unidade:

Sites

Configurar o NAT para permitir uma comunicação entre redes sobreposta

No *link* a seguir você poderá se aprofundar no conhecimento sobre o NAT.

<http://bit.ly/2052TiK>

Como usar o HSRP para fornecer redundância em uma rede BGP *multihomed*

No *link* a seguir você encontrará um texto com detalhes do HSRP e configuração.

<http://bit.ly/2Q0uqBM>

Vídeos

LabCisco: Configuração de Listas de Controle de Acesso

Aprenda detalhes sobre ACL.

https://youtu.be/EU_x-cx76oA

CISCO PACKET TRACER #1 - MONTANDO A ESTRUTURA DA REDE

O *packet tracer* é um simulador usado para configuração de equipamentos de redes, veja no vídeo a seguir como usá-lo.

<https://youtu.be/h1DSGTaxOSw>

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