Redes de Computadores

Introdução à comunicação de dados e redes de computadores

Versão 1.0
Março de 2017

Prof. Jairo

jairo@uni9.pro.br
professor@jairo.pro.br

http://www.jairo.pro.br/

Sumário

1 – Conceitos de comunicação de dados e redes de computadores

Numa definição simples, rede de computador é formada por um conjunto de módulos processadores capazes de trocar informação e compartilhar recursos, interligados por um sistema de comunicação que faz uso de um protocolo de comunicação comum a todos estes módulos.

A rede serve como meio de comunicação para compartilhamento de informações com redução de custos e deve apresentar confiabilidade e escalabilidade. Numa rede, a informação trafega em forma de pacotes de dados.

Para facilitar a compreensão, normalmente as redes são classificadas tanto pela ***área*** quanto pela ***topologia***.

2 – Topologias e classificação das redes

Para facilitar o entendimento, as redes são classificadas pela **área** e pela **topologia**.

2.1 - Classificação pela área

A classificação plea área define a rede pelas suas dimensões e abrangência física, que são *LAN*, *MAN*, *WAN*, *WLAN*, *VPN*, *PAN*, *CAN*, *GAN*, *HAN* e *SAN*.

2.1.1 - LAN (Local Area Network)

São redes locais com abrangência de até aproximadamente 10 Km. A LAN tem três características distintas: tamanho limitado, tecnologia da transmissão e topologia.

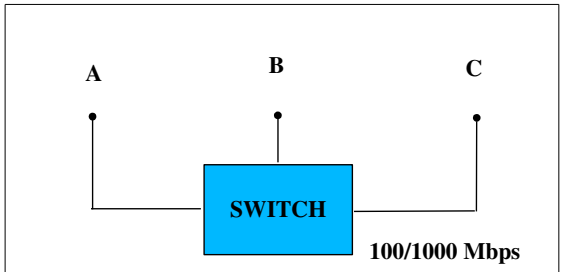

***Fig 1**: LAN típica*

2.1.2 - MAN (Metropolitan Area Network)

São redes com abrangência entre aproximadamente 10 a 100 Km.

2.1.3 - WAN (Wide Area Network)

São redes com abrangência numa área maior que 100 Km. O melhor exemplo é a rede pública de abrangência mundial conhecida como internet.

2.1.4 - WLAN (Wireless Local Area Network)

São redes locais que usam para comunicação tecnologias wireless, como o wi-fi.

2.1.5 - VPN (Virtual Private Network)

A VPN é uma rede privada criada dentro de uma rede pública (internet, WAN). Normalmente é usado VPN para, de casa, com o uso da internet, acessar o ambiente de trabalho. Este acesso é seguro, pois a VPN cria um túnel protegido dentro da rede pública.

2.1.6 - PAN (Personal Area Network)

São redes usadas em residências ou pequenos escritórios, atualmente se populariza devido à evolução da comunicação *wireless* (sem cabos) nesse tipo de rede, que facilita e barateia a instalação.

2.1.7 - CAN (Campus Area Network)

É uma rede MAN de alguma Universidade, com objetivo de interligar os campi espalhados numa região metropolitana. A rede da Uninove pode ser classificada como CAN.

2.1.8 - GAN (Global Area Network)

São redes usadas principalmente por multinacionais, que devido a sua extensão global necessita de uma rede privada de grandes extensões. Exemplo: McDonalds.

2.1.9 - HAN (Home Area Network)

É uma rede local doméstica, existe apenas numa residência. Normalmente usa wi-fi.

2.1.10 - SAN (Storage Area Network)

São redes usadas para interligar dispositivos de armazenamento de dados (HDs) externos (*storages*), dispositivos de backup (fitas) e servidores nos *data centers* (centro de dados).

2.2 - Classificação pela topologia

Na classificação pela topologia adotam-se os métodos de interconexão, que são ***ponto a ponto*** e ***difusão***.

2.2.1 – Ponto a ponto

A rede é ponto a ponto quando a comunicação ocorre apenas em dois nós ligados fisicamente. As redes ponto a ponto pela topologia classificam-se em *estrela*, *laço* e *árvore*.

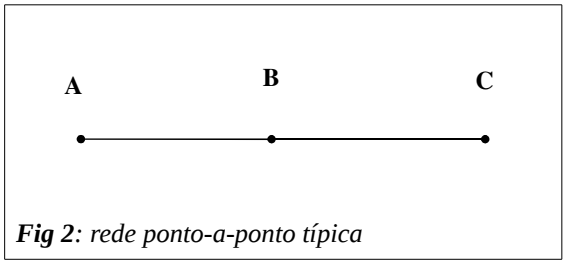

***Fig 2**: rede ponto-a-ponto típica*

2.2.1.1 - Estrela

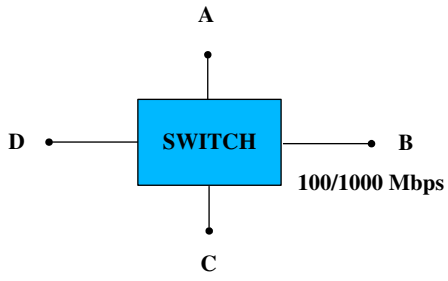

***Fig 3**: rede estrela*

A rede estrela normalmente usa um concentrador de rede (*switch*), cuja função é conectar dois ou mais nós processadores. Embora essa topologia seja muito popular, tem como desvantagem um ponto único de falha, que ocorre caso o concentrador falhe.

2.2.1.2 - Laço

A topologia em laço é apenas uma versão modificada da estrela, porém nesse caso não existe a necessidade do *switch*.

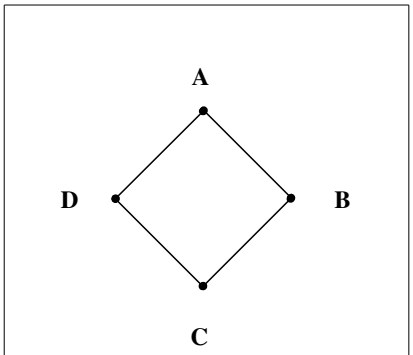

***Fig 4**: rede em laço*

2.2.1.3 - Árvore

A árvore é uma configuração hierárquica.

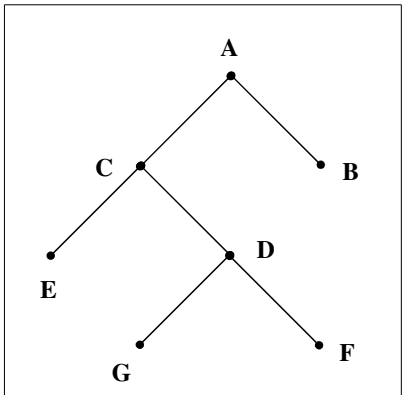

***Fig 5**: configuração hierárquica*

2.2.2 - Difusão

Nesta topologia de rede, os módulos processadores compartilham um canal de comunicação único, e os dados enviados por um módulo são recebidos por todos os outros. Neste caso, é necessário algum método para controlar o acesso simultâneo a esta rede, ou seja, faz-se necessário alguma arbitragem. Esta arbitragem é necessária devido ao compartilhamento do meio físico.

Como exemplo, no caso da rede *estrela* (figura 3, acima), temos um anel lógico sobre uma estrela física, e por usar um switch é classificado como topologia ponto a ponto. Mas se substituir o switch por um hub, então torna-se topologia difusão.

No caso da estrela física com tecnologia Ethernet com hub como concentrador, costuma-se usar o algoritmo CSMA/CD[1] como árbitro.

O exemplo clássico de rede de difusão é o *barramento*.

2.2.2.1 - Barramento

É a topologia onde os nós na rede apresentam-se em forma de uma barra, como exemplo temos as antigas redes *ethernet* que usavam cabos coaxiais.

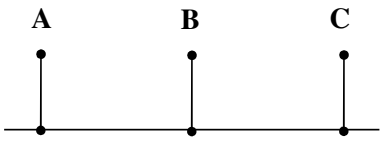

***Fig. 6**: barramento*

1 CSMA/CD protocol: Carrier Sense Multiple Access with Collision Detection

3 – Endereçamento físico e lógico

A definição de endereçamento envolve alocar um endereço para cada nó da rede, endereço este que seja unívoco dentro desta mesma rede.

O endereço pode ser tanto físico quanto lógico. Se estamos em uma rede local (LAN), a comunicação entre os nós (módulos processadores) é feita usando-se o endereço físico, se a comunicação envolve o inter redes (internet), é necessário um endereço lógico.

No caso do endereço físico temos como exemplo o MacAdress (*Ethernet*), que é composto de 6 bytes (48 bits), por exemplo 44:8a:5b:94:63:9a. Ainda como exemplo, apesar de haver um número muito grande de fabricantes de interfaces de redes, não existe o caso de dois destes equipamentos terem o mesmo endereço Mac pois os três primeiros bytes do endereço físico é um número constante determinado para aquele fabricante específico, e a outra parte do endereço é o próprio fabricante que determina, no estilo *serial number* (número de série).

No caso do endereço lógico temos como exemplo o IP da arquitetura internet (TCP/IP, *Transmission Control Protocol/Internet Protocol*).

A versão atual mais usada do TCP/IP ainda é a versão 4, ou ipv4.

A representação mais usada para o endereço ipv4 é:

xxx.xxx.xxx.xxx

Onde xxx é um número decimal entre 0 e 255. Como exemplo de endereço ipv4 temos 192.168.1.10, que é um endereço de 32 bits (4 bytes).

Porém, aos poucos está chegando a nova versão do TCP/IP, que é a versão 6 ou ipv6. A representação mais comum para ipv6 é:

hhhh:hhhh:hhhh:hhhh:hhhh:hhhh:hhhh:hhhh

Onde hhhh é um número hexadecimal de 4 dígitos (16 bits ou 2 bytes), por exemplo fe80. Como exemplo de endereço ipv6 temos 2804:012c:0139:9aeb:478a:5bff:fe34:6095, que é um endereço de 128 bits (16 bytes).

A razão dessa gradual substituição de endereços de internet ipv4 por ipv6 é devido ao esgotamento da disponibilidade de endereços para atender a uma demanda que aumenta ano após ano.

Abaixo é mostrado o número máximo (teórico) de endereços nas versões ipv4 e ipv6.

ipv4: 2^{32} => 4294967296 ($4{,}3x10^{9}$)
ipv6: 2^{128} => $3{,}4x10^{38}$

Portanto, com a adoção do ipv6, haverá um incremento em cerca de 10^{29} vezes mais endereços disponíveis. Isto provavelmente deverá atender a demanda de endereços que a *internet das coisas* irá necessitar nas próximas décadas.

Outro aspecto importante a ser considerado é que na versão ipv6 o endereço físico (MacAddress) pode ser incorporado ao endereço lógico, resultando numa construção redundante. Convém lembrar que no ipv4 o endereço lógico e o endereço físico são distintos para uma mesma interface.

E como o endereço físico é de 48 bits, então o número máximo (teórico) de endereços é:

MacAddress: 2^{48} => $2{,}8x10^{14}$

Portanto, o número máximo de MacAddress é cerca de 6500 vezes maior que o de endereços ipv4. Mas se os endereços ipv4 já estão esgotados, não vai levar muito tempo para esgotar também os endereços físicos. E isso fatalmente irá ocorrer com a chegada da internet das coisas.

4 – Noções de roteamento

A função do roteamento consiste no processo de escolha do melhor caminho que um pacote de dados tome ao viajar entre os nós de origem e de destino.

Quando os nós processadores estão na mesma sub-rede (mesma LAN), a tarefa de roteamento é trivial, porém quando os nós estão em sub-redes diferentes essa comunicação ocorre via *gateway*.

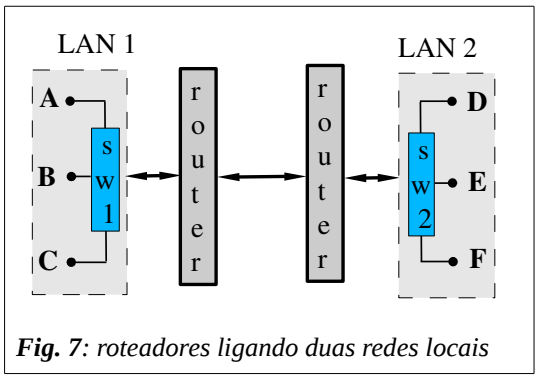

***Fig. 7**: roteadores ligando duas redes locais*

O *gateway* é que faz o roteamento dos pacotes de dados de uma sub-rede para outra, baseado em endereços lógicos de destino e origem.

Sub-rede, nesse caso, é uma rede vista do inter rede (internet) e não uma segmentação de rede.

Os roteadores são equipamentos projetados para executar a tarefa de roteamento, e possuem algoritmo interno que permite a realização dessa tarefa. No processo de roteamento o "melhor" caminho para o pacote é função da métrica (distância, quantidade de saltos e largura de banda).

O roteamento é a principal função de um *gateway*, e pode ser estático ou dinâmico.

4.1 – Roteamento estático

Se as rotas forem simples, elas podem ser configuradas estáticas, neste caso a tabela de roteamento é construída manualmente pelo administrador da rede.

As tabelas de roteamento estáticas não se ajustam automaticamente em acordo com as possíveis alterações na métrica da rede, desse modo roteamento estático deve ser utilizado somente onde as rotas não sofram alterações.

As vantagens do roteamento estático são a segurança proporcionada pela não divulgação de rotas usadas e à redução da sobrecarga na rede introduzida pela troca de pacotes de roteamento originadas pelo uso de protocolos de roteamento, que ocorre no roteamento dinâmico.

4.2 – Roteamento dinâmico

Nas redes onde existe muitas alternativas de rota para um mesmo ponto deve ser utilizado roteamento dinâmico.

O roteamento dinâmico faz uso de protocolos de roteamento tais como RIP (Routing Information Protocol), OSPF (Open Short Path First), EIGRP (Enhanced Interior Gateway Routing Protocol) ou BGP (Border Gateway Protocol) .

Neste caso, a tabela de roteamento dinâmica é criada e mantida a partir de informações trocadas entre os roteadores pelos protocolos de roteamento. Estes protocolos são desenvolvidos para distribuir informações que ajustam as rotas dinamicamente de modo a refletir as alterações nas condições da rede.

A principal função de um protocolo de roteamento é fornecer as informações necessárias para poder fazer o roteamento, mediante criação e atualização de tabelas de roteamento.

Estes protocolos são desenvolvidos para alterar para uma rota alternativa quando a rota primária se tornar inoperável, além de decidir qual é a rota preferida para um destino.

5 - Organismos de padronização e internet

No início, o desenvolvimento das redes não seguia um padrão universalmente aceito: cada fabricante independentemente decidia como deveria funcionar a sua solução ou produto. Isto levava a produtos frequentemente incompatíveis entre um vendedor e outro.

Com o objetivo de simplificar as redes de computadores foram adotados padrões para os dispositivos, equipamentos e protocolos de comunicação em rede.

De forma abrangente, normalmente os padrões podem ser classificados como:

- ***padrão de jure***: é aquele aprovado por uma organização de padronização formal e credenciada;
- ***padrão de fato*** (de facto): é aquele que é aceito e usado pelo público e pela indústria em geral. Quer dizer, aquele que é de fato implementado e realmente usado;
- ***padrão proprietário***: é aquele produzido especificamente por uma empresa e não é de domínio público;
- ***padrão de consórcio***: é aquele produzido por um grupo ou consórcio de empresas.

Abaixo segue alguns exemplos de padrões usados nas redes de computadores.

5.1 – IEEE

O IEEE (*Institute of Electrical and Electronic Engineers* - Instituto de Engenheiros Elétricos e Eletrônicos) é a maior sociedade técnico-profissional dedicada ao avanço da teoria e prática da engenharia nos campos da eletricidade, eletrônica e computação.

Entre seus associados estão engenheiros, cientistas, pesquisadores e outros profissionais, isto em cerca de 160 países. Esta sociedade existe há mais de 100 anos e hoje conta com mais de 420.000 membros.

Qualquer pessoa, com diversos graus de conhecimento acadêmico e experiência profissional pode se inscrever para integrar o time do IEEE.

5.2 – ISO

A ISO (*International Organization for Standardization* – Organização Internacional para Normalização) é uma entidade internacional responsável pelo desenvolvimento de normas para produtos, processos, procedimentos e serviços. A ISO aprova padrões internacionais em todos os

campos técnicos, exceto eletricidade e eletrônica, áreas na qual a IEEE já é responsável. O objetivo da ISO é remover barreiras técnicas que dificultem o comércio internacional.

A ISO também é importante pelo desenvolvimento de certificações internacionais, tais como ISO 9001 e ISO 14001.

Por exemplo, a imagem comum em CD ou DVD, conhecida por ISO, é devido ao padrão ISO 9660, que trata de um tipo específico de sistema de arquivos.

No Brasil, a ABNT (Associação Brasileira de Normas Técnicas) é um membro fundador da ISO internacional. Como exemplo, os padrões de teclados ABNT e ABNT 2 foram certificados pela ABNT.

Foi a ISO que criou o padrão aberto OSI (*Open Systems Interconection* - Interconexão de Sistemas Abertos), que é um conjunto de padrões relativos à comunicação de dados em rede. Sistema aberto é o que não depende de uma arquitetura específica, e que também é conhecido por "Camadas OSI".

5.3 – ANSI

A ANSI (*American National Standards Institute* – Instituto Nacional Americano de Padrões) é uma organização americana sem fins lucrativos, cujo objetivo é normalizar os meios computacionais e melhorar a qualidade de vida e dos negócios nos Estados Unidos.

Tem vários padrões, entre os quais:

- ANSI C: é um guia para a criação de compiladores e de programas na linguagem C;
- SQL ANSI: normaliza a Linguagem SQL.

5.4 – ASCII

ASCII (*American Standard Code for Information Interchange* - Código Padrão Americano para o Intercâmbio de Informação) é uma padronização de conjunto de códigos para a indústria de computadores. A tabela ASCII associa um determinado número à representação de um caracter.

Alguns exemplos de caracteres relacionados ao código ASCII são:

Código 07	=	BEL (bell, bip ou sinal audível)
Código 08	=	BS (espaço em branco)
Código 36	=	$ (cifrão)
Código 65	=	A (letra A, maiúsculo ou caixa alta)

Código 97 = a (letra a, minúsculo ou caixa baixa)
Código 243 = ¾ (três quartos)

O ASCII original representa caracteres com apenas 7 bits, atualmente o ASCII *Extended* (estendido) trabalha com 8 bits. O código ASCII estendido contempla os códigos de 00 a 255 (256 caracteres).

A tabela ASCII é dividida em três partes:

- **caracteres de controle**: por exemplo bip (bell, sinal audível), tabulação horizontal, escape. Estes caracteres não tem representação gráfica;
- **caracteres *printable***: que podem ser representados graficamente, por exemplo a, 3, @;
- **caracteres extendidos**: por exemplo ®, Ø, Ü.

Internamente, cada caracter é representado por um número binário (código) de 7 ou 8 bits (segmento de 128 ou 256 caracteres), e a tabela ASCII é que faz a conversão do caracter em acordo com o código.

5.5 – ITU-R

ITU (*International Telecommunication Union* - União Internacional de Telecomunicações) é a agência da ONU especializada em tecnologias de informação e comunicação, destinada a padronizar e regular as ondas de rádio e telecomunicações internacionais. Está dividida em três setores, onde um deles é o ITU-R.

ITU-R (*ITU Radiocommunication Sector* – Setor de Radiocomunicações do ITU) é o responsável pelas recomendações de gestão do espectro de radiofrequência. O uso das bandas de frequências eletromagnéticas de wi-fi e bluetooth são padronizados pelo ITU-R.

5.6 – Internet Standards

Os Padrões para a Internet (*Internet Standards*) vem da IETF (*The Internet Engineering Task Force* – Força Tarefa de Engenharia de Internet). IETF é uma atividade organizada da ISOC (*Internet Society* – Sociedade da Internet).

O IAB (*The Internet Architecture Board* - Conselho de Arquitetura da Internet) é um comitê do IETF, que é quem elabora as definições da arquitetura TCP/IP em RFC (*Request for Comments* – Pedido de Comentários).

Todas as definições da arquitetura TCP/IP estão em RFC elaboradas pelo IAB (*The Internet Architecture Board*), que também é um padrão aberto.

TCP/IP é a uma arquitetura de rede.

6 - Modelo de referência RM-OSI e modelo TCP/IP

Para descrever e implementar a tarefa de comunicação em rede são criados modelos.

Os modelos atuais são apresentados em camadas funcionais, num conceito de **arquitetura de rede**.

6.1 – Arquitetura de rede

Quanto à arquitetura, a rede divide a tarefa de comunicação em várias camadas funcionais, onde a camada inferior presta serviços à camada superior que requisita estes serviços.

Como exemplo, imaginemos o caso de um diretor de um setor de uma empresa (empresa A) que queira enviar um documento a outro diretor em outra empresa (empresa B). A maneira convencional é esse diretor transferir a tarefa para a sua secretária, que por sua vez redige o documento e envia para o boy. O boy, por sua vez, entrega o documento ao chefe de malote que despacha o documento para o endereço correto. Uma vez chegando lá, o documento segue todo esse cerimonial na "pilha" hierárquica, porém agora em sentido inverso, até chegar às mãos do diretor. Embora burocrático, esse procedimento traz vantagens, e a maior de todas é liberar os diretores das tarefas mais básicas, as quais são atribuídas aos seus subordinados.

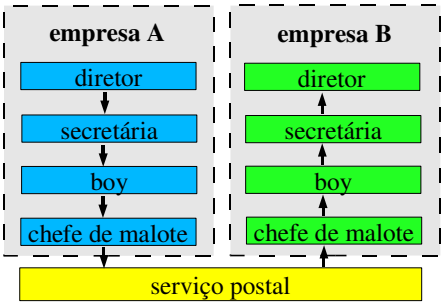

***Fig 8**: pilha hierárquica*

No caso de uma arquitetura de rede, no lugar do diretor está o *software* aplicativo do usuário, por exemplo um navegador da internet, e no caso do serviço postal está o meio físico de comunicação em rede, como exemplo temos o cabo de rede.

A arquitetura de rede amplamente utilizada hoje é o TCP/IP (*Transmission Control Protocol/Internet Protocol*), que teve sua origem em meados da década de 1960 como um projeto militar do Departamento de Defesa dos EUA e que foi desenvolvido na ARPA (*Advanced Research Project Agency*). Desse projeto resultou uma rede inicialmente conhecida como ARPANET, que entrou em operação experimental em 1969 e que posteriormente introduziu novidades no conceito de comunicação.

Entre essa novidades estão *comutação de pacotes* (conceito de roteamento de pacotes), divisão da tarefa de comunicação em *camadas funcionais* (conceito de arquitetura de rede) e interligação de computadores entre universidades americanas e de outros países.

Simultaneamente a isso, outros fabricantes já possuíam as suas arquiteturas proprietárias,

como era o caso da IBM com SNA (*Systems Network Architecture*) e Digital com Decnet.

No final dos anos 1970 havia uma demanda potencial de crescimento para redes, porém também havia uma crise criada pela heterogeneidade de padrões, protocolos e equipamentos de comunicação. Por exemplo, ARPANET com arquitetura específica para atender as suas redes.

Tudo isso levou a um esforço para o desenvolvimento e implantação de arquiteturas abertas, e é nesse contexto que surge o modelo de referência RM-OSI (*Reference Model/Open Systems Interconnect*).

Sabemos hoje que o RM-OSI, desde a sua criação no início dos anos 1980, manteve-se na prática apenas como um modelo acadêmico ou modelo padrão (padrão de jure), enquanto o TCP/IP - por ser aberto, simples e o primeiro a se difundir pelas redes do mundo inteiro - se tornou o modelo *de fato* usado no mercado.

6.2 – Modelo de referência RM-OSI

Podemos dividir o RM-OSI em 3 partes, uma parte inferior orientada a redes ou comunicação composta por 3 camadas (física, enlace e rede), uma parte central que verifica a entrega dos dados composta pela camada de transporte e uma parte superior orientada a aplicações ou serviços composta pelas camadas de sessão, apresentação e aplicação.

O RM-OSI está dividido em 7 camadas: *física*, *enlace*, *rede*, *transporte*, *sessão*, *apresentação* e *aplicação*.

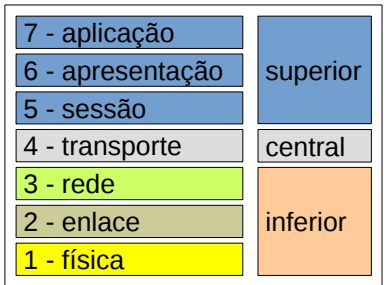

***Fig 9**: modelo RM-OSI*

6.2.1 - Física

É a camada responsável por transmitir *bits* através de uma ligação. Aceita quadros da camada de enlace de dados e traduz esses *bits* em sinais do meio físico. Cuida de questões como o tipo do cabo em uso e o esquema de sinalização. Define o modo de transmissão (unidirecional, bidirecional, etc), modo de conexão (ponto a ponto, multiponto) e modo de tratamento dos erros.

6.2.2 - Enlace

É a camada responsável pela transferência de dados entre pontos de uma ligação física, fraciona as mensagens recebidas do emissor em unidades de dados denominadas quadros, que correspondem a algumas centenas de *bytes*. Essa camada trata de detecção de erros e controle de fluxo, que é a necessidade de armazenamento de dados a transmitir quando a transmissão não for efetuada a uma mesma taxa (por exemplo, 100 e 1000 Mbps). Essa camada também resolve problemas relativos a quadros danificados, perdidos ou duplicados.

6.2.3 - Rede

Nessa camada, as mensagens formatadas são denominadas pacotes. É função dessa camada encaminhar os pacotes de dados do emissor ao receptor. Essa camada deve resolver todos os problemas relacionados à interconexão de redes heterogêneas, como por exemplo incompatibilidades no endereçamento e incoerências com relação ao tamanho das mensagens.

6.2.4 - Transporte

A função dessa camada é aceitar dados da camada de sessão, quebrar esses dados em pacotes menores se necessário e passá-los para a camada de rede. Uma característica dessa camada é implementar um diálogo fim a fim, ou seja, o processo executando no sistema fonte dialoga com o processo executando no nó destino através de cabeçalhos (*headers*) e informações de controle contidas nas mensagens desse nível. Essa camada implementa um mecanismo de controle de fluxo fim a fim para evitar que o sistema fonte envie mensagens numa taxa superior àquela que o sistema destino possa receber. Normalmente cria uma conexão de rede para cada conexão de transporte requerida pela camada de sessão.

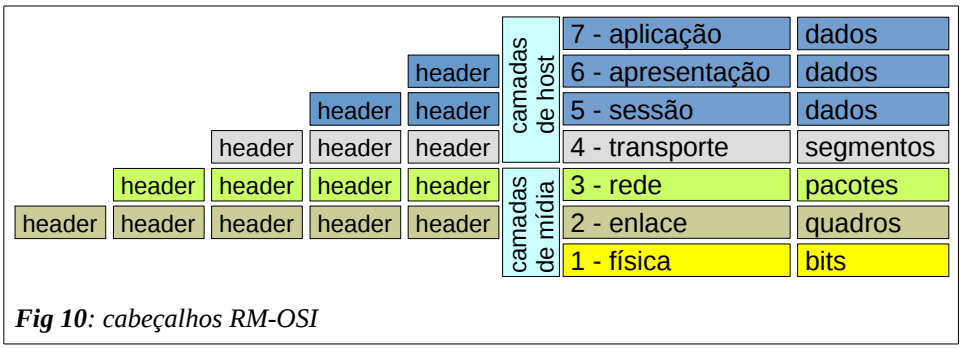

***Fig 10**: cabeçalhos RM-OSI*

6.2.5 - Sessão

Essa camada trata da coordenação entre processos de comunicação entre os nós na rede, verifica se uma conexão permite comunicação em duplex parcial ou completo, sincroniza fluxo de dados e restabelece conexão em caso de falha.

NOTA:
Os serviços em rede podem ser *orientados à conexão*, como é o caso do SAP (*service access point*) ou socket (Unix) ou podem ser *sem conexão*.

6.2.6 - Apresentação

Essa camada trata de formato de dados, traduções e conversões de código. Cuida da sintaxe e semântica dos dados transmitidos, além da compressão e criptografia. Na prática, essa camada é frequentemente incorporada na camada de aplicação.

6.2.7 - Aplicação

Essa camada consiste de protocolos que definem aplicações específicas orientadas para usuários, como navegador da internet, correio eletrônico e transferência de arquivos.

6.3 – Modelo TCP/IP

O TCP/IP é composto por dois protocolos principais, o IP (*Internet Protocol*) e o TCP (*Transmission Control Protocol*). O endereçamento IP é do tipo datagrama (não orientado à conexão), já o TCP é o protocolo de transmissão (transporte), que é orientado à conexão.

O TCP/IP oferece um serviço relativamente confiável, mesmo em redes não confiáveis. Em redes de alta qualidade, onde a confiabilidade não é importante, pode-se utilizar o UDP (*User Datagram Protocol*) que não é orientado à conexão.

O termo TCP/IP designa uma família de protocolos de comunicação de dados, tais como FTP, SMTP e HTTP.

Essa família de protocolos teve origem na ARPANET, um projeto do Departamento de Defesa dos EUA. Essa família de protocolos foi desenvolvida para ser usada num meio não-confiável, mas mesmo assim atualmente o TCP/IP é amplamente usado até em LANs que não têm acesso à internet.

O segredo do sucesso do TCP/IP vem principalmente do fato dele ter sido o primeiro protocolo de comunicação em rede a atingir uma abrangência mundial.

Outras características igualmente importantes do TCP/IP são:

- protocolo aberto, público, independente de equipamentos e sistemas operacionais;
- não define protocolo para o nível físico, podendo por exemplo usar *ethernet* e *token ring*;
- esquema de endereçamento lógico unívoco;
- protocolos de aplicação que atendem à demanda dos usuários.

O modelo mais aceito (padrão internet) divide a arquitetura TCP/IP em 4 camadas: **acesso à rede** ou **interface de rede**, **internet**, **transporte** e **aplicação**. Mas existem outros autores que consideram esta divisão em 5 camadas, o grande problema em dividir em cinco camadas é que não parece haver acordo entre eles de como deve ser esta divisão.

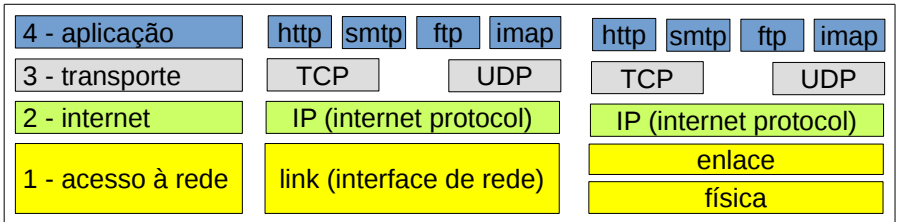

***Fig 11**: pilha TCP/IP com 4 e 5 camadas*

6.3.1 - Acesso à rede

Essa camada provê os meios para que os dados sejam transmitidos a outros nós processadores na mesma rede. Essa camada pode abranger as 3 primeiras camadas do RM-OSI, porém não define propriamente os protocolos para esses 3 níveis e sim como utilizar os protocolos já existentes para suportar a transmissão.

6.3.2 - Internet

A camada internet tem como principais funções:

- definir o datagrama IP, que é a unidade básica de transmissão;
- definir o esquema de endereçamento IP;
- rotear datagramas IP;
- fragmentar e remontar datagramas IP.

6.3.3 - Transporte

Os principais protocolos dessa camada são TCP e UDP. O TCP é orientado à conexão com detecção e correção de erros fim a fim, já o UDP é não orientado à conexão e não confiável, por outro lado o UDP é muito leve (causa pouco *overhead*) na rede.

Como exemplo comparativo, o TCP tem aspecto de ligação telefônica (completa a ligação, que é chamada de *conexão*) enquanto o UDP se assemelha ao serviço postal (correio), no sentido de transmitir pacotes isolados.

6.3.4 - Aplicação

A camada aplicação é a que provê protocolos que se comunicam, de um lado, com os aplicativos do usuário (lado cliente) e na outra ponta com os aplicativos servidores (serviços).

Exemplos de protocolos da camada de aplicação são HTTP, FTP, SMTP e DNS.

RM-OSI	TCP/IP		
7) Aplicação	SNMP, TFTP, NFS, DNS, BOOTP	FTP, TELNET, FINGER, SMTP, POP, IMAP, SSH, HTTP	**Aplicação**
6) Apresentação			
5) Sessão			
4) Transporte	UDP	TCP	**Transporte**
3) Rede	IP, icmp[2]		**Internet**
2) Enlace	placas de interface de rede		**Interface de rede**
1) Física	meio de transmissão		

Tabela 1: *arquitetura TCP/IP*

Semelhante ao modelo RM-OSI, cada camada da pilha de protocolos adiciona um cabeçalho (*header*) com informações de controle. Essa adição de informações de controle é denominada *encapsulamento*.

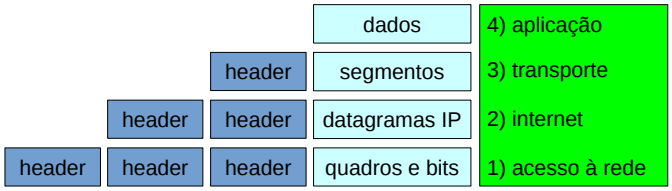

Fig. 12: *encapsulamento na pilha TCP/IP*

6.4 – Comparação de camadas entre RM-OSI e TCP/IP

Ao contrário do modelo RM-OSI, que tem um compromisso acadêmico de ser um modelo de referência, a arquitetura do protocolo TCP/IP em camadas não tem qualquer outro compromisso que não seja a funcionalidade.

Desse modo, estabelecer relação precisa entre as camadas do modelo RM-OSI e TCP/IP torna-se tarefa difícil.

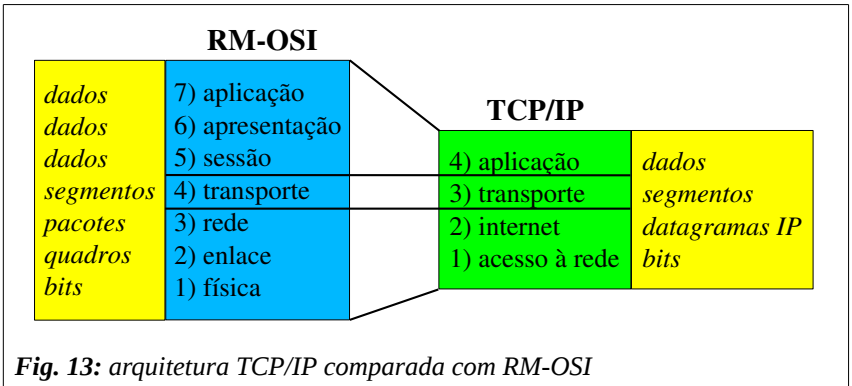

Fig. 13: *arquitetura TCP/IP comparada com RM-OSI*

O modelo OSI (RM-OSI) evoluiu a partir de uma definição formal elaborada por comissões da ISO buscando desenvolver um produto que atendesse não só as necessidades dos usuários, mas

2 icmp: *Internet Control Message Protocol*, um protocolo específico para diagnóstico de comunicação em rede.

também aos desenvolvedores de serviços e soluções em rede e fabricantes de equipamentos de redes.

Já o TCP/IP nasceu da necessidade do mercado e de produtos necessários para resolver o problema da demanda por comunicação em rede, e como o seu uso se expandiu rapidamente, uma série de implementações foram feitas para incorporar ao TCP/IP muitos produtos desenvolvidos fora da arquitetura internet.

Usualmente costuma-se dizer que a arquitetura OSI é um modelo de *jure*, enquanto a arquitetura internet é modelo de *fato*. Ou seja, enquanto o OSI academicamente define padrões, a arquitetura internet apresenta produtos ao mercado.

Comparando a estrutura das duas arquiteturas, observa-se que a parte referente às sub-redes de acesso da arquitetura internet corresponde à camada física, enlace e, parcialmente, a de rede no modelo OSI, sem que haja padronização nesse aspecto.

O IP corresponde à camada de rede, enquanto TCP e UDP oferecem serviços semelhantes aos prestados pelos protocolos de transporte do modelo OSI. Já a camada aplicação da arquitetura internet é sozinha responsável pelos serviços prestados pela camada de sessão, apresentação e aplicação do modelo OSI.

Pelo fato da arquitetura TCP/IP possuir menos camadas que o modelo OSI, isso implica na sobrecarga de algumas camadas em funções específicas definidas no modelo OSI. Como exemplo, a transferência de arquivos no ambiente TCP embute as funções correspondentes à camada de apresentação no próprio protocolo FTP. Embora ocorra essa sobrecarga, por outro lado o TCP/IP nos fornece aplicações simples, eficientes e de fácil implementação a nível de produtos.

Já a arquitetura OSI é criticada pelos seus modelos e soluções excessivamente acadêmicos, que atendem a requisições de propósito geral e não facilitam soluções imediatas, em acordo com as exigências dos usuários.

Existe também um esforço de aproximação entre estas duas arquiteturas, tentando aproveitar o que cada uma tem de melhor, buscando encontrar uma solução mista.