www.leitejunior.com.br
Informática para Concursos Públicos
leitejuniorbr@yahoo.com.br
leitejuniorbr@hotmail.com

ÍNDICE

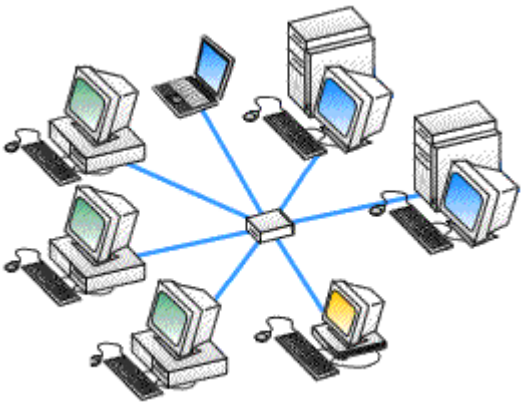
REDES DE COMPUTADORES....4
EXTENSÃO GEOGRÁFICA....4
SAN(STORAGE AREA NETWORK)....4
RAN(REGIONAL AREA NETWORK)....4
CAN(CAMPUS AREA NETWORK)....4
PAN(PERSONAL AREA NETWORK) / WPAN(WIRELESS PERSONAL AREA NETWORK)....4
LAN(LOCAL AREA NETWORK)....4
MAN(METROPOLITAN AREA NETWORK)....5
WAN(WIDE AREA NETWORK)....5
WLAN(WIRELESS LOCAL AREA NETWORK)....5
TOPOLOGIA....6
ANEL....6
BARRAMENTO OU BARRA(BUS)....6
ESTRELA....6
ÁRVORE....6
ARQUITETURAS DE REDES....7
ARQUITETURA ETHERNET(IEEE 802.3)....7
CARACTERÍSTICAS GERAIS....7
ACESSO CSMA-CD....7
GERAÇÕES....7
VELOCIDADES - PADRÃO VBASEC(VELOCIDADE BASE CABO)....7
TIPOS DE CABOS....7
CABO COAXIAL GROSSO....7
CABO COAXIAL FINO....8
CABO DE PAR-TRANÇADO....8
MONTAGEM DOS CABOS....9
CABO DIRETO(STRAIGHT) T-568A E T-568B....9
PADRÃO T-568A....9
PADRÃO T-568B....9
CABO INVERTIDO (CROSS-OVER)....10
PADRÃO T-568-A....10
PADRÃO T-568-B....10
CABO DE FIBRA ÓPTICA....10
TIPOS DE FIBRAS....11
ARQUITETURA WLAN / WIRELESS FIDELITY(WI-FI) – IEEE 802.11....11
CARACTERÍSTICAS GERAIS....11
ACESSO CSMA-CA....11
FORMAS DE COMUNICAÇÃO....11
TIPO DE TRANSMISSÃO....11
INFRAVERMELHO (IrDA)....11
BLUETOOTH....12
IEEE 802.11....13
IEEE 802.11a....13
IEEE 802.11b....13
IEEE 802.11g....13
IEEE 802.11n....13
ARQUITETURA WMAN / WIRELESS MAN(WI-MAX) – IEEE 802.16....14
CARACTERÍSTICAS GERAIS....14
HARDWARE DE REDE....15
PLACA DE REDE....15
ENDEREÇO MAC(Media Access Control)....15
HUB....15
CASCATEAMENTO (HUB)....16
REPETIDOR....16
PONTE / BRIDGE....16

PONTE SEGMENTADORA....16
PONTE TRADUTORA....17
ACCESS POINT - AP....17
SWITCH....17
ROTEADOR - ROUTER....18
ROTEADORES ESTÁTICOS....18
ROTEADORES DINÂMICOS....18
NAT - NETWORK ADDRESS TRANSLATION....18
SERVIDORES....19
TIPOS DE SERVIDORES....19
GATEWAY....19
O QUE É INTRANET?....20
USAMOS UMA INTRANET PARA....20
CONTEÚDOS USADOS EM UMA INTRANET....20
QUE É EXTRANET?....21
USAMOS UMA EXTRANET PARA....21
A INTERNET....21
BACKBONE....22
RNP - REDE NACIONAL DE ENSINO E PESQUISA....22
PROVEDOR DE ACESSO....22
TIPOS DE CONEXÃO....23
DIAL-UP / DISCADA....23
ISDN / RDSI....23
ADSL - BANDA LARGA....23
REDE ELÉTRICA / BPL / PLC....24
LAN – REDE LOCAL....25
TV A CABO....25
CONEXÃO 3G....25
DOMÍNIO DE INTERNET....26
DOMÍNIO GEOGRÁFICO – 1º. NÍVEL....26
DOMINIO DE TIPO – 2º. NÍVEL....26
DOMINIO DE INSTITUIÇÃO – 3º. NÍVEL....26
ONDE REGISTRAR UM DOMÍNIO....26
URL – UNIFORM RESOURCE LOCATOR....26
PROTOCOLOS....27
MODELO DE CAMADA OSI E TCP/IP....27
CAMADA 1 - FÍSICA....27
DISPOSITIVOS DA CAMADA....27
CAMADA 2 - LIGAÇÃO DE DADOS (ENLACE)....27
DISPOSITIVOS DA CAMADA....27
CAMADA 3 - REDE....28
DISPOSITIVOS DA CAMADA....28
IP -INTERNET PROTOCOL....28
ICMP - INTERNET CONTROL MESSAGE PROTOCOL....28
ARP – ADDRESS RESOLUTION PROTOCOL....29
RARP - REVERSE ARP....29
CAMADA 4 - TRANSPORTE....29
TCP - TRANSMISSION CONTROL PROTOCOL....29
UDP - USER DATAGRAM PROTOCOL....29
CAMADA 5 - SESSÃO....29
CAMADA 6 - APRESENTAÇÃO....29
CAMADA 7 - APLICAÇÃO....29
PORTAS DE COMUNICAÇÃO....29
HTTP – HYPER TEXT TRANSFER PROTOCOL....30
HTTPS – HYPER TEXT TRANSFER PROTOCOL SECURE....30
SSL - SECURE SOCKETS LAYER....30
TLS - TRANSPORT LAYER SECURITY....30
DHCP - DYNAMIC HOST CONFIGURATION PROTOCOL....31
IRC - INTERNET RELAY CHAT....31
SNMP - SIMPLE NETWORK MANAGEMENT PROTOCOL....31
POP - POST OFFICE PROTOCOL....31
IMAP - INTERNET MESSAGE ACCESS PROTOCOL....31
SMTP - SIMPLE MAIL TRANSFER PROTOCOL....31

FTP - FILE TRANSFER PROTOCOL....31
TFTP – TRIVIAL FILE TRANSFER PROTOCOL....32
TELNET - TERMINAL EMULATOR....32
SSH - SECURE SHELL....32
NTP – NETWORK TIME PROTOCOL....32
NNTP – NETWORK NEWS TRANSFER PROTOCOL....32
DNS – DOMAIN NAME SERVICE....32
KERBEROS....33
VPN – VIRTUAL PRIVATE NETWORK....34
INTRODUÇÃO....34
ACESSO REMOTO VIA INTERNET....34
CONEXÃO DE COMPUTADORES NUMA INTRANET....34
REQUISITOS BÁSICOS....35
TUNELAMENTO....35
IPSEC – INTERNET PROTOCOL SECURITY....36

REDES DE COMPUTADORES

São dois ou mais computadores ligados entre si com a finalidade de compartilhar aplicativos, recurso, dados e periféricos.



EXTENSÃO GEOGRÁFICA

SAN(STORAGE AREA NETWORK)

- Rede cujo objetivo é o armazenamento de dados com alto desempenho.

RAN(REGIONAL AREA NETWORK)

- Rede de dados que interconecta negócios, residências e governos em uma região geográfica específica. São maiores que as LANs MANs, mas menores que WANs. São comumente caracterizadas pelas conexões de alta velocidade utilizando cabo de fibra ótica ou outra mídia digital.

CAN(CAMPUS AREA NETWORK)

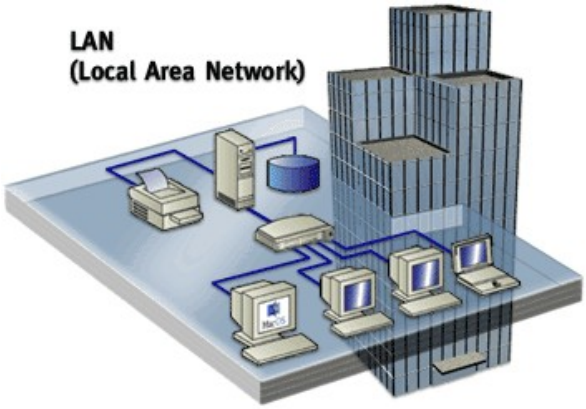
- Rede que usa ligações entre computadores localizados em áreas de edifícios ou prédios diferentes, como em campus universitários ou complexos industriais.

PAN(PERSONAL AREA NETWORK) / WPAN(WIRELESS PERSONAL AREA NETWORK)

- Possui dispositivos ligados para um único usuário. Normalmente um dispositivo bluetooth é usado neste tipo de rede.

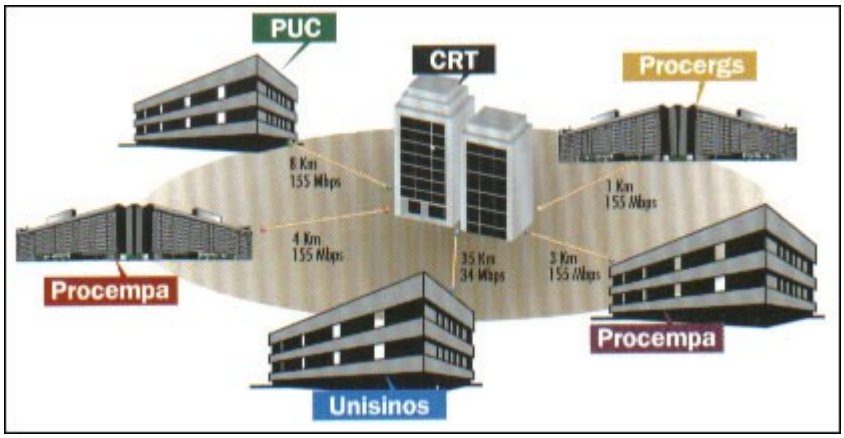
LAN(LOCAL AREA NETWORK)

- São denominadas locais por cobrirem apenas uma área limitada. Utilizadas para conectar estações, servidores, periféricos e outros dispositivos que possuam capacidade de processamento em uma casa, escritório, escola e edifícios próximos.



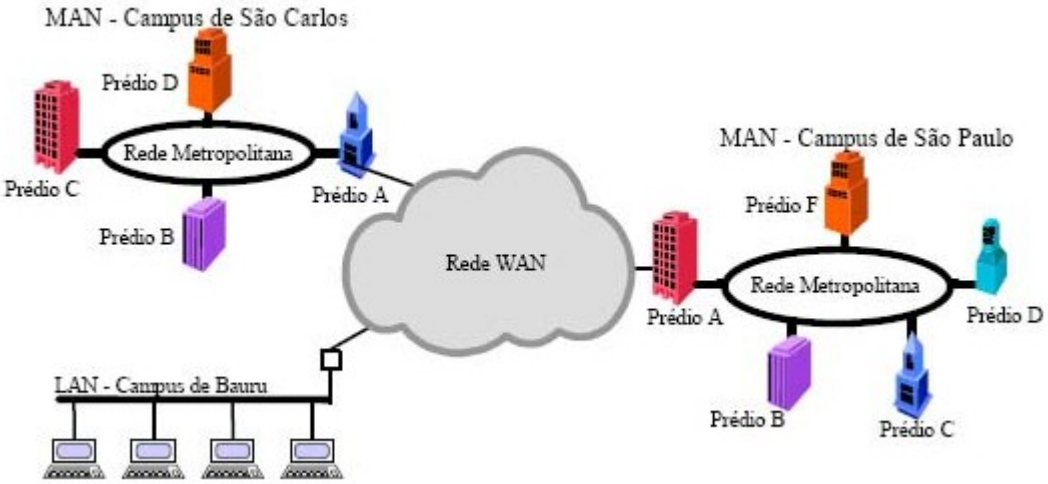
MAN(METROPOLITAN AREA NETWORK)

- Pode abranger um grupo de escritórios vizinhos ou uma cidade inteira, podendo ser privada ou pública. Esse tipo de rede é capaz de transportar dados e voz, podendo inclusive ser associado a rede de televisão a cabo local.



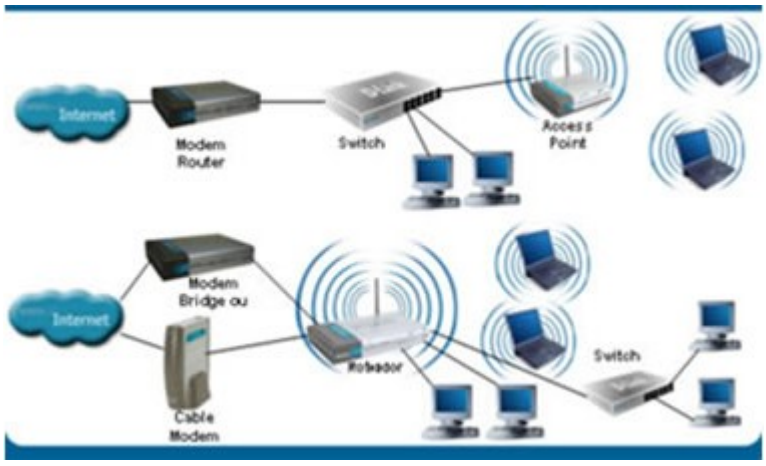
WAN(WIDE AREA NETWORK)

- Rede de computadores que abrange uma grande área geográfica. A Internet é um exemplo de WAN.



WLAN(WIRELESS LOCAL AREA NETWORK)

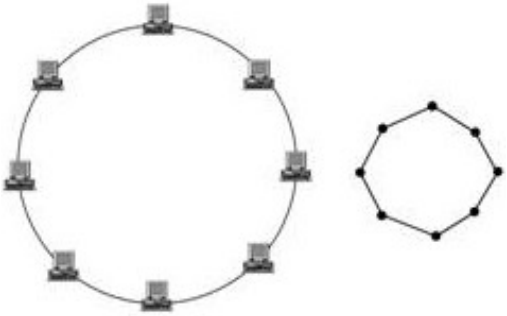
- Rede local sem fio. Conhecida por Wi-Fi(Wireless Fidelity - fidelidade sem fios). Conecta seus componentes usando ondas de rádio freqüência.



TOPOLOGIA

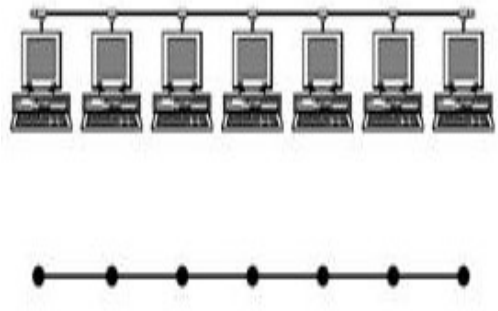
Define como os computadores estão ligados fisicamente a uma rede.

ANEL



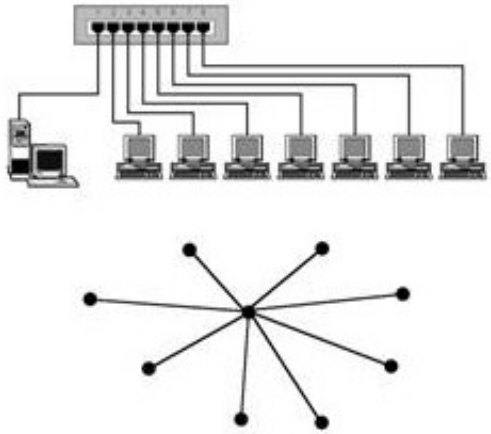
- A topologia de rede em anel consiste em estações conectadas através de um circuito fechado, em série.
- As configurações mais usuais são unidirecionais.
- O padrão mais conhecido é o Token Ring(IEEE 802.5).
- Um pacote(token) fica circulando no anel, pegando dados das máquinas e distribuindo para o destino.
- Somente um dado pode ser transmitido por vez neste pacote.
- Nesta topologia cada estação está conectada a apenas duas outras estações.
- Uma desvantagem é que se uma máquina falhar, toda a rede pode ser comprometida.

BARRAMENTO OU BARRA(BUS)



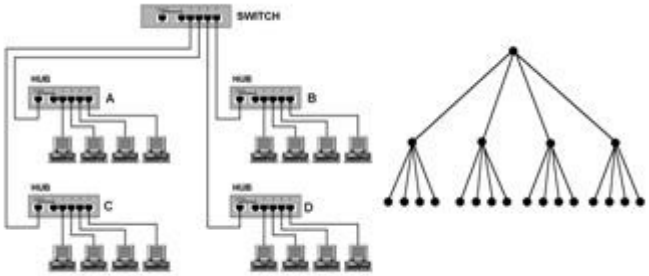
- Todas as estações compartilham um mesmo cabo.
- Essa topologia utiliza cabo coaxial.
- O tamanho máximo do trecho da rede está limitado ao limite do cabo, 185 metros no caso do cabo coaxial fino.
- Transfere dados por Broadcast(difusão).
- Todos os receptores recebem o sinal.
- Como todas as estações compartilham um mesmo cabo, somente uma transação pode ser efetuada por vez, isto é, não há como mais de um micro transmitir dados por vez. Logo, quanto mais computadores ligados a rede, mais lenta ela fica.
- Diferente da rede em anel, se uma das máquinas falhar, a rede não é comprometida.

ESTRELA



- Esta é a topologia mais recomendada e usada atualmente.
- Todas as estações são conectadas a um periférico CONCENTRADOR(hub ou switch).
- Utilizando um HUB, a topologia fisicamente será em estrela, porém logicamente ela continua sendo uma rede de topologia de barra. O Hub é um periférico que repete para todas as suas portas os pacotes que chegam, assim como ocorre na topologia de barra(broadcast).
- Utilizando um SWITCH, a rede será tanto fisicamente quanto logicamente em estrela. Ele analisa o cabeçalho de endereçamento dos pacotes de dados, enviando os dados diretamente ao destino, sem replicá-lo desnecessariamente para todas as suas portas. Isso faz com que a rede torne-se mais segura e muito mais rápida, pois praticamente elimina problemas de colisão. Além disso, duas ou mais transmissões podem ser efetuadas simultaneamente, desde que tenham origem e destinos diferentes.

ÁRVORE



- É equivalente a várias redes em estrela ligadas entre si.
- É o caso de conexões de múltiplos hubs ou switches.
- Na figura ao lado, o primeiro nó da rede é o switch. Nele estão ligados 4(quatro) hubs, e em cada um deles estão ligados 4(quatro) computadores.

ARQUITETURAS DE REDES

- Conjuntos de características que especificam como uma rede funciona.

- Ethernet: Com fio. IEEE 802.3.
- WLan - Wireless Fidelity(Wi-Fi). Sem fio. IEEE 802.11.
- WMan - Wireless Man(Wi-Max). Sem fio. IEEE 802.16.

ARQUITETURA ETHERNET(IEEE 802.3)

CARACTERÍSTICAS GERAIS

- O IEEE(Institute of Electrical and Electronics Engineers) dos Estados Unidos, é um dos grupos que lideram a padronização de redes no mundo.
- A Ethernet foi padronizada pelo IEEE com o código 802.3(IEEE 802.3).

ACESSO CSMA-CD

- Carrier Sense Multiple Access with Collision Detection.
- **CS:** As placas de rede "escutam" a rede para ver se é possível transmitir;
- **MA:** É possível que haja acesso múltiplo (duas ou mais placas acessam ao mesmo tempo);
- **CD:** Se houver acesso múltiplo, detecta e corrige a colisão.

GERAÇÕES

- **Ethernet:** 10Mbps usava cabos coaxiais (10base2, 10base5) ou cabos de par-trançado (10baseT).
- **Fast Ethernet:** 100Mbps com par-trançado (100baseT) ou fibra óptica (100baseF).
- **Giga Ethernet:** 1000Mbps (1Gbps) com diversos tipos de cabos.

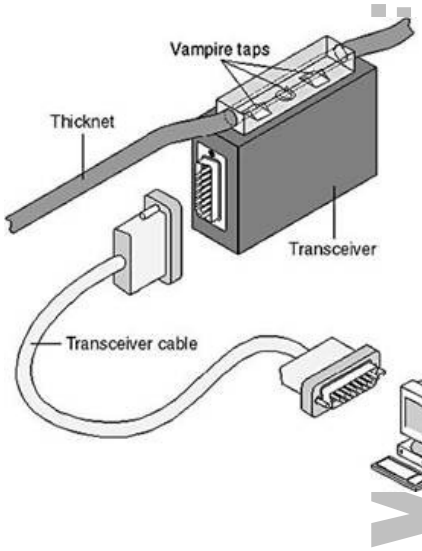
VELOCIDADES - PADRÃO VBASEC(VELOCIDADE BASE CABO)

- 10base5: cabo coaxial grosso(thick) 500m de distância.
- 10base2: cabo coaxial fino(thin) 185m de distância.
- 10baseT: cabo de par-trançado – 100m de distância.
- 100baseT2: par-trançado cat. 3; usa 2 dos 4 pares de fios do cabo. 100m de extensão.
- 100baseT4: par-trançado cat. 3; usa 2 dos 4 pares de fios do cabo. 100m de extensão.
- 100baseTX: par-trançado cat. 5; usa 2 dos 4 pares de fios do cabo. 100m de extensão.
- 100baseFX: fibra óptica. 2 km de extensão.
- 1000baseT: par-trançado cat. 5. 100m de extensão.
- 1000baseCX: cabo twiaxial(coaxial com 2 núcleos). 25m de extensão.
- 1000baseSX: fibra-óptica multimodo. 550m de extensão.
- 1000baseLX: fibra-óptica monomodo. Cerca de 5.000m de extensão.

TIPOS DE CABOS

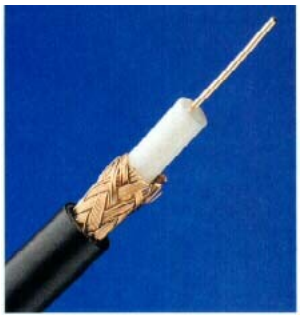
CABO COAXIAL GROSSO

- Chamado "Thick Ethernet/Thicknet" ou 10Base5.
- É conectado à placa de rede através de um transceiver.
- Especificação RG-213 A/U(Núcleo de fio trançado) ou RG-213 /U (Núcleo de cobre sólido).
- Velocidade de 10 Mbps.
- Cada segmento de rede pode ter, no máximo, 500 metros.
- Cada segmento de rede pode ter, no máximo, 100 nós(pontos de conexão).
- Distância mínima de 2,5m entre cada nó da rede.



CABO COAXIAL FINO

- Chamado de "Thin Ethernet/Thinnet" ou 10Base2.
- Utiliza a especificação RG-58 A/U(Núcleo de fio trançado) ou RG-58 /U(Núcleo de cobre sólido).
- Cada segmento da rede pode ter, no máximo, 200m(185 metros).
- Cada segmento pode ter, no máximo, 30 nós(pontos).
- Distância mínima de 0,5m entre cada nó(ponto) da rede.
- Velocidade de transferência é de 10 Mbps(1,25 MB/s).
- Utiliza conector BNC para interconexão.



CABO DE PAR-TRANÇADO

- É formador por pares de fios se entrelaçam por toda a extensão do cabo minimizando interferências externas ou do sinal de um dos fios para o outro.
- Utiliza conector RJ-11(telefone) ou RJ-45(computador).
- Distância limite é de 100 metros.
- 10/100BaseT.

- **Tipos de Cabos**
  - **Cat 1:** Usado em sistemas telefônicos.

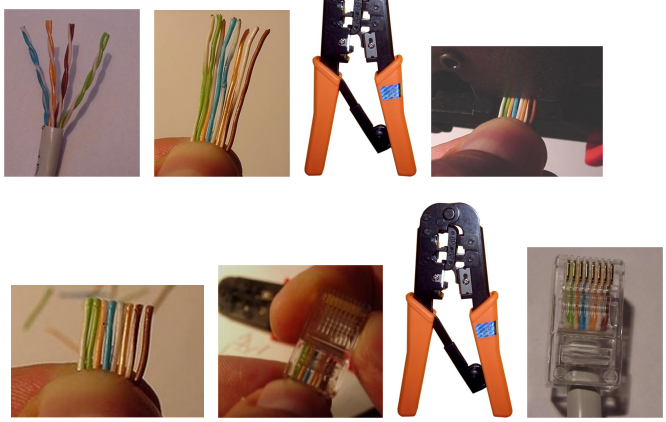
  - **Cat 5:** Mais usado atualmente em redes de computadores. Possui 4(quatro) pares de fios.
    - **UTP(Unshielded Twisted Pair – não blindado):** São 4(quatro) pares de fios entrelaçados e revestidos por uma capa de PVC. Mais usado atualmente e mais barato.

    - **STP (Shield Twisted Pair - blindado):** Possui uma proteção metálica entre os pares e envolvendo todos eles, minimizando o risco de interferências.

- **Conectores**
  - **RJ-11:** Conector com 4(quatro)/6(pinos) pinos. Usando em sistemas telefônicos com cabos UTP Cat 1.

  - **RJ-45:** Conector com 8(oito) pinos. Usando em redes locais com cabos UTP Cat 5.

- **Alicate de Crimpar**
  - Usado para crimpar o cabo de par-trançado ao conector RJ-45.



MONTAGEM DOS CABOS

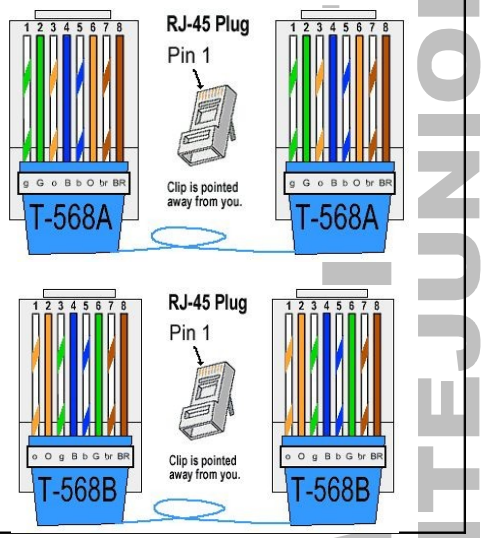
Existem dois padrões de montagem dos cabos.

CABO DIRETO(STRAIGHT) T-568A E T-568B

- utilizado para ligação da placa de rede(micro) ao hub.

PADRÃO T-568A
- 1- Branco com Verde
- 2- Verde
- 3- Branco com Laranja
- 4- Azul
- 5- Branco com Azul
- 6- Laranja
- 7- Branco com Marrom
- 8- Marrom

PADRÃO T-568B
- 1- Branco com Laranja
- 2- Laranja
- 3- Branco com Verde
- 4- Azul
- 5- Branco com Azul
- 6- Verde
- 7- Branco com Marrom
- 8- Marrom



CABO INVERTIDO (CROSS-OVER)

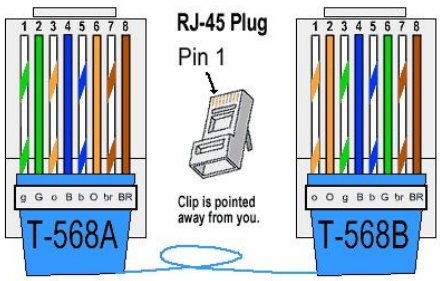
- Utilizado para ligação entre 2(dois) hubs (cascateamento) ou para ligar 2(dois) micros pela placa de rede (padrão RJ-45) sem a utilização de hub.

PADRÃO T-568-A

- 1- Branco com Verde
- 2- Verde
- 3- Branco com Laranja
- 4- Azul
- 5- Branco com Azul
- 6- Laranja
- 7- Branco com Marrom
- 8- Marrom

PADRÃO T-568-B

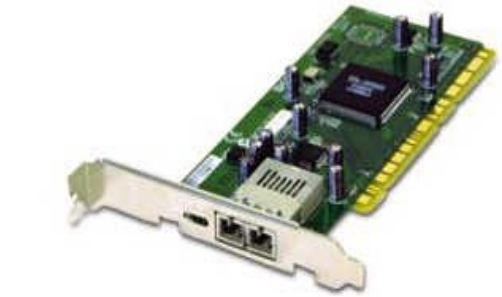
- 1- Branco com Laranja
- 2- Laranja
- 3- Branco com Verde
- 4- Azul
- 5- Branco com Azul
- 6- Verde
- 7- Branco com Marrom
- 8- Marrom



- **Características da Montagem**
  - São montados usando apenas 2(dois) pares de fios nas implementações atuais(half-duplex) pinos 1 e 2 (para enviar); 3 e 6 (para receber).
  - **HALF-DUPLEX:** Este termo é usado em relação a placas de rede e outros dispositivos de comunicação. Operando neste modo, o dispositivo pode transmitir e receber dados, mas uma coisa de cada vez. Exemplo, Walk-Talk.
  - **FULL-DUPLEX:** Os dados podem ser transmitidos e recebidos simultaneamente. Exemplo, aparelho telefônico.

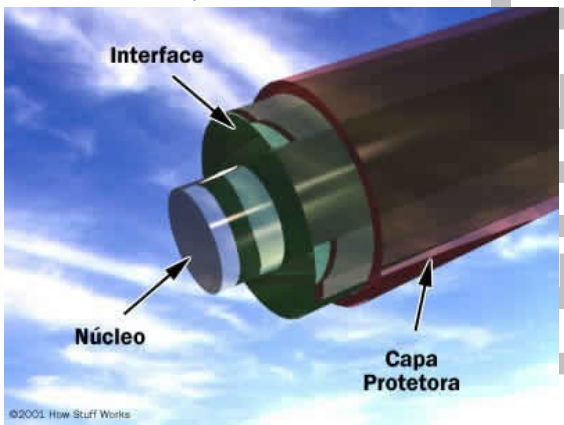
CABO DE FIBRA ÓPTICA

- Permite transmissão de dados em alta velocidade e são completamente imunes a qualquer tipo de interferência eletromagnética, porém, são muito mais caros e difíceis de instalar.
- Como os cabos são feitos de plástico e fibra de vidro(ao invés de metal) são resistentes à corrosão.



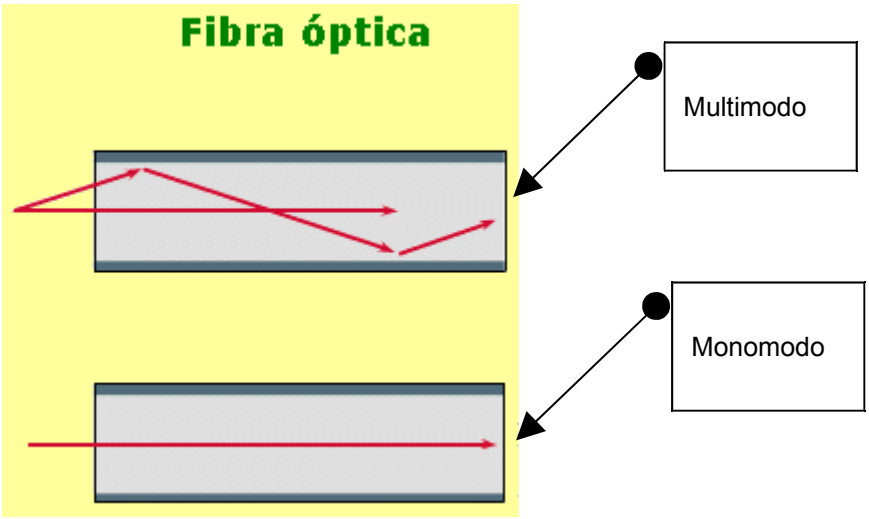
Placa de Rede com Conectores para Fibra Ótica.

- O cabo de fibra óptica é formado por um núcleo extremamente fino de vidro, ou de um tipo especial de plástico, coberto por fibra de vidro que envolve e protege o núcleo, uma camada de plástico protetora chamada de cladding, uma camada de isolamento e finalmente uma capa externa chamada bainha.



TIPOS DE FIBRAS

- **MULTIMODO:** fibra óptica com núcleo mais grosso. Admite a transmissão de vários sinais simultaneamente (vários feixes). Custo menos alto.
- **MONOMODO:** fibra com núcleo mais fino transmite apenas um feixe. Conseguem transmitir por extensões maiores de cabo. Custo mais alto.



ARQUITETURA WLAN / WIRELESS FIDELITY(WI-FI) – IEEE 802.11

CARACTERÍSTICAS GERAIS

- É um conjunto de padrões de compatibilidade baseado nas especificações IEEE 802.11.
- É uma rede interligada sem fios chamada de WLan(Wireless LAN).

ACESSO CSMA-CA

- Carrier Sense Multiple Access with Collision Avoidance.
- **CS:** As placas de rede "escutam" a rede para ver se é possível transmitir.
- **MA:** É possível que haja acesso múltiplo (duas ou mais placas acessam ao mesmo tempo);
- **CA:** Se houver acesso múltiplo, evitar colisão.

FORMAS DE COMUNICAÇÃO

- **Modo infraestrutura:** normalmente o mais encontrado, utiliza um concentrador de acesso (Access Point-AP).
- **Modo ponto a ponto (ad-hoc):** permite que um pequeno grupo de máquinas se comunique diretamente, sem a necessidade de um AP(Access Point).

TIPO DE TRANSMISSÃO

INFRAVERMELHO (IrDA)

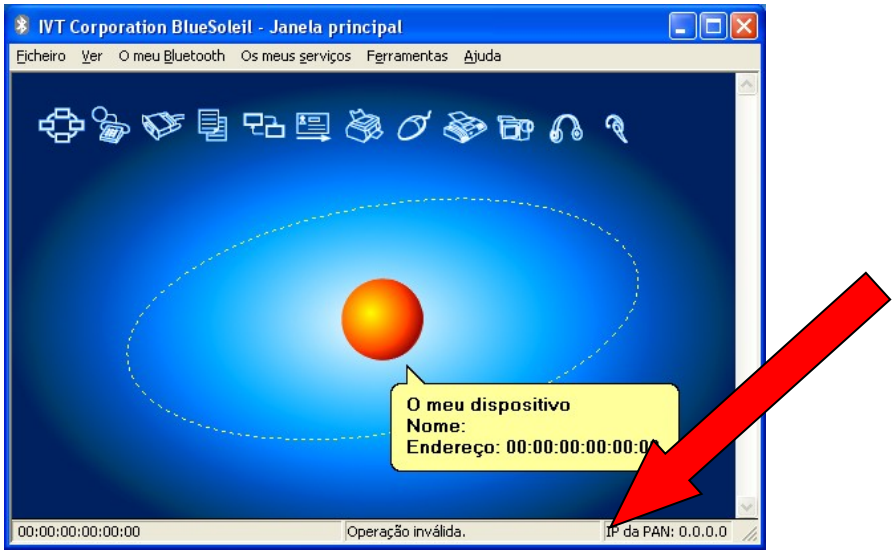
- IrDA(Infrared Data Association) desenvolveu o padrão utilizado nos transmissores infravermelhos que equipam os PCs, notebooks, impressoras e handhelds atuais.
- Utiliza como meio de comunicação a radiação infravermelha.
- Possuem um alcance bem limitado, cerca de 1(um) metro.
- Não deve ter barreiras entre os pontos de comunicação.
- O transmissor deve estar apontado diretamente para o receptor.
- Baixa velocidade de transmissão até 115Kbps(14,3KB/s).

BLUETOOTH

- É uma tecnologia que permite uma comunicação simples, rápida, segura e barata entre computadores, smartphones, telefones celulares, mouses, teclados, fones de ouvido, impressoras e outros dispositivos, utilizando ondas de rádio no lugar de cabos.
- Possibilita a comunicação desses dispositivos uns com os outros quando estão dentro do raio de alcance.
- Os dispositivos usam um sistema de comunicação via rádio, por isso não necessitam estar na linha de visão um do outro, e podem estar até em outros ambientes, contanto que a transmissão recebida seja suficientemente potente.

- **Classe: Potência - Distância**
  - Classe 1: potência máxima de 100 mW - alcance de até 100(cem) metros.
  - Classe 2: potência máxima de 2,5 mW - alcance de até 10(dez) metros.
  - Classe 3: potência máxima de 1 mW - alcance de até 1(um) metro.

- Cada dispositivo é dotado de um número único de 48 bits(6 Bytes) que serve de identificação, no formato 00:00:00:00:00:00.
- Esse número é denominado "Endereço de Bluetooth"(Bluetooth Address) e são únicos e exclusivos para cada dispositivo fabricado, assim como o Endereço MAC das placas de rede.



- **Versão - Taxa de Transferência**
  - Versão 1.2 - 1 Mbps(0,12MB/s).
  - Versão 2.0 + EDR - 3 Mbps(0,37MB/s).
  - Versão 3.0(Em desenvolvimento) - 53 - 480 Mbps(60 MB/s).

IEEE 802.11

- Estabelece normas para a criação e para o uso de redes sem fio.
- A transmissão dessa rede é feita por sinais de radiofreqüência, que se propagam pelo ar e podem cobrir áreas na casa das centenas de metros.
- Para uma rede desse tipo ser estabelecida, é necessário que os dispositivos (STA - de "station") se conectem a aparelhos que fornecem o acesso. Estes são genericamente denominados Access Point(AP).
- Quando um ou mais STAs se conectam a um AP, tem-se, portanto, uma rede denominada Basic Service Set(BSS).
- Service Set Identifier(SSID) é o nome dado(pelo usuário) a sua rede sem fio.

- Protocolos de segurança para redes sem fio.
  - **WEP**(Wired Equivalent Privacity)
    - Usa algoritmo RC4 de criptografia simétrica(chave de cifragem = chave de decifragem)
  - **WPA**(Wi-Fi Protected Access)
    - Mais segura que o WEP.
    - Esse protocolo usa chaves de 256 bits.

IEEE 802.11a

- Velocidades de 6 Mbps, 9 Mbps, 12 Mbps, 18 Mbps, 24 Mbps, 36 Mbps, 48 Mbps e 54 Mbps(6,75MB/s).
- Pode chegar a 108 Mbps(13,5MB/s) por fabricantes não padronizados.
- Alcance geográfico de sua transmissão é de cerca de 50 metros.
- Freqüência de operação é 5GHz.
- Incompatibilidade com os padrões 802.11b/g.

IEEE 802.11b

- Velocidade de transmissão: 1 Mbps, 2 Mbps, 5,5 Mbps e 11 Mbps(1,3MB/s).
- Opera na freqüência de 2.4GHz.
- Área de cobertura é de 400 metros em ambientes abertos
- Área de cobertura de 50 metros em lugares fechados(escritórios e residências).
- Pode sofrer interferência na transmissão e recepção de sinais por funciona na mesma freqüência dos telefones móveis, fornos microondas e dispositivos Bluetooth.

IEEE 802.11g

- Compatibilidade com os dispositivos 802.11b
- Velocidade de 54Mbps(6,75MB/s).
- Funciona dentro da freqüência de 2,4 GHz.
- Vantagem e desvantagem: a mesma do 802.11b.

IEEE 802.11n

- Iniciou seu desenvolvimento em 2004.
- Em fase final de homologação. Opera nas faixas de 2,4GHz e 5GHz.
- Sucessor do 802.11g, tal como este foi do 802.11b.
- O 802.11n tem como principal característica o uso de um esquema chamado Multiple-Input Multiple-Output(MIMO), capaz de aumentar consideravelmente as taxas de transferência de dados através da combinação de várias vias de transmissão.
- Pode fazer transmissões na faixa de 300Mbps(37,5MB/s) e, teoricamente, pode atingir taxas de até 600Mbps(75MB/s).

ARQUITETURA WMAN / WIRELESS MAN(WI-MAX) – IEEE 802.16

CARACTERÍSTICAS GERAIS

- Redes metropolitanas sem fio de uso corporativo que atravessam cidades e estados.
- Utilizada entre os provedores de acesso e seus pontos de distribuição.
- A WiMax possui o padrão 802.16 que é um dos últimos padrões de banda larga para rede MAN(Metropolitan Area Network/Rede de Área Metropolitana) definido pelo IEEE.
- Tem como objetivo estabelecer a parte final da infra-estrutura de conexão de banda-larga (last mile) oferecendo conectividade para mais diversos fins: por exemplo uso doméstico, hotspot e empresarial.
- Capacidade de estabelecer uma rede MESH(rede em malha), compartilhando recursos e diminuindo custos da rede.
- Estabelecer uma conexão mais direta da rede domestica com a rede principal(core network) da internet.
- Oferece conexão de até 75 Mbps(9 MB/s) em um raio de 50 km.
- Possui especificação de espectro de RF de 2 a 66Ghz.

HARDWARE DE REDE

- São dispositivos usados para a interconexão de periféricos e transferência de dados.

PLACA DE REDE

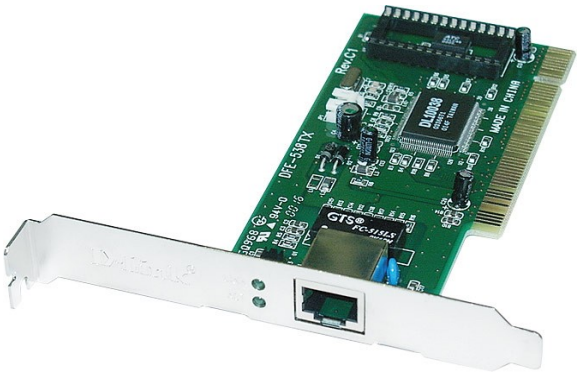
- Chamada de "adaptador de rede" ou "interface de rede" ou NIC(Network Interface Connection) ou Placa Ethernet.
- Não entende pacotes TCP/IP, apenas endereços MAC (endereços físicos).
- Opera na **CAMADA DE ENLACE** (camada 2) do modelo OSI.
- É responsável pela conexão do computador a estrutura da rede.
- Cada computador tem que ter sua própria placa de rede.
- Velocidade de transmissão: 10 Mbps(Ethernet), 100 Mbps(Fast Ethernet) e 1000 Mbps(Giga Ethernet)

ENDEREÇO MAC(Media Access Control).

- Usado para identificar fisicamente a placa de rede.
- São endereços de 48 bits, representados através de 12 dígitos hexadecimais (00:15:00:4B:68:DB).
- São gravados na ROM da própria placa, durante sua fabricação.
- Cada placa de rede possui um único endereço MAC.

- Embora os termos "frame" e "pacote" sejam freqüentemente usados como sinônimos, existe uma diferença entre eles. O termo **"pacote"** é usado quando estiver se referindo aos pacotes TCP e o termo **"frame"** quando estiver se referindo às transmissões efetuadas pelas placas de rede.
- No **frame** é inserido o endereço de origem e de destino dos dados, além de 32 bits de CRC, que são usados pela placa de destino para verificar a integridade do **frame** recebido.
- Sempre que um frame chega corrompido, a placa solicita sua retransmissão, de forma a garantir que os dados recebidos são sempre os mesmos que foram enviados.

- Este sistema permite que as redes Ethernet sejam usadas em redes com qualquer protocolo, sem ficarem restritas ao TCP/IP. A rede age como uma camada genérica de transporte, com suas próprias regras, que se limita a transportar informações de um ponto a outro, sem tentar entender o conteúdo dos pacotes.

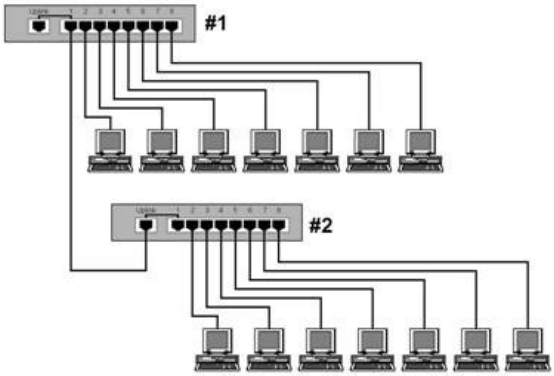


HUB

- É o elemento central de uma rede baseada em cabo par-trançado.
- Opera na **CAMADA FÍSICA** (camada 1) do modelo OSI.
- Tem como função regenerar os sinais e os transmitir para as suas portas (BROADCAST).
- Não entende o endereço MAC.
- Os nós (estações) são conectados as portas do hub e se houver algum problema em uma estação, a rede não será afetada.
- A rede só será paralisada se o hub apresentar algum problema.

CASCATEAMENTO (HUB)

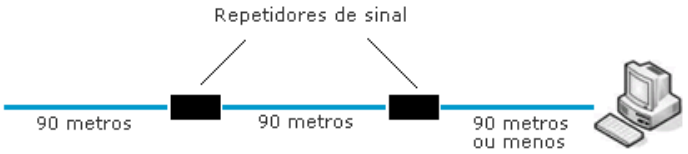
- Pode-se conectar dois ou mais hubs entre si usando uma porta chamada "Up Link".
- Basta ligar as portas "Up Link" de ambos os hubs, usando um cabo de rede normal.
- Existem alguns hubs que não possuem a porta "Up Link", usando um cabo cross-over pode-se conectar os dois hubs. A única diferença neste caso é que ao invés de usar as portas "Up Link", usará duas portas comuns.



REPETIDOR

- Utilizado para interligação de redes idênticas.
- Opera na CAMADA FÍSICA (camada 1) do modelo OSI.
- Amplifica e regenera eletricamente os sinais transmitidos no meio físico.

1. Esquema mostrando o uso de repetidores:

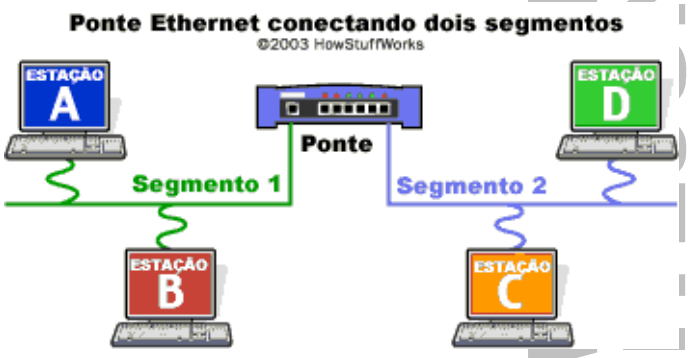


Nota: Não se deve usar mais do que três repetidores em linha. Em caso de distâncias grandes, a melhor opção é usar a fibra ótica.

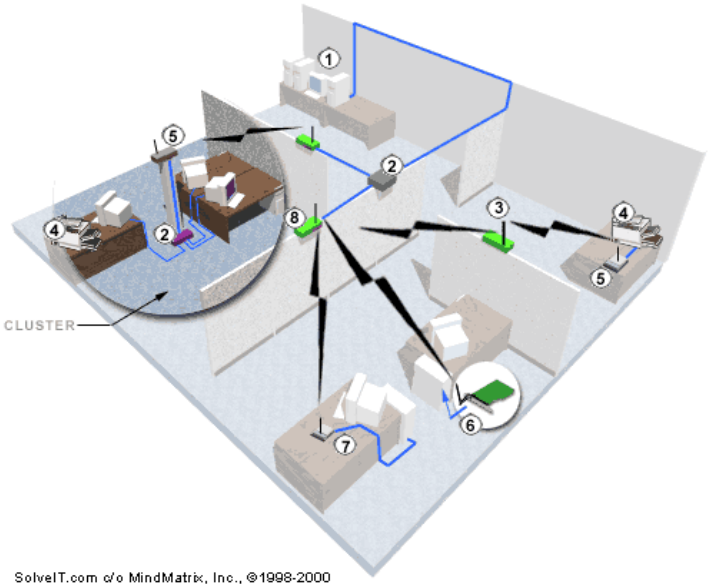
PONTE / BRIDGE

- Utilizada para segmentar uma rede grande em duas redes menores aumentando seu desempenho.
- Opera na CAMADA DE ENLACE (camada 2) do modelo OSI.
- É capaz de entender endereços MAC filtrando tráfegos entre segmentos de uma rede, só tem um problema, não filtra conteúdo enviado por broadcast.
- Permite o tráfego de qualquer tipo de protocolo.
- Interligar redes que possuem mesma arquitetura(segmentadora) e arquiteturas diferentes(tradutora).
- É composta de duas portas que conectam os segmentos de uma rede . O tráfego gerado por um segmento fica confinado no mesmo evitando assim que haja interferência no tráfego do outro segmento. O tráfego só atravessará para o outro segmento, se a estações origem e destino não estiverem no mesmo segmento.

PONTE SEGMENTADORA

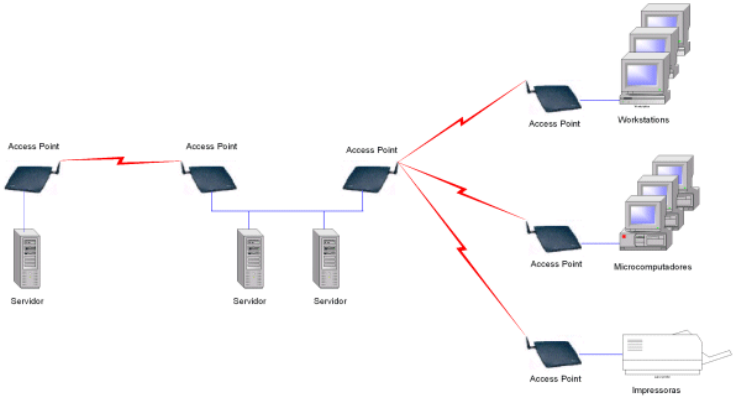


PONTE TRADUTORA



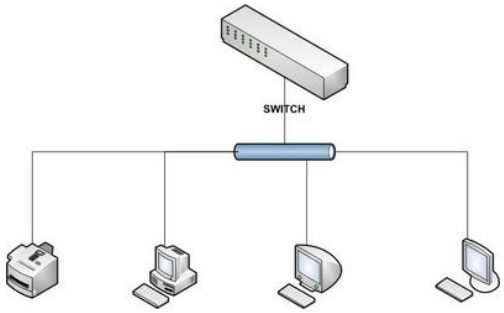
ACCESS POINT - AP

- É um dispositivo que atua como ponte entre uma rede sem fio e uma rede tradicional.
- O Access Point(AP) transforma o tráfego da rede convencional(via cabos) em sinal de rádio Wi-Fi.
- Por meio de Access Points, usuários de PDAs ou notebooks equipados com Wi-Fi podem acessar a rede local da empresa ou navegar pela Internet.
- Todo sinal Wi-Fi é proveniente de um ponto de acesso. Os pontos de acesso (Access Points) podem operar no padrão 802.11a, 11b ou 11g.



SWITCH

- Um switch é bem mais esperto que um hub e uma ponte.
- Opera na **CAMADA DE ENLACE** (camada 2) do modelo OSI.
- Não entende o TCP/IP.
- O switch faz uma comutação (ligação) entre as máquinas origem e destino, isolando as demais portas desse processo.
- Possui uma tabela de encaminhamento chamada **TABELA MAC**. Nessa tabela está especificado a associação das máquinas as portas do switch.



ROTEADOR - ROUTER

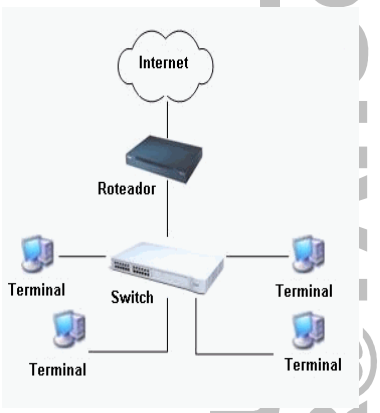
- Equipamento utilizado em redes de maior porte.
- Opera na CAMADA DE REDE (camada 3) do modelo OSI.
- Entende endereços MAC e endereços IP.
- Permite uma comunicação complexa entre diversos segmentos de redes com protocolos e arquiteturas diferenciadas.
- Sabe o endereço de cada segmento, tendo a capacidade de determinar qual o melhor caminho para envio de dados, além de filtrar o tráfego de broadcast.
- Podemos dizer que um roteador é uma ponte/switch melhorado.
- Fornece melhor gerenciamento do tráfego, pode compartilhar status de conexão e informações com outro roteadores e usar essa informação para driblar conexões lentas ou instáveis.
- Podem ter firewall.

ROTEADORES ESTÁTICOS

- Este tipo é mais barato e é focado em escolher sempre o menor caminho para os dados, sem considerar se o caminho tem ou não congestionamento. Configurado manualmente pelo administrador da rede.
-

ROTEADORES DINÂMICOS

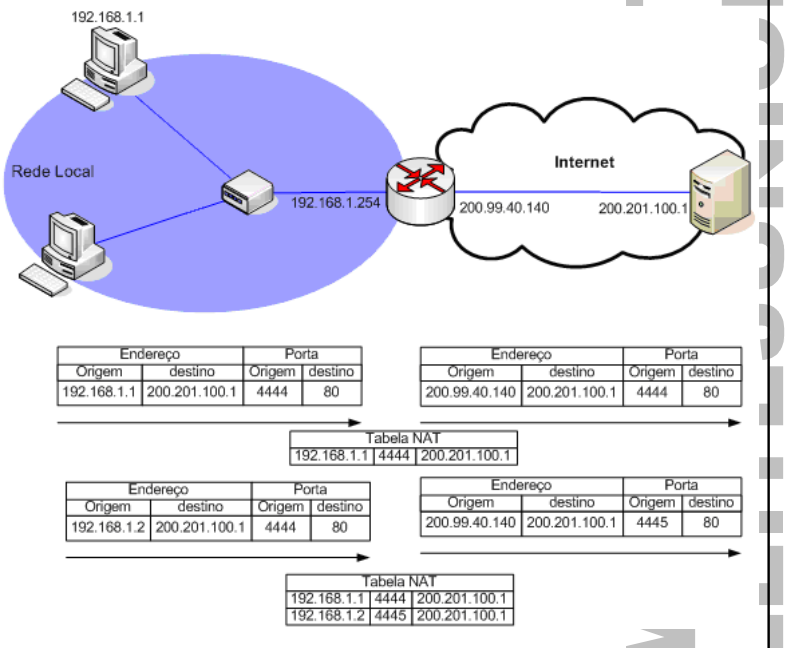
- Mais sofisticado(e conseqüentemente mais caro), considera se há ou não congestionamento na rede. Ele trabalha para fazer o caminho mais rápido, mesmo que seja o caminho mais longo. Não adianta utilizar o menor caminho se esse estiver congestionado. Muitos dos roteadores dinâmicos são capazes de fazer compressão de dados para elevar a taxa de transferência.



- **Use roteador para...**
  - Enviar pacotes diretamente a um computador de destino em outras redes ou segmentos.
  - Reduzir a pressão sobre a rede.
  - Dar velocidade à rede.

NAT - NETWORK ADDRESS TRANSLATION

- Graças a um serviço do roteador chamado NAT, ele realiza uma tradução de endereços IPs privados da rede interna traduzindo-os para um IP válido, que está configurado na interface do roteador conectado a internet.
- Isso é possível porque existe uma faixa de IPs reservados que podem ser usados em uma rede interna.
- Um dos grandes benefícios do NAT é o fato de que a sua rede interna fica escondida da Internet, porque todos os pacotes que irão trafegar pela internet partindo de sua rede interna, terão na verdade como endereço origem, o endereço IP válido da interface de saída do roteador.
- Opera na CAMADA DE REDE (camada 3) do modelo OSI.



Rede usando NAT

SERVIDORES

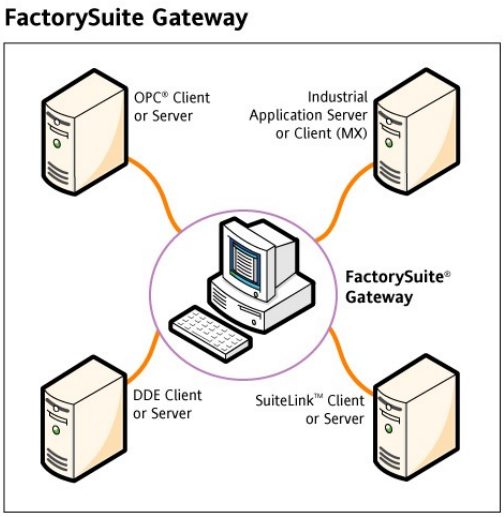
- É um sistema de computação que fornece serviços a uma rede de computadores.
- O termo servidor é largamente aplicado a computadores completos, embora um servidor possa equivaler a um software ou a partes de um sistema computacional, ou até mesmo a uma máquina que não seja necessariamente um computador.
- Os computadores que acessam os serviços de um servidor são chamados clientes.
- As redes que utilizam servidores são do tipo cliente-servidor.

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 de banco de dados:** Servidor que possui e manipula informações contidas em um banco de dados, como, por exemplo, um cadastro de usuários.
- **Servidor DNS:** Servidores responsáveis pela conversão de endereços de sites em endereços IP e vice-versa. DNS é um acrônimo de Domain Name System, ou sistema de nomes de domínios.
- **Servidor Proxy:** Atua como um intermediador entre o usuário e a Internet. Usado para compartilhar uma conexão de Internet com vários computadores.
- **Servidor de imagens:** Tipo especial de servidor de banco de dados, especializado em armazenar imagens digitais.

GATEWAY

- Significa portão de entrada.
- Opera na CAMADA DE TRANSPORTE (gateway de transporte) e APLICAÇÃO (gateway de aplicação) do modelo OSI.
- **GATEWAYS DE TRANSPORTE**: Conectam dois computadores (ou redes) que utilizem diferentes protocolos de transporte orientados a conexão. Exemplo: interligação de uma rede TCP/IP com uma rede ATM(Asynchronous Transfer Mode – Redes de alta velocidade).
- **GATEWAYS DE APLICAÇÃO:** Reconhecem o formato e o conteúdo dos dados e convertem mensagens e um formato para outro. Exemplo: um gateway de correio eletrônico poderia converter mensagens da Internet em mensagens SMS para telefones celulares.
- Habilita a comunicação entre diferentes arquiteturas e ambientes.
- Realiza a conversão dos dados de um ambiente para o outro de modo que cada ambiente seja capaz de entender os dados.
- ROUTER/ROTEADOR e FIREWALL, são exemplos de gateway.
- Um PROXY pode ser interpretado como um gateway, já que serve como intermediador de uma conexão.



O QUE É INTRANET?

- É uma aplicação interna de uma empresa que visa fornecer conteúdo, informação e aplicativos que facilitem o trabalho de seus colaboradores, muitas vezes em grupo ou através de workplaces(locais de trabalho).
- Geralmente uma Intranet é acessada somente por funcionários e seu acesso é restrito de dentro da companhia, não podendo acessar fora de sua rede interna.
- O objetivo é permitir que a Intranet seja utilizada como ferramenta de comunicação e colaboração, refletindo o espírito da empresa em manter a cultura organizacional já existente.
- Uma Intranet é uma rede de computadores privada que assenta sobre a suite de protocolos da Internet(TCP/IP).
- Resumidamente, o conceito de intranet pode ser interpretado como "uma versão privada da Internet", ou uma mini-Internet confinada a uma organização.

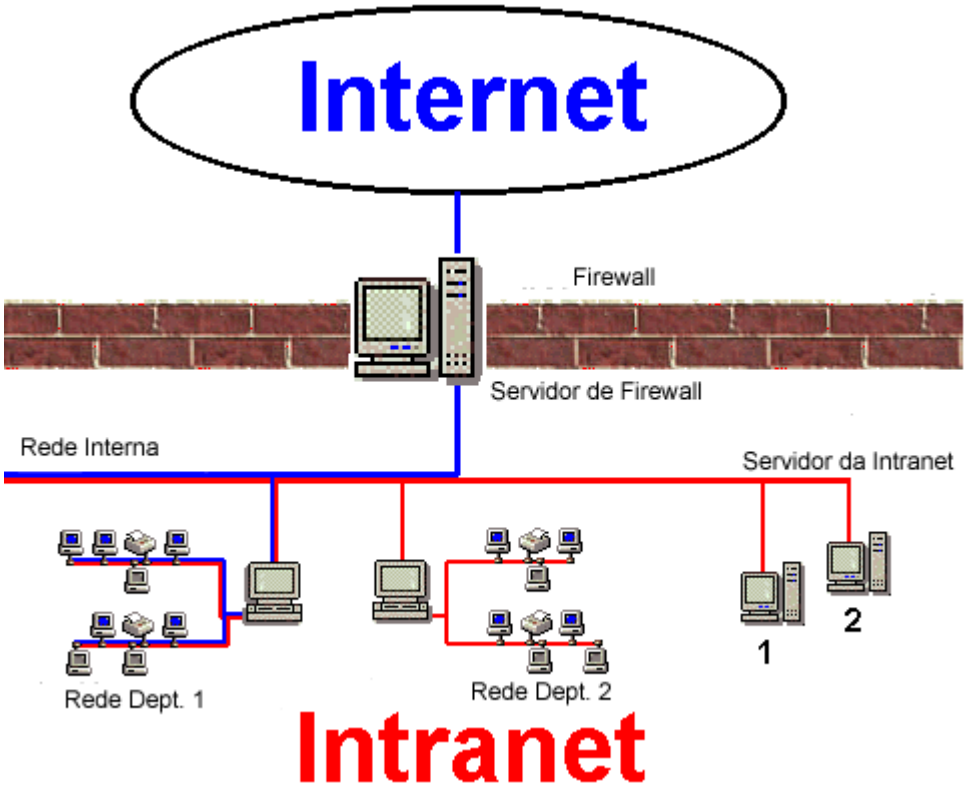
USAMOS UMA INTRANET PARA...

- Módulos para comunidade e colaboração online (blogs, fóruns, enquetes);
- Personalizar informações para colaboradores de cada departamento;
- Atualizar conteúdo por gestores de cada área da empresa;
- Gestão e disseminação do conhecimento unificada (gerenciamento de conteúdo);

CONTEÚDOS USADOS EM UMA INTRANET...

- Conteúdo de recursos humanos como normas e procedimentos;
- Lista de ramais;
- Aniversariantes da semana;
- Informações úteis (dicas de restaurantes, farmácias, etc);
- Cardápio do restaurante;
- E-mail, chat, fóruns, etc;
- Ferramentas de comunicação;
- Compartilhamento de arquivos, dentre outros.

- Uma Intranet também pode ser acessada por parceiros ou por colaboradores remotamente e pode ser chamada de Extranet.

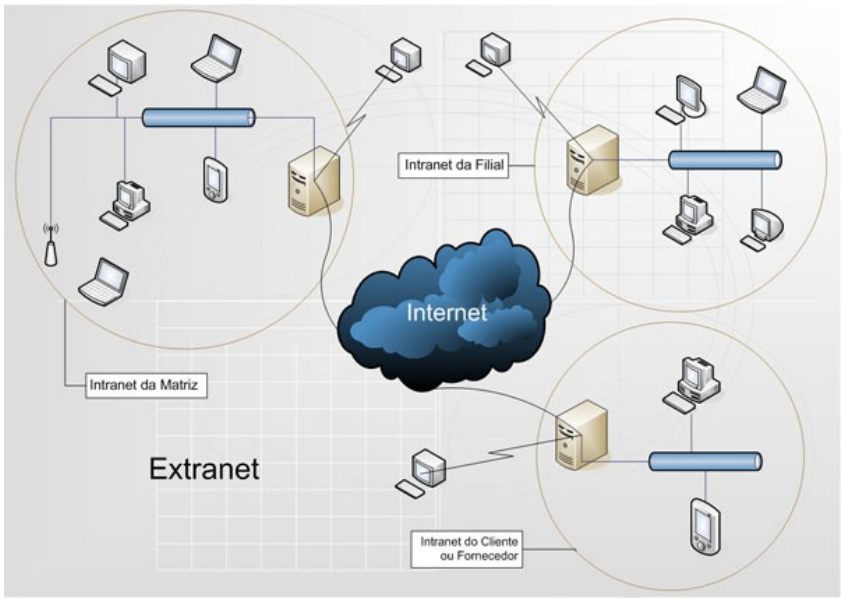


QUE É EXTRANET?

- Uma EXTRANET é uma rede privada, semelhante à uma Intranet, que usa recurso de telecomunicações para permitir acesso remoto, usando os protocolos da Internet.
- O objetivo de uma Extranet é compartilhar com segurança informações de negócio de uma empresa entre seus colaboradores, parceiros e fornecedores.
- Uma Extranet também pode ser vista como uma extensão de uma Intranet.

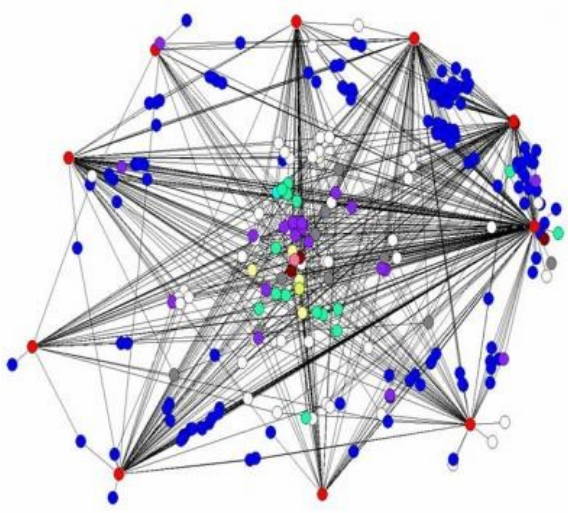
USAMOS UMA EXTRANET PARA...

- Trocar grandes volumes de dados usando Electronic Data Interchange (EDI);
- Compartilhar catálogos de produtos com parceiros e representantes;
- Colaborar com outras empresas na junção de esforços de desenvolvimento;
- Uso compartilhado de programas de treinamento com outras empresas;
- Fornecer acesso a serviços para outras companhias;
- Compartilhar notícias e informações interessantes com parceiros.



A INTERNET

- Maior conjunto de redes interligadas do Mundo.
- Não é uma rede e sim, um conjunto de várias redes ligadas por roteadores baseada na pilha de protocolos TCP/IP.
- Nasceu em 1970 com um projeto de defesa dos EUA.
- No Brasil, chegou no final da década de 80, incentivada pela RNP – Rede Nacional de Ensino e Pesquisa.
- Embratel e RNP são alguns BACKBONEs no Brasil.



BACKBONE

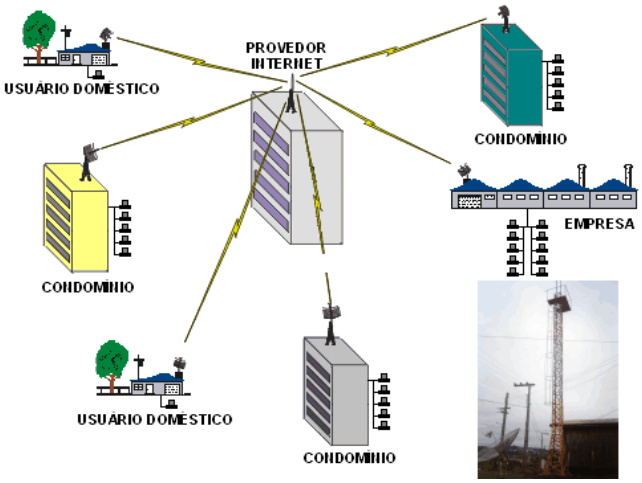
- Significa, espinha dorsal.
- São áreas de alta velocidade interligando grandes empresas de telecomunicações pelo mundo.

RNP - REDE NACIONAL DE ENSINO E PESQUISA

- Criada pelo Ministério da Ciência e Tecnologia para interligar o ambiente acadêmico brasileiro, tanto em nível nacional como internacional.

PROVEDOR DE ACESSO

- Para conectar a Internet é necessário se conectar a uma estrutura de rede que a compõe.
- **O PROVEDOR** é a empresa que permite esse tipo de conectividade, conectando-se diretamente a um BACKBONE.



TIPOS DE CONEXÃO

- Existem várias formas de conectar a Internet usando velocidades diferenciadas. Vejamos algumas abaixo:

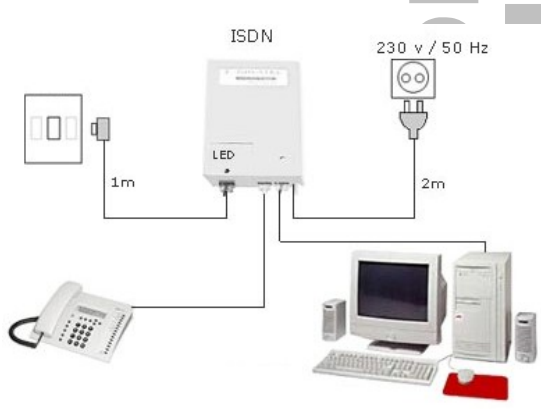
DIAL-UP / DISCADA

- Utiliza um modem(V.90) e uma linha telefônica para se ligar a um nó de uma rede de computadores do ISP(Internet Service Provider/Fornecedor de Acesso a Internet).
- A partir desse momento, o ISP se encarrega de fazer o routing para a Internet.
- Velocidade da conexão de no máximo de 56Kbps(7KB/s), muito baixa para os dias de hoje.
- Utiliza o protocolos SLIP e PPP da rede de telefonia.
- O PPP (ponto a ponto) é um protocolo da camada de enlace usada pelas redes de telefonia.
- Custo variado, pois depende do tempo que se mantém conectado.


Discador, Placa de Fax/Modem e Modem

ISDN / RDSI

- Significa, Rede Digital de Serviços Integrados.
- Utiliza 3 canais de comunicação diferentes.
- Dois canais de 64 Kbps cada ou 128 Kbps (juntos) para transmissão de dados e um canal de 16 Kbps para transferência de sinais de controle.
- Os dois canais são duas linhas que podem ser usadas e conjunto ou separada transmitindo dados e voz.



Esquema ISDN

ADSL - BANDA LARGA

- Significa, ASYMMETRIC DIGITAL SUBSCRIBER LINE – Linha de Assinante Assíncrona Digital.
- Utiliza linha telefônica para transmissão de dados em alta velocidade, separando voz e dados.
- Um Modem ADSL é usado para estabelecer a conexão entre o usuário e a central telefônica.
- Pode ser conectado ao computador usando uma porta USB ou RJ-45 da placa de rede.
- Velocidade de download(baixar) podem ir de 256 Kbps(32 KB/s)a 6 Mbps(0,75 MB/s).
- Velocidade de upload(subir) podem ir de 16 Kbps(2 KB/s) a 640 Kbps(80 KB/s).
- Para separar voz de dados na linha telefônica é instalado na linha do usuário um pequeno aparelho chamado SPLITTER.
- Caminho da informação: central telefônica > roteador > Provedor > Internet.
- Os dados vão para um equipamento chamado DSLAM (Digital Subscriber Line Access Multiplexer), que limita a velocidade do usuário e uni várias linhas ADSL.
- O sinal é enviado para uma linha ATM (Asynchronous Transfer Mode) de alta velocidade que está conectada à internet.
- Utiliza o protocolo PPPoE (Point-to-Point over Ethernet - RFC 2516) que emula uma ligação telefônica usando uma rede local.
- RFC (Request for Comments). É um documento que descreve os padrões de cada protocolo da Internet.
- Custo fixo, mesmo usando 24x7(24 horas por 7 dias).

Modem ADSL

REDE ELÉTRICA / BPL / PLC

- BPL - Broadband over Power Lines, ou PLC - Power Line Communications é nada mais que a injeção de sinais de alta frequência na fiação elétrica para transmitir dados e voz em banda larga pela rede de energia elétrica, utiizando uma infra-estrutura já disponível, não necessitando de obras em uma edificação para ser implantada.
- Os sinais de Internet são transmitidos pela rede elétrica usando uma frequência diferente, entre 30 e 91,7 MHz, contra os 50 e 60 Hz da rede elétrica.
- A conexão com o computador concretiza-se por um modem ligado diretamente na tomada.
- Este tipo de internet de alta velocidade já vem sendo pesquisada a anos, e agora está saindo da fase de testes e passando para a comercialização.
- O sistema já existe e foi regulamentado no dia 13 de abril de 2009 pela Anatel-Agência Nacional de Telecomunicações. Em agosto de 2009 a ANEEL-Agência Nacional de Energia Elétrica aprovou e regulamentou a tecnologia.

VELOCIDADE

- Nos testes realizados em prédios do bairro de Moema na zona sul de São Paulo pela AES Telecom, empresa da Eletropaulo, permitiram chegar a 80 mbps por edifício.
- A distribuição da banda será de acordo com a demanda de cada usuário.
- A velocidade mínima para essa internet é de 20mbps, para cada transformador na rua.
- Cada transformador terá capacidade para distribuir a internet para 50 casas, ou seja, se 50 casas estiverem utilizando a internet em simultâneo, a velocidade cai para 50 kbps por casa, isso se equivale a uma internet discada.

PREÇO

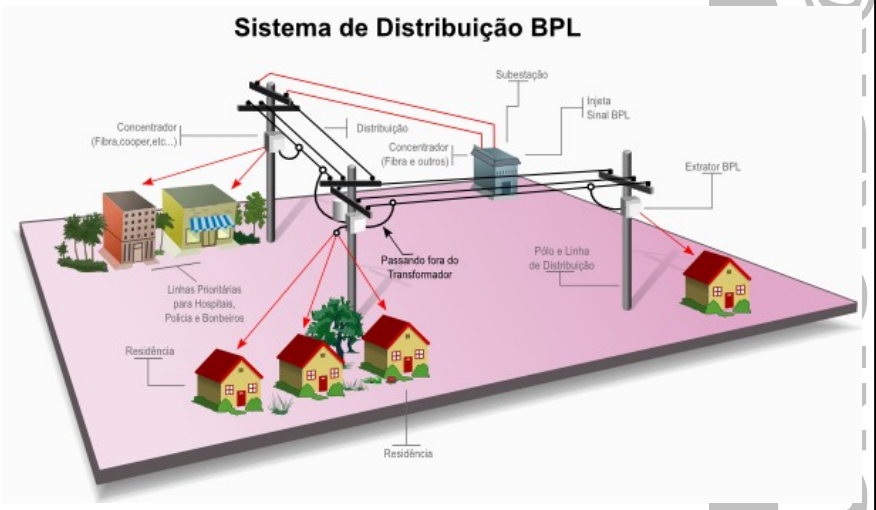
- Os modems custam cerca de R$3 mil cada um, mas, deverão baratear de acordo com que a demanda aumenta.
- Segundo dados iniciais, a internet por rede elétrica custará cerca de 50% mais barato do que as tecnologias em internet hoje em dia.

INTERFERÊNCIA

- Aparelhos como liquidificador, micro-ondas, secador de cabelos, etc, podem causar interferências que geram uma diminuição na velocidade da conexão.

DISTRIBUIÇÃO

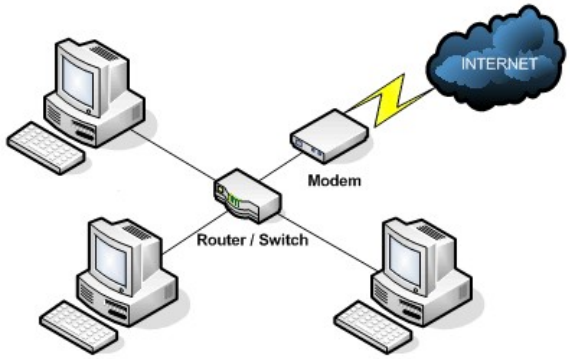
- No início ocorrerá a distribuição principalmente a edifícios e condomínios, pelo alto custo que é de adquirir e instalar os equipamentos necessários para a distribuição.



LAN – REDE LOCAL

- É uma forma de ligar vários computadores, em uma LAN, a uma única conexão com a Internet.
- Pode ser ADSL, Cabo ou Dial Up.
- Conecta-se a LAN a um roteador e este permanece ligado ao provedor de acesso, que fornecerá apenas um endereço IP para a rede toda, sendo intermediado pelo roteador.

NAT (Network Address Translation - Tradução de Endereços de Rede) é um protocolo, localizado no Gateway da rede que permite que vários computadores, com endereços IP válidos internamente, possam acessar a Internet por meio de um único endereço IP válido.



Rede LAN.

TV A CABO

- Utiliza as redes de transmissão de TV por cabo convencionais (chamadas de CATV - Community Antenna Television) para transmitir dados em alta velocidade.
- As velocidades variam de 256 Kbps(32 KB/s) a 30 Mbps(3,75 MB/s), fazendo uso da porção de banda não utilizada pela TV a cabo.
- Utiliza um modem especial chamado CABLE MODEM.
- Pode ser conectado usando uma placa de rede Ethernet ou porta USB.

Cable Modem

CONEXÃO 3G

- É a terceira geração de padrões e tecnologias de telefonia móvel, substituindo o 2G.
- Permitem a telefonia por voz e a transmissão de dados a longas distâncias, tudo em um ambiente móvel.
- Normalmente, são fornecidos serviços com taxas de 5 a 10 Megabits por segundo.

Celular, Modem e Cartão

DOMÍNIO DE INTERNET

- São nomes que respeitam regras hierárquicas de posicionamento mundial.
- Temos como exemplo **www.leitejunior.com.br.**
- Para interpretar o domínio temos que entender os níveis de domínio.

DOMÍNIO GEOGRÁFICO – 1º. NÍVEL

- O .br informa o país onde o domínio foi registrado. No caso, Brasil.
- Existem outros representações de domínio espalhada pelo planeta, como .pt(Portugal), .it(Itália), .fr(França), etc.
- Quando o domínio não possui esta representação podemos afirmar que o domínio foi registrado na estrutura dos Estados Unidos ou podemos dizer que é um domínio Internacional.

DOMINIO DE TIPO – 2º. NÍVEL

- Identifica a classe a que pertence o domínio.
- O mais tradicional é o .com(comercial).
- Existe também o .gov(governamental), .edu(educacional), .org(organizacional), etc.

DOMINIO DE INSTITUIÇÃO – 3º. NÍVEL

- Identifica o nome da entidade.
- No caso, leitejunior.

ONDE REGISTRAR UM DOMÍNIO

- Existe um site, o www.registro.br, que permite fazer o cadastro ou consulta de domínios brasileiros.

URL – UNIFORM RESOURCE LOCATOR

- É o endereço único de um conteúdo na web.
- Temos como exemplo http://www.leitejunior.com.br/forum/default.asp
- O endereço representa o PROTOCOLO://DOMÍNIO/PASTA/ARQUIVO.

PROTOCOLOS

- Conjunto de regras com o objetivo de permitir a comunicação entre computadores.
- Regras que governam a transmissão de dados, incluindo inicialização, verificação, coleta de dados, endereçamento e correção de erros.

MODELO DE CAMADA OSI E TCP/IP

- **OSI** - Open Systems Interconnection - Interconexão de Sistemas Abertos.
- **ISO -** International Organization for Standardization.

- **TCP/IP** – É um conjunto de protocolos de comunicação usado na Internet. É formado pelo nome dos dois protocolos mais importantes da Internet. O TCP-Transmission Control Protocol e o IP-Internet Protocol.

- Usado para facilitar o processo de padronização e obter interconectividade entre máquinas de diferentes sistemas operativos.
- Esse modelo serve de base para qualquer tipo de rede, seja de curta, média ou de longa distância.

CAMADAS OSI	PROTOCOLOS	TCP/IP
7 - APLICAÇÃO	HTTP, IRC, SNMP, POP3, IMAP, SMTP, FTP, TELNET	5 – APLICAÇÃO
6 - APRESENTAÇÃO		
5 - SESSÃO		
4 - TRANSPORTE	TCP e UDP	4 – TRANSPORTE
3 – REDE	IPv4, IPv6, roteador, ICMP, ARP, RARP, RIP, OSPF	3 – REDE
2 - LIGAÇÃO DE DADOS (ENLACE)	Switch, CSMA/CD, CSMA/CA, Ethernet, IEEE 802.11, Token Ring	2 - LIGAÇÃO DE DADOS (ENLACE)
1 – FÍSICA	HUB, cabos UTP, Coaxial, Fibra Óptica, repetidores, ondas de RF	1 - FÍSICA

CAMADA 1 - FÍSICA

- Esta camada está diretamente ligada ao equipamento de cabeamento ou outro canal de comunicação e é aquela que se comunica diretamente com o controlador da interface de rede.
- Define as características elétricas e mecânicas do meio, taxa de transferência dos bits, voltagens, etc...
- Move bits através de um meio físico (elétrico, luminoso ou eletromagnético).
- Confirmação e retransmissão de frames.

DISPOSITIVOS DA CAMADA

HUB, cabo par-trançado, conectores (RJ-45 e BNC), cabo de fibra óptica, cabo coaxial, repetidores, ondas de rádio frequência, infravermelho.

CAMADA 2 - LIGAÇÃO DE DADOS (ENLACE)

- Protocolos e equipamentos podem manipular o dado bruto dando a ele algum significado.
- Pega os dados recebidos da camada de Rede e os transforma em quadros (frames) que serão trafegados pela rede adicionando informações como o endereço da placa de rede de origem o endereço da placa de rede de destino.
- Camada que detecta e corrige erros que possam acontecer no nível físico (colisões).
- Responsável pela transmissão e recepção de quadros e pelo controle de fluxo.
- Estabelece um protocolo de comunicação entre sistemas diretamente conectados.

DISPOSITIVOS DA CAMADA

Switch, pontes, protocolos CSMA/CD e CSMA/CA, diversas tecnologias de redes, como, Ethernet, IEEE 802.11, Token Ring, ATM, FDDI.

CAMADA 3 - REDE

- É responsável pelo endereçamento dos quadros (frames) entre uma origem e um destino, independentes do ambiente de redes em que eles se encontram.
- Movimenta pacotes a partir de sua fonte original até seu destino através de um ou mais enlaces.
- Não se preocupa com a ordenação dos quadros (frames) nem com o controle do fluxo. Onde, o primeiro a sair (origem) pode ser o quinto a chegar (destino).
- Os protocolos dessa camada têm a função de encontrar a melhor rota para entrega dos quadros (frames).
- Utiliza o endereço IP que tem a função de localizar as máquinas da origem e destino, mesmo que as máquinas estejam em redes diferentes.

DISPOSITIVOS DA CAMADA

Roteador , endereço IP, ICMP, ARP, RARP.

IP -INTERNET PROTOCOL

- É o mais importante da pilha TCP/IP, tendo duas funções, rotear mensagens entre uma origem e destino e endereçar estações.
- Manipula pequenas unidades de informação chamadas de pacotes ou datagramas IP.
- O datagrama contém o endereço do remetente e do destinatário, o tempo de vida (TTL-Time To Live), o protocolo de transporte, etc.
- É um protocolo **não orientado a conexão**, pois o emissor não tem a garantia de que o datagrama chegará o destino.

- É um endereço numérico, único, que identifica qualquer equipamento ou conexão realizada em uma interconexão de redes.
- É formado por números binários(bits) representados em uma notação decimal.
- Endereço IP em representação decimal: 200.249.65.130
- São usados números que podem variar de 0 a 255.
- Endereço IP em representação binária: 11101010.10101001.11110000.11010111. A cada bloco de 8 bits é colocado um ponto para facilitar a visualização. Internamente esse ponto não existe.
- Pode-se dizer que o IP é formado por 4 bytes ou 4 octetos ou 32 bits.

- **IP Fixo:** Configurado diretamente no computador pelo usuário ou administrado da rede. Normalmente, usado em servidores ou quando se quer identificar de forma direta um computador.
- **IP Dinâmico:** Configurado para ser recebido automaticamente por um computador quando este se conecta a rede. O IP Dinâmico é fornecido por um servidor que usa o protocolo DHCP(Dynamic Host Configuration Protocol).

- **Versão IPv4:** Versão usada atualmente, formada por 4 bytes (4 octetos ou 32 bits).
- **Versão IPv6:** Usa endereços com 16 bytes(16 octetos ou 128 bits). Pode ser representado em hexadecimal. Criado para substituir o IPv4, pois, a quantidade de IPv4 que existe está se esgotando.

ICMP - INTERNET CONTROL MESSAGE PROTOCOL

- Utilizado para enviar mensagens de controle entre uma origem e um destino, retornando valores dessas mensagens.
- As mensagens ICMP geralmente são enviadas automaticamente em uma das seguintes situações:
  - Um pacote IP não consegue chegar ao seu destino (tempo de vida do pacote expirado).
  - O Gateway não consegue retransmitir os pacotes na frequência adequada (Gateway congestionado.
  - O Roteador indica uma rota melhor para a máquina a enviar pacotes.

- Digitando o comando **PING www.leitejunior.com.br** no "prompt de comando" do Windows, temos.

```
F:\Documents and Settings\Usuario>ping www.leitejunior.com.br

Disparando contra www.leitejunior.com.br [189.38.80.53] com 32 bytes de dados:

Resposta de 189.38.80.53: bytes=32 tempo=2030ms TTL=103
Resposta de 189.38.80.53: bytes=32 tempo=1219ms TTL=103
Resposta de 189.38.80.53: bytes=32 tempo=1175ms TTL=103
Resposta de 189.38.80.53: bytes=32 tempo=1501ms TTL=103

Estatísticas do Ping para 189.38.80.53:
    Pacotes: Enviados = 4, Recebidos = 4, Perdidos = 0 (0% de perda),
Aproximar um número redondo de vezes em milissegundos:
    Mínimo = 1175ms, Máximo = 2030ms, Média = 1481ms

F:\Documents and Settings\Usuario>
F:\Documents and Settings\Usuario>
```

ARP – ADDRESS RESOLUTION PROTOCOL

- Permite associar um endereço IP a um endereço MAC.
- É usado somente na rede local.
- A estação manda um pacote de broadcast (chamado "ARP Request"), contendo o endereço IP do host destino e ele responde com seu endereço MAC.

- Digitando o comando **ARP -a** no "prompt de comando" do Windows, temos.

```
F:\Documents and Settings\Usuario>arp -a

Interface: 192.168.1.6 --- 0x2
  Endereço IP           Endereço físico       Tipo
  192.168.1.1           00-0f-a3-27-60-1b     dinâmico
```

RARP - REVERSE ARP

- Faz o processo inverso do ARP, permite associar um endereço MAC a um endereço IP.
- Os dispositivos que usam o RARP exigem que haja um servidor RARP presente na rede para responder às solicitações RARP.
- O DHCP utiliza RARP. Ao receber o pacote de broadcast enviado por uma estação, o servidor DHCP sabe apenas o endereço MAC da estação e não seu endereço IP. Ele é capaz de responder à solicitação graças ao RARP. Sem ele, não teríamos DHCP.

CAMADA 4 - TRANSPORTE

- Realiza comunicação, confiável ou não, entre a origem e o destino, garantindo ou não o fluxo dos pacotes.
- Recebe os dados da camada superior e os divide, entregando a camada de rede.

TCP - TRANSMISSION CONTROL PROTOCOL

- Significa, Protocolo de Controle de Transmissão.
- É um dos protocolos sob os quais assenta o núcleo da Internet nos dias de hoje.
- Verifica se os dados são enviados de forma correta, na sequência apropriada e sem erros.
- Recebe as mensagens dos protocolos acima dele e divide em pacotes identificando a origem e o destino.
- **Orientado à conexão** - a aplicação envia um pedido de conexão para o destino e usa a "conexão" para transferir dados.
- **Confiabilidade** - usa várias técnicas para proporcionar uma entrega confiável dos pacotes de dados. Corrigindo a falta de um determinado pacote, a entrega fora de ordem e duplicidade.

UDP - USER DATAGRAM PROTOCOL

- Significa, Protocolo de Datagramas de Usuário.
- A entrega não é confiável, pois, os pacotes podem ser entregues fora de ordem ou até perdidos.
- Não é orientado à conexão.
- Feito para transmitir dados pouco sensíveis, como streaming de áudio e vídeo.

CAMADA 5 - 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 sendo transmitidos. Se por ventura a rede falhar, os computadores reiniciam a transmissão dos dados a partir da última marcação recebida pelo computador receptor.
- O LOGON (informação de usuário e senha) em um sistema é um exemplo de início de uma sessão.

CAMADA 6 - APRESENTAÇÃO

- Esta camada formata e encripta os dados para serem transmitidos através da rede, evitando problemas de compatibilidade.
- Às vezes é chamada de camada de Tradução.

CAMADA 7 - APLICAÇÃO

- Faz a interface entre o protocolo de comunicação e o aplicativo que o solicitou.
- Permite que o usuário possa interagir com os recursos do sistema. Acesso a email, navegação na Internet, bate papo, transferência de arquivos, etc.

PORTAS DE COMUNICAÇÃO

- Cada protocolo desta camada utiliza uma porta TCP/UDP para transmissão e recepção dos dados.
- Ao todo são 65.536 portas TCP/UDP, mas, usamos apenas 1024 portas TCP/UDP.
- As portas TCP mais usadas podem ser chamadas de "WELL KNOWN PORTS".

HTTP – HYPER TEXT TRANSFER PROTOCOL

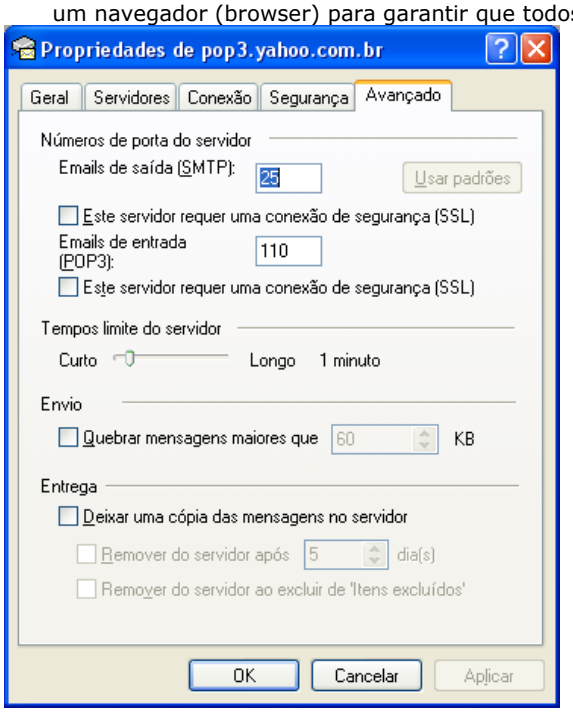
- Significa, Protocolo de Transferência de Hipertexto.
- Utiliza a porta 80 do TCP.
- Realiza a transferência de páginas na World Wide Web(WWW).
- Utiliza a linguagem HTML(Hipertext Markup Language), linguagem básica de construção de página web. Transferindo as páginas do servidor para a máquina do usuário utilizando um navegador(browser).

HTTPS – HYPER TEXT TRANSFER PROTOCOL SECURE

- Significa, Protocolo de Transferência de Hipertexto com Segurança(criptografado).
- Utiliza a porta 443 do TCP.
- Utiliza recursos de criptografia para efetuar a transferência dos dados, utilizado um protocolo de segurança SSL (Secure Sockets Layer).
- Não é 100% seguro, não evita a interceptação dos dados, mas, dificulta a legibilidade dos dados.

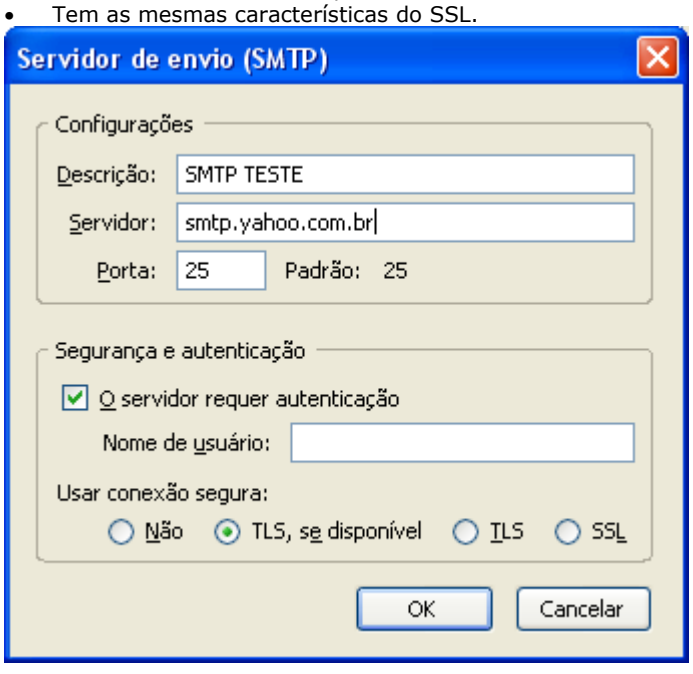
SSL - SECURE SOCKETS LAYER

- Significa, Camada de Ligação(cliente/servidor) Segura.
- É um padrão global em tecnologia de segurança que cria um canal criptografado entre um servidor web e um navegador (browser) para garantir que todos os dados transmitidos sejam sigilosos e seguros.



TLS - TRANSPORT LAYER SECURITY

- Significa, Camada de Transporte Segura.
- É uma versão mais atual que a do SSL.
- Tem as mesmas características do SSL.



DHCP - DYNAMIC HOST CONFIGURATION PROTOCOL

- Significa, Protocolo de Configuração Dinâmica de Host.
- Utiliza a porta 546 (cliente) e 547 (servidor) do TCP/UDP.
- Oferece configuração dinâmica de host(computadores), com concessão de endereços IP e outros parâmetros de configuração (máscara, gateway, etc)

IRC - INTERNET RELAY CHAT

- Significa, Protocolo de Mensagem Instantânea (bate-papo).
- Utiliza a porta 6667 do TCP.
- Utilizado basicamente como bate-papo (chat) e troca de arquivos, permitindo a conversa em grupo ou privada, sendo o antecessor dos mensageiros instantâneos atuais.
- No sistema operativo Windows, o mais famoso é o mIRC.

SNMP - SIMPLE NETWORK MANAGEMENT PROTOCOL

- Significa, Protocolo de Gerenciamento Simples de Redes.
- Utiliza a porta 161 do UDP.
- Facilita o intercâmbio de informação entre os dispositivos de rede.
- Possibilita aos administradores de rede gerir o desempenho da rede, encontrar e resolver problemas de rede, e planejar o seu crescimento.

POP - POST OFFICE PROTOCOL

- Significa, Protocolo de Postagem de Documentos.
- Utiliza a porta 110 do TCP.
- O POP3 é a versão mais utilizada.
- Permite que todas as mensagens contidas numa caixa de correio eletrônico sejam transferidas para um computador local, retirando as mensagens do servidor.
- Existem configurações que permitem deixar uma cópia da mensagem no servidor.

IMAP - INTERNET MESSAGE ACCESS PROTOCOL

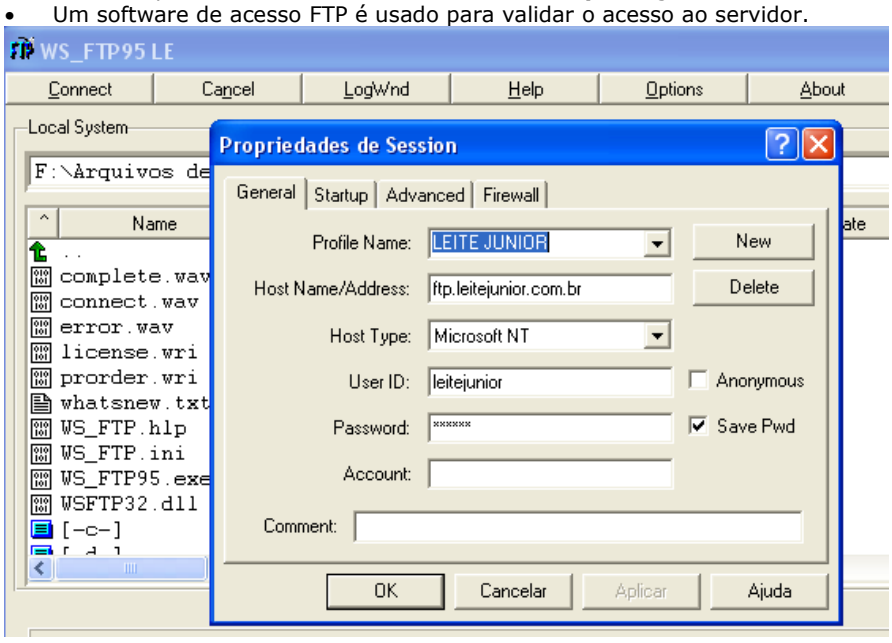
- Significa, Protocolo de Acesso a Mensagens na Internet.
- Utiliza a porta 143 do TCP.
- É um protocolo de gerenciamento de correio eletrônico superior em recursos ao POP3.
- A última versão é o IMAP4.
- As mensagens ficam armazenadas no servidor e o internauta pode ter acesso a suas pastas e mensagens em qualquer computador, tanto por webmail como por cliente de correio eletrônico.
- Outra vantagem deste protocolo é o compartilhamento de caixas postais.

SMTP - SIMPLE MAIL TRANSFER PROTOCOL

- Significa, Protocolo de Transferência Simples de Email.
- É responsável pelo envio de e-mail através da Internet.
- Utiliza a porta 25 do TCP.

FTP - FILE TRANSFER PROTOCOL

- Significa, Protocolo de Transferência de Arquivos.
- Utiliza a porta 20 do TCP para transferência de dados, transparente para o usuário.
- Utiliza a porta 21 do TCP para transferência de informações de autenticação (login, senha, etc).
- Usado para transferir arquivos entre sistemas. Normalmente transferimos arquivos grandes.
- Um exemplo de um servidor de transferência é **ftp.leitejunior.com.br**.
- Um software de acesso FTP é usado para validar o acesso ao servidor.



TFTP – TRIVIAL FILE TRANSFER PROTOCOL

- É uma versão simplificada do FTP, que utiliza portas UDP para a transferência dos dados e não inclui suporte à correção de erros.
- Utiliza a porta 69 do UDP.
- Ele pode ser usado para transferência de arquivos em geral, sendo mais usado em sistemas de boot remoto, como, BIOS de placa de rede, permitindo que o sistema operacional seja carregado diretamente através da rede, sem precisar de um HD ou outra unidade de armazenamento.

TELNET - TERMINAL EMULATOR

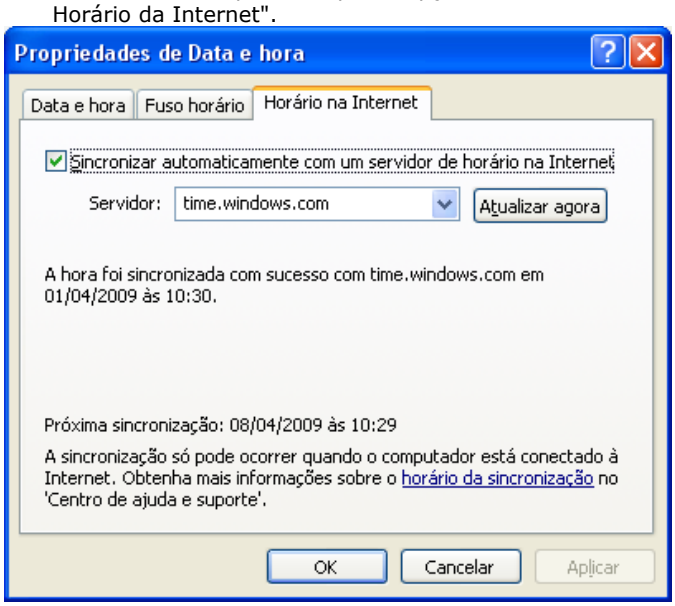
- Significa, Emulador de Terminal.
- Utiliza a porta 23 do TCP.
- É um protocolo cliente/servidor que permite que um computador possa ser um terminal do outro. Permitindo acesso remoto a esse computador.
- Utiliza comando de texto puro, facilitando a captura dos dados transmitidos.
- Este protocolo vem sendo gradualmente substituído pelo SSH.

SSH - SECURE SHELL

- Significa, Interface Segura.
- Utiliza a porta 22 do TCP.
- Possui as mesmas funcionalidades do TELNET, com a vantagem da conexão entre o cliente e o servidor ser criptografada.

NTP – NETWORK TIME PROTOCOL

- Significa, Protocolo de Tempo de Rede.
- Utiliza a porta 123 do UDP.
- Usado para sincronizar o relógio do sistema em relação a outras máquinas da rede ou da Internet.
- No Windows XP, por exemplo, a opção de usar o NTP está disponível no "Painel de Controle / Data e hora / Horário da Internet".



NNTP – NETWORK NEWS TRANSFER PROTOCOL

- Significa, Protocolo de Transferência de Notícias na Rede.
- Utiliza a porta 119 do TCP.
- Usado no serviço de News, reunindo vários usuários de grupos de notícias (newsgroup).
- Podendo ser configurado em clientes de email como o Outlook Express.

DNS – DOMAIN NAME SERVICE

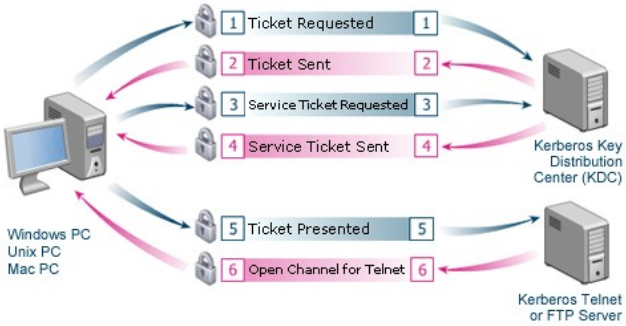
- Significa, Serviço de Nome de Domínio.
- Utiliza a porta 53 do UDP.
- Usado para traduzir nomes de domínios (URL - Uniform Resource Locator) em endereço IP.
- Ao digitar www.leitejunior.com.br o endereço é enviado ao servidor de DNS que efetua a troca do referido endereço pelo respectivo IP.

KERBEROS

- Utiliza a porta 88 do TCP.
- Criado pelo MIT (Massachusetts Institute of Technology), no meado dos anos 80.
- Recebeu este nome devido a um cachorro da mitologia grega que possuía três cabeças e rabo de serpente, que vigiava os portões de Hades, tendo como sua principal missão evitar a entrada de pessoas ou de coisas indesejáveis.

- Nome dado ao serviço de autenticação do projeto Athena por ele estar baseado em três servidores, e possuir uma função de defesa que só permite a entrada de clientes autorizados.
- Utiliza uma **CRIPTOGRAFIA SIMÉTRICA** para segurança dos dados.

- Necessita de três servidores para que possa fazer a autenticação com mais segurança:
- **- Servidor de Autenticação (SA)**
- Responsável pela autenticação em si do usuário, pois a partir de um pedido a este servidor, ele receberá um ticket e uma chave de sessão, podendo assim continuar tentando se conectar com o sistema.
- **- Servidor de Concessão de Ticket (TGS)**
- Como o nome já d iz, é o responsável pela concessão dos tickets para os serviços que utilizam o Kerberos.
- **- Servidor de Administração (KADM)**
- Responsável pelo controle das chaves secretas, cadastrando-as tanto no cliente quanto no servidor. Para isso o usuário precisa fazer o seu cadastramento, escolhendo um username e uma senha.



- Primeiramente são registrados no banco de dados do servidor Kerberos a chave secreta dos clientes e também a chave secreta dos serviços. Este registro é feito pelo servidor de Administração, como foi falado anteriormente.
- Para que possa haver a autenticação do usuário no protocolo Kerberos, este entra com o seu identificador (username) e a sua senha, a qual sofrerá um processo criptográfico e se tornará a sua chave secreta.
- Esta chave secreta será comparada com aquela chave secreta que foi cadastrada no banco de dados para este username, em caso de confirmação, o usuário pode prosseguir com o processo de autenticação, caso contrario ele é expulso do sistema, e tem que estabelecer uma nova conexão. Com a confirmação do cliente é gerada uma chave de sessão.

VPN – VIRTUAL PRIVATE NETWORK

- O uso de Redes Privadas Virtuais racionaliza os custos de redes corporativas oferecendo "confidencialidade" e integridade no transporte de informações através de redes públicas.

INTRODUÇÃO

Utilizar uma rede pública como a Internet em vez de linhas privativas para implementar redes corporativas é denominada de Virtual Private Network (VPN) ou Rede Privada Virtual.

As VPNs são túneis de criptografia entre pontos autorizados, criados através da Internet ou outras redes públicas e/ou privadas para transferência de informações, de modo seguro, entre redes corporativas ou usuários remotos.

A segurança é a primeira e mais importante função da VPN. Uma vez que dados privados serão transmitidos pela Internet, que é um meio de transmissão inseguro, eles devem ser protegidos de forma a não permitir que sejam modificados ou interceptados.

Outro serviço oferecido pelas VPNs é a conexão entre corporações (Extranets) através da Internet, além de possibilitar conexões dial-up criptografadas que podem ser muito úteis para usuários móveis ou remotos, bem como filiais distantes de uma empresa.

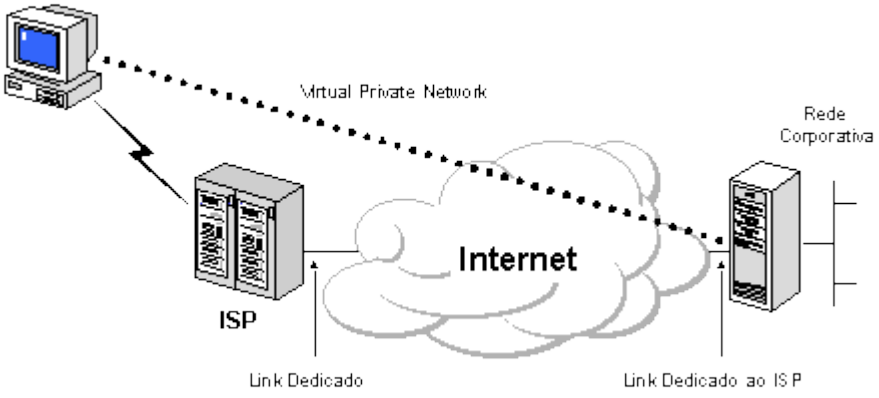
Uma das grandes vantagens decorrentes do uso das VPNs é a redução de custos com comunicações corporativas, pois elimina a necessidade de links dedicados de longa distância que podem ser substituídos pela Internet.

As LANs podem, através de links dedicados ou discados, conectar-se a algum provedor de acesso local e interligar-se a outras LANs, possibilitando o fluxo de dados através da Internet.

Outro fator que simplifica a operacionalização da WAN é que a conexão LAN-Internet-LAN fica parcialmente a cargo dos provedores de acesso.

ACESSO REMOTO VIA INTERNET

O acesso remoto a redes corporativas através da Internet pode ser viabilizado com a VPN através da ligação local a algum provedor de acesso (Internet Service Provider - ISP). A estação remota disca para o provedor de acesso, conectando-se à Internet e o software de VPN cria uma rede virtual privada entre o usuário remoto e o servidor de VPN corporativo através da Internet.



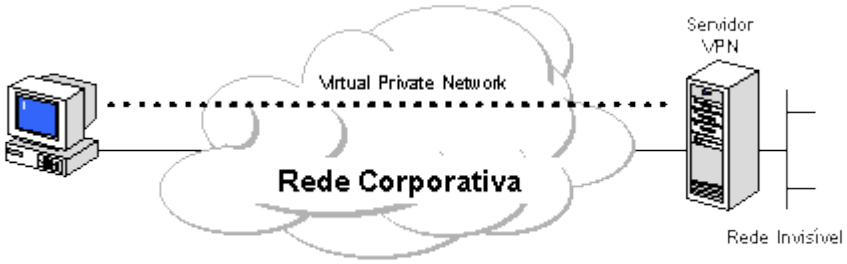
CONEXÃO DE COMPUTADORES NUMA INTRANET

Em algumas organizações, existem dados confidenciais cujo acesso é restrito a um pequeno grupo de usuários. Nestas situações, redes locais departamentais são implementadas fisicamente separadas da LAN corporativa. Esta solução, apesar de garantir a "confidencialidade" das informações, cria dificuldades de acesso a dados da rede corporativa por parte dos departamentos isolados.

As VPNs possibilitam a conexão física entre redes locais, restringindo acessos indesejados através da inserção de um servidor VPN entre elas.

Observe que o servidor VPN não irá atuar como um roteador entre a rede departamental e o resto da rede corporativa uma vez que o roteador possibilitaria a conexão entre as duas redes permitindo o acesso de qualquer usuário à rede departamental sensitiva. Com o uso da VPN o administrador da rede pode definir quais usuários estarão credenciados a atravessar o servidor VPN e acessar os recursos da rede departamental restrita.

Adicionalmente, toda comunicação ao longo da VPN pode ser criptografada assegurando a "confidencialidade" das informações. Os demais usuários não credenciados sequer enxergarão a rede departamental.



REQUISITOS BÁSICOS

A VPN deve dispor de recursos para permitir o acesso de clientes remotos autorizados aos recursos da LAN corporativa, viabilizar a interconexão de LANs de forma a possibilitar o acesso de filiais, compartilhando recursos e informações e, finalmente, assegurar privacidade e integridade de dados ao atravessar a Internet bem como a própria rede corporativa.

A seguir são enumeradas características mínimas desejáveis numa VPN:

- **AUTENTICAÇÃO DE USUÁRIOS**

Verificação da identidade do usuário, restringindo o acesso às pessoas autorizadas. Deve dispor de mecanismos de auditoria, provendo informações referentes aos acessos efetuados - quem acessou, o quê e quando foi acessado.

- **GERENCIAMENTO DE ENDEREÇO**

O endereço do cliente na sua rede privada não deve ser divulgado, devendo-se adotar endereços fictícios para o tráfego externo.

- **CRIPTOGRAFIA DE DADOS**

Os dados devem trafegar na rede pública ou privada num formato cifrado e, caso sejam interceptados por usuários não autorizados, não deverão ser decodificados, garantindo a privacidade da informação. O reconhecimento do conteúdo das mensagens deve ser exclusivo dos usuários autorizados.

- **GERENCIAMENTO DE CHAVES**

O uso de chaves que garantem a segurança das mensagens criptografadas deve funcionar como um segredo compartilhado exclusivamente entre as partes envolvidas. O gerenciamento de chaves deve garantir a troca periódica das mesmas, visando manter a comunicação de forma segura.

- **SUPORTE A MÚLTIPLOS PROTOCOLOS**

Com a diversidade de protocolos existentes, torna-se bastante desejável que uma VPN suporte protocolos padrão de fato usadas nas redes públicas, tais como IP (Internet Protocol), IPX (Internetwork Packet Exchange), etc.

TUNELAMENTO

As redes virtuais privadas baseiam-se na tecnologia de tunelamento cuja existência é anterior às VPNs.

Ele pode ser definido como processo de encapsular um protocolo dentro de outro.

O uso do tunelamento nas VPNs incorpora um novo componente a esta técnica: antes de encapsular o pacote que será transportado, este é criptografado de forma a ficar ilegível caso seja interceptado durante o seu transporte.

O pacote criptografado e encapsulado viaja através da Internet até alcançar seu destino onde é desencapsulado e decriptografado, retornando ao seu formato original.

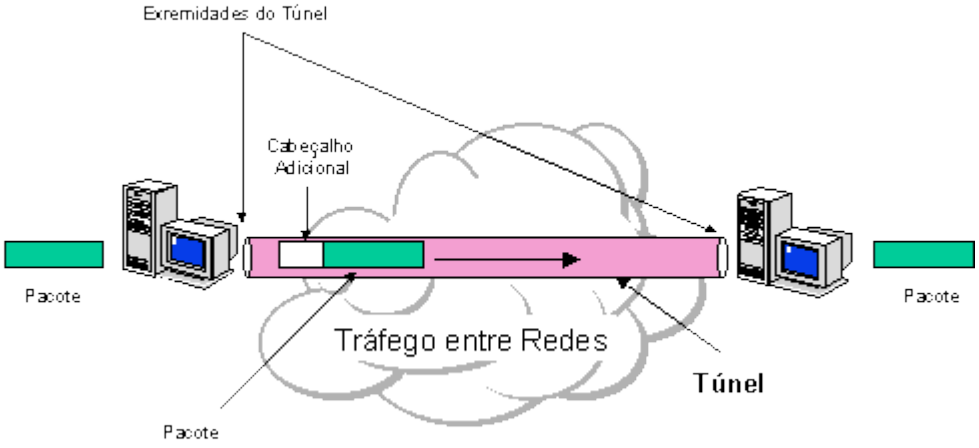
Uma característica importante é que pacotes de um determinado protocolo podem ser encapsulados em pacotes de protocolos diferentes. Por exemplo, pacotes de protocolo IPX podem ser encapsulados e transportados dentro de pacotes TCP/IP.

O protocolo de tunelamento encapsula o pacote com um cabeçalho adicional que contém informações de roteamento que permitem a travessia dos pacotes ao longo da rede intermediária. Os pacotes encapsulados são roteados entre as extremidades do túnel na rede intermediária.

Túnel é a denominação do caminho lógico percorrido pelo pacote ao longo da rede intermediária. Após alcançar o seu destino na rede intermediária, o pacote é desencapsulado e encaminhado ao seu destino final.

A rede intermediária por onde o pacote trafegará pode ser qualquer rede pública ou privada.

Note que o processo de tunelamento envolve encapsulamento, transmissão ao longo da rede intermediária e desencapsulamento do pacote.



IPSEC – INTERNET PROTOCOL SECURITY

O IPSec é um protocolo padrão da camada 3 projetado pelo IETF que oferece transferência segura de informações fim a fim através de rede IP pública ou privada.

Essencialmente, ele pega pacotes IP privados, realiza funções de segurança de dados como criptografia, autenticação e integridade, e então encapsula esses pacotes protegidos em outros pacotes IP para serem transmitidos.

As funções de gerenciamento de chaves também fazem parte das funções do IPSec.

O IPSec trabalha como uma solução para interligação de redes e conexões via linha discada. Ele foi projetado para suportar múltiplos protocolos de criptografia possibilitando que cada usuário escolha o nível de segurança desejado.

Os requisitos de segurança podem ser divididos em 2 grupos, os quais são independentes entre si, podendo ser utilizado de forma conjunta ou separada, de acordo com a necessidade de cada usuário:

Autenticação e Integridade; Confidencialidade.

Para implementar estas características, o IPSec é composto de 3 mecanismos adicionais:

AH - Autentication Header;
ESP - Encapsulation Security Payload;
ISAKMP - Internet Security Association and Key Management Protocol.