



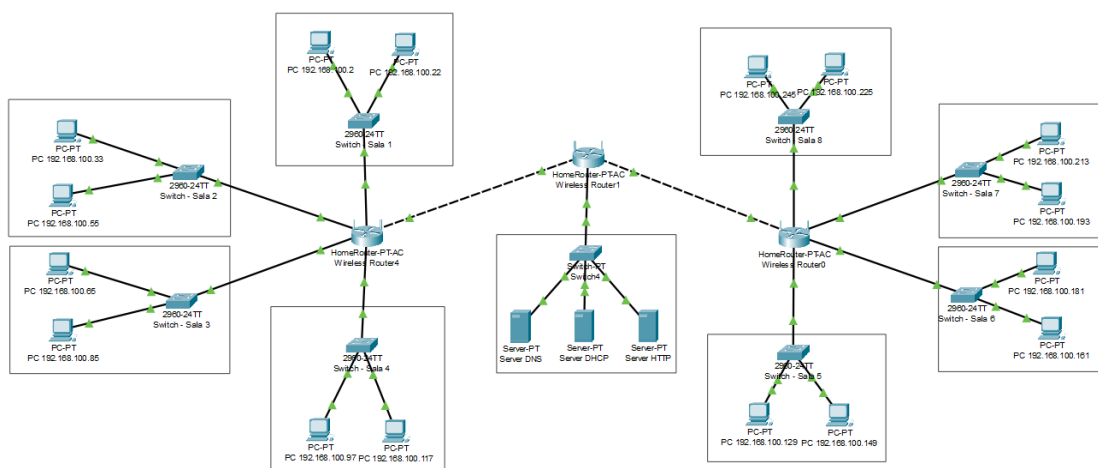
Prova 2º bimestre

Lívia Faria (00020451@fepi.edu.br), Lucas Faria (00019790@fepi.edu.br) e Wesley Bernardes (00020321@fepi.edu.br).

1) Uma rede de computadores com hub tem problemas de instabilidade e é necessário a implantação de um novo sistema com as seguintes características:

- A) O domínio de colisão deve ter separados os segmentos, mas pode-se ter mesmo domínio de broadcast;
- B) São 20 computadores em cada LAN e cada uma delas em um dos 08 prédios separados fisicamente;
- C) A ligação entre elas deve ser realizada por meio de roteadores;
- D) Cada LAN estar em uma rede separada;
- E) Os IPs devem ser estáticos;
- F) Deve ter serviços de DNS, DHCP e HTTP;
- G) A rede Wireless deve estar disponível.

Resposta:



O modelo construído, teve como objetivo sanar quaisquer problemas de instabilidade que um HUB proporcionava. Sendo assim, a equipe implantou roteadores para fazer uma ligação entre switches de oito prédios distintos à Internet. Cada prédio possui 20 computadores, inseridos em uma LAN e alocados em redes separadas com IPs configurados estaticamente.

Foram criados três servidores (DNS, HTTP, DHCP) que possuíam IPs iguais ao da tabela abaixo:

- **HTTP:** 192.168.100.247
- **DNS:** 192.168.100.248
- **DHCP:** 192.168.100.249

Foi definido como gateway padrão da rede o IP: 192.168.100.1.

Os IPs dos computadores foram definidos na tabela abaixo:

Local	Faixa de Endereço		Máscara
	Início	Fim	
Sala 01	192.168.100.0	192.168.100.30	255.255.255.224
Sala 02	192.168.100.32	192.168.100.62	255.255.255.224
Sala 03	192.168.100.64	192.168.100.94	255.255.255.224
Sala 04	192.168.100.96	192.168.100.126	255.255.255.224
Sala 05	192.168.100.128	192.168.100.158	255.255.255.224
Sala 06	192.168.100.160	192.168.100.190	255.255.255.224
Sala 07	192.168.100.192	192.168.100.222	255.255.255.224
Sala 08	192.168.100.224	192.168.100.254	255.255.255.224

2) Elabore os procedimentos para conexão com a internet

Para configurarmos uma rede sem fio no Windows, precisamos seguir certas regras que tornarão os acessos mais seguros.

Pré-requisitos:

- **Conexão de internet de banda larga ou modem.** Uma conexão de Internet de banda larga é uma conexão de Internet de alta velocidade. As conexões DSL e a cabo são duas das conexões de banda larga mais comuns. Para obter uma conexão de banda larga, entre em contato com um provedor de serviços de Internet (ISP). Normalmente, os ISPs que fornecem conexões DSL são companhias telefônicas, e os ISPs que fornecem conexões a cabo são empresas de TV a cabo. Muitas vezes, os ISPs oferecem modems de banda larga. Alguns ISPs também oferecem um modem/roteador sem fio combinado. Você também pode encontrá-los em lojas de computadores ou aparelhos eletrônicos, e online.
- **Roteador sem fio.** O roteador envia informações entre sua rede e a Internet. Com um roteador sem fio, você pode conectar os computadores a sua rede usando sinais de rádio em vez de cabos. Há vários tipos diferentes de tecnologias de rede sem fio, que incluem 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac e 802.11ax.
- **Adaptador de rede sem fio.** O adaptador de rede sem fio é um dispositivo que conecta seu computador a uma rede sem fio. Para conectar o computador portátil ou desktop a sua rede sem fio, o computador deve ter um adaptador de rede sem fio. A maioria dos laptops e tablets, além de alguns computadores desktop, vêm com um adaptador de rede sem fio já instalado.

Passos para conexão:

- **Configurando o modem e a conexão de internet:** quando tivermos todo o equipamento, iremos precisar configurar o modem e a conexão de Internet. Caso o modem não seja configurado pelo provedor de serviços de Internet (ISP), siga as instruções que acompanham o modem para conectá-lo ao computador e à Internet. Agora, se a rede está uma conexão DSL, conecte o modem à tomada do telefone. Se estivermos usando o cabo, conecte o modem a uma tomada de cabo.
- **Posicionando o roteador sem fio:** precisamos colocar o roteador sem fio em lugar onde ele receberá o sinal mais forte com o mínimo de interferência. Existem boas práticas como:
 - **Colocar o roteador sem fio em um local central,** assim podemos aumentar a intensidade do sinal sem fio por toda casa.
 - **Posicionar o roteador sem fio longe do chão, das paredes e de objetos de metal,** como arquivos de metal. Quando menos barreiras físicas houver

entre o computador e o sinal do roteador, maior a probabilidade de usar toda a intensidade do sinal do roteador.

- **Reduzir a interferência**, certos equipamentos de rede usam uma frequência de rádio de 2,4 GHz. Essa é a mesma frequência da maioria das micro-ondas e de muitos telefones sem fio. Se você ligar o micro-ondas ou receber uma chamada em um telefone sem fio, o sinal sem fio pode ser interrompido temporariamente. Você pode evitar a maioria desses problemas usando um telefone sem fio com frequência mais alta, como 5,8 GHz.
- **Protegendo a rede sem fio:** segurança sempre é importante; com uma rede sem fio, é ainda mais importante porque o sinal da rede pode ser transmitido para fora da casa. Se você não proteger sua rede, as pessoas com computadores próximos poderão acessar as informações armazenadas nos computadores da rede e usar sua conexão de Internet. Para conseguirmos torna a rede mais segura, podemos:
 - **Altere o nome de usuário padrão e a senha.** Isso ajuda a proteger o roteador. A maioria dos fabricantes de roteadores têm um nome de usuário e uma senha padrão no roteador, além de um nome de rede padrão (também conhecido como SSID). Alguém pode usar essas informações para acessar seu roteador sem você saber. Para evitar isso, mude o nome de usuário e a senha padrão do roteador. Veja instruções na documentação de seu dispositivo.
 - **Configure uma chave de segurança (senha) para sua rede.** As redes sem fio têm uma chave de segurança de rede que ajuda a protegê-las do acesso não autorizado. Recomendamos o uso Wi-Fi segurança do Acesso Protegido 3 (WPA3) se o roteador e o computador a suportam. Consulte a documentação do roteador para obter informações mais detalhadas, incluindo qual tipo de segurança é suportado e como defini-lo.

Alguns roteadores dão suporte à Configuração de Wi-Fi Protegido (WPS). Se o roteador der suporte a WPS e estiver conectado à rede, siga estas etapas para configurar uma chave de segurança de rede:

1. Faça o seguinte, dependendo de qual versão do Windows estiver em execução no seu computador:
 - No Windows 7 ou no Windows 8.1, selecione **Iniciar**, comece a digitar **Central de Rede e Compartilhamento** e então escolha-a na

lista.

- Em Windows 10, selecione **Iniciar**, em seguida, selecione **Configurações > Rede & Internet > Status > Central de Compartilhamento e Rede**.
- No Windows 11, selecione **Iniciar**, digite painel de controle e selecione **Painel de Controle > Rede e Internet > Central de Compartilhamento e Rede**.

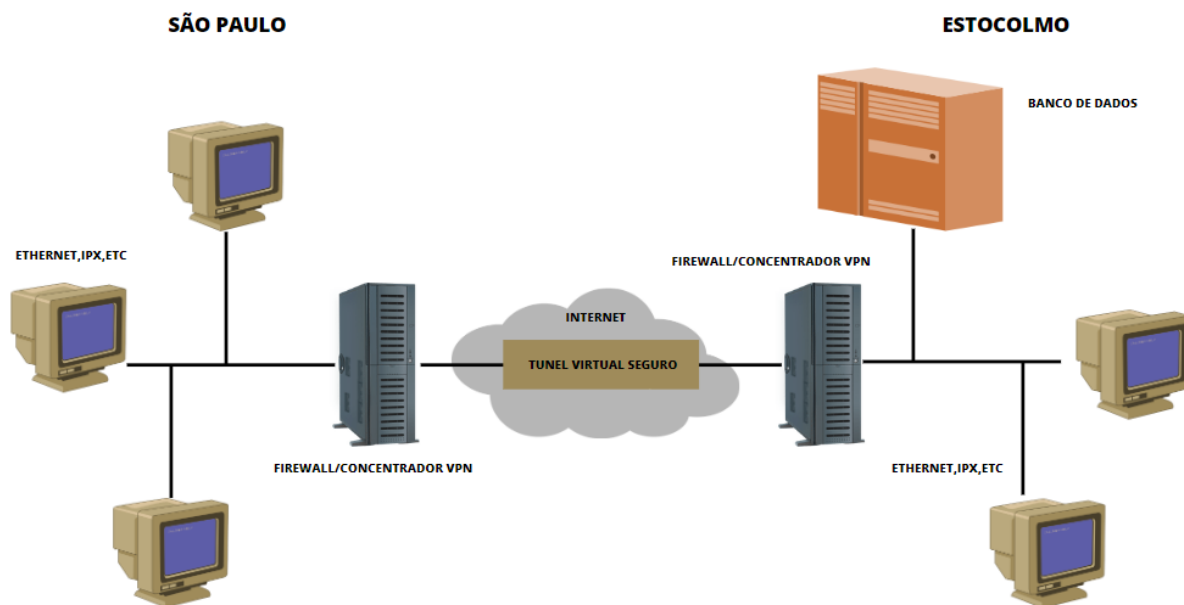
2. Escolha **Configurar uma nova conexão ou rede**.

3. Escolha **Configurar uma nova rede** e selecione **Avançar**.

O assistente o guiará pela criação de um nome de rede e uma chave de segurança. Se o roteador for compatível com ele, o assistente será padrão para a segurança do Acesso Protegido wi-fi (WPA2 ou WPA3). Recomendamos que você use o WPA3, se possível, porque ele oferece melhor segurança do que a segurança WPA2, WPA ou WEP (Privacidade Equivalente com Fio). Com WPA3, WPA2 ou WPA, você também pode usar uma frase-senha, para que não seja preciso lembrar de uma sequência enigmática de letras e números.

- **Anote a chave de segurança e guarde-a em um local seguro.** Você também pode salvar sua chave de segurança em um pen drive de acordo com as instruções do assistente. (Salvar sua chave de segurança em uma unidade flash USB está disponível no Windows 8 e Windows 7, mas não no Windows 10 ou Windows 11.)
- **Use um firewall.** Um firewall é um hardware ou software que ajuda a proteger seu computador de usuários não autorizados ou software mal-intencionado (malware). A execução de um firewall em cada computador de sua rede pode ajudar a controlar a disseminação de software mal-intencionado na rede e a proteger seus computadores quando você acessa a Internet. O Firewall do Windows está incluído nesta versão do Windows.

3) Faça a modelagem para a aplicação de VPN para a conexão das redes em outros pontos geográficos



A Rede Privada Virtual (VPN) é uma forma segura de compartilhamento de dados e informações entre organizações. No exemplo acima, temos como objetivo de enviar ou receber arquivos confidenciais entre a organização de São Paulo e Estocolmo. Este modelo, funciona da seguinte forma: os dados enviados da organização de São Paulo, passam por uma filtragem pelo Firewall inserido na rede e através do VPN, em uma rede pública, que seria a Internet, recebe uma chave para codificação. Assim chegando no Firewall da organização de Estocolmo, onde o arquivo será decodificado, analisado e entregue de forma limpa para empresa, sem qualquer tipo de desvio ou invasão na documentação.