Ministério da Educação
Instituto Médio Politécnico "Alda Lara"

SISTEMA DE EXPLORAÇÃO E ARQUITETURA DO COMPUTADOR

Classe: 11ª

- Tema :1 - Arquitetura de computadores

Introdução à terminologia básica

Terminologia é um conjunto determinado de vocábulos próprios de uma ciência, de uma arte, de um ofício ou de uma profissão.
Microprocessador é um equipamento eletrônico, preparado para executar determinados procedimentos de acordo com a linguagem de comando específica. Utiliza duas áreas de memorias, a Ram como Memórias de dados, onde armazena temporariamente informações e a Rom como Memórias, onde "Lê" as instruções que deve executar.

O que é um Microcontralador?

Um microcontralador é praticamente um computador em um chip, no chip do microcontralador contém todos os itens como processador, memória Rom, memória Ram, periféricos de entrada/saída, conversor analógico /digital, etc. O microcontralador pode ser programado diversas funções mais faz apenas aquilo que está em seu programa para executar outras funções ele tem que ser reprogramado.

Exemplos de um microcontrolador:

- PIC que que são da família de microcontralador fabricados pela Microchip.
- Atmel AVR que são da família de microcontralador fabricados pela Atmel.

- Intel MCS que são da família de microcontralador fabricados pela Intel.

Os microcontralador fica no interior de outro dispositivo eletrônico para que possam controlar suas funções, como alarmes, eletrodomésticos, veículos etc.

O que é um microprocessador?

O microprocessador, também chamado de processador, é basicamente um circuito integrado que realiza as funções de cálculo e tomada de decisão. Ele é um cérebro eletrônico em um chip, tabletes e todos os equipamentos eletrônicos que se baseiam nele para executar suas funções.

1.2.Apresentação da arquitetura

O microcontrolador terá que aceder as várias áreas de memórias e controlar todos os periféricos de acordo com o software nele introduzido. Assim sendo, a forma de controlar toda a informação, enviar e receber dados, é processado como se um carteiro se tratasse. Existem dois barramentos fundamentais na sua arquitetura interna: o barramento de dados e o barramento de endereços. É através destes dois barramentos internos que é colocada a informação a escrever ou ler e o endereço de destino /origem dessa informação.

1.3Tipos de Arduino

Introdução

O arduino é uma plataforma utilizada para prototipação circuitos e eletrônicos.O projeto do arduino teve o início em 2005 na cidade de Ivrea ,Itália .O arduino é compostos por uma placa microcontrolador e um ambiente programação baseado wirring em c++ .

Tanto hardware como o ambiente de programação do arduino são

livres ,ou seja ,qualquer pessoa pode modificá-lo e reproduzi-los.
O Arduino também é conhecido de plataforma e computação física.
Tipos de arduino

Existem vários tipos de Arduino com especificidades de hardware. Arduino lista os seguintes tipos:

- Arduino UNO
- ArduinoLeonardo
- Arduino Due
- Arduino Esplora
- Arduino Mega
- Arduino MegaADK
- Arduino Ethernet
- ArduinoMini
- Arduino LilyPad
- Arduino Micro
- Arduino Nano
- Arduino ProMini
- Arduino Pro
- Arduino Fio

Arduino. Uno

A placa Arduino UNO já está em sua terceira revisão e você pode seu os esquema elétrico no site arduino ,ou até mesmo os arquivos do projeto para edição .ela tem duas camadas apenas e várias características interessantes de projeto seguir serão apresentadas s principais características do seu hardware.

Hardware de Arduino

Alimentação da placa Arduino

A placa pode ser alimentada pela conexão Usb ou por uma fonte de alimentação, conforme exibido na figura abaixo:
a alimentação externa é feita através do conector Jack com positivo no centro ,onde o valor de tensão da fonte externa deve estar entre os limites 6v ,.a 20v, porém se alimentada com uma tensão abaixo de 7V,a tensão de funcionamento da placa ,que no Arduino UNO é de 5v , pode ficar instável e quando alimentada com tensão da placa .Dessa forma, é recomendado para tensões de fonte externa valores de 7V, a 12V.

Mapa das Entradas e Saída do arduino.

As portas de E e S do arduino e suas funções.

As duas principais partes (funções) de um programa desenvolvido para o Arduino são:◦ setup () : onde devem ser definida s algumas configurações iniciais do programa. Executa uma única vez. ◦loop (): função principal do programa .Fica executa ndoin definidamente. } Todo programa para o Arduino deve ter estas duas funções.
Exemplo1: formato das funções setup() e loop()

Os pinos digitais

O Arduino possui tanto portas digitais como portas analógicas. As portas servem para comunicação entre o Arduino e dispositivos externos, por exemplo: ler um botão, acender um led ou uma lâmpada. Conforme já mencionado, o Arduino UNO, possui 14 portas digitais e 6 portas analógicas (que também podem ser utilizadas como portas digitais).

Os Pinos analógicos

Portas Analógicas são utilizadas para entrada de dados .Os valores lidos em uma porta analógica variam de 0V a 5V.Para ler uma valor em uma porta analógica basta utilizar a função analogRead(pin).

Os conversores analógicos-digitais(ADC) do Arduinos ão de 10bits. Os conversoresADC (doInglêsAnalogDigitalConverter) permitem uma precisão de 0.005Vou5mV.
Os valores lidos em uma porta analógica variam de 0a1023(10bits), onde 0 representa 0Ve1023 representa 5V.

O Arduino UNO possui 6 (seis) portas analógicas. Por padrão todas as portas analógicas são definidas como entrada de dados, desta forma não é necessário faz e resta definição na função setup().O conversor analógico-digital do Arduino é de 10 (dez) bits, logo a faixa de valores lidos variade 0 a 1023

A porta serial do Arduino

O monitor serial é utilizado para comunicação entre o Arduino e o computador (PC). O monitor serial pode ser aberto no menu tools opção serial monitor, ou pressionando asteclasCTRL+SHIFT+M. As principais funções do monitor serial são :
begin(),read(),write(),print(),println()eavailable().

Tema 2- Programação em Linguagem máquina (assemby)

2.1 Introdução à linguagem máquina

Depois de conhecidos os recursos disponibilizados pelo microprocessador/ microcontrolador e implementado o hardware necessário (micro, memoria externa, periféricos ,etc) ,é necessário instrui-lo no sentindo da sequência de operações que deve levar a cabo. A esta sequência de operações (instruções) é dados o nome de programa.

2.2 Tipos de endereçamentos e instruções associadas.

2.2.1 Endereçamento imediato

Neste tipo de endereçamento, o valor a ser guardado na memória é localizado logo após o código da instrução. Por exemplo, para carregar o acumulador com o valor 20h usa-se a seguinte instrução

a qual utiliza endereçamento imediato:

Mov A,# 20h

2.2.2 Endereçamento directo

sempre que o valor a ser transferindo é obtido através da especificação direta da posição da memória que o contém. Por exemplo, para transferir para o acumulador o conteúdo da posição de memória interna 30h:

Mov A, 30h

2.2.3 Endereçamento indireto

o endereçamento inderecto é um poderoso modo de endereçamento ,que ,em muitos casos,permite um nível de flexibilidade .A posição de memória onde se encontra o valor a ser transferido é indicada de forma indireta recorrendo ao conteúdo de outra posição de memória (ou registo no caso do 8051).

Por exemplo, a seguinte instrução executa a transferência do conteúdo da posição de memória no registo R0 para o acumulador.

Mov A,@RO

Se R0 contém o valor 30h e a posição de memória 30h contém o valor Ffh,no fim da executação da instrução o acumulador conterá o valor ffh.

2.2.4 Endereçamento externo directo

A memória externa ´acedida usando um conjunto de instruções que recorrem ao endereçamento externo directo . Neste caso, é usando um registo de 16 bits ,o DPTR(Data Pointer), que contém a posição de memória externa a aceder:

Movx A,@DPTR

Movx A,@DPTR A

2.2.5 Endereçamento de código de programa

A memória externa pode também ser acedida de forma inderecta. Esta forma de endereçamento é, normalmente, usada em pequenas aplicações com pequena capacidade de memória. Um

exemplo deste tipo de endereçamento é a instrução:

MOVX @RO, A

É usado o registo RO para indirectamente indicar a posição de memória externa onde se pode guardar o conteúdo do acumulador. Lembre - se que RO é uma posição de memória.

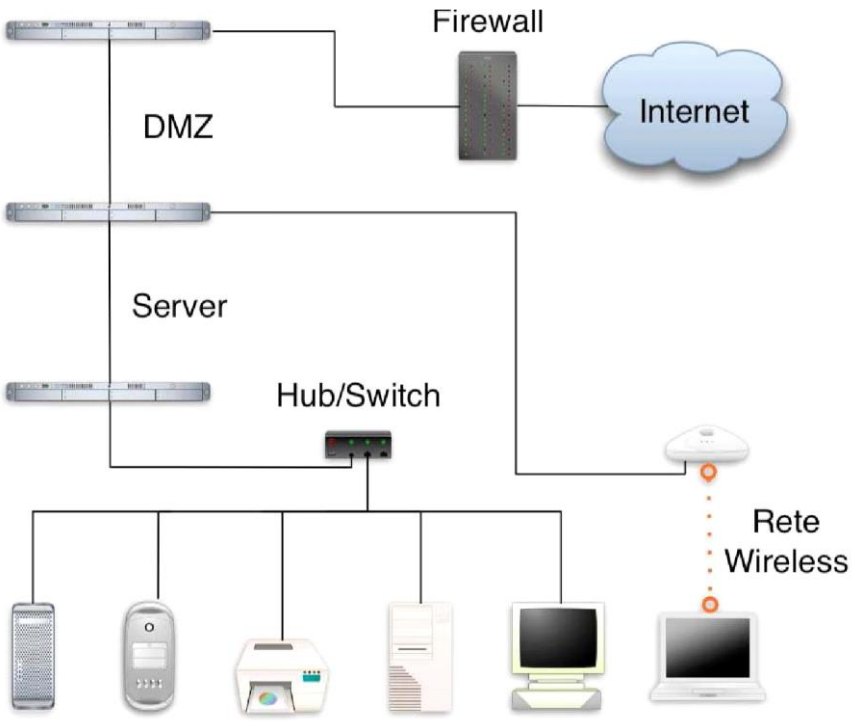
Programação Assembly

Breve história da linguagem Assembly,a programas eram escritos em linguagem de maquina na década 50 anos o Assembly surge para facilitar a programação .

Surgimento das inguagens de lto nível surgiu na década de 70 e 80 e passou ser pouco usada.Era dos microprocessadores e sistemas embarcados na década de 90 ate oje ,o Assemby volta na busca desempenho e velocidade.

Conceito de linguagem Assembly

Por vezes chamada de assembly ou ASL,a linguagem assembly e uma linguagem de baixo nível de programação usada para a interface com o hardware do computador. A linguagem assembly usa comandos estruturados em vez de números e permite eu os programadores consigam ler mais facilmente assembly é uma linguagem difícil e geralmente é substituída por uma linguagem mais elevada tal como a linguagem de programação C.



Versao: 1.0

Tema 3 – Conceitos sobre redes de computadores

1. Redes de comunicação de dados

1.1 Caracterização da necessidade de comunicação

O nascimento das redes de computadores, não por acaso, esta associada a corrida espacial. Boa parte dos elementos e aplicações essenciais para a comunicação entre computadores, como o protocolo TCP/IP, a tecnologia de comutação de pacotes de dados e o correio eletrônico, estão relacionados ao desenvolvimento da Arpanet, a rede que deu origem a internet. Ela foi criada por um programa desenvolvido pela Advanced Research Projects Agency (ARPA) mais tarde rebatizada como DARPA.

A agencia nasceu de uma iniciativa do departamento de defesa dos estados unidos, na época preocupado em não perder terreno na corrida tecnológica deflagrada pelos russos com o lançamento do

satélite Sputinik, em 1957. Roberts, acadêmico do MIT (Instituto de Tecnologia de Massachusetts), era um dos integrantes da DARPA e um dos pais da Arpanet, que começou em 1969 conectando quatro universidades: UCLA – Universidade da Califórnia em Los Angeles, Stanford, Santa Bárbara e Utah. A separação dos militares da Arpanet só ocorreu em 1983, com a criação da Milnet.

1.2 Tecnologias de comutação

1.2.1 Comutação por Circuitos

Na comutação por circuitos, um circuito físico real é formado entre os dois equipamentos que desejam se comunicar. Os elementos de comutação da rede unem (ou conectam) circuitos ponto a ponto independentes até formar um "cabo" que interligue os dois pontos.

comutação por circuitos, em redes de telecomunicações, é um tipo de alocação de recursos para transferência de informação que se caracteriza pela utilização permanente destes recursos durante toda a transmissão. É uma técnica apropriada para sistemas de comunicações que apresentam tráfego constante (por exemplo, a comunicação de voz), necessitando de uma conexão dedicada para a transferência de informações contínuas.

Essencialmente, uma comunicação via comutação por circuitos entre duas estações se subdivide em três etapas: o estabelecimento do *circuito*, a conversação e a desconexão do circuito.

Na primeira etapa, uma rota fixa entre as estações envolvidas é estabelecida para que elas possam se comunicar. Entre uma ponta e outra da comunicação, é determinada e alocada uma conexão bidirecional (isto é, um circuito), contendo um canal dedicado para cada estação transceptora até o término da comunicação.

Em seguida, as estações envolvidas podem trocar informações entre si, transmitindo e recebendo dados através do circuito já estabelecido. Esta transferência de dados corresponde a segunda etapa da comutação de circuitos.

Após um período indeterminado, a conexão é finalmente encerrada, quase sempre pela ação de uma das estações comunicantes. Nesta última etapa, todos os nós intermediários do circuito precisam ser desalocados de modo a serem reutilizados, conforme necessário, para formar novos circuitos entre quaisquer estações pertencentes à rede. Para tanto, sinais de controle são transmitidos para estes nós, liberando recursos para outras conexões.

Existem três maneiras diferentes de se alocar canais de comunicação em comutação de circuitos. São elas:

Chaveamento espacial: é estabelecido um caminho entre duas estações por meio de enlaces físicos permanentes durante toda a comunicação. Ao longo desse caminho, uma sucessão de chaves físicas, cada uma em um nó intermediário, formam um circuito através da interconexão entre suas portas;

Chaveamento de freqüências: é estabelecida uma associação entre dois canais de freqüência em cada enlace. Um nó intermediário, ao receber um sinal de uma onda portadora de determinada freqüência, realiza a filtragem e demodulação deste sinal para sua posterior modulação e transmissão na outra freqüência associada.

Chaveamento do tempo: é estabelecida uma associação de dois canais de tempo em cada enlace. Cada nó intermediário associa um canal TDM síncrono de uma linha com outro canal TDM síncrono de outra linha, demultiplexando o sinal de um circuito desejado para ser multiplexado e encaminhado para outro nó.

A comutação por circuitos é muito empregue em sistemas telefônicos, devido a natureza contínua que caracteriza a

comunicação por voz. Este comportamento constante da comunicação é um fator determinante para o emprego de tal técnica, uma vez que a utilização de comutação de circuitos em transmissões de dados que se caracterizam por rajadas ou longos períodos de inatividade resulta em desperdício da capacidade do meio físico.

1.2.2 Comutação por Mensagem

Na comutação por mensagem não é estabelecido um caminho dedicado entre os dois equipamentos que desejam trocar informações. A mensagem que tem que ser enviada é transmitida a partir do equipamento de origem para o primeiro elemento de comutação, que armazena mensagem e a transmite para o próximo elemento. Assim a mensagem é transmitida pela rede até que o último elemento de comutação entregue-a ao equipamento de destino. Neste tipo de comunicação a rede não estabelece o tamanho mensagem, podendo esta ser ilimitada.

A comutação por mensagens foi o precursor da comutação de pacotes, onde mensagens eram roteadas na rede inteira, um hop por vez. Sistemas de comutação de pacotes são hoje em dia geralmente implementados sobre comutação de pacotes ou circuitos.

O e-mail é um exemplo de um sistema de comutação por mensagens.

1.2.3 Comutação por Pacotes (datagrama, circuitos virtuais)

A comutação por pacotes possui uma filosofia de transmissão semelhante a comutação de mensagem, ou seja os pacotes são transmitidos através dos elementos de comutação da rede até o seu destino.

No contexto de redes de computadores, a comutação de pacotes é um paradigma de comunicação de dados em que pacotes

(unidade de transferência de informação) são individualmente encaminhados entre nós da rede através de ligações de dados tipicamente partilhadas por outros nós. Este contrasta com o paradigma rival, a comutação de circuitos, que estabelece uma ligação virtual entre ambos nós para seu uso exclusivo durante a transmissão (mesmo quando não há nada a transmitir). A comutação de pacotes é utilizada para optimizar o uso da largura de banda da rede, minimizar a latência (i.e., o tempo que o pacote demora a atravessar a rede) e aumentar a robustez da comunicação.

A comutação por pacotes é mais complexa, apresentando maior variação na qualidade de serviço, introduzindo jitter e atrasos vários; porém, utiliza melhor os recursos da rede, uma vez que são utilizadas técnicas de multiplexagem temporal estatística.

A comutação por pacotes pode efetuar-se de dois modos:

Com ligação (circuito virtual): é estabelecido um caminho virtual fixo (sem parâmetros fixos, como na comutação de circuitos) e todos os pacotes seguirão por esse caminho. Uma grande vantagem é que oferece a garantia de entrega dos pacotes, e de uma forma ordenada. Ex: ATM (comutação de células), Frame Relay e X.25;

Sem ligação (datagrama): os pacotes são encaminhados independentemente, oferecendo flexibilidade e robustez superiores, já que a rede pode reajustar-se mediante a quebra de um link de transmissão de dados. É necessário enviar-se sempre o endereço de origem. Ex: endereço
IP.

A principal diferença entre a comutação por Pacotes e a comutação por circuitos é que, ao contrario da primeira, na comutação por pacotes o tamanho dos bloco de transmissão é definido pela rede. Em conseqüência, a mensagem a ser transmitida deve ser quebrada em unidades menores (pacotes).

Ao quebrar a mensagem em pacotes, a rede pode transmitir os

pacotes de uma mesma mensagem por vários caminhos diferentes, otimizando os recursos da rede. A desvantagem é que os pacotes podem chegar na ordem trocada, necessitando a criação de mecanismos de ordenamento.

Item	Comutação		
	Circuitos	Mensagem	Pacotes
Estabelecimento do circuito	Obrigatório	Sem necessidade	Sem necessidade
Caminho físico dedicado	Sim	Não	Não
Cada pacote segue a mesma rota	Sim	Sim	Não
A falha do elemento comutador impossibilita a comunicação	Sim	Sim	Não
Recursos da rede disponibilizados	Fixo	Dinâmico	Dinâmico
Desperdício de recursos da rede	Sim	Médio	Não
Exemplos de serviços	Telefonia	E-mail	IP, Frame Relay

Tabela 1

4.Classificação das redes de computadores

2.1 Abrangência

As redes de computadores quanto a sua abrangência podem ser classificadas basicamente como redes de area local (LAN) e redes de area alargadas (WAN):

2.1.1 Redes locais

Redes de Area Local (LAN): uma rede que liga computadores próximos, normalmente em um mesmo prédio ou, no máximo, entre prédios próximos e podem ser ligados por cabos apropriados (chamados cabos de rede). Ex: Redes de computadores das empresas em geral. Qualquer rede cujo raio de alcance seja menor do que 10 Km se encaixa nesta categoria.As LANS existem desde a década de 60, quando eram usadas pelo Laboratório de Livermore para ajudar na pesquisa de armas atômicas. Nas próximas décadas, o seu uso se espalhou em outros setores da sociedade. A principal utilidade das LANs era compartilhar o uso de espaço em disco e impressoras - que eram muito caros na época.

A popularização das LANs foi algo que ocorreu lentamente, principalmente devido aos vários protocolos existentes que eram incompatíveis entre si. Cada fornecedor de placas de redes possuía o seu próprio protocolo que se comunicava somente com outros dispositivos do mesmo fabricante. Entretanto, este entrave passou a diminuir muito com o tempo, pois cada vez mais o mercado dava preferência à equipamentos capazes de se comunicar com equipamentos de diferentes fornecedores. Atualmente já existem protocolos oficiais que cada fabricante precisa seguir se quiser que seus equipamentos sejam compatíveis com os demais.

Métodos de acesso

Ethernet: E, actualmente, o padrão de redes locais que conheceu maior difusão. E definido fundamentalmente ao nivel da camada de ligação de dados e a sua implementação começa por ser feita nas proprias placas de rede.

As redes Ethernet conheceram grande difusão em topologias de burramento (bus) com cabos coaxiais. Entretanto, com a difusão da tecnologia dos

Hubs, tornaram-se mais comuns em topologias em estrela, com cabos UTP.

As taxas de transmissao situam-se a partida na casa dos 10 Mbits/seg.

Token Ring: E igualmente definido ao nivel da camada de ligação de dados e implementado nas placas de rede. Dispoem-se, normalmente, em topologias de anel ou de anel com com configuaração de estrela usando cabos de pares entrançados.

FDDI(Fiber Distributed Data Interface): Abrange os niveis fisicos e de ligacao de dados(as duas primeiras camadas do modelo OSI).

Enquanto os padroes Ethernet e Token Ring tem aplicacao exclusivamente em redes locais, o padrao FDDI permite o desenvolvimento de redes com um ambito maior, momeadamente redes do tipo MAN (Metropolitan Area Network), bem como pode servir de base a interligacao de redes locais, com as redes de campus.

Frame Relay: Semelhante ao X.25, no aspecto em que tambem utiliza a tecnologia de comutacao de pacotes, mas com a diferenca de que neste caso, as decisoes quanto ao encamiamento (Routing) dos pacotes sao feitas ao nivel da camada de ligacao de dados ao passo que no X.25 essas decissoes processam-se ao nivel da camada de rede.

E tambem implementado numa interface que liga o computador a rede, que pode ser baseada em linhas publicas ou privadas. As taxas de transmissao podem situarz-se na casa dos 1,5 Mbits/s.

2.1.2 Redes alargadas

Redes de Área Alargada - WAN: Redes que se estendem além das proximidades físicas dos computadores. Como, por exemplo, redes ligadas por conexão telefônica, por satélite, ondas de rádio, etc. (Ex: A Internet, as redes dos bancos internacionais, como o CITYBANK).

Qualquer rede cuja área é maior do que uma cidade se encaixa nesta categoria. Existem WANs que possuem uma área de alcance que cruzam até mesmo diferentes estados e países.

A primeira rede deste tipo surgiu em 1965 quando um computador em Massachussets e outro na Califórnia foram ligados entre si. Atualmente, a maior WAN existente é a Internet.

WANs são muito utilizadas por empresas de telefone que costumam fornecer serviços de acesso à Internet.

Métodos de modulação

Modulação é o processo de variação de altura (amplitude), de intensidade, frequência, do comprimento e/ou da fase de onda numa onda de transporte, que deforma uma das características de um sinal portador (amplitude, fase ou frequência) que varia proporcionalmente ao sinal modulador.
A modulação é a modificação de um sinal eletromagnético inicialmente gerado, antes de ser irradiado, de forma que este transporte informação sobre uma onda portadora.

é o processo no qual a informação a transmitir numa comunicação é adicionada a ondas eletromagnéticas. O transmissor adiciona a informação numa onda básica de tal forma que poderá ser recuperada na outra parte através de um processo reverso chamado demodulação.

A maioria dos sinais, da forma como são fornecidos pelo transmissor, não podem ser enviados diretamente através dos canais de transmissão. Conseqüentemente, é necessário modificar

esse sinal através de uma onda eletromagnética portadora, cujas propriedades são mais convenientes aos meios de transmissão. A modulação é a alteração sistemática de uma onda portadora de acordo com a mensagem (sinal modulante), e pode incluir também uma codificação.

É interessante notar que muitas formas de comunicação envolvem um processo de modulação, como a fala por exemplo. Quando uma pessoa fala, os movimentos da boca são realizados a taxas de freqüência baixas, na ordem dos 10 Hertz, não podendo a esta freqüência produzir ondas acústicas propagáveis. A transmissão da voz através do ar é conseguida pela geração de tons (ondas) portadores de alta frequência nas cordas vocais, modulando estes tons com as ações musculares da cavidade bucal. O que o ouvido interpreta como fala é, portanto, uma onda acústica modulada, similar, em muitos aspectos, a uma onda elétrica modulada.

O dispositivo que realiza a modulação é chamado modulador.

Basicamente, a modulação consiste em fazer com que um parâmetro da onda portadora mude de valor de acordo com a variação do sinal modulante, que é a informação que se deseja transmitir.

Dependendo do parâmetro sobre o qual se atue, temos as seguintes tipos de modulação mais frequentes: modulação por frequência e modulação por Amplitude.

Modulação por Fraquencia

FM é a abreviatura para modulação em frequência ou frequência modulada (frequency modulation -, em inglês).

Iniciada nos Estados Unidos no início do século XX, FM é uma modalidade de radiodifusão que usa a faixa 87,5 Mhz a 108 Mhz com modulação em frequência.

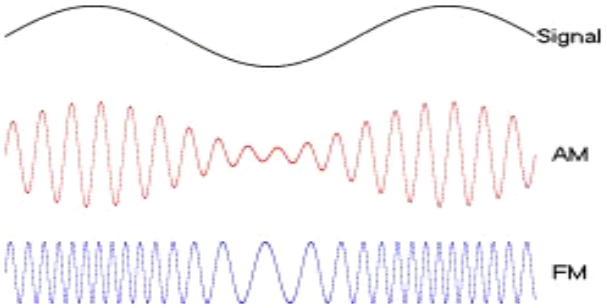


Fig 1 – Modulação por frequencia

Uma rádio em FM apresenta uma ótima qualidade sonora mas com limitado alcance, chegando em média a 100 quilômetros de raio de alcance. Em condições esporádicas de propagação, é possível sintonizar emissores a centenas de quilômetros. A potência dos sistemas de emissão pode variar entre poucos watts (rádios locais) até centenas de quilowatts, no caso de retransmissores de grande cobertura.

O FM dispõe de um sistema de envio de informação digital, o RDS (Radio Data System) que permite apresentar informações sobre a emissora sintonizada. Também, a boa qualidade de som desta gama de frequências de radiodifusão é adequada ao uso da estereofonia.

A qualidade da transmissão por modulação em frequência fez com que esta fosse adotada para a transmissão do áudio da TV aberta (canais 2 a 13).

Um das desvantagens dos receptores FM é de apresentarem uma característica conhecida como efeito de captura. Esse efeito ocorre da seguinte maneira: se existirem dois ou mais sinais de FM emitidos na mesma frequência, o receptor de FM irá responder ao sinal de maior potência e ignorar os menores (os restantes).

Modulação por Amplitude ou simplesmente AM (do inglês Amplitude Modulation - Modulação por Amplitude), é a forma de modulação em que a amplitude de um sinal senoidal, chamado

portadora, varia em função do sinal de interesse, que é o sinal modulador. A frequência e a fase da portadora são mantidas constantes. Matematicamente, é uma aplicação direta da propriedade de deslocamentos em frequências da transformada de Fourier, assim como da propriedade da convolução.

5. Hierarquia

2.2.1 Ponto–a–ponto ou Peear to Pear

Em redes deste tipo, cada nó só pode se comunicar com nós adjacentes. É como em uma brincadeira de telefone sem fio no qual para que uma mensagem chegue até alguém, ela precisa passar por vários intermediários, já que só é possível falar com as pessoas que estejam ao seu lado.

É constituída por computadores ou outros tipos de unidades de processamento que não possuem um papel fixo de cliente ou servidor, pelo contrário, costumam ser considerados de igual nível e assumem o papel de cliente ou de servidor dependendo da transação sendo iniciada ou recebida de um outro par da mesma rede.

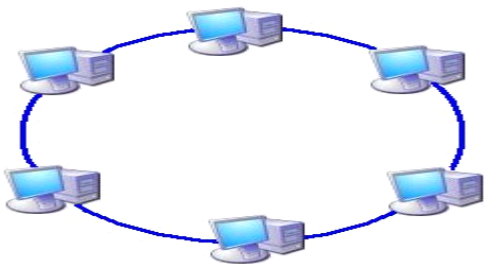


Fig 2 – Rede Ponto a Ponto

Computadores são conectados em grupo para que outros usuários possam compartilhar recursos e informações. Não há um local central para autenticação de usuários, armazenamento de arquivos ou acesso a recursos. Isso significa que os usuários devem lembrar em qual computador do grupo de trabalho está o recurso ou a informação compartilhada que desejam acessar. Isso significa também que os usuários precisam efetuar login em cada computador para acessar os recursos compartilhados no computador indicado.

Na maioria das redes ponto a ponto, é difícil para os usuários rastrearem onde está a informação porque os dados são geralmente armazenados em vários computadores. Isso dificulta o backup de informações de negócios importantes, e, na maioria dos casos, as pequenas empresas não conseguem concluir backups. Em muitos casos, há várias versões do mesmo arquivo em computadores diferentes no grupo de trabalho.

Em algumas redes ponto a ponto, a pequena empresa utiliza um computador com um sistema operacional cliente (como o Microsoft Windows 98 ou Windows XP Professional) como o "servidor" designado para a rede. Embora o salvamento de dados em um local central seja útil, ele não oferece uma solução robusta para muitas das necessidades de uma pequena empresa, como a colaboração em documentos.

Os nós da rede Peer-to-Peer podem diferir em termos de configuração local, capacidade de processamento, capacidade de armazenamento, largura de banda, entre outras características particulares.

A correta operação de sistemas ponto aa ponto não depende da existência de um sistema de administração centralizado. Assim, sistemas ponto a ponto se confudem com sistemas descentralizados. Num sistema totalmente descentralizado, não só todos os hospedeiros são iguais, mas também não há hospedeiros com atribuições especiais, como administração e descoberta de

serviços.

Características

Sistemas ponto a ponto compartilham essas características:

O seu design garante que cada usuário contribui com recursos para o sistema.

Apesar de que eles podem diferir nos recursos que contribuem, todos os nodos em um sistema peer-to-peer possuem as mesmas capacidades funcionais e responsabilidades.

2.2.2 Cliente /Servidor

Uma arquitetura na qual o processamento da informação é dividido em módulos ou processos distintos. Um processo é responsável pela manutenção da informação (servidores) e outros responsáveis pela obtenção dos dados (os clientes).

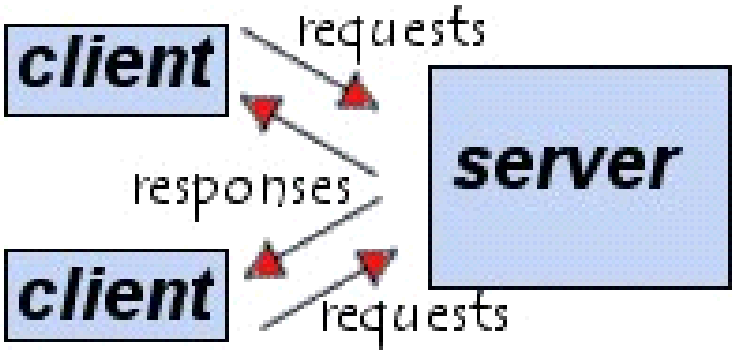


Fig 3 – Esquema Cliente/Servidor

Os processos cliente enviam pedidos para o processo servidor graças ao seu endereço IP e a porta, e este por sua vez processa e envia os resultados dos pedidos com a ajuda do endereço da máquina cliente e da sua porta.

Nos sistemas cliente/servidor o processamento tanto do servidor

como o do cliente são equilibrados, se for gerado um peso maior em um dos dois lados, provavelmente, esse não é um sistema cliente/servidor.

Geralmente, os serviços oferecidos pelos servidores dependem de processamento específico que só eles podem fazer. O processo cliente, por sua vez, fica livre para realizar outros trabalhos. A interação entre os processos cliente e servidor é uma troca cooperativa, em que o cliente é o ativo e o servidor reativo, ou seja o cliente requisita uma operação, e neste ponto o servidor processa e responde ao cliente.

- Cliente

O processo de cliente é ativo, ou seja são eles que solicitam serviços a outros programas, os servidores. Normalmente o cliente é dedicado à sessão do usuário, começando e terminando com a sessão.

Um cliente pode interagir com um ou mais servidores, mas pelo menos um processo servidor é necessário.

A nível de aplicação, o primeiro ponto a residir no cliente é a interface com o usuário.

Algumas tarefas a serem realizadas pelo Cliente:

- Manipulação de tela
- Interpretação de menus ou comandos
- Entrada e validação dos dados
- mento de Ajuda
- Processa
- Recuperação de erro
- Manipulação de janelas

- Gerenciamento de som e vídeo (em aplicações multimídia)

Gerenciando a interação com o usuário, o cliente esconde do usuário o servidor e a rede, caso houver. Para o usuário a impressão é que a aplicação está sendo rodada completamente local.

Se, por acaso, o programa que interage com o usuário fizer simplesmente chamada de rotina, e ficar por conta do servidor todo o processamento este certamente não é um sistema cliente/servidor.

- *Servidores*

Servidores são programas que respondem as solicitações por serviços compartilhados. Ele é um processo reativo, disparado pela chegada de pedidos de seus clientes.

Geralmente, o processo servidor roda o tempo todo, oferecendo serviços a muitos clientes.

Em alguns sistemas, o processo servidor em vez de responder diretamente, cria um processo escravo exclusivamente para cada pedido de cliente. O servidor banco de dados Oracle trabalha desta forma, quando chega um pedido, ele cria um processo escravo dedicado a trabalhar neste pedido, deixando assim o processo mestre livre para receber outros pedidos imediatamente.

Para que o servidor possa manipular os dados e prover segurança são combinadas rotinas de gerenciamento de dados com as funções de controle encontradas nos sistemas operacionais.

- *Comunicação*

A comunicação entre o cliente e o servidor é do estilo transacional e cooperativo. A natureza transacional significa que o servidor envia de volta para o cliente somente os dados relevantes. A

natureza cooperativa significa que ocorre um processamento significativo nos dois extremos, clientes e servidor.

As primeiras aplicações em rede foram elaboradas utilizando a tecnologia de compartilhamento de arquivos. Por exemplo, quando um usuário iniciava uma aplicação , o código executável da aplicação tinha que ser transmitido. Numa aplicação de banco de dados era transmitido todo o código executável do banco de dados e a cada atualização todo o banco de dados também tinha que ser transmitido, além disso os arquivos de índice também eram necessários para atualização. Quando trocada por uma aplicação cliente/servidor o executável do banco de dados permaceu no servidor, junto com ele todos os arquivos de índices de bancos de dados, trafegando pela rede apenas os dados do pedido de gravação do cliente.
Agora vamos considerar uma aplicação baseada em host e acessada por uma rede com software de emulação de terminal. Assim, todos os toques de teclas e a maior parte das instruções de controle de tela são transmitidas através da rede. A rede transporta todo os dados informados pelo usuário, como a escolha de um menu. Se um usuário pedir ajuda, trafegam pela rede todas as mensagens de ajuda, a responsabilidade pelo controle da tela é do host.

No caso de um sistema cliente/servidor, por exemplo, uma companhia aérea utilizando um sistema de reservas de passagens, onde temos um banco de dados compartilhado com os dados dos vôos, dados dos passageiros, tripulação, etc. O software cliente passa para o servidor somente os dados da operação como reserva, nome do passageiro, vôo, data, todos eles já validados. O servidor recebendo estes dados, processa e armazena no banco de dados e envia o resultado de volta. Neste caso, o cliente é responsável pelo controle da tela e nenhuma informação deste tipo trafega pela rede.

A diferença é especialmente notada em aplicações baseadas em

registros, onde a incidência de informações é muito alta.

Com estes exemplos podemos ver como o sistema cliente/servidor diminui o tráfego na rede em relação as arquiteturas anteriores. Logicamente com isto não podemos dizer que uma aplicação cliente/servidor não gera tráfego de rede, mas o impacto de uma aplicação cliente/servidor bem elaborada é mínimo.

Uma característica dos sistemas cliente/servidor é a utilização de plataformas de hardware e softwares diferentes de um para outro. Dentro deste mix de recursos as aplicações devem se comunicar de forma transparente. Aí entra o chamado middleware, que é todo o software existente entre os dois processos, para que eles se comuniquem. O núcleo do middleware é o sistema operacional da rede. Além do sistema operacional é importante também o protocolo que rege a forma pela qual os clientes solicitam informações e serviços ao servidor, como o NetBIOS, o RPC e o SPX.

Um servidor processa a informação sem interagir com outros servidores. Os clientes que interagem com mais de um servidor tem a responsabilidade de ativá-los quando necessário.

O processamento do servidor geralmente inclui:

- Acessar,
- armazenar,
- organizar os dados compartilhados,
- atualizar dados previamente armazenados
- gerenciamento dos recursos compartilhados

Recursos compartilhados podem ser: dados, CPU, armazenamento em disco ou fita, capacidade de impressão, comunicação e até gerenciamento de vídeo e memória.

Exemplos de Servidores:

Um bom exemplo de servidor é o servidor de backup, que pode fornecer recursos de backup e recuperação em fita para várias máquinas numa rede.

O X-Windows é outro bom exemplo de sistemas cliente/servidor, ele oferece serviços de vídeo acessíveis pela rede para clientes trabalhando em qualquer ponto.

As aplicações em banco de dados cliente/servidor em sua maioria são montados em cima de banco de dados SQL prontos como Oracle, Informix, Ingress, Sybase, etc. Por exemplo, uma aplicação desenvolvidas com uma linguagem de 4ª geração (4GL) Progress interagindo com dispositivo de banco de dados Oracle é uma aplicação cliente/servidor, onde o Progress constitui o processo cliente e o dispositivo Oracle é o processo servidor, ambos rodam em nível de aplicação caracterizando assim uma aplicação cliente/servidor.

- *Sincronização*

Nos sistemas cliente/servidor não é necessária a utilização de mecanismos especiais para sincronizar o processamento concorrente, pois a passagem de mensagens de comunicação cliente/servidor elimina a necessidade de um sincronismo explícito. Normalmente esta comunicação é implementada utilizando-se as chamadas de processamento remoto – RPCs (Remote Procedure Calls). Na maioria das aplicações o cliente para de executar após enviar um pedido para o servidor.

Existem alguns mecanismos que permitem que o cliente continue executando após ter envido uma mensagem de pedido. Esse é um cliente não bloqueado que deve lembrar de verificar o resultado mais tarde ou utilizar um mecanismo que interrompa quando o resultado chegar. Mesmo assim , na maioria dos casos o sincronismo ainda está implícito ao mecanismo de passagem de mensagens. Uma exceção é quando o cliente impede que seja

interrompido em execuções de códigos críticos, isto acontece em sistemas de tempo real.
No servidor os pedidos de vários clientes podem chegar simultaneamente, ou inclusive chegar um pedido enquanto outro está sendo executado. O servidor deve ter um recurso para por os pedidos em fila ou processá-los ao mesmo tempo. Uma forma para que o servidor possa processar os pedidos concorrentemente é gerar um processo-filho para cada pedido, de qualquer forma o servidor tem que saber para onde enviar as respostas. A relação mestre/escravo difere da cliente/servidor por não termos um processo mestre governando todas as ações do escravo. Por exemplo, se um servidor gera processos-filhos para executar os pedidos concorrentemente, estes são escravos pois são governados pelo servidor.

- *Vantagens*

- Escalabilidade: Um sistema cliente/servidor pode ser expandido verticalmente pela adição de mais recursos à máquina servidora ou aumento do número de servidores – ou horizontalmente, pelo aumento do número de máquinas servidoras.
- Independência de plataformas: Os sistemas cliente/servidor não ficam presos a um ambiente de software ou hardware.
- Melhor Performance: Com a força de processamento distribuída, o tempo de processamento é menor, consequentemente o tempo de resposta também é menor.
- Fácil Acesso aos Dados: Como é o processo cliente que gerencia a interface, deixando o servidor livre para manipular os dados, este por sua vez fica mais disponível.
- Redução de Custos Operacionais: Como os custos de hardware e software estão constantemente sendo reduzidos, a troca dos sistemas grandes por sistemas com redes integradas pode ser feita com um baixo custo.

- Melhor Seguranca: porque o número de pontos de entrada que permitem o acesso aos dados é menos importante.
- Administração a nível do servidor : como os clientes têm pouca importância neste modelo, têm menos necessidade de ser administrados.
- Uma rede evolutiva: graças a esta arquitectura, é possível suprimir ou acrescentar clientes sem estar a perturbar o funcionamento da rede e sem modificação essencial

- Desvantagens

A arquitectura cliente/servidor tem no entanto algumas lacunas, entre as quais:

- Um custo elevado: devido ao tecnicismo do servidor .
- Um elo fraco: o servidor é o único elo fraco da rede cliente/servidor, já que toda a rede está estruturada em redor dele! Felizmente, o servidor tem uma grande tolerância às avarias devido ao sistemas de backup.

2.3 Topologias

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

Há várias formas nas quais se pode organizar a interligação entre cada um dos nós (computadores) da rede. Topologias podem ser descritas fisicamente e logicamente. A topologia física é a verdadeira aparência ou layout da rede, enquanto que a lógica descreve o fluxo dos dados através da rede.

Ao longo da historia das redes, varias topologias foram experimentadas, com maior ou menor sucesso. Os três tipos

abaixo são esquemas básicos empregados na conexão dos computadores. Os outros são variantes deles:

2.3.1 Estrela (STAR)

A mais comum atualmente, a topologia em estrela utiliza cabos de par trançado e um concentrador normalmente um hub ou switch. 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 nó ligado ao componente defeituoso ficará fora da rede. Esta topologia se aplica apenas a pequenas redes, já que os concentradores costumam ter apenas oito ou dezesseis portas. Em redes maiores é utilizada a topologia de árvore, onde temos vários concentradores interligados entre si por comutadores ou roteadores.

Fig 4 - Topologia em estrela

2.3.2 Barramento (BUS)

Uma topologia de rede em que todos os computadores são ligados em um mesmo barramento físico de dados. Apesar de os dados não passarem por dentro de cada um dos nós, apenas uma máquina pode “escrever” no barramento num dado momento. Todas as outras “escutam” e recolhem para si os dados destinados a elas. Quando um computador estiver a transmitir um sinal, toda

a rede fica ocupada e se outro computador tentar enviar outro sinal ao mesmo tempo, ocorre uma colisão e é preciso reiniciar a transmissão.

Essa topologia utiliza cabos coaxiais. Para cada barramento existe um único cabo, que vai de uma ponta a outra. O cabo é seccionado em cada local onde um micro será inserido na rede. Com o seccionamento do cabo formam-se duas pontas e cada uma delas recebe um conector BNC. No micro é colocado um "T" conectado à placa que junta as duas pontas. Embora ainda existam algumas instalações de rede que utilizam esse modelo, é uma tecnologia obsoleta.

Embora esta topologia descrita fisicamente ter caído em desuso, logicamente ela é amplamente usada. Redes ethernet utilizam este tipo lógico de topologia.

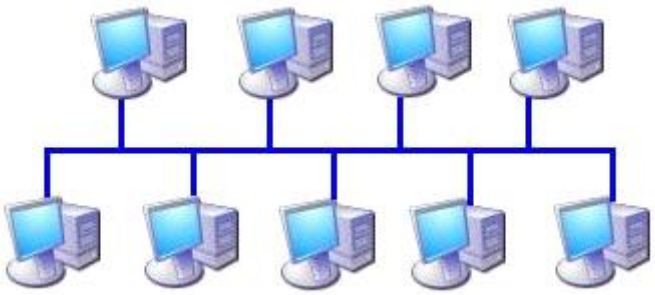


Fig 5 - Topologia em barramento

2.3.3 Anel (RING)

Na topologia em anel os dispositivos são conectados em série, formando um circuito fechado (anel). Os dados são transmitidos unidirecionalmente de nó em nó até atingir o seu destino. Uma mensagem enviada por uma estação passa por outras estações, através das retransmissões, até ser retirada pela estação destino ou pela estação fonte.Os sinais sofrem menos distorção e atenuação no enlace entre as estações, pois há um repetidor em

cada estação. Há um atraso de um ou mais bits em cada estação para processamento de dados. Há uma queda na confiabilidade para um grande número de estações. A cada estação inserida, há um aumento de retardo na rede. É possível usar anéis múltiplos para aumentar a confiabilidade e o desempenho. É a topologia das redes Token Ring, popularizadas pela IBM nos anos 80. Hoje, esse modelo é mais utilizado em sistemas de autmação industrial.

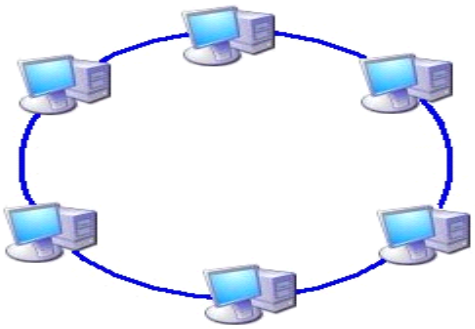


Fig 6– Topologia em Anel

2.4 Suporte de Transmissão

Muitos sistemas de comunicação fazem a transmissão dos dados utilizando fios de cobre (como par trançado, cabo coaxial), ou fibra ótica. Outros entretanto, transmitem os dados pelo ar, não utilizando qualquer tipo de meio físico, como é o caso da transmissão por raios infravermelhos, lasers, microondas e rádio. Cada uma destas técnicas é adequada a certas aplicações, que podem ser empregadas em LANs e WANs . Os meios de transmissao classificam-se em guiados e nao guiados.

2.4.1 Meios de Transmissao Guiados

Cabos

O projeto de cabeamento de uma rede, que faz parte do meio físico usado para interligar computadores, é um fator de extrema importância para o bom desempenho de uma rede. Esse projeto

envolve aspectos sobre a taxa de transmissão, largura de banda, facilidade de instalação, imunidade a ruídos, confiabilidade, custos de interface, exigências geográficas, conformidade com padrões internacionais e disponibilidades de componentes.

O sistema de cabeamento determina a estabilidade de uma rede. Pesquisas revelam que cerca de 80% dos problemas físicos ocorridos atualmente em uma rede tem origem no cabeamento, afetando de forma considerável a confiabilidade da mesma. O custo para a implantação do cabeamento corresponde a aproximadamente 6% do custo total de uma rede, mais 70% da manutenção de uma rede é direcionada aos problemas oriundos do cabeamento.

Fig 7 - Cabos

Em matéria de cabos, os mais utilizados são os cabos de par trançado, os cabos coaxiais e cabos de fibra óptica. Cada categoria tem suas próprias vantagens e limitações, sendo mais adequado para um tipo específico de rede.

Cabos de par trançado

São os mais usados pois tem um melhor custo beneficio, ele pode ser comprado pronto em lojas de informática, ou feito sob medida,

ou ainda produzido pelo próprio usuário, e ainda são 10 vezes mais rápidos que os cabos coaxiais.

O cabo par trançado surgiu com a necessidade de se ter cabos mais flexíveis e com maior velocidade de transmissão, ele vem substituindo os cabos coaxiais desde o início da década de 90. Hoje em dia é muito raro alguém ainda utilizar cabos coaxiais em novas instalações de rede, apesar do custo adicional decorrente da utilização de hubs e outros concentradores. O custo do cabo é mais baixo, e a instalação é mais simples.

O nome “par trançado” é muito conveniente, pois estes cabos são constituídos justamente por 4 pares de cabos entrelaçados. Os cabos coaxiais usam uma malha de metal que protege o cabo de dados contra interferências externas; os cabos de par trançado por sua vez, usam um tipo de proteção mais sutil: o entrelaçamento dos cabos cria um campo eletromagnético que oferece uma razoável proteção contra interferências externas.

Fig 8 – Cabos de par trancado

Existem basicamente dois tipos de cabo par trançado. Os Cabos sem blindagem chamados de UTP (Unshielded Twisted Pair) e os blindados conhecidos como STP (Shielded Twisted Pair). A única diferença entre eles é que os cabos blindados além de contarem com a proteção do entrelaçamento dos fios, possuem uma blindagem externa (assim como os cabos coaxiais), sendo mais adequados a ambientes com fortes fontes de interferências, como grandes motores elétricos e estações de rádio que estejam muito próximas. Outras fontes menores de interferências são as

lâmpadas fluorescentes (principalmente lâmpadas cansadas que ficam piscando), cabos elétricos quando colocados lado a lado com os cabos de rede e mesmo telefones celulares muito próximos dos cabos.

Na realidade o par trançado sem blindagem possui uma ótima proteção contra ruídos, só que usando uma técnica de cancelamento e não através de uma blindagem. Através dessa técnica, as informações circulam repetidas em dois fios, sendo que no segundo fio a informação possui a polaridade invertida. Todo fio produz um campo eletromagnético ao seu redor quando um dado é transmitido. Se esse campo for forte o suficiente, ele irá corromper os dados que estejam circulando no fio ao lado (isto é, gera Ruído).

Fig 9 – Placa de rede para cabo de par trancado

Além disso, como a informação é transmitida duplicada, o receptor pode facilmente verificar se ela chegou ou não corrompida. Tudo o que circula em um dos fios deve existir no outro fio com intensidade igual, só que com a polaridade invertida. Com isso, aquilo que for diferente nos dois sinais é ruído e o receptor tem como facilmente identificá-lo e eliminá-lo.

Quanto maior for o nível de interferência, menor será o desempenho da rede, menor será a distância que poderá ser usada entre os micros e mais vantajosa será a instalação de cabos blindados. Em ambientes normais porém os cabos sem blindagem

costumam funcionar bem.

Existem no total, 5 categorias de cabos de par trançado. Em todas as categorias a distância máxima permitida é de 100 metros. O que muda é a taxa máxima de transferência de dados e o nível de imunidade a interferências. Os cabos de categoria 5 que tem a grande vantagem sobre os outros 4 que é a taxa de transferência que pode chegar até 100 mbps, e são praticamente os únicos que ainda podem ser encontrados à venda, mas em caso de dúvida basta checas as inscrições no cabo, entre elas está a categoria do cabo, como na foto abaixo.

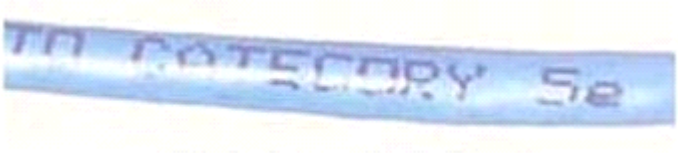


Fig 10 – Cabo com categoria 5e

A utilização do cabo de par trançado tem suas vantagens e desvantagens, vejamos as principais:

Vantagens

- Preço: Mesma com a obrigação da utilização de outros equipamentos na rede, a relação custo beneficia se torna positiva.

- Flexibilidade: Como ele é bastante flexível, ele pode ser facilmente passado por dentro de conduítes embutidos em paredes.

- Facilidade: A facilidade com que se pode adquirir os cabos, pois em qualquer loja de informática existe esse cabo para venda, ou até mesmo para o próprio usuário confeccionar os cabos.

- Velocidade: Atualmente esse cabo trabalha com uma taxa de transferência de 100 Mbps.

Desvantagens

- Comprimento: Sua principal desvantagem é o limite de comprimento do cabo que é de aproximadamente 100 por trecho.

- Interferência: A sua baixa imunidade à interferência eletromagnética, sendo fator preocupante em ambientes industriais.

No cabo de par trançado tradicional existem quatro pares de fio. Dois deles não são utilizados pois os outros dois pares, um é utilizado para a transmissão de dados (TD) e outro para a recepção de dados (RD). Entre os fios de números 1 e 2 (chamados de TD+ e TD–) a placa envia o sinal de transmissão de dados, e entre os fios de números 3 e 6 (chamados de RD+ e RD–) a placa recebe os dados. Nos hubs e switches, os papéis desses pinos são invertidos. A transmissão é feita pelos pinos 3 e 6, e a recepção é feita pelos pinos 1 e 2. Em outras palavras, o transmissor da placa de rede é ligado no receptor do hub ou switch, e vice-versa.

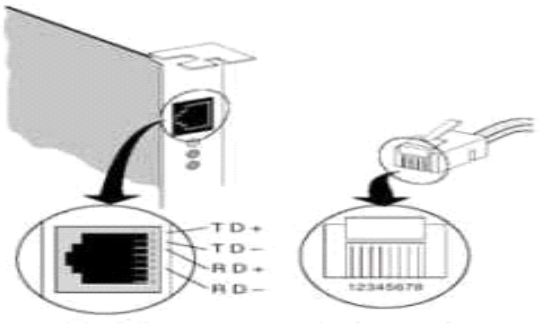


Fig 11 – Pares de Fios de TD e RD

Um cuidado importante a ser tomado é que sistemas de telefonia utilizam cabos do tipo par trançado, só que este tipo de cabo não serve para redes locais.

Cabos Coaxiais

Os cabos coaxiais permitem que os dados sejam transmitidos através de uma distância maior que a permitida pelos cabos de par trançado sem blindagem (UTP), mas por outro, lado não são tão flexíveis e são mais caros que eles. Outra desvantagem é que a maioria delas requerem o barramento ISA, não encontradas nas Placas mães novas.

O cabo coaxial foi o primeiro cabo disponível no mercado, e era até a alguns anos atrás o meio de transmissão mais moderno que existia em termos de transporte de dados, existem 4 tipos diferentes de cabos coaxiais, chamados de 10Base5, 10Base2, RG-59/U e RG-62/U.

O cabo 10Base5 é o mais antigo, usado geralmente em redes baseadas em mainframes. Este cabo é muito grosso, tem cerca de 0.4 polegadas, ou quase 1 cm de diâmetro e por isso é muito caro e difícil de instalar devido à baixa flexibilidade. Outro tipo de cabo coaxial é o RG62/U, usado em redes Arcnet. Temos também o cabo RG-59/U, usado na fiação de antenas de TV.

Os cabos 10Base2, também chamados de cabos coaxiais finos, ou cabos Thinnet, são os cabos coaxiais usados atualmente em redes Ethernet, e por isso, são os cabos que você receberá quando pedir por “cabos coaxiais de rede”. Seu diâmetro é de apenas 0.18 polegadas, cerca de 4.7 milímetros, o que os torna razoavelmente flexíveis.

Os cabos coaxiais são cabos constituídos de 4 camadas: um condutor interno, o fio de cobre que transmite os dados; uma camada isolante de plástico, chamada de dielétrico que envolve o cabo interno; uma malha de metal que protege as duas camadas internas e, finalmente, uma nova camada de revestimento, chamada de jaqueta.

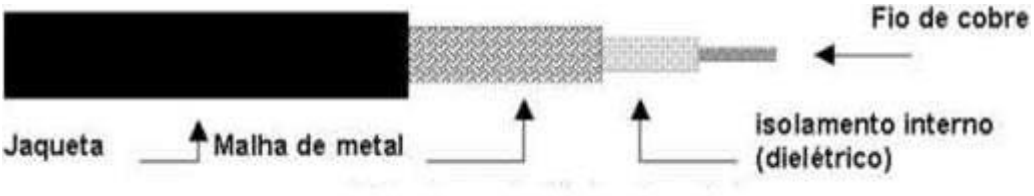


Fig 12 – Estrutura do Cabo Coaxial

O cabo Thin Ethernet deve formar uma linha que vai do primeiro ao último PC da rede, sem formar desvios. Não é possível portanto formar configurações nas quais o cabo forma um "Y", ou que usem qualquer tipo de derivação. Apenas o primeiro e o último micro do cabo devem utilizar o terminador BNC.

Fig 12 – Placa de rede para rede com cabo coaxial

O Cabo 10base2 tem a vantagem de dispensar hubs, pois a ligação entre os micros é feita através do conector "T", mesmo assim o cabo coaxial caiu em desuso devido às suas desvantagens:

- Custo elevado,
- Instalação mais difícil e mais fragilidade,
- Se o terminador for retirado do cabo, toda a rede sai do ar.

Redes formadas por cabos Thin Ethernet são de implementação um pouco complicada. É preciso adquirir ou construir cabos com medidas de acordo com a localização física dos PCs. Se um dos PCs for reinstalado em outro local é preciso utilizar novos cabos, de

acordo com as novas distâncias entre os PCs. Pode ser preciso alterar duas ou mais seções de cabo de acordo com a nova localização dos computadores. Além disso, os cabos coaxiais são mais caros que os do tipo par trançado.

Fig 13 – Placa de rede para rede com cabo coaxial

O “10” na sigla 10Base2, significa que os cabos podem transmitir dados a uma velocidade de até 10 megabits por segundo, “Base” significa “banda base” e se refere à distância máxima para que o sinal pode percorrer através do cabo, no caso o “2” que teoricamente significaria 200 metros, mas que na prática é apenas um arredondamento, pois nos cabos 10Base2 a distância máxima utilizável é de 185 metros.

Fig 14 – Cabo de rede coaxial

Usando cabos 10Base2, o comprimento do cabo que liga um micro ao outro deve ser de no mínimo 50 centímetros, e o comprimento total do cabo (do primeiro ao último micro) não pode superar os 185 metros. É permitido ligar até 30 micros no mesmo cabo, pois acima disso, o grande número de colisões de pacotes irá prejudicar

o desempenho da rede, chegando a ponto de praticamente impedir a comunicação entre os micros em casos extremos.

Fibra Optica

Permitem transmissões de dados a velocidades muito maiores e são completamente imunes a qualquer tipo de interferência eletromagnética, porém, são muito mais caros e difíceis de instalar, demandando equipamentos mais caros e mão de obra mais especializada. Apesar da alta velocidade de transferência, as fibras ainda não são uma boa opção para pequenas redes devido ao custo.

Sem as fibras ópticas, a Internet e até o sistema telefônico que temos hoje seriam inviáveis. Com a migração das tecnologias de rede para padrões de maiores velocidades como ATM, Gigabit Ethernet e 10 Gigabit Ethernet, o uso de fibras ópticas vem ganhando força também nas redes locais. O produto começou a ser fabricado em 1978 e passou a substituir os cabos coaxiais nos Estados Unidos na segunda metade dos anos 80. Em 1988, o primeiro cabo submarino de fibras ópticas mergulhou no oceano, dando inicio a superestrada da informação. O físico indiano Narinder Singh Kanpany é o inventor da fibra óptica, que passou a ter aplicações praticas na década de 60 com o advento da criação de fontes de luz de estado sólido, como o raio laser e o LED, diodo emissor de luz. Sua origem, porem, data do século 19, com os primeiros estudos sobre os efeitos da luz.

Existem dois tipos de fibras ópticas: As fibras multímodo e as monomodo. A escolha de um desses tipos dependera da aplicação da fibra.

As fibras multímodo são mais utilizadas em aplicações de rede locais (LAN), enquanto as monomodo são mais utilizadas para aplicações de rede de longa distancia (WAN). São mais caras, mas também mais eficientes que as multímodo. Aqui no Brasil, a

utilização mais ampla da fibra óptica teve inicio ma segunda metade dos anos 90, impulsionada pela implementação dos backbones das operadoras de redes metropolitanas.

Ao contrário dos cabos coaxiais e de par trançado, que nada mais são do que fios de cobre que transportam sinais elétricos, a fibra óptica transmite luz e por isso é totalmente imune a qualquer tipo de interferência eletromagnética. Além disso, como os cabos são feitos de plástico e fibra de vidro (ao invés de metal), são resistentes à corrosão.

O cabo de fibra óptica é formado por um núcleo extremamente fino de vidro, ou mesmo de um tipo especial de plástico. Uma nova cobertura de fibra de vidro, bem mais grossa envolve e protege o núcleo. Em seguida temos uma camada de plástico protetora chamada de cladding, uma nova camada de isolamento e finalmente uma capa externa chamada bainha.

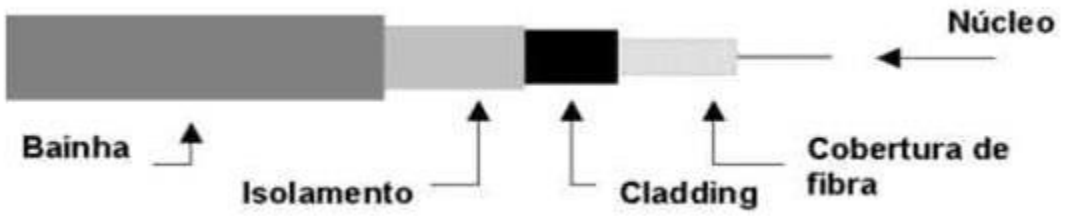


Fig 15 – Estrutura do Cabo de Fibra Optica

A transmissão de dados por fibra óptica é realizada pelo envio de um sinal de luz codificado, dentro do domínio de freqüência do infravermelho a uma velocidade de 10 a 15 MHz. As fontes de transmissão de luz podem ser diodos emissores de luz (LED) ou lasers semicondutores. O cabo óptico com transmissão de raio laser é o mais eficiente em potência devido a sua espessura reduzida. Já os cabos com diodos emissores de luz são muito baratos, além de serem mais adaptáveis à temperatura ambiente e de terem um ciclo de vida maior que o do laser.

O cabo de fibra óptica pode ser utilizado tanto em ligações ponto a ponto quanto em ligações multímodo. A fibra óptica permite a transmissão de muitos canais de informação de forma simultânea pelo mesmo cabo. Utiliza, por isso, a técnica conhecida como multiplexação onde cada sinal é transmitido numa freqüência ou num intervalo de tempo diferente.

Fig 16 – Placa de Rede com Conectores para Fibra Optica

A fibra óptica tem inúmeras vantagens sobre os condutores de cobre, sendo as principais:

- Maior alcance
- Maior velocidade
- Imunidade a interferências eletromagnéticas

O custo do metro de cabo de fibra óptica não é elevado em comparação com os cabos convencionais. Entretanto seus conectores são bastante caros, assim como a mão de obra necessária para a sua montagem. A montagem desses conectores, além de um curso de especialização, requer instrumentos especiais, como microscópios, ferramentas especiais para corte e polimento, medidores e outros aparelhos sofisticados.

Fig 17 – Cabo de Fibra Optica

Devido ao seu elevado custo, os cabos de fibras ópticas são usados apenas quando é necessário atingir grandes distâncias em redes que permitem segmentos de até 1 KM, enquanto alguns tipos de cabos especiais podem conservar o sinal por até 5 KM (distâncias maiores são obtidas usando repetidores).

Mesmo permitindo distâncias tão grandes, os cabos de fibra óptica permitem taxas de transferências de até 155 mbps, sendo especialmente úteis em ambientes que demandam uma grande transferência de dados. Como não soltam faíscas, os cabos de fibra óptica são mais seguros em ambientes onde existe perigo de incêndio ou explosões. E para completar, o sinal transmitido através dos cabos de fibra é mais difícil de interceptar, sendo os cabos mais seguros para transmissões sigilosas. A seguir veremos os padrões mais comuns de redes usando fibra ótica:

- FDDI (Fiber Distributed Data Interface)
- FOIRL (Fiber- Optic InterRepeater Link)
- 10BaseFL
- 100BaseFX
- 1000BaseSX
- 1000BaseLX

2.4.2 Meios de Transmissao Não Guiados

Na realidade, o ar (ou espaço livre) constitui-se de um meio natural para a propagação de sinais eletromagnéticos, podendo talvez, ser considerado o melhor suporte de transmissão, quando se fala em conectividade. Tal afirmação baseia-se no fato de que o ar provê uma interconexão completa, e permite uma grande flexibilidade na localização das estações.

Existem também alguns incovenientes com relação ao sistema, sendo que os principais são:

- Custo dos equipamentos ;
- Regulamentação pública .

A escolha de canais de radiofrequência para sistemas de comunicação, de uma forma geral, é bastante complicada, pois vários fatores devem ser observados, entre eles:

- Banda passante desejada;
- Área de cobertura;
- Disponibilidade do espectro;
- Interferências e fontes de ruído;
- Regulamentação pública;
- Custos dos equipamentos.

Excepto pela radiação eletromagnética, e provavelmente as ondas gravitacionais, que podem se propagar através do vácuo, as ondas existem em um meio cuja deformação é capaz de produzir forças de restauração através das quais elas viajam e podem transferir energia de um lugar para outro sem que qualquer das partículas do meio seja deslocada; isto é, a onda não transporta matéria. Há, entretanto, oscilações sempre associadas ao meio de propagação.

Uma onda pode ser longitudinal quando a oscilação ocorre na direcção da propagação, ou transversal quando a oscilação ocorre na direcção perpendicular à direcção de propagação da onda.

Ondas de Rádio e micro-ondas

Trata-se do mesmo tipo de ondas que são radiações eletromagnéticas com comprimento de onda maior e freqüência menor do que a radiação infravermelha. São usadas para a comunicação em rádios amadores, radiodifusão (rádio e televisão), telefonia móvel situadas normalmente, na faixa dos 2 a 2,5 Gigahertzs.

Nesta também estão incluídas as ondas do tipo VHF e UHF.

Um dos vários tipos de onda, as ondas hertzianas são popularmente conhecidas como ondas de rádio-frequência ou simplesmente ondas de rádio. Usadas, principalmente, em difusão de rádio, elas estão também presentes na difusão de televisão, em sistemas de comunicação terrestre ou via satélite, radionavegação, radiolocalização e diatermia.

Em Física, as ondas hertzianas podem ser definidas, de maneira simples, como radiações eletromagnéticas produzidas por inversões rápidas de corrente em um condutor. Elas são parte das ondas que formam uma onda eletromagnética, juntamente com Transmissão por irradiação eletromagnetica. Dados transmitidos por sinais eletricos irradiados por antenas através do espaço. O rádio (receptor) é um aparelho que tem a função de receber estas ondas eletromagnéticas, através de sua antena, e transformá-las em sons compreensíveis ao ouvido humano. As ondas hertzianas dividem-se em bandas de rádio que variam entre as frequências de 30 kilohertz (muito baixas) a 300 mil megahertz (extremamente altas). Estas bandas são agrupadas e classificadas de acordo com a frequência em que transmitem. As frequências são classificadas em grupos, e estes grupos são comumente chamados por: onda curta, onda média e onda longa. Dentro destes segmentos, encaixam-se estações de radiodifusão, serviços de comunicação

aérea, marítima, telegrafia etc.

As ondas de radio podem passar atraves de paredes, enquanto as microondas necessitam, regra geral, de um espaco limpo de obstrucoes.

A principal desvantagem deste tipo de redes e a sua normallmente baixa capacidade em termos de velocidade de transmissao que se situa, por exemplo, na ordem dos 250 a 4800 Kbits/seg

2.4.5 Infravermelho

A radiação infravermelha é uma radiação não ionizante na porção invisível do espectro eletromagnético que está adjacente aos comprimentos de onda longos, ou final vermelho do espectro da luz visível. Ainda que em vertebrados não seja percebida na forma de luz, a radiação pode ser percebida como calor, por terminações nervosas especializadas da pele, conhecidas como termorreceptores.
Esta radiação é muito utilizada nas trocas de informações entre computadores, celulares e outros eletrônicos, através do uso de um

2.4.5 BLUETOOTH

O nome Bluetooth é uma homenagem ao rei da Dinamarca e Noruega Harald Blåtand - em inglês Harold Bluetooth (traduzido como dente azul, embora em dinamarquês signifique de tez escura). Blåtand é conhecido por unificar as tribos norueguesas, suecas e dinamarquesas. Da mesma forma, o protocolo procura unir diferentes tecnologias, como telefones móveis e computadores.
O logotipo do Bluetooth é a união das runas nórdicas ᚼ(Hagall) e (Berkanan) correspondentes às letras H e B no alfabeto latino.
É um protocolo padrão de comunicação primariamente projetado para baixo consumo de energia com baixo alcance, (dependendo da potência: 1 metro, 10 metros, 100 metros) baseado em

microchips transmissores de baixo custo em cada dispositivo. O Bluetooth 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.

Dispositivos Bluetooth operam na faixa ISM (Industrial, Scientific, Medical) centrada em 2,45 GHz que era formalmente reservada para alguns grupos de usuários profissionais. Nos Estados Unidos, a faixa ISM varia de 2400 a 2483,5 MHz. Na maioria da Europa a mesma banda também está disponível. No Japão a faixa varia de 2400 a 2500 MHz. Os dispositivos são classificados de acordo com a potência e alcance, em três níveis: classe 1, classe 2 e classe 3 (uma variante muito rara). A banda é dividida em 79 portadoras espaçadas de 1 MegaHertz, portanto cada dispositivo pode transmitir em 79 freqüências diferentes; para minimizar as interferências, o dispositivo mestre, após sincronizado, pode mudar as freqüências de transmissão de seus escravos por até 1600 vezes por segundo. Teoricamente sua velocidade pode chegar a 721 Kbps e possui três canais de voz.

Classe	Potência máxima permitida	Alcance (Aproximadamente
Classe 1	100 mW (20 dBm)	até 100 metros
Classe 2	2.5 mW (4 dBm)	até 10 metros
Classe 3	1 mW (0 dBm)	~ 1 metro

Tabel
a 2
Deve-se ressaltar que, na maioria dos casos, o alcance efetivo dos dispositivos de classe 2 é estendido se eles se conectam a dispositivos de classe 1, se comparados com redes puras de classe

2. Isso pode ser obtido pela alta sensibilidade e potência de transmissão do dispositivo de classe 1. A alta potência de transmissão do dispositivo de classe 1 permite a recepção da alta potência pelo dispositivo de classe 2. Além disso, a alta sensibilidade do dispositivo de classe 1 permite a recepção da baixa potência de transmissão de força dos dispositivos de classe 2, permitindo assim a operação de dispositivos de classe 2 a grandes distâncias. Dispositivos que possuem um amplificador de potência na transmissão têm uma sensibilidade de recepção melhorada, e existem antenas altamente otimizadas que normalmente alcançam distâncias de 1 km usando o padrão Bluetooth classe 1.

Versão	Taxa de transmissão
Versão 1.2	1 Mbit/s
Versão 2.0 + EDR	3 Mbit/s
Versão 3.0	24 Mbit/s

Tabela 3

Para usar a tecnologia Bluetooth, o dispositivo deve ser compatível com certos perfis Bluetooth. Esses perfis determinam as possíveis aplicações e usos da tecnologia.

As aplicações mais prevalentes do Bluetooth incluem:

- Controle sem fio e comunicação entre celulares e fones de ouvido sem fio ou sistemas viva voz para carros. Essa foi uma das mais antigas aplicações da tecnologia a se tornar popular.

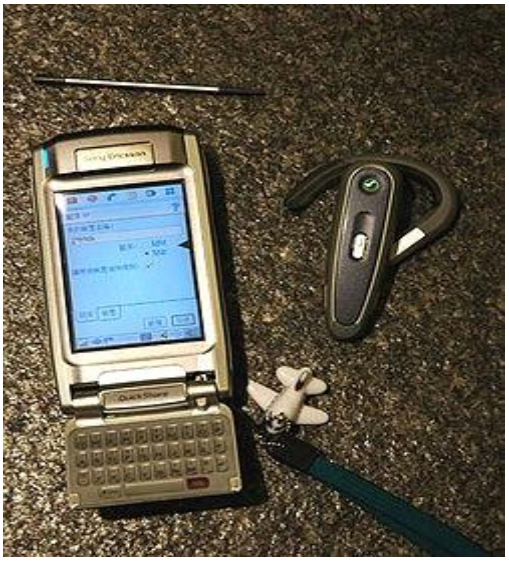


Fig 18 - Sony Ericsson P910i e auricular Bluetooth.

- Comunicação sem fio entre PCs em um espaço pequeno onde pequena banda é necessária.

- Comunicação sem fio entre PCs e dispositivos de entrada e saída, como mouse, teclados e impressoras.

- Comunicação sem fio entre telefones celulares e estações de telefonia fixa, para funcionar como um telefone sem fio dentro da área de cobertura e economizar em tarifas de serviço telefônico.

- Transferência de arquivos entre dispositivos usando OBEX.

- Tranferência de contatos, anotações e eventos de calendário e lembretes entre dispositivos com OBEX.

- Substituição de dispositivos seriais tradicionais com fio em equipamentos de teste, receptores GPS, equipamentos médicos, leitores de código de barras e dispositivos de controle de tráfego.

Existem vários produtos ativados por Bluetooth, como celulares,

impressoras, modems e fones de ouvido sem fio. A tecnologia é útil quando é necessária transferência de informações entre dois ou mais dispositivos que estão perto um do outro ou em outras situações onde não é necessária alta taxa de transferência. O Bluetooth é comumente usado para transferir dados de áudio para/de celulares (por exemplo, com um fone sem fio) ou transferir dados entre computadores de bolso (transferência de arquivos).

Bluetooth simplifica a descoberta e configuração de serviços entre dispositivos. Os dispositivos Bluetooth anunciam todos os serviços que eles suportam e podem fornecer, e por isso, faz com que o uso de serviços seja simples pela falta da necessidade de configurar endereços de rede ou permissões como em outras tecnologias.

3. Protocolos

Uma rede de computadores não pode ser bem estabelecida considerando apenas o hardware como preocupação principal como nas primeiras redes, actualmente o software é considerado uma das partes mais importantes na concepção de novas tecnologias de redes de computadores.

Na ciência da computação, um protocolo é uma convenção ou padrão que controla e possibilita uma conexão, comunicação ou transferência de dados entre dois sistemas computacionais. De maneira simples, um protocolo pode ser definido como "as regras que governam" a sintaxe, semântica e sincronização da comunicação ou ainda conjunto estabelecido ou aceito de procedimentos, regras ou especificações formais que governam a comunicação entre os nós de uma rede. Os protocolos podem ser implementados pelo *hardware*, *software* ou por uma combinação dos dois.

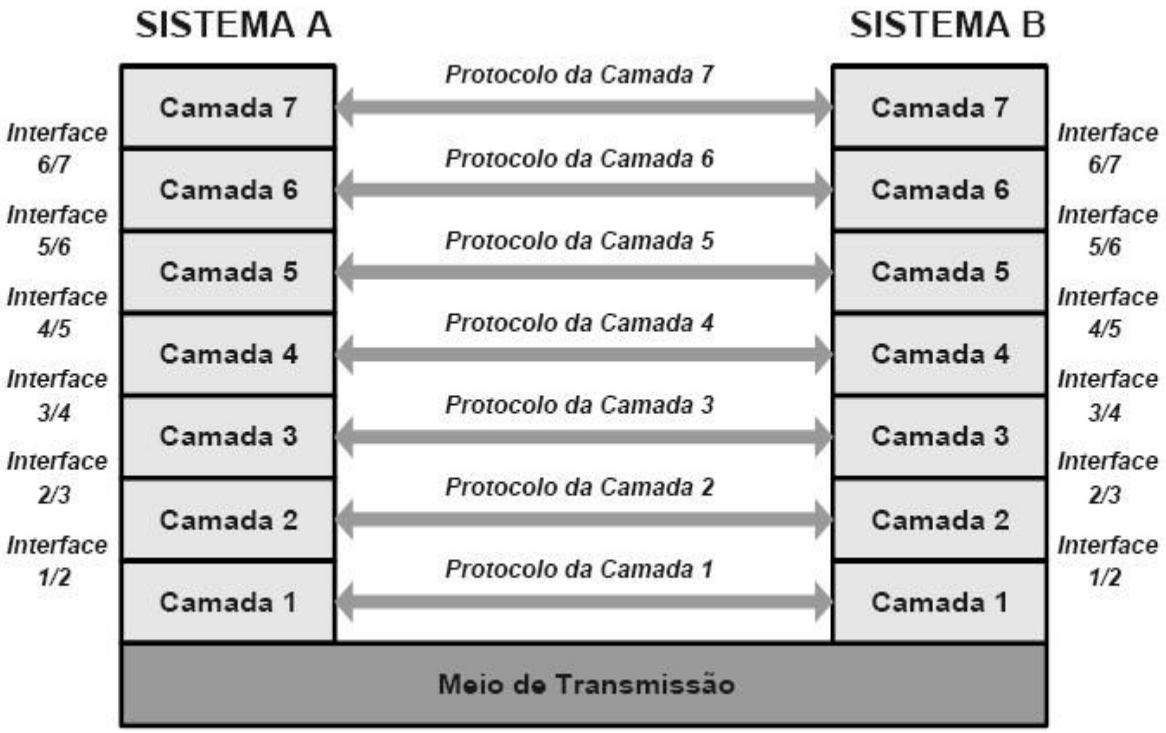


Fig 19 – Protocolos

É difícil generalizar sobre protocolos pois eles variam muito em propósito e sofisticação. A maioria dos protocolos especifica uma ou mais das seguintes propriedades:

- Detecção da conexão física subjacente ou a existência de um nó;

- Estabelecimento de ligação (handshaking);

- Negociação de várias características de uma conexão;

- Como iniciar e finalizar uma mensagem;

- Como formatar uma mensagem;

- O que fazer com mensagens corrompidas ou mal formatadas;

- Como detectar perda inesperada de conexão e o que fazer em seguida;

- Término de sessão ou conexão

3.2 Protocolos de comunicação

O uso difundido e a expansão dos protocolos de comunicação é ao mesmo tempo um pré-requisito e uma contribuição para o poder e sucesso da Internet. O par formado por IP e TCP é uma referência a uma coleção dos protocolos mais utilizados. A maioria dos protocolos para comunicação via Internet é descrita nos documentos RFC do IETF.

Geralmente apenas os protocolos mais simples são utilizados sozinhos. A maioria dos protocolos, especialmente no contexto da comunicação em rede de computadores, são agrupados em pilhas de protocolo onde as diferentes tarefas que perfazem uma comunicação são executadas por níveis especializados da pilha.

Enquanto uma pilha de protocolos denota uma combinação específica de protocolos que trabalham conjuntamente, um modelo de referência é uma arquitetura de software que lista cada um dos níveis e os serviços que cada um deve oferecer. O modelo clássico OSI, em sete níveis, é utilizado para conceitualizar pilhas de protocolo.

Exemplos de protocolos de comunicação em rede

- IP (Internet Protocol)
- DHCP (Dynamic Host Configuration Protocol)
- TCP (Transmission Control Protocol)
- HTTP (Hypertext Transfer Protocol)
- FTP (File Transfer Protocol)
- Telnet (Telnet Remote Protocol)
- SSH (SSH Remote Protocol)
- POP3 (Post Office Protocol 3)
- SMTP (Simple Mail Transfer Protocol)
- IMAP (Internet Message Access Protocol)

3.3 Protocolos de roteamento

Todos os protocolos de roteamento realizam as mesmas funções básicas. Eles determinam a rota preferida para cada destino e distribuem informações de roteamento entre os sistemas da rede. Como eles realizam estas funções, em particular eles decide qual é a melhor rota, é a principal diferença entre os protocolos de roteamento.

Tipos de Protocolos

IGP (Interior Gateway Protocol) - Estes são utilizados para realizar o roteamento dentro de um Sistema Autônomo. Existem vários protocolos IGP, vejamos alguns:

- RIP (Routing Information Protocol)
- IGRP (Interior Gateway Routing Protocol)
- Enhanced IGRP
- OSPF (Open Shortest Path First)
- IS-IS (Intermediate System-to-Intermediate System)

EGP (Exterior Gateway Protocol) - Estes são utilizados para realizar o roteamento entre Sistemas Autônomos diferentes. É dividido em:

EGP (Exterior Gateway Protocol) - protocolo tem o mesmo nome que o seu tipo.
BGP (Border Gateway Protocol)

6. Modelos de referência

4.1 Arquitectura OSI

ISO foi uma das primeiras organizações a definir formalmente uma

forma comum de conectar computadores. 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. Cada protocolo implementa uma funcionalidade assinalada a uma determinada camada.

A ISO costuma trabalhar em conjunto com outra organização, a ITU (International Telecommunications Union), publicando uma série de especificações de protocolos baseados na arquitetura OSI.

Este modelo é dividido em 7 camadas hierárquicas, ou seja, cada camada usa as funções da própria camada ou da camada anterior, para esconder a complexidade e transparecer as operações para o usuário, seja ele um programa ou uma outra camada.

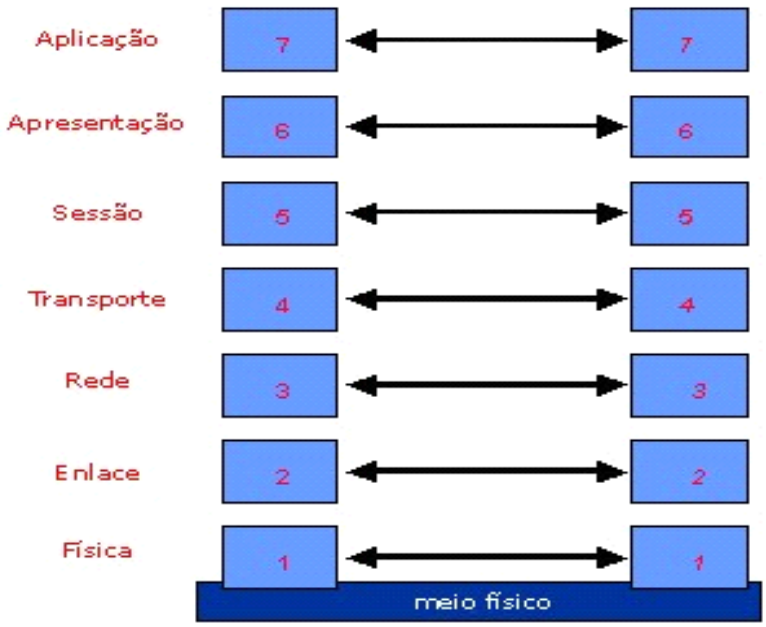


Fig 20 Camadas do Modelo OSI

1 - Camada Física

Define as características técnicas dos dispositivos elétricos (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. Preocupa-se, portanto, em permitir uma comunicação bastante simples e confiável, na maioria dos casos com controle de erros básico:

- Move bits (ou bytes, conforme a unidade de transmissão) através de um meio de transmissão.
- Define as características elétricas e mecânicas do meio, taxa de transferência dos bits, tensões etc.
- Controle de acesso ao meio.
- Controle da quantidade e velocidade de transmissão de informações na rede.

Não é função do nível físico tratar problemas como erros de transmissão, esses são tratados pelas outras camadas do modelo OSI.

2 - Camada Enlace ou 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.

Exemplo de protocolos nesta camada: PPP, LAPB, NetBios.

Na Rede Ethernet cada placa de rede possui um endereço físico, que deve ser único na rede.

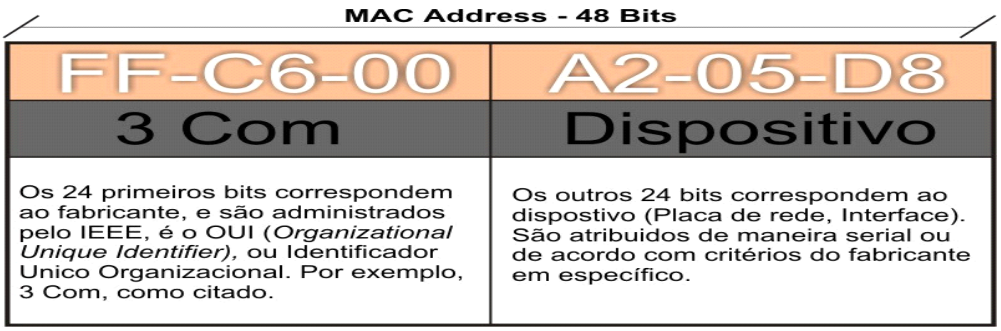


Fig 21 Estrutura do Endereco Fisico

3 - Camada de Rede

É responsável pelo endereçamento dos pacotes, convertendo endereços lógicos (ou IP) em endereços físicos , 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.

Essa camada é usada quando a rede possui mais de um segmento e, com isso, há mais de um caminho para um pacote de dados percorrer da origem ao destino.

Funções da Camada:

- Encaminhamento, endereçamento, interconexão de redes, tratamento de erros, fragmentação de pacotes, controle de congestionamento e sequenciamento de pacotes.

- 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.

4 - Camada de Transporte

É responsável por usar os dados enviados pela camada de Sessão

e dividilos em pacotes que serão transmitidos para a camada de Rede. No receptor, a camada de Transporte é responsável por pegar os pacotes recebidos da camada de Rede, remontar o dado original e assim enviá-lo à camada de Sessão.

Isso inclui controle de fluxo, ordenação dos pacotes e a correção de erros, tipicamente enviando para o transmissor uma informação de recebimento, informando que o pacote foi recebido com sucesso.

A camada de Transporte separa as camadas de nível de aplicação (camadas 5 a 7) das camadas de nível físico (camadas de 1 a 3). A camada 4, Transporte, faz a ligação entre esses dois grupos e determina a classe de serviço necessária como orientada a conexão e com controle de erro e serviço de confirmação, sem conexões e nem confiabilidade.

O objetivo final da camada de transporte é proporcionar serviço eficiente, confiável e de baixo custo. O hardware e/ou software dentro da camada de transporte e que faz o serviço é denominado entidade de transporte.

A entidade de transporte comunica-se com seus usuários através de primitivas de serviço trocadas em um ou mais TSAP(Transport Service Access Point), que são definidas de acordo com o tipo de serviço prestado: orientado ou não à conexão. Estas primitivas são transportadas pelas TPDU (Transport Protocol Data Unit).

A ISO define o protocolo de transporte para operar em dois modos:

- Orientado a conexão.

- Não-Orientado a conexão.

Como exemplo de protocolo orientado à conexão, temos o TCP, e de protocolo não orientado à conexão, temos o UDP. É obvio que o protocolo de transporte não orientado à conexão é menos confiável. Ele não garante - entre outras coisas mais -, a entrega

das TPDU, nem tampouco a ordenação das mesmas. Entretanto, onde o serviço da camada de rede e das outras camadas inferiores é bastante confiável - como em redes locais -, o protocolo de transporte não orientado à conexão pode ser utilizado, sem o overhead inerente a uma operação orientada à conexão.
O serviço de transporte baseado em conexões é semelhante ao serviço de rede baseado em conexões. O endereçamento e controle de fluxo também são semelhantes em ambas as camadas. Para completar, o serviço de transporte sem conexões também é muito semelhante ao serviço de rede sem conexões. Constatado os fatos acima, surge a seguinte questão: "Por que termos duas camadas e não uma apenas?". A resposta é sutil, mas procede: A camada de rede é parte da sub-rede de comunicações e é executada pela concessionária que fornece o serviço (pelo menos para as WAN). Quando a camada de rede não fornece um serviço confiável, a camada de transporte assume as responsabilidades, melhorando a qualidade do serviço.

5 - 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. Se porventura a rede falhar, os computadores reiniciam a transmissão dos dados a partir da última marcação recebida pelo computador receptor.

Disponibiliza serviços como pontos de controles periódicos a partir dos quais a comunicação pode ser restabelecida em caso de pane na rede.

Abre portas para que várias aplicações possam escalonar o uso da rede e aproveitar melhor o tempo de uso. Por exemplo, um browser quando for fazer o download de várias imagens pode requisitá-las juntas para que a conexão não fique desocupada

numa só imagem.

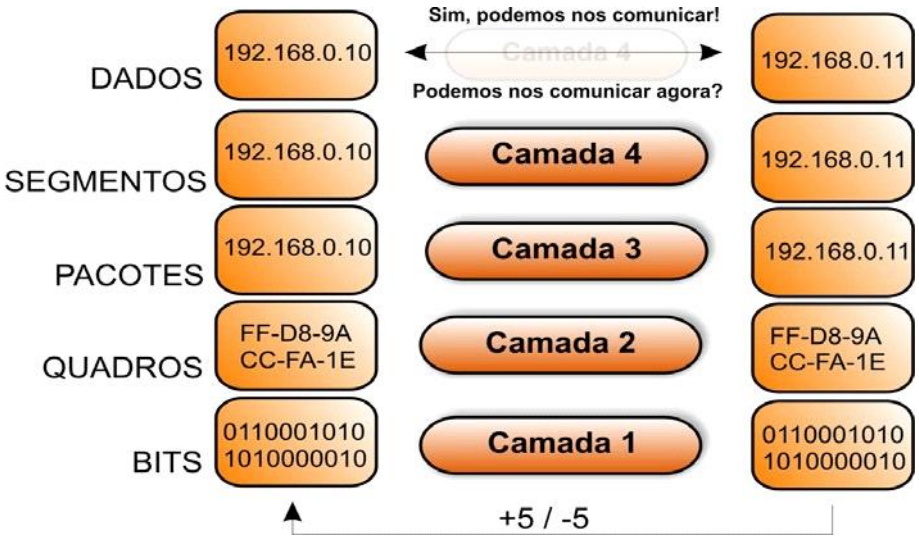


Fig 22 Demostracao da Funcao da Camda de Sessao

7 - Camada de Apresentação

Também chamada de 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. Pode ter outros usos, como compressão de dados e criptografia.

Os dados recebidos da camada sete são comprimidos, e a camada 6 do dispositivo receptor fica responsável por descomprimir esses dados. A transmissão dos dados torna-se mais rápida, já que haverá menos dados a serem transmitidos: os dados recebidos da camada 7 foram "encolhidos" e enviados à camada 5.

Para aumentar a segurança, pode-se usar algum esquema de criptografia neste nível, sendo que os dados só serão decodificados na camada 6 do dispositivo receptor.

Ela trabalha transformando os dados em um formato no qual a

camada de aplicação possa aceitar.

7 - Camada de Aplicação

Faz a interface entre o protocolo de comunicação e o aplicativo que pediu ou receberá a informação através da rede. Por exemplo, ao solicitar a recepção de e-mails através do aplicativo de e-mail, este entrará em contato com a camada de Aplicação do protocolo de rede efetuando tal solicitação. Tudo nesta camada é direcionado aos aplicativos. Telnet e FTP são exemplos de aplicativos de rede que existem inteiramente na camada de aplicação.

Como podemos observar, o modelo de protocolo trabalha com 7 camadas para padronizar a transmissão de dados em uma rede.Essas camadas nem sempre são as mesmas que iremos encontrar nos outros protocolos, mas o processo de troca de informações é o mesmo.

4.2 TCP/IP

é um acrônimo para o termo Transmission Control Protocol/Internet Protocol Suite, ou seja é um conjunto de protocolos, onde dois dos mais importantes (o IP e o TCP) deram seus nomes à arquitetura. O protocolo IP, base da estrutura de comunicação da Internet é um protocolo baseado no paradigma de chaveamento de pacotes (packet-switching).

representa um conjunto de protocolos que permitem que diversos equipamentos que constituem uma rede possam comunicar entre si. É um protocolo estruturado por camadas na qual cada camada utiliza e presta serviços às camadas adjacentes. Cada camada apenas trata das informações que correspondem à sua função.

Os protocolos TCP/IP podem ser utilizados sobre qualquer

estrutura de rede, seja ela simples como uma ligação ponto-a-ponto ou uma rede de pacotes complexa. Como exemplo, pode-se empregar estruturas de rede como Ethernet, Token-Ring, FDDI, PPP, ATM, X.25, Frame-Relay, barramentos SCSI, enlaces de satélite, ligações telefônicas discadas e várias outras como meio de comunicação do protocolo TCP/IP.

A arquitetura TCP/IP, assim como OSI realiza a divisão de funções do sistema de comunicação em estruturas de camadas.

Em TCP/IP as camadas são:

- Aplicação - Tranporte - Inter-Rede - Rede

1 - Camada de rede

Responsável pelo envio de datagramas construídos pela camada Inter-Rede. Esta camada realiza também o mapeamento entre um endereço de identificação de nível Inter-rede para um endereço físico ou lógico do nível de Rede. A camada Inter-Rede é independente do nível de Rede.

Alguns protocolos existentes nesta camada são:

Por exemplo, cada máquina situada em uma rede Ethernet, Token-Ring ou FDDI possui um identificador único chamado endereço MAC ou endereço físico que permite distinguir uma máquina de outra, possibilitando o envio de mensagens específicas para cada uma delas. Tais rede são chamadas redes locais de computadores.

Da mesma forma, estações em redes X.25, Frame-Relay ou ATM também possuem endereços que as distinguem uma das outras.

As redes ponto-a-ponto, formadas pela interligação entre duas máquinas não possuem, geralmente, um endereçamento de nível de rede (modelo TCP/IP), uma vez que não há necessidade de

identificar várias estações.

2 - Camada Inter-Rede

Esta camada realiza a comunicação entre máquinas vizinhas através do protocolo IP. Para identificar cada máquina e a própria rede onde estas estão situadas, é definido um identificador, chamado endereço IP, que é independente de outras formas de endereçamento que possam existir nos níveis inferiores. No caso de existir endereçamento nos níveis inferiores é realizado um mapeamento para possibilitar a conversão de um endereço IP em um endereço deste nível.

Exemplo de alguns protocolos existentes nesta camada são:

- Protocolo de transporte de dados: IP - Internet Protocol

- Protocolo de controle e erro: ICMP - Internet Control Message Protocol

- Protocolo de controle de grupo de endereços: IGMP - Internet Group Management Protocol

O protocolo IP realiza a função mais importante desta camada que é a própria comunicação inter-redes. Para isto ele realiza a função de roteamento que consiste no transporte de mensagens entre redes e na decisão de qual rota uma mensagem deve seguir através da estrutura de rede para chegar ao destino.

O protocolo IP utiliza a própria estrutura de rede dos níveis inferiores para entregar uma mensagem destinada a uma máquina que está situada na mesma rede que a máquina origem. Por outro lado, para enviar mensagem para máquinas situadas em redes distintas, ele utiliza a função de roteamento IP. Isto ocorre através do envio da mensagem para uma máquina que executa a função de roteador. Esta, por sua vez, repassa a mensagem para o destino ou a repassa para outros roteadores até chegar no destino.

3 - Camada de Transporte

Esta camada reúne os protocolos que realizam as funções de transporte de dados fim-a-fim, ou seja, considerando apenas a origem e o destino da comunicação, sem se preocupar com os elementos intermediários. A camada de transporte possui dois protocolos que são o UDP (User Datagram Protocol) e TCP (Transmission Control Protocol).

O protocolo UDP realiza apenas a multiplexação para que várias aplicações possam acessar o sistema de comunicação de forma coerente.

O protocolo TCP realiza, além da multiplexação, uma série de funções para tornar a comunicação entre origem e destino mais confiável. São responsabilidades do protocolo TCP: o controle de fluxo, o controle de erro, a sequenciação e a multiplexação de mensagens.

A camada de transporte oferece para o nível de aplicação um conjunto de funções e procedimentos para acesso ao sistema de comunicação de modo a permitir a criação e a utilização de aplicações de forma independente da implementação. Desta forma, as interfaces socket ou TLI (ambiente Unix) e Winsock (ambiente Windows) fornecem um conjunto de funções-padrão para permitir que as aplicações possam ser desenvolvidas independentemente do sistema operacional no qual rodarão.

4- Camada de Aplicação

A camada de aplicação reúne os protocolos que fornecem serviços de comunicação ao sistema ou ao usuário.

Pode-se separar os protocolos de aplicação em protocolos de serviços básicos ou protocolos de serviços para o usuário:

Protocolos de serviços básicos: que fornecem serviços para

atender as próprias necessidades do sistema de comunicação TCP/IP: DNS, BOOTP, DHCP Protocolos de serviços para o usuário: FTP, HTTP, Telnet, SMTP, POP3, IMAP, TFTP, NFS, NIS, LPR, LPD, ICQ, RealAudio, Gopher, Archie, Finger, SNMP e outros

4.3 Relação entre OSI e TCP/IP

A arquitetura TCP/IP possui uma série de diferenças em relação à arquitetura OSI. Elas se resumem principalmente nos níveis de aplicação e Inter-rede da arquitetura TCP/IP. Como principais diferenças pode-se citar:

- OSI trata todos os níveis, enquanto TCP/IP só trata a partir do nível de Rede OSI.

- OSI tem opções de modelos incompatíveis. TCP/IP é sempre compatível entre as várias implementações.

- OSI oferece serviços orientados a conexão no nível de rede, o que necessita de inteligência adicional em cada equipamento componente da estrutura de rede. Em TCP/IP a função de roteamento é bem simples e não necessita de manutenção de informações complexas.

- TCP/IP tem função mínima (roteamento IP) nos nós intermediários
  (roteadores)

- Aplicações TCP/IP tratam os níveis superiores de forma monolítica, Desta forma OSI é mais eficiente pois permite reaproveitar funções comuns a diversos tipos de aplicações. Em TCP/IP, cada aplicação tem que implementar suas necessidades de forma completa.

A figura abaixo ilustra a comparação entre TCP/IP e OSI. Note que a camada Inter-rede de TCP/IP apresenta uma altura menor que o

correspondente nível de Rede OSI. Isto representa o fato de que uma das funções do nível de Rede OSI é realizada pelo nível de Rede TCP/IP. Esta função é a entrega local de mensagens dentro da mesma rede. O IP só trata a entrega e a decisão de roteamento quando o origem e o destino da mensagem estão situados em redes distintas.

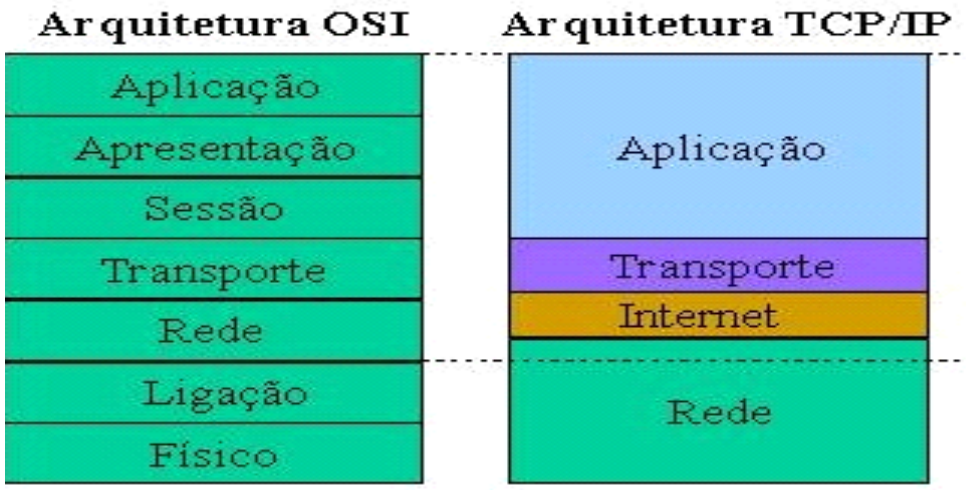


Fig 23 Comparacao Entre os Modelos de Referencia

4.4 Normas e Recomendacoes OSI-CCITT

A utilização de normas nas comunicações de dados é uma necessidade óbvia. Estes são necessários para gerir o uso e interligação de equipamentos tanto a nível físico, como eléctrico e mesmo a nível dos processos e procedimentos manipulação os dados.

O reconhecimento da necessidade de normas comuns não era partilhada pela indústria de computadores pois enquanto que os construtores de equipamento de telecomunicações reconheciam a necessidade de interligação do seu equipamento com equipamento de terceiros, os primeiros tentavam "prender os clientes" em torno da suas ofertas de tecnologia.

A proliferação de computadores e o seu uso para processamento distribuído tornou, no entanto, esta posição insustentável pelo que, cada vez mais, o uso de computadores e comunicações passa

pelo respeito de normas que permitem a sua interligação, independentemente de marca ou características específicas.

4.4.1 Vantagens e desvantagens do uso de normas

Vantagens

- Assegura a existência de um mercado mais alargado para um dado equipamento (hardware ou software), permitindo produções em maior escala com consequentes reduções de preço;
- Permite que produtos de diferentes construtores possam comunicar entre si, dando ao utilizador maior flexibilidade na selecção e uso de equipamento;

Desvantagens

- O seu uso tende a desacelerar a evolução e desenvolvimento de novos produtos; enquanto a norma é desenvolvida, sujeita a revisão, discutida e aprovada, é possível utilizar novas tecnologias mais eficientes, que entretanto tenham sido disponibilizadas;
- Existência de múltiplas normas com o mesmo objectivo. Não se trata propriamente de uma desvantagem do uso de normas mas sim da sua concepção (regista-se uma crescente cooperação entre as várias entidades responsáveis pela normalização para a aceitação e estudo conjunto de normas);
- Existência de áreas técnicas onde coexistem mais do que uma norma com objectivos sobrepostos e que são incompatíveis.

4.4.2 Entidades responsáveis pela normalização

São várias as organizações que estão envolvidas no desenvolvimento ou promoção de normas, das quais se destacam as seguintes, pela sua importância internacional:

- *International Organization for Standardization; ISO*
- *International Telegraph and Telephone Consultive Committee; CCITT*
- *The American Nacional Standards Institute; ANSI*
- *Electronics Industries Association; EIA*
- *Institute of Electrical and Electronics Engineers; IEEE*

International Organization for Standardization; ISO

A ISO é uma agência internacional para o desenvolvimento de normas num alargado conjunto de actividades. Trata-se de uma organização voluntária, de carácter público, em que os seus membros são designados pelas instituições de normalização de cada uma das nações participantes, acrescidas de um conjunto de organizações observadoras não votantes.

Embora a ISO não seja uma organização governamental, mais de 70% dos seus membros são instituições estatais de diferentes países vocacionadas para a criação de normas ou organizações de carácter público. O membro Português é o IPQ - Instituto Português de Qualidade e o correspondente dos Estados Unidos da América é o ANSI.

A ISO foi fundada em 1946 e é responsável por mais de 5000 normas sobre os mais diversos campos. O seu propósito é promover o desenvolvimento da normalização e actividades conexas que facilitem a troca internacional de bens e serviços e que permitam o desenvolvimento e cooperação em actividades intelectuais, científicas, tecnológicas e económicas, a nível mundial.

Uma área importante de standardização (normalização) diz respeito à interligação de sistemas abertos ("open systems interconnection" - OSI), que propõe um modelo de referência para comunicação de dados.

Para desenvolver uma norma ISO, da sua proposta à forma final, é necessário ultrapassar um exaustivo percurso constituído por sete

fases; o objectivo é conseguir que a norma obtida seja aceite no máximo de países possível:

O CCITT é um comité da International telecommunications Union (ITU), que é ela própria uma organização das Nações Unidas. Embora os membros do CCITT sejam os governos dos diversos países, estes delegam a sua representação quase sempre nos operadores de telecomunicações, que no caso Português corresponde à Portugal Telecom.

A missão do CCITT é o estudo e emissão de recomendações em questões técnicas, de operação e de tarifas, relacionadas com a telegrafia e o telefone. O seu objectivo principal é normalizar, na extensão necessária, técnicas e operações em telecomunicações de modo a alcançar a compatibilidade ponto a ponto em ligações de comunicações internacionais, quaisquer que sejam os países de origem e destino.

O CCITT está organizado em 15 grupos de estudo que preparam as normas, designadas por recomendações pelo CCITT. O trabalho desenvolvido pelo CCITT está estruturado em ciclos de quatro anos. A cada quatro anos é realizada uma assembleia geral onde é estabelecido o programa para os quatro anos seguintes, baseado nas propostas dos vários grupos de estudo que, por sua vez, auscultaram os membros do comité. A assembleia revê as propostas criando e eliminando os grupos que achar conveniente e procede à elaboração de objectivos.

Baseados nos objectivos definidos, cada grupo de estudo, prepara uma proposta de recomendação a ser submetida na próxima assembleia. Antes de ser aprovada a proposta pela assembleia, o estudo efectuado é objecto de publicação como recomendação CCITT. Existe forma de acelerar o processo, mas em geral trata-se de um processo de aprovação bastante lento.

Dentro da área das comunicações de dados e de processamento de informação, existe uma diferença que tem dividido os interesses do CCITT e da ISO. O CCITT tem como preocupação fundamental a transmissão de dados e aspectos relacionados com a rede de

comunicação.

De um modo geral, é possível afirmar que estes ocupam os três níveis inferiores da arquitectura OSI. A ISO tem tradicionalmente uma maior preocupação com as comunicações por computador e aspectos relacionados com o processamento distribuído, o que corresponderá aos níveis 4 a 7 do modelo de referência OSI.

No entanto, o constante aumento da área de sobreposição entre o processamento de dados e a comunicação de dados tem provocado a sobreposição das áreas de trabalho destas duas organizações. Tanto a ISO como a CCITT tem vindo a cooperar estreitamente nas áreas onde se faz sentir mais este fenómeno tentando eliminar a ocorrência de normas concorrentes.

The American Nacional Standards Institute; ANSI

A ANSI é uma organização não lucrativa e independente que agrega entidades responsáveis pela realização de normas e por utilizadores. Os seus membros incluem sociedades profissionais, associações de comércio, organismos regulamentadores, organismos do governo americano, empresas industriais e grupos de utilizadores. A organização ANSI é a mais representativa a nível americano e é também a que representa este país como membro votante na ISO.

A ANSI publica as normas Norte Americanas mas não as desenvolve. Em vez disso, as normas são desenvolvidas por outros grupos que são reconhecidos como competentes para o seu desenvolvimento. Muito deste trabalho é efectuado por organizações membros da ANSI, como é o caso do IEEE - Institute of Electrical and Electronics Engineers, que desenvolveram, entre outras, as normas 802 IEEE para redes locais.

Electronics Industries Association; EIA

Associação comercial de empresas de electrónica, membro da

ANSI. Está principalmente orientada para normas de nível mais baixo do modelo de referência OSI (nível físico).

Institute of Electrical and Electronics Engineers; IEEE

Associação profissional que é membro da ANSI. Preocupa-se fundamentalmente com os dois níveis mais baixos do modelo de referência OSI (nível físico e nível de ligação lógica)

5. Redes públicas de dados

5.1 Linhas comutadas

Comutação é o conjunto de operações para interligar circuitos que permitem a conexão entre dois ou mais assinantes. Existem vários tipos de centrais de comutação, conforme as funções exercidas, apresenta as fases características de cada tipo.

A comutação é o processo de interligar dois ou mais pontos entre si. No caso de telefones, as centrais telefônicas comutam (interligam) dois terminais por meio de um sistema automático, seja ele eletromecânico ou eletrônico.

O termo comutação surgiu com o desenvolvimentos das Redes Publicas de Telefonia e significa alocação de recursos da rede (meios de transmissão, etc...) para comunicação entre dois equipamentos conectados aquela rede. A comutação pode ser por circuitos, mensagens ou por pacotes.

5.2 Linhas dedicadas

Linhas privadas dedicadas é um método testado e aprovado de interconexão de redes em áreas amplas (WAN). São muito utilizadas nas interconexões entre operadoras.

Quando são feitas conexõs de linha privada, é necessária uma

porta de roteador para cada conexão, em conjunto com uma CSU/DSU (unidade de serviço de canal/unidade de serviço digital) separada ou integrada (na placa), bem como um circuito do provedor de serviços.

O Serviço de Acesso por Linha Dedicada proporciona às empresas a ligação permanente à Internet de um computador ou de uma rede de computadores através de um circuito digital dedicado. Desta forma, qualquer utilizador dessa rede pode aceder à Internet quando e sempre que quiser. A ligação está permanentemente online, não havendo assim que suportar custos telefónicos.

Uma ligação permanente através de uma linha dedicada permite-lhe ainda dispor de servidores nas suas instalações, permanentemente ligados à Internet.

O Serviço de Acesso por Linha Dedicada fornece-lhe uma solução de conectividade a um custo mensal fixo, independentemente da utilização da Internet.
Dirigido a médias e grandes empresas com uma estratégia Internet "madura" e também, independentemente da dimensão, a empresas cuja actividade requer a existência de um servidor nas suas instalações disponível 24/7 ou que necessitem de transferir grandes volumes de informação.

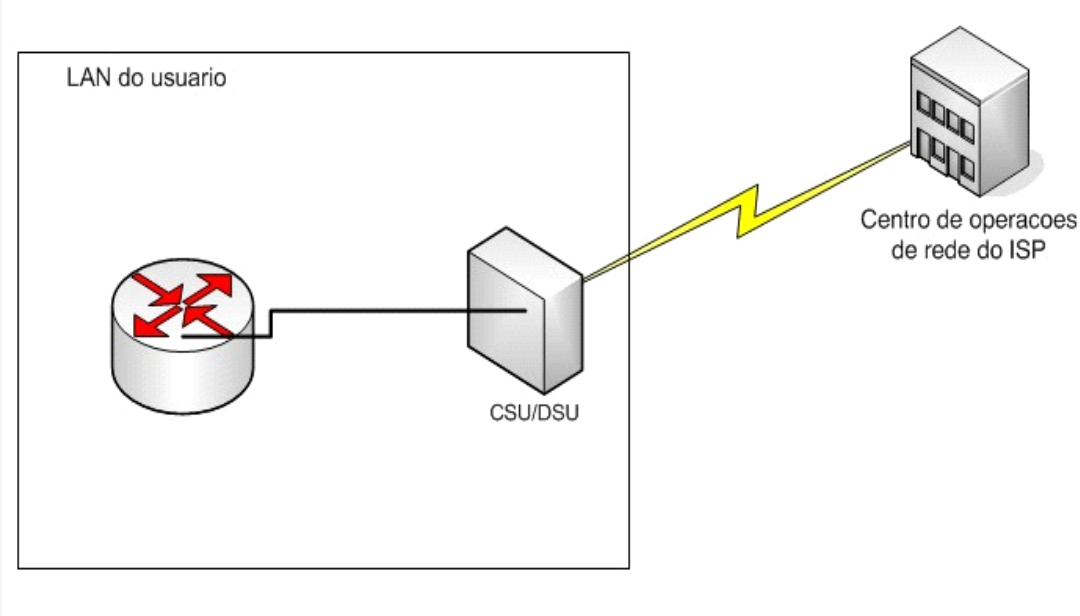


Fig 24 Linha Dedicada

6. Redes digitais com integração de serviços

6.1 Significado e objectivos

A Rede Digital com Integração de Serviços, RDIS, (em inglês ISDN, Integrated Services Digital Network), é uma rede baseada em transmissão e comutação digitais, sendo caracterizada pela integração do acesso dos utilizadores aos diversos serviços e redes actualmente existentes através de interfaces normalizadas fisicamente suportadas numa única linha digital.

O objectivo fundamental, a atingir a prazo razoável, é a criação de uma única rede de telecomunicações, uniformizada a nível internacional, que permita a comutação dos vários serviços e tipos de informação.

A situação actual caracteriza-se pela existência de diversas redes de telecomunicações públicas independentes, com a sua estrutura própria de transmissão e de comutação. Esta solução como se pode facilmente constatar não é a mais eficiente em termos de utilização de recursos e de meios técnicos e humanos, quer ao

nível de operação quer ao nível de exploração das redes. Assim, à medida que o número de serviços de telecomunicações aumenta com a tendência para aumentar o número de redes diferentes, impunha-se uma tentativa de unificação das redes de telecomunicações públicas, nomeadamente através de um único acesso do assinante.

A RDIS é a resposta no sentido de uma integração da maior parte dos serviços de telecomunicações actualmente existentes. Assim o utilizador pode através de uma única linha de assinante ter acesso a um conjunto diversificado de informações, sob a forma de voz, dados, texto e imagem, com uma característica fundamental que é a de que todos estes tipos de informação poderem ser digitalizados.

As redes públicas de telecomunicações sofreram várias e profundas transformações tecnológicas ao longo do seu pouco mais de um século de existência.

Paralelamente ao aumento da sua área geográfica e de número de utilizadores, as redes de telecomunicações foram-se diversificando, tendo sido criadas várias redes especializadas à medida que iam aparecendo novos serviços.

Podemos considerar na evolução tecnológica das redes públicas de telecomunicações cinco etapas fundamentais, tomando como base a rede telefónica por ser até aos dias de hoje a rede dominante em dimensão e número de utilizadores:

- Rede analógica
- Rede com transmissão digital e comutação analógica
- Rede digital integrada (RDI)
- Rede digital com integração de serviços (RDIS) - RDIS de banda larga (RDIS-BL).

Analisamos em seguida, as características fundamentais da rede

digital com integracao de servicos que sao a quarta e quinta etapas da evolucao listada acima por ser o nosso objecto de estudo objectivo:

6.1.1 Rede digital com integração de serviços (RDIS)

A quarta fase da evolução das redes telefónicas e de dados está actualmente a ser iniciada, sendo caracterizada pela integração a médio prazo dos vários serviços actualmente dispersos em várias redes dedicadas, tais como as redes telefónica, de telex e de dados numa única rede, denominada Rede Digital com Integração de Serviços (RDIS).
Uma característica fundamental da RDIS é a digitalização da linha do assinante, o que permite eliminar o último obstáculo analógico ainda existente na rede digital integrada. Com a digitalização da rede de assinante, os utilizadores passarão a ter acesso a canais digitais de ritmo muito superior aos permitidos pela rede analógica.

6.1.2 RDIS de banda larga

A quinta fase da evolução das redes de telecomunicações tem como característica fundamental a integração de todos os serviços, incluindo aqueles que requerem um débito elevado, como video interactivo em tempo real e distribuição de televisão de alta definição, que serão suportados numa RDIS dita de banda larga. Esta fase requer suportes de transmissão e tecnologias de comutação bastante diferentes da fase anterior, devido fundamentalmente aos altos ritmos necessários para os novos serviços, onde sem dúvida as tecnologias ópticas desempenharão um papel importante, tanto na transmissão como na comutação.

A RDIS de banda larga está neste momento numa fase de investigação e desenvolvimento a nível mundial, estando simultaneamente em normalização no ITU-T, o qual já aprovou um

conjundo de recomendações preliminares nesta área.

8. Sistemas abertos, proprietários e distribuídos

7.1 Introdução

As primeiras empresas a utilizarem computadores para processamento comercial foram as grandes corporações. O modelo utilizado era totalmente centralizado.

No início da década de 60 foram criados os primeiros protocolos de comunicação BSC-1 (*Binary Synchronous Communications*) para transmissão de informações remotas em lote e BSC-3 (*Poll- Select*) que permitia a interação do usuário com o sistema através de terminais, ou seja, o processamento *online*. Estes avanços tecnológicos proporcionaram um alto grau de conectividade para os sistemas da época, revolucionando a gestão da informação.

O avanço seguinte foi a criação das arquiteturas de rede que além da conectividade, proporcionavam um certo grau de interoperação entre os sistemas distintos de um mesmo fornecedor de tecnologia. Entre as várias arquiteturas de redes utilizadas, destacaram-se o SNA (IBM), o XNS (XEROX) e a DECNET (Digital), criadas por seus fornecedores e incompatíveis entre si. Quando as corporações necessitaram conectar seus diferentes sistemas, perceberam que estavam limitadas aos seus fornecedores de tecnologia e começaram a entender os custos relacionados a manutenção do que hoje chamamos de Sistemas Proprietários.

A incompatibilidade era a barreira contra a competição, gerando mercados cativos para cada fornecedor de tecnologia. Produtos foram criados para ultrapassar esta barreira através da transcodificação das diferentes linguagens. No entanto, as tecnologias eram completamente distintas entre seus fornecedores e, às vezes, entre sistemas de um mesmo fornecedor.

Os custos para operacionalizar tais conexões era excessivamente alto e estas proporcionavam uma funcionalidade conjunta muito fraca. A implantação de novas versões mais poderosas destas arquiteturas de redes poderia se tornar inviável em decorrência dos altos custos para readaptação do software de comunicação necessário à interconexão destes sistemas. Apesar da relação custo-benefício desfavorável, muitas empresas ainda têm seus sistemas de informação baseados neste modelo.

Iniciou-se a busca de sistemas abertos para resolver os problemas de conexão, integração de aplicações e transparência no acesso às informações. Os usuários de tecnologia necessitavam de padrões que considerassem alguns elementos básicos:

- Sistema operacional
- Arquitetura de rede
- Protocolos utilizados nesta arquitetura
- Hardware
- Meios físicos de transmissão de dados
- Interfaces do sistema

Nestas áreas, foi possível assistir a uma crescente consolidação, resultado de esforços de grupos de usuários, instituições de padronização e do surgimento de grandes quantidades de produtos obedientes aos padrões, sendo oferecidos por diversos fornecedores. O precursor desse movimento foi o sistema operacional UNIX.

7.2 Conceitos

Os sistemas abertos são nada mais que definições públicas e consensuais de interfaces. Ou seja, o usuário tem à sua disposição diversas opções em sistema operacional, protocolo de comunicação, interface gráfica, banco de dados ou outros componentes que, obedecendo a padrões, garantem portabilidade de suas aplicações para diferentes plataformas,

enquanto que os sitemas proprietarios sao os que como o proprio nome diz nao obedecem padrões internacionais.

Um sistema aberto possui as seguintes características:

- O sistema obedece a especificações bem definidas e disponíveis para a indústria;
- As especificações são seguidas por produtos de diversos fabricantes de computadores independentes (concorrentes);
- As especificações não são controladas por um grupo pequeno de fabricantes;
- As especificações não estão restritas à arquitetura ou tecnologia de um computador específico.

7.3 Vantagens e Desvantagens

O maior benefício dos sistemas abertos é a liberdade de escolha de plataformas de hardware e software. Dessa forma, o cliente pode concentrar mais sua atenção às aplicações críticas para seu negócio, sem estar limitado à oferta de um único fornecedor. Além disso, o sistema operacional UNIX foi concebido desde o princípio como um sistema multiusuário e multitarefa; isso o torna mais adequado ao papel de servidor de redes, podendo concentrar em uma só máquina a execução de diversas tarefas simultâneas. Também devido a isso, sempre foi forte o seu uso para comunicações e integração com máquinas heterogêneas, como os mainframes corporativos.

As redes corporativas atuais baseiam-se nestes padrões (abertos), através de vários componentes. São eles que viabilizam a implementação de sistemas distribuídos, aplicações cliente-servidor, processamento corporativo: novos e eficazes modelos de utilização do poder computacional nas empresas hoje.

8. Segurança

O conceito de *Segurança Informática* ou *Segurança de Computadores* está intimamente relacionado com o de Segurança da Informação, incluindo não apenas a segurança dos dados/informação, mas também a dos sistemas em si. Está relacionada com proteção de um conjunto de dados, no sentido de preservar o valor que possuem para um indivíduo ou uma organização.

Os sistemas de informação são vulneráveis a destruição, abuso, alteração, erro, fraude e a falhas de programas e equipamentos. Os sistemas on-line e os que utilizam a Internet são os mais vulneráveis, pois seus dados e arquivos podem ser acessados imediata e diretamente em terminais de computador ou em muitos pontos de rede. Crackers podem invadir redes e causar sérios danos ao sistema e às informações armazenadas, sem deixar qualquer rastro. Vírus de computador podem se propagar rapidamente entupindo a memória de computadores e destruindo arquivos. Os softwares em si também apresentam problemas e a má qualidade dos dados também pode causar sérios impactos sobre o desenvolvimento do sistema.

Qualquer grande empresa precisa tomar providencias especiais para evitar as vulnerabilidades e garantir a seguranca da informacao. Para tanto, planos de recuperação pós-desastre incluem procedimentos e instalações para restaurar os serviços de comunicação após terem sofrido algum tipo de problema. Quando a empresa utiliza intranet ou Internet, firewalls e sistemas de detecção de invasão ajudam a salvaguardar redes internas contra o acesso não autorizado.

São características básicas da segurança da informação os atributos de confidencialidade, integridade e disponibilidade, não estando esta segurança restrita somente a sistemas

computacionais, informações eletrônicas ou sistemas de armazenamento. O conceito se aplica a todos os aspectos de proteção de informações e dados.

8.1 Nível de segurança

Ao projectar um rede e preciso identificar os potenciais ataques. As organizações devem decidir o nível de segurança a estabelecer para uma rede ou sistema os recursos físicos e lógicos a necessitar de proteção. No nível de segurança devem ser quantificados os custos associados aos ataques e os associados à implementação de mecanismos de proteção para minimizar a probabilidade de ocorrência de um ataque. A seguranca pode ser dividida em dois niveis a fisica e a logica:

8.1.1 Segurança física

Considera as ameaças físicas como incêndios, desabamentos, relâmpagos, alagamento, accesso de pessoas nao aoutorizadas, forma inadequada de tratamento e manuseamento do material.

É muito importante a segurança física dos computadores e toda a enfrastrutura que envolve a uma rede. Deve-se avaliar o grau de segurança proporcionado aos recursos envolvidos no ambiente de sistemas em relação às ameaças externas existentes.

O ambiente onde os servidores ficam deve ter restrição de acesso físico, limpeza e organização, dispositivos para monitoramento vinte e quatro horas por dia e equipamentos de combate a sinistros. A infra-estrutura para os servidores deve contar com rede elétrica estabilizada e cabeamento estruturado. As estações de trabalho devem ter mobília adequada, equipamentos protegidos com lacres ou cadeados, limpeza e configuração compatível com a carga de trabalho.

Os mecanismos de segurança que apóiam os controles físicos sao: portas, trancas, paredes, blindagem, guardas, etc

8.1.2 Segurança lógica

Segurança lógica é a forma como um sistema é protegido no nível de sistema operacional e de aplicação. Normalmente é considerada como proteção contra ataques, mas também significa proteção de sistemas contra erros não intencionais, como remoção acidental de importantes arquivos de sistema ou aplicação, acessos remotos à rede, backup desatualizados e ate mesmo virus .

A seguir salietamos alguns mecanismos que ajudam a garantir a seguranca logica em um sistema informatico:

Autenticação: apenas usuários autorizados podem ter acesso à rede e dentro da rede, eles só podem ter acesso aos recursos realmente necessários para a execução de suas tarefas. Sendo que os recursos críticos devem ser monitorados e seu acesso restrito a poucas pessoas que nostram relevantes.

Criptografia: permite a transformação reversível da informação de forma a torná-la ininteligível a terceiros. Utiliza-se para tal, algoritmos determinados e uma chave secreta para, a partir de um conjunto de dados não criptografados, produzir uma sequência de dados criptografados. A operação inversa é a decifração.

Assinatura digital. um conjunto de dados criptografados, associados a um documento do qual são função, garantindo a integridade do documento associado, mas não a sua confidencialidade.

Firewall: é um sistema desenvolvido para prevenir acessos não autorizados a uma rede local de computadores. São implementados através de programas de computador e dispositivos eletrônicos. Através dele, os dados que entram ou saem da rede são examinados com a finalidade de bloquear os dados que não estão de acordo com os critérios de segurança.

Antivirus: são programas de computador concebidos para prevenir, detectar e eliminar vírus de computador.
Existe uma grande variedade de produtos com esse intuito no mercado, a diferença entre eles está nos métodos de detecção, no preço e nas funcionalidades.

9.1.3 Endereçamento IP

8.1.4 Conceito e Notação

Endereçamento IP ou IP ("Internet Protocol", ou Protocolo da Internet) é nada mais, nada menos, que o seu endereço na rede. É como se fosse um número de telefone ou o endereço de uma carta.

O QUE É O IPV4?

O IPv4 é a quarta e mais difundida versão do protocolo IP. Com endereços no padrão 32 bits, é bem antigo e possui vários problemas — desde falhas de segurança incontornáveis até o esgotamento da sua capacidade de expansão. Hoje, em todo o mundo, já está bem difícil conseguir um endereço nesse padrão.

Constituição do endereço IP

No IPV4, os endereço IP são compostos por 4 blocos ou octeto de 8 bits (32 bits no total), que são representados através de números de 0 a 255. e separados por um ponto.

Exemplo: "200.156.23.43" ou "64.245.32.11".

de rede.

Não podem existir na rede dois endereços IP iguais.

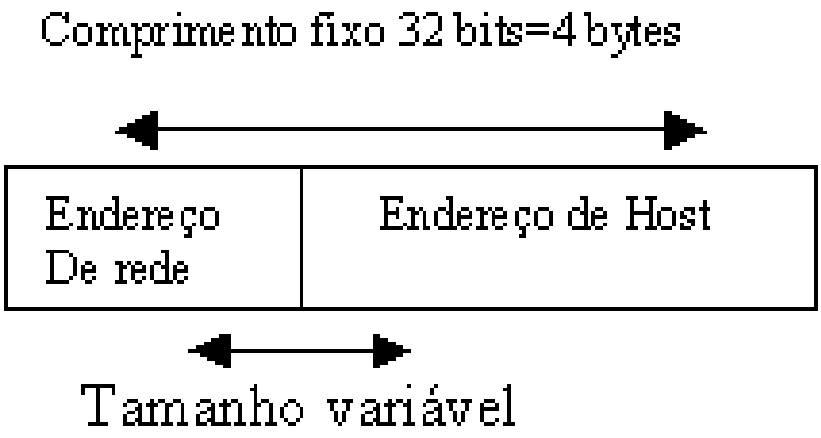
Classe de endereçamentos

O primeiro octeto ou byte define a classe do endereço IP.

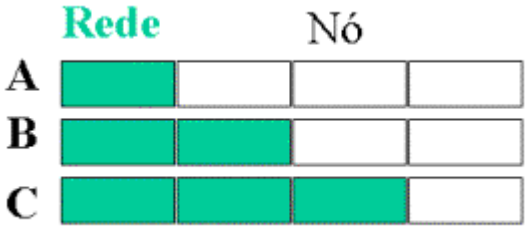
Existem várias classes definidas e normalizadas : - Classes A, B, C, D e E.

Cada endereço é constituído por um número de rede e um número

de Host - ou nó

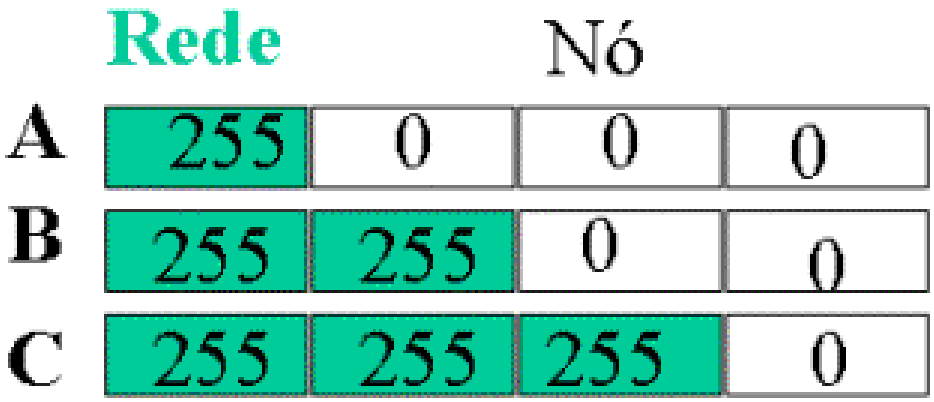


Classe

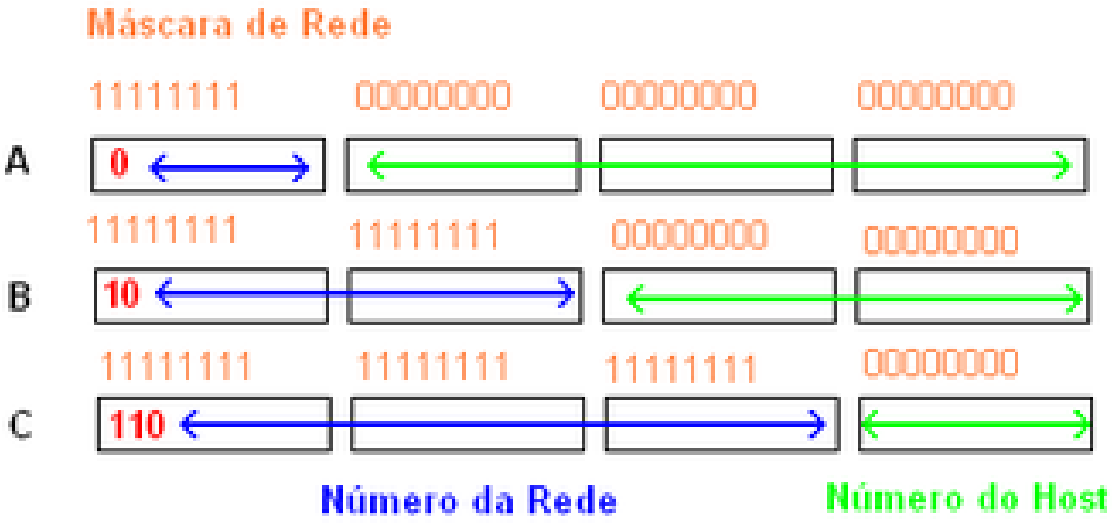


os endereços IP da classe A são usados em locais onde é necessário uma rede apenas, mas uma grande quantidade de máquinas nela.
Para isso, o primeiro byte é usado como identificador da rede e os demais servem como identificador dos computadores.
os endereços IP da classe B são usados nos casos onde a quantidade de redes é equivalente ou semelhante à quantidade de computadores.
Para isso, usa-se os dois primeiros bytes do endereço IP para identificar a rede e os restantes para identificar os computadores.
os endereços IP da classe C são usados em locais que requerem grande quantidade de redes, mas com poucas máquinas em cada uma.
Assim, os três primeiros bytes são usados para identificar a rede e o último é utilizado para identificar as máquinas.
Acordo com classe de endereços defenem _se as seguintes

mascaras



Mascaras de rede de decimal



Classe	Primeiro Octeto	Parte da rede (N) e parte para hosts (H)	Máscara	Nº Redes	Endereços por rede
A	1-127	N.H.H.H	255.0.0.0	**126** (2^7-2)	**16,777,214** (2^{24}-2)
B	128-191	N.N.H.H	255.255.0.0	**16,382** (2^{14}-2)	**65,534** (2^{16}-2)
C	192-223	N.N.N.H	255.255.255.0	**2,097,150** (2^{21}-2)	**254** (2^8-2)
D	224-239	Multicast	NA	NA	NA
E	240-255	experimental	NA	NA	NA

- Cada endereço é constituído por um número de rede e um número de Host - ou nó de rede.
- Não podem existir na rede dois endereços IP iguais.
- Vejamos o número de redes e de máquinas por rede (hosts) que temos para cada uma das classes:

Total de numero de rede e host que cada classe

Suporta.

Classe A - 1º byte de 1- a - 127	Classe B - 1º byte de 128-
· Até 128 (2^7) redes distintas · Até 16.777.216 (2^{24}) hosts por rede	· Até 16.384 (2^{14}) rede · Até 65.535 (2^{16}) host

· Até 2.097.152 (2^{11}) redes distintas · Até 256 (2^{8}) hosts por rede	Classe D - 1º byte de 224 · Usada para Multicast Classe E - 1º byte de 240

Restrições aos endereços IP

O endereço 0.0.0.0 é reservado para máquinas que não conhecem o seu endereço IP.

Ex: - 0.0.10.20 - a máquina sabe o IP relativo aos Hosts, mas não sabe a que rede pertence

O endereço 255.255.255.255 é um IP reservado para as máquinas fazerem broadcast (mensagem que é enviada para todos os sistemas da rede de forma a mostrar a difusão).

Os endereços iniciados por 127 (1º byte) e por um número superior a 223 não devem ser usados , pois destinam-se a finalidades muito especificas.

De acordo com a classe de endereço definem-se as seguintes máscaras.

Conceitos

Endereço de rede - É um Endereço de Protocolo da Internet (Endereço IP), do inglês Internet Protocol address (IP address), é um rótulo numérico atribuído a cada dispositivo (computador, impressora, smartphone etc.) conectado a uma rede de computadores que utiliza o Protocolo de Internet para comunicação.

Broadcast

é o endereço utilizada na rede para mensagem que é enviada para todos os sistemas da rede de forma a mostrar a difusão. A **difusão** é a acção e o efeito de **difundir** (propagar, divulgar ou espalhar).

Mascara(de rede e sub-redes)

Uma máscara de sub-rede é um número de 32-bit que mascara um endereço IP e divide o endereço IP em endereço de rede e endereço de host.

Gateway

o **endereço gateway**, é a porta de saída para outra **rede**.

9. Trabalho teórico-prático sobre o tema