2023

Introdução às redes

Baseado no material da

CCNA CISCO

Módulo I – As redes hoje

Índice

1 - As redes de hoje

1.0 – Introdução: O que vou aprender neste módulo?
1.1 - Redes afetam nossas vidas
1.1.1 - Redes Conecte-nos
1.1.2 - Não Há Limites
1.2 - Componentes de rede
1.2.1 - Funções do Host
1.2.2 - Ponto a ponto
1.2.3 - Dispositivos Finais
1.2.4 - Dispositivos Intermediários
1.2.5 - Meios de rede
1.3 - Representações e topologias de rede
1.3.1 - Representações de Rede
1.3.2 - Diagramas de Topologia
1.4 - Tipos comuns de redes
1.4.1 - Redes de Vários Tamanhos
1.4.2 - LANs e WANs
1.4.3 - A Internet
1.4.4 - Intranets e Extranets
1.5 - Conexões com a Internet
1.5.1 - Tecnologias de Acesso à Internet
1.5.2 - Conexões com a Internet para Residências e Pequenos Escritórios
1.5.3 - Conexões Corporativas com a Internet
1.5.4 - A Rede Convergente
1.5.5 - *Packet Tracer*: representação da Rede
1.6 - Redes confiáveis
1.6.1 - Arquitetura de Redes
1.6.2 - Tolerância a Falhas
1.6.3 - Escalabilidade
1.6.4 - Qualidade do Serviço
1.6.5 - Segurança da rede
1.7 - Tendências das redes
1.7.1 - Tendências recentes
1.7.2 - Traga seu próprio dispositivo (BYOD)
1.7.3 - Colaboração On-line
1.7.4 - Comunicações em vídeo
1.7.5 - Computação em nuvem
1.7.6 - Tendências Tecnológicas em Casa
1.7.7 - Rede Powerline
1.7.8 - Banda Larga Sem Fio
1.8 - Segurança de Redes
1.8.1 - Ameaças à Segurança
1.8.2 - Soluções de Segurança
1.9 - Módulo Prático - O que eu aprendi neste módulo?

As redes de hoje

1.0 O que vou aprender neste módulo?

Título do módulo: As redes de hoje

Objetivo do módulo: Explicar os avanços em tecnologias de rede modernas.

Título do Tópico	Objetivo do Tópico
Redes afetam nossas vidas	Explicar como as redes afetam nossas vidas diárias.
Componentes de rede	Explicar como os dispositivos de host e de rede são usados.
Representações e topologias de rede	Explicar representações de rede e como elas são usadas na rede topologias.
Tipos comuns de redes	Comparar as características de tipos comuns de redes.
Conexões com a Internet	Explicar como LANs e WANs se interconectam com a Internet.
Redes confiáveis	Descrever os quatro requisitos básicos de uma rede confiável.
Tendências das redes	Explicar como tendências como BYOD, colaboração on-line, vídeo e nuvem a computação está mudando a forma como interagimos.
Segurança da rede	Identificar algumas ameaças e soluções básicas de segurança para todas as redes.

1.1Redes afetam nossas vidas

1.1.1 Redes Conecte-nos

Entre todas as coisas essenciais para a existência humana, a necessidade de interagir com os outros está logo abaixo das nossas necessidades básicas. A comunicação é quase tão importante para nós quanto nossa dependência de ar, água, comida e abrigo.

No mundo de hoje, com o uso de redes, estamos conectados como nunca estivemos. Pessoas que têm ideias podem se comunicar instantaneamente com as demais para torná-las uma realidade. Novos acontecimentos e descobertas são conhecidos no mundo inteiro em questão de segundos. Indivíduos podem até mesmo se conectar e jogar com seus amigos separados por oceanos e continentes.

1.1.2 Não Há Limites

Os avanços nas tecnologias de redes são talvez as mudanças mais significativas no mundo hoje. Eles estão ajudando a criar um mundo em que fronteiras nacionais, distâncias geográficas e limitações físicas se tornem menos relevantes, apresentando obstáculos cada vez menores.

A internet mudou a maneira pela qual nossas interações sociais, comerciais, políticas e pessoais ocorrem. A natureza imediata das comunicações pela Internet incentiva a criação de comunidades globais. As comunidades globais permitem a interação social que é independente de localização ou fuso horário.

A criação de comunidades on-line para a troca de ideias e informações tem o potencial de aumentar as oportunidades de produtividade ao redor do mundo.

A criação da nuvem nos permite armazenar documentos e imagens e acessá-los em qualquer lugar, a qualquer hora. Portanto, quer estejamos em um trem, em um parque ou em pé no topo de uma montanha, podemos acessar facilmente nossos dados e aplicativos em qualquer dispositivo.

1.2 Componentes de rede

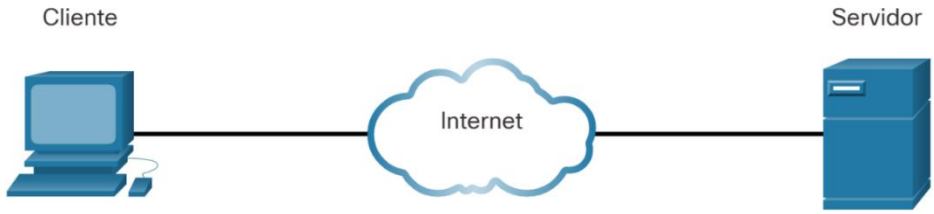
1.2.1 Funções do Host

Se você quiser fazer parte de uma comunidade on-line global, seu computador, tablet ou smartphone deve primeiro estar conectado a uma rede. Essa rede deve estar conectada à Internet. Este tópico discute as partes de uma rede. Veja se você reconhece esses componentes em sua própria rede doméstica ou escolar!

Todos os computadores que estão conectados a uma rede e participam diretamente da comunicação em rede são classificados como hosts. Os hosts podem ser chamados de dispositivos finais. Alguns hosts também são chamados de clientes. No entanto, o termo hosts refere-se especificamente a dispositivos na rede que recebem um número para fins de comunicação. Este número identifica o host dentro de uma rede específica. Este número é chamado de endereço IP (Internet Protocolo). Um endereço IP identifica o host e a rede à qual o host está conectado.

Servidores são computadores com software que lhes permite fornecer informações, como e-mail ou páginas da Web, para outros dispositivos finais na rede. Cada serviço exige um software de servidor separado. Por exemplo, um computador exige um software de servidor Web, para que possa prover serviços web à rede. Um computador com software de servidor pode fornecer serviços simultaneamente a muitos clientes diferentes.

Como mencionado anteriormente, os clientes são um tipo de host. Os clientes têm software para solicitar e exibir as informações obtidas do servidor, conforme mostrado na figura.



PC cliente e um servidor conectado através de uma nuvem simbolizando a Internet

Um exemplo de software cliente é um navegador, como Chrome ou FireFox. Um único computador pode também executar vários tipos de software cliente. Por exemplo, um usuário pode verificar o e-mail e visualizar uma página da Web enquanto troca mensagens instantâneas e ouve um fluxo de áudio. A tabela lista três tipos comuns de software de servidor.

Tipo	Descrição
E-mail	O servidor de executa o software do servidor de e-mail. Clientes usam cliente de e-mail software, como o Microsoft Outlook, para acessar o e-mail no servidor.
Web	O servidor web executa o software do servidor web. Os clientes usam software de navegador, como o Windows Internet Explorer, para acessar páginas da web no servidor.
Arquivo	O servidor de arquivos armazena arquivos corporativos e de usuário em um local central. Os dispositivos clientes acessam esses arquivos com software cliente, como o Explorador de arquivos do Windows.

1.2.2 Ponto a ponto

O software cliente e o servidor geralmente são executados em computadores separados, mas também é possível que um computador seja usado para ambas as funções ao mesmo tempo. Em pequenas empresas e em casas, muitos computadores funcionam como servidores e clientes na rede. Esse tipo de rede é chamado de rede ponto a ponto.

A imagem é uma pequena rede ponto a ponto com uma impressora à esquerda, conectada a um ponto de compartilhamento de impressão no meio, conectada a um peer de compartilhamento de arquivos à direita. Sob a topologia, há uma lista das vantagens e desvantagens da rede ponto a ponto. As vantagens da rede ponto a ponto: fácil de configurar, menos complexo e com menor custo, porque os dispositivos de rede e os servidores dedicados podem não ser necessários e podem ser usados para tarefas simples, como transferir arquivos e compartilhar impressoras. As desvantagens da rede ponto a ponto: sem administração centralizada, nem tão segura nem escalável, todos os dispositivos podem atuar como clientes e servidores, o que pode diminuir o desempenho.

As vantagens da rede peer-to-peer:

- 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.

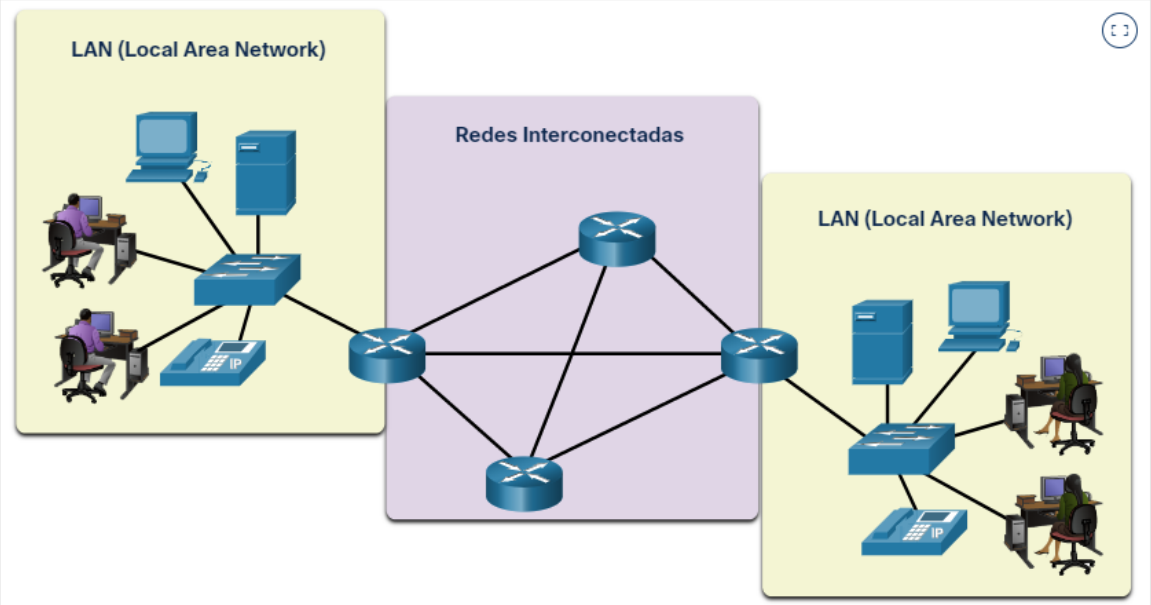
As desvantagens da rede peer-to-peer:

- Nenhuma administração centralizada;
- Não é tão segura;
- Não é escalável;

- Todos os dispositivos podem atuar como clientes e servidores, podendo deixar seu desempenho lento.

1.2.3 Dispositivos Finais

Os dispositivos de rede com os quais as pessoas estão mais familiarizadas são dispositivos finais. Para distinguir um dispositivo final de outro, cada dispositivo final em uma rede tem um endereço. Quando um dispositivo final inicia a comunicação, ele usa o endereço do dispositivo final de destino para especificar onde entregar a mensagem.



As mensagens podem seguir rotas alternativas.

Os dados se originam em um dispositivo final, fluem pela rede e chegam a outro dispositivo final.

1.2.4 Dispositivos Intermediários

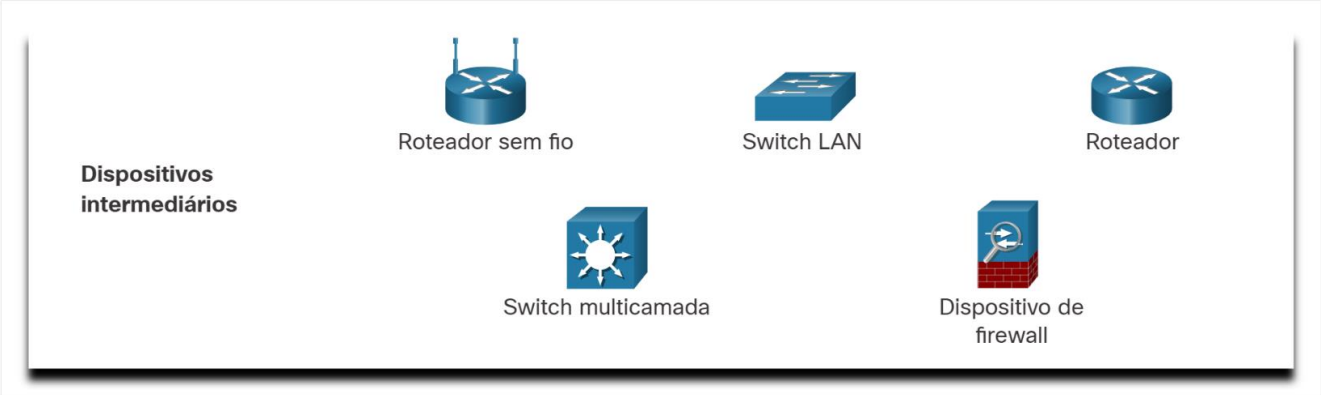
Dispositivos intermediários conectam os dispositivos finais individuais à rede. Eles podem conectar várias redes individuais para formar uma internetwork. Eles oferecem conectividade e asseguram que os dados fluam pela rede.

Esses dispositivos intermediários usam o endereço do dispositivo final de destino, em conjunto com as informações sobre as interconexões de rede, para determinar o caminho que as mensagens devem percorrer na rede. Exemplos dos dispositivos intermediários mais comuns e uma lista de funções são mostrados na figura.

Os dispositivos de rede intermediários executam algumas destas funções:

- Regenerar e retransmitir sinais de comunicação;
- Manter informação sobre quais caminhos existem pela rede e pela rede interconectada;
- Notificar outros dispositivos sobre erros e falhas de comunicação;
- Direcionar dados por caminhos alternativos quando houver falha em um link;
- Classificar e direcionar mensagens de acordo com as prioridades;
- Permitir ou negar o fluxo de dados, com base em configurações de segurança.

Observação: Não mostrado é um hub Ethernet herdado. Um hub Ethernet também é conhecido como repetidor multiporta. Os repetidores regeneram e retransmitem sinais de comunicação.



Observe que todos os dispositivos intermediários executam a função de um repetidor.

1.2.5 Meios de rede

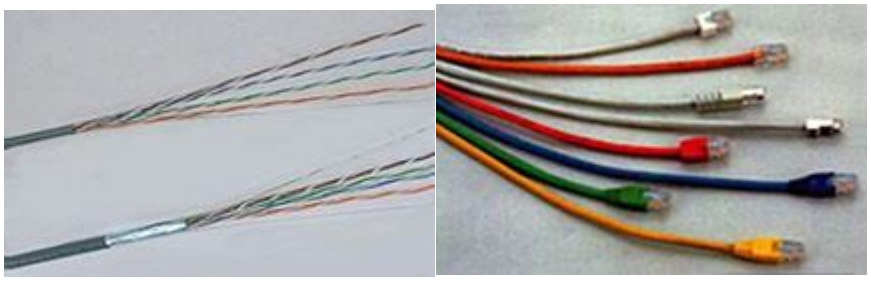
A comunicação transmite através de uma rede na mídia. A mídia fornece o canal pelo qual a mensagem viaja da origem ao destino.

As redes modernas usam principalmente três tipos de mídia para interconectar dispositivos, como mostrado na figura:

- **Fios de metal dentro de cabos** - Os dados são codificados em impulsos elétricos.
- **Fibras de vidro ou plástico nos cabos (cabo de fibra óptica)** - Os dados são codificados em pulsos de luz.
- **Transmissão sem fio** - Os dados são codificados através da modulação de frequências específicas de ondas eletromagnéticas.

Há três imagens de mídia de rede comum seguidas de critérios a serem usados ao escolher mídia de rede. A imagem superior mostra fios de par trançado e conectores usados com mídia de cobre. A imagem do meio é um cabo de fibra óptica multi-strand e conectores de fibra óptica. A imagem inferior mostra dispositivos sem fio, incluindo um roteador e uma câmera. Critérios a considerar ao escolher a mídia de rede: Qual é a distância máxima que a mídia pode transmitir com sucesso um sinal? 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?

Cobre



Fibra ótica

Sem fio

Critérios a serem considerados ao escolher a mídia de rede:

- 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?

Diferentes tipos de meios de rede possuem diferentes características e benefícios. Nem todos os meios de rede têm as mesmas características, nem são apropriados para a mesma finalidade.

1.3 Topologias de rede

1.3.1 Representações de Rede

Arquitetos e administradores de rede devem ser capazes de mostrar como suas redes serão. Eles precisam ser capazes de ver facilmente quais componentes se conectam a outros componentes, onde eles serão localizados e como eles serão conectados. Os diagramas de redes geralmente usam símbolos, como os mostrados na figura, para representar os diferentes dispositivos e conexões que compõem uma rede.

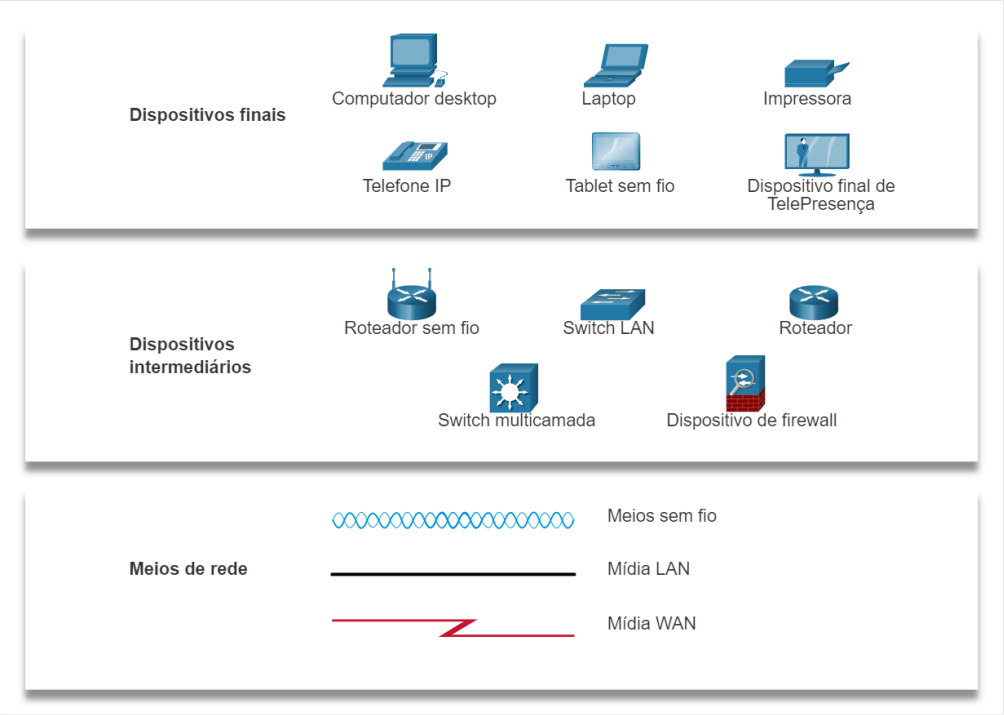
Um diagrama fornece uma maneira fácil de entender como os dispositivos se conectam em uma rede grande. Esse tipo de "fotografia" de uma rede é conhecido como um diagrama de topologia. A capacidade de reconhecer as representações lógicas dos componentes físicos de rede é crucial para se permitir visualizar a organização e a operação de uma rede.

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

Observação: Os termos porta e interface são frequentemente usados alternadamente.

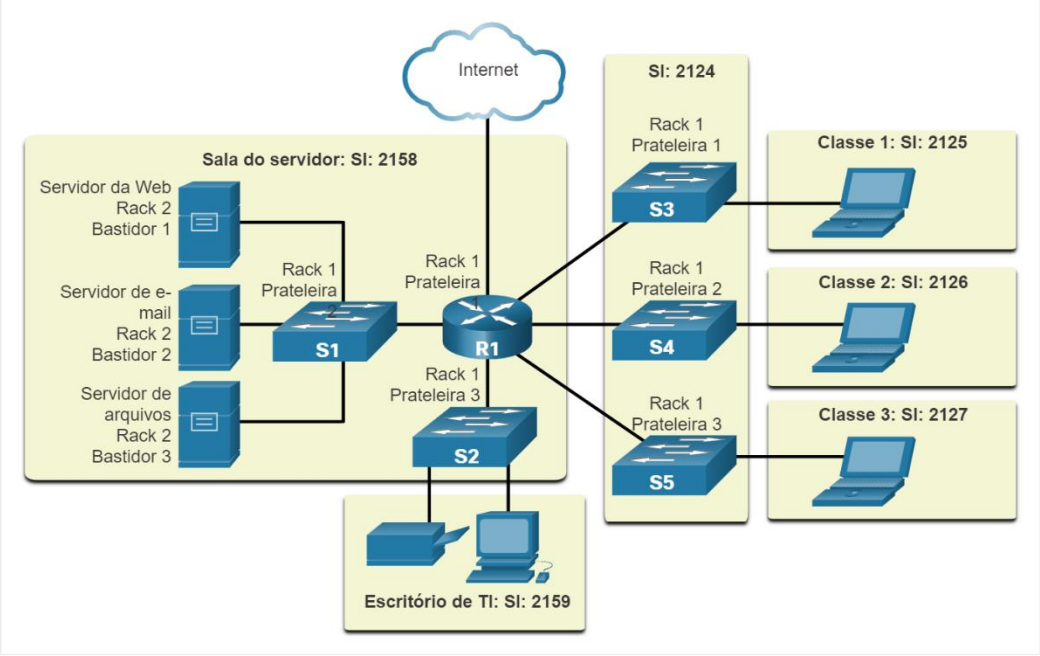
1.3.2 Diagramas de Topologia



Os diagramas de topologia são documentação obrigatória para qualquer pessoa que trabalhe com uma rede. Eles fornecem um mapa visual de como a rede está conectada. Existem dois tipos de diagramas de topologia: físicos e lógicos.

Diagramas de topologia física

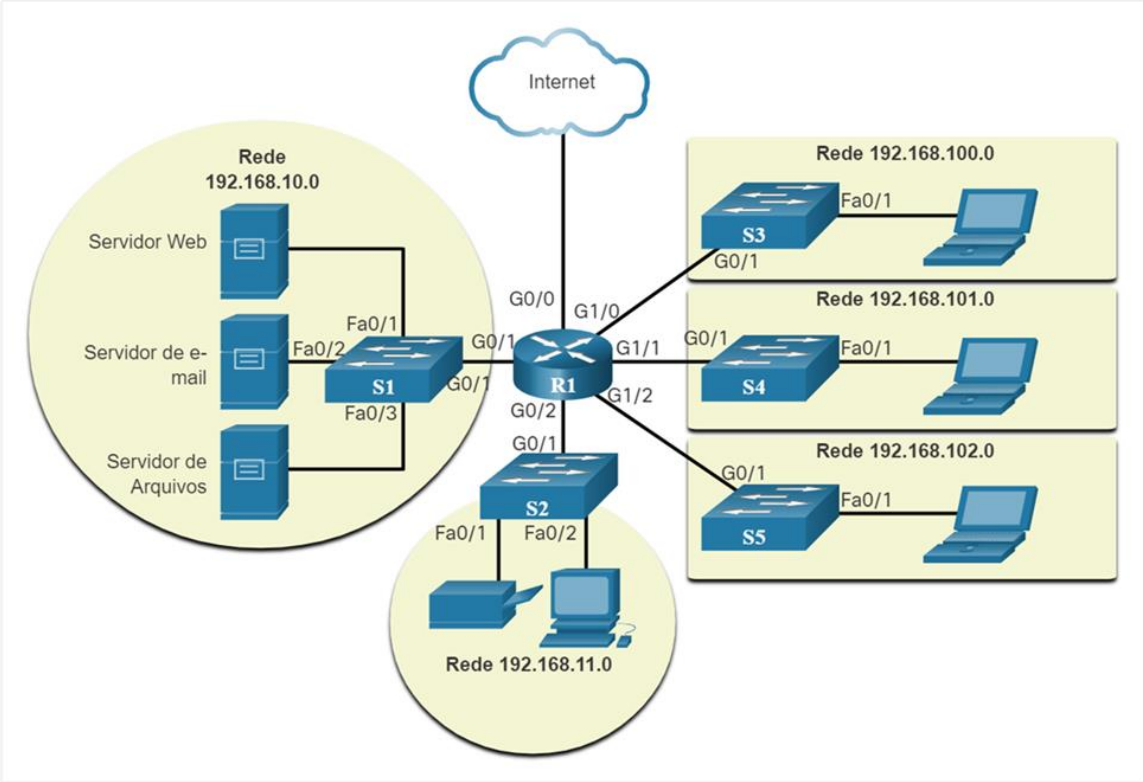
Os diagramas de topologia física ilustram a localização física dos dispositivos intermediários e a instalação dos cabos, conforme mostrado na figura. Você pode ver que as salas em que esses dispositivos estão localizados estão rotuladas nesta topologia física.



Diagramas de topologia lógica

Diagramas de topologia lógica ilustram dispositivos, portas e o esquema de endereçamento da rede, conforme mostrado na figura. Você pode ver quais dispositivos finais estão conectados a quais dispositivos intermediários e que mídia está sendo usada.

As topologias mostradas nos diagramas físico e lógico são apropriadas para seu nível de entendimento nesse momento do curso. Pesquise na Internet "diagramas de topologia de rede" para ver alguns exemplos mais complexos. Se você adicionar a palavra "cisco" para sua frase de pesquisa, você encontrará muitas topologias usando ícones semelhantes ao que você viu nessas figuras.



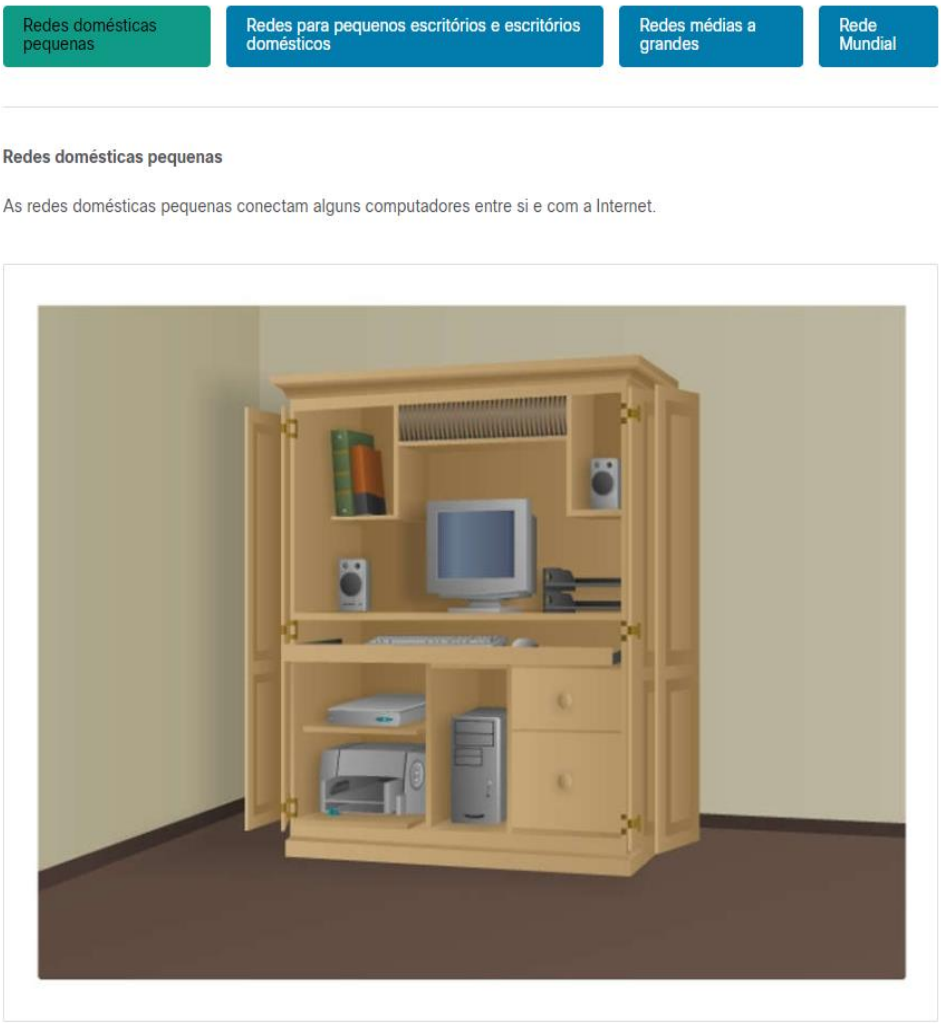
1.4 Tipos comuns de redes

1.4.1 Redes de Vários Tamanhos

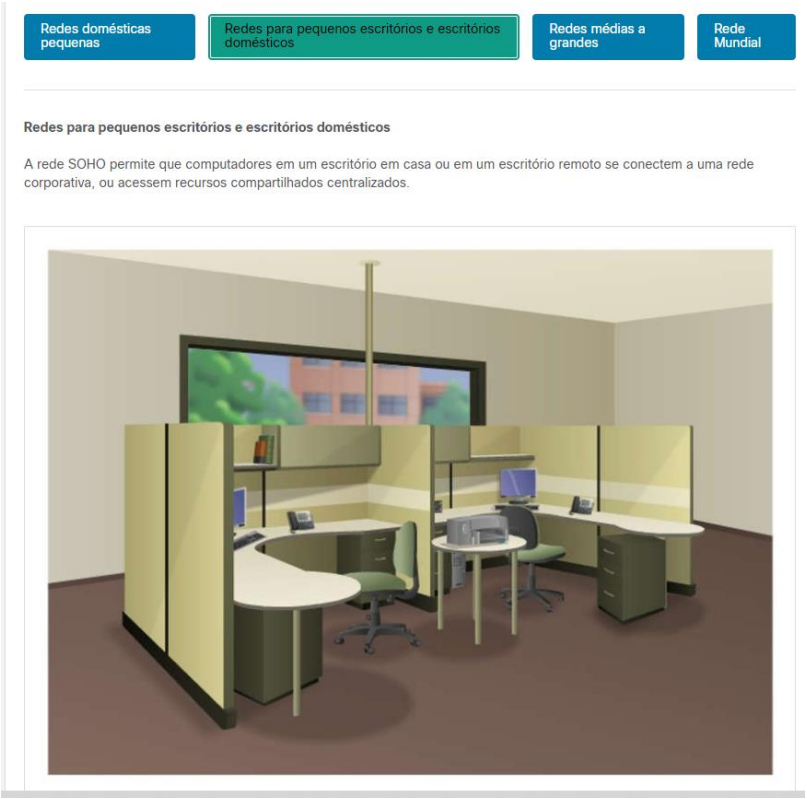
Agora que você está familiarizado com os componentes que compõem as redes e suas representações em topologias físicas e lógicas, você está pronto para aprender sobre os muitos tipos diferentes de redes.Existem redes de vários tamanhos. Eles variam de redes simples compostas por dois computadores a redes que conectam milhões de dispositivos.As redes domésticas simples permitem que você compartilhe recursos, como impressoras, documentos, imagens e música, entre alguns dispositivos finais locais.

As redes de pequeno escritório e escritório doméstico (SOHO) permitem que as pessoas trabalhem em casa ou em um escritório remoto. Muitos trabalhadores independentes usam esses tipos de redes para anunciar e vender produtos, pedir suprimentos e se comunicar com os clientes. Empresas e grandes organizações usam redes para fornecer consolidação, armazenamento e acesso a informações em servidores de rede. As redes fornecem e-mail, mensagens instantâneas e colaboração entre funcionários. Muitas organizações usam a conexão de sua rede à Internet para fornecer produtos e serviços aos clientes.A internet é a maior rede existente. Na verdade, o termo Internet significa uma "rede de redes". É uma coleção de redes públicas e privadas interconectadas. Em pequenas empresas e residências, muitos computadores funcionam como servidores e clientes na rede. Esse tipo de rede é chamado de rede ponto a ponto.

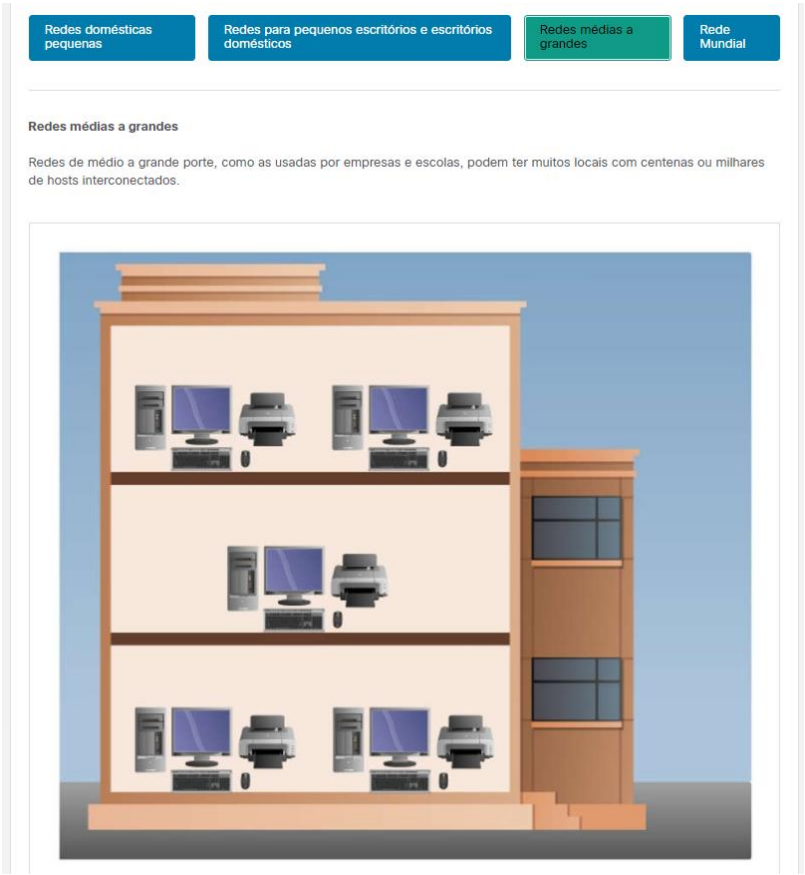
Redes domésticas pequenas



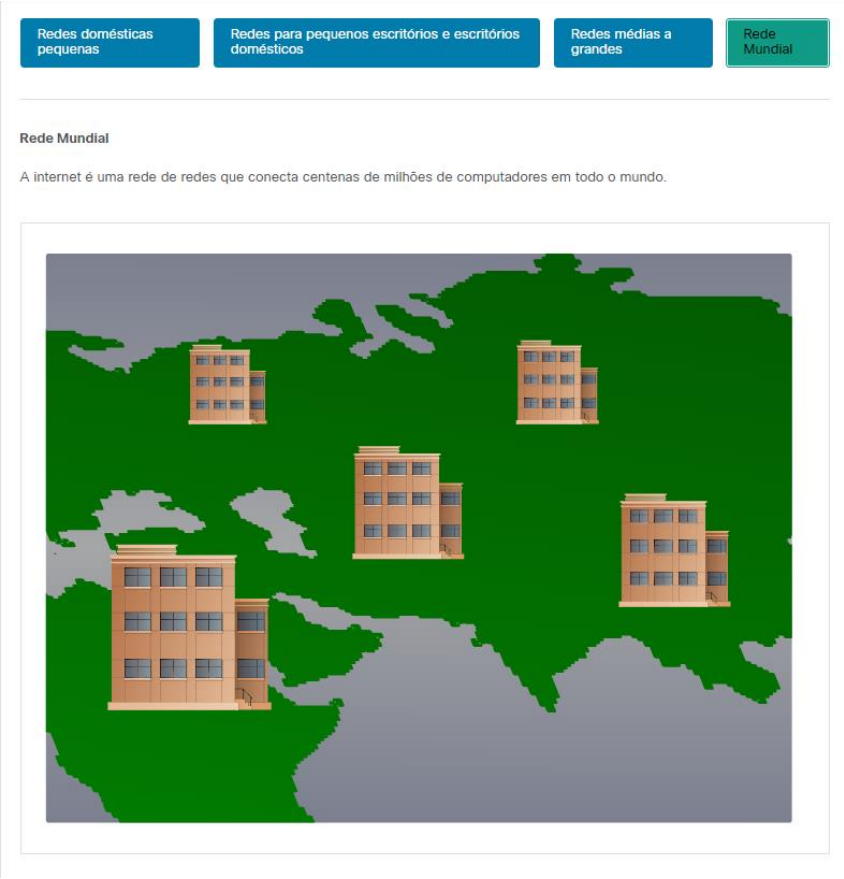
Redes para pequenos escritórios e escritórios domésticos (SOHO - Small Office Home Office)



Redes médias a grandes



Rede Mundial



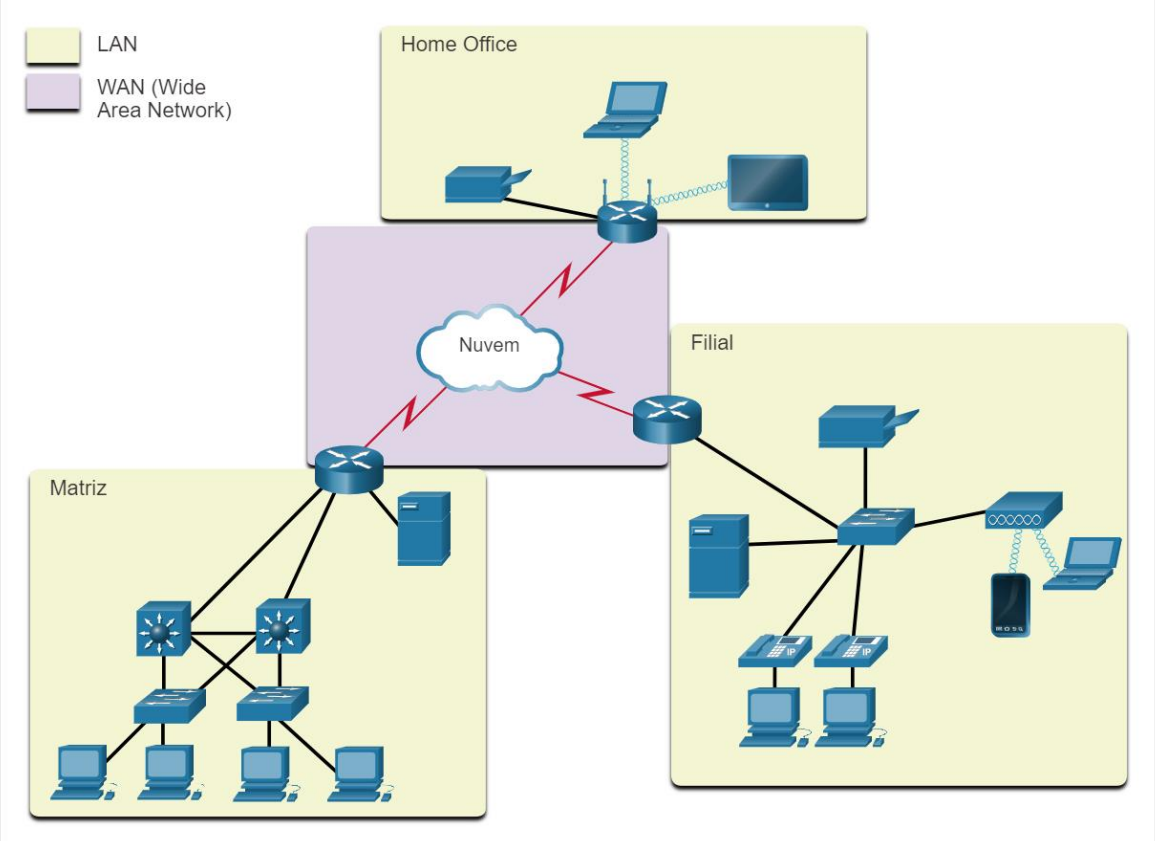
A internet é uma rede de redes que conecta centenas de milhões de computadores em todo o mundo. Redes mundiais mostrando um mapa global com cinco edifícios

1.4.2 LANs e WANs

As infra-estruturas de rede variam muito em termos de:

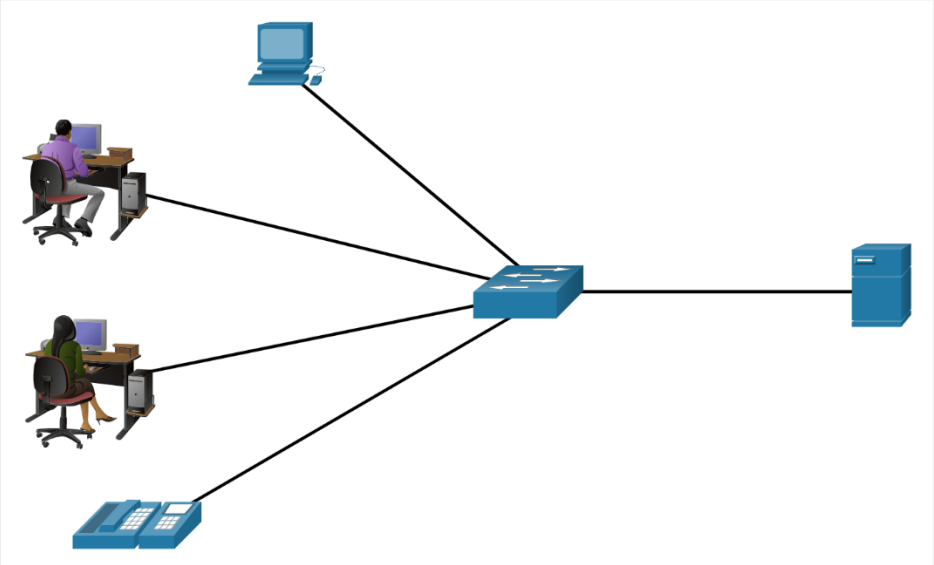
- Tamanho da área coberta;
- Número de usuários conectados;
- Número e tipos de serviços disponíveis;
- Área de responsabilidade.

Os dois tipos mais comuns de infraestruturas de rede são as redes locais (LANs) e as redes de longa distância (WANs). Uma LAN é uma infraestrutura de rede que fornece acesso a usuários e dispositivos finais em uma pequena área geográfica. Normalmente, uma LAN é usada em um departamento dentro de uma empresa, uma casa ou uma rede de pequenas empresas. Uma WAN é uma infraestrutura de rede que fornece acesso a outras redes em uma ampla área geográfica, que normalmente pertence e é gerenciada por uma corporação maior ou por um provedor de serviços de telecomunicações. A figura mostra LANs conectadas a uma WAN.



LANs

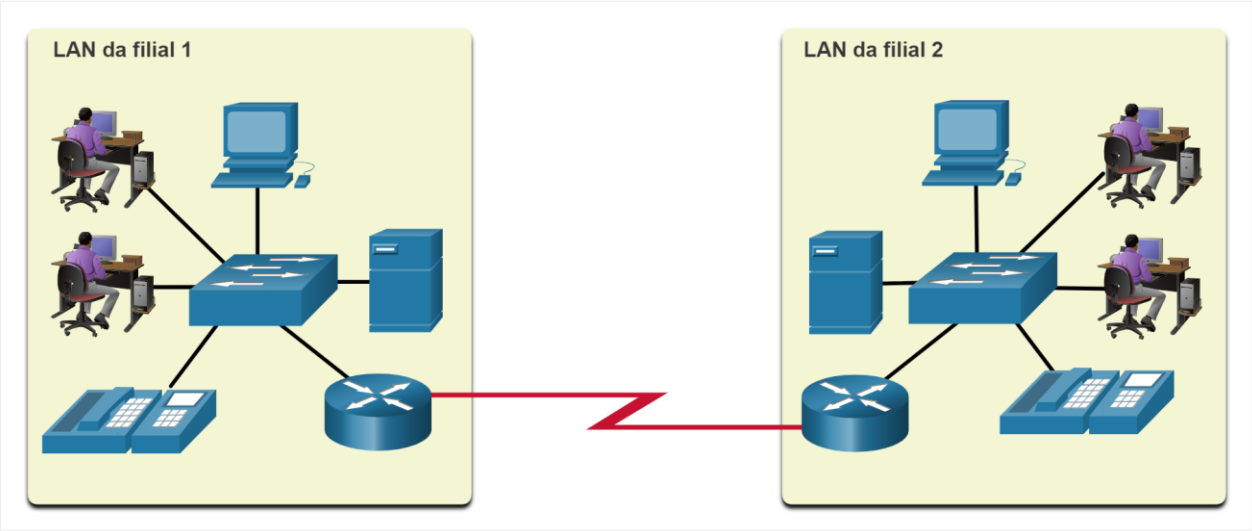
Uma LAN é uma infraestrutura de rede que abrange uma pequena área geográfica. As LANs têm características específicas:



- LANs interconectam dispositivos finais em uma área limitada, como uma casa, uma escola, um edifício de escritórios ou um campus.
- Uma LAN é geralmente administrada por uma única organização ou pessoa. O controle administrativo é imposto no nível da rede e governa as políticas de segurança e controle de acesso.
- As LANs fornecem largura de banda de alta velocidade para dispositivos finais internos e dispositivos intermediários, conforme mostrado na figura.

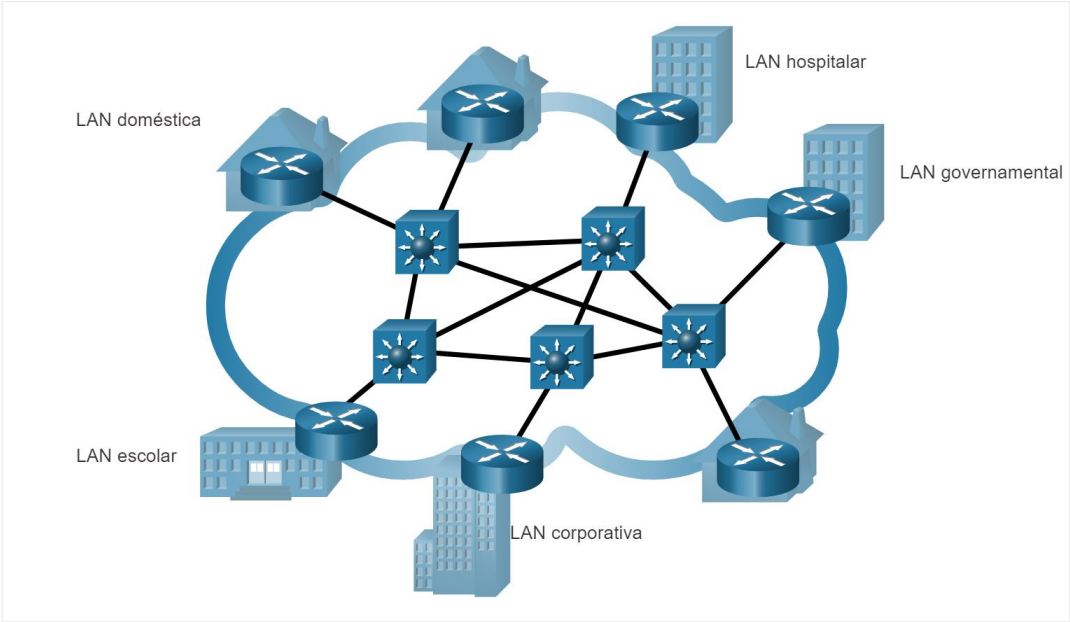
Uma rede que atende uma casa, prédio pequeno ou campus pequeno é considerada uma LAN.

WANs



1.4.3 A Internet

A internet é uma coleção mundial de redes interconectadas (internetworks, ou internet para abreviar). A figura mostra uma maneira de visualizar a Internet como uma coleção de LANs e WANs interconectadas.



As LANs utilizam serviços WAN para se interconectarem.

Algumas LANs do exemplo são conectadas entre si por meio de uma WAN. As WANs estão conectadas entre si. As linhas de conexão de WAN, em vermelho, representam todas as variações de modos de conexão de rede. As WANs podem se conectar através de fios de cobre, cabos de fibra ótica e transmissões sem fio (não mostradas).

A internet não é de propriedade de nenhum indivíduo ou grupo. Garantir a comunicação efetiva por essa infraestrutura diversa exige a aplicação de tecnologias e protocolos consistentes

e geralmente reconhecidos, bem como a cooperação de muitas agências de administração de redes. Existem organizações que foram desenvolvidas para ajudar a manter a estrutura e a padronização de protocolos e processos da Internet. Essas organizações incluem a Internet Engineering Task Force (IETF), a Internet Corporation for Assigned Names and Numbers (ICANN) e a Internet Architecture Board (IAB), além de muitas outras.

1.4.4 Intranets e Extranets

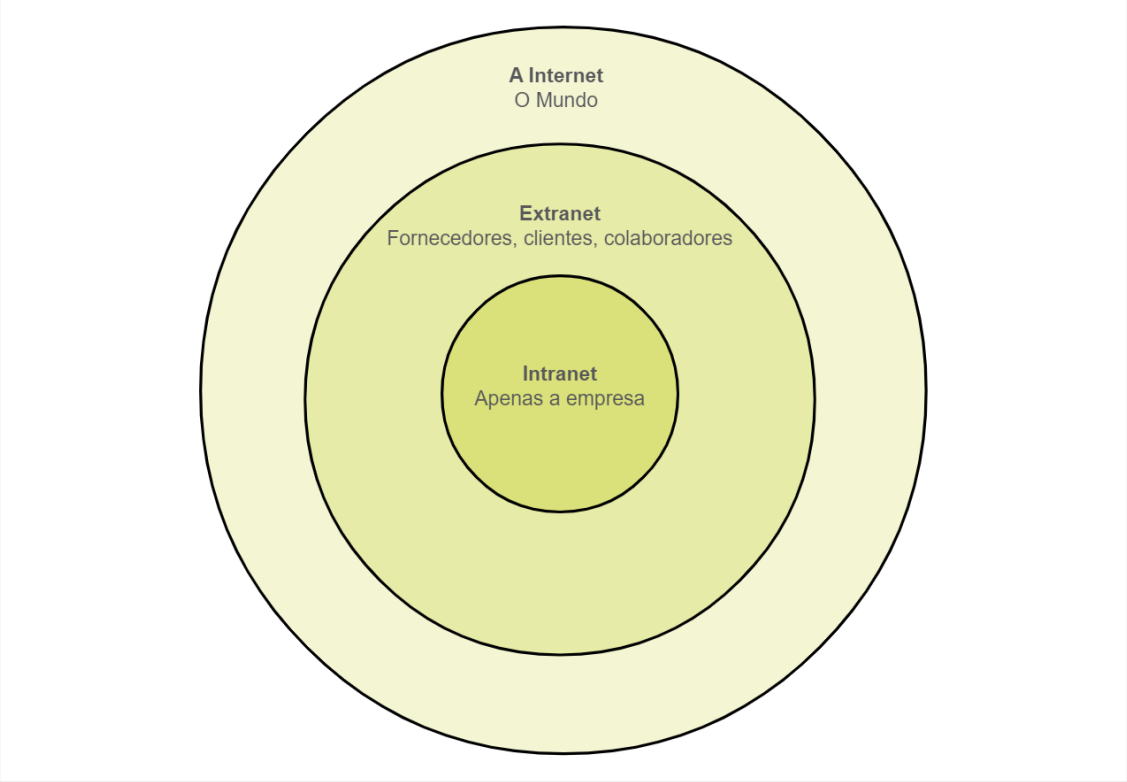
Existem outros dois termos semelhantes ao termo internet: intranet e extranet.

A Intranet é um termo frequentemente usado para se referir a uma conexão privada de LANs e WANs que pertence a uma organização. Uma intranet é projetada para ser acessada apenas por membros da organização, funcionários ou outras pessoas autorizadas.

Uma organização pode usar uma extranet para fornecer acesso seguro e protegido a indivíduos que trabalham para uma organização diferente, mas exigem acesso aos dados da organização. Aqui estão alguns exemplos de extranets:

- Uma empresa que fornece acesso a fornecedores e contratados externos;
- Um hospital que fornece um sistema de reservas aos médicos para que eles possam marcar consultas para seus pacientes;
- Um escritório local de educação que está fornecendo informações sobre orçamento e pessoal às escolas de seu distrito.

A figura ilustra os níveis de acesso que diferentes grupos têm a uma intranet da empresa, uma extranet da empresa e à internet.



1.5 Conexões com a Internet

1.5.1Tecnologias de Acesso à Internet

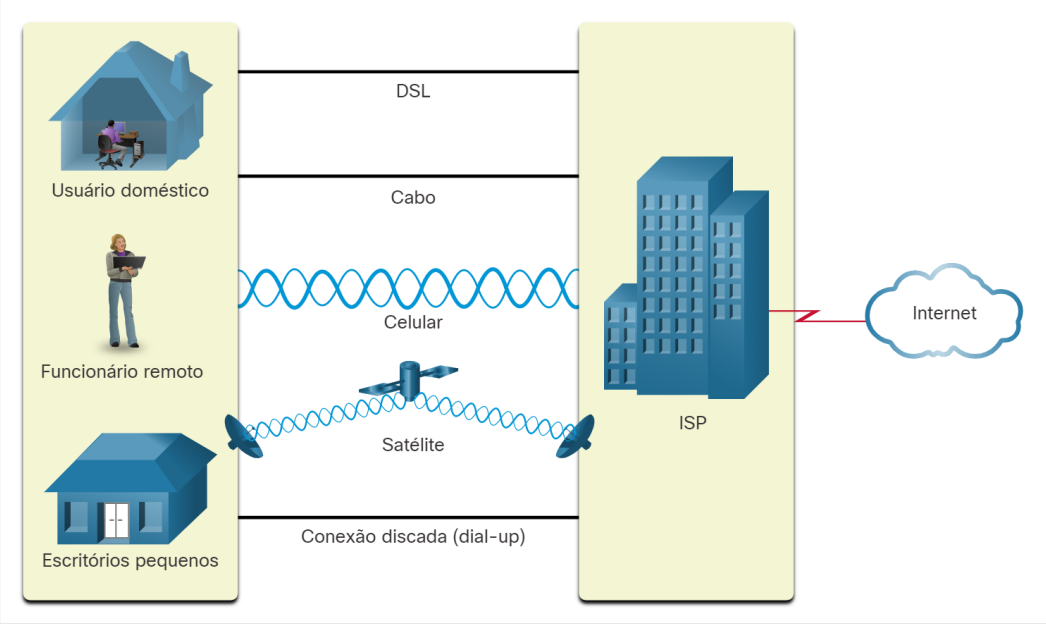
Então, agora você tem uma compreensão básica do que compõe uma rede e os diferentes tipos de redes. Mas, como você realmente conecta usuários e organizações à Internet? Como você deve ter adivinhado, existem muitas maneiras diferentes de fazer isso.

Usuários domésticos, trabalhadores remotos e pequenos escritórios geralmente exigem uma conexão com um ISP para acessar a Internet. As opções de conexão variam muito entre os ISPs e as localizações geográficas. No entanto, as opções populares incluem banda larga a cabo, a banda larga via digital subscriber line (DSL), WANs sem fio e serviços de telefonia móvel celular.

As organizações geralmente precisam acessar outros sites corporativos e a Internet. Conexões rápidas são necessárias para dar suporte a serviços comerciais que incluem telefones IP, videoconferência e armazenamento em data center. As controladoras oferecem interconexões de nível empresarial. Os serviços populares de nível empresarial incluem DSL, linhas dedicadas e Metro Ethernet.

1.5.2 Conexões com a Internet para Residências e Pequenos Escritórios

A figura ilustra opções de conexão comuns para usuários de pequenos escritórios e escritórios domésticos.



Opções de conexão comuns para usuários de pequenos escritórios e escritórios domésticos

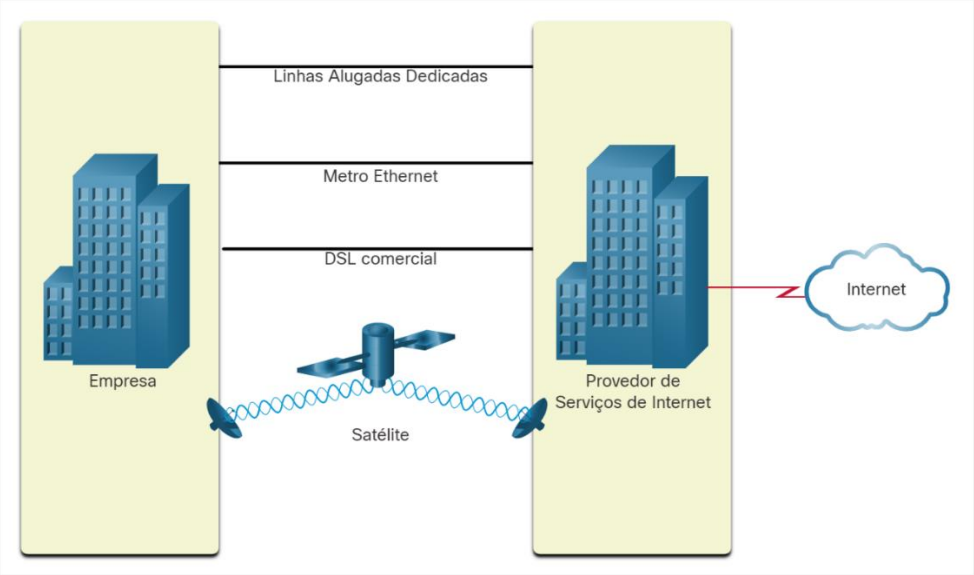
- **Cabo** - Normalmente oferecido por provedores de serviços de televisão a cabo, o sinal de dados da Internet transmite no mesmo cabo que fornece televisão a cabo. Ele fornece alta largura de banda, alta disponibilidade e uma conexão sempre ativa à Internet.
- **DSL** - As linhas de assinante digital também fornecem alta largura de banda, alta disponibilidade e uma conexão sempre ativa à Internet. O DSL funciona utilizando a linha telefônica. Em geral, usuários de pequenos escritórios e escritórios domésticos se conectam com o uso de DSL Assimétrico (ADSL), o que significa que a velocidade de download é maior que a de upload.
- **Celular** - O acesso celular à Internet usa uma rede de telefonia celular para se conectar. Onde quer que você possa obter um sinal de celular, você pode obter acesso à Internet por celular. O desempenho é limitado pelos recursos do telefone e da torre de celular à qual está conectado.
- **Satélite** - A disponibilidade do acesso à Internet via satélite é um benefício nas áreas que, de outra forma, não teriam conectividade com a Internet. As antenas parabólicas exigem uma linha de visão clara para o satélite.
- **Conexão Discada (Dial-up)** – Uma opção de baixo custo que usa qualquer linha telefônica e um modem. A baixa largura de banda fornecida por uma conexão de modem dial-up não é suficiente para grandes transferências de dados, embora seja útil para acesso móvel durante a viagem.

A escolha da conexão varia dependendo da localização geográfica e da disponibilidade do provedor de serviço.

1.5.3 Conexões Corporativas com a Internet

As opções de conexão corporativas são diferentes das opções do usuário doméstico. As empresas podem exigir largura de banda maior, largura de banda dedicada e serviços gerenciados. As opções de conexão disponíveis diferem dependendo do tipo de provedor de serviços localizado nas proximidades.

A figura ilustra opções de conexão comuns para empresas.



Opções de conexão comuns para empresas

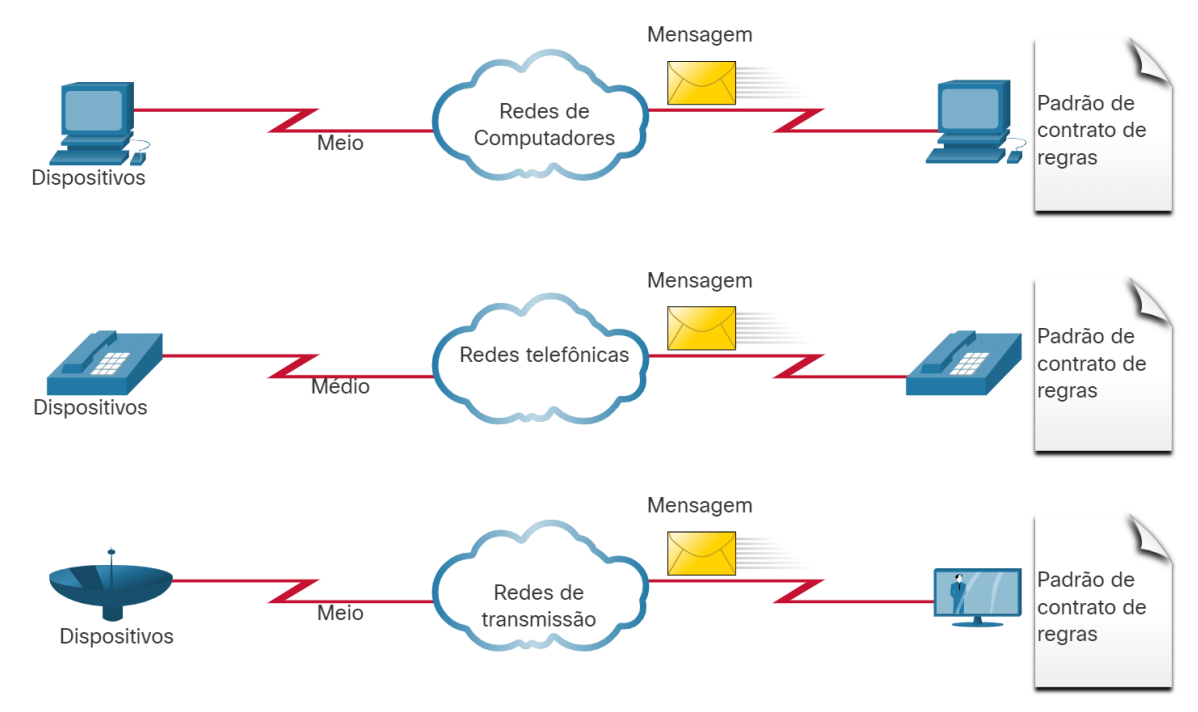
- **Linha Alugada Dedicada** - As linhas alugadas são circuitos reservados na rede do provedor de serviços que conectam escritórios geograficamente separados para redes privadas de voz e / ou dados. Os circuitos são alugados a uma taxa mensal ou anual.
- **Metro Ethernet** - Isso às vezes é conhecido como Ethernet WAN. Neste módulo, vamos nos referir a ele como Metro Ethernet. As ethernet metropolitanas estendem a tecnologia de acesso à LAN na WAN. Ethernet é uma tecnologia de LAN que você aprenderá em um módulo posterior.
- **DSL de negócios** - O DSL comercial está disponível em vários formatos. Uma escolha popular é a linha de assinante digital simétrica (SDSL), que é semelhante à versão DSL do consumidor, mas fornece uploads e downloads nas mesmas velocidades altas.
- **Satélite** - O serviço de satélite pode fornecer uma conexão quando uma solução com fio não está disponível.

A escolha da conexão varia dependendo da localização geográfica e da disponibilidade do provedor de serviço.

1.5.4 A Rede Convergente

Redes Separadas Tradicionais

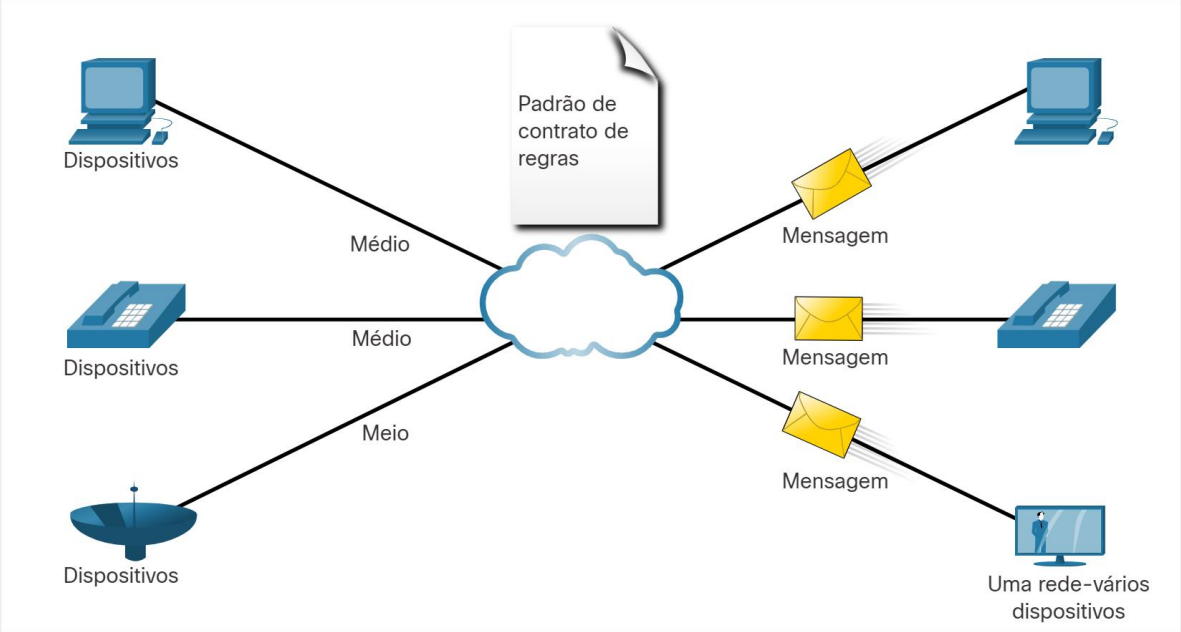
Considere uma escola construída há trinta anos. Naquela época, algumas salas de aula eram cabeadas para a rede de dados, a rede telefônica e a rede de vídeo para televisões. Essas redes separadas não puderam se comunicar. Cada rede usava tecnologias diferentes para transmitir o sinal de comunicação. Cada rede possuía seu próprio conjunto de regras e padrões para assegurar a comunicação bem-sucedida. Vários serviços foram executados em várias redes.



Redes separadas de computador, telefone e difusão

Redes convergentes

Hoje, as redes separadas de dados, telefone e vídeo convergem. Diferentemente das redes dedicadas, as redes convergentes são capazes de fornecer dados, voz e vídeo entre muitos tipos diferentes de dispositivos na mesma infraestrutura de rede. Essa infraestrutura de rede usa o mesmo conjunto de regras, os mesmos contratos e normas de implementação. As redes de dados convergentes transportam vários serviços em uma rede.



Rede de dados convergida com vários serviços em uma rede.

1.5.5 Vídeo - Baixe e instale o Packet Tracer

Este vídeo mostra como baixar e instalar o Packet Tracer. Você usará o Packet Tracer para simular a criação e teste de redes no seu computador. Packet Tracer é um programa de software divertido, leve para casa e flexível que lhe dará a oportunidade de usar as representações de rede e teorias que você acabou de aprender a construir modelos de rede e explorar LANs e WANs relativamente complexos.

Os alunos normalmente usam o Packet Tracer para:

- Preparar-se para um exame de certificação.
- Praticar o que eles aprenderam em cursos de rede.
- Aprimorar as qualificações para entrevistas de emprego.
- Avaliar o impacto da adição de novas tecnologias nos projetos de rede atuais.
- Desenvolver qualificações profissionais para empregos na Internet das Coisas (IoT).
- Concorrer no Global Design Challenges (dê uma olhada no 2017 PT 7 Design Challenge no Facebook).

O Packet Tracer é uma ferramenta de aprendizado de grande importância usada em muitos cursos da Cisco Networking Academy.

Para obter e instalar sua cópia do Cisco Packet Tracer, siga estas etapas:

Etapa 1. Faça login na página "Estou aprendendo" da Cisco Networking Academy.
Etapa 2. Selecione Recursos.
Etapa 3. Selecione Baixar Packet Tracer.
Etapa 4. Selecione a versão do Packet Tracer que desejar.
Etapa 5. Salve o arquivo no computador.
Etapa 6. Inicie o programa de instalação do Packet Tracer.
Clique em Reproduzir no vídeo para ver o passo a passo do processo de download e instalação do Packet Tracer.

1.5.6 Vídeo - Introdução ao Cisco Packet Tracer

Packet Tracer é uma ferramenta que permite simular redes reais. Ele fornece três menus principais:

- Você pode adicionar dispositivos e conectá-los através de cabos ou sem fio.
- Você pode selecionar, excluir, inspecionar, rotular e agrupar componentes dentro da rede.
- Você pode gerenciar sua rede abrindo uma rede existente/amostra, salvando sua rede atual e modificando seu perfil de usuário ou preferências.

Se você tiver usado qualquer programa, como um processador de texto ou planilha, você já está familiarizado com os comandos do menu Arquivo localizados na barra de menus superior. Os comandos Abrir, Salvar, Salvar Como e Sair funcionam como fariam para qualquer programa, mas há dois comandos que são especiais para o Packet Tracer.

O comando Abrir Amostras exibirá um diretório de exemplos pré-construídos de recursos e configurações de vários dispositivos de rede e Internet das Coisas incluídos no Packet Tracer.

O comando Sair e Logout removerá as informações de registro para esta cópia do Packet Tracer e exigirá que o próximo usuário desta cópia do Rastreador de Pacotes faça o procedimento de login novamente.

Clique em Reproduzir no vídeo para saber como usar os menus e como criar sua primeira rede de Packet Tracer.

1.5.7 Packet Tracer: representação da Rede

Nesta atividade, você explorará como o Packet Tracer serve como uma ferramenta de modelagem para representações de rede.

1.6 Redes confiáveis

1.6.1 Arquitetura de Redes

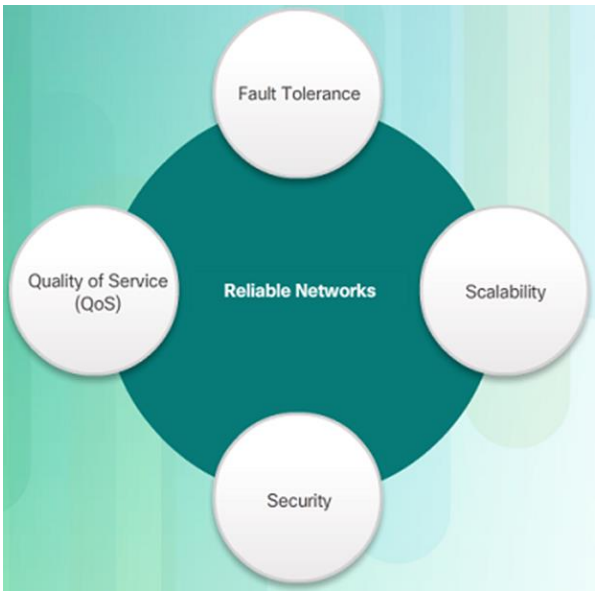
Você já esteve ocupado trabalhando on-line, e achou que "a internet caiu"? Como você sabe até agora, a internet não caiu, você acabou de perder sua conexão com ela. Isso é muito frustrante. Com tantas pessoas no mundo confiando no acesso à rede para trabalhar e aprender, é imperativo que as redes sejam confiáveis. Nesse contexto, confiabilidade significa mais do que sua conexão à Internet. Este tópico se concentra nos quatro aspectos da confiabilidade da rede.

O papel da rede mudou de uma rede somente de dados para um sistema que permite a conexão de pessoas, dispositivos e informações em um ambiente de rede convergente rico em

mídia. Para que as redes funcionem com eficiência e cresçam nesse tipo de ambiente, a rede deve ser construída sobre uma arquitetura de rede padrão.

As redes também suportam uma ampla gama de aplicativos e serviços. Elas devem operar sobre muitos tipos diferentes de cabos e dispositivos, que compõem a infraestrutura física. O termo arquitetura de redes, neste contexto, refere-se às tecnologias que apoiam a infraestrutura e os serviços programados e as regras, ou protocolos, que movimentam os dados na rede.

À medida que as redes evoluem, aprendemos que há quatro características básicas que os arquitetos de rede devem atender para atender às expectativas do usuário:



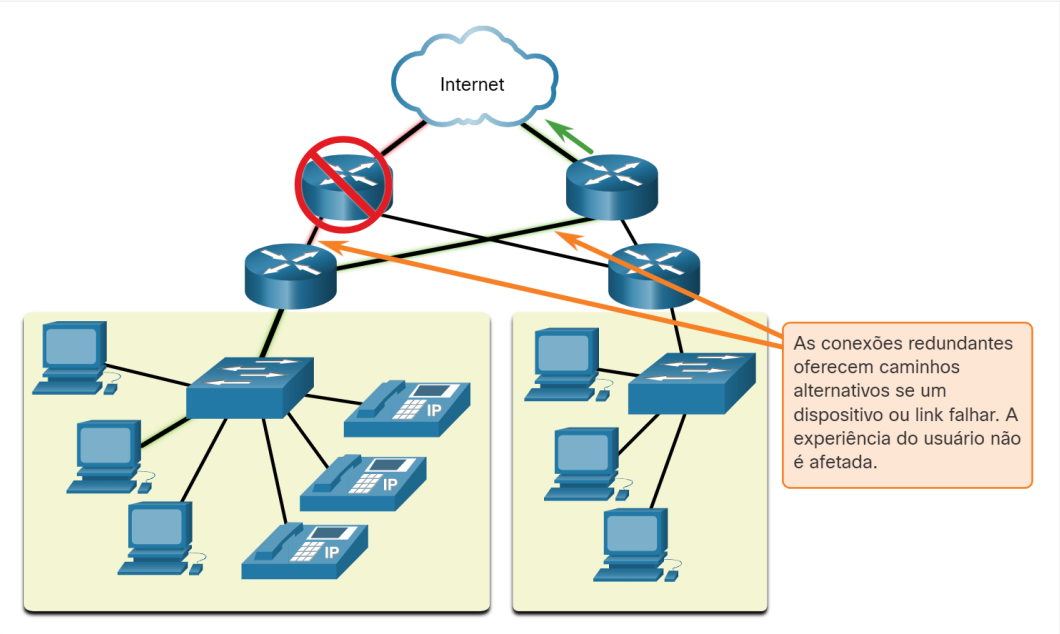
- Tolerância a falhas;
- Escalabilidade;
- Qualidade de serviço (QoS);
- Segurança.

1.6.2 Tolerância a Falhas

Uma rede tolerante a falhas é aquela que limita o número de dispositivos afetados durante uma falha. Ela foi desenvolvido para permitir uma recuperação rápida quando ocorre uma falha. Essas redes dependem de vários caminhos entre a origem e o destino de uma mensagem. Se um caminho falhar, as mensagens serão instantaneamente enviadas por um link diferente. Ter vários caminhos para um destino é conhecido como redundância.

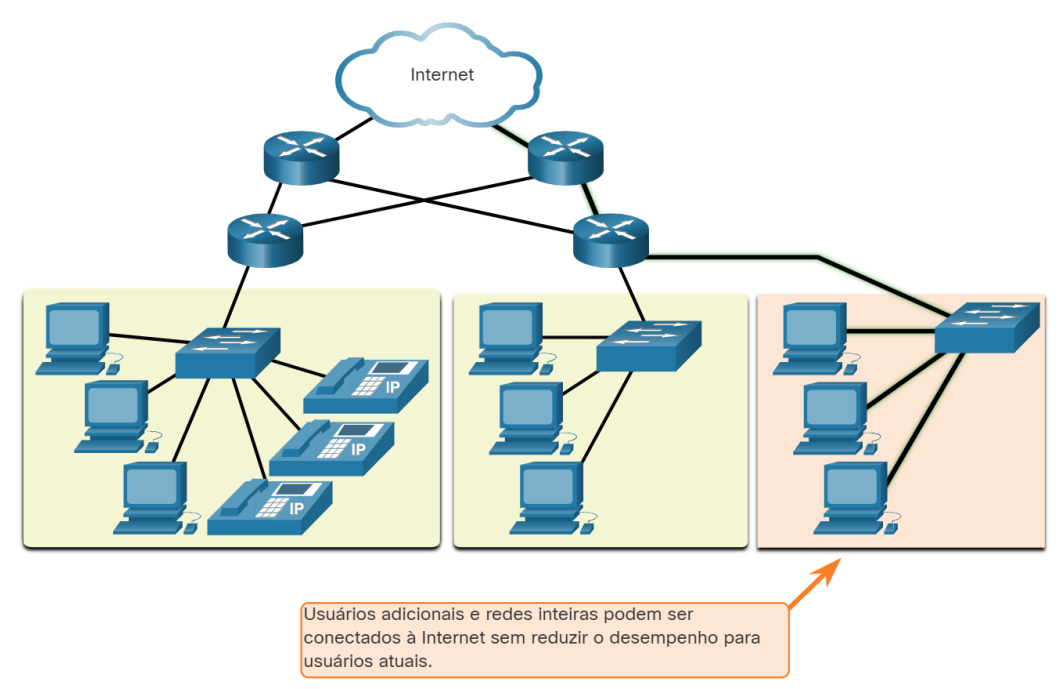
A implementação de uma rede comutada por pacotes é uma das maneiras pelas quais redes confiáveis fornecem redundância. A comutação de pacotes divide os dados do tráfego em pacotes que são roteados por uma rede compartilhada. Uma única mensagem, como um e-mail ou stream de vídeo, é dividido em vários blocos, chamados pacotes. Cada pacote tem as informações de endereço necessárias da origem e do destino da mensagem. Os roteadores na rede alternam os pacotes com base na condição da rede no momento. Isso significa que todos os pacotes em uma única mensagem podem seguir caminhos muito diferentes para o mesmo destino. Na figura, o

usuário desconhece e não é afetado pelo roteador que está alterando dinamicamente a rota quando um link falha.



1.6.3 Escalabilidade

Uma rede escalável se expande rapidamente para oferecer suporte a novos usuários e aplicativos. Ele faz isso sem degradar o desempenho dos serviços que estão sendo acessados por usuários existentes. A figura mostra como uma nova rede é facilmente adicionada a uma rede existente. Essas redes são escaláveis porque os projetistas seguem padrões e protocolos aceitos. Isso permite que os fornecedores de software e hardware se concentrem em melhorar produtos e serviços sem precisar criar um novo conjunto de regras para operar na rede.

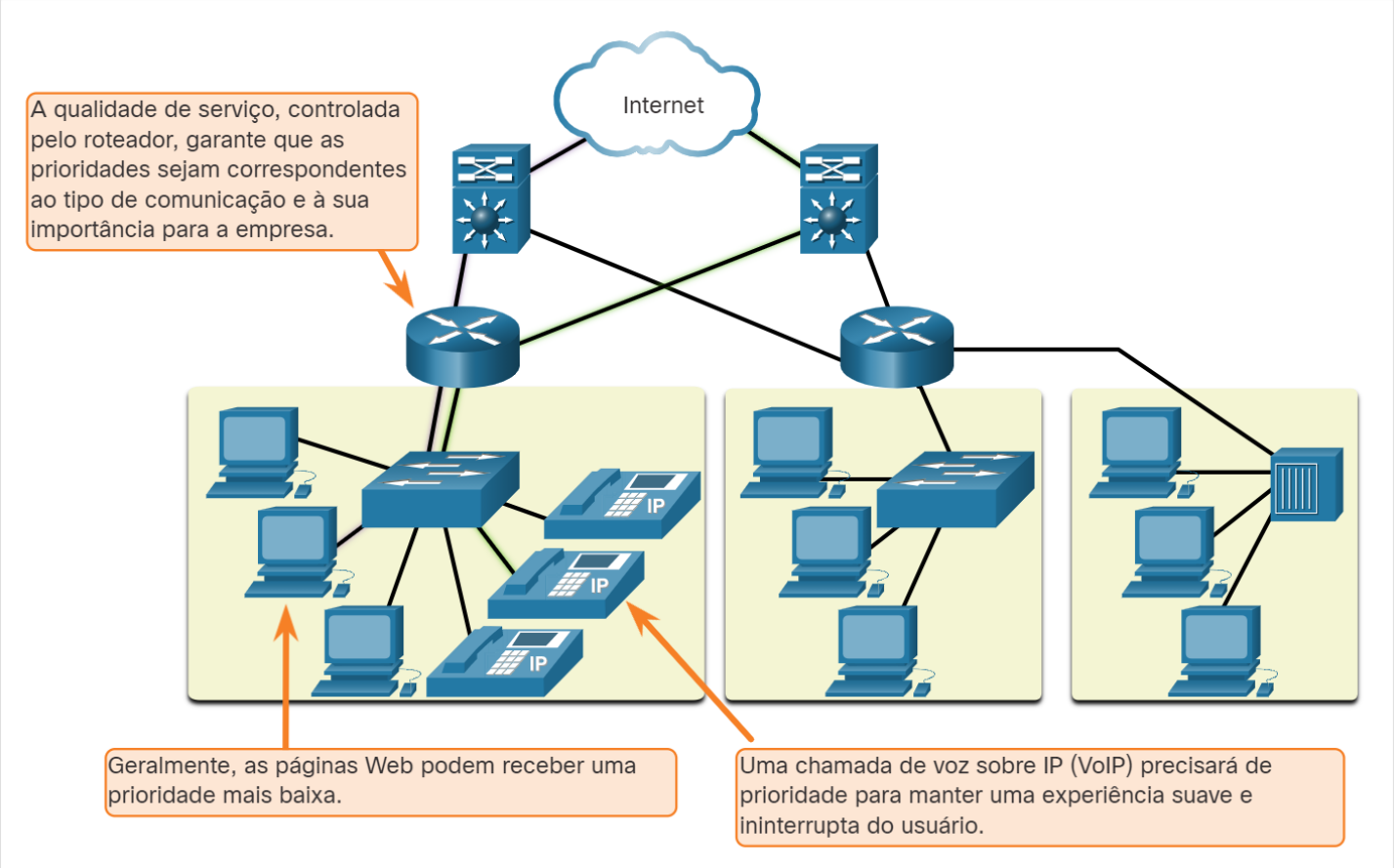


1.6.4 Qualidade do Serviço

A qualidade do serviço (QoS) é um requisito crescente das redes atualmente. Novos aplicativos disponíveis para usuários em redes, como transmissões de voz e vídeo ao vivo, criam expectativas mais altas em relação à qualidade dos serviços entregues. Você já tentou assistir a um vídeo com intervalos e pausas constantes? Conforme o conteúdo de vídeo, voz e dados continua a convergir na mesma rede, o QoS se torna um mecanismo essencial para gerenciar os congestionamentos e garantir a entrega confiável do conteúdo para todos os usuários.

O congestionamento acontece quando a demanda por largura de banda excede a quantidade disponível. A largura de banda é medida pelo número de bits que podem ser transmitidos em um único segundo, ou bits por segundo (bps). Ao tentar uma comunicação simultânea pela rede, a demanda pela largura de banda pode exceder sua disponibilidade, criando um congestionamento na rede.

Quando o volume de tráfego é maior do que o que pode ser transportado pela rede, os dispositivos retêm os pacotes na memória até que os recursos estejam disponíveis para transmiti-los. Na figura, um usuário está solicitando uma página da Web e outro está em uma ligação. Com uma política de QoS configurada, o roteador é capaz de gerenciar o fluxo do tráfego de voz e de dados, priorizando as comunicações por voz se a rede ficar congestionada.

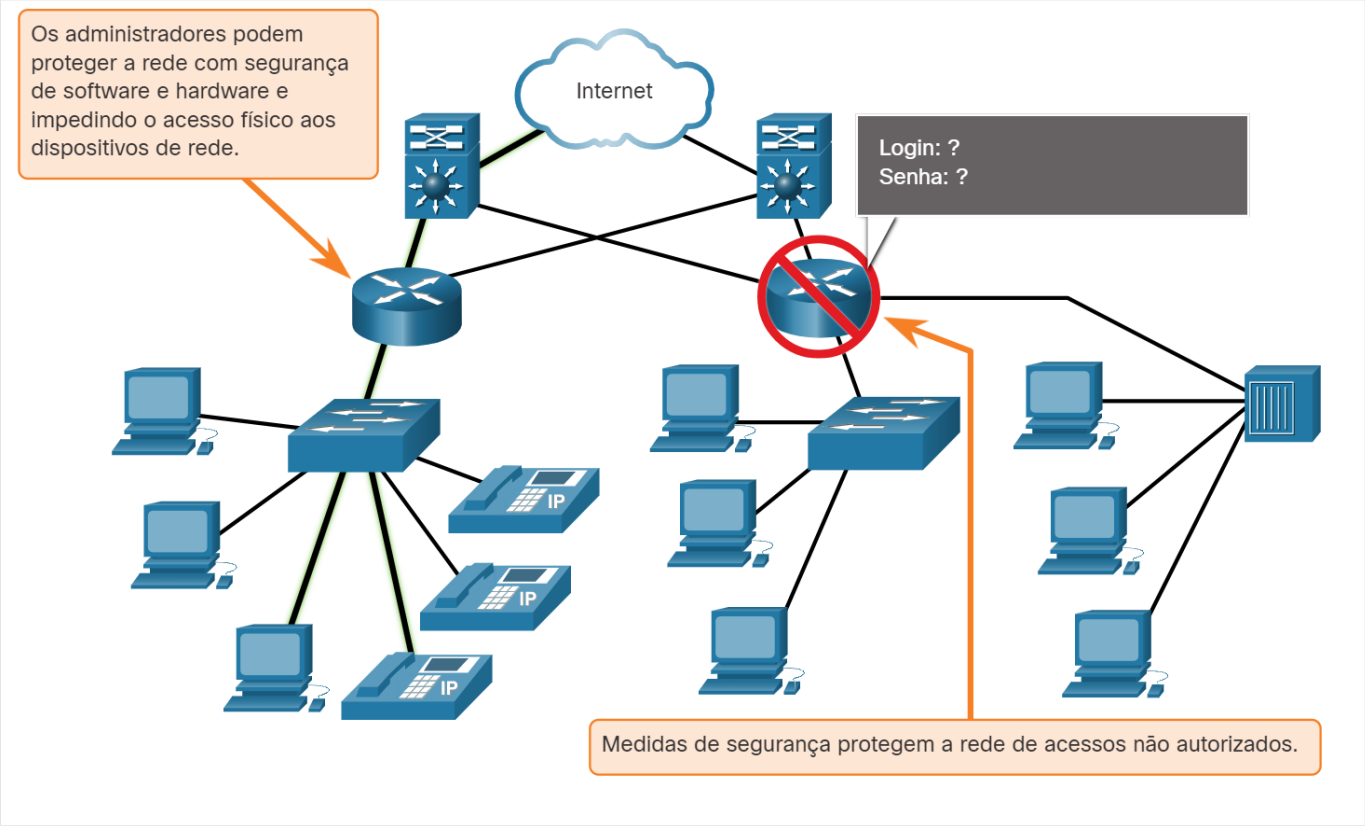


1.6.5 Segurança da rede

A infraestrutura da rede, os serviços e os dados contidos nos dispositivos conectados à rede são recursos pessoais e comerciais críticos. Os administradores de rede devem abordar dois tipos

de preocupações de segurança de rede: segurança da infraestrutura de rede e segurança da informação.

Proteger a infraestrutura de rede inclui proteger fisicamente os dispositivos que fornecem conectividade de rede e impedir o acesso não autorizado ao software de gerenciamento que reside neles, conforme mostrado na figura.



Os administradores de rede também devem proteger as informações contidas nos pacotes transmitidos pela rede e as informações armazenadas nos dispositivos conectados à rede. Para atingir os objetivos de segurança de rede, existem três requisitos principais.

- **Confidencialidade** - Confidencialidade dos dados significa que apenas os destinatários pretendidos e autorizados podem acessar e ler dados.
- **Integridade** - A integridade dos dados garante aos usuários que as informações não foram alteradas na transmissão, da origem ao destino.
- **Disponibilidade** - A disponibilidade de dados garante aos usuários acesso oportuno e confiável aos serviços de dados para usuários autorizados.

1.7 Tendências das redes

1.7.1 Tendências recentes

Você sabe muito sobre redes agora, do que elas são feitas, como elas nos conectam e o que é necessário para mantê-las confiáveis. Mas as redes, como todo o resto, continuam a mudar. Existem algumas tendências em rede que você, como estudante da NetAcad, deve conhecer.

À medida que novas tecnologias e dispositivos do usuário final chegam ao mercado, as empresas e os consumidores devem continuar se ajustando a esse ambiente em constante mudança. Existem várias tendências de rede que afetam organizações e consumidores:

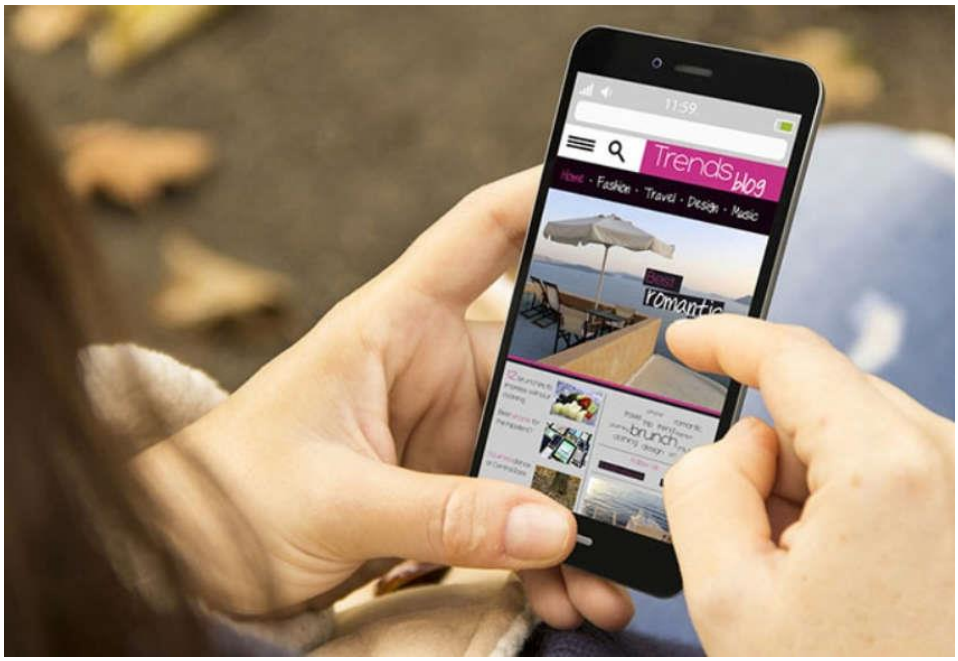
- BYOD (Bring Your Own Device);
- Colaboração on-line;
- Comunicação por vídeo;
- Computação em nuvem.

1.7.2 Traga seu próprio dispositivo (BYOD)

O conceito de qualquer dispositivo, para qualquer conteúdo, de qualquer maneira, é uma grande tendência global que requer mudanças significativas na maneira como usamos os dispositivos e os conectamos com segurança às redes. Isso se chama Traga seu próprio dispositivo (BYOD).

O BYOD permite aos usuários finais a liberdade de usar ferramentas pessoais para acessar informações e se comunicar através de uma rede comercial ou do campus. Com o crescimento de dispositivos de consumo e a queda de custo relacionada, funcionários e estudantes podem ter dispositivos avançados de computação e rede para uso pessoal. Isso inclui laptops, notebooks, tablets, smartphones e e-readers. Estes podem ser adquiridos pela empresa ou escola, adquiridos pelo indivíduo ou por ambos.

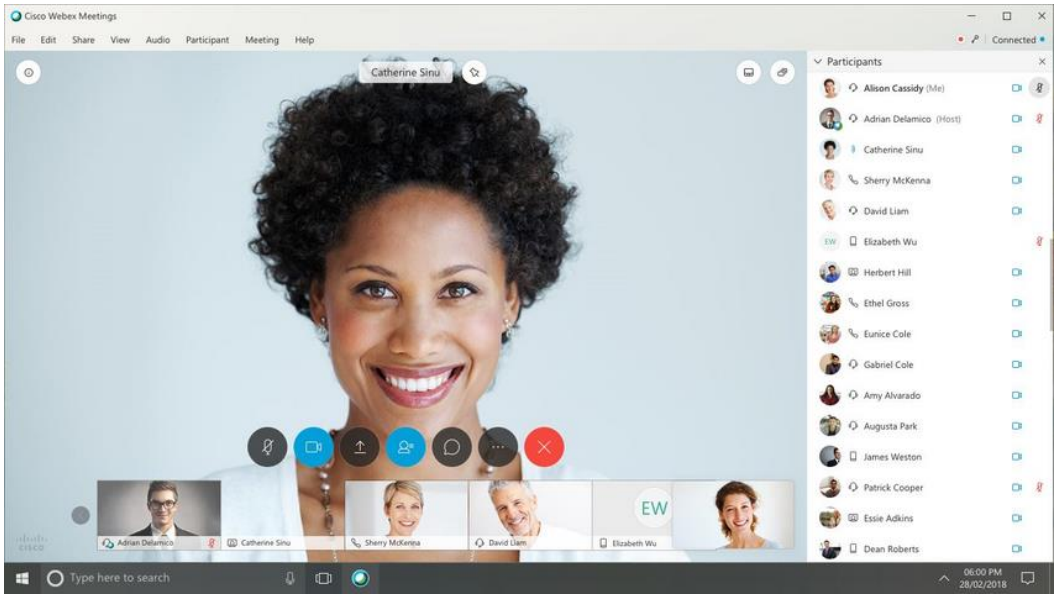
BYOD significa o uso de qualquer dispositivo, de qualquer propriedade e em qualquer lugar.



1.7.3 Colaboração On-line

As pessoas querem se conectar à rede não só para acessar as aplicações de dados, mas também para colaborar com outras pessoas. A colaboração é definida como "ato de trabalho com outro ou outros em um projeto em parceria". As ferramentas de colaboração, como o Cisco WebEx,

mostrado na figura, oferecem aos funcionários, alunos, professores, clientes e parceiros uma maneira de conectar, interagir e alcançar instantaneamente seus objetivos.



A colaboração é uma prioridade crítica e estratégica que as organizações estão usando para permanecer competitivas. A colaboração também é uma prioridade na educação. Os alunos precisam colaborar para ajudar uns aos outros na aprendizagem, desenvolver as habilidades de equipe usadas na força de trabalho e trabalhar juntos em projetos baseados em equipe.

1.7.4 Comunicações em vídeo

Outra faceta da rede crítica para o esforço de comunicação e colaboração é o vídeo. O vídeo é usado para comunicação, colaboração e entretenimento. Chamadas de vídeo são feitas de e para qualquer pessoa com uma conexão à Internet, independentemente de onde elas estão localizadas.

A videoconferência é uma ferramenta poderosa para se comunicar com outras pessoas, local e globalmente. O vídeo está se tornando um requisito fundamental para a colaboração efetiva à medida que as empresas se expandem pelos limites geográficos e culturais.

1.7.5 Computação em nuvem

A computação em nuvem é uma das maneiras pelas quais acessamos e armazenamos dados. A computação em nuvem nos permite armazenar arquivos pessoais, até fazer backup de uma unidade inteira em servidores pela Internet. Aplicativos como processamento de texto e edição de fotos podem ser acessados usando a nuvem.

Para as empresas, a computação em nuvem amplia os recursos de TI sem exigir investimento em nova infraestrutura, treinamento de novas equipes ou licenciamento de novo software. Esses serviços estão disponíveis sob demanda e são entregues economicamente a qualquer dispositivo que esteja em qualquer lugar do mundo, sem comprometer a segurança ou a função.

A computação em nuvem é possível devido aos data centers. Os data centers são instalações usadas para hospedar sistemas de computador e componentes associados. Um data center pode ocupar uma sala de um edifício, um ou mais andares ou todo um prédio do tamanho de um armazém. Os data centers normalmente são muito caros de construir e manter. Por esse motivo,

apenas as grandes empresas usam data centers construídos de forma privada para abrigar os dados e fornecer serviços aos usuários. Empresas de pequeno porte que não podem arcar com a manutenção de seu próprio data center podem reduzir os custos gerais de propriedade ao alugar um servidor e armazenar serviços em uma empresa de data center maior na nuvem.

Para segurança, confiabilidade e tolerância a falhas, os provedores de nuvem geralmente armazenam dados em data centers distribuídos. Em vez de armazenar todos os dados de uma pessoa ou uma organização em um data center, eles são armazenados em vários data centers em locais diferentes.

Existem quatro tipos principais de nuvens: nuvens públicas, nuvens privadas, nuvens híbridas e nuvens da comunidade, conforme mostrado na tabela.

Tipos de Nuvem

Tipo de nuvem	Descrição
Nuvens públicas	Aplicativos e serviços baseados em nuvem oferecidos em uma nuvem pública são criados disponível para a população em geral. Os serviços podem ser gratuitos ou são oferecidos em um modelo de pagamento por uso, como pagar por armazenamento on-line. A nuvem pública usa a internet para fornecer serviços.
Nuvens privadas	Os aplicativos e serviços baseados em nuvem oferecidos em uma nuvem privada são destinado a uma organização ou entidade específica, como um governo. A nuvem privada pode ser configurada usando o rede, embora isso possa ser caro para construir e manter. Uma nuvem privada também pode ser gerenciada por uma organização externa com acesso estrito segurança.
Nuvens híbridas	Uma nuvem híbrida é composta de duas ou mais nuvens (exemplo: parte privada, parte pública), onde cada parte permanece um objeto distinto, mas ambos são conectado usando uma única arquitetura. Indivíduos em uma nuvem híbrida seria capaz de ter graus de acesso a vários serviços com base em direitos de acesso do usuário.
Nuvens comunitárias	Uma nuvem de comunidade é criada para uso exclusivo por entidades ou organizações específicas. As diferenças entre nuvens públicas e nuvens da comunidade são as necessidades funcionais que foram personalizadas para a comunidade. Por exemplo, organizações de saúde devem manter a conformidade com políticas e leis (por exemplo, HIPAA) que exigem confidencialidade e autenticação especial. As nuvens comunitárias são usadas por várias organizações que têm necessidades e preocupações semelhantes. As nuvens comunitárias são semelhantes a um ambiente de nuvem pública, mas com níveis definidos de segurança, privacidade e até mesmo conformidade normativa de uma nuvem privada.

1.7.7 Tendências Tecnológicas em Casa

As tendências de rede não estão apenas afetando a maneira como nos comunicamos no trabalho e na escola, mas também mudando muitos aspectos da casa. As mais novas tendências para casas incluem a "tecnologia residencial inteligente".

A tecnologia de casa inteligente se integra aos aparelhos diários, que podem ser conectados a outros dispositivos para tornar os aparelhos mais "inteligentes" ou automatizados. Por exemplo, você pode preparar a comida e colocá-la no forno para cozinhar antes de sair de casa durante o dia. Você programa seu forno inteligente para a comida que você quer que ele cozinhe. Ele também seria conectado ao seu 'calendário de eventos' para determinar a que horas você deveria estar disponível para comer e ajustar os horários de início e a duração do cozimento de acordo. Poderia até mesmo definir os tempos e as temperaturas de cozimento baseados em mudanças na programação. Além disso, uma conexão de smartphone ou tablet permite conectar-se diretamente ao forno, para fazer os ajustes desejados. Quando a comida estiver pronta, o forno envia uma mensagem de alerta para você (ou alguém que você especificar) que a comida está pronta e aquecendo.

Atualmente, a tecnologia de casa inteligente está sendo desenvolvida para todos os cômodos de uma casa. A tecnologia doméstica inteligente se tornará mais comum à medida que as redes domésticas e a tecnologia de Internet de alta velocidade se expandirem.

Uma representação da tecnologia de casa inteligente mostrando uma nuvem com setas apontando para uma casa, um carro e um smartphone. O texto na parte inferior diz: O telefone inteligente é atualizado a partir da nuvem com o status dos dispositivos domésticos inteligentes e do carro inteligente; o usuário pode então usar o telefone inteligente para interagir com a casa inteligente e o carro inteligente.

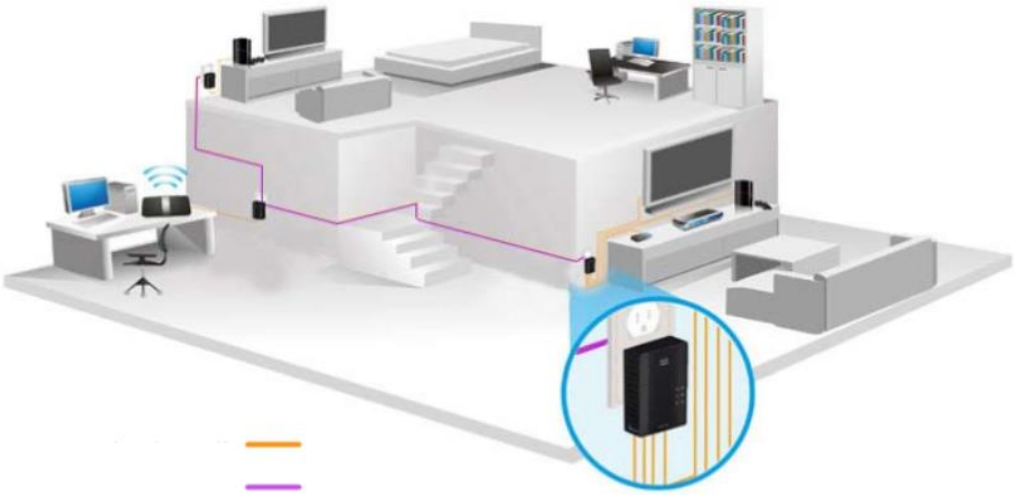
Nuvem

O smartphone é atualizado a partir da nuvem com o status dos dispositivos domésticos inteligentes e do carro inteligente. O usuário pode então usar o telefone inteligente para interagir com a casa inteligente e o carro inteligente.

1.7.8 Rede Powerline

A rede Powerline para redes domésticas usa a fiação elétrica existente para conectar dispositivos, conforme mostrado na figura.

Uma planta aberta de uma casa usando rede elétrica para uma rede doméstica. Existem três adaptadores de linha de força PLEK400 de 4 portas conectados a três tomadas elétricas diferentes, todas conectadas por meio de conexões com fio. Cada adaptador tem pelo menos uma conexão de linha elétrica a um dispositivo em rede, incluindo desktops e TVs.



Usando um adaptador padrão powerline, os dispositivos podem se conectar à LAN onde quer que haja uma tomada elétrica. Nenhum cabo de dados precisa ser instalado, e há pouca ou nenhuma eletricidade adicional usada. Usando a mesma fiação que fornece a eletricidade, a rede powerline envia informações ao enviar dados em determinadas frequências.

A rede Powerline é especialmente útil quando os pontos de acesso sem fio não conseguem alcançar todos os dispositivos em casa. A rede Powerline não substitui o cabeamento dedicado em redes de dados. No entanto, é uma alternativa quando os cabos da rede de dados ou as comunicações sem fio não são possíveis ou eficazes.

1.7.9 Banda Larga Sem Fio

Em muitas áreas onde cabo e DSL não estão disponíveis, a rede sem fio pode ser usada para se conectar à Internet.

Provedor de serviços de Internet sem fio

Um provedor de serviços de Internet sem fio (WISP) é um provedor de serviços de Internet que conecta assinantes a um ponto de acesso ou hot spot designado usando tecnologias sem fio semelhantes encontradas em redes locais sem fio domésticas (WLANs). Os WISPs são mais comumente encontrados em ambientes rurais onde DSL ou serviços a cabo não estão disponíveis.

Embora uma torre de transmissão separada possa ser instalada para a antena, normalmente a antena está conectada a uma estrutura elevada existente, como uma torre de água ou uma torre de rádio. Uma antena parabólica pequena ou grande é instalada no teto do assinante dentro do alcance do transmissor WISP. A unidade de acesso do assinante é conectada à rede com fio dentro de casa. Da perspectiva de usuário doméstico, a configuração não é muito diferente do serviço de cabo ou DSL. A principal diferença é a conexão da casa para o ISP ser sem fio em vez de um cabo físico.

Serviço de banda larga sem fio

Outra solução sem fio para casas e pequenas empresas é a banda larga sem fio, como mostra a figura.

Esta solução usa a mesma tecnologia celular que um telefone inteligente. Uma antena é instalada fora da residência, fornecendo conectividade com ou sem fio para dispositivos na casa. Em muitas áreas, a banda larga sem fio doméstica está competindo diretamente com serviços DSL e a cabo.

1.8 Segurança de Redes

1.8.1 Ameaças à Segurança

Você, sem dúvida, ouviu ou leu notícias sobre uma rede da empresa sendo violada, dando aos atores ameaçadores acesso às informações pessoais de milhares de clientes. Por esse motivo, a segurança de rede sempre será uma prioridade máxima dos administradores.

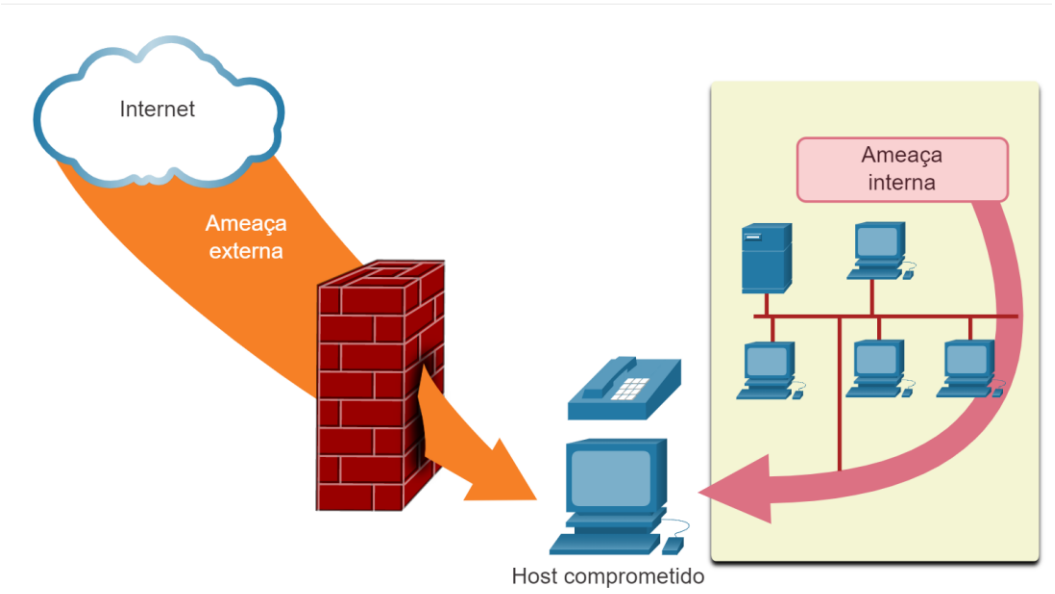
A segurança da rede é parte integrante da rede de computadores, independentemente de a rede estar em uma casa com uma única conexão à Internet ou se é uma corporação com milhares de usuários. A segurança da rede deve considerar o ambiente, bem como as ferramentas e os requisitos da rede. Ele deve poder proteger os dados e, ao mesmo tempo, permitir a qualidade do serviço que os usuários esperam da rede.

A proteção de uma rede envolve protocolos, tecnologias, dispositivos, ferramentas e técnicas para proteger dados e mitigar ameaças. Vetores de ameaça podem ser internos ou externos. Hoje, muitas ameaças à segurança de rede externa se originam da Internet.

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.

Também é importante considerar ameaças internas. Há muitos estudos que mostram que as violações mais comuns ocorrem por causa de usuários internos da rede. Isso pode ser atribuído a dispositivos perdidos ou roubados, mau uso acidental por parte dos funcionários e, no ambiente comercial, até mesmo funcionários mal-intencionados. Com as estratégias BYOD em evolução, os dados corporativos ficam muito mais vulneráveis. Portanto, ao desenvolver uma política de segurança, é importante abordar ameaças de segurança externas e internas, conforme mostrado na figura.



1.8.2 Soluções de Segurança

Nenhuma solução única pode proteger a rede da variedade de ameaças existentes. Por esse motivo, a segurança deve ser implementada em várias camadas, com uso de mais de uma solução. Se um componente de segurança falhar na identificação e proteção da rede, outros poderão ter êxito.

Uma implementação de segurança para redes domésticas é normalmente bastante básica. Normalmente, você o implementa nos dispositivos finais, bem como no ponto de conexão com a Internet, e pode até confiar nos serviços contratados pelo ISP.

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

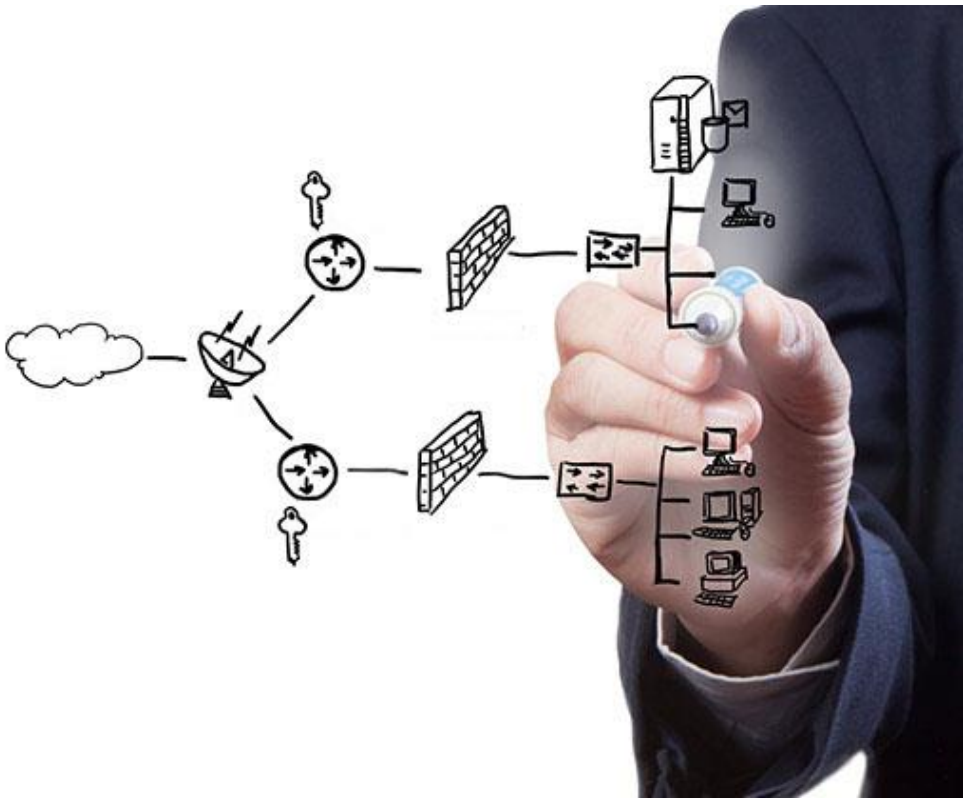
- **Antivirus e antispyware** - Esses aplicativos ajudam a proteger os dispositivos finais contra a infecção por software malicioso.
- **Filtragem por firewall** - A filtragem por firewall bloqueia o acesso não autorizado dentro e fora da rede. Isso pode incluir um sistema de firewall baseado em host 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.

Em contrapartida, a implementação de segurança para uma rede corporativa geralmente consiste em vários componentes incorporados à rede para monitorar e filtrar o tráfego. Idealmente, todos os componentes trabalham juntos, o que minimiza a manutenção e melhora a segurança. Redes maiores e redes corporativas usam antivírus, antispyware e filtragem por firewall, mas também têm outros requisitos de segurança:

- **Sistemas de firewall dedicados** - Eles fornecem recursos de firewall mais avançados que podem filtrar grandes quantidades de tráfego com mais granularidade.
- **Listas de controle de acesso (ACL)** - Eles filtram ainda mais o acesso e o encaminhamento de tráfego com base em endereços e aplicativos IP.
- **Sistemas de prevenção de intrusões (IPS)** - Identificam ameaças de rápida disseminação, como ataques de dia zero ou hora zero.
- **Redes privadas virtuais (VPN)** - fornecem acesso seguro a uma organização para trabalhadores remotos.

Os requisitos de segurança de rede devem considerar o ambiente, os vários aplicativos e os requisitos de computação. Ambientes domésticos e comerciais devem poder proteger seus dados e, ao mesmo tempo, permitir a qualidade do serviço que os usuários esperam de cada tecnologia. Além disso, as soluções de segurança implementadas devem ser adaptáveis às tendências de crescimento e variáveis da rede.

O estudo das ameaças à rede e de técnicas de mitigação é iniciado com um claro entendimento da infraestrutura de roteamento e de comutação usada para organizar serviços de rede.



1.9 Módulo Prático O que eu aprendi neste módulo?

Redes afetam nossas vidas

No mundo de hoje, com o uso de redes, estamos conectados como nunca estivemos. Pessoas que têm ideias podem se comunicar instantaneamente com as demais para torná-las uma realidade. A criação de comunidades on-line para a troca de ideias e informações tem o potencial de aumentar as oportunidades de produtividade ao redor do mundo. A criação da nuvem nos permite armazenar documentos e imagens e acessá-los em qualquer lugar, a qualquer hora.

Componentes de rede

Todos os computadores que estão conectados a uma rede e participam diretamente da comunicação em rede são classificados como hosts. Os hosts podem ser chamados de dispositivos finais. Alguns hosts também são chamados de clientes. Muitos computadores funcionam como servidores e clientes na rede. Esse tipo de rede é chamado de rede ponto a ponto. Um dispositivo final é a origem ou o destino de uma mensagem transmitida pela rede. Dispositivos intermediários conectam dispositivos finais individuais à rede e podem conectar várias redes individuais para formar uma rede interconectada. Esses dispositivos intermediários usam o endereço do dispositivo final de destino, em conjunto com as informações sobre as interconexões de rede, para determinar o caminho que as mensagens devem percorrer na rede. A mídia fornece o canal pelo qual a mensagem viaja da origem ao destino.

Representações e topologias de rede

Os diagramas de redes geralmente usam símbolos para representar os diferentes dispositivos e conexões que compõem uma rede. Um diagrama fornece uma maneira fácil de entender como os dispositivos se conectam em uma rede grande. Esse tipo de "fotografia" de uma

rede é conhecido como um diagrama de topologia. Os diagramas de topologia física ilustram a localização física de dispositivos intermediários e a instalação de cabos. Os diagramas de topologia lógica ilustram dispositivos, portas e o esquema de endereçamento da rede.

Tipos comuns de redes

As redes domésticas pequenas conectam alguns computadores entre si e com a Internet. A rede de pequeno escritório / escritório doméstico (SOHO) permite que computadores em um escritório doméstico ou remoto se conectem a uma rede corporativa ou acessem recursos compartilhados centralizados. Redes de médio a grande porte, como as usadas por empresas e escolas, podem ter muitos locais com centenas ou milhares de hosts interconectados. A internet é uma rede de redes que conecta centenas de milhões de computadores em todo o mundo. Os dois tipos mais comuns de infraestruturas de rede são as redes locais (LANs) e as redes de longa distância (WANs). Uma LAN é uma infraestrutura de rede que abrange uma pequena área geográfica. Uma WAN é uma infraestrutura de rede que abrange uma ampla área geográfica. Intranet refere-se a uma conexão privada de LANs e WANs que pertence a uma organização. Uma organização pode usar uma extranet para fornecer acesso seguro e protegido a indivíduos que trabalham para uma organização diferente, mas exigem acesso aos dados da organização.

Conexões com a Internet

As conexões à Internet SOHO incluem telefone a cabo, DSL, celular, satélite e dial-up. As conexões de internet de negócios incluem Linha Leased Dedicated, Metro Ethernet, Business DSL e Satellite. A escolha da conexão varia dependendo da localização geográfica e da disponibilidade do provedor de serviço. Redes separadas tradicionais usavam diferentes tecnologias, regras e padrões. As redes convergentes fornecem dados, voz e vídeo entre muitos tipos diferentes de dispositivos na mesma infraestrutura de rede. Essa infraestrutura de rede usa o mesmo conjunto de regras, os mesmos contratos e normas de implementação. Packet Tracer é um programa de software flexível que permite usar representações de rede e teorias para construir modelos de rede e explorar LANs e WANs relativamente complexas.

Redes Confiáveis

O termo arquitetura de rede refere-se às tecnologias que suportam a infraestrutura e os serviços e regras ou protocolos programados que movem dados pela rede. À medida que as redes evoluem, aprendemos que existem quatro características básicas que os arquitetos de rede devem atender às expectativas dos usuários: Tolerância a falhas, Escalabilidade, Qualidade de Serviço (QoS) e Segurança. Uma rede tolerante a falhas é aquela que limita o número de dispositivos afetados durante uma falha. Ter vários caminhos para um destino é conhecido como redundância. Uma rede escalável se expande rapidamente para oferecer suporte a novos usuários e aplicativos. As redes são escaláveis porque os designers seguem padrões e protocolos aceitos. A QoS é um mecanismo primário para gerenciar congestionamentos e garantir a entrega confiável de conteúdo a todos os usuários. Os administradores de rede devem abordar dois tipos de preocupações de segurança de rede: segurança da infraestrutura de rede e segurança da informação. Para atingir os objetivos de segurança da rede, existem três requisitos principais: Confidencialidade, Integridade e Disponibilidade.

Tendências de rede

Existem várias tendências recentes de rede que afetam organizações e consumidores: Traga seu próprio dispositivo (BYOD), colaboração on-line, comunicações de vídeo e computação em nuvem. BYOD significa o uso de qualquer dispositivo, de qualquer propriedade e em qualquer lugar. As ferramentas de colaboração, como o Cisco WebEx, oferecem a funcionários, alunos, professores, clientes e parceiros uma maneira de conectar, interagir e alcançar instantaneamente seus objetivos. O vídeo é usado para comunicação, colaboração e entretenimento. Chamadas de vídeo são feitas de e para qualquer pessoa com uma conexão à Internet, independentemente de onde elas estão localizadas. A computação em nuvem nos permite armazenar arquivos pessoais, até fazer backup de uma unidade inteira em servidores pela Internet. Aplicativos como processamento de texto e edição de fotos podem ser acessados usando a nuvem. Existem quatro tipos principais de nuvens: nuvens públicas, nuvens privadas, nuvens híbridas e nuvens personalizadas. Atualmente, a tecnologia de casa inteligente está sendo desenvolvida para todos os cômodos de uma casa. A tecnologia doméstica inteligente se tornará mais comum à medida que as redes domésticas e a tecnologia de Internet de alta velocidade se expandirem. Usando a mesma fiação que fornece a eletricidade, a rede powerline envia informações ao enviar dados em determinadas frequências. Um provedor de serviços de Internet sem fio (WISP) é um provedor de serviços de Internet que conecta assinantes a um ponto de acesso ou hot spot designado usando tecnologias sem fio semelhantes encontradas em redes locais sem fio domésticas (WLANs).

Segurança de rede

Existem várias ameaças externas comuns às redes:

- Vírus, worms e cavalos de Troia;
- Spyware e adware
- Ataques de dia zero
- Ataques do ator de ameaças;
- Ataques de negação de serviço;
- Interceptação e roubo de dados;
- Roubo de identidade.

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

- Antivírus e antispyware;
- Filtragem por firewall.

Redes maiores e redes corporativas usam antivírus, antispyware e filtragem por firewall, mas também têm outros requisitos de segurança:

- Sistemas de firewall dedicados;
- ACLs (Access control lists, listas de controle de acesso);
- IPS (Intrusion prevention systems, sistemas de prevenção de intrusão);
- Redes privadas virtuais (VPN).