Internet e Protocolos

Sumário

Aula 1- Rede de computadores- definição 3
Tipos de Redes de computadores. 4
Aula 2 -Protocolo IP versão 4 6
Aula 3 -Binário 10
Aula 4-DNS 11
Aula 5- DHCP. 15
Aula 6- Modelo OSI 18
Aula 7- Protocolo TCP 21
Protocolo UDP 23
Aula 8- Servidor 24
Tipos de servidores 25
Aula 9- Domínio 26
Aula 10- Unidade Organizacional 28
Aula 11- Grupos em domínio. 29
Aula 12- Dispositivos de rede. 30
Aula 13- Rede Wireless. 33
Protocolos de Criptografia 36
Utilizando Roteador como repetidor 38
Aula 14- Roteamento 39
Aula 15- Topologia de rede 41
Meios de transmissão. 45
Aula 16- Cabeamento Estruturado 46

Aula 1- Rede de computadores- definição.

Uma rede de computadores consiste de dois ou mais computadores e outros dispositivos conectados entre si de modo a compartilharem seus recursos (dados, impressoras, mensagens,emails) etc.

Estrutura de uma rede de computadores.

Estrutura Fisica= cabos, modem, placa de rede, switch, roteador, servidor, impressora.

Estrutura Lógica= Protocolo IP,TCP, DNS, DHCP,HTTP,POP3,IMAIP.

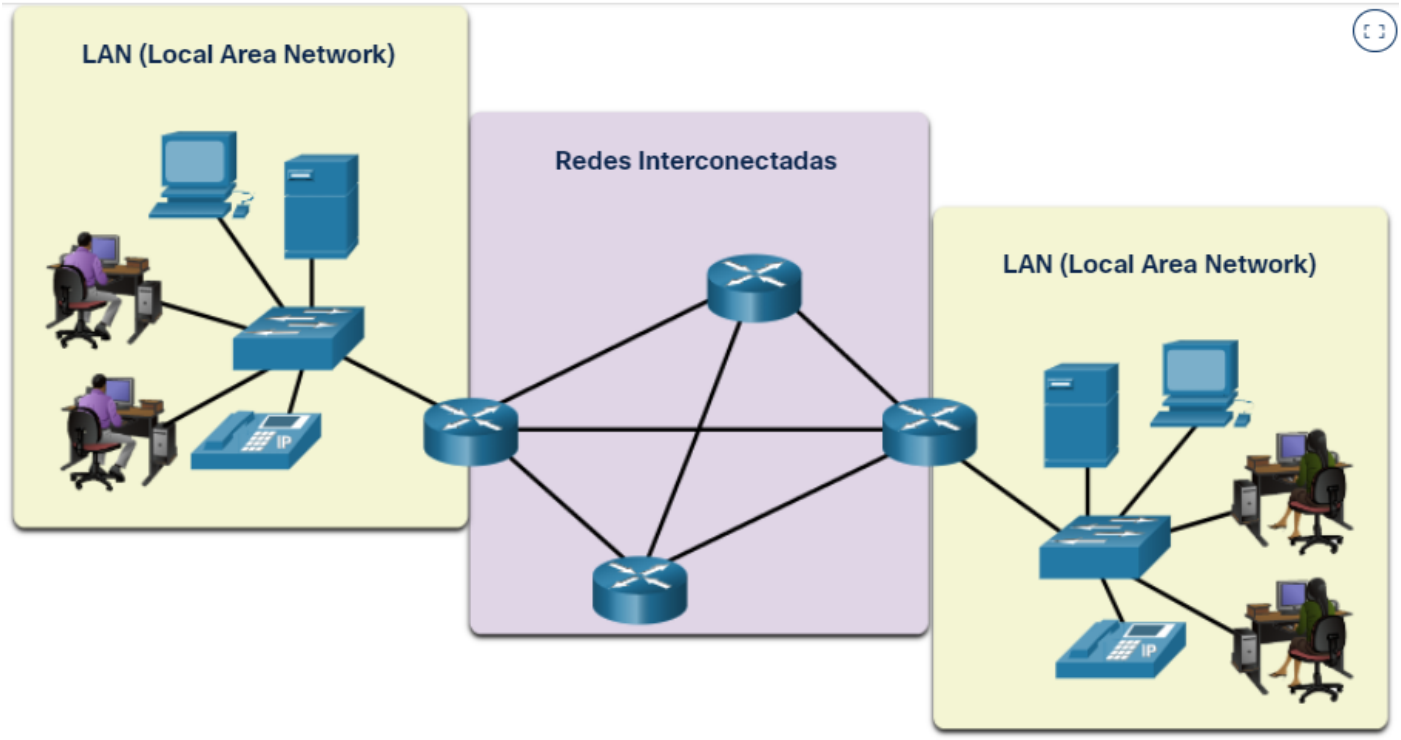
Internet

Rede de computadores interligados: servidores, host, sistemas finais executando aplicações distribuídas, sobre Enlaces de comunicação que pode ser Fibra cobre, rádio, satélite.

Tipos de Redes de computadores.

LAN local área network- As chamadas Local Área Networks, ou Redes Locais, interligam computadores presentes dentro de um mesmo espaço físico. Isso pode acontecer dentro de uma empresa, de uma escola ou dentro da sua própria casa, sendo possível a troca de informações e recursos entre os dispositivos participantes.

WAN- Wide área network- Rede de longa distância é uma rede de computadores que abrange uma grande área geográfica, como um país ou continente. Interconexão de várias redes através de fibras e sistemas distribuídos.



Redes de Computadores ponto-a-ponto

São redes de computadores pequenas usadas em grupos sem a utilização de um servidor onde computadores compartilham entre dados e arquivos entre si, Baixo custo, fácil implementação e Baixa segurança.

É uma arquitetura de sistemas distribuídos caracterizada pela descentralização das funções de rede, em que cada nodo realiza tanto funções de servidor quanto cliente.

Redes de Computadores Cliente/Servidor

São usadas em redes de computadores com mais de 10 micros e com a utilização de um servidor que tem a função de compartilhar de arquivos, recursos e gerenciamento com segurança.

Nesta arquitetura, um ponto central pode enviar informações para vários pontos, utilizando um mesmo meio e fazendo derivações ao longo do meio. Esse tipo de ligação pode existir numa arquitetura de redes conectadas a grandes distancias entre si, chamadas de redes wan(wide área network).

Aula 2 -Protocolo IP versão 4

IP Sigla para "Internet Protocol ou Protocolo de Internet", a norma, protocolo que define o processo de endereçamento e transmissão de dados pela Internet.

Endereço IP, é um número de 32 bits formado por quatro octetos e representado na forma decimal. Cada octeto tem 8 bits.

A primeira parte do endereço identifica uma rede específica, a segunda parte identifica um host dentro dessa rede.

Exemplo
128. 6. 4. 7.
Rede host

Tipos de endereços IPs

Endereço IP estático (ou fixo) é um endereço IP atribuído manualmente e não se altera por si só. O administrador que atribui um IP manualmente ao computador.

Endereço IP dinâmico, (ou automático) por sua vez, são endereços IPs atribuídos automaticamente através de um servidor DHCP disponível na rede. O computador atribui um Ip automaticamente através de solicitação na rede de um servidor DHCP.

APIPA (Automatic Private IP addressing)

É um recurso que configura endereços IP automaticamente. O APIPA elimina erros associados com a falta de endereços IP. Por padrão um computador primeiro tenta contatar um servidor DHCP na rede para obter automaticamente um endereço IP.

Classes de IP- IANA (Internet Assigned Numbers Authority) divide a utilização de IPs para redes em, basicamente, 3 classes principais e duas que podem ser consideradas secundárias.

Classe A: 0.0.0.0 até 127.0.0.0 Permite até 16.777.214 de computadores em cada rede. (Máximo de 126 redes);

Classe B: 128.0.0.0 até 191.255.0.0 Permite até 65.534 computadores em uma rede.
(Máximo de 16.384 redes);

Classe C: 192.0.0.0 até 223.255.255.254 permite até 254 computadores em uma rede.
(Máximo de 2.097.152 redes);

Classe D: 224.0.0.0 até 239.255.255.255 – *multicast*

Classe E: 240.0.0.0 até 255.255.255.255 *multicast* reservado

Máscara

A máscara funciona como uma extensão do IP, como se complementasse o IP para a identificação de sub-redes. Ela define qual parte do endereço IP é Correspondente a sub-rede ou relativa a identificação dos hosts.

As máscaras de sub-rede distinguem a identificação de host da identificação de rede em um endereço IP

Quando se usam classes para endereços IP, todas as classes de endereço tem uma mascara de sub-rede padrao. Quando se divide uma rede em segmentos, ou sub-redes, pode se usar a mascara de sub-rede padrao para que a classe divida o endereço Ip de rede.

Uma máscara de rede representada em binario são 4 octetos de bits (11111111.11111111.11111111.11111111).

8bit x 4 octetos = 32 bit. (11111111.11111111.11111111.11111111 = 255.255.255.255)

8bit x 3 octetos = 24 bit. (11111111.11111111.11111111.00000000 = 255.255.255.0)

8bit x 2 octetos = 16 bit. (11111111.11111111.00000000.00000000 = 255.255.0.0)

8bit x 1 octetos = 8 bit. (11111111.00000000.00000000.00000000 = 255.0.0.0)

No exemplo 10.0.0.0/8, segundo o explicado anteriormente, indicaria que a máscara de rede é 255.0.0.0

Broadcasting- um endereço broadcast é um endereço IP (e o seu endereço é sempre o último possível na rede ou sub-rede) que permite que a informação seja enviada para todas as maquinas de uma LAN, MAN, WAN .

Multicast é um método ou técnica de transmissão de um pacote de dados para múltiplos destinos ao mesmo tempo

Endereço MAC

Endereço MAC (do inglês **Media Access Control**) é o endereço físico de 48 bits do computador, ou, mais especificamente, da interface de rede(placa de rede). O protocolo é responsável pelo controle de acesso de cada estação à rede Ethernet.

Representa-se um endereço MAC escrevendo, exactamente, 12 dígitos hexadecimais agrupados dois a dois – os grupos são separados por dois pontos. Exemplo:

00:00:5E: 00:01:03

Os três primeiros **octetos** são destinados à identificação do fabricante,

Os tres posteriores são fornecidos pelo fabricante. É um endereço único, e, não existem, em todo o mundo, duas placas com o mesmo endereço.

No Linux o comando é ifconfig.

No Windows o comando ipconfig.

ARP (Address Resolution Protocol ou ARP)

É um protocolo usado para encontrar um endereço da camada de enlace (Ethernet, por exemplo) a partir do endereço da camada de rede (como um endereço IP).

O ARP realiza resolução de um endereço IP em um endereço MAC nos pacotes de dados de saída. O Pacote inclui os endereços IP de origem e de destino.

No momento em que cada pacote de saída é encapsulado em um quadro, inclui-se o endereço MAC de origem e de destino.

Aula 3 -Binário

O sistema binário ou de base 2 é um sistema de numeração posicional em que todas as quantidades se representam com base em dois números, ou seja, **zero** e **um** (0 e 1).[1]
Os computadores digitais trabalham internamente com dois níveis de tensão, pelo que o seu sistema de numeração natural é o sistema binário (aceso, apagado)

Visualizamos e utilizamos o endereço IP com números **decimais**, mas para entender o conceito vamos relembrar os **binários** e fazer a conversão de decimal para binário e vice versa. Cada parte do número IP é definido por um **octeto**, que é um conjunto de 8 bits.

Da mesma maneira que o sistema decimal utiliza a base 10, o hexadecimal utiliza base 16, o binário utiliza a base 2, então podemos visualizar da seguinte forma:

Vamos utilizar o primeiro octeto de um endereço de classe C como exemplo para explicar a conversão de decimal para binário:

Decimal para Binário

Ex: 192

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	**64**	**32**	**16**	**8**	**4**	**2**	**1**
1	**1**	**0**	**0**	**0**	**0**	**0**	**0.**

128 + 64 = 192 11000000= 192

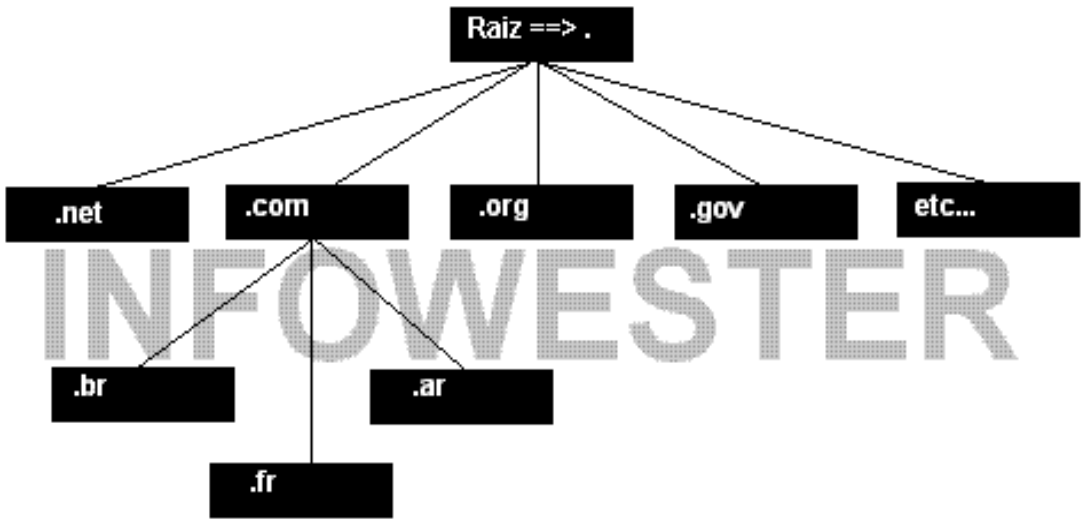
Aula 4-DNS

DNS é a sigla para **D**omain **N**ame **S**ystem (Sistema de Domínio de Nomes). Trata-se de um recurso usado em redes TCP/IP (o protocolo utilizado na internet e na grande maioria das redes) que permite acessar computadores sem que o usuário ou sem que o próprio computador tenha conhecimento de seu endereço IP.

Cada site da internet é acessível por um endereço IP. O problema é que existe tantos que é praticamente impossível decorar o IP de cada um. Imagine que ao invés de digitar *www.uol.com.br*para acessar este site, você tivesse que informar ao navegador o endereço *200.178.123.25*.

Para lidar com esse problema é que o DNS é usado. É ele que permite o uso de nomes (também chamados de domínios) ao invés dos IPs no acesso aos sites. Basicamente, na internet, o DNS é um conjunto de grandes bancos de dados distribuídos em servidores de todo o mundo que indicam qual IP é associado a um nome (ou seja, um endereço do tipo *www.nomedosite.com*).

Quando você digita um endereço em seu navegador, seu computador solicita aos servidores de DNS de seu provedor de internet que encontre o endereço IP associado a *www.uol.com.br* Se os servidores não tiverem essa informação, ele se comunica com outros que possam ter.



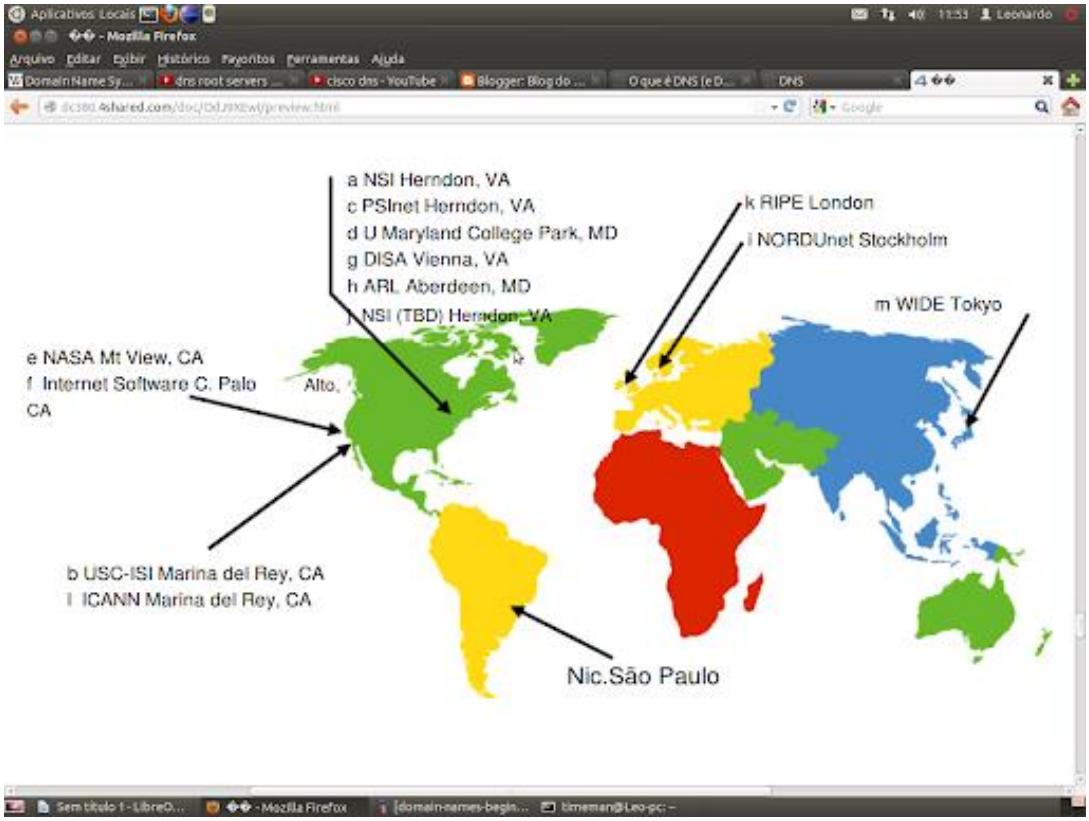
Note que dentro de cada domínio (.com, .net, .gov) existem outras subdivisões. Por exemplo, dentro de .com há .com.br, .com.fr, .com.ar, etc.

O DNS é administrado por uma Autoridade de Inscrição de Nome na Internet. Esta entidade é responsável por manter domínios de nível de topo que são nomeados através de organizações e por fim, por países.

O sistema de distribuição de nomes de domínio foi introduzido em 1984 e com ele os nomes de hosts residentes em um banco de dados puderam ser distribuídos entre servidores múltiplos, baixando assim a carga em qualquer servidor que provê administração no sistema de nomeação de domínios.

Em virtude do banco de dados de DNS ser distribuído, seu tamanho é ilimitado e o desempenho não degrada tanto quando se adiciona mais servidores nele.

Existem 13 servidores DNS raiz no mundo todo e sem eles a Internet não funcionaria. Destes, dez estão localizados nos Estados Unidos da América, um na Ásia e dois na Europa.



Para aumentar a base instalada destes servidores, foram criadas Réplicas localizadas por todo o mundo, inclusive no Brasil desde 2003.

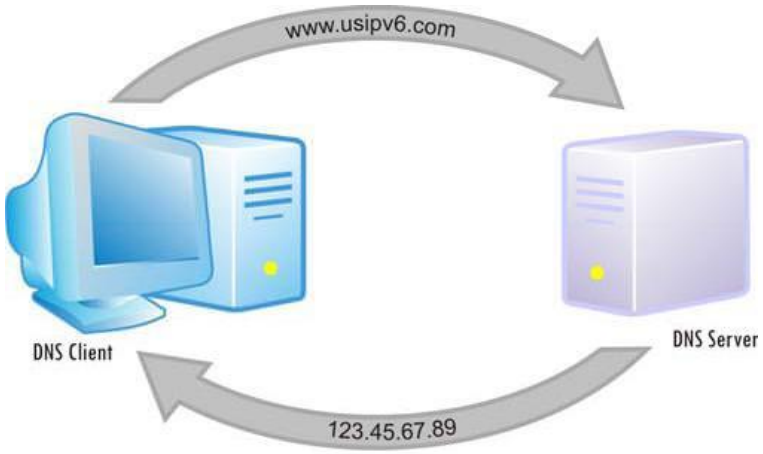
Há dois tipos de zonas que podem ser criadas no DNS:

Zona primária DNS- para a qual são feitas todas as atualizações para os registros pertencentes àquela zona (relacionando nome da máquina em Ip e vice-versa).

Zona secundária DNS - que é representada por uma cópia de somente leitura da zona primária.

Uma **zona** é uma parte do banco de dados DNS que contém os registros de recursos que pertencem à parte contígua do espaço dhs.

https://who.is/whois/etecjardimangela.com.br



Registros DNS

A – O A, também conhecido por hostname, é o registro central de um DNS, ele vincula um domínio ou subdomínio a um endereço IP direto. Os registros de DNS do tipo A são a razão final da existência do sistema de resolução de nomes, e o tipo de registros que dá nome ao serviço. Este é, hoje, um dos dois tipos de registros que se destinam a fazer o que o nome diz… resolver nomes.

AAAA – A internet cresceu de tal forma que o número de IPs inicialmente disponíveis está praticamente esgotado e já não permite acompanhar o crescimento da rede. Hoje existem computadores numa grande percentagem de casas, e cada vez mais existe um computador na mão (ou no bolso) de casa pessoa (os Smartfones). Para ultrapassar este problema foi criado um conjunto de endereços, designados com o nome IPv6. Sendo assim, registros AAAA executam a mesma função de A, porém, para um endereço IPv6.

NS – Name Server (Servidor de Domínio), especifica servidores DNS para o domínio ou subdomínio. Pelo menos, dois registros NS devem ser definidos para cada domínio. Geralmente, um principal e outro secundário.

CNAME – Significa Canonical NAME. Especifica um apelido (alias) para o hostname (A). É uma forma de redirecionamento.

Comando

Ipconfig /flushdns- limpar cache dns.

Ipconfig /displaydns- exibe todas as entradas DNS em cache.

Nslookup- identifica servidor dns.

Iponfig /release- excluir endereço ip.

Ipconfig /renew- renovar endereço ip.

Aula 5- DHCP.

Dynamics Host Configuration Protocol (ou Protocolo de configuração dinâmica de Host) é um protocolo de serviço TCP/IP que oferece configuração dinâmica de computadores, com concessão de endereços IP de host e outros parâmetros de configuração (IP, mascara, DNS, Gateway) para clientes de rede.

Funcionamento

Um cliente envia um pacote UDP em *broadcast* (destinado a todas as máquinas) com um pedido DHCP. O Servidor DHCP captura o pacote UDP e responde com as configuraçoes onde constará um endereço IP, uma mascara de rede e outros dados opcionais como gateway e DNS.

O servidor DHCP renova os endereços Ips e mascaras após certo periodo. A concessão do IP e mascara expira em 7 dias, sendo renovado pelo servidor DHCP após este periodo de tempo.

O DHCP usa modelo cliente-servidor, no qual o servidor DHCP mantém o gerenciamento centralizado dos endereços IP usados na rede.

Escopo DHCP

Um escopo é uma faixa de endereços IP. A faixa deve estar dentro da faixa de endereços da rede onde o servidor DHCP será utilizado. Por exemplo, se você utilizará o servidor DHCP na seguinte rede: 10.10.20.0/255.255.255.0, você poderá criar escopos como os exemplificados a seguir:

10.10.10.20 a 10.10.10.100 Escopo 1
192.168.10.1 a 192.168.10.130 Escopo 2
192.168.10.131 a 192.168.10.200 Escopo 3

Cada sub-rede pode ter somente um único escopo DHCP com um único intervalo contínuo de endereços IP, definido em um servidor DHCP.

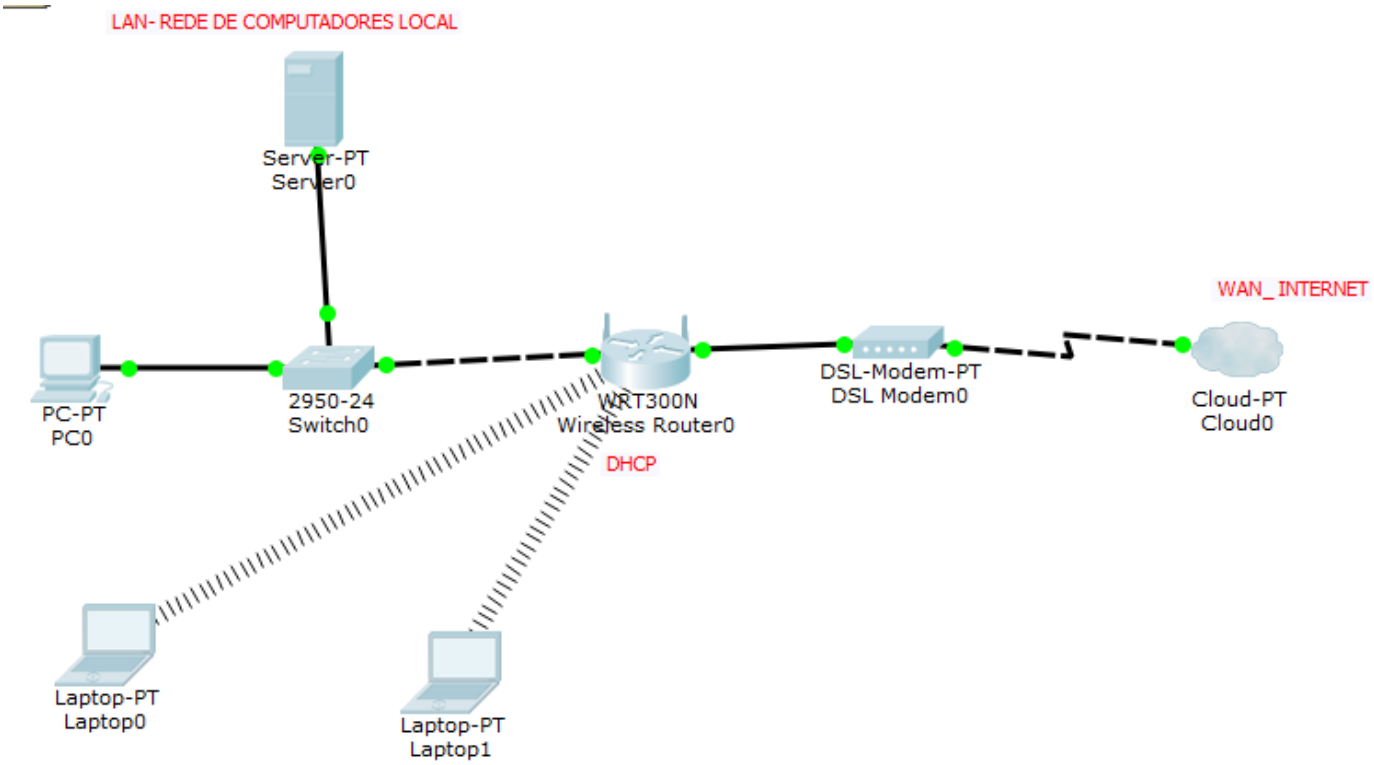
Intervalos de exclusão

Você pode definir intervalos de exclusão para retirar de um escopo, endereços que você não quer que sejam concedidos pelo servidor DHCP para os clientes da rede. Por exemplo, você pode excluir os 10 primeiros endereços no escopo 10.10.20.30 a 10.10.20.100, criando uma exclusão de 10.10.20.30 a 10.10.20.40.

Vantagens

Não precisa configurar manualmente cada cliente com um endereço IP.
Reduz a possibilidade de duplicação de endereços IP.

EXEMPLO DHCP COM ROTEADOR



Aula 6- Modelo OSI

O Modelo OSI foi apresentado pela internationals standards organization ou organizaçao Internacional de Padrões com o intuito de padronizar os protocolos de comunicaçoes em camadas.

Sua arquitetura é chamada OSI (*Open Systems Interconnection*), Camadas OSI ou Interconexão de Sistemas Abertos. Esta arquitetura é um modelo que divide as redes de computadores em sete camadas, de forma a se obter camadas de abstração

O modelo de referencia OSI é arquitetura modelo que divide as redes de computadores em sete camadas, de forma a se obter uma padronizaçao de comunicaçao entre computadores.

O modelo divide os protocolos em sete camadas:

Aplicaçao, Apresentaçao, sessao, transporte, rede,enlace e fisica.

7 - Camada de Aplicação

A camada de aplicação é responsável por identificar e estabelecer a aplicação (programa) o qual será utilizado entre a máquina destinatária e o usuário como também disponibiliza os recursos (protocolo) para que tal comunicação aconteça.

6 - Camada de Apresentação

A camada de Apresentação, também chamada camada de Tradução, converte o formato do dado recebido pela camada de Aplicação em um formato comum a ser usado na transmissão desse dado, ou seja, um formato entendido pelo protocolo usado. Um exemplo comum é a conversão do padrão de caracteres (código de página) quando o dispositivo transmissor usa um padrão diferente do ASCII.

5 - Camada de Sessão

A camada de Sessão permite que duas aplicações em computadores diferentes estabeleçam uma sessão de comunicação. Nesta sessão, essas aplicações definem como será feita a transmissão de dados e coloca marcações nos dados que estão a ser transmitidos.

4 - Camada de Transporte

A camada de transporte é responsável por pegar os dados enviados pela camada de Sessão e dividi-los em pacotes que serão transmitidos para a camada de Rede.

Orientado a conexão.

Não-Orientado a conexão

3 - Camada de Rede

A camada de Rede é responsável pelo endereçamento dos pacotes, convertendo endereços lógicos (IP) em endereços físicos (MAC) , de forma que os pacotes consigam chegar corretamente ao destino. Essa camada também determina a rota que os pacotes irão seguir para atingir o destino, baseada em fatores como condições de tráfego da rede e prioridades.

Funções da Camada:

Movimenta pacotes a partir de sua fonte original até seu destino através de um ou mais enlaces.

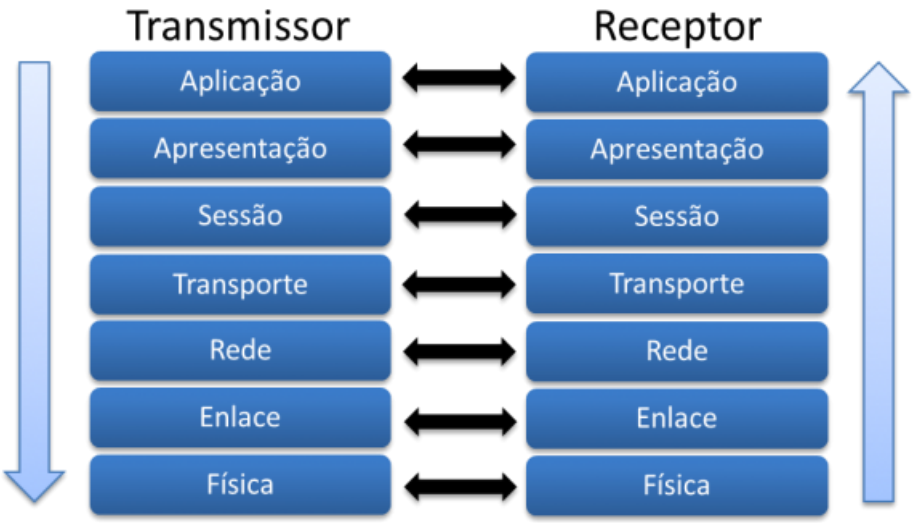
Define como dispositivos de rede descobrem uns aos outros e como os pacotes são roteados até seu destino final.

2 - Camada de Enlace

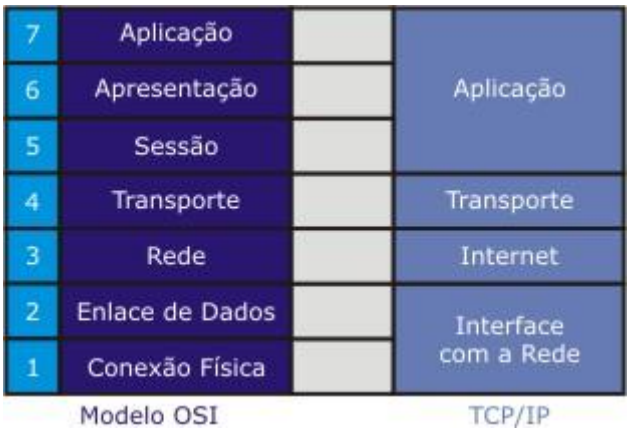
A camada de ligação de dados também é conhecida como camada de enlace ou *link* de dados. Esta camada detecta e, opcionalmente, corrige erros que possam acontecer no nível físico. É responsável pela transmissão e recepção (delimitação) de quadros e pelo controle de fluxo. Ela também estabelece um protocolo de comunicação entre sistemas diretamente conectados

1 - Camada Física

A camada física define as características técnicas dos dispositivos elétricos e ópticos (físicos) do sistema. Ela contém os equipamentos de cabeamento ou outros canais de comunicação (ver modulação) que se comunicam diretamente com o controlador da interface de rede.



A arquitetura do TCP/IP pode ser vista na Figura 1.



Aula 7- Protocolo TCP

TCP" Transmission Control Protocol" ou protocolo de controle de transmissão é o protocolo que define o processo de transmissão de pacotes (packet) de informações em redes de telecomunicações, garantindo que eles sejam recebidos na mesma ordem em que foram emitidos.

TCP é um do protocolodo nível da camada de transporte (camada 4) do Modelo OSI e é sobre o qual assentam a maioria das aplicações cibernéticas, como o SSH, FTP, HTTP — portanto, a *World Wide Web*.

O Protocolo TCP verifica se os dados são enviados de forma correta, na sequência apropriada e sem erros, pela rede.

As características fundamentais do TCP são:

Orientado à conexão - A aplicação envia um pedido de conexão para o destino e usa a "conexão" para transferir dados.

Ponto a ponto - uma conexão TCP é estabelecida entre dois pontos.

Confiabilidade **-** O TCP usa várias técnicas para proporcionar uma entrega confiável dos pacotes de dados, que é a grande vantagem que tem em relação ao UDP, e motivo do seu uso extensivo nas redes de computadores. O TCP permite a recuperação de pacotes perdidos, a eliminação de pacotes duplicados, a recuperação de dados corrompidos, e pode recuperar a ligação em caso de problemas no sistema e na rede.

Full duplex **-** É possível a transferência simultânea em ambas direções (cliente-servidor) durante toda a sessão.

Handshake - Mecanismo de estabelecimento e finalização de conexão a três e quatro tempos, respectivamente, o que permite a autenticação e encerramento de uma sessão completa. O TCP garante que, no final da conexão, todos os pacotes foram bem recebidos.

Entrega ordenada - A aplicação faz a entrega ao TCP de blocos de dados com um tamanho arbitrário num fluxo (ou *stream*) de dados, tipicamente em octetos. O TCP parte estes dados em segmentos de tamanho especificado pelo valor MTU. Porém, a circulação dos pacotes ao longo da rede (utilizando um protocolo de encaminhamento, na camada inferior, como o IP) pode fazer com que os pacotes não cheguem ordenados. O TCP garante a reconstrução do *stream* no destinatário mediante os *números de sequência*.

Controle de fluxo **-** O TCP usa o campo janela ou *window* para controlar o fluxo. O receptor, à medida que recebe os dados, envia mensagens ACK (=Acknowledgement), confirmando a recepção de um segmento; como funcionalidade extra, estas mensagens podem especificar o tamanho máximo do *buffer* no campo (janela) do segmento TCP, determinando a quantidade máxima de bytes aceita pelo receptor.

Protocolo UDP

O User Datagram Protocol (UDP) é um protocolo simples da camada de transporte nãoconfiável. É um protocolo que permite a comunicação entre computadores diferentes, sem conexão que não garante de a chegada dos pacotes em ordem particular.

Ele permite que a aplicação escreva um datagrama encapsulado num pacote IPv4 ou IPv6, e então enviado ao destino. Mas não há qualquer tipo de garantia que o pacote irá chegar ou não.

O protocolo UDP não é confiável. Caso garantias sejam necessárias, é preciso implementar uma série de estruturas de controle, tais como timeouts, retransmissões, acknowlegments, controle de fluxo, etc.

Também dizemos que o UDP é um serviço sem conexão, pois não há necessidade de manter um **relacionamento longo entre cliente e o servidor.**

Protocolos que utilizam o UDP

TFTP- Este protocolo é semelhante ao FTP, porém sem confirmação de recebimento pelo destino ou reenvio. É comumente usado por administradores de rede ao se fazer o *download* do IOS (*InternetworkOperational System*) de um roteador ou do arquivo de inicialização.

SNMP- É utilizado para configurar dispositivos como *switches* ou roteadores e permite que estes enviem o seu *status*.

DHCP- É utilizado em redes que sofrem constantes alterações na topologia e o administrador não pode verificar o IP (*Internet Protocol*) de cada máquina devido a enorme quantidade, então o roteador distribui IPs automaticamente para as estações. Como esta atribuição é feita com a utilização do UDP, caso haja algum problema o usuário terá que pedir o reenvio ou reiniciar a máquina.

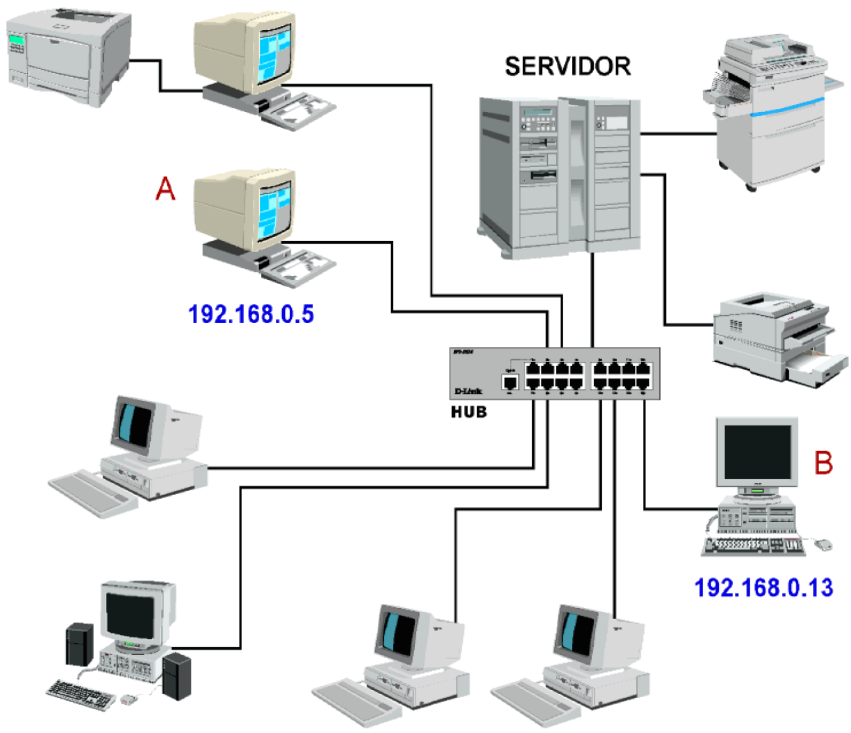
.

DNS-Um tradutor dos nomes na rede, na qual cada IP pode ser correspondido com um nome.

Aula 8- Servidor

Computador com alto desempenho em hardware (memória, processador, HD) e um sistema operacional especifico para rede que fornece serviços a uma rede de computadores.

Servidor dedicado- é servidor dedicado a um unico serviço(servidor web ou servidor DHCP).
Esses serviços podem ser de natureza diversa, como por exemplo, arquivos, DNS, DHCP e correio eletrônico.Os computadores que acessam os serviços de um servidor são chamados clientes.



Tipos de servidores

Servidor de arquivos: Servidor que armazena arquivos de diversos usuários.

Servidor web: Servidor responsável pelo armazenamento de páginas de um determinado site, requisitados pelos clientes através de *browsers*.

Servidor de e-mail: Servidor responsável pelo armazenamento, envio e recebimento de mensagens de correio eletrônico.

Servidor de impressão: Servidor responsável por controlar pedidos de impressão de arquivos dos diversos clientes.

Servidor DNS: Servidores responsáveis pela conversão de endereços de sites em endereços IP e vice-versa.

Servidor domínio: é a unidade central da estrutura lógica no Active Directory. Um domínio é uma coleção de entidades de segurança (como contas de usuários e de computadores) e outros objetos(como impressoras e pastas compartilhadas.

Servidor FTP: Permite acesso de outros usuários a um disco rígido ou servidor. Esse tipo de servidor armazena arquivos para dar acesso a eles pela internet.

Compartilhamento é a atividade de tornar arquivos ou recursos disponíveis para outros usuários através de *download* pela Internet ou também em redes .
Compartilhamento de Drive.

O compartilhamento de unidade de disco é util em varias situaçoes. Por exemplo , se um computador estiver com unidade de CD ou disquete defeituosa, podera usar a de outro computador, atraves da rede.Este tipo de compartilhamento não da o direito de gravaçao de CDs.

Aula 9- Domínio

Domínio é a unidade central, uma estrutura lógica contendo coleção de entidades de segurança (como contas de usuários e de computadores e outros objetos como impressoras e pastas compartilhadas) cujo acesso a rede é gerenciado por um computador central(servidor) chamando controlador de dominio.

AD Active Directory é um conjunto de arquivos localizados no servidor de domínio, no qual estão todas as informações que permitem controlar o acesso dos usuários à rede. Nele ficam registrados os nomes e senhas de usuários, suas permissões de acesso a arquivos, impressoras e outros recursos da rede, as cotas de disco, os computadores .

Vantagens

Logon único: com esse recurso, o usuário necessita fazer apenas um logon para acessar os recursos em diversos servidores da rede, inclusive e-mail e banco de dados.

Conta de usuário única: As contas de usuários ficam armazenadas no banco de dados do AD.

Gerenciamento centralizado: com os domínios baseados no AD, temos uma administração centralizada. Todas as informações sobre contas de usuários, grupos e recursos da rede, podem ser administradas a partir de um único local no domínio.

Escalabilidade: os domínios podem crescer a qualquer momento, sem limite de tamanho. A forma de administração é a mesma para uma rede pequena ou grande.

Floresta é um ou mais domínios que compartilham uma configuração, um esquema e um catálogo global comuns.

Tabajara.com- pai- SP, Tabajara2.com- filho- MG

Arvore consiste em domínios de uma floresta que compartilham um namespace DNS contiguo e tem duas relações de confiança transitivas e bidirecionais entre domínios pai e filho.

Controlador de Domínio (DC – Domain Controller) : é o computador que possui o AD instalado, ou seja, é um servidor que possui uma cópia da base de dados do AD.

Aula 10- Unidade Organizacional

Unidade Organizacional é um tipo de objeto contêiner que você usa para organizar objetos em um domínio. Ela pode conter objetos como contas de usuários, grupos, computadores, impressoras e outras entidades organizacionais.

Objetivos

Organizar objetos em domínio , como grupos de usuários, contas de usuários e contas de computadores.

Delegar controle administrativo.

Você pode atribuir controle administrativo completo (permissão controle total) sobre todos os objetos na unidade organizacional

Simplificar o gerenciamento de recursos geralmente agrupados.

Você pode usar as configurações da diretiva de grupo para gerenciar a definição das configurações de computador e de usuário**.**

Aula 11- Grupos em domínio.

Os grupos são uma coleção de contas de usuários e de computadores que podem ser gerenciadas com uma única unidade.

Objetivos

Simplificam a administração, permitindo que você conceda permissões a uma única vez a um grupo para os recursos.

Podem estar localizados no active directory ou localmente em um computador individual. São caracterizados pelo escopo ou pelo tipo.

Tipos de grupos

Grupos globais

É um grupo de segurança que pode conter usuários, grupos e computadores que fazem parte do mesmo domínio do grupo global.

Grupos universais

É um grupo de segurança que pode conter usuários, grupos e computadores que fazem parte de qualquer domínio de sua floresta.

Grupos de domínio locais.

É um grupo de domínio local que pode conter outros grupos de domínio locais.

Aula 12- Dispositivos de rede.

Placa de rede. Uma placa de rede é um dispositivo de hardware responsável pela comunicação de um computador em uma rede de computadores. A placa de rede controla o envio e recebimento de dados de um computador conectado a uma rede, através de ondas eletromagnéticas, cabos metálicos ou cabos de fibra óptica.

Fast Ethernet- Uma rede compatível com Fast Ethernet (**também chamada de 10/100**) transfere dados em taxas de até 100 Mb/s e é suportado por qualquer dispositivo de rede disponível no mercado, já que é o mais antigo dos padrões.

Gigabit Ethernet- Criado em 1999, o padrão Gigabit (**também conhecido como 10/100/1000**) ainda é o mais recente dos tipos de rede. Ele promete velocidades de até **1 Gb/s** – daí o nome –, 10 vezes maiores que o Fast Ethernet.

Switch - É um dispositivo utilizado em redes de computadores para interligar vários computadores e reencaminhar Pacotes (informação) em diversos segmentos da rede.
O switch encaminha os dados diretamente ao seu destinatário, ao contrário dos hubs´s que enviam os dados à todas as portas (Broadcast).

HUB ou Concentrador é a parte central de conexão de uma rede. Dispositivo utilizado em redes de computadores para interligar vários computadores em muito usado no começo das redes de computadores ele é o dispositivo ativo que concentra a ligação entre diversos computadores que estão em uma Rede de área local ou LAN.

A diferença entre o hub e o switch é que estes tomam decisões com base no endereço MAC e os hubs não tomam nenhuma decisão. Devido isso os switches tornam as LAN´s muito mais eficientes

(**Roteador (router),** é um equipamento usado conectar as sub-redes ou fazer a comunicação entre diferentes redes de computadores.

Os roteadores utilizam tabelas de rotas para decidir sobre o encaminhamento de cada pacote de Dados recebido.

Características

• Operam na camada e 3 do modelo ISO/OSI (REDE)

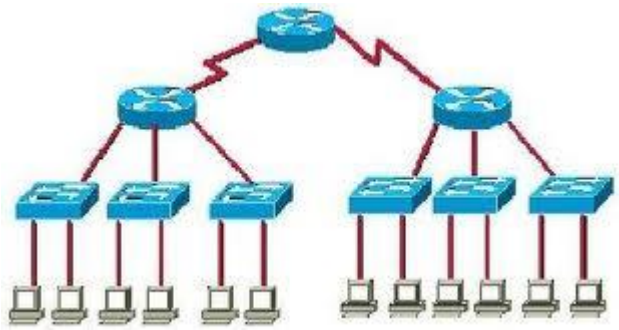
• Seleciona a rota mais apropriada para encaminhar os pacotes recebidos

• Utilizam os protocolos de roteamento RIP, OSPF, IGRP, BGP, EGP

• Interligam redes geograficamente distantes

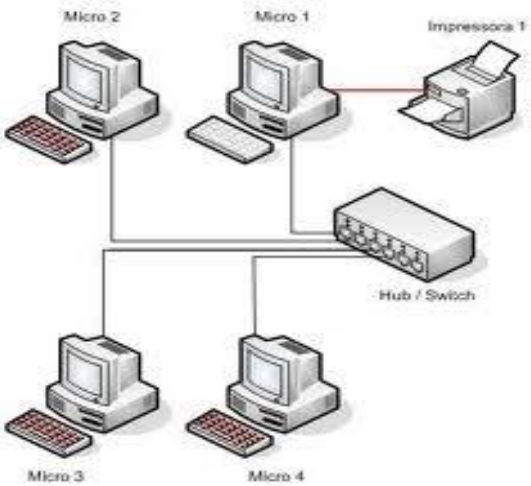
• Geralmente é definido como GATEWAY PADRÃO da rede.

Sub-redes é um segmento físico de uma rede, separado do resto da rede por um ou mais roteadores. Uma rede composta por várias sub-redes conectadas por roteadores é geralmente chamada de conexão entre redes.



Impressora local é aquela que está fisicamente conectada ao seu computador e que pode ser compartilhada na rede ou não.

Impressora de rede é aquele que está fisicamente conectada a outro computador da rede (servidor) e você imprime nela por meio da rede.



Aula 13- Rede Wireless.

As redes sem fio também conhecidas como **IEEE 802.11**, Wi-Fi ou WLANs, são redes de computadores sem fios, que utilizam sinais de rádio (ondas eletromagnéticas) para a sua comunicação com roteador ou internet.
Este tipo de rede define duas formas de comunicação:

- ✓ **Modo infraestrutura:** normalmente o mais encontrado, utiliza um concentrador de acesso (Access Point ou AP).

- ✓ **Modo ponto a ponto (ad-hoc):** permite que um pequeno grupo de máquinas se comunique diretamente, sem a necessidade de um AP.

Estas redes ganharam grande popularidade pela mobilidade que proveem aos seus usuários e pela facilidade de instalação e uso em ambientes domésticos e empresariais, hotéis, conferências, aeroportos etc.

WLAN (Wireless Local Área Network) é uma rede local que usa ondas de rádio (ondas eletromagnéticas) para fazer uma conexão com a Internet ou entre uma rede através de um roteador wireless.

Através da utilização de portadoras de rádio ou infravermelho, as WLANs estabelecem a comunicação de dados entre os pontos da rede.

IEEE-Instituto de Engenheiros Eletricistas e Eletrônicos ou IEEE é uma organização profissional de engenheiros eletrônicos sem fins lucrativos, fundada nos Estados Unidos que define os protocolos padrões utlizados nas comunicaçao de rede sem fio.

Padrões de comunicações wireless IEEE 802.11

IEEE 802.11 A
Taxas de transmissão (envio e recebimento) de **54 MBPS.**
Alcance menor do que a 802.11b e **opera em 5GHZ**
Alcance de até 60 e 100 metros.

IEEE 802.11 b
Taxas de transmissão (envio e recebimento) de **11 MBPS.**
Largamente utilizada hoje em dia e **opera em 2.4GHz.**
Alcance de até 100 e 300 metros

IEEE 802.11g

Taxas de transmissão de (envio e recebimento) **54 Mbps** podendo chegar a alguns casos a **108 Mbps.**

Operando em 2.4GHz.

Alcance de até 100 e 300 metros.

IEEE 802.11 N

Taxas de transmissão de **65 Mbps a 600 Mbps**. –

Método de transmissão: MIMO-OFDM - Faixa de freqüência: **2,4 GHz e/ou 5 GHz.**

IEEE 802.11 AC –

Taxas de transmissão (envio e recebimento) de **1.2 Gigas**.

Este padrão foi desenvolvido entre 2011 e 2013, com previsão de lançamento somente para o início de 2014.

O Padrão Trabalha com multi estações de transferência sem-fio de na escala de 1,2 Gbit/s em link único de transferência, graças ao conceito de extensão de interface, já implementado no modelo 802.11n

Padrões de Redes Wireless

Padrão	Taxa máxima de transmissão	Frequência	Compatibilidades
802.11a	54 Mbps	5 GHz	Não
802.11b	11 Mbps	2.4 GHz	Não
802.11g	54 Mbps	2.4 GHz	802.11b
802.11n	600 Mbps	2.4 GHz ou 5 GHz	802.11b/g
802.11ac	1.3 Gbps	2.4 GHz e 5.5 GHz	802.11b/g/n
802.11ad	7 Gbps	2.4 GHz, 5 GHz e 60 GHz	802.11b/g/n/ac

Fonte:www.cisco.com

Protocolos de Criptografia

Criptografia (Do Grego *kryptós*, "escondido", e *gráphein*, "escrita") É o estudo dos princípios e técnicas pelas quais a informação pode ser transformada da sua forma original para outra ilegível, de forma que possa ser conhecida apenas por seu destinatário (detentor da "chave secreta"), o que a torna difícil de ser lida por alguém não autorizado.

WEP (*Wired Equivalent Privacy*) primeiro protocolo de segurança tendo como objetivo dar segurança às **redes sem fio** por meio de um processo de autenticação, mas com o passar do tempo o protocolo ficou desatualizado e foram descoberto várias vulnerabilidades no protocolo WEP onde hoje ele e facilmente quebrando em pouco tempo, apesar do protocolo ainda ser um dos mais usados hoje em dia e padrão dos modens mais antigos.

WEP2 ou **WPA** (*Wi-Fi Protected Access*) foi lançado em 2003 e apenas um grande upgrade no WEP tendo como objetivo melhorar a segurança das redes sem fio, WPA utiliza o algoritmo RC4 o mesmo sistema de encriptação utilizado no WEB , o **TKIP** (*Temporal Key Integrity Protocol*).

WPA2 utiliza a criptografia **AES** (*Advanced Encryption Standard*) mais segura que a TKIP, mas exige mais processamento e algumas placas mais antigas não suportam o WPA2 nem mesmo atualizado a firmware.

WPA-PSK de maneira simples WPA-PSK é uma criptografia forte em que as chaves de criptografia (TKIP) e frequentemente mudada o que garante mais segurança protegendo de ataque hack, muito utilizado por usuários domésticos.

WPA2-PSK e ainda mais seguro de que o WPA-PSK onde sua criptografia (AES) e extremamente forte e resistência a ataques, adotado como padrão de criptografia do governo americano.

PROTOCOLO PPOE ou POINT-TO-POINT PROTOCOL – Vivo /SPEED

È um protocolo para conexão de usuários em uma rede Ethernet a internet. Seu uso é típico nas conexões de um ou múltiplos usuários em uma LAN a internet através de uma linha DSL.

PROTOCOLO DYNAMIC IP. CLARONET /LIVE TIM

È um IP automático que fará a conexão com a internet e fornecido pela empresa provedora de acesso a internet.


Wireless Router
TL-WA850RE
Alcance Wireless do Roteador
Alcance Wireless Estendido
Funciona como um Adaptador de Rede Wireless

Utilizando Roteador como repetidor

Primeiro Roteador ligado com o modem

Segundo roteador Ligado no primeiro na porta LAN

Obs. Porta Lan com Porta Lan

Aula 14- Roteamento

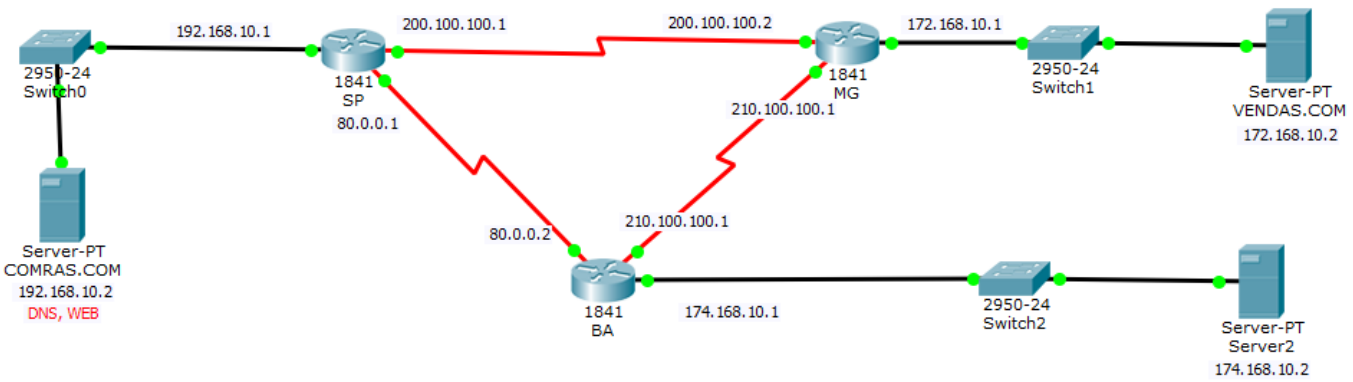
É o mecanismo que permite a comunicação entre dois dispositivos que estejam em redes diferentes. O dispositivo responsável para realização do roteamento é conhecido como Roteador. Mas outros dispositivos conectados a duas ou mais redes também poderão atuar no papel de roteador

Roteamento estático.

O roteamento estático normalmente é configurado quando uma tabela de roteamento estático é construída manualmente pelo administrador do sistema, uma rede com um número limitado de roteadores para outras redes poderem ser configuradas com roteamento estático, e pode ou não ser divulgada para outros dispositivos de roteamento na rede.

Tabelas estáticas não se ajustam automaticamente à alterações na rede, portanto devem ser utilizadas somente onde as rotas não sofrerem alterações.

Algumas vantagens do roteamento estático são melhor controle e segurança obtida pela divulgação somente das rotas necessárias e também a redução do broadcast, multicast ou unicast flooding introduzidos na rede pela troca de mensagens dos protocolos de roteamento dinâmicos como OSPF, IS-IS, RIP e EIGRP.



Roteamento dinâmico

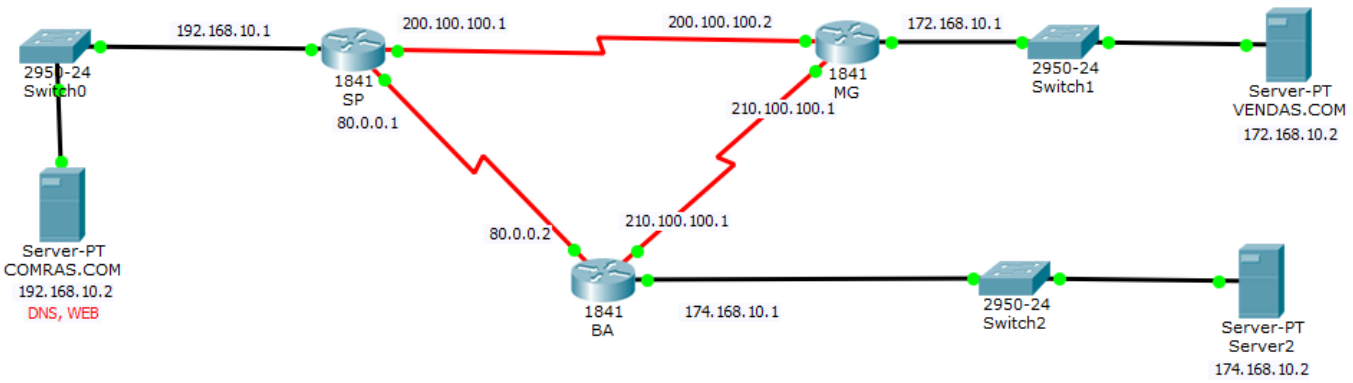
O **RIP** (Routing Information Protocol) é um padrão para troca de informações entre os *gateways* e *hosts* de roteamento. Atualmente existem muitos protocolos de roteamento utilizados para toda a rede.

O RIP emite mensagens de atualização das suas rotas (Tabelas de Roteamento) em intervalos regulares (a cada 30 segundos) e quando a topologia da rede mudar.

Quando um roteador recebe uma atualização do roteamento que inclua mudanças a uma entrada, atualiza sua tabela de roteamento para refletir a rota nova. O valor métrico (salto) para o trajeto é aumentado por 1 e o remetente é indicado como o hop seguinte.

Protocolos de roteamento podem resolver situações complexas de roteamento mais rápida e eficientemente que o administrador do sistema eles são desenvolvidos para trocar para uma rota alternativa quando a rota primária se torna inoperável e para decidir qual é a rota preferida para um destino.

Em redes onde existem várias alternativas de rotas para um destino onde devem ser utilizados.



Aula 15- Topologia de rede

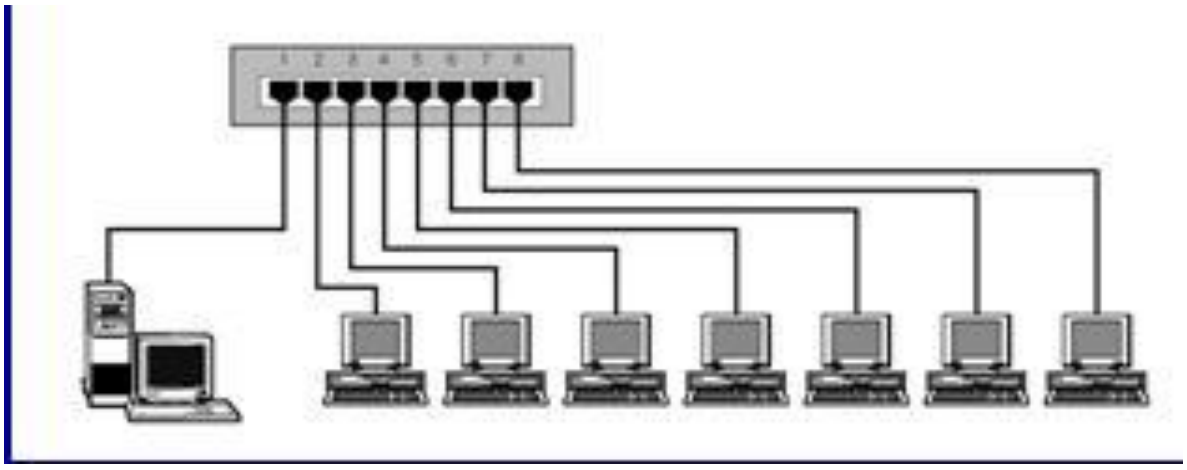
A topologia de rede descreve como é o layout de uma rede de computadores através da qual há o tráfego de informações, e também como os dispositivos fisicos estão conectados a ela.

Topologia de rede Barramento

Esta topologia é a arquitetura de redes ethernet ligadas por cabos coaxiais, em que as estações (computadores) de rede vão sendo conectados ao longo do cabo.

O sinal elétrico que transporta a informação é difundido ao longo de todo o cabo para todas as estações nas duas direções, ou seja, bidirecional.
Uma das vantagens dessa forma de conexão é o baixo custo e a rapidez com que se consegue ligar novos nos ao barramento.

A desvantagem é que se o cabo partir em algum ponto, toda a rede para de funcionar.
O comprimento do cabo e o número máximo de estações em uma rede são determinados, pela atenuação do sinal.
Atenuação (definida como a diminuição da intensidade de um sinal ao propagar-se através de um meio de transmissão).
O fluxo de dados é bidirecional.
Conexão multiponto compartilhando o meio de transmissão.

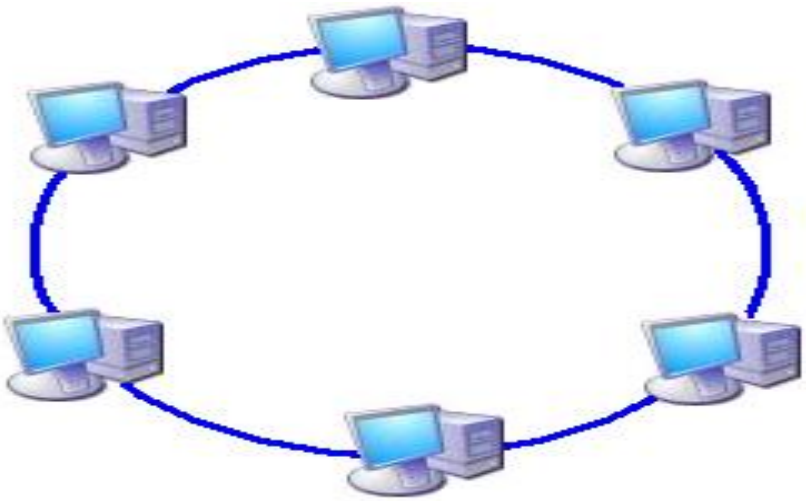


Topologia de Rede Anel

Nesta arquitetura, os dados circulam num cabo que conecta todas as estaçoes num formato circular.
os dados passam por todos os nos da rede, até encontrar o no com o endereço destino dos dados.
o fluxo dos dados ao longo do anel é unidirecional, ou seja, ele é transmitido e caminha
em apenas um sentido.
Numa arquitetura em anel, para alcançar seu destino, os dados devem obrigatoriamente passar pelos nos intermediarios.

A mensagem circula pelo anel até ser retirada pelo nó destino ou retornar ao nó fonte.

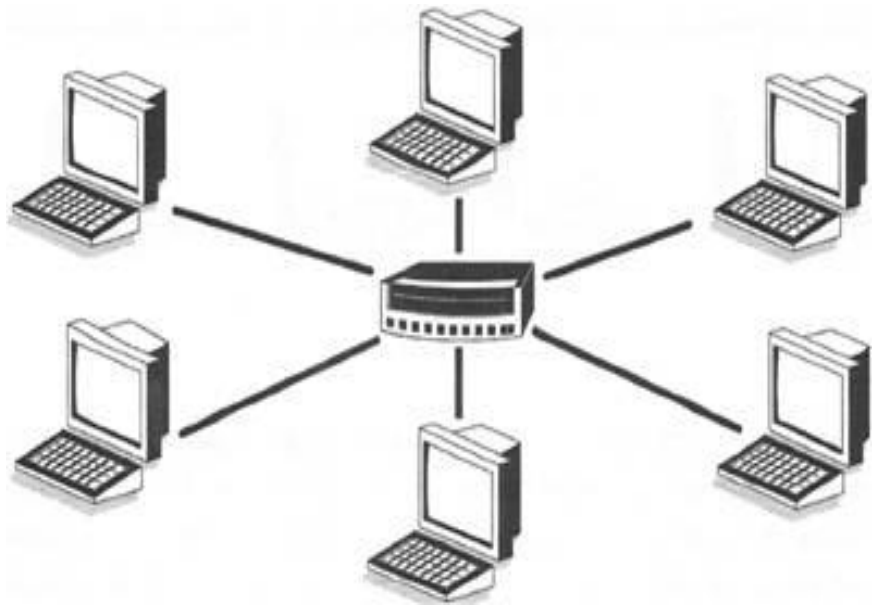
Vantagens Desempenho uniforme, menos cabo.
Desvantagens. Se uma estação para, todas param. Difíceis de isolar problemas na rede.



Topologia de rede Estrela

A mais comum atualmente, a topologia em estrela utiliza cabos de par trançado e um concentrador como ponto central da rede. O concentrador se encarrega de retransmitir todos os dados para todas
as estações, mas com a vantagem de tornar mais fácil a localização dos problemas, já que , se um dos cabos, uma das portas do concentrador ou uma das placas de rede estiver com problemas, apenas o no ligado ao componente defeituoso fica fora da rede

Todas as mensagens passam pelo nó central.
Cada estação possui um canal de comunicação.
Nó central geralmente é um switch.



Desvantagens
Falhas no nó central paralisam todo o sistema.
Baixa modularidade (limite imposto pelo nó central).
Desempenho depende do nó central.
Exige grande quantidade de cabos

Topologia de Redes híbrida

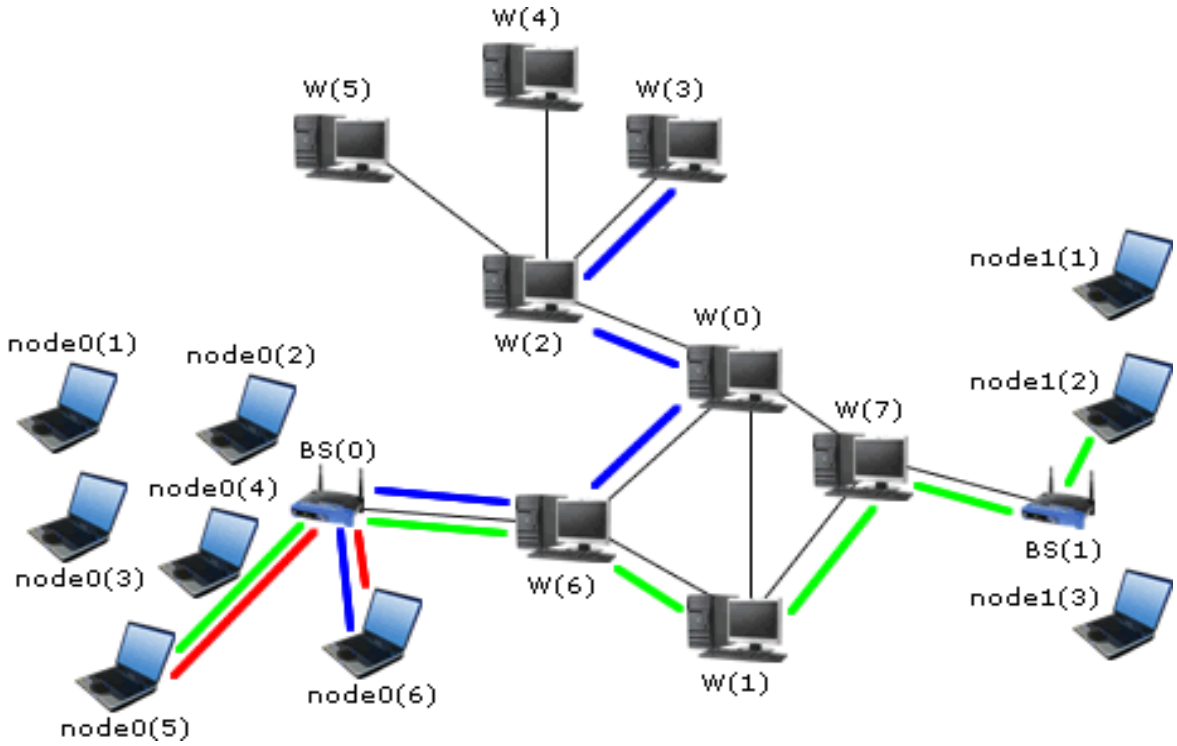
É uma Combinação de uma ou mais topologia de rede.

Usam a Combinação de técnicas de conexão ponto-a-ponto.

Vantagens

Reaproveitamento da infraestrutura existente ou expansão com uso de novas tecnologias.

Interconexão de várias sub-redes de comunicação.



Meios de transmissão.

Existem basicamente três meios utilizados na transmissão de dados;

1-transmissão por fios ou cabos de cobre, na qual os dados sao transmitidos por sinais elétricos que se propagam no metal.
exemplo: cabo coaxial ou par trançado.

2-transmissão por fibra óptica, na qual os dados são transmitidos por sinais luminosos que se propagam pelo vidro ou plástico que forma a fibra óptica.
exemplo: cabo de fibra óptica.

3-transmissão por irradiação eletromagnética em que os dados são transmitidos por sinais elétricos irradiados por antenas através do espaço.
exemplos: ondas de rádio, infravermelho e laser.

4- Cabos de par trançados são os mais usados, pois tem um melhor custo-benefício.
O nome "par trançado" é muito conveniente, pois estes cabos são constituídos justamente pro 4 pares de cabos entrelaçados.
Existem dois tipos de cabo par trançado:
UTP- unshielded twisted pair - cabos sem blindagem ;
STP- shielded twisted pair - cabos blindados com uma manta de aluminio
As taxas usadas nas redes com o cabo par trançado são:
10 Mbps (Ethernet);
100 Mbps (FastEthernet)ou
1000 Mbps (Gigabit Ethernet).
10000 Mbps ou 10Gbps (10Gigabit Ethernet).

Aula 16- Cabeamento Estruturado

É a forma organizada e padronizada de conectores, Cabos e meios de transmissão para redes de informática e telefonia, de modo a tornar a infraestrutura de cabos independentemente do tipo de aplicação e do layout.

ABNT - Associação Brasileira de Normas Técnicas se baseia nas normas ANSI/EIA/TIA.

http://www.abnt.org.br/default.asp

Fundada em 1940, a **Associação Brasileira de Normas Técnicas (ABNT)** é o órgão responsável pela normalização técnica no país, fornecendo a base necessária ao desenvolvimento tecnológico brasileiro.

É uma entidade privada, sem fins lucrativos, reconhecida como único Foro Nacional de Normalização através da Resolução n.º 07 do CONMETRO, de 24.08.1992.

É membro fundador da ISO (International Organization for Standardization), da COPANT (Comissão Panamericana de Normas Técnicas) e da AMN (Associação Mercosul de Normalização).

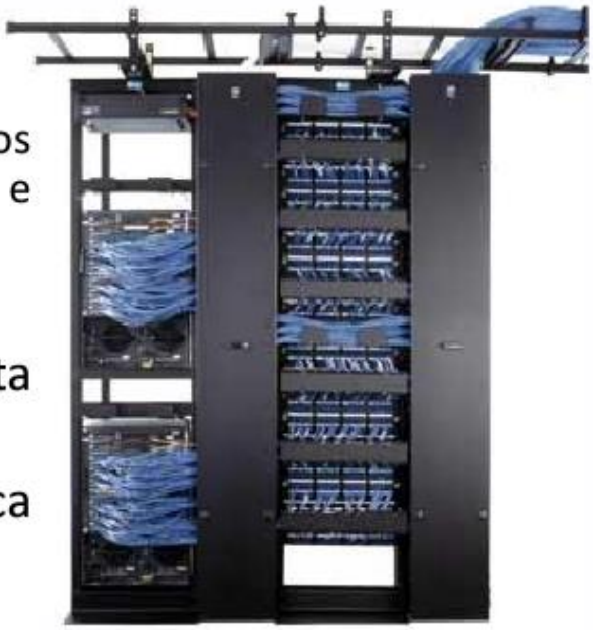
A ABNT é a representante oficial no Brasil das seguintes entidades internacionais: ISO (InternationalOrganization for Standardization), IEC (InternationalEletrotechnicalComission).

Sala de equipamentos

Local onde são abrigados os principais equipamentos ativos de rede, como PABX, servidores, switches, hubs, roteadores etc.

Sala de Equipamentos

- Abrigam:
  - MCs e ICs (patch panels).
  - Demais equipamentos (servidores, roteadores e switches, por exemplo).
- Possui acesso restrito.
- Raramente experimenta mudanças estruturais.
- Em um prédio, fica normalmente no térreo.

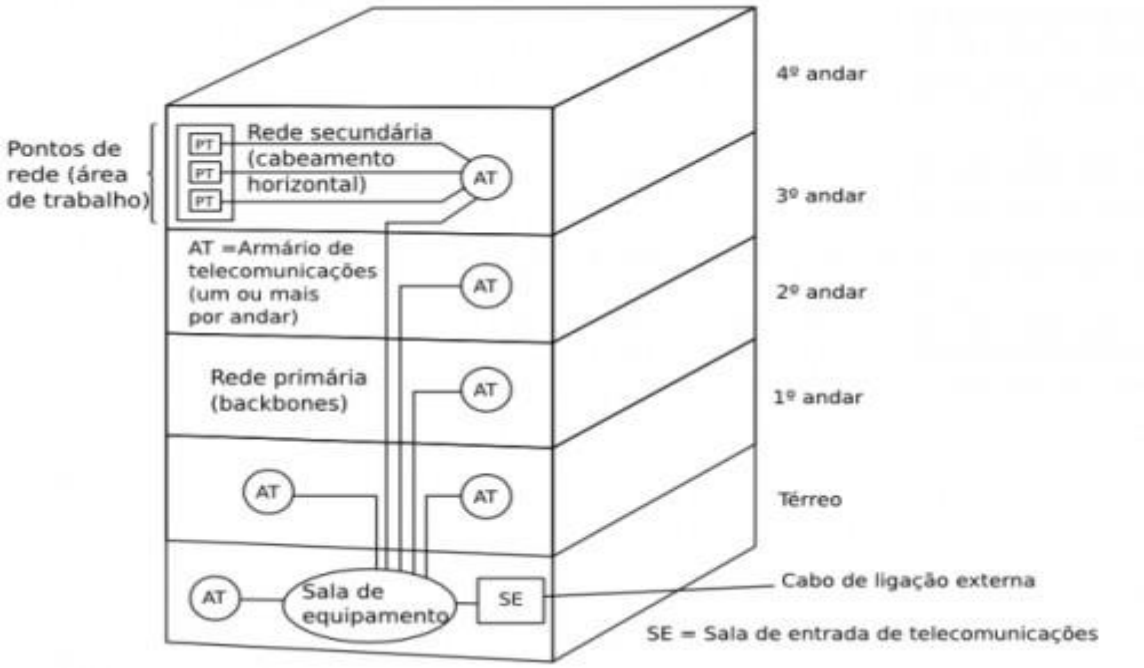


Dimensão da sala de equipamentos (acordo com a norma ANSI/TIA/EIA 569-A.)

Estações de trabalho	área (M2)
Até 100	14 (Mínima)
101 a 400	37
401 a 800	74
801 a 1200	111

Cabeamento vertical

Conjunto de cabos (cobre e fibra ótica) da rede vertical que possibilita a conexão entre os vários pontos de administração dos andares de um edifício a sala de equipamentos.



Armário de telecomunicações.

É o espaço destinado para acomodação de equipamentos, terminação e manobras de cabos. É o ponto de conexão entre o backbone e o cabeamento horizontal.

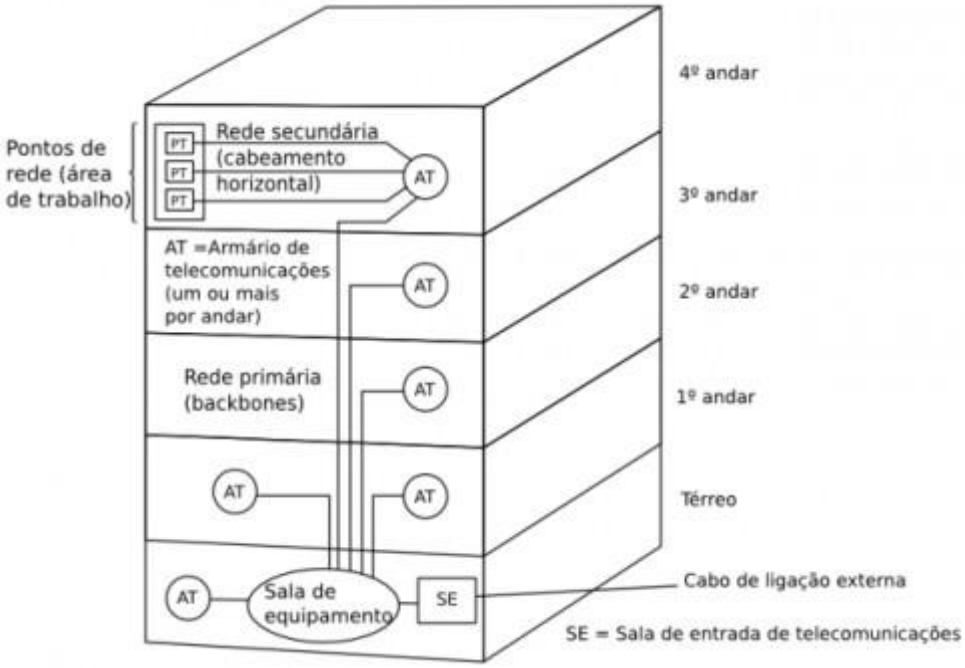
Patch Panels (Painéis de Conexão)

- Intermediário entre tomadas e Equipamentos de rede.

- Melhoram a organização dos cabos e facilitam a reconfiguração da rede.
- Construídos para fixação em racks.

Cabeamento horizontal

Conjunto de cabos horizontal, geralmente instalados em tetos, paredes ou no chão , que possibilita a conexão entre os pontos de saída da estação de trabalho aos armários de telecomunicações.

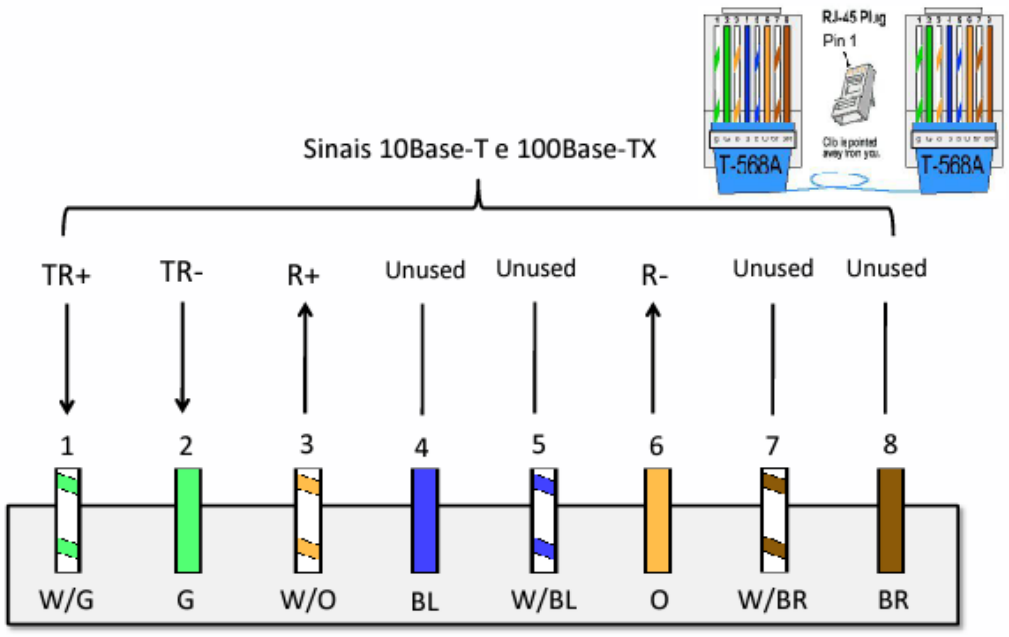


Área de trabalho

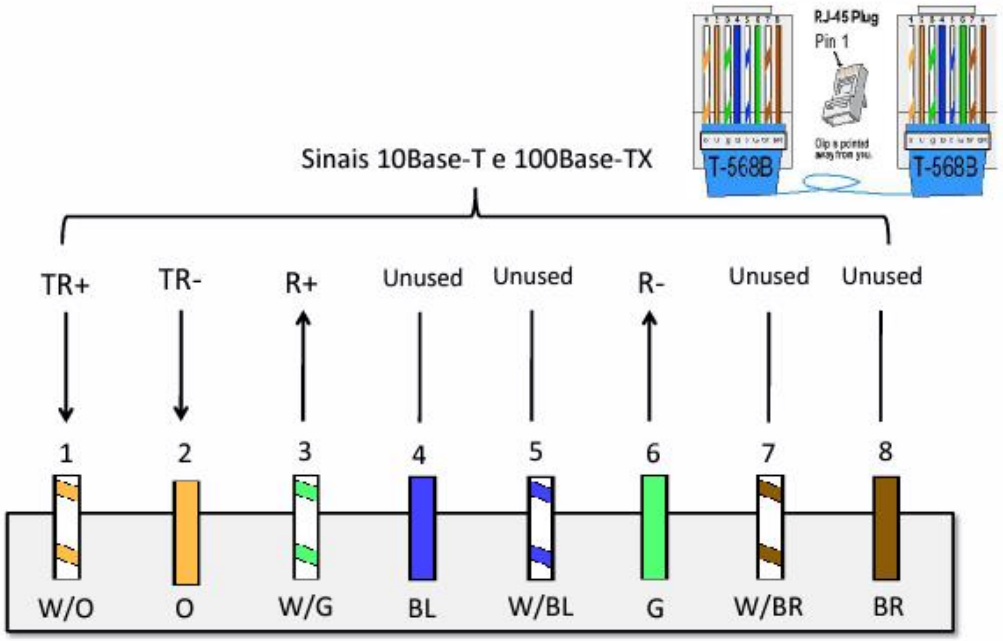
Conjunto de conectores, tomadas, adaptadores, plugs e outros pontos de saída que possibilita a fácil conexão dos terminais de voz, dados , a estações de trabalho a rede.

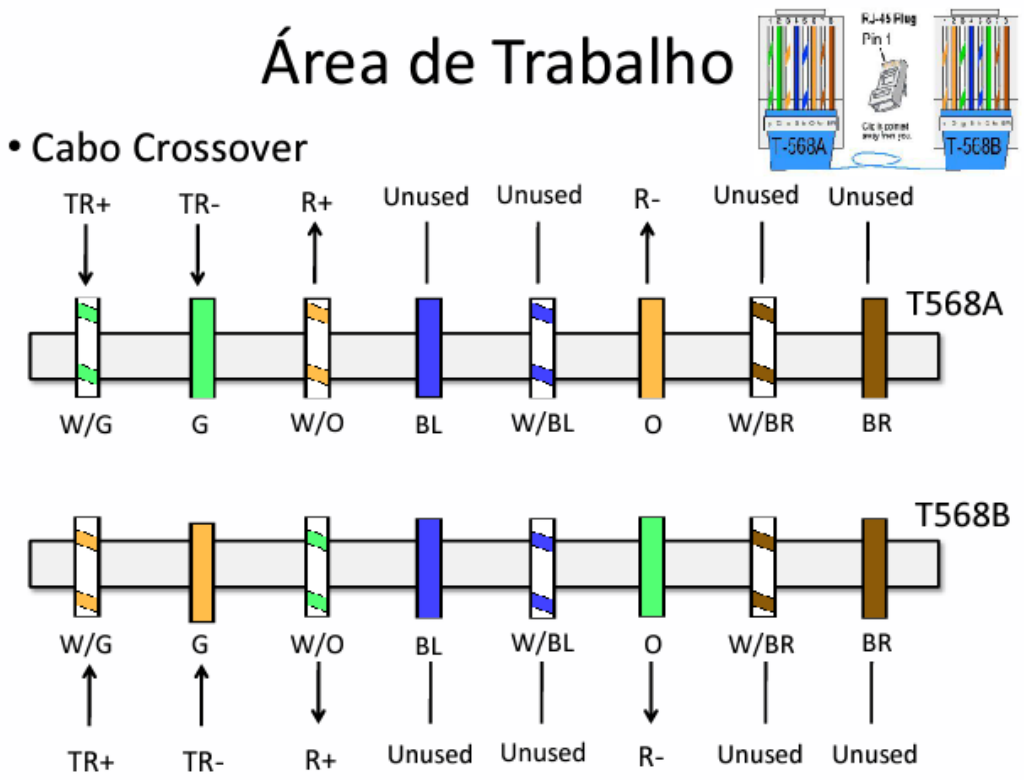
Tipos diferenciados no mercado de conectores e tomados de parede, de chão e de superfície.

Área de Trabalho – T568A



Área de Trabalho – T568B





Tipos de Cabos par trançado (resumo)

As taxas usadas nas redes com o cabo par trançado são:
10 Mbps (Ethernet);
100 Mbps (FastEthernet)ou
1000 Mbps (Gigabit Ethernet).
10000 Mbps ou 10Gbps (10Gigabit Ethernet).

Categoria 2 Transmissões de dados de até 4 Mbps .

Categoria 3 Transmissões de dados de até 10 Mbps.

Categoria 4 Transmissões de dados de até 20 Mbps.

Categoria 5 Transmissões de dados de até 100 Mbps.

Categoria do cabo 5e (Cat5e) Transmissões de dados de até 100 Mbps.

Categoria do cabo 6 (Cat6) Transmissões de dados de até 1000 Mbps (Gigabits).

Por que devo me preocupar com a segurança digital?

Computadores domésticos e corporativos são utilizados para realizar inúmeras tarefas, tais como: transações financeiras, sejam elas bancárias ou mesmo compra de produtos e serviços; comunicação, por exemplo, através de *e-mails*; armazenamento de dados, sejam eles pessoais ou comerciais, etc.

É importante que você se preocupe com a segurança de seu computador, pois você, provavelmente, não gostaria que:

- Suas senhas e números de cartões de crédito fossem furtados e utilizados por terceiros;
- Sua conta de acesso a Internet fosse utilizada por alguém não autorizado;
- Seus dados pessoais, ou até mesmo comerciais, fossem alterados, destruídos ou visualizados por terceiros;
- Seu computador deixasse de funcionar, por ter sido comprometido e arquivos essenciais do sistema terem sido apagados, etc.
-

Por que alguém iria querer invadir meu computador?

A resposta para esta pergunta não é simples. Os motivos pelos quais alguém tentaria invadir seu computador são inúmeros. Alguns destes motivos podem ser:

- Utilizar seu computador em alguma atividade ilícita, para esconder a real identidade e localização do invasor;
- Utilizar seu computador para lançar ataques contra outros computadores;
- Utilizar seu disco rígido como repositório de dados;
- Destruir informações (vandalismo);
- Disseminar mensagens alarmantes e falsas;
- Ler e enviar *e-mails* em seu nome;
- Propagar vírus de computador;
- Furtar números de cartões de crédito e senhas bancárias;
- Furtar a senha da conta de seu provedor, para acessar a Internet se fazendo passar por você;
- Furtar dados do seu computador, como por exemplo, informações do seu Imposto de Renda.