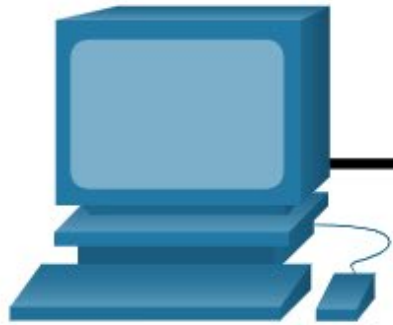


A large, faded, light gray watermark of the SENAI logo is visible in the background, spanning across the bottom half of the slide.

Prof. Nadson Andrey



Cliente



Servidor



Funções do Host

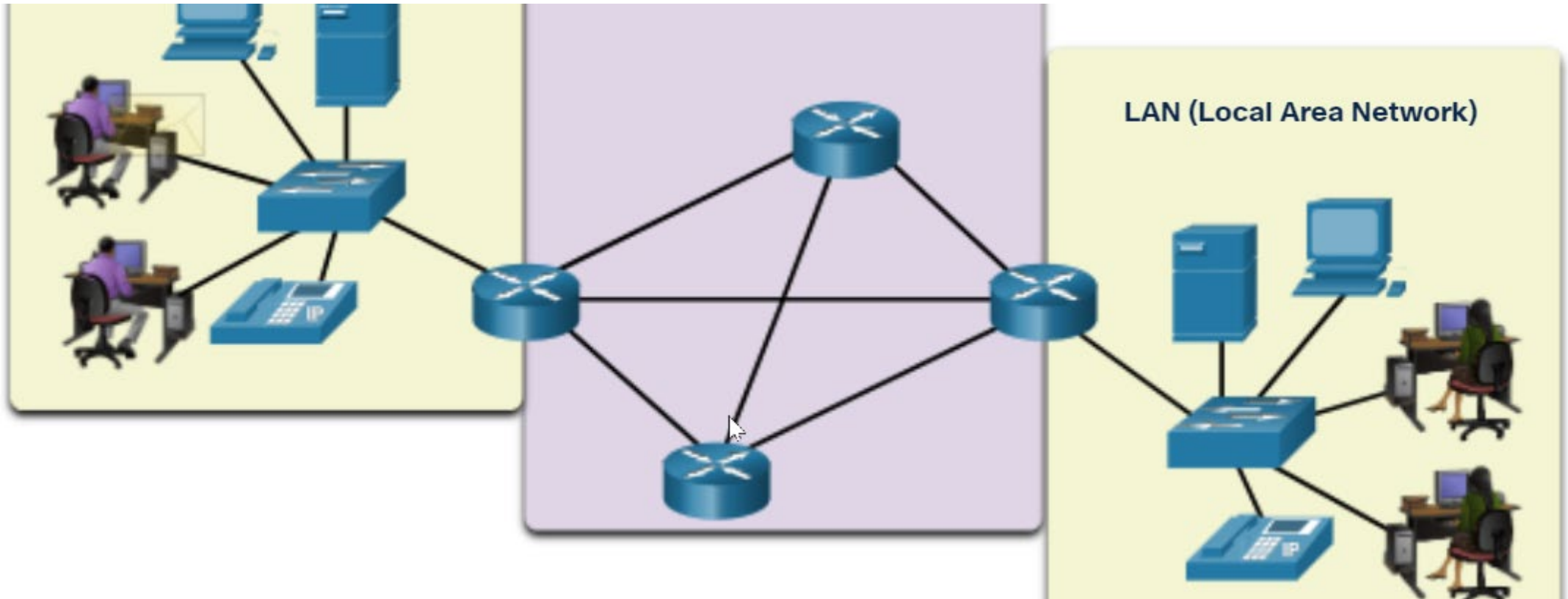
- Se você quiser fazer parte de uma comunidade on-line global, seu computador, tablet ou smartphone deve primeiro estar conectado a uma rede. Todos os computadores que estão conectados a uma rede e participam diretamente da comunicação em rede são classificados como hosts. Os hosts podem ser chamados de dispositivos finais.





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.



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.

Dispositivos intermediários



Roteador sem fio



Switch LAN



Roteador



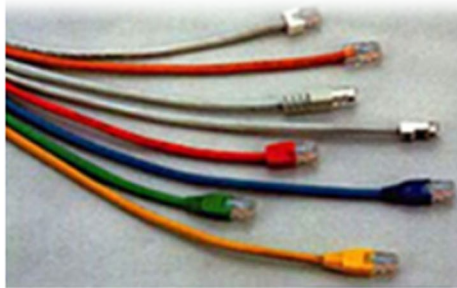
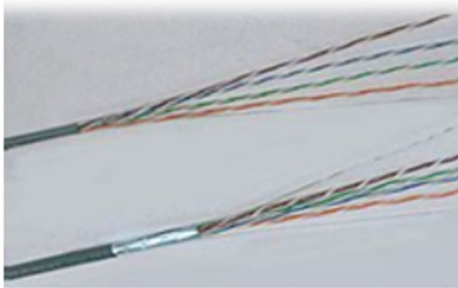
Switch multicamada



Dispositivo de firewall

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.



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.



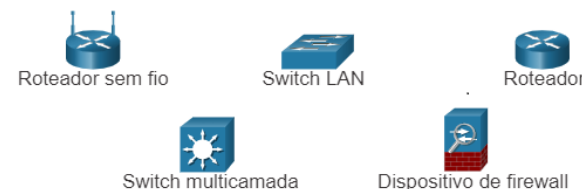
Representações de Rede

- 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.

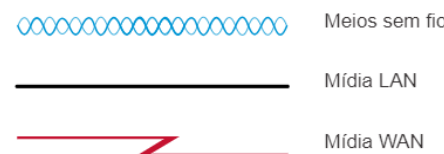
Dispositivos finais

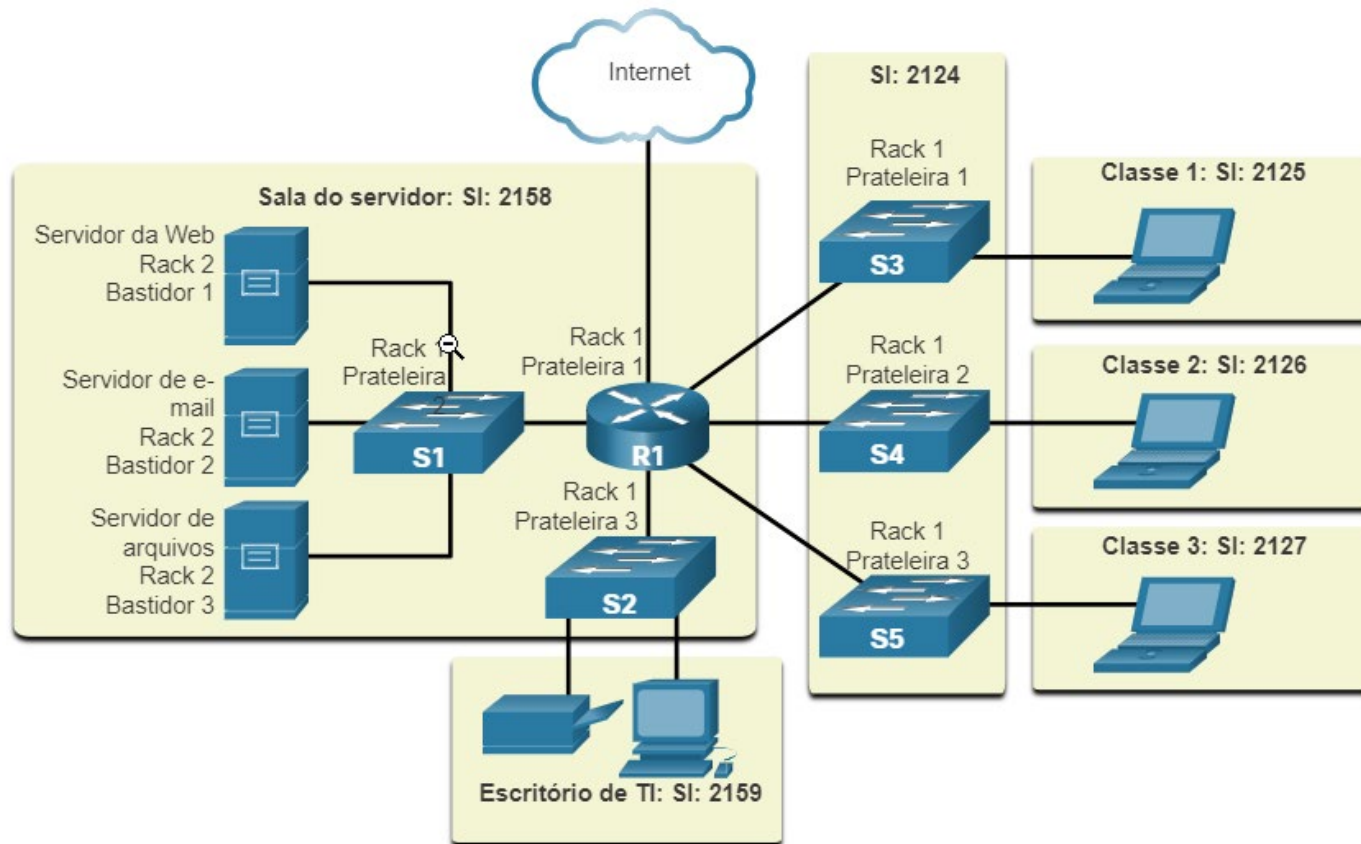


Dispositivos intermediários



Meios de rede





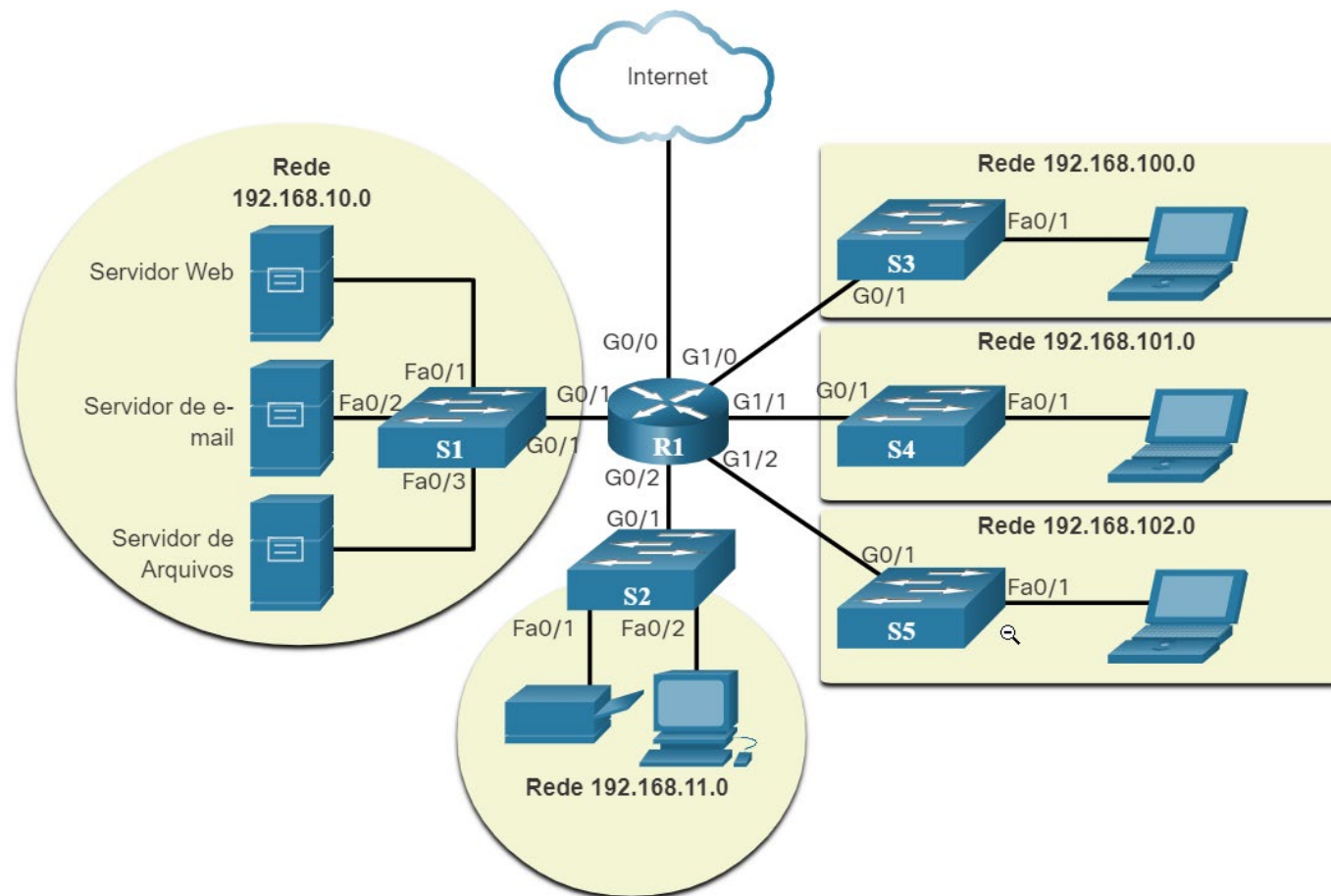
Diagramas de topologia física

- Os diagramas de topologia física ilustram a localização física dos dispositivos intermediários e a instalação dos cabos, conforme mostrado na figura

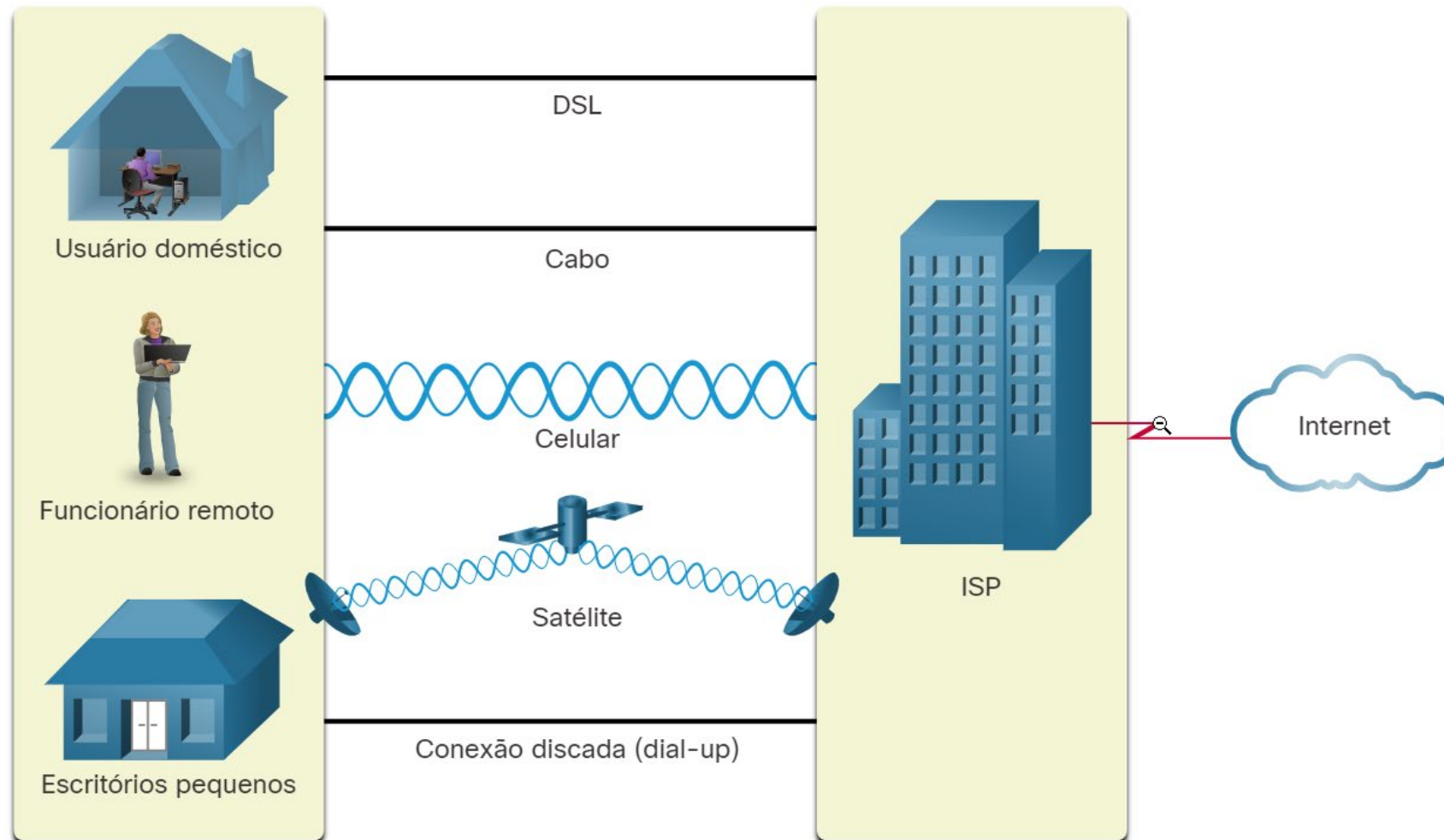


Diagramas de topologia lógica

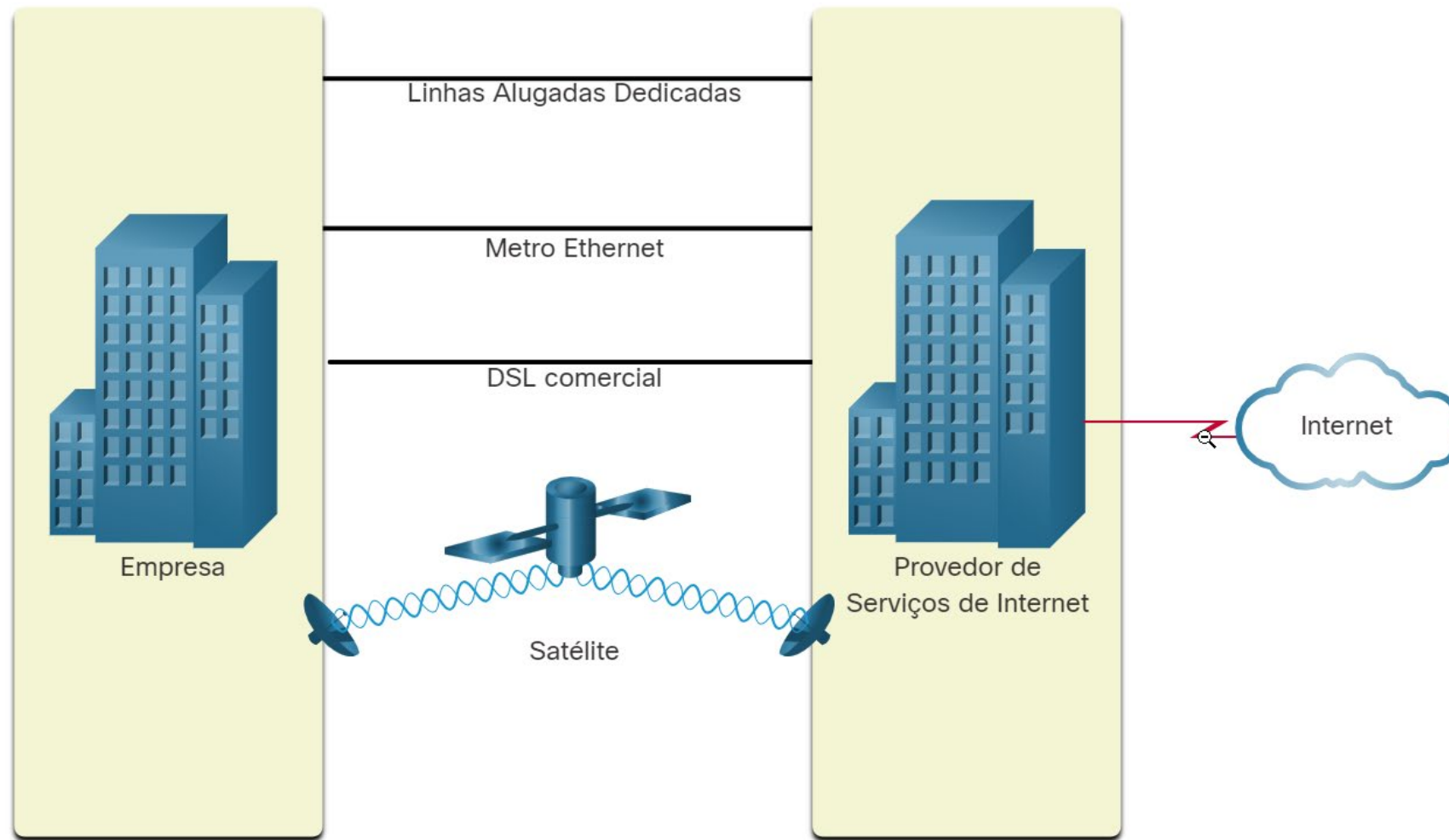
- Diagramas de topologia lógica ilustram dispositivos, portas e o esquema de endereçamento da rede, conforme mostrado na figura.



Conexões com a Internet para Residências e Pequenos Escritórios

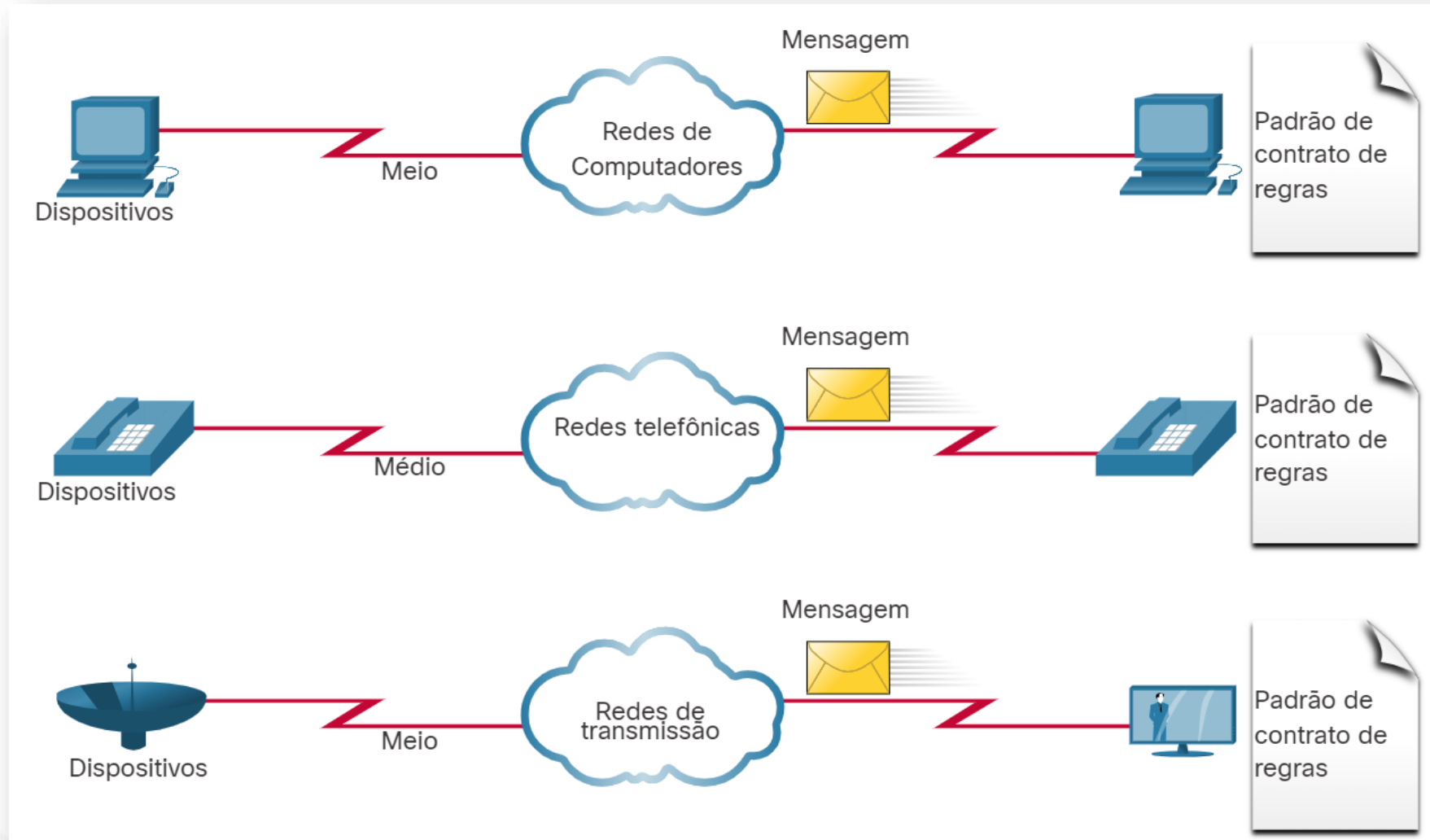


Conexões Corporativas com a Internet



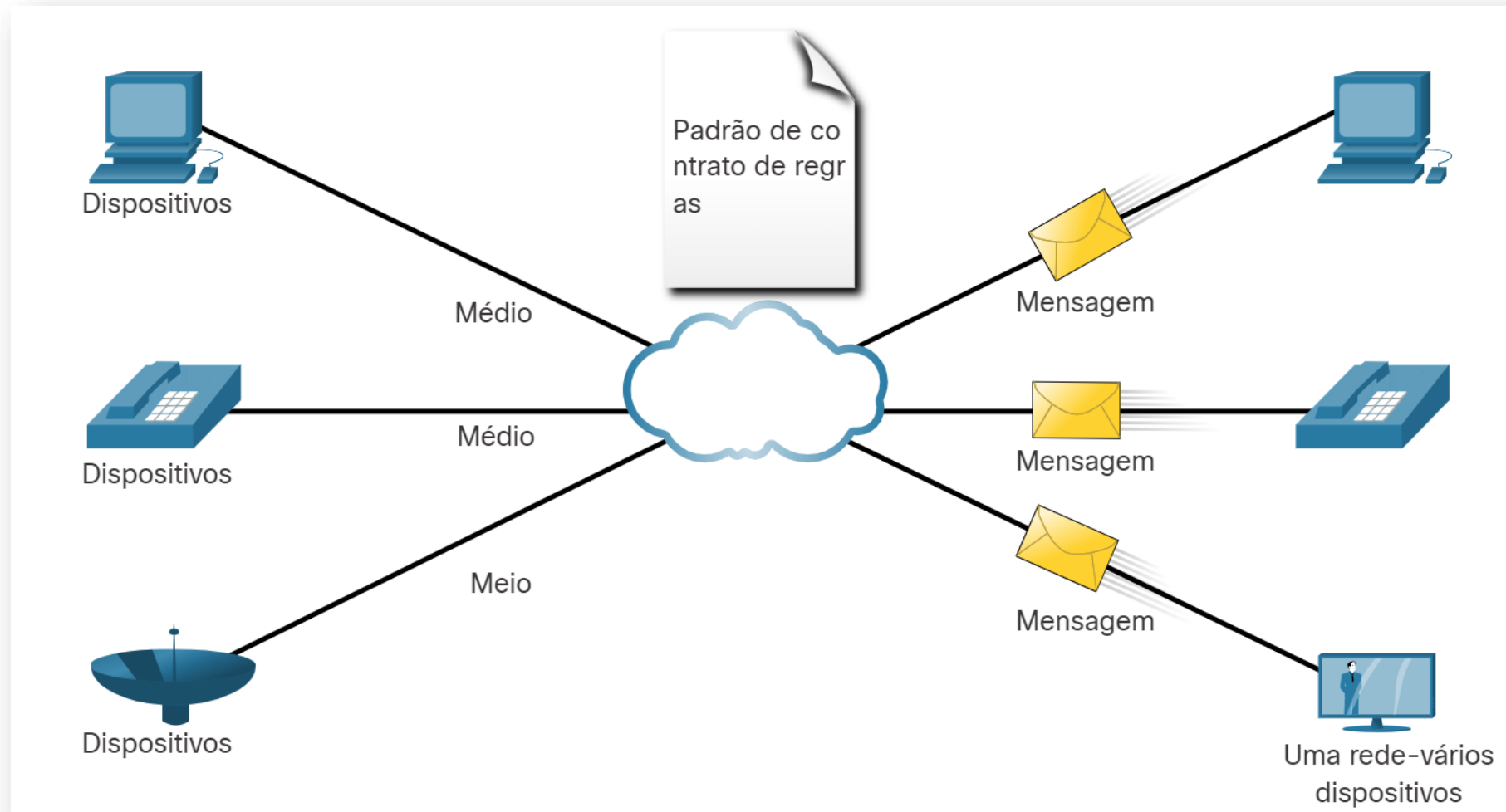
A Rede Convergente

Redes Separadas Tradicionais

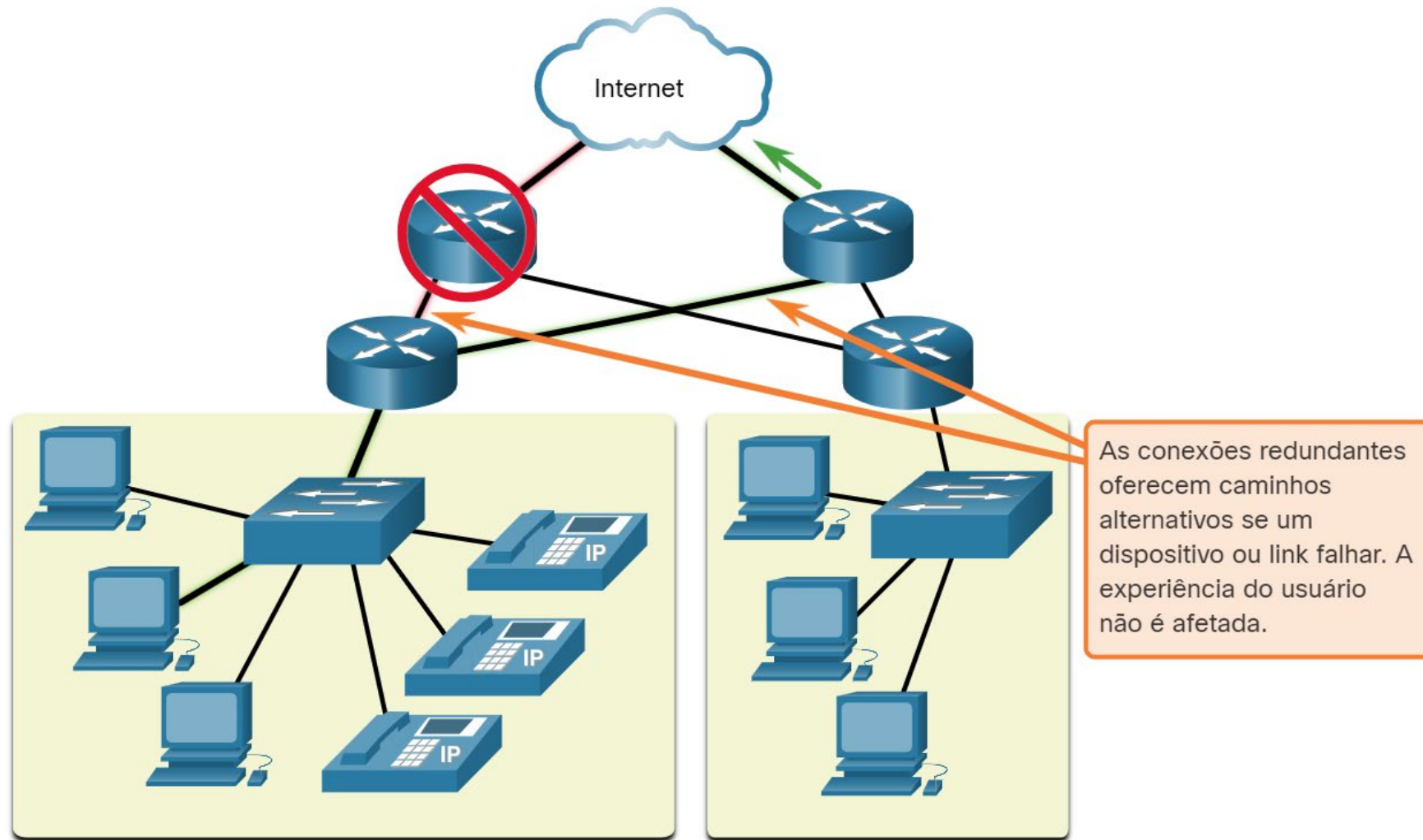


A Rede Convergente

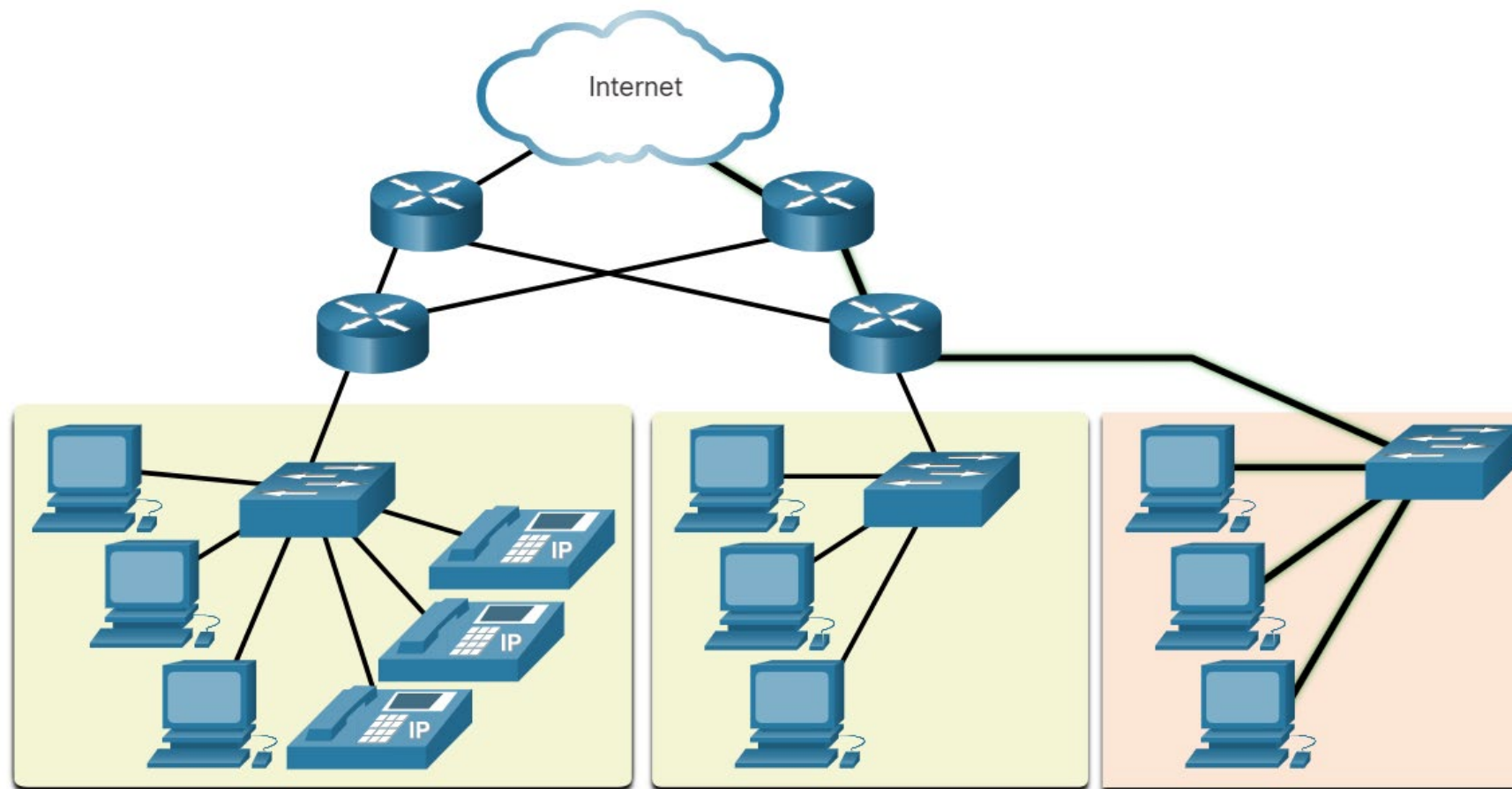
Redes convergentes



Tolerância a Falhas



Escalabilidade

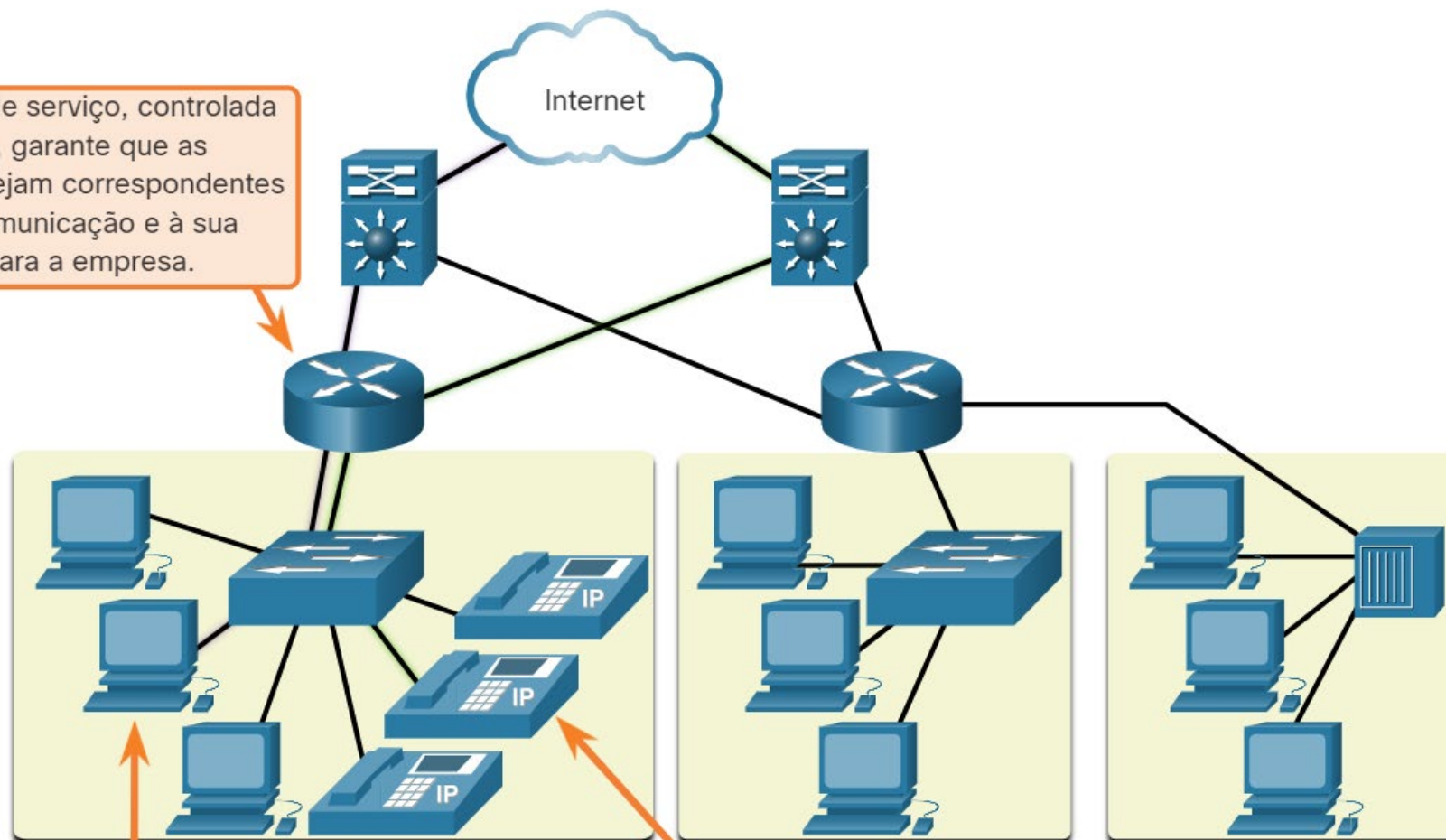


Usuários adicionais e redes inteiras podem ser conectados à Internet sem reduzir o desempenho para usuários atuais.



Qualidade de Serviço (QoS)

A qualidade de serviço, controlada pelo roteador, garante que as prioridades sejam correspondentes ao tipo de comunicação e à sua importância para a empresa.



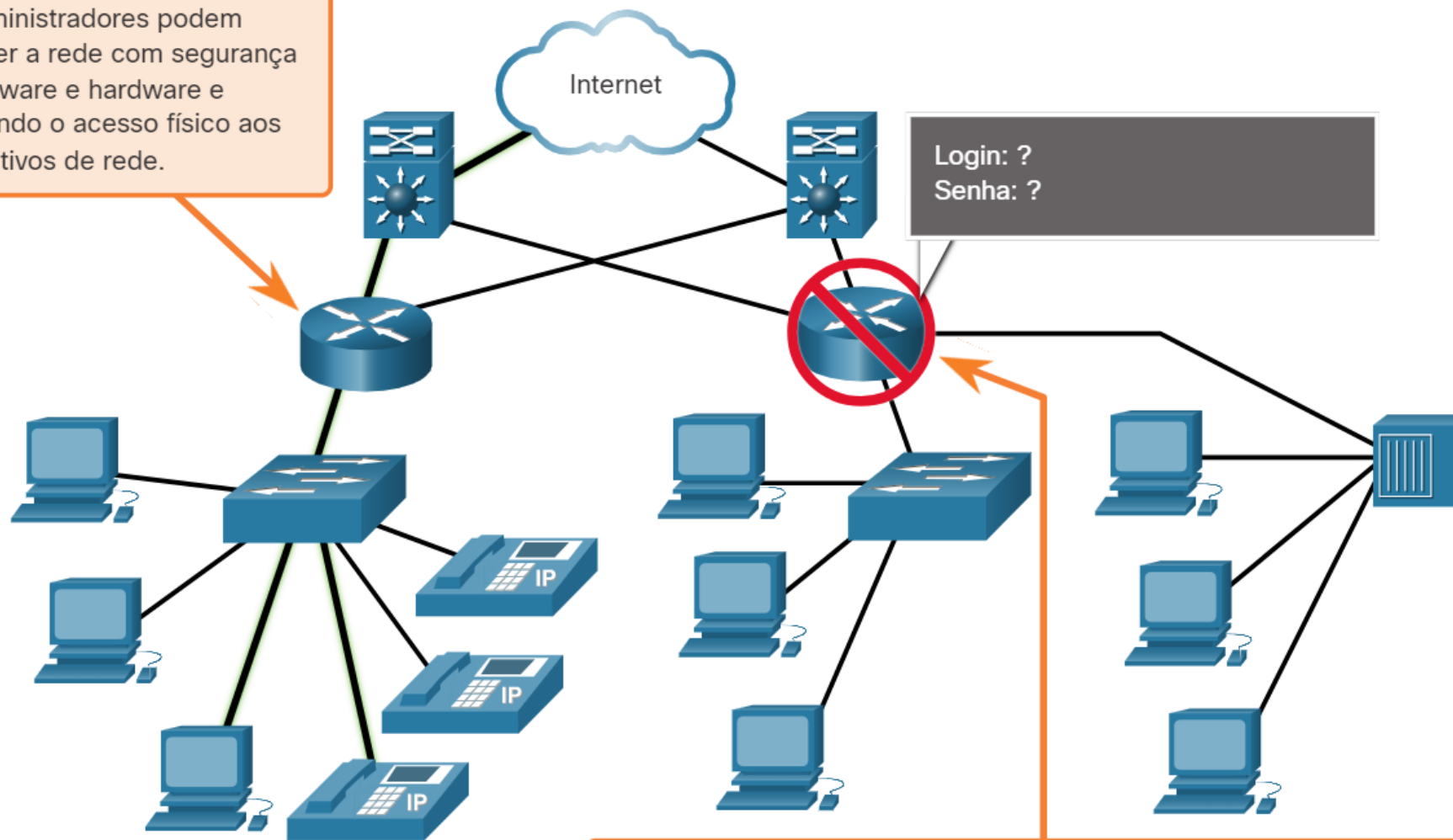
Geralmente, as páginas Web podem receber uma prioridade mais baixa.

Uma chamada de voz sobre IP (VoIP) precisará de prioridade para manter uma experiência suave e ininterrupta do usuário.



Segurança da Rede

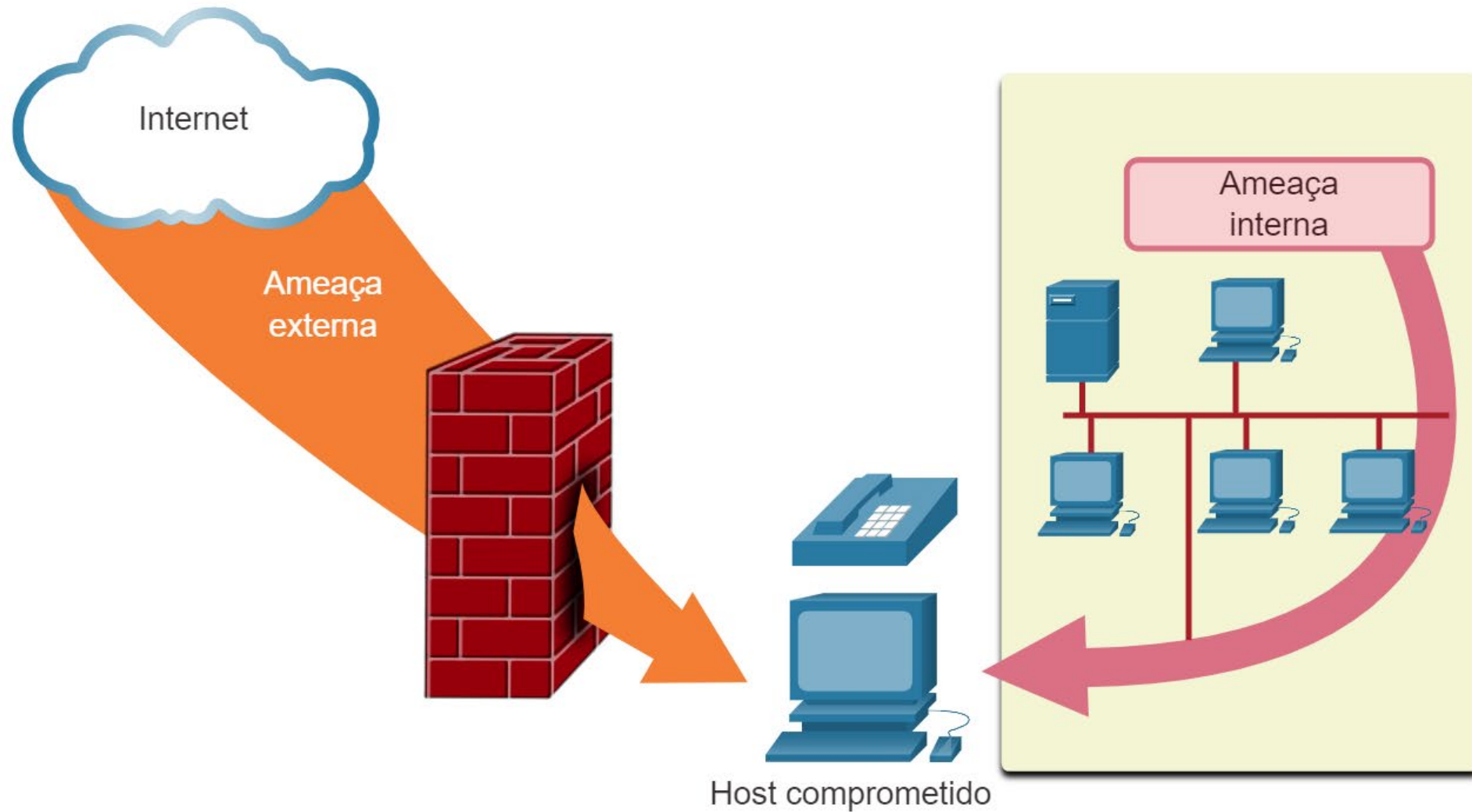
Os administradores podem proteger a rede com segurança de software e hardware e impedindo o acesso físico aos dispositivos de rede.



Medidas de segurança protegem a rede de acessos não autorizados.



Ameaça externa e Ameaça Interna

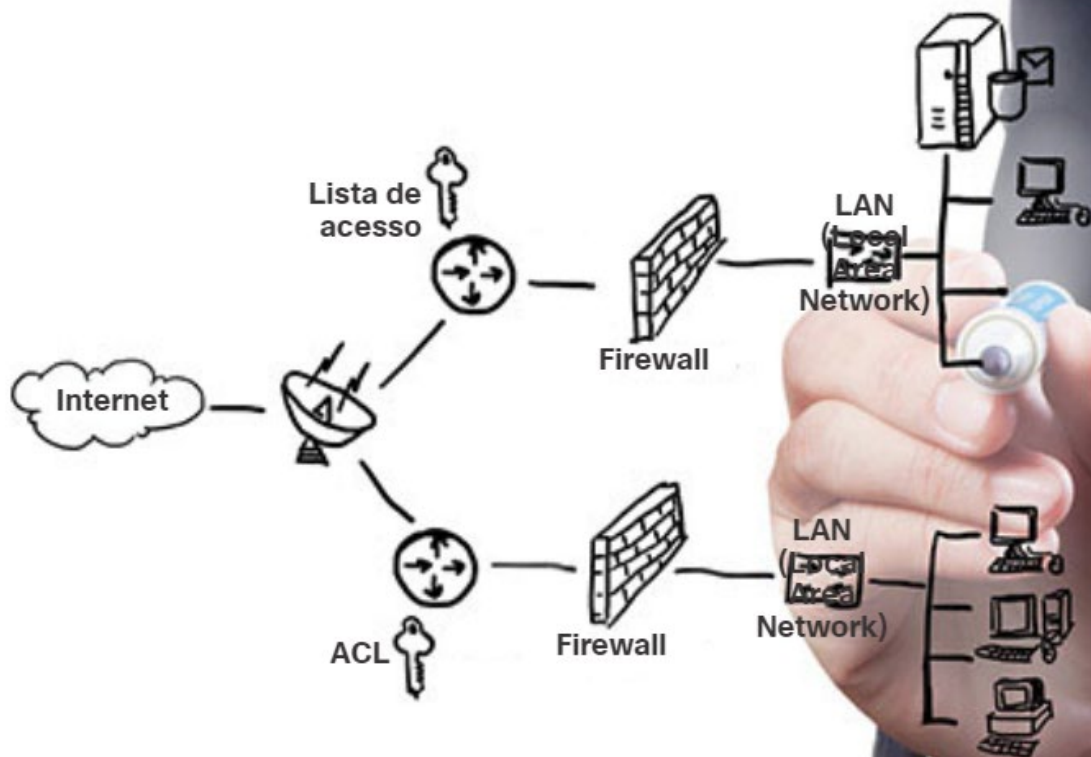


Existem várias ameaças externas comuns às redes:

- **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.



Soluções de Segurança



Soluções 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.





Fim da Apresentação

