Projeto de rede para duas salas de escritório

José Pimenta | Nº9 | 12ºP3 |UFCD-0846

REPÚBLICA PORTUGUESA EDUCAÇÃO
direção-geral educação
PESSOAS 2030
PORTUGAL 2030
Cofinanciado pela União Europeia
SELO DE CONFORMIDADE EQAVET
escola secundária VIRIATO

RESUMO

O presente trabalho tem por objetivo, a elaboração de um manual prático que permita aos leitores, sejam ou não, técnicos de redes, instalar uma rede local básica em casa ou no local de trabalho, sem recorrer a sessões de formação presenciais.

São abordados vários aspetos essenciais para a compreensão dos paradigmas de redes locais. Faz-se também, um estudo prático e sucinto de todos os componentes envolvidos no processo de comunicação, numa rede local.

Assim sendo, este manual permitirá ao leitor compreender o funcionamento de uma rede local, assim como o processo de instalação e configuração.

ÍNDICE

RESUMO 2
1- **introdução** 4
2- **arquiteturas de redes** 5
Topologias de Rede 5
Modelo OSI 6
Arquitetura tcp/ip 7
comparação modelo tcp/ip e osi 8
Sockets e portas 9
Protocolo ip (internet protocol) 10
Endereços ip 11
3- **topologias e cablagem de redes** 12
Topologias 12
cabos de rede e montagem da ficha rj45 14
4- **tecnologias de redes locais** 15
ethernet 15
Redes locais sem fios 16
beneficios de uma rede local sem fios 16
métodos de transmissão 17
padrões de redes sem fios 18
segurança em redes sem fios 19
5- **equipamentos de interligação da rede** 20
repetidores 20
Pontes (briges) 21
hubs 22
switches 23
Routers 24
servidores 25
6- **gestão e segurança de rede** 26
Documentação 26
segurança da rede 27
manutenção da rede 28
ataques a rede 29
7- **rede para duas salas de escritório uma em frente a outra** 30

1- INTRODUÇÃO

No panorama contemporâneo das organizações e ambientes de trabalho, a implementação eficaz de infraestruturas de rede desempenha um papel crucial na promoção da comunicação eficiente e na partilha de recursos. Neste contexto, o presente trabalho propõe-se a abordar a conceção e elaboração de uma rede em estrela destinada a interligar duas salas de escritório situadas uma em frente à outra. A escolha por uma topologia em estrela é motivada pela sua simplicidade, escalabilidade e facilidade de manutenção, características que se revelam particularmente vantajosas para ambientes de média dimensão, como o descrito.

O intuito principal deste trabalho é proporcionar uma visão abrangente sobre o processo de planeamento, instalação e configuração de uma rede local que possibilite a comunicação fluida entre duas salas distintas. Ao enfocar uma abordagem prática e aplicada, almejo não apenas fornecer conhecimentos teóricos, mas também capacitar os leitores, independentemente do seu nível técnico, a efetuarem a implementação desta solução de forma autónoma.

Ao longo deste documento, serão explorados os fundamentos teóricos associados às redes em estrela, bem como as especificidades inerentes à interconexão de duas salas contíguas. Será igualmente apresentado um estudo detalhado dos componentes envolvidos, desde hardware a protocolos de comunicação, com o intuito de proporcionar uma compreensão holística do sistema proposto.

Desta forma, acredito que este trabalho não só contribuirá para o enriquecimento do conhecimento sobre redes, mas também servirá como guia prático e acessível para aqueles que desejam implementar uma solução de rede em estrela em ambientes de escritório interligados.

2- ARQUITETURAS DE REDES

TOPOLOGIAS DE REDE

Uma topologia de rede refere-se à estrutura física ou lógica pela qual os dispositivos de uma rede de computadores estão interligados. A escolha da topologia de rede influencia diretamente na eficiência, desempenho e facilidade de manutenção da rede.

Existem várias topologias de rede, cada uma com características específicas. Alguns dos tipos mais comuns são:

Topologia em Estrela: Nesta topologia, todos os dispositivos estão conectados a um ponto central, geralmente um switch ou hub. Isso facilita a administração da rede, torna a deteção de problemas mais simples e isola falhas em um dispositivo, sem afetar os outros.

Topologia em Anel: Os dispositivos são conectados em um formato de anel, onde cada dispositivo está conectado ao dispositivo adjacente. A informação circula pelo anel até atingir o destinatário desejado. Esta topologia é menos comum devido à sua vulnerabilidade a falhas, uma vez que a quebra em qualquer ponto do anel pode interromper toda a comunicação.

Topologia em Barramento: Nesta topologia, todos os dispositivos estão conectados a um único cabo, conhecido como barramento. Embora seja uma das topologias mais simples, é mais suscetível a colisões de dados e dificulta a deteção de falhas.

Topologia em Malha: Cada dispositivo está conectado a vários outros na rede. Isso cria redundância e aumenta a confiabilidade da rede, pois a falha em um caminho não impede a comunicação.

Topologia em Árvore: Uma combinação da topologia em estrela e em barramento, onde os dispositivos estão organizados em hierarquias, semelhante a uma estrutura de árvore. Essa topologia é mais escalável e oferece redundância.

MODELO OSI

O Modelo OSI (Open Systems Interconnection) é o modelo de referência utilizado para entender e descrever as funcionalidades dos protocolos de rede. Vamos abordar brevemente cada um deles:

Camada Física: Lida com a transmissão de bits brutos sobre um meio físico, como cabos ou sinais sem fio.

Camada de Enlace de Dados: Gerencia a comunicação entre dispositivos adjacentes na mesma rede. Controla o fluxo de dados, detecção e correção de erros.

Camada de Rede: Responsável pelo roteamento dos dados entre diferentes redes. Fornece serviços de roteamento e encaminhamento.

Camada de Transporte: Fornecer comunicação ponto-a-ponto, garantindo a entrega confiável de dados. Responsável pelo controle de fluxo, correção de erros e retransmissão de dados.

Camada de Sessão: Gerencia, estabelece e encerra as sessões entre aplicativos em dispositivos diferentes.

Camada de Apresentação: Lida com a tradução, compressão e criptografia dos dados. Garante que os dados sejam apresentados de maneira compreensível.

Camada de Aplicação: Fornece serviços de rede diretamente aos aplicativos do usuário, como e-mail, navegadores web e outros.

ARQUITETURA TCP/IP

A arquitetura TCP/IP (Transmission Control Protocol/Internet Protocol) é o conjunto de protocolos de comunicação utilizados para a transmissão de dados na Internet.

Camada de Ligação de Dados: Nesta camada, são tratadas as comunicações de dados entre dispositivos em redes locais (LAN). Engloba protocolos como Ethernet, Wi-Fi e outros protocolos de ligação.

Camada de Rede: A camada de rede é responsável pelo encaminhamento de dados entre diferentes redes. O protocolo principal nesta camada é o Protocolo da Internet (IP), usado para endereçar e encaminhar pacotes de dados entre dispositivos em redes diferentes.

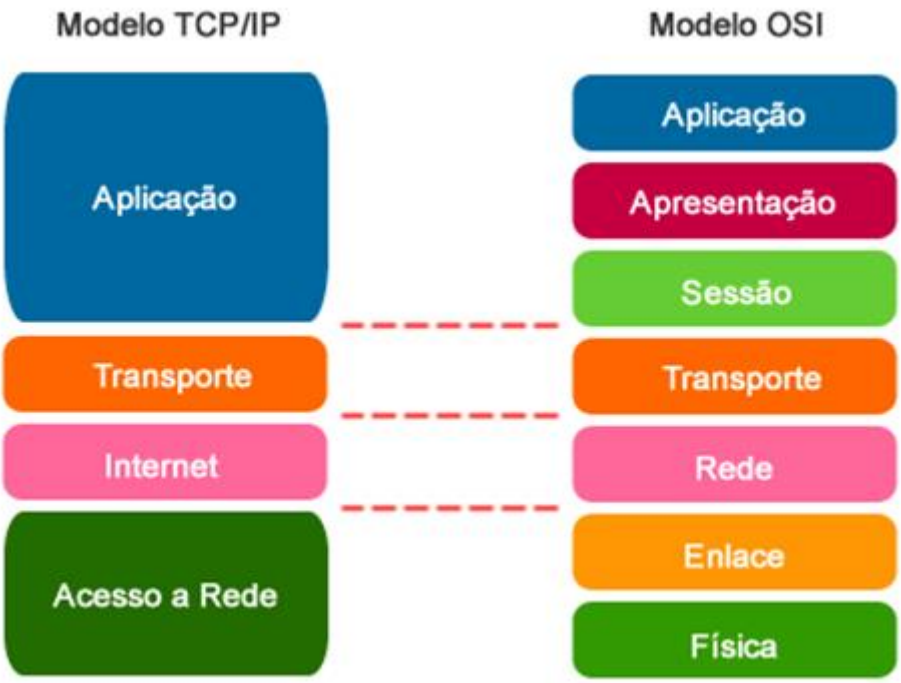
Camada de Transporte: A camada de transporte proporciona comunicação de hospedeiro para hospedeiro, gerindo a transmissão de dados de forma fiável. Os protocolos mais comuns nesta camada são o Protocolo de Controlo de Transmissão (TCP) e o Protocolo de Datagrama de Utilizador (UDP).

TCP (Protocolo de Controlo de Transmissão): Fornece comunicação orientada para a conexão, garantindo a entrega ordenada e fiável de dados. É usado para aplicações que requerem uma transmissão segura e sem perdas de dados, como transferência de ficheiros, navegação na web, etc.

UDP (Protocolo de Datagrama de Utilizador): Proporciona comunicação não orientada para a conexão e é mais leve do que o TCP. É usado em situações em que uma entrega mais rápida é preferível, mesmo que isso signifique sacrificar a fiabilidade, como em transmissões de vídeo ou jogos online.

Camada de Aplicação: Na camada de aplicação é onde as aplicações de utilizador interagem com o protocolo. Aqui, encontrará uma variedade de protocolos para serviços específicos, como HTTP (Protocolo de Transferência de Hipertexto) para navegação na web, SMTP (Protocolo de Transferência de Correio Simples) para e-mails, FTP (Protocolo de Transferência de Ficheiros) para transferência de ficheiros, entre muitos outros.

COMPARAÇÃO MODELO TCP/IP E OSI



SOCKETS E PORTAS

No mundo da tecnologia, conceitos como sockets e portas desempenham um papel fundamental na facilitação da troca de informações entre sistemas computacionais. Esses elementos são essenciais para a implementação de comunicação eficiente, seja entre processos em uma máquina local ou entre dispositivos em redes globais.

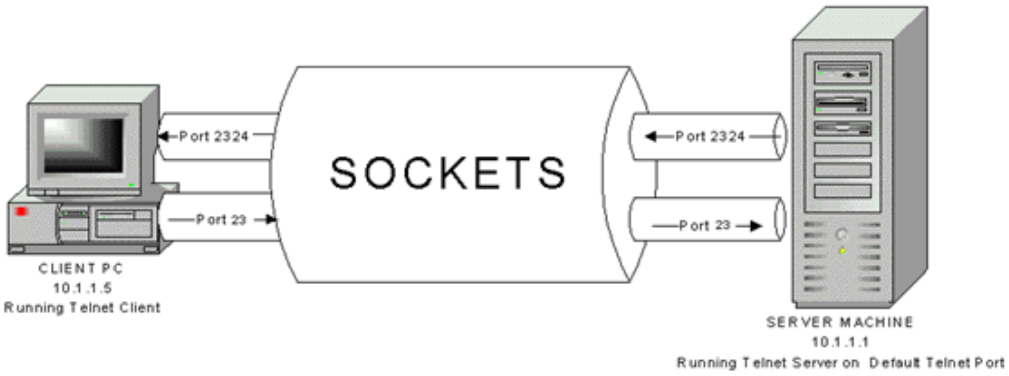
Sockets:

Os sockets, em termos simples, são pontos de extremidade que permitem a comunicação entre diferentes programas ou processos, tanto localmente quanto através de uma rede. Eles proporcionam uma abstração que simplifica a transmissão de dados, sendo essenciais para o desenvolvimento de aplicações que dependem da interação entre sistemas.

Portas:

As portas, por sua vez, desempenham o papel de direcionadores de tráfego, permitindo que diferentes serviços em um mesmo dispositivo se comuniquem de forma organizada. Cada porta é associada a um serviço específico, contribuindo para a identificação única de processos em execução e facilitando a entrega precisa de dados.

Em conjunto, sockets e portas formam a base para a comunicação eficaz em redes de computadores. Seja na transmissão de dados em uma rede local ou na interação global através da internet, esses conceitos desempenham um papel crucial na criação de aplicações e serviços que conectam o mundo digital de maneira transparente e eficiente.



PROTOCOLO IP (INTERNET PROTOCOL)

O Internet Protocol (IP) é um conjunto de regras que governa a comunicação de dados na Internet. Ele fornece um endereçamento único para cada dispositivo conectado a uma rede e define como os dados são divididos em pacotes, roteados entre dispositivos e reagrupados no destino. O IP faz parte da camada de rede no modelo de referência OSI (Open Systems Interconnection) e é fundamental para o funcionamento da Internet.

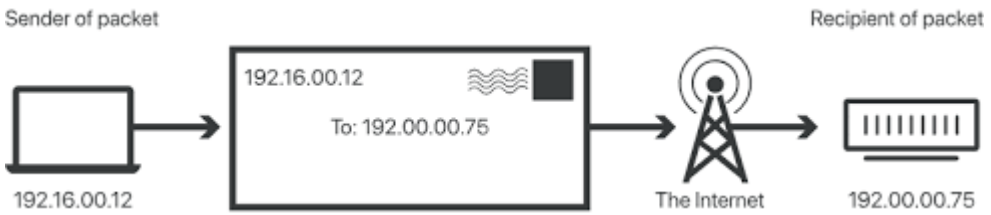
Existem duas versões principais do Internet Protocol: IPv4 (Internet Protocol version 4) e IPv6 (Internet Protocol version 6).

IPv4: Esta é a versão mais amplamente utilizada. Os endereços IPv4 são compostos por 32 bits, o que permite aproximadamente 4,3 bilhões de endereços únicos. No entanto, devido ao crescimento exponencial da Internet, o esgotamento gradual dos endereços IPv4 se tornou um problema.

IPv6: Introduzido para resolver o problema de escassez de endereços IPv4, o IPv6 usa endereços de 128 bits, proporcionando um espaço de endereço virtualmente ilimitado. Isso é especialmente importante com a proliferação de dispositivos conectados à Internet. O IPv6 é compatível com o IPv4, permitindo uma transição suave.

O funcionamento básico do IP envolve a fragmentação de dados em pacotes, a atribuição de endereços IP a dispositivos e o roteamento desses pacotes através de redes interconectadas até alcançarem seu destino. O IP não lida com aspectos de garantia de entrega, confiabilidade ou controle de fluxo; essas funções podem ser tratadas por protocolos de camadas superiores, como o TCP (Transmission Control Protocol).

Além disso, o IP opera em conjunto com outros protocolos de camadas superiores, como o TCP e o UDP (User Datagram Protocol), que oferecem serviços mais especializados, como controle de fluxo (TCP) ou comunicação sem conexão (UDP). O conjunto TCP/IP, composto por TCP, IP e outros protocolos relacionados, é a base da comunicação na Internet.



ENDEREÇOS IP

Os endereços IP (Internet Protocol) são identificados através de números (e letras) exclusivos atribuídos a cada dispositivo em uma rede que utiliza o protocolo IP para comunicação. Eles são essenciais para o encaminhamento de dados na Internet. Existem duas principais versões de endereços IP, conhecidas como IPv4 e IPv6.

IPv4 (Internet Protocol version 4):

Os endereços IPv4 são compostos por 32 bits, divididos em quatro conjuntos de octetos, representados em notação decimal separada por pontos (por exemplo, 192.168.0.1). Cada octeto pode variar de 0 a 255. No total, IPv4 oferece aproximadamente 4,3 bilhões de endereços únicos.

Exemplo de endereço IPv4:

192.168.1.1

IPv6 (Internet Protocol version 6):

Devido à limitação de endereços disponíveis no IPv4, foi desenvolvida a versão IPv6, que utiliza endereços de 128 bits. A notação IPv6 utiliza grupos de quatro dígitos hexadecimais, separados por dois pontos (por exemplo, 2001:0db8:85a3:0000:0000:8a2e:0370:7334). O IPv6 proporciona um espaço de endereço praticamente ilimitado.

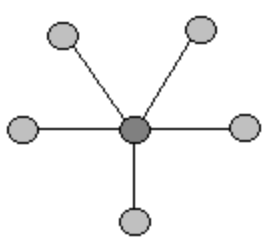
Exemplo de endereço IPv6:

2001:0db8:85a3:0000:0000:8a2e:0370:7334

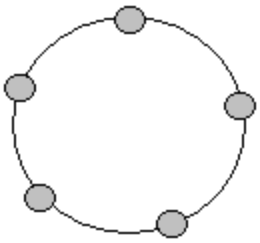
3- TOPOLOGIAS E CABLAGEM DE REDES

TOPOLOGIAS

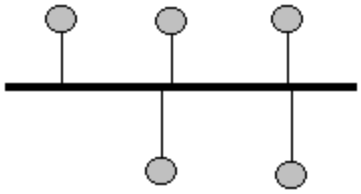
"topologia" refere-se à disposição física ou lógica dos elementos numa rede de computadores. É a estrutura ou configuração geral da rede, incluindo como os dispositivos estão interligados e como a comunicação ocorre entre eles. Existem várias topologias comuns, como a topologia em barramento, em estrela, em anel, em árvore, entre outras, cada uma com características específicas adequadas para diferentes necessidades e ambientes de rede.



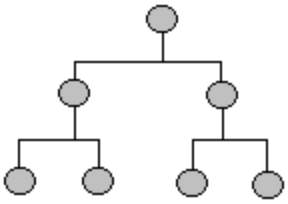
Estrela



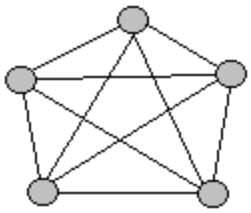
Anel



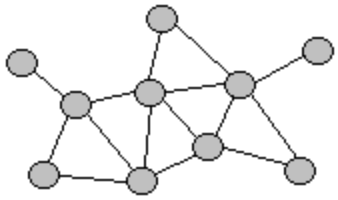
Barramento



Árvore



Ponto a Ponto



Mesh

Topologia em barramento (bus):

Todos os dispositivos estão ligados a um único cabo, que serve como um barramento partilhado, os dados são transmitidos de um dispositivo para outro ao longo do barramento.

Topologia em estrela (star):

Cada dispositivo numa rede com topologia em estrela está ligado a um ponto central, como um switch ou um hub, todos os dados passam através desse ponto central, se um dispositivo falhar, geralmente não afeta o resto da rede.

Topologia em anel (ring):

Cada dispositivo é ligado diretamente a dois outros dispositivos, formando um circuito fechado ou anel, os dados são transmitidos numa única direção ao longo do anel.

Topologia em árvore (tree):

Esta topologia é uma combinação de topologia em estrela e topologia em barramento, os dispositivos são organizados hierarquicamente, com sub-redes individuais ligadas a uma espinha dorsal central.

Topologia mista (mixed):

Esta topologia é uma combinação de duas ou mais das topologias acima, pode ser usada para criar redes complexas que atendem a requisitos específicos de uma organização.

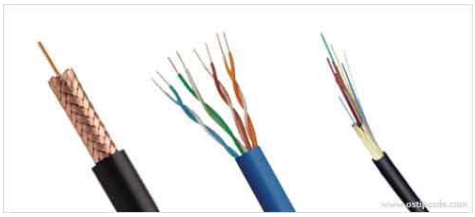
CABOS DE REDE E MONTAGEM DA FICHA RJ45

Os "cabos de rede" referem-se aos cabos utilizados para estabelecer conexões físicas entre dispositivos em redes de computadores. Esses cabos são usados para transmitir dados entre dispositivos, como computadores, switches, routers, impressoras, entre outros. Existem diferentes tipos de cabos de rede, cada um com suas próprias características e aplicações, incluindo cabos de pares entrançados (como o cabo Ethernet), cabos coaxiais e cabos de fibra ótica.

Cabos coaxiais: Cabos de comunicação que consistem em um condutor central cercado por uma camada isolante, uma malha metálica e uma capa externa. São utilizados para transmitir sinais de alta frequência, como os utilizados em redes de televisão por cabo ou em redes de computadores.

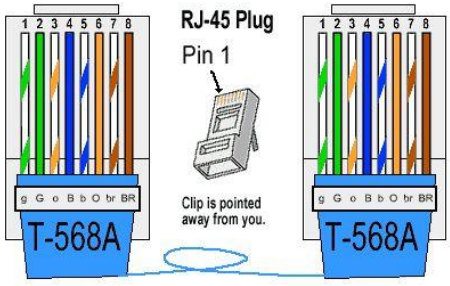
Cabos de pares entrançados (twisted pairs): Cabos que consistem em pares de fios de cobre entrançados um ao redor do outro para reduzir a interferência eletromagnética. São amplamente utilizados em redes de computadores, telefonia e outras aplicações de comunicação de dados.

Cabos de fibra ótica: Cabos compostos por filamentos de vidro ou plástico, capazes de transmitir sinais de luz ao longo de grandes distâncias com alta velocidade e largura de banda. São utilizados em redes de alta velocidade e em situações onde a imunidade à interferência eletromagnética é essencial.



Tomadas para cabos com conectores RJ-45 fêmea: São as tomadas utilizadas para conectar cabos de pares entrançados, comumente encontradas em ambientes de rede. Os conectores RJ-45 são os mais comuns para cabos Ethernet.

Montagem de tomadas RJ-45: Refere-se ao processo de instalação e montagem das tomadas de rede RJ-45, onde os cabos de pares entrançados são conectados para estabelecer a comunicação em uma rede.



4- TECNOLOGIAS DE REDES LOCAIS

ETHERNET

Ethernet é uma tecnologia de redes de computadores que estabelece padrões para a comunicação entre dispositivos numa rede local (LAN - Local Area Network). É amplamente utilizada em ambientes comerciais, residenciais e industriais para interligar dispositivos como computadores, impressoras, switches, routers e outros equipamentos de rede.

Velocidades da “Ethernet”:

10 Mbps (Megabits por segundo): Este foi o padrão original da Ethernet, conhecido como 10BASE-T. Suporta uma taxa máxima de transferência de dados de 10 megabits por segundo.

100 Mbps (Megabits por segundo): Também conhecido como Fast Ethernet, este padrão melhorou o original 10 Mbps Ethernet, fornecendo uma taxa máxima de transferência de dados de 100 megabits por segundo. É comumente referido como 100BASE-TX.

1000 Mbps (Megabits por segundo) ou 1 Gbps (Gigabit por segundo): Conhecido como Gigabit Ethernet, este padrão oferece taxas de transferência de dados de até 1 gigabit por segundo. É comumente referido como 1000BASE-T.

10 Gbps (Gigabits por segundo): Este é 10 vezes mais rápido que o Gigabit Ethernet, fornecendo taxas de transferência de dados de até 10 gigabits por segundo. É referido como 10GBASE-T.

Cada um destes padrões Ethernet tem a sua própria gama de dispositivos compatíveis e é adequado para diferentes ambientes de rede, dependendo de fatores como largura de banda necessária, distância sobre a qual os dados precisam ser transmitidos e considerações de custo.

REDES LOCAIS SEM FIOS

Redes locais sem fios, mais comumente conhecidas como redes Wi-Fi (Wireless Fidelity), são redes de computadores ou dispositivos que se comunicam entre si usando ondas de rádio em vez de cabos físicos. Essas redes são amplamente utilizadas em ambientes domésticos, comerciais e públicos devido à sua conveniência e facilidade de implantação.

BENEFICIOS DE UMA REDE LOCAL SEM FIOS

Mobilidade: Uma das maiores vantagens do Wi-Fi é a capacidade de ligar dispositivos à rede sem a necessidade de fios físicos. Isso permite uma maior mobilidade para dispositivos como laptops, smartphones, tablets e dispositivos IoT, que podem conectar-se à rede em qualquer lugar dentro do alcance do sinal Wi-Fi.

Conveniência: Sem a necessidade de fios, a configuração e a manutenção de uma rede Wi-Fi são mais simples e menos dispendiosas do que as redes com fio.

Flexibilidade: As redes Wi-Fi permitem que os dispositivos sejam facilmente adicionados à rede ou removidos dela, sem a necessidade de conectar ou desconectar cabos físicos. Isso torna mais fácil expandir ou reconfigurar uma rede conforme as necessidades mudam.

Cobertura Estendida: Com a instalação de repetidores ou extensores de alcance, é possível estender a cobertura da rede Wi-Fi para áreas que podem estar fora do alcance direto do router sem fios.

Acesso Conveniente à Internet: Com uma rede Wi-Fi, os dispositivos podem ligar-se à internet sem a necessidade de conexões com fio, permitindo um acesso fácil e conveniente à web em toda a casa ou escritório.

Suporte para Múltiplos Dispositivos: As redes Wi-Fi são capazes de suportar vários dispositivos conectados simultaneamente, permitindo que várias pessoas usem a rede ao mesmo tempo, sem interferência entre os dispositivos.

Facilidade de Implementação: Configurar uma rede Wi-Fi é geralmente mais fácil e mais rápido do que instalar uma rede com fio, pois não requer a passagem de cabos através de paredes ou pisos. Isso torna as redes Wi-Fi uma escolha popular para ambientes residenciais e comerciais.

Economia de Custos: Embora haja um investimento inicial em hardware, como routers e adaptadores sem fio, a longo prazo, as redes Wi-Fi podem ser mais econômicas do que as redes com fio devido à redução nos custos de instalação e manutenção.

MÉTODOS DE TRANSMISSÃO

Transmissão Analógica: Este método envolve a representação contínua de dados, utilizando formas de onda analógicas. É frequentemente usado em comunicações de voz e áudio, onde os sinais são transmitidos como ondas sonoras.

Transmissão Digital: Neste método, os dados são representados discretamente, em forma de bits, sendo codificados em sequências binárias (0s e 1s). A transmissão digital é mais resistente a ruídos e distorções e é amplamente usada em redes de computadores e comunicações de dados.

Transmissão em Banda Base: Este método transmite sinais digitais diretamente sobre o meio de transmissão, como um cabo de cobre ou fibra óptica. Os sinais são codificados em pulsos elétricos ou ópticos e transmitidos em sua forma original.

Modulação de Amplitude (AM) e Modulação de Frequência (FM): Estes são métodos comuns de modulação usados na transmissão de sinais analógicos. Na modulação de amplitude, a amplitude do sinal portador é modificada de acordo com o sinal de entrada. Na modulação de frequência, a frequência do sinal portador é modificada.

Modulação de Amplitude em Quadratura (QAM): Este é um método de modulação usado em transmissões digitais, onde múltiplos sinais digitais são combinados e transmitidos simultaneamente em diferentes fases e amplitudes. É amplamente utilizado em sistemas de comunicação digital, como transmissões de televisão digital e Internet de alta velocidade.

Spread Spectrum: Este método distribui o sinal de dados sobre uma largura de banda maior do que a necessária para a transmissão normal, o que ajuda a melhorar a resistência a interferências e ruídos. Ele é comumente usado em tecnologias sem fio, como Wi-Fi e Bluetooth.

Multiplexagem: Este método permite que vários sinais sejam combinados em um único canal de comunicação, permitindo uma utilização mais eficiente do meio de transmissão. Existem várias técnicas de multiplexagem, incluindo a divisão de tempo (TDM), a divisão de frequência (FDM) e a divisão de código (CDM).

PADRÕES DE REDES SEM FIOS

Os padrões de redes sem fios são especificações técnicas estabelecidas pela IEEE (Institute of Electrical and Electronics Engineers) que definem como dispositivos sem fio devem operar e se comunicar entre si. Esses padrões são projetados para garantir a interoperabilidade entre dispositivos de diferentes fabricantes e para promover a compatibilidade e o desempenho das redes sem fio.

Existem vários padrões de redes sem fio (Wi-Fi) que foram desenvolvidos ao longo do tempo para melhorar a velocidade, alcance, segurança e eficiência das comunicações sem fio. Aqui estão alguns dos principais padrões de Wi-Fi:

IEEE 802.11b: Lançado em 1999, o 802.11b foi um dos primeiros padrões Wi-Fi comercializados. Opera na banda de frequência de 2,4 GHz e suporta velocidades de até 11 Mbps.

IEEE 802.11a: Também lançado em 1999, o 802.11a opera na banda de frequência de 5 GHz e suporta velocidades de até 54 Mbps. Ele oferece maior largura de banda e menos interferência do que o 802.11b, mas tem um alcance menor.

IEEE 802.11g: Lançado em 2003, o 802.11g opera na banda de frequência de 2,4 GHz e suporta velocidades de até 54 Mbps. Ele é compatível com o 802.11b e oferece um alcance semelhante, mas com uma velocidade de transferência mais rápida.

IEEE 802.11n: Introduzido em 2009, o 802.11n é projetado para oferecer maior alcance e velocidades mais rápidas do que os padrões anteriores. Ele opera nas bandas de frequência de 2,4 GHz e/ou 5 GHz e suporta velocidades teóricas de até 600 Mbps.

IEEE 802.11ac: Lançado em 2013, o 802.11ac é conhecido como Wi-Fi 5. Ele opera exclusivamente na banda de frequência de 5 GHz e oferece velocidades mais rápidas e maior largura de banda do que o 802.11n, com velocidades teóricas de até 3,5 Gbps.

IEEE 802.11ax: Introduzido em 2019, o 802.11ax é conhecido como Wi-Fi 6. Ele oferece melhor desempenho em ambientes densos com muitos dispositivos conectados, além de maior eficiência energética. O 802.11ax opera nas bandas de frequência de 2,4 GHz e/ou 5 GHz, com velocidades teóricas de até 9,6 Gbps.

IEEE 802.11ad: Também conhecido como WiGig, o 802.11ad opera na banda de frequência de 60 GHz e suporta velocidades de até 7 Gbps. Ele é projetado para aplicações de curto alcance e alta largura de banda, como transferência de arquivos de alta definição e realidade virtual.

SEGURANÇA EM REDES SEM FIOS

A segurança em redes sem fio é uma preocupação importante devido à natureza das comunicações sem fio, que podem ser mais facilmente intercetadas por pessoas não autorizadas. Aqui estão algumas práticas e medidas de segurança comuns para proteger redes sem fio:

Criptografia de Dados: Utilize criptografia para proteger os dados transmitidos pela rede sem fio. Os protocolos de criptografia, como WPA2 (Wi-Fi Protected Access 2) ou WPA3, ajudam a proteger a confidencialidade das comunicações, tornando os dados ilegíveis para qualquer pessoa que não possua a chave de criptografia adequada.

Senhas Fortes: Configure senhas fortes e únicas para a rede Wi-Fi e para o acesso ao roteador sem fio. Evite senhas padrão ou previsíveis, como "admin" ou "password". Use uma combinação de letras maiúsculas e minúsculas, números e caracteres especiais para aumentar a segurança da senha.

SSID Oculto: Desabilite a transmissão do SSID (Service Set Identifier) da rede, se possível, para evitar que a rede seja facilmente detetada por dispositivos não autorizados. Isso pode dificultar o acesso não autorizado à rede, embora não seja uma medida de segurança completamente eficaz.

Filtragem de MAC Address: Implemente a filtragem de endereços MAC para permitir apenas dispositivos específicos a se conectarem à rede Wi-Fi. Embora essa medida possa ser contornada com técnicas de spoofing de MAC address, ela ainda oferece uma camada adicional de proteção.

Atualizações de Firmware: Mantenha o firmware do roteador sem fio e dos dispositivos clientes atualizados para garantir que quaisquer vulnerabilidades de segurança conhecidas sejam corrigidas. Verifique regularmente se há atualizações de firmware e aplique-as conforme necessário.

Firewalls: Configure firewalls nos roteadores sem fio e nos dispositivos clientes para filtrar o tráfego de rede e bloquear acessos não autorizados. Os firewalls podem ajudar a proteger a rede contra ameaças externas e internas.

VPN (Virtual Private Network): Use uma VPN para criar uma conexão segura entre dispositivos remotos e a rede corporativa ou doméstica. Isso criptografa o tráfego de dados e protege a privacidade e a segurança das comunicações.

Desativação de Serviços Não Utilizados: Desative serviços e funcionalidades não utilizados nos roteadores sem fio para reduzir a superfície de ataque e melhorar a segurança da rede.

5- EQUIPAMENTOS DE INTERLIGAÇÃO DA REDE

REPETIDORES

Os repetidores são dispositivos usados em redes sem fio para estender o alcance do sinal Wi-Fi, permitindo que dispositivos conectados se comuniquem com o roteador sem fio em distâncias maiores.

Funcionamento: Um repetidor Wi-Fi recebe o sinal sem fio do roteador principal e o retransmite em uma área estendida.

Configuração: A configuração de um repetidor geralmente envolve conectá-lo à rede sem fio existente e posicionar o dispositivo em uma localização onde ele possa receber um sinal forte do roteador principal e ainda ser capaz de transmitir o sinal para as áreas desejadas.

Redução da Velocidade: É importante notar que o uso de repetidores pode resultar em uma redução na velocidade da conexão Wi-Fi, pois os repetidores precisam retransmitir o sinal recebido, o que pode levar a um atraso no tempo de resposta.

Compatibilidade: Nem todos os roteadores e repetidores são compatíveis entre si. Certifique-se de escolher um repetidor que seja compatível com o roteador sem fio existente e que suporte os mesmos padrões e frequências de Wi-Fi.

Pontos de Acesso Sem Fio: Além dos repetidores, os pontos de acesso sem fio (APs) são outra opção para estender o alcance de uma rede sem fio. Os APs são dispositivos semelhantes aos roteadores sem fio, mas são usados para criar novos pontos de acesso à rede, em vez de apenas repetir o sinal existente.

Considerações de Segurança: Ao configurar repetidores ou APs adicionais, é importante garantir que as medidas de segurança, como criptografia de dados, senhas fortes e filtros de endereço MAC, sejam aplicadas para proteger a integridade da rede sem fio estendida.

PONTES (BRIGES)

As pontes, também conhecidas como bridges em inglês, são dispositivos usados em redes de computadores para conectar redes locais (LANs) separadas e permitir a comunicação entre elas.

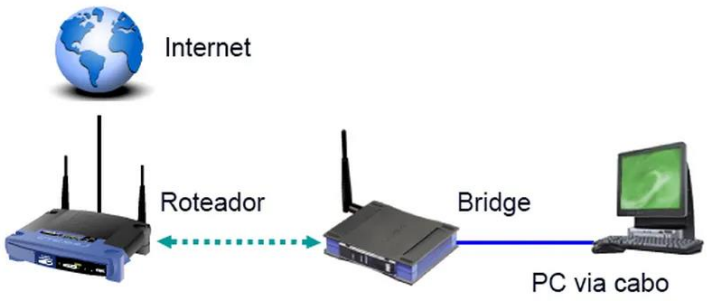
Conexão de Redes: As pontes são usadas para conectar redes locais que usam diferentes protocolos de rede ou que operam em diferentes segmentos de rede

Filtragem de Tráfego: As pontes examinam o tráfego de rede que passa por elas e decidem se o tráfego deve ser encaminhado para outra rede ou não, com base no endereço MAC de destino dos pacotes de dados.

Segmentação de Rede: As pontes também são usadas para segmentar redes maiores em segmentos menores, o que pode melhorar o desempenho e a eficiência da rede, bem como reduzir o tráfego desnecessário.

Pontes Sem Fio: Além das pontes tradicionais, existem também as pontes sem fio, que são usadas para conectar redes locais sem fio (Wi-Fi) entre si. Elas podem ser usadas para estender o alcance de uma rede sem fio ou para conectar redes sem fio separadas.

Configuração e Gerenciamento: As pontes geralmente são configuradas e gerenciadas por meio de interfaces de administração baseadas na web ou por meio de linha de comando, dependendo do modelo e fabricante. Elas podem ser configuradas para definir parâmetros como endereços MAC permitidos, filtros de tráfego e prioridades de rede.



HUBS

Hubs são dispositivos de rede que atuam como concentradores simples de dados, permitindo que vários dispositivos se conectem entre si em uma rede local (LAN).

Concentração de Tráfego: Um hub recebe dados de um dispositivo e os retransmite para todos os outros dispositivos conectados a ele. Ele opera na camada física do modelo OSI e não possui inteligência para tomar decisões com base no endereço de destino dos pacotes de dados.

Operação em Broadcast: Os hubs operam em um modo de transmissão chamado broadcast, o que significa que os dados enviados por um dispositivo são replicados e transmitidos para todos os outros dispositivos na rede, independentemente do endereço de destino.

Dispositivos de Rede Passivos: Os hubs são dispositivos de rede passivos, o que significa que não fazem qualquer processamento ou filtragem dos dados que passam por eles.

Simplicidade e Baixo Custo: Os hubs são dispositivos simples e econômicos em comparação com outros dispositivos de rede, como switches e roteadores. Eles são frequentemente usados em ambientes domésticos ou em pequenas redes onde a simplicidade e o baixo custo são mais importantes do que o desempenho ou a segurança.

Desvantagens: Devido à sua operação em broadcast, os hubs podem causar congestionamentos e colisões de dados em redes com tráfego intenso. Além disso, como os dados são replicados para todos os dispositivos, a segurança das comunicações é comprometida, uma vez que qualquer dispositivo conectado à rede pode potencialmente capturar e visualizar todo o tráfego de dados.

SWITCHES

Os switches são dispositivos de rede essenciais usados para conectar vários dispositivos em uma rede local (LAN) e direcionar o tráfego de dados de forma eficiente

Encaminhamento de Pacotes: Os switches operam na camada de enlace de dados do modelo OSI e usam endereços MAC (Media Access Control) para encaminhar pacotes de dados para os dispositivos corretos na rede.

Encaminhamento Baseado em Endereço MAC: Os switches mantêm tabelas de endereços MAC para cada porta, registrando quais dispositivos estão conectados a cada porta do switch. Com base nessa informação, os switches encaminham os pacotes apenas para as portas necessárias, reduzindo o tráfego desnecessário e melhorando a largura de banda disponível para cada dispositivo.

Desempenho: Os switches oferecem melhor desempenho do que os hubs, uma vez que não replicam os pacotes para todos os dispositivos na rede. Isso resulta em uma comunicação mais rápida e eficiente entre os dispositivos conectados.

Segurança: Como os switches encaminham pacotes apenas para os dispositivos de destino específicos, eles oferecem maior segurança do que os hubs, onde todos os dispositivos podem acessar todos os dados transmitidos na rede.

Gerenciamento: Alguns switches oferecem recursos avançados de gerenciamento, como VLANs (Virtual Local Area Networks), QoS (Quality of Service), controle de tráfego e monitoramento de rede, permitindo uma administração mais eficaz da rede.

Tipos de Switches: Existem switches de diferentes portas, como switches de 8, 16, 24 ou 48 portas, para atender às necessidades específicas de diferentes redes. Além disso, existem switches gerenciáveis e não gerenciáveis, com diferentes níveis de funcionalidades de gerenciamento.

ROUTERS

Os routers são dispositivos de rede essenciais que desempenham um papel fundamental na interconexão de redes locais (LANs) e no roteamento de dados entre diferentes redes.

Encaminhamento de Pacotes: Os routers operam na camada de rede do modelo OSI e são responsáveis por encaminhar pacotes de dados entre diferentes redes. Eles tomam decisões de roteamento com base em endereços IP e na tabela de roteamento, determinando o melhor caminho para os dados viajarem de um dispositivo para outro.

Interconexão de Redes: Os routers são usados para conectar redes locais separadas, como a rede local de uma casa ou escritório à Internet, ou para conectar diferentes redes em uma empresa. Eles atuam como os pontos de entrada e saída para o tráfego de dados entre essas redes.

Encapsulamento e Desencapsulamento: Os routers encapsulam dados em pacotes com cabeçalhos IP e enviam esses pacotes pela rede para o destino correto. Quando os pacotes chegam ao seu destino, os routers desencapsulam os dados, removendo os cabeçalhos IP e entregando os dados aos dispositivos finais.

NAT (Network Address Translation): Muitos routers suportam NAT, que permite que vários dispositivos em uma rede local compartilhem um único endereço IP público. Isso é útil para economizar endereços IP públicos e proteger a rede local de ameaças externas.

Firewall e Segurança: Alguns routers incluem recursos de firewall embutidos para proteger a rede contra ameaças externas, como hackers e malwares. Eles podem filtrar o tráfego de entrada e saída com base em regras de segurança configuráveis pelo usuário.

DHCP (Dynamic Host Configuration Protocol): Muitos routers incluem um servidor DHCP que atribui automaticamente endereços IP e outras configurações de rede aos dispositivos conectados à rede local. Isso simplifica a configuração e gerenciamento de dispositivos na rede.

Redes Sem Fio (Wi-Fi): Muitos routers incluem funcionalidade sem fio e atuam como pontos de acesso Wi-Fi, permitindo que dispositivos sem fio se conectem à rede local

SERVIDORES

Os servidores são computadores ou sistemas dedicados que fornecem serviços, recursos ou funcionalidades específicas para outros dispositivos na rede.

Fornecimento de Serviços: Os servidores são projetados para fornecer serviços específicos para clientes ou outros dispositivos na rede. Isso pode incluir serviços como armazenamento de arquivos, hospedagem de sites, envio de e-mails, compartilhamento de impressoras, autenticação de usuários, banco de dados, entre outros.

Hardware e Software Específicos: Os servidores geralmente são configurados com hardware e software especializados para otimizar o desempenho e a confiabilidade do serviço que estão fornecendo.

Escalabilidade: Os servidores devem ser capazes de escalar para atender às demandas crescentes de usuários e tráfego de rede. Isso pode ser alcançado através de técnicas como a adição de mais recursos de hardware, implementação de clusters de servidores ou escalonamento horizontal.

Segurança: Os servidores devem ser protegidos contra ameaças de segurança, como ataques de hackers, malwares, negação de serviço, entre outros. Isso pode ser feito através da implementação de firewalls, sistemas de deteção de intrusões, atualizações regulares de software, políticas de segurança e práticas de segurança de rede.

Gerenciamento e Monitoramento: Os servidores requerem gerenciamento e monitoramento contínuos para garantir seu desempenho, segurança e disponibilidade.

Virtualização: Muitos servidores modernos utilizam tecnologias de virtualização para maximizar a eficiência e a utilização dos recursos de hardware. Isso permite que um único servidor execute múltiplas máquinas virtuais.

6- GESTÃO E SEGURANÇA DE REDE

DOCUMENTAÇÃO

A documentação de uma rede é um conjunto de informações detalhadas sobre a infraestrutura de rede de uma organização

Diagramas de Rede: Diagramas que representam a topologia física e lógica da rede, incluindo dispositivos de rede, conexões, segmentos de rede, endereços IP, sub-redes e outros componentes.

Inventário de Hardware: Uma lista detalhada de todos os dispositivos de hardware de rede.

Configurações de Dispositivos: Documentação das configurações de cada dispositivo de rede, incluindo endereços IP, máscaras de sub-rede, gateways padrão, configurações de VLAN, configurações de firewall, configurações de QoS e outros parâmetros de configuração.

Políticas de Segurança: Documentação das políticas de segurança da rede, incluindo políticas de senha, políticas de acesso, políticas de firewall, políticas de VPN, políticas de controle de acesso à rede e outras medidas de segurança implementadas na rede.

Procedimentos de Manutenção: Procedimentos e cronogramas para a manutenção regular da rede, incluindo backups de dados, atualizações de firmware, atualizações de software, monitoramento de desempenho, testes de segurança e outras tarefas de manutenção.

Procedimentos de Resolução de Problemas: Procedimentos para diagnosticar e resolver problemas de rede, incluindo procedimentos para identificar e corrigir falhas de conectividade, falhas de desempenho, problemas de segurança, e outros problemas relacionados à rede.

Documentação de Aplicações e Serviços: Informações sobre os aplicativos e serviços que dependem da rede, incluindo descrições dos aplicativos, requisitos de conectividade de rede, dependências de infraestrutura de rede e outras informações relevantes.

Contratos de Serviço e Licenças: Cópias de contratos de serviço, acordos de nível de serviço (SLAs), contratos de manutenção de hardware, contratos de suporte de software e licenças de software para todos os dispositivos e serviços de rede.

SEGURANÇA DA REDE

A segurança de uma rede é uma preocupação crítica para garantir a integridade, confidencialidade e disponibilidade dos dados e recursos de rede

Firewalls: Implementar firewalls de rede para controlar o tráfego de entrada e saída da rede, bloquear acessos não autorizados e proteger contra ameaças externas.

Segurança de Senhas: Utilizar senhas fortes e exclusivas para todos os dispositivos de rede, incluindo roteadores, switches, servidores e dispositivos finais.

Criptografia de Dados: Criptografar dados sensíveis durante a transmissão e armazenamento para protegê-los contra acesso não autorizado.

Atualizações de Segurança: Manter todos os dispositivos de rede e software atualizados com as últimas correções de segurança e patches de software.

Políticas de Acesso: Implementar políticas de acesso que limitem o acesso apenas a usuários autorizados e dispositivos confiáveis

Segmentação de Rede: Dividir a rede em segmentos ou VLANs (Virtual Local Area Networks) para isolar diferentes tipos de tráfego e reduzir a superfície de ataque

Monitoramento de Rede: Implementar ferramentas de monitoramento de rede para detetar atividades suspeitas, anomalias de tráfego e possíveis violações de segurança.

Backup e Recuperação de Dados: Realizar backups regulares de dados críticos e manter cópias de backup em locais seguros e fora do local.

Conscientização e Treinamento de Usuários: Educar os usuários sobre as melhores práticas de segurança cibernética, incluindo a importância de senhas seguras, atualizações de software, deteção de phishing e relatórios de incidentes de segurança. Os usuários são muitas vezes a primeira linha de defesa contra ameaças cibernéticas.

Plano de Resposta a Incidentes: Desenvolver e implementar um plano de resposta a incidentes para lidar com possíveis violações de segurança de forma eficaz e coordenada.

MANUTENÇÃO DA REDE

A manutenção da rede é uma atividade essencial para garantir que a infraestrutura de rede de uma organização funcione de forma eficaz, segura e confiável.

Atualizações de Firmware e Software: Manter todos os dispositivos de rede, incluindo roteadores, switches, firewalls e servidores, atualizados com as últimas versões de firmware e software.

Monitoramento de Desempenho: Utilizar ferramentas de monitoramento de rede para acompanhar o desempenho da rede, incluindo largura de banda, utilização de recursos, latência, pacotes perdidos e outros indicadores-chave de desempenho

Backup Regular de Configurações: Realizar backups regulares das configurações de dispositivos de rede, como roteadores, switches e firewalls

Testes de Redundância e Tolerância a Falhas: Verificar regularmente a funcionalidade de recursos de redundância e tolerância a falhas, como links de backup, protocolos de roteamento redundantes e configurações de cluster

Limpeza e Organização Física: Manter o ambiente físico da rede limpo, organizado e livre de poeira e sujeira

Testes de Segurança e Vulnerabilidade: Realizar testes regulares de segurança e vulnerabilidade na rede para identificar e corrigir potenciais vulnerabilidades de segurança.

Gerenciamento de Inventário: Manter um inventário atualizado de todos os dispositivos de rede, incluindo informações detalhadas sobre cada dispositivo, como número de série, modelo, localização, configuração e status de manutenção.

Treinamento e Desenvolvimento de Pessoal: Investir em treinamento e desenvolvimento contínuos para a equipe de TI responsável pela manutenção da rede.

Avaliação e Melhoria Contínua: Avaliar regularmente a eficácia dos processos de manutenção da rede e identificar áreas de melhoria.

ATAQUES A REDE

Os ataques à rede são uma ameaça significativa à segurança da informação e podem resultar em interrupções do serviço, comprometimento de dados confidenciais e danos à reputação da organização.

Ataques de Negação de Serviço (DDoS): Ataques DDoS visam sobrecarregar os recursos de uma rede, como servidores, roteadores ou firewalls, tornando-os inacessíveis para usuários legítimos.

Ataques de Injeção de Código (SQL Injection, XSS): Esses ataques exploram vulnerabilidades em aplicativos da web para inserir comandos maliciosos ou scripts nos sistemas de banco de dados ou nas páginas da web, permitindo que os atacantes acessem, modifiquem ou excluam dados.

Ataques de Spoofing: Ataques de spoofing envolvem a falsificação do endereço IP de origem de um pacote de dados para mascarar a identidade do atacante ou enganar os sistemas de segurança da rede.

Ataques de Man-in-the-Middle (MitM): Nesses ataques, um invasor intercepta e monitora as comunicações entre dois dispositivos, podendo alterar ou redirecionar o tráfego de dados.

Ataques de Phishing: Os ataques de phishing envolvem o envio de e-mails ou mensagens falsas que parecem ser legítimas, na tentativa de enganar os usuários a fornecer informações confidenciais, como senhas.

Ataques de Ransomware: Ransomware é um tipo de malware que criptografa os dados de um sistema e exige um resgate para restaurar o acesso.

Explorações de Vulnerabilidade: Os atacantes frequentemente exploram vulnerabilidades conhecidas em sistemas operacionais, aplicativos ou dispositivos de rede para ganhar acesso não autorizado.

Ataques de Force Brute: Nesses ataques, os invasores tentam repetidamente adivinhar credenciais de acesso, como nomes de usuário e senhas, até que tenham sucesso.

Ataques de Evasão de Segurança: Esses ataques visam contornar os controles de segurança, como firewalls ou sistemas de detecção de intrusões, para permitir que o tráfego malicioso passe despercebido.

7- REDE PARA DUAS SALAS DE ESCRITÓRIO UMA EM FRENTE A OUTRA

Após toda a pesquisa realizada (encontra-se acima) podemos finalmente montar a nossa rede consoante as nossas necessidades.

Topologia escolhida: topologia em estrela,

Equipamentos necessários:

1 switch com 48 portas para podermos enviar os dados em segurança

1 Cabo de fibra ótica para ligar ao router

1 router para que as salas tenham acesso ao WiFi

1 Repetidor para que o sinal da sala 1 seja acessado sem problemas na sala 2

Cabos rj45 para interligar os computadores ao switch

1 Bastidor para abrigarmos o switch e router

1 impressora para que os funcionários possam imprimir os documentos necessários

10 computadores para cada sala.

CONCUSÃO

Com este trabalho pude relembrar vários conceitos estudados nos anos anteriores, pude também aprender novos conceitos, implementar alguns conceitos que já sabia, perceber um pouco mais da importância da segurança na rede de computadores, pude também enfatizar os componentes da rede e por fim fornecer um guia com vários aprendizados.