ELDON CARVALHO VAZ DA CONCEIÇÃO

Redes locais de computadores

Uma visão global e prática

Trabalho Científico apresentado ao Departamento de Ciência e Tecnologia do Instituto Superior de Educação, curso de Licenciatura em Informática - Ramo Educacional como requisito parcial para obtenção do grau de Licenciatura, sob a orientação do Eng.º José Lino Teixeira.

Palmarejo 2006

O Júri

_____

_____

_____

ISE

Palmarejo 2006

RESUMO

O presente trabalho tem por objectivo, a elaboração de um manual prático que permita aos leitores, sejam ou não, técnicos de redes, instalar uma rede local básica em casa ou no local de trabalho, sem recorrer a sessões de formação presenciais.

São abordados vários aspectos essenciais para a compreensão dos paradigmas de redes locais.

Faz-se também, um estudo prático e sucinto de todos os componentes envolvidos no processo de comunicação, numa rede local.

Assim sendo, este manual permitirá ao leitor compreender o funcionamento de uma rede local, assim como o processo de instalação e configuração.

Índice geral

Índice de figuras

Índice de quadros

1. INTRODUÇÃO

A possibilidade e facilidade de comunicar e trocar informações com membros de outros departamentos ou secção da empresa/instituição sem ter de deslocar fisicamente é algo do qual não se pode abrir mão.

A partilha permanente de recursos e informações, constitui algo de imprescindível numa sociedade de informação e conhecimento.

Por essa e outras razões, torna-se extremamente clara, a necessidade de se fazer uma abordagem permanente dos paradigmas de redes locais de computadores.

A instalação e configuração de uma rede local de computadores não é um processo complicado, tanto que qualquer pessoa com conhecimentos fundamentais de informática, pode instalar e configurar uma rede local, claro está, desde que acompanhado por um manual elaborado de forma clara, prática e concisa. Há quem tenha instalado a sua primeira rede, baseando-se simplesmente em dicas técnicas disponíveis em alguns sites da Internet e sem nenhum apoio adicional.

O trabalho ora apresentado, pretende ser, além de um requisito para a obtenção do grau de Licenciatura, um manual que permita aos leitores que não sejam técnicos de rede, instalar uma rede local em casa ou no escritório sem recorrer a sessões de formação presenciais. Para os técnicos de rede, um manual que lhes permita actualizar os seus conhecimentos ou mesmo um modelo de manual para técnicos professores que vão ministrar um curso de redes locais de computadores e claro, sempre aberto a sugestões.

A metodologia utilizada para a elaboração deste trabalho baseou-se em pesquisas bibliográficas, pesquisas na Internet, experiências em laboratório e conversas/entrevistas com alguns técnicos de rede.

Sendo um trabalho de fim de um curso de Licenciatura em Ensino de Informática, a essência é uma mistura de pedagogia (ensino) com aspectos técnicos (informática). Dessa mistura, resulta um trabalho científico-tecnológico com suporte pedagógico, ou seja, os conteúdos são organizados de forma gradual e por ordem de prioridade e é utilizada uma linguagem simples que possibilite uma rápida captação e aprendizagem dos conteúdos.

São abordados vários temas, iniciando com conceitos fundamentais para a compreensão dos processos de comunicação, passando pela preparação e instalação das infraestruturas de cablagem, estudo das tecnologias de base disponíveis para redes locais, equipamentos de interligação de rede e terminando com considerações básicas sobre a gestão e segurança de redes.

2. ARQUITECTURAS DE REDES

A comunicação entre sistemas de computadores só se efectiva através da utilização de um conjunto de regras que são designadas por arquitecturas/protocolos de comunicação.

As arquitecturas de comunicação definem e descrevem um conjunto de conceitos que deverão ser considerados, para que haja comunicação. Englobam conceitos como camadas, serviços, protocolos, modos de comunicação, nomes e endereços. Estes, por sua vez, são aplicados à comunicação entre sistemas reais que são constituídos por hardware, software de comunicação, processos de aplicação e utilizadores humanos.

Uma arquitectura de comunicação pode ser proprietária ou aberta. É proprietária quando for específico de um dado fabricante e aberta quando é independente do fabricante, sendo uma arquitectura pública. Neste capítulo, destacam-se o modelo de referência OSI e a arquitectura/protocolo TCP/IP que são arquitecturas abertas.

2.1 O modelo de referência OSI (Open System Interconnection)

O modelo OSI foi desenvolvido pela ISO (International Standards Organization)[1] com o objectivo de fornecer um modelo que servisse de guia para qualquer fabricante de tecnologias para redes.

O modelo de referência OSI é constituído por camadas que permitem simplificar, em pequenos módulos, as operações necessárias para que dois computadores possam comunicar. A figura 2.1 mostra como estão organizadas as camadas.

[1] Instituição internacional de especificação de padrões.

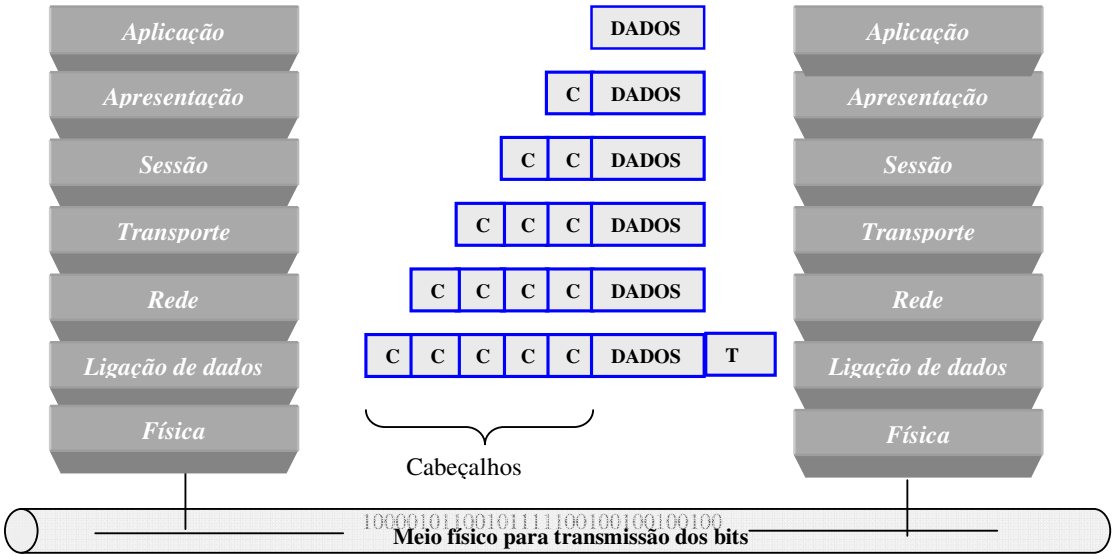

Figura 2.1 – Modelo OSI

Camada de Aplicação (Application Layer) – Esta camada é constituída pelas aplicações do utilizador e outras aplicações de rede. A sua principal função é fornecer serviços de redes às aplicações.

Camada de Apresentação (Presentation Layer) - Trata da representação dos dados, formatação de códigos e negociação da sintaxe de transferência de dados. Certifica de que os dados provenientes da rede possam ser usados pelas aplicações e também certifica de que as informações enviadas pelas aplicações possam ser transmitidas na rede.

Camada de Sessão (Session Layer) – Estabelece, mantém e administra sessões entre aplicações de rede.

Camada Transporte (Transport Layer) – Segmenta e reagrupa dados numa cadeia de dados para serem transmitidos. Garante a conexão entre dois sistemas.

Camada de Rede (Network Layer) – Determina o melhor caminho para transportar dados de um sistema para outro.
Utiliza um esquema de endereçamento lógico que pode ser gerido por um administrador de rede.

Camada de Ligação de Dados (Data Link Layer) - Possibilita a transmissão física através dos meios físicos de transmissão. Engloba a notificação de erros, topologias de rede e controlo de fluxo. Utiliza endereços MAC (Media Access Control) que são também designados de endereços físicos.

Camada Física (Physical Layer) - Fornece os meios eléctricos, mecânicos, processuais, e funcionais para activar e manter a ligação física entre sistemas. De forma resumida, fornece os meios físicos para transmissão dos bits e trata dos processos de codificação e descodificação de bits.

2.1.1 Encapsulamento de dados

O conceito de encapsulamento de dados está ilustrado na figura 2.1 Os C's indicam **cabeçalhos** e o T indica um **trailer**, sendo ambos adicionados aos dados durante a passagem pelas diferentes camadas.

Quando os dados enviados por um sistema A chegam a um sistema B, cada camada sabe o que fazer com esses dados através do cabeçalho que as suas camadas correspondentes no sistema A colocaram.

Cada camada comunica com a camada correspondente em outro sistema. Por exemplo, a camada de transporte de um sistema A comunica somente com a camada de transporte de um sistema B. Mas essa comunicação não é directa, ou seja, antes de uma camada comunicar com a camada correspondente, terá de usar serviços das camadas inferiores.

Cada camada oferece um conjunto de serviços a camada imediatamente superior. A camada de apresentação presta serviço à camada de aplicação, a camada de sessão presta serviço à camada de apresentação e assim sucessivamente. O processo vai se repetindo até os dados serem transmitidos para outro sistema.

Os dados são encapsulados em pacotes no sistema emissor e desencapsulados no sistema destinatário.

Para melhor entender o processo de encapsulamento de dados, veja os passos necessários para enviar um e-mail segundo o modelo OSI:

1º – Assim que o utilizador envia o e-mail, os caracteres alfanuméricos são convertidos em dados, com início na camada de aplicação até a camada de sessão.

2º – A camada de transporte prepara os dados e envia para a camada de rede. Também certifica de que os dois sistemas possam comunicar.

3º – Na camada de rede os dados são colocados num pacote que contém os endereços de origem e destino dos sistemas em comunicação. O pacote é enviado por dispositivos de rede.

4º – Cada dispositivo de rede deve colocar o pacote numa frame Ehernet na camada de ligação de dados. A frame possibilita a conexão, por exemplo, de outros dispositivos com a placa de rede, em redes com tecnologia Ehernet.

5º – Finalmente, a frame é convertida em sequência de bits para que possa ser transmitido pela rede através dos meios físicos de transmissão.

2.2 A arquitectura TCP/IP

Embora o modelo OSI tenha sido reconhecido universalmente, os especialistas defenderam que qualquer outra arquitectura desenvolvida com base nesse modelo, deveria ser simplificada, reduzindo o número de camadas intervenientes no processo de comunicação.

A arquitectura TCP/IP atingiu com enorme êxito, os objectivos primordiais inicialmente estabelecidos para o modelo OSI.

O TCP/IP tornou-se padrão dado à possibilidade de conectar redes heterogéneas e por ser uma arquitectura aberta. A figura 2.2 mostra como o modelo de camadas foi simplificado na arquitectura TCP/IP.

Figura 2.2 - Modelo OSI e TCP/IP

Camada Aplicação: Representa, tal como no modelo OSI, a interface entre as aplicações e o software de rede. Tecnicamente trata-se de APIs (Application Programming Interface)[2] implementadas em ficheiros DLLs (Dynamic Link Lybrary). Existem muitos utilitários e serviços padrões do TCP/IP na camada de aplicação, assim como, FTP, Telnet, SNMP, DNS, etc.
O Microsoft TCP/IP fornece duas interfaces para aplicações de rede: Windows Sockets e a interface NetBIOS.

Camada Transporte: Neste nível actuam os protocolos TCP (Transmission Control Protocol e UDP (User Datagram Protocol). O método desejado de entrega de dados determina qual o protocolo de transporte a ser utilizado.
O TCP é um protocolo orientado à conexão, o que significa que proporciona comunicação confiável, enquanto que o UDP, sendo um protocolo não orientado à conexão, não garante que os pacotes sejam entregues, sendo a aplicação responsável pela entrega dos pacotes de dados.

Camada Rede: Está relacionada com o encaminhamento e entrega dos pacotes de dados no destinatário que pode estar na mesma rede ou em outra rede. Engloba os protocolos IP, ARP, ICMP e o IGMP.

Camada de Interface de Rede: Engloba a placa de rede, drivers e a interface NDIS[3] (Network Driver Interface Specification). É responsável pela troca de informação entre computadores, manipulando sinais eléctricos e utilizando um determinado protocolo que depende da tecnologia de rede usada. Lida com tecnologias de comunicação como Ethernet, Token ring, etc.

[2] São compostas por procedimentos e funções a que os programas recorrem para comunicar via rede.

[3] API padrão que permite que uma placa de rede suporte vários protocolos ao mesmo tempo. Por exemplo, permite que a placa de rede suporte tanto a arquitectura TCP/IP como o IPX.

2.3 Fundamentos do TCP/IP

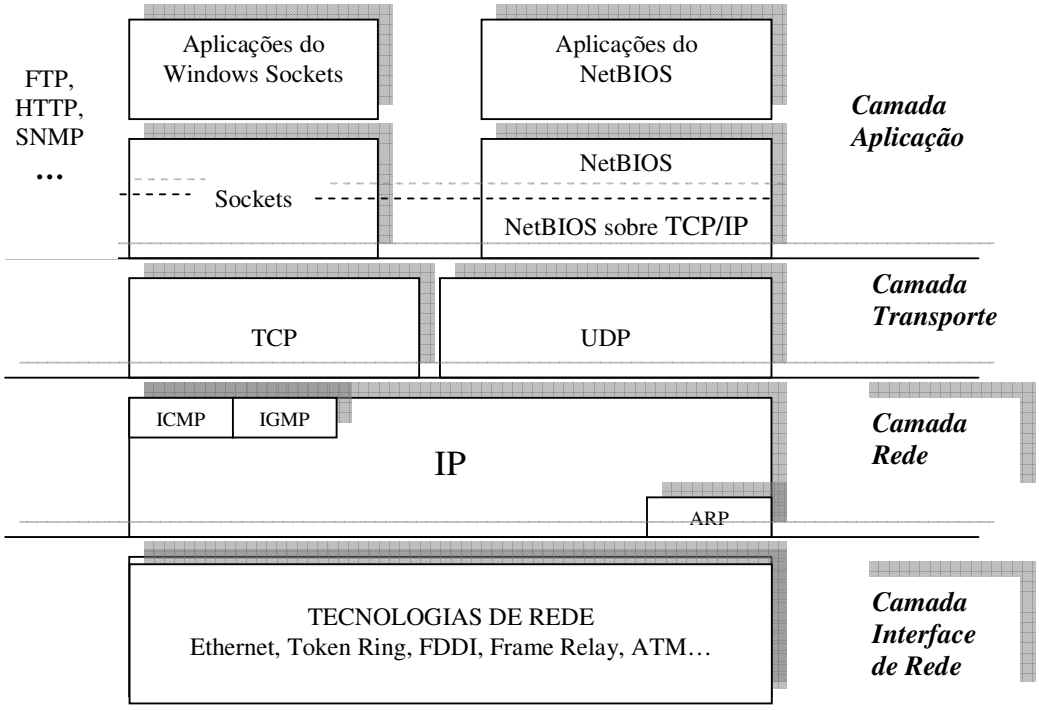

Figura 2.3 - Componentes das camadas do protocolo TCP/IP nos sistemas Microsoft

2.3.1 Sockets e Portas

Todas as aplicações de rede utilizam sockets directa ou indirectamente para comunicar e, muitas vezes, para compreender o funcionamento destas aplicações, há que ter conhecimento sobre sockets.

Basicamente, um socket consiste numa associação de um endereço e de um número designado por port number (número de porta) que, usadas em conjunto, definem o host com o qual se pretende comunicar.

As portas podem usar qualquer número entre 0 e 65535. Os números das portas das aplicações do lado cliente são dinamicamente determinados pelo sistema operativo, quando existe uma solicitação por serviço e os números das portas conhecidas para aplicações do lado servidor são predeterminados pelo Internet Assigned Numbers Authority (IANA)[4].

Quando, por exemplo, um browser como o Internet Explorer tenta estabelecer comunicação com um servidor http para aceder às páginas Web, utiliza um socket formado pelo endereço

[4] Instituição internacional responsável pela gestão de números de portas.

do servidor http, associado à porta (port) 80. Então o socket seria criado com a seguinte informação:

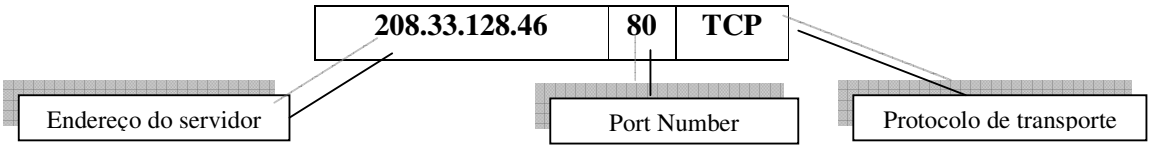

Figura 2.4 - Constituição de um socket

Nos sistemas da Microsoft, os números das portas podem ser examinados no ficheiro **services** que se encontra no directório **Windows\system32\drivers\etc**.

Cada socket está associado à uma aplicação que pode ser, por exemplo, um browser ou uma aplicação de correio electrónico.

A utilização do endereço, em conjunto com a porta 80 indica que o computador quer comunicar com o servidor HTTP cujo endereço é 208.33.128.46. O servidor, por sua vez, sabe o que responder porque tem conhecimento de que a porta 80 é utilizada quando se quer abrir uma conexão HTTP.

O **Windows Sockets** (WinSock) é um API que permite estabelecer a comunicação com outros componentes que usam TCP/IP com base na utilização de um socket que vai servir de elo entre aplicações e serviços que correm nos dois hosts.

Os números das portas conhecidas vão de 1 até 1023. A lista completa dos números de portas reservadas abrange a gama de 1 a 1023. As portas bem conhecidas (well-known ports) como do FTP, TELNET, HTTP, etc, encontram-se no intervalo de 1 a 255. As portas entre 1024 e 65535 podem ser usadas livremente por qualquer aplicação cliente.

A figura 5 mostra como se processa a comunicação utilizando sockets, entre um host cliente com endereço 138.205.5.96 e um servidor http com o endereço 208.33.128.46:

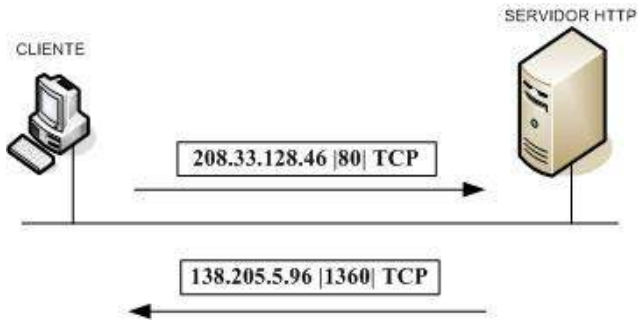

Figura 2.5 - Comunicação via socket

O cliente cria um socket com uma porta bem conhecida, mas o servidor responde com uma porta superior a 1024 que pode ser usada livremente. Ou seja, o servidor negoceia com o cliente para estabelecerem a sessão na porta 1360 que não está reservada a nenhum protocolo.

2.3.2 O protocolo IP (Internet Protocol)

O IP distingue-se de outros protocolos pelo facto de ser o que realmente permite a identificação dos hosts envolvidos na comunicação.

A essência do que circula na rede são os pacotes IP que através do processo de encapsulamento, levam no seu interior pacotes TCP ou UDP.

Os datagramas IP são transportados por outros tipos de componentes, dependendo da tecnologia de rede utilizada. Se a tecnologia for **ATM**, o pacote IP seria transportado dentro de uma ***célula ATM***, dentro de ***tokens*** caso a rede seja **Token Ring** e dentro de ***frames*** no caso de redes **Ethernet**.

2.3.3 Endereços IP

Cada host de uma rede TCP/IP (routers, impressoras de rede, servidores, etc) tem de ter um endereço IP que deve ser único em toda a rede em que o host actua, ou seja, dois hosts que actuam na mesma rede não podem ter o mesmo endereço IP.

Esse endereço é formado por quatro números na notação decimal, o que equivale a 32 bits (4 grupos de 8 bits). Como exemplo de um endereço IP temos o seguinte: 198.27.254.87.

O endereço é representado em notação decimal para ser mais amigável ao utilizador, já que trabalhar com dígitos binários seria extremamente tedioso e cansativo.

Além do endereço IP de 32 bits (IP versão 4), existe um outro tipo de endereço IP que é constituído por 128 bits (IP versão 6), mas que ainda está num processo de migração. Na Internet pode-se encontrar várias informações sobre a nova versão do IP que foi desenvolvido devido à limitação dos números de hosts e de redes suportados pelos endereços de 32 bits.

2.3.4 Classes de endereços e máscara de sub-rede (subnet mask)

Num endereço IP, parte do endereço identifica a rede (network ID) ou segmento de rede a que o host pertence e o resto representa a identificação do host (host ID) dentro dessa rede.

O que vai determinar quantos bits vão identificar a rede e os hosts é a máscara de sub-rede da classe a que o endereço pertence. Existem 5 classes de endereços IP: A, B, C, D e E.

Para saber a classe de um determinado endereço, basta conhecer as características de cada classe, apresentadas nas tabelas abaixo:

Classe	Gama de endereços
A	**0**.0.0.0 a **126**.255.255.255
B	**128**.0.0.0 a **191**.255.255.255
C	**192**.0.0.0 a **223**.255.255.255
D	**224**.0.0.0 a **239**.255.255.255
E	**240**.0.0.0 a **247**.255.255.255

Tabela 1 – Gama de endereços por classe

Agora já é possível saber a que classe pertence um determinado endereço. Basta ver o primeiro byte. Assim sendo, pode-se facilmente ver que o endereço 197.23.58.11 é da classe C porque o primeiro byte (197) pertence ao intervalo de endereços da classe C.
Cada classe tem uma máscara de sub-rede que vai indicar quantos bits do endereço identifica a rede e os hosts, como indica a tabela 2.

Classe	Máscara
A	255.0.0.0 (11111111.00000000.00000000.00000000)
B	255.255.0.0 (11111111.11111111.00000000.00000000)
C	255.255.255.0 (11111111.11111111.11111111.00000000)

Tabela 2 – Máscara de sub-rede para cada classe

Os bits mais significativos (1) representam o network ID e os menos significativos (0) representam o host ID. Assim sendo, pode-se concluir que para uma rede da classe C é possível definir 256 endereços ($2^{8\ bits}$), já que a parte reservada para identificação dos hosts tem 8 bits. Mas desses 256 endereços nem todos podem ser atribuídos, pois, alguns são de uso reservado. A tabela 3 apresenta um resumo do intervalo de endereços válidos, total de endereços de rede e total de hosts por rede em cada classe A, B e C.

Classe	Intervalo de endereços Válidos	Total de endereços de rede	Total de hosts por rede
A	1.0.0.0 a 126.0.0.0	$2^7 - 2$	$2^{24} - 2$
B	128.1.0.0 a 191.254.0.0	$2^{14} - 2$	$2^{16} - 2$
C	192.0.1.0 a 223.255.254.0	$2^{21} - 2$	$2^8 - 2$

Tabela 3 – Intervalos de endereços válidos por classe

Existem vários casos de endereços reservados. Por exemplo, o endereço de rede 0.0.0.0 é definido para broadcasts e 127.0.0.1 é definido como endereço de loopback que serve para testar o TCP/IP na própria máquina.

2.3.5 Endereços IP oficiais e privados

Os endereços IP oficiais (visíveis na Internet) são atribuídos por entidades responsáveis pela gestão dos endereços.

Os endereços oficiais são utilizados apenas por entidades que prestam algum tipo de serviço na Internet. Para se obter um endereço IP oficial, há que pagar uma taxa. Por exemplo, A CV Telecom possui endereço IP oficial. Os utilizadores domésticos têm acesso à Internet, utilizando endereços IP temporários fornecidos pelo provedor de serviços de internet, de maneira que esses endereços não são oficiais. Em computadores que não estão ligados directamente à Internet, pode-se utilizar endereços não oficiais ou privados. Estes endereços foram definidos em três gamas:

Classe	Gama
A	10.0.0.0 a 10.255.255.255
B	172.16.0.0 a 172.31.255.255 169.254.0.0 a 169.254.255.255 (só para redes Microsoft)
C	192.168.0.0 a 192.168.255.255

Tabela 4 – Gama de endereços privados

Para melhor compreender estes conceitos, convém analisar um exemplo prático.

Uma empresa possui um endereço IP oficial que utiliza na sua ligação à Internet. Dentro do edifício onde está instalada, existem vários hosts em rede. A empresa quer que todos os

computadores dessa rede tenham acesso à Internet. Mas como fazer isso, se ela possui apenas um endereço IP oficial? A solução seria recorrer a endereços não oficiais ou privados. O administrador de rede pode utilizar qualquer uma das gamas de endereços especificados na tabela acima para atribuir endereços IP aos hosts dentro da rede, pois, estes não estão visíveis na Internet.

Todo o processo de conexão à Internet estará a cargo do host que possui o endereço IP oficial. Assim sendo, quando um host qualquer da rede necessita de conectar à Internet, o host com IP oficial estabelece a ligação, mas com o seu próprio endereço IP que é o único reconhecido na Internet. Os outros hosts da rede não podem ligar directamente à Internet porque não possuem um IP oficial.

2.3.6 Resolução de endereços IP

Quando se enviam pacotes IP para a rede, os endereços IP devem ser traduzidos em endereços físicos (MAC Address), de forma a serem interpretados pela tecnologia de rede subjacente que pode ser, por exemplo, a Ethernet.

O processo de tradução de endereços IP em endereços Ethernet é realizado pelo protocolo ARP (Address Resolution Protocol) e compreende os seguintes passos:

- Sempre que é necessário enviar um pacote para determinado endereço IP, é consultada uma tabela ARP[5] para determinar se existe uma entrada que contenha já a correspondência entre o endereço IP e o endereço físico: se existir é usado esse endereço físico;
- Caso não exista na tabela de ARP o endereço físico correspondente ao endereço IP pretendido, o protocolo ARP envia uma mensagem de broadcast para a rede que será recebida por todos os hosts, solicitando o endereço físico correspondente ao endereço IP em causa;
- O host com o endereço IP pretendido responderá à mensagem de ARP enviando uma resposta contendo o seu endereço físico; essa resposta será recebida pelo host original que guardará o endereço físico na sua tabela ARP e enviará o pacote.

A conversão de endereços físicos para endereços IP é realizada pelo protocolo RARP (Reverse Address Resolution Protocol), sendo usada essencialmente por hosts que não possuem um sistema operativo no arranque. Mas estes hosts têm endereços de hardware e na

[5] Esta tabela pode ser consultada com o comando **arp –a** a partir da linha de comandos do MSDOS.

hora do arranque enviam uma mensagem RARP, com o objectivo de saber quais são os endereços IP que correspondem aos seus endereços físicos.
Existem servidores RARP que manipulam as solicitações RARP e respondem com o endereço IP para o host solicitante, podendo assim, continuar com o processo de arranque.

2.3.7 Resolução de nomes e atribuição de endereços nos sistemas Microsoft

Numa rede local com sistemas da Microsoft, os computadores são referenciados por um nome em vez de endereço IP, o que significa que a cada nome corresponde um endereço IP.
A resolução de nomes é um processo que visa obter endereços IP de hosts, em função dos seus nomes. Existem dois tipos de nomes: **NetBIOS names e host names**.
O NetBIOS name é configurado durante o processo de instalação do sistema operativo. Engloba o **nome do computador**, nome **de domínio ou grupo de trabalho** e **nomes de utilizadores** registados num domínio. Os nomes NetBIOS devem ser únicos e devem ter no máximo 15 caracteres.
Para obter endereços IP em função de nomes NetBIOS o sistema pode utilizar a seguinte sequência que não é sempre igual:

1. **NetBIOS name cache** : contém registos de nomes NetBIOS previamente registados e pode ser consultada com o comando **nbtstat –c**, pressupondo que o nome já foi resolvido pelo menos uma vez.
2. **Broadcast:** caso o **name cache** esteja vazia ou não contenha a equivalência entre o nome procurado e um endereço IP, é emitida uma série de broadcasts.
3. **Ficheiro LMHOSTS**: um ficheiro texto onde o administrador de rede pode adicionar equivalências entre NetBIOS names e endereços IP. No Windows podemos encontrar o ficheiro no directório **Windows\system32\drivers\etc** com a extensão **.sam** que significa sample (amostra). Então a primeira coisa a fazer é copiar este ficheiro para o mesmo directório, mas sem extensão. Não se deve alterar o ficheiro original, pois, contém informação sobre como usar LMHOSTS.
4. **NetBIOS name server:** em redes Microsoft é, normalmente, representado por um servidor WINS.
5. **DNS server:** embora seja utilizado para fornecer endereços IP em função de *host names* e não *NetBIOS names,* também é possível recorrer a este tipo de servidor quando nenhuma das opções anteriores tiver sucesso.

6. **Ficheiro HOSTS:** parecido com o LMHOSTS, contém equivalências entre host names e endereços IP. O sistema recorre a este ficheiro em último caso. Também se encontra no directório **Windows\system32\drivers\etc**.

Quando se usa um comando NetBIOS como **nbtstat** é usada a resolução de nomes NetBIOS.
A resolução de host names é usada apenas quando é executado um comando que utilize sockets directamente, como o **ping**, **telnet**, **ftp** etc.
Os host names podem conter no máximo 255 caracteres e podem estar associados a nomes de domínios. Como exemplo de host names temos: **www.ise.cv**, **ftp.microsoft.com**, **localhost**, etc.
Para se obter endereços IP em função de host names também há uma sequência a seguir:

1. **Comparação com o nome local:** se o nome especificado for igual ao do host onde se executa o comando faz-se logo a resolução.
2. **Ficheiros HOSTS.**
3. **Servidor DNS:** Se os processos anteriores não resultarem, procura-se, caso sejam especificados, um ou mais servidores DNS na rede.
4. **Servidor WINS:** embora seja utilizado para resolver nomes NetBIOS, o sistema procura ali também o nome de um host.
5. **Broadcast.** A seguir é enviado um broadcast para todos os hosts da rede.
6. **LMHOSTS:** Este é o último local onde o endereço é procurado.

A resolução de nomes facilita o trabalho ao utilizador. Se não existisse esse processo, o utilizador teria de fornecer o endereço IP de todos os hosts com os quais pretende comunicar. Por exemplo, para ter acesso ao Hotmail, em vez de usar o nome **www.hotmail.com**, teria de introduzir o endereço IP do servidor do **Hotmail**.
É muito mais fácil memorizar nomes do que endereços IP.

Os endereços IP podem ser atribuídos de forma estática ou dinâmica.
Para uma rede com poucos computadores, torna-se fácil atribuir endereços IP, máscaras de sub-rede[6] e gateways manualmente a cada computador. A figura 2.6 mostra o processo de configuração estática no Windows XP.

[6] Todos os hosts de um segmento de rede devem ter a mesma máscara de sub-rede para que possam comunicar.

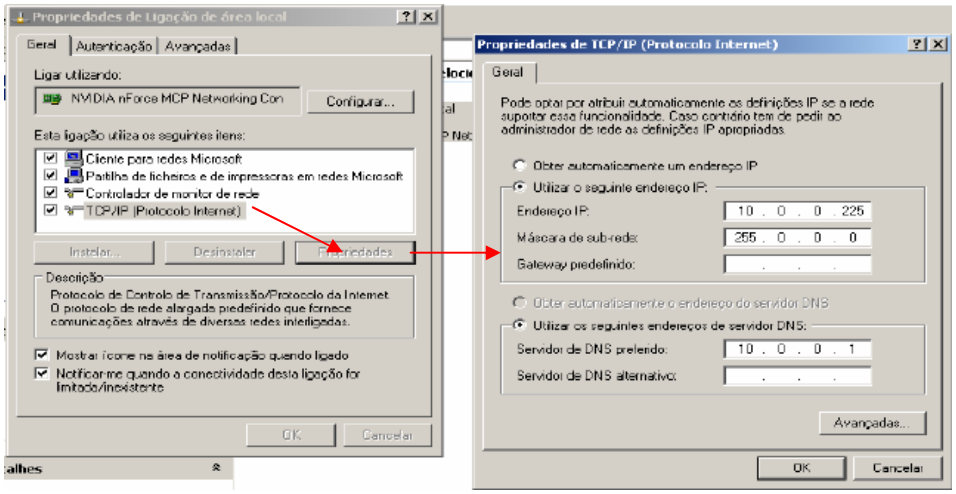

Figura 2.6 - Configuração estática de endereço IP no Windows XP

Numa rede local com 100 computadores, configurar cada computador manualmente seria extremamente cansativo, podendo induzir a erros. Assim sendo, o administrador de rede pode optar por uma configuração dinâmica.

Este tipo de configuração implica a utilização de um servidor **DHCP** que centraliza todas as configurações necessárias.

O DHCP atribui endereços IP automaticamente a todos os hosts da rede. Quanto um host tenta conectar à rede pela primeira vez, envia um broadcast para encontrar um servidor DHCP e a informação de endereçamento IP. Este processo é designado por **DHCP DISCOVER**.

O servidor DHCP, ao receber a mensagem, envia uma mensagem de oferta de endereço (**DHCP OFFER**) ao host solicitante.

O host aceita a oferta e envia uma mensagem ao servidor DHCP (**DHCP REQUEST**), solicitando um endereço IP.

O servidor DHCP que fez a oferta, atribui um endereço ao host e envia uma mensagem de confirmação (**DHCP ACKNOWLEDGMENT**).

Embora a configuração dinâmica seja muito mais flexível, existem casos em que a configuração estática torna-se obrigatória, por exemplo, no caso de servidores, já que são estaticamente referenciados por servidores DNS, servidores WINS, etc. Nesses computadores, existem algumas modificações que têm de ser feitas manualmente.

Outra vantagem tem a ver com a facilidade de migração de um host de uma rede para outra, sem necessidade de alterar as configurações de rede. Se a configuração fosse estática, seria necessário a reconfiguração (network ID, máscara de sub-rede etc) do host para se integrar na nova rede.

Claro que uma rede pequena não justifica a aquisição de um servidor DHCP dedicado. O administrador deverá ter sempre em conta a relação custo/benefício.
A configuração de servidores (DNS, WINS, DHCP etc) não é objectivo deste trabalho, mas com as informações aqui apresentadas, pode-se perfeitamente decidir qual o método de resolução de nomes e endereços (estática ou dinâmica) a aplicar na rede.
Cada sistema operativo acarreta um conjunto de funções específicas que o técnico que vai instalar a rede deverá conhecer, devendo para tal, adquirir um manual do sistema. Por exemplo, um técnico pode instalar uma rede local com todos os cabos ligados aos equipamentos, mas na hora de configurar o sistema (que pode ser Windows 2000 server, Windows NT server, Unix, etc) terá de conhecer as suas funcionalidades. Para tal pode comprar ou emprestar um livro sobre o sistema que vai utilizar na rede.

Neste segundo capítulo, fez-se uma abordagem teórico-prática sobre a arquitectura TCP/IP, visto que é a arquitectura da Internet.
Existem técnicos que conseguem instalar uma rede local, mas no caso de surgirem problemas, ou não conseguem resolver, ou resolvem o problema, mas depois de muito tempo. Para uma sociedade como a actual, exige-se técnicos que consigam dar respostas em tempo útil e, para tal, há que dominar com alguma profundidade, os conceitos abordados aqui principalmente no que toca à resolução de nomes e atribuição de endereços.
Os conceitos apresentados até aqui, são de extrema importância para quem quer instalar e configurar uma rede local baseado no protocolo TCP/IP.

3. TOPOLOGIAS E CABLAGEM DE REDES

A topologia de uma rede refere-se à forma como os hosts da rede estão organizados. Determina caminhos físicos existentes e utilizáveis entre quaisquer pares de hosts conectados a essa rede.

Na construção de sistemas de cablagem podem ser utilizadas várias topologias que vão, juntamente com os outros equipamentos, definir a eficiência e velocidade da rede. Vamos estudar as topologias que podem ser encontradas em instalações de redes locais, são elas: ***barramento (bus), estrela (star), anel (ring), árvore (tree) e mistas (mesh).***

3.1 Topologia em bus

Uma topologia em bus conecta vários hosts num mesmo cabo coaxial. Os terminadores colocados nas extremidades do cabo absorvem os sinais, para que estes não sejam reflectidos. Caso não sejam utilizados terminadores, os sinais espalham-se pela rede, tornando-a inutilizável.

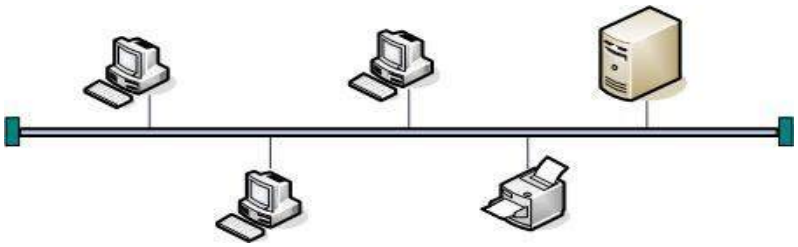

Figura 3.1 - Topologia em bus

As vantagens de uma topologia em bus são o custo e a facilidade de instalação.

Uma desvantagem dessa topologia, tem a ver com o facto de, no caso de haver corte ou falha num dos cabos da rede, a rede não funcionar.

Se houver corte do cabo, os sinais não chegam ao terminador, o que significa que os sinais são espalhados pela rede, inutilizando-a.

Os hosts na rede, só podem transmitir dados um de cada vez, o que constitui uma desvantagem. Caso dois ou mais hosts da rede tentem transmitir dados ao mesmo tempo, ocorrerá uma colisão provocando a degradação da rede.

Para recuperação e controlo do acesso à rede, é utilizado um método chamado **CSMA/CD** (Carrier Sense Multiple Access Colision Detect) que evita a ocorrência de outra colisão.

Utilizando esse método, quando ocorrer uma colisão, esta é prolongada até que todos os hosts da rede percebam que houve uma colisão. Depois da colisão ser detectada por todos os hosts, a transmissão é interrompida. O CSMA/CD obriga cada host a aguardar a sua vez antes de tentar retransmitir os dados, para evitar uma nova colisão.

3.2 Topologia em estrelas

Numa topologia em estrela, todos os hosts da rede estão conectados a um dispositivo central que pode ser um hub ou um switch. É a topologia mais utilizada nas redes locais.

Quando um host envia dados para outro host, o hub/switch recebe os dados e transmite-os para o host de destino.

Como cada host está conectado ao nó central por um cabo UTP ou STP separado, falhas num dos cabos só vai comprometer o host ligado a esse cabo que não consegue comunicar-se com os restantes hosts. Contudo, se o dispositivo central falhar, toda a rede falha. As vantagens da topologia incluem o grau de confiança da rede e facilidade de manutenção.

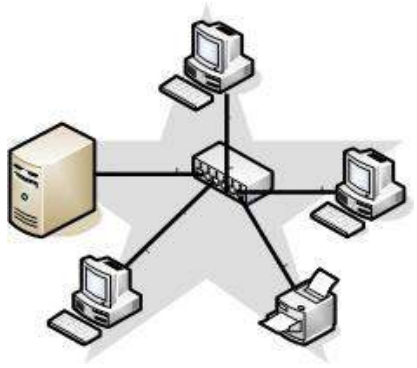

Figura 3.2 - Topologia em estrela

Uma desvantagem em relação à topologia bus, reside no facto de utilizar um equipamento adicional para conexão dos hosts que é o dispositivo central (hub/switch) o que implica um custo adicional.

Porém, mais vale ter uma rede confiável, mesmo que seja um pouco mais custoso, do que ter uma rede barata com baixo grau de confiança.

3.3 Topologias em anel

Na topologia em anel, cada host na rede está ligado a dois outros hosts. Não há início nem fim do cabo, formando um anel.

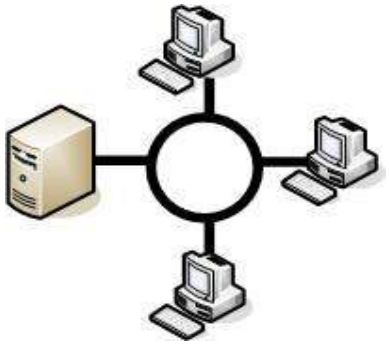

Figura 3.3 – Topologia em anel

Os hosts utilizam um **transceptor**[7] para comunicar com os hosts adjacentes. Os transceptors regeneram os sinais que recebem e retransmitem-nos novamente para a rede.

A maior vantagem desta topologia é a redundância e garantia de comunicação em caso de corte de um dos cabos.

3.4 Topologia em árvore

Esta topologia é composta por vários níveis hierárquicos, assumindo o meio físico uma estrutura arborescente com vários níveis. Pode ser vista como resultante da interligação hierarquizada de várias topologias em estrela.

3.5 Topologia mista

A topologia mista resulta da combinação de várias topologias simples. Em cada nível hierárquico do sistema de cablagem, adopta-se a topologia mais adequada.

[7] Transceptor = Transmissor/Receptor – transmite e recebe sinais da rede. Faz a conversão dos sinais, adaptando-os ao dispositivo de rede. Ex.: conversão de sinais de fibra óptica para sinais eléctricos e vice-versa.

Com esta topologia, procura-se explorar as melhores características das topologias envolvidas. Alguns exemplos são topologias de estrelas conectadas em anel e árvores conectadas em barramento. A figura 3.4 ilustra uma topologia mista que conecta várias topologias em estrela utilizando uma topologia em anel.

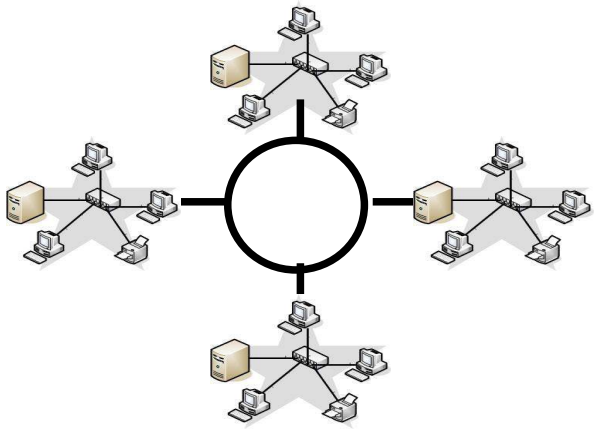

Figura 3.4 – Topologia mista

Depois de estudar as topologias, resta conhecer os meios físicos de transmissão, ou seja, os cabos de rede e outros componentes de cablagem.

Os cabos utilizados nas redes são: **coaxiais, pares entrançados e fibras ópticas**.

3.6 Cabos coaxiais

Existem dois tipos de cabos coaxiais: fino (Thin Ethernet) e grosso (Thick Ethernet).

O cabo coaxial fino encaixa-se num conector do tipo BNC (British Naval Conector).

As figuras a seguir mostram os componentes utilizados nas conexões com cabos Thin Ethernet. Os conectores **"T"** (figura 3.7) são acoplados ao conector **BNC** da placa de rede, e nele são conectados os cabos que ligam o host aos seus vizinhos. O terminador (figura 3.5) deve ser ligado no último conector "**T**" da cadeia.

Figura 3.5 – Terminador

Figura 3.6 - Conector BNC

Figura 3.7 - Conector T

O cabo Thin Ethernet deve formar uma linha que vai do primeiro ao último host da rede, sem desvios. Apenas o primeiro e o último host da linha devem utilizar o terminador BNC. A

figura 3.8 mostra como deverá ficar o cabo ligado à placa de rede dos hosts que ficam no meio da linha e a figura 3.9 mostra como deverá ficar o cabo ligado à placa de rede dos hosts que ficam na extremidade da rede.

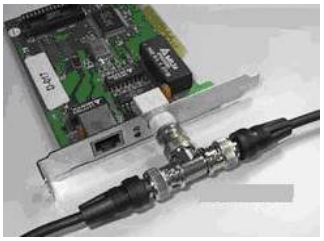

Figura 3.8 - Conexão de cabos Thin Ethernet na placa de rede utilizando conector "T"

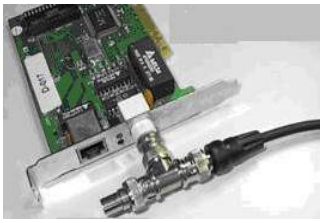

Figura 3.9 - Conexão de cabos Thin Ethernet na placa de rede com terminador na extremidade

Como pode verificar nas figuras acima, os hosts são ligados por duas secções de cabos. Em cada um deles, são usados conectores "**T**" para permitir as conexões nas placas. O host que fica no meio liga-se aos outros dois através de duas secções de cabo Thin Ethernet, ligados ao conector "**T**". Os hosts, localizados nas extremidades (primeiro e último host da rede), possuem terminadores BNC.

Vale a pena lembrar que os cabos Thin Ethernet não são usadas em redes novas, mas pode surgir casos em que seja necessário fazer a manutenção em redes antigas, baseadas neste tipo de cabo.

O cabo Thick Ethernet encaixa-se num conector AUI (Attachment Unit Interface). Este conector não é entretanto, ligado directamente ao cabo da rede. Sua ligação é feita através de um cabo adicional (AUI drop cable, mostrado na figura 3.10).

Figura 3.10 - AUI Drop cable

Este cabo é finalmente ligado à rede através de um transceptor. Neste tipo de cablagem, o conector AUI de 15 pinos da placa de rede é ligado através de um cabo a um dispositivo chamado MAU (media attachment unit, ou media access unit, ou multistation access unit). o MAU perfura o cabo de rede thick Ethernet, alcançando a parte condutora que transmite os dados. Este dispositivo tem como principal função, transmitir e receber da rede os sinais gerados e recebidos pelo conector AUI. Por isso é também chamado de transceptor. As demais portas da placa de rede (ligadas aos conectores RJ-45 e BNC) possuem transceptors embutidos na própria placa (onboard). Cada MAU por sua vez, é fixado ao cabo da rede propriamente dito. As secções deste cabo formam uma cadeia, de forma similar à formada por cabos Thin Ethernet. São usados terminadores nas extremidades. Na figura 3.11 é ilustrada a ligação do drop cable ao conector AUI da placa de rede.

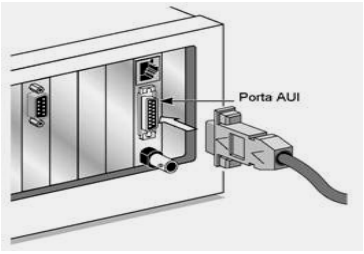

Figura 3.11 - Ligação ao conector AUI

A figura 3.12 mostra como fica configurada a ligação com o cabo Thick Ethernet.
Quando o cabo atravessa o conector vampiro do MAU, é perfurado por pequenos ”dentes” que provoca o contacto com o condutor interno do cabo. Dessa forma, o MAU poderá transmitir e receber sinais da rede.

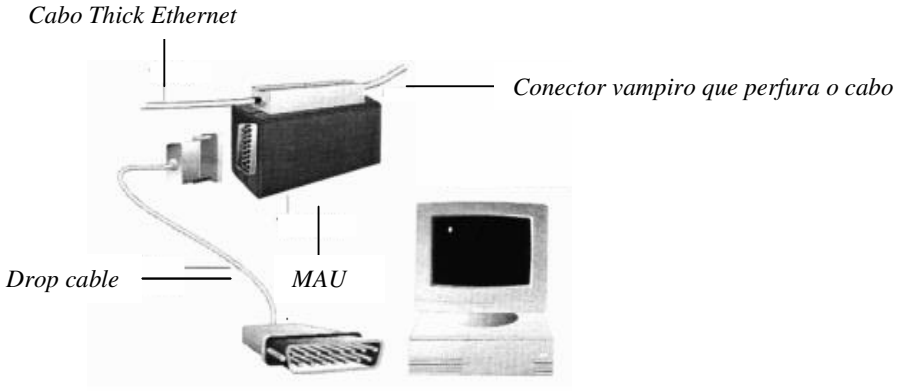

Figura 3.12 - Esquema de ligação de cabo Thick Ethernet

Redes com este tipo de cabo já caíram em desuso há alguns anos. Visando facilitar a sua migração para cabos de pares entrançados (conectores RJ-45), foram desenvolvidos conversores entre esses dois padrões. Caso a placa possua apenas o conector AUI, pode-se fazer a sua ligação com uma rede baseada em pares entrançados, através de um adaptador (transceptor) como o mostrado na figura 3.13. Possui uma conexão AUI, que deve ser ligado à placa de rede através de um drop cable, e uma conexão RJ-45, para ligação nas redes modernas.

Figura 3.13 - Adaptador AUI-RJ-45

3.7 Cabos de pares entrançados (twisted pairs)

Os cabos de pares entrançados são constituídos por um conjunto de 2 ou 4 pares de fios condutores. Os dois fios que formam cada par, são entrançados entre si com o objectivo de evitar interferências electromagnéticas. Normalmente são utilizados com conectores RJ-11 (possuem 2 pares de fios e são utilizados nas instalações telefónicas) e RJ-45 (4 pares de fios). Existem dois tipos de cabos de pares entrançados: **UTP** (Unshielded Twisted Pair) e **STP** (Shielded Twisted Pair). Existem várias categorias de cabos UTP e STP[8], mas vou abordar apenas os mais utilizados que são das categorias 3 (UTP/STP Cat 3) e 5 (UTP/STP Cat 5). O tipo e a categoria normalmente são impressos no cabo.

Os cabos Cat 3 podem ser utilizados para transmissão de voz (telefone) ou dados (até 10 Mbps). Não é o tipo de cabo recomendado para redes de dados porque a sua largura de banda máxima de 10 Mbps não se aplica às novas tecnologias de redes locais.

Os cabos Cat 5 podem ser utilizados tanto para transmissão de voz como para transmissão de dados a alta velocidade. A largura de banda é de 100Mbps, mas com algumas tecnologias actuais pode chegar a 1000Mbps. O comprimento máximo do cabo é de 100 metros, mas pode-se utilizar dispositivos que permitem a regeneração dos sinais do cabo para superar essa limitação.

[8] Existem cabos UTP e STP nas categorias 1, 2, 3, 4, 5, 6, 7. Os mais populares são os da categoria 3 e 5.

O cabo UTP, por ser mais barato e fácil de instalar, é mais utilizado que o cabo STP.

A principal diferença entre os dois tipos de cabos reside no facto do cabo STP utilizar um protecção de folha metálica em torno dos pares de fio, sendo mais adequado a ambientes com fortes fontes de interferências, como grandes motores eléctricos e estações de rádio que estejam muito próximas.

Quanto maior for o nível de interferência electromagnética, menor será o desempenho da rede, pois, essas interferências podem alterar o sinal original ou até destruí-la.

Numa rede com cabo de pares entrançados, cada host utiliza um cabo com conectores RJ-45 em suas extremidades. As conexões são simples porque são independentes. Para adicionar um novo host à rede, basta ligar uma extremidade do cabo na placa de rede e a outra extremidade no hub/switch. A figura 3.14 apresenta um cabo UTP com conectores RJ-45.

Figura 3.14 - Cabo UTP com conectores RJ-45

3.7.1 Preparação de cabos UTP

Para construir cabos de rede com par entrançado e conectores RJ-45, deve-se possuir as ferramentas apropriadas, assim como nos cabos coaxiais. A ferramenta utilizada é um alicate para crimp de conectores RJ-45. Há que ter em atenção que existe um tipo de alicate, semelhante ao do RJ-45, que é usado para conectores RJ-11, que tem 4 contactos e é usado para cabos telefónicos. Os conectores RJ-45 possuem 8 contactos. A figura 3.15 mostra-nos um alicate para crimp de conectores RJ-45.

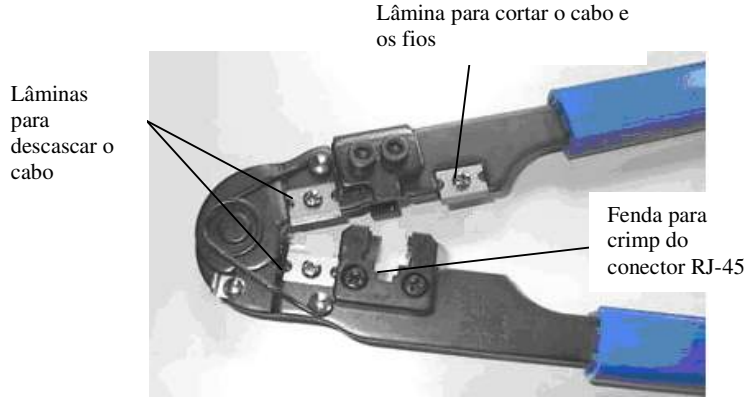

Figura 3.15 - As partes de um alicate para crimp RJ-45

Também existem alicates que suportam os dois tipos de conectores.

Para construir o cabo, os passos são os seguintes:

1º - Use a lâmina para cortar o cabo no tamanho necessário.

2º - Use as lâminas para descascar o cabo, retirando cerca de 3 cm da capa plástica. É preciso alguma prática para fazer a operação correctamente. As lâminas devem cortar a capa plástica sem tocar nos fios. Depois de fazer um corte superficial, puxe o cabo para que a parte plástica seja retirada.

Figura 3.16 - Descascando o cabo

3º - Separe os pares uns dos outros na seguinte ordem, da esquerda para direita: verde/branco-verde laranja / branco-laranja, azul/branco-azul, marrom/branco-marrom. Depois de separar os pares, falta organizar os fios. Teoricamente pode-se utilizar qualquer combinação de fios, desde que se faça a mesma combinação nas duas extremidades. Para este exemplo, será utilizada a seguinte combinação: Branco-verde / Verde, Branco-laranja / Azul, Branco-azul / Laranja, Branco-marrom / Marrom que corresponde ao padrão **T568A**[9]. Além deste, existe o padrão **T568B** cuja combinação é: Branco-laranja / Laranja, Branco-verde / Azul, Branco-azul / Verde, Branco-marrom / Marrom. É aconselhável utilizar um destes padrões para uniformizar o sistema de cablagem e facilitar manutenções posteriores.

Figura 3.17 - Combinação dos fios para serem conectados no RJ-45

[9] Os padrões T568A e T568B foram definidos por entidades internacionais de padronização de equipamentos para redes.

4º - Corte as extremidades dos 8 fios com as lâminas de corte, de modo a ficarem todos com o mesmo comprimento. O comprimento total da parte descascada deverá ser aproximadamente 1,5cm.

5º - Introduza cuidadosamente os 8 fios dentro do conector RJ-45. Cada um dos oito fios deve entrar totalmente no conector. Depois da conexão, confira se os 8 fios estão na ordem correcta.

6º - Estando os fios na ordem correcta, só falta agora fazer o crimp com o alicate para afixar o cabo no conector. Introduza o conector na fenda apropriada existente no alicate e aperte-o. Nesta operação duas coisas acontecerão. Os oito contactos metálicos existentes no conector entrarão em contacto com os 8 fios correspondentes. Ao mesmo tempo, uma parte do conector irá prender com força a parte do cabo que está com a capa plástica externa. O cabo ficará definitivamente fixo no conector. Para terminar, há que testar o cabo utilizando testadores de cabos RJ-45. O par é constituído por um testador e um terminador.

Figura 3.18 - Testando cabos RJ-45

Uma das extremidades do cabo deve ser ligada ao testador, no qual se deve pressionar o botão ON/OFF. Em seguida, encaixa-se a outra extremidade do cabo no terminador. Pressionando o botão ON/OFF no testador, uma luz (LED)[10] acenderá intermitentemente. Também no terminador, quatro LEDS acenderão intermitentemente em sequência, indicando que cada um dos quatro pares está correctamente ligado.

[10] LED (Light Emitting Diode)- Diodo emissor de luz – componente electrónico que emite uma luz quando é atravessado pela corrente eléctrica.

3.7.2 Tomadas para cabos com conectores RJ-45 fêmea

Além dos conectores RJ-45 usados nos cabos (RJ-45 macho) temos os conectores RJ-45 fêmea, onde se vai encaixar o RJ-45 macho. Uma rede bem estruturada passa pela utilização não só de calhas de paredes por onde passam os cabos, como também pela utilização de tomadas de paredes onde se vai ligar os cabos. A quantidade de tomadas em cada sala depende da quantidade de computadores a serem ligados à rede nessa sala. Por exemplo, numa sala de aula normal duas tomadas são suficientes, mas para um laboratório de informática precisará de muitas tomadas, pois, estarão vários computadores em rede. Antes de tudo, deve-se traçar a localização das tomadas e passar o cabo pela calha até chegar ao local escolhido. A figura 3.19 apresenta exemplos de tomadas RJ-45.

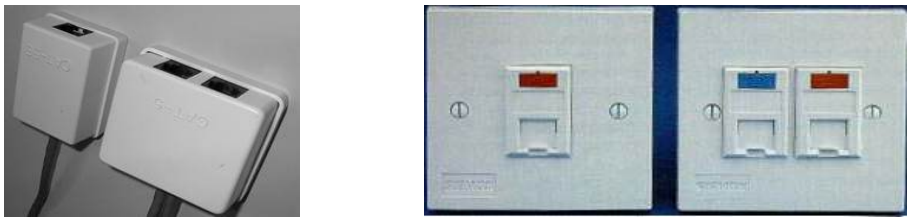

Figura 3.19 – Tomadas RJ-45

Na figura 3.20, estão ilustrados dois conectores RJ-45 fêmea que constituem as tomadas.

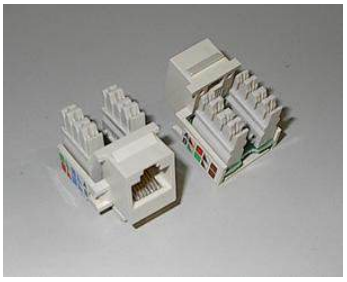

Figura 3.20 – Conectores RJ-45 fêmea

3.7.3 Montagem de tomadas RJ-45

A cápsula inferior da tomada fica afixada na parede através de parafusos. Pode-se utilizar um perfurador de parede e, em seguida, afixar a cápsula utilizando buchas e parafusos. Em caso de dúvidas, as tomadas são acompanhadas de manuais de instruções de instalação passo a passo. É importante ter os manuais, principalmente no caso de produtos não padronizados, pois, existem vários fabricantes e cada um pode utilizar uma especificação diferente.

Os passos são os seguintes:

1º - Use um alicate para crimp RJ-45 para descascar o cabo até aproximadamente 3 cm.

2º - Encaixe cada um dos fios nas posições correctas, usando um dos padrões de cablagem (T568A ou T568B). Os fios devem ser totalmente encaixados nas fendas do conector. Para tal é utilizada uma ferramenta especial como a da figura 3.21.

3º - Para cada uma das 8 posições do conector, posicione a ferramenta de inserção como está ilustrado na figura 3.21. A ferramenta tem uma extremidade cortante que deverá eliminar o excesso do fio. A parte cortante deve ficar orientada para o lado externo do conector. Pressione a ferramenta firme e perpendicularmente à ficha. A ferramenta fixa o fio no conector, eliminando ao mesmo tempo o excesso.

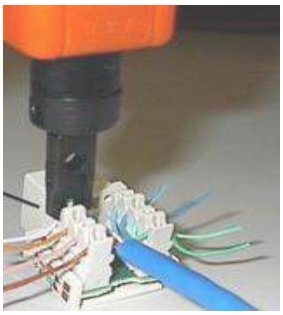

Figura 3.21 - Afixação dos fios no conector RJ-45 fêmea

4º - Depois da conexão, deve-se proceder ao teste. A secção completa do cabo terá um conector RJ-45 macho numa extremidade (para ser conectado a um equipamento de interligação de rede) e um conector RJ-45 fêmea na outra extremidade (onde se vai conectar um host qualquer da rede). A figura 3.22 apresenta a configuração de uma secção com tomadas.

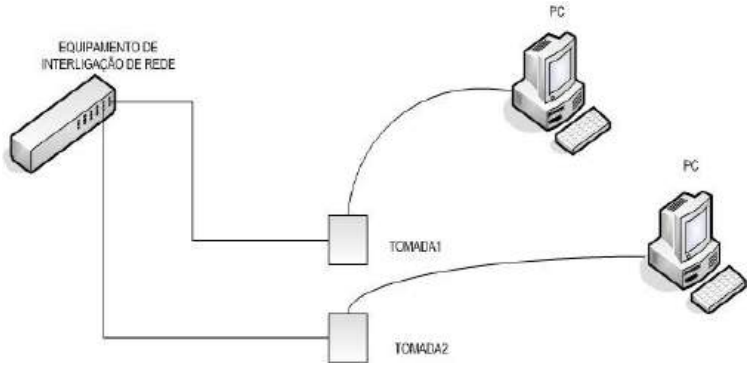

Figura 3.22 - Configuração de conexões com tomadas RJ-45

Pode-se também ligar dois computadores directamente (sem hub/switch), utilizando um cabo de par entrançado cruzado. Para tal, há que inverter os pares de transmissão e recepção numa das extremidades do cabo. A tabela 5 mostra como combinar os fios para construir um cabo cruzado.

Combinação dos fios		
Extremidade A		Extremidade B
1	------	**3**
2	------	**6**
3	------	**1**
4	------	**4**
5	------	**5**
6	------	**2**
7	------	**7**
8	------	**8**

Tabela 5 - Combinação de fios para cabo UTP cruzado.

3.8 Cabos de fibra óptica

Um cabo de fibra óptica transmite informação representada por impulsos de luz, em detrimento de sinais eléctricos utilizados pelos cabos de cobre. As três principais vantagens da fibra óptica em relação aos condutores de cobre são:

- Maior alcance.
- Maior velocidade.
- Imunidade a interferências electromagnéticas.

A figura 3.23 mostra a constituição interna de um cabo de fibra óptica. A fibra propriamente dita forma o **núcleo** que é fabricado utilizando um vidro especial com elevado grau de pureza. A maioria dos cabos de fibra óptica usados em redes possuem fibras com dimensões de 50 ou 63,5 microns [11].

[11] microns – unidade de medida representado pelo símbolo **µm** que equivale a 1/1000 milímetros.

O núcleo é rodeado por outra camada também de vidro. Na camada mais externa do cabo existe um protector tipo plástico.

Os cabos ópticos usados em redes de computadores são constituídos por vários pares de fibras.

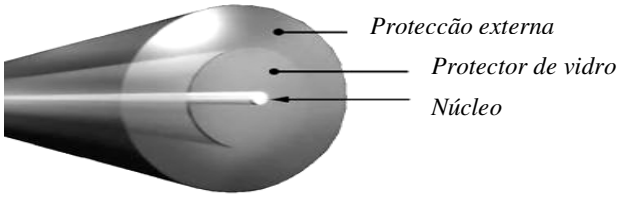

Figura 3.23 – Constituição interna de um cabo de fibra óptica

As características de propagação óptica de uma fibra dependem, essencialmente, das características e dimensões do seu núcleo, sendo este aspecto utilizado para agrupar as fibras ópticas em duas grandes famílias: monomodo e multimodo.

As fibras monomodo são usadas em telefonia e em aplicações que exigem longas linhas, com vários quilómetros.

As fibras multimodo são menos dispendiosas do que os monomodo. A dimensão do núcleo é de 50 ou 63,5 microns. O alcance da onda pode chegar até 2 km. Este tipo de fibra é aplicado em redes locais.

Os conectores para fibras ópticas são muito caros, assim como a mão-de-obra necessária para a montagem do cabo.

Para preparar um cabo óptico, é necessário frequentar um curso de especialização em montagem de cabos de fibras ópticas, que são ministrados, normalmente, pelos fabricantes dos cabos e conectores. A montagem dos conectores requer, além de um curso de especialização, instrumentos especiais como microscópios, ferramentas especiais para corte e polimento, medidores e outros aparelhos sofisticados.

Existem vários tipos de conectores para cabos de fibra óptica. Existem conectores do tipo SC (figura 3.24), ST, MTRJ entre outros. Muitos equipamentos de interligação de redes mais modernos, possuem conexões directas para cabos de fibras ópticas com esses tipos de conectores. Também se pode converter qualquer conexão de rede baseada em cabos de cobre

(ex: RJ-45 ou coaxial) para cabos ópticos, utilizando um dispositivo de conversão. Existem conversores entre RJ-45 e ST, RJ-45 e SC, RJ-45 e MTRJ, etc.

Figura 3.24 – Cabos com conectores SC.

Algumas placas de rede mais modernas, possuem conexão directa para cabos de fibras ópticas. A placa mostrada na figura 3.25 tem dois conectores tipo SC.

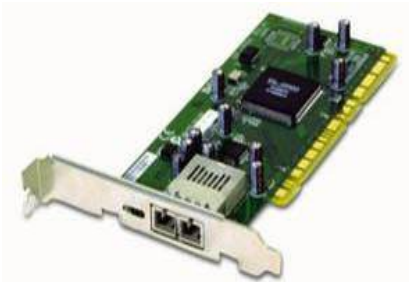

Figura 3.25 – Placa de rede com conectores para fibras

Devido ao seu elevado custo, os cabos de fibras ópticas são utilizados apenas quando é necessário atingir distâncias maiores, para operar com taxas de transmissão mais altas e em ambientes com muita interferência electromagnética.

Nas redes locais actuais, a maioria dos sistemas de cablagem estruturada possuem topologias em árvore (ou em estrela no caso de redes locais de pequenas dimensões), correspondendo cada um dos níveis da árvore a um dos níveis hierárquicos dos sistemas de cablagem.
Para cada topologia, recorre-se a um determinado tipo de cabo de rede, por isso, torna-se fundamental que o técnico que vai instalar ou dar manutenção numa rede, seja capaz de preparar esses cabos. Também pode-se recorrer às lojas que vendem cabo, mas supondo que a instituição onde se vai instalar a rede já tenha os componentes para preparação dos cabos, não seria coerente se o técnico recomendasse a compra do cabo, em vez de preparar com as suas própria mãos porque não sabe como fazê-lo.

4. TECNOLOGIAS DE REDES LOCAIS

As tecnologias de redes locais, em conjunto com os componentes de cablagem, definem a velocidade da rede.

Como foi referido no capítulo anterior, temos cabos de rede em pares entrançados que atingem os 100Mbps, mas que, com algumas tecnologias, podem chegar aos 1000Mbps, dependendo da tecnologia dos equipamentos a que estão conectados.

Neste capítulo vamos estudar e analisar as várias tecnologias disponíveis e dar maior grande ênfase às tecnologias de rede locais sem fios (WLAN – Wireless LAN)[12] que surgiram no mercado em grande força e que para muitos ainda é uma tecnologia um pouco desconhecida.

Nas redes locais, a tecnologia dominante é a **Ethernet**.

Além da Ethernet temos outras tecnologias, como sendo o **Token Ring** e **FDDI.**

4.1 Ethernet

A tecnologia Ethernet foi desenvolvida pela Xerox, Intel e Digital nos meados de 70, normalizada pelo IEEE[13] (Institute of Electrical and Electronics Enginers - norma 802.3) e pela ISO (International Organization for Standardization – ISO 8802-3).

Abrange 4 camadas do modelo OSI: Física, Enlace de dados, Rede e Transporte.

[12] Wireless é um termo em inglês que significa exactamente "sem fios".

[13] Associação profissional internacional para formação e normalização na área de redes informáticas.

Utiliza o CSMA/CD como método de base para controlo de acesso ao meio físico em todas as suas variantes, mas em variantes mais recentes foram feitas várias alterações para integrar a alta velocidade com a eficiência.

Normalmente, os padrões Ethernet são especificados por **X Base –Y,** em que **X** indica a taxa de transmissão em Mbps, **Base** significa que a transmissão é efectuada em banda de base[14] (Baseband) e **Y** um número ou letras que indicam o tipo ou o comprimento máximo do meio físico utilizado.

4.1.1 Ethernet a 10Mbps

Estas tecnologias permitem uma taxa de transmissão de 10Mbps, são elas:
10Base5, 10Base 2, 10BaseT e 10BaseFL.

A variante 10Base5 utiliza cabos coaxiais grossos (Thicknet), para formar uma topologia em Bus. O comprimento máximo do cabo é de 500m, sem utilizar nenhum dispositivo de regeneração do sinal.

A variante 10Base2 utiliza cabos coaxiais finos (Thinnet) também para formar uma topologia em Bus. O comprimento máximo do cabo é de 185m.

A variante 10BaseT utiliza cabos de pares entrançados e são utilizados, normalmente, nas topologias em estrela e árvore. O comprimento máximo do cabo é de 100m.

A variante 10BaseFL utiliza fibra óptica para conectar dois hosts a uma distância de 2Km.

4.1.2 Ethernet a 100Mbps ou Fast Ethernet

Permitem uma taxa de transmissão até 100Mbps, são elas: **100baseTX, 100BaseT4** e **100BaseFX**.

A variante 100BaseTX criado a par do desenvolvimento da tecnologia Fast Ethernet [15] utiliza cabos de pares entrançados para transmitir dados a 100Mbps.

A variante 100BaseT4 difere da 100BaseTX no tipo de cabo utilizado. Enquanto que 100BaseTX utiliza cabo UTP Cat.5 (apenas dois pares são utilizados na transmissão de dados

[14] Técnica de sinalização digital que utiliza toda a largura de banda do cabo para apenas um canal de dados. Outra técnica seria o broadband que é uma técnica de sinalização analógica que partilha a largura de banda por diferentes canais.

[15] Evolução da Ethernet para suportar taxas de transmissão a 100Mbps.

full duplex[16]) a variante 100BaseT4 utiliza cabo UTP Cat.3 (todos os pares são utilizados na transmissão dos dados em half duplex[17]). Destas duas variantes, o mais utilizado é a 100BaseTX. O comprimento dos cabos é de 100m.

A variante 100BaseFX utiliza cabos de fibra óptica para transmitir dados a 100Mbps a uma distância de até 2Km.

4.1.3 Ethernet a 1000Mbps ou Gigabit Ethernet

Permitem uma taxa de transmissão a 1000Mbps. Engloba as variantes **1000Base-SX, 1000BASE-LX** e **1000BASE-T**.

A variante 1000BASE-SX utiliza fibra óptica multimodo para transmitir dados a 1000Mbps. O comprimento máximo do cabo depende do tipo de fibra utilizado, variando de 220m a 550m.

A variante 1000BASE-LX pode utilizar fibra óptica monomodo ou multimodo para transmitir dados a 1000Mbps. Utilizando fibra multimodo, o comprimento máximo do cabo é de 550m. Utilizando o monomodo, o comprimento máximo é de 5Km.

A variante 1000Base-T utiliza cabo de pares entrançados para transmitir dados a 1000Mbps. O comprimento máximo do cabo é de 100m.

4.1.4 Ethernet a 10Gbps

Esta é a mais nova versão da Ethernet que permite uma taxa de transmissão até 10Gbps. Permite que a tecnologia Ethernet seja utilizada não só em redes locais, como também em redes alargadas a alta velocidade.

As principais variantes são: **10GBASE-SR, 10GBASE-SW, 10GBASE-LR, 10GBASE-LW, 10GBASE-ER, 10GBASE-EW** e **10GBASE-LX4.**

A tabela 6 apresenta um resumo das características de cada variante:

Variante	Tipo de cabo	Comprimento máximo
10GBASE-SR	Fibra óptica multimodo	300m
10GBASE-SW	Fibra óptica multimodo	300m
10GBASE-LR	Fibra óptica monomodo	10Km

[16] Transmissão de dados em dois sentidos simultaneamente num mesmo cabo.

[17] Transmissão de dados em apenas um sentido de cada vez num mesmo cabo.

10GBASE-LW	Fibra óptica monomodo	10km
10GBASE-ER	Fibra óptica monomodo	40Km
10GBASE-EW	Fibra óptica monomodo	40Km
10GBASE-LX4	Fibra óptica multimodo	300m
	Fibra óptica monomodo	10Km

Tabela 6 – Características das variantes Ethernet

Esta tecnologia foi pensada para redes ponto-a-ponto, o que significa que não suporta tecnologia cliente/servidor. Assim sendo, é aplicada particularmente na interligação de redes locais ou metropolitanas, ou seja, é uma tecnologia vocacionada para constituição de redes de *backbone*[18].

Ainda estão a ser realizadas testes e experiências com esta nova tecnologia no seio de uma associação de profissionais de rede, a 10GEA (10 Gigabit Ethernet Alliance).

4.2 Togen Ring

A tecnologia Token Ring, (IEEE 802.5 e ISSO 8802.5) ao contrário da Ethernet, não chegou a atingir grande implantação no mercado das redes locais. O custo de implementação é superior ao da tecnologia Ethernet.

Emprega uma topologia em anel, com controlo de acesso ao meio físico por passagem de testemunho. Suporta largura de banda até 100Mbps sobre cabos de cobre coaxial e pares entrançados.

O método de controlo por passagem de testemunho é simples. Mesmo que nenhum host pretenda transmitir dados, um pacote de controlo – o testemunho (token) – é enviado de um host para outro (isto é, cada host recebe o testemunho e repete-o de imediato para o próximo host). Quando um host pretende transmitir informação, tem que aguardar que o testemunho lhe seja enviado. Na posse do testemunho, poderá enviar um pacote de dados para o anel, que será repetido por todos os hosts. Quando o pacote chega ao host de destino, este deve copiá-lo para a sua memória e repeti-lo para o próximo host. O pacote circula pelo anel até chegar ao host que o inseriu, sendo retirado por este. Quando o host acaba de transmitir, passa o testemunho para o próximo host do anel.

[18] Backbone significa coluna vertebral em português, o que permite concluir que, em termos de redes informáticas, possibilita a interligação de vários sistemas de redes, fornecendo todos os recursos de transmissão a alta velocidade. É constituído por cabos e equipamentos de alta velocidade.

4.3 FDDI (Fiber Distributed Data Interface)

O FDDI é uma tecnologia também vocacionada para redes de **backbone**.

Funciona a 100Mbps com topologia em anel e método de controlo por passagem de testemunho. Suporta até 500 hosts, podendo atingir uma extensão de 100Km (em anel duplo). Foi desenvolvida para ser utilizada com fibra óptica, mas também pode ser utilizada com cabos de pares entrançados.

Com a configuração em anel duplo, um dos anéis é usado para transmissão/recepção e o outro é usado em caso de falha, para reconfiguração do anel. Esta configuração garante que, em caso de falha, os hosts ligados aos dois anéis ficarão sempre ligados ao anel reconfigurado, podendo transmitir e receber dados. Os hosts que estão ligados apenas ao anel principal, poderão não ser abrangidas pelo anel reconfigurado após a falha.

4.4 Redes Locais sem fios (WLANs - Wireless LANs)

As tecnologias de redes sem fios surgem em grande força no mercado de redes.

As redes locais sem fios fornecem todas as funcionalidades e benefícios das tecnologias de redes tradicionais, tais como Ethernet e Token Ring, sem as limitações inerentes à utilização dos cabos.

As redes sem fios redefinem a forma de ver as redes locais. Neste caso, a ligação entre hosts não implica, obrigatoriamente, a utilização de cabos e conectores. Numa infraestrutura, utilizando as tecnologias de redes sem fios, não é necessário passar cabos pela parede e essa infraestrutura pode ser alterada e transferida facilmente, de acordo com as necessidades pontuais da organização.

4.4.1 Benefícios de uma rede local sem fios

A norma IEEE 802.11, referente às redes locais sem fios, proporciona os seguintes benefícios:

- Para conectar redes em dois edifícios separados por um obstáculo físico ou legal, pode ser utilizada tanto uma ligação fornecida por um operador de telecomunicações, como criar uma ligação ponto-a-ponto sem fios utilizando tecnologias de redes sem fios. A não recorrência aos serviços das operadoras de telecomunicações pode proporcionar uma significante redução de custos para a organização.
- Pode-se utilizar as redes locais sem fios para criar uma rede temporária que vai funcionar por um determinado período de tempo. Por exemplo, no caso das

convenções ou exposições comerciais, o tipo de rede mais viável seria o sem fios, em vez de passar cabos que terão que ser removidos após o término dos eventos.

- As redes sem fios também são utilizadas em edifícios ou locais considerados como patrimónios históricos, onde são proibidas realização de qualquer tipo de obras. Nesse locais não há como instalar os cabos, pois, seria necessário modificar algumas estruturas do edifício, o que é desaconselhável.
- Para os utilizadores domésticos, as redes sem fios também podem ser muito atractivas, principalmente para aqueles que pretendem conectar os vários computadores que têm em casa sem ter que perfurar as paredes e passar cabos.
- O profissional que realiza várias deslocações e cujo computador de trabalho primário é um portátil, pode mudar de um lugar para outro e continuar sempre conectado à rede. Isto permite-o deslocar para vários lugares abrangidos pela rede e continuar a ter acesso aos dados.
- Mesmo que não exista nenhuma infraestrutura de rede sem fios, os utilizadores com computadores portáteis podem formar a sua própria rede sem fios para comunicar e partilhar dados entre si.
- Permite um rápido acesso à Internet nas redes públicas.

4.4.2 Métodos de transmissão

Assim como o padrão Ethernet 802.3 utiliza diferentes métodos de transmissão sobre cabos de cobre e ópticos, o padrão WLAN 802.11 também se serve de diferentes métodos de transmissão na interface ar. Tais métodos incluem **raios infravermelhos (infrared)**, a transmissão em **bandas estreitas (narrowband)** e transmissão com **espalhamento de espectro (spread spectrum)**. São especificados dois métodos de transmissão em Spread Spectrum na banda dos 2.4GHZ que não necessitam de licença para serem utilizadas: **FHSS (Frequency-hopping spread spectrum) e DSSS (Direct sequence spread spectrum)**.

FHSS é limitada por uma taxa de transferência de 2Mbps e é recomendada apenas para algumas aplicações específicas. Para a maioria das aplicações de redes sem fios, recomenda-se a DSSS.

4.4.3 Formas de comunicação

Nas redes locais sem fios, existem duas formas básicas de comunicação: infraestrutura e ad-hoc (independente).

- No modo infraestrututa que é o mais popular, os terminais sem fios (dispositivos com placas de rede sem fios, tais como um computador portátil ou um assistente digital pessoal - PDA) estabelecem ligação com os pontos de acesso sem fios. Estes pontos de acesso funcionam como pontes entre terminais sem fios e o sistema de distribuição de redes existente. Os pontos de acesso (Wireless Access Point) são, normalmente, interligados por um backbone. À medida que se afasta do ponto de acesso e o sinal de um ponto de acesso sem fios enfraquece, pode-se estabelecer ligação com um novo ponto de acesso. Por exemplo, numa grande empresa, o dispositivo sem fios pode ligar-se a vários pontos de acesso diferentes à medida que se vai deslocando em diferentes pisos de um edifício ou em diferentes edifícios num centro. Como resultado, mantém-se um acesso contínuo a recursos de rede.

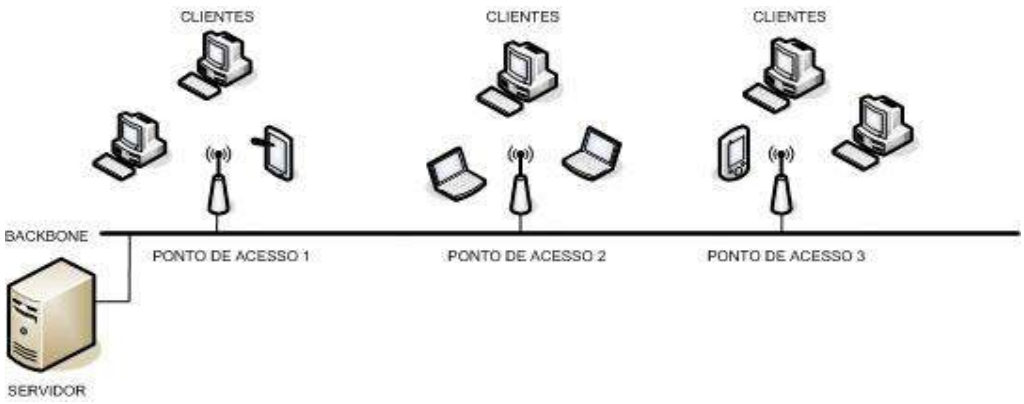

Figura 4.1 - Rede sem fios no modo infraestrutura

- No modo ad-hoc, os terminais sem fios interligam-se directamente, sem utilizar pontos de acesso sem fios. Por exemplo, se estiver numa reunião com colegas, os vários dispositivos sem fios podem ser interligados e formar uma rede temporária.

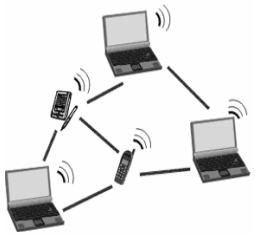

Figura 4.2- Rede sem fios no modo ad-hoc

Para se instalar uma rede sem fios, precisar-se-á no mínimo, de um adaptador de rede sem fios para cada PC ou portátil da rede. Para os PCs pode-se utilizar um modelo interno baseado em PCI[19] ou um adaptador de USB. Para os portáteis, a melhor opção seria um modelo de PC Card ou um mini-PCI Card, caso seja suportado pelo sistema.

Para além das placas de rede, necessitar-se-á também de um router ou um ponto de acesso. Um router sem fios combina as funções de router de banda larga e ponto de acesso sem fios. Provavelmente a rede ficará mais bem servida com um router sem fios, já que, normalmente, custa o mesmo que um ponto de acesso e fornece tudo o que se necessita num só dispositivo.

Figura 4.3 – Placa de rede sem fios (para PC)

Figura 4.4 - Router sem fios

No Windows XP, a configuração de um host para fazer parte de uma rede sem fios é simples. Basta seguir as instruções e fornecer os dados solicitados pelo assistente de configuração de rede sem fios que pode ser iniciado a partir da janela "Os meus locais na rede". Mas antes da configuração da rede, convém conhecer os padrões de segurança em redes sem fios, pois, serão solicitados durante a configuração.

4.4.4 Padrões de redes sem fios

O IEEE definiu 4 padrões de redes sem fios cujo as designações e características são resumidamente apresentadas na tabela abaixo:

Padrão	Taxa de transferência	Gama de frequências	Utilização
802.11	2Mbps	2,4 a 2,5 GHz	Não é muito utilizado
802.11b	11Mbps	2,4 a 2,5 GHz	Muito utilizado
802.11a	54Mbps	5,725 a 5,875GHz	Não é muito utilizado devido ao

[19] Baía de expansão que se encontra na placa-mãe de um PC, onde se pode instalar placas adicionais.

			custo elevado da licença.
802.11g	54Mbps	2,4 a 2,5 GHz	Está a ganhar popularidade

Tabela 7 – Padrões de redes sem fios.

4.4.5 Segurança em redes sem fios

Apesar dos benefícios proporcionados pelas tecnologias de redes locais sem fios, estas introduzem ameaças de segurança que não existem nas redes locais com cabos. Ao contrário dos sistemas de cablagem fechados de uma rede Ethernet que podem ser fisicamente seguras, os frames das redes sem fios são transmitidas como ondas de rádio que se propagam na interface ar, podendo ser captada por qualquer outro dispositivo wireless. Assim sendo, qualquer computador abrangido pela rede sem fios, pode enviar e receber as frames. Caso não haja mecanismos de protecção, utilizadores mal-intencionados podem usar a rede para ter acesso à informações confidenciais, atacar um computador da rede ou outro computador na Internet.

Para proteger a rede, deve-se configurar algumas opções de autenticação e encriptação.

A autenticação requer que os computadores forneçam uma conta de acesso válida (por exemplo, nome de utilizador e palavra-passe) ou provem que foram configurados com uma chave de autenticação antes de lhes serem permitidos transmitir frames na rede sem fios. A autenticação evita que um host se conecte a uma rede sem fios antes de realizar uma autenticação com sucesso. A encriptação requer que todas as frames da rede sejam encriptadas (codificadas), de forma a serem interpretadas apenas pelo utilizador que os recebe.

São suportados os seguintes padrões de segurança:

- IEEE 802.11
- IEEE 802.1X
- Wi-Fi Protected Access (WPA)
- Wi-Fi Protected Access 2 (WPA2)

IEEE 802.11

O padrão original IEEE 802.11 definiu o método de autenticação de chaves aberto e partilhado para a autenticação e WEP (Wired Equivalent Privacy) para a encriptação. O WEP pode usar chaves de encriptação de 40bits ou 104 bits. Contudo, este padrão de segurança provou ser relativamente fraco em ambientes públicos e privados com muito tráfego. Devido

à sua susceptibilidade a ataques e ao aparecimento de novos padrões de segurança, não teve sucesso.

IEEE 802.1X

A autenticação neste padrão foi desenhada para WLANs de tamanho médio e grande que contêm uma infraestrutura de autenticação que consiste em servidores de autenticação e base de dados de contas como o Active Directory[20].

O IEEE 802.1X evita que um host se conecte a uma rede sem fios antes de realizar uma autenticação com sucesso. Para tal utiliza o EAP (Extensible Authentication Protocol – Protocolo de Autenticação Extensível).

A autenticação numa rede sem fios pode basear-se em diferentes métodos de autenticação tais como os que utilizam nome de utilizadores e palavra-passe ou certificados digitais.

WPA

Embora o padrão 802.1X supere a fraca autenticação do padrão original 802.11, este não constitui uma solução para a fragilidade do WEP. Enquanto o IEEE 802.11i era finalizada, a aliança Wi-Fi (organização constituída por comerciantes de equipamentos), criou um padrão conhecido como WPA (Wi-Fi Protected Access). Este padrão substitui o WEP com um método de encriptação muito mais sofisticado conhecido como TKIP (Temporal Key Integrity Protocol). O WPA permite também o uso opcional do AES (Advanced Encryption Standard – Padrão Avançado de Encriptação) para encriptação.

O WPA pode ser encontrado em dois modos diferentes:

- **WPA-Enterprise (Empresas)** que utiliza a autenticação do padrão 802.1X e é desenhado para infraestruturas de médio e grande porte.
- **WPA-Personal (Pessoal)** que utiliza uma chave pré-partilhada (PSK) para a autenticação e é desenhada para infraestrutura de redes.

WPA2

O objectivo da certificação do WPA2 é o suporte a funções adicionais do padrão IEEE 802.11i que ainda não está incluído nos produtos que suportam WPA. Por exemplo, WPA2 requer suporte tanto para encriptação TKIP como para encriptação AES.

O WPA2 pode também ser encontrado em dois modos diferentes:

[20] Sistema de gestão de recursos do servidor utilizado nos sistemas Windows 2000/2003 Server.

- **WPA2-Enterprise** que utiliza autenticação do padrão 802.1X e é desenhada para infraestruturas de médio e grande porte.
- **WPA2-Personal** que utiliza PSK para autenticação e é desenhada para infraestruturas de redes**.**

O Windows XP suporta os seguintes padrões de segurança para redes locais sem fios:

- 802.11 com WEP.
- 802.1X.
- WPA (Windows XP SP1[21] com actualizações adicionais ou Windows XP com SP2).
- WPA2 (Windows XP SP2 com actualizações adicionais).

Pode-se encontrar mais informações sobre padrões de segurança em redes locais sem fios no Windows XP no site da Microsoft (**http://www.microsoft.com**).

A seguir vão algumas sugestões de segurança para redes de diferentes tamanhos.

Redes de médio e grande porte

Para redes desse tipo que usam a autenticação 802.1X, devemos utilizar uma das seguintes tecnologias de segurança:

- WPA-Enterprise (Empresas) com autenticação 802.1X.
- WPA2-Enterprise (Empresas) com autenticação 802.1X.

É importante lembrar que para criar uma rede baseada em WPA, todos os componentes e equipamentos devem suportar esta tecnologia, o que deve ser garantido antes de se efectuar a requisição desses equipamentos.

Redes de pequeno porte (escritório/casa)

Para redes desse tipo que não usam a autenticação 802.1X, devemos utilizar o modo de infraestrutura e uma das seguintes tecnologias de segurança:

- WPA-Personal (pessoal) com autenticação PSK.
- WPA2-Personal (pessoal) com autenticação PSK.

[21] SP = Service pack – são pacotes e actualizações que a Microsoft disponibiliza periodicamente no seu site da Internet com o objectivo de tornar os sistemas mais seguros e também para fazer com que estes suportem as tecnologias mais recentes.

5. EQUIPAMENTOS DE INTERLIGAÇÃO DE REDES

Para que uma rede de computadores possa funcionar é necessário que existam, além da estrutura de cablagem, dispositivos cuja função é controlar a comunicação entre os diversos componentes da rede.

Este capítulo é dedicado ao estudo de cada um dos principais equipamentos utilizados na interligação de redes locais.

5.1 Repetidores

Os repetidores são dispositivos de hardware utilizados para a conexão de dois ou mais segmentos de uma rede local. Actuam na camada física do modelo OSI, exercendo a única função de regeneração dos sinais eléctricos entre dois segmentos de rede da mesma tecnologia. A figura 5.1 ilustra dois segmentos de redes com topologias em estrela, interligados por um repetidor.

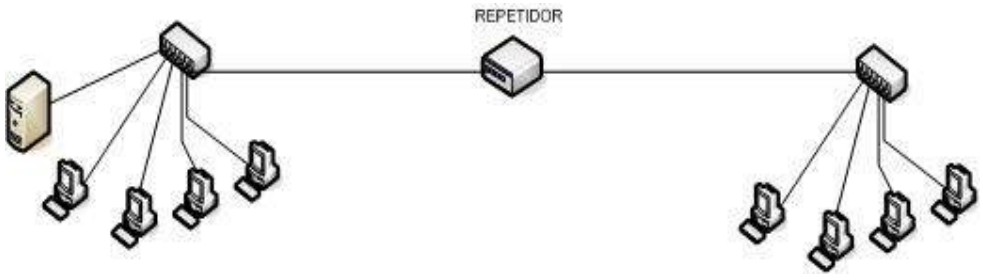

Figura 5.1 – Rede com Repetidor

Supondo que a distância entre os dois segmentos ultrapassa 150 metros e que o cabo utilizado é de pares entrançados, o repetidor regenera os sinais provenientes dos segmentos, pois, esse tipo de cabo está limitado a uma distância de 100 metros. Assim sendo, o repetidor vai garantir a integridade dos sinais e a sua passagem para outro segmento.

O número máximo de repetidores entre os segmentos de rede depende da tecnologia utilizada. No caso da Ethernet, o número máximo de repetidores é quatro, ou seja, um sinal na rede não pode atravessar mais do que quatro repetidores.

5.2 Pontes (bridges)

Os bridges são equipamentos que possuem a capacidade de segmentar uma rede local em várias sub-redes, diminuindo assim o fluxo de dados na rede. Actuam nas camadas físicas e de enlace de dados. Quando um host envia um sinal, este é recebido apenas pelas estações que estão no segmento do bridge. Também só permite a passagem do sinal se este for destinado para um host que está fora do segmento onde se encontra o host que enviou o sinal. Assim, a principal função dos bridges é filtrar pacotes entre segmentos de LAN's.

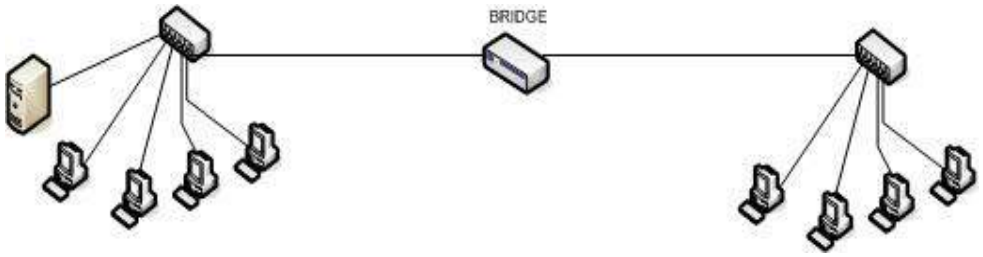

Figura 5.2 – Rede com Bridge (ponte)

Os bridges se diferem dos repetidores porque manipulam pacotes ao invés de sinais eléctricos. A vantagem em relação aos repetidores é que não retransmitem ruídos, erros e consequentemente, não retransmitem frames mal formadas. Uma frame deve estar completamente válida para ser retransmitida por uma bridge.

5.3 Hubs

Os Hubs actuam na camada física do modelo OSI e podem ser passivos ou activos. Um hub passivo recebe as informações por uma das suas portas e transmite-as para o host de destino por outra porta. Não é ligado à corrente eléctrica e não possui capacidade de processamento de sinais.

Um Hub activo recebe dados através de uma das suas portas e, neste caso, funciona como um repetidor multiportas, regenerando o sinal antes de transmiti-lo para o destino através de outra porta. Ao contrário do hub passivo, é alimentado pela corrente eléctrica.

Cada host da rede está conectado ao Hub através de um cabo de pares entrançados, independentemente dos outros hosts, o que garante maior flexibilidade e facilidade de gestão da rede.

Pode-se ainda, interligar dois hubs entre si através de uma porta designada "UpLink", aumentando assim o número de hosts na rede. A conexão de vários hubs entre si vai originar uma topologia em árvore (várias topologias em estrelas).

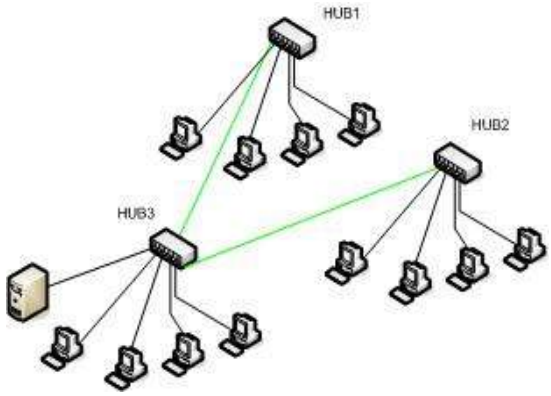

Figura 5.3 – Interligação de vários Hubs

5.4 Switches (comutadores)

Os switches, também designados de Hubs inteligentes e que também podem ser considerados como bridges multiportas, são dispositivos que verificam automaticamente o endereço físico de cada host conectado às suas portas. A semelhança com o Hubs reside no facto de possuírem várias portas com conectores RJ-45 fêmea às quais se conectam cabos com conectores RJ-45 macho. A semelhança com os bridges reside no facto de isolarem o tráfego dos segmentos. Quando um pacote é enviado para a rede, o switch verifica o endereço físico antes de enviar o pacote para o host de destino.

Ao contrário dos hubs, os switches não espalham os sinais pela rede (broadcast). Transmitem dados apenas para o host de destino, evitando assim que outros hosts da rede tenham acesso a esses dados. Dessa forma, obtém-se largura de banda dedicada para cada porta do switch, o que não acontece com os hubs. Por exemplo, um switch com largura de banda de 100Mbps, tem essa largura de banda disponível em cada uma das suas portas, podendo todos os hosts transmitir dados a 100Mbps. Assim sendo, pode-se concluir que, com os switches, obtém-se

uma rede com maior largura de banda, com menos colisões e consequentemente uma rede mais rápida.

Como acontece com os hubs, os switches também podem ser interligados entre si através de uma porta UpLink, formando topologia em árvore.

A figura 5.4 mostra um switch Fast Ethernet (100Mbps) com cabos UTP conectados às suas portas.

Figura 5.4 – Switch (comutador) com cabos UTP conectados

5.5 Routers (encaminhadores)

Os routers são dispositivos que actuam nas camadas Física, Ligação de dados e Rede do modelo OSI. Podem ser utilizados para interligarem vários segmentos de uma LAN ou várias LANs distintas. A principal função de um router é o encaminhamento dos pacotes de dados entre LANs ou segmentos de LANs.

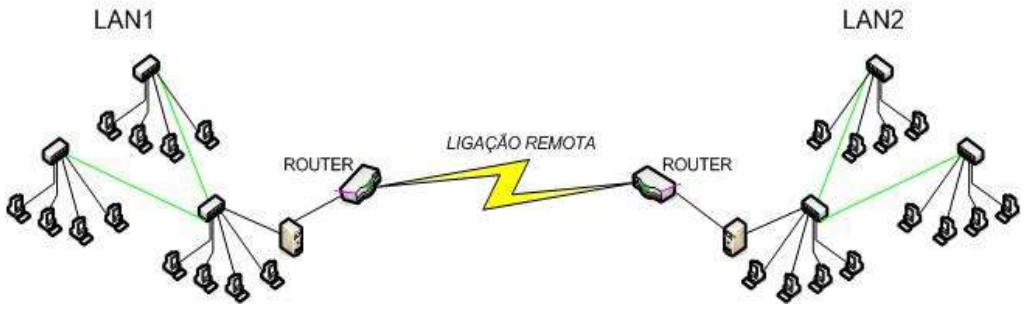

Figura 5.5 – Ligação de duas LANs remotas através de routers

O encaminhamento dos pacotes é realizado com base nos endereços IP dos cabeçalhos dos pacotes. Por isso, os routers actuam também na camada de Rede que inclui o protocolo IP.

Os routers possuem várias opções de interface com LAN’s e WAN's. Por exemplo, podem ter opções de interfaces LAN, portas UTP, FDDI ou AUI, através das quais é feita a conexão com a rede local. As interfaces WAN's servem para realizar a conexão com dispositivos de

transmissão remota (modems), seguindo os padrões de protocolos V-35, RS-449, RS-232 entre outros.

Para configurar um router, a primeira informação que se deve ter é o seu endereço IP. Tendo o endereço, pode-se aceder ao seu programa de configuração através de um navegador como o Internet Explorer. Por exemplo, para se abrir o programa de configuração de um router cujo endereço é 10.0.0.1, deve-se digitar o endereço na barra de endereço do navegador como mostra a figura 5.6.

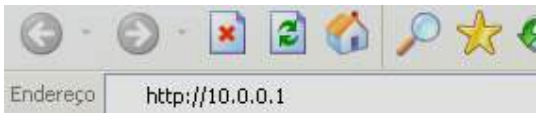

Figura 5.6 – Activando programa de configuração de um router

Para mais informações, deve-se sempre consultar o manual que acompanha o router.

Para encaminhar os pacotes, os routers podem ser configurados de forma estática ou dinâmica, utilizando nesse caso, protocolos de encaminhamento como o RIP (Routing Information Protocol) e OSPF (Open Shortest Path First).

Todos os computadores da rede possuem uma tabela de encaminhamento local (routing table) que contém as equivalências entre endereços de rede e endereços de gateways para outras redes ou segmentos de redes. Esta tabela pode ser consultada com o comando **route print** a partir da linha de comandos do MS-DOS. A figura 5.7 mostra o resultado da execução do referido comando.

Figura 5.7 – Resultado da execução do comando route print

A configuração estática passa por inserir os endereços de gateway manualmente, na tabela de encaminhamento de todos os PCs da rede. Isso pode ser feito com o comando **route –p add**. Por exemplo, **route –p add 169.253.0.0 mask 255.255.0.0 169.254.11.165,** significa dizer ao PC em causa que todos os pacotes de dados destinados à rede **169.253.0.0** cuja máscara de sub-rede é **255.255.0.0**, devem ser enviados para o gateway cujo endereço é **169.254.11.165**. Assim, será inserida uma entrada na tabela de encaminhamento do PC. O **–p** significa

persistente. Sem esse comando, a informação de encaminhamento inserida só estaria disponível depois de reiniciar o computador.

Para eliminar uma entrada na tabela local, pode-se utilizar o comando **route delete**. Por exemplo, **route delete 169.253.0.0 mask 255.255.0.0**, elimina a informação de encaminhamento para a rede **169.253.0.0** cuja máscara de sub-rede é **255.255.0.0**.

A configuração estática só é praticável em redes de pequenas dimensões com dois segmentos no máximo.

Para redes com três ou mais segmentos, recomenda-se a utilização da configuração dinâmica utilizando, por exemplo, o protocolo RIP que é mais simples e de mais fácil configuração do que o OSPF.

Os protocolos de configuração dinâmica trocam informações contidas nas suas tabelas de encaminhamento automaticamente, dispensando qualquer tipo de entrada manual nas tabelas locais dos PCs da rede.

5.6 Servidores

Na prática qualquer computador rápido pode ser um servidor de rede, desde que possua um sistema servidor como, por exemplo, o Windows 2000 Server da Microsoft. Pode-se então, utilizar um PC Pentium IV com boa velocidade e configurá-lo como servidor da nossa rede local. Porém, por norma o servidor de rede deve ser o computador com maior recursos e potência do que os restantes computadores da rede, já que vai suportar vários serviços solicitados pelos PCs clientes.

Normalmente, um servidor (físico) possui vários discos rígidos, processadores e também unidades para realização de cópias de segurança dos dados.

Nos dias de hoje um bom servidor deverá oferecer suporte físico e lógico às recentes tecnologias de gestão de recursos de hardware e de rede.

Um servidor com, por exemplo, o sistema Windows 2000 Server, pode ser configurado para fornecer vários serviços. Pode ser configurado para funcionar como servidor DHCP, DNS, servidor de impressão, servidor Web etc.

Nas grandes redes, são utilizados servidores específicos para cada serviço, para evitar o congestionamento da rede e do próprio servidor devido à grande quantidade de solicitações por parte dos PCs clientes.

Por tudo que já se viu até aqui, pode-se concluir que os equipamentos de interligação de redes são indispensáveis. Alguns desses equipamentos já caíram ou tendem a cair em desuso, sendo

substituídos por tecnologias recentes com maior capacidade e fiabilidade. Por exemplo, o hub tende a ser substituído pelo switch que oferece maior velocidade e controlo do meio físico de transmissão, embora possa constituir uma topologia em estrela ou árvore tal como o hub.
Outro factor muito importante é a baixa de preços dos produtos que induzem quase sempre à substituição de tecnologias mais antigas pelas mais recentes.

6. GESTÃO E SEGURANÇA DE REDE

Após a instalação da rede, há que a gerir para que tudo funcione como foi planejado e com a maior eficiência possível.

Neste capítulo serão abordados alguns aspectos básicos referentes à gestão de redes locais.

A gestão de uma rede engloba vários aspectos como documentação, segurança e manutenção da rede.

6.1 Documentação

A documentação de uma rede é muito importante e crucial para o bom funcionamento e manutenção da rede. Inclui os seguintes componentes:

- Diagramas que indicam os caminhos por onde passam os cabos.
- Tipos de cabos utilizados em cada secção.
- Tamanho de cada cabo.
- Identificação de cada cabo com etiquetas.
- Detalhes da configuração de hardware e software dos servidores e dos PCs clientes (sistema operativo, discos, memória, placa de rede, etc.).

A documentação de cada um desses componentes facilita o trabalho do técnico durante a manutenção, principalmente na detecção de falhas.

6.2 Segurança

A segurança de uma rede tem como meta principal, proteger a rede de acessos indevidos ou mal-intencionados, cujo objectivo é impedir o bom funcionamento dessa rede.

Envolve tanto segurança lógica (políticas de segurança, definição de passwords e utilização de firewall), como segurança física (acesso físico aos compartimentos onde estão os servidores da rede e protecção contra variações da tensão eléctrica).

6.2.1 Cópias de segurança

Uma outra operação que pode ser incluída nas medidas de segurança é a cópia de segurança[22] dos dados mais importantes da rede. Tem como principal objectivo a cópia de dados importantes para a organização que não podem ser perdidos, para unidades de discos amovíveis. Assim, caso haja avarias, por exemplo, no servidor, os dados poderão ser recuperados a partir das suas cópias nos discos amovíveis. Se os dados recuperados são actualizados ou não, vai depender do período de tempo entre cada backup. Para que os dados recuperados sejam os mais recentes possíveis, convém realizar cópias de segurança em pequenos períodos de tempo.

O sistema operativos possuem ferramentas de backup próprias, mas pode-se também utilizar ferramentas de terceiros.

6.2.2 Ataques à rede

Um aspecto muito importante a ter em conta quando se trata de segurança de rede, tem a ver com ataques à rede com o objectivo de roubar ou danificar dados confidenciais. Portanto, muito perigoso caso haja num PC da rede, documentos confidenciais que não devem ser vistos por outras pessoas.

Estes ataques normalmente são realizados por pessoas com bom conhecimento de redes ou por curiosos que tentam testar as suas capacidades técnicas, sendo popularmente designados por hackers. No entanto convém salientar que os hackers, normalmente não invadem redes com más-intenções. Os que invadem redes para proveito próprio são designados de crackers. Seja qual for, não é desejável que pessoas não autorizadas tenham acesso à rede.

Existem vários tipos de ataques e a maioria deles aproveitam falhas (bugs) nos sistemas ou outros softwares. Por exemplo, quando um determinado programa está a ser executado, este

[22] Backup em inglês.

pode deixar uma porta aberta. Pessoas com conhecimento dessa falha podem utilizar essa porta para ter acesso não autorizado à nossa rede.

Para evitar esses ataques, é imprescindível manter o sistema e outros programas com as últimas actualizações disponíveis no site da Internet dos respectivos fabricantes. Por exemplo, se utiliza sistemas da Microsoft, pode actualizá-los a partir do site do mesmo.

Também é indispensável a utilização de um firewall que bloqueia as portas, impedindo o acesso por parte de pessoas não autorizadas. Basicamente, um firewall funciona como um porteiro que só dá acesso a dados provenientes de outros hosts, se estes forem solicitados pelo host em que está instalado. Caso algum outro host tente utilizar uma porta sem autorização, o firewall entra em acção, bloqueando a porta imediatamente. Existem vários firewalls no mercado, mas gostaria aqui de realçar o **ZoneAlarm** da **Zone Labs** que funciona bem em pequenas redes. O Windows XP SP2 já vem com um bom firewall integrado por isso, caso já não o tenha feito, actualize o seu sistema para o SP2. Esse firewall pode ser activado ou desactivado a partir da central de segurança do sistema.

6.2.3 Programas malignos

Os programas malignos (geralmente designados por vírus) são programas que podem destruir os dados dos nossos computadores ou afectar a performance da nossa rede.

Existem vários tipos desses programas: **vírus padrão**, **worms (vermes)** e **Trojans (Cavalos-de-Tróia)**.

O vírus padrão é um programa que infecta os ficheiros do nosso computador (normalmente ficheiros executáveis[23]), inserindo uma cópia sua dentro desses ficheiros. A cópia do vírus é executada logo que o ficheiro infectado é carregado para a memória, permitindo assim a contaminação de novos ficheiros.

Um worm é um programa que se propaga automaticamente pelo computador, criando uma cópia de si mesmo em todos os discos conectados ao computador. Também atacam sistemas, explorando eventuais falhas ou portas abertas. Às vezes bloqueia o computador infectado, impedindo o seu funcionamento.

Um Cavalo-de-Tróia ou Trojan é um programa destrutivo que é apresentado como sendo um programa útil como jogos e utilitários, mas que realiza operações malignas quando se executa esse programa.

Algumas medidas podem ser tomadas para evitar a contaminação por estes programas:

[23] Esses ficheiros têm extensão .exe

- Evitar fazer download de programas da Internet sem ter certeza de que provêm de fontes fidedignas.
- Antes de abrir uma disquete ou pen drive, passar um antivírus para certificar-se de que estes não contêm vírus.
- Alertar e sensibilizar os utilizadores da rede sobre essas ameaças e respectivas medidas de segurança.
- Manter o sistema e os programas antivírus sempre actualizados.
- Utilizar um firewall.

Outras ameaças recentes são os **Spywares** (programas espiões). Estes programas captam dados pessoais nos nossos computadores e enviam-nos pela Internet para outras pessoas (normalmente ladrões virtuais). Existem ferramentas específicas para remoção desses programas e podem ser encontrados facilmente na Internet. Uma ferramenta eficaz para a remoção de Spywares é o **Spybot-Search and Destroy**.

6.2.4 Manutenção da rede

A manutenção da rede é uma operação que garante o funcionamento de cada um dos equipamentos e componentes intervenientes nas comunicações a serem realizadas na rede. Inclui testes de conectividade e manutenções correctivas.

Depois de instalar todos os componentes de cablagem e interligar todos os equipamentos, resta testar se as conexões estabelecidas funcionam realmente.

Numa rede Microsoft, existem vários comandos de teste de conectividade, alguns deles descritos a seguir:

ping - envia pacotes ICMP para verificar a conexão com o host de destino especificado pelo endereço IP e pode ser executado a partir da linha de comandos do MSDOS .

Ex.: **ping 10.73.24.1**

Se tudo estiver bem configurado, deverá receber uma resposta como o da figura 6.1.

```
A enviar para 10.73.24.1 com 32 bytes de dados:

Resposta de 10.73.24.1: bytes=32 tempo=2ms TTL=255
Resposta de 10.73.24.1: bytes=32 tempo=2ms TTL=255
Resposta de 10.73.24.1: bytes=32 tempo=2ms TTL=255
Resposta de 10.73.24.1: bytes=32 tempo=2ms TTL=255
```

Figura 6.1 – Resultado da execução do comando ping com sucesso

Caso contrário, significa que algo não está bem configurado. Deverá então tentar descobrir a causa do problema que pode ser um cabo desligado ou mal conectado, problemas com a configuração do TCP/IP ou ainda problema de hardware.

tracert – mostra o caminho que um pacote de dados atravessa para chegar ao host de destino especificado pelo endereço IP e pode ser executado a partir da linha de comandos do MSDOS.
Ex.: **tracert 192.123.46.88**

netstat – apresenta estatísticas sobre protocolos e conexões TCP/IP actuais e pode ser executado a partir da linha de comandos do MSDOS.
Ex.: **netstat –a**

Ipconfig – mostra a configuração de endereços IP e pode ser executado a partir da linha de comandos do MSDOS. Pode ser utilizado com outros comandos.
Ex.: **ipconfig/all** – mostra informações sobre a configuração IP da(s) placa(s) de rede do computador.
Ipconfig /release [nome_da_placa_de_rede] – liberta o endereço IP da placa de rede especificada, desactivando o TCP/IP.
Ipconfig /renew [nome_da_placa_de_rede] – renova o endereço IP da placa de rede especificada. No Windows XP podemos realizar essas operações com o comando **Reparar** no menu de contexto da ligação de área local.

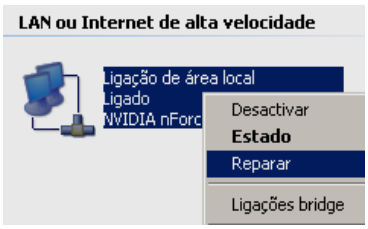

Figura 6.2 – Reparação de uma ligação de rede (mesmo efeito que Ipconfig /release e Ipconfig /renew)

7. CONCLUSÃO

Para concluir, podemos afirmar que a execução deste trabalho atingiu o objectivo inicialmente proposto, que era de criar um manual técnico para montagem de redes locais de pequena dimensão.

Foram abordados aspectos de natureza teórica para assimilar os conceitos envolvidos na criação de redes locais, desde aspectos referentes a protocolos de comunicação essenciais para perceber a fiabilidade da rede, aspectos referentes à topologia da rede, de modo a dimensionar e optimizar a estrutura física da rede. Foi dada uma especial atenção ao TCP/IP, como protocolo padrão de comunicação de redes de dados, evidenciando a respectiva pilha protocolar, os serviços disponibilizados e as suas principais características. Foram abordadas questões relativas ao endereçamento IP, classes de endereços e endereços públicos e privados.

De seguida foi feita uma referência às tecnologias de redes locais, diferenciando cada tecnologia e elucidando em que situação cada tecnologia poderá ser aplicada. Especial atenção foi dada a Ethernet, por ser a tecnologia predominante em redes locais.

Estes conceitos teóricos são fundamentais para perceber como funcionam as redes locais e para permitir aos técnicos identificar em tempo útil os problemas que possam afectar a rede e a sua consequente resolução.

De seguida foi feita uma abordagem, essencialmente prática sobre a montagem da estrutura física, ou seja, como fazer os cabos, como fazer os pontos de acesso à rede e como diferenciar os vários tipos de cabos.

Os equipamentos de ligação de redes foram analisados numa perspectiva essencialmente prática, realçando a forma como funcionam e como devem ser utilizados, de modo a facilitar a compreensão e a utilização desses equipamentos na montagem de uma rede local. A configuração da rede, a partilha da ligação à Internet, a partilha de recursos de rede e a resolução de problemas de acesso à rede também foram aspectos analisados em detalhe.
Por último foram abordados questões relacionadas com a segurança, manutenção e gestão da rede. Os cuidados necessários a ter com acessos indevidos, a integridade das informações, a ameaça dos vírus e outros códigos malignos que poderão corromper ou mesmo destruir informações, são aspectos que necessitam de uma atenção especial, pois, podem pôr em causa todo o trabalho feito na montagem e instalação de uma rede local.
Com este relatório pretende-se que os leitores tenham acesso a um manual técnico para montagem e manutenção de redes locais, tendo sido utilizada uma abordagem prática e uma linguagem técnica de fácil compreensão.
Para aprofundar mais os conhecimentos e capacidades em termos de instalação, manutenção e gestão de redes, recomenda-se que se faça um estudo mais detalhado de alguns aspectos, a destacar, a pilha protocolar TCP/IP, aprofundando noções relativas a endereçamento IP, recuperação de erros e controlo de fluxo, a segurança das redes locais, tendo em especial atenção questões relativas a autenticação e encriptação, firewall's, tradução de endereços de rede e segurança na Internet.

BIBLIOGRAFIA

CISCO PRESS, *Cisco Networking Academy Program, Second-Year Companion Guide*, 2ª Edição, Indianopolis 2001.

COLECÇÃO SCHAUM, *Teorias e problemas de rede de computadores*, Editora Bookman; trad. de Walter da Cunha Borelli, Porto Alegre, Bookman 2003.

LOUREIRO, Paulo, *TCP/IP em Redes Microsoft para profissionais*, 5ª Edição Actualizada, Editora FCA, Lisboa Maio 2003.

MONTEIRO, Edmundo, BOAVIDA, Fernando, *Engenharia de redes informáticas*, 4ª Edição, Editora FCA, Agosto 2000.

ODOM, Wendell, *Cisco CCNA Exam #640-607 - Certification Guide*, Publicção da Cisco Press, Indianopolis 2002.

SOUSA, Lidenberg Barros de, *Redes de computadores – Dados, voz e imagens*, 6ªedição, Editora Érica, São Paulo 1999.

TERESO, Cláudio, *Redes Locais em Windows 98 & 95 – Curso Completo*, 2ª Edição, Editora FCA, Fevereiro 1999.

As tecnologias de rede Wireless. [Em linha]. Disponível em http://www.rnp.br/newsgen/9805/wireless.html. [Consultado em 18/04/06].

Categories of twisted pair cabling systems. [Em linha]. Disponível em http://searchdatacenter.techtarget.com/sDefinition/0,,sid80_gci211752,00.html. [Consultado em 24/04/06].

Ethernet (IEEE 802.3) Resources. [Em linha]. Disponível em http://www.ethermanage.com/ethernet/ethernet.html. [Consultado em 18/04/06].

ICANN FAQs. [Em linha]. Disponível em http://www.icann.org/faq/. [Consultado em 16/03/06].

IEEE 802.11 LAN/MAN Wireless LANS. [Em linha]. Disponível em http://standards.ieee.org/getieee802/802.11.html. [Consultado em 29/03/06].

IEEE 802.3 LAN/MAN CSMA/CD Access Method. [Em linha]. Disponível em http://standards.ieee.org/getieee802/802.3.html. [Consultado em 29/03/06].

Internet Protocol V4 Address Space. [Em linha]. Disponível em http://www.iana.org/assignments/ipv4-address-space. [Consultado em 27/05/06].

IP Address Services. [Em linha]. Disponível em http://www.iana.org/ipaddress/ip-addresses.htm. [Consultado em 27/05/06].

Local Area Network. [Em linha]. Disponível em http://www.techfest.com/networking/lan.htm. [Consultado em 24/04/06].

Placas de redes, hubs e cabeamento. [Em linha]. Disponível em http://www.laercio.com.br/site2/artigos/SOFT/soft-008/soft-008.htm. [Consultado em 23/11/05].

Port Numbers. [Em linha]. Disponível em http://www.iana.org/assignments/port-numbers. [Consultado em 27/05/06].

Security Center. [Em linha]. Disponível em http://www.microsoft.com/technet/Security/default.mspx. [Consultado em 11/05/06].
UNH-IOL KnowledgeBase. [Em linha]. Disponível em http://www.iol.unh.edu/training. [Consultado em 18/04/06].

Wireless LAN Technologies and Windows XP. [Em linha]. Disponível em http://www.microsoft.com/technet/prodtechnol/winxppro/evaluate/wrlsxp.mspx. [Consultado em 11/05/06].

LISTA DE ACRÓNIMOS

AES - Advanced Encryption Standard

API - Application Programming Interface

ARP - Address Resolution Protocol

ATM - Assincronous Transfer Mode

AUI - Attachment Unit Interface

BNC - British Naval Connector

CSMA/CD - Carrier Sense Multiple Access/Colision Detect

DHCP - Dynamic Host Control Protocol

DLL - Dynamic Link Lybrary

DNS - Domain Name System

DSSS - Direct Sequence Spread Spectrum

EAP - Extensible Autentication Protocol

FDDI - Fiber Distributed Data Interface

FHSS - Frequency-Hopping Spread Spectrum

FTP - File Transfer Protocol

HTTP - Hyper Text Transfer Protocol

ICMP - Internet Control Message Protocol

IEEE - Institute of Electrical and Electronics Engineers

IGMP - Internet Group Message Protocol

IP - Internet Protocol

ISO - Internacional Standard Organization

LAN - Local Area Network

LED - Light Emittin Diode

MAC - Media Acces Control

MAU - Media Access Unit

MS-DOS - Micrsoft Disk Operating System

NDIS - Network Driver Interface Specification

OSI - Open System Interconnection

OSPF - Open Shortest Path First

PC - Personal Computer

RARP - Reverse Address Resolution Protocol

RIP - Routing Information Protocol

STP - Shielded Twisted pair

TCP - Transmission Control Protocol

TCP/IP - Transmission Control Protocol/Internet Protocol

TKIP - Temporal Key Integrity Protocol

UDP - User Datagram Protocol

USB - Universal Serial Bus

UTP - Unshielded Twisted pair

WAN - Wide Area Network

WEP - Wired Equivalent Privacy

WINS - Windows Internet Name Service

WLAN - Wireless Local Area Network