Redes

#2 - Padrão GSM: é um padrão internacional para redes de telefonia celular criado na década de 1980. Foi desenvolvido para substituir as tecnologias analógicas (como o 1G) por redes digitais (2G). Permite chamadas de voz e troca de mensagens (SMS) entre celulares. Por ser um padrão global, seu celular GSM funciona em vários países (basta ter um chip compatível).

#3 - Cabo UTP:

É um tipo de cabo de rede composto por pares de fios trançados sem blindagem. É o mais comum em redes locais (LAN) devido ao seu baixo custo e facilidade de instalação. Exemplos: Cat5e, Cat6, Cat6a. Os pares trançados ajudam a reduzir interferências eletromagnéticas.

Diferença entre UTP e FTP:

- **UTP**: Não possui blindagem, mais barato, mais flexível e fácil de instalar.
- **FTP:** Possui uma blindagem de folha metálica envolvendo todos os pares, o que ajuda a reduzir interferências externas. É usado em ambientes com maior interferência eletromagnética.
- **Alicate de Crimpagem:** Ferramenta usada para prender os conectores RJ-45 (ou RJ-11) nas pontas dos cabos de rede. O processo de crimpagem insere os contatos metálicos do conector nos fios do cabo, garantindo conexão elétrica e mecânica. Essencial na montagem de cabos de rede personalizados.

Punch Down Tool:

- Também chamada de ferramenta de impacto, é usada para inserir os fios dos cabos de rede em blocos de conexão (como patch panels ou keystone jacks). Ela pressiona e corta o fio no slot adequado, garantindo boa conexão. Muito usada em cabeamento estruturado.

#4 - **ARPANET (1969)**

Criada pelo Departamento de Defesa dos EUA para conectar centros de pesquisa e garantir troca de informações mesmo sob ataques nucleares.

➞ Foi a primeira rede de computadores comutada por pacotes.
➞ Começou com apenas 4 nós (UCLA, Stanford, UCSB e Utah).
➞ Objetivo inicial: comunicação militar e acadêmica segura.

TCP/IP (1983)

Protocolo de comunicação que substituiu o antigo NCP na ARPANET.

➞ Tornou possível conectar diferentes tipos de redes com um padrão comum.
➞ TCP/IP virou o protocolo oficial da ARPANET em 1º de janeiro de 1983.
➞ Foi o **marco técnico** da criação da internet como conhecemos.

NSFNET (1986)

Rede criada pela National Science Foundation (EUA) para conectar universidades e centros de pesquisa.

➞ Substituiu a ARPANET como principal espinha dorsal da rede.

➞ Abriu caminho para o uso acadêmico e comercial da internet.

➞ Facilitou a expansão para fora dos EUA.

WWW – World Wide Web (1991)

Criada por Tim Berners-Lee no CERN (Suíça).

➞ Trouxe a ideia de sites com links, HTML, navegadores e URL.

➞ Deu à internet uma interface visual e acessível ao público.

➞ Foi a revolução que popularizou o uso da internet.

Internet Moderna (1990s em diante)

Com a combinação de TCP/IP + WWW, a internet cresceu rapidamente:

➞ Chegada da internet ao Brasil (1994–1995).

➞ Criação de provedores, e-mails, redes sociais, streaming etc.

➞ Hoje é uma rede global de bilhões de dispositivos interconectados, usada para tudo: comunicação, trabalho, educação, lazer.

#5 - Terminais burros: No início da computação, os terminais não possuíam capacidade de processamento local, ou seja, não executavam programas por conta própria. Dependiam inteiramente de um mainframe central, e se ele apresentasse falhas ou caísse, todos os terminais conectados paravam de funcionar. Com o avanço tecnológico nos anos 1980, surgiram os microcomputadores, que trouxeram autonomia ao usuário, permitindo o trabalho offline. Isso foi possível graças à popularização dos microchips, que reduziram o custo dos computadores e possibilitaram a criação de máquinas com processador próprio, como o IBM PC e o Apple II. Além disso, esses equipamentos passaram a contar com armazenamento local, inicialmente por meio de disquetes e, posteriormente, com a inclusão de discos rígidos.

A evolução das redes de computadores levou à separação entre dois papéis distintos: clientes e servidores. O cliente é o computador que consome serviços oferecidos pela rede, por exemplo, seu celular acessando vídeos no YouTube. Já o servidor é a máquina responsável por fornecer esses serviços, como os servidores do Google que armazenam e distribuem os vídeos. Esse modelo cliente-servidor é a base das redes modernas e da internet como conhecemos hoje.

 # 6 - **PAN – Personal Area Network (Rede de Área Pessoal)**

- **Alcance:** Muito pequeno (cerca de 1 a 10 metros).
- **Exemplos:** Conexão entre celular e fone Bluetooth, smartwatch, teclado sem fio, etc.
- **Uso:** Comunicação entre dispositivos de uma única pessoa.
- **Tecnologias comuns:** Bluetooth, USB, NFC.

LAN – Local Area Network (Rede de Área Local)

- **Alcance:** Dentro de um prédio, sala ou residência (até alguns quilômetros).
- **Exemplos:** Rede de computadores em uma casa, escola, empresa ou laboratório de informática.
- **Uso:** Compartilhamento de arquivos, impressoras, internet.

- **Tecnologias comuns:** Ethernet, Wi-Fi.

MAN – Metropolitan Area Network (Rede de Área Metropolitana)

- **Alcance:** Abrange uma cidade ou região metropolitana.
- **Exemplos:** Rede interligando filiais de uma empresa em bairros diferentes da mesma cidade.
- **Uso:** Conexão entre LANs de uma área urbana.
- **Tecnologias comuns:** Fibra óptica, rádio digital, enlaces dedicados.

WAN – Wide Area Network (Rede de Longa Distância)

- **Alcance:** Abrange países, continentes ou o mundo inteiro.
- **Exemplos:** A própria **Internet** é uma WAN.
- **Uso:** Conectar várias LANs e MANs em lugares distantes.
- **Tecnologias comuns:** Satélite, links dedicados, redes públicas.

 # 7 - IPv4 tem 2^{32} endereços possíveis, ou seja, aproximadamente 4,3 bilhões.

No começo isso parecia muito, mas com o avanço da internet e dispositivos conectados, acabou não sendo suficiente.

Por isso foi criado o IPv6, com 2^{128} endereços possíveis — algo como 340 decilhões (número absurdamente maior).

Não foi só por quantidade de endereços.

IPv6 também melhora segurança, eficiência, roteamento, e elimina a necessidade de NAT em muitos casos.

Tipos de envio de dados

- **Unicast**: mensagem para um único destinatário.
- **Broadcast**: mensagem para todos os dispositivos da rede.
- **Multicast**: mensagem para um grupo específico (nem todos, nem só um).

8 - **IP Público**

O que é: Único na internet, usado para identificar dispositivos globalmente.

Exemplo: O IP do seu roteador (fornecido pela operadora).

Problema: IPv4 tem apenas ~4 bilhões de combinações (esgotadas).

IP Privado

- **O que é**: Usado dentro de redes locais (LANs), não roteável na internet.

Máscara de Sub-rede

- **O que é?**

Define quantos bits do IP são da rede e quantos são do host.

Sub-redes (Subnetting)

Para que serve? Dividir uma rede grande em redes menores.

Exemplo:

Rede 192.168.1.0/24 pode ser dividida em 4 sub-redes /26:

192.168.1.0/26 (hosts 1-62)

192.168.1.64/26 (hosts 65-126)

 # 9 – Configurando o wi-fi pelo Windows e pesquisando IPs de sites pelo cmd, além de configurar uma nova senha da internet.

Comando	**Função Principal**	**Sistema**
ping	Testa conectividade e latência	Todos
tracert	Mostra o caminho até o destino (hops)	Windows
traceroute	Versão Linux/Mac do tracert	Linux/Mac
ipconfig	Mostra IP, gateway e rede local	Windows
ipconfig /all	Mostra dados detalhados da rede (inclui MAC)	Windows
ifconfig	Versão Linux/Mac do ipconfig	Linux/Mac

 # 10 – Para acessar as configurações do seu roteador TP-Link, abra o Prompt de Comando (CMD) no Windows e digite o comando ipconfig. Em seguida, localize o campo "Gateway Padrão", que corresponde ao endereço IP do seu roteador, geralmente algo como 192.168.0.1 ou 192.168.1.1. Copie esse endereço e cole na barra do seu navegador para acessar a interface de administração. A partir daí, você poderá realizar diversas configurações, como alteração do nome e da senha da rede Wi-Fi, bloqueio ou liberação de dispositivos via endereço MAC, controle de largura de banda, atualização de firmware e outras opções importantes de segurança e desempenho.

 # 11 – As configurações avançadas do Wi-Fi e o posicionamento estratégico do roteador dentro de casa fazem toda a diferença na qualidade do sinal. Redes Wi-Fi de 2.4 GHz, por exemplo, oferecem 13 canais disponíveis no Brasil, mas apenas os canais 1, 6 e 11 são não sobrepostos, ou seja, não sofrem interferência entre si. Utilizar aplicativos como o Xirrus (no PC) ou similares no celular permite analisar as redes vizinhas e escolher o canal menos congestionado, melhorando o desempenho. Outro ponto importante é a largura do canal: canais de 20 MHz oferecem maior estabilidade, enquanto canais de 40 MHz permitem maior velocidade de

transmissão, mas estão mais sujeitos a interferências. Além disso, obstáculos físicos como paredes e eletrodomésticos também afetam o sinal, por isso o roteador deve ser posicionado em um local central e elevado, longe de barreiras e fontes de interferência.

#12 - **Conceitos Fundamentais**

Endereço IP: Composto por 4 octetos (ex: 192.168.1.0).

Máscara de Sub-rede: Define qual parte do IP é rede e qual parte é host.

Exemplo de máscara: 255.255.255.192

Classe de Endereço IP:

Classe A: 0.0.0.0 a 127.255.255.255

Classe B: 128.0.0.0 a 191.255.255.255

Classe C: 192.0.0.0 a 223.255.255.255

Cálculo de Sub-redes

Objetivo: Dividir uma rede grande em redes menores (sub-redes).

Cálculo do salto (incremento entre sub-redes):

256 - 192 = 64 → Cada sub-rede tem 64 endereços IP.

Aplicações práticas

Cada sub-rede pode ser usada para setores distintos:

Recepção

Call center

Secretaria

Coordenação

 # 13 e # 14 – mostrando os detalhes de diferentes cabos e montando eles

 # 15 – montagem de tomadas de superfície de rede

 # 16 - WiFi Inspector, Fing

Permitem ver quais dispositivos estão conectados ao roteador, incluindo:

- Nome do dispositivo
- Endereço MAC (único para cada aparelho)
- Fabricante

- Úteis para detectar se vizinhos ou intrusos estão usando seu Wi-Fi.

Endereço MAC

- MAC (Media Access Control): identificador único e físico da placa de rede.
- Exemplo: celular da mãe, notebook, TV – cada um tem um MAC.
- Pode ser usado para permitir ou bloquear acesso no roteador.

Controle de acesso por MAC no roteador

- O roteador geralmente tem:
- Lista de dispositivos permitidos (Whitelist)
- Lista de dispositivos bloqueados (Blacklist)

Exemplo prático demonstrado:

Identificaram um MAC estranho (vizinho) usando a rede.

- Copiaram o MAC e adicionaram à lista de bloqueio no painel do roteador.
- O aparelho do vizinho perdeu o acesso à internet.

Dicas e cuidados com o controle por MAC

- Muita atenção ao configurar: se errar e bloquear o dispositivo errado (como seu próprio notebook), pode ficar sem acesso.
- Caso trave o acesso: reinicie o roteador para restaurar as configurações de fábrica.
- MAC pode ser alterado (clonado) por alguém mais experiente, então esse método não é infalível.

Estratégia de segurança sugerida

- Desabilitar temporariamente a senha do Wi-Fi.
- Conectar apenas os dispositivos autorizados.
- Ativar o controle por MAC com lista de permitidos.
- Reativar a senha, se quiser, e ocultar o nome da rede (SSID) para aumentar a segurança.
- Opcional: deixar a rede visível, mas restrita apenas aos MACs autorizados.

 # 17 - O que é o Cisco Packet Tracer?

- Simulador de redes desenvolvido pela Cisco para ensino e treinamento em infraestrutura de redes.
- **Principais recursos**:
    - Permite criar topologias de rede virtuais (roteadores, switches, PCs, servidores).
    - Simula protocolos de rede (TCP/IP, DHCP, DNS, OSPF, VLANs, etc.).

Para que serve?

- **Aprendizado de redes**: Ideal para entender conceitos como:

    - Sub-nets e configuração de IPs.
    - Roteamento estático e dinâmico (RIP, OSPF, EIGRP).
    - VLANs, STP, ACLs, NAT, DHCP.
- **Preparação para certificações**:
    - CCNA (Cisco Certified Network Associate).
    - CCNP (nível avançado).
- **Testes sem hardware físico**:
    - Simula falhas, tráfego e troubleshooting sem risco.

 # 18 - **Como usar apps como Fing ou WiFi Inspector para:**

- Identificar dispositivos conectados ao roteador.
- Verificar os endereços MAC (identificadores únicos das placas de rede).
- Bloquear ou permitir o acesso desses dispositivos

Controle de Acesso no Roteador

- Como bloquear dispositivos desconhecidos pelo MAC.
- Como configurar o roteador para permitir apenas dispositivos autorizados.
- Explica que há dois modos: "lista de permitidos" ou "lista de bloqueados".

Criou uma página básica em html para mostrar que a conexão http deu certo com o servidor.

 # 19 - O **WDS** é uma tecnologia que permite interligar pontos de acesso (APs) sem fio para estender uma rede Wi-Fi sem a necessidade de cabos. É útil para cobrir grandes áreas (ex: escritórios, casas grandes) ou conectar prédios próximos.

Conexões Físicas e Reinício

- **Cabo de rede principal:** Vem do modem principal da operadora e é conectado à porta azul (WAN) do primeiro roteador.
- **Portas LAN (1–4):** Usadas para conectar o roteador ao PC ou ao segundo roteador.
- **Reset do roteador:** Pressiona-se o botão de reset com objeto pontiagudo por ~10 segundos até todas as luzes acenderem/apagarem, retornando às configurações de fábrica.

Acesso ao Painel do Roteador

- Acessa-se o painel via navegador usando o IP padrão (ex: 192.168.0.1 ou 192.168.1.1).
- Criação de senha de acesso e configuração inicial do Wi-Fi: nome da rede (SSID) e senha simples para teste.
- Teste de velocidade para verificar se há internet funcionando no primeiro roteador.

Preparando o Segundo Roteador como Repetidor (WDS)

- Conecta-se um cabo LAN do primeiro roteador para uma porta LAN do segundo.
- Reset do segundo roteador.
- Acesso ao IP do segundo roteador (ex: 192.168.0.1 ou 192.168.1.254) e troca do IP para um diferente, mas na mesma faixa (ex: se o principal é 192.168.0.1, o segundo pode ser 192.168.0.254).
- Desabilita o DHCP do segundo roteador, pois quem vai distribuir IPs será o primeiro.
- Coloca IP fixo temporário no PC (ex: 192.168.0.222) para não perder o acesso após desativar o DHCP.

Ativando o Modo WDS

- Acessa a configuração Wi-Fi > WDS Bridging (nome pode variar).
- O roteador escaneia as redes Wi-Fi próximas.
- Escolhe-se a rede criada no primeiro roteador.
- Digita-se a senha da rede principal.
- Confirma-se que os parâmetros são compatíveis (canal, segurança, etc).

Testes Finais

- Após salvar configurações:
    - Retorna-se o IP do PC para automático (DHCP).
    - Conecta-se à rede Wi-Fi normalmente.
    - Verifica-se se há navegação e internet funcionando também pelo segundo roteador.

 # 20 - A **câmera do estúdio** está gerando um campo eletromagnético muito forte. Esse campo está bloqueando ou degradando o sinal Wi-Fi entre o roteador principal e o repetidor WDS. Isso faz com que o roteador repetidor não consiga se comunicar com o principal, mesmo com a configuração correta.

 # 21 - **Objetivo do Repetidor**

- Capturar o sinal do roteador principal e retransmiti-lo, estendendo a cobertura.
- Deve copiar a mesma configuração do roteador (nome da rede e senha) — isso garante que os dispositivos se conectem automaticamente ao ponto com sinal mais forte.

Acesso à Interface Web

- O acesso ao repetidor é feito via navegador com um IP padrão (exemplo: 192.168.0.254).
- Esse IP não faz parte da rede principal ainda — é só um IP de configuração temporário.

Análise do Sinal com o Wi-Fi Analyzer

- Utilizam o app Wi-Fi Analyzer para verificar:

- O sinal fraco da rede original lá de baixo (em vermelho).
- A nova rede gerada pelo repetidor (em marrom), que ainda está sem conexão à internet.