AULA 1 — CISCO

Componentes da rede

As vantagens da rede ponto-a-ponto:

- Fácil de configurar;
- Menos complexo;
- Menor custo porque os dispositivos de rede e os servidores dedicados podem não ser necessários;
- Pode ser usada para tarefas simples como transferir arquivos e compartilhar impressoras.

As desvantagens das rede ponto-a-ponto:

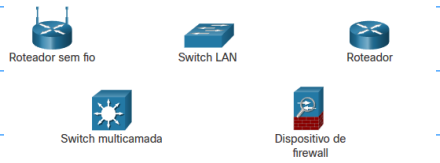
- Nenhuma administração centralizada;
- Não é tão segura;
- Não é escalável;
- Todos os dispositivos podem atuar como clientes e servidores, podendo deixar seu desempenho lento.

Dispositivos Finais

- É onde a mensagem se origina ou onde ela termina.

Dispositivos Intermediários

- Conectam os dispositivo finais à rede

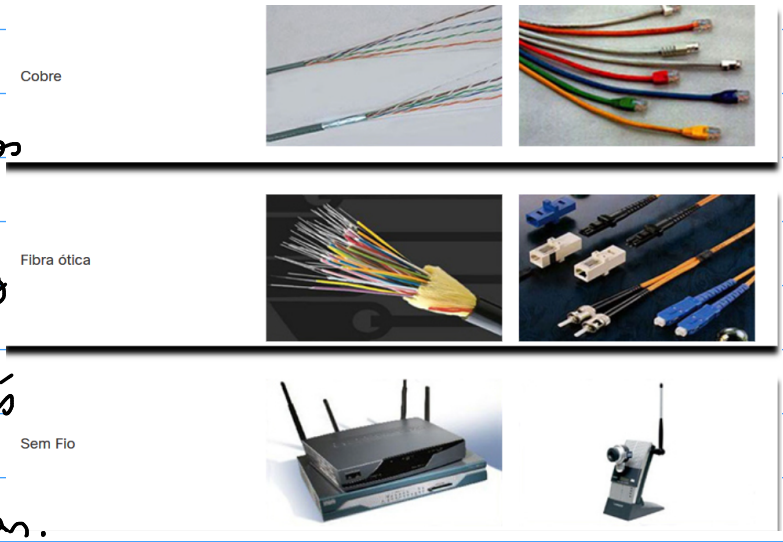


→ Principais funções

- Regenerar e retransmitir sinais de comunicação.
- Manter informações sobre quais caminhos existem pela rede e pela rede interconectada.
- Notificar outros dispositivos sobre erros e falhas de comunicação.
- Direcionar os dados por caminhos alternativos em caso de falhas
- Classificar e direcionar mensagens de acordo com as prioridades.
- Permitir ou negar fluxo de dados, com base nas configurações de segurança.

Meios de rede

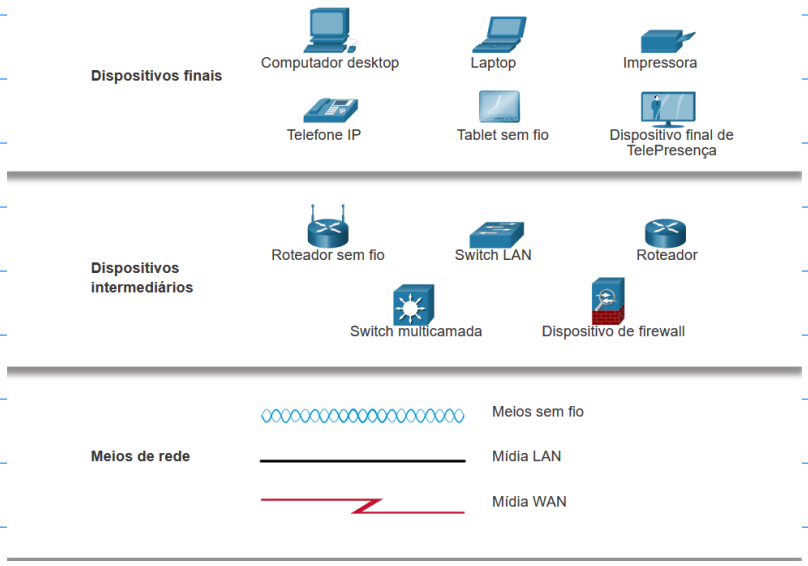
- Tipos principais
  - Fios de metal dentro de cabos
    - Dados são codificados em impulsos elétricos
  - Fibra de vidro ou plásticos (Fibra ótica)
    - Dados são codificados em pulsos de luz
  - Transmissão sem fio
    - Os dados são codificados através de modulação de frequências específicas de ondas eletromagnéticas.



Critérios para escolha.

- Qual é a distância máxima pela qual o meio físico consegue carregar um sinal com êxito?
- Qual é o ambiente em que a mídia será instalada?
- Qual é a quantidade de dados e a que velocidade deve ser transmitida?
- Qual é o custo do meio físico e da instalação?

Resumindo...



Além dessas representações, é utilizada terminologia especializada para descrever como cada um desses dispositivos e mídias se conectam:

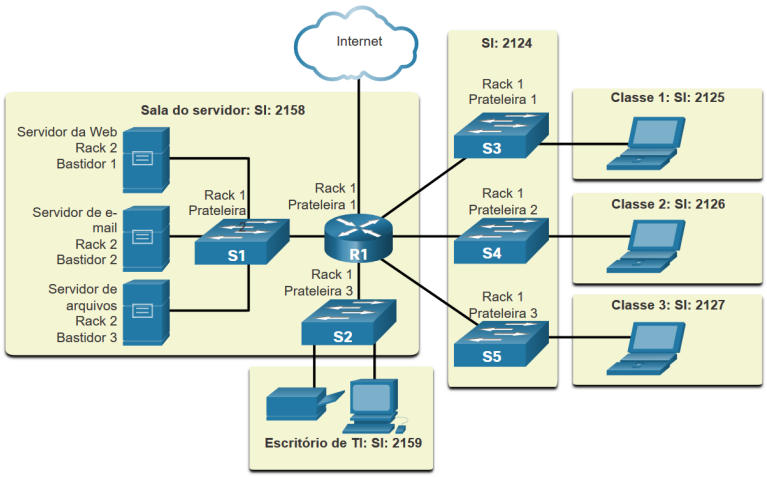
- Placa de interface de rede (NIC)
  - Uma NIC conecta fisicamente o dispositivo final à rede.

- Porta física
  - Um conector ou tomada em um dispositivo de rede onde a mídia se conecta a um dispositivo final ou outro dispositivo da rede.

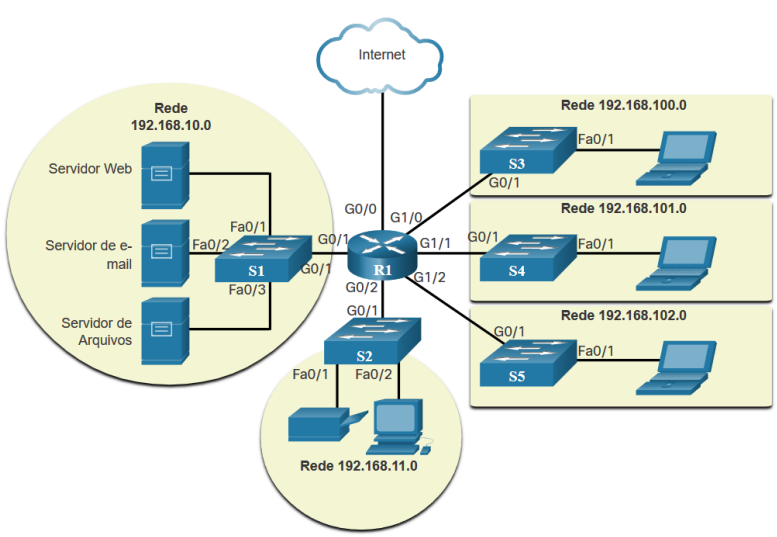
- Interface
  - Portas especializadas em um dispositivo de rede que se conectam a redes individuais. Como roteadores conectam redes, as portas em um roteador são chamadas de interfaces de rede.

▶ Diagramas de topologia

- Física

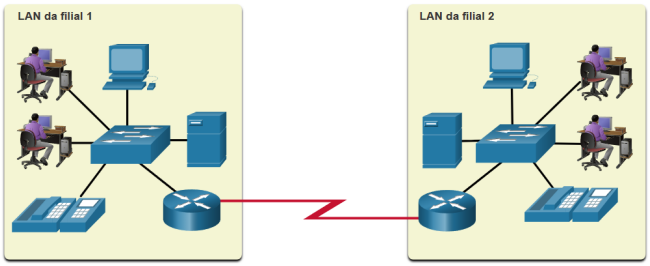


o Lógica



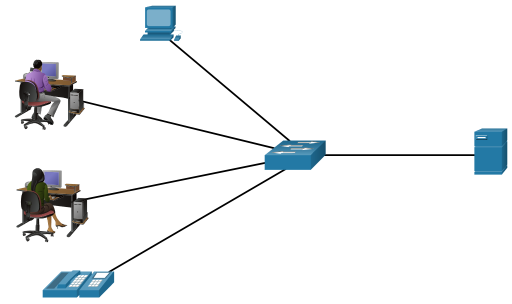
WANs e LANs

→ Infraestrutura de rede que abrange uma grande área geográfica



- Links com velocidades mais lentos entre os LANs.
- Administrada por vários Adms

→ Infraestrutura de rede que abrange uma pequena área geográfica



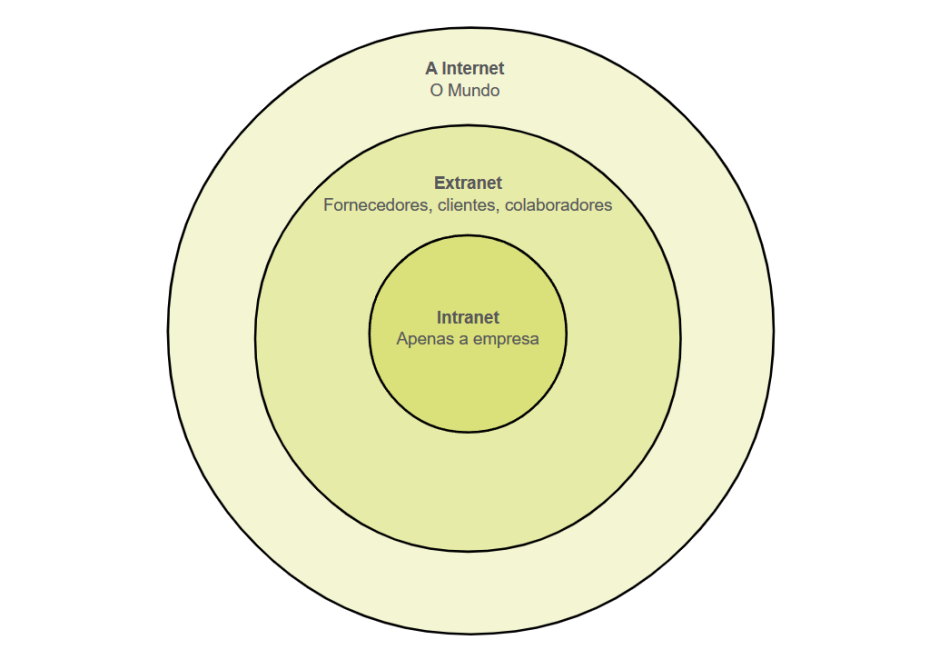
Uma rede que atende uma casa, prédio pequeno ou campus pequeno é considerada uma LAN.

- Maior largura de banda
- Apenas 1 Adm

Intranet e Extranet

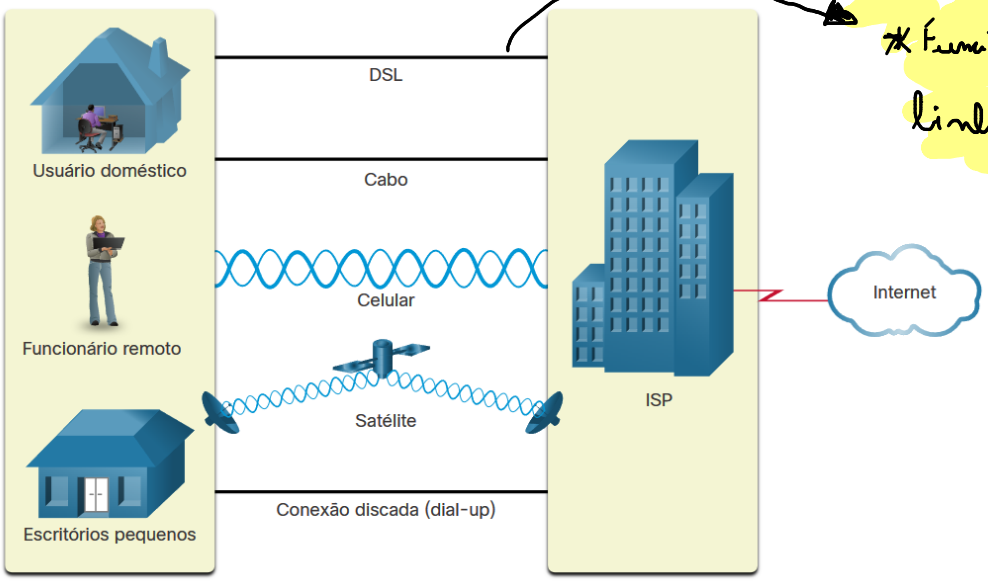
↳ Conexão privada de Wans e Lans

↳ Conexão mais pública, ou "de fora"



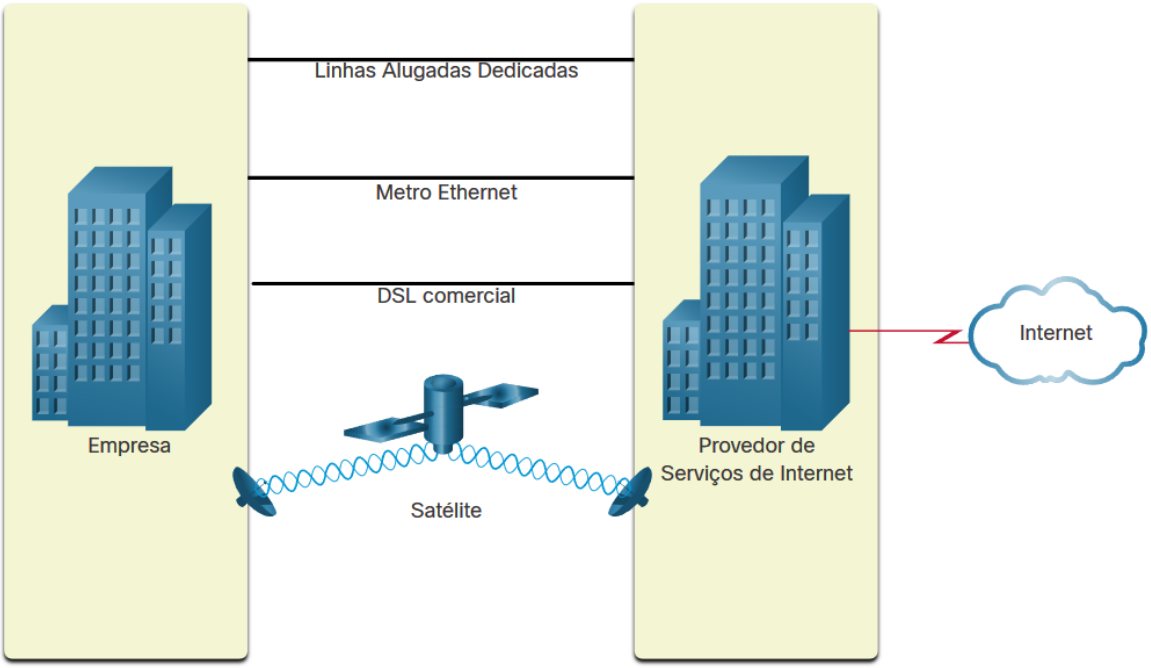
Conexões com internet para residências e pequenos escritórios.

* Funciona via ligação linha Telefônica



Conexões corporativas

Geralmente demanda maior largura de banda

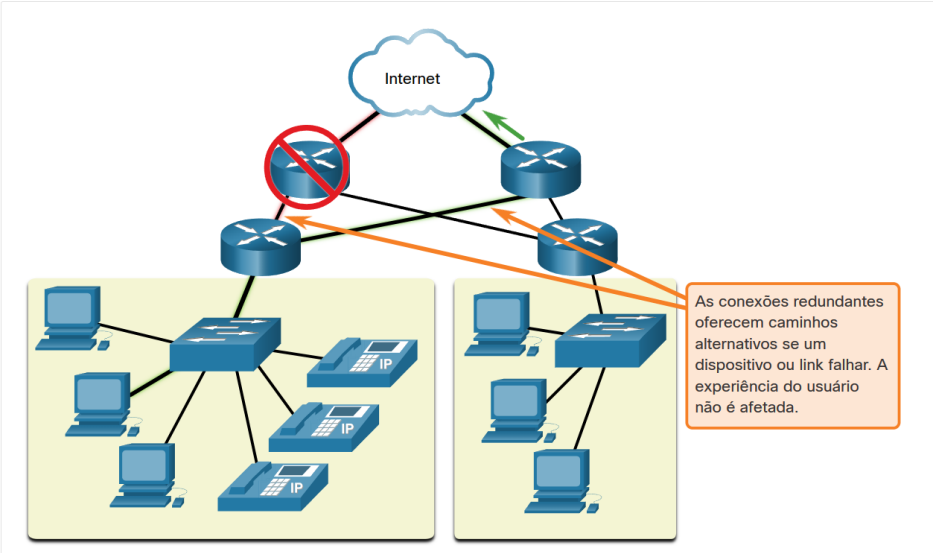


Arquitetura de redes

- Tolerância a falhas

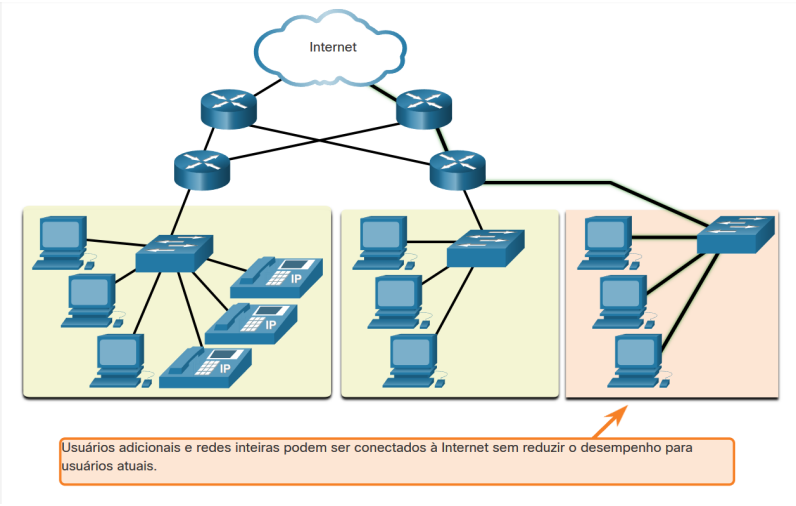
• Rede que limita o número de dispositivos afetados durante uma falha

↳ Divide as mensagens em vários blocos (Pacotes), onde cada pacote tem as informações de endereço necessários da origem e destino da mensagem.



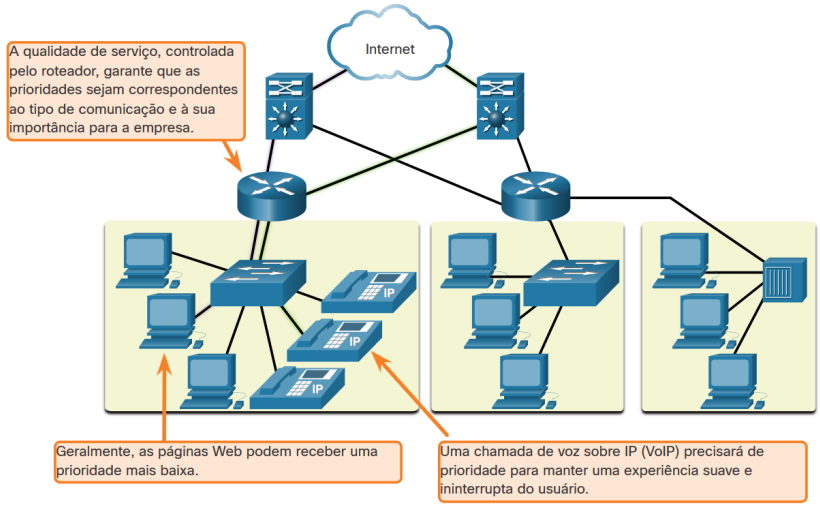
- Escalabilidade

° Capacidade da rede se expandir sem que os usuários já existentes sejam afetados (perca de desempenho).



- Qualidade do Serviço (QoS)

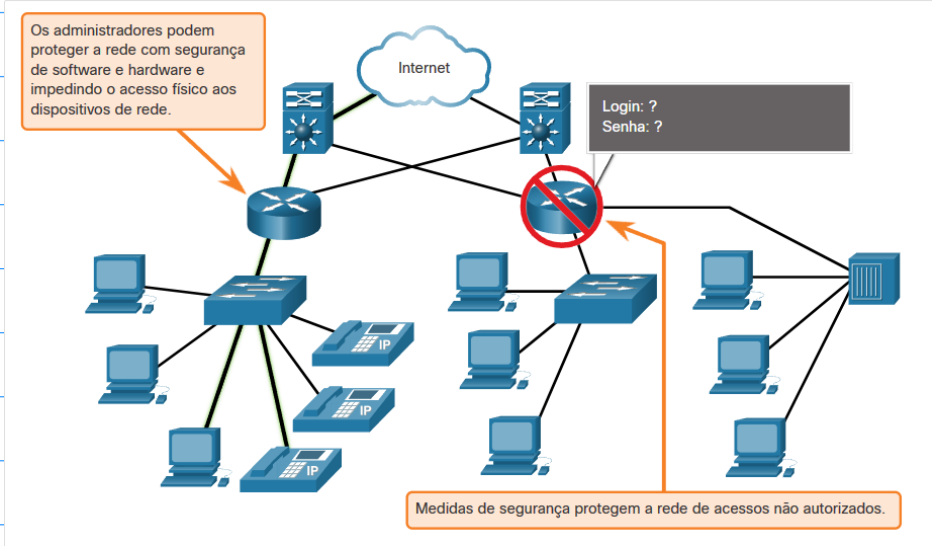
↳ O congestionamento acontece quando a demanda de largura de banda excede a quantidade disponível. (medido em bits por segundo)



— Segurança da rede

o Segurança da infraestrutura:

· Proteger fisicamente os dispositivos que fornecem conectividade de rede e impedir o acesso não autorizado aos softwares de gerenciamento.



* Para atender os de segurança de rede existem 3 requisitos:

1 — Confidencialidade

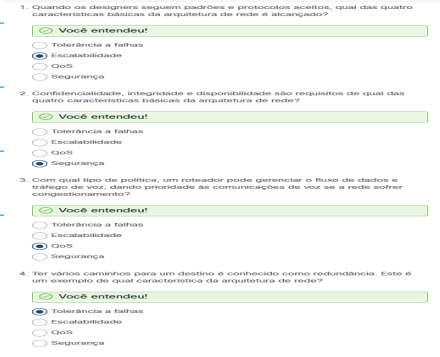
· Apenas os destinatários pretendidos e autorizados podem ler e acessar os dados.

2 — Integridade

· Garante que as informações não foram alteradas na Transmissão.

3 — Disponibilidade

· Garante aos usuários acesso oportuno e confiável aos serviços de dados para usuários autorizados.


1. Quando os designers seguem padrões e protocolos aceitos, qual das quatro características básicas da arquitetura de rede é alcançado?
Você entendeu!
Tolerância a falhas
Escalabilidade
QoS
Segurança
2. Confidencialidade, integridade e disponibilidade são requisitos de qual das quatro características básicas da arquitetura de rede?
Você entendeu!
Tolerância a falhas
Escalabilidade
QoS
Segurança
3. Com qual tipo de política, um roteador pode gerenciar o fluxo de dados e tráfego de voz, dando prioridade às comunicações de voz se a rede sofrer congestionamento?
Você entendeu!
Tolerância a falhas
Escalabilidade
QoS
Segurança
4. Ter vários caminhos para um destino é conhecido como redundância. Este é um exemplo de qual característica da arquitetura de rede?
Você entendeu!
Tolerância a falhas
Escalabilidade
QoS
Segurança

- Tendencias recentes

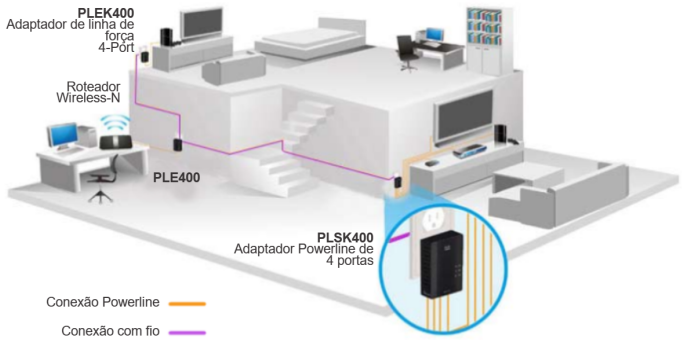
o BYOD → Uso de qualquer dispositivo, de qualquer propriedade e em qualquer lugar.

o Colaboração online → Trabalho de varias pessoas em parceria. Ex: Zoom, meet

o

o Rede Powerline

↳ Usa a fiação elétrica existente para conectar os dispositivos, através de um adaptadores padrão powerline



Você identificou com sucesso as respostas corretas.

1. As comunicações por vídeo são uma boa ferramenta de conferência para usar com outras pessoas localizadas em outro lugar da sua cidade, ou mesmo em outro país.
2. O recurso BYOD descreve o uso de ferramentas pessoais para acessar informações e se comunicar em uma rede comercial ou do campus.
3. A computação em nuvem contém opções como Público, Privado, Personalizado e Híbrido.
4. O Powerline está sendo usado ao conectar um dispositivo à rede usando uma tomada elétrica.
5. A banda larga sem fio usa a mesma tecnologia celular que um telefone inteligente.

- Banda larga sem fio

* WISPs → fornecedores de redes sem fio

* ISP (provedor de serviços de internet)

· organização que fornece acesso à internet para empresas e individuos

Existem várias ameaças externas comuns às redes:

- **Vírus, worms e cavalos de Tróia** - Eles contêm software ou código malicioso em execução no dispositivo do usuário.
- **Spyware e adware** - Estes são tipos de software que são instalados no dispositivo de um usuário. O software, em seguida, coleta secretamente informações sobre o usuário.
- **Ataques de dia zero** - Também chamados de ataques de hora zero, ocorrem no primeiro dia em que uma vulnerabilidade se torna conhecida.
- **Ataques de ator de ameaça** - Uma pessoa mal-intencionada ataca dispositivos de usuário ou recursos de rede.
- **Ataques de negação de serviço** - Esses ataques atrasam ou travam aplicativos e processos em um dispositivo de rede.
- **Interceptação de dados e roubo** - Esse ataque captura informações privadas da rede de uma organização.
- **Roubo de identidade** - Esse ataque rouba as credenciais de login de um usuário para acessar informações privadas.

Estes são os componentes básicos de segurança para uma rede doméstica ou de pequeno escritório:

- **Antivirus e antispyware** - Esses aplicativos ajudam a proteger os dispositivos finais contra a infecção por software malicioso.
- **Filtragem por firewall** - A filtragem por firewall bloqueia o acesso não autorizado dentro e fora da rede. Isso pode incluir um sistema de firewall baseado em host que impede o acesso não autorizado ao dispositivo final ou um serviço básico de filtragem no roteador doméstico para impedir o acesso não autorizado do mundo externo à rede.

1. Um ataque de DoS diminui a velocidade ou trava equipamentos e programas.
2. Uma VPN cria uma conexão segura para trabalhadores remotos.
3. Um firewall bloqueia o acesso não autorizado à sua rede.
4. Um ataque de dia zero ou hora zero ocorre no primeiro dia em que uma vulnerabilidade se torna conhecida.
5. Um vírus, worm ou cavalo de Tróia é um código malicioso em execução em dispositivos do usuário.