DlteC do Brasil®
www.dltec.com.br
info@dltec.com.br | 41 3045.7810

DLTEC DO BRASIL

MODELO OSI

Modelo OSI

O conteúdo dessa apostila é uma adaptação da matéria online do Curso Online Modelo OSI.

Para mais informação visite www.dltec.com.br

Seja muito bem-vindo(a) ao curso Modelo OSI!

Nesse curso iremos estudar com mais detalhe o modelo de referência OSI e suas diferenças para a arquitetura TCP/IP.

Lembre-se que apesar da implementação prática ter sido realizada com o TCP/IP, o modelo OSI acaba sendo uma referência para a classificação e posicionamento dos equipamentos em uma rede.

Além disso, o modelo de OSI ele serve como base para os testes e resolução de problemas em ambientes de rede.

Nesse capítulo você também irá estudar as semelhanças e diferenças entre as camadas do modelo OSI e as integrantes da pilha de protocolos do TCP/IP.

A DlteC estará com você em todos os momentos dessa jornada!

Bons estudos!

Introdução

Olá!

Modelo de Referência OSI é um assunto básico, porém fundamental para quem está entrando no mundo das Redes de Computadores.

Esse conhecimento é fundamental para entendermos o funcionamento de uma rede, como os dispositivos são classificados e como resolver problemas em Redes de Computadores.

Esperamos que você aproveite ao máximo este material, que foi idealizado com o intuito verdadeiro de fazê-lo(a) obter êxito no exame. Estamos torcendo pelo seu sucesso!

Bons estudos!

Modelo OSI

Objetivos

Ao final desse curso você deverá ter conhecimentos sobre:

- Compreender os motivos do desenvolvimento do Modelo de Referência OSI.
- Compreender cada camada do Modelo OSI:
  - Aplicação
  - Apresentação
  - Sessão
  - Transporte
  - Rede
  - Enlace
  - Física
- Conhecer exemplos de protocolos e dispositivos situados em cada uma das camadas do modelo OSI.
- Entender e descrever o processo de encapsulamento e desencapsulamento de dados.
- Entender como utilizar o modelo OSI no processo de resolução de problemas de Redes de Computadores.
- Saber explicar as semelhanças e diferenças entre as camadas do modelo OSI e a pilha de protocolos do TCP/IP.
- Conhecer os protocolos e dispositivos existentes em cada camada do Modelo OSI.

Sumário

1 Introdução ao Curso

Bem-vindo ao **Curso Modelo OSI**, o qual também faz parte do conteúdo da formação **Redes** da DlteC do Brasil.

O curso **Modelo OSI** possui como objetivo fornecer ao aluno uma visão abrangente sobre as camadas ou Layers do modelo de referência que até hoje é de fundamental importância para a compreensão do funcionamento das Redes de Computadores.

Ao final do curso, você deverá ser capaz de:

- Compreender os motivos do desenvolvimento do Modelo de Referência OSI.
- Compreender cada camada do Modelo OSI:
  - Aplicação
  - Apresentação
  - Sessão
  - Transporte
  - Rede
  - Enlace
  - Física
- Conhecer exemplos de protocolos e dispositivos situados em cada uma das camadas do modelo OSI.
- Entender e descrever o processo de encapsulamento de dados.
- Entender como utilizar o modelo OSI no processo de resolução de problemas de Redes de Computadores.
- Saber explicar as semelhanças e diferenças entre as camadas do modelo OSI e a pilha de protocolos do TCP/IP

Esse curso possui E-Book e não esqueça que ao final do curso você poderá emitir o seu certificado!

1.1 Como Estudar com o Material da DlteC

Nesse curso você terá **vídeo aulas**, **material de leitura** e **laboratórios em simuladores** para o aprendizado do conteúdo.

Posso somente ler ou assistir aos vídeos? NÃO RECOMENDAMOS!

O ideal é você assistir aos vídeos e na sequência ler os conteúdos ou...

... se preferir leia os conteúdos e depois assistia aos vídeos, tanto faz.

POR QUE LER E ASSISTIR?

Simples, porque **um conteúdo complementa o outro**.

Assim você terá um aproveitamento muito melhor do curso.

2 Introdução ao Modelo de Referência OSI

Os protocolos surgiram para que a comunicação pudesse ser realizada de maneira eficaz e padronizada, porém no início das redes cada fabricante estava implementando sua comunicação em rede de uma maneira própria, ou seja, com protocolos "**proprietários**".

Você vai ouvir muito na área de TI a palavra "**proprietário**", a qual significa que é de um determinado fabricante (ou Vendor) e normalmente não consegue interoperar com outros fabricantes diferentes.

O oposto dos protocolos **proprietários** são os protocolos **abertos**, os quais são padronizados por órgãos internacionais como a **IETF** (Internet Engineering Task Force), **ISO** (International Standard Organization) e a **ITU** (International Telecommunication Union).

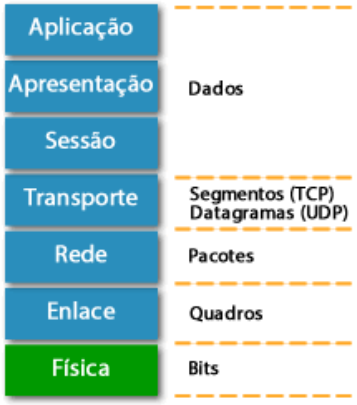
Portanto, esse desenvolvimento proprietário causava um problema sério para as empresas e usuários, pois eles ficavam "amarrados" a um determinado fabricante, dificultando o desenvolvimento de sistemas e a integração das redes.

Para resolver esse problema foi criado o modelo de referência OSI (Open Systems Interconnection), o qual foi desenvolvido pela ISO (International Standard Organization) com o objetivo de criar uma **estrutura para definição de padrões** para a conectividade e interoperabilidade de sistemas diferentes, ou seja, para que diferentes fabricantes pudessem montar protocolos que fossem **interoperáveis**.

Esse modelo define um conjunto de **7 camadas** (em inglês ***layers***) e os serviços atribuídos a cada uma, porém o modelo OSI é uma **referência** e não uma **implementação**!

O modelo OSI criado em 1971, formalizado em 1983 e lançado em 1984 com objetivo de ser um padrão para protocolos de comunicação entre os mais diversos sistemas em uma rede local.

Os objetivos dessa divisão em camadas são:



- Fornecer serviços para a camada imediatamente superior.
- Esconder da camada superior os detalhes de implementação dos seus serviços.
- Estabelecer a comunicação somente com as camadas adjacentes de um sistema.
- Facilitar o desenvolvimento de aplicativos e aplicações padronizadas.

Dessa maneira um desenvolvedor de aplicações não precisaria se preocupar com a comunicação de rede, pois basta fornecer as informações dentro de um padrão aceito pela camada de aplicação e a "rede" cuidaria do restante.

Assim como a comunicação em rede não ficaria "presa" a padrões específicos de um determinado fabricante, pois tudo seria desenvolvido seguindo padrões definidos pela ISO, garantindo a interoperabilidade entre diferentes fabricantes.

2.1 Comunicação em Rede

Uma Rede de Computadores é um conjunto de dispositivos processadores capazes de trocar informações e compartilhar recursos, interligados por um sistema de comunicação.

Outra definição:
"Redes de Computadores são conjuntos de máquinas destinadas ao processamento de dados independentes, com conexão entre seus sistemas operacionais por apenas um processo tecnológico (TANENBAUM, 2003)."

Este sistema de comunicação é composto por elementos ou dispositivos que tem funções bem específicas na rede, tais como os switches que têm a função de dar acesso à rede para os computadores, já os roteadores possuem a função de encaminhar os pacotes IP para os destinos corretos e assim por diante.

Toda essa troca de informação é realizada através de **protocolos**, mas afinal o que é um protocolo?

Na ciência da computação ou informática, um protocolo é uma **convenção ou padrão que controla e possibilita uma conexão, comunicação, 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 seja, que controlam essa "**conversa**" entre os dispositivos.

Os protocolos podem ser implementados pelo hardware, software ou por uma combinação dos dois.

É bem simples de visualizar a importância dos protocolos de comunicação em rede, imagine você em uma reunião em que diversas pessoas estão sentadas ao redor da mesa querendo expor seus problemas e pontos de vista.

Se não houver uma **regra ou protocolo** fica impossível de haver a **comunicação**, concorda?

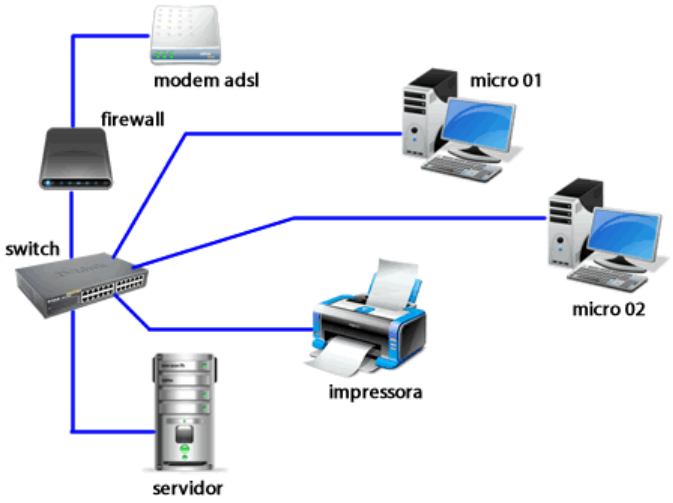
Pois é simples de visualizar que se todos falarem ao mesmo tempo ninguém irá se entender.

A função dos protocolos de rede é bem semelhante, porém muito mais complexa e com uma variedade de padrões, os quais vamos estudar os principais.

Falando em termos simples, uma rede precisa dos seguintes protocolos:

1. Que regulem o acesso aos meios físicos (como a família Ethernet com CSMA/CD, PPP, Frame-relay);
2. Que regulem o envio pela rede e endereçamento lógico da rede (representado pelo protocolo IP);
3. Que regulem o envio das informações dentro dos computadores e separem as diversas comunicações (representado pelo TCP e UDP) e
4. Protocolos que forneçam os serviços de rede aos usuários (representado pelo HTTP, FTP, Telnet, DNS e demais serviços que estamos habituados a utilizar).

Lembre-se: o que queremos em uma rede é que uma determinada informação que está em nosso computador atravesse um meio de comunicação e chegue a outro computador ou servidor para ser processado, como isso será realizado são os protocolos que definem.



É muito importante que você entenda esse fluxo de informações e os diversos dispositivos que os pacotes irão passar, veremos isso ao longo do curso.

2.2 Modelo OSI e a Comunicação em Rede

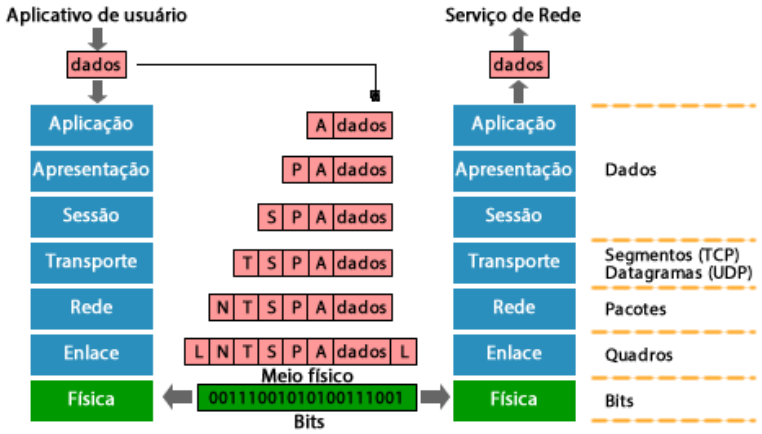
Portanto, o modelo de referência OSI quebra a rede em pedaços ou fatia a rede para que o desenvolvimento seja mais simples e modular.

Cada camada é independente da outra e é como se entre dois hosts houvesse uma conexão camada a camada independentemente uma das outras.

O controle das informações de cada camada é realizado através de uma unidade de protocolo chamada PDU (protocol data unity), as quais são inseridas no início, chamada de "cabeçalho" (em inglês header).

Esses cabeçalhos são lidos no destino para que o computador saiba o que fazer com a informação. Nele estão contidos instruções, endereços e demais controles necessários para que a comunicação flua entre os dois computadores.

O processo de recebimento dos dados do usuário pela camada 7 até sair em bits na camada 1 é chamado de "encapsulamento".



O aplicativo do usuário envia seus dados através da camada de aplicação, esses dados são enviados através da rede e chegam até o destino, o qual normalmente é um serviço de rede disponibilizado por um servidor.

As diversas etapas necessárias para encaminhar esses dados até o destino são tratadas pelas camadas, seguindo regras e padrões pré-estabelecidos.

Agora vamos estudar as camadas do modelo OSI uma a uma separadamente, seguindo da camada física para a camada de aplicação.

2.3 Terminologia do Modelo OSI

O modelo OSI tem alguns termos que você vai encontrar em vários websites e bibliografias, mesmo em versões traduzidas, em Inglês.

Por exemplo, o termo "**camada**" é muitas vezes chamado de "**layer**" ou simplesmente é descrito como "**L**" mais o **número** da camada.

Por exemplo, a camada de enlace pode ser chamada de Camada-2, Layer-2 ou L2.

Você já deve ter lido o termo switch L2 ou L3, isso quer dizer que é um switch que está posicionado na camada de enlace (L2) ou pode estar posicionado na camada de Rede (L3).

Portanto saiba a terminologia em português, sua versão em inglês e seus sinônimos conforme abaixo:

- **Camada de Aplicação**: Camada 7, Layer 7, L7 ou **Application** Layer
- **Camada de Apresentação**: Camada 6, Layer 6, L6 ou **Presentation** Layer
- **Camada de Sessão**: Camada 5, Layer 5, L5 ou **Session** Layer
- **Camada de Transporte**: Camada 4, Layer 4, L4 ou **Transport** Layer
- **Camada de Rede**: Camada 3, Layer 3, L3 ou **Network** Layer
- **Camada de Enlace**: Camada 2, Layer 2, L2 ou **DataLink** Layer
- **Camada de Física**: Camada 1, Layer 1, L1 ou **Physical** Layer

Nós vamos utilizar TODAS as nomenclaturas acima durante o curso para que você esteja acostumado ao final com qualquer uma delas na sua vida prática.

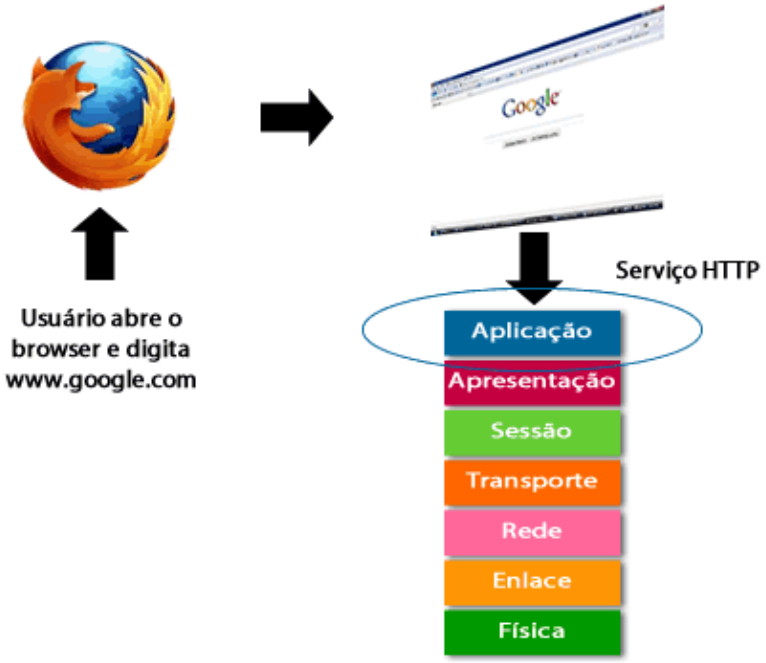
3 Camada de Aplicação

A Camada de Aplicação (Camada 7, Layer 7, L7 ou Application Layer) é a camada superior do modelo de referência OSI, sendo responsável pela interface com as aplicações dos computadores (hosts), ou seja, a camada de aplicação tem a função de dar acesso à rede aos aplicativos dos usuários que estão instalados nos computadores.

A camada de aplicação é a mais simples de se entender, pois ela é como o usuário interage diretamente com a rede.

Por exemplo, usando um protocolo bem definido como o protocolo de transferência de hipertexto (HTTP) o usuário busca uma página da Web sem se importar sobre como o comando HTTP viaja através da rede, ou seja, ele apenas sabe que ao enviar um comando pelo seu navegador de Internet, o aplicativo (ou servidor da Web) na outra extremidade vai receber e sabe como processá-lo.

Veja a figura a seguir onde temos um exemplo em que o usuário abre seu web browser e digita www.google.com, portanto a camada que vai fazer interface com o aplicativo é a 7, ou seja, a camada de aplicação vai pegar os dados do usuário e prepará-los para que eles sejam enviados através das camadas e tenham acesso à rede.



Nessa camada temos diversos serviços de rede, tais como:

- **Serviço de tradução de nomes de Internet**: DNS (TCP/UDP 53)
- **Serviços de e-mail**: SMTP (TCP 25), POP3 (TCP 110) e IMAP (TCP 143)
- **Serviços de terminal e acesso remoto**: RDP (TCP 3389) Telnet (TCP 23) e SSH (TCP 22)
- **Serviços de web**: HTTP (TCP 80) e HTTPS (TCP 443)
- **Gerenciamento de redes**: SNMP (UDP 161)
- **Troca de arquivos em rede**: FTP (TCP 20/21), SFTP (TCP 22) e TFTP (UDP 69)
- **Fornecimento de endereços IPs dinâmicos**: DHCP (UDP 67/68) e DHCPv6 (UDP 546 e 547)
- **Voz e Vídeo sobre IP**: RTP/RTCP (UDP 16384-32767), SIP (TCP/UDP 5060/5061) e H.323 (TCP 1720)
- **Serviços de diretórios**: LDAP (TCP/UDP 389) e LDAPS (TCP 636)
- **Compartilhamento de arquivos**: SMB (TCP 445)
- **Sincronização dos relógios dos dispositivos de Rede**: NTP (UDP 123)

Note que ao lado de cada serviço de rede, os quais vamos estudar em breve, têm uma indicação sobre o tipo de protocolo da camada de transporte e qual porta é utilizada pelo servidor.

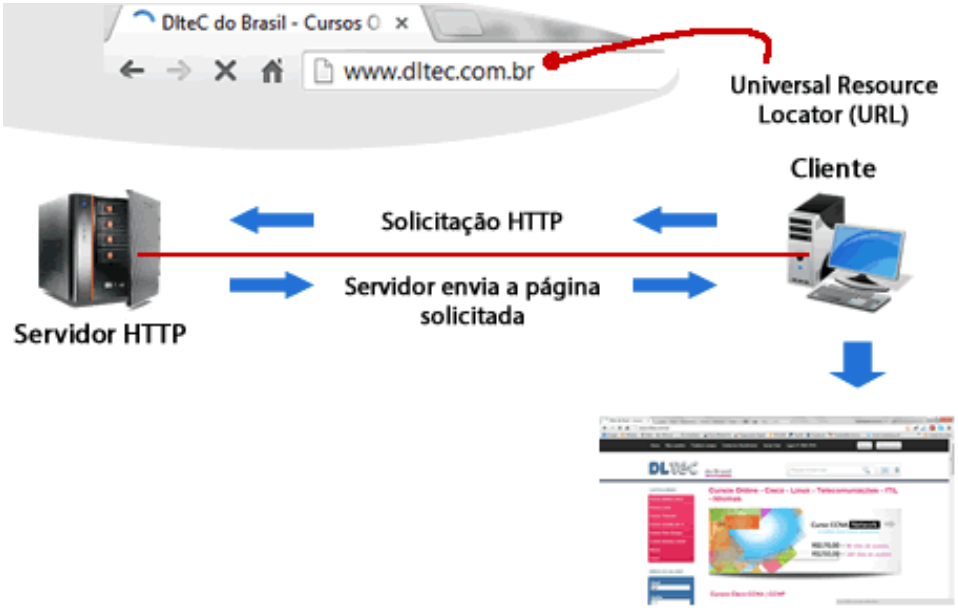
Os serviços de rede da camada de aplicação têm uma íntima ligação com o tipo de protocolo de transporte e seu número de porta (vamos estudar no capítulo sobre a camada-4), por isso mesmo já vamos citar nesse capítulo esses números.

A seguir vamos estudar o conceito de arquitetura cliente/servidor.

3.1 Arquitetura Cliente Servidor

Para entender o funcionamento de uma rede devemos ter em mente que a grande maioria das aplicações e serviços de rede são arquiteturas **Cliente/Servidor**.

Você pode até não ter ouvido esse termo ainda, mas usa diariamente quando acessa uma página de web, pois seu micro utiliza um browser (Mozilla ou Google Chrome) que é um **cliente** para o serviço de web (protocolo HTTP ou HTTPS) e a página que você acessa está hospedada (instalada ou guardada) em um **servidor** web (servidor HTTP ou HTTPS).



É claro que muitas vezes o seu computador pode se tornar um servidor também, por exemplo, quando você compartilha uma impressora ou arquivos em rede através do seu computador, ele estará atuando como servidor quando outro usuário de rede estiver imprimindo ou puxando arquivos das suas pastas.

Resumindo o assunto, os servidores sempre estão prontos para receber uma conexão de rede e fornecer um determinado serviço, já os clientes são os solicitantes que irão utilizar esses serviços.

Os números de porta TCP ou UDP representam as aplicações onde esses serviços de rede estão ativos ou "escutando", ou seja, aguardando conexões dos clientes.

Normalmente essas portas onde rodam os serviços de rede são chamadas de portas bem conhecidas ou "Well Known Ports".

3.2 Protocolos L7

Como profissional da área de infraestrutura de TI você precisa entender as funções dos protoclos da camada de aplicação e o meio de transporte que cada uma delas utiliza.

Abaixo vamos repetir a lista de protocolos já mostrados e depois explicar de maneira breve os principais deles.

- **Serviço de tradução de nomes de Internet**: DNS (TCP/UDP 53)
- **Serviços de e-mail**: SMTP (TCP 25), POP3 (TCP 110) e IMAP (TCP 143)
- **Serviços de terminal e acesso remoto**: RDP (Remote Desktop Protocol - TCP 3389) Telnet (TCP 23) e SSH (Secure Shell - TCP 22)
- **Serviços de web**: **HTTP** (TCP 80) e HTTPS (TCP 443)
- **Gerenciamento de redes**: SNMP (UDP 161)
- **Troca de arquivos em rede**: FTP (TCP 20/21), SFTP (Secure File Transfer Protocol - TCP 22) e TFTP (UDP 69)
- **Fornecimento de endereços IPs dinâmicos**: **DHCP** (UDP 67/68) e DHCPv6 (UDP 546 e 547)

- **Voz e Vídeo sobre IP**: RTP/**RTCP** (Real-Time Protocol e Real-Time Control Protocol - UDP 16384-32767), SIP (Session Initiation Protocol - TCP/UDP 5060/5061) e H.323 (TCP 1720)
- **Serviços de diretórios**: LDAP (Lightweight Directory Access Protocol - TCP/UDP 389) e LDAPS (Lightweight Directory Access Protocol over TLS/SSL - TCP 636)
- **Compartilhamento de arquivos**: SMB (Server Message Block - TCP 445)
- **Sincronização dos relógios dos dispositivos de Rede**: NTP (Network Time Protocol - UDP 123)

Vamos fazer apenas uma observação sobre o protocolo RTCP, pois ele é considerado em muitas bibliografias como um exemplo da camada de sessão, porém como ele trabalha em conjunto com o RTP deixamos na lista para consolidar essa ideia.

Abaixo temos mais de detalhes sobre alguns dos principais protocolos da camada de aplicação:

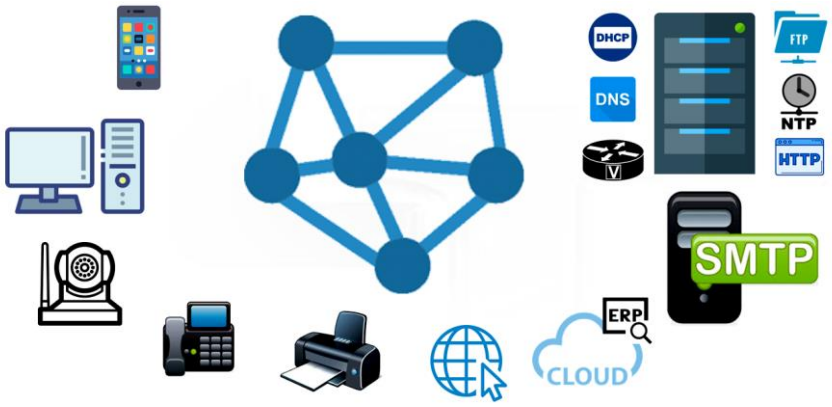
- **DNS (Domain Name System – Sistema de Nomes de Domínio)** – O DNS é um sistema usado na Internet para converter os nomes de domínios e seus respectivos nós de rede divulgados publicamente em endereços IP.
- **DHCP (Dinamic Host Configuration Protocol)** – Utilizado para fornecer dados de configuração das interfaces dinamicamente aos computadores e demais endpoints da rede. Os dados fornecidos são no mínimo endereço IP, máscara de rede, endereço do roteador padrão e servidor DNS. Sem ele os administradores de rede teriam um imenso trabalho braçal.
- **WWW ou HTTP (Hypertext Transfer Protocol)** – Serviço básico utilizado pelos navegadores de Internet ou browsers para acessar o conteúdo das páginas web. Sua versão segura (com ciptografia) é o HTTPS (Hypertext Transfer Protocol Secure).
- **NTP (Network Time Protocol)** - É o protocolo que permite a sincronização dos relógios dos dispositivos de uma rede como servidores, estações de trabalho, roteadores e outros dispositivos com fontes de referências de tempo confiáveis (servidores NTP).
- **FTP (File Transfer Protocol – Protocolo de Transferência de Arquivos)** – é um serviço confiável, orientado a conexões, que usa o TCP para transferir arquivos. Suporta transferências bidirecionais de arquivos binários e ASCII.
- **TFTP (Trivial File Transfer Protocol – Protocolo de Transferência de Arquivos Simples)** – serviço sem conexão que usa o UDP (User Datagram Protocol – Protocolo de Datagrama de Usuário). É usado no roteador para transferir arquivos de configuração e imagens IOS da Cisco e para transferir arquivos entre sistemas que suportam TFTP. É útil em algumas redes locais porque opera mais rápido do que o FTP em um ambiente estável.
- **SMTP (Simple Mail Transfer Protocol – Protocolo Simples de Transferência de Correio)** – Administra a transmissão de correio eletrônico através de redes de computadores. Ele não oferece suporte à transmissão de dados que não estejam em texto simples.
- **POP3 e IMAP4** – São os protocolos utilizados pelos clientes para a leitura do e-mail. A diferença entre eles é que o POP3 (Post Office Protocol version 3) baixa os arquivos para o micro do usuário apagando no servidor, já o IMAP (Internet Message Access Protocol version 4) é possível deixar uma cópia dos e-mails, utilizando como um espelho sem apagar as mensagens, assim o usuário pode ler seus e-mails antigos independente do micro que está utilizando.
- **Telnet (Terminal emulation – Emulação de terminal)** – Permite o acesso remoto a outro computador. Permite que um usuário efetue logon em um host da Internet e execute comandos, porém os dados são transmitidos em texto claro, podendo ser capturado e lido por um invasor no meio do caminho. Existe também uma versão segura chamada Secure Shell ou SSH, o qual possibilita a transferência de informações criptografadas pela rede.
- **NFS (Network File System – Sistema de Arquivos de Rede)** – Conjunto de protocolos de sistema de arquivos distribuído, desenvolvido pela Sun Microsystems, que

permite acesso a arquivos de um dispositivo de armazenamento remoto, como um disco rígido, através da rede.

- **SNMP (Simple Network Management Protocol – Protocolo Simples de Gerenciamento de Rede)** – Oferece uma forma de monitorar e controlar dispositivos de rede e de gerenciar configurações, coleta de dados estatísticos, desempenho e segurança.

Normalmente esses protocolos são chamados também de "**Serviços de Rede**".

3.3 Visão Prática da Camada de Aplicação



Normalmente muitas bibliografias trazem o modelo OSI da camada física para a camada de aplicação, ou seja, iniciam as explicações de baixo para cima no modelo de referência.

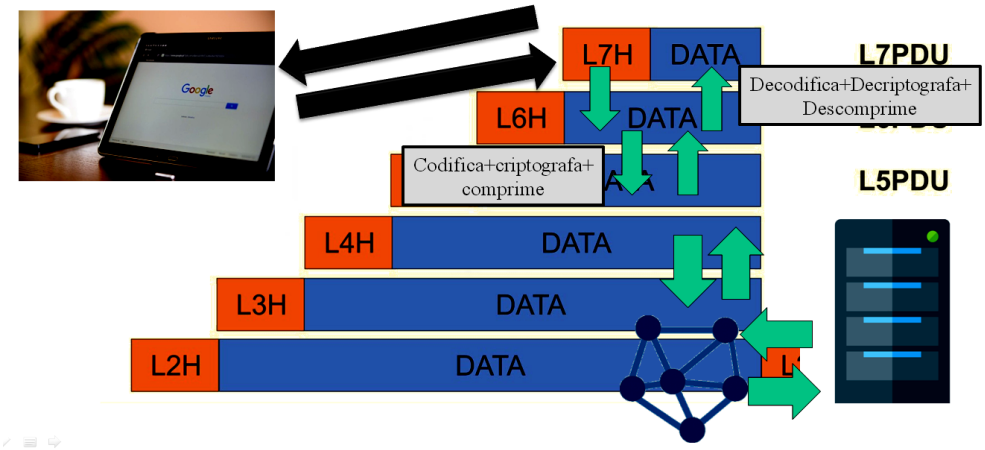
Porém resolvemos inverter essa sequência para que você entenda a importância das aplicações, sua variedade e complexidade.

Muitos iniciantes no mundo de redes preocupam-se apenas com cabeamento e infraestrutura física, quando as aplicações são o verdadeiro sentido de uma rede, pois rede sem aplicação vira um "emaranhado de fios".

Durante a vídeo aula desse tópico você terá mais um pouco da visão prática das aplicações de rede!

4 Camada de Apresentação

A camada de Apresentação (Camada 6, Layer 6, L6 ou Presentation Layer) é responsável pelas transformações ou traduções adequadas nos dados antes do seu envio a camada de sessão, sendo que essas transformações podem ser referentes à compressão de textos, criptografia, conversão de padrões de terminais e arquivos para padrões de rede e vice-versa.



Portanto tem o objetivo de fazer com que os dois lados "falem a mesma língua". Suas funções típicas são:

- Formatação de dados
- Compressão e criptografia
- Compatibilização entre aplicações (sintaxe)

4.1 Exemplos da Camada de Apresentação

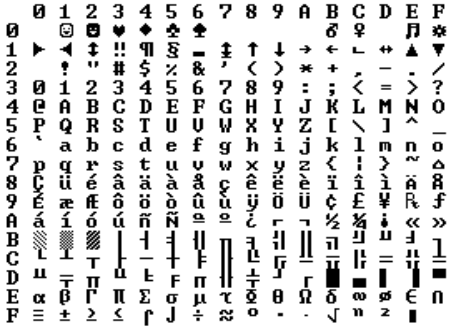
Portanto, a camada de apresentação pega os dados do formato do aplicativo e os converte para o formato de rede, potencialmente criptografando ou compactando a representação dos dados.

Hoje em dia, as camadas de aplicação e apresentação podem ser combinadas para usar XML ou JSON para transporte de dados entre aplicativos.

```
<empinfo>
  <employees>
    <employee>
      <name>Scott Philip</name>
      <salary>£44k</salary>
      <age>27</age>
    </employee>
    <employee>
      <name>Tim Henn</name>
      <salary>£40k</salary>
      <age>27</age>
    </employee>
    <employee>
      <name>Long yong</name>
      <salary>£40k</salary>
      <age>28</age>
    </employee>
  </employees>
</empinfo>
```

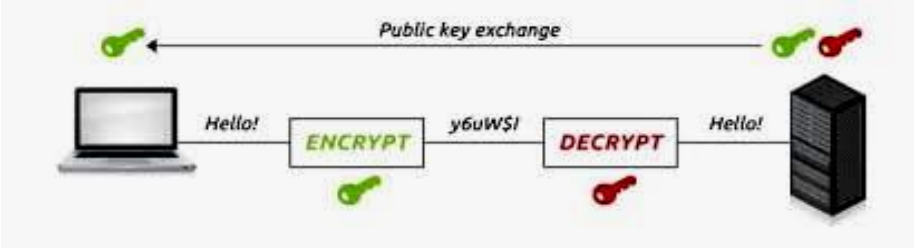
```
{ "empinfo" :
   {
        "employees" : [
        {
          "name" : "Scott Philip",
          "salary" : £44k,
          "age" : 27,

        },

        {
          "name" : "Tim Henn",
          "salary" : £40k,
          "age" : 27,
        },

        {
         "name" : "Long Yong",
         "salary" : £40k,
         "age" : 28,

        }
                ]
    }
}
```

Além disso, o ASCII ou Unicode também podem ser considerados exemplos da camada de apresentação, pois cada lado precisa saber como os comandos de rede são codificados.



Também na transmissão de arquivos de mídia a camada de apresentação pode ter que compatibilizar formatos como jpeg, mpeg, bmp, midi, wav e mp3.

Outros exemplos da camada-6 incluem Multi-Purpose Internet Mail Extensions (MIME) para e-mail, Secure Socket Sockets Layer (SSL) e Transport Layer Security (TLS) para criptografia de dados.



5 Camada de Sessão

A Camada de Sessão (Camada 5, Layer 5, L5 ou Session Layer) é provavelmente a menos compreendida, já que as pessoas tendem a pensar em sessões mantidas dentro da camada de aplicação, como a sessão de um navegador.

Na realidade não é bem essa a função dessa camada, na realidade a camada 5 mantém vários processos em um aplicativo do usuário final sincronizados.

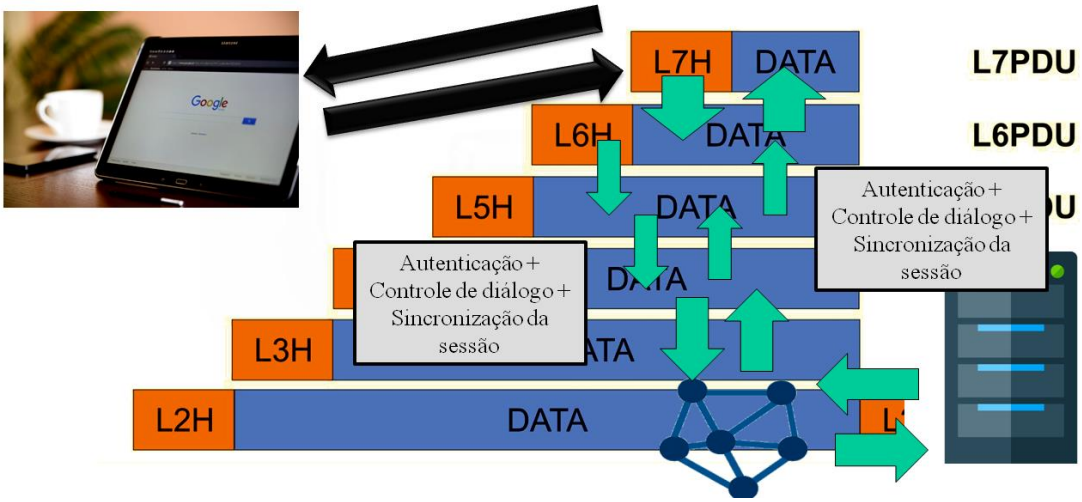
Por exemplo, imagine uma vídeo chamada do Skype, você precisa manter o áudio e vídeo em sincronia, ou então vai parecer um filme estrangeiro mal dublado em português, onde a boca do ator está parada e o narrador está ainda falando.

A camada de sessão ajuda a controlar os pontos de sincronização nas informações trocadas.

Além disso, também pode prover um mecanismo para checkpoint e recuperação de sessões, embora esse seja um aspecto da camada de sessão que o TCP/IP não implementou.

Funções da camada de sessão:

- **Controle de diálogo**: esta camada permite que dois sistemas iniciem a comunicação um com o outro em half-duplex ou full-duplex.
- **Gerenciamento de token**: esta camada evita que as duas partes envolvidas na comunicação tentem uma mesma operação crítica ao mesmo tempo.
- **Sincronização**: esta camada permite que um processo adicione pontos de verificação que são considerados pontos de sincronização no fluxo de dados. Exemplo: se um sistema está enviando um arquivo de 800 páginas, recomenda-se adicionar checkpoints a cada 50 páginas. Isso garante que a unidade de 50 páginas seja recebida e confirmada com sucesso. Isso é benéfico no momento do travamento, por exemplo, se um travamento acontecesse na página 110, não haverá necessidade de retransmitir as páginas de 1 a 100.



A camada de sessão também tem a função de disponibilizar acessos remotos, estabelecendo serviços de segurança, verificando a identificação do usuário, sua senha de acesso e suas características, por exemplo, seus perfis de usuário e autorizações.

Atua como uma interface entre os usuários e as aplicações de destino, podendo inclusive fornecer sincronização entre as tarefas dos usuários, conforme já citado anteriormente.

5.1 Exemplos da Camada de Sessão

Abaixo seguem alguns exemplos de protocolos que podem ser considerados de camada 5:

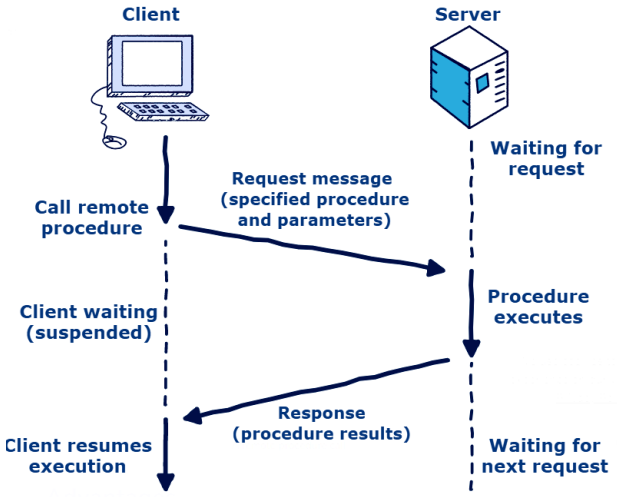
- OSI Session Layer Protocol (X.225, ISO 8327)
- Remote Procedure Call Protocol (RPC)
- Structured Query Language (SQL)
- Network Basic Input/Output System (NetBIOS)
- Network File Systrem (NFS)
- X Windows - Remote desktop sessions
- AppleTalk Session Protocol (ASP)
- AppleTalk Data Stream Protocol (ADSP)

Vamos utilizar uma RPC como exemplo da camada de sessão.

Chamada de procedimento remoto (Remote Procedure Call Protocol - RPC) é uma técnica de computação distribuída na qual um programa de computador chama um procedimento (sub-rotina ou serviço) para executar em um espaço de endereço diferente do seu.

O procedimento pode ser no mesmo sistema ou em um sistema diferente conectado em rede.

A ideia por trás do RPC é que um programa de computador pode chamar e executar uma sub-rotina em um sistema remoto da mesma forma que chamaria uma sub-rotina local, mas os detalhes de comunicação da rede são ocultados do usuário.

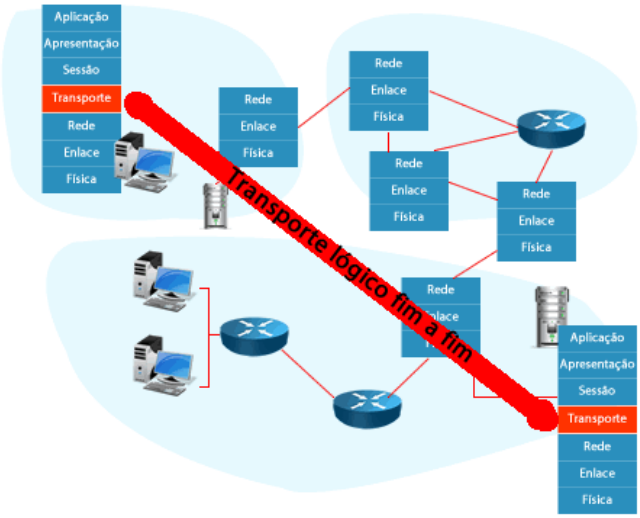


Portanto, uma sessão é aberta entre o cliente e o servidor que fará a execução da rotina.

No cliente a sessão é suspensa até que o servidor processe a rotina e envie a resposta para que ele possa retomar a atividade e finalizar a execução.

6 Camada de Transporte

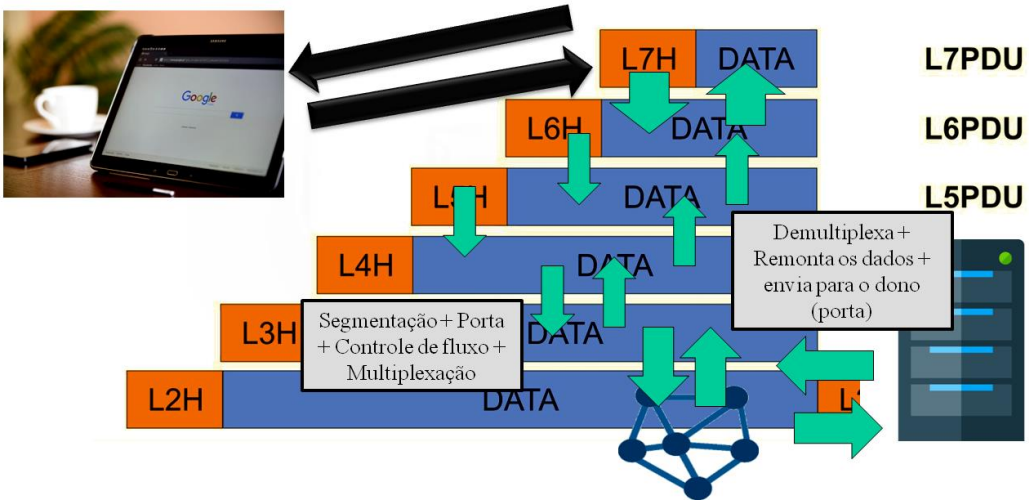
Na Camada de Transporte (Camada 4, Layer 4, L4 ou Transport Layer) temos o conceito de comunicação fim-a-fim.



A camada 4 possui mecanismos que fornecem uma comunicação confiável e transparente entre dois computadores, isto é, assegura que todos os segmentos cheguem corretamente ao destino e na ordem correta.

Funções da camada 4:

- Comunicação orientada a conexão
- Segmentação dos dados
- Ordenação no envio e recebimento dos segmentos
- Confiabilidade
- Controle de fluxo
- Controle de congestionamento
- Identificação dos fluxos e serviços (número de portas)
- Multiplexação das portas



A camada 4 normalmente é caracterizada pelas especificações do protocolo chamado TCP (Transmission Control Protocol), o qual é utilizado em aplicações que necessitam de garantia na entrega e controle de fluxo, pois ele é orientado a conexão.

Porém, existem outros protocolos L4 que não são orientados a conexão e utilizado em aplicações que necessitam de velocidade, pois sem tantos controles como o TCP ele acaba sendo naturalmente mais veloz. Por exemplo, o UDP (User Datagram Protocol).

Na camada 4 quando falamos do fluxo TCP chamamos as informações de **segmentos**, já o fluxo UDP é chamado de **datagrama**.

Um segmento de dados é uma Service Data Unit, que é usada para encapsulamento na camada 4 (camada de transporte).
Ele consiste em elementos de protocolo que contêm controle de informações da Camada 4.

Ao endereçar o segmento de dados, é atribuído um endereço da Camada 4, portanto, uma porta.

O segmento de dados é encapsulado na camada 3 em um pacote de dados.

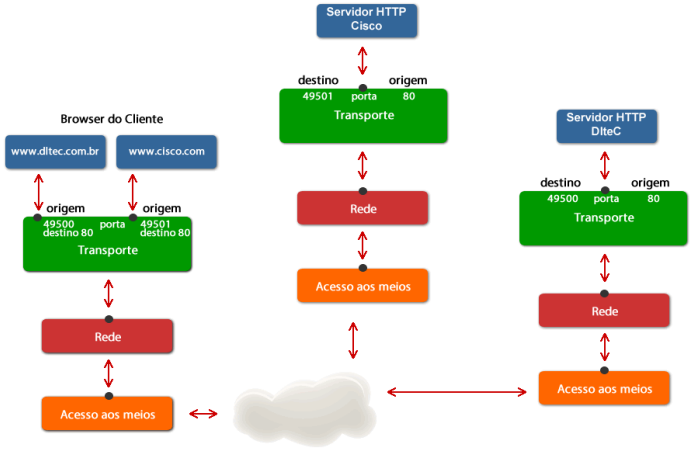
A camada de transporte fornece acesso padronizado às camadas 5 a 7 orientadas para a aplicação, de modo que elas não precisam considerar as características da rede de comunicações.

Cinco diferentes classes de serviços de diferentes graus são definidas na camada 4 do modelo OSI e podem ser utilizadas pelas camadas superiores, desde o serviço mais simples ao mais confortável com mecanismos multiplexação de dados, proteção contra erros e procedimentos de solução de problemas.

6.1 Exemplos da Camada de Transporte

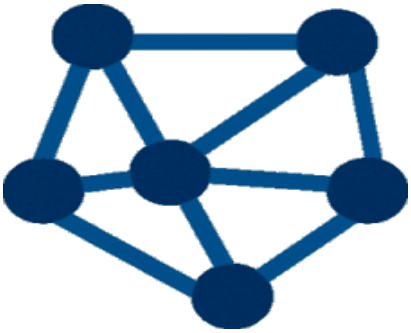
Exemplos de protocolos situados na camada 4 do modelo OSI:

- TCP - Transmission Control Protocol
- UDP - User Datagram Protocol
- SPX - Sequenced Packet Exchange
- ATP - AppleTalk Transaction Protocol
- FCP - Fibre Channel Protocol

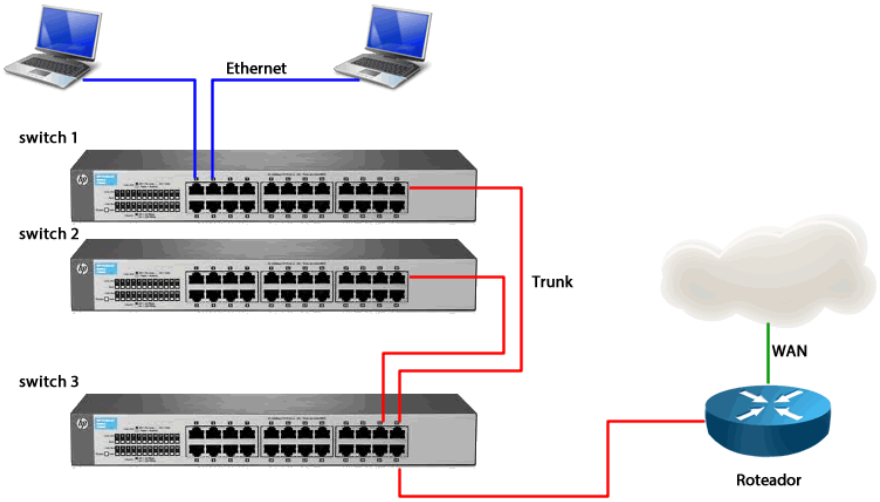


7 Camada de Rede

A Camada de Rede (Camada 3, Layer 3, L3 ou Network Layer) é responsável pelo **esquema de endereçamento** global de uma rede, ou seja, o endereçamento que permite identificar um dispositivo a **longa distância**, e também pelo **roteamento dos pacotes** através dessas diversas redes.



Portando o layer 3 a função de fornecer um canal de comunicação independente do meio, pois ela transmite pacotes de dados através da rede utilizando um esquema de endereçamento lógico que pode ser "roteado" através de diversas redes até chegar ao seu destino.



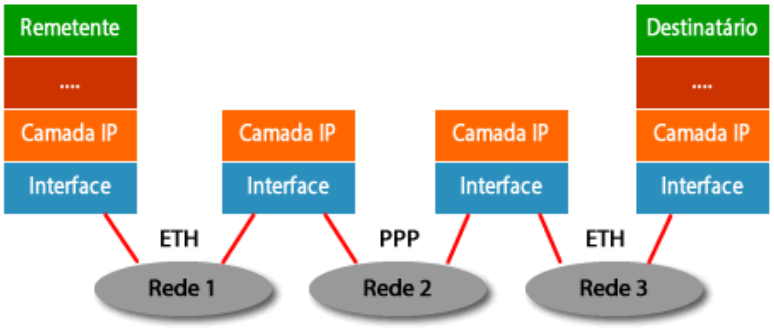
Diferente da camada 4, a camada 3 não possui garantia de entrega, ou seja, não é orientada a conexão (transmissão "best effort" dos pacotes).

As funções características da camada 3 são:

- Esquema de endereçamento lógico
- Construção e manutenção de tabelas de roteamento (protocolos de roteamento)
- Roteamento e chaveamento de pacotes
- Fragmentação de pacotes

As informações trocadas pelos protocolos de camada 3, tais como o IP, são chamadas de **pacotes**. Os protocolos de camada 3 utilizados atualmente tanto na Internet como nas Intranets são o IP versão 4 (IPv4) e o IP versão 6 (IPv6).

É importante ressaltar aqui que a comunicação em rede propriamente dita é realizada pelas camadas 1, 2 e 3.



A partir da camada 4 estamos tratando de uma comunicação mais interna dos computadores, pois elas não são utilizadas na rede para o roteamento e envio das informações.

Uma das funções da camada de rede do modelo OSI, é fornecer a conectividade através do roteamento dos pacotes por entre as diversas redes que compõe uma Intranet ou até mesmo na Internet.

Nem sempre dois hosts estão diretamente conectados e por isso mesmo precisam ter seus pacotes encaminhados ou roteados até alcançarem seu destino.

Quem cumpre esse papel de descobrir as rotas e inseri-las nas tabelas de roteamento são os administradores de rede ou então os protocolos de roteamento dinâmicos.

Quando o próprio administrador configura as rotas em um roteador ou endpoint chamamos esse processo de roteamento estático, pois a parte "inteligente" de descoberta de rotas é feita por um ser humano e no roteador serão inseridas rotas manuais definidas pelo administrador de rede para as diversas redes que compõe a Intranet e também a saída para a Internet.

Esse processo manual é mais econômico para os dispositivos, pois quem pensa é o administrador, porém mais complicado de administrar.

Os protocolos de roteamento dinâmicos têm a função de analisar os endereços de rede de cada roteador e descobrir sozinho os melhores caminhos para as diversas redes que compõe a infraestrutura de uma empresa.

Temos protocolos de roteamento específicos para as Intranets, chamados de IGP (Interior Gateway Protocol), tais como o RIP, OSPF, IS-IS e EIGRP.

Na Internet com o protocolo IP versão 4 o protocolo de roteamento utilizado entre os diversos provedores de serviço, operadoras de Telecomunicação e empresas com Sistemas Autonômos (que possuem sua própria faixa de endereços de Internet) é o BGP-4 (Border Gateway Protocol versão 4).

Portanto, um protocolo de roteamento dinâmico tem um processo que roda nos roteadores, coletando e trocando informações sobre rotas entre eles.

Essas informações são processadas em cada roteador e uma decisão sobre a melhor rota é tomada para que a tabela de roteamento seja alimentada.

7.1 Dispositivos e Protocolos da Camada de Rede

Na camada de rede temos protocolos roteados, protocolos de roteamento e dispositivos L3.

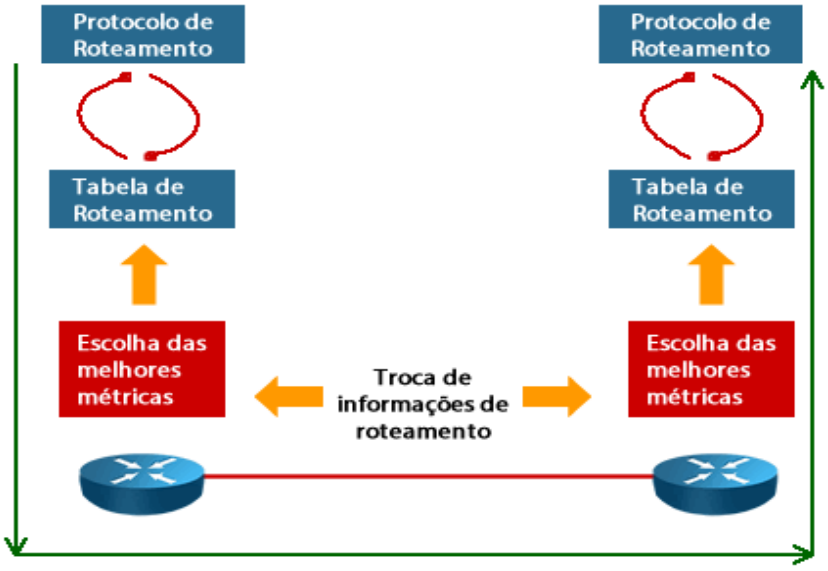
Exemplos de protocolos roteados (fornecem o pacote de camada-3 e esquema de endereçamento):

- IPv4/IPv6 - Internet Protocol
- IPX - Internetwork Packet Exchange

	Internet Protocol version 4 (IPv4)	Internet Protocol version 6 (IPv6)
Publicação	1981	1999
Tamanho do Endereço	32-bit	128-bit
Notação	Decimal: 192.149.252.76	Hexadecimal: 3FFE:F200:0234:AB00: 0123:4567:8901:ABCD
Notação em Prefixo	192.149.0.0/24	3FFE:F200:0234::/48
Quantidade de Endereços	2^{32} = ~4,294,967,296	2^{128} = ~340,282,366, 920,938,463,463,374, 607,431,768,211,456

Exemplos de protocolos de roteamento (descobrem rotas ou melhores caminhos até redes de destino de forma dinâmica):

- RIPv1/v2
- RIPng
- OSPF/OSPFv3
- IS-IS
- EIGRP/EIGRPv6
- BGP



Exemplos de dispositivos de camada-3:

- Roteadores
- Switches L3

8 Camada de Enlace

A Camada de Enlace (Camada 2, Layer 2, L2 ou DataLink Layer) tem a função de esconder as características físicas do meio de transmissão para as camadas superiores, pois ele transforma os bits em quadros (frames).

Sua principal função é fornecer um meio de transmissão confiável entre dois sistemas adjacentes.

As funções mais comuns da camada 2 são:

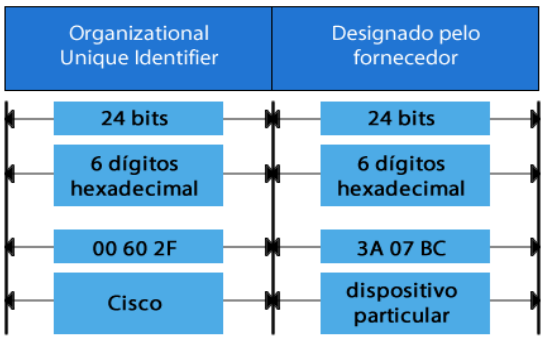
- Controle de acesso aos meios físicos
- Delimitação e formato dos quadros de bits

Protocolo Ethernet

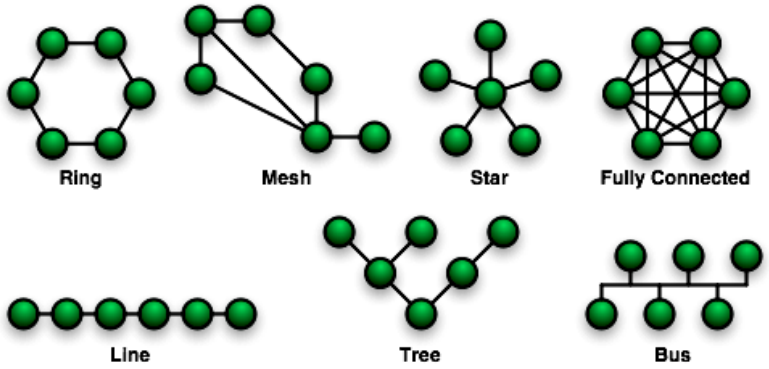
Quadro

Nome do campo	Preâmbulo	Endereço de Destino	Endereço de Origem	Tipo	Dados	Seqüência de Verificação do Quadro
Comprimento	8 bytes	6 bytes	6 bytes	2 bytes	46 - 1500 bytes	4 bytes

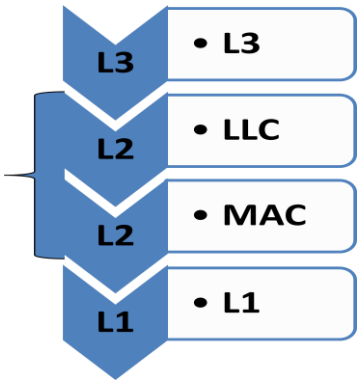
- Detecção de erros
- Sequenciamento dos dados
- Controle de fluxo de quadros
- Endereçamento físico (endereço MAC)



- Topologia lógica da rede



Para redes locais a camada de enlace é dividida em dois subníveis: LLC (Logical Link Control) e MAC (Media Access Control), sendo que a LLC faz interface com a camada de rede e o MAC com a camada física.



A sub-camada LLC é responsável pelo Multiplexing/De-Multiplexing dos protocolos L3 e os serviços lógicos à camada 3.

Já a subcamada MAC é responsável pelo enquadramento (Framing/De-Framing) e interação com L1, por exemplo, processamento do cabeçalho L2, checksum e tratamento de colisões em L1 (CSMA/CD).

Os representantes da camada de enlace são as placas de rede, switches e bridges.

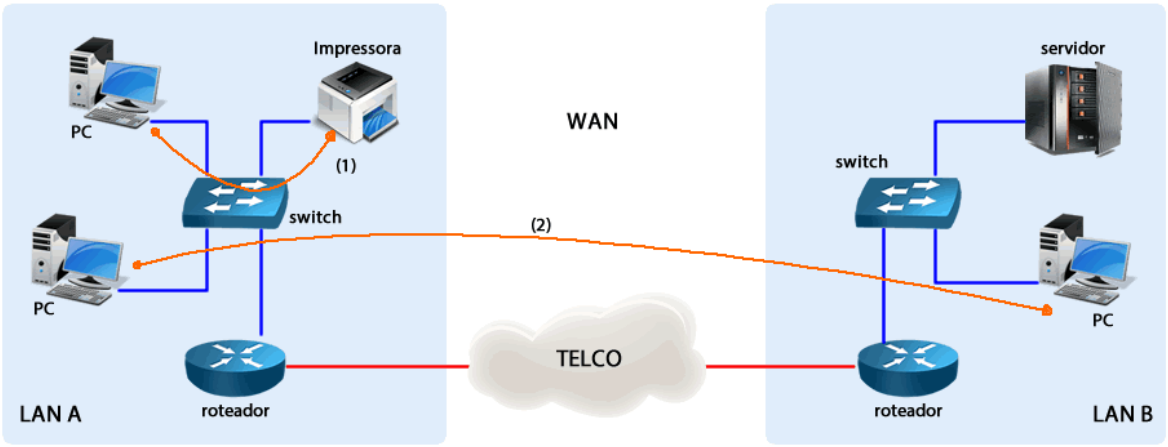
Nas redes atuais recomenda-se o uso de switches no lugar dos HUBs por questões de desempenho e segurança, pois os switches ao invés de enviar uma informação recebida para todas as portas ele cria um caminho virtual ponto a ponto entre os computadores que estão se comunicando, o que melhora sensivelmente o desempenho e a segurança da rede, pois impede que terceiros consigam espiar o tráfego de rede, técnica chamada de "sniffing".

As informações trocadas pelos protocolos de camada 2, tais como o protocolo ethernet, fastethernet, PPP, HDLC e demais são chamadas de **Quadros ou Frames**.

No próximo tópico vamos estudar melhor os exemplos de protocolos e dispositivos da camada de enlace.

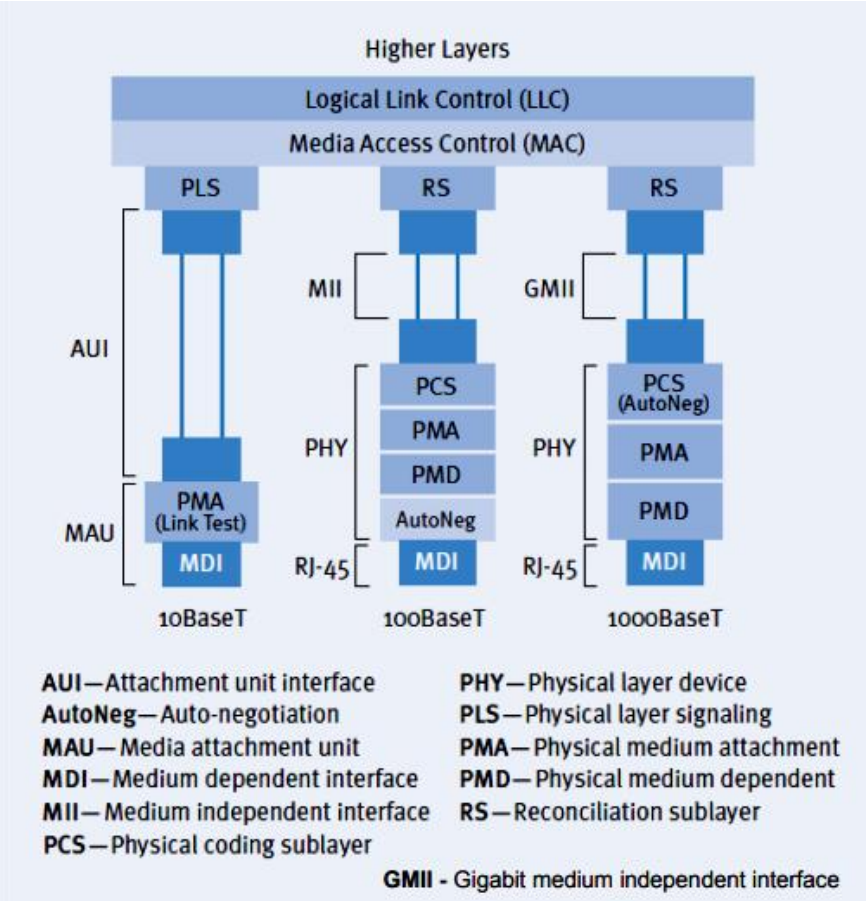
8.1 Dispositivos e Protocolos da Camada de Enlace

Na camada de enlace podemos encontrar protocolos utilizados para envio de quadros (frames) em redes locais (LAN - 1) e WANs (Wide Area Network - 2), protocolos de controle, protocolos de descoberta de vizinhos na rede e dispositivos como switches e bridges.



Exemplos de protocolos de Redes Locais (LAN):

- Família de protocolos Ethernet (IEEE 802.3: Ethernet, Fast Ethernet, Gigabit Ethernet, 10 Gigabit Ethernet...)



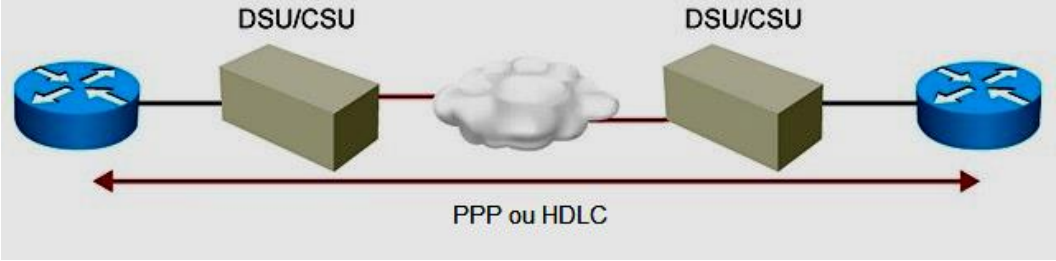
- IEEE 802.11 (Wireless LAN: 802.11 a/b/g/n/ac/ax)

Tecnologia	Novo Nome	Frequência
802.11	Wi-Fi 0	2.4GHz
802.11a	Wi-Fi 1	5GHz
802.11b	Wi-Fi 2	2.4GHz
802.11g	Wi-Fi 3	2.4GHz Only
802.11n	Wi-Fi 4	2.4GHz e 5GHz
802.11ac	Wi-Fi 5	5GHz
802.11ax	Wi-Fi 6	2.4GHz e 5GHz

- FDDI (Fiber Distributed Data Interface)
- Token Ring

Exemplos de protocolos utilizados em Redes WAN:

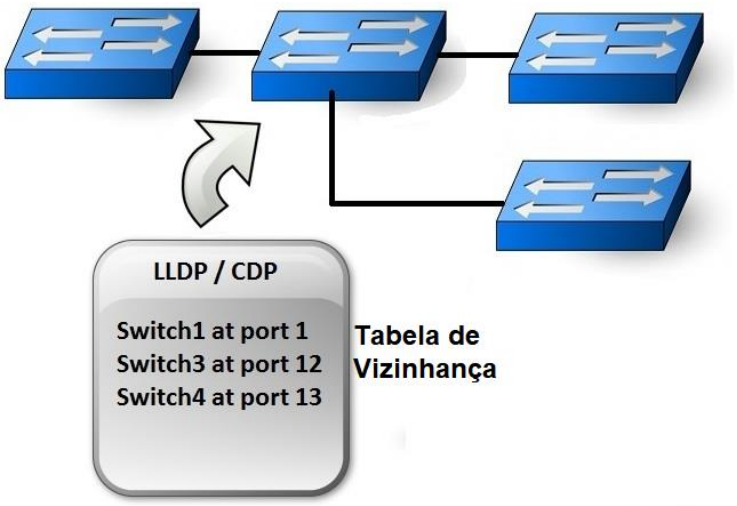
- PPP (Point-to-Point Protocol)
- High-Level Data Link Control (HDLC)



- Frame-relay
- Asynchronous Transfer Mode (ATM)
- Serial Line Internet Protocol (SLIP)
- MPLS (Camada 2.5)

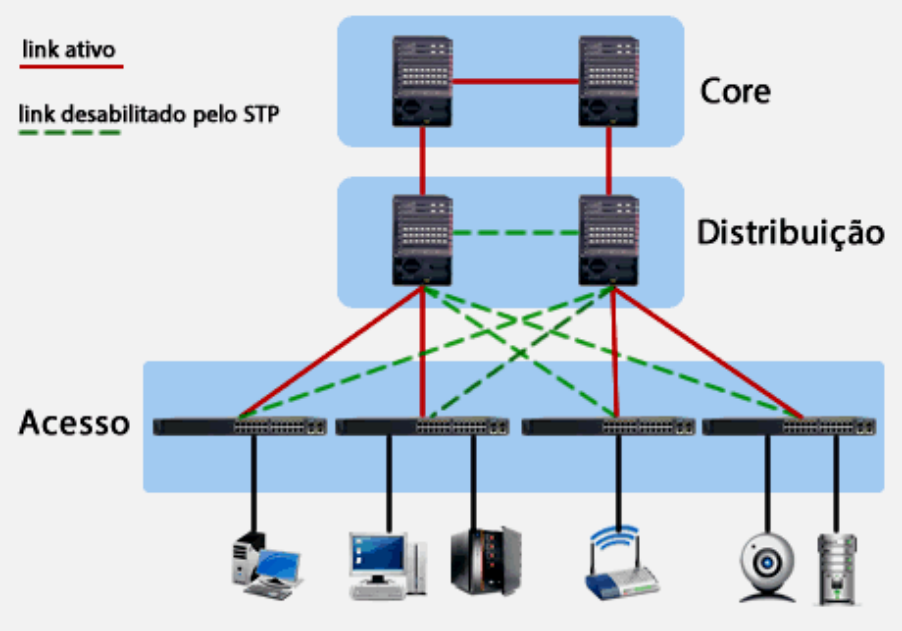
Protocolos para descoberta de vizinhos na rede:

- LLDP (Link layer discovery protocol)
- CDP (Cisco Discovery Protocol)



Protocolos de controle e proteção de Redes L2:

- STP (Spanning tree protocol)
- RSTP (Rapid Spanning tree protocol)
- MSTP (Multiple Spanning tree protocol)



- Unidirectional Link Detection (UDLD)
- 802.1Q

Dispositivos de camada 2:

- Placas de rede (NIC – Network Interface Cards)
- Bridges
- Switches (L2)
- Access Points (APs)

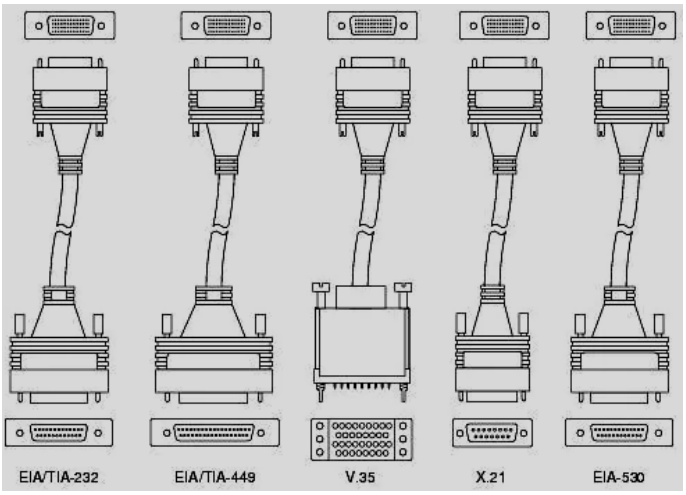
9 Camada Física

A camada Física (Camada 1, Layer 1, L1 ou Physical Layer) trata da **transmissão transparente de sequências de bits pelo meio físico**, sendo a **parte final da comunicação**, ou seja, onde a transmissão pelo meio de comunicação **realmente acontece**.

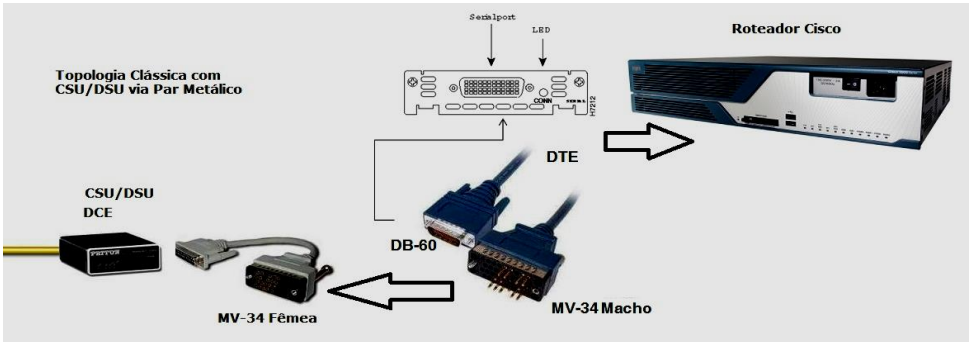
É no L1 onde os BITs são realmente trafegados entre os dispositivos de Rede!

Nessa camada estão definidos:

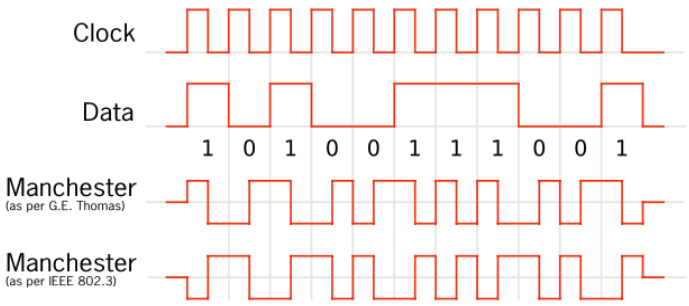
- Padrões mecânicos (conectores, painéis de conexão, cabos, etc...)



- Padrões funcionais (DCE ou DTE, por exemplo)



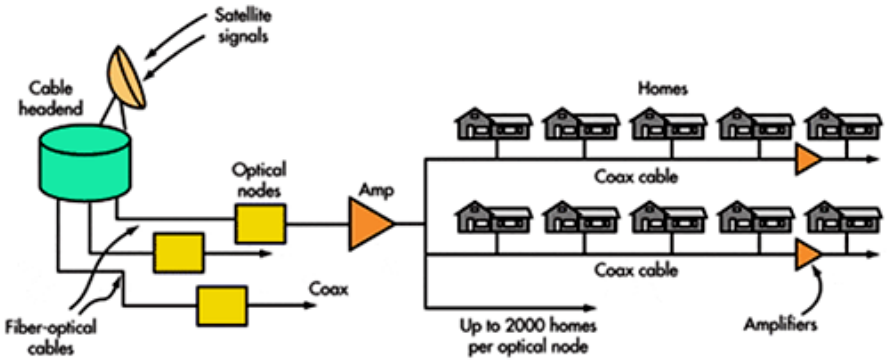
- Especificações elétricas (voltagens, codificação de linha, etc...)



- Procedimentos para acesso a esse meio físico.

Nessa camada também temos as especificações dos meios de transmissão, como por exemplo:

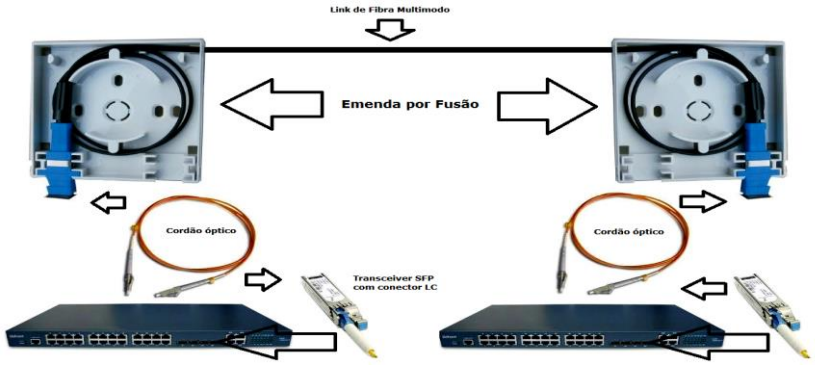
- Cabo coaxial



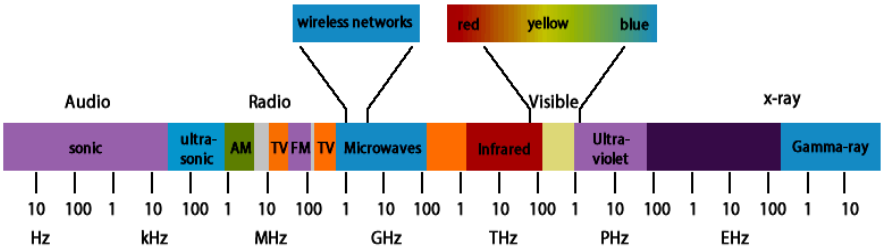
- Par metálico (UTP e STP)

UTP Categories - Copper Cable				
UTP Category	**Data Rate**	**Max. Length**	**Cable Type**	**Application**
CAT1	Up to 1Mbps	-	Twisted Pair	Old Telephone Cable
CAT2	Up to 4Mbps	-	Twisted Pair	Token Ring Networks
CAT3	Up to 10Mbps	100m	Twisted Pair	Token Rink & 10BASE-T Ethernet
CAT4	Up to 16Mbps	100m	Twisted Pair	Token Ring Networks
CAT5	Up to 100Mbps	100m	Twisted Pair	Ethernet, FastEthernet, Token Ring
CAT5e	Up to 1 Gbps	100m	Twisted Pair	Ethernet, FastEthernet, Gigabit Ethernet
CAT6	Up to 10Gbps	100m	Twisted Pair	GigabitEthernet, 10G Ethernet (55 meters)
CAT6a	Up to 10Gbps	100m	Twisted Pair	GigabitEthernet, 10G Ethernet (55 meters)
CAT7	Up to 10Gbps	100m	Twisted Pair	GigabitEthernet, 10G Ethernet (100 meters)

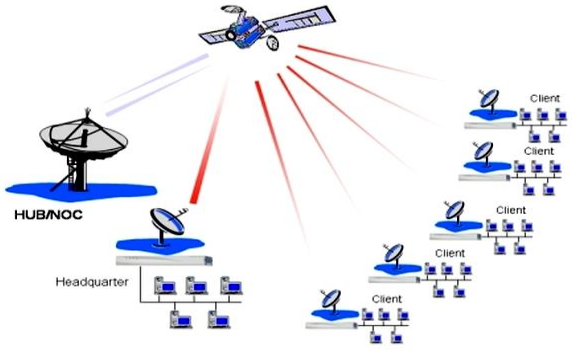
- Fibra óptica (monomodo ou multimodo)



- Rádio transmissão (rádios digitais ponto a ponto, Wifi, espalhamento espectral, etc.)

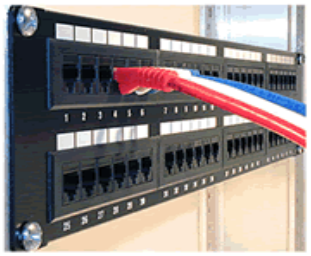


- Transmissão via satélite



Nas redes mais antigas era aqui na camada física que os computadores eram interconectados utilizando os **HUBs**, os quais são dispositivos simples que encaminham os bits recebidos para todas as portas simultaneamente.

Apesar de não recomendado eles ainda são encontrados no mercado e utilizados em redes domésticas e de pequeno porte pelo seu custo ser extremamente baixo.

9.1 Dispositivos da Camada Física

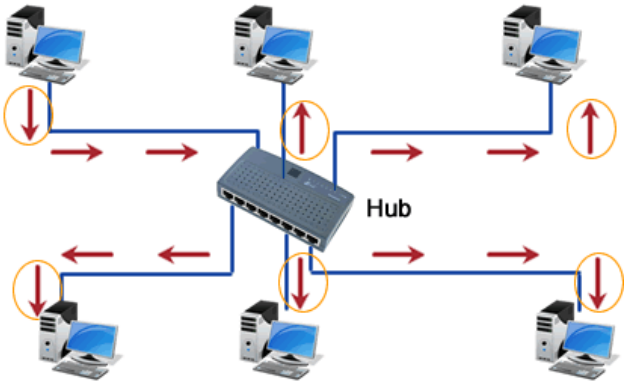
Os dispositivos que estão situados na camada física são os componentes do cabeamento estruturado, tais como conectores, transceiver, patch panels, cabos, HUBs e repetidores (repeaters).

Veja as figuras a seguir.

9.2 Funcionamento dos Hubs e Repetidores

Os Hubs e Repetidores são dispositivos simples que encaminham os bits recebidos para todas as **portas simultaneamente**.

São equipamentos que não tem "inteligência" no encaminhamento, isto é, eles não têm a capacidade de ler endereços ou tomar decisões baseadas em quaisquer tipos de informações, eles simplesmente atuam como um "curto-circuito" ou um "barramento" encaminhando a informação recebida em uma porta para todas as outras conforme imagem a seguir.

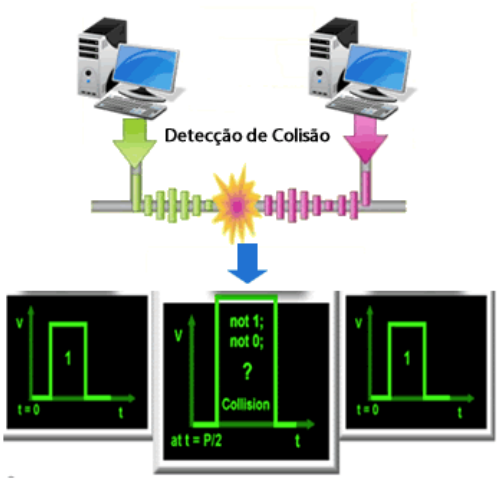


Essa transmissão realizada pelos Hubs e Repetidores é realizada com apenas um par metálico, sendo realizada tanto a transmissão quanto a recepção dos dados pelo mesmo par.

Como os bits são sinais elétricos (ondas eletromagnéticas), por exemplo -5 Volts seria o bit zero e +5 Volts o bit 1, se houver a transmissão de dois deles ao mesmo tempo ocorrerá um problema chamado "**colisão**".

Uma colisão é no "popular" uma "batida" e é isso mesmo, as ondas colidem ou batem uma na outra e o resultado dessa colisão vai ser uma coisa que nem é um bit zero nem um bit 1, ou seja, um sinal que não pode ser interpretado e deve ser descartado.

Se o computador detecta uma colisão, toda transmissão é interrompida e é emitido um sinal ("jam" de 48 bits) para anunciar que ocorreu uma colisão, o qual tem o objetivo de evitar colisões sucessivas.



Quando isso ocorre os computadores devem parar de transmitir e tomar uma ação, a qual é assumir um tempo aleatório randômico e quem acabar o contador antes inicia a transmitir novamente.

Tecnicamente essa ação é chamada "**algoritmo de backoff**".

Outro termo utilizado quando temos redes com Hub e repetidores é o "**Domínio de Colisão**".

Esse termo nada mais é que todas as portas que estão ligadas por Hub ou repetidores que podem ter seus bits colididos, por exemplo, se temos um hub de 24 portas todos os micros que estão conectados nessas 24 portas estão em um mesmo domínio de colisão.

Agora, se conectarmos uma das portas desse hub em outro hub de 24 portas, teremos então um domínio de colisão de 48 portas com 46 hosts que podem ter suas informações colidindo entre si (46 porque gastamos 2 portas, uma de cada hub, para interligá-los), e assim por diante.

Portanto **quanto maior esse domínio de colisão mais problemas sua rede vai ter**, pois temos mais hosts com probabilidade de transmitir simultaneamente e ter seus bits colidindo!


Domínio de colisão 1
24 portas


Domínio de colisão 2
24 portas


Agora que os hubs foram conectados entre si temos um domínio de colisão maior, com 48 portas

Para fechar o assunto, temos então que os hubs são dispositivos para conectarmos os hosts em uma LAN utilizando apenas um par metálico, por isso eles utilizam a transmissão "half-duplex" e estão sujeitos a colisões, portanto as placas de rede precisam ativar o protocolo CSMA/CD.

Aqui temos a explicação do porquê os hubs apresentam uma performance baixa em redes grandes, imagine 50 micros ligados a vários hubs cascateados (ligados uns nos outros), todos tentando acessar a rede, o número de colisões será grande (pois todos estarão em um único domínio de colisão) e a rede ficará naturalmente mais lenta.

Você verá na camada de enlace que os equipamentos de camada 2 conseguem "segmentar" os domínios de colisão e melhorar a performance da rede.

Outro ponto negativo dos hubs é a questão de segurança, pois como a informação trocada entre dois hosts é copiada para todos os outros, se instalarmos em um micro dessa rede um programa que abra essa comunicação, chamado sniffer, poderemos capturar os pacotes trocados e "espiar" essa comunicação.

Assim os atacantes (hackers) conseguiriam descobrir usuários e senhas de rede que sejam trocadas em modo texto, ou seja, sem nenhum mecanismo de proteção como a criptografia.

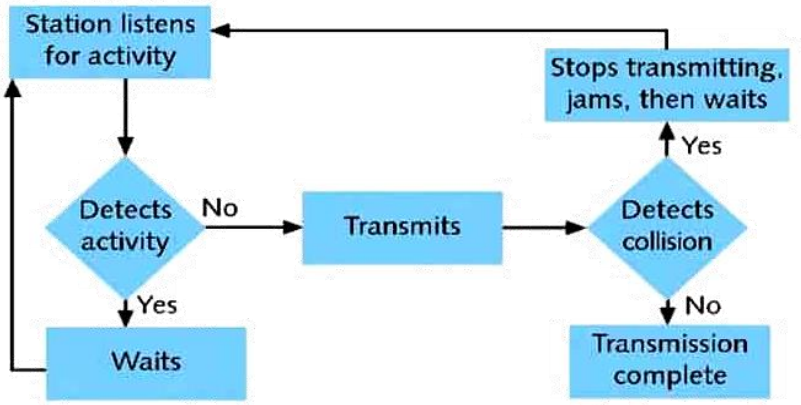
9.3 Protocolos CSMA/CD e CSMA/CA

Todo esse procedimento descrito no tópico anterior está programado nas placas de rede dos computadores que estão conectados aos hubs e é chamado de protocolo CSMA/CD (Carrier Sense Multiple Access with Collision Detection) quando elas estão em modo half-duplex.

A tradução da sigla em português diz bem o que é esse protocolo:

- **CS (Carrier Sense)**: Capacidade de identificar se está ocorrendo transmissão, ou seja, o primeiro passo na transmissão de dados em uma rede Ethernet com hub ou repetidor é verificar se o cabo está livre.
- **MA (Multiple Access)**: Capacidade de múltiplos nós concorrerem igualmente pelo meio de transmissão, ou seja, o protocolo CSMA/CD não gera nenhum tipo de prioridade (daí o nome de Multiple Access, acesso múltiplo). Como o CSMA/CD não gera prioridade pode ocorrer de duas placas tentarem transmitir dados ao mesmo tempo e quando isso ocorre há uma colisão, resultando em que nenhuma das placas consegue transmitir dados.

- **CD (Collision Detection)**: Capacidade de detectar a colisão quando ela ocorrer, ou seja, reconhecer quando um sinal diferente do que foi projetado para os bits zero e um e acionar o algoritmo de backoff.



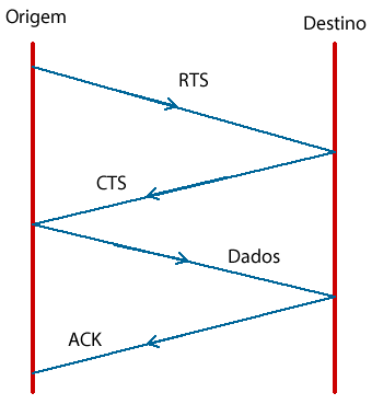
Devido a transmissão e recepção não poder ocorrer simultaneamente, pois temos apenas um meio físico, ela é chamada de "**half-duplex**", o half em português quer dizer metade, o que é a pura realidade do que ocorre na prática.

Se você tem que transmitir e somente em outro período o receptor responde, ou seja, ocorre metade do processo de cada vez, por isso o nome "**half-duplex**".

Já em uma rede sem fio, como não há como detectar uma colisão, é preciso um novo protocolo de acesso aos meios, chamado de CSMA/CA ou "Carrier Sense Multiple Access with Collision Avoidance".

Nas redes com fio temos a detecção da colisão, porém nas redes sem fio temos que "evitar uma colisão", por isso o termo "CA – Collision Avoidance".

Portanto, ambos tipos de redes (com e sem fio) utilizam a detecção de portadoras ou "Carrier Sense", a diferença é que nas redes com fio as colisões são detectadas e nas redes sem fio são evitadas com o uso do protocolo RTS (Request to Send – requisição para enviar) e CTS (Clear to Send – Pronto para enviar).



Como em uma rede sem fio não é possível que a estação transmita e receba ao mesmo tempo fica impossível de detectar uma colisão.

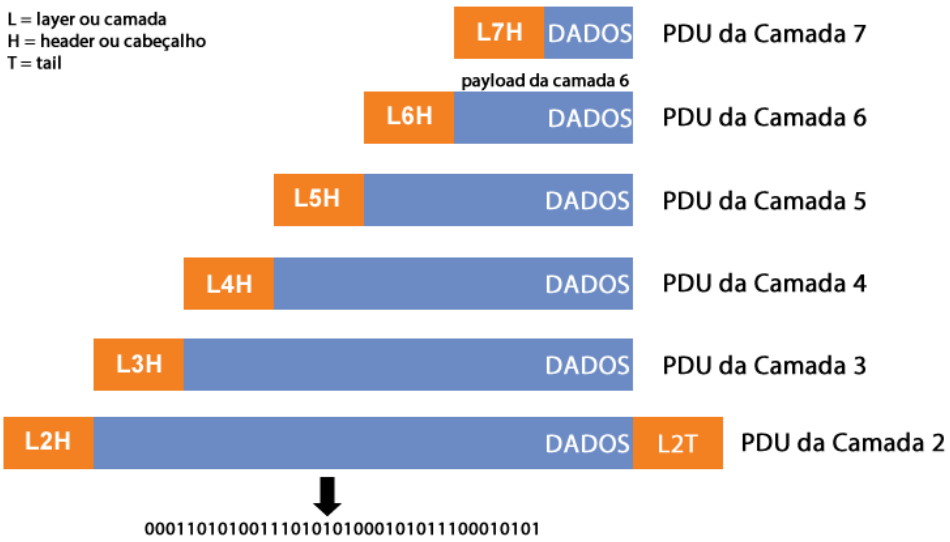
Portanto, o RTS/CTS do CSMA/CA lembra muito o handshake triplo realizado pelo TCP para estabelecer uma conexão antes de iniciar o envio dos segmentos, porém aqui estamos em camada 2.

10 Processo de Encapsulamento dos Dados

Como vimos, o modelo de referência OSI quebra as diversas tarefas necessárias para que um dado seja enviado pela rede em pedaços ou fatias para que o desenvolvimento seja mais simples e modular.

Lembre-se que cada camada vai possuir um formato específico contendo informações de controle, sendo chamado de Unidade de Dados de Protocolo ou **PDU** (Protocol Data Unity), os quais são inseridos no início, na parte chamada de "cabeçalho" (em inglês header) e em algumas vezes no final, chamado de Trailer ou Tail.

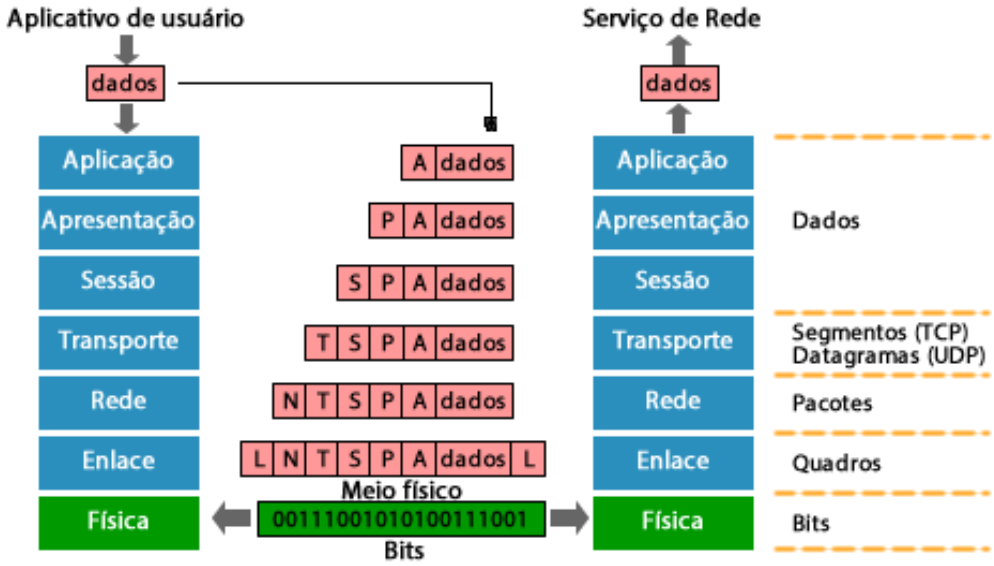
Esses cabeçalhos e tails são lidos no destino para que cada camada saiba o que fazer com a informação. Nele estão contidos instruções, endereços e demais controles necessários para que a comunicação flua entre os dois computadores. Veja a figura a seguir.



Note que cada camada ou layer será inserida na camada inferior como dados, chamado em inglês muitas vezes de payload.

Quando o host de destino recebe a informação ela tem seu cabeçalho/tail lido, depois removido e passado para a camada superior, no processo inverso até os dados que foram enviados pela camada de aplicação serem recebidos pelo aplicativo do host de destino.

Portanto, esse processo de recebimento dos dados do usuário pela camada 7 até sair em bits na camada 1 é chamado de "encapsulamento".

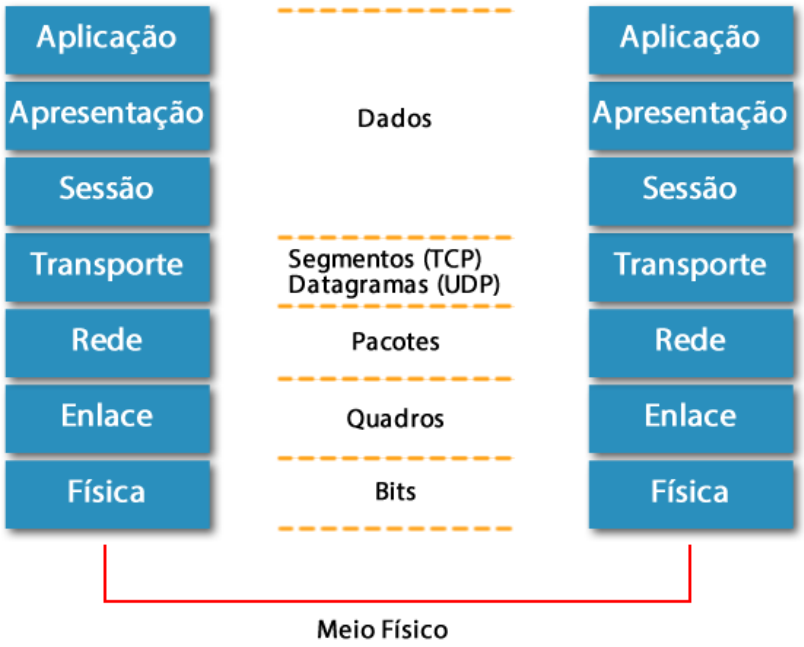


Fica bem claro nas duas animações que tudo inicia no aplicativo do host (computador do usuário).

A partir desse momento, quando um aplicativo quer acessar a rede para comunicar-se com um host remoto, ocorrem os seguintes passos:

1. A camada de aplicação (camada ou layer 7) recebe os dados da aplicação, insere seu cabeçalho e essas informações (cabeçalho de aplicação + dados do aplicativo) são passados para a camada de apresentação.
2. Em seguida a camada de apresentação recebe esses dados, insere suas informações de controle, ou seja, seu cabeçalho e envia esses dados para camada de sessão.
3. Os dados vindos da camada de apresentação recebidos pela camada de sessão, a qual também insere seus dados de controle (seu cabeçalho) e esses dados são enviados à camada de transporte.
4. Os dados recebidos da camada de sessão pela camada de transporte serão agora segmentados (quebrados em pedaços menores) e enviados à camada de rede.
5. A camada de rede recebe os **segmentos** da camada de transporte, insere seus dados de controle (incluindo os endereços de origem e destino de rede) e envia seus **pacotes** para a camada de enlace prepará-los para que eles sejam enviados através do meio físico.
6. Na camada de enlace os pacotes são **enquadrados** recebendo as informações de controle e normalmente um **endereçamento físico** em seu cabeçalho, podem ter inserido também um **tail** contendo informações para controle de erros e são finalmente enviados para a camada física.
7. Na camada física os **quadros** recebidos da camada de enlace são convertidos no padrão físico que estiver sendo utilizado (elétrico, óptico, sinal de rádio, etc.) e enviado pelo meio de transmissão até o destino ou então para o próximo salto responsável pelo roteamento da informação até o destino final.

É importante ficar atendo ao nome "técnico" dado a cada PDU conforme figura a seguir.



Você pode encontrar também bibliografias que utilizam a palavra **datagrama** para descrever os PDUs da camada de rede do protocolo **IP** e da camada de transporte quando utilizando o protocolo **UDP**, isso porque ambos os protocolos são "**Best effort**" (melhor esforço), ou seja, não são orientados a conexão como o protocolo de transporte TCP.

Analise ainda a figura anterior e veja que ao ser recebido pela Máquina B ou Host B a informação passará pelo processo inverso do encapsulamento até chegar ao aplicativo que deve recebê-la, esse processo é o **desencapsulamento**.

Ou seja, a camada física passa os bits para a camada de enlace, a qual verifica se os endereços físicos e demais informações de controle são realmente para aquele host, retira seu cabeçalho e passa para a camada de rede.

A camada de rede lê o cabeçalho, verifica se o endereço de destino contido nele é realmente o seu e depois retira todo seu cabeçalho e passa a informação para a camada de transporte. Isso se repete até a camada de aplicação da Máquina B enviar os dados para o aplicativo de destino para que ele seja processado e uma ação seja tomada, a qual pode ser, por exemplo, inserir um novo e-mail em sua caixa de entrada.

Então chegamos ao fim do estudo do modelo OSI e você deve aqui ter aprendido a nomenclatura de cada camada, o que cada uma delas faz, quais os dispositivos que estão em cada uma delas e o processo de encapsulamento.

Na sequência veremos o TCP/IP, o qual é a pilha de protocolos de rede que realmente foram implementadas nas redes, porém toda a referência do mundo de redes é sobre o modelo OSI, por isso é tão importante entender ambos!

10.1 Dispositivos e Protocolos: Revisão

OSI	Dispositivos	Protocolo	TCP/IP
Aplicação	Firewall, PC, Server, Endpoints, Application Firewall, IPS, IDS	SMTP, HTTP, HTTPS, FTP, TFTP, Telnet, SSH	Aplicação
Apresentação	N/A	JPEG, JPG, TIFF, GIF, MIME, MP3, MP4	
Sessão	N/A	SQL, NFS, RPC	
Transporte	Firewall, IPS, IDS	TCP, UDP, SPX	Transporte
Rede	Router, Switch L3	IPv4, IPv6, IPX, OSPF, BGP, RIP, RIPng	Internet
Enlace	Switch (L2), Bridge, AP	Ethernet, PPP, HDLC, Frame-relay, ATM, SLIP, 802.11a/b/g/n/ac/ax	Acesso à Rede
Física	Hub, Repetidor, Transceiver	Padrões de Modem, Série V	

11 Modelo OSI na Prática: Visão de Rede e Troubleshooting

Não são todos os estudantes e profissionais de Redes de Computadores que conseguem visualizar como conectar essa teoria que estudamos até aqui com o seu dia a dia, ou seja, como aplicar esse conhecimento nas tarefas diárias e resolução de problemas de Rede.

Muitos pensam no modelo OSI como algo somente teórico, que deve ser decorado para passar na prova de certificação, concurso público ou em uma matéria da Faculdade e que depois pode ser esquecido, pois não é utilizável na prática.

Esse é um erro grave, cometido por muitos, mas que pode ser facilmente reparado.

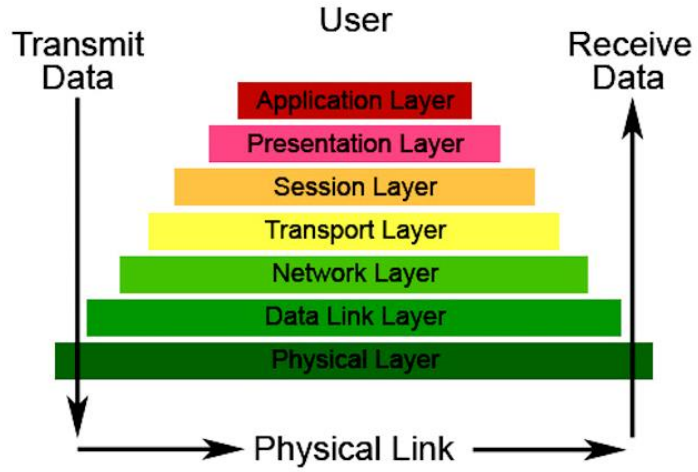
Vamos agora ver como o modelo OSI pode ajudar um administrador de rede facilitando seu dia a dia.

11.1 Entendendo a Rede como um Todo

É bem comum encontrarmos no mercado de trabalho profissionais que são capazes de bloquear uma porta do switch, configurar um endereço IP em uma interface etc.

Mas nem todos conseguem realmente visualizar como rede funciona, com uma visão macro.

O entendimento do modelo OSI lhe dá a capacidade de entender como os bits são enviados através de sinais elétricos via fios de cobre; como esses bits são remontados em quadros pelo Ethernet na camada 2; como esses quadros são comutados para o destino certo, como o PC desmonta os quadros e pacotes para verificar se ele é o IP de destino; como ele quebra o segmento da camada de transporte, responde com um reconhecimento (ACK), e envia os dados para a camada sessão, apresentação e de aplicação, e como toda comunicação, por menor que seja, exige que todo esse processo aconteça muitas e muitas vezes por segundo.



Através do entendimento do modelo OSI você poderá entender os conceitos de configuração de recursos avançados como Listas de Controle de Acesso mais facilmente.

Tendo o conhecimento de que o protocolo da camada de transporte e que os números de portas são utilizados para identificar aplicações, você poderá entender com maior clareza a criação de listas de controle de acesso que definem o tráfego desejado, por exemplo.

11.2 Modelo OSI no Troubleshooting de Rede

Uma vez que você entenda o modelo OSI, você será capaz de realizar troubleshooting muito mais facilmente e de maneira mais eficaz.

Na hora de realizar o troubleshooting tenha em mente como o modelo OSI trabalha: o tráfego flui da camada de aplicação para baixo, em direção a camada física e então trafegam no meio físico (cabo ethernet, por exemplo) até a camada física do receptor.

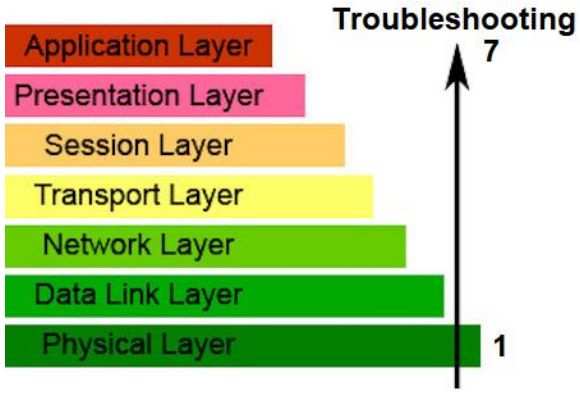
Uma vez no receptor, flui da camada física em direção à camada de aplicação.

Do ponto de vista do receptor, ele agora agirá como emissor, os dados seguirão o caminho inverso, indo da camada 7 até a 1, trafegando pelo meio físico até a outra ponta e assim sucessivamente.

Então se uma das camadas do modelo OSI não está funcionando, o tráfego não flui nesse processo.

Por exemplo, se a camada de enlace não funciona o tráfego nunca irá conseguir ir da camada de aplicação para a física, pois no meio do caminho a camada de enlace não funcionou.

Uma das abordagens mais utilizadas é realizar o troubleshooting indo de baixo para cima, ou seja, da camada 1 (física) em direção a camada 7 (aplicação).



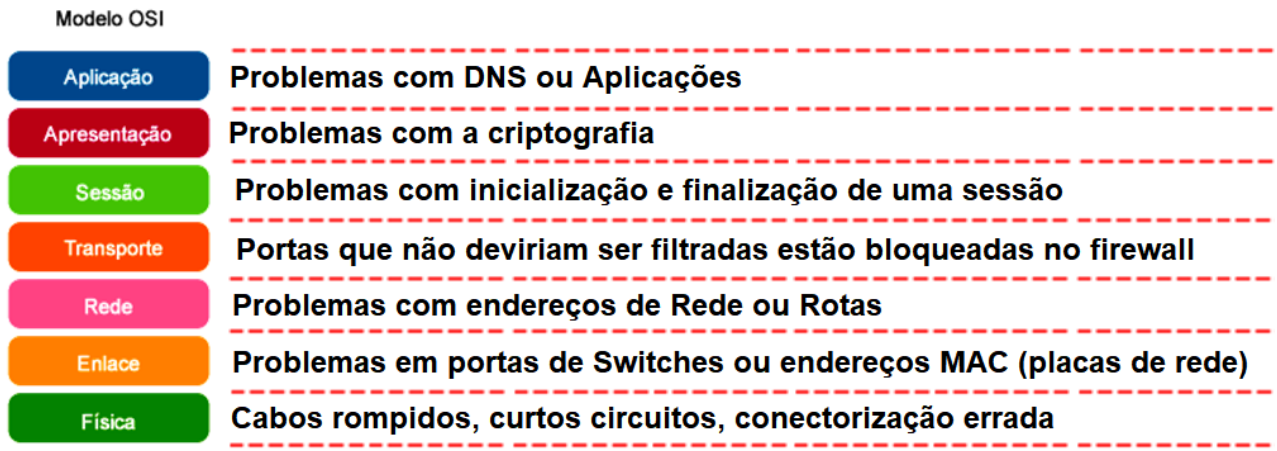
Inicie investigando a camada física (cabos e conectores, por exemplo), pois aqui estão mais de 90% dos problemas na prática.

Se encontrar algum problema, conserte-o, teste novamente e se a comunicação falhar passe para a camada de enlace.

Ao investigar a camada 2 verifique por exemplo se não existe nenhum endereço MAC duplicado investigando a tabela MAC em seu switch.

Depois passe para a camada 3 e verifique o endereçamento IP, máscaras de rede e assim sucessivamente.

Veja um resumo dos problemas na figura a seguir.



Tenha em mente que o entendimento do modelo OSI irá lhe trazer muito mais benefícios do que simplesmente passar em uma prova, seja ela para o que for.

Procure sempre, no seu dia a dia fazer analogias e tentar trazer um determinado problema para dentro do modelo OSI.

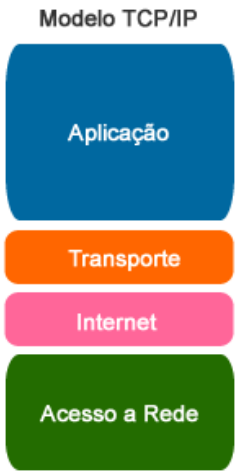
Com um pouco de prática, estudo e determinação isso irá se tornar cada vez mais fácil para você.

E com certeza, seu entendimento da rede como um todo irá aumentar, melhorando também sua performance profissional.

12 Modelo OSI versus TCP/IP

Apesar do modelo OSI ser uma referência para as redes, pois todos os dispositivos são caracterizados pela sua camada no modelo OSI, a arquitetura TCP/IP é a que foi realmente implementada e está em uso até os dias de hoje, tanto nas redes internas como na Internet.

A arquitetura TCP/IP tradicionalmente é composta por 4 camadas (formando a pilha da estrutura do protocolo) conforme mostra a figura abaixo.

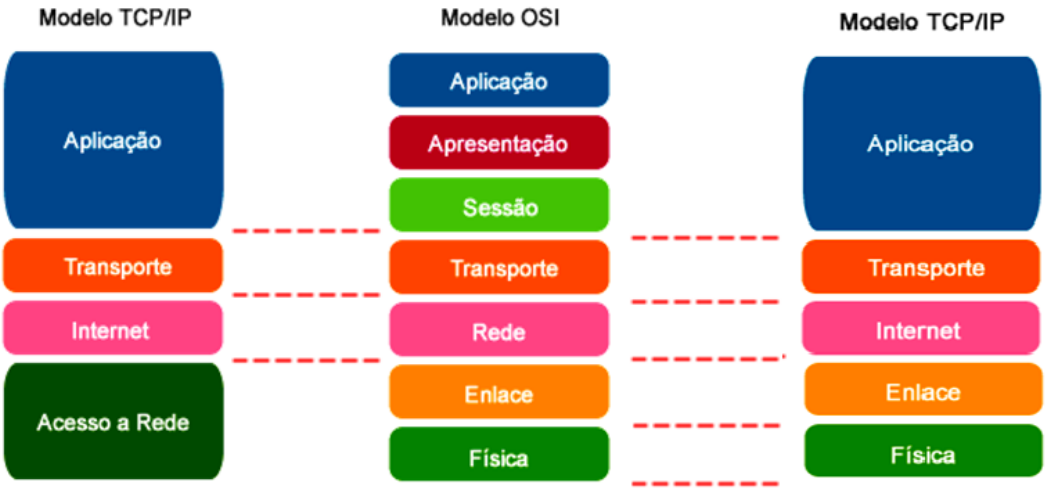


Na prática, as camadas 5, 6, e 7 do modelo OSI foram mescladas para formar a camada de Aplicação do TCP/IP.

Já as camadas 3 e 4 dos dois modelos são similares, porém a camada 3 do TCP/IP é chamada de Internet.

Já as camadas 1 e 2 do modelo OSI foram mescladas no TCP/IP para formar a camada de acesso aos meios ou acesso à rede.

Veja abaixo que existe uma versão didática da pilha de protocolos TCP/IP que é dividida em 5 camadas, sendo que as camadas 4, 2 e 1 são idênticas às respectivas camadas do modelo OSI, porém a camada 3 continua sendo chamada de Internet no TCP/IP e Rede no modelo OSI.



Vamos agora a uma descrição breve de cada camada da arquitetura TCP/IP.

Camada de Acesso à Rede ou Acesso aos Meios
Esta é a camada inferior da arquitetura TCP/IP tem as funcionalidades referentes às camadas 1 e 2 do Modelo OSI.

Se você utilizar o TCP/IP em 5 camadas as camadas física e de enlace tem a mesma função que as camadas do modelo OSI.

Camada Internet
A camada Internet, também conhecida como de Rede ou Internetwork, é equivalente a camada 3 do Modelo OSI. Os protocolos IP e ICMP (ping) estão presentes nesta camada.

Camada de Transporte
A camada de Transporte equivale à camada 4 do Modelo OSI. Seus dois principais protocolos são o TCP e o UDP.

Camada de Aplicação
A camada superior é chamada de camada de aplicação equivalente às camadas 5, 6 e 7 do Modelo OSI. Os protocolos mais conhecidos são: HTTP, FTP, Telnet, DNS e SMTP.

Para finalizar, aqui é importante você entender e se acostumar com a nomenclatura de rede, pois iremos abordar tanto o modelo OSI como o TCP/IP posteriormente.

Mas por que é tão importante saber o OSI e TCP/IP?

A resposta é simples, para que você conheça os equipamentos de rede e principalmente entenda o fluxo de informações que são trocados entre dois hosts.

Somente assim você terá condições de projetar e resolver problemas reais de rede!

13 Conclusão do Curso Modelo OSI e Certificado

Parabéns por ter chegado ao final do curso Modelo OSI!

Tenha certeza de que compreendeu todos os conceitos aqui mostrados:

- Motivos do desenvolvimento do Modelo de Referência OSI.
- Função de cada camada do Modelo OSI:
  - Aplicação
  - Apresentação
  - Sessão
  - Transporte
  - Rede
  - Enlace
  - Física
- Entender e descrever o processo de encapsulamento e desencapsulamento de dados.
- Conhecer os protocolos e dispositivos existentes em cada camada do Modelo OSI.
- Saber explicar as semelhanças e diferenças entre as camadas do modelo OSI e a pilha de protocolos do TCP/IP.
- Entender como utilizar o modelo OSI no processo de resolução de problemas de Redes de Computadores.

Não esqueça que você deve ler e assistir tudo para obter o seu certificado de conclusão do curso.

Ficamos por aqui e nos encontramos nos próximos cursos!!!!!