Cisco | Networking Academy®
Mind Wide Open™

Atividade PT 6.4.1: Desafio: Integração das habilidades no Packet Tracer

Diagrama de topologia

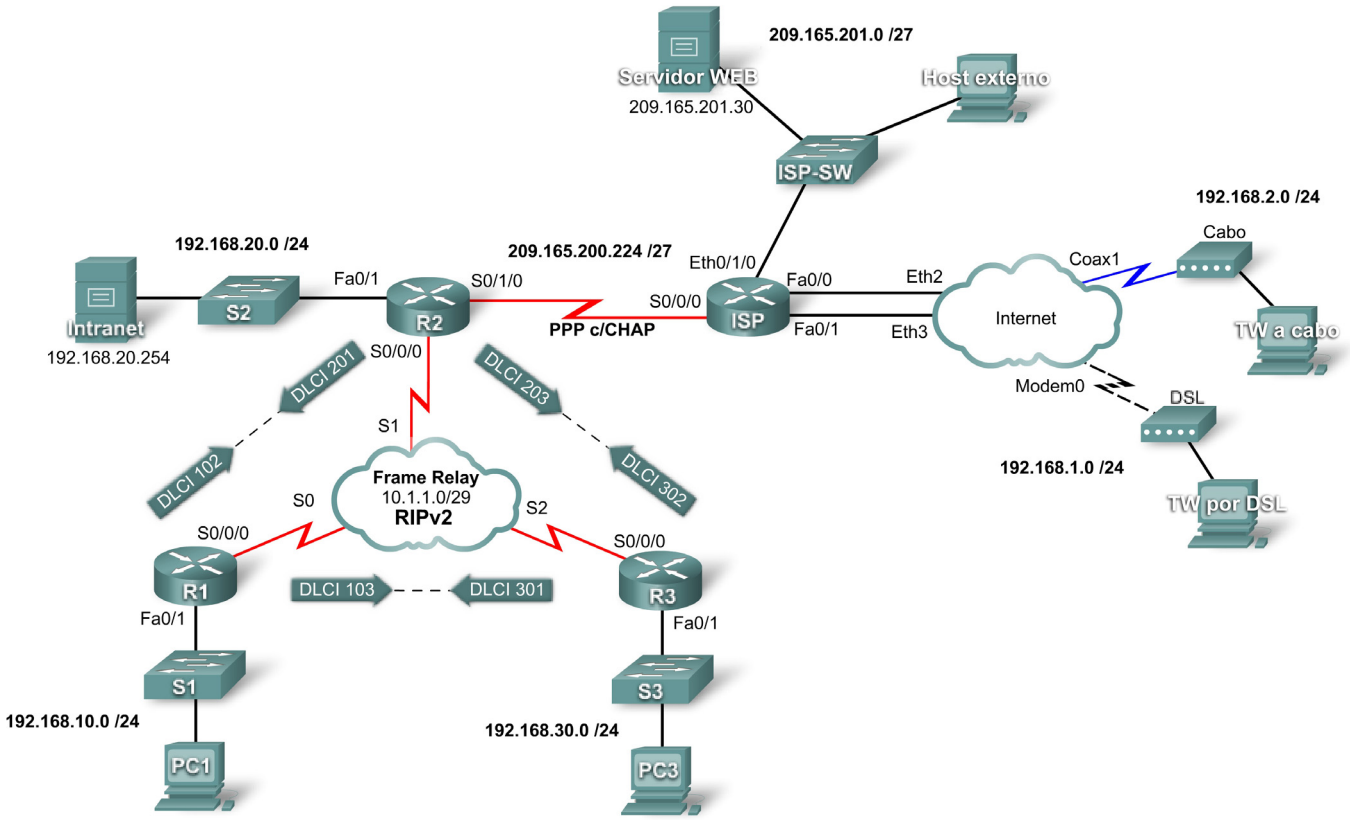

Tabela de endereçamento

Dispositivo	Interface	Endereço IP	Máscara de sub-rede
R1	**Fa0/1**	192.168.10.1	255.255.255.0
	S0/0/0	10.1.1.1	255.255.255.248
R2	**Fa0/1**	192.168.20.1	255.255.255.0
	S0/0/0	10.1.1.2	255.255.255.248
	S0/1/0	209.165.200.225	255.255.255.224
R3	**Fa0/1**	192.168.30.1	255.255.255.0
	S0/0/0	10.1.1.3	255.255.255.248
ISP	**S0/0/0**	209.165.200.226	255.255.255.224
	Eth0/1/0	209.165.201.1	255.255.255.224
	Fa0/0	192.168.1.1	255.255.255.0
	Fa0/1	192.168.2.1	255.255.255.0
PC1	**Placa de rede**	192.168.10.10	255.255.255.0
PC3	**Placa de rede**	192.168.30.10	255.255.255.0
Intranet	**Placa de rede**	192.168.20.254	255.255.255.0
TW por DSL	**Placa de rede**	192.168.1.10	255.255.255.0
TW a cabo	**Placa de rede**	192.168.2.10	255.255.255.0
Servidor Web	**Placa de rede**	209.165.201.30	255.255.255.224
Host de saída	**Placa de rede**	209.165.201.10	255.255.255.224

Objetivos de aprendizagem

- Aplicar configurações básicas de roteador.
- Configurar roteamento dinâmico e padrão.
- Estabelecer serviços de funcionário remoto.
- Testar a conectividade antes da configuração da ACL.
- Aplicar políticas ACL.
- Testar a conectividade depois da configuração da ACL.

Introdução

Esta atividade exige que você configure uma rota padrão bem como um roteamento dinâmico utilizando o RIP versão 2. Você também adicionará dispositivos de banda larga à rede. Por fim, você irá configurar as ACLs em dois roteadores para controlar o tráfego de rede. Como Packet Tracer é muito específico quanto à forma de classificação das ACLs, você precisará configurar as regras ACL na ordem fornecida.

Tarefa 1: Aplicar configurações básicas do roteador

Com as informações do diagrama de topologia e da tabela de endereçamento, defina as configurações básicas do dispositivo em R1, R2 e R3. Os nomes do host são configurados para você.

Inclua o seguinte:

- Console e linhas vty
- Banners
- Desabilite pesquisa de nome de domínio
- Descrições de interface

Tarefa 2: Configurar roteamentos dinâmico e padrão

Etapa 1. Configurar um roteamento padrão.

R2 precisa de uma rota padrão. Use o argumento *exit-interface* na configuração de rota padrão.

Etapa 2. Configurar um roteamento dinâmico.

Configure RIPv2 em R1, R2 e R3 para todas as redes disponíveis. R2 precisa passar sua configuração de rede padrão para os demais roteadores. Além disso, não se esqueça de utilizar o comando **passive-interface** em todas as interfaces ativas não utilizadas no roteamento.

Etapa 3. Verifique os resultados.

O percentual de conclusão deve ser 59%. Do contrário, clique em **Check Results** para ver a necessidade de componentes ainda não concluídos.

Tarefa 3: Estabelecer serviços de funcionário remoto

Etapa 1. Adicione dispositivos WAN.

Adicione uma DSL e um modem a cabo de acordo com o diagrama de topologia.

Etapa 2. Nomear os dispositivos WAN.

Use a guia **Config** para alterar o nome de exibição de cada dispositivo WAN para **Cable** e **DSL,** respectivamente.

Etapa 3. Conectar os dispositivos WAN.

Conecte os dispositivos WAN aos PCs e à Internet usando os cabos e as interfaces apropriados.

Etapa 4. Verifique os resultados.

O percentual de conclusão deve ser 86%. Do contrário, clique em **Check Results** para ver a necessidade de componentes ainda não concluídos.

Tarefa 4: Testar conectividade antes da configuração de ACL

Neste momento, todas as filiais da topologia devem ter conectividade. Alternar os modos de simulação e em tempo real pode agilizar a convergência.

Tarefa 5: Aplicar políticas ACL

Etapa 1. Criar e aplicar a política de segurança número 1.

Implemente as seguintes regras ACL usando o número 101 da ACL:

1. Dê a hosts na rede 192.168.30.0/24 acesso à Web em qualquer destino.
2. Dê a hosts na rede 192.168.30.0/24 acesso ICMP a qualquer destino.
3. Negue explicitamente qualquer outro acesso com origem na rede.

Etapa 2. Criar e aplicar a política de segurança número 2.

Como o ISP representa a conectividade com a Internet, configure uma ACL chamada **FIREWALL** na seguinte ordem:

1. Dê acesso Web via TW DSL ao servidor de Intranet.
2. Dê acesso Web via cabo TW ao servidor de Intranet.
3. Só permita respostas ping de entrada em ISP e em qualquer origem além dele.
4. Só permita sessões TCP estabelecidas em ISP e em qualquer origem além dele.
5. Bloqueie explicitamente todo o acesso de entrada do ISP e qualquer origem além do ISP.

Etapa 3. Verifique os resultados.

O percentual de conclusão deve ser 100%. Do contrário, clique em **Check Results** para ver a necessidade de componentes ainda não concluídos.

Tarefa 6: Testar conectividade depois da configuração de ACL

Os funcionários remotos não podem executar ping para o servidor de Intranet, mas podem acessar seu servidor HTTP pelo navegador. Incluídas na atividade estão três PDUs, duas das quais devem falhar e uma deve ter êxito. Verifique **Connectivity Tests** no menu **Check Results** para ter certeza de que os resultados da conclusão sejam 100%.

