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

DLTEC DO BRASIL

PROTOCOLO TCP/IP

Protocolo TCP/IP

O conteúdo dessa apostila é uma adaptação da matéria online do Curso Protocolo TCP/IP.

Para mais informação visite www.dltec.com.br

Seja muito bem-vindo(a) ao curso Protocolo TCP/IP.

Falar da importância do TCP/IP e seus protocolos para os profissionais de Redes e Infraestrutura de TI é algo simples, pois na prática as Redes se comunicam utilizando o TCP/IP!

Maioria dos padrões, protocolos, boas práticas, endereçamento, topologias e muito mais dependem do conhecimento do TCP/IP para uma boa compreensão.

Aproveite muito bem o material, pois é com uma base sólida que os verdadeiros profissionais conseguem se diferenciar e chegar mais longe!

Lembre-se que o conteúdo é vasto, mas DlteC estará com você em todos os momentos dessa jornada!

Bons estudos!

Introdução

Olá!

Seja bem-vindo ao **Curso Protocolos TCP/IP**.

Apesar do modelo OSI ser a referência para as redes e toda sua nomenclatura, pilha de protocolos TCP/IP é o que foi realmente implementado na prática e está em uso até os dias de hoje.

O TCP/IP está em uso tanto nas redes internas (Intranets ou Redes Corporativas) como na Internet e provedores de Serviço em geral.

Esperamos que você aproveite ao máximo este material, que foi idealizado com o intuito verdadeiro de fazê-lo(a) um verdadeiro profissional da Infra de TI!

Estamos torcendo pelo seu sucesso!

Bons estudos!

Curso Protocolo TCP/IP

Objetivos

Ao final desse curso você deverá ter conhecimentos sobre:

- Descrever as características, funções e exemplos de protocolos das camadas do protocolo TCP/IP:
  - Aplicação
  - Transporte
  - Internet
  - Acesso aos meios
- Diferenças entre os protocolos TCP e UDP
- O que é uma arquitetura cliente/servidor
- Funcionamento e características do protocolo TCP
  - Formato do segmento TCP
  - Estabelecimento uma Conexão TCP
  - Confirmação de Recebimento de Segmentos TCP
  - Retransmissão de Segmentos TCP
  - Controle de Congestionamento TCP
  - Reagrupamento de Segmentos TCP
- Funcionamento e características do protocolo UDP
  - Formato do datagrama UDP
- Principais Portas TCP e UDP
- Introdução ao endereçamento IP
  - Formato do pacote e endereço IPv4
  - Formato do pacote e endereço IPv6
  - Princípios de Roteamento IP
- Principais protocolos da camada de Acesso aos Meios
- Endereços de camada-2 e comunicação em redes na camada de acesso aos meios
- Interpretar os campos do endereçamento MAC
- Processo de encapsulamento e desencapsulamento no TCP/IP
- Tipos e padrões de cabeamento

Sumário

1 Introdução ao Curso

Bem-vindo ao **Curso Protocolo TCP/IP**!

O **Curso Protocolo TCP/IP** possui como objetivo fornecer ao aluno uma visão abrangente sobre os protocolos integrantes do TCP/IP, suas funções e características.

Ao final do curso, você deverá ser capaz de:

- Descrever as características, funções e exemplos de protocolos das camadas do protocolo TCP/IP:
  - Aplicação
  - Transporte
  - Internet
  - Acesso aos meios
- Diferenças entre os protocolos TCP e UDP
- Arquitetura cliente/servidor
- Funcionamento e características do protocolo TCP
  - Formato do segmento TCP
  - Estabelecimento uma Conexão TCP
  - Confirmação de Recebimento de Segmentos TCP
  - Retransmissão de Segmentos TCP
  - Controle de Congestionamento TCP
  - Reagrupamento de Segmentos TCP
- Funcionamento e características do protocolo UDP
  - Formato do datagrama UDP
- Principais Portas TCP e UDP
- Introdução ao endereçamento IP
  - Formato do pacote e endereço IPv4
  - Formato do pacote e endereço IPv6
  - Princípios de Roteamento IP
- Principais protocolos da camada de Acesso aos Meios
- Endereços de camada-2 e comunicação em redes na camada de acesso aos meios
- Interpretar os campos do endereçamento MAC
- Processo de encapsulamento e desencapsulamento no TCP/IP
- Tipos e padrões de cabeamento

Não esqueça que ao final do curso você poderá emitir o seu certificado!

1.1 Como Estudar com o Material da DlteC do Brasil

Nesse curso você terá **vídeo aulas** e **material de leitura** 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**. Principalmente se você está se preparando para a prova de certificação é crucial que você tanto veja os vídeos como a matéria de leitura!

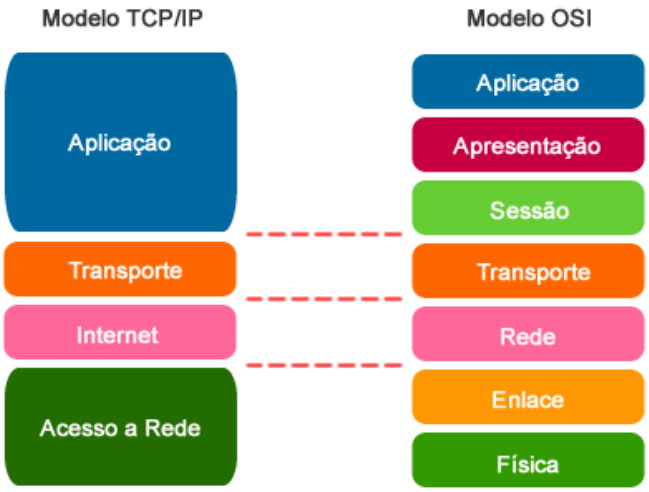
2 Visão Geral do Protocolo TCP/IP

Apesar do modelo OSI ser a referência para as redes e toda sua nomenclatura, a arquitetura **TCP/IP é a que foi realmente implementada** e está em uso até os dias de hoje tanto nas redes internas (Intranets ou Redes Corporativas) como na Internet.

A arquitetura TCP/IP é composta por apenas 4 camadas (formando a pilha da estrutura do protocolo), sendo que 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 do modelo OSI são similares às camadas 2 e 3 do TCP/IP, inclusive a camada de transporte do TCP/IP tem o mesmo nome, porém a camada 3 do modelo OSI (rede) no TCP/IP é chamada de **Internet**.

Por fim, 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 a figura a seguir.



No TCP/IP não costumamos nos referir por camadas e sim pelos nomes delas, pois quando nos referimos pelo número da camada estamos falando do OSI.

Você pode encontrar bibliografias dividindo o TCP/IP em cinco camadas, tratando a camada de Acesso a Rede ou Acesso aos meios físicos como: Enlace ou Data Link e Física.

Essa divisão em 5 camadas ao invés de 4 camadas é puramente didática, pois a RFC 1122 não prevê o protocolo TCP/IP em 5 camadas.

Vamos estudar as camadas do TCP/IP e suas principais características.

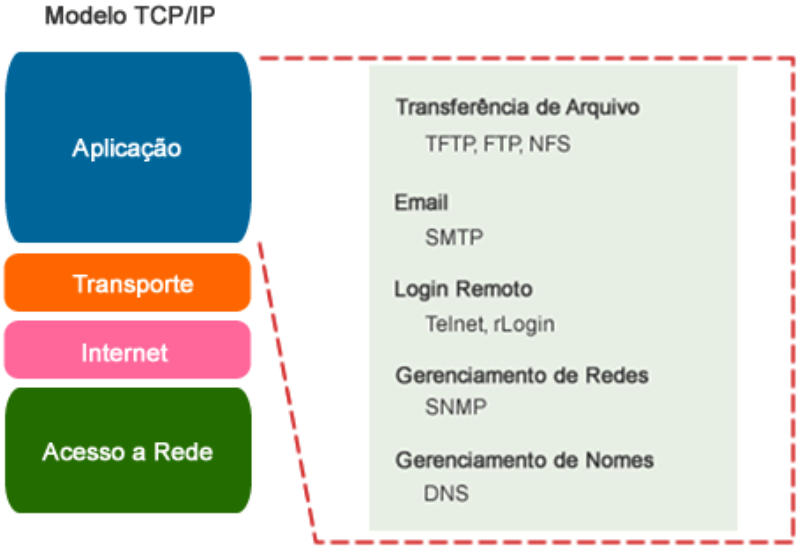
3 Camada de Aplicação

Assim como no Modelo OSI, a camada de Aplicação (Application Layer) é a camada superior do modelo TCP/IP.

Ela é responsável por fornecer a interface entre as aplicações que utilizamos para comunicação e a rede subjacente pela qual nossas mensagens são transmitidas.

Os protocolos da camada de aplicação são utilizados para troca de dados entre programas executados nos hosts de origem e de destino.

Existem diversos protocolos da camada de Aplicação, e outros novos estão em constante desenvolvimento, veja alguns exemplos na figura a seguir.



A camada de aplicação do modelo TCP/IP trata de protocolos de alto nível, questões de representação, codificação e controle de diálogos, ou seja, o que as camadas 5, 6 e 7 do modelo OSI fazem separadamente a aplicação do TCP/IP trata como um pacote só, fazendo interface direta com a camada de transporte.

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.
- **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 IMAP** – São os protocolos utilizados pelos clientes para a leitura do e-mail. A diferença entre eles é que o POP3 baixa os arquivos para o micro do usuário apagando no servidor, já o IMAP 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**" ou "Network Services".

4 Camada de Transporte

A função da camada de Transporte (Transport Layer) é proporcionar a identificação dos serviços de rede, segmentação de dados e o controle necessário para reagrupar esses segmentos em fluxos de comunicação. Veja a figura abaixo.

Para tal a camada de transporte deve ser capaz de fazer as seguintes tarefas:

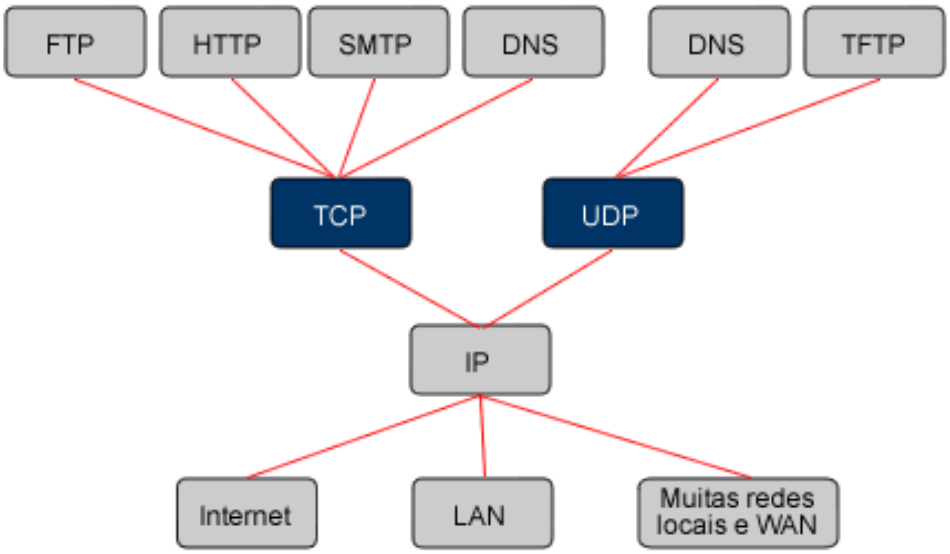
- Rastreamento de Conversações Individuais
- Segmentação de Dados
- Reagrupamento de Segmentos
- Identificação das Aplicações (número de porta TCP ou UDP)

No TCP/IP a camada de transporte pode oferecer dois caminhos ou serviços, confiável através do protocolo TCP e não confiável através do protocolo UDP.

Mas note que na teoria geral essa camada se refere às características gerais do protocolo TCP normalmente.

Ambos os protocolos gerenciam a comunicação de múltiplas aplicações que desejam acessar a rede simultaneamente.

Veja a figura a seguir para entender melhor o posicionamento da camada de transporte dentro da pilha de protocolos TCP/IP.



Perceba que as aplicações normalmente usam um ou outro protocolo como serviço de transporte ponto a ponto.

O TCP é um protocolo orientado à conexão, descrito na RFC 793. O TCP causa sobrecarga adicional na rede, pois possui funções adicionais - entrega ordenada, entrega confiável e controle de fluxo.

Cada segmento TCP tem 20 bytes de overhead no cabeçalho que encapsula o dado da camada de Aplicação, enquanto o segmento UDP tem apenas 8 bytes.

Algumas das aplicações que usam TCP são:

- Navegadores web (HTTP e HTTPS)
- E-mail (SMTP, POP e IMAP)
- FTP
- DNS – consulta entre servidores

O UDP é um protocolo simples e sem conexão, descrito na RFC 768.

Ele tem a vantagem de fornecer uma entrega de dados com baixa sobrecarga e maior velocidade, pois ele não possui os mecanismos de controle do TCP.

Sua desvantagem é que não é confiável, por isso a camada de aplicação deve tratar dessas características.

Os segmentos de comunicação em UDP são chamados datagramas.

Estes datagramas são enviados como o "**melhor esforço**" por este protocolo da camada de Transporte, ou seja, o UDP envia e não espera por confirmação nem tampouco controla fluxo.

As aplicações que usam UDP incluem:

- DNS – consulta de cliente a servidor
- Voz Sobre IP (RTP – Real time protocol)
- TFTP
- SNMP

Lembre-se, o que define o TCP é confiabilidade e o que define o UDP é velocidade!

São características comuns ao TCP e UDP:

- Segmentação de dados das aplicações das camadas superiores.
- Envio de segmentos de um dispositivo em uma ponta para um dispositivo em outra ponta.
- Multiplexação de informações da camada de aplicação (transporte de vários fluxos simultaneamente).
- Identificação das aplicações e conexões de cliente utilizando números de porta.

São características exclusivas do TCP:

- Estabelecimento de operações ponta a ponta (hand-shake de três vias).
- Controle de fluxo proporcionado pelas janelas móveis (janelamento).
- Confiabilidade proporcionada por números de sequência e confirmações de entrega dos segmentos.
- Retransmissão de segmentos perdidos.

Podemos fazer aqui uma comparação da aplicação sendo um veículo que tem duas estradas para escolher, uma das estradas é segura e com certeza você vai chegar ao seu destino, porém ela tem tantos pontos de checagem, pedágios e outros mecanismos de controle de tráfego que acaba sendo mais lenta, esse é o TCP.

Por outro lado, temos uma pista sem controle de tráfego nenhum e por isso ela é muito mais rápida, porém para trafegar nessa pista seu carro vai precisar que você tenha um mapa preciso, GPS e muita atenção do motorista (a aplicação), pois ela não tem indicações. Esse é o UDP.

Por isso o UDP é utilizado, por exemplo, para o tráfego de Voz sobre a rede IP e implementações de VPN (redes virtuais privadas), pois a voz e o acesso VPN precisam de velocidade. Já aplicações como HTTP para leitura de páginas não precisam dessa urgência, por isso utilizam o TCP como meio de transporte.

4.1 Protocolos TCP e UDP

Assista a vídeo aula com a revisão sobre o TCP versus UDP.

5 Protocolo TCP

O TCP é um dos principais protocolos da camada transporte do modelo TCP/IP.

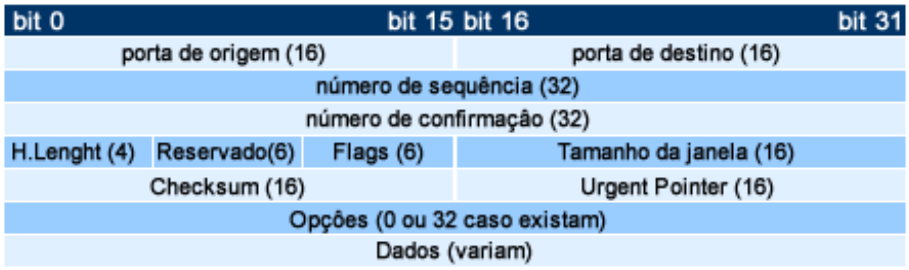
Sua versatilidade e robustez o torna adequado a redes globais, uma vez que este protocolo verifica se os dados são enviados de forma correta, na sequência apropriada e sem erros pela rede.

As características fundamentais do TCP são:

- **Orientado à conexão** - A aplicação envia um pedido de conexão para o destino e usa a "conexão" para transferir dados.
- **Ponto a ponto** - uma conexão TCP é estabelecida entre dois pontos.
- **Confiabilidade** - O TCP usa várias técnicas para proporcionar uma entrega confiável dos pacotes de dados, que é a grande vantagem que tem em relação ao UDP, e motivo do seu uso extensivo nas redes de computadores. O TCP permite a recuperação de pacotes perdidos, a eliminação de pacotes duplicados, recuperação de dados corrompidos e pode recuperar a ligação em caso de problemas no sistema e na rede.
- **Full duplex** - É possível a transferência simultânea em ambas as direções (cliente-servidor) durante toda a sessão.
- **Handshake** – Possui mecanismo de estabelecimento e finalização de conexão a três e quatro tempos, respectivamente, o que permite a autenticação e encerramento de uma sessão completa. O TCP garante que, no final da conexão, todos os pacotes foram bem recebidos.
- **Entrega ordenada** - A aplicação faz a entrega ao TCP de blocos de dados com um tamanho arbitrário num fluxo (ou stream) de dados, tipicamente em octetos. O TCP parte estes dados em segmentos de tamanho especificado pelo valor MTU. Porém, a circulação dos pacotes ao longo da rede (utilizando um protocolo de encaminhamento, na camada inferior, como o IP) pode fazer com que os pacotes não cheguem ordenados. O TCP garante a reconstrução do stream no destinatário mediante os números de sequência.
- **Controle de fluxo** - O TCP usa o campo janela ou window para controlar o fluxo. O receptor, à medida que recebe os dados, envia mensagens ACK (=Acknowledgement), confirmando a recepção de um segmento. Como funcionalidade extra, estas mensagens podem especificar o tamanho máximo do buffer no campo (janela) do segmento TCP, determinando a quantidade máxima de bytes aceita pelo receptor. O transmissor pode transmitir segmentos com um número de bytes que deverá estar confinado ao tamanho

da janela permitido: o menor valor entre sua capacidade de envio e a capacidade informada pelo receptor.

Veja na figura a seguir os campos do cabeçalho do segmento TCP e logo abaixo a explicação de cada campo.



- **Porta de origem**: Número da porta de origem.
- **Porta de destino**: Número da porta de destino.
- **Número de sequência**: Número utilizado para garantir a sequência correta dos dados que estão chegando. Especifica o número do último octeto (byte) em um segmento.
- **Número de confirmação**: Próximo octeto TCP esperado. Especifica o octeto seguinte esperado pelo receptor.
- **H.Lenght**: Comprimento do cabeçalho do segmento em bytes.
- **Reservado**: Definido como zero.
- **Flags**: Funções de controle, como a configuração e término de uma sessão. Utilizado no gerenciamento de sessões e no tratamento de segmentos.
- **Janela**: Número de octetos que o remetente está disposto a aceitar. É o valor da janela dinâmica, quantos octetos podem ser enviados antes da espera do reconhecimento.
- **Checksum**: Cálculo de verificação feito a partir de campos do cabeçalho e dos dados. Utilizado para verificação de erros no cabeçalho e dados.
- **Urgent Pointer**: Indica o final de dados urgentes. Utilizado somente com um sinalizador URG flag.
- **Opção**: Informações opcionais. Uma opção atualmente definida é o tamanho máximo do segmento TCP.
- **Dados**: Dados de protocolo da camada superior, chamado também de Payload.

5.1 Arquitetura Cliente/Servidor e Estado das Portas TCP/UDP

Vamos agora ver como funciona o processo do TCP em um servidor ao executar diversas aplicações.

Cada processo de aplicação sendo executado no servidor é configurado para usar um número de porta, seja no modo padrão ou manualmente através de um administrador do sistema.

Conforme já comentamos em um mesmo servidor não podem existir dois serviços designados ao mesmo número de porta dentro dos mesmos serviços da camada de Transporte.

Por exemplo, um host executando uma aplicação de servidor web e uma aplicação de transferência de arquivo não pode ter ambos configurados para usar a mesma porta.

Quando uma aplicação de servidor ativa é designada a uma porta específica, essa porta é considerada como estando "aberta" (listening ou escutando) no servidor. Isto significa que a camada de Transporte aceita e processa segmentos endereçados àquela porta.

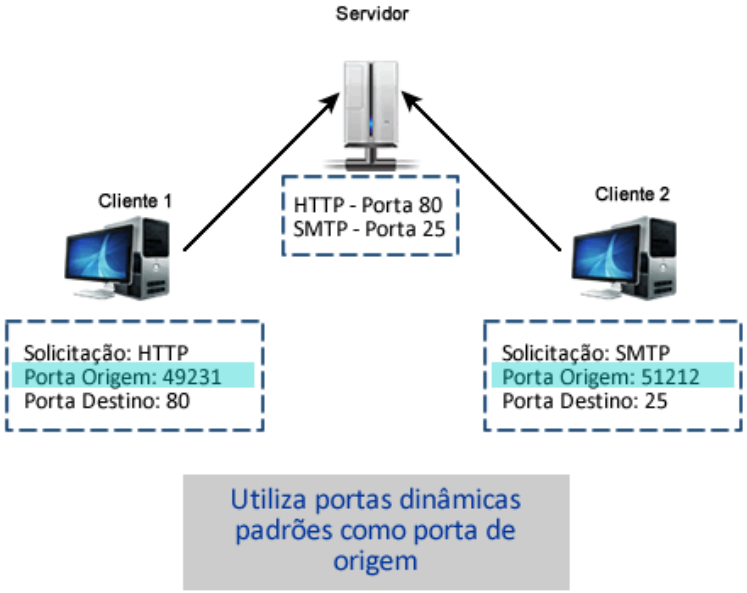
Qualquer solicitação de cliente que chega endereçada a essa porta é aceita e os dados são transmitidos à aplicação do servidor.

Pode haver muitas portas simultâneas abertas em um servidor, uma para cada aplicação de servidor ativa, pois é comum para um servidor fornecer mais de um serviço, como serviço web e servidor FTP ao mesmo tempo no mesmo servidor.

Esse modelo de acesso a serviços de rede é chamado arquitetura cliente/servidor, pois temos os computadores clientes que precisam acessar informações que são disponibilizadas pelos servidores de rede.

Veja nas figuras a seguir um exemplo de comunicação cliente/servidor através do TCP.

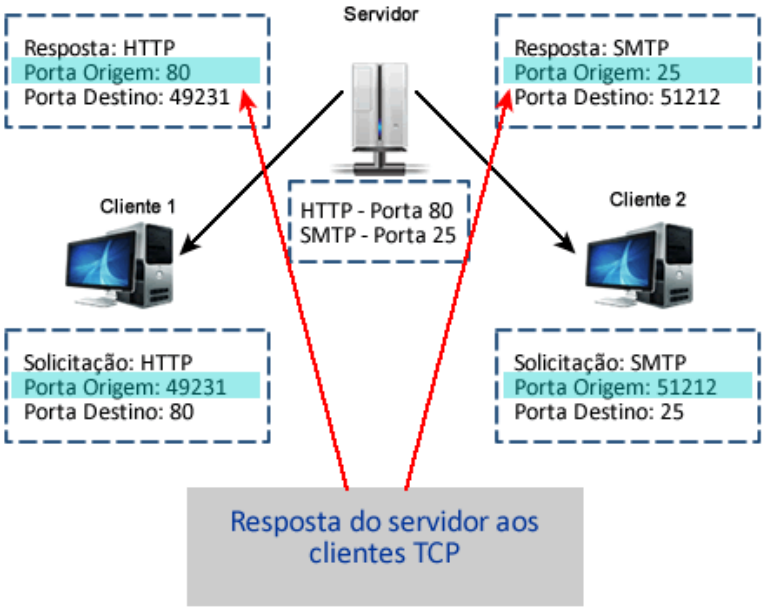
Nesse exemplo o computador chamado cliente 1 deseja acessar uma página de Web e o cliente 2 enviar um e-mail. Na primeira figura temos os clientes enviando a solicitação ao servidor utilizando como porta de origem os números 49231 e 51212 respectivamente.



A porta de destino do cliente 1 é a 80, pois ele deseja acessar o serviço de HTTP, já do cliente 2 é 25, pois ele deseja enviar um email através do SMTP. Veja a figura a seguir com as portas destacadas.

O servidor recebe as solicitações, verifica se existe serviço ativo nessas portas e passa as informações recebidas para a camada de aplicação, a qual passa para os aplicativos que cuidam de cada um dos recursos solicitados.

Após os aplicativos tratarem as solicitações, o servidor responde aos clientes utilizando a porta do serviço solicitado como origem e destino a porta que o cliente enviou como origem na sua solicitação.



Essa troca de informações será feita até que a requisição esteja completa ou um problema de rede ocorra e interrompa o tráfego.

A mesma analogia pode ser feita para o protocolo UDP, o qual também funciona no modelo Cliente/Servidor, porém suas portas não têm os estados das portas TCP, pois o UDP não é orientado a conexão.

Por isso mesmo uma porta de um serviço em UDP está escutando/aberta (listening) ou não. Alguns sistemas operacionais não mostrarão o estado "Listen" ou "Listening" para o UDP, apenas mostrarão que ele está ativo na saída do comando de verificação.

Comandos para verificar portas abertas em computadores e servidores:

- Windows: netstat –a
- Linux: netstat –tulpn
- MAC-OS: lsof -i | grep LISTEN

Os comandos acima são sugestões, pois existem normalmente mais opções para se fazer esse tipo de verificação, por exemplo, utilizando um programa externo de varredura de portas como o NMAP.

Mas lembre-se, nem tudo é ameaça, pois existem diversos programas e recursos dos sistemas operacionais que utilizam internamente comunicações TCP e UDP, portanto ao utilizar esses comandos acima não se assuste!

5.2 Estabelecendo uma Conexão TCP

O TCP é classificado como um protocolo orientado a conexão, mas o que significa isso?

Para que dois hosts se comuniquem utilizando o TCP é necessário que seja estabelecida uma conexão antes que os dados possam ser trocados.

Depois da comunicação ter sido completada, as sessões devem ser fechadas e a conexão é encerrada.

É esse mecanismo de conexão e sessão que fornecem a característica de confiabilidade ao TCP.

Dentro do cabeçalho de segmento TCP, existem seis campos de 1 bit que contêm a informação de controle usada para gerenciar os processos TCP. Esses campos são:

- URG - Indicador urgente de campo significativo
- **ACK** - Campo significativo de confirmação
- PSH - função Push
- RST - Restabelecer a conexão
- **SYN** - Sincronizar números de sequência
- FIN - Não há mais dados do remetente

Estes campos são referidos como flags (flags), porque o valor de um desses campos é apenas 1 bit e, portanto, tem apenas dois valores: 1 ou 0, sendo que quando o valor de bit é definido como 1, ele indica que a informação de controle está contida no segmento.

Cada conexão representa dois fluxos de comunicação, ou sessões e para estabelecer uma conexão, os hosts realizam um handshake triplo (negociação em três vias).

Bits de controle no cabeçalho TCP indicam o progresso e o status da conexão. Abaixo as funções do handshake triplo:

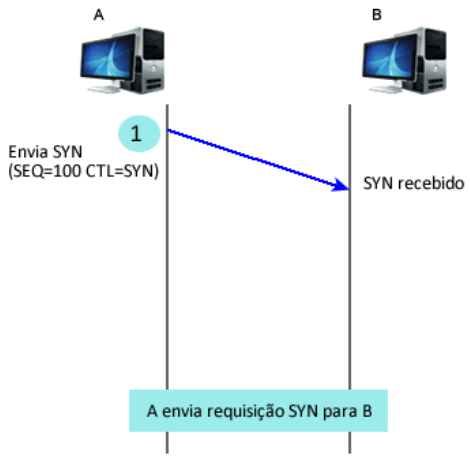
- Confirma que o dispositivo de destino esteja presente na rede.
- Verifica se o dispositivo de destino tem um serviço ativo e está aceitando solicitações no número de porta de destino que o cliente pretende usar para a sessão.

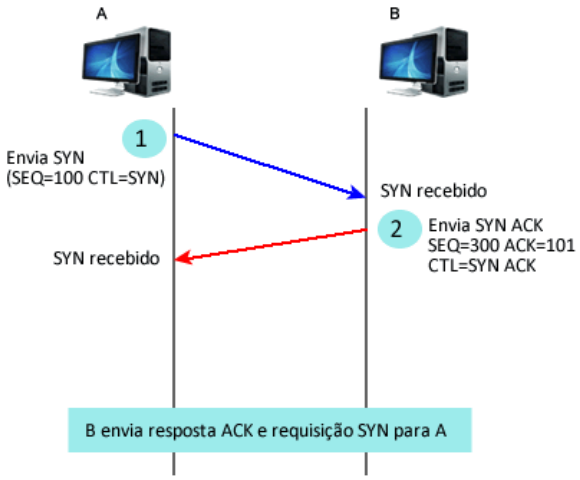
- Informa o dispositivo de destino que o cliente de origem pretende estabelecer uma sessão de comunicação nesse número de porta.

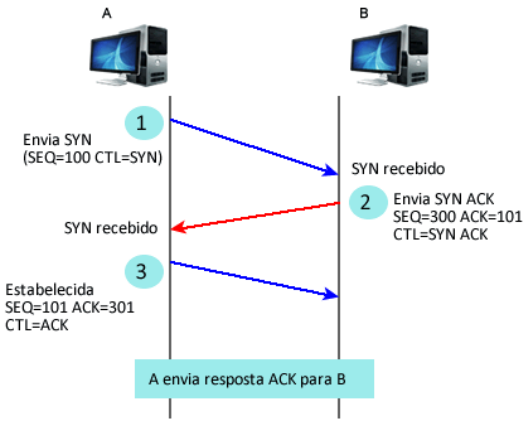
Em todas as conexões TCP, o host que serve como um cliente é quem inicia a sessão para o servidor. Os três passos no estabelecimento de uma conexão TCP são:

1. O cliente envia um segmento contendo um valor sequencial inicial (ISN – Initial Sequence Number) com o flag SYN ativo. Esse segmento serve como uma solicitação ao servidor para começar uma sessão.
2. O servidor responde com um segmento contendo um valor de confirmação igual ao valor sequencial recebido mais 1, mais seu próprio valor sequencial de sincronização (flag SYN e ACK ativos). O valor é maior do que o número sequencial porque o ACK é sempre o próximo Byte ou Octeto esperado.
3. O cliente responde com um valor de confirmação igual ao valor sequencial que ele recebeu mais um. Isso completa o processo de estabelecimento da conexão.

Veja as figuras abaixo com a ilustração da abertura da conexão com handshake de três vias.







5.3 Confirmação de Recebimento de Segmentos TCP

Outro campo importante no cabeçalho TCP é o "**número de confirmação**".

O número de sequência definido durante a abertura da conexão TCP e o número de confirmação são utilizados para confirmar o recebimento dos bytes de dados contidos nos segmentos.

O número de sequência é o número relativo de bytes que foram transmitidos na sessão com iniciado pelo ISN definido no início da conexão, já o número de confirmação é o valor recebido mais 1.

O TCP usa o número de confirmação em segmentos enviados de volta à origem para indicar o próximo byte que o receptor espera receber nessa sessão.

Isto é chamado de confirmação esperada ou confirmação positiva.

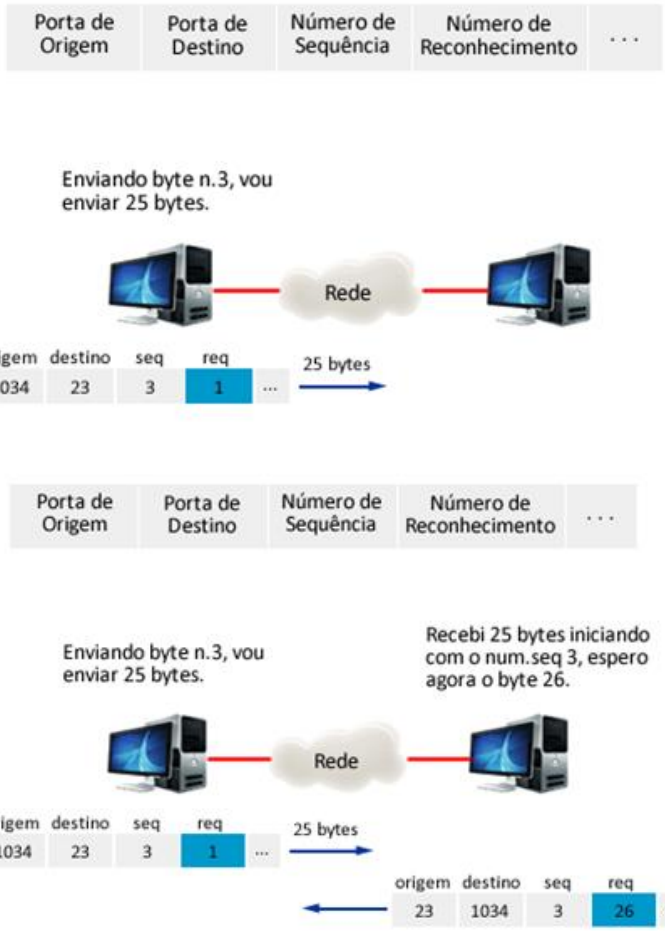
Dessa forma o TCP assegura que cada segmento atinja o seu destino.

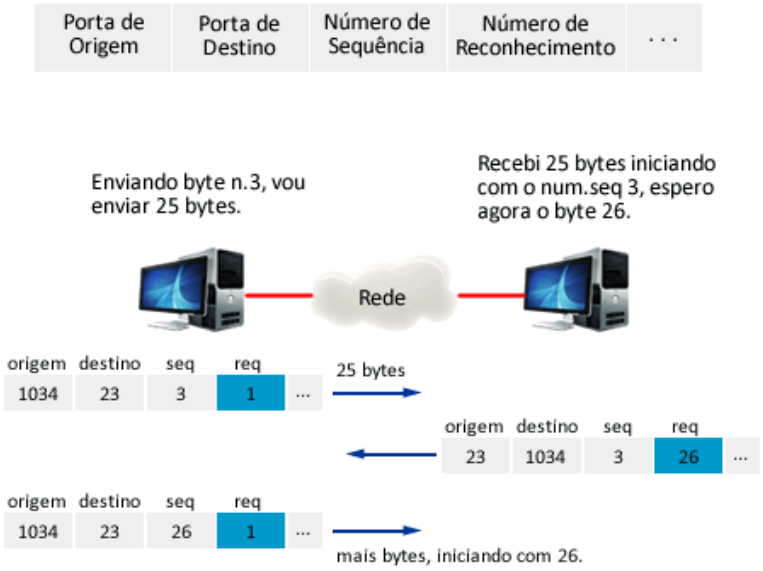
A origem é informada de que o destino recebeu todos os bytes neste fluxo de dados até, mas não incluindo, o byte indicado pelo número de confirmação.

Espera-se que o emissor envie um segmento que utilize um número de sequência que é igual ao número de confirmação.

Lembre-se, cada conexão é na verdade composta por duas sessões unidirecionais. Os números de sequência e de confirmação estão sendo trocados em ambas as direções.

Vamos exemplificar com as figuras a seguir, sendo que a explicação está contida nas próprias imagens.





Vamos supor que o host da esquerda está enviando dados para o host da direita. Ele envia um segmento contendo 25 bytes de dados para essa sessão e um número de sequência igual a 3 no cabeçalho.

O host receptor da direita recebe o segmento na Camada 4 (Camada de Transporte) e determina que o número de sequência é 3 e que ele tem 25 bytes de dados.

O host então envia um segmento de volta ao host da esquerda para confirmar o recebimento deste dado. Neste segmento, o host define o número de confirmação em 26 para indicar que o próximo byte de dados que ele espera receber nessa sessão é o byte número 26.

Quando o host emissor da esquerda recebe essa confirmação, ele pode agora enviar o próximo segmento contendo dados para essa sessão iniciando com o byte número 26.

Examinando esse exemplo, se o host de envio tiver que esperar pela confirmação de recebimento de cada 25 bytes, a rede teria muito overhead.

Para reduzir o overhead dessas confirmações, múltiplos segmentos de dados podem ser enviados e confirmados com uma única mensagem TCP na direção oposta.

Esta confirmação contém um número de confirmação baseado no número total de bytes recebidos na sessão.

Por exemplo, começando com um número de sequência de 1000, se 10 segmentos de 1000 bytes cada fossem recebidos, o número de confirmação 11001 seria retornado à origem.

##
SIN=1000
10 segmentos de 1000 bytes = 10 x 1000 = 10000
ACK=1000 + 10000 + 1 = 11001
##

A quantidade de dados que a origem pode transmitir antes que uma confirmação seja recebida é chamada de tamanho da janela. O Tamanho de Janela é um dos campos no cabeçalho TCP que habilita o gerenciamento de dados perdidos e o controle de fluxo.

5.4 Retransmissão de Segmentos TCP

Por melhor que seja o projeto de uma rede ocasionalmente ocorrerão perdas de alguns dados.

As perdas podem ocorrer por diversos motivos, por exemplo:

- Problemas Físicos (L1) e de Enlace (L2)
- Problemas no roteamento dos pacotes IP (L3)
- Congestionamento na rede ou nuvem que conecta transmissor e receptor
- Excesso de processamento no Receptor

O TCP considera que o segmento foi perdido após um tempo do não recebimento da confirmação da recepção (ACK).

Para contornar essa perda de dados, o TCP possui um mecanismo que retransmite segmentos com dados não confirmados.

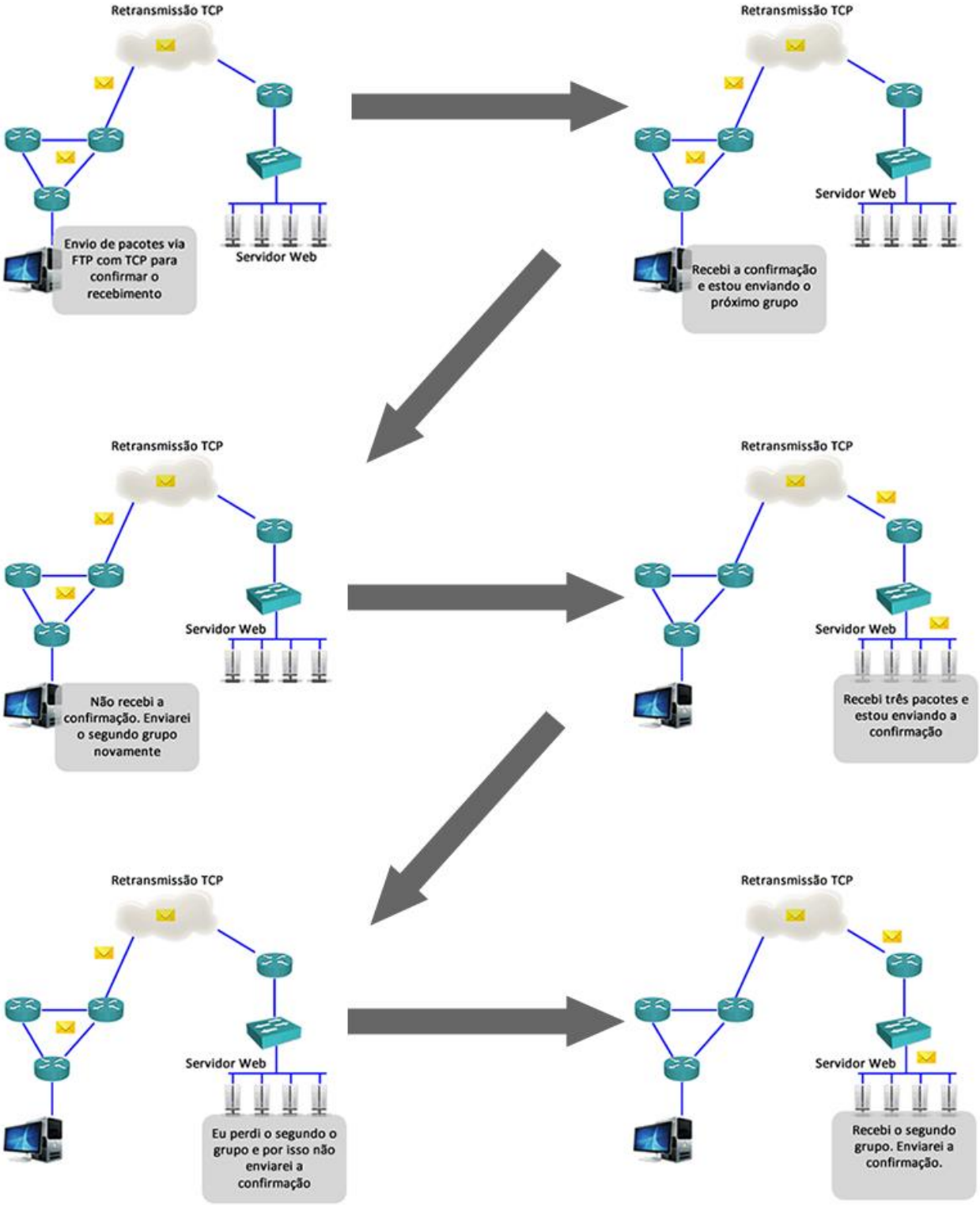
Por exemplo, se os segmentos com números de sequência de 1000 a 3000 e de 4000 a 5000 fossem recebidos, o número de confirmação seria 3001. Isto porque existem segmentos com os números de sequência de 3001 a 3999 que não foram recebidos.

Quando o TCP no host de origem percebe que não recebeu uma confirmação depois de um período pré-determinado de tempo, ele voltará ao último número de confirmação que recebeu e retransmitirá os dados a partir daquele ponto para frente.

Na prática, se você desconfiar que a sua rede está congestionada verifique o número de retransmissões solicitadas pelos equipamentos, pois se está existindo muita necessidade de retransmissão é sinal de que os pacotes não estão chegando ao seu destino e a mais provável causa é uma sobrecarga na rede ou um congestionamento.

Isso pode ser verificado colocando um "Analisador de Protocolo" como o Wireshark para fazer uma varredura dos pacotes que estão sendo trocados na rede.

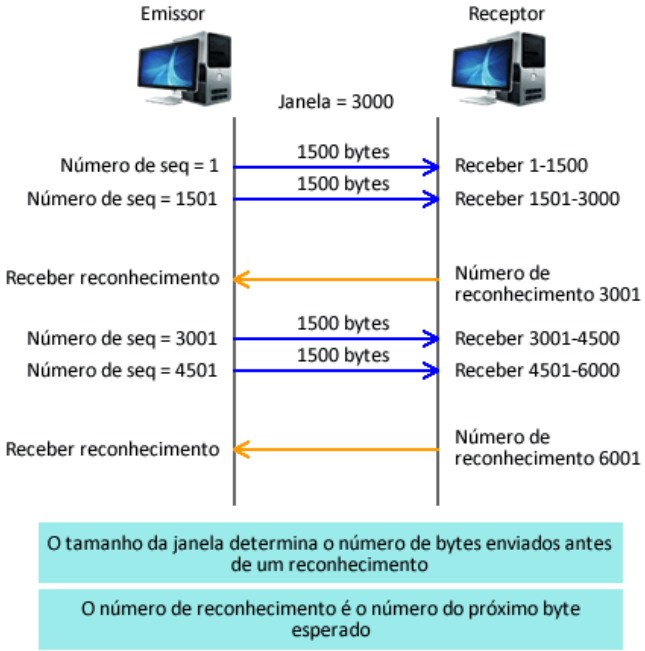
Veja as figuras a seguir com um exemplo de retransmissão.



5.5 Controle de Congestionamento TCP

O controle de congestionamento no TCP é realizado através do tamanho da janela de transmissão (window size), ou seja, através de quantos bytes foram confirmados através do número de reconhecimento.

Por exemplo, o computador que iniciou a comunicação tentou mandar uma quantidade de 1500 bytes por janela, se o receptor não conseguir tratar essa quantidade de informações ou a rede estiver lenta, a confirmação não será 1501, como deveria, e sim um número menor até ajustar o tamanho da janela, por isso esse processo é chamado de janelamento (windowing) ou janela móvel ou deslizante (sliding window).



Outra forma de controle de congestionamento é chamada "**Slow Start**", ou seja, o TCP inicia o envio de informações com poucos bytes e vai aumentando o tamanho da janela gradativamente até que seja encontrado o valor ideal. Esse processo é dinâmico e se adapta às condições da rede.

5.6 Reagrupamento de Segmentos TCP

Mais uma vez (para gravar bem) vamos reforçar que o TCP é um protocolo orientado a conexão.

No entanto, quando algum serviço utiliza o protocolo TCP para enviar dados, os segmentos de dados podem chegar fora de ordem. Mas por quê?

Porque os diversos segmentos podem percorrer caminhos diferentes para chegar no destino.

Um segmento pode ser roteado dentro da rede e percorrer um caminho que tenha uma velocidade mais rápida ou um delay menor.

No entanto, para que a mensagem original seja entendida pelo receptor, os dados desses segmentos precisam ser reagrupados ou reordenados em sua ordem original. Para isso existe no cabeçalho TCP o campo "número de sequência".

Durante a instalação de uma sessão, um número de sequência inicial (ISN) é definido.

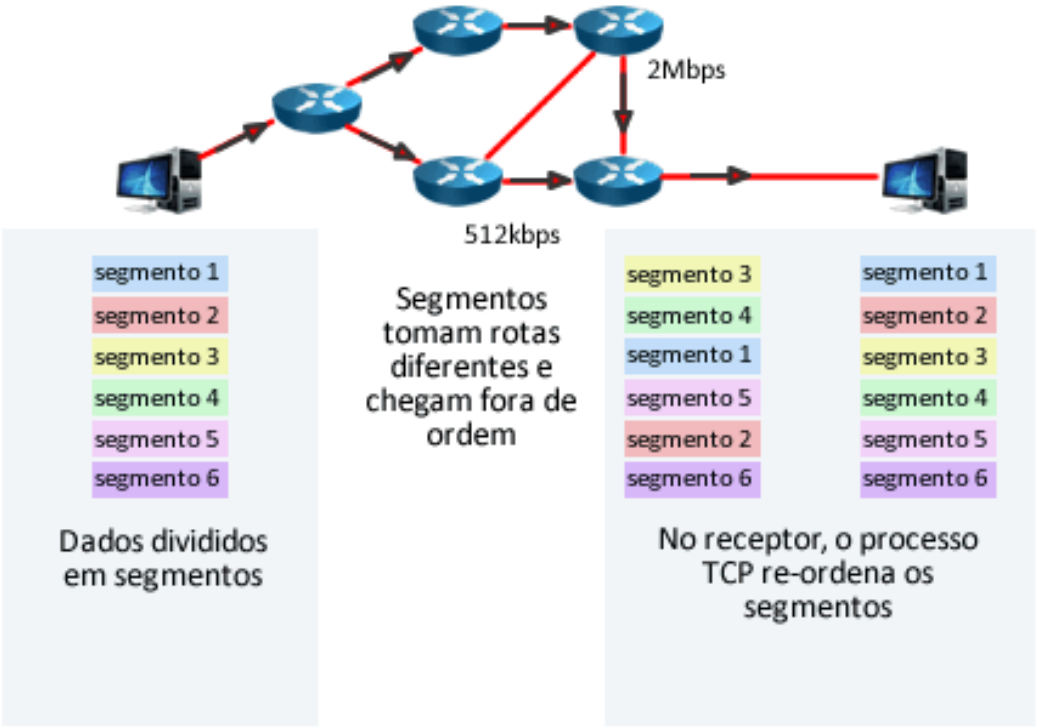
Este número de sequência inicial representa o valor de partida para os bytes para esta sessão. À medida que os dados são transmitidos durante a sessão, o número de sequência é incrementado pelo número de bytes que foram transmitidos.

Dessa forma cada segmento pode ser identificado e reconhecido, pois cada um terá um número de sequência único que seguirá uma ordem definida.

O processo TCP do receptor coloca os dados de um segmento em um buffer. Os segmentos são então colocados na ordem do número de sequência apropriada e passados para a camada de Aplicação quando reagrupados.

Quaisquer segmentos que cheguem com números de sequência não contíguos são retidos para processamento posterior. Então, quando os segmentos com os bytes perdidos chegam, esses segmentos são processados.

Esse processo de sequenciamento é que fornece a confiabilidade do TCP, pois garante que os segmentos serão entregues na ordem corretas e sem faltar nenhum pedaço.



6 Protocolo UDP

Ao contrário do TCP o protocolo UDP não é orientado a conexão, portanto não possui mecanismos sofisticados de controle de congestionamento e erros como o TCP.

O UDP tramite os datagramas de forma "best-effort" ou seja "melhor esforço", ficando a cargo das aplicações tratarem dos erros e controle da transmissão.

O único campo de controle do UDP é o Checksum para verificar a integridade do datagrama recebido. Veja na figura a seguir o datagrama do UDP.

Sobre a comunicação através de portas o funcionamento do UDP é similar ao TCP, tendo portas específicas para determinados serviços.

A grande diferença é que não existe conexão, elas sempre estão preparadas para receber dados de um host remoto que deseja se comunicar.

Pelo fato do UDP ser mais simples, ele acaba se tornando mais rápido e preferido para aplicações onde a velocidade é fundamental, como a voz sobre o protocolo IP ou VoIP.

O protocolo RTP (Real Time Protocol) utiliza o serviço UDP para transmitir a voz entre aparelhos IP.

Outro exemplo de aplicação são as VPN's ou redes virtuais privadas, elas também normalmente utilizam serviço UDP para transmissão dos seus dados criptografados, pois os pacotes acabam sendo enviados mais rápidos e com menos cabeçalho, pois o UDP tem bem menos bits de controle que o TCP.

As portas do UDP não tem estado, pois elas estão sempre prontas para receber dados.

bit 0	bit 15 bit 16	bit 31
porta de origem (16)	porta de destino (16)	
comprimento (16)	checksum (16)	
Dados (caso existam)		

- **Porta de origem**: Número da porta chamadora.
- **Porta de destino**: Número da porta chamada.
- **Comprimento**: Número de bytes que inclui cabeçalho e dados.
- **Checksum**: Cálculo de verificação (checksum) feito através de campos do cabeçalho e dados.
- **Dados**: Dados de protocolo de camada superior.

7 Portas TCP e UDP

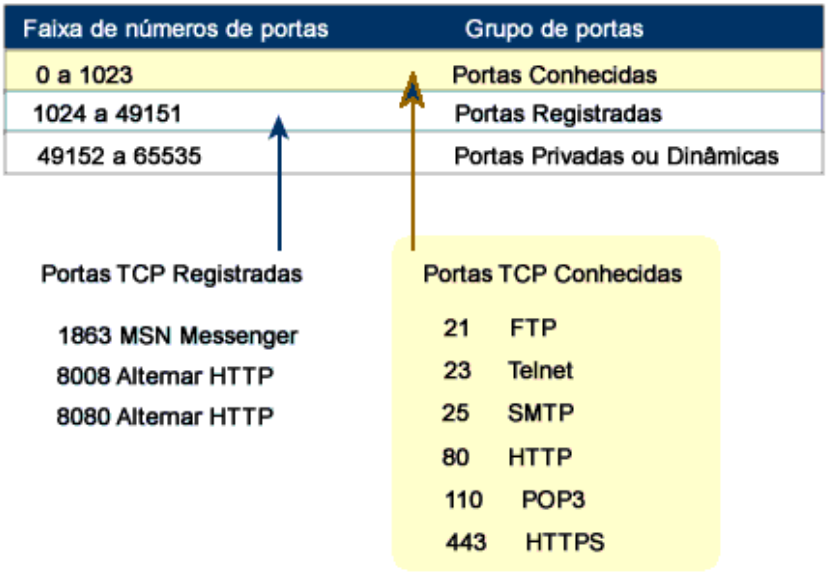
A IANA (Internet Assigned Numbers Authority) é o órgão não governamental responsável pela designação de vários padrões de endereçamento internacionalmente, dentre eles os números de portas. Veja na figura a seguir uma classificação geral dos números de porta alocados pela IANA.

Faixa de números de portas	Grupo de portas
0 a 1023	Portas conhecidas
1024 a 49151	Portas Registradas
49152 a 65535	Portas Privadas ou Dinâmicas

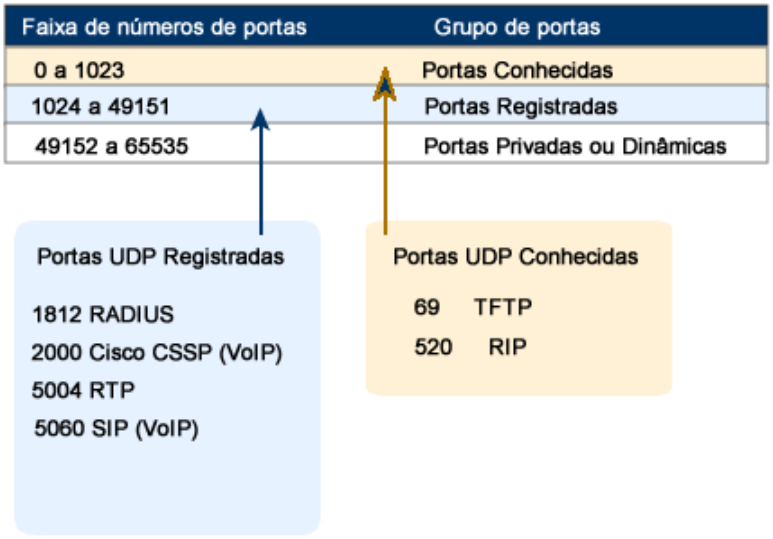
Portanto existem três diferentes tipos de números de portas:

- **Portas Conhecidas (Números 0 a 1023)** - Esses números de portas estão reservados para serviços e aplicações. Eles são comumente usados para aplicações como o HTTP (servidor web) POP3/SMTP (servidor de e-mail) e Telnet. Através da definição destas portas conhecidas para aplicações de servidor, aplicações de clientes podem ser programadas para solicitar uma conexão com essa porta específica e seu serviço associado. São também chamadas como **Well Known Ports**.
- **Portas Registradas (Números 1024 a 49151)** - Estes números de portas são designados para processos ou aplicações de usuário. Estes processos são principalmente aplicações individuais que um usuário escolheu para instalar em vez de aplicações comuns que receberiam uma Porta Conhecida. Quando não usadas para um recurso de servidor, estas portas também podem ser dinamicamente selecionadas por um cliente como sua porta de origem.
- **Portas Dinâmicas ou Privadas (Números 49152 a 65535)** - Elas são geralmente designadas dinamicamente a aplicações de cliente quando se inicia uma conexão. Não é muito comum um cliente se conectar a um serviço usando uma Porta Dinâmica ou Privada, embora alguns programas de compartilhamento de arquivos peer-to-peer o façam.

Exemplo de números portas TCP:



Exemplos de portas UDP:



Abaixo segue uma lista de portas e serviços interessantes de serem gravados:

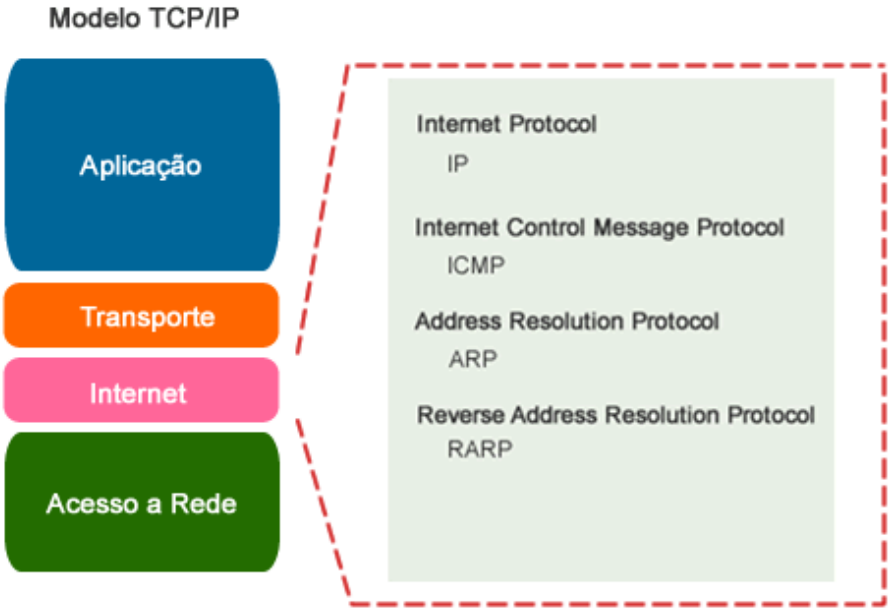
- **Serviço de tradução de nomes de Internet**: DNS (TCP/UDP 53)
- **Fornecimento de endereços IPs dinâmicos**: DHCP (UDP 67/68) e DHCPv6 (UDP 546 e 547)
- **Sincronização dos relógios dos dispositivos de Rede**: NTP (UDP 123)
- **Serviços de web**: HTTP (TCP 80) e HTTPS (TCP 443)
- **Serviços de e-mail**: SMTP (TCP 25), POP3 (TCP 110) e IMAP (TCP 143)
- **Troca de arquivos em rede**: FTP (TCP 20/21), SFTP (TCP 22) e TFTP (UDP 69)
- **Serviços de terminal e acesso remoto**: RDP (TCP 3389) Telnet (TCP 23), SSH (TCP 22) e VNC (TCP 5800/5900)
- **Gerenciamento de redes**: SNMP (UDP 161) e SYSLOG (TCP/UDP 514)
- **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)

8 Camada de Internet

A finalidade da Camada de Internet (Internet Layer) é a mesma que a camada de rede do modelo OSI, ou seja, fornecer esquema de endereçamento e escolher o melhor caminho para os pacotes viajarem através da rede.

A determinação do melhor caminho e a comutação de pacotes também ocorre nesta camada.

Veja os principais protocolos da camada de Internet na figura a seguir.



Abaixo seguem as principais funções de cada um dos protocolos:

- O **IP** oferece roteamento de pacotes sem conexão, e uma entrega de melhor esforço. Ele não se preocupa com o conteúdo dos pacotes, apenas procura um caminho até o destino.
- O **ICMP** (Internet Control Message Protocol – Protocolo de Mensagens de Controle da Internet) oferece recursos de controle e de mensagens, tais como ping.
- O **ARP** (Address Resolution Protocol – Protocolo de Resolução de Endereços) determina o endereço da camada de enlace (endereço MAC) para os endereços IP conhecidos.
- O **RARP** (Reverse Address Resolution Protocol – Protocolo de Resolução Reversa de Endereços) determina os endereços IP quando o endereço MAC é conhecido.
- **Protocolos de roteamento** são responsáveis por ler o endereçamento IP configurado e trocar informações de rota para definir o melhor caminho entre as diversas redes da Internetwork. Exemplos de protocolos de roteamento são:
    - RIP versões 1 e 2 (RIPv1 e RIPv2 - Routing Information Protocol – IPv4)
    - OSPF (chamado de OSPFv2 para IPv4 - Open Shortest Path First)
    - IS-IS (Intermediate System to Intermediate System – IPv4 e IPv6)
    - EIGRP (Enhanced Interior Gateway Routing Protocol – IPv4)
    - RIPng (Routing Information Protocol next generation –IPv6)
    - OSPFv3 (OSPF versão 3 para redes IPv6)
    - EIGRPv6 (IPv6)
    - BGP-4 (Border Gateway Protocol - IPv6 e IPv4)

O protocolo IP atualmente possui duas versões: **IPv4 (32 bits)** e **IPv6 (128 bits)**, ou seja, a IP versão 4 e IP versão 6.

Atualmente a maioria das redes utiliza o IPv4, porém a implementação do IPv6 vem crescendo vertiginosamente a partir do lançamento global realizado em 2012.

Ambas as versões do protocolo IP são "**best effort**", ou seja, enviam suas informações na rede como o UDP estudado anteriormente, sem pedir confirmações.

8.1 Introdução ao Protocolo IP versão 4 ou IPv4

Abaixo segue o cabeçalho do protocolo IP versão 4 e logo abaixo a descrição dos campos.

+	0 - 3	4 - 7	8 - 15	16 - 18	19 - 31
0	Versão	Tamanho do cabeçalho	*Tipo de Serviço* (ToS) (agora DiffServ e ECN)	Comprimento (pacote)	
32	Identificador			*Flags*	*Offset*
64	*Tempo de Vida* (TTL)		Protocolo	*Checksum*	
96	Endereço origem				
128	Endereço destino				
160	Opções				
192	*Dados*				

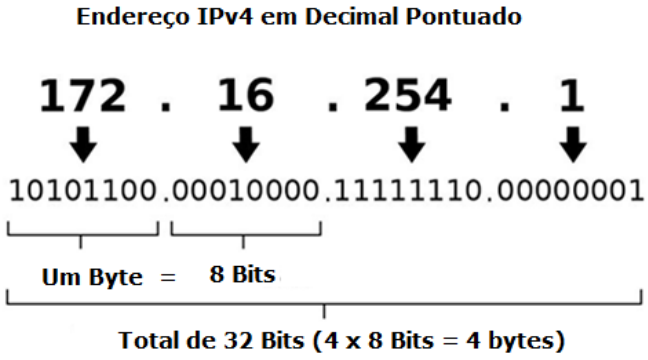
- **Versão (version)**: Definido como 4.
- **IHL (header length)**: Comprimento do Cabeçalho da Internet com o número de palavras de 32 bits no cabeçalho IPv4.
- **Tipo de serviço**: Definido na RFC 791 e define o tipo de serviço (ToS – Type of Service), agora DiffServ e ECN utilizados para definir marcação de QoS.
- **Tamanho total (total length)**: Define todo o tamanho do datagrama incluindo cabeçalho e dados. O tamanho mínimo do datagrama ou pacote IP é de vinte bytes e o máximo é 64 Kbytes, porém o MTU mínimo que os hosts precisam suportar é de 576 bytes. Se os pacotes ultrapassarem o MTU precisam ser "fragmentados", ou seja, quebrados em pedaços menores para caberem dentro do tamanho máximo do protocolo do caminho. No IPv4 a fragmentação pode ser feita pelos computadores ou diretamente nos roteadores.

- **Identificador (identifier)**: Usado principalmente para identificar fragmentos do pacote IP original.
- **Flags**: Usado para controlar ou identificar fragmentos.
- **Offset do fragmento**: permite que um receptor determine o local de um fragmento em particular no datagrama IP original.
- **Tempo de vida**: Chamado de TTL (time to live) ajuda a prevenir que os pacotes IP entrem em loop na rede. Utilizado para o teste de traceroute.
- **Protocolo (protocol)**: Define o protocolo que será transportado no pacote, sendo que os protocolos comuns e os seus valores decimais incluem o ICMP (1) e o TCP (6).
- **Checksum**: Campo de verificação de erros para o cabeçalho do datagrama IPv4. Cobre apenas verificação do cabeçalho, não dos dados.
- **Endereço de origem (source)/destino (destination)**: Campos que trazem os endereços de origem (transmissor) e de destino (receptor) de 32 bits cada um. Os endereços IP têm seus campos divididos em 4 conjuntos de 8 bits, ou seja, 4 bytes escritos em decimal pontuado, por exemplo, 192.168.1.1.
- **Opções (options)**: Normalmente não utilizados.
- **Dados (data ou payload)**: Informações das camadas superiores, por exemplo, segmentos TCP ou datagramas UDP.

Sem dúvida alguma os campos de endereçamento de origem e destino são os mais importantes do cabeçalho IP, pois eles que fornecem o endereçamento lógico utilizado para transporte do pacote através da rede.

Lembre-se que o quadro de camada-2 é trocado durante a viagem do IP pela rede conforme o protocolo utilizado pelo link local, já o pacote IP é aberto somente pelo destino da transmissão.

Abaixo segue como um endereço IP é escrito em decimal pontuado e depois em bits.



Com 32 bits temos um total de 2^32 bits ou 4.294.967.296 de possíveis endereços IP. Portanto, o primeiro endereço IP versão 4 possível tem todos os bits em zero e o último todos os bits em 1:

- 1º endereço IP: 00000000.00000000.00000000.00000000 -> 0.0.0.0
- Último endereço IP: 11111111.11111111.11111111.11111111 -> 255.255.255.255

A faixa de variação dos endereços entre o primeiro 0.0.0.0 e o último 255.255.255.255 corresponde a todo espaço de endereçamento IPv4 disponível.

Essa faixa foi dividida no início em classes (A, B, C, D e E) para possibilitar a divisão dos endereços entre instituições e empresas para possibilitar o endereçamento dos computadores na Internet. As classes A, B e C são as faixas de endereços utilizadas para endereçar hosts e navegar nas Intranets e Internet. Nessas classes temos endereços de Unicast e Broadcast.

A classe D é reservada para a comunicação em Multicast, sendo que a classe E é reservada.

Atualmente a Internet não segue mais o padrão de classes, pois ela é "Classless", ou seja, a divisão dos endereços não depende mais desse padrão de classes, seguindo um padrão chamado CIDR ou "Classless Inter-Domain Routing".

8.2 Introdução ao Protocolo IP Versão 6 ou IPv6

A maior diferença entre o IPv4 e o IPv6 com certeza é o número de endereços IP disponíveis em cada um dos protocolos.

No IPv4 temos 4,294,967,296 endereços, enquanto no IPv6 temos um total de 340,282,366,920,938,463,463,374,607,431,768,211,456 endereços IP. Note abaixo como a diferença é gritante:

IPv4: **4,294,967,296**
IPv6: **340,282,366,920,938,463,463,374,607,431,768,211,456**

Esta diferença de valores entre o IPv4 e o IPv6 representa aproximadamente **79 octilhões de vezes** a quantidade de endereços IPv6 em relação a endereços IPv4, além disso, mais de **56 octilhões de endereços** por ser humano na Terra, considerando-se a população estimada em 6 bilhões de habitantes.

Tecnicamente as funcionalidades da Internet continuarão as mesmas com a introdução do IPv6 na rede e, com certeza, ambas versões do protocolo IP deverão funcionar ao mesmo tempo, tanto nas redes já implantadas em IPv4 como em novas redes que serão montadas.

Atualmente as redes que suportam IPv6 também suportam o IPv4 e ambos os protocolos deverão ser utilizados por um bom tempo ainda.

Acompanhe na tabela onde mostramos uma comparação simples em termos somente do formato dos endereços e quantidades.

	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

Outras diferenças importantes são:

- A introdução dos endereços de anycast e a retirada dos endereços de broadcast.
- O grande vilão do IPv4, o broadcast, no IPv6 não existe mais.
- Agora no IPv6 temos endereços de unicast, multicast e anycast.
- Caso seja necessário enviar uma mensagem a todos os hosts pode-se utilizar um pacote de multicast para o endereço de link-local de destino chamado de "all nodes address" (FF02::1).

Outro ponto importante é que no IPv6 ainda temos a parte de rede, sub-rede e host, como no IPv4, mas não utilizamos mais o termo **máscara** e sim somente **prefixo**.

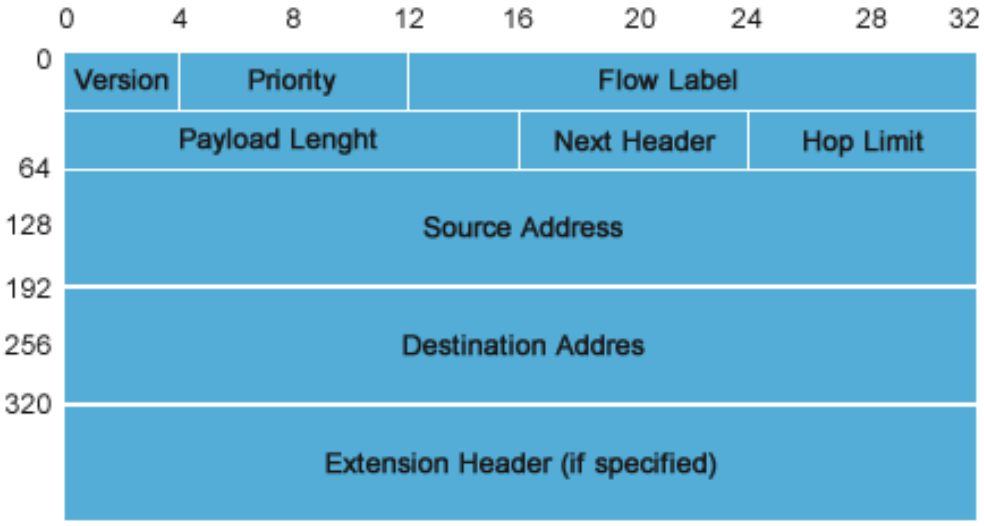
O prefixo do IPv6 tem a mesma funcionalidade do prefixo do CIDR e conta a quantidade de bits de rede ou sub-rede que a máscara tem, sendo que os bits 1 continuam indicando a porção de redes e os bits zero os hosts.

No exemplo dado na tabela anterior temos a rede 3FFE:F200:0234::/48 e o /48 representa o prefixo dessa rede, ou seja, os primeiros 48 bits do endereço são bits de rede e os demais 80 bits (128-48) são de host.

Isso mesmo, temos 80 bits para hosts nesse exemplo.

O cabeçalho do pacote IPv6 é bem mais simples que o do IPv4, contendo apenas 8 campos principais e caso serviços adicionais sejam necessários existem extensões de cabeçalho que podem ser utilizadas.

O cabeçalho (header) básico está na figura a seguir.



A descrição de cada campo segue abaixo:

- **Version (versão - 4 bits)**: Contém o valor para versão 6.
- **Priority ou Traffic Class (classe de tráfego - 8 bits):** Um valor de DSCP para QoS (qualidade de serviços).
- **Flow Label (identificador de fluxo - 20 bits)**: Campo opcional que identifica fluxos individuais. Idealmente esse campo é configurado pelo endereço de destino para separar os fluxos de cada uma das aplicações e os nós intermediários de rede podem utilizá-lo de forma agregada com os endereços de origem e destino para realização de tratamento específico dos pacotes.
- **Payload Length (tamanho do payload - 16 bits)**: Tamanho do payload em bytes.
- **Next Header (próximo cabeçalho - 8 bits)**: Cabeçalho ou protocolo que virá a seguir. É utilizado para identificar que existem cabeçalhos de extensão após o principal.
- **Hop Limit (limite de saltos - 8 bits)**: Similar ao tempo de vida de um pacote IPv4 (TTL - time to live) utilizado no teste de traceroute.
- **Source Address (endereço IPv6 de origem - 128 bits)**: Endereço IP de quem está enviando os pacotes.
- **Destination Address (endereço IPv6 de destino - 128 bits)**: Endereço IP do host remoto que deve receber os pacotes.

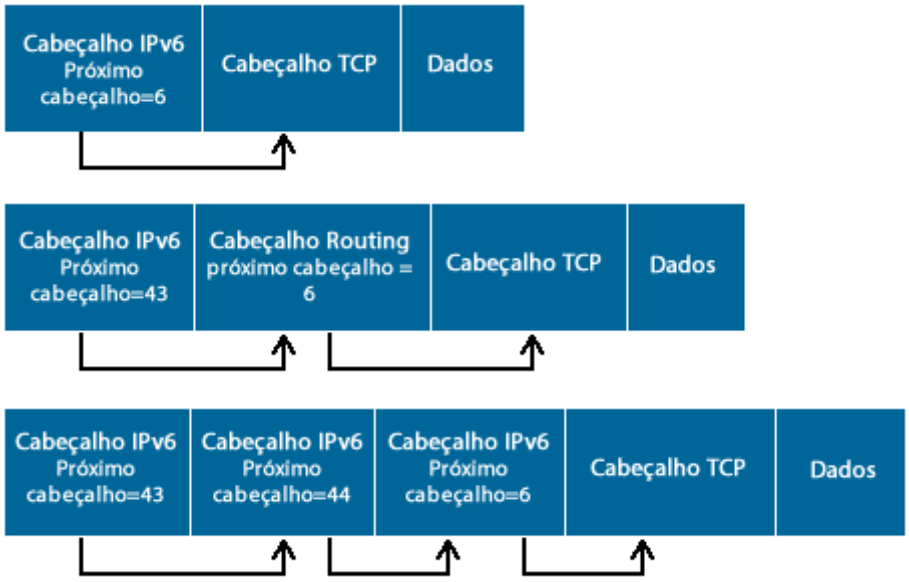
Aqui vem mais uma diferença do IPv6, pois no IPv4 o cabeçalho base continha todas as informações principais e opcionais (mesmo que não fossem utilizadas).

Já o IPv6 trata essas informações adicionais como cabeçalhos opcionais chamados de "**cabeçalhos de extensão**".

Os cabeçalhos de extensão são inseridos entre o cabeçalho base e o cabeçalho da camada imediatamente acima (payload), não tendo nem quantidade ou tamanho fixo.

Caso existam múltiplos cabeçalhos de extensão no mesmo pacote, eles serão encadeados em série formando uma "cadeia de cabeçalhos".

A figura a seguir mostra um exemplo dessa situação.



De uma maneira resumida seguem os cabeçalhos de extensão possíveis e seus identificadores:

- **Hop-by-hop Options (0)**: Transporta informações adicionais que devem ser examinadas por todos os roteadores de caminho, por isso o nome hop-by-hop que em português significa **salto a salto**.
- **Routing (43)**: Definido para ser utilizado como parte do mecanismo de suporte a mobilidade do IPv6.
- **Fragment (44)**: Indica se o pacote foi fragmentado na origem.
- **Encapsulating Security Payload (50) e Authentication Header (51)**: fazem parte do cabeçalho IPSec, utilizados para criptografia do payload.
- **Destination Options (60)**: Transporta informações que devem ser processadas apenas pelo computador de destino.

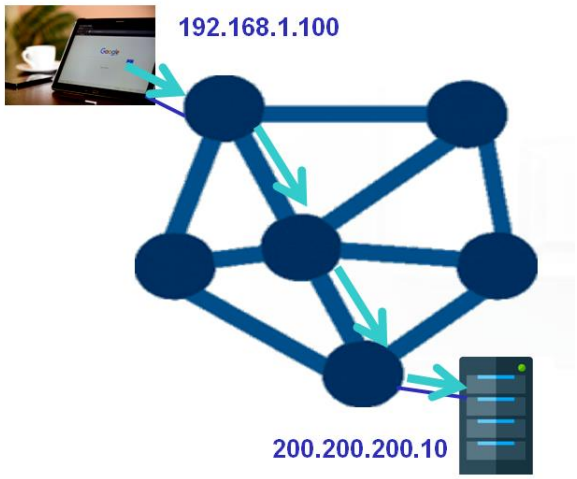
Portanto, o cabeçalho do IPv6 além de ser mais simples que o do IPv4, também trata de questões como QoS e segurança de maneira nativa, ou seja, dentro do próprio cabeçalho sem a necessidade de implementações e recursos adicionais como era necessário para o IPv4.

8.3 Introdução ao Roteamento IP

Uma das principais funções da camada de Internet no TCP/IP é de realizar o "roteamento" ou "encaminhamento" dos pacotes IP até seus destinos.

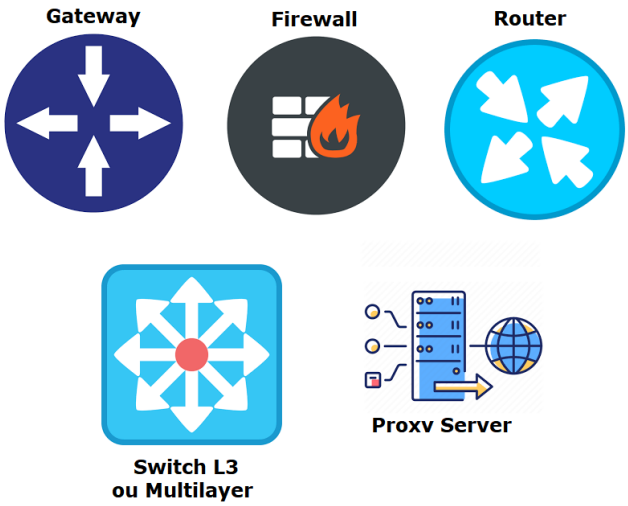
Uma rede IP é composta de várias redes, sub-redes e dispositivos que conectam essas redes.

Ler esse endereçamento todo e "traçar rotas" entre as diversas redes é papel do Roteamento IP.



Leia-se IP como IPv4 ou IPv6, pois o processo de roteamento é muito parecido entre as duas versões de protocolo de Internet.

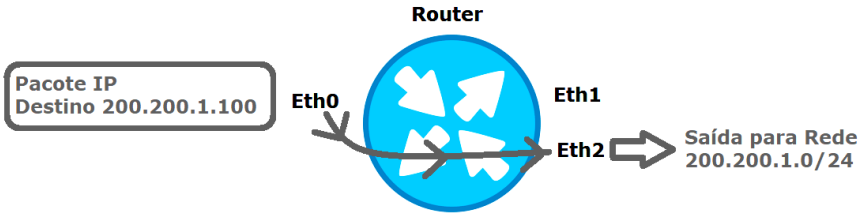
Quem executa essa missão tradicionalmente em uma rede são os Roteadores, porém switches L3, Firewalls, Servidores Proxy e outros dispositivos podem ser utilizados para essa função servindo como um Gateway de Rede.



A função de rotear ou **encaminhar pacotes** através da rede é realizada por roteadores, switches L3, Firewalls, ou seja, dispositivos que atuam como Gateways de rede.

Essa missão é cumprida através de um **protocolo de roteamento**, o qual foi projetado para alimentar a principal tabela que um roteador ou Gateway de rede mantém: a "**tabela de roteamento**" ou "**routing table**".

A tabela de roteamento guarda as informações das redes que um roteador pode alcançar, sendo que o roteador lê o endereço IP de destino, consulta sua tabela de roteamento e encaminha o pacote para a interface de saída mais apropriada.



Caso determinada rede não seja conhecida pelo roteador, ou seja, a **rota** para aquela rede não está na tabela de roteamento, ele descartará a rota e enviará uma mensagem de "unreachable" (fora de alcance) através do protocolo ICMP para o computador que estava tentando se comunicar com a rede em questão.

Portanto, sempre que entra um pacote IP em um roteador ele lê o **endereço de destino** contido no pacote e verifica se a rede a que esse pacote IP pertence está presente em sua tabela de roteamento.

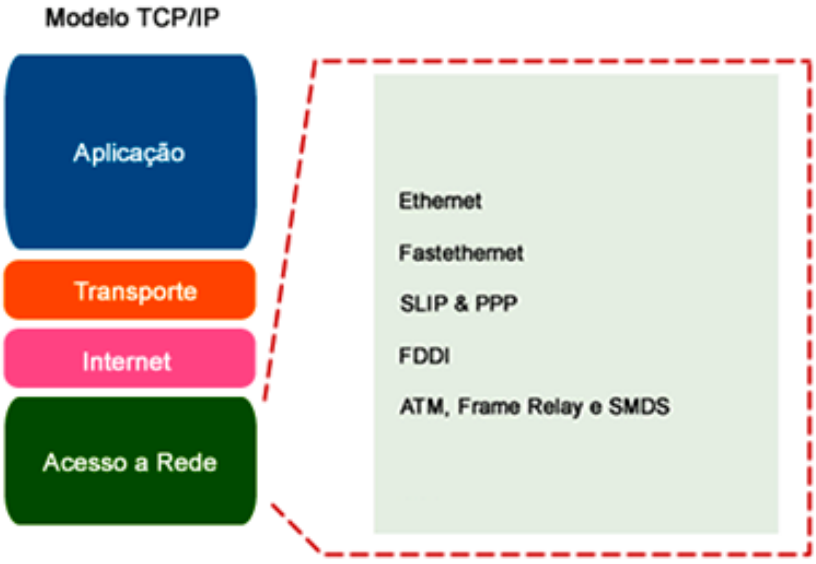
Caso não esteja, ou ele descarta o pacote ou então envia para uma rede **padrão** (**default gateway**), a qual pode ser uma rota para a internet, por exemplo.

9 Camada de Acesso aos Meios (Data Link e Camada Física)

O objetivo da camada de acesso à rede (algumas fontes bibliográficas também chamam de acesso aos meios ou Network Access Layer) é que o pacote IP estabeleça efetivamente um link físico com os meios físicos disponíveis da rede de maneira transparente, ou seja, não importando o meio de transmissão que esteja sendo utilizado.

Aqui **algumas bibliografias podem dividir de forma didática** a camada de acesso aos meios em duas camadas, assim como o modelo OSI: Enlace e Física, o que tornaria o TCP/IP com cinco camadas.

Essa camada inclui detalhes de tecnologia de redes locais e de WANs e todos os detalhes contidos na camada física e de enlace de dados do modelo OSI e suas funções incluem o mapeamento de endereços IP para endereços físicos de hardware e o encapsulamento de pacotes IP em quadros. Veja a figura a seguir.



É importante lembrar que durante a transmissão de dados em uma rede IP os cabeçalhos da camada de acesso à rede ou camada de enlace do modelo OSI variam de acordo com a tecnologia adotada, porém o cabeçalho do IP nunca irá variar do início ao fim da comunicação.

Os quadros ou frames são montados e remontados a cada salto de rede diferente que o IP navega, mas o IP nunca é alterado.

Além disso, a camada de acesso aos meios define um endereço físico que pode variar de formato e tamanho conforme protocolo específico.

Já a parte física da camada de acesso aos meios define as especificações elétricas, mecânicas, funcionais e de procedimentos para ativar, manter e desativar o link físico entre sistemas finais.

Características como tipos de cabo (UTP ou fibra óptica), níveis de voltagem, distâncias máximas de transmissão, conectores físicos são definidos pelas especificações da camada física.

A camada física tem como função básica a adaptação do sinal ao meio de transmissão.

Nessa camada estão situados os Hubs, repetidores, transcievers, patch pannel, cabos e conectores.

Os padrões de nível físico utilizados são, por exemplo, X.21, X.21 bis, V.24, V.28, V.35, RS-232 I.430, I.431, G.703, etc.

9.1 Protocolos de Camada de Enlace (Data Link)

A camada de enlace ou Data Link Layer ou apenas Link Layer no TCP/IP tem a função de fornecer acesso à rede para os protocolos da Camada de Internet, assim como fazer o encapsulamento e endereçamento dos quadros ou Frames.

Cuida também do controle de erros dos quadros que serão transportados pela camada física.

Para cada tipo de meio físico existe um tipo específico ou alguns tipos de protocolos da camada de enlace que podemos utilizar para controlar o acesso a esse meio físico.

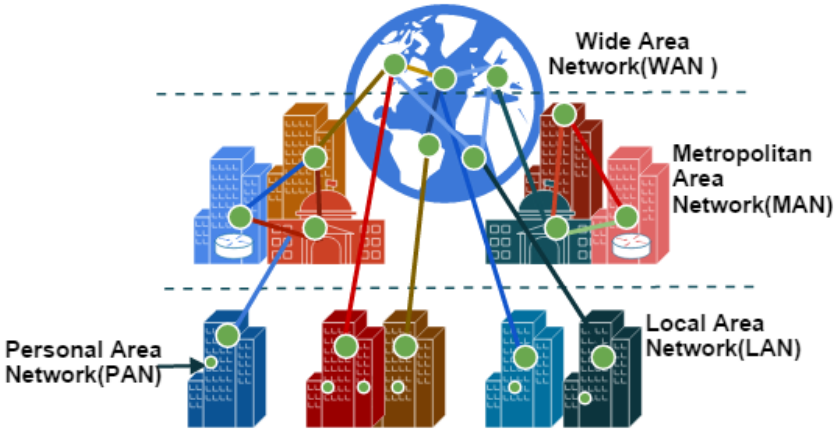
Por exemplo, o protocolo Ethernet faz o controle do acesso dos computadores a uma rede cabeada com pares metálicos ou fibras ópticas.

Já a família de protocolos 802.11 faz controle do acesso a uma rede sem fio (Wifi ou wireless LAN).

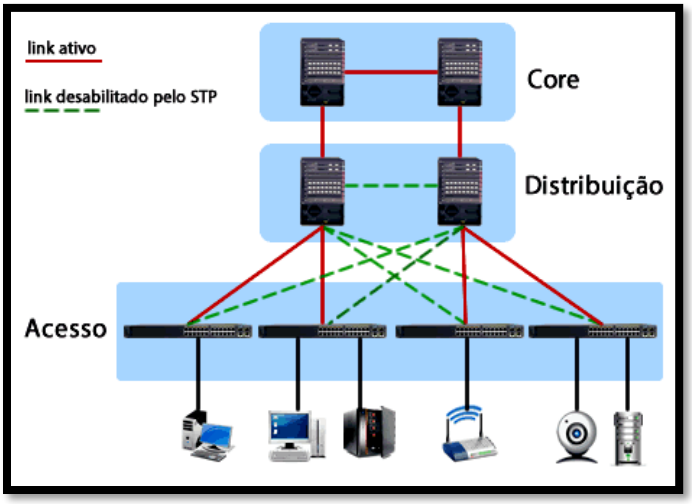
Normalmente as redes são classificadas pela sua abrangência e cada tipo de rede pode utilizar determinados meios físicos, portanto, determinadas tecnologias de enlace.

Podemos classificar as redes como:

- **Personal Area Networks (PAN)**: também designadas de redes de área pessoal, são redes que usam tecnologias de rede sem fios para interligar os mais variados dispositivos (computadores, smartphones, etc) numa área muito reduzida.
- **LAN – Local Area Network**: ou simplesmente Rede Local, é um grupo de dispositivos processadores interligados em uma rede em um mesmo ambiente.
- **MAN – Metropolitan Area Network**: é uma rede dentro de uma determinada região (normalmente dentro de uma mesma cidade) onde os dados são armazenados em uma base comum, por exemplo, uma rede de um determinado banco ou farmácia dentro de uma mesma cidade.
- **WAN – Wide Area Network**: é a rede de interligação de diversos sistemas de computadores, ou redes locais, localizados em regiões fisicamente distantes.

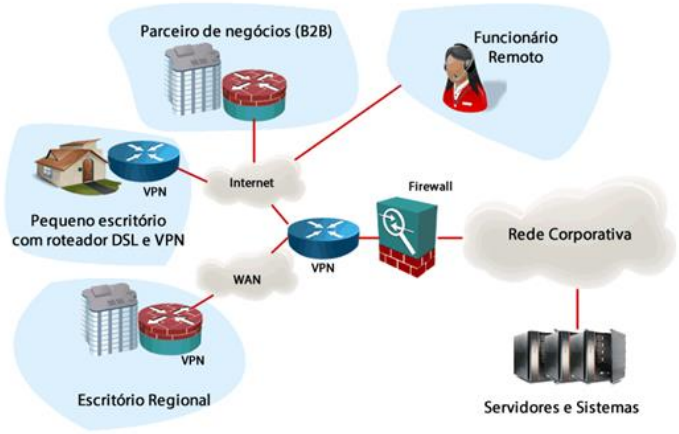


Por exemplo, em uma rede LAN temos protocolos como os da família Ethernet nas redes cabeadas e 802.11 nas redes sem fio ou Wireless LAN.

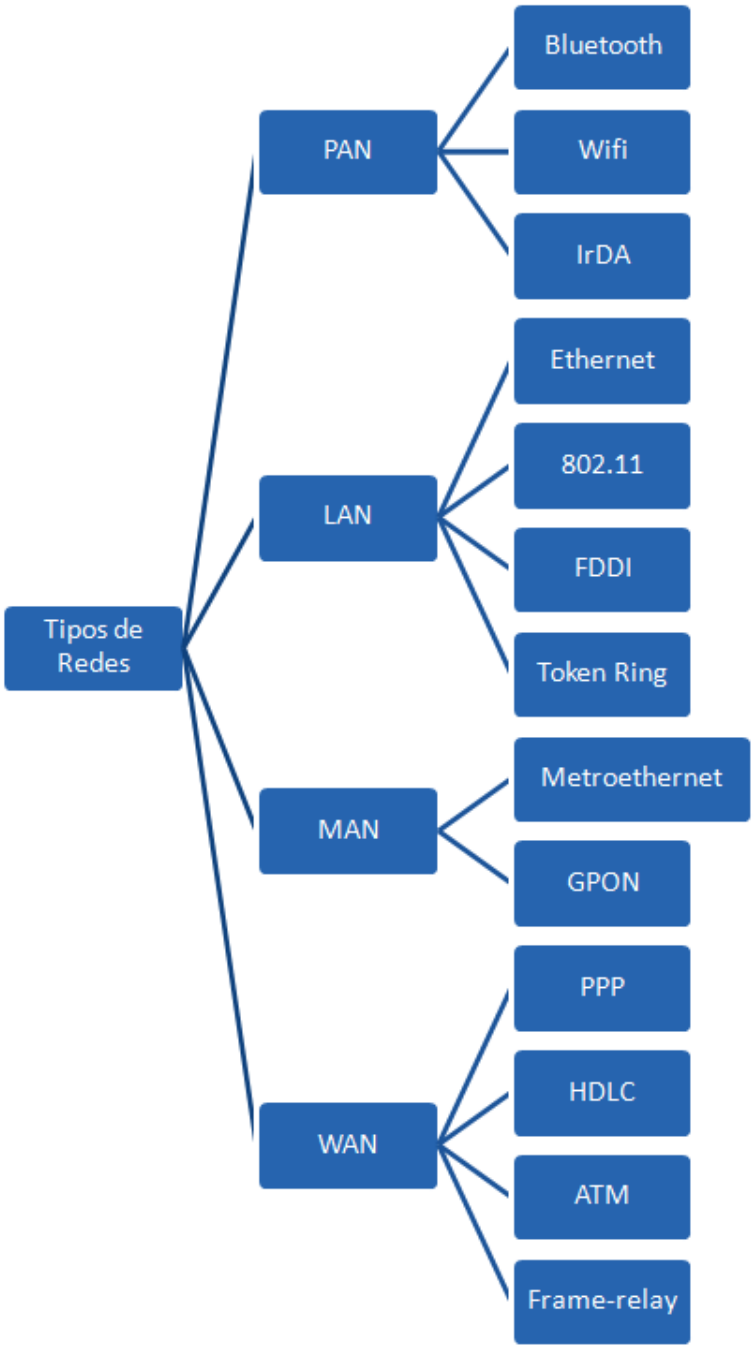


Nas redes metropolitanas ou MAN temos tecnologias como Metroethernet e GPON.

Nas WANs podemos utilizar tecnologias como PPP, HDLC e Frame-relay.



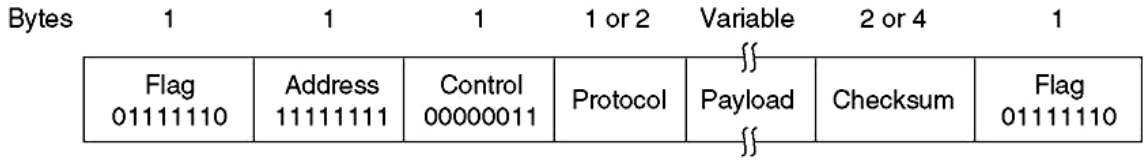
Veja imagem a seguir com um resumo dos tipos de rede por abrangência e exemplos de protocolos de acesso.



9.2 Endereços de Camada-2 e MAC Address

Os endereços de camada-2 têm a função de identificar um dispositivo dentro daquela rede local específica, ou seja, tem uma significância local.

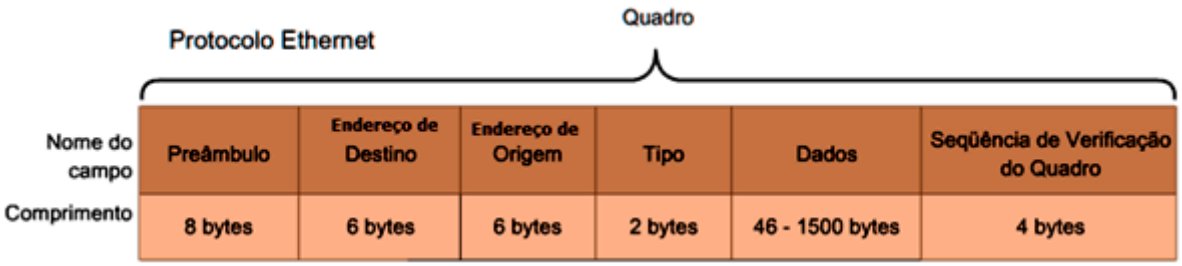
As tecnologias de LAN, MAN ou WAN possuem seus quadros específicos com diferentes tipos de endereçamento, por exemplo, uma rede WAN PPP (Point-to-Point Protocol) o endereço é sempre fixo, pois a rede é ponto a ponto e não tem necessidade de identificar o vizinho com um endereço de camada-2. Veja exemplo na imagem a seguir.



Note que o campo Address, onde temos o endereço em um quadro PPP é fixo com oito bits um (11111111), pois em uma rede ponto a ponto temos apenas dois dispositivos.

Em redes multiacesso (multi-access), ou seja, redes onde podem existir mais de dois dispositivos, há a necessidade de endereçamento.

O principal exemplo de redes multiacesso é a família Ethernet, a qual utiliza o quadro a seguir.



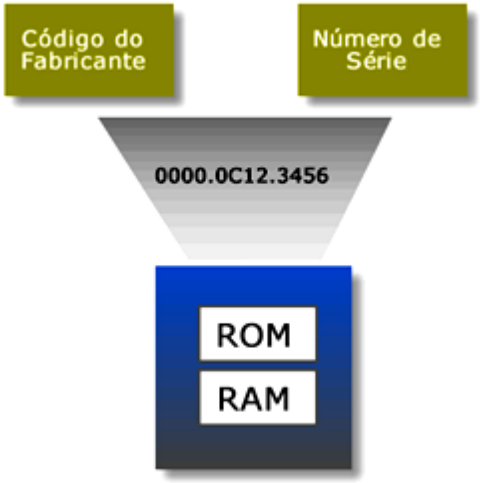
Note que no quadro Ethernet existe o endereço de origem (source address) e um endereço de destino (destination address), pois nesse tipo de rede podemos ter diversos dispositivos, portanto precisamos identificar "**quem está querendo falar com quem"**.

O nome do endereço utilizado dentro de um quadro ethernet é "**Endereço MAC**" (MAC Address ou Media Access Control Address), sendo que muitas vezes vamos nos referir apenas por **MAC**.

Esse é o mais importante dos endereços da camada de acesso aos meios e da camada de enlace do Modelo OSI, por ser utilizado nas placas de rede de computadores e servidores.

O endereço MAC (Media Access Control) é o endereço físico da estação, ou melhor, da interface de rede.

É um endereço de 48 bits, representado em hexadecimal. Este endereço é o utilizado na camada 2 (Enlace) do Modelo OSI em redes Ethernet.



Os três primeiros octetos são destinados à identificação do fabricante, os 3 posteriores são números arbitrados pelo fabricante, ou seja, um serial.

É um endereço único, ou seja, não existem, em todo o mundo, duas placas com o mesmo endereço físico, pelo menos na teoria, pois na prática são relatados casos de placas de rede "clonadas" (piratas) com seriais iguais, porém isso é uma história para quando começarmos a praticar em switches.

O endereço MAC pode ser escrito de outras formas dependendo do sistema operacional do endpoint, por exemplo, em máquinas Windows ele seria escrito da seguinte maneira:

- 00-00-0C-12-34-56

Em um computador com Linux o mesmo endereço seria visualizado como 00:00:0C:12:34:56, portanto o importante é que são 12 algarismos em Hexa, totalizando 48 bits, pois cada algarismo em Hexa possui 4 bits.

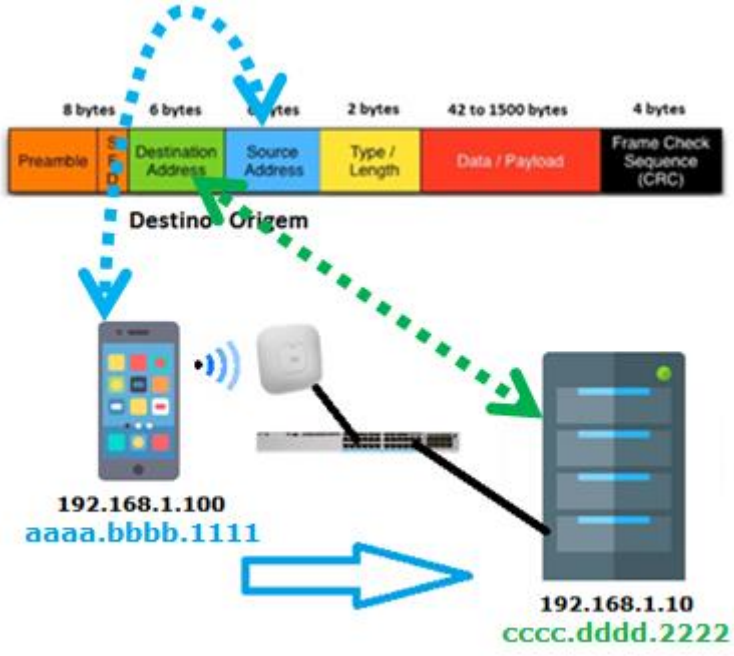
Em dispositivos Cisco ele normalmente é escrito em três conjuntos de 4 algarismos Hexadecimais, por exemplo, "afc0.dd1a.bbac".

Abaixo segue um resumo das características de um endereço MAC:

- Endereço da camada 2
- Gravado no chip da ROM em uma placa de rede Ethernet
- Número exclusivo de 48 bits que está gravado como doze números hexadecimais.
- Os primeiros 24 bits representam o fornecedor ou o fabricante (OUI)
- Os últimos 24 bits do fornecedor formam o número de série

Lembre-se que em uma rede LAN podemos ter uma comunicação entre dispositivos que estão na mesma rede ou sub-rede ou entre dispositivos que estão em redes ou sub-redes diferentes.

Por exemplo, dois computadores dentro da mesma LAN trocando arquivos compartilhados é uma comunicação dentro da mesma rede e será realizada diretamente entre eles, ou seja, os endereços MAC de origem e destino utilizados serão os MACs dos próprios dispositivos. Veja figura com um exemplo a seguir.

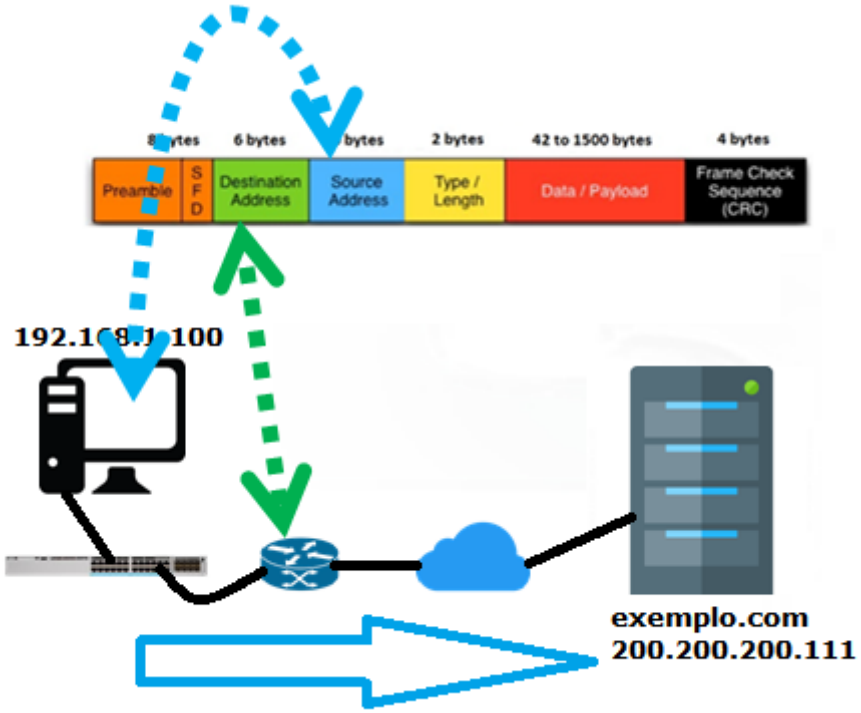


Quando dois computadores em redes diferentes ou um computador tenta acessar um servidor que está na Internet, um intermediário será necessário para o encaminhamento dos pacotes.

Esse intermediário é o gateway da rede, o qual pode ser um roteador local, por exemplo.

Nesse tipo de comunicação o MAC de origem será do computador e o de destino será o MAC do gateway e não mais o do computador ou servidor remoto.

Veja exemplo na figura a seguir onde o PC da rede local acessa o servidor da web "exemplo.com", note que o MAC de destino do quadro de camada-2 será o do roteador local e não o do servidor da web.



10 Padrões da Camada Física no TCP/IP

A camada física no TCP/IP tem função similar ao L1 do modelo OS, ou seja, ela especifica as características de hardware que serão utilizadas naquela conexão.

Por exemplo, a camada física especifica as características físicas dos meios de comunicação, descrevendo os padrões de hardware, especificações elétricas (níveis de voltagem, codificação de linha, etc.), especificações para a mídia de rede (meio físico), tipos de conectores e pinagem padrão para cada tipo de conexão física.

Podemos ter os seguintes meios físicos utilizados para comunicação em redes:

- Cabos metálicos (Cabo Coaxial e Par Trançado - UTP e STP).
- Fibra óptica (Monomodo ou Multimodo).
- Rádio Transmissão (rádios digitais ponto a ponto, Wifi, espalhamento espectral, etc.).
- Transmissão via satélite.

10.1 Cabos Metálicos de Pares Trançados (UTP e STP)

Já os pares metálicos UTP (Unshielded Twisted Pair) e STP (Shielded Twisted Pair) são utilizados em redes locais ou LANs cabeadas para conectar roteadores, switches, computadores, servidores, access points e demais dispositivos de rede entre si.

Sendo que o UTP é mais utilizado em redes internas e o STP podendo ser utilizado em ambientes com interferência eletromagnética acentuada, porém nesses casos o uso da fibra óptica é mais recomendado nos dias de hoje.

As principais vantagens de uso do cabo par trançado são taxa de transmissão, baixo custo do cabo e baixo custo de manutenção de rede. As taxas usadas nas redes com o cabo par trançado são:

- 10 Mbps (Ethernet)
- 100 Mbps (Fast Ethernet)
- 1000 Mbps (Gigabit Ethernet)
- 10.000 Mbps ou 10Gbps (10Gigabit Ethernet)

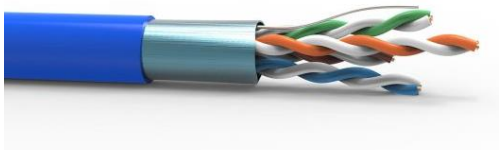
O mais utilizado na prática é o cabo não blindado denominado UTP (Unshielded Twisted Pair ou Par Trançado sem Blindagem), o qual pode ser utilizado para transmissão tanto de dados como voz.

Os cabos UTP foram padronizados pelas normas da EIA/TIA-568-B. Abaixo seguem alguns padrões de cabos UTP:

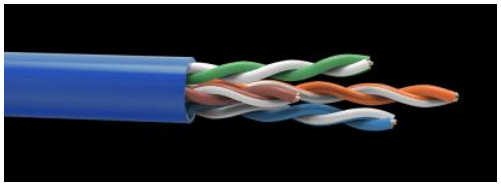
Category	Speed	Frequency
CAT 1	Carry only voice	1MHz
CAT 2	4Mbps	4MHz
CAT 3	10Mbps	16Mhz
CAT 4	16Mbps	20Mhz
CAT 5	100Mbps	100Mhz
CAT 5e	1000Mbps	100Mhz
CAT 6	1000Mbps	250MHz
CAT 7	10Gbps	600MHz
CAT 7a	10Gbps	1000Gbps
CAT 8	25Gbps	2000Mhz

A seguir temos uma breve descrição das principais categorias de cabos que você deve saber.

- **Categoria 3 (CAT3)**: É um cabo não blindado (UTP) usado para dados de até 10Mbits com a capacidade de banda de até 16 MHz. Foi muito usado nas redes Ethernet criadas nos anos noventa (10BASET).
- **Categoria 5 (CAT5)**: usado em redes fast ethernet em frequências de até 100 MHz com uma taxa de 100 Mbps. Não utilizado mais atualmente, pois foi substituído pela categoria 5e.



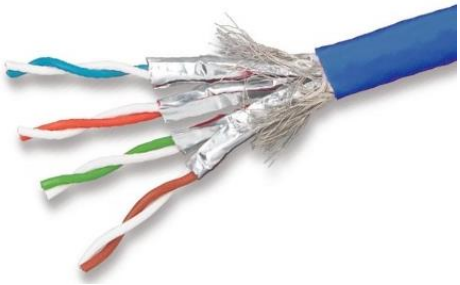
- **Categoria 5e (CAT5e)**: é uma melhoria da categoria 5. Pode ser usada para frequências até 125 MHz em redes 1000BASE-T gigabit ethernet. Ela foi criada com a nova revisão da norma EIA/TIA-568-B. Esse padrão é utilizado até os dias de hoje.



- **Categoria 6 (CAT6)**: definido pela norma ANSI EIA/TIA-568-B-2.1 possui bitola 24 AWG e banda passante de até 250 MHz e pode ser usado em redes gigabit ethernet com velocidade de 1Gbps.

- **Categoria 6a (CAT 6A)**: é uma melhoria dos cabos CAT6. O a de CAT6a significa augmented (ampliado). Os cabos dessa categoria suportam até 500 MHz e podem ter até 55 metros no caso da rede ser de 10Gbps, caso contrário podem ter até 100 metros para as velocidades de 10/100/1000 Mbps. Para que os cabos CAT 6a sofressem menos interferências os pares de fios são separados uns dos outros, o que aumentou o seu tamanho e os tornou menos flexíveis. Essa categoria de cabos tem os seus conectores específicos que ajudam evitar interferências.

- **Categoria 7 (CAT7)**: Embora o cabo Ethernet Categoria 7 suporte transmissão de 10bps a uma velocidade de 600Mhz em uma distância de 100 metros, o teste prova que ele atinge 40Gbps em um comprimento de 50m e atinge incríveis 100 Gbps em um comprimento de 15m, sendo recomendado para conexões entre dispositivos que necessitam de alta velocidade como, por exemplo, servidores em um Data Center.

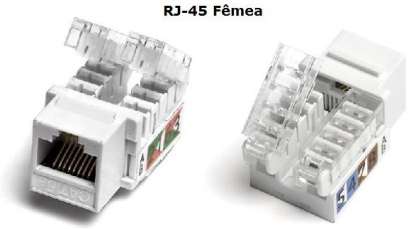


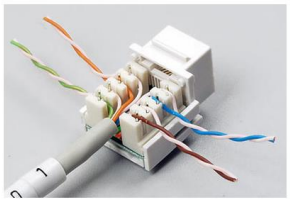
Em todas as categorias, a **distância máxima permitida é de 100 metros**.

Para a conexão dos cabos UTP são utilizados os conectores RJ-45 macho ou fêmea.

RJ-45 Macho

RJ-45 Fêmea





Os conectores machos são utilizados como terminação das conexões e os fêmeas, conhecidos como keystone jacks, são utilizados nos painéis de distribuição (de patch-panels), nas tomadas de telecomunicações (utilizadas nas mesas e paredes), placas de rede e assim por diante.

10.1.1 Montagem e Testes dos Cabos UTP

Essa montagem pode ser basicamente de dois tipos cabos, um chamado cabo direto e outro chamado cabo cruzado (cross), as quais estão baseadas nos padrões T568A e T568B.

Antes de vermos os padrões vamos conhecer as cores dos fios, que são:

- Laranja e branco
- Laranja
- Verde e branco
- Azul
- Azul e branco
- Verde
- Castanho (ou marrom) e branco
- Castanho (ou marrom)

A norma EIA/TIA-568-B prevê duas montagens para os cabos, denominadas T568A e T568B.

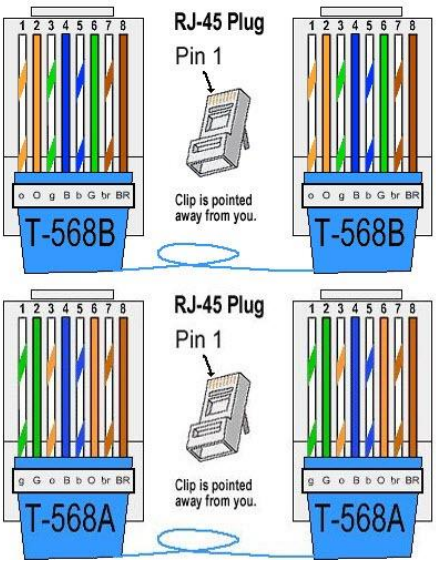
A montagem T568A usa a sequência branco e verde, verde, branco e laranja, azul, branco e azul, laranja, branco e castanho, castanho.

A montagem T568B usa a sequência branco e laranja, laranja, branco e verde, azul, branco e azul, verde, branco e castanho, castanho.

Um cabo cujas duas pontas usam a mesma montagem é denominado "Cabo Direto" (T568B-T568B), e serve para ligar estações de trabalho e roteadores a switches ou hubs.

Um cabo em que cada ponta é usada um padrão diferente (T568A-T568B) é denominado "Cabo Crossover", e serve para ligar equipamentos do mesmo tipo entre si.

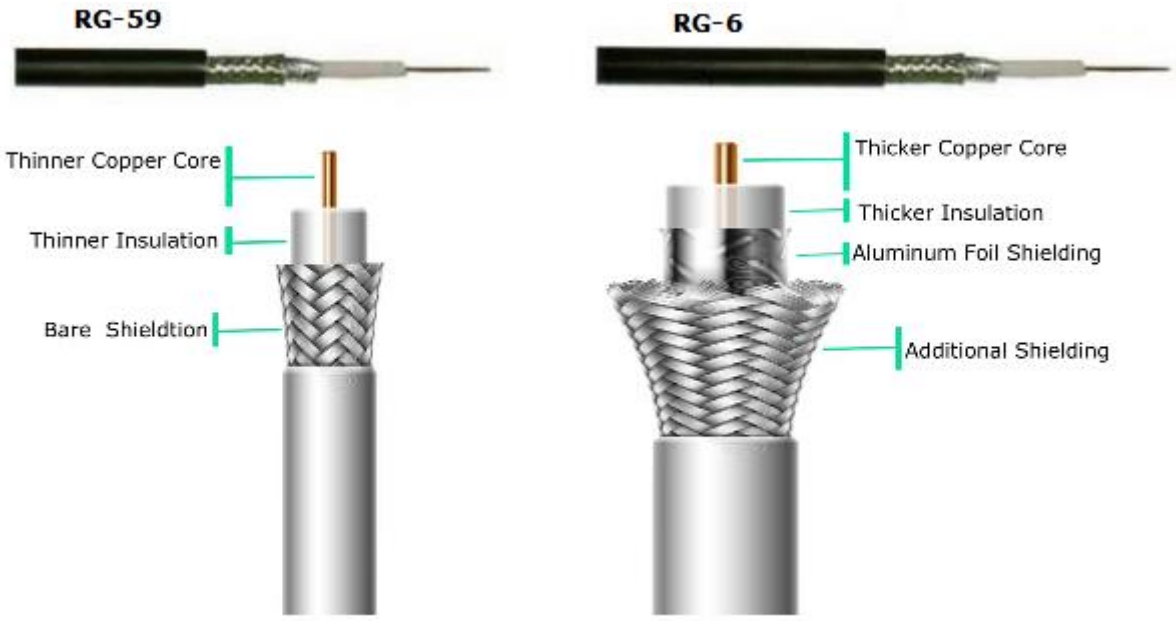
Veja na figura a seguir os padrões de montagem de cada cabo.



10.2 Cabos Coaxiais

Os principais tipos de cabos coaxiais utilizados em redes de TV a Cabo e banda larga são o RG-6 e RG-59, pois eles são os dois tipos de cabos coaxiais predominantes no uso residencial.

Veja imagem ilustrativa a seguir.



O cabo RG-6 usa um condutor central maior do que o RG-59, portanto, a atenuação de longa distância é um fator pequeno.

Portanto, o RG-6 é a primeira escolha em cenários de alta largura de banda, incluindo Internet de banda larga e serviços a cabo de TV digital por satélite de alta definição, pois ele pode ser utilizado para distâncias mais longas.

O condutor central maior do RG-6 significa que ele tem a capacidade de manter a largura de banda na faixa de giga-hertz, que é o dobro da largura de banda do RG-59.

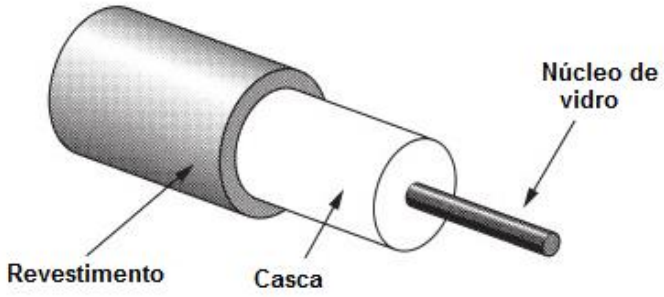
Normalmente os cabos coaxiais podem utilizar conectores do tipo F (F-Type) e BNC, veja imagem a seguir com cada um dos tipos de conectores.

Para soluções de TV a cabo e banda larga é mais comum o uso do conector tipo F.

10.3 Fibras Ópticas

A fibra óptica pode ser representada como um tubo flexível de vidro onde a luz se propaga.

Essa é uma representação básica da fibra óptica.



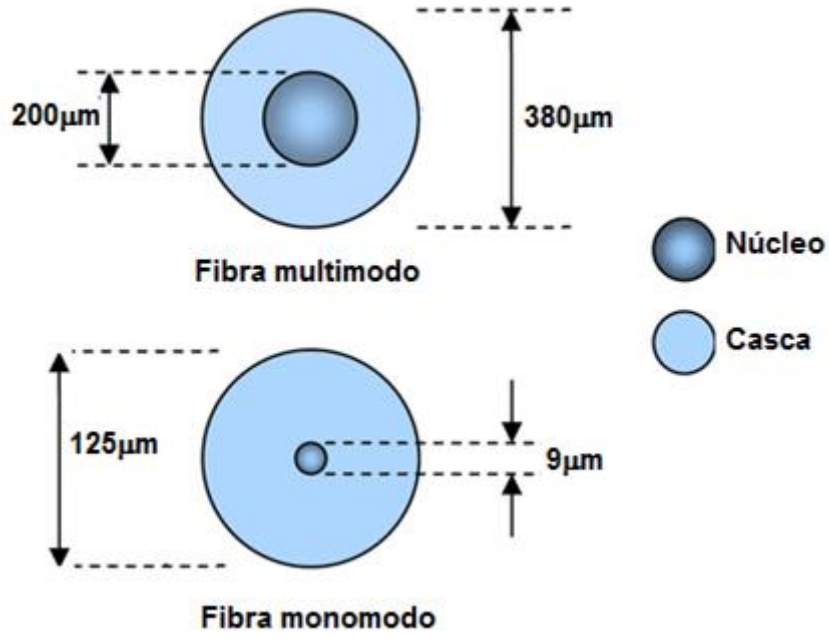
Esse tubo é chamado de núcleo e, portanto, é o meio onde a luz se propaga.

O núcleo é coberto com uma casca que tem a função de proteger e garantir que a luz fique confinada dentro do núcleo.

A casca, por sua vez, também é coberta por um revestimento de proteção.

Na prática os cabos possuem diversos revestimentos de proteção conforme a sua aplicação.

Você vai ver que existem diversos tipos de fibras ópticas e abaixo temos a representação dos diâmetros típicos de fibras do tipo multimodo e monomodo.



A luz de um LED ou um laser é colocada na ponta do núcleo e então ocorre a propagação até o destino.

A forma com que a luz se propaga no núcleo é o objeto de estudo da óptica, assim como os tipos de fibra óptica.

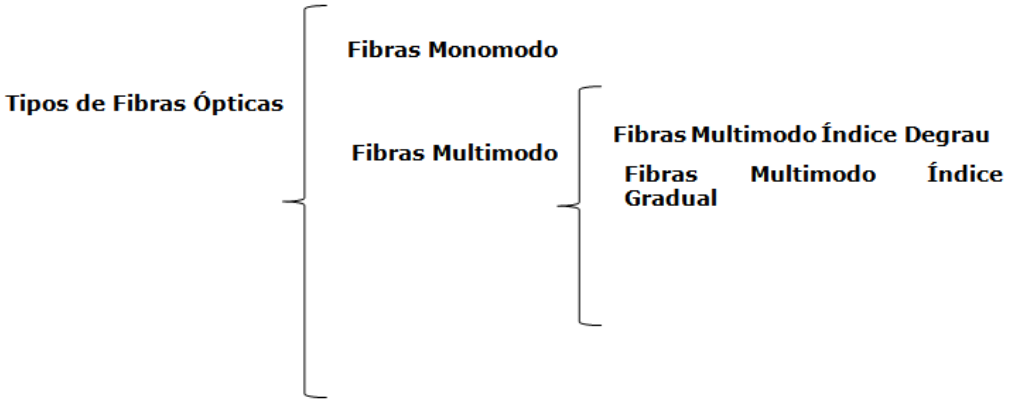
A lei de snell, os conceitos de refração e dispersão são aplicados diretamente na tecnologia de fabricação das fibras.

Isso faz toda a diferença na hora de projetar e dimensionar um sistema de comunicações ópticas, pois dependendo da distância e uso da fibra óptica podemos baratear ou onerar um projeto de rede.

As Fibras ópticas ser divididas em 2 grupos:

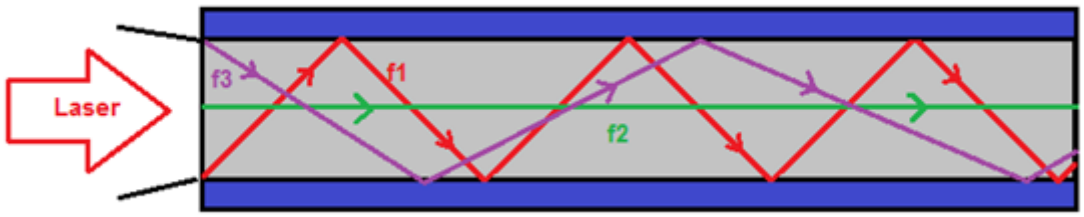
- Fibras Multimodo
- Fibras Monomodo

As Fibras multimodo podem ser de índice degrau ou índice gradual.



10.3.1 Fibras Ópticas Multimodo

Imagine uma fibra óptica com um laser na ponta como na figura a seguir.



Observe que a luz que sai do laser se propaga de vários modos:

1. Um feixe (f1) sai da parte de baixo do laser e reflete na parte de cima do núcleo da fibra óptica e vai se propagando em zigue-zague até o destino.
2. Um segundo feixe (f2) sai da parte do meio do laser e se propaga em linha reta na fibra óptica até chegar do outro lado da fibra.
3. E finalmente, um feixe (f3), sai da parte de cima do laser e reflete na parte de baixo do núcleo da fibra óptica e vai se propagando em zigue-zague até a outra extremidade.

Como esses 3 feixes, "n" feixes saem do laser resultando em "n" modos de propagação, portanto, dentre os tipos de fibra óptica, aquela que proporciona esse tipo de propagação é chamada de fibra multimodo.

As fibras multimodo foram as primeiras a surgir e possuem um núcleo maior que as fibras monomodo, o que resulta nos "n" modos de propagação.

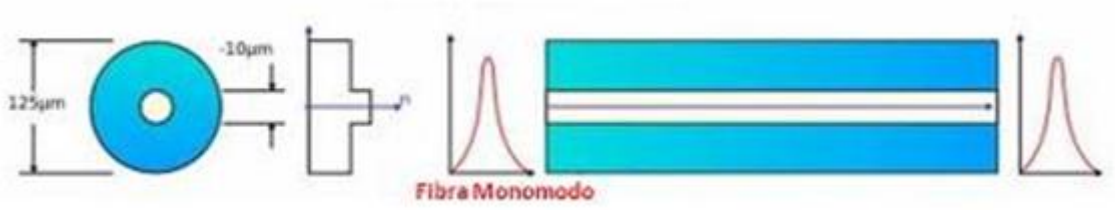
Como elas são menos "exigentes" no modo que a luz se propaga são também mais "baratas", porém suportam distâncias menores que as monomodo que vamos estudar a seguir.

10.3.2 Fibras Ópticas Monomodo

Antes de mais nada, imaginemos uma fibra com um núcleo tão fino que quando a luz do laser é acoplada, o feixe de luz transportado permite somente um modo de transmissão.

Nesse caso existe somente um caminho possível para a propagação, ou seja, somente um modo.

Entre os diversos tipos de fibra óptica, as fibras com essas características são denominadas fibras monomodo.



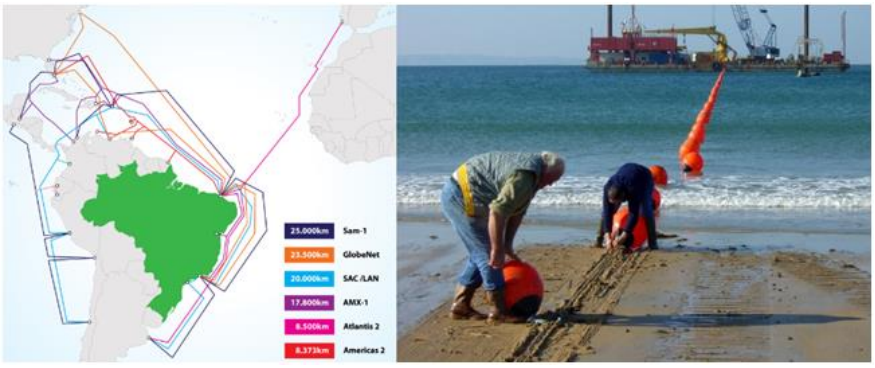
A fabricação de fibras ópticas monomodo é mais complexa devido à dificuldade mecânica de fibras tão finas.

Nas fibras monomodo anula-se a dispersão modal e obtém-se uma menor atenuação.

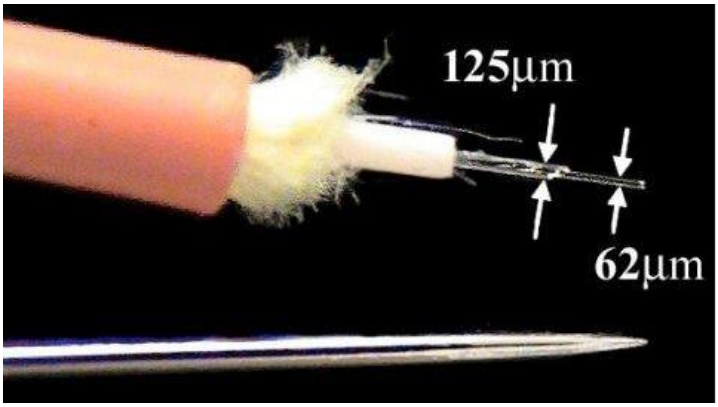
A conectividade do laser, contudo, é mais difícil o que exige que o laser utilizado seja mais preciso de alta qualidade elevando o custo de todo o sistema.

A princípio as fibras monomodo são utilizadas em sistemas de média e longas distâncias, cabos de fibras estaduais, backbones de grandes distâncias e inclusive em comunicações intercontinentais (cabos submarinos) onde há a transmissão de altas taxas de dados.

Por exemplo, podem ser utilizadas em cabos submarinos.

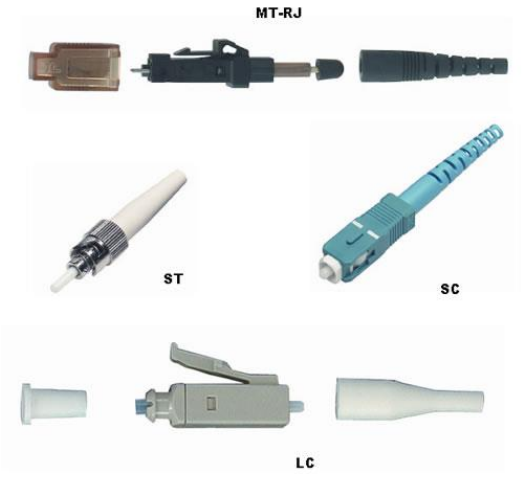


Para você ter uma ideia das dimensões de uma fibra veja a figura a seguir, trata-se de uma fibra multimodo em que a casca tem 125 mícrons e o núcleo 62,5 mícrons, abaixo tem uma agulha para comparação das dimensões.



10.3.3 Principais Tipos de Conectores Ópticos

Os conectores ópticos tem a função de deixar a fibra perfeitamente alinhada nos pontos de conexão para que o sinal luminoso possa ser transmitido sem grandes perdas. Os quatro tipos de conectores mais comuns são LC, SC, ST e MT-RJ, veja a figura abaixo.



Os conectores ST e SC eram os mais populares até pouco tempo atrás, mas os LC têm crescido bastante em popularidade e podem vir a tornar-se o padrão dominante.

Os conectores MT-RJ também têm crescido em popularidade devido ao seu formato compacto, mas ainda estão restritos a alguns nichos. Como cada conector oferece algumas vantagens sobre os concorrentes e é apoiada por um conjunto diferente de empresas, a escolha recai sobre o conector usado pelos equipamentos que pretender usar.

O LC (Lucent Connector) é um conector miniaturizado que, como o nome sugere, foi originalmente desenvolvido pela Lucent. Ele tem bastante popularidade, sobretudo no uso de fibras monomodo. Ele é o mais comumente usado em transceivers 10 Gigabit Ethernet.

É possível também utilizar conectores diferentes dos dois lados do cabo, usando conectores LC de um lado e conectores SC do outro, por exemplo. Além disso, existem adaptadores para que você possa conectar fibras do mesmo tipo ou de tipos diferentes. Veja a figura a seguir com um cordão com conector MT-RJ em uma ponta e outra com conector LC. O cordão óptico também é conhecido como "pigtail".

Outro equipamento muito comum de ser encontrado em redes que utilizam fibras ópticas são as caixas de distribuição ópticas (que podem ser também caixas de emendas ópticas ou caixas de terminações ópticas), utilizadas para acomodar as conexões de fibra e é onde normalmente fica terminado um circuito de fibra.

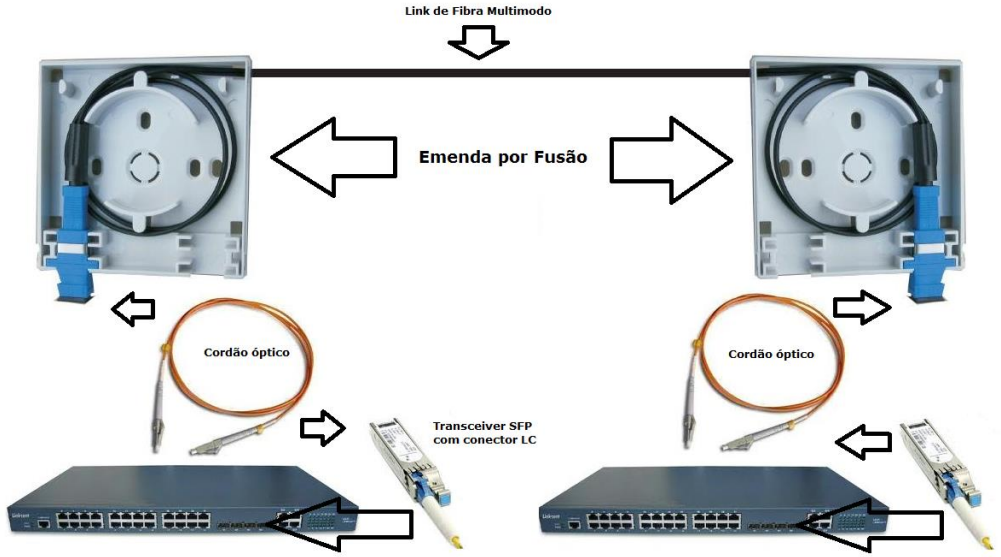
Elas são utilizadas para conectar do equipamento, como um switch ou conversor óptico à fibra de maneira segura, pois como a fibra é mais sensível que um cabo óptico deixá-la solta seria muito arriscado, seria similar ao patch pannel de uma rede metálica. Veja a figura seguinte com uma caixa de terminações ópticas.

Vamos agora montar um circuito simples com uma conexão óptica entre switches de uma empresa.

Por exemplo, temos dois switches com interface SFP com conectores do tipo LC que utiliza fibra multimodo (MM). Portanto, vamos precisar de um cabo de fibra multimodo e duas caixas de

terminação ópticas com conectores do tipo LC, lançar um cabo com fibras entre os dois pontos e fazer emendas nas caixas de terminação óptica.

Uma vez o circuito montado o caminho precisa ser testado e depois precisaremos de cordões ópticos para ligar das portas dos switches para a caixa de terminação óptica.



10.3.4 Onde Devo Utilizar os Tipos de Fibra Óptica Monomodo e Multimodo na prática?

A grande vantagem da fibra monomodo cabos de fibra óptica é a possibilidade de transmissão de sinais em longa distância.

Normalmente essas distâncias podem ser de até 120 quilômetros sem o uso de regeneradores ópticos.

Já as fibras multimodo tem uma faixa máxima de transmissão é de cerca de 2 km.

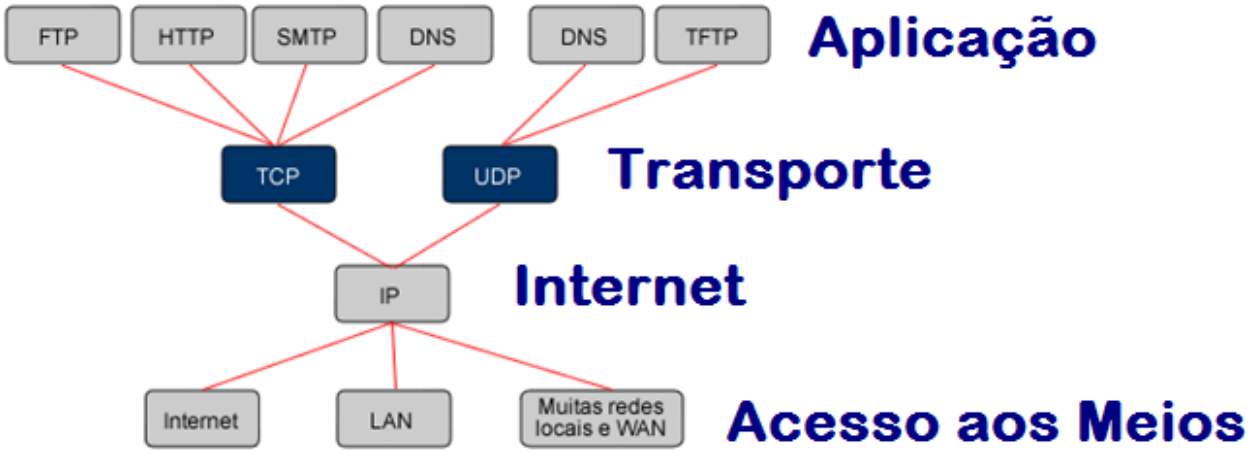
Portanto, se sua empresa tem links internos de até 2km conectando os switches de Core, Distribuição e Acesso, as fibras multimodo podem ser utilizadas tranquilamente.

Agora, se houver necessidade de links com distâncias superiores a 2km até 120km o uso de uma fibra óptica monomodo é mais recomendado.

11 Encapsulamento de Dados no TCP/IP

Portanto no TCP/IP o processo de encapsulamento é um pouco diferente, mais simples, pois a camada de Aplicação envia seus dados para a camada de Transporte.

A camada de transporte envia seus segmentos ou datagramas para a camada de Internet (não é mais Rede do TCP/IP), a qual envia seus pacotes para a camada de acesso aos meios para que as informações (bits) sejam enviadas no meio físico.



Com o TCP/IP em cinco camadas a Internet envia seus pacotes para a camada de Data Link, a qual envia seus quadros ou frames para a camada física.

Tenha sempre em mente essa nomenclatura das informações trocadas entre as camadas, tanto do modelo OSI como TCP/IP, isso é importante para a prova e para sua vida prática!

12 Conclusão e Certificado

Tenha certeza de que compreendeu todos os conceitos aqui mostrados, pois ao final desse curso você deve ter conhecimentos dos seguintes assuntos:

- Descrever as características, funções e exemplos de protocolos das camadas do protocolo TCP/IP:
  - Aplicação
  - Transporte
  - Internet
  - Acesso aos meios
- Diferenças entre os protocolos TCP e UDP
- Funcionamento e características do protocolo TCP
  - Formato do segmento TCP
  - Estabelecimento uma Conexão TCP
  - Confirmação de Recebimento de Segmentos TCP
  - Retransmissão de Segmentos TCP
  - Controle de Congestionamento TCP
  - Reagrupamento de Segmentos TCP
- Funcionamento e características do protocolo UDP
  - Formato do datagrama UDP
- Arquitetura Cliente/Servidor
- Principais Portas TCP e UDP
- Introdução ao endereçamento IP
  - Formato do pacote e endereço IPv4
  - Formato do pacote e endereço IPv6
  - Princípios de Roteamento IP
- Principais protocolos da camada de Acesso aos Meios
- Endereços de camada-2 e comunicação em redes na camada de acesso aos meios
- Interpretar os campos do endereçamento MAC
- Processo de encapsulamento e desencapsulamento no TCP/IP
- Tipos e padrões de cabeamento

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!!!!!