MANUAL DO ALUNO

DISCIPLINA COMUNICAÇÃO DE DADOS

Módulos 3 e 4

República Democrática de Timor-Leste
Ministério da Educação

FICHA TÉCNICA

TÍTULO
MANUAL DO ALUNO - Disciplina de Comunicação de Dados
Módulos 3 a 4

AUTOR
BRUNO MORAIS

COLABORAÇÃO DAS EQUIPAS TÉCNICAS TIMORENSES DA DISCIPLINA
XXXXXXX

COLABORAÇÃO TÉCNICA NA REVISÃO

DESIGN E PAGINAÇÃO
UNDESIGN - JOAO PAULO VILHENA
EVOLUA.PT

IMPRESSÃO E ACABAMENTO
XXXXXX

ISBN
XXX - XXX - X - XXXXX - X

TIRAGEM
XXXXXXX EXEMPLARES

COORDENAÇÃO GERAL DO PROJETO
MINISTÉRIO DA EDUCAÇÃO DE TIMOR-LESTE
2014

Índice

Protocolos de Rede 9

Apresentação 10

Objetivos de aprendizagem 10

Âmbito de conteúdos 11

Introdução ao TCP/IP 13

História e futuro do TCP/IP 13

Camada de aplicação 13

Camada de Transporte 15

Camada de Internet 17

Camada de acesso à rede 19

Comparação modelo OSI com o modelo TCP/IP 21

Arquitetura da Internet 22

Endereços de Internet 26

Endereçamento IP 26

Converter binários em decimais 27

Endereçamento IPv4 29

Sintaxe do endereço IPv4 29

Endereços IPv4 unicast 31

Endereços IPv4 multicast 31

Endereços IPv4 de difusão 32

Classes de endereços IP 33

Classe A 34

Classe B 34

Classe C 34

Classe D 36

Classe E 36

Resumo para as Classes de Endereços 36

Endereço Loopback 38

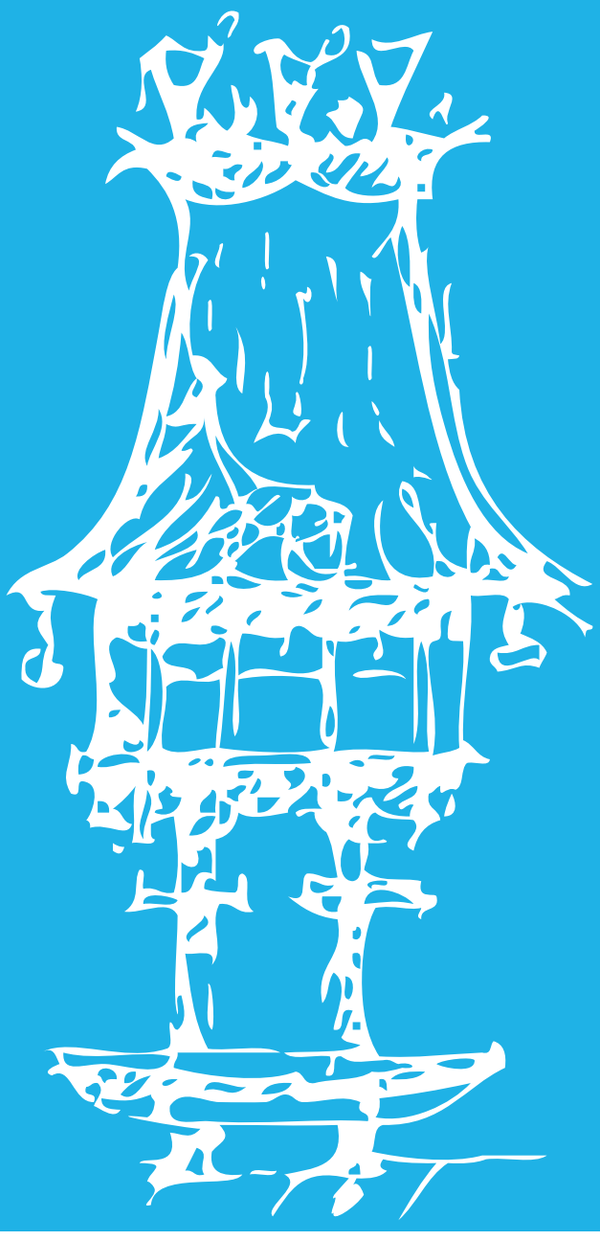
Endereços IP reservados 39

Endereços Privados e Públicos 39
Introdução às Sub-Redes 40
Estabelecimento do endereço da máscara de sub-rede 42
Aplicação da máscara de sub-rede 44
Divisão de redes das classes A e B em sub-redes 46
IPV4 x IPV6 48
Obter um endereço IP 50
Obtendo um endereço da Internet 50
Atribuição estática do endereço IP 51
Atribuição de endereço IP utilizando RARP 52
Atribuição de endereço IP BOOTP 52
Gestão de Endereços IP com uso de DHCP 53
Funcionamento 54
Problemas de resolução de endereços 61
Protocolo de Resolução de Endereços (ARP) 61
Funcionamento do protocolo ARP 63
Cache ARP 64
ARP - Encapsulamento Identificação 64
Formato do ARP 65
Camada de Transporte TCP/IP 67
Introdução à camada de transporte 67
Controle de fluxo 68
Visão geral de estabelecimento, manutenção e término de sessões 69
Handshake triplo 71
Janelamento 73
Confirmação 75
Protocolo de Controlo de Transmissão (TCP) 77
Protocolo de Datagrama de Usuário (UDP) 78
Números de porta TCP e UDP 79
A Camada de Aplicação 82
Introdução à camada de aplicação TCP/IP 82

DNS 83
FTP 83
HTTP 85
SMTP 86
SNMP 87
Telnet 89
Exercícios Propostos 90
Bibliografia 93
Meios e Equipamentos de Transmissão de Dados 95
Apresentação 96
Objetivos de aprendizagem 96
Âmbito de conteúdos 97
A importância dos meios físicos de transmissão 99
Meios de transmissão metálicos 100
Utilização e adaptação às exigências do mercado 101
Caraterísticas elétricas dos cabos metálicos 107
Cabos simples 109
Linhas de condutores aéreos 109
Cabos de pares entrançados 110
Designações de acordo com o tipo de blindagem 110
Cabo UTP como o mais utilizado 113
Ferramentas para os cabos UTP 119
Tipos de ligações e respetivos esquemas 121
Elaboração de cabos 124
Corte do cabo 124
Preparação/separação do cabo: 125
Colocação da ficha RJ-45 126
Cravar o cabo com o alicate 128
Cabos coaxiais 129
Cabo coaxial grosso 130

Vantagens 131
Desvantagens 131
Cabo Coaxial Fino 131
Vantagens 132
Desvantagens 132
Cuidados na instalação do cabo coaxial 132
Cabo Coaxial x Par Entrançado 133
Meios de Fibra Ótica 134
Vantagens 136
Desvantagens 136
Aplicações de Fibras Óticas 137
Como funciona a transmissão ótica 137
Fibras Óticas Multimodo 138
Fibra Ótica Multimodo com Índice Degrau 139
Fibra Ótica Multimodo com Índice Gradual 139
Fibras Óticas Monomodo 140
Fibra Ótica X Cobre 141
Meios sem fios 143
Ligações via rádio 144
Ligações em micro-ondas 145
Ligações em infravermelhos 146
Ligações laser 147
Porque usar Cablagem Estruturada 148
Funções de uma rede estruturada 149
Áreas compreendidas pela rede estruturada 150
Componentes da cablagem estruturada 152
Equipamento Passivo e Ativo 156
Equipamentos de interligação de redes 157
Repetidores 157
Pontes (Bridge) 158
Principio 159

Funcionamento 159
Concentrador (Hub) 159
Tipos de concentradores 160
Ligação de vários hubs 160
Comutadores (Switch) 161
Encaminhadores (Routers) 162
Aspeto de um router 163
Router sem fios 165
Exercícios Propostos 166
Bibliografia 169



Protocolos de Rede

Módulo 3

Apresentação

A Internet foi desenvolvida para oferecer uma rede de comunicação que pudesse continuar funcionando em tempos de guerra. Embora tenha evoluído de maneira bem diferente daquela imaginada por seus idealizadores, ela ainda é baseada no conjunto de protocolos TCP/IP. O projeto do TCP/IP é ideal para uma rede descentralizada e robusta como é a Internet. Muitos protocolos usados hoje em dia foram criados usando o modelo TCP/IP de quatro camadas.

No presente módulo analisaremos os dois modelos de rede TCP/IP e OSI. Cada modelo oferece sua própria estrutura para explicar como uma rede funciona, mas há muita sobreposição entre eles. Sem conhecer os dois, é possível que um administrador de rede não tenha uma perceção suficientemente clara sobre as razões pelas quais uma rede funciona da maneira que funciona.

Neste módulo é abordado como é distribuído o endereço IP por parte dos router porque qualquer dispositivo da Internet que queira comunicar-se com outros dispositivos da Internet precisa ter um identificador exclusivo. Esse identificador é conhecido como endereço IP, porque os r*outer's* usam um protocolo, da camada três, o protocolo IP, para encontrar o melhor caminho até esse dispositivo. O IPv4, versão atual do IP, foi concebido antes que houvesse uma grande procura por endereços. O crescimento explosivo da Internet tem ameaçado esgotar os endereços IP. As sub- redes, a tradução de endereços de rede (NAT, *Network Address Translation*) e o endereçamento privado são usados para expandir o endereçamento IP sem que esses endereços esgotem. Uma outra versão do IP, conhecida como IPv6, apresenta melhorias em relação à versão atual, oferecendo um espaço de endereçamento muito maior, integrando ou eliminando os métodos usados para lidar com as deficiências do IPv4.

Objetivos de aprendizagem

- Explicar por que a Internet foi desenvolvida e como o TCP/IP se situa no projeto da Internet;
- Relacionar as quatro camadas do modelo TCP/IP;
- Descrever as funções de cada camada do modelo TCP/IP;

- Comparar o modelo OSI e o modelo TCP/IP;
- Descrever a função e a estrutura dos endereços IP;
- Entender por que a divisão em sub-redes é necessária;
- Explicar a diferença entre os endereçamentos públicos e privado;
- Entender a função dos endereços IP reservados;
- Explicar a utilização do endereçamento estático e dinâmico para um dispositivo;
- Entender como o endereçamento dinâmico pode ser feito utilizando RARP, BootP e DHCP;
- Utilizar o ARP para obter o endereço MAC e enviar um pacote para outro dispositivo;
- Entender as questões relacionadas ao endereçamento entre redes;
- Planear a escolha dos endereços IP;
- Papel dos protocolos IP, TCP, UDP, ICMP, ARP;
- Entender como funciona uma rede Ethernet e a relação desta com o TCP/IP;
- Identificar as Arquiteturas proprietárias.

Âmbito de conteúdos

- Introdução ao TCP/IP
  - História e futuro do TCP/IP
  - Camada de aplicação
  - Camada de Transporte
  - Camada de Internet
  - Camada de acesso à rede
  - Comparação modelo OSI com o modelo TCP/IP
  - Arquitetura da Internet
- Endereços de *Internet*
  - Endereçamento IP
  - Conversão decimal/binário
  - Endereçamento IPv4
  - Endereços IP classes A, B, C, D e E
  - Endereços IP reservados

- Endereços IP públicos e privados
- Introdução às sub-redes
- IPv4 X IPv6

- Obter um endereço IP
  - Obtendo um endereço da Internet
  - Atribuição estática do endereço IP
  - Atribuição de endereço IP utilizando RARP
  - Atribuição de endereço IP BOOTP
  - Gestão de Endereços IP com uso de DHCP
  - Problemas de resolução de endereços
  - Protocolo de Resolução de Endereços (ARP)
- Camada de Transporte TCP/IP
  - Introdução à camada de transporte
  - Controle de fluxo
  - Visão geral de estabelecimento, manutenção e término de sessões
  - Handshake triplo
  - Janelamento
  - Confirmação
  - Protocolo de Controlo de Transmissão (TCP)
  - Protocolo de Datagrama de Usuário (UDP)
  - Números de porta TCP e UDP
- A Camada de Aplicação
  - Introdução à camada de aplicação TCP/IP
  - DNS
  - FTP
  - HTTP
  - SMTP
  - SNMP
  - Telnet

Introdução ao TCP/IP

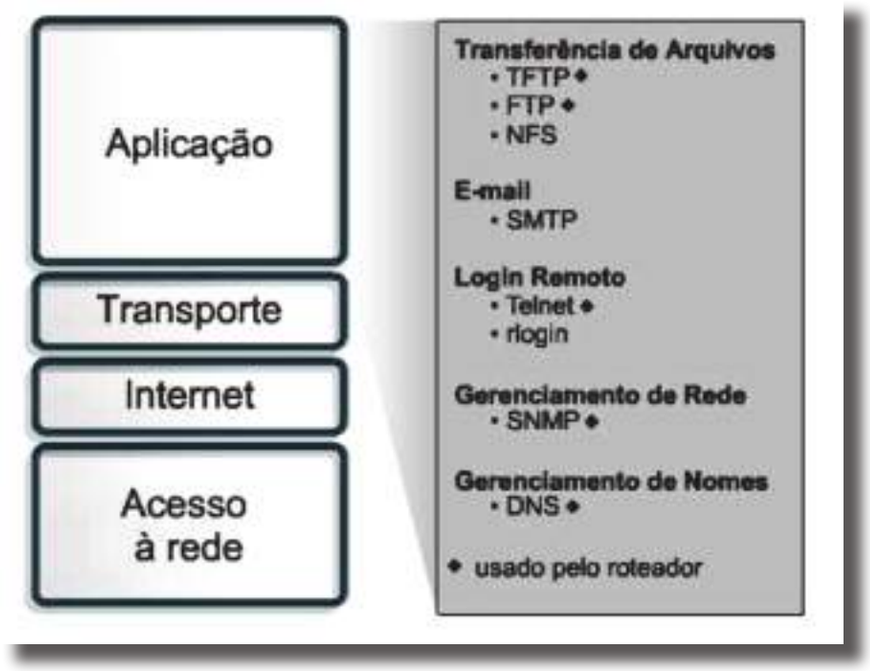
História e futuro do TCP/IP

O Departamento de Defesa dos Estados Unidos (DoD) criou o modelo de referência TCP/IP porque queria uma rede que pudesse sobreviver a qualquer condição. Para ilustrar, imagine um mundo atravessado por muitos cabos, fios, microondas, fibras óticas e conexões de satélite. Imagine também a necessidade de transmitir dados independentemente da condição de um determinado nó ou rede. O DoD exigia transmissão confiável de dados para qualquer destino da rede sob quaisquer circunstâncias. A criação do modeloTCP/IP ajudou a resolver esse difícil problema de projeto. Desde então, o modelo TCP/IP tornou-se o padrão no qual a Internet se baseia.

Ao estudar as camadas do modelo TCP/IP, é preciso ter em mente a intenção original da Internet, assim, haverá menos confusão. O modelo TCP/IP tem quatro camadas: a camada de aplicação, a camada de transporte, a camada de Internet e a camada de acesso à rede. Algumas das camadas do modelo TCP/IP têm o mesmo nome das camadas do modelo OSI. É essencial não confundir as funções das camadas dos dois modelos, pois as camadas contêm diferentes funções em cada modelo. A versão atual do TCP/IP foi padronizada em setembro de 1981.

Camada de aplicação

A camada de aplicação do modelo TCP/IP trata de protocolos de alto nível, questões de representação, codificação e controlo de diálogos. O conjunto de protocolos TCP/IP combina todas as questões relacionadas às aplicações numa única camada e garante que esses dados são empacotados corretamente antes de passá-los adiante para a próxima camada. O TCP/IP inclui não somente especificações da camada de Internet e transporte, tais como IP e TCP, mas também especificações para aplicações comuns. O TCP/IP tem protocolos que suportam transferência de ficheiros, correio eletrónico e login remoto, em adição aos seguintes:



FTP (File Transfer Protocol – Protocolo de Transferência de Arquivos) – O FTP é um serviço confiável, orientado a ligações, que usa o TCP para transferir ficheiros entre sistemas que suportam o FTP. Este protocolo suporta transferências bidirecionais de ficheiros binários e ASCII.

TFTP (Trivial File Transfer Protocol – Protocolo de Transferência de Arquivos Simples) – O TFTP é um serviço sem ligação que usa o UDP (User Datagram Protocol – Protocolo de Datagrama de utilizador). Esse protocolo é usado no router para transferir arquivos de configuração e imagens IOS bem como para transferir ficheiros entre sistemas que suportam TFTP. É útil em algumas redes locais porque opera mais rápido do que o FTP num ambiente estável.

NFS (Network File System – Sistema de ficheiros de Rede) – O NFS é um conjunto de protocolos de sistema de ficheiros distribuído, desenvolvido pela Sun Microsystems, que permite acesso a ficheiros de um dispositivo de armazenamento remoto, como um disco rígido, através da rede.

SMTP (Simple Mail Transfer Protocol – Protocolo Simples de Transferência de Correio) – O SMTP gere a transmissão de correio eletrónico através de redes de computadores. Ele não oferece suporte à transmissão de dados que não sejam em texto simples.

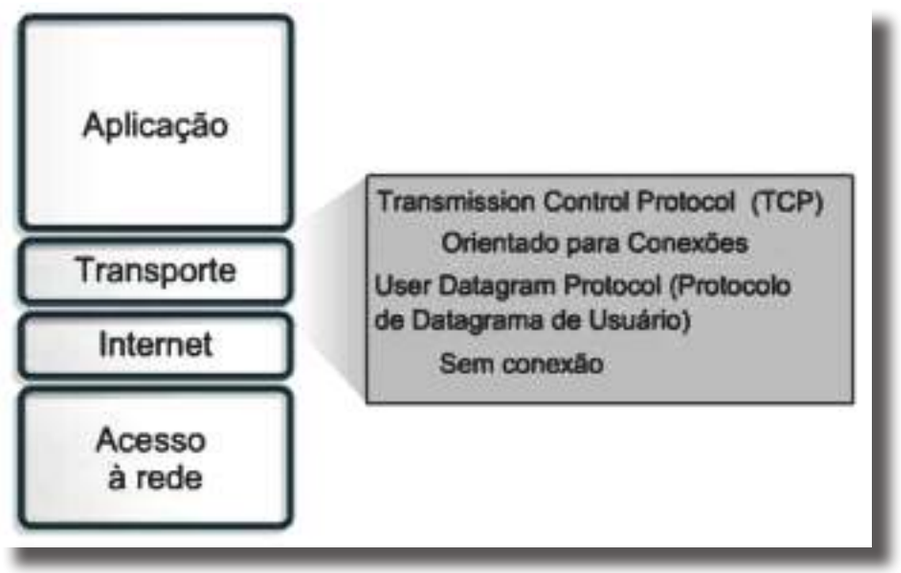
Telnet (Terminal emulation – Emulação de terminal) – O Telnet permite o acesso remoto a outro computador. Ele permite que um utilizador efetue login num host da Internet e execute comandos.
Um cliente Telnet é chamado host local. Um servidor Telnet é chamado host remoto.

SNMP (Simple Network Management Protocol – Protocolo Simples de Gerenciamento de Rede) – O SNMP é um protocolo que oferece uma forma de monitorizar e controlar dispositivos de rede e de gerir configurações, recolha de dados estatísticos, desempenho e segurança.

DNS (Domain Name System – Sistema de Nomes de Domínio) – O DNS é um sistema usado na Internet para converter Os nomes de domínios e os seus respetivos nós de rede divulgados publicamente em endereços IP.

Camada de Transporte

A camada de transporte oferece serviços de transporte desde o host de origem até o host de destino. Forma uma ligação lógica entre dois pontos da rede, o host emissor e o host recetor. Os protocolos de transporte segmentam e remontam os dados das aplicações de camada superior enviados dentro do mesmo fluxo de dados, ou ligação lógica, entre os dois pontos. O fluxo de dados da camada de transporte oferece serviços de transporte ponta-a-ponta.



Geralmente, a Internet é representada por uma nuvem. A camada de transporte envia pacotes de dados da origem para o destino recetor através dessa nuvem. O controlo ponta-a-ponta, fornecido pelas janelas móveis e pela confiabilidade dos números de sequenciamento e das confirmações, é a principal tarefa da camada de transporte quando se usa o TCP. A camada de transporte também define a conectividade ponta-a-ponta entre as aplicações do host. Os serviços de transporte incluem todos os serviços abaixo:

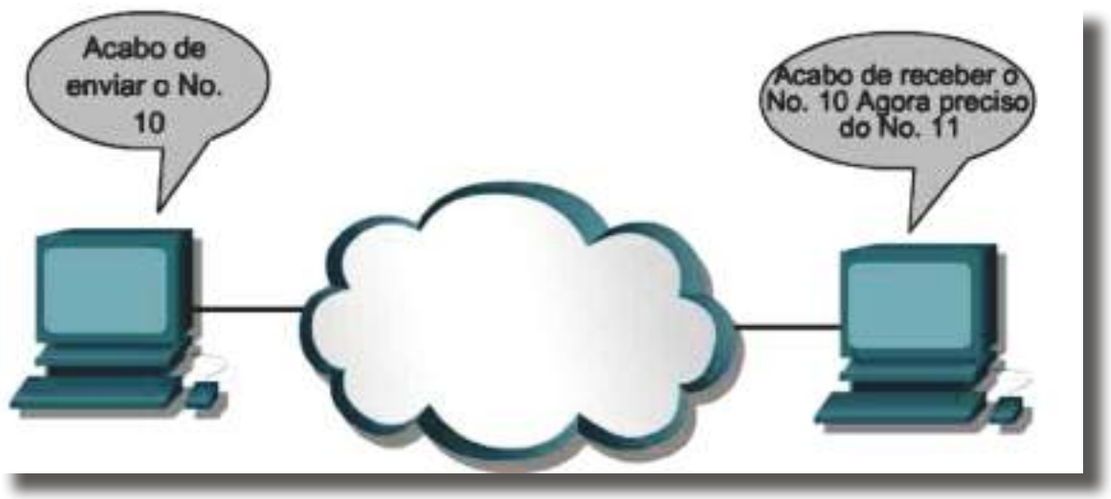
TCP e UDP

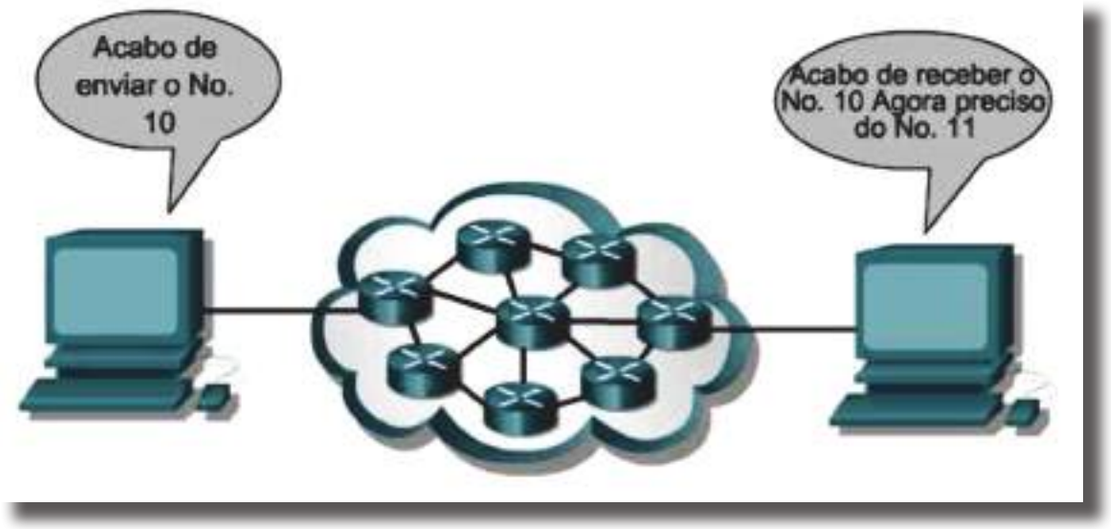
- Segmentação de dados das aplicações de camadas superiores.
- Envio de segmentos de um dispositivo numa ponta para um dispositivo em outra ponta.

Apenas TCP

- Estabelecimento de operações ponta-a-ponta.
- Controle de fluxo proporcionado pelas janelas móveis.
- Confiabilidade proporcionada pelos números de sequência e confirmações.

Como foi dito, a Internet é representada por uma nuvem. Essa nuvem trata de questões como “Qual dos vários caminhos é o melhor para uma caminho especifico?”

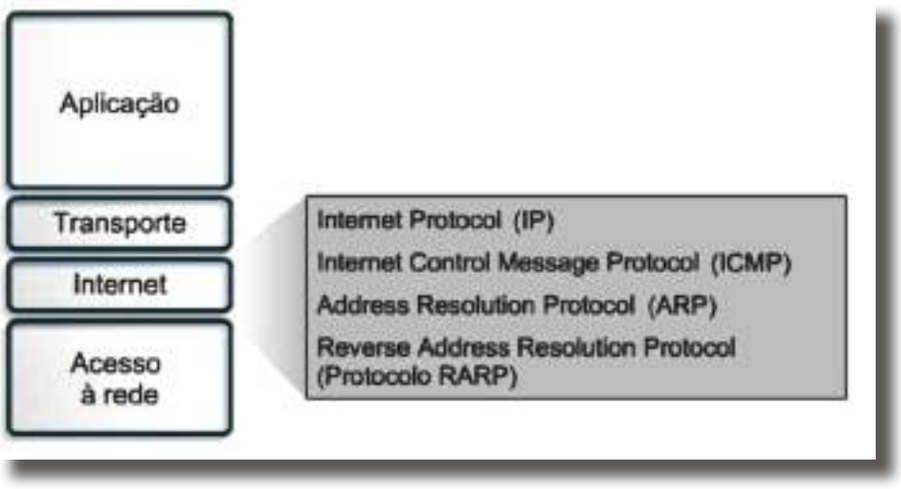




Camada de Internet

A finalidade da camada de Internet é escolher o melhor caminho para os pacotes viajarem através da rede. O principal protocolo que funciona nessa camada é o IP (Internet Protocol). A determinação do melhor caminho e o routing de pacotes ocorre nesta camada.

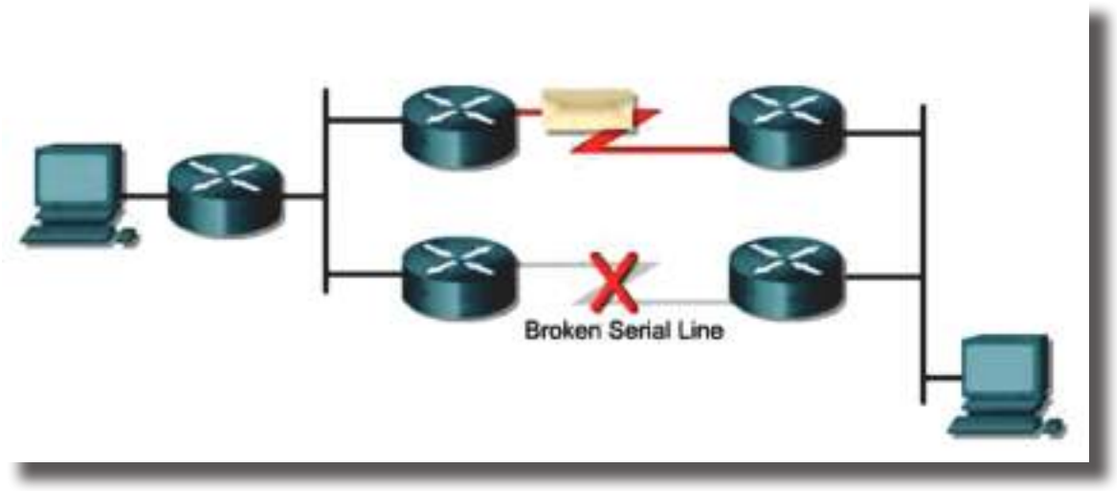
Os seguintes protocolos operam na camada de Internet TCP/IP:



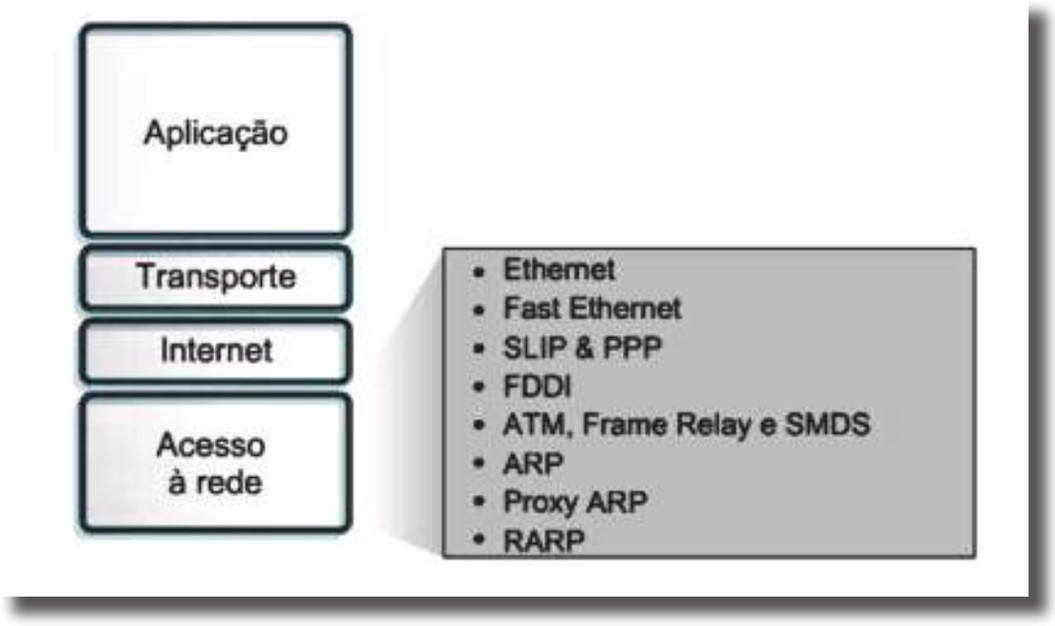
- O IP oferece comutação de pacotes sem conexão, e uma entrega de melhor esforço. Ele não se preocupa com o conteúdo dos pacotes, apenas procura um caminho até o destino.

- *O ICMP (Internet Control Message Protocol* – Protocolo de Mensagens de Controlo da Internet) oferece recursos de controlo e de mensagens.
- *O ARP (Address Resolution Protocol* – Protocolo de Resolução de Endereços) determina o endereço da camada de ligação de dados (o 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.

O IP realiza as seguintes operações:



O propósito da Internet é selecionar o melhor caminho do percurso dos pacotes através da rede

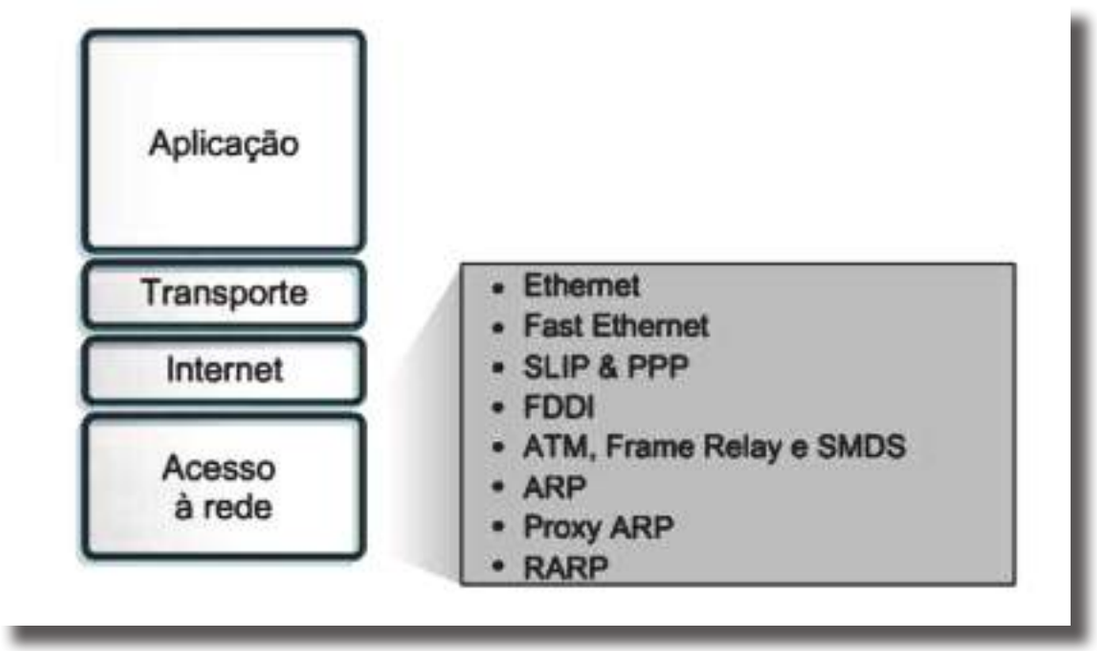


- Define um pacote e um esquema de endereçamento.
- Transfere dados entre a camada de Internet e as camadas de acesso à rede.
- Comuta os pacotes para os hosts remotos.

Finalmente, como esclarecimento sobre a tecnologia, o IP às vezes é considerado um protocolo não confiável. Isso não significa que o IP não entregue os dados de maneira precisa através de uma rede. Chamá-lo de protocolo não confiável significa simplesmente que o IP não realiza a verificação e correção de erros. Essa função é realizada pelos protocolos de camadas superiores, as camadas de transporte ou de aplicação.

Camada de acesso à rede

A camada de acesso à rede é também denominada camada host-to-network. A camada de acesso à rede é a camada que cuida de todas as questões necessárias para que um pacote IP estabeleça efetivamente um link físico com os meios físicos da rede. Isso inclui detalhes de tecnologia de redes locais, WANs e todos os detalhes contidos nas camadas física e de ligação de dados do modelo OSI.



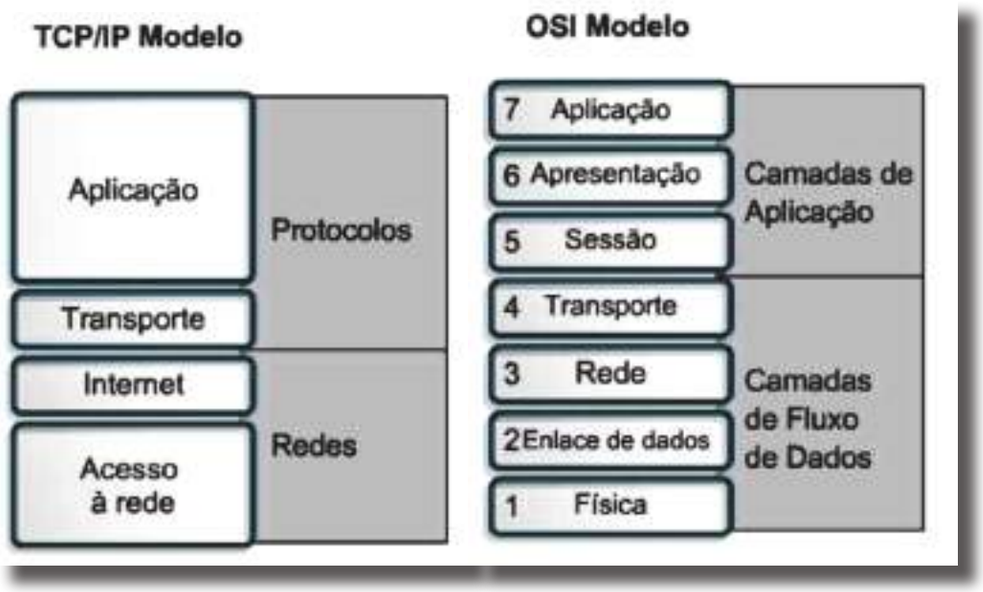
Drivers de aplicações, de placas de modem e de outros dispositivos operam na camada de acesso à rede. A camada de acesso à rede define os procedimentos para estabelecer uma interface com o hardware de rede e para aceder o meio de transmissão. Padrões de protocolos conhecidos são detetada e instalados como o SLIP (Serial Line Internet Protocol – Protocolo de Internet de Linha Serial) e o PPP (Pointto- Point Protocol – Protocolo Ponto a Ponto) oferecem acesso à rede através de uma ligação com modem. Devido a uma complexa interação entre as especificações de hardware, software e meios de transmissão, há muitos protocolos que operão nesta camada. A maioria dos protocolos reconhecíveis opera nas camadas de transporte e de Internet do modelo TCP/IP.

As funções da camada de acesso à rede incluem o mapeamento de endereços IP para endereços físicos de hardware e o encapsulamento de pacotes IP em quadros. Com base no tipo de hardware e na interface de rede, a camada de acesso à rede define a ligação com os meios físicos da rede.

Um bom exemplo de configuração da camada de acesso à rede seria a de um sistema Windows usando uma placa de rede de terceiros. Conforme a versão do Windows, a placa de rede seria detetada automaticamente pelo sistema operacional e os drivers adequados seriam instalados. Se a versão do Windows fosse mais antiga, o utilizador precisa especificar o driver da placa de rede. O fabricante da placa fornece esses drivers em discos ou CD-ROMs.

Comparação modelo OSI com o modelo TCP/IP

A seguir, vamos ver uma comparação entre o modelo OSI e o modelo TCP/IP, observando suas semelhanças e diferenças:



Semelhanças entre os modelos OSI e TCP/IP:

- Ambos são divididos em camadas.
- A camada de transporte do TCP/IP utiliza o protocolo UDP.
- Ambos são divididos em camadas de transporte e de rede equivalentes.
- A tecnologia de routing de pacotes (e não de routing de circuitos) é prevista por ambos.
- Os profissionais de rede precisam conhecer ambos os modelos.

Diferenças entre os modelos OSI e TCP/IP:

- O TCP/IP combina as camadas de apresentação e de sessão dentro da sua camada de aplicação.
- O TCP/IP combina as camadas física e de ligação/enlace de dados do modelo OSI numa única camada.
- O TCP/IP parece ser mais simples por ter menos camadas.
- A camada de transporte do TCP/IP, que utiliza o UDP, nem sempre garante a entrega confiável dos pacotes, ao contrário da camada de transporte do modelo OSI.

A Internet desenvolve-se com o uso dos padrões de protocolos TCP/IP. O modelo TCP/IP ganha credibilidade graças aos seus protocolos. Por outro lado, as redes normalmente não são implementadas sobre o protocolo do modelo OSI. O modelo OSI é usado como guia para a compreensão do processo de comunicação.

Arquitetura da Internet

Embora a Internet seja complexa, há algumas ideias básicas relacionadas à sua operação. Nesta seção, vamos examinar a arquitetura básica da Internet. A Internet é uma ideia que aparenta ser simples, quando repetida em grande escala, permite a comunicação de dados quase instantânea ao redor do mundo entre quaisquer pessoas, em qualquer lugar, a qualquer momento.

As redes locais são redes menores, limitadas a uma área geográfica. Muitas redes locais ligadas entre si possibilitam o funcionamento da Internet. Mas as redes locais têm limitações de escala. Embora tenham havido avanços tecnológicos que melhoraram a velocidade das comunicações, com o Ethernet Metro Optical, Gigabit e 10 Gigabits, a distância ainda representa um problema.

Focar a comunicação no nível da camada de aplicação entre os computadores de origem e destino e os computadores intermediários é uma forma de ter uma visão geral da arquitetura da Internet. Colocar instâncias idênticas de uma aplicação em todos os computadores da rede poderia facilitar a entrega de mensagens através da grande rede. Entretanto, isso apresenta problemas de escala. Para que um novo software funcione corretamente, é necessário que as novas aplicações sejam instalados em todos os computadores da rede. Para que um novo hardware funcione corretamente, é necessário modificar o software.

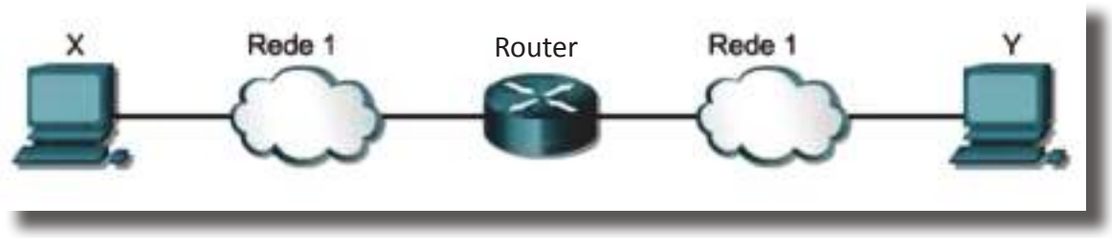
Qualquer falha de um computador intermediário ou de uma aplicação do computador causaria uma rutura na cadeia de mensagens a ser transmitidas. A Internet usa o princípio da interconexão de camadas de rede. Usando o modelo OSI como exemplo, o objetivo é construir a funcionalidade da rede em módulos independentes. Isso permite uma diversidade de tecnologias de LAN nas camadas 1 e 2 e uma diversidade de aplicações a funcionar nas camadas 5, 6 e 7.

O modelo OSI oferece um mecanismo no qual os detalhes das camadas inferiores e superiores estão separados. Isso permite que os dispositivos de rede intermediários "comutem" o tráfego sem ter que se preocupar com os detalhes da LAN.

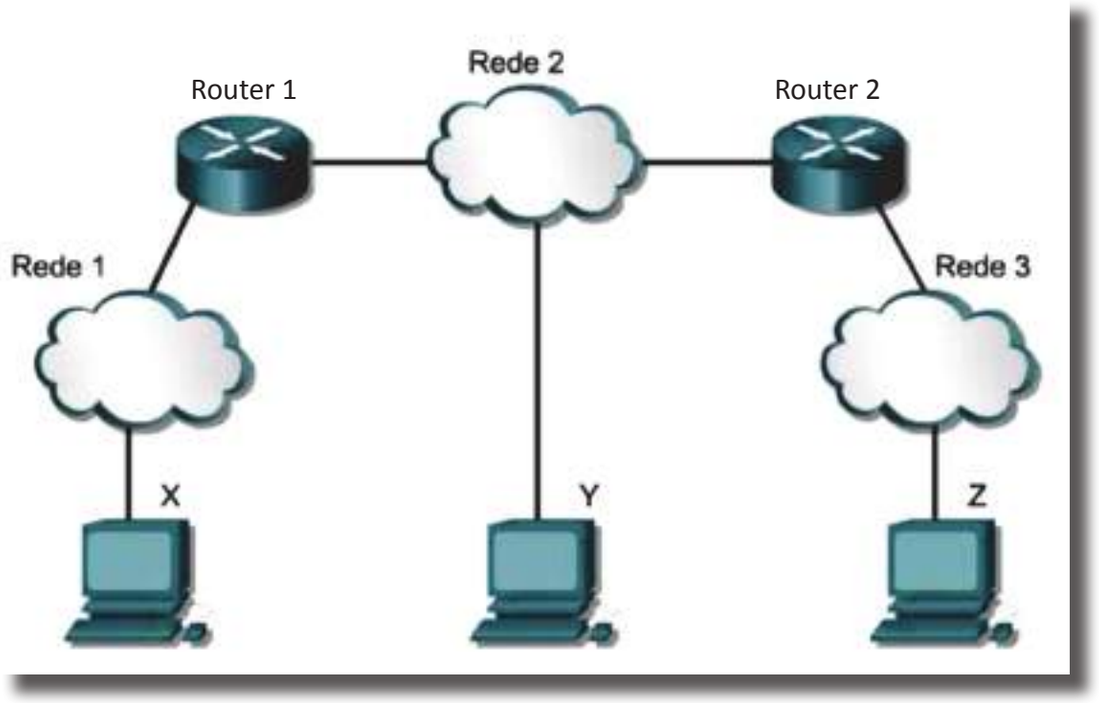
Isto leva ao conceito de internet working, ou construção de redes compostas. Uma rede de redes é chamada de internet (com "i" minúsculo). Quando falamos das redes que se desenvolveram a partir do Departamento de Defesa dos EUA, nas quais funciona a World Wide Web (www) ou rede mundial, usamos o "I" maiúsculo, Internet. As internets devem ser escalonáveis com relação à quantidade de redes e computadores ligados. A interligação de redes deve ser capaz de lidar com o transporte de dados através de enormes distâncias. Deve ser flexível para dar conta das constantes inovações tecnológicas.

Deve ser capaz de se ajustar às condições dinâmicas da rede. E as internets devem ser econômicas. Por fim, as internets devem ser projetadas para permitir comunicações de dados para qualquer pessoa, a qualquer momento, em qualquer lugar.

A figura resume a ligação de uma rede física a outra por meio de um computador de função especial, chamado router. Essas redes são descritas como diretamente conectadas ao router. O router é necessário para decisões sobre os caminhos a serem utilizados para que ocorra a comunicação entre duas redes. São necessários muitos routers para manusear grandes volumes de tráfego de rede.

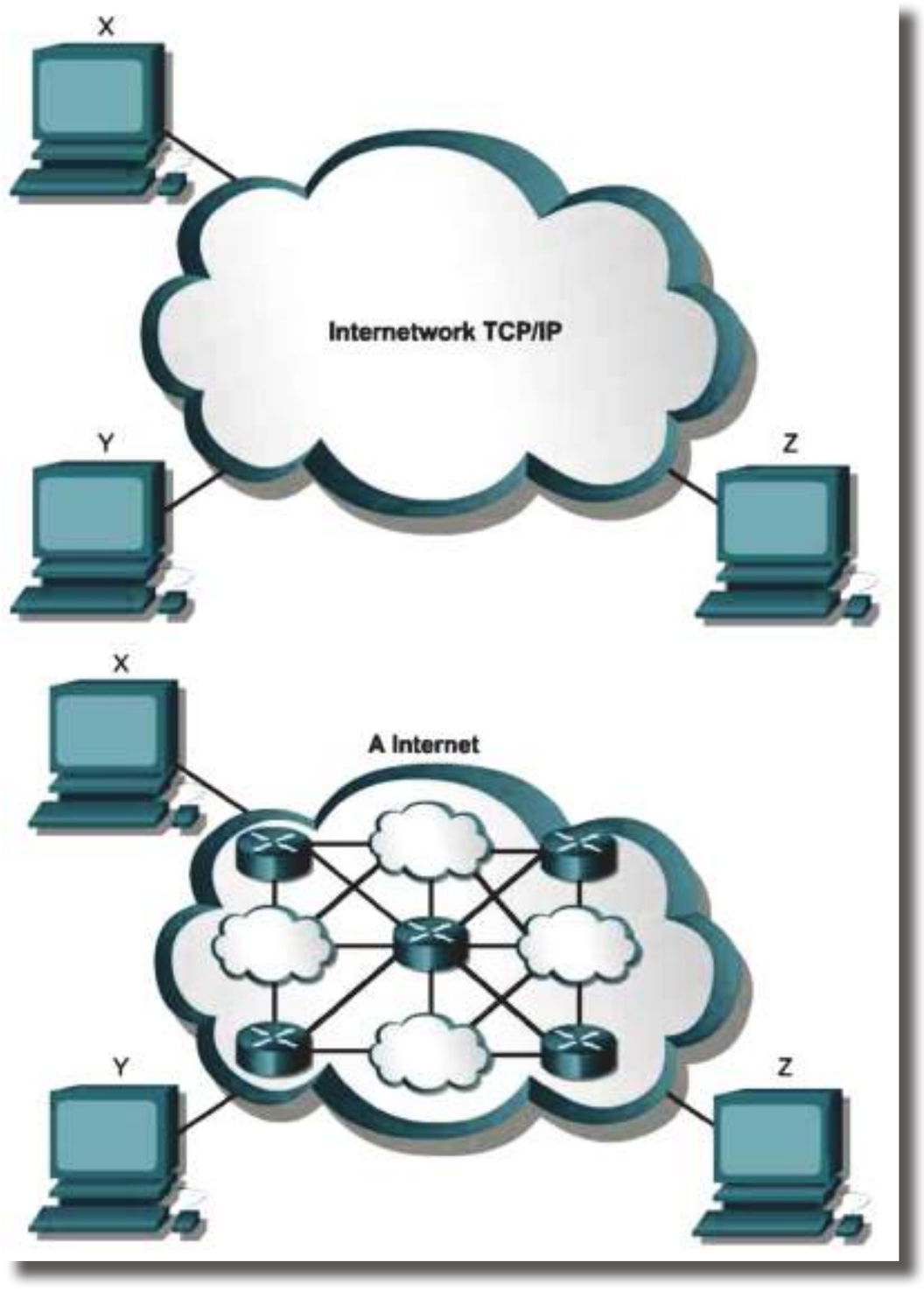


A figura expande a ideia para três redes físicas ligadas por dois routers. Os routers tomam decisões complexas para permitir que todos os utilizadores em todas as redes se comuniquem. Nem todas as redes estão diretamente ligadas entre si. O router precisa de algum método para lidar com essa situação.



Uma opção é que o router mantenha uma lista de todos os computadores e de todos os caminhos até eles. Assim, o router decidiria como encaminhar os pacotes de dados com base nessa tabela de referência. O encaminhamento é baseado no endereço IP do computador de destino. Essa opção ficaria difícil conforme fosse aumentando a quantidade de utilizadores. A escalabilidade é introduzida quando o router mantém uma lista de todas as redes, mas deixa os detalhes da entrega local para as redes físicas locais. Nesta situação, os routers passam mensagens para os outros routers. Cada router partilha informações sobre quais as redes estão ligadas a ele. Isso cria a tabela de roteamento.

A figura mostra a transparência exigida pelos utilizadores. Mesmo assim, as estruturas físicas e lógica dentro da nuvem da Internet podem ser extremamente complexas, conforme indica a figura. A Internet tem crescido rapidamente para aceitar cada vez mais utilizadores. O fato da Internet se ter tornado tão grande, com mais de 90.000 rotas centrais e 300.000.000 de utilizadores finais, é uma prova da solidez da sua arquitetura.



Dois computadores, em qualquer parte do mundo, seguindo certas especificações de hardware, software e protocolo, podem comunicar-se de maneira confiável. A padronização das práticas e dos procedimentos para movimentação de dados através das redes tornou a Internet possível.

Endereços de Internet

Endereçamento IP

Cada anfitrião TCP/IP é identificado por um endereço IP lógico. Este endereço é exclusivo para cada anfitrião que comunica utilizando TCP/IP. Cada endereço IP de 32 bits identifica uma localização de um sistema anfitrião na rede da mesma forma que um nome de rua identifica uma casa numa cidade.

Tal como um nome de rua tem um formato de duas partes padrão (um nome de rua e um número de porta), cada endereço IP divide-se internamente em duas partes, um ID de rede e um ID de anfitrião:

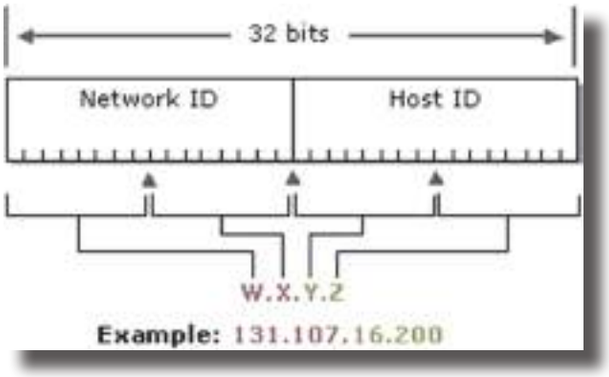
- O ID de rede, também designado por endereço de rede, identifica um único segmento de rede dentro de um conjunto de redes TCP/IP maior (uma rede de redes). Todos os sistemas que acedem e partilham o acesso à mesma rede têm um ID de rede comum dentro do respetivo endereço IP completo. Este ID também é utilizado para identificar exclusivamente cada rede dentro de um conjunto de redes maior.
- O ID de anfitrião, também designado por endereço de anfitrião, identifica um nó (uma estação de trabalho, servidor, router ou outro dispositivo TCP/IP) TCP/IP dentro de cada rede. O ID de anfitrião de cada dispositivo identifica um único sistema exclusivamente dentro da própria rede.

Segue-se o exemplo de um endereço IP de 32 bits:

10000011 01101011 00010000 11001000

Para facilitar o endereçamento IP, os endereços IP são representados por notações decimais com pontos. O endereço IP de 32 bits é segmentado em quatro octetos de 8 bits. Os octetos são convertidos para números decimais (sistema numérico com base-10) e separados por pontos. Deste modo, o exemplo de endereço IP anterior é 131.107.16.200 quando convertido para notações decimais com pontos.

A ilustração seguinte mostra um exemplo de vista de um endereço IP (131.107.16.200) dividido em secções de rede e de ID de anfitrião. A parte do ID de rede (131.107) é indicada pelos primeiros dois números do endereço IP. A parte do ID de anfitrião (16.200) é indicada pelos últimos dois números do endereço IP.



Como os endereços IP identificam dispositivos numa rede, um endereço IP exclusivo tem de ser atribuído a cada dispositivo na rede.

Em geral, a maioria dos computadores têm apenas uma única placa de rede instalada, pelo que requerem apenas um único endereço IP. Se um computador tiver várias placas de rede instaladas, cada placa necessitará do respetivo endereço IP.

Converter binários em decimais

Como todos os endereços IP e valores da máscara de rede são compostos por um campo de dados de 32 bits de comprimento padrão, são visualizados e interpretados pelos computadores como sendo uma cadeia numérica binária simples, tal como:

10000011 01101011 00000111 00011011

Para comunicar facilmente endereços IP e escrevê-los rapidamente em configurações, poderá utilizar a notação decimal com pontos para converter números de endereço IP a partir do formato binário.

Com a notação decimal com pontos, cada número de endereço de 32 bits é visualizado como quatro agrupamentos distintos de 8 bits. Cada um dos quatro agrupamentos de 8 bits consecutivos é referido como octeto.

O primeiro octeto utiliza os primeiros 8 bits (casas de bit 1 a 8), o segundo octeto utiliza os 8 bits seguintes (casas de bit 9 a 16), seguidos pelo terceiro octeto (casas de bit 17 a 24) e pelo quarto octeto (casas de bit 25 a 32). São utilizados pontos para separar os quatro octetos que são descritos como valores de números decimais separados no endereço IP.

A tabela seguinte mostra a notação científica para cada casa de bit num octeto individual e o valor decimal equivalente.

Os valores decimais equivalentes para casas de bit num octeto de endereço IP único.

Octeto	1º bit	2º bit	3º bit	4º bit	5º bit	6º bit	7º bit	8º bit
Notação científica	27	26	25	24	23	22	21	20
Notação decimal	128	64	32	16	8	4	2	1

Por exemplo, se a primeira casa de bit estiver preenchida com um valor de bit 1, o valor decimal equivalente é 128. Quando o valor de bit é 0, o valor decimal equivalente também é 0.

Se todas as casas de bit num octeto estiverem preenchidas com uns (1), o valor decimal equivalente mais elevado é 255. Se todas as casas de bit estiverem preenchidas com zeros (0), o valor decimal equivalente mais baixo é 0.

Para ver como cada octeto num endereço IP é convertido de um número binário de 8 dígitos para um número decimal equivalente de 0 a 255, segue-se um breve exemplo.

A cadeia binária seguinte mostra o primeiro octeto num endereço IP:

10000011

Neste número binário de 8 dígitos, a primeira, a sétima e a oitava casas de bit são preenchidas com uns. Todas as outras casas de bit são preenchidas com zeros. Se utilizar a tabela anterior como referência, poderá efetuar uma simples adição de cada valor

equivalente decimal da casa de bit para localizar a soma decimal desta cadeia de octetos, como se segue:

1º bit (128) + 7º bit (2) + 8º bit (1) = total do octeto (131)

Como a soma é 131, o primeiro octeto do endereço IP de exemplo é 131. Depois de utilizar este método para os outros octetos, o resultado final da conversão é o equivalente decimal com pontos: 131.107.7.27.

Endereçamento IPv4

Para o IP versão 4, cada host TCP/IP é identificado por um endereço IP lógico. O endereço IP é um endereço de camada de Rede e não depende do endereço de camada de Vínculo de Dados (como um endereço MAC de um adaptador de rede). É necessário um endereço IP exclusivo para cada host e componente de rede que se comunica usando TCP/IP, que pode ser atribuído manualmente ou usando o protocolo DHCP.

O endereço IP identifica um local do sistema na rede da mesma forma que um endereço de rua identifica uma casa em um quarteirão da cidade. Assim como um endereço de rua deve identificar uma residência exclusiva, um endereço IP deve ser um identificador global exclusivo para a rede e ter um formato uniforme.

Cada endereço IP inclui uma ID de rede e uma ID de host.

- A ID de rede (também conhecida como endereço de rede) identifica os sistemas que estão localizados na mesma rede física delimitada por routers IP. Todos os sistemas na mesma rede física devem ter a mesma ID de rede. A ID de rede deve ser exclusiva para a rede.
- A ID do anfitrião (também conhecida como endereço de host) identifica uma estação de trabalho, servidor, routers ou outro host TCP/IP em uma rede. O endereço de host deve ser exclusivo para a ID de rede.

Sintaxe do endereço IPv4

Um endereço IP é composto por 32 bits. Em vez de expressar os 32 bits dos endereços IPv4 de uma só vez usando notação binária ($Base_2$), o padrão é segmentar esses 32 bits

de um endereço IPv4 em quatro campos de 8 bits denominados *octetos*. Cada octeto é convertido num número decimal (base 10) de 0 a 255 e separado por um ponto (.). Esse formato é denominado *notação decimal com ponto*. A tabela a seguir mostra um exemplo de endereço IP nos formatos binário e decimal com ponto.

Endereço IP nos formatos binário e decimal com ponto

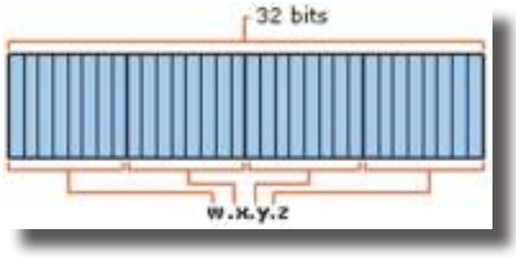
Formato binário	Notação decimal com ponto
11000000 10101000 00000011 00011000	192.168.3.24

Por exemplo, o endereço IPv4 11000000101010000000001100011000 é:

- Segmentado em blocos de 8 bits: 11000000 10101000 00000011 00011000.
- Cada bloco é convertido em decimal: 192 168 3 24
- Os octetos adjacentes são separados por um ponto: 192.168.3.24.

A notação *w.x.y.z*é usada como referência a um endereço IP generalizado e é mostrada na figura a seguir.

Endereço IP



Tipos de endereço IPv4

Os padrões da Internet definem os seguintes tipos de endereço IPv4:

- *Unicast.* Atribuído a uma única interface de rede localizada em uma sub-rede específica na rede e usado para comunicações um-para-um.
- *Multicast*. Atribuído a uma ou mais interfaces de rede localizadas em diversas sub-redes na rede e usado para comunicações um-para-muitos.
- *Difusão*. Atribuído a todas as interfaces de rede localizadas em uma sub-rede na rede e usado para comunicações um-para-todos em uma sub-rede.

Endereços IPv4 unicast

O endereço IPv4 unicast identifica um local da interface na rede da mesma forma que um endereço de rua identifica uma casa em um quarteirão da cidade. Assim como um endereço de rua deve identificar uma residência exclusiva, um endereço IPv4 unicast deve ser um identificador global exclusivo para a rede e ter um formato uniforme.

Cada endereço IPv4 unicast inclui uma ID de rede e uma ID de host.

- A ID de rede (também conhecida como endereço de rede) é a parte fixa de um endereço IPv4 unicast que identifica o conjunto de interfaces que estão localizadas no mesmo segmento de rede física ou lógica conforme delimitado pelos routers IPv4. Um segmento de rede nas redes TCP/IP também é conhecido como sub-rede. Todos os sistemas na mesma sub-rede física ou lógica devem usar a mesma ID de rede e a ID de rede deve ser exclusiva para toda a rede TCP/IP.
- A ID de host (também conhecida como endereço de host) é a parte variável de um endereço IPv4 unicast que é usada para identificar a interface de um nó da rede em uma sub-rede. A ID de host deve ser exclusiva para a ID de rede.

Se a ID de rede for exclusiva para a rede TCP/IP e a ID de host for exclusiva para a ID de rede, então todo o endereço IPv4 unicast composto pela ID de rede e ID de host será exclusivo para toda a rede TCP/IP.

Endereços IPv4 multicast

Os endereços IPv4 multicast são usados para entrega de pacote único um-para-muitos. Em uma intranet habilitada para IPv4 multicast, um pacote IPv4 endereçado a um endereço IPv4 multicast é encaminhado pelos routers às sub-redes em que há hosts escutando o tráfego enviado ao endereço IPv4 multicast. O IPv4 multicast oferece um serviço eficiente de entrega um-para-muitos para diversos tipos de comunicação.

Os endereços IPv4 multicast são definidos pela classe D de endereço de Internet: 224.0.0.0/4. Os endereços IPv4 multicast variam de 224.0.0.0 a 239.255.255.255. Os endereços IPv4 multicast para o prefixo de endereço 224.0.0.0/24 (224.0.0.0 a 224.0.0.255) são reservados pra o tráfego de multicast da sub-rede local.

Endereços IPv4 de difusão

O IPv4 usa um conjunto de endereços de difusão para fornecer um serviço de entrega um-para-todos na sub-rede. Os pacotes enviados aos endereços IPv4 de difusão são processados por todas as interfaces na sub-rede. Estes são os diferentes tipos de endereço IPv4 de difusão:

- *Difusão de rede*. Formado pela configuração de todos os bits do host como 1 para um prefixo de endereço com classificação. Um exemplo de um endereço de difusão de rede para a ID de rede com classificação 131.107.0.0/16 é 131.107.255.255. As difusões de rede são usadas para enviar pacotes a todas as interfaces de uma rede com classificação. Os routers IPv4 não encaminham pacotes de difusão de rede.
- *Difusão de sub-rede*. Formado pela configuração de todos os bits do host como 1 para um prefixo de endereço sem classificação. Um exemplo de endereço de difusão de rede para a ID de rede sem classificação ID 131.107.26.0/24 é 131.107.26.255. As difusões de sub-rede são usadas para enviar pacotes a todos os hosts de uma rede sem classificação. Os routers IPv4 não encaminham pacotes de difusão de sub-rede. Para um prefixo de endereço com classificação, não há endereço de difusão de sub-rede, apenas um endereço de difusão de rede. Para um prefixo de endereço sem classificação, não há endereço de difusão de rede, apenas um endereço de difusão de sub-rede.
- *Difusão direcionada a todas as sub-redes*. Gerado configurando todos os bits do host de ID de rede com classificação original como 1 para um prefixo de endereço sem classificação. Um pacote endereçado à difusão direcionada a todas as sub-redes foi definido para ter acesso a todos os hosts em todas as sub-redes de uma ID de rede baseada em classe dividida em sub-redes. Um exemplo de um endereço de difusão direcionado a todas as sub-redes para a ID de rede dividida em sub-redes 131.107.26.0/24 é 131.107.255.255. A difusão direcionada a todas as sub-redes corresponde ao endereço de difusão de rede da ID de rede com classificação original. Os routers IPv4 podem encaminhar todos os pacotes de difusão direcionada a todas as sub-redes; porém, o uso do endereço de difusão direcionada a todas as sub-redes é desaprovado no RFC 1812.

- *Difusão limitada*. Gerado configurando todos os 32 bits do endereço IPv4 como 1 (255.255.255.255). O endereço de difusão limitada é usado para entrega um-para-todos na sub-rede local quando a ID da rede local é desconhecida. Tipicamente, os nós IPv4 usam apenas o endereço de difusão limitada durante um processo de configuração automática como um protocolo BOOTP ou DHCP. Por exemplo, com o DHCP, um cliente DHCP deve usar o endereço de difusão limitada para todo o tráfego enviado até que o servidor DHCP confirme o uso da configuração de endereço IPv4 oferecida. Os routers IPv4 não encaminham pacotes de difusão limitada.

Classes de endereços IP

A comunidade da Internet definiu cinco classes de endereços. Os endereços das classes A, B, C, D e E são usados para atribuição aos nós TCP/IP.

A classe de endereços define os bits usados nas partes referentes à identificação de rede e de host de cada endereço. A classe de endereço também define o número de redes e de hosts por rede para os quais se pode oferecer suporte.

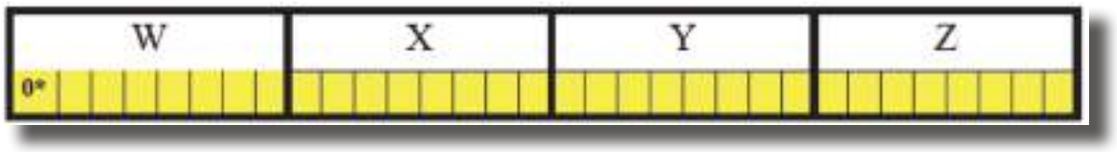
A tabela a seguir usa w.x.y.z para designar os valores dos quatro octetos em qualquer endereço IP. Ela é usada para mostrar:routing

- Como o valor do primeiro octeto (*w*) de qualquer endereço IP indica de forma eficaz a classe de endereço.
- Como os octetos de um endereço são divididos na identificação da rede e do host.
- O número possível de redes e hosts por rede disponível para cada classe.

Classe	Valor de w	Identificação da rede	Identificação do host	Número de redes	Número de hosts por rede
A	1-126	w	x.y.z	126	16,777,214
B	128-191	w.x	y.z	16,384	65,534
C	192-223	w.x.y	z	2,097,152	254
D	224-239	Reservado para endereçamento de multicast	N/D	N/D	N/D
E	240-254	Reservado para uso experimental	N/D	N/D	N/D

Classe A

Inicia-se com 0 (zero) como o bit mais significativo (chamados também **MSB**, Most Significant Bits). Os próximos 7 bits de um endereço de Classe A identificam a rede e os restantes 24 bits são usados para endereçar o host. Portanto, numa rede de Classe A pode haver um host 224. Não é fácil, todavia, para uma empresa ou para uma universidade obter um endereço de Classe A completo.



*Bit mais significativo

Classe B

Iniciam-se com 10 (dez) como os bits mais significativos. Os próximos 14 bits identificam a rede e os restantes 16 bits servem para endereçar os hosts (mais de 65.000). Os endereços de Classe B, que já foram muito comuns para empresas e universidades, são hoje muito difíceis de obter por causa da atual escassez de endereços IPv4 disponíveis.

Retornando ao exemplo anterior, pode-se ver que o host 132.199.15.99 (ou o equivalente hexadecimal 0x84c70f63) encontra-se em uma rede de Classe B, já que 0x84 = 1000... (em binário).

Portanto, o endereço 132.199.15.99 pode ser dividido na parte de rede que é 132.199.0.0 e na parte do host que é 15.99.

Classe C

É identificada pelos bits mais significativos iguais a 110, permitindo apenas 256 hosts em cada uma das 221 possíveis redes de Classe C (na realidade, o número de hosts possíveis é 254). Os endereços de Classe C são mais comumente encontrados em pequenas empresas.

Existe também uma série de endereços que se iniciam com “111”, e que são muito usados para outros fins (por exemplo, multicast).

Observe que os bits utilizados para identificar a rede fazem, não obstante, parte do próprio endereço de rede.

Quando se separa à parte de rede da parte de host é comodo utilizar a assim chamada netmask (máscara de rede). Trata-se de um valor a ser usado como "máscara", em que todos os bits de rede são assentados em "1" e todos os bits de host em "0". Pondo juntos com um AND lógico o endereço com a netmask obtém-se o endereço da rede.
Reportando-se ao exemplo anterior, 255.255.0.0 é uma possível netmask de 132.199.15.99. Quando se aplica a netmask ao endereço, permanece a parte de rede 132.199.0.0. Para os endereços em notação CIDR, o número indicado de bits de rede especifica também quais dos bits mais significativos devem ser postos em "1" para se obter a netmask da rede correspondente.

Para os endereços de rede Classe A/B/C existe uma netmask default (Máscara de Sub-Rede Padrão) é usada quando a rede em questão não tem necessidade de ser dividida, ou seja, segmentada:

- Classe A (/8): netmask default (padrão): 255.0.0.0, primeiro byte do endereço: 1-127 .
- Classe B (/16): netmask default (padrão): 255.255.0.0, primeiro byte do endereço: 128-191.
- Classe C (/24): netmask default (padrão): 255.255.255.0, primeiro byte do endereço: 192-223.

Um tipo particular de endereço que é bom conhecer é o endereço de broadcast. As mensagens enviadas a este endereço são recebidas por todos os hosts da rede correspondente. O endereço de broadcast é caracterizado pelo fato de ter todos os bits de host colocados em "1".

Por exemplo, dado o endereço 132.199.15.99 com a máscara de rede 255.255.0.0, o endereço de broadcast é 132.199.255.255.
Assim se perguntarmos se podemos utilizar um endereço de host com todos os bits em "0" ou em "1".

A resposta é não, porque o primeiro é o endereço da rede e o segundo, o endereço de broadcast, e estes dois endereços devem estar sempre presentes. Agora pode-se compreender porque uma rede de Classe B pode conter no máximo 216-2 = 65.534 hosts, e uma rede de Classe C pode conter 28-2 = 254.

Além dos vários tipos de endereço já citados, há um outro que é especial. Trata-se do endereço 127.0.0.1, que se refere sempre ao host local (localhost). Isso significa que quando se "fala" com o 127.0.0.1, comunica-se na realidade consigo mesmo, sem dar lugar a nenhuma atividade de rede, o que pode ser útil ao usar os serviços instalados na própria máquina ou para fazer simulações e testes quando não há outro host na rede.

Classe D

É identificada pelos bits mais significativos iguais a 1110, não utilizado para numerar redes, e sim para aplicações multicast (O tráfego da rede destinado a um conjunto de hosts que pertencem a um grupo de difusão seletiva).

Classe E

Esta classe foi definida como tendo os quatro primeiros bits do número IP como sendo sempre iguais a 1, 1, 1 e 1. A classe E é uma classe especial e está reservada para uso futuro.

Resumo para as Classes de Endereços

Os endereços IP foram divididos em classes para facilitar a comutação de pacotes. Nesta divisão, um endereço de classe A por exemplo tem o seu primeiro octeto reservado para o endereço de rede e os demais são utilizados para as máquinas, já no endereço classe B, temos os dois primeiros octetos reservados para a rede e os demais para as máquinas, no endereço de classe C os três primeiros octetos são reservados para a rede e somente o último octeto para as máquinas. Isto significa que os endereços de classe C são usados por pequenas redes, até o limite de 256 computadores (utilizando somente um endereço

de classe C), já os endereços de classe B, são para redes maiores suportando até 65.536 computadores na mesma rede e os de classe A suportam até 1.6777.216. Existem ainda os endereços de Classe D que são utilizados para enviar mensagens multicasting (uma mensagem enviada através de um único endereço IP para vários destinatários) e o broadcasting (uma mensagem enviada através de um único endereço IP para todos os destinatários de uma determinada rede). A faixa de endereços IP de cada classe é mostrada na Tabela a seguir.

De	até	Classe de Endereço
0	126	A
128	191	B
192	223	C
224	239	D
240	247	E

Na figura a seguir é apresentada cada classe com a sua respetiva representação binária e a quantidade de Host (Computadores) que podem estar ligados dentro daquela classe de endereços.

A tabela em baixo ilustra as classes de endereços com as suas faizas decimais e a sua representação binária

Classe	Faixa de Endereços	Representação Binária	Utilização
A	1-126.X.X.X	0nnnnnnn.hhhhhhhh.hhhhhhhh.hhhhhhhh	
B	128-191.X.X.X	10nnnnnn.nnnnnnnn.hhhhhhhh.hhhhhhhh	
C	192-223.X.X.X	110nnnnn.nnnnnnnn.nnnnnnnn.hhhhhhhh	
D	224-239.X.X.X	1110xxxx.xxxxxxxx.xxxxxxxx.xxxxxxxx	Multicast/ Broadcast
E	240-247.X.X.X	11110xxx.xxxxxxxx.xxxxxxxx.xxxxxxxx	Reservado

Onde,

X é um número que varia de 0 à 255.

n é o número de bits da rede.

h é o número de bits do host.

x é o número de bits da rede e do host.

Endereço Loopback

Observe que o endereço 127.X.X.X não é mostrado na tabela acima, isto porque este endereço foi reservado para Loopback.

Por convenção, toda a máquina que trabalhe com TCP/IP possuí uma interface de Loopback, além das interfaces de rede que possui. Esta interface não liga a nenhuma rede. O seu objetivo é permitir teste de comunicação interprocessos dentro da mesma máquina.

Quando um programa usa o endereço de loopback para enviar dados, o software do protocolo retorna o dado sem gerar tráfego na rede (isto é muito utilizado para testar programas, inclusive quando não se tem placa de rede). A comunicação vai pelo caminho normal, saindo do nível de aplicação, passando pelo nível de transporte (TCP ou UDP) e chegando ao nível IP, que retorna a comunicação de volta ao nível de aplicação de um outro processo. A especificação determina que um pacote enviado para a rede 127

nunca deve aparecer em nenhuma rede. O endereço de loopback utilizado pela quase totalidade das implementações é 127.0.0.1.

Endereços IP reservados

Assim como a classe de endereços 127.0.0.0 é reservada para loopback, existem outros endereços reservados que não podem ser utilizados em nenhuma máquina conectada à Internet. Esses endereços são reservados para redes que nunca se ligarão à Internet ou que se ligarão através de um proxy (assim como as Intranets).Nenhum destes endereços pode ser anunciado, o que quer dizer que se uma máquina for conectada a Internet com algum endereço reservado ela não conseguirá passar pelos gateways core. Os endereços reservados da Internet são especificados pela RFC1597 e são os seguintes:

Rede	Máscara
10.0.0.0	255.0.0.0
172.16.0.0	255.240.0.0
192.168.0.0	255.255.0.0

Endereços Privados e Públicos

Endereços públicos são definidos pela InterNIC e equivalem a um identificador ou IP válidos, reconhecidos mundialmente.

Endereços privados são definidos em TCP/IP como sendo endereços que nunca serão atribuídos pela InterNIC e que podem ser utilizados pelas empresas para numerar os seus hosts internos.

Desta forma uma empresa precisa apenas adquirir IPs públicos para os computadores que estão expostos na Internet, normalmente servidores de Web para publicação da home page, servidores de correio (e-mail), servidores de DNS, etc.

Para numerar os restantes computadores, as empresas podem utilizar IPs de classes privadas.

O IANA (*Internet Assigned Numbers Authority*) reservou os seguintes blocos de IP para as redes privadas.

Classe	Blocos
A	10.0.0.1 até 10.255.255.254
B	172.16.0.1 até 172.31.255.254
C	192.168.0.1 até 192.168.255.254

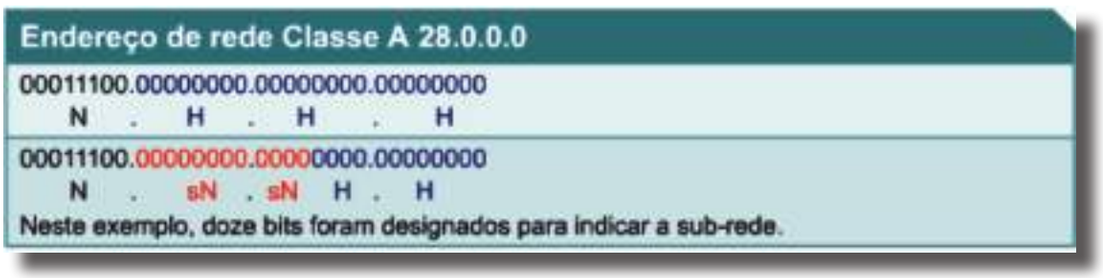
Nunca existirão routers na Internet que contenham rotas para endereços de IP privados, o que garante o uso dos mesmos apenas nas redes locais internas (Intranets).

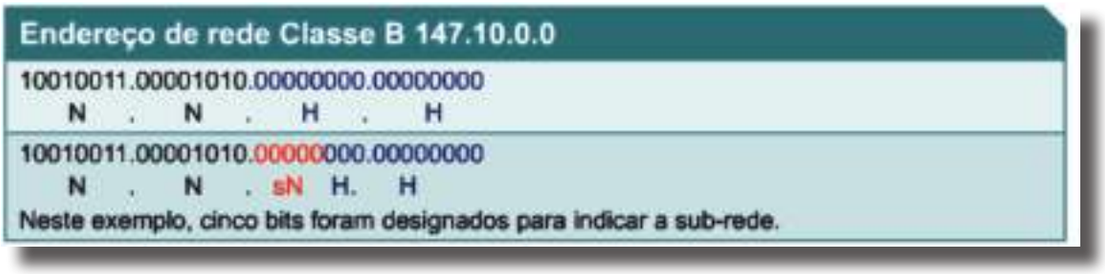
Como última observação, lembramos que é muito comum o uso de IPs privados. As empresas adotam os IPs privados pelo fato deles nunca serem utilizados pele InterNIC e também porque eles nunca serão utilizados para expor computadores na Internet. O seu uso só tem sentido na rede interna.

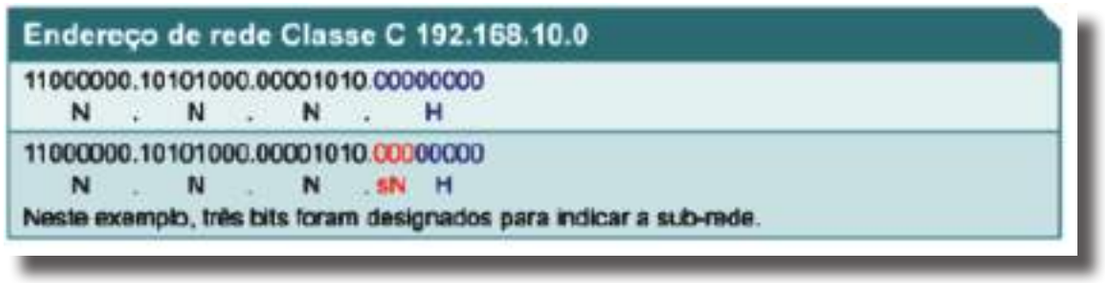
Introdução às Sub-Redes

Para criar a estrutura de sub-redes, os bits do host devem ser reatribuídos como bits da sub-rede. Esse processo é frequentemente chamado "'pedir emprestado"' bits. No entanto, um termo mais preciso seria "'emprestar"' bits. O ponto de partida para este processo é sempre o bit do host mais à esquerda, aquele mais próximo ao último octeto da rede.

Os endereços de sub-rede incluem a parte da rede de classe A, classe B e classe C, mais um campo de sub-rede e um campo de host. O campo da sub-rede e o campo do host são criados da parte original do host do endereço IP principal. Isso é feito com a atribuição de bits da parte do host à parte de rede original do endereço. A capacidade de dividir a parte do host original do endereço nos novos campos de sub-rede e de host proporciona flexibilidade de endereçamento ao administrador da rede.







Além da necessidade de gestão, a divisão em sub-redes permite que o administrador da rede ofereça contenção de broadcast e segurança nos níveis inferiores na rede local. Ela proporciona alguma segurança, pois o acesso a outras sub-redes está disponível somente através dos serviços de um router.

Além disso, a segurança de acesso pode ser proporcionada com o uso de listas de acesso. Essas listas podem permitir ou negar acesso a uma sub-rede com base em diversos critérios, proporcionando, assim, mais segurança. Alguns proprietários de redes das classes A e B também descobriram que a divisão em sub-redes cria uma fonte de lucros para a organização através do aluguer ou da venda de endereços IP não usados anteriormente.

A divisão em sub-redes é um função interna à rede. Para fora da rede, uma LAN é vista como uma única rede sem que sejam apresentados detalhes da estrutura da rede interna. Esta visão da rede mantém as tabelas de routing pequenas e eficientes. Dado o endereço do nó local 147.10.43.14, pertencente à sub-rede 147.10.43.0, o mundo externo à LAN vê apenas o número anunciado da rede principal 147.10.0.0.

A razão para isso é que o endereço da sub-rede 147.10.43.0 é utilizado apenas dentro da LAN à qual a sub-rede pertence.

Estabelecimento do endereço da máscara de sub-rede

A seleção do número de bits a serem usados no processo de sub-redes dependerá do número máximo de hosts exigido por sub-rede. É necessária alguma compreensão de números binários e de valores de posição dos bits em cada octeto ao calcular o número de sub-redes e de hosts criados quando esse bit foi tomado por empréstimo.

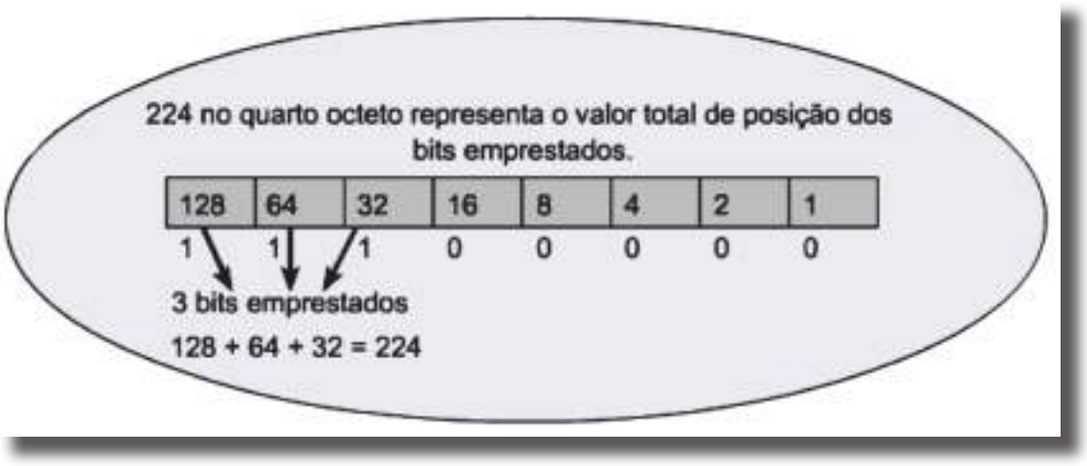
Bits emprestados	1	2	3	4	5	6	7	8
Valor	128	64	32	16	8	4	2	1

Os dois últimos bits do último octeto, independentemente da classe de endereço IP, jamais poderão ser atribuídos à sub-rede. Eles são chamados de os últimos dois bits significativos. O uso de todos os bits disponíveis para criar sub-redes, exceto esses dois últimos, resultará em sub-redes com apenas dois hosts utilizáveis. Esse é um método prático de conservação de endereços para o endereçamento de links de routers serie. No entanto, para uma rede local em funcionamento, ele resultaria em custos proibitivos de equipamento.

A máscara de sub-rede fornece ao router as informações necessárias para determinar em que rede e sub-rede um host específico reside. A máscara de sub-rede é criada com o uso de 1s binários nas posições dos bits relativos à rede. Os bits da sub-rede são determinados com a adição do valor às posições dos bits tomados por empréstimo. Se tivessem sido tomados três bits, a máscara para um endereço de classe C seria 255.255.255.224. Essa máscara também pode ser representada, no formato de barras, como /27. O número após a barra é o total de bits usados para a parte da rede e da sub-rede.

Formato com barras	/25	/26	/27	/28	/29	/30	N/A	N/A
Máscara	128	192	224	240	248	252	254	255
Bits emprestados	1	2	3	4	5	6	7	8
Valor	128	64	32	16	8	4	2	1

Um endereço classe C com máscara /25 pede emprestado apenas um bit, como apresentado na tabela acima. Entretanto, um endereço classe B com uma máscara /25 pede emprestado 9 bits .



Para determinar o número de bits a serem usados, o projetista da rede precisa calcular quantos hosts a maior sub-rede requer e o número necessário de sub-redes. Por exemplo, a rede precisa de 6 sub-redes com 25 hosts cada. Uma maneira de determinar a quantidade de bits que devem ser emprestados é através da tabela de sub-redes. Consultando a linha “Sub-redes Utilizáveis”, a tabela indica que para ter seis sub-redes são necessários 3 bits adicionais na máscara de sub-rede.

A tabela mostra que desta forma são criados 30 hosts utilizáveis por sub-rede, o que irá satisfazer os requisitos deste esquema. A diferença entre hosts utilizáveis e total de hosts resulta do uso do primeiro endereço disponível como ID e do último endereço disponível como broadcast para cada sub-rede. Tomar emprestado o número apropriado de bits para acomodar o número necessário de sub-redes e de hosts por sub-rede pode ser resultado de um ato de balanceamento, que pode resultar em endereços de host não utilizados em múltiplas sub-redes.

O método usado para criar a tabela de sub-redes pode ser usado para resolver todos os problemas da divisão em sub-redes. Esse método usa a seguinte fórmula:

Formato com barras	/25	/26	/27	/28	/29	/30	N/A	N/A
Máscara	128	192	224	240	248	252	254	255
Bits emprestados	1	2	3	4	5	6	7	8
Valor	128	64	32	16	8	4	2	1
Total de Sub-redes		4	8	16	32	64		
Sub-redes Utilizáveis		2	6	14	30	62		
Total de Hosts		64	32	16	8	4		
Hosts Utilizáveis		62	30	14	6	2		

Número de sub-redes utilizáveis = dois elevado ao número de bits de sub-rede atribuídos ou pedidos emprestados, menos dois. O menos dois é dos endereços reservados para ID da rede e de broadcast da rede.

(2 núm. de bits emprestados) – 2 = sub-redes utilizáveis

(2^3) – 2 = 6

Número de hosts utilizáveis = dois elevado ao número de bits restantes menos dois (endereços reservados para ID da sub-rede e broadcast da sub-rede).

(2 núm. de bits restantes) – 2 = hosts utilizáveis

(2^5) – 2 = 30

Aplicação da máscara de sub-rede

Uma vez estabelecida a máscara de sub-rede, ela pode ser usada para criar o esquema de sub-redes. A tabela apresentada na figura é um exemplo das sub-redes e endereços criados pela atribuição de três bits ao campo de sub-rede. Isso criará oito sub-redes com 32 hosts por sub-rede. Ao numerar sub-redes, comece com zero (0). A primeira sub-rede é sempre chamada sub-rede zero.

No. da sub-rede	ID da sub-rede	Intervalo de Hosts	ID do broadcast
0	192.168.10.0	.1--.30	192.168.10.31
1	192.168.10.32	.33--.62	192.168.10.63
2	192.168.10.64	.65--.94	192.168.10.95
3	192.168.10.96	.97--.126	192.168.10.127
4	192.168.10.128	.129--.158	192.168.10.159
5	192.168.10.160	.161--.190	192.168.10.191
6	192.168.10.192	.193--.222	192.168.10.223
7	192.168.10.224	.225--.254	192.168.10.255

Quando se preenche a tabela de sub-redes, três dos campos são automáticos; os outros exigem cálculos. A ID da sub-rede zero é igual ao número da rede principal, sendo, neste caso, 192.168.10.0. A ID de broadcast para toda a rede é o maior número possível, sendo, neste caso, 192.168.10.255. O terceiro número fornecido é a ID de sub-rede para a sub-rede número sete. Esse número reflete os três octetos da rede com o número da máscara de rede inserido na quarta posição do octeto. Foram atribuídos três bits ao campo de sub-rede com valor cumulativo 224. A ID para a sub-rede sete é 192.168.10.224. Com a inserção desses números, foram estabelecidos pontos de verificação, que verificarão a precisão quando a tabela for concluída.

Formato com barras	/25	/26	/27	/28	/29	/30	N/A	N/A
Máscara	128	192	224	240	248	252	254	255
Bits emprestados	1	2	3	4	5	6	7	8
Valor	128	64	32	16	8	4	2	1
Total de Sub-redes		4	8	16	32	64		
Sub-redes Utilizáveis		2	6	14	30	62		
Total de Hosts		64	32	16	8	4		
Hosts Utilizáveis		62	30	14	6	2		

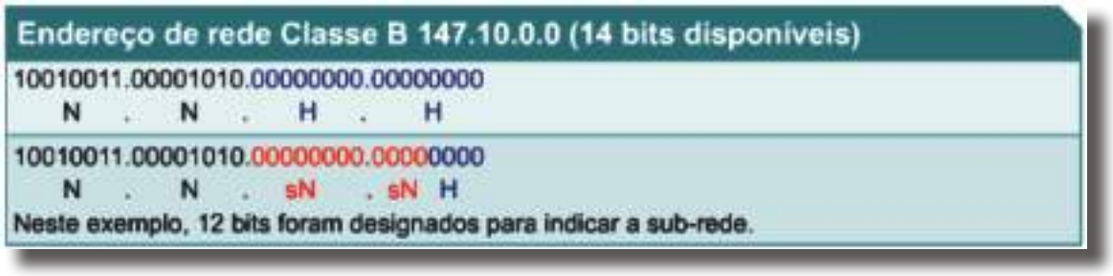
Consultando-se a tabela de divisão em sub-redes ou utilizando-se a fórmula, os três bits atribuídos ao campo de sub-rede resultarão no total de 32 hosts atribuídos a cada sub-rede. Essas informações fornecem a contagem de etapas para cada ID de sub-rede. Adicionando-se 32 a cada número precedente, começando com a sub-rede zero, é estabelecida a ID para cada sub-rede. Observe que a ID de sub-rede tem todos os 0s binários na parte do host.

O campo de broadcast é o último número em cada sub-rede e tem todos os uns binários na parte do host. Esse endereço pode fazer broadcast apenas para os membros de uma única sub-rede. Como a ID de sub-rede para a sub-rede zero é 192.168.10.0 e há um total de 32 hosts, a ID de broadcast será 192.168.10.31. Começando em zero, o 32o número seqüencial será 31. É importante lembrar que zero (0) é um número real no mundo das redes.

O equilíbrio da coluna de ID de broadcast pode ser obtido com o mesmo processo usado na coluna de ID de sub-rede. Simplesmente, adicione 32 à ID de broadcast precedente da sub-rede. Outra opção é começar na parte inferior e preencher até o alto da coluna, subtraindo um da ID de sub-rede precedente.

Divisão de redes das classes A e B em sub-redes

O procedimento de divisão em sub-redes das classes A e B é idêntico ao da classe C, exceto que pode envolver um número significativamente maior de bits. O número de bits disponíveis para atribuição ao campo de sub-rede em um endereço de Classe A é 22, enquanto um endereço de classe B tem 14 bits.



Endereço de rede Classe A 28.0.0.0 (22 bits disponíveis)
00011100.00000000.00000000.00000000 N . H . H . H
00011100.00000000.00000000.00000000 N . sN . sN . sN H Neste exemplo, 20 bits foram designados para indicar a sub-rede.

A atribuição de 12 bits de um endereço de classe B ao campo de sub-rede cria uma máscara de sub-rede 255.255.255.240, ou /28. Todos os oito bits foram atribuídos no terceiro octeto, resultando em 255, valor total dos oito bits. Quatro bits foram atribuídos no quarto octeto, resultando em 240. Lembre-se que, a máscara com barra é a soma total dos bits atribuídos à sub-rede mais os bits fixos da rede.

Máscara	128	192	224	240	248	252	254	255
Bits Emprestados	1	2	3	4	5	6	7	8
Valor	128	64	32	16	8	4	2	1
Sub-redes	2	4	8	16	32	64	128	256

A atribuição de 20 de um endereço de classe A ao campo de sub-rede cria uma máscara de sub-rede 255.255.255.240, ou /28. Todos os oito bits dos segundo e terceiro octetos foram atribuídos ao campo de sub-rede e quatro bits do quarto octeto.

Dois levado à potência de	É igual a
0	1
1	2
2	4
3	8
4	16
5	32
6	64
7	128
8	256
9	512
10	1024
11	2048
12	4096
13	8192
14	16384
15	32768

Nessa situação, é visível que a máscara de sub-rede para os endereços das classes A e B parece idêntica. A menos que a máscara esteja relacionada a um endereço de rede, não é possível saber quantos bits foram atribuídos ao campo de sub-rede.

Qualquer que seja a classe de endereço a ser dividida em sub-redes, as regras a seguir são as mesmas:

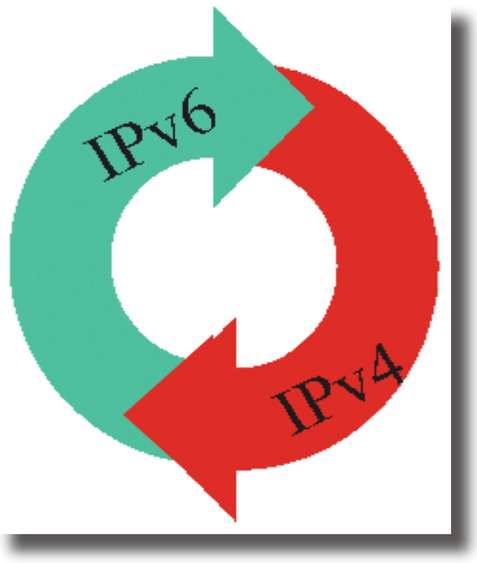
Total de sub-redes = 2 elevado ao número de bits tomados por empréstimo

Total de hosts= 2 elevado ao número de bits restantes

Sub-redes utilizáveis = 2 elevado ao número de bits tomados por empréstimo **menos 2**

Hosts utilizáveis= 2 elevado ao número de bits restantes **menos 2**

IPV4 x IPV6



O protocolo IPv4 é a tecnologia que está por trás da rede mundial Internet. O rápido crescimento da Internet tem esgotado esta tecnologia e muitos esforços têm sido feitos para a sua evolução. Entre as limitações apresentadas pelo IPv4, podemos destacar o uso de endereços compostos por 32 bits divididos em classes. IPv6 é uma nova versão do protocolo IP, projetado como uma evolução do IPv4. O IPv6 resolve muitos dos problemas presentes no IPv4 e inclui melhorias, como o uso de endereços hierárquicos e suporte a novas facilidades de routing que possibilitarão o contínuo crescimento da Internet.

As máquinas atualmente interligadas através da Internet têm endereços que as identificam de forma única. Estes endereços são compostos por 32 bits. Os primeiros bits são usados para identificar a rede onde a máquina se encontra e o restante é usado para identificar a própria máquina na rede. Por exemplo, no endereço 164.41.14.1, os digitos 164.41 identificam a rede, enquanto os digitos 14.1 identificam a máquina na rede.

Para melhorar a sua distribuição, os endereços foram agrupados em classes. Cada classe utiliza um número diferente de bytes para identificar a rede (classe A - 1 byte, classe

B - 2 bytes e classe C - 3 bytes). O número restante de bytes é usado para identificar a máquina na rede. Na realidade, em qualquer uma das classes, o primeiro byte não é integralmente usado para identificar a rede, pois parte do byte é usada para identificar a classe à qual o endereço pertence.

Através da divisão em classes, é possivel endereçar uma quantidade razoável de redes. O problema, entretanto, ocorre devido à grande requisição de endereços classe B. Esta procura deve-se ao fato de que o número total de máquinas que podem ser interligadas através de uma rede classe C é relativamente pequeno.

Diante dos problemas decorrentes do uso do protocolo IPv4, desde 1991 a Internet Engineering Task Force (IETF), organização responsável pelos padrões dos protocolos usados na Internet, tinha como objetivo evoluir o protocolo. O novo protocolo deveria resolver o esgotamento da capacidade de endereçamento, ser eficiente no roteamento, flexivel e transparente às aplicações dos utilizadores. Após inúmeros esforços, foi definido o protocolo IPv6.

Este protocolo é uma nova versão do protocolo IPv4. Ao mesmo tempo que mantém a compatibilidade com a versão anterior, resolve vários de seus problemas. Suporta endereços hierárquicos de grande tamanho (128 bits) e apresenta novas facilidades de routing. O tamanho do espaço de endereçamento passa a ser enorme: bilhões de vezes o tamanho do espaço de endereçamento do IPv4. Apesar do tamanho ser, na prática, menor do que o valor teórico, pois a atribuição e o routing de endereços segue uma organização hierárquica, estima-se que estejam disponíveis 1.564 endereços para cada metro quadrado da superfície da Terra!

Obter um endereço IP

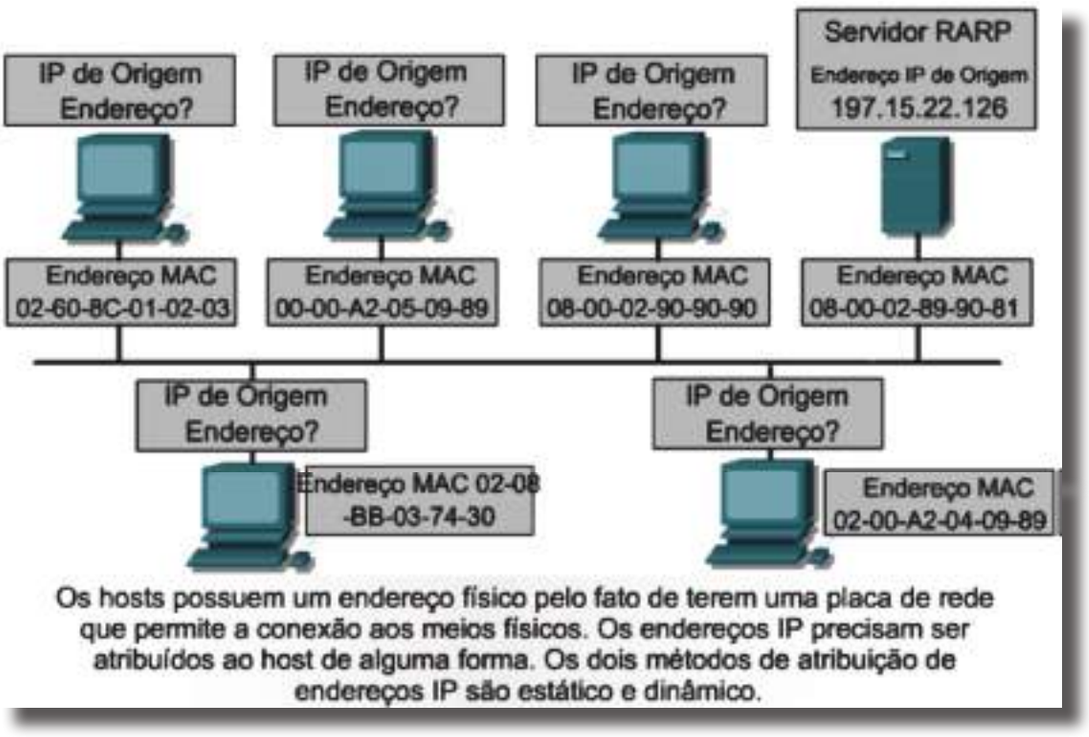
Obtendo um endereço da Internet

Para um prestador de serviço adquirir uma faixa de endereços IP, precisa enviar uma solicitação a uma entidade controladora, como a Comissão Gestora, enviando as características do projeto de expansão que demonstrem claramente as necessidades.

Os prestadores de serviço, como as Operadoras de Telecomunicações, repassam blocos destes endereços para os seus clientes (empresas). E utilizam parte da faixa recebida para fornecer serviços como IP sobre ADSL, IP RDIS, etc..

Cada host precisa de um endereço único para poder funcionar na Internet.

Os endereços MAC dos hosts têm apenas significado local, identificando o host dentro da Rede Local, ou seja como é um endereço da camada 2, o router não o utiliza para encaminhamento fora da LAN.



Para o utilizador final, basta configurar o seu posto de trabalho com a opção de configuração automática (utilizando o protocolo DHCP).

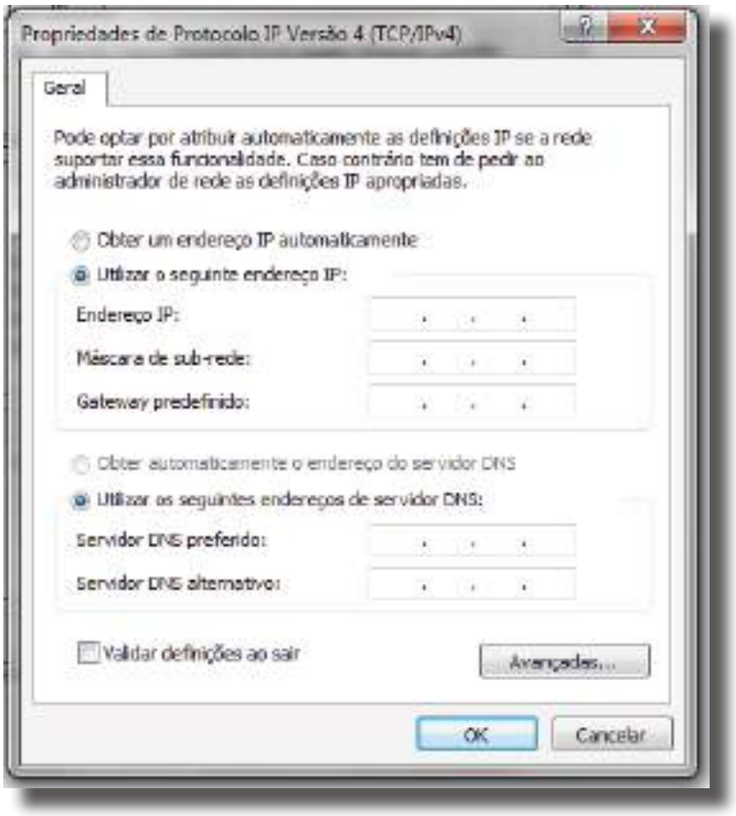
Atribuição estática do endereço IP

Podemos atribuir manualmente um endereço IP a um *host*. Vários tipos de equipamentos suportam esta configuração, a diferença está na forma de executar a entrada dos dados. Alguns sistemas operacionais permitem a configuração gráfica e outros através de linha de comando.

Normalmente, os parâmetros mais comuns a serem configurados são:

- Endereço IP;
- Máscara;
- *Default Gateway;*
- Servidor de DNS.

Para o sistema operacional *Windows* temos:



Atribuição de endereço IP utilizando RARP

O RARP (*Reverse Address Resolution Protocol*) envia um datagrama em broadcast à rede, respondido pelo servidor RARP, que preenche os campos ausentes ou desconhecidos do remetente.

É utilizado principalmente para estacoes *diskless*.

O protocolo RARP associa um endereço MAC conhecido a um endereço IP. É necessário a existência de um servidor RARP para o processamento dos pedidos. Um dispositivo ao arrancar pode desconhecer o seu endereço IP.

- O dispositivo conhece o endereço MAC associado à sua NIC.
- Envia uma mensagem de RARP Request para o endereço de broadcast.
    - Todos os dispositivos da rede recebem e processam o pedido mas só o servidor de RARP responde.
    - Na mensagem de RARP reply vai a indicação do endereço IP atribuído.

Atribuição de endereço IP BOOTP

O protocolo BOOTP (BootStrap) é uma forma alternativa de atribuição de endereços para postos de trabalho *diskless*. Com o propósito similar ao protocolo RARP, o BOOTP pode configurar estes postos de trabalho a partir do *boot* (inicialização da maquina).

O seu funcionamento consiste em:

- O posto de trabalho envia uma solicitação de BOOTP em *broadcast*.
- O servidor responde à solicitação com todas as informações necessárias para o funcionamento do posto de trabalho.

A vantagem do BOOTP, em relação ao RARP, é que pode disponibilizar muito mais informações aos postos de trabalho.

O BOOTP pertence a camada de Aplicação do TCP/IP.

O protocolo BOOTP permite além da obtenção do endereço IP, a obtenção do endereço IP de um router, do endereço IP de um servidor e de alguma informação específica.

- Não fornece atribuição dinâmica de endereços.
    - Um administrador de rede cria um ficheiro de configuração que especifica

os parâmetros de cada dispositivo.

- Significa que cada host tem de ter um perfil BOOTP com uma atribuição de endereço IP.
- Não pode haver dois perfis com o mesmo endereço IP.

Utiliza o UDP para transportar as mensagens.

Gestão de Endereços IP com uso de DHCP

O protocolo DHCP (*Dynamic Host Configuration Protocol*) é utilizado para fornecer as configurações básicas de endereçamento IP e proporcionar o controlo da utilização dos endereços.

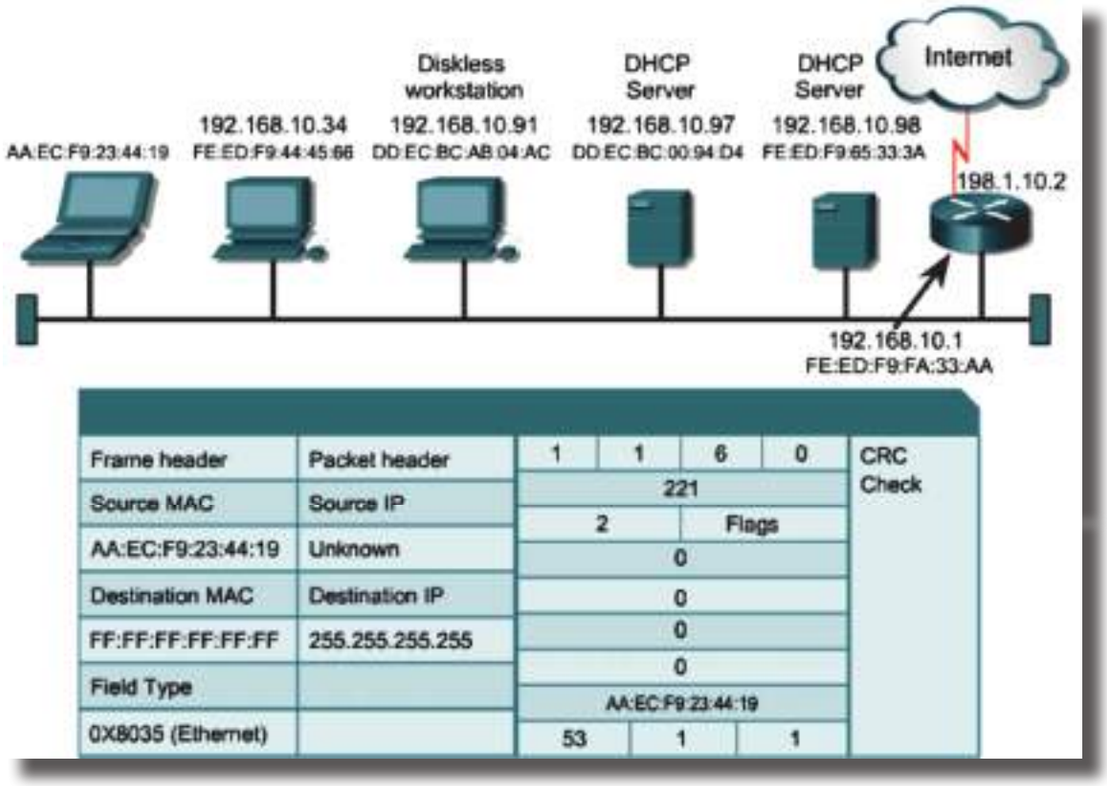
Facilita a configuração dos postos de trabalho, principalmente em redes com grande número de hosts.

O protocolo DHCP é o sucessor do BOOTP.

- O DHCP permite a um host obter um endereço IP dinamicamente sem que o administrador tenha de configurar um perfil individual para cada dispositivo.
- Tudo o que é necessário ao usar o DHCP é um intervalo de endereços IP definido num servidor DHCP.
- Quando os hosts entram em contacto com o servidor DHCP e solicitam um endereço, o servidor DHCP escolhe um endereço e atribui-o a esse host.
- Com o DHCP, toda a configuração de rede de um computador pode ser obtida numa única mensagem.
- Inclui todos os dados fornecidos pela mensagem BOOTP, o endereço IP atribuído e uma máscara de sub-rede.

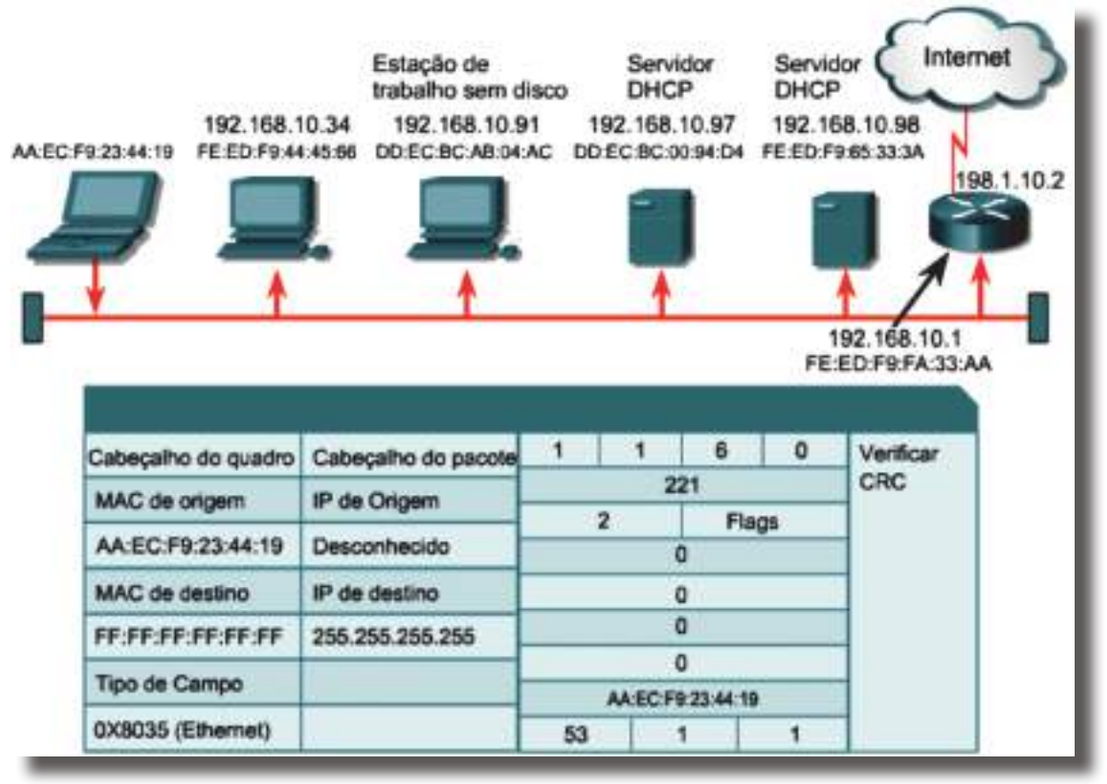
Funcionamento

O computador AA:EC:F9:23:44:19 gera um DHCP request.



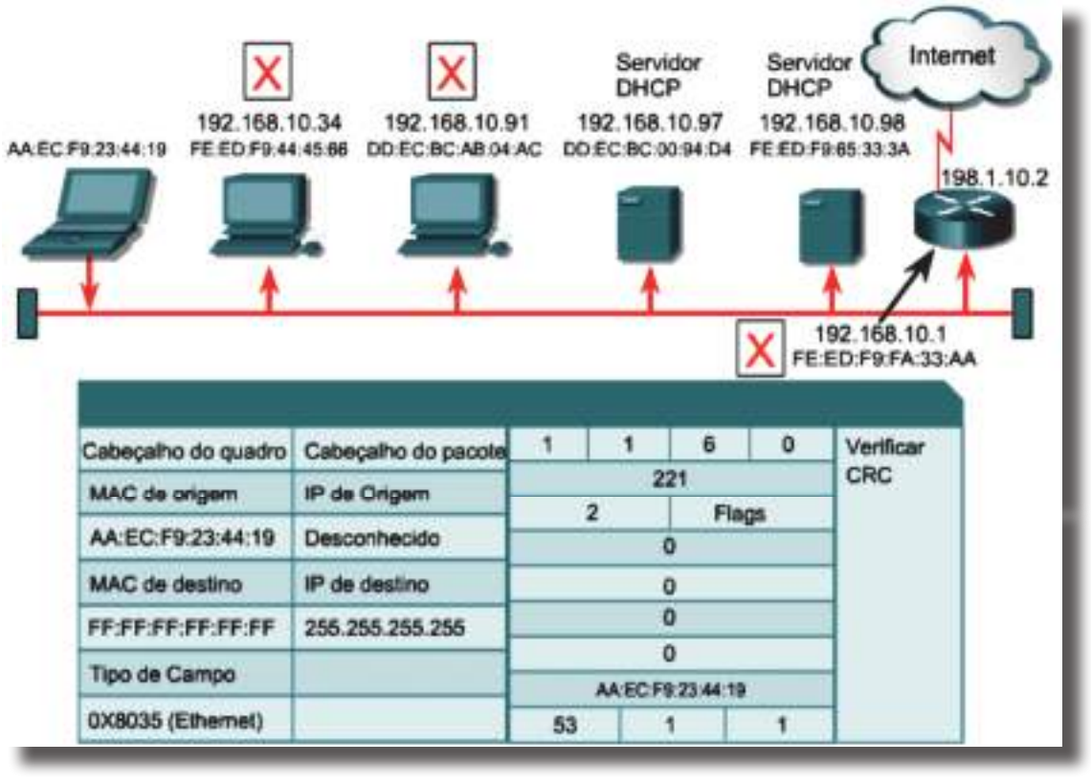
Frame header	Packet header	1	1	6	0	CRC Check
Source MAC	Source IP	221				
AA:EC:F9:23:44:19	Unknown	2	Flags			
Destination MAC	Destination IP	0				
FF:FF:FF:FF:FF:FF	255.255.255.255	0				
Field Type		0				
0X8035 (Ethernet)		AA:EC:F9:23:44:19				
		53	1	1		

O DHCP request é transmitido



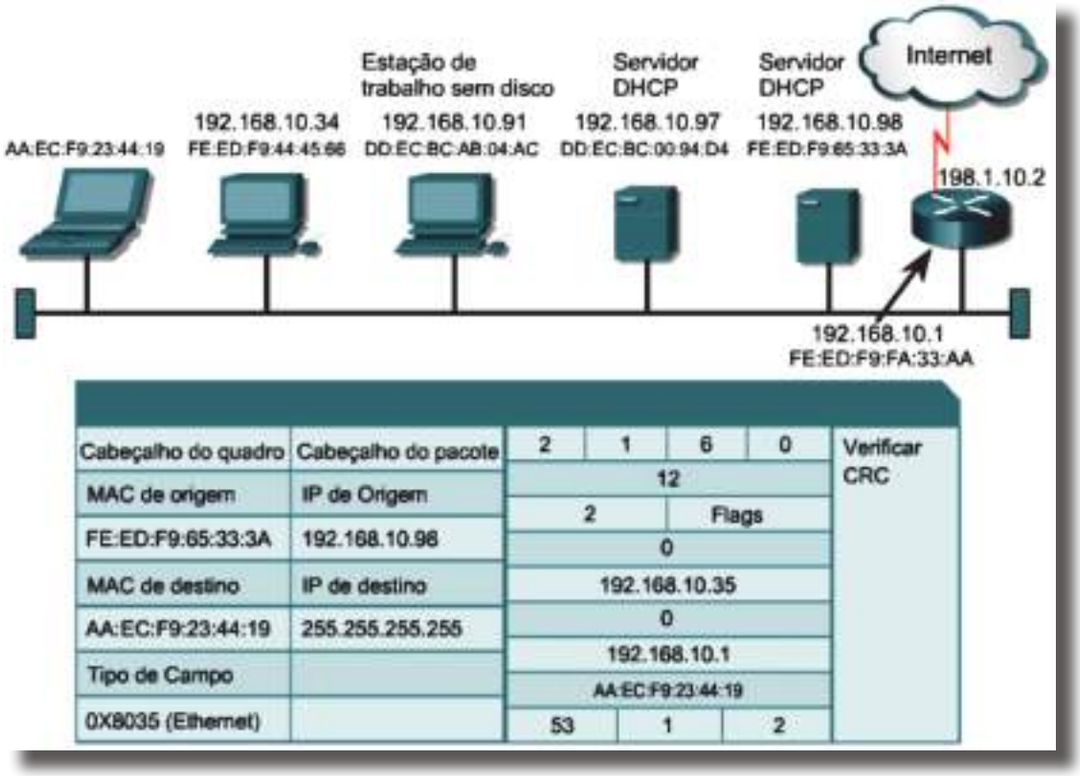
Cabeçalho do quadro	Cabeçalho do pacote	1	1	6	0	Verificar CRC
MAC de origem	IP de Origem	221				
AA:EC:F9:23:44:19	Desconhecido	2	Flags			
MAC de destino	IP de destino	0				
FF:FF:FF:FF:FF:FF	255.255.255.255	0				
Tipo de Campo		0				
0X8035 (Ethernet)		AA:EC:F9:23:44:19				
		53	1	1		

Todos os dispositivos com exceção dos servidores DHCP descartam o pedido.



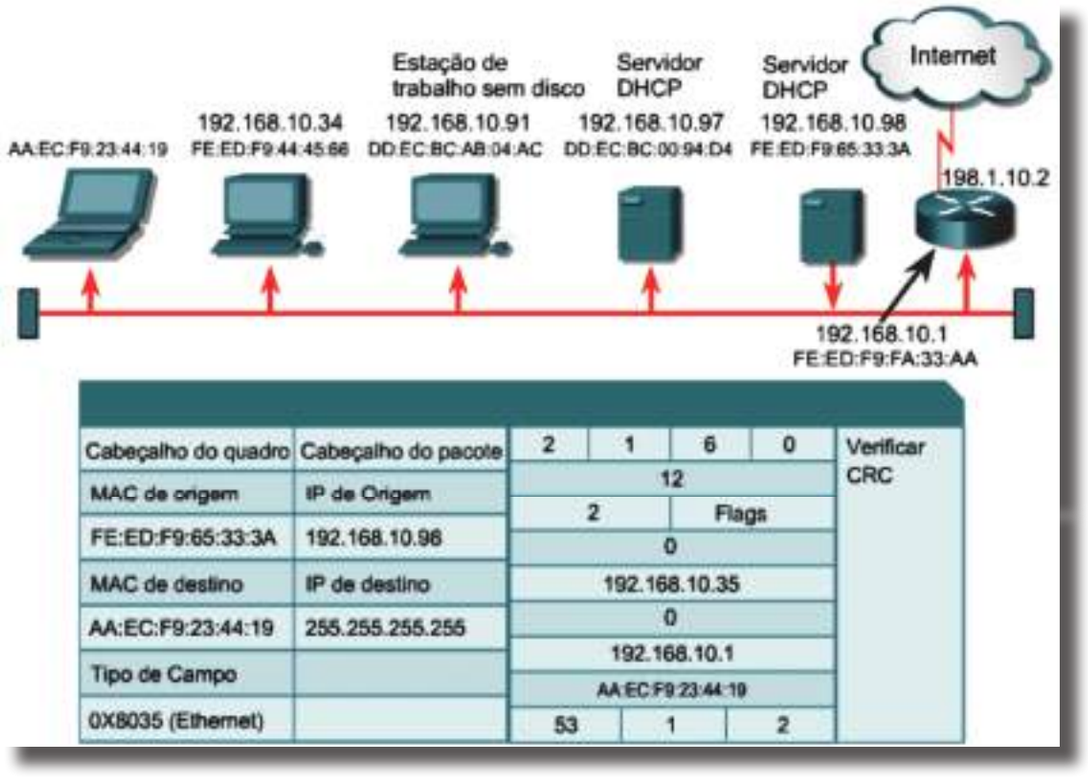
Cabeçalho do quadro	Cabeçalho do pacote	1	1	6	0	Verificar CRC
MAC de origem	IP de Origem	221				
AA:EC:F9:23:44:19	Desconhecido	2	Flags			
MAC de destino	IP de destino	0				
FF:FF:FF:FF:FF:FF	255.255.255.255	0				
Tipo de Campo		0				
0X8035 (Ethernet)		0				
		AA:EC:F9:23:44:19				
		53	1	1		

O servidor prepara um DHCP offer onde é incluído o endereço IP do cliente, o endereço IP do servidor DHCP e o endereço IP do gateway por omissão.

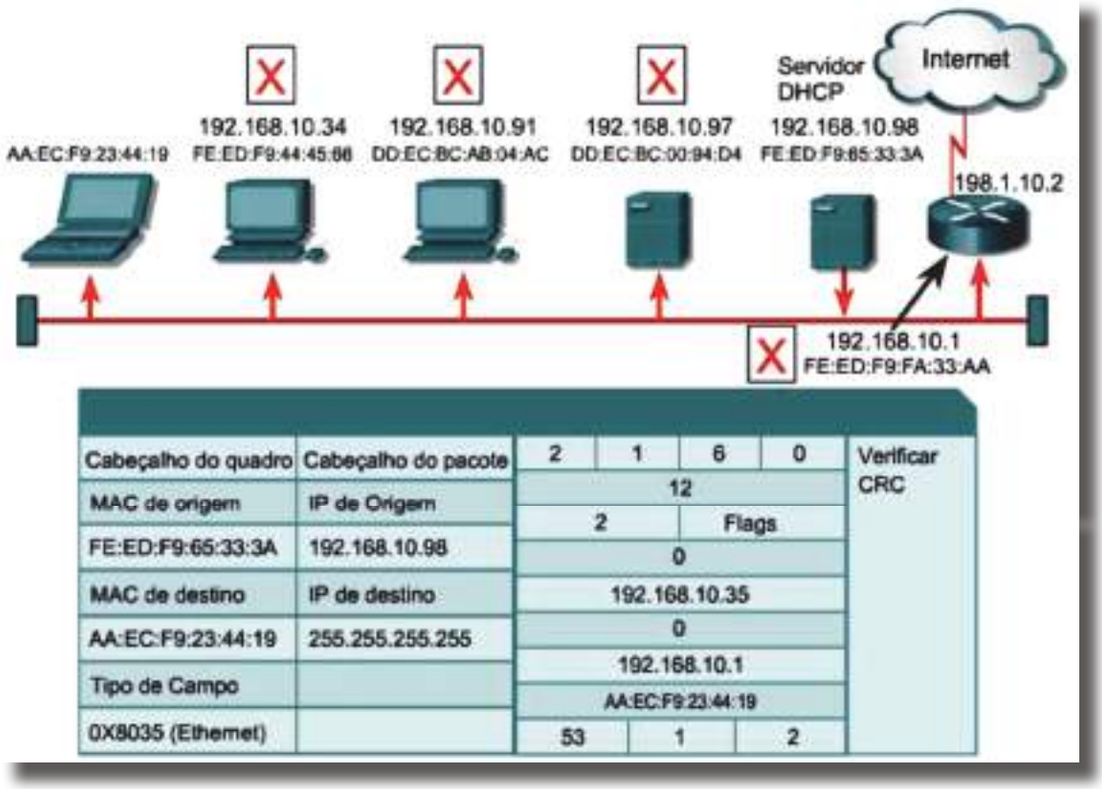


Cabeçalho do quadro	Cabeçalho do pacote	2	1	6	0	Verificar CRC
MAC de origem	IP de Origem	12				
FE:ED:F9:65:33:3A	192.168.10.98	2	Flags			
MAC de destino	IP de destino	0				
AA:EC:F9:23:44:19	255.255.255.255	192.168.10.35				
Tipo de Campo		0				
0X8035 (Ethernet)		192.168.10.1				
		AA:EC:F9:23:44:19				
		53	1	2		

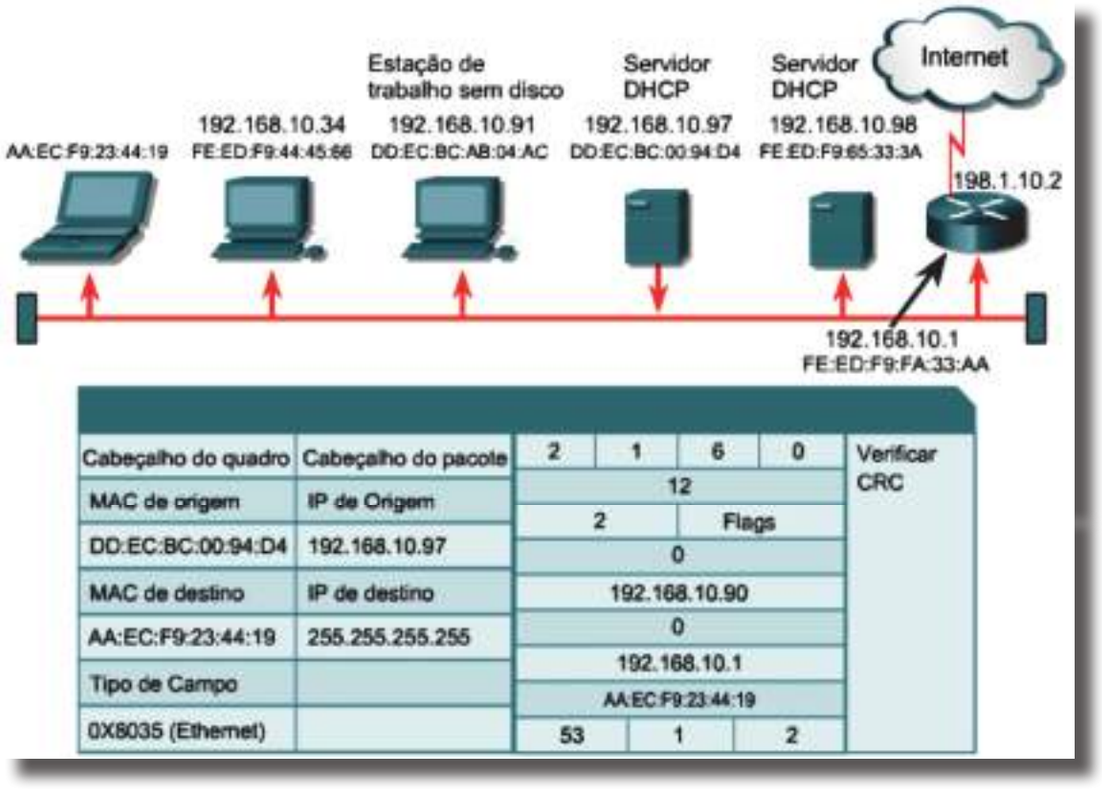
O servidor DHCP envia o DHCP offer ao computador que enviou o pedido.



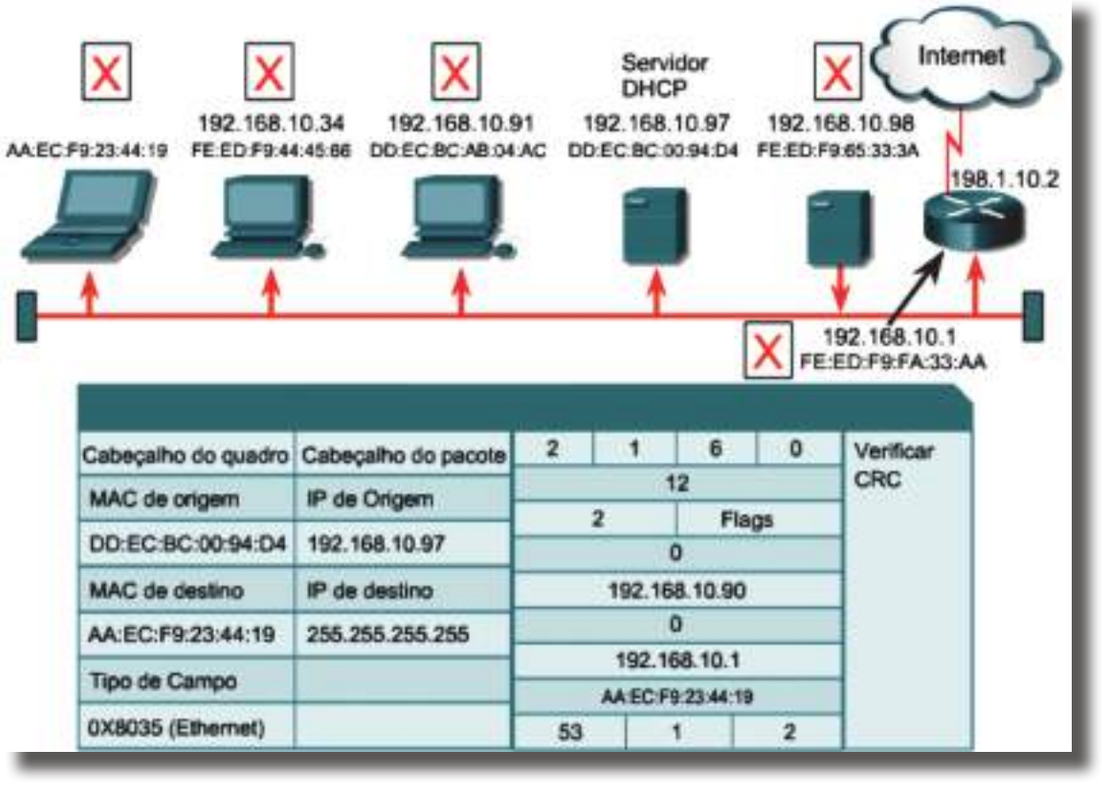
Só o computador com o endereço MAC de destino processa a informação.



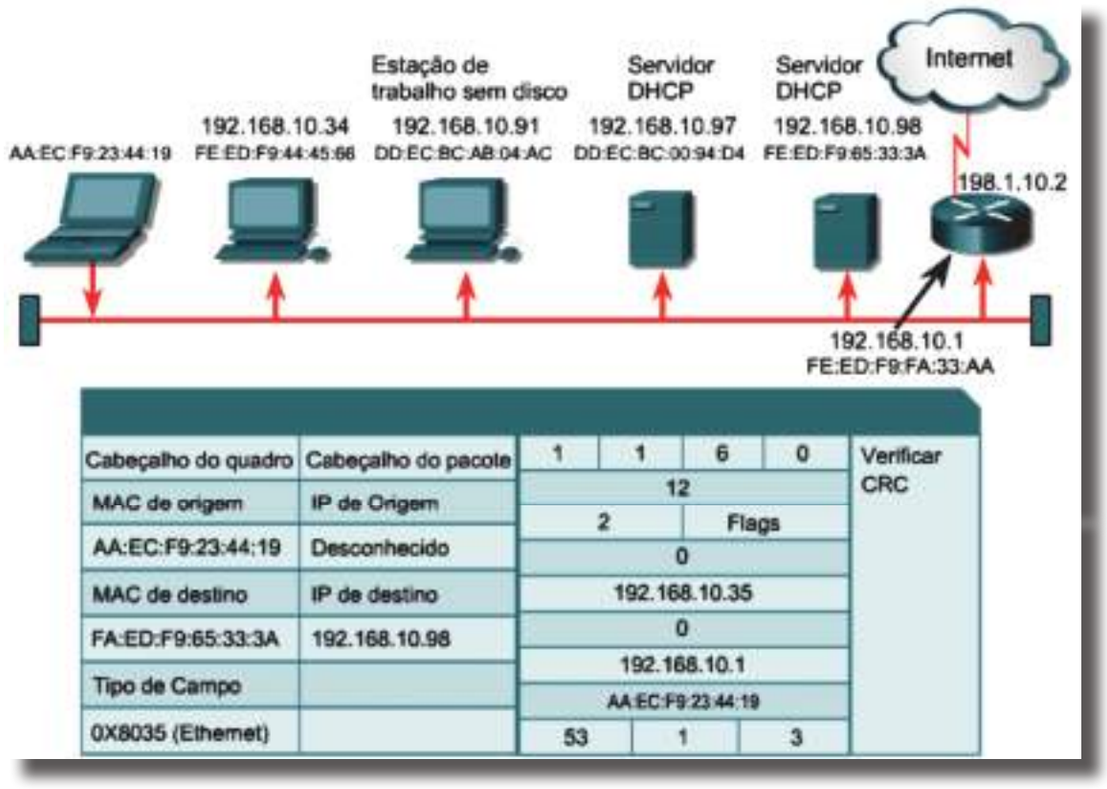
O segundo servidor DHCP envia um DHCP offer.



Só o computador com o endereço MAC de destino processa a trama.

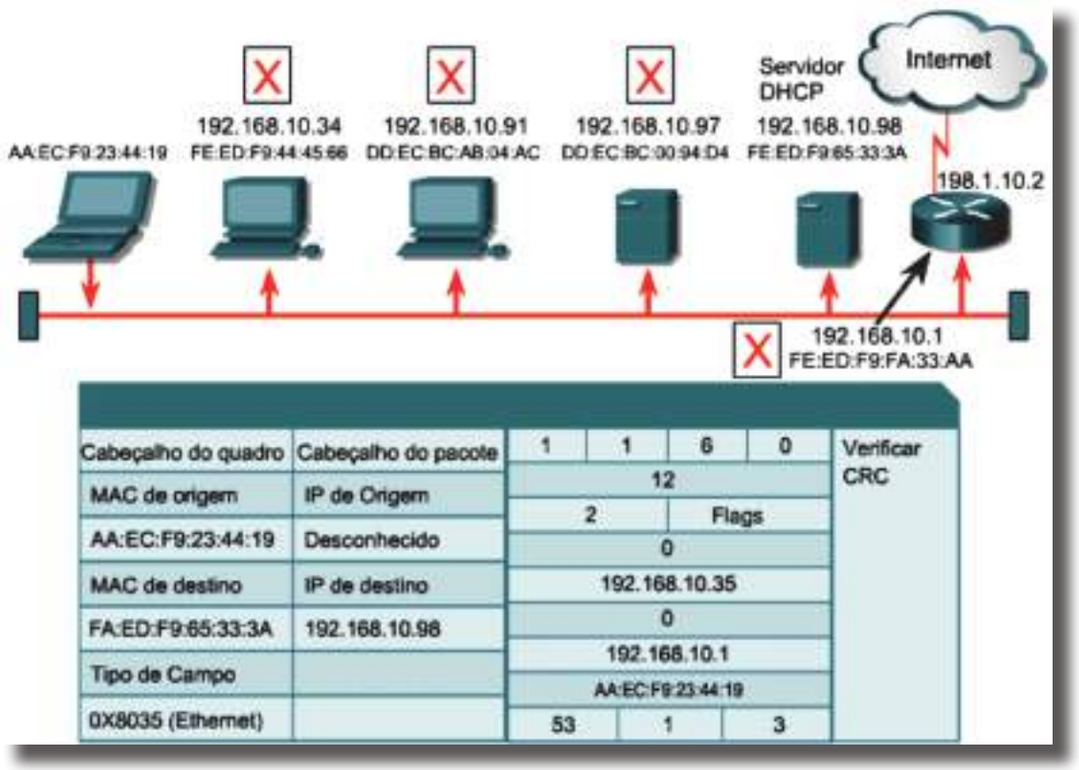


O computador envia um DHCP request endereçado ao servidor DHCP a indicar ter aceitado a oferta.



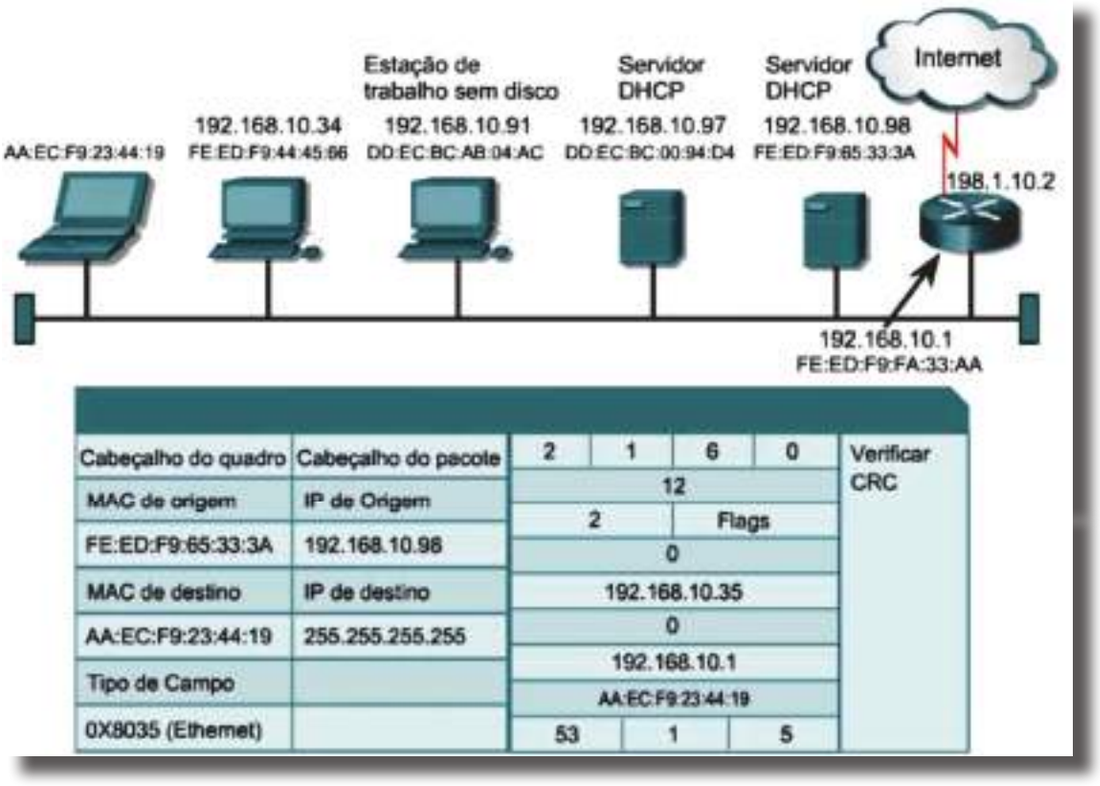
Cabeçalho do quadro	Cabeçalho do pacote	1	1	6	0	Verificar CRC
MAC de origem	IP de Origem	12				
AA:EC:F9:23:44:19	Desconhecido	2		Flags		
MAC de destino	IP de destino	0				
FA:ED:F9:65:33:3A	192.168.10.98	192.168.10.35				
Tipo de Campo		0				
0X8035 (Ethernet)		192.168.10.1				
		AA:EC:F9:23:44:19				
		53	1	3		

Só o servidor DHCP com o endereço MAC de destino processa a informação.



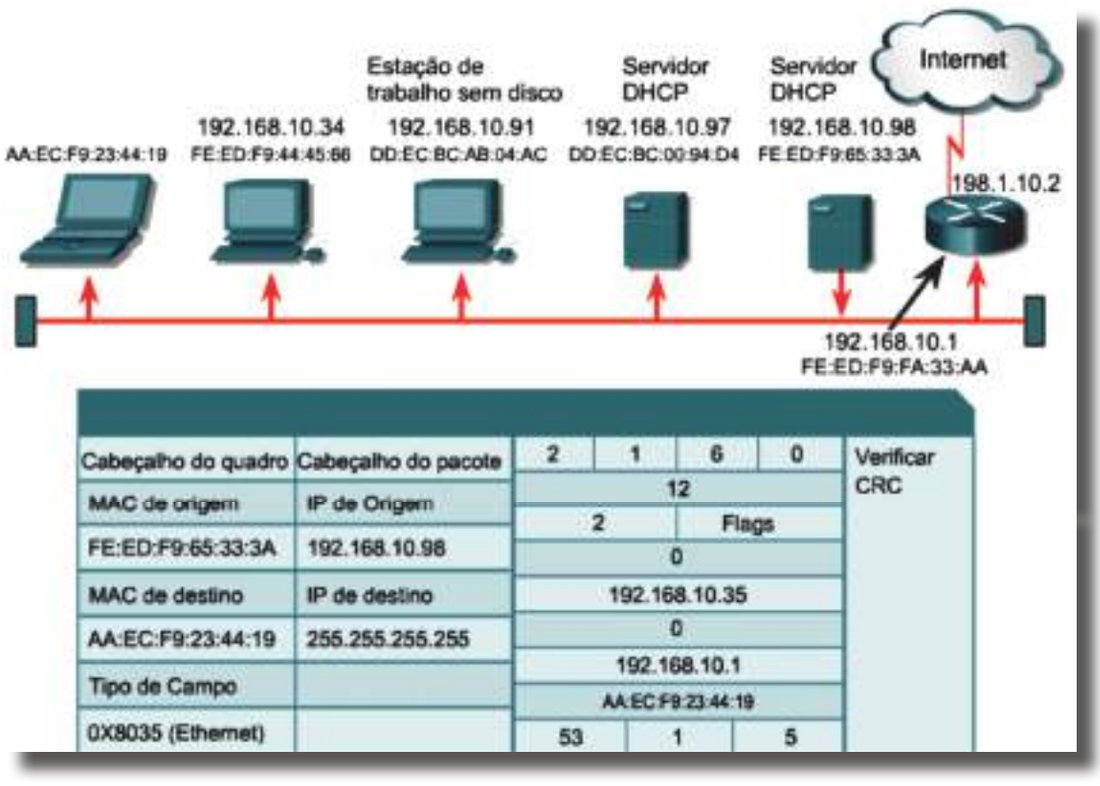
Cabeçalho do quadro	Cabeçalho do pacote	1	1	6	0	Verificar CRC
MAC de origem	IP de Origem	12				
AA:EC:F9:23:44:19	Desconhecido	2		Flags		
MAC de destino	IP de destino	0				
FA:ED:F9:65:33:3A	192.168.10.98	192.168.10.35				
Tipo de Campo		0				
0X8035 (Ethernet)		192.168.10.1				
		AA:EC:F9:23:44:19				
		53	1	3		

O servidor DHCP selecionado cria um DHCP ACK.



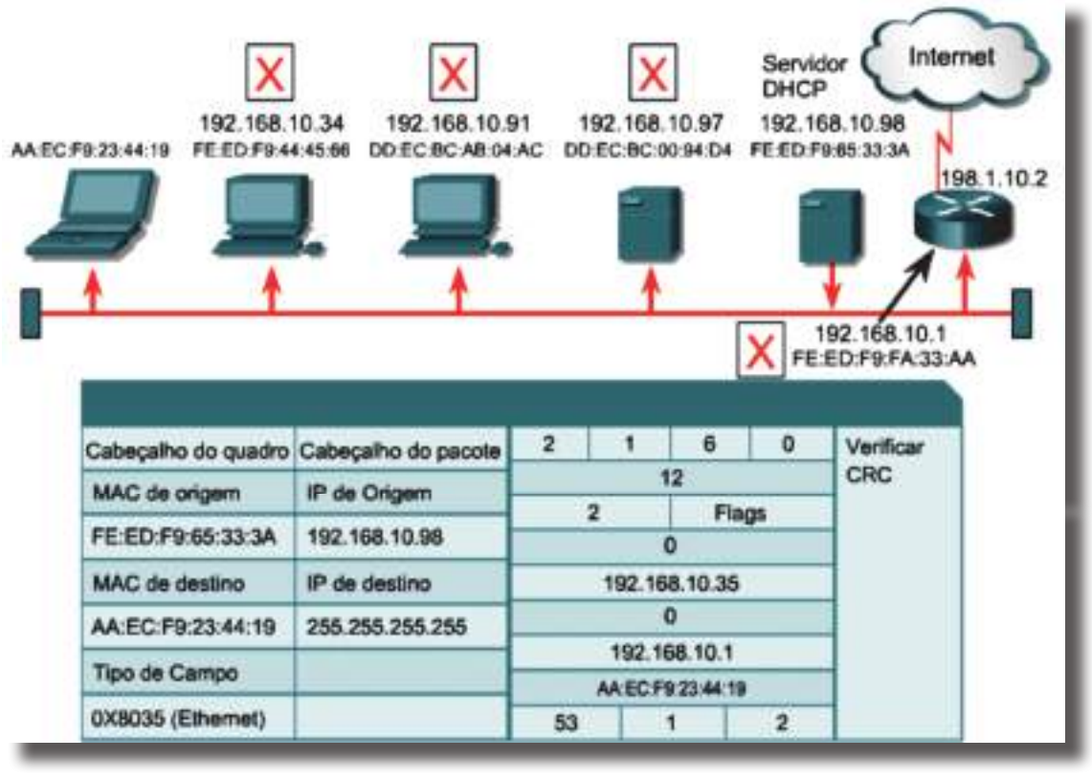
Cabeçalho do quadro	Cabeçalho do pacote	2	1	6	0	Verificar CRC
MAC de origem	IP de Origem	12				
FE:ED:F9:65:33:3A	192.168.10.98	2		Flags		
MAC de destino	IP de destino	0				
AA:EC:F9:23:44:19	255.255.255.255	192.168.10.35				
Tipo de Campo		0				
0X8035 (Ethernet)		192.168.10.1				
		AA:EC:F9:23:44:19				
		53	1	5		

O DHCP ACK é transmitido.

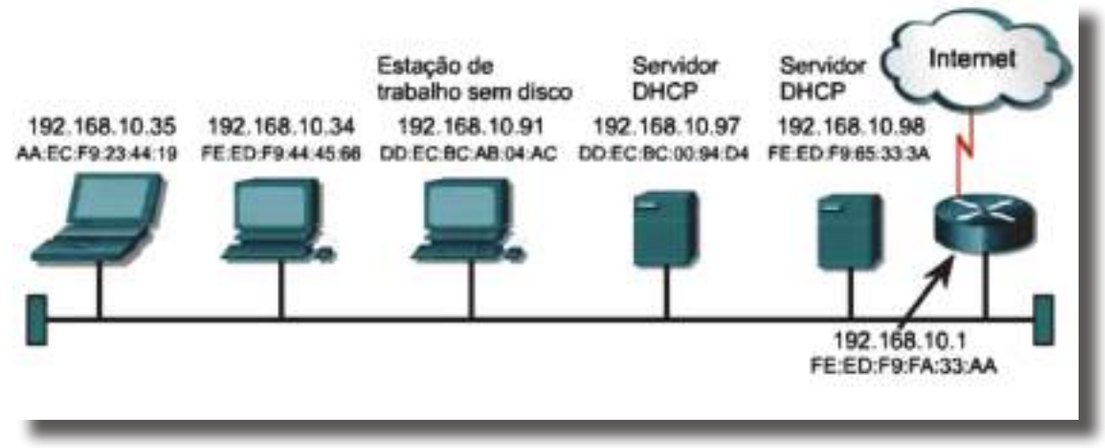


Cabeçalho do quadro	Cabeçalho do pacote	2	1	6	0	Verificar CRC
MAC de origem	IP de Origem	12				
FE:ED:F9:65:33:3A	192.168.10.98	2		Flags		
MAC de destino	IP de destino	0				
AA:EC:F9:23:44:19	255.255.255.255	192.168.10.35				
Tipo de Campo		0				
0X8035 (Ethernet)		192.168.10.1				
		AA:EC:F9:23:44:19				
		53	1	5		

Só o computador com o endereço MAC de destino processa a informação.



A partir deste ponto, o computador pode começar a utilizar o endereço IP atribuído assim como a restante informação incluída no DHCP offer.



Problemas de resolução de endereços

Os problemas mais frequentes encontrados, no que diz respeito ao endereçamento, são relativos a atribuição de mascaras incorretas as estacoes e nós da rede, configuração incorreta de gateways, ou parâmetros de rooting dinâmicos (principalmente *classless* e *classfull*).

Para se comunicar com um dispositivo tem de se conhecer o endereço IP e o endereço MAC do destinatário.

- É necessário um método para se converter automaticamente endereços IP em endereços MAC.
- A criação manual de tabelas de conversão não é exequível.

No TCP/IP existe um protocolo chamado ARP (Address Resolution Protocol) que obtém automaticamente os endereços MAC a partir dos endereços IP para transmissão local.

- Surgem outros problemas quando o destinatário se encontra fora da rede local.

O TCP/IP tem uma variação do ARP chamada Proxy ARP, que fornece o endereço MAC de um dispositivo intermediário para transmissão fora da LAN para outro segmento da rede.

Protocolo de Resolução de Endereços (ARP)

O endereço IP é utilizado para routing, ou seja, a escolha do caminho ideal em determinada circunstância e o instante para a ligação entre dois nós. Para solucionar o problema de mapear o endereço de nível superior (IP) para endereço físico (Ethernet) foi proposto (e aceite) através da RFC826 o Address Resolution Protocol (ARP).

O ARP permite que um host encontre o endereço físico (MAC) de um host destino, tendo apenas o seu endereço IP.

Apesar de ter sido criado especificamente para uso com IP sobre Ethernet, devido à forma que foi implementado, o seu uso não está restrito a este ambiente.

O mapeamento de endereços pode ser feito de duas maneiras:

- Mapeamento direto
- Mapeamento dinâmico

O ARP é dividido em duas partes: a primeira determina endereços físicos quando envia um pacote, e a segunda responde aos pedidos de outros hosts. Geralmente antes de enviar, o host consulta a cache ARP à procura do endereço físico. Se encontrar o endereço, anexa-o no frame e envia acrescentando os dados. Se o host não encontrar o endereço, é realizado um broadcast de pedido ARP.

A segunda parte do código do ARP manuseia os pacotes recebidos da rede. Quando chega um pacote, o programa extrai e examina o endereço físico e IP para verificar se já existe a entrada no cache e atualiza novamente sobrescrevendo os endereços. Depois, o recetor começa a processar o resto do pacote.

O recetor processa dois tipos de entrada de pacotes ARP:

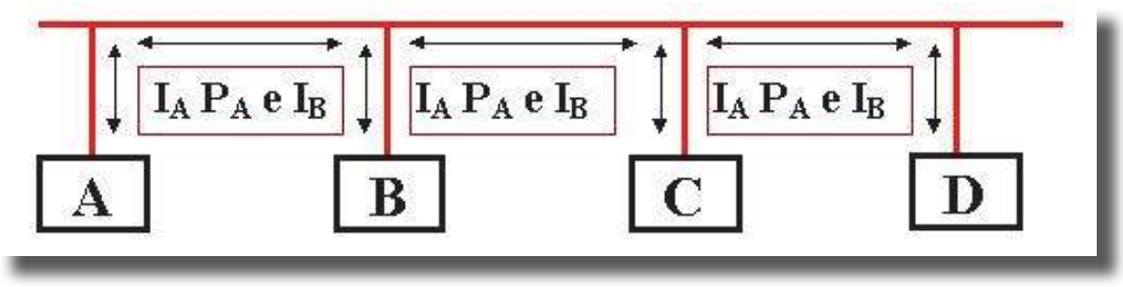
- *Pedido ARP de um outro host*: o recetor envia o endereço físico ao emissor e armazena o endereço do emissor no cache. Se o endereço IP do pacote recebido não for igual do recetor, o pacote ARP é ignorado.
- *Resposta de um pedido ARP:* Após verificar a entrada na cache ARP, o recetor verifica primeiro a resposta com o pedido ARP enviado anteriormente. Enquanto o recetor espera pela resposta, as aplicações podem gerar outros pacotes que geralmente esperam na fila. Após verificar o endereço IP, o recetor atualiza os pacotes com o mesmo. O ARP retira os pacotes da fila depois de fornecer os endereços.

Se durante o broadcast o destinatário não puder aceitar um pedido, o host emissor deve armazenar o pacote enviado para retransmiti-lo. Pode acontecer, também, que o hardware de um host ter sido substituído. Se algum host tentar enviar dados para ele, utilizará um endereço não existente na rede, por isso é importante atualizar e remover os endereços na cache em períodos regulares.

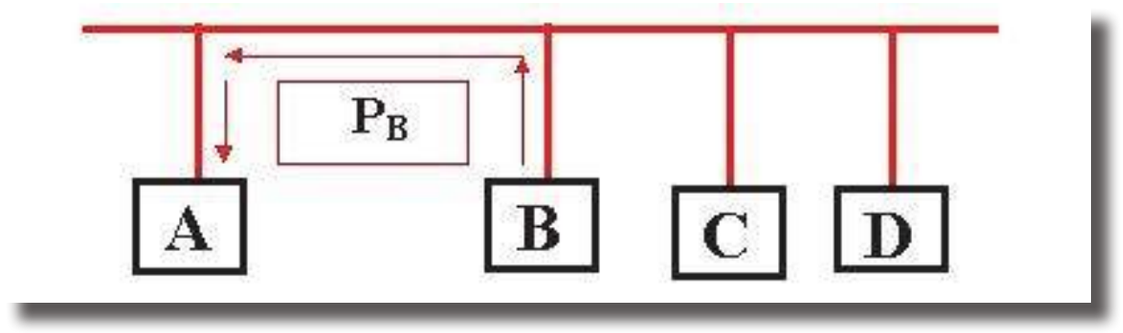
Funcionamento do protocolo ARP

Consiste no envio de um frame em broadcasting com endereço IP do destino, o qual responde com um datagrama que contem o seu endereço IP e o endereço físico. A máquina que gerou o broadcasting passa a usar o endereço físico do destino para enviar os seus datagramas.

Na seguinte figura o host envia o pacote para todos os hosts.



O host A, cujo endereço IP é I_A e endereço físico P_A, deseja enviar dados ao host B, cujo IP é I_B porém de endereço físico desconhecido. O host A envia um datagrama especial em broadcast.



Apenas o host B responde, pois o datagrama foi endereçado via IP. O datagrama de resposta é constituído do endereço IP (I_B) mais o endereço físico P_B. A partir desse instante o host A passa a endereçar o host B apenas com os seus endereços já conhecidos (P_B e I_B).

Resumidamente, o ARP funciona da seguinte forma:

- Quando uma máquina ***A*** quer falar com uma máquina ***B*** e não sabe o seu endereço físico, envia um pacote ARP de request em modo broadcast.
- Todas as máquinas em operação recebem o pedido, mas somente a máquina ***B*** responde, pois ela reconhece que o endereço pedido é o seu.
- ***A*** Guarda o endereço físico de ***B*** F_B em cache.
- ***A*** envia mensagem para F_B.

Cache ARP

Numa rede de grande porte e ocupada, o envio de pacotes em broadcasting interromperá todos os hosts para que eles processem cada pacote da rede. Essa interrupção prejudicará de maneira significativa a eficiência da rede e torná-la-ia mais lenta. Para reduzir os broadcasts, os hosts de redes que precisam utilizar o ARP mantêm uma lista de endereços IP e Ethernet que correspondem aos obtidos por solicitações anteriores. Isto é apresentado como Cache ARP e é atualizado sempre que uma solicitação for enviada. Depois de algum tempo o endereço no ARP Cache é removido, independentemente de estar a ser usado ou não. Isto é chamado de *Aging*.

ARP - Encapsulamento Identificação

As mensagens ARP devem ser transmitidas nos frames. Para identificar se os frames ARP estão a carregar o pedido (request) ou a resposta, o campo do tipo do cabeçalho (header) recebe um valor específico, e a mensagem ARP é enviada no campo dos dados. Quando o frame é recebido, o host verifica o tipo de frame para determinar o seu conteúdo.

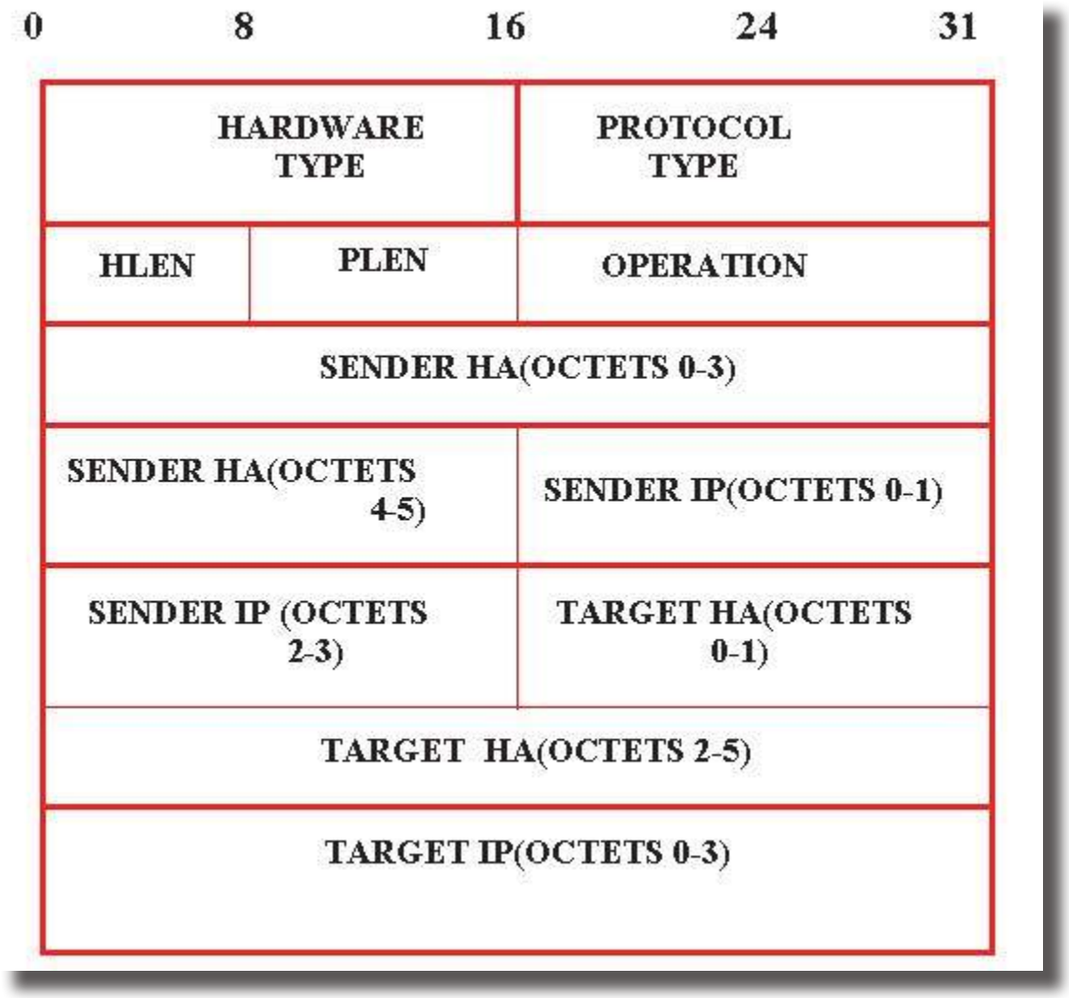
Formato do ARP

Os dados nos pacotes do ARP não possuem um cabeçalho de formato fixo, ao contrário de outros protocolos. A mensagem é montada para ser utilizada em diferentes redes. Por isso, o primeiro campo no cabeçalho indica os comprimentos dos campos seguintes. O ARP pode ser usado com endereços físicos e protocolos arbitrários. Ao contrário da maioria dos protocolos, o pacote ARP não alinha no tamanho de 32-bits. Por exemplo, o endereço do emissor (sender) ocupa 6 octetos contíguos, expandindo-se para próxima linha.

Descrição do Campos

- *Hardware Type* (tipo do hardware): composto de dois octetos, especifica o tipo de hardware utilizado na rede física. Se for 1, é rede Ethernet.
- *Protocol Type* (tipo do protocolo): composto de dois octetos, especifica o endereço do protocolo utilizado no nível superior do emissor.
- *Operation* (operação): especifica se o datagrama é um pedido ARP (request 1) ou uma resposta ARP (reply 2), ou ainda um RARP (request 3, reply 4).
- *HLEN e PLEN*: habilitam o ARP para ser usado com redes arbitrárias porque eles especificam o comprimento dos endereços do hardware e dos protocolos do nível superior. O HLEN (Hardware Lenght) é utilizado para identificar o tamanho dos campos SENDER HA e TARGET HA. PLEN (Protocol Lenght) especifica o tamanho dos campos SENDER IP e TARGET IP.
- *SENDER HA* (Sender Hardware Address) : endereço físico (Ethernet) de quem envia o pacote.
- *SENDER IP* (Sender Protocol Address): endereço lógico (IP) de quem envia o pacote.
- *TARGET HA* (Target Hardware Address) : Endereço físico desejado. Na operação de request vai em branco, e, quem responder preenche este campo.
- *TARGET IP* (Target Protocol Address) : Endereço lógico da máquina desejada.

A figura seguinte representa o formato ARP.

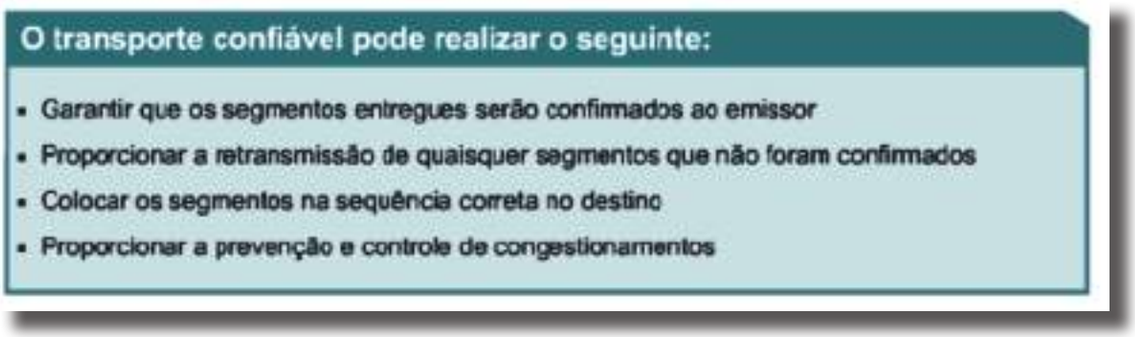


Quando um emissor faz um pedido, envia o endereço TARGET IP (ARP) ou o endereço físico TARGET HA (RARP). Antes de responder, o destinatário atualiza os endereços recebidos e muda a operação para resposta (reply). Assim, a resposta carrega os endereços do emissor assim como os endereços IP e físico do destinatário.

Camada de Transporte TCP/IP

Introdução à camada de transporte

As responsabilidades principais da camada de transporte, camada 4 do modelo OSI, são transportar e regular o fluxo de informações da origem até o destino, de forma confiável e precisa. Controlo fim-a-fim e confiabilidade são proporcionados por janelas deslizantes, números de sequência e confirmações.



Para compreender a confiabilidade e o controle de fluxo, imagine alguém que estuda um idioma estrangeiro durante um ano e, então, visita o país onde esse idioma é usado. Na conversação, as palavras devem ser repetidas para que haja confiabilidade e deve-se falar lentamente para que o sentido da conversa não se perca; isso é controlo de fluxo.

A camada de transporte fornece serviços de transporte do host ao host origem de destino. Ela estabelece uma ligação lógica entre as extremidades da rede. Protocolos na camada de transporte segmentam e remontam os dados que são enviados por várias aplicações de camada superior no mesmo fluxo de dados da camada de transporte. Esses dados da camada de transporte fornecem serviços de transporte fim-a-fim.

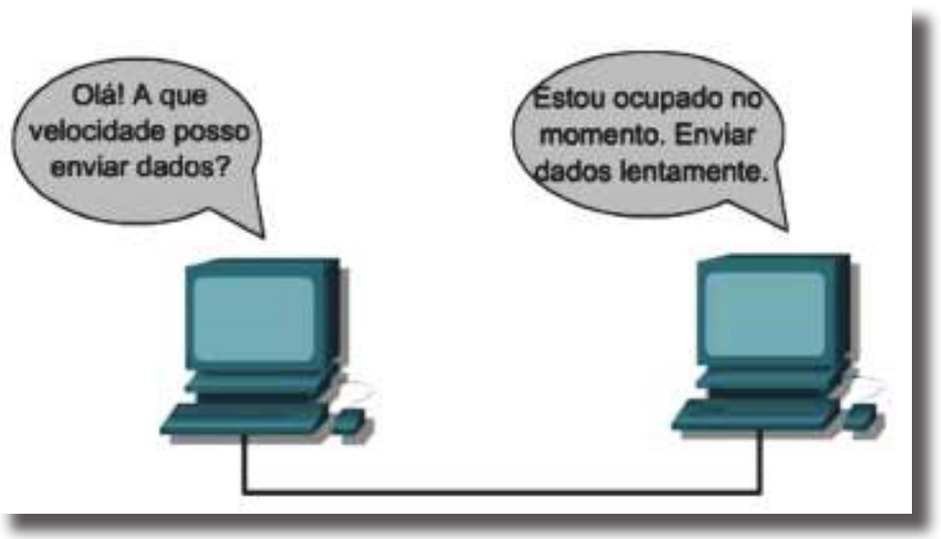
O fluxo de dados da camada de transporte é uma ligação lógica entre as extremidades de uma rede. As responsabilidades principais são transportar e regular o fluxo de informações da origem ao destino de forma confiável e precisa. A responsabilidade principal da camada 4 é fornecer controlo fim-a-fim usando janelas móveis e oferecer confiabilidade nos números de sequência e nas confirmações. A camada de transporte define a conectividade fim-a-fim entre aplicações de host. Os serviços de transporte incluem os seguintes serviços básicos:

- Segmentação de dados de aplicações de camada superior;
- Estabelecimento de operações fim-a-fim;
- Transporte de segmentos de um host final ao outro;
- Controle de fluxo proporcionado por janelas móveis;
- Confiabilidade proporcionada por números de sequência e por confirmações.
-

O TCP/IP é uma combinação de dois protocolos individuais. O IP opera na camada 3 e é um protocolo sem conexão, que oferece um serviço de entrega de melhor esforço (best effort) numa rede. O TCP opera na camada 4 e é um serviço orientado à conexão que oferece controlo de fluxo e confiabilidade. Estes protocolos juntos fornecem uma ampla variedade de serviços e são a base de todo um conjunto de protocolos, chamado TCP/IP. A Internet foi construída com base nesse conjunto de protocolos.

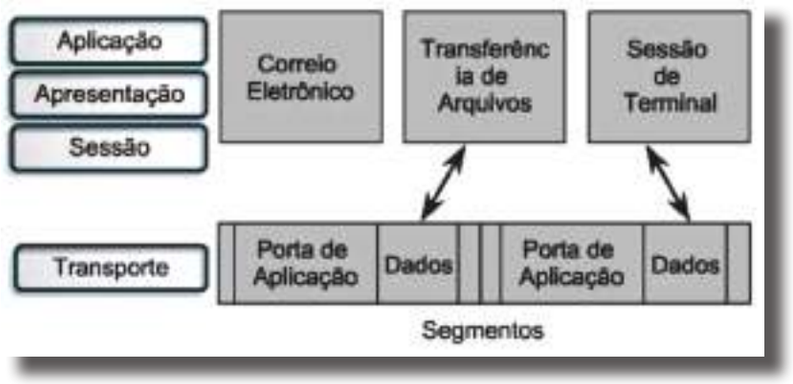
Controle de fluxo

À medida que a camada de transporte envia segmentos de dados, ela procura garantir que eles não sejam perdidos. Um host recetor que não consiga processar dados com a mesma rapidez com que chegam pode causar perda de dados. O host recetor é, então, forçado a descartá-los. O controlo de fluxo evita que um host transmissor sobrecarregue os buffers de um host recetor. O TCP fornece o mecanismo para controlo de fluxo, permitindo a comunicação entre os hosts de envio e de receção. Os dois hosts, então, estabelecem uma taxa de transferência de dados satisfatória para ambos.



Visão geral de estabelecimento, manutenção e término de sessões

Várias aplicações podem partilhar a mesma ligação de transporte no modelo de referência OSI. Esse processo é chamado de multiplexação de conversas de camada superior. Várias conversas simultâneas da camada superior podem ser multiplexadas sobre uma única ligação. A funcionalidade de transporte é realizada segmento-por-segmento. Por outras palavras, diferentes aplicações podem enviar segmentos de dados de acordo com a política primeiro a chegar, primeiro a ser servido (First-come, first-served). O segmento que chegar primeiro será servido primeiro. Esses segmentos podem então ser roteados para o mesmo destino, ou para diferentes destinos.

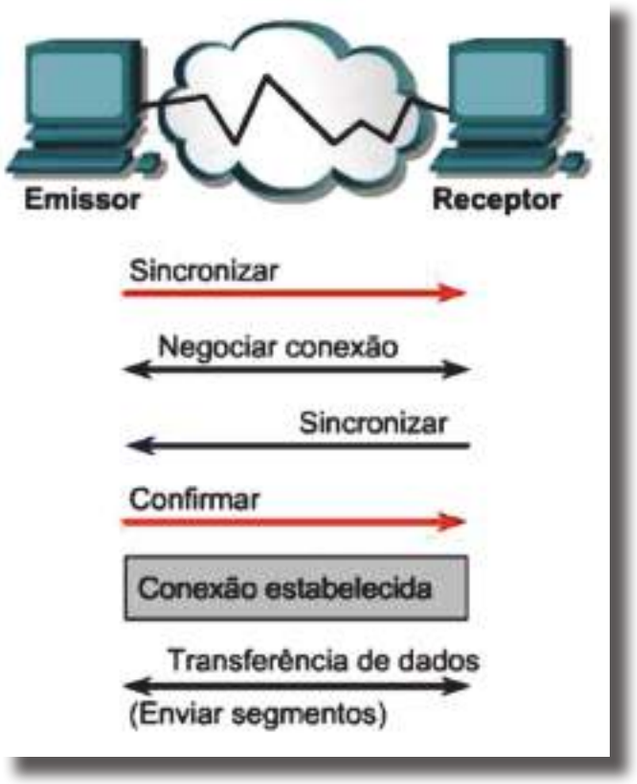


Uma função da camada de transporte é estabelecer uma sessão orientada à ligação entre dispositivos similares na camada de aplicação. Para que a transferência de dados comece, as aplicações de envio e de receção informam aos respetivos sistemas operacionais que será iniciada uma ligação. Um nó inicia uma ligação que deverá ser aceite pelo outro. Os módulos do software de protocolo nos dois sistemas operacionais comunicam-se enviando mensagens pela rede, para verificar se a transferência está autorizada e se ambos os lados estão prontos.

A ligação é estabelecida e a transferência de dados começa após ter ocorrido toda a sincronização. Durante a transferência, as duas máquinas continuam a comunicar-se com seu software de protocolo, para verificar se os dados estão a ser recebidos corretamente.

A Figura mostra uma ligação típica entre os sistemas de envio e de receção. O primeiro handshake solicita sincronização. O segundo e o terceiro confirmam a solicitação de

sincronização inicial e também sincronizam os parâmetros de ligação na direção oposta. O segmento de handshake final é uma confirmação usada para informar ao destino que ambos os lados concordam que foi estabelecida uma ligação. Após o estabelecimento da conexão, começa a transferência de dados.

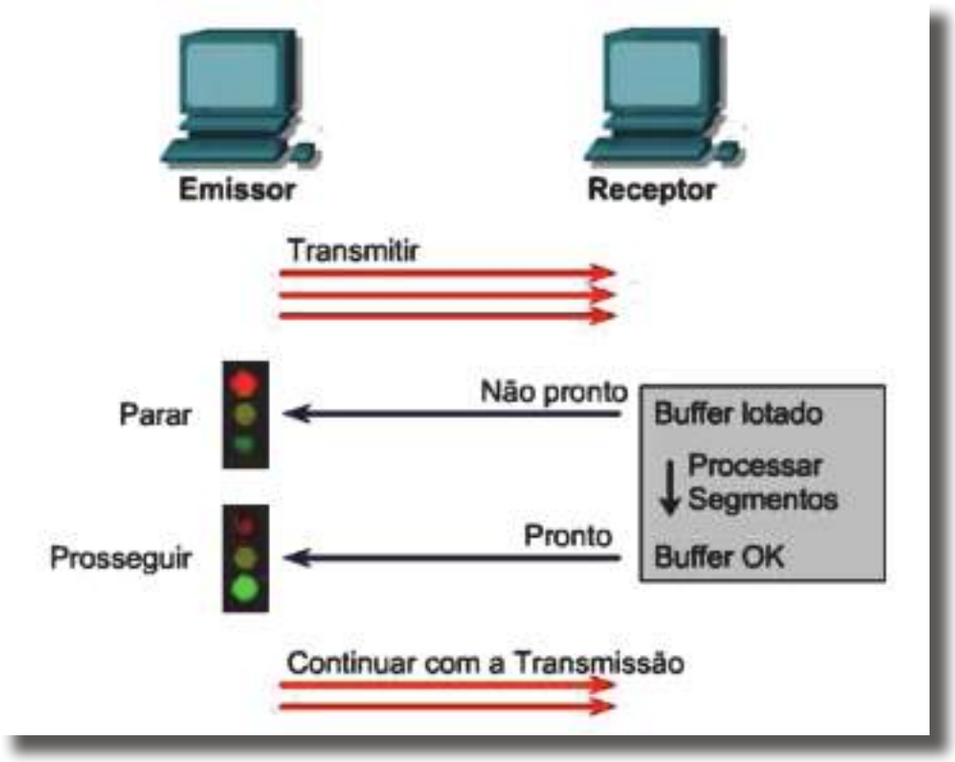


Congestionamento durante a transferência de dados pode ocorrer por dois motivos:

- Primeiro, um computador com alta velocidade pode gerar tráfego mais rapidamente do que uma rede pode ser capaz de transferir.
- Segundo, se muitos computadores precisarem enviar datagramas simultaneamente a um único destino, esse destino pode sofrer congestionamento, embora o problema não tenha uma origem única.

Quando os datagramas chegam muito rapidamente para que um host ou gateway os processe, eles são armazenados temporariamente na memória. Se o tráfego prosseguir, o host ou gateway, por fim, esgotará a sua memória e deverá descartar os datagramas adicionais que chegarem.

Em vez de permitir que os dados sejam perdidos, o processo TCP na máquina que está a receber os dados pode emitir um indicador de "não-pronto" (not-ready) para o remetente. Atuando como uma placa de "STOP", esse indicador sinaliza para que o remetente pare de enviar dados. Quando o recetor puder lidar com mais dados, ele enviará um indicador de transporte de "pronto" (Ready). Quando esse indicador é recebido, o remetente retoma a transmissão de segmentos.



No final da transferência de dados, o host transmissor envia um sinal que indica o final da transmissão. O host recetor na extremidade da sequência de dados confirma o fim da transmissão e a conexão é encerrada.

Handshake triplo

O TCP é um protocolo orientado a ligações. Ele requer o estabelecimento de uma conexão antes do começo da transferência de dados. Para que uma ligação seja estabelecida ou inicializada, os dois hosts devem sincronizar os seus *Initial Sequence Numbers* (ISNs). A sincronização é feita através da troca de segmentos de estabelecimento de conexão que transportam um bit de controle chamado SYN, para a sincronização, e os ISNs. Os

segmentos que transportam o bit SYN também são chamados "SYNs". Essa solução requer um mecanismo adequado para a obtenção de um número de sequência inicial e um handshake simples para a troca de ISNs.

A sincronização requer que cada um dos lados envie seu número de sequência inicial (ISN) e que receba uma confirmação dessa troca através de um acknowledgment (ACK) enviado pelo outro lado. Cada um dos lados também deve receber o ISN do outro lado e enviar um ACK de confirmação. A sequência é:

1. O host (A) inicia uma ligação ao enviar um pacote SYN para o host (B) indicando que o seu ISN = X:

A —> B SYN, seq de A = X

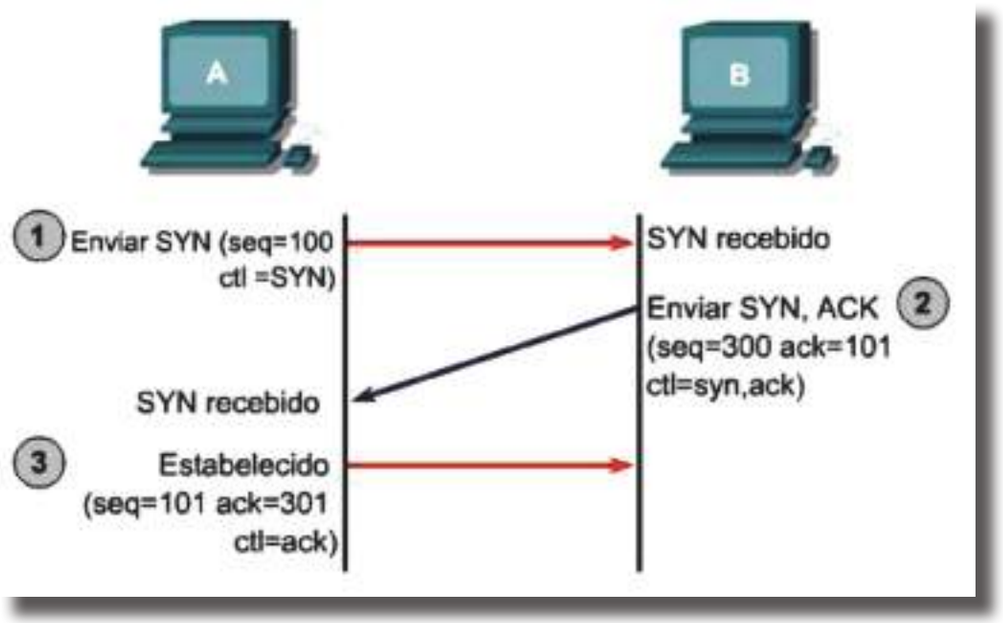
2. B recebe o pacote, grava que a seq de A = X, responde com um ACK de X + 1, e indica que seu ISN = Y. O ACK de X + 1 significa que o host B já recebeu todos os bytes até ao byte X e que o próximo byte esperado é o X + 1:

B —> A ACK, seq de A = X, SYN seq de B = Y, ACK = X + 1

3. A recebe o pacote de B, e fica a saber que a sequência de B = Y, e responde com um ACK de Y + 1, que finaliza o processo de estabelecimento da ligação:

A —> B ACK, seq de B = Y, ACK = Y + 1

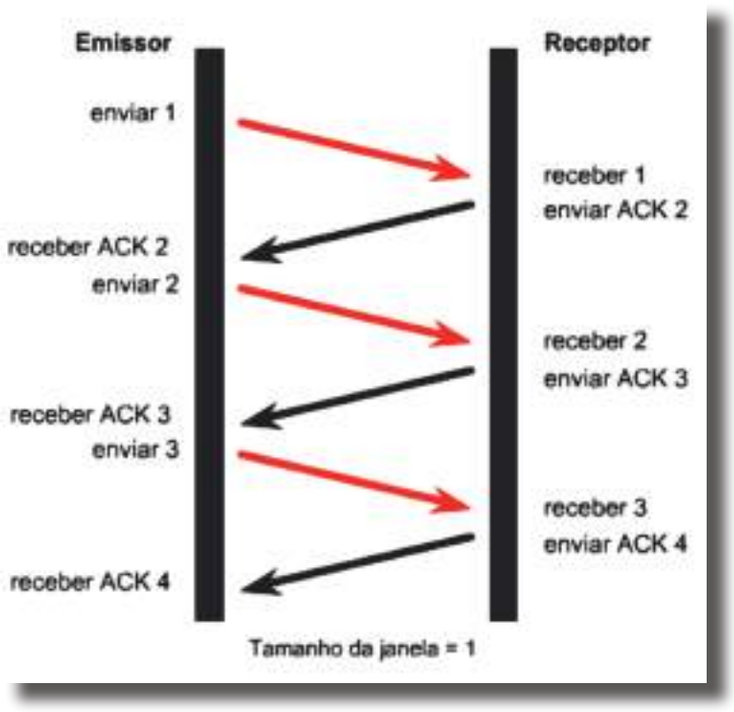
Essa troca é chamada handshake triplo.



Um handshake triplo é necessário porque os números de sequência não são vinculados a um relógio global na rede e os protocolos TCP podem ter mecanismos diferentes para captar o ISN. O recetor do primeiro SYN não tem meios para saber se este é um segmento antigo atrasado, a menos que tenha registrado o último número de sequência usado na ligação. Nem sempre é possível lembrar esse número. Assim, o recetor deve pedir ao remetente que verifique esse SYN.

Janelamento

Os pacotes de dados devem ser enviados ao recetor na mesma ordem em que foram transmitidos, para que haja uma transferência de dados fiável, orientada à ligação. O protocolo falha se algum pacote for perdido, danificado, duplicado ou recebido em ordem diferente. Uma solução fácil é fazer com que o recetor confirme a receção de cada pacote antes do envio do pacote seguinte.



Se o remetente precisar de esperar por uma confirmação após enviar cada pacote, o throughput será lento. Por isso, a maioria dos protocolos fiáveis, orientados à conexão, permitem mais de um pacote em tráfico na rede de cada vez. Como há tempo disponível após o encerramento da transmissão de dados pelo remetente e antes que o recetor

termine o processamento de qualquer confirmação recebida, esse intervalo é usado para transmitir mais dados. O número de pacotes de dados restantes que o emissor tem permissão para ter sem ter recebido uma confirmação é conhecido como tamanho da janela ou janela.

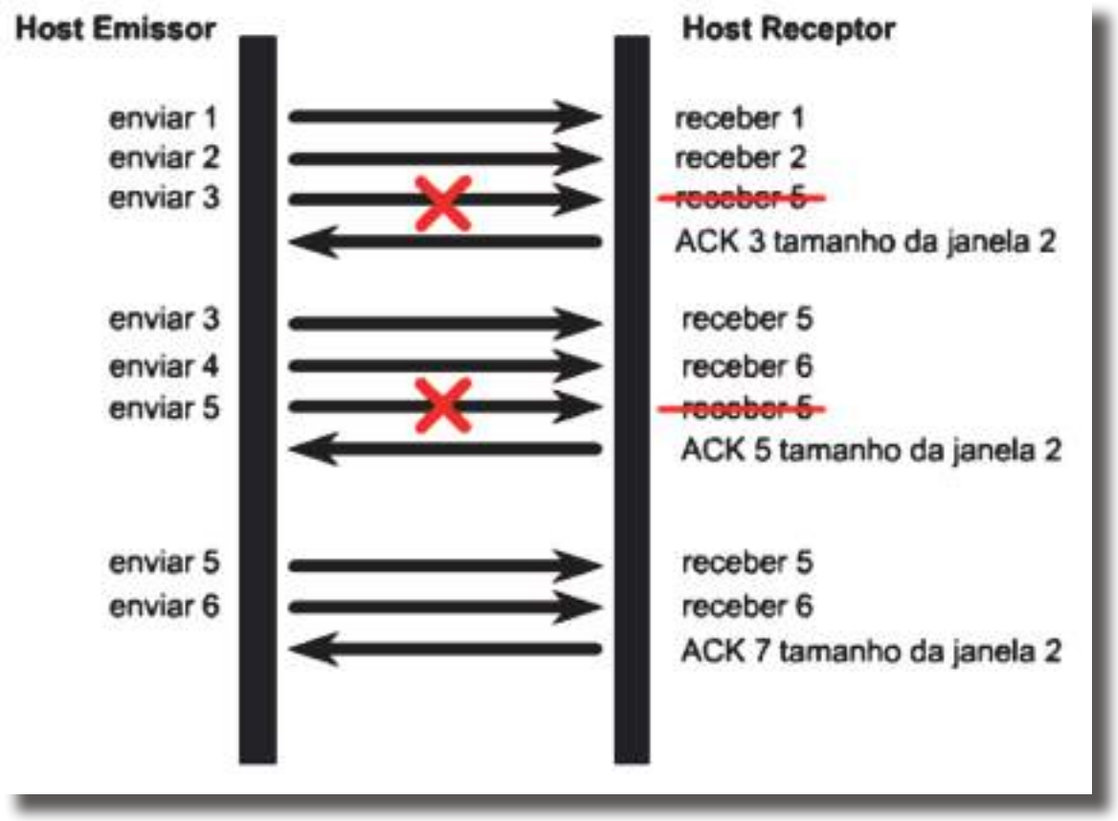
O TCP usa confirmações esperadas. A expressão "confirmações esperadas" significa que o número da confirmação refere-se ao pacote esperado em seguida. A expressão "janelamento" refere-se ao facto de o tamanho da janela ser negociado dinamicamente durante a sessão do TCP. O janelamento é um mecanismo de controlo de fluxo. O janelamento exige que o dispositivo de origem receba uma confirmação do destino depois de transmitir uma determinada quantidade de dados. O processo de receção TCP informa uma "janela" ao TCP de envio. Essa janela especifica o número de pacotes, a começar com o número da confirmação, que o processo TCP recetor está preparado para receber no momento.

Com um tamanho de janela três, o dispositivo de origem pode enviar três bytes ao destino. O dispositivo de origem deve, então, aguardar uma confirmação. Se o destino receber os três bytes, ele enviará uma confirmação ao dispositivo de origem, que poderá então transmitir mais três bytes. Se o destino não receber os três bytes, devido a sobrecarga nos buffers, não enviará a confirmação. Por não receber a confirmação, a origem saberá que os bytes deverão ser retransmitidos e que a taxa de transmissão deverá ser diminuída.

Os tamanhos de janela do TCP são variáveis durante todo o tempo de vida de uma ligação. Cada confirmação contém um anúncio de janela que indica o número de bytes que o recetor pode aceitar. O TCP também mantém uma janela de controle de congestionamento. Essa janela tem, normalmente, tamanho igual ao da janela do recetor. No entanto, ela é reduzida à metade quando um pacote se perde, talvez como resultado de congestionamento na rede. Essa técnica permite que a janela seja expandida ou reduzida conforme necessário, para gerir o espaço no buffer e o processamento. Um tamanho de janela maior permite o processamento de mais dados.

Conforme mostra a Figura, o remetente envia três pacotes antes de esperar por um ACK. Se o recetor puder lidar com um tamanho de janela de dois pacotes apenas, a janela descarta o pacote três, especifica três como o próximo pacote e dois como o novo tamanho de janela.

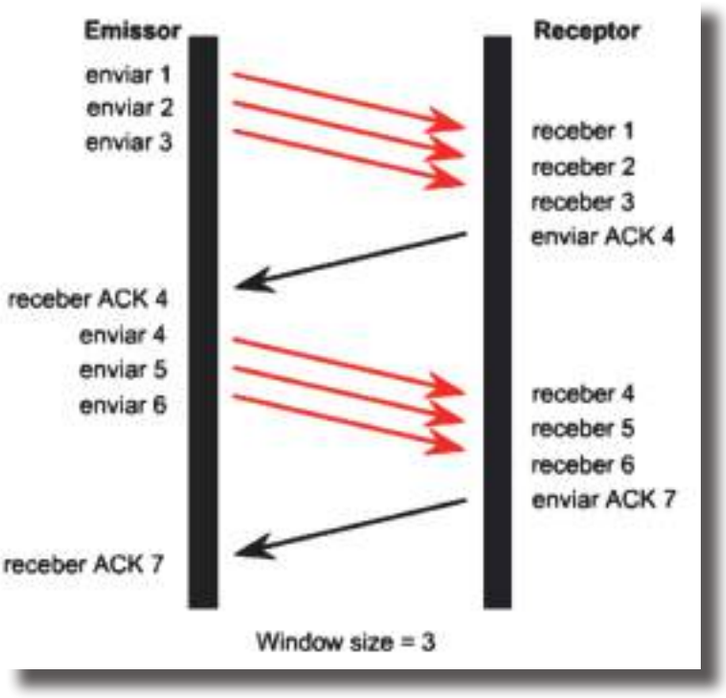
O remetente envia os próximos dois pacotes, mas ainda especifica três como tamanho de janela. Isso significa que o remetente ainda esperará uma conformação de três pacotes do recetor. O recetor responde solicitando o pacote cinco, novamente especificando dois como tamanho de janela.



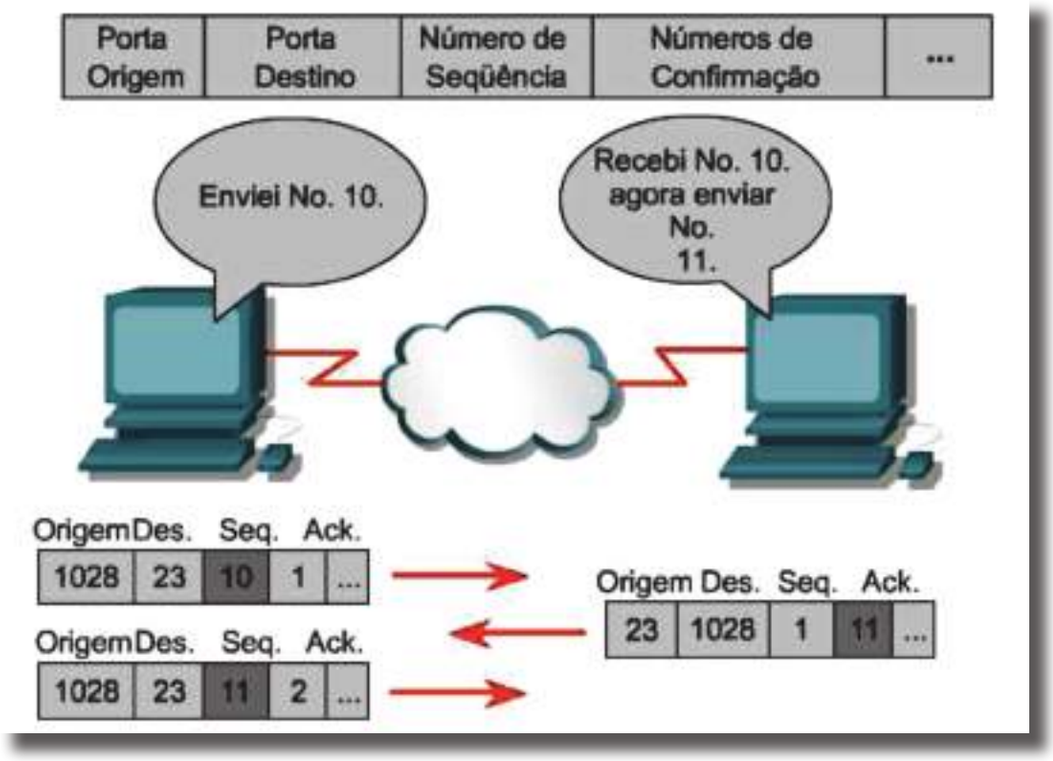
Confirmação

A entrega fiável garante que um fluxo de dados enviado de um dispositivo seja, através de uma ligação de dados, entregue a outro dispositivo, sem duplicação ou perda de dados. A confirmação positiva com retransmissão é uma técnica que garante a entrega confiável de dados. Ela exige que um recetor se comunique com a origem e retorne uma mensagem de confirmação quando os dados são recebidos. O remetente mantém o registo de cada pacote de dados (segmento TCP) enviado e espera uma confirmação. Ele também aciona um timer (temporizador) quando envia um segmento e retransmitirá um segmento se o timer expirar antes que chegue uma confirmação.

A Figura mostra o remetente a transmitir os pacotes de dados 1, 2 e 3. O recetor confirma a receção dos pacotes, solicitando o pacote 4. Ao receber a confirmação, o remetente envia os pacotes 4, 5 e 6. Se o pacote 5 não chegar ao destino, o recetor confirma solicitando o reenvio do pacote 5. O remetente reenvia o pacote 5 e recebe uma confirmação para prosseguir com a transmissão do pacote 7.



O TCP fornece a sequência de segmentos com uma confirmação de referência de encaminhamento. Cada segmento é numerado antes da transmissão. Na estação recetora, o TCP reagrupa os segmentos numa mensagem completa. Se um número de sequência estiver em falta na série, aquele segmento será retransmitido. Os segmentos não confirmados dentro de um determinado período serão retransmitidos.



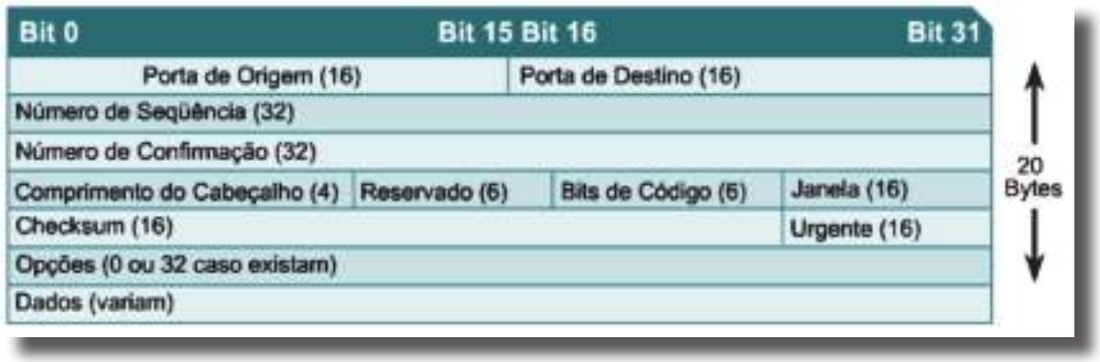
Protocolo de Controlo de Transmissão (TCP)

O Protocolo de Controlo de Transmissão (Transmission Control Protocol TCP) é um protocolo da camada 4 orientado à conexão que fornece transmissão de dados full duplex confiável. O TCP faz parte da pilha de protocolos TCP/IP. Num ambiente de ligação orientada à conexão, é estabelecida uma conexão entre as extremidades antes do início da transferência de informações. O TCP é responsável por decompor as mensagens em segmentos, reagrupá-los na estação de destino, reenviar qualquer item não recebido e reagrupar essas mensagens com base nos segmentos. O TCP proporciona um circuito virtual entre aplicações do utilizador final.

Os protocolos que usam o TCP incluem:

- FTP (File Transfer Protocol);
- HTTP (Hypertext Transfer Protocol);
- SMTP (Simple Mail Transfer Protocol);
- Telnet.

Veja a seguir as definições dos campos no segmento TCP:



- Porta de origem: Número da porta chamadora;
- Porta de destino: Número da porta chamada;
- Número de sequência: Número usado para garantir a sequência correta dos dados que estão a chegar;
- Número de confirmação: Próximo octeto TCP esperado;
- HLEN: Número de palavras de 32 bits no cabeçalho;
- Reservado: Definido como zero;
- Bits de código: Funções de controlo, como a configuração e término de uma sessão;
- Janela: Número de octetos que o remetente está disposto a aceitar;
- Checksum: Uma cálculo de verificação (checksum) feito a partir de campos do cabeçalho e dos dados;
- Urgent Pointer (Ponteiro de Urgência): Indica o final de dados urgentes;
- Opção: Uma opção atualmente definida, tamanho máximo do segmento TCP;
- Dados: Dados de protocolo de camada superior.

Protocolo de Datagrama de Usuário (UDP)

O Protocolo de Datagrama de utilizador (User Datagram Protocol UDP) é o protocolo de transporte sem ligação da pilha de protocolos TCP/IP. O UDP é um protocolo simples que troca datagramas, sem confirmações ou entrega garantida. O processamento de erros e a retransmissão devem ser tratados por protocolos de camada superior.

O UDP não usa janelamento nem confirmações; assim, a fiabilidade, se necessária, é fornecida por protocolos da camada de aplicação. O UDP é projetado para aplicações que não precisem de juntar sequências de segmentos.

Os protocolos que ultilizam o UDP incluem:

- TFTP (Trivial File Transfer Protocol);
- SNMP (Simple Network Management Protocol);
- DHCP (Dynamic Host Control Protocol);
- DNS (Sistema de Nomes de Domínio).

Veja a seguir as definições dos campos no segmento UDP:

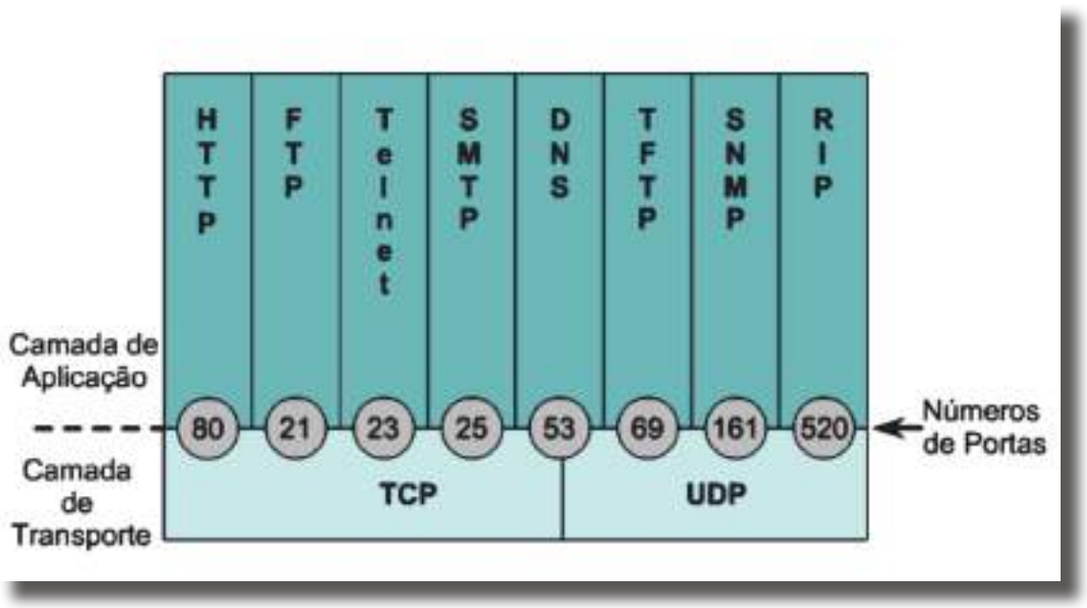
- Porta de origem: Número da porta chamadora;
- Porta de destino: Número da porta chamada;
- Comprimento: Número de bytes que inclui cabeçalho e dados;
- Checksum: Um cálculo de verificação (checksum) feito a partir de campos do cabeçalho e dos dados;
- Dados: Dados de protocolo de camada superior.

Números de porta TCP e UDP

Tanto o TCP quanto o UDP usam números de porta (soquete) para passar as informações às camadas superiores. Os números de porta são usados para manter registos de diferentes conversas que cruzam a rede ao mesmo tempo.

Os desenvolvedores de aplicações de software concordaram em usar números de porta bastante conhecidos, emitidos pelo órgão Internet Assigned Numbers Authority (IANA). Toda conversa destinada à aplicação FTP usa os números de porta padrão 20 e 21. A porta 20 é usada para a parte de dados e a porta 21 é usada para controlo. As conversações que não envolvem uma aplicação com número de porta conhecido recebem números de

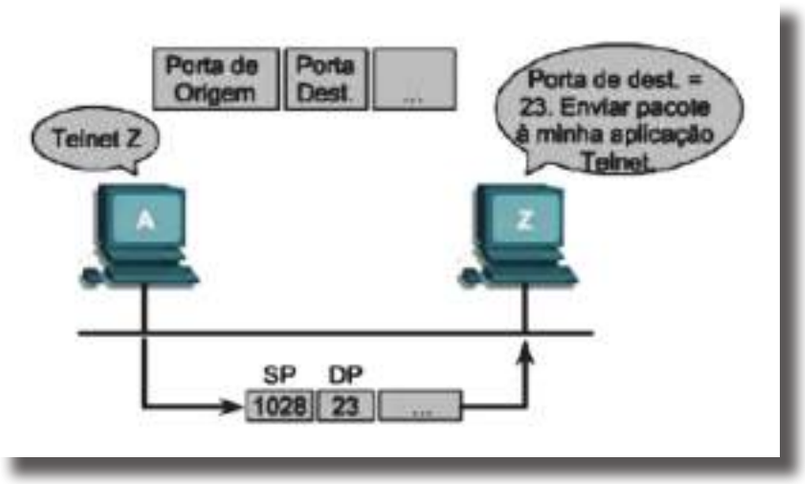
porta aleatórios num intervalo específico acima de 1023. Algumas portas são reservadas no TCP e no UDP, embora possa haver aplicações que não os suportem. Os números de portas têm os seguintes intervalos atribuídos:



- Números abaixo de 1024 são considerados números de porta conhecidos.
- Números acima de 1023 recebem números de porta atribuídos dinamicamente.
- Números de porta registados são aqueles registados para aplicações específicas de fabricantes. A maioria desses números é superior a 1024.

Decimal	Keyword	Description
0		Reservado
1-4		Não atribuído
5	RJE	Remote Job Entry
7	ECHO	Echo
9	DISCARD	Descartar
11	USERS	Usuários Ativos
13	DAYTIME	Hora do dia
15	NETSTAT	Quem está Ativo ou NETSTAT
17	QUOTE	Cota do dia
19	CHARGEN	Gerador de Caracteres
20	FTP-DATA	File Transfer Protocol (dados)
21	FTP	File Transfer Protocol
23	TELNET	Conexão de Terminal
25	SMTP	Simple Mail Transfer Protocol
37	TIME	Hora do dia
39	RLP	Resource Location Protocol
42	NAMESERVER	Servidor de Nomes de Host

Os sistemas finais usam números de portas para selecionar a aplicação correta. O host de origem atribui dinamicamente números de porta de origem gerados na própria origem. Esses números são sempre superiores a 1023.



A Camada de Aplicação

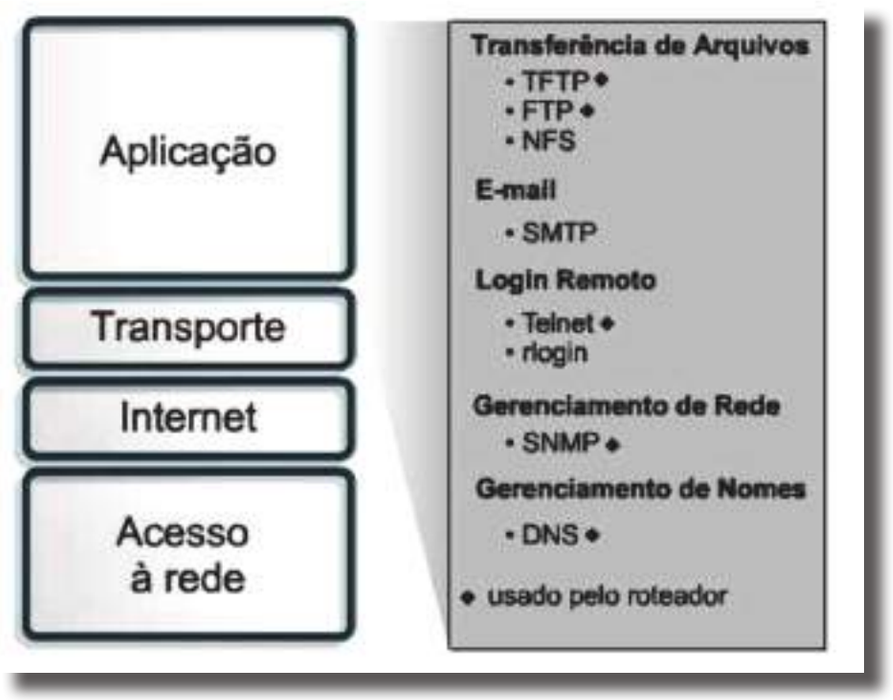
Introdução à camada de aplicação TCP/IP

Quando o modelo TCP/IP foi criado, as camadas de sessão e de apresentação do modelo OSI foram agrupadas na camada de aplicação do modelo TCP. Isso significa que as questões de representação, codificação e controlo de diálogo são tratadas na camada de aplicação e não em camadas inferiores separadas, como ocorre no modelo OSI. O projeto garante que o modelo TCP/IP forneça máxima flexibilidade na camada de aplicação para desenvolvedores de software.

Os protocolos TCP/IP que suportam transferência de ficheiros, e-mail e login remoto são, provavelmente, os mais familiares aos utilizadores da Internet. Esses protocolos incluem as seguintes aplicações:

Sistema de Nomes de Domínios (DNS)

- File Transfer Protocol (FTP);
- Hypertext Transfer Protocol (HTTP);
- Simple Mail Transfer Protocol (SMTP);
- Simple Network Management Protocol (SNMP);
- Telnet.



DNS

A Internet foi construída com base num esquema de endereçamento hierárquico. Esse esquema permite que o routing tenha por base classes de endereços, e não endereços individuais. O problema que isso cria para o utilizador é a associação do endereço correto ao site da Internet. É muito fácil esquecer um endereço IP de um determinado site, porque não há nada que permita a associação do conteúdo do site ao seu endereço. Imagine a dificuldade em lembrar os endereços IP de dezenas, centenas ou até mesmo milhares de sites na Internet.

Um sistema de nomes de domínio foi desenvolvido para associar o conteúdo do site ao seu endereço. O Domain Name System (DNS) é um sistema usado na Internet para converter nomes de domínios e seus nós de rede anunciados publicamente em endereços IP. Um domínio é um grupo de computadores associados pela sua localização geográfica ou pelo seu tipo de negócio. Um nome de domínio é uma cadeia de caracteres, números ou ambos. Normalmente, um nome ou uma abreviatura que represente o endereço numérico de um site na Internet formará o nome do domínio. Existem mais de 200 domínios de nível superior na Internet, cujos exemplos incluem:

- **.us:** Estados Unidos
- **.uk:** Reino Unido
-

Há também nomes genéricos, cujos exemplos incluem:

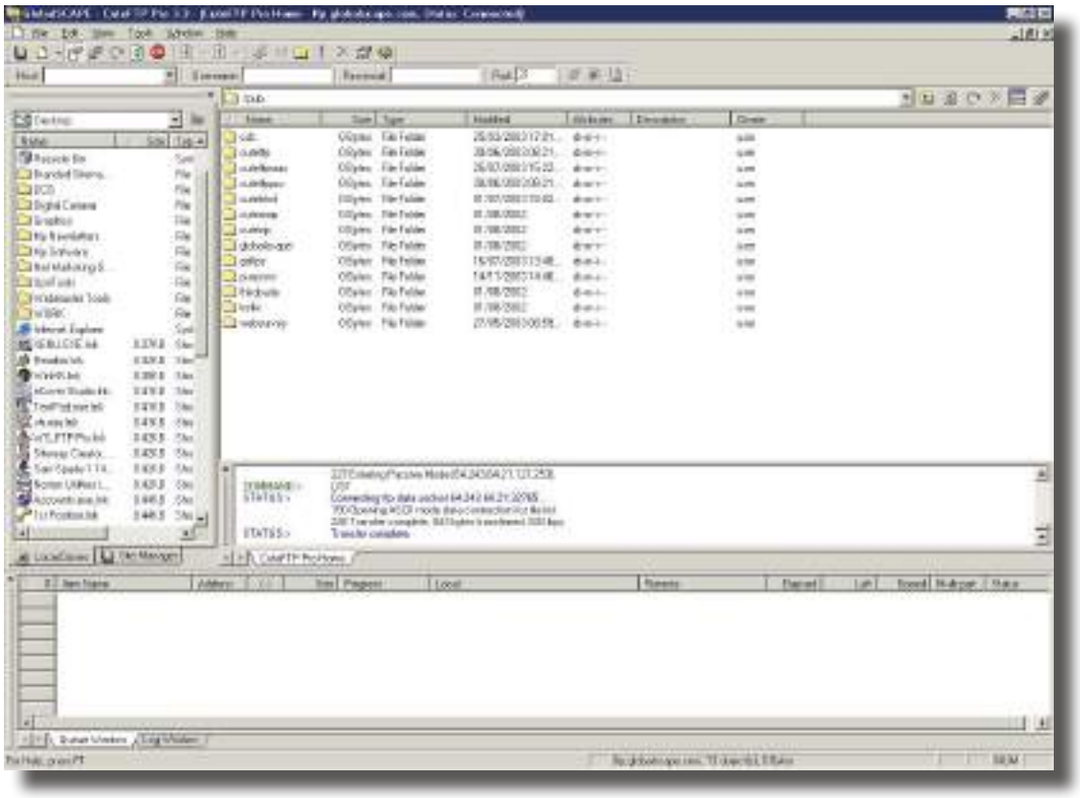
- **.edu:** sites educacionais
- **.com:** sites comerciais
- **.gov:** sites governamentais
- **.org:** sites não-profissionais
- **.net:** serviço de rede

FTP

O FTP é um serviço confiável, orientado à conexão, que usa TCP para transferir ficheiros entre sistemas que suportam FTP. A finalidade principal do FTP é transferir ficheiros de um computador para outro, copiando e movendo ficheiros dos servidores para os clientes

e vice-versa. Quando os ficheiros são copiados de um servidor, o FTP primeiramente estabelece uma ligação de controlo entre o cliente e o servidor. De seguida, é estabelecida uma segunda ligação, que é um link entre os computadores através dos quais os dados são transferidos. A transferência de dados pode ocorrer em modo ASCII ou binário.

Esses modos determinam a codificação usada para ficheiros de dados que, no modelo OSI, é uma tarefa da camada de apresentação. Quando a transferência é concluída, a ligação dos dados é finalizada automaticamente. Quando toda a sessão de cópia e movimentação de ficheiros é concluída, o link de comandos é fechado quando o utilizador efetua logoff e encerra a sessão.



O TFTP é um serviço sem ligação que usa o User Datagram Protocol (UDP). O TFTP é usado no router para transferir ficheiros de configuração e imagens e para transferir ficheiros entre sistemas que suportam TFTP. O TFTP foi criado para ser pequeno e de fácil implementação. Assim, não possui a maioria dos recursos do FTP. O protocolo TFTP pode ler ou gravar ficheiros de ou para um servidor remoto, respetivamente, mas não pode listar diretórios e atualmente não inclui mecanismos para autenticar os utilizadores. É útil em algumas LANs porque opera mais rápido que o FTP e funciona bem numa rede estável.

HTTP

O HyperText Transfer Protocol (HTTP) opera na World Wide Web, que é a parte da Internet que tem crescido mais rapidamente e a mais usada. Uma das razões principais do extraordinário crescimento da Web é a facilidade com que ela permite o acesso às informações. Um navegador da Web é uma aplicação cliente, o que significa que, para funcionar, exige um componente de cliente e um componente servidor. Um navegador da Web apresenta os dados em formatos multimídia nas páginas Web que usam texto, figuras, som e vídeo. As páginas Web são criadas com uma linguagem de formato chamada Linguagem de marcação de hipertexto (HTML). A HTML direciona um navegador da Web numa determinada página da Web a produzir a aparência da página de uma maneira específica. Além disso, a HTML especifica locais para a colocação de textos, ficheiros e objetos que serão transferidos do servidor Web para o navegador da Web.

Os hiperlinks facilitam a navegação na World Wide Web. Um hiperlink é um objeto, palavra, frase ou figura numa página da Web. Quando esse hiperlink é clicado, direciona o navegador para uma nova página da Web. A página da Web contém, frequentemente oculta na sua descrição HTML, um local de endereço conhecido como Localizador Uniforme de Recursos (URL).

No URL http://www.abc.com/edu/, a parte "http://" informa ao navegador que protocolo deve ser usado. A segunda parte, "www", é o nome do host ou o nome de uma máquina específica em um endereço IP específico. A última parte, /edu/, identifica o local específico na pasta do servidor que contém a página da Web padrão.

http://	www.	abc.com	/edu/
Identifica para o navegador o protocolo que deve usar.	Identifica o nome do host ou o nome de uma máquina específica.	Representa a entidade de domínio do site web.	Identifica a pasta onde as páginas web estão no servidor. Como nenhum nome é específico, o navegador irá carregar a página padrão identificada pelo servidor.

Um navegador da Web normalmente abre uma página inicial ou "home page". O URL da home page já foi armazenado na área de configuração do navegador da Web e pode ser alterado a qualquer momento. Na página inicial pode-se clicar num dos hiperlinks da página Web ou de digitar uma URL na barra de endereços do navegador. O navegador da Web examina o protocolo para determinar se ele precisa abrir outro programa e determina o endereço IP do servidor Web usando DNS. De seguida, as camadas de transporte, de rede, de ligação de dados e física trabalham em conjunto para iniciar uma sessão com o servidor Web.

Os dados transferidos para o servidor HTTP contêm o nome da pasta do local da página da Web. Os dados também podem conter um nome de ficheiro específico de uma página HTML. Se nenhum nome for fornecido, deve ser usado o nome default conforme especificado na configuração do servidor.

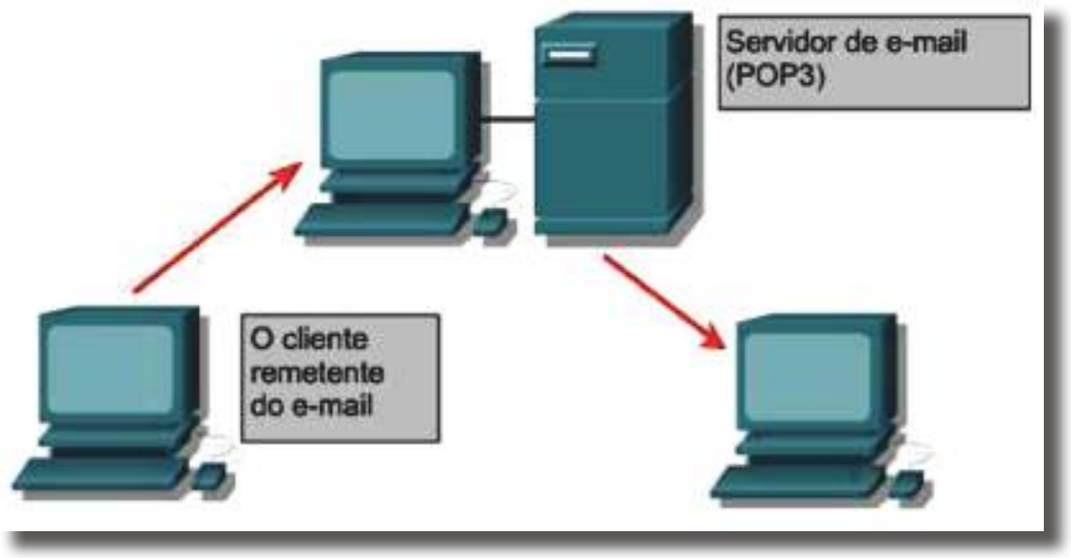
O servidor responde à solicitação enviando ao cliente da Web todos os ficheiros de texto, áudio, vídeo e de figuras especificados nas instruções HTML. O navegador cliente reagrupa todos os ficheiros para criar uma visualização da página da Web e, depois, termina a sessão. Se outra página localizada no mesmo servidor ou em outro for clicada, o mesmo processo será executado novamente.

SMTP

Os servidores de correio eletrónico comunicam-se usando o Simple Mail Transfer Protocol (SMTP) para enviar e receber correspondência. O protocolo SMTP transporta mensagens de e-mail em formato ASCII usando o TCP.

Quando um servidor de correio eletrónico recebe uma mensagem destinada a um cliente local, armazena-a e espera que ela seja aberta pelo cliente. Os clientes podem coletar a sua correspondência de várias formas. Podem usar programas que acedem os ficheiros do servidor de correio diretamente ou coletar a sua correspondência usando um dos muitos protocolos de rede existentes. Os protocolos mais populares de correio para clientes são o POP3 e o IMAP4, que usam o TCP para transportar dados. Embora os clientes de correio usem esses protocolos especiais para coletar correspondência, eles usam quase sempre o SMTP para enviá-la. Como são usados dois protocolos diferentes e, possivelmente, dois servidores diferentes, para enviar e receber correspondência, é

possível que os clientes de correio possam executar uma tarefa mas não a outra. Assim, normalmente é uma boa ideia resolver separadamente os problemas de envio e de receção de e-mail.



Ao examinar a configuração de um cliente de correio, verifique se as configurações de SMTP e de POP ou IMAP estão corretas. Um bom metodo para testar se um servidor de correio pode ser alcançado é executar o Telnet na porta SMTP (25) ou na porta POP3 (110). O seguinte formato de comando é usado na linha de comando do Windows para testar a capacidade de alcançar o serviço SMTP no servidor de correio no endereço IP 192.168.10.5:

C:\>telnet 192.168.10.5 25

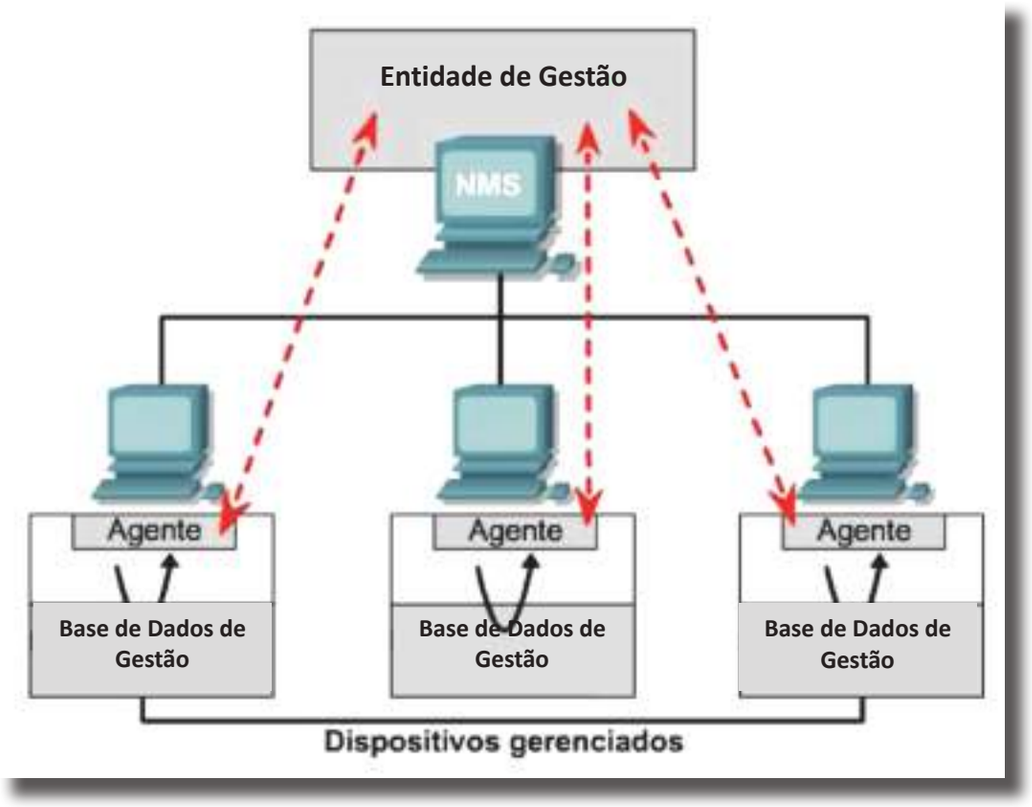
O protocolo SMTP não oferece muito em termos de segurança e não exige autenticação. Os administradores frequentemente não permitem que hosts que não compõem a sua rede usem o seu servidor SMTP para enviar ou retransmitir correspondência.

SNMP

O Protocolo de gestão de Rede Simples (SNMP) é um protocolo da camada de aplicação que facilita a troca de informações de gestão entre dispositivos de rede. O SNMP permite que os administradores de rede façam a gestão do desempenho, encontrem e

solucionem problemas e planeiem o crescimento das redes. O SNMP usa o UDP como protocolo da camada de transporte.

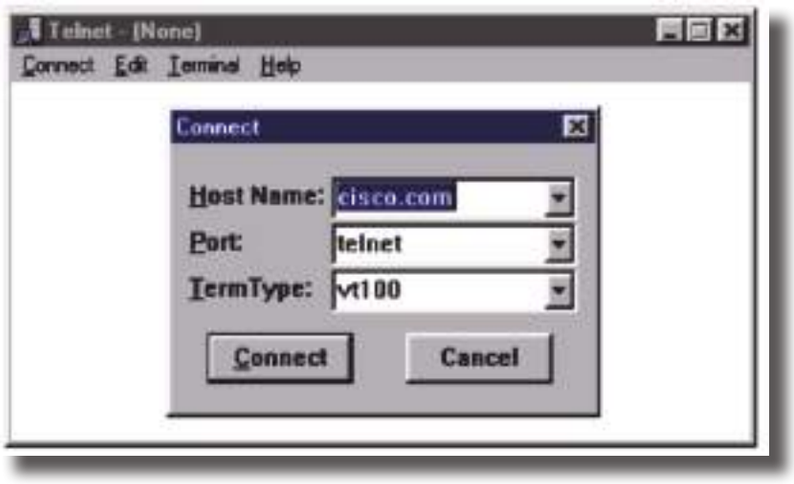
Uma rede administrada SNMP consiste nos três componentes a seguir:



- *Management Protocol* (NMS sistema de gerenciamento de rede): O NMS executa aplicações que monitorizam e controlam dispositivos gerenciados. O conjunto de recursos de processamento e de memória exigido para a gestão de uma rede é fornecido pelo NMS. Deve haver um ou mais NMSs em qualquer rede administrada.
- *Dispositivos geridos:* Dispositivos geridos são nós de rede que contêm um agente SNMP e que residem numa rede administrada. Os dispositivos geridos coletam e armazenam informações de gestão, disponibilizando-as para os NMSs que usam o SNMP. Os dispositivos geridos, às vezes chamados elementos da rede, podem ser routers, servidores de acesso, comutadores, bridges, hubs, computadores hosts ou impressoras.
- *Agentes:* Agentes são módulos de software de gestão de rede que residem em dispositivos geridos. Um agente tem conhecimento local de informações de gestão e converte-as para uma forma compatível com o SNMP.

Telnet

O software cliente Telnet permite efetuar login num host remoto da Internet que esteja executando uma aplicação de servidor Telnet e, de seguida, executar comandos usando a linha de comando. Um cliente Telnet é chamado host local. Um servidor Telnet, que usa um software especial chamado daemon, recebe o nome de host remoto.



Uma sessão Telnet começa como qualquer outro programa de comunicação, ou seja com um endereço para se ligar a um computador host. O endereço pode ser um endereço IP (192.168.10.11) ou um nome de domínio.

Para fazer a ligação utilizando um cliente Telnet, deve ser selecionada a opção de conexão. Uma caixa de diálogo normalmente solicita um nome de host e um tipo de terminal. O nome de host é o endereço IP ou nome de DNS do computador remoto. O tipo de terminal descreve o tipo de emulação de terminal que o cliente Telnet deverá realizar. O telnet não utiliza qualquer recurso de processamento do computador que está a transmitir. O que ele faz é transmitir as teclas digitadas localmente ao host remoto e enviar a saída no ecrã de volta ao monitor local. Todo o processamento e o armazenamento ocorrem no computador remoto.

O Telnet atua na camada de aplicação do modelo TCP/IP. Assim, ele atua nas três camadas mais altas do modelo OSI. A camada de aplicação lida com comandos. A camada de apresentação lida com formatação, normalmente ASCII. A camada de sessão transmite. No modelo TCP/IP, todas essas funções são consideradas parte da camada de aplicação.

Exercícios Propostos

1. Quem foi o criador do modelo TCP/IP, e porquê?

2. Por quantas camadas é composto o modelo TCP/IP? Diga quais são.

3. Quais são os protocolos que a camada de aplicação do modelo TCP/IP trata?

4. Diga o que entende por NFS (Network File System)

5. Diga em que consiste a camada de transporte do modelo TCP/IP.

6. Que serviços oferece a camada de transporte?

7. Qual a finalidade da camada de Internet do modelo TCP/IP, e qual o protocolo mais usado?

8. A função do Internet Protocol é?

9. Porque se diz que o IP é considerado um protocolo não confiável?

10. Qual é a função da camada de acesso à rede?

11. Existem diversas semelhanças e diferenças entre os modelos TCP/IP e OSI. Enumere algumas delas.

12. Por quantos bits é composto um endereço IP e para qual a função?

13. Em quantas partes se divide um endereço IP?

14. Do seguinte endereço IP diga qual a parte correspondente ao ID da rede e ao ID do anfitrião.

15. O que é o ID de Rede e o ID de anfitrião?

16. Existem tipos de endereços diferentes? Se sim diga quais.

17. Existem cinco classes de endereços IP. Diga quais são explicando peplo menos uma delas.

18. Construa uma tabela onde mostre a faixa de endereços IP de cada classe.

19. Que tipo de endereço é o 127.X.X.X?

20. Existem mais endereços reservados para alem do 127.X.X.X?Quais?

21. O que são endereços públicos e endereços privados?

22. Como é calculado o n.º de sub redes utilizáveis e o nº de host utilizáveis?

23. O que é o IPv6 e para que serve?

24. Como se obtém um endereço IP?

25. Quais são os dois métodos de atribuição de endereços IP?

26. Como é atribuído um endereço IP utilizando RARP?

27. Qual é a função do protocolo BOOTP?

28. Para que serve o protocolo DHCP?

29. Como é dividido o Protocolo ARP?

30. Como funciona o protocolo ARP?

31. Quais são os serviços que incluem o serviço de transporte?

32. Como funciona o controlo de fluxo da camada de transporte?

33. O congestionamento durante a transferência de dados pode ocorrer por dois motivos. Quais?

34. O que é o TCP?

35. Qual a função do TCP?

36. O que é o UDP e para que serve?

37. O que acontece com as conversações que não usem números de portas conhecidos?

38. Para que serve o DNS?

39. O que é um domínio e de exemplo de alguns que conheça.

40. Qual é a finalidade do FTP?

41. Qual é o significado da http e qual é a função do HTML?

42. No URL: http://www.abc.com/edu/ para que serve o http://, o www., o abc.com, e o /edu/?

43. Os servidores de correio eletrónico comunicam-se utilizando que tipo de protocolo?

44. Qual o significado do protocolo SNMP e qual a sua função?

Bibliografia

Baptista, Carlos Pedro Zaragoza, *Fundamental dos Sistemas Digitais.* Lisboa: FCA – Editora Informática, 2003.

Gouveia, José; Magalhães, Alberto, *Curso Técnico de Hardware.* Lisboa: FCA – Editora Informática, 2003.

Gouveia, José; Magalhães, Alberto, *Hardware Montagem, Atualização, Detecção e Reparação de Avarias em PCs e Periféricos* 4ª ed.. Lisboa: FCA – Editora Informática, 2004.

Gouveia, José; Magalhães, Alberto. *Hardware para PC´s e Redes.* Lisboa: FCA – Editora Informática, 2004.

Loureiro, Paulo, *TCP / IP em Redes Microsoft – Para Profissionais.* Lisboa: FCA – Editora Informática, 2004.

Marques, José Alves; Guedes, Paulo, *Tecnologia de Sistemas Distribuídos.* Lisboa: FCA – Editora Informática, 2004.

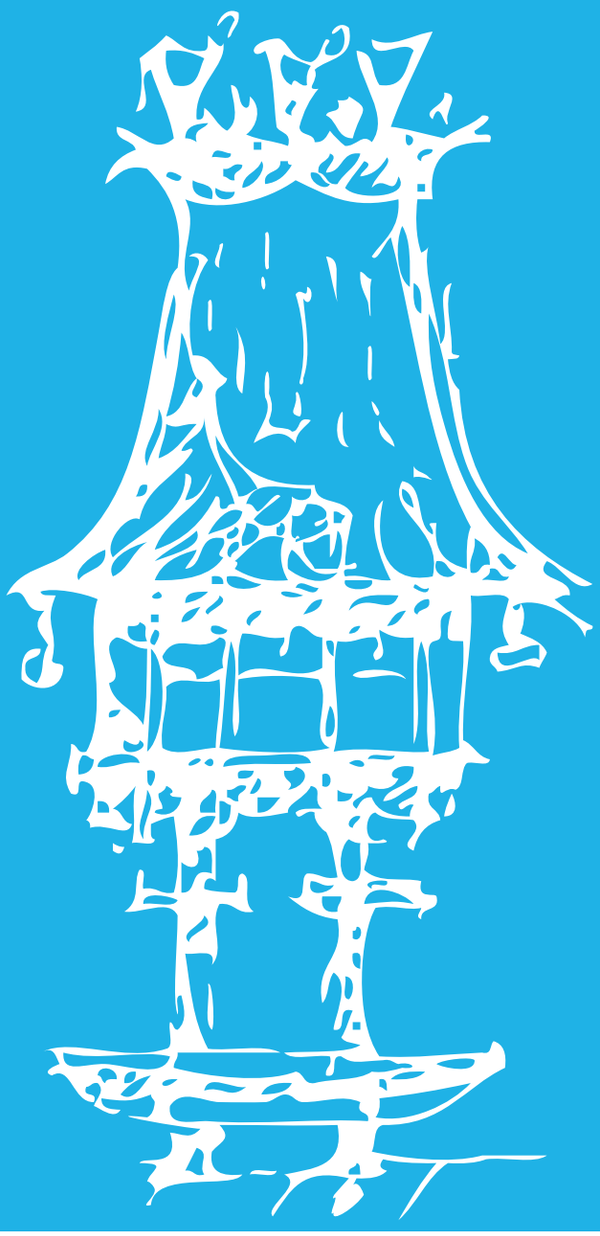
Monteiro, Edmundo; Boavista, Fernando, *Engenharia de Redes Informáticas.* Lisboa: FCA – Editora Informática, 2005.

Monteiro, Rui Vasco *et al.*, *Tecnologia dos Equipamentos Informáticos.* Lisboa: FCA – Editora Informática, 2005.

Nunes, Mário Serafim; Casaca, Augusto Júlio, *Redes Digitais Com Integração de Serviços.* Editorial Presença, 2001.

Rodrigues, Eleri; Magalhães, Maurício F., *Redes de comunicação*. DCA – FEEC UNICAMP, 1996. Rodrigues, Luís Silva, *Arquiteturas dos Sistemas de Informação.* Lisboa: FCA – Editora Informática, 2003.

Sousa, Sérgio, *Tecnologias de Informação - O que são? Para que Servem?* - 4ª ed.. Lisboa: FCA – Editora Informática, 2005.



Meios e Equipamentos de Transmissão de Dados

Módulo 4

Apresentação

Neste módulo abordaremos os meios de transmissão de dados que são usados em quase todas as redes locais. Estão disponíveis diferentes tipos de meios físicos, cada tipo tem as suas vantagens e desvantagens. Uma seleção cuidada dos meios físicos é a chave para uma operação eficiente de redes.

Vamos também estudar a forma como a fibra ótica é o meio mais usado para as transmissões ponto-a-ponto a grandes distâncias e colmata largura de banda necessárias para *backbones* das redes locais e em *WANs*. A conetividade física permitiu um aumento na produtividade, tornando possível a partilha de informação e meios. Os sistemas de redes tradicionais exigem que as estações de trabalho permaneçam estacionárias permitindo movimentação apenas dentro dos limites dos meios e da área de escritórios. Por último vemos como a tecnologia sem fio elimina essas restrições e oferece uma portabilidade verdadeira ao mundo da computação. Atualmente, a tecnologia sem fio não fornece transferências a alta velocidade, segurança ou confiabilidade no tempo de atividade nas redes com fios. Portanto, a flexibilidade da tecnologia sem fio justifica o sacrifício.

Objetivos de aprendizagem

- Compreender os meios físicos de transmissão como um dos principais componentes dos sistemas de comunicação;
- Agrupar os meios físicos em três famílias: meios metálicos, fibra ótica e sem fios;
- Conhecer e caraterizar os diversos meios de transmissão;
- Entender os condutores metálicos como o mais simples e divulgado meio físico de comunicação;
- Identificar e distinguir os vários meios de transmissão metálicos e sua aplicação;
- Distinguir os tipos de cabos de par trançado, nomeadamente a importância da versão UTP;
- Saber identificar os diferentes tipos de cabos, esquemas e ferramentas a utilizar;

- Elaborar diferentes tipos de cabos;
- Conhecer as vantagens e desvantagens da utilização de meios de fibra ótica;
- Distinguir os tipos de fibras óticas existentes;
- Compreender a crescente evolução e utilização dos meios sem fios;
- Distinguir as tecnologias disponíveis pelos meios sem fios;
- Enunciar as especificações, dimensionamento e caraterísticas dos diversos tipos de cablagem;
- Entender que os sistemas de cablagem devem ser genéricos, flexíveis e estruturados em níveis hierárquicos;
- Compreender a necessidade de serem garantidas as atividades de normalização;
- Distinguir equipamentos passivos e ativos e entender o seu papel na rede;
- Identificar os diversos equipamentos de interligação de redes;
- Conhecer as caraterísticas gerais e o respetivo modo de funcionamento dos diversos equipamentos de interligação, diagnóstico e teste;
- Saber efetuar testes a cablagem, nomeadamente o cabo de par entrançado;
- Identificar e saber utilizar outro equipamento de rede.

Âmbito de conteúdos

- A importância dos meios físicos de transmissão
- Meios de transmissão metálicos
  - Utilização e adaptação às exigências do mercado
  - Caraterísticas e propriedades
  - Linhas de condutores aéreos
  - Cabos simples
  - Cabos de pares entrançados
    - Importância e utilização
    - Designações de acordo com o tipo de blindagem
      - Cabo UTP como o mais utilizado
      - Ferramentas para os cabos UTP
    - Tipos de ligações e respetivos esquemas
    - Elaboração de cabos

- Cabos coaxiais
- Meios de Fibra Ótica
  - Vantagens e desvantagens
  - Caraterísticas e propriedades
  - Tipos de Fibras Óticas
- Meios sem fios
  - Crescente utilização e evolução
  - Ligações em micro-ondas
  - Ligações via rádio
  - Ligações em infravermelhos
  - Ligações laser
- Caraterização dos meios de transmissão
- Especificações
  - Cabos recomendados
  - Comprimentos máximos
  - Classes de ligações
  - Dimensionamento
- Cablagem estruturada
- Componentes da Cablagem estruturada
  - Equipamento Passivo e Ativo
- Equipamentos de interligação de redes
  - Repetidores
  - Concentradores
  - Pontes
  - Comutadores
  - Encaminhadores
  - Distribuidores

A importância dos meios físicos de transmissão

Nas redes de comunicação e computadores, os meios de transmissão são os caminhos físicos através dos quais ocorre a comunicação entre um determinado remetente e o seu respetivo destinatário. De maneira geral, podemos classificar os meios de transmissão em *guiados* e *não-guiados.* No caso dos meios guiados, temos uma comunicação que ocorre em meios físicos tais como os cabos coaxiais, pares entrançados e fibra ótica. Por outro lado, nos meios não-guiados, a comunicação é estabelecida utilizando-se a atmosfera terrestre ou o espaço. Este segundo tipo de transmissão é, usualmente, denominado de comunicação sem fios *(wireless).* Ainda em relação aos meios não-guiados, podemos citar os exemplos dos satélites, do uso de micro-ondas e do infravermelho.

De forma geral, na transmissão de dados, os dois aspetos mais importantes que devemos observar são os meios físicos de comunicação utilizados e as características dos sinais a serem transmitidos. A preocupação com estes fatores é a necessidade do estabelecimento de determinados parâmetros para atingirmos uma certa qualidade na transmissão.

Numa transmissão guiada, por exemplo, o cuidado que devemos observar para atingir uma qualidade de transmissão aceitável é o tipo de meio físico empregue na transmissão. Este é o fator limitante do ambiente. Por outro lado, numa comunicação onde utilizamos os meios não-guiados, a largura de banda do sinal gerado no dispositivo de transmissão sem fio é o ponto no qual devemos concentrar nossa atenção para uma transmissão satisfatória.

Meios de transmissão metálicos

Os condutores metálicos são os mais simples e mais divulgados meios físicos de comunicação usados na transmissão de sinais elétricos, ou seja, qualquer condutor que utilize um elemento metálico que conduza eletricidade. O condutor mais utilizado é o cobre. A forma como o condutor é disposto determina o tipo do cabo. Assim podemos ter os cabos coaxiais e os cabos trançados.

Existem diversos tipos de meio de transmissão, cada qual com as suas características próprias, tais como estas:

- Custo;
- Capacidade;
- Facilidade de Instalação;
- Atenuação;
- Imunidade a ruídos.

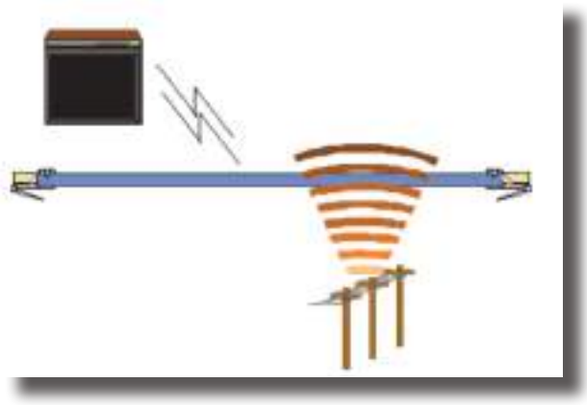
Custo: Geralmente é o fator decisivo para a aquisição ou expansão de um sistema. Quanto maior o custo de instalação e manutenção, mais difícil se torna a utilização do meio.

Capacidade: A sua forma física e técnica de fabricação determinam as características dos meios de transmissão e estas por sua vez determinam a faixa de passagem, ou seja, o espectro de frequências que podem circular pelo cabo sem grande atenuação. É a banda de frequência que o meio apresenta. Para nossos objetivos, a velocidade, em bps (bits por segundo) determina a capacidade do meio. Por exemplo, o cabo coaxial Ethernet tem uma capacidade de 10 Mbps e o cabo entrançado categoria 5 tem uma capacidade de 100 Mbps. Quanto maior é a taxa de transmissão, mais crítica ela se torna, sendo mais suscetível a interferência por ruídos.

Facilidade de Instalação: Quanto mais fácil for a instalação do meio, menor será o custo de implantação, expansão e manutenção.

Atenuação: São as perdas do sinal que trafega pelo meio e que são impostas pelas suas características elétricas nos cabos metálicos.

Imunidade à Ruídos: À exceção dos cabos óticos, todos os meios estão sujeitos a ruídos, ou seja, a interferência eletromagnética (EMI - Electromagnetic Interference), e a interferência por radiofrequência (RFI - Radio Frequency Interference) que surgem quando ondas eletromagnéticas cruzam o meio e tem intensidade suficiente para causar algum tipo de distorção no sinal.



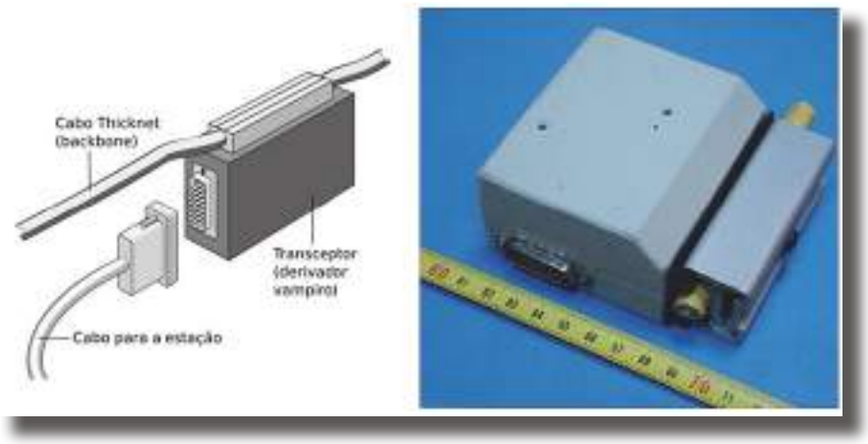
Os ruídos podem ainda ser classificados em quatro tipos. Ruído térmico, provocado pela agitação dos eletrões do condutor, presente em todos os canais de comunicação. Ruído de intermodulação, presente em sistemas multiplexados, Ruído de Diafonia onde o sinal de um condutor interfere no de outro. Ruído Impulsivo, aquele gerado de forma aleatória por sistemas de energia, iluminação, máquinas, etc.

Utilização e adaptação às exigências do mercado

Atualmente, as redes Ethernet de 100 megabits (Fast Ethernet) e 1000 megabits (Gigabit Ethernet) são as mais usadas. Ambos os padrões utilizam cabos de par entrançado categoria 5 ou 5e, que estão largamente disponíveis, o que facilita a migração de um para o outro. As placas também são compatíveis, pois podemos perfeitamente misturar placas de 100 e 1000 megabits na mesma rede, mas, ao usar placas de velocidades diferentes, a velocidade é sempre nivelada por baixo, ou seja, as placas Gigabit são obrigadas a respeitar a velocidade das placas mais lentas.

Antes deles, tivemos o padrão de 10 megabits, que também foi largamente usado (e ainda pode ser encontrado em algumas instalações) e, no outro extremo, já está disponível o padrão de 10 gigabits (10G), mil vezes mais rápido que o padrão original. Tal evolução obrigou também a melhorias nos cabos de rede.

As primeiras redes Ethernet utilizavam cabos thicknet, um tipo de cabo coaxial grosso e pouco flexível, com 1 cm de diâmetro. Um único cabo era usado como backbone para toda a rede e as estações eram conectadas a ele através de transcetores, também chamados de "vampire taps" ou "derivadores vampiros", nome usado porque o contato do transcetor perfurava o cabo thicknet, fazendo contato com o fio central. O transcetor era então ligado a um conector AUI de 15 pinos na placa de rede, através de um cabo menor.

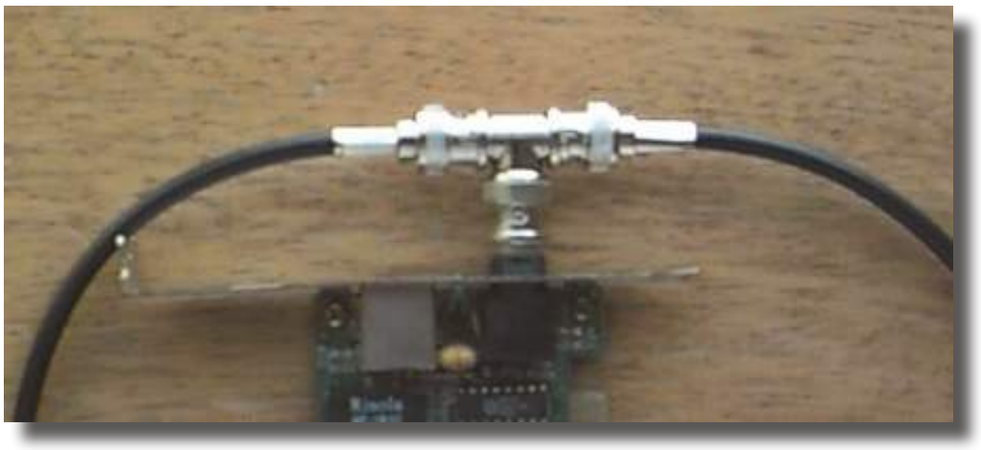


Este era essencialmente o mesmo tipo de cabo utilizado no protótipo de rede Ethernet desenvolvido no PARC (Palo Alto Research Center Incorporated), mas continuou a ser usado durante a maior parte da década de 80, embora oferecesse diversos problemas práticos, entre eles a dificuldade em se lidar com o cabo central, que era pesado e pouco flexível, sem falar no custo dos transcetores.

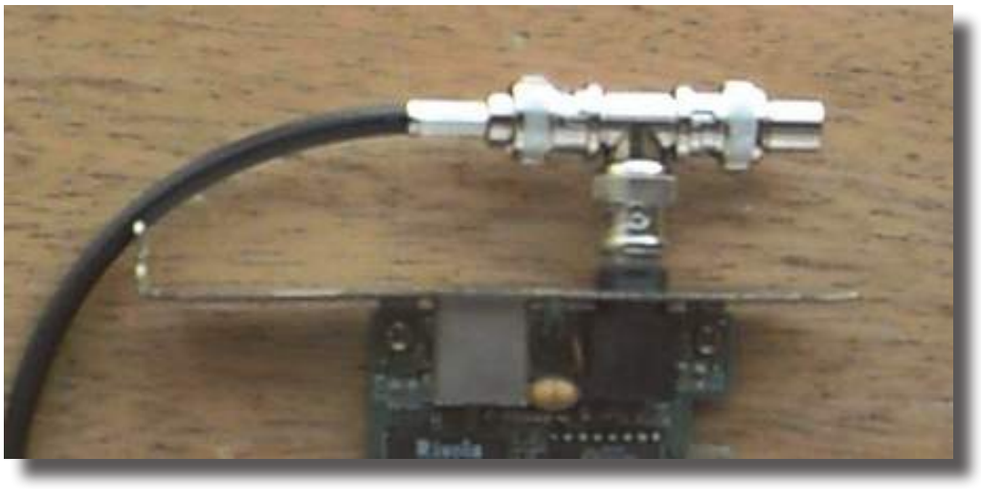
Estas redes eram chamadas de 10BASE-5, sigla que é a junção de 3 informações. O "10" se refere à velocidade de transmissão, 10 megabits, o "BASE" é abreviação de "baseband modulation", o que indica que o sinal é transmitido diretamente, de forma digital (sem o uso de modems, como no sistema telefónico), enquanto o "5" indica a distância máxima que o sinal é capaz de percorrer, nada menos do que 500 metros.

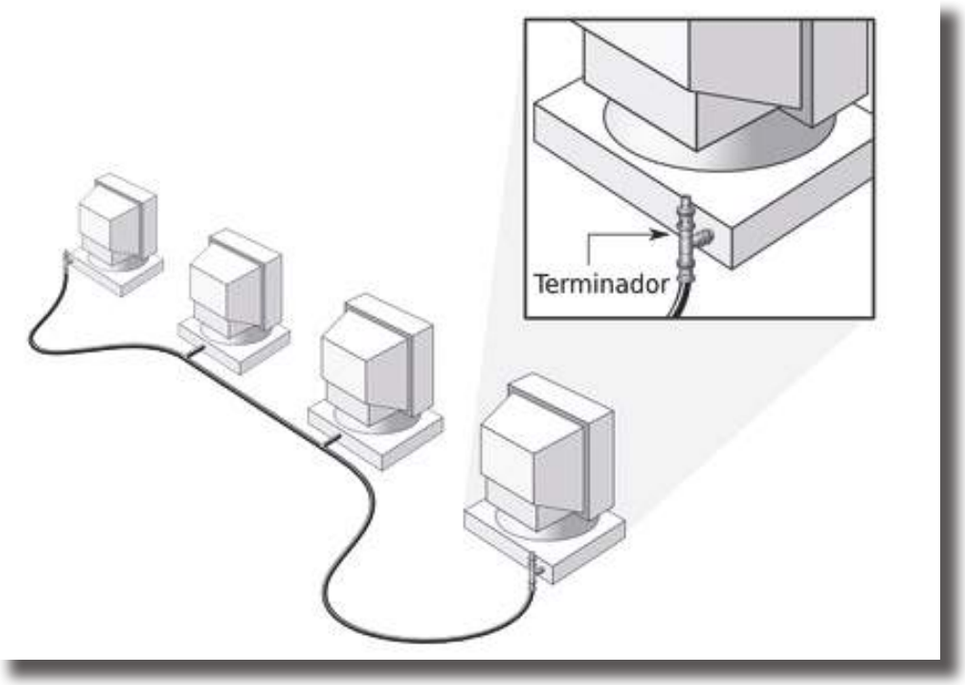
As redes 10BASE-5 logo deram origem às redes 10BASE-2, ou redes thinnet, que utilizavam cabos RG58/U, bem mais finos. O termo “thinnet” vem justamente da palavra “thin” (fino), enquanto “thicknet” vem de “thick” (espesso).

Nelas, os transcetores foram miniaturizados e movidos para dentro das próprias placas de rede e a ligação entre as estações passou a ser feita usando cabos mais curtos, ligados por um conector em forma de T. Ele permitiu que as estações fossem ligadas diretamente umas às outras, transformando os vários cabos separados em um único cabo contínuo.



Nas duas extremidades eram usados terminadores, que fecham o circuito, evitando que os sinais que cheguem ao final do cabo retornem na forma de interferência.





Apesar da importância, os terminadores eram dispositivos passivos, bastante simples e baratos. O grande problema era que, se o cabo fosse desligado em qualquer ponto (no caso de um cabo partido, ou com mal contacto, por exemplo), toda a rede ia abaixo, já que era dividida em dois segmentos sem terminação. Como não eram usados leds nem indicadores de conexão, existiam apenas duas opções para descobrir onde estava o problema: usar um testador de cabos (um aparelho que indicava com precisão em que ponto o cabo estava partido, mas que era caro) ou ir testando ponto por ponto, até descobrir onde estava o problema.

Temos aqui o conector BNC, incluindo a ponteira e a bainha, o conector T e o terminador que, junto com o cabo coaxial, eram os componentes básicos das redes 10BASE-2.

Os cabos podiam ser cravados na hora, de acordo com o comprimento necessário, usando um alicate especial. O cravamento consistia em descascar o cabo coaxial, encaixá-lo dentro do conector, cravar a ponteira, de forma a prender o fio central e de seguida cravar a bainha, prendendo o cabo ao conector BNC.

Assim como os alicates para cravamento de cabos de par entrançado que são vendidos atualmente, os alicates de cravamento de cabos coaxiais não eram muito caros.

Fig. 1: De*scarnador de cabos coa*xiais à esquerda e o alicate de cravar à direita

Apesar de ainda ser muito suscetível a problemas, o cabo das redes 10BASE-2 era muito mais simples e barato do que o das redes 10BASE-5, o que possibilitou a popularização das redes, sobretudo em empresas e escritórios. Se tivermos acesso a alguns micros 386 ou 486 antigos, é provável que encontre placas de rede que ainda incluem o conector AUI (para redes 10BASE-5), como a que é apresentada na figura a seguir.

Fig. 2: Placa de rede ISA com conetor AUI

A placa da foto é uma placa ISA de 10 megabits, que além do conector AUI, inclui o conector BNC para cabos coaxiais thinnet e o conector RJ45 para cabos de par entrançado atual. Estas placas foram muito usadas durante o início da década de 90, o período de transição entre os três tipos de cabeamento. Naturalmente, apesar das três fichas estarem presentes, só era possível utilizar um de cada vez. A vantagem era que se podia migrar dos cabos coaxiais para os cabos de par entrançado trocando apenas o cabeamento, sem precisar trocar as placas de rede.

A única desvantagem das redes thinnet em relação às thicknet é que o uso de um cabo mais fino reduziu o alcance máximo da rede, que passou a ser de apenas 185 metros, o que de qualquer forma era mais do que suficiente para a maioria das redes locais. Por incrível que possa parecer, o obsoleto padrão 10BASE-5 foi o padrão Ethernet para fios de cobre com o maior alcance até hoje, com os seus 500 metros. Apenas os padrões baseados em fibra ótica são capazes de superar esta marca.

Continuando, independentemente do tipo, os cabos coaxiais seguem o mesmo princípio básico, que consiste em utilizar uma camada de blindagem para proteger o cabo central de interferências eletromagnéticas presentes no ambiente. Quanto mais espesso o cabo e mais grossa é a camada de blindagem, mais eficiente é o isolamento, permitindo que o sinal seja transmitido a uma distância muito maior.

Fig. 3: Exemplo de cabo Coaxial

Apesar disso, os cabos coaxiais estão longe de entrar em desuso. Além de serem usados nos sistemas de TV a cabo e em outros sistemas de telecomunicação, eles são usados em todo tipo de antenas, incluindo antenas para redes wireless. Até mesmo as fichas tipo N, tipicamente usadas nas antenas para redes wireless de maior ganho são descendentes diretas das fichas BNC usadas nas redes 10BASE-2. Como pode ver, muitas tecnologias

que pareciam ser coisa do passado, acabam retornando de formas imprevisíveis.

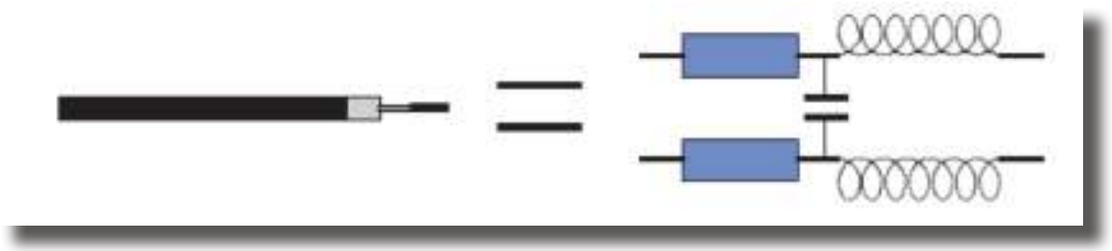
Existem diversas categorias de cabos de par entrançado (como veremos em detalhes no próximo capítulo), que se diferenciam pela qualidade e pelas frequências suportadas. Por exemplo, cabos de categoria 3, que são largamente utilizados em instalações telefónicas podem ser usados em redes de 10 megabits, mas não nas redes de 100 e 1000 megabits atuais. Da mesma forma, os cabos de categoria 5e que usamos atualmente não são adequados para as redes de 10 gigabits, que exigem cabos de categoria 6, ou 6a. Todos eles utilizam o mesmo conector, o RJ-45, mas existem diferenças de qualidade entre as fichas destinadas a diferentes padrões de cabos.

Os sucessores naturais dos cabos de par entrançado são os cabos de fibra óptica, que suportam velocidades ainda maiores e permitem transmitir a distâncias praticamente ilimitadas, com o uso de repetidores. Os cabos de fibra ótica são usados para criar os backbones que interligam os principais routers da Internet. Sem eles, a grande rede seria muito mais lenta e o acesso muito mais caro.

Caraterísticas elétricas dos cabos metálicos

Nos cabos metálicos existem características elétricas que devemos ter em conta, aquando da aquisição dos mesmos, para assim atenuar possíveis perdas de sinal e redução de ruido/interferências dos mesmos. Os principais aspetos a ter em conta são a:

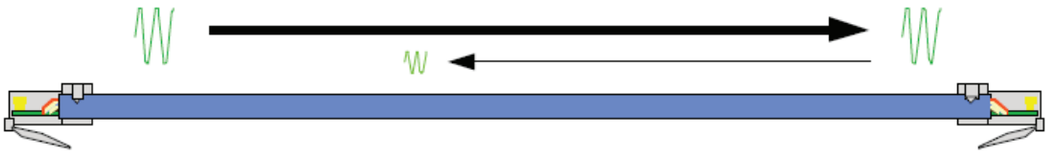
Impedância: É a resistência elétrica à passagem dos sinais elétricos de característica alternada, tais como os sinais de rede. A impedância é medida em Ohms e é sempre maior do que a resistência elétrica para sinais de característica contínua, tais como os que um medidor do tipo ohmímetro emite para medir a resistência elétrica. Na prática, o fato de um cabo ter uma dada impedância determina que todos os componentes que forem ligados a ele, tais como outros cabos e fichas, devem ter a mesma impedância, de forma a evitar perdas por reflexão dos sinais elétricos.



Atraso de Propagação: As componentes elétricas existentes no cabo fazem com que um sinal elétrico demore um tempo maior do que a velocidade da luz para percorrerem um cabo. Na prática, isto implica em que se houverem dispositivos separados por um cabo muito longo, estes podem não conseguir sincronizar suas operações.

Atenuação: É a redução da intensidade do sinal determinado pelo comprimento do cabo. Assim, quanto mais longo for o cabo, maior será a atenuação do sinal e, consequentemente, menos intenso chegará ao seu destino, ou seja se o cabo for muito longo nenhum sinal chega ao destino. Nos cabos metálicos, a atenuação é elétrica e nos cabos óticos é ótica. Em todo caso a unidade para medida de atenuação é o dB (decibell).

Ecos: São reflexões que ocorrem sempre que um sinal trafega por um meio que tem uma dada impedância e encontra um outro meio de impedância diferente, mesmo que esta diferença seja mínima. Esta impedância diferente pode surgir devido à utilização de um outro tipo de cabo, devido a um mau contacto ou a uma má ligação do cabo.



Cabos simples

Os cabos simples são construídos por dois ou mais condutores, normalmente de cobre envolvidos por um material isolante e agrupados em feixe com um isolamento exterior envolvente, ou dispostos lado-a-lado em faixa (flat cable).

Podem também dispor de blindagem exterior envolvente em fita ou malha metálica.

Neste tipo de ligações, um dos condutores é usado como referência elétrica comum (terra sinal), e os restantes são usados para transportar os sinais elétricos.

Linhas de condutores aéreos

As linhas de condutores aéreos são constituídas por um par de condutores de cobre nu, sendo o isolamento garantido pelo espaço livre que separa os condutores e presos a suportes físicos nas cruzetas dos postes telefónicos.

Este meio de comunicação foi muito usado no passado para transmissão de voz, encontrando-se, atualmente, em desuso.

Este meio de transmissão não pode ser usado para débitos elevados, nem para grandes distâncias, sendo típicas utilizações abaixo dos 19,2 Kbps em distâncias inferiores a 50 metros.

Cabos de pares entrançados

O cabo de par entrançado (Twisted pair) é um tipo de cabo que tem um feixe de dois fios no qual eles são entrançados um ao redor do outro para cancelar as interferências eletromagnéticas de fontes externas e interferências mútuas (linha cruzada ou, em inglês, crosstalk) entre cabos vizinhos. O numero de tranças (normalmente definida em termos de tranças por metro) é parte da especificação de certo tipo de cabo. Quanto maior o número de tranças, menor é o ruído. Foi um sistema originalmente produzido para transmissão telefónica analógica que utilizou o sistema de transmissão por par de fios.

Aproveita-se esta tecnologia que já é tradicional por causa do seu tempo de uso e do grande número de linhas instaladas. A matéria-prima fundamental utilizada para a fabricação destes cabos é o cobre, por oferecer ótima condutividade e baixo custo, portanto deve-se analisar com bastante cuidado a segurança contra descargas elétricas. Um acidente com descarga elétrica em qualquer ponto da rede pode comprometer toda a rede.

Designações de acordo com o tipo de blindagem

Uma questão importante relativa aos cabos entrançados é. Os cabos sem blindagem são mais baratos, mais flexíveis e mais fáceis de cravar e por isso são de longe os mais populares, mas os cabos blindados podem prestar bons serviços em ambientes com forte interferência eletromagnética, como grandes motores elétricos ou grandes antenas de transmissão que estejam muito próximas.

Outras fontes menores de interferências são as lâmpadas fluorescentes (principalmente lâmpadas desgastadas, são aquelas que estão sempre a piscar), cabos elétricos, quando colocados lado a lado com os cabos de rede, e mesmo telemóveis muito próximos dos cabos. Este tipo de interferência não chega a interromper o funcionamento da rede, mas pode causar perda de pacotes.

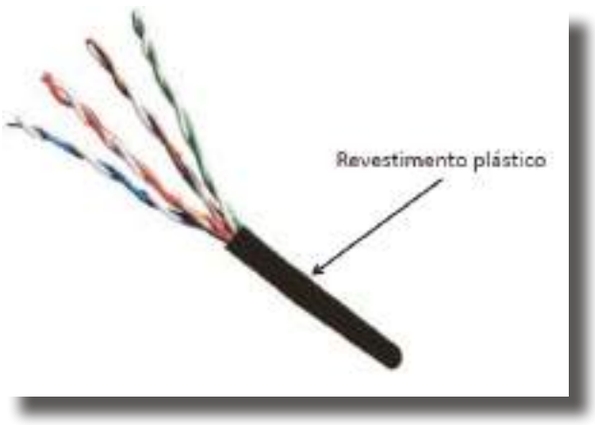
No final de cada pacote frame Ethernet são incluídos 32 bits de CRC, que permitem verificar a sua integridade. Ao receber cada frame, a estação verifica se a soma dos bits bate com o valor do CRC. Sempre que a soma der errado, ela solicita a retransmissão do pacote, o que é repetido indefinidamente, até que ela receba uma cópia intacta. Sobre este sistema de verificação feito pelas placas de rede (nível 2 do modelo OSI) ainda temos

a verificação feita pelo protocolo TCP (nível 4), que age de forma similar, verificando a integridade dos pacotes e solicitando retransmissão dos pacotes danificados. Esta dupla verificação garante uma confiabilidade muito boa.

Mesmo numa rede bem cablada, pacotes corrompidos esporadicamente são uma ocorrência normal, já que nenhuma cablagem é perfeita, mas um grande volume de perda de pacotes é um indício de que algo está errado. Quanto mais intensa for a interferência, maior será o volume de frames corrompidos e de retransmissões e pior será o desempenho da rede, tornando mais vantajoso o uso de cabos blindados.

Os cabos blindados, dividem em três categorias: FTP, STP e SSTP, já UTP não possuem blindagem.

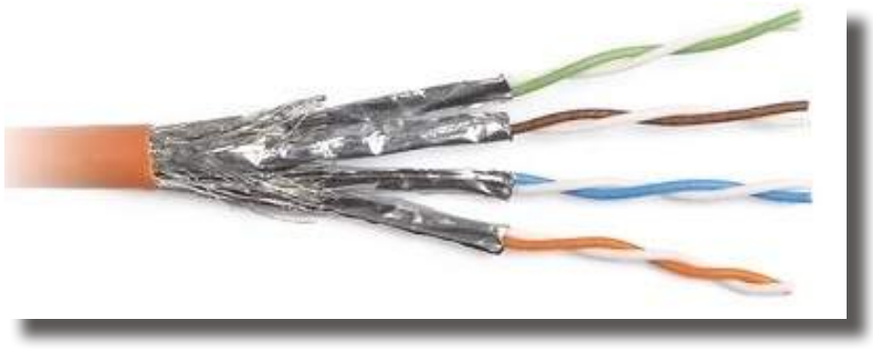
UTP (Unshielded Twisted Pair que significa, literalmente, "cabo de par entrançado sem blindagem") São os mais comuns em instalações residenciais e comerciais devido ao fácil manuseamento, instalação, permitindo taxas de transmissão de até 100 Mbps com a utilização do cabo CAT 5e. É o mais barato para distâncias de até 100 metros. A sua estrutura é de quatro pares de fios entrançados e revestidos por uma capa de PVC. Pela falta de blindagem este tipo de cabo não se recomenda instalar próximo de equipamentos que possam gerar campos magnéticos (fios de rede elétrica, motores, inversores de frequência) e também não podem ficar em ambientes com humidade.



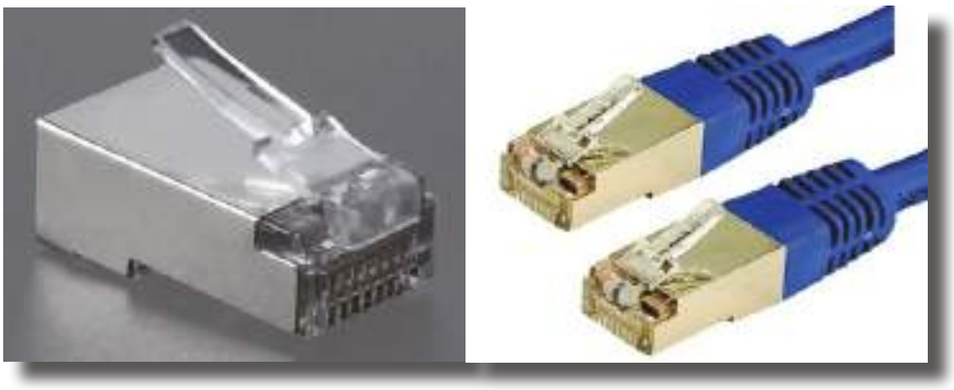
FTP (Foiled Twisted Pair) são os que utilizam a blindagem mais simples. Neles, uma fina folha de aço ou de liga de alumínio envolve todos os pares do cabo, protegendo-os contra interferências externas, mas sem fazer nada em relação ao crosstalk, ou seja, a interferência estre os pacotes de cabos:

STP (Shielded Twisted Pair) vão um pouco além, usando uma blindagem individual para cada par de cabos. Isso reduz o crosstalk e melhora a tolerância do cabo em relação à distância, o que pode ser usado em situações onde for necessário cravar cabos fora do padrão, com mais de 100 metros.

SSTP (Screened Shielded Twisted Pair), também chamados de SFTP (Screened Foiled Twisted Pair), que combinam a blindagem individual para cada par de cabos com uma segunda blindagem externa, envolvendo todos os cabos, o que torna os cabos especialmente resistentes a interferências externas. Eles são mais adequados a ambientes com fortes fontes de interferências.



Para melhores resultados, os cabos blindados devem ser combinados com fichas RJ-45 blindadas. Estas incluem uma proteção metálica que protege a parte destrançada do cabo que vai dentro da ficha, evitando que ela se torne o elo mais fraco da cadeia.



Quanto maior for o nível de interferência, menor será o desempenho da rede, menor será a distância que poderá ser usada entre os computadores e mais vantajosa será a instalação de cabos blindados. Em ambientes normais, porém, os cabos sem blindagem funcionam perfeitamente bem, justamente por isso os cabos blindados são relativamente pouco usados.

Cabo UTP como o mais utilizado

O cabo UPT é o mais utilizado em redes de escritórios e empresas onde não há a necessidade de um isolamento de sinal muito grande. Como já foi dito este tipo de cabos possui quatro pares de cobre entrançados e cobertos com uma proteção externa simples que apenas mantem os fios juntos e protege-os evitando assim de serem amassados e/ou partidos facilmente.

Uma das grandes vantagens é a sua flexibilidade e espessura. O UTP não preenche as tubagens com tanta rapidez como os outros tipos de cabos com blindagem. Isto faz aumentar o numero de conexões possíveis sem diminuir seriamente o espaço útil.

Os cabos UTP foram padronizados pelas normas da EIA/TIA com a norma 568 e são divididos em categorias, levando em conta o nível de segurança e o diâmetro do fio, onde os números maiores indicam fios com diâmetros menores.

NOTA: Em todas as categorias, a distância máxima permitida é de 100 metros (com exceção das redes 10G com cabos categoria 6, onde a distância máxima cai para apenas 55 metros). O que muda é a frequência e, consequentemente, a taxa máxima de transferência de dados suportada pelo cabo, e o nível de imunidade a interferências externas.

Categorias 1 e 2: Estas duas categorias de cabos não são mais reconhecidas pela TIA (Telecommunications Industry Association), que é a responsável pela definição dos padrões de cabos. Elas foram usadas no passado em instalações telefónicas e os cabos de categoria 2 chegaram a ser usados em redes Arcnet de 2.5 megabits e redes Token Ring de 4 megabits, mas não são adequados para uso em redes Ethernet.

Categoria 3: Este foi o primeiro padrão de cabos de par entrançado desenvolvido especialmente para uso em redes. O padrão é certificado para sinalização de até 16 MHz, o que permitiu o seu uso no padrão 10BASE-T, que é o padrão de redes Ethernet de 10 megabits para cabos de par entrançado. Existiu ainda um padrão de 100 megabits para cabos de categoria 3, o 100BASE-T4, mas é pouco usado e não é suportado por todas as placas de rede.

A principal diferença do cabo de categoria 3 para os obsoletos cabos de categoria 1 e 2 é o entrançamento dos pares de cabos. Enquanto nos cabos 1 e 2 não existe um padrão definido, os cabos de categoria 3 (assim como os de categoria 4 e 5) possuem pelo menos 24 tranças por metro e, por isso, são muito mais resistentes a ruídos externos. Cada par de cabos tem um número diferente de tranças por metro, o que atenua as interferências entre os pares de cabos.

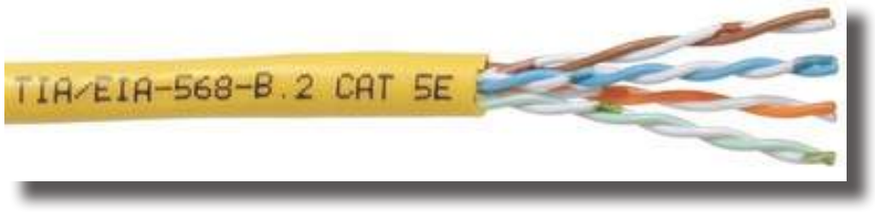
Categoria 4: Esta categoria de cabos tem uma qualidade um pouco superior e é certificada para sinalização de até 20 MHz. Cabos com esta categoria foram usados em redes Token Ring de 16 megabits e também podiam ser utilizados em redes Ethernet em substituição aos cabos de categoria 3, mas na prática não se usa. Assim como as categorias 1 e 2, a categoria 4 também já não é reconhecida pela TIA e os cabos já não são fabricados, ao contrário dos cabos de categoria 3, que continuam a ser usados em instalações telefónicas.

Categoria 5: Os cabos de categoria 5 são o requisito mínimo para redes 100BASE-TX e 1000BASE-T, que são, respetivamente, os pacotes de rede de 100 e 1000 megabits usados atualmente. Os cabos cat 5 seguem padrões de fabrico muito mais estritos e suportam frequências de até 100 MHz, o que representa um grande salto sobre os cabos cat 3.

Apesar disso, é muito raro encontrar cabos cat 5 à venda atualmente, pois eles foram substituídos pelos cabos **categoria 5e** (o "e" vem de "enhanced"), uma versão aperfeiçoada do padrão, com normas mais estritas, desenvolvidas de forma a reduzir a interferência entre os cabos e a perda de sinal, o que ajuda em cabos mais longos, perto dos 100 metros permitidos.

Os cabos cat 5e devem suportar os mesmos 100 MHz dos cabos cat 5, mas este valor é uma especificação mínima e não um número exato. Nada impede que fabricantes produzam cabos acima do padrão, certificando-os para frequências mais elevadas. Com isto, não é difícil encontrar no mercado cabos cat 5e certificados para 110 MHz, 125 MHz ou mesmo 155 MHz, embora na prática isso não faça muita diferença, já que os 100 MHz são suficientes para as redes 100BASE-TX e 1000BASE-T.

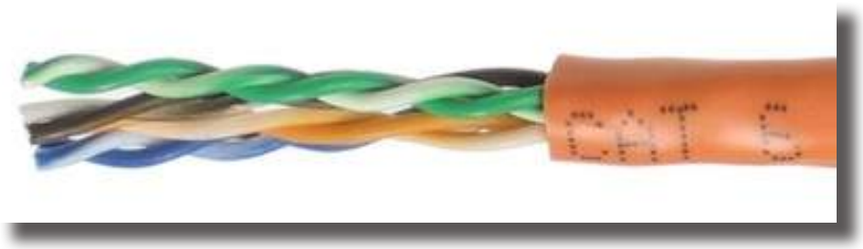
É fácil descobrir qual é a categoria dos cabos, pois a informação vem decalcada no próprio cabo, como na imagem a seguir.



Os cabos 5e são os mais comuns atualmente, mas estão em processo de substituição pelos cabos categoria 6 e categoria 6a, que podem ser usados em redes de 10 gigabit.

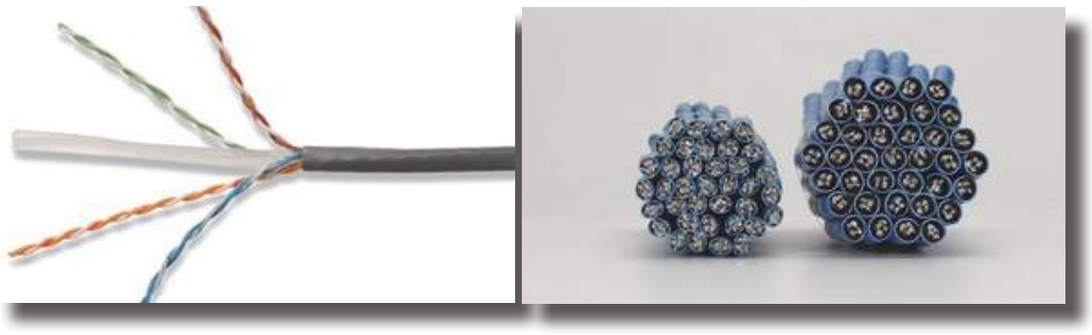
Categoria 6: Esta categoria de cabos foi originalmente desenvolvida para ser usada no padrão Gigabit Ethernet, mas com o desenvolvimento do padrão para cabos categoria 5 a sua adoção acabou por ser retardada, já que, embora os cabos categoria 6 ofereçam uma qualidade superior, o alcance continua sendo de apenas 100 metros, de forma que, embora a melhor qualidade dos cabos cat 6 seja sempre desejável, acaba por não existir muito ganho na prática.

Os cabos categoria 6 utilizam especificações ainda mais estritas que os de categoria 5e e suportam frequências de até 250 MHz. Além de serem usados em substituição dos cabos cat 5 e 5e, eles podem ser usados em redes 10 gigabit, mas nesse caso o alcance é de apenas 55 metros.



Para permitir o uso de cabos de até 100 metros em redes 10G foi criada uma nova categoria de cabos, a **categoria 6a** ("a" de "augmented", ou ampliado). Estes suportam frequências de até 500 MHz e utilizam um conjunto de medidas para reduzir a perda de sinal e tornar o cabo mais resistente a interferências.

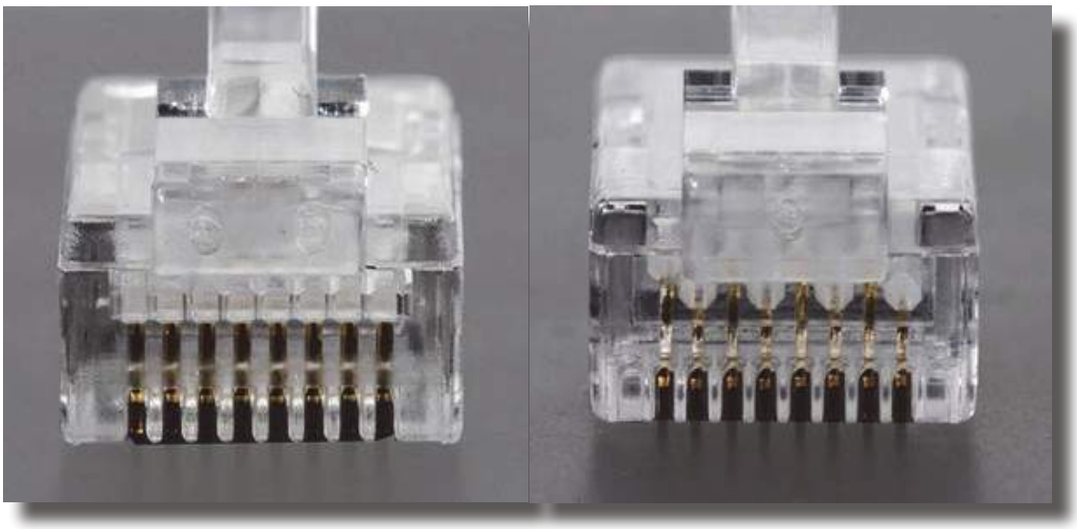
Uma das medidas para reduzir o crosstalk (interferências entre os pares de cabos) no cat 6a foi distanciá-los usando um separador. Esta separação aumentou a espessura dos cabos de 5.6 mm para 7.9 mm e tornou-os um pouco menos flexíveis. A diferença pode parecer pequena, mas ao juntar vários cabos o espaço ocupado já se torna considerável.



É importante notar que existem também diferenças de qualidade entre as fichas RJ-45 destinadas a cabos categoria 5 e os cabos cat6 e cat6a, de forma que é importante verificar as especificações.

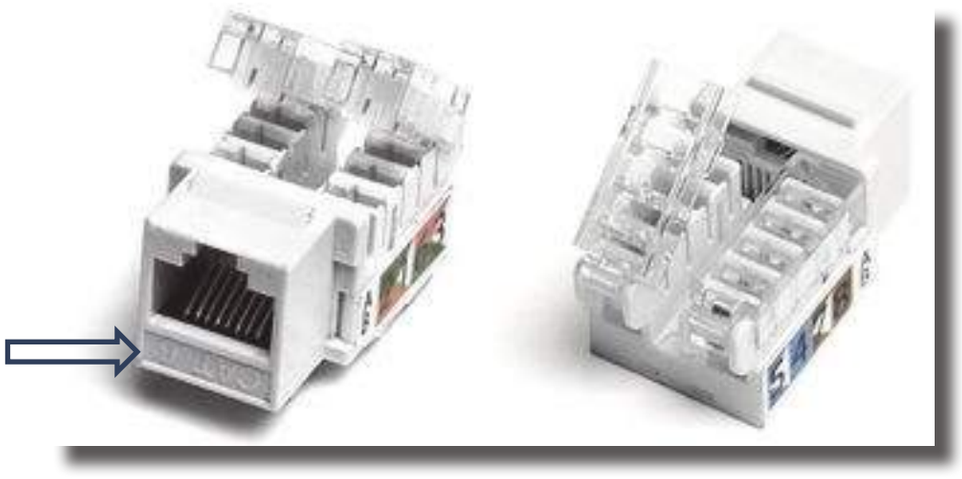
Aqui temos um conector RJ-45 cat 5 (imagem da esquerda) ao lado de um cat 6 (Imagem da direita). Vendo os dois lado a lado é possível notar pequenas diferenças, a principal delas é que no conector cat 5 os 8 fios do cabo ficam lado a lado, formando uma linha

reta enquanto no conector cat 6 eles são dispostos em zig-zag, uma medida para reduzir o cross-talk e a perda de sinal.



Embora o formato e a aparência seja a mesma, as fichas RJ-45 destinadas a cabos cat 6 e cat 6a utilizam novos materiais, suportam frequências mais altas e introduzem muito menos ruído no sinal. Utilizando fichas RJ-45 cat 5, a sua cablagem é considerada cat 5, mesmo que sejam utilizados cabos cat 6 ou 6a.

O mesmo se aplica a outros componentes de cablagem, como patch-panels, tomadas, keystone jacks (as fichas fêmea usadas em tomadas de parede) e assim por diante. Componentes cat 6 costumam trazer a categoria decalcada (uma forma de os fabricantes diferenciarem os seus produtos, já que componentes cat 6 e 6a são mais caros), como neste keystone jack onde se nota o “CAT 6” escrito em baixo relevo.



Existem também os cabos **categoria 7**, que podem vir a ser usados no padrão de 100 gigabits, que está em estágio inicial de desenvolvimento.

Outro padrão que pode vir (ou não) a ser usado no futuro são as fichas TERA, padrão desenvolvido pela Siemon. Embora muito mais caro e complexo que as fichas RJ45 atuais, o TERA oferece a vantagem de ser inteiramente blindado e utilizar um sistema especial de encaixe, que reduz a possibilidade de mau contato.

Cabos de padrões superiores podem ser usados em substituição de cabos dos padrões antigos, além de trazerem a possibilidade de serem aproveitados nos padrões de rede seguintes. Entretanto, investir em cabos de um padrão superior ao que se realmente precisa nem sempre é uma boa ideia, já que cabos de padrões recém-introduzidos são mais caros e difíceis de encontrar. Além disso, não existe garantia de que os cabos usados serão mesmo suportados dentro do próximo padrão de redes até que ele esteja efetivamente concluído.

Por exemplo, quem investiu em cabos de categoria 6, a pensar em aproveitá-los em redes de 10 gigabits acabou por ficar frustrando, pois no padrão 10G a distância máxima usando cabos cat 6 é de apenas 55 metros e foi introduzido um novo padrão, o 6a. O mesmo pode acontecer com os cabos categoria 7, não existe nenhuma garantia de que eles sejam mesmo suportados no padrão de 100 gigabits. Pode muito bem ser introduzido um novo padrão de cabos, ou até mesmo que os cabos de cobre sejam abandonados a favor dos de fibra ótica.

Ferramentas para os cabos UTP

Independentemente do tipo de rede que se pretenda instalar, seja ela uma rede local doméstica ou empresarial, em ambas vamos precisar de montar o cabo de rede.

O tipo de padrão mais comum é o de Categoria 5 (também chamado de cat5, ou UTP5), que suporta velocidades de até 100 Mb/s (Megabits por segundo).

Serão apresentadas a seguir ferramentas utilizadas na montagem do cabo.

Cabo UPT Cat 5:

Normalmente pode ser encontrado em caixas de 150/300 metros de cabo, porém normalmente as lojas vendem também por metro.

Sempre que possível use cabos de boa qualidade! Um cablagem bem feita depende muito da qualidade do cabo, além de também influenciar na montagem das fichas nas extremidades do mesmo. Os cabos categoria 5 possuem 4 pares de fio coloridos. Atenção neste item, pois cabos de boa qualidade possuem os padrões de cores facilmente identificáveis (atenção aos fios branco/cor).

Fichas RJ-45:

Por norma são muito baratas (caso não se tenha muita prática em ligação de cabos de rede, é bom ter algumas de reserva "extra" para possíveis defeitos na hora da montagem dos cabos de rede).

Alicate de cravar:

Normalmente é a ferramenta mais cara neste tipo de montagem de rede por conta própria (existem testadores de cabos que são muito caros, mas são utilizado em montagens profissionais de grandes redes). Volta-se a recomendar que uma ferramenta de má qualidade, pensando somente no preço, pode resultar em problemas ao cravar as fichas no cabo, muitas vezes imperceptíveis inicialmente, mas originando no futuro erros de rede que poderão ocupar muito do nosso tempo num eventual problema na rede.

Normalmente estes alicates permitem a utilização para fichas RJ45 como RJ11 (usadas em telefones). Também possuem uma secção para "corte" dos cabos e para descarnar o isolamento.

Alicate de corte:

De secção diagonal com isolamento e de tamanho pequeno preferencialmente.

Testador de cabo:

Apesar de não ser uma ferramenta obrigatória, é possível encontrar modelos simples e não muito caros, que poderão ser de grande ajuda na montagem dos cabos.

Tipos de ligações e respetivos esquemas

Antes de iniciar o cravamento de fichas, é necessário escolher um dos padrões de sequência para as fichas. Existem dois padrões utilizados: eles são conhecidos como EIA/TIA 568A e EIA/TIA 568B. Ambos funcionam perfeitamente.

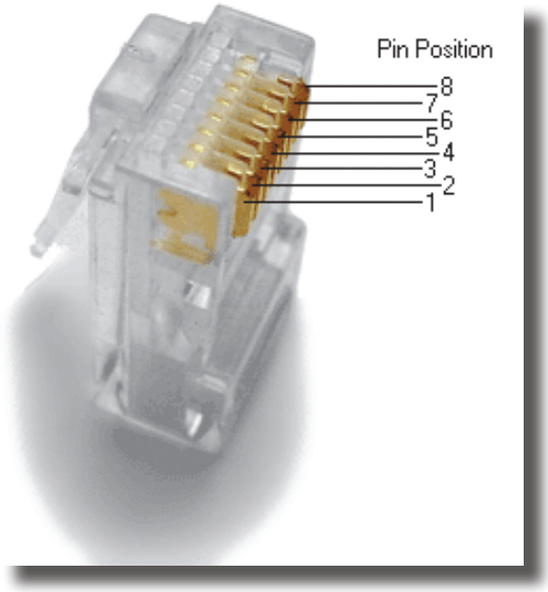


Fig. 4: Numeração dos pinos da ficha RJ-45

Existem ainda dois tipos de cabo: os cabos diretos, e os cabos crossover.

Nos cabos diretos, ambas as pontas são feitas utilizando o mesmo padrão, enquanto nos cabos crossover uma ponta utiliza o padrão EIA/TIA 568A e outra o EIA/TIA 568B.

Cabo Direto:

Os cabos diretos são utilizados para interligar computadores com HUBs/Switchs. Nestes cabos, as pontas devem ser exatamente iguais, pois caso contrário a transferência de dados não irá ocorrer. O padrão utilizado em um dos cabos deverá ser o mesmo na rede inteira.

É verdade que se pode criar a própria sequência e utilizá-la na nossa rede, entretanto é extremamente aconselhável que se utilize uma destas duas sequências sugeridas. Não apenas por questões de funcionamento correto, mas também por questões de padronização. Se outra pessoa precisar corrigir algum problema nos nossos cabos, ela saberá qual é a sequência utilizada e será muito mais fácil para resolver o problema.

Cabo Direto CAT5 (EIA 568B)	
FICHA #1	**FICHA#2**
Branco/Laranja	Branco/Laranja
Laranja	Laranja
Branco/Verde	Branco/Verde
Azul	Azul
Branco/Azul	Branco/Azul
Verde	Verde
Branco/Castanho	Branco/Castanho
Castanho	Castanho

FICHA #1 **FICHA #2**

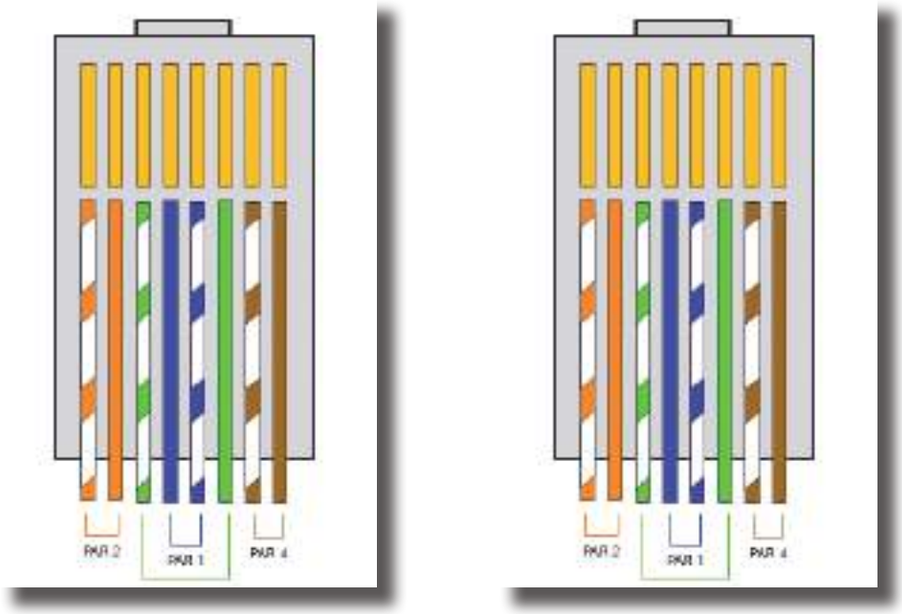


Fig. 5: Cabo UTP direto

Cabo Crossover:

Caso seja necessário interligar apenas dois computadores, é possível utilizar um cabo do tipo crossover, o qual dispensa o uso de HUB/Switch. Se for preciso partilhar a internet, será necessário que um dos dois computadores possua duas placas de rede. Numa delas liga-se o cabo crossover e na outra liga-se o cabo da internet, o qual será um cabo direto. Os cabos crossover também devem ser utilizados para ligar um HUB/Switch a outro.

Segue a seguir a tabela com a fiação respetiva de cada ficha

Cabo Crossover CAT5 (EIA 568B e EIA 568A)	
FICHA #1	**FICHA#2**
Branco/Laranja	Branco/Verde
Laranja	Verde
Branco/Verde	Branco/Laranja
Azul	Azul
Branco/Azul	Branco/Azul
Verde	Laranja
Branco/Castanho	Branco/Castanho
Castanho	Castanho

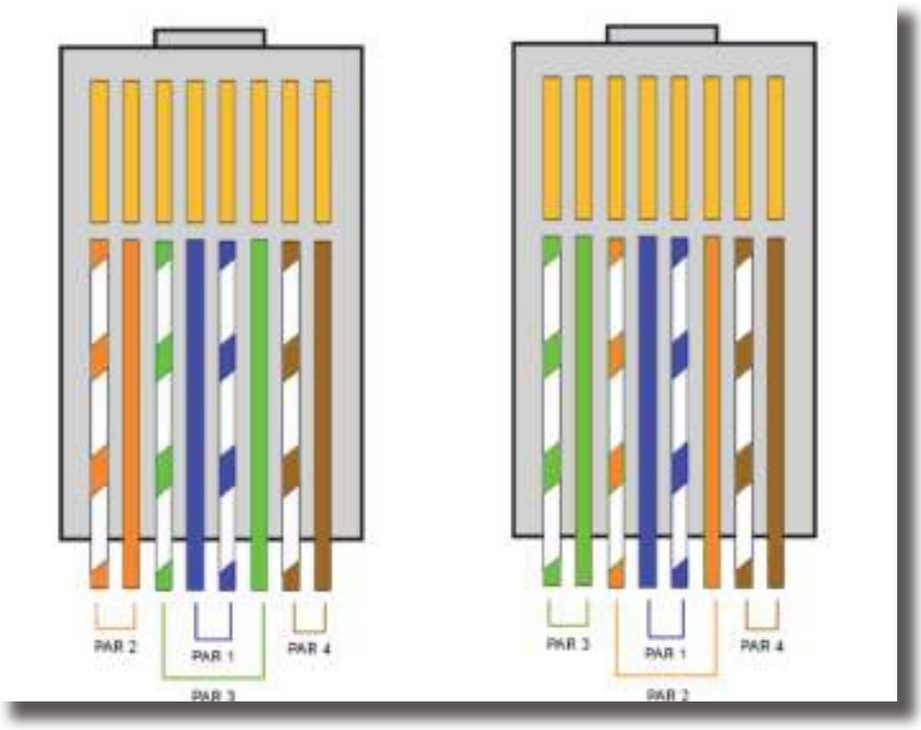
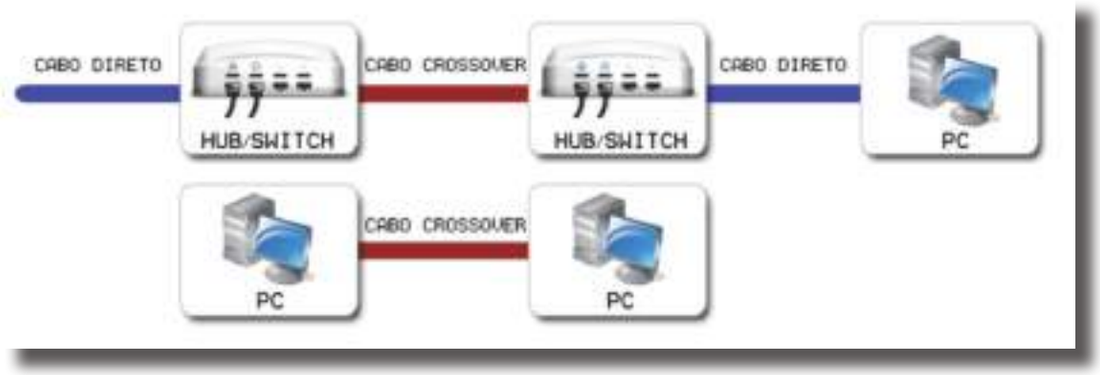


Fig. 6: Cabo UTP crossover

Segue um exemplo do funcionamento com os dois tipos de cabos.



Elaboração de cabos

Agora que já sabemos os tipos de cabo e quando devemos utiliza-los, e também já conhecemos o alicate de cravar, é possível fazermos o nosso próprio cabo de rede. Escolhemos um padrão de sequência para as pontas dos cabos e usamos apenas este padrão em toda a rede (salvo em casos de conexão de HUB/Switch com outro HUB/Switch, que é quando é necessário o uso do cabo crossover).

Corte do cabo

Corta-se um pedaço do cabo de rede do tamanho que precisarmos.

NOTA: Não é possível fazer emendas, portanto, ao medir o tamanho necessário, tenha muito cuidado, considere curvas, subidas, descidas, saliências, reentrâncias, etc. E não se esqueça: se sobrar é possível cortar, mas se faltar a solução fica bem mais cara.

Após a medição faça um corte reto e limpo, como na imagem abaixo.

Fig. 7: Cabo UTP após corte

Corte um pedaço da capa do cabo. Para isso colocamos o cabo no compartimento para descarnar a proteção do cabo e giramos o alicate, de modo que a proteção que envolve o cabo seja cortada. Não utilize muita força, pois se fizer isso você poderá cortar um dos fios internos do cabo. Caso isso ocorra, reinicie o processo.

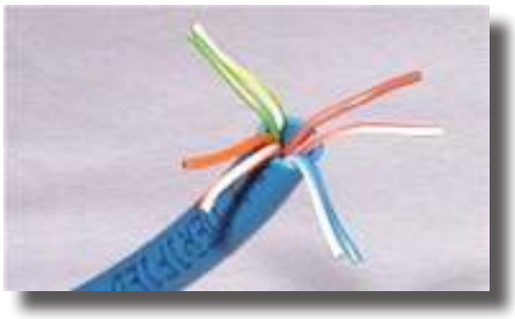
Fig. 8: Corte da capa do cabo

Os cabos coloridos estarão separados em pares, e cada par possui uma cor específica. Separe os cabos estique-os para deixá-los bem lisos, para que assim fique mais fácil e eficiente de se trabalhar com eles.

Preparação/separação do cabo:

Após o corte da proteção do cabo, é necessário separar os cabos/fios internos conforme a cor de cada um.

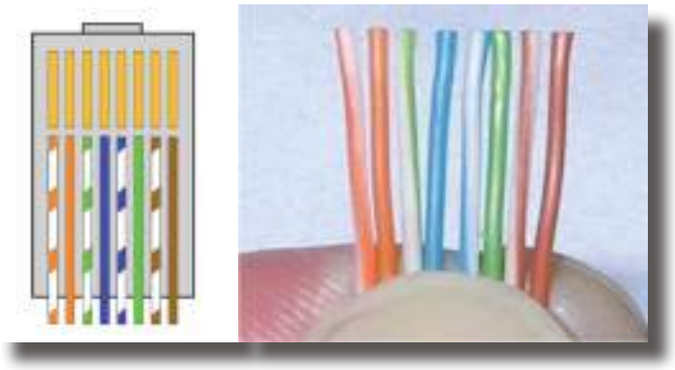
Verá que são 4 pares de cabo coloridos, sendo cada par composto por uma cor (azul, verde, laranja ou castanho), e seu "par" branco (branco com listas azuis, branco com listas verdes, branco com listas laranja, branco com listas castanhas).



Agora que os cabos internos estão separados, deverá alinhá-los conforme a ordem desejada (se é um cabo direto ou um cabo cross-over), da esquerda para a direita.

NOTA: A ordem é importante pois seguem um padrão definido na indústria, e mesmo funcionando utilizando um padrão diferente, poderá resultar em mais trabalho na hora de fazer algum tipo de manutenção posterior no cabo, ou identificação, etc. A prática normalmente ensina-nos que é muito mais prático e rápido seguir um padrão

Seguindo o padrão da imagem em baixo, alinhe os cabos internos no seu dedo indicador, de maneira uniforme. Após o alinhamento, corte as pontas, de maneira a que fiquem exatamente do mesmo tamanho, e com cerca de 1 a 1,5 centímetros da capa de isolamento.



Colocação da ficha RJ-45

A maneira mais prática de inserir o cabo numa ficha RJ-45 é da seguinte maneira:

- Segure a ficha RJ-45 firmemente, numa das mãos e o cabo separado na outra, como a figura acima.
- A medida que for inserindo os cabos para dentro da ficha, force os cabos de forma CONJUNTA, para que não haja problemas de contacto. Empurre os

cabos verificando bem se todos estão a seguir o caminho correto dentro da ficha, mantendo-se paralelos. É possível sentir uma pequena resistência, mas a ficha e o cabo são dimensionados para entrar justos, sem folgas, e sem muita dificuldade.

- Empurre os cabos por toda a extensão da ficha RJ-45. Eles devem encostar à parede contrária ao orifício de entrada. É possível conferir olhando de lado (como na imagem abaixo) e na parede onde eles terminam (uma série de pontos). Se algum dos cabos não tiver entrado corretamente, temos de retirar a ficha e começar novamente.
- No final, forçamos um pouco o revestimento do cabo entrançado, de forma que este revestimento passe completamente o ressalto na ficha (que será pressionado pelo alicate de cravar mais tarde). Veja na imagem lateral abaixo. Inserir todos os cabos corretamente, sem folgas, de forma justa, é puramente jeito e pratica. Depois de vários cabos, estaremos mais à vontade nesta tarefa e parecerá muito mais simples que na primeira vez, porém as primeiras.

Fig. 9: Ficha mal cravada

Fig. 10: Ficha bem cravada

Cravar o cabo com o alicate

Antes de partir para o uso do alicate, verifique novamente se os cabos estão bem montados nas fichas: os fios até ao fim e a capa de cobertura a passar o ressalto da ficha. Estando tudo ok, insira a ficha montada, com cuidado para não desmontar, na abertura própria do seu alicate de cravar (veja imagem abaixo).

Fig. 11: Alicate a cravar ficha RJ-45

Com a outra mão no alicate, comece a apertar, finalizando com as 2 mãos em um bom aperto, porém sem partir a ficha.

Após este procedimento, verifique lateralmente na ficha se todos os contactos foram para dentro da ficha, estando uniformes e a encostar nos fios. Se houver algum problema, que não seja falta de pressão no alicate, não há como recuperar a ficha, o cabo deverá ser retirado, ou cortado, e a ficha estará perdida.

DICA: Verifique sempre com cuidado se as ligações estão bem feitas, se os fios estão bem encaixados e os contactos bem feitos. Se tiver um testador de cabos, aproveite para de seguida testar se está tudo ok. Verifique com atenção se os cabos serão diretos ou crossover na montagem dos fios na ficha.

Cabos coaxiais

Um cabo coaxial consiste num fio de cobre rígido que forma o núcleo, envolto por um material isolante que, por sua vez, é envolto num condutor cilíndrico, frequentemente na forma de uma malha entrelaçada. O condutor externo é coberto por uma capa plástica protetora, que o protege contra o fenômeno da indução, causada por interferências elétricas ou magnéticas.

Fig. 12: Camadas do cabo coaxial

Além da utilização em redes locais, é muito usado para sinais de televisão, como por exemplo, transmissão de TV por cabo. Muitas empresas também o usam na construção de sistemas de segurança, sistemas de circuitos fechados de TV e outros.

O cabo coaxial está melhor protegido do que o cabo de par entrançado e por isso pode transmitir a maiores distâncias e a velocidades maiores. São utilizados dois tipos de cabos coaxiais:

Cabo de 50 ohms, frequentemente usado para transmissão digital;

Cabo de 75 ohms, é mais usado para transmissão analógica.

A construção e proteção do cabo coaxial dão uma boa combinação de largura de banda e excelente imunidade ao ruído. Para distâncias de até um 1 km são permitidas velocidades de até 2 Gbps. Eram muito usados na área dos telefones, porém estão a ser substituídos por fibras óticas.

Atualmente são muitos usados na área de TV por cabo.

Os cabos de 50 ohms foram muito usados em redes nos anos 80 e início dos 90, eles eram basicamente de dois tipos o coaxial fino e o grosso.

- Coaxial Grosso - usava fichas do tipo vampiro, e eram também conhecidos por yelow cable;
- Coaxial Fino - usava as fichas T que são mais comuns e mais baratos, estes tipos de cabos ainda são encontrados em algumas instalações de redes locais.

Cabo coaxial grosso

Também conhecido como cabo coaxial banda larga ou 10BASE5, é utilizado para transmissão analógica. A especificação 10BASE5 refere-se à transmissão de sinais Ethernet utilizando esse tipo de cabo. O 5 informa o tamanho máximo aproximado do cabo como sendo de 500 metros.

Fig. 13: Cabo coaxial grosso

Este cabo tem uma cobertura plástica protetora extra que ajuda a manter a humidade longe do condutor central. Esta cobertura torna o cabo coaxial grosso numa boa escolha quando se utilizam grandes comprimentos numa rede de barramento linear. Durante a instalação, o cabo não precisa de ser cortado pois a ficha (*vampire tap*) perfura-o.

A impedância utilizada nesta modalidade de transmissão é de 75 Ohms. O seu diâmetro externo é de aproximadamente 0,4 polegadas ou 9,8 mm.

O cabo coaxial de 75 ohms é usado para transmissão analógica em sistemas de TV por cabo. Ele é chamado de broadband (banda larga). Embora o termo “broadband” venha do mundo das telecomunicações, onde se refere a algo maior do que 4 kHz, no mundo da rede de computadores “broadband cable” significa algum cabo de rede usado para transmissão analógica.

Desde o uso do broadband para redes, os cabos são usados para transmissões de sinal analógico com largura de banda de 300 a 450 MHz a distâncias de até 100 km, que é muito menos crítico que a transmissão de sinais digitais. Para transmitir sinais digitais numa rede analógica, cada interface deve conter dispositivos eletrónicos para converter o conjunto de bits de saída para um sinal analógico, e o sinal analógico de entrada no conjunto de bits.

Vantagens

- Comprimento maior que o coaxial fino;
- É muito utilizado para transmissão de imagens e voz.

Desvantagens

- Difícil instalação
- Custo elevado em relação ao cabo coaxial fino.

Cabo Coaxial Fino

Também conhecido como cabo coaxial banda base ou 10BASE2, é utilizado para transmissão digital, já foi o meio mais utilizado em redes locais. O sinal é injetado diretamente no cabo. A topologia mais usual é a topologia em BUS. A construção e blindagem do cabo coaxial proporcionam-lhe uma boa combinação de alta largura de banda e excelente imunidade ao ruído. A largura de banda depende do tamanho do cabo.

Fig. 14: Cabo coaxial fino

A especificação 10BASE2 refere-se à transmissão de sinais Ethernet utilizando esse tipo de cabo. O 2 informa o tamanho máximo aproximado do cabo como sendo de 200 metros. Na verdade, o comprimento máximo é 185 metros.

A impedância utilizada nesta modalidade de transmissão é de 50 Ohms. As taxas variam de 10 a 50 Mbps e o tempo de trânsito de 4 a 8 ns/m.

Vantagens

- É maleável;
- Fácil de instalar;
- Sofre menos reflexões do que o cabo coaxial grosso, possuindo maior imunidade a ruídos eletromagnéticos de baixa frequência.

Desvantagens

- Custo elevado em relação ao par entrançado;
- Custo elevado das suas interfaces;
- Falhas por mau contato nas fichas;
- Difícil manipulação devido a sua rigidez;
- Topologia de Barramento ou Linear.

Cuidados na instalação do cabo coaxial

É necessário verificar a qualidade dos elementos que constituem a cablagem dos cabos, fichas e terminadores. Estes devem ser de boa qualidade para evitar folgas nos encaixes, o que poderia causar mau funcionamento em toda rede.

Os cabos não podem ser tracionados, torcidos, amassados ou dobrados em excesso pois isso pode alterar as suas características físicas.

Quanto à ligação, o tipo mais comum de fichas usado por estes cabos coaxiais é o BNC (Bayone-Neill-Concelman). Diferentes tipos de adaptadores estão disponíveis para fichas BNC incluindo fichas tipo T e terminadores. As fichas são os pontos mais fracos em qualquer rede.

Fig. 15: Ficha BNC

Cabo Coaxial x Par Entrançado

As características de transmissão de dados em cabo coaxial são consideravelmente melhores do que em par entrançado. Quando usado em conjunto com técnicas de transmissão de banda larga oferece uma largura de banda que pode ir até aos 300 Mbps. Isso abre a possibilidade de ser usado como base para uma rede de cabo partilhado, com parte da largura de banda sendo usada para transmissão de dados, e a restante para a transmissão de outras informações, tais como sinais TV ou voz digitalizada.

Tem uma atenuação mais baixa que o par entrançado (especialmente a altas frequências) o que significa que tem menos necessidade de repetidores. Dado que a blindagem do cabo é parte do circuito do sinal, a terra pode introduzir ruído. Uma segunda blindagem resolve o problema, representando, no entanto um custo adicional.

Comparado com o par entrançado, o cabo coaxial tem uma imunidade de ruído de cross-talk bem melhor, e uma fuga eletromagnética mais baixa. Porém, em relação ao custo, o do cabo coaxial é mais elevado do que o do par entrançado, principalmente quando se pensa em termos de interfaces para ligação do cabo.

Meios de Fibra Ótica

Uma fibra ótica é constituída de material dielétrico, em geral, sílica ou plástico, em forma cilíndrica, transparente e flexível, de dimensões microscópicas comparáveis às de um fio de cabelo.

Esta forma cilíndrica é composta por um núcleo envolto por uma camada de material também dielétrico, chamada casca. Cada um desses elementos possui índices de refração diferentes, fazendo com que a luz percorra o núcleo refletindo na fronteira com a casca.

Fig. 16: Exemplo de Fibra Ótica

A fibra ótica possui duas camadas com índices de refração diferentes o que faz com que a luz sofra reflexão total quando tenta passar do núcleo para a casca, quando isso acontece, ela é refletida de volta para o núcleo e assim percorre toda a extensão da fibra.

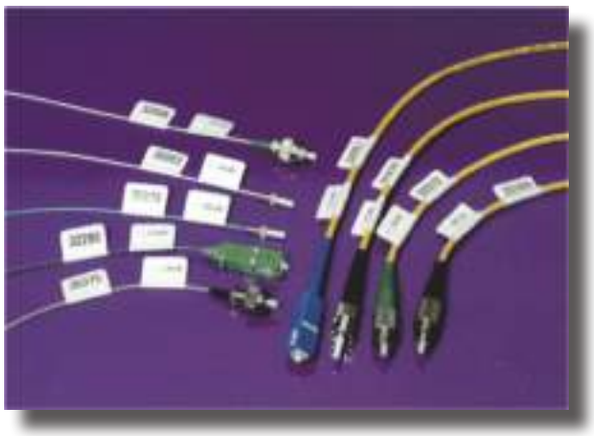


Fig. 17: Exemplos de cordões de fibras óticas

A fibra ótica utiliza sinais de luz codificados para transmitir os dados, mas como todos os sistemas atuais de computação funcionam a base de eletrões (eletrónica) e não a base de fotões (fotónica) é necessário a conversão do sinal elétrico em luminoso antes da transmissão através da fibra.

Isso é feito através de um conversor de sinais elétricos para sinais óticos, um transmissor, um recetor e um conversor de sinais óticos para sinais elétricos.

A atenuação das transmissões por fibra ótica não dependem da frequência utilizada, portanto a taxa de transmissão é muito mais alta. É totalmente imune a interferências eletromagnéticas, não precisa de ligação à terra e mantém os pontos que liga eletricamente isolados um do outro. Entretanto, pode ocorrer dispersão modal se a fibra for multimodo.

A transmissão ótica está também sujeita à dispersão espectral ou cromática. A luz que passa na fibra é composta de diferentes frequências e comprimentos de onda. O índice de refração difere para cada comprimento de onda e permite às ondas viajarem a diferentes velocidades. Os LED's, que possuem um grande espalhamento de comprimento de onda, estão sujeitos a uma dispersão de espectro considerável. Os lasers exibem uma luz quase monocromática (número limitado de comprimentos de onda) e não sofre qualquer dispersão cromática significativa.

O padrão 10BaseF refere-se à especificação do uso de fibras óticas para sinais Ethernet.

A ficha mais usada em fibras óticas é a ficha ST, similar à ficha BNC. No entanto, um novo tipo de fichas está a ficar mais conhecido, a ficha SC. É quadrada e é mais fácil de usar em espaços pequenos.

Fig. 18: Ficha ST

Fig. 19: Ficha SC

Vantagens

Perdas de transmissão baixa e banda passante grande: mais dados podem ser enviados sobre distâncias mais longas, desse modo diminui-se o número de fios e reduz-se o número de repetidores necessários nesta extensão, reduzindo o custo do sistema e complexidade.

Pequeno tamanho e peso: vem resolver os problemas de espaço e congestionamento de dutos no subsolo das grandes cidades e em grandes edifícios comerciais. É o meio de transmissão ideal em aviões, navios, satélites, etc.

Imunidade a interferências: não sofrem interferências eletromagnéticas, pois são compostas de material dielétrico, e asseguram imunidade a pulsos eletromagnéticos.

Isolamento elétrico: não há necessidade de se preocupar com a ligação à terra e problemas de interface de equipamento, uma vez que é constituída de vidro ou plástico, que são isolantes elétricos.

Segurança do sinal: possui um alto grau de segurança, pois não irradiam significativamente a luz propagada.

Matéria-prima abundante: é constituída por sílica, material abundante e não muito caro. Sua despesa aumenta no processo requerido para fazer vidros ultrapuros deste material.

Desvantagens

Fragilidade das fibras óticas sem encapsulamento: deve-se ter cuidado ao lidar-se com as fibras, pois elas partem com facilidade.

Dificuldade de conexões das fibras óticas: por ser de pequeníssima dimensão, exigem procedimentos e dispositivos de alta precisão na realização de conexões e junções.

Acopladores tipo T com perdas muito grandes: essas perdas dificultam a utilização da fibra ótica em sistemas multiponto.

Impossibilidade de alimentação remota de repetidores: requer alimentação elétrica independente para cada repetidor, não sendo possível a alimentação remota através do próprio meio de transmissão.

Falta de padronização dos componentes óticos: o contínuo avanço tecnológico e a relativa imaturidade não têm facilitado e estabelecimento de padrões.

Alto custo de instalação e manutenção.

Aplicações de Fibras Óticas

- Sistemas de comunicação.
- Rede Telefónica: serviços de backbone de telecomunicações, interligando centrais de tráfego interurbano e interligação de centrais telefónicas urbanas;
- Cabos Submarinos: sistemas de transmissão em cabos submarinos.
- Televisão por Cabo (CATV): transmissão de sinais de vídeo através de fibras óticas.
- Sistema de Energia e Transporte: distribuição de energia elétrica e sistema de transmissão ferroviário.
- Redes Locais de Computadores: aplicações em sistemas de longa distância e locais. Na busca de padrões a fim de facilitar a conectividade e minimizar os custos de aquisição e implantação com fibras óticas, foi desenvolvido o FDDI.
- Sistemas sensores.
- Aplicações industriais: sistemas de telemetria e supervisão em controle de processos.
- Aplicações médicas: sistemas de monitorização interna ao corpo humano e instrumentação cirúrgica.
- Automóveis: monitoração do funcionamento do motor e acessórios.
- Aplicações militares.

Como funciona a transmissão ótica

O sinal luminoso é transmitido para a fibra ótica sob a forma de pulso '0'/'1' representando uma sequência de símbolos binários. As ondas passam através do núcleo da fibra, que é coberto por uma camada chamada cladding. A refração do sinal é controlada pelo desenho do cabo, os recetores e os transmissores. O sinal luminoso não pode escapar do cabo ótico porque o índice de refração no núcleo é superior ao índice de refração do cladding. Deste modo, a luz viaja através do cabo num caminho todo espelhado.

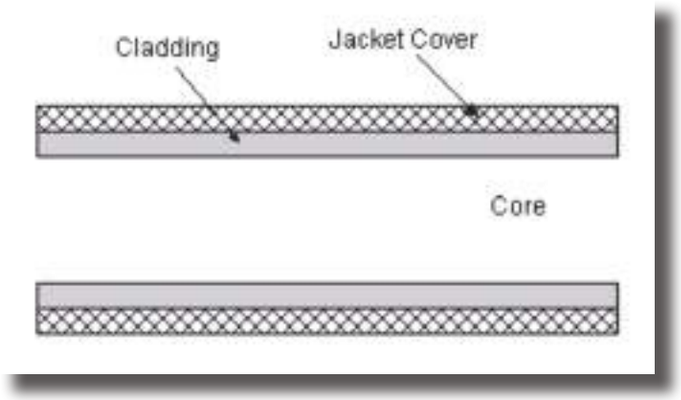


Fig. 20: Visão longitudinal de uma fibra ótica

A fonte emissora da luz é usualmente um laser ou um LED. Os lasers proporcionam para uma grande largura de banda um rendimento da capacidade que é significativamente maior do que outros métodos. Por exemplo, um cabo de dois fios tem um parâmetro de distância de largura de banda de 1Mhz/Km, um cabo coaxial tem 20 Mhz/Km, e a fibra ótica tem 400 Mhz/Km.

Há vários métodos para transmitir os raios luminosos através da fibra: multimodo com índice degrau, multimodo com índice gradual e monomodo. Existem assim dois tipos de fibras óticas são elas: Monomodo e Multimodo.

Fibras Óticas Multimodo

As fibras multimodo foram as primeiras a surgirem, e são classificadas quanto à relação entre os níveis de refração entre a casca e o núcleo. Elas são de dois tipos:

1. Multimodo com índice degrau: Esta fibra possui o núcleo feito por apenas um material, ou seja, com índice de refração constante. A principal consequência disso é uma menor capacidade de transmissão devido ao fenómeno de dispersão que causa vários "modos". A sua largura de banda é de até 35 Mhz/km.

2. Multimodo com índice gradual: Esta fibra possui o núcleo composto por vários elementos com índices de refração diferentes, isto tenta diminuir a diferença de tempo de propagação diminuindo assim a dispersão dos vários "modos". A sua largura de banda é de até 500 Mhz/km.

Fibra Ótica Multimodo com Índice Degrau

Foi o primeiro tipo a surgir e é também o mais simples. Na fibra multimodo com índice degrau, o núcleo e o cladding estão claramente definidos. O núcleo é constituído de um único tipo de material (plástico, vidro), ou seja, tem índice de refração constante, e tem diâmetro variável, entre 50 e 400 mm.

Os raios de luz refletem no cladding em vários ângulos, resultando em comprimentos de caminhos diferentes para o sinal. Isto causa o espalhamento do sinal ao longo da fibra e limita a largura de banda do cabo para aproximadamente 35 Mhz/km. Este fenómeno é chamado dispersão modal. A atenuação é elevada (maior que 5 dB/km), fazendo com que essas fibras sejam utilizadas em transmissão de dados em curtas distâncias e iluminação.

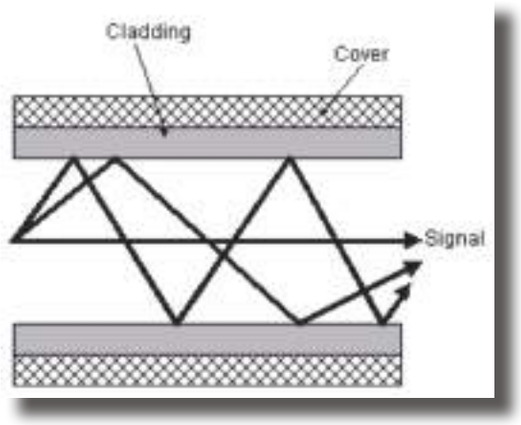


Fig. 21: Fibra ótica multimodo com índice degrau

Fibra Ótica Multimodo com Índice Gradual

Na fibra ótica multimodo com índice gradual, a interface núcleo/cladding é alterada para proporcionar índices de refração diferentes dentro do núcleo e do cladding. Os raios de luz viajam no eixo do cabo encontrando uma grande refração, tornando baixa sua velocidade de transmissão. Os raios que viajam na direção do cabo têm um índice de refração menor e são propagados mais rapidamente. O objetivo é ter todos os modos do sinal à mesma velocidade no cabo, de maneira a reduzir a dispersão modal. Esta fibra pode ter larguras de banda de até 500 Mhz.km. O núcleo tem, tipicamente, entre 125 e 50 mm e a atenuação é baixa (3 dB/km), sendo que por este motivo é utilizada em telecomunicações.

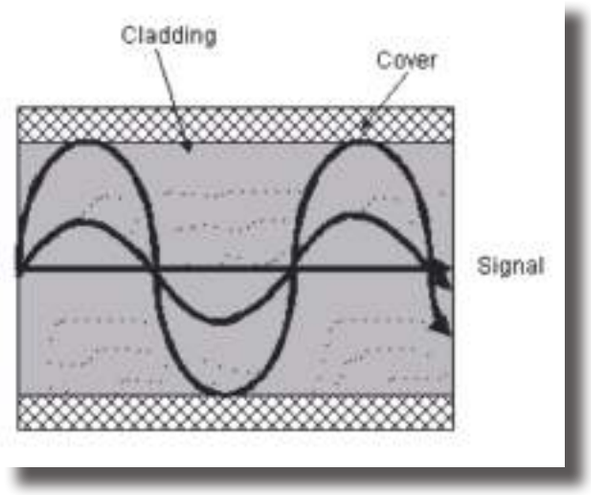


Fig. 22: Fibra ótica multimodo com índice gradual

Fibras Óticas Monomodo

Nas fibras monomodo a luz percorre a fibra em apenas "um modo" o que diminui a dispersão do sinal e evita o problema que possuem a fibras multimodo. A sua principal característica é a pequena dimensão do núcleo e, por possuir uma menor dispersão, atinge larguras de banda de até 1Ghz/km.

O tamanho do núcleo, 8 micrómetros (µm) de diâmetro, e o índice núcleo/cladding permite que apenas um modo seja propagado através da fibra, consequentemente diminuindo a dispersão do pulso luminoso. A emissão de sinais em fibras óticas monomodo é possível com LED's ou lasers, podendo atingir taxas de transmissão na ordem de 100 GHz/km, com atenuação entre 0,2 dB/km e 0,7 dB/km.

Contudo, o equipamento como um todo é mais caro que o dos sistemas multimodo. Esta fibra possui grande expressão em sistemas telefónicos e interligação de redes em localidades distantes.

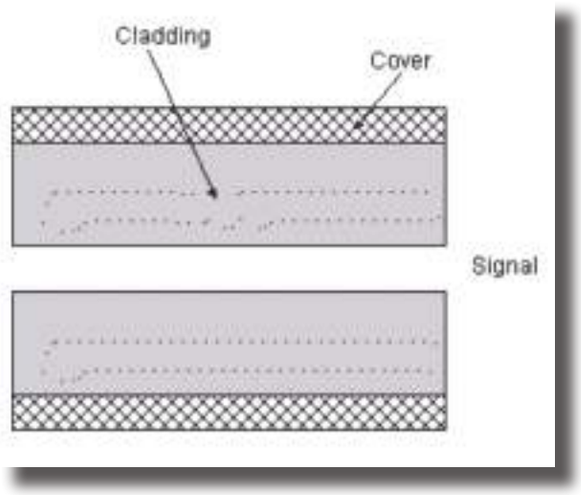


Fig. 23: Fibra ótica monomodo

Fibra Ótica X Cobre

O grande ponto da discussão sobre qual o meio de transmissão a utilizar está concentrado nas capacidades e limitações do cobre e da fibra ótica nas redes de computadores atuais. Muitas conceções erradas têm encoberto os fatos acerca das capacidades e da facilidade que hoje já existe em utilizar a fibra.

Os melhoramentos da tecnologia, juntamente com a redução do seu custo, têm feito da fibra ótica uma opção viável para redes de alta performance, em substituição aos caros cabos de cobre.

A fibra ótica tem vantagens e desvantagens em relação aos cabos de cobre. Ela pode criar larguras de banda muito maiores do que o cobre. Apenas esta característica justificaria o seu uso nas redes de última geração, embora o cobre domine na atual planta instalada de telecomunicações.

Devido à baixa atenuação, os repetidores óticos só são necessários a cerca de 30Km de distância, o que em comparação com o cobre, representa uma economia significativa. A fibra também tem a vantagem de não ser afetada por picos de voltagem ou interferências magnéticas. Ela também está imune à ação corrosiva de alguns elementos químicos e, consequentemente, adapta-se muito bem a áreas industriais.

Além disso, a fibra é mais leve que o cobre. Mil pares entrançados com 1 Km de comprimento pesam aproximadamente 8 Toneladas. Duas fibras têm mais capacidade e pesam cerca de 100Kg, reduzindo de maneira significativa a necessidade de sistemas

mecânicos de suporte, cuja manutenção é extremamente cara. Nas novas rotas, as fibras têm preferência por terem um custo de instalação muito mais baixo.

Por fim, as fibras não desperdiçam luz e dificilmente são intercetadas. Por estas razões, trata-se de uma alternativa muito mais segura contra possíveis escutas telefónicas.

A razão para que a fibra seja melhor do que o cobre é inerente às questões físicas subjacentes a estes dois materiais. Quando os eletrões se movem dentro de um fio, eles afetam um ao outro e, além do mais, são afetados pelos eletrões existentes fora do fio. Os fotões de uma fibra não afetam um ao outro (não têm carga elétrica) e não são afetados pelos fotões dispersos existentes do lado de fora da fibra.

Como desvantagens em relação ao cabo metálico, os cabos de fibra ótica e fichas são muito difíceis de instalar e as interfaces de fibra são mais difíceis de se montar e mais caras do que as interfaces elétricas. Os custos dos componentes para fibra ótica (máquinas de fusão, testes, etc., ainda são muito caros e de utilização altamente especializada).

Meios sem fios

A transmissão sem fio pode ser feita por raios infravermelhos, lasers, micro-ondas (radiação eletromagnética de comprimento de onda um pouco superior ao infravermelho) e rádio, não requerendo um meio físico.

A comunicação a laser ou infravermelho é totalmente digital e altamente direcional tornando-a praticamente imune a grampos ou interferências. Porém, dependendo da onda escolhida, chuva e neblina podem fazer com que haja interferência.

Para comunicações distantes, a transmissão por radiofrequência ou micro-ondas é uma boa alternativa. Antenas parabólicas podem transmitir para outras antenas a dezenas de quilómetros. Quanto mais alta a antena, maior o alcance. Os sinais transmitidos podem dividir-se e propagar-se por caminhos ligeiramente diferentes. Quando esses sinais se recombinam, surgem as interferências reduzindo a potência do sinal. A propagação pode ser prejudicada devido a tempestades ou outros fatores atmosféricos.

Neste tipo de transmissão (radiofrequência), os pacotes de informações são enviados pelo ar utilizando canais de frequência de rádio (que variam de Kilohertz até Gigahertz) ou por sinais infravermelhos (frequência na casa dos Terahertz). O ar funciona como um meio para os sinais eletromagnéticos se propagarem. Podem transmitir tanto sinais analógicos como digitais.

Com o grande avanço na utilização de Laptops, Palmtops, etc. existe uma tendência dos meios de comunicação de se concentrarem em fibras óticas e wireless.

As transmissões sem fio são baseadas na propagação de ondas eletromagnéticas no espaço. Só são necessários meios físicos nas estações emissoras e recetoras e em estações repetidoras intermediarias.

Os sistemas são divididos de acordo com a porção do espectro que utilizam, que também determina a sua largura de banda. A distribuição geral do espectro eletromagnético entre distintos serviços para exploração é determinada por entidades governamentais de cada país.

Quando os eletrões se movem estes criam ondas eletromagnéticas que podem se propagar através do espaço e mesmo no vácuo. Estas ondas foram previstas pelo alemão Heinrich Hertz em 1887.

O número de oscilações por segundo de uma onda eletromagnética é chamado de sua frequência e medido em Hz (em homenagem ao alemão Hertz).

Ligações via rádio

As propriedades das ondas de rádio dependem de sua frequência. Com frequências baixas, as ondas de rádio podem passar bem por obstáculos. Em altas frequências as ondas tendem a viajar em linhas finas (feixes pequenos), porém tendem a contornar obstáculos.

As ondas de rádio são muito usadas na comunicação porque são fáceis de gerar, propagam-se em todos os sentidos, transmitem sobre largas áreas geográficas e penetram em vários tipos de materiais. Os seus problemas principais estão na dependência da frequência utilizada. Se for baixa, as ondas de rádio seguem a curvatura da Terra, podendo não chegar ao seu destino devido à perda de potência com a distância percorrida. Se for alta, as ondas de rádio viajam em linha reta em direção à ionosfera, onde são refletidas para a Terra, o que permite a comunicação entre dois pontos ainda mais afastados por causa de uma perda de potência mais lenta, porém sujeitas à interferência.

No entanto, as ondas de rádio não são um meio confiável de transmissão, pois são bastante suscetíveis a interferências elétricas e magnéticas, bem como a interferências causadas por objetos ou fenómenos naturais (ex: chuva).

A radiodifusão é bastante útil para interligação entre redes locais distantes entre si e que mantêm níveis elevados de tráfego, já que este meio de transmissão é capaz de oferecer largura de banda maior, suprindo assim as necessidades que não poderiam ser consolidadas por circuitos telefónicos.

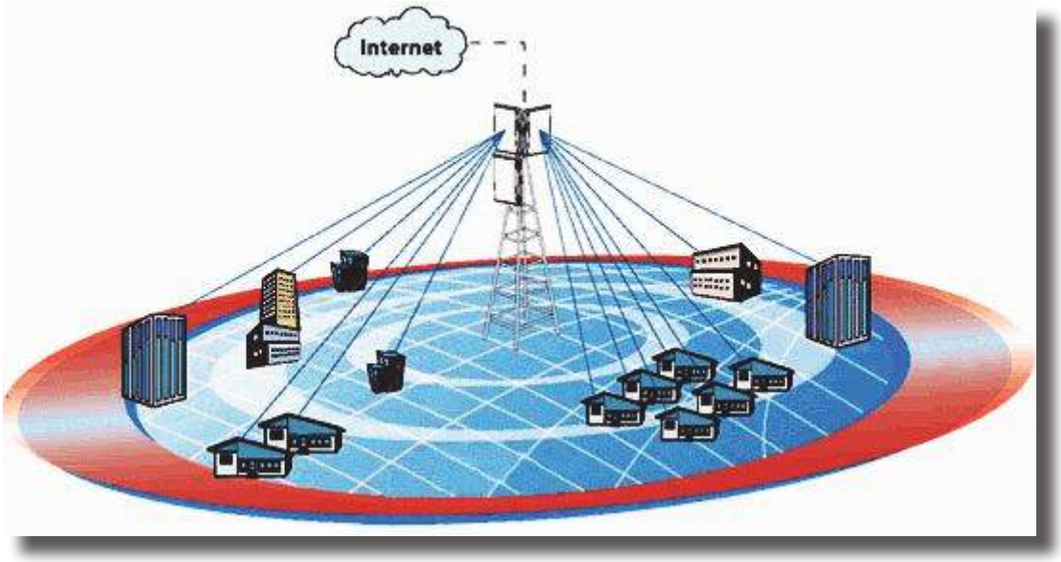


Fig. 24: Exemplo de uma ligação via radio

Ligações em micro-ondas

Este tipo de meio de transmissão é muito usado na comunicação telefónica entre grandes distâncias, nos telemóveis, etc. É barato e fácil de implementar, mas é muito suscetível a fenómenos elétricos, magnéticos e atmosféricos (ex: chuva).

Rádios de alta frequência (GHz) usam antenas parabólicas. A transmissão é feita num feixe muito fino e pode alcançar longas distâncias, porem necessitando ter vista direta.

Este tipo de transmissão é influenciado pela geografia. Para frequências acima de 10 GHz o sinal é influenciado pelas condições atmosféricas (chuva, neve, nevoeiro, etc.). A velocidade de propagação é próxima à da luz.

Apesar de tudo, incluindo o aparecimento das fibras óticas, a sua utilização ainda é grande.

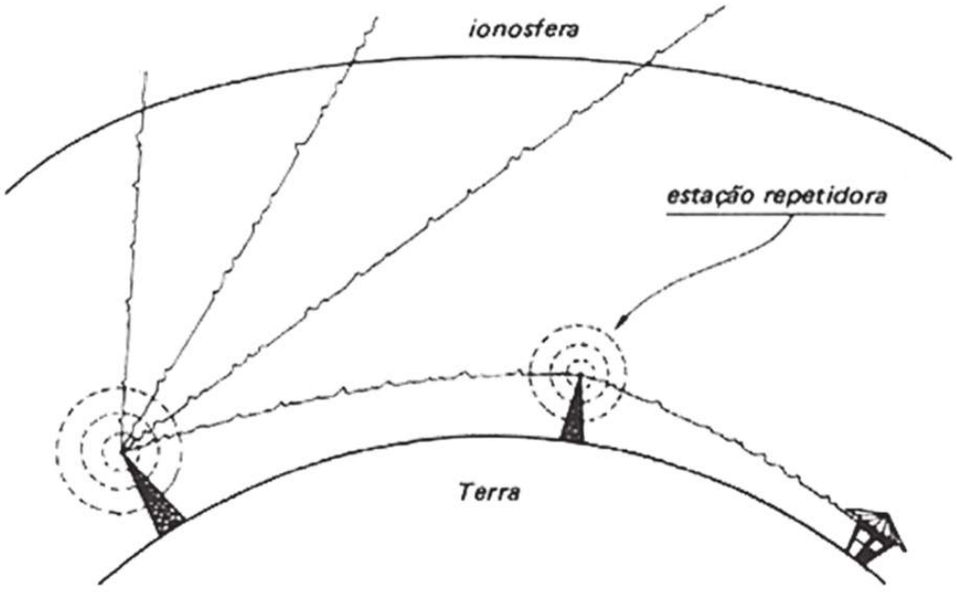


Fig. 25: Exemplo de uma ligação em micro-ondas

Ligações em infravermelhos

O exemplo mais comum da utilização dos raios infravermelhos está nas nossas casas, através dos telecomandos da televisão, vídeo, etc. Têm como vantagens principais o baixo custo e facilidade de construção, mas pecam por não poderem atravessar grande parte dos materiais. No entanto, essa desvantagem também pode ser tornada útil, através do seu uso em, por exemplo, redes locais dentro do mesmo espaço. Desta maneira, qualquer novo dispositivo que suporte a comunicação via infravermelho pode participar na rede tendo, apenas, de estar no mesmo espaço.

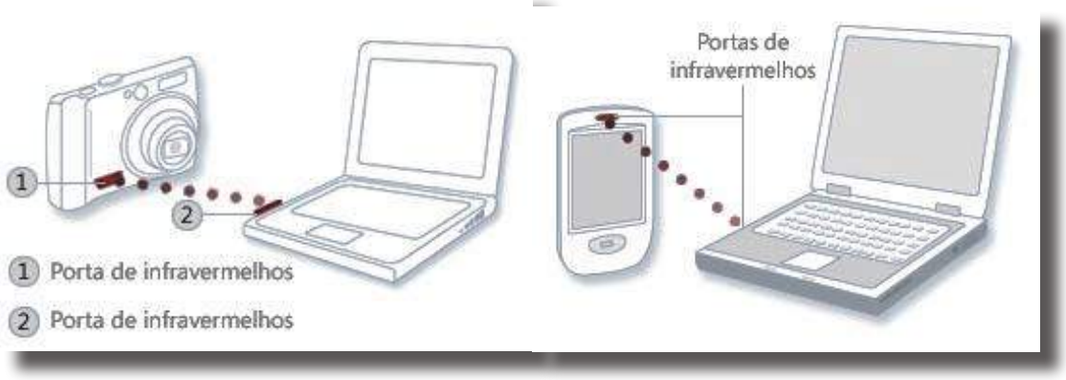


Fig. 26: Exemplo de ligações em infravermelhos

Ligações laser

São utilizadas na transmissão de sinais em fibra ótica. Podem ser usadas para transportar informação em espaço aberto entre dois pontos em linha reta à vista.

Este tipo de ligações é bastante utilizado para interligar redes privadas onde não é possível ou viável economicamente a instalação de cabos de fibra ótica.

Podemos destacar algumas vantagens deste tipo de tecnologia como a enorme largura de banda (622Mbps a distâncias superiores a 3 Km). Não é necessário obter a aprovação de entidades gestoras do espaço radielétrico para a instalação das ligações.

Já como desvantagem esta tecnologia é sensível ás condições atmosféricas (nevoeiros, poeiras,…) e a necessidade de manter um alinhamento rigoroso dos dispositivos emissor e recetor (algo que pode ser complicado em longas distâncias).

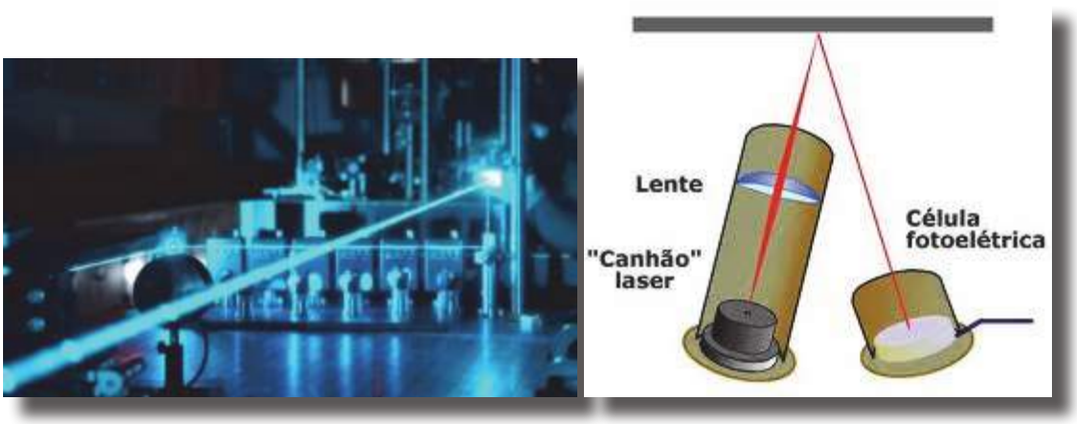


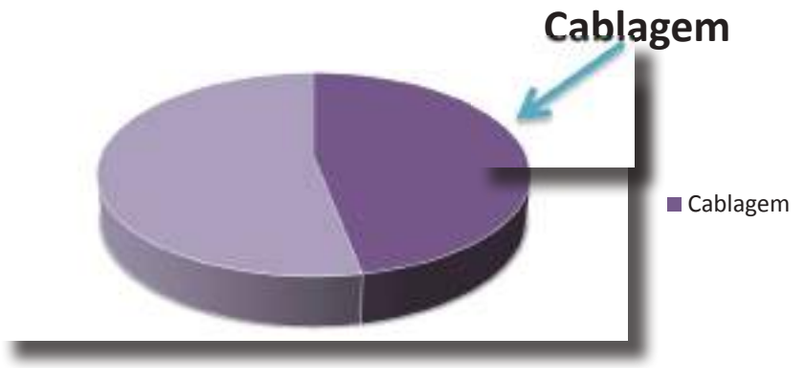
Fig. 27: Exemplo de ligação laser

Cablagem Estruturada

A rede estruturada é a que se baseia num sistema de produtos (cabos, adaptadores, fichas, painéis) padronizados, necessários a formação de uma rede que possa integrar comunicação de voz, dados e vídeo e que pode ser facilmente redirecionada para prover um meio de transmissão entre quaisquer pontos da rede. A base da rede estruturada é o cabo entrançado.

Porque usar Cablagem Estruturada

As primeiras redes locais, surgidas no início dos anos 80 empregavam a tecnologia de cabos coaxiais que devido ao seu baixo custo permaneceu em uso intenso por 15 anos.
Nos últimos anos porém, a crescente necessidade por multimeios de comunicação nas empresas (dados, telefones, fax, vídeo, videoconferência, etc…) incrementou dramaticamente a necessidade de se criar e manter uma infraestrutura física de comunicações organizada e eficiente. Por outro lado com o aumento do fluxo de informações de todos os tipos, surgiu o inevitável aumento de banda larga (maior velocidade) o que acarretou novas preocupações que não existiam no passado.
Além do mais se o sistema de cablagem for instalado de forma errada, sem respeitar as normas e procedimentos técnicos adequados isto poderá resultar em perda de tempo, desempenho e recursos na medida que surgirem problemas operacionais quanto ao funcionamento, ampliação e manutenção da rede, criando uma situação incompatível com a atual realidade económica que determina a redução de todo tipo de custo desnecessário nas empresas.
Estatísticas apontam para o fato de que o sistema de cablagem chega a responder até 47% do total de falhas de uma rede.



Isto é compreensível na medida que, historicamente, a infraestrutura de cabos geralmente é relegada a segundo plano. O sistema de cabos estruturado baseia-se na utilização de cabos entrançados, abandonando a tecnologia anterior de cabos coaxiais. Com isto é possível reduzir o número de falhas, o tempo de manutenção, os custos de mudanças de localização das estações de rede e da ampliação do sistema. Grandes empresas com amplas instalações físicas não podem mais abrir mão para estabelecer uma estratégia para o sistema de comunicação em todos os níveis. Empresas menores podem não vislumbrar tão claramente esta necessidade, porém elas obterão as mesmas vantagens ao adotarem um mínimo de planeamento e procedimentos técnicos.

Os sistemas de cablagem estruturada devem ser altamente flexíveis podendo ser adaptados para operar com quaisquer tipos de sinais transmitidos pela rede, independentemente dos computadores ligados em rede e do lay-out das instalações prediais.

O custo do sistema de cablagem geralmente situa-se em torno de 5% a 10% do custo total da rede, incluindo nesta projeção o custo dos computadores e programas.

Funções de uma rede estruturada

- Garantir um nível de performance satisfatório do sistema de cablagem;
- Garantir a homogeneidade das características elétricas dos equipamentos interligados;
- Garantir a compatibilidade dos componentes de forma a facilitar a manutenção e ampliação;

- Permitir a rápida mudança de uma tomada para voz, dados, fax ou vídeo;
- Permitir a operação de redes com velocidades de 100 Mbps ou mais;
- Permitir a transmissão de dados com protocolos mais antigos ou proprietários com a adição de conversores, tais como “baluns”;
- Permitir a elaboração de projetos consistentes e organizados;
- Permitir a fácil implantação e manutenção;
- Prover um sistema de interfaces padronizadas;
- Prover suporte a diferentes equipamentos e aplicações.

Com a utilização de hubs, bridges, routers, switches e outros dispositivos ativos, é possível interligar redes com topologias e sistemas de cablagem distintos num mesmo sistema de cablagem estruturada.
Em inglês o termo “cabling” equivale a cablagem estruturada.

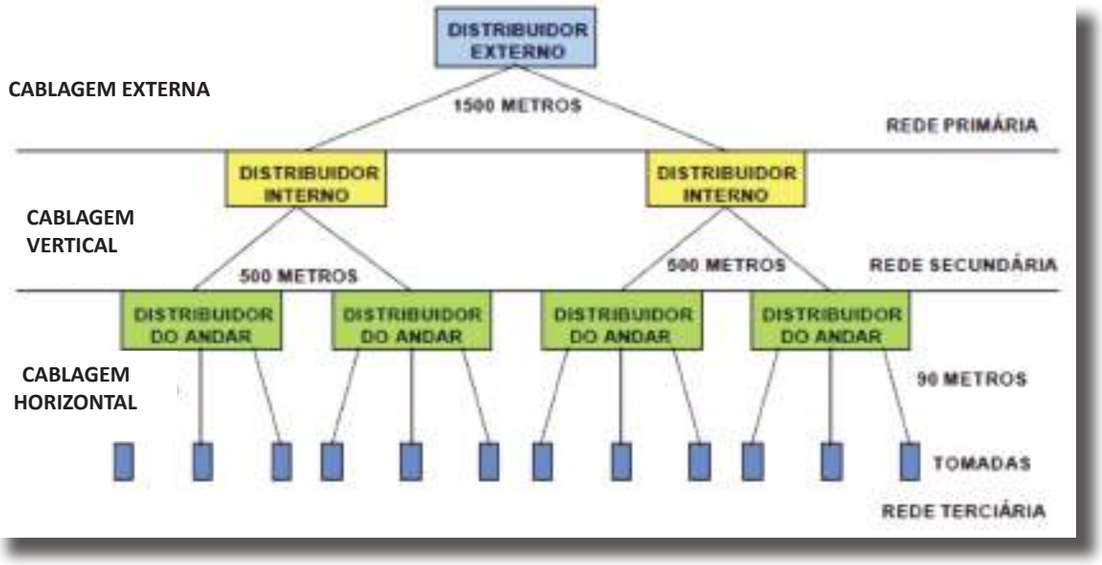
Áreas compreendidas pela rede estruturada

A rede estruturada pode ser dividida em três níveis ou áreas: primária, secundária e terciária.

Rede Primária: Interliga instalações prediais através de uma área ampla, geralmente pública, através de cabos óticos ou outros meios.

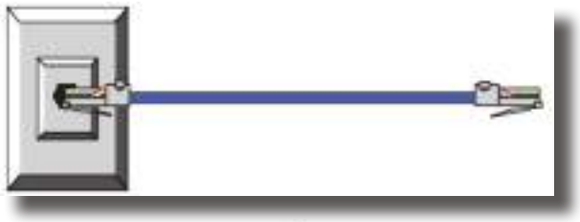
Rede Secundária: Interliga os distribuidores numa instalação predial através de condutores metálicos ou óticos. Engloba o Backbone e a rede vertical.

Rede Terciária: Interliga os distribuidores as estações de rede. Engloba o backbone e a rede horizontal.

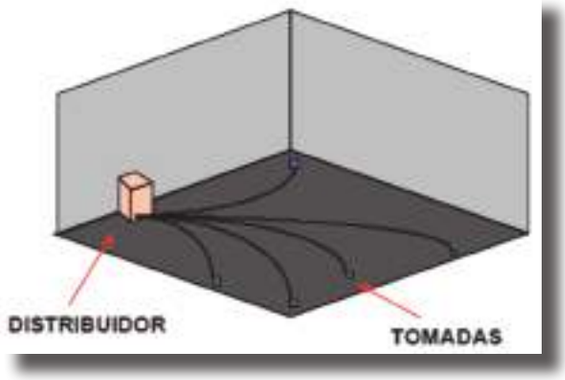


A rede terciária pode ser dividida em três subsistemas:

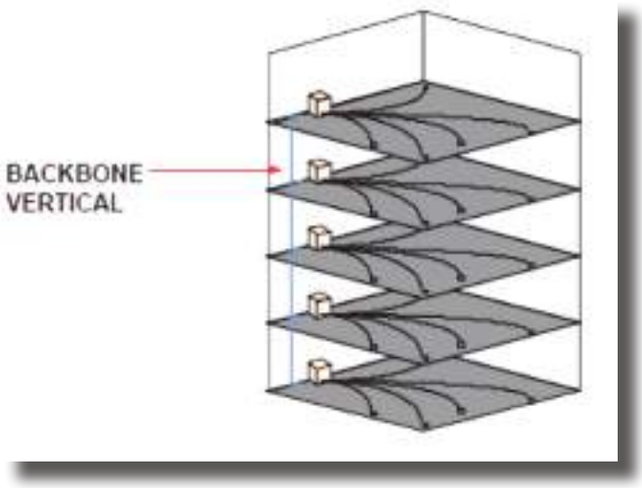
Subsistema Estação de Trabalho: Cabos, fichas e tomadas que possibilitam a ligação da estação a rede.



Subsistema Horizontal: Sistema de cabos que se espalham no sentido horizontal, no chão ou no teto e que interligam o Subsistema Estação de Trabalho aos armários de telecomunicações. Em redes maiores podemos ter um backbone horizontal.



Subsistema Vertical: Sistema de cabos que interliga os armários de telecomunicações dos andares da instalação predial.

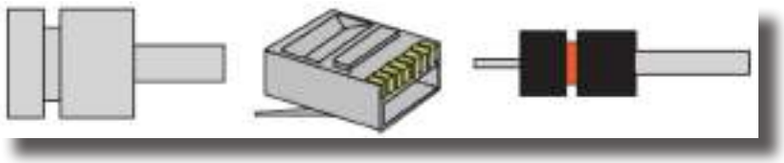


Componentes da cablagem estruturada

A seguir são descritos elementos para cablagem definidos pelas normas internacionais para a cablagem estruturada, EIA/TIA 568, 569, TSB36/40 e ISO 11801, bem como outros empregues normalmente pelo mercado mas que não são mencionados por estas normas.

Cabos: São a base do sistema de cablagem. Numa rede estruturada podemos ter todo tipo de cabos de rede para atender as especificações dos protocolos Ethernet, Token-Ring, Fast-Ethernet, FDDI, ATM, etc, além de cabos de voz, vídeo, etc. Na prática encontramos frequentemente os cabos entrançados, óticos e coaxiais, nesta ordem.

Fichas: As fichas são o ponto mais crítico de uma rede local. Fichas de baixa qualidade podem apresentar problemas tais como mal contato, fendas e rompimentos. Mal instalados podem acarretar em ruídos e mal contato intermitente provocando problemas na rede. Cada cabo exige o emprego de um conector específico.

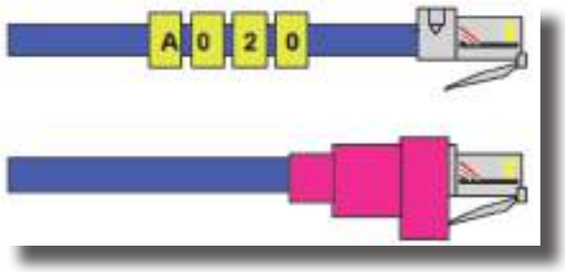


PRINCIPAIS FICHAS PARA REDES LOCAIS

- CABO COAXIAL FINO: Ficha BNC
- CABO COAXIAL GROSSO: Ficha Vampiro
- CABO PAR ENTRANÇADO UTP: Ficha RJ45
- CABO PAR ENTRANÇADO BLINDADO: FichaIBM Tipo1
- CABO ÓTICO FORIL: Ficha ST
- CABO ÓTICO FDDI: Ficha FDDI

Segmento de Cabo: Uma rede é constituída de vários pedaços de cabos, denominados segmentos. Os segmentos são preparados e interligados conforme as necessidades da rede.

Identificadores: As normas estabelecem o uso de etiquetas de papel para identificação dos cabos. Por serem pouco duráveis, na prática aplicam-se anilhas de plástico e capas coloridas para uma identificação permanente.



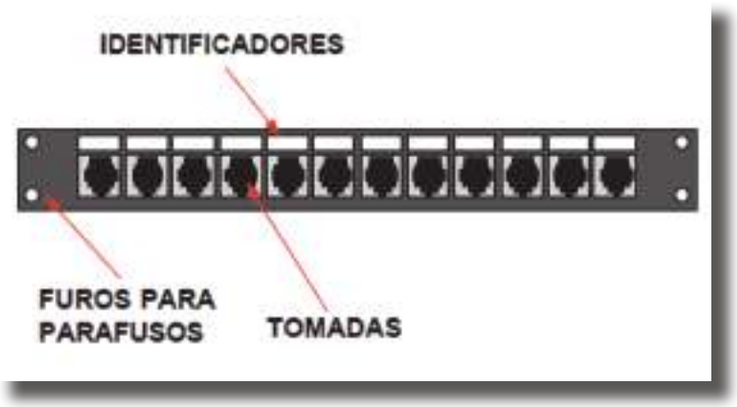
Backbone: Literalmente significa "espinha dorsal". É o cabo principal de uma rede local. O backbone pode ser vertical ou horizontal, conforme se estenda num ou noutro sentido. O backbone pode ser constituído por um cabo de rede comum.

Patch Panel: Os patch panels são o coração de uma rede estruturada pois, através deles o sistema de cabos pode ser reconfigurado. São utilizados junto aos blocos de distribuição e em áreas de distribuição a nível horizontal para interligar as estações da rede. Os patch panels devem ser capazes de estabelecer ligações rápidas, confiáveis e seguras garantindo uma performance satisfatória com taxas de operação de 100 Mbps. Existem inúmeros fabricantes de patch panels. Eles são adquiridos conforme o número de portas desejadas.
Os valores mais comuns são 12, 16, 24 e 48 portas.

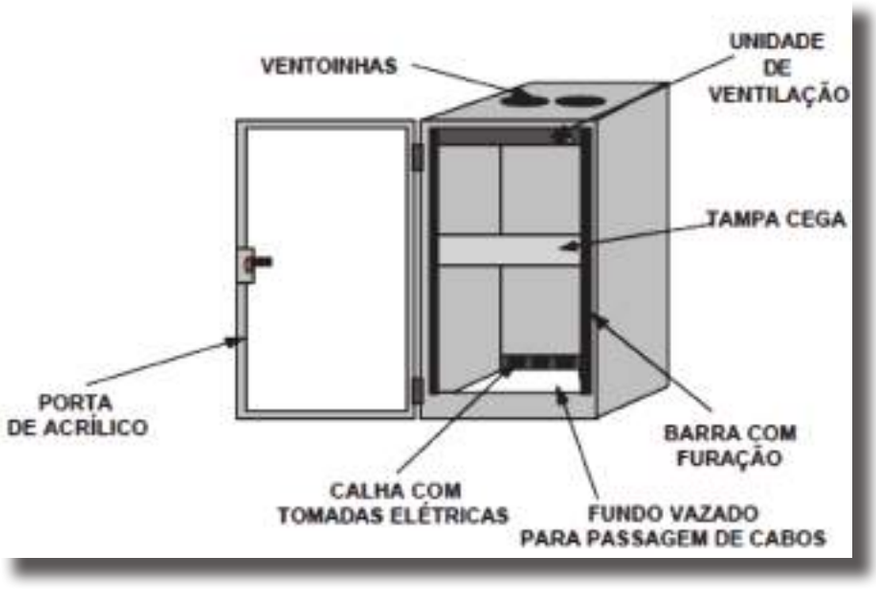
Patch Cord: Pequeno segmento de cabo que interliga um patch panel a outro ou um hub ao patch panel. O mesmo que Cord Panel.

Área de Trabalho: Espaço entre uma tomada e uma estação de rede.

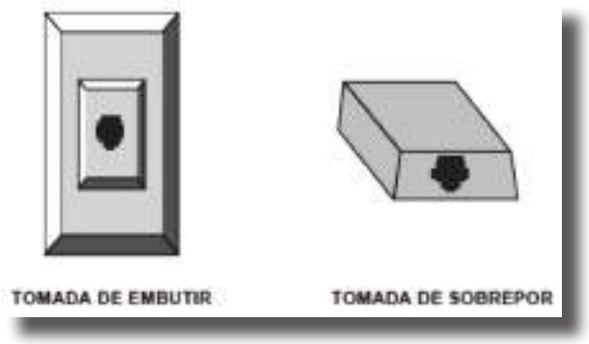
Bloco de Distribuição: O mesmo que distribuidores. São dispositivos empregues para concentrar grandes quantidades de cabos. Destes paineis partem os cabos de rede, outros cabos (voz, vídeo, etc), e os meios de transmissão para interligação com redes distantes. A partir dos blocos, os cabos seguem para os patch panels.



Caixa/Bastidor: (O mesmo que Rack) Armário de aço com dimensões padronizadas (geralmente 19 polegadas de largura) e com encaixes apropriados para hubs, patch-panels, cabos, etc.



Tomada: Ponto de ligação entre o segmento de cabo que vem do painel de distribuição com o que vai até à estação. Normalmente utiliza-se tomadas de parede e opcionalmente tomadas de chão. Existem diversos tipos, das mais simples até ás mais sofisticadas, com uma única ou múltiplas fichas fêmea. Em inglês, o mesmo que Telecommunication Outlet (tomada de telecomunicações).



Rede Vertical: É o backbone que interliga os diversos andares de uma instalação predial.

Rede Horizontal: É o sistema de cablagem instalado num andar ou piso da instalação predial que interliga as tomadas de rede aos painéis ou blocos de distribuição ali existentes.

Cablagem Plena: É o cabo constituído por materiais resistentes ao fogo e que liberam pouca fumaça ao queimar. Nos EUA o NEC (National Electric Code) determina as normas e codificações para estes cabos.

Calhas: Dutos de plástico ou PVC empregues para agrupar e proteger os cabos da rede dentro da instalação predial em locais visíveis.

Esteiras: Dutos geralmente de ferro galvanizado empregues para agrupar e proteger os cabos de rede em ambientes externos (ao ar livre) ou em áreas internas críticas tais como corredores, depósitos, fábricas, etc…

Etiquetas e Marcadores: São utilizadas para identificar cabos e painéis. Usam-se marcadores para identificar cabos e etiquetas para identificar painéis.

Equipamento Passivo e Ativo

Considera-se equipamento ativo, todo o equipamento gerador, recetor de código ou conversor de sinais elétricos ou óticos. Estes equipamentos têm a capacidade de efetuar cálculos e processar os dados que recebe, gerindo-os de modo inteligente. Exemplo deste tipo de equipamentos são os routers, switches, hubs e bridges.

Já os dispositivos passivos são aqueles que não interferem com os dados ou sinais que passam por eles e permitem a interligação dos equipamentos ativos. Exemplos deste tipo de equipamentos são as tomadas, rede de cabos, distribuidores e patch panels.

Equipamentos de interligação de redes

Para que uma rede de computadores possa funcionar é necessário que existam, além dos cabos propriamente dito, dispositivos de hardware e software cuja função é controlar a comunicação entre os diversos componentes da rede.

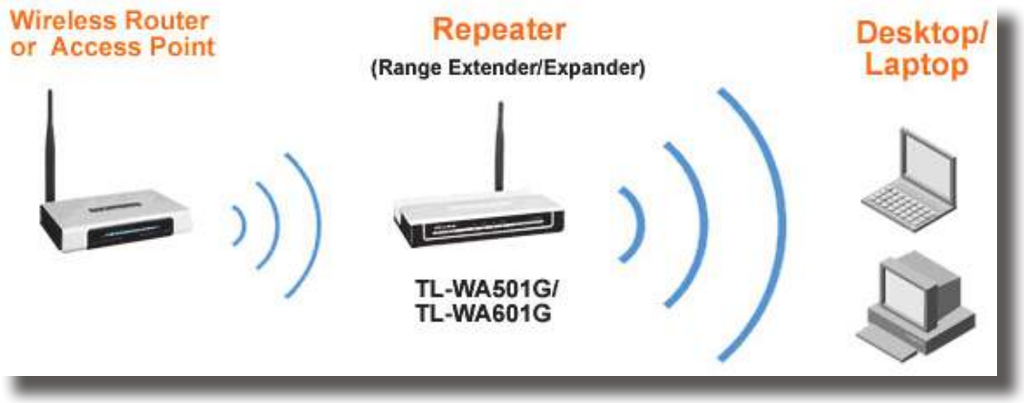
Vários dispositivos são usados numa rede, onde cada um deles possui funções específicas e distintas. Como exemplos de equipamentos dedicados podemos citar os repetidores, concentradores (hub), pontes (Bridge), comutadores (switch), encaminhadores (Routers), etc., que tem a finalidade de interpretar os sinais digitais processados na rede e encaminhá-los ao seu destino, obedecendo a um determinado padrão e protocolo.

Essa interação entre dispositivos permite a partilha das informações entre todos os utilizadores da rede.

Repetidores

Numa linha de transmissão, o sinal sofre distorções e enfraquecimento tanto mais importantes quanto seja longa a distância que separa dois elementos ativos. Geralmente, dois nós de uma rede local não podem distar de mais de algumas centenas de metros, é a razão pela qual um equipamento suplementar é necessário para além desta distância. Um repetidor (em inglês *repeater*) é um equipamento simples que permite regenerar um sinal entre dois nós da rede, para aumentar a distância de uma rede. O repetidor trabalha unicamente a nível físico (camada 1 do modelo OSI), quer dizer que trabalha apenas a nível das informações binárias que circulam na linha de transmissão e que não é capaz de interpretar os pacotes de informações.

Por outro lado, um repetidor pode permitir a constituição de um interface entre dois suportes físicos de tipos diferentes, ou seja, pode permitir ligar um segmento de par entrançado a um fio de fibra ótica, por exemplo.

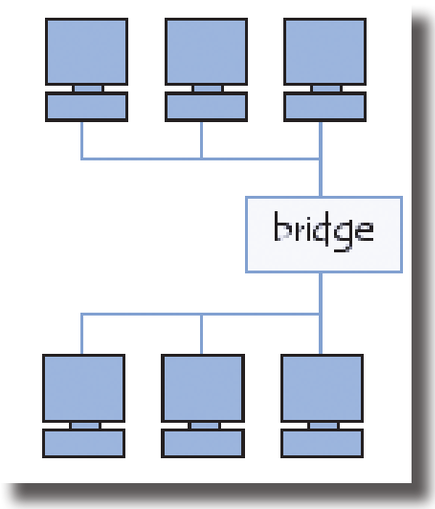


Pontes (Bridge)

Uma ponte é um dispositivo material que permite ligar redes que trabalham com o mesmo protocolo. Assim, contrariamente ao repetidor, que trabalha a nível físico, a ponte trabalha igualmente ao nível lógico (a nível da camada 2 do modelo OSI), quer dizer que é capaz de filtrar os dados e deixar passar unicamente aquelas cujo endereço corresponde a uma máquina situada no extremo da ponte.

Assim, a ponte permite segmentar uma rede conservando a nível da rede local os dados destinados ao nível local e transmitir os dados destinados às outras redes. Isto permite reduzir o tráfego (nomeadamente as colisões) em cada uma das redes e aumentar o nível de confidencialidade, porque as informações destinadas a uma rede não podem ser "ouvidas" noutra maquina.

Por outro lado, a operação de filtragem realizada pela ponte pode conduzir a um ligeiro atraso aquando da passagem de uma rede à outra, é a razão pela qual as pontes devem ser colocadas judiciosamente numa rede.



Uma ponte serve habitualmente para transitar pacotes entre duas redes do mesmo tipo.

Principio

Uma ponte possui duas conexões a duas redes distintas. Quando a ponte recebe um pacote de dados num dos seus interfaces, analisa o endereço MAC do destinatário e do emissor. Se por acaso a ponte não conhece o emissor, armazena o seu endereço numa tabela para se "recordar" de que lado da rede se encontra o emissor. Assim, a ponte é capaz de saber se o emissor e o destinatário estão situados no mesmo lado ou numa parte ou noutra da ponte. No primeiro caso, a ponte ignora a mensagem, no segundo a ponte transmite os dados para a outra rede.

Funcionamento

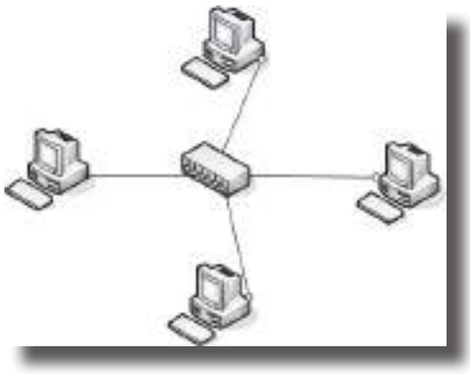
Uma ponte funciona de acordo com a camada Ligação dados do modelo OSI, o que quer dizer que opera a nível dos endereços físicos das máquinas. Na realidade, a ponte está ligada a várias redes locais, chamadas segmentos. A ponte elabora uma tabela de correspondência entre os endereços das máquinas e o segmento ao qual pertencem e "ouve" os dados que circulam nos segmentos.

Aquando de uma transmissão de dados, a ponte verifica na tabela de correspondência o segmento ao qual pertencem os computadores emissores e recetores (graças ao seu endereço físico, chamado endereço MAC, e não o seu endereço IP. Se estes pertencerem ao mesmo segmento, a ponte não faz nada, no caso contrário vai empurrar os dados para o segmento ao qual pertence o destinatário.

Concentrador (Hub)

Um concentrador (ou hub) é um elemento material que permite concentrar o tráfego da rede que provém de vários hosts, e gerar de novo o sinal. O concentrador é assim uma entidade que possui diversas portas (possui tantas portas quantas as máquinas que pode ligar entre elas, geralmente 4, 8, 16 ou 32). O seu único objetivo é recuperar os dados binários que chegam a uma porta e difundi-los para o conjunto das portas. Da mesma maneira que o repetidor, o concentrador opera ao nível 1 do modelo OSI, e esta é a razão pela qual às vezes é chamado "repetidor multiports".

O concentrador permite assim ligar várias máquinas entre elas, às vezes dispostas em estrela, daí o nome de *hub* (que significa centro de roda em inglês), para ilustrar o facto de que se trata do ponto de passagem das comunicações das diferentes máquinas.



Tipos de concentradores

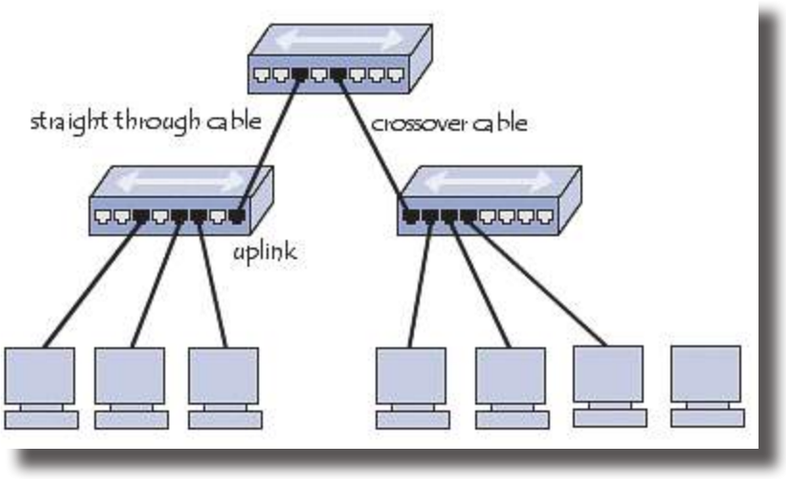
Distinguem-se várias categorias de concentradores:

- Os concentradores ditos "**ativos**": são alimentados eletricamente e permitem regenerar o sinal nas diferentes portas
- Os concentradores ditos "**passivos**": permitem apenas difundir o sinal a todos os hóspedes conectados sem amplificação

Ligação de vários hubs

É possível ligar vários hubs entre eles a fim de concentrar um maior número de máquinas, fala-se então de ligação em cascata (às vezes chamada *daisy chains* , em inglês). Para o efeito, basta ligar os hubs com um cabo cruzado, isto é, um cabo que liga as fichas de receção de uma extremidade às fichas de receção da outra.

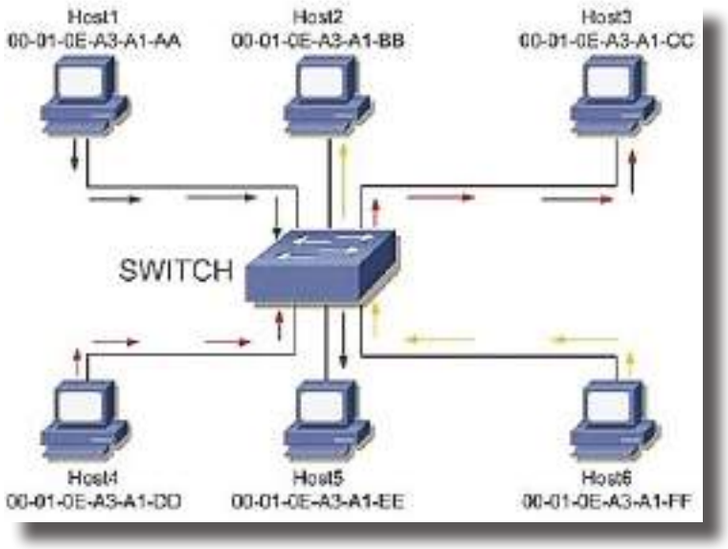
Os concentradores em geral são dotados de uma porta especial chamada “uplink” que permite utilizar um cabo direito para ligar as portas entre elas. Há igualmente hubs capazes de cruzar ou descruzar automaticamente as suas portas, caso estejam ligados a um hóspede ou a um hub.



Se deseja-mos ligar várias máquinas a uma conexão de Internet, um hub não é suficiente. É necessário recorrer a um switch ou a um comutador ou então deixar um computador ligado diretamente à Internet como ponte estreita (ficará, por conseguinte, constantemente ligado quando os outros computadores da rede desejarem aceder à Internet).

Comutadores (Switch)

Embora o termo switch possa referir-se a diferentes tipos de dispositivos que trabalham em diferentes camadas do modelo OSI — um comutador ATM (Asynchronous Transfer Mode) trabalha na camada de rede (camada 3), e historicamente utilizou-se o termo packet switch para designar routers — no uso mais frequente, hoje em dia, refere-se a dispositivos que comutam tramas, efetuando autoaprendizagem e filtragem com base nos endereços MAC. No fundo, um comutador Ethernet é uma bridge com múltiplas portas. É, portanto, um dispositivo que opera na camada de ligação lógica (camada 2) do modelo OSI.



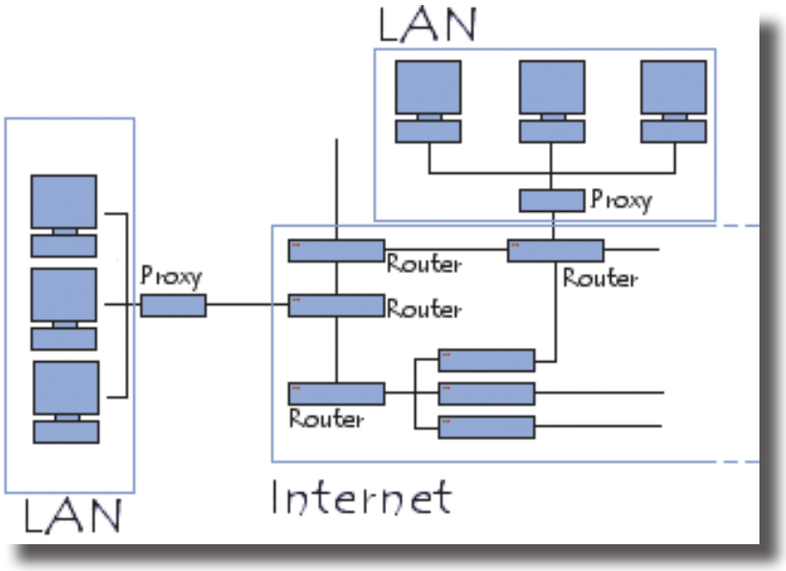
Em termos de aspeto, um comutador Ethernet é muito semelhante a um *hub*, como pode ver-se na figura a seguir, por vezes, a única maneira de os distinguir visualmente é pelo fato de ter escrito *hub* ou *switch*…

Encaminhadores (Routers)

O router é um equipamento de interconexão de redes informáticas que possibilita o encaminhamento dos pacotes entre duas redes ou mais, com o objetivo de determinar o caminho que o pacote de dados deve tomar.

Quando um utilizador chama uma URL/Link, o cliente Web (navegador) interroga o servidor de nomes (DNS), que lhe indica o endereço IP da máquina visada.

O seu computador envia o pedido ao router mais próximo, ou seja, à gateway, por defeito da rede onde se encontra. Este router vai, então, determinar para que máquina os dados serão encaminhados, de maneira a que o caminho escolhido seja o melhor. Para fazer isso, os routers mantêm atualizadas as tabelas de encaminhamento, verdadeiro mapeamento de itinerários a seguir, em função do endereço visado. Existem inúmeros protocolos para realizar esta tarefa.



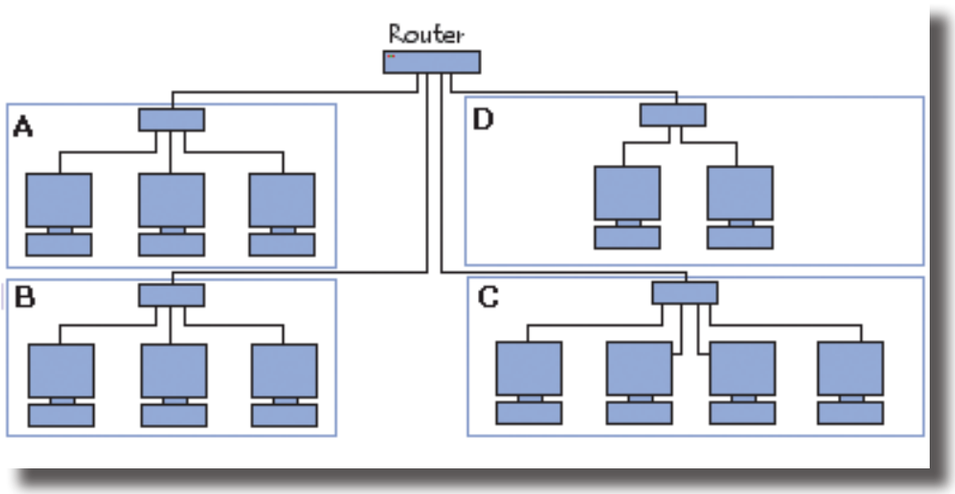
Além de sua função de encaminhamento, os routers permitem a manipulação dos dados que circulam sob a forma de datagramas para se certificarem da passagem de um tipo de rede a outro. Ora, na medida em que as redes não têm as mesmas capacidades em termos de dimensão de pacotes de dados, os routers estão encarregues de fragmentar os pacotes de dados, para permitir a sua circulação.

Aspeto de um router

Os primeiros routers eram simples computadores que tinham várias placas de rede, onde estava cada uma ligada a uma rede diferente. Já os routers atuais são materiais que se dedicam, na maior parte dos casos, à tarefa de encaminhamento. Em geral, apresentam-se sob a forma de *servidores 1U* como apresentado nas figuras a seguir.

Este tipo de chassis permite acolher uma placa-mãe standard bem como um ou vários discos rígidos IDE, SCSI ou Serial ATA. Contudo, dada a pouca altura da caixa, é geralmente aconselhável que a placa-mãe integre o máximo de periféricos de entrada/saída necessários para o funcionamento do servidor (placa gráfica, placa SCSI, suporte RAID, placa de rede).

Um router possui múltiplos interfaces de rede, cada um ligado a uma rede diferente. Assim sendo, ele tem tantos endereços IP quantas as redes diferentes às quais está ligado.



Router sem fios

O princípio de um router sem fios é o mesmo que o do router convencional, exceto que ele possibilita aos dispositivos sem fios (estações Wireless por exemplo) ligar-se às redes às quais o router está conectado, através de ligações com fios (geralmente Ethernet). Normalmente têm uma porta Wan e quatro ou mais portas Lan.

Exercícios Propostos

1. Como podemos classificar os meios de transmissão?

2. Quais são as características a ter em conta na escolha do tipo de cabo?

3. Os ruídos podem ser classificados em quatro tipos. Diga quais exemplificando cada um.

4. Que tipos de cabos usavam as primeiras redes ethernet?

5. Os transcetores eram conhecidos por “Vampire Taps”. Diga porquê?

6. Qual é a única desvantagem das redes thinnet em relação às ticknet?

7. Quais são as características elétricas dos cabos metálicos?

8. Explique sucintamente em que consiste o ECO.

9. Que tipo de cabos de par trançado conhece?

10. Existem alguma diferença a nível de blindagem entre cabos de par trançado que mencionou?

11. Para obter um melhor resultado em comunicações de pares trançados, que tipo de conetores devem ser utilizados e porquê?

12. Os cabos de par trançado podem ser divididos em categorias. Diga quais.

13. Na categoria 5 ouve algum upgrade? Se sim diga qual a necessidade de tal alteração

14. Existem dois padrões de sequência para as fichas RJ45. Diga quais são e em que diferem.

15. Que diferença existe entre um cabo direto e um cabo crossover?

16. Para que servem cabos do tipo direto?

17. Para que servem os cabos do tipo crossover?

18. Desenhe um esquema onde sejam usados os dois tipos de cabos.

19. Diga como é constituído um cabo coaxial.

20. Existe alguma diferença na impedância dos cabos coaxiais para transmissões analógicas e digitais?

21. Quais são as vantagens e desvantagens do cabo coaxial grosso?

22. Quais as vantagens e desvantagens do cabo coaxial fino?

23. Quais os cuidados necessários a ter na instalação de cabos coaxiais?

24. Como é constituída a fibra ótica?

25. Explique o funcionamento da fibra ótica.

26. Diga duas vantagens e duas desvantagens da fibra ótica.

27. Refira algumas aplicações da fibra ótica.

28. Que tipo de fibras conhece?

29. As fibras óticas Multimodo podem ser com índice degrau ou gradual. Explique a diferença entre ambas.

30. Diga o que entende sobre fibras monomodo.

31. De que maneira pode ser feita uma transmissão sem fios?

32. Porque se usam muito as ligações via rádio.

33. Conhece algum tipo de aparelho que use infravermelhos? Diga uma vantagem e uma desvantagem desta tecnologia.

34. Defina rede estruturada.

35. Refira algumas funções de uma rede estruturada.

36. A rede estruturada pode ser dividida em três níveis ou áreas: primária, secundária e terciária. Explique cada uma delas.

37. Quais são os componentes que fazem parte da cablagem estruturada?

38. Para que servem as Calhas e as Esteiras?

39. Qual é a diferença entre equipamentos Passivos e Ativos?

40. Diga que tipos de equipamentos são usados para interpretar os sinais digitais processados na rede e encaminhá-los ao seu destino em redes.

41. Para que serve um repetidor?

42. Qual é o objetivo de um Hub?

43. O que é um Router?

Bibliografia

Baptista, Carlos Pedro Zaragoza, *Fundamental dos Sistemas Digitais.* Lisboa: FCA – Editora Informática, 2003.

Gouveia, José; Magalhães, Alberto, *Curso Técnico de Hardware.* Lisboa: FCA – Editora Informática, 2003.

Gouveia, José; Magalhães, Alberto, *Hardware Montagem, Atualização, Detecção e Reparação de Avarias em PCs e Periféricos* 4ª ed.. Lisboa: FCA – Editora Informática, 2004.

Gouveia, José; Magalhães, Alberto. *Hardware para PC´s e Redes.* Lisboa: FCA – Editora Informática, 2004.

Loureiro, Paulo, *TCP / IP em Redes Microsoft – Para Profissionais.* Lisboa: FCA – Editora Informática, 2004.

Marques, José Alves; Guedes, Paulo, *Tecnologia de Sistemas Distribuídos.* Lisboa: FCA – Editora Informática, 2004.

Monteiro, Edmundo; Boavista, Fernando, *Engenharia de Redes Informáticas.* Lisboa: FCA – Editora Informática, 2005.

Monteiro, Rui Vasco *et al.*, *Tecnologia dos Equipamentos Informáticos.* Lisboa: FCA – Editora Informática, 2005.

Nunes, Mário Serafim; Casaca, Augusto Júlio, *Redes Digitais Com Integração de Serviços.* Editorial Presença, 2001.

Rodrigues, Eleri; Magalhães, Maurício F., *Redes de comunicação*. DCA – FEEC UNICAMP, 1996.

Rodrigues, Luís Silva, *Arquiteturas dos Sistemas de Informação.* Lisboa: FCA – Editora Informática, 2003.

Sousa, Sérgio, *Tecnologias de Informação - O que são? Para que Servem?* - 4ª ed.. Lisboa: FCA – Editora Informática, 2005.

Notas