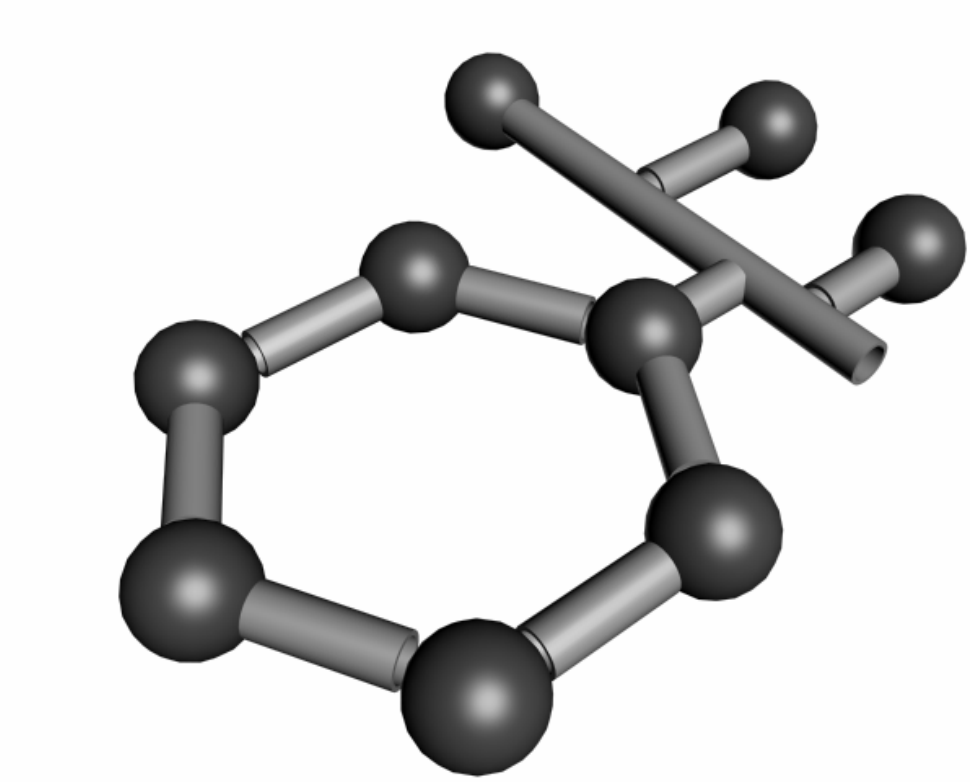
Universidade de Aveiro

Departamento de Electrónica e Telecomunicações

Instalação e Administração de uma Rede Local de Comunicação de Dados



Rui Pedro Sanches de Castro Lopes

Aveiro, Abril de 1998

Universidade de Aveiro

Departamento de Electrónica e Telecomunicações

Instalação e Administração de uma Rede Local de Comunicação de Dados

Dissertação de Mestrado

Rui Pedro Sanches de Castro Lopes

Aveiro, Abril de 1998

RESUMO

A dependência crescente da sociedade em relação às redes de comunicação de dados implica uma adaptação permanente a novas e mais eficazes soluções tecnológicas. A optimização de algumas características tais como fiabilidade, velocidade de transmissão, integração de serviços, segurança e extensibilidade são actualmente motivo de investigação e desenvolvimento.

Nesta dissertação identificam-se, numa primeira etapa, as diferentes tecnologias de comunicação disponíveis, suas vantagens e desvantagens. Esta recolha de informação pretende dar ao leitor uma perspectiva alargada sobre potenciais soluções para o projecto e instalação de uma rede local.

A construção de infra-estruturas de comunicação deve contemplar ainda, para além dos mecanismo de comunicação, os sistemas de gestão. Neste trabalho procuram-se identificar e sintetizar os modelos associados a esta área (IETF/SNMP, OSI/CMIP, TMN). A influência da Internet faz-se sentir, inclusivamente, no âmbito da gestão de redes, pelo que foi realizado um levantamento de tecnologia que permite realizar a gestão com ferramentas da Internet (JMAPI, WBEM, CORBA)

Como corolário deste estudo desenvolveu-se um sistema de gestão baseado em SNMP e Java. Procurou-se neste trabalho dar prioritariamente resposta a requisitos como modularidade, utilização distribuída, interface de utilizador e tratamento automático da informação de gestão.

ABSTRACT

The increasing social dependency in data communication networks maintains the continuous learning of the state of the art and of more efficient technological solutions. The optimisation of some characteristics such as reliability, transmission speed, service integration, security and extensibility constitutes issues for further development.

In this dissertation, the available communication infrastructure technologies had been identified, its advantages and its disadvantages. This information intends to be an useful guide on potential solutions for the design and installation of a local computer network.

Besides communications mechanisms, the development of communication infrastructures should include network management solutions. This work identifies some management models (IETF/SNMP, OSI/CMIP, TMN). The Internet influence in network management scenario is also investigated. A survey of the emerging technology was carried out aiming at the management on the basis of Internet tools (JMAPI, WBEM, CORBA).

In this study, an SNMP/Java based system is developed. The system aims are to provide a modular and distributed architecture, a user-friendly interface and automatic management information processing tools.

AGRADECIMENTOS

Durante o desenvolvimento desta dissertação, muitas foram as sugestões de colegas e amigos. Cabe-me aqui deixar expresso o meu reconhecimento a todos aqueles que directa ou indirectamente contribuíram para a realização deste trabalho.

Ao Prof. Doutor José Luís Oliveira, meu orientador, não só pelo apoio científico e pedagógico, mas, acima de tudo, pela amizade e empenhamento que revelou durante o desenvolvimento deste trabalho.

À minha família agradeço o auxílio, apoio e encorajamento que me prestaram, imprescindíveis para a conclusão desta dissertação.

Ao Instituto de Engenharia de Sistemas e Computadores, em particular, ao Grupo de Telemática, o qual facultou todos os meios necessários para o desenvolvimento do presente trabalho.

Ao Prof. Doutor Joaquim Arnaldo Martins, Prof. Doutor Joaquim Sousa Pinto e Prof. Doutor Nelson Rocha pelos valiosos conselhos que nunca me negaram e pela disponibilidade que sempre revelaram.

Por último, agradeço a muitos outros amigos, que deixo no anonimato, por não querer correr o risco de esquecer algum.

A todos, um sincero obrigado.

ÍNDICE

LISTA DE FIGURAS

LISTA DE TABELAS

1 MOTIVAÇÕES E ENQUADRAMENTO

1.1 Introdução

Desde tempos longínquos que o ser humano sentiu necessidade de comunicar. As formas utilizadas têm vindo a beneficiar de evoluções constantes, mercê da disponibilização de novas técnicas e do aparecimento de novas necessidades, resultantes do aumento das zonas geográficas a cobrir e do número de utilizadores a servir.

A evolução das técnicas de comunicação motivou a adopção de novas formas de comunicar e de trabalhar. Os meios de comunicação actuais permitem, por exemplo, a transferência de documentos entre secções ou departamentos de uma instituição, a redacção de artigos por autores dispersos geograficamente, a execução remota de aplicações, a impressão remota de documentos ou a consulta a bases de dados remotas.

O aparecimento de canais de comunicação mais eficientes, conjugado com a disponibilização de novos equipamentos terminais e com o desenvolvimento de aplicações mais complexas principalmente em termos de funcionalidades e interacção com os utilizadores tem contribuído para uma dependência crescente dos utilizadores em relação a este tipo de redes.

Em redes já instaladas torna-se frequente a actualização de equipamento e/ou tecnologia, pelo que é importante considerar a integração do sistema existente com a nova solução. Cada projecto deve prever os avanços tecnológicos e apresentar opções que não sejam incompatíveis com soluções que possam surgir a curto ou a médio prazo. Para que esta previsão seja o mais correcta possível é necessário um bom conhecimento dos conceitos e da tecnologia mais utilizada em redes locais de comunicação de dados, acompanhar a investigação e extrapolar para uma possível solução futura.

O objectivo da instalação de uma rede local é oferecer um serviço de comunicação de dados que visa um conjunto de utilizadores. O serviço deve apresentar um nível óptimo ou quase óptimo de qualidade pois caso contrário corre-se o risco da rede não ser utilizada e gerar grande frustração junto de utilizadores e administradores. O esforço de instalação bem como os gastos efectuados serão perdidos e a rede tornar-se-á inviável. É essencial dotar a rede de mecanismos e/ou ferramentas que permitam monitorar e corrigir situações anómalas que possam surgir durante a operação, de forma a aumentar o grau de confiança que o serviço apresenta face aos seus utilizadores.

A proposta desta dissertação é a apresentação e a discussão das principais tecnologias de rede, das suas vantagens e lacunas e propor configurações que permitam tirar o melhor partido do equipamento existente. A instalação de uma rede não termina na instalação de equipamento, pelo que a dissertação continua com a apresentação de várias arquitecturas de gestão "clássicas" e a sua relação com arquitecturas mais recentes baseadas em tecnologia Internet, com a finalidade de propor um conjunto de soluções e ferramentas que permitam melhorar o desempenho destes modelos.

1.2 Redes Locais de Comunicação de Dados

A instalação de uma Rede Local de Comunicação de Dados (LAN – *Local Area Network*) é precedida por uma fase de planeamento, onde se faz o levantamento das necessidades, se admitem soluções e se calculam os custos. O estudo da configuração, da tecnologia e do equipamento tem como base o estudo realizado e constitui uma das etapas do planeamento.

Os componentes activos tais como repetidores, comutadores e encaminhadores são normalmente instalados em armários (armários de telecomunicações). A estrutura de cabos expande-se dos armários de telecomunicações até às estações de trabalho, havendo zonas em que o número de cabos passados atinge as várias dezenas. Em edifícios sem calha técnica ou com calha técnica pouco acessível (coberta com tecto falso, por exemplo) pode ser necessário restruturar algumas partes do edifício, o que vem agravar o custo total em termos de recursos humanos e de despesas com construção civil.

O comprimento total de cabos que constituem o sistema pode atingir dezenas ou mesmo centenas de quilómetros, pelo que, apesar de o preço unitário não ser muito elevado, o custo total constitui uma parte considerável do orçamento final.

Por outro lado, existem várias soluções aplicáveis de acordo com a necessidade e com o orçamento disponível. Cada uma apresenta características que a torna mais eficiente em determinadas configurações, pelo que é necessário estar ciente do tipo de configurações, tecnologia e equipamento existente de forma a realizar as melhores opções de acordo com a situação.

O capítulo 2 tem como objectivo apresentar a tecnologia, componentes e configurações mais utilizados actualmente. Este será o ponto de partida para a instalação de uma rede local de comunicação de dados.

1.3 Redes de Alta Velocidade

A crescente dependência dos utilizadores de computadores face às redes de comunicação de dados, bem como o desenvolvimento de novas aplicações suscitam a necessidade de maiores velocidades de transferência de informação.

A procura de soluções deste tipo é geralmente efectuada com o objectivo de melhorar o desempenho de sistemas já instalados. Neste contexto o conhecimento detalhado desta nova tecnologia ajuda a atingir um compromisso razoável entre o orçamento disponível e as necessidade de curto, médio e longo prazo.

Actualmente, existe um conjunto de soluções alternativas, neste domínio, que justifica um estudo acerca da tecnologia, equipamento e características de cada uma. O levantamento qualitativo e quantitativo, dos esforços de investigação na área das redes locais, permite gerar conclusões acerca do tipo de solução mais adequada relativamente a um determinado projecto.

De entre as diversas tecnologias capazes de oferecer taxas de 100 ou mais milhões de bits por segundo (Mbps), a *Fast Ethernet* tem-se tornado uma escolha bastante atractiva. Este facto deve-se ao facto de a *Fast Ethernet* apresentar-se como uma evolução directa da tecnologia mais usada no mundo – a Ethernet. A próxima vaga anunciada, de que existem já produtos disponíveis no mercado, é a *Gigabit Ethernet*, evolução directa da *Fast Ethernet* como esta é da Ethernet.

Por outro lado, a tecnologia não se resume a soluções baseadas em Ethernet e várias soluções apresentam-se como suas concorrentes. Como exemplo pode-se referir o ATM, 100VG – AnyLAN, HIPPI ou *Fibre Channel*. Estas apresentam características que permitem tirar proveito de algumas falhas da Ethernet de modo a serem viáveis em termos de mercado.

No capítulo 3 é feito um estudo comparativo entre as várias soluções, divididas em dois grupos: soluções baseadas em Ethernet e soluções não Ethernet.

1.4 Arquitecturas de Gestão

A diversidade de opções tecnológicas para construir uma rede local de dados, abriu caminho ao aumento de complexidade das tarefas de gestão, que vinham sendo efectuadas de um modo mais ou menos empírico e desorganizado. A proliferação de diversas soluções de rede (como Ethernet, *Token-ring*, FDDI, ATM, entre outras), diversos sistemas (Windows 95/NT, Unix, MacOS) e diversos modelos protocolares (TCP/IP, NetBEUI, IPX/SPX, entre outros) traduz-se numa dificuldade acrescida das tarefas de gestão.

As anomalias podem resultar de múltiplos factores tais com erros de sistema, envelhecimento de materiais ou factores humanos associados a uma utilização deficiente. Este tipo de problemas são imprevisíveis pelo que é necessário monitorar continuamente a operação da rede para que se possam detectar. A necessidade incluir sistemas de gestão é criada pela importância financeira de maximizar o tempo útil de operação de uma rede.

A gestão de uma rede inclui as fases de inicialização, em que é efectuada a configuração necessária para que esta deve ficar operacional, monitorização modificação de parâmetros de funcionamento. Durante a operação devem ser identificadas, isoladas e resolvidas eventuais anomalias. A própria expansão da rede deve ser acompanhada por monitorização com vista a optimizar o desempenho para a situação.

No sentido de proceder à normalização de uma arquitectura genérica de gestão de redes, alguns organismos internacionais têm apresentado modelos e arquitecturas de gestão. A ISO (*International Standards Organisation*) desenvolveu, a partir da década de setenta, um grande esforço na tentativa de apresentar uma arquitectura de referência para redes de comunicação de dados. Deste trabalho resultou o modelo OSI (*Open Systems Interconnection*) ao qual foram posteriormente acrescentadas especificações para regulamentar os mecanismos de gestão e troca de informação de gestão.

Apesar de todo este trabalho, os atrasos consecutivos e a complexidade dos documentos gerados foram factores que possibilitaram o aparecimento de outras soluções. Foi o caso do modelo de gestão Internet, mais conhecido por modelo de gestão SNMP (*Simple Network Management Protocol*). As normas da arquitectura SNMP foram sendo aprovadas, ao contrário do OSI, de acordo com a sua aceitação e desenvolvimento. Actualmente, esta constitui a solução mais utilizada neste mercado

No domínio das telecomunicações surge uma arquitectura de gestão baseada no modelo de gestão OSI, proposta e desenvolvida pelo ITU-T (*International Telecommunications Union – Telecommunication Standardisation Sector*). Esta arquitectura – TMN (*Telecommunications Management Network*) – apesar de ser

baseada num modelo pouco aceite para redes locais de dados, apresenta-se como a escolha preferencial no mercado das telecomunicações.

No capítulo 4 serão dicutidas em maior detalha estas três arquitecturas.

1.5 Gestão Baseada em WWW

A WWW (*World Wide Web*) constitui a "janela" mais popular da Internet, no sentido em que apresenta uma interface gráfica baseada no conceito de hipermédia. No início dos anos noventa, Tim Berners-Lee, enquanto trabalhava no CERN, desenvolveu o primeiro cliente WWW, o primeiro servidor WWW e definiu normas como URL (*Uniform Resource Locator*), HTML (*Hypertext Markup Language*) e HTTP (*Hypertext Transport Protocol*). Um ano depois aparecia o NCSA Mosaic, o *browser* mais popular da altura. Como resultado, foi fundada a empresa Mosaic Communications Corp., mais tarde Netscape, que depressa controlou 70% do mercado dos *browsers*. A Microsoft, apercebendo-se da oportunidade que surgia, lançou um *browser* próprio, o Internet Explorer.

Todos os *browsers* apresentam uma interface gráfica definida pela linguagem HTML. A interface tem o mesmo aspecto independentemente do *browser* e da plataforma. Esta característica ajudou a popularizar a WWW sobrepondo-se actualmente à própria Internet.

A independência de plataforma e a simplicidade da interface são características que tornam desejável a integração dos modelos de gestão com o WWW. Existem várias formas de o conseguir, passando pelo desenvolvimento de aplicações de gestão em linguagens interpretadas como a Java, utilização de CGI (*Common Gateway Interface*) associada a um servidor WWW ou desenvolvimento de aplicações utilizando ferramentas proprietárias como a JMAPI (*Java Management API*) ou WBEM (*Web-Based Enterprise Management*).

O capítulo 5 faz uma apresentação de tecnologia que permite integrar soluções de gestão de redes com a Internet.

1.6 Gestão de Uma Rede Local de Comunicação de Dados

As aplicações de gestão disponíveis no mercado requerem, muitas vezes, plataformas poderosas e não se encontram ao alcance do orçamento de pequenas e médias empresas. Apesar dos vários modelos, o nível de automação nestes sistemas de gestão de redes é baixo ou praticamente nulo, cabendo ao utilizador realizar de forma manual toda e qualquer alteração ou configuração.

O grau de complexidade das aplicações e dos sistemas está em crescimento contínuo. Num breve período de tempo, o gestor será incapaz de absorver por si só o grande volume de informação de gestão disponível. O primeiro passo em direcção à gestão automática passa pela definição de tarefas que possam ser executadas de forma calendarizada, facilitando a realização de operações repetitivas. O passo seguinte será o desenvolvimento de sistemas de gestão inteligentes baseados numa camada de abstracção de informação, capazes de tomar decisões sem intervenção do utilizador.

Em 1997, no Departamento de Electrónica e Telecomunicações da Universidade de Aveiro, foi iniciado o desenvolvimento de um sistema de gestão de redes baseado no modelo de gestão SNMP e ligado à WWW pela linguagem Java, que visa construir uma camada de abstracção de dados sobre a informação de gestão. Posteriormente, a

camada de abstracção servirá como base para o desenvolvimento de ferramentas de decisão automática.

Presentemente o sistema reúne já ferramentas de detecção de máquinas e agentes, ferramentas de visualização de topologia e ferramentas de consulta de informação (*MIB browser*). Encontra-se em desenvolvimento um conjunto de assistentes para a definição de tarefas e respectiva calendarização que vão constituir a camada de abstracção de informação.

O capítulo 6 faz a apresentação do sistema e dá indicações do trabalho futuro de modo a complementar o sistema com ferramentas de gestão automática.

2 REDES LOCAIS DE COMUNICAÇÃO DE DADOS

2.1 Introdução

A evolução das redes de comunicação de dados acompanha, em estreita relação, os avanços verificados ao nível dos sistemas. Desde o desenvolvimento de sistemas UNIX, operados a partir de terminais, passando por modelos como o de cliente/servidor e, posteriormente, por conceitos como o de *Network Computer*, as necessidades de comunicação mantêm-se. Do ponto de vista do utilizador, estas assentam essencialmente na partilha de ficheiros, de recursos e de aplicações. A troca de informação pode ser realizada por métodos convencionais como por exemplo papel ou discos amovíveis, mas a deslocação de material implica o dispêndio de efectivos inerentes ao transporte e o tempo necessariamente gasto. Tal como o telefone evita a deslocação dos intervenientes na conversação, as redes de comunicação de dados permitem a troca de informação sem a necessidade de transporte de material.

Num tal cenário, as redes de comunicação tomam, uma importância crescente, que se manifesta na quantidade de soluções existentes. É vulgar hoje em dia a coexistência de diversos tipos de técnicas de distribuição (topologias), equipamentos de ligação, sistemas terminais (servidores, estações de trabalho, impressoras, etc.) e serviços (WWW, ftp, etc.). Esta diversidade abriu caminho para um aumento de complexidade das tarefas de gestão.

As redes de comunicação encontram-se, geralmente, classificadas de acordo com a sua extensão geográfica. A classificação é feita segundo três categorias:

- LAN (*Local Area Network*) – as redes locais são redes limitadas a um edifício ou conjunto de edifícios próximos. Localizados numa área restrita, o equipamento e sistemas utilizados são geralmente privados. As curtas distâncias que separam os intervenientes tornam possível a utilização de velocidades de transmissão elevadas e de uma multiplicidade de protocolos. A configuração e segurança da rede é geralmente feita ao nível dos sistemas.
- MAN (*Metropolitan Area Network*) – as redes metropolitanas estendem-se por dezenas ou mesmo centenas de quilómetros. Geralmente cobrem uma cidade ou um *campus* e são tipicamente propriedade de uma empresa operadora de telecomunicações de dados. As redes metropolitanas interligam, normalmente, sistemas geograficamente dispersos, pelo que é comum o suporte nativo de vários protocolos de comunicação. A velocidade de comunicação, algumas vezes inferior ao das LAN, é ainda relativamente elevada, dependendo do suporte físico e da tecnologia adoptada.
- WAN (*Wide Area Network*) – em termos de cobertura geográfica, as redes alargadas estendem-se por centenas ou milhares de quilómetros. A sua dimensão e a multiplicidade de suportes físicos que utiliza tornam este tipo de redes dependentes de diversas empresas operadoras de telecomunicações. Por razões económicas, a utilização de canais de comunicação em redes WAN depende de uma activação prévia que se prolonga por um período bem definido, com um mínimo de duração.

Os processos envolvidos na troca de informação assumem a sua forma mais simples quando o número de intervenientes se reduz a dois. Neste caso, a rede de comunicação consiste numa ligação directa entre as duas entidades. A interligação de estações raras vezes se reduz a uma simples ligação física entre dois pontos. Normalmente há necessidade de equipamento extra que regenere, distribua ou encaminhe, de forma expedita, o sinal de comunicação.

A distribuição de estações pode assumir diversas formas, denominadas topologias. Cada configuração define equipamento de extensão e interligação com características próprias.

2.2 Topologias

As redes locais de comunicação de dados são caracterizadas por distâncias relativamente reduzidas a separar o equipamento terminal. Por outro lado, a sua reduzida dimensão torna dispensáveis algoritmos de encaminhamento complexos, o que simplifica a conexão e desconexão de equipamento terminal.

A estratégia de distribuição de ligações é condicionada por uma série de factores, tais como o custo, a fiabilidade, a expansibilidade e a facilidade de manutenção. As mais comuns são as topologias em Estrela, Anel, Árvore e Linear (*Bus*) [Halsall92, Beauchamp88, Tanenbaum96]. Cada topologia possui vantagens e desvantagens intrínsecas. É possível realizar combinações de configurações básicas, numa tentativa de anular inconvenientes e introduzir novas vantagens.

2.2.1 Estrela

A topologia em Estrela caracteriza-se por possuir um ou mais pontos de ligação (nós) centrais, responsáveis por transmitir a informação para os vários ramos (Figura 2.1).

Cada estação (DTE – *Data Terminal Equipment*) está ligada ao nó central (com função de repetidor) através de duas ligações unidireccionais, uma para transmissão e outra para recepção.

Uma transmissão efectuada por qualquer estação dá entrada no nó central. Este recebe o sinal e coloca-o em todas as portas de saída. Deste modo, apesar de as ligações representarem uma estrela, qualquer transmissão é recebida por todas as estações e não é possível que duas estações ocupem o meio em simultâneo salvo os casos em que são usados comutadores. O nó pode ser activo (com regeneração do sinal) ou passivo (sem regeneração).

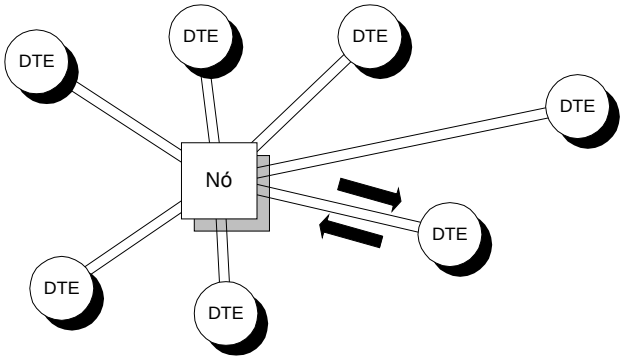


Figura 2.1 – Topologia em Estrela.

Aspectos positivos:

- Uma falha na rede pode ser facilmente detectada e isolada.
- O custo de cada conexão adicional é baixo desde que não estejam ocupadas todas as portas do nó.

Aspectos negativos:

- A comunicação está dependente do nó central, pelo que, se a unidade central falhar, a rede fica totalmente inoperante.

2.2.2 Anel

A configuração em anel é constituída por uma sequência de repetidores que formam um circuito fechado. O meio de transmissão é unidireccional, com ligações ponto a ponto (Figura 2.2):

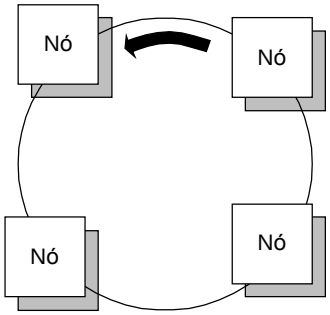


Figura 2.2 – Topologia em Anel.

A mensagem flui de nó em nó, sendo repetido por estes para a estação seguinte. Cada nó é relativamente simples, uma vez que não é necessário qualquer tipo de encaminhamento.

Aspectos positivos:

- A sua concepção é simples, o que minimiza problemas associados ao projecto.
- O repetidor existente em cada nó fornece uma certa compatibilidade entre os diferentes meios de transmissão (cobre, fibra).

- O anel pode ser duplo, de forma a diminuir a possibilidade de problemas de vulnerabilidade do cabo ou de falhas dos repetidores.

Aspectos negativos:

- A localização de uma avaria implica o acesso a todos os repetidores.
- Em termos de segurança, o anel não é muito fiável. Qualquer estação pode ver informação não dirigida a ele, por modificação da lógica de reconhecimento de endereços.

2.2.3 Árvore

A topologia em árvore baseia-se num conjunto de concentradores, distribuídos de forma semelhante aos nós dos ramos de uma árvore e que repetem a informação da raiz para os seus diversos ramos. Uma transmissão proveniente de qualquer estação percorre os concentradores até à raiz, sendo repetida em caminho inverso até ser recebida por cada uma das estações (Figura 2.3).

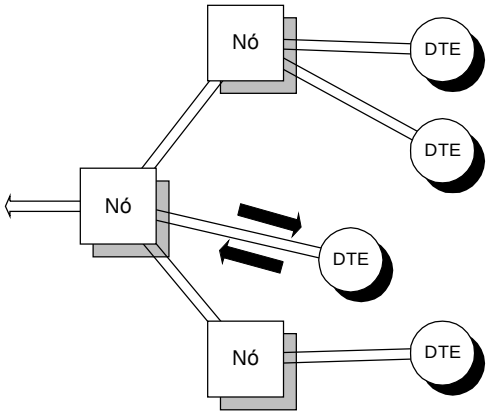


Figura 2.3 – Topologia em Árvore.

Os concentradores podem ser dotados de alguma inteligência na identificação do ramo destinatário. Com este processo reduz-se o tráfego total, canalizando-se a informação unicamente para os ramos a que é destinada.

A árvore pode ser vista como uma estrela com vários níveis hierárquicos.

Aspectos positivos:

- A falha de um nó não implica a total inoperabilidade da rede.
- Uma falha na rede pode ser facilmente detectada e isolada.

Aspectos negativos:

- A extensão da rede pode implicar a aquisição de novos nós, aumentado o investimento necessário.
- Se não existirem portas livres, a ligação de novas estações à rede pode não ser simples.

2.2.4 Linear

A topologia linear, também conhecida por ***Bus***, segue uma configuração multiponto, ou seja, o meio de comunicação pode ser partilhado por três ou mais estações. Quando qualquer estação transmite o meio é totalmente ocupado pela comunicação pelo que todas as outras estações têm de aguardar que este seja libertado (Figura 2.4).

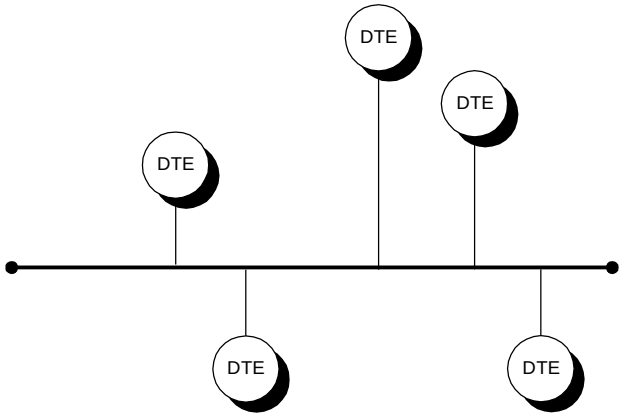


Figura 2.4 – Topologia Linear.

A mensagem emitida é difundida a partir do nó origem em ambas as direcções até às extremidades do cabo. Os nós receptores devem reconhecer se a mensagem lhe é destinada e de onde provém, de modo a poder responder sem equívocos.

O meio é partilhado por todas as estações, pelo que podem surgir alguns problemas de acesso ao meio. Um deles passa pela determinação do instante em que o meio se encontra livre para transmissão. A solução para este problema encontra-se na utilização de técnicas de acesso como o CSMA/CD (*Carrier Sense Multiple Access with Collision Detection*), *Token Bus* ou escalonamento temporal (*polling*) por parte de uma estação de controlo.

Aspectos positivos:

- A ligação de novas estações à rede pode implicar realizar extensões ao meio de transmissão o que pode resultar numa tarefa complexa.
- Baixo custo de instalação.

Aspectos negativos:

- A avaria de um nó pode tornar todo o segmento ou todo o espaço partilhado inoperacional.
- A detecção e isolamento de avarias é mais difícil e demorada do que, por exemplo, na estrela (arquitectura centralizada).
- Do ponto de vista de segurança é vulnerável a uma utilização mal intencionada por parte de um utilizador.
- Sempre que ocorram cortes ou danos no cabo todos os sistemas do segmento respectivo são afectados.

2.3 Equipamento de Extensão e Interligação

A comunicação entre entidades processa-se seguindo um determinado conjunto de operações:

- O emissor constrói a mensagem e adapta-a ao meio físico de transmissão.
- A mensagem é transportada pelo meio de transmissão.
- Eventualmente, a mensagem chega ao receptor.
- O receptor interpreta a mensagem.

O meio de transmissão, por condicionantes físicas, não se apresenta adequado ao transporte de todo o tipo de sinal. A atmosfera, por exemplo, propaga mais facilmente um sinal sonoro do que um sinal eléctrico.

Assumindo que o sinal se encontra numa forma adequada ao meio, a comunicação só tem significado se for recebida pela entidade destinatária e esta só receberá a mensagem se existir um mecanismo de entrega eficiente.

Em resumo, o sucesso da comunicação depende do sucesso da transmissão do sinal, da correcta identificação dos intervenientes e da correcta recepção da mensagem. As operações executadas numa comunicação podem ser divididas em três níveis (Figura 2.5).

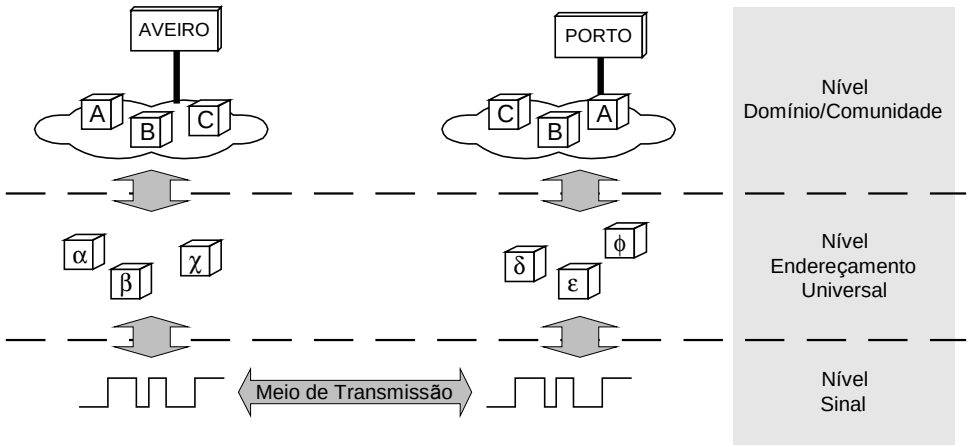


Figura 2.5 – Modelo geral de comunicação.

O nível de endereçamento universal define um mecanismo de identificação único. Um identificador único é atribuído a cada uma das entidades que partilha o mesmo universo de endereçamento, da mesma forma que as impressões digitais identificam cada ser humano inequivocamente. Este identificador permite que a mensagem seja inequivocamente recebida.

O endereçamento de comunidade/domínio define a localização dos interlocutores, assim como a sua identificação na respectiva comunidade. Por exemplo, uma pessoa chamada Manuel que habita no Porto não é o mesmo Manuel que habita em Aveiro.

A mensagem enviada contém o identificador de comunidade, identificador de entidade e a informação transmitida sob a forma de um sinal. Este constitui o nível

inferior do modelo de comunicação. O sinal percorre o meio de transmissão até, eventualmente, ser recebido pela entidade adequada.

Uma arquitectura de comunicação de dados segue um modelo semelhante ao anteriormente apresentado. Com a finalidade de dividir responsabilidades, o modelo de comunicação é dividido em camadas e definidos protocolos específicos para cada camada.

2.3.1 Repetidores e Concentradores (*HUBs*)

Tal como em qualquer sistema físico, um sistema de transmissão de dados dissipa energia. Um sinal eléctrico, tal como as ondas sonoras, sofre atenuação ao longo do canal que percorre. Depois de percorrida uma certa distância, o sinal transmitido torna-se mesmo imperceptível (Figura 2.6 – a). Uma forma de compensar este fenómeno consiste em injectar energia, em determinados pontos, distribuídos ao longo do canal de transmissão. Adicionalmente, um mecanismo de regeneração do sinal elimina o ruído introduzido pelo canal de transmissão (Figura 2.6 – b).

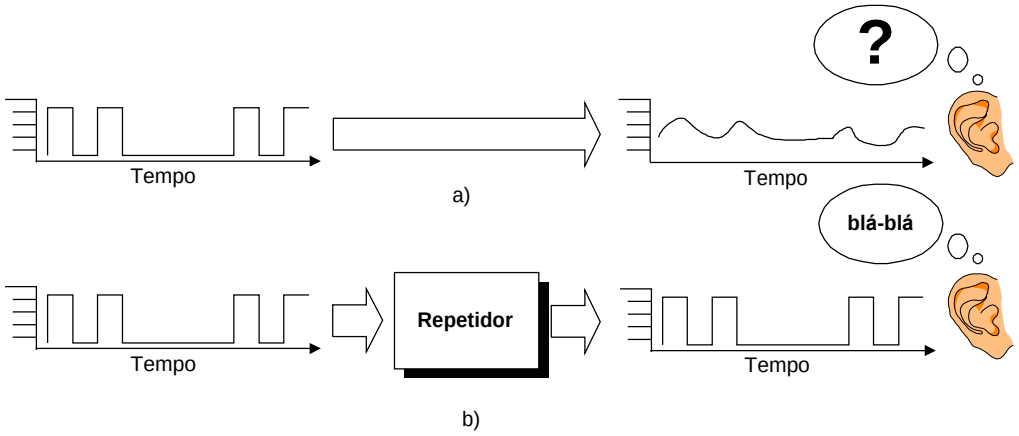


Figura 2.6 - Funcionamento básico de um Repetidor.

O aparelho responsável por esta função é designado por Repetidor (*repeater*) [Smythe95]. Um repetidor limita-se a ser um regenerador transparente de sinal que potencialmente elimina o ruído e as perdas resultantes da transmissão.

Os repetidores funcionam normalmente nos dois sentidos, repetindo o sinal proveniente de qualquer dos segmentos a ele ligado para o(s) segmento(s) oposto(s). Por este motivo, as entradas/saídas são denominadas portas. Os repetidores podem ter mais de duas portas (repetidor multiporta), sendo comuns 4, 6 ou mais em cada aparelho (Figura 2.7). Este facto possibilita a formação de redes mais complexas, compostas por vários troços. Em caso de falha de um troço, por avaria de uma estação ou por uma ligação mal feita, este é posto fora de serviço, não afectando o resto da rede.

É usual, em algumas configurações de rede, a utilização de aparelhos com funções semelhantes às de um repetidor, com um maior número de portas (tipicamente, de 12 a 36). Cada porta, normalmente, admite a ligação de apenas uma estação numa ligação ponto-a-ponto, tornando a lógica de controlo mais simples. Este componente é denominado Concentrador (*HUB*) e possibilita a reunião de todos os cabos que interligam os terminais em apenas um ponto (ou nó) de acesso. Os concentradores, tal como os repetidores, não fazem qualquer análise ao tráfego.

Os repetidores introduzem um atraso na transmissão do sinal que, apesar de reduzido, afecta a comunicação. Por este motivo, o número de repetidores encadeados encontra-se limitado a um valor que depende do tipo de tecnologia de transmissão. Por exemplo, para redes Ethernet a 10 Mbps o número máximo de repetidores entre duas estações é de quatro, enquanto que para o *Fast Ethernet* (100 Mbps) este número desce para dois. O espaçamento máximo entre repetidores depende do tipo de cabo e do método de controlo de acesso ao meio utilizado.

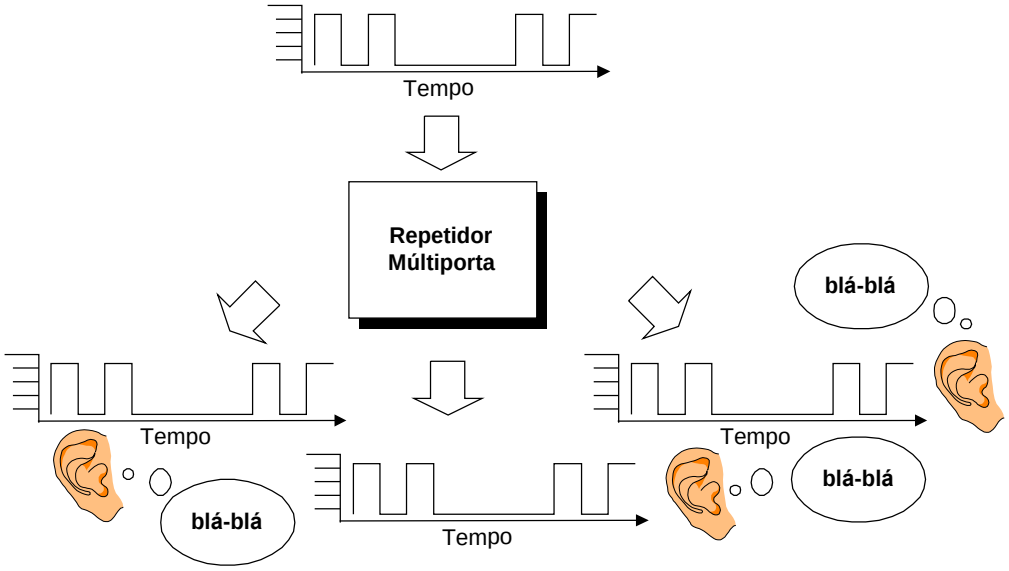


Figura 2.7 - Funcionamento básico de um repetidor multiporta.

2.3.2 Ponte

Muitas das técnicas de transmissão de dados assentam no método de difusão, um esquema em que, potencialmente, todos podem receber. Com o crescimento do número de sistemas ligados e de aplicações que usam a rede a taxa de ocupação do meio de transmissão pode atingir valores elevados que leva ao congestionamento. Numa empresa, cada departamento ou secção pode inclusive, disputar o meio com outros departamentos ou outras secções que nada têm a ver com a primeira. Por exemplo, a informação trocada entre os utilizadores do departamento gráfico de uma empresa consiste, em grande parte, em dados/imagens, que não interessam à secção de contabilidade. Se estes dados forem difundidos por todos os departamentos e secções haverá informação a circular que ninguém vai ler, resultando num desperdício de recursos.

Perante tal cenário, será desejável confinar predominantemente tráfego respeitante a secções específicas. Este problema é facilmente resolvido por interrupção permanente da conexão entre secções, mas pode haver ocasiões em que tal solução não é aceitável. Outra solução poderá consistir na descodificação do endereço do receptor da mensagem e identificação da secção à qual pertence. Desta forma, a informação será transmitida para a secção seguinte apenas se o endereço indicado não estiver na secção de origem. O componente que realiza estas funções actua não apenas ao nível do sinal, como o repetidor, mas necessita ter um conhecimento básico do formato da mensagem, por forma a descodificar o endereço do receptor.

A análise dos endereços das estações emissoras e receptoras permite restringir o tráfego a troços onde este faz sentido, libertando outros onde não seria necessário. O componente que realiza estas funções é denominado Ponte (***bridge***) [Peterson96]. A ponte não é programável, no entanto possui a capacidade de se adaptar ao meio onde se encontra inserida. Desde a sua activação, esta inicia uma análise contínua ao tráfego e constrói uma tabela interna que reflecte a posição relativa das diversas estações relativamente às suas portas [Stallings94]. Esta tabela permite enviar os pacotes de informação somente para a porta adequada, libertando assim os restantes troços (Figura 2.8).

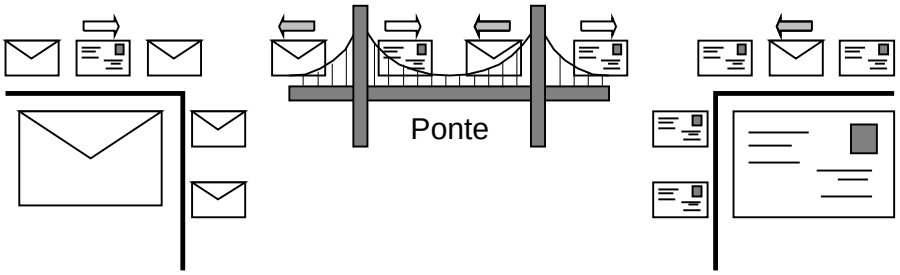


Figura 2.8 – Funcionamento de uma Ponte.

A instalação de uma ponte visa a segmentação da rede em "ilhas" de tráfego, por isso a sua localização deve ser planeada atendendo a que as "ilhas" já devem existir pela natureza das trocas de dados entre os vários sistemas de rede.

2.3.3 Comutadores (*Switches*)

Os Comutadores têm um princípio de funcionamento semelhante às pontes. Na realidade, a sua relação com as pontes é semelhante à relação entre os concentradores e os repetidores. Os comutadores apresentam várias portas (tal como os concentradores) e têm a capacidade de separar o tráfego de forma semelhante às pontes (Figura 2.9).

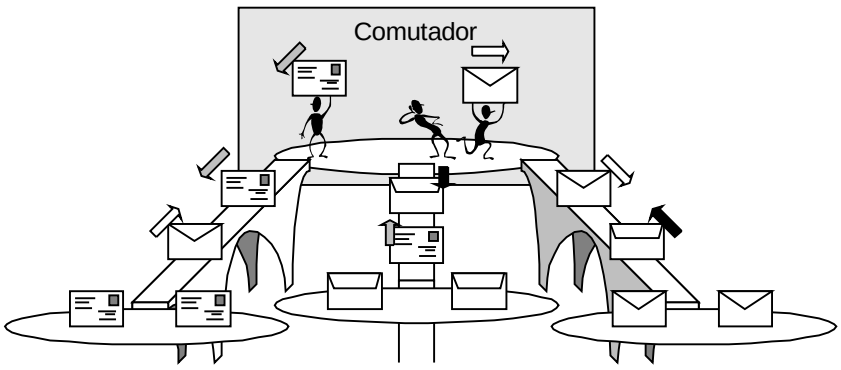


Figura 2.9 – Funcionamento básico de um comutador.

O comutador consegue responder à velocidade de cada porta pelo que, internamente, a sua largura de banda corresponde à soma das larguras de banda de cada troço (***full-duplex***). Para o caso de um comutador Ethernet de 10 Mbps com 8 portas, a largura de banda interna do comutador será 80 Mbps. Se o comutador for ***half-duplex***, a largura de banda interna será metade, ou seja, 40 Mbps.

A eficiência de um componente deste tipo resulta da redução de tráfego nos troços a que está ligado. A sua utilização deve ser planeada de forma a optimizar o desempenho das transacções e ainda de uma distribuição mais imune a falhas de segurança (como *sniffers*). Uma das estratégia de ligação será ligar a um comutador, por intermédio de uma porta de maior velocidade, uma estação com uma alta taxa de consulta (por exemplo, um servidor de ficheiros) e utilizar as portas de mais baixa velocidade para ligar cada secção ou troço. O comutador funciona como um *backbone* de alta velocidade relativamente aos troços que interliga.

2.3.4 Encaminhadores

As redes constituídas por repetidores e pontes têm um funcionamento semelhante a um sistema de difusão: uma transmissão por parte de uma entidade é potencialmente escutada por todas as outras estações. Esta estratégia não pode ser indefinidamente aplicada porque, por um lado, nos arriscamos a enviar uma trama para a máquina ao lado e esta ir parar igualmente a qualquer parte do mundo e ainda porque o endereçamento dos sistemas é limitado. Assim, cada zona de endereçamento comum (domínio) é geralmente confinada a uma área geográfica bem definida. A arquitectura apresentada na Figura 2.10 apresenta dois domínios denominados AVEIRO e PORTO, intercalados por intermédio de uma estação. As siglas 'A' a 'H' representam o endereço de cada ligação (interface de rede), diferente para todas as entidades.

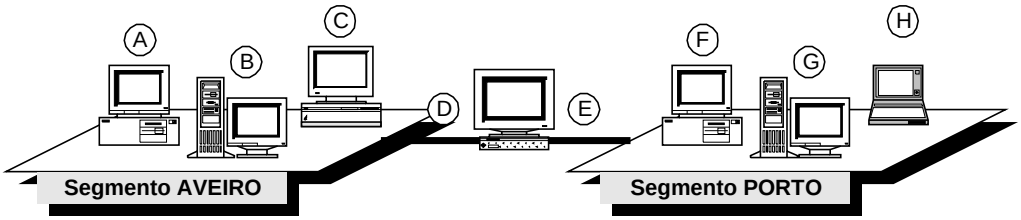


Figura 2.10 – Subredes interligadas por um encaminhador.

A distribuição sugere que as estações 'A', 'B' e 'C' possam comunicar directamente uns com os outros, assim como as estações pertencentes ao domínio PORTO. Por outro lado, a comunicação entre as estações pertencentes a domínios diferentes, 'A', 'B' e 'C' com 'F', 'G' ou 'H', só pode ser efectuada com o auxílio da entidade de ligação.

A comunicação entre máquinas pertencentes ao mesmo domínio de difusão (*broadcast*) pode ser efectuada colocando uma mensagem no meio de transmissão com os endereços de remetente e destinatário perfeitamente assinalados. Por exemplo, a estação 'A' para enviar uma mensagem para a 'C' necessita apenas de construir a mensagem, adicionar-lhe a identificação de emissor ('A'), do destinatário ('C') e colocar o sinal no meio de transmissão.

A comunicação entre a estação 'A' e a 'F', por exemplo, não pode ser efectuada sem intervenção da estação 'D'/'E'. Para que esta receba a transmissão, o endereço de destino da mensagem terá de ser 'D', pelo que o verdadeiro destino ('F') não é assinalado. O mecanismo criado para tornar a comunicação possível assenta na criação do conceito de subrede. A cada segmento, ou domínio de difusão, é atribuído um endereço de subrede. No caso da Figura 2.11, AVEIRO tem o endereço de subrede 193.136.171 e PORTO é identificado por 193.136.80. Cada estação pertencente à respectiva subrede é identificada pela concatenação do endereço de

subrede e um endereço local. Por exemplo, a estação 'A' tem o endereço 193.136.171.10 (AVEIRO.EstaçãoA).

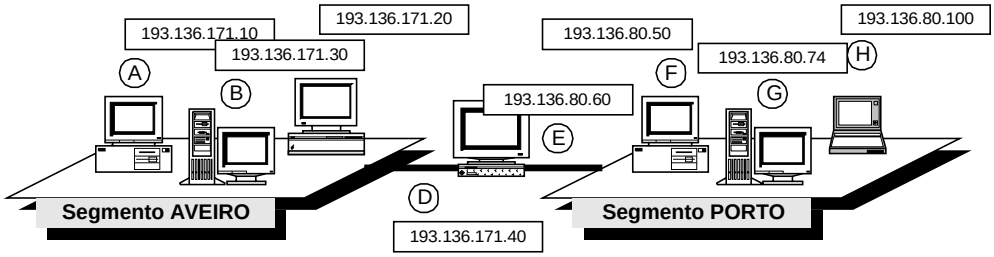


Figura 2.11 – Definição de domínios.

A transmissão da estação 193.136.171.10 ('A') para a 193.136.80.50 ('F') processa-se, simplificadamente, da seguinte forma:

- A estação 193.136.171.10 envia uma mensagem para o destino 193.136.80.50 (subrede PORTO). Como o destinatário se encontra numa rede diferente, esta é enviada à interface D, ou seja, ao 193.136.171.40.
- A estação 'D' (193.136.171.40) reconhece um endereço de subrede diferente do emissor da mensagem e transmite-a, pela interface E, para a subrede PORTO com endereço de emissor 193.136.171.10 e interface 'F'.
- A estação 193.136.80.50 recebe a mensagem dirigida à interface 'F', com endereço de emissor 193.136.171.10.

O cenário apresentado constitui um caso típico de interligação de redes na Internet. Os componentes com funções semelhantes às da estação 'D'/'E' são denominados Encaminhadores (*routers*) [Huitema95] e possibilitam a interligação de redes com diferentes endereços de subrede (Figura 2.12), ao contrário das pontes e repetidores que efectuam ligações entre estações ou segmentos de uma mesma rede.

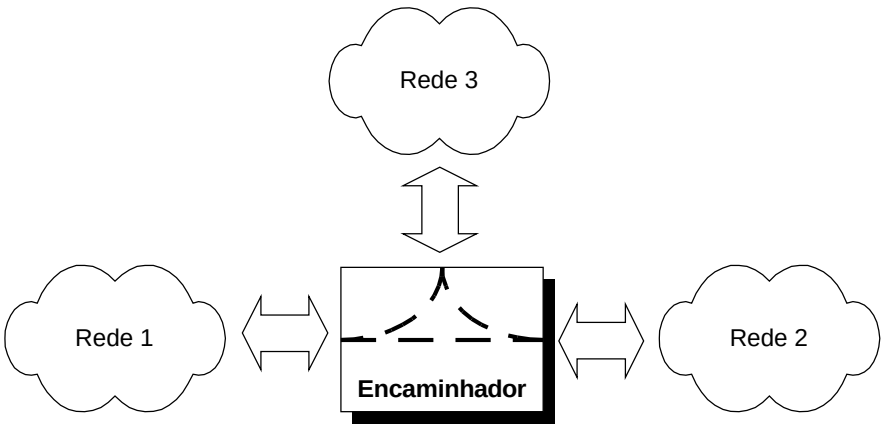


Figura 2.12 – Funcionamento básico de um Encaminhador.

O encaminhador é inicialmente programado pelo administrador, que introduz informação sobre que pacotes de informação deve encaminhar e para onde e posteriormente faz aquisição de informação dos endereços das estações em cada uma das redes a que está ligado.

As redes interligadas por encaminhadores podem diferir no método de controlo de acesso ao meio. No entanto os endereços de rede devem ser do mesmo tipo.

2.3.5 Relação com o modelo OSI

O modelo apresentado no início desta secção define três níveis (Figura 2.5). Cada um dos componentes acima descritos desempenha funções a um determinado nível. O repetidor, como componente regenerador de sinal, actua ao nível físico, ou seja, de sinal; a ponte selecciona o tráfego com base no identificador universal; o encaminhador troca mensagens entre diferentes subredes.

Os níveis definidos encontra-se especificados numa arquitectura para redes de comunicação, o modelo de referência OSI (*Open System Interconnection*), da ISO (*International Standards Organisation*). De acordo com este modelo, o nível de sinal será o nível físico, o de endereçamento universal será o lógico e o nível de comunidade/domínio será o de rede (Figura 2.13).

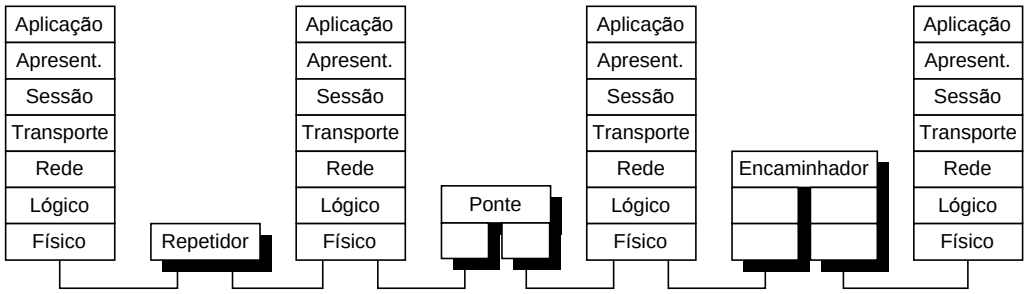


Figura 2.13 - Relação dos componentes com o modelo OSI.

2.4 Transmissão de Informação

A transmissão de informação é efectuada através de sinais que são influenciados pelo meio de transmissão (atenuação e ruído). Estes sinais podem apresentar várias formas dependendo do tipo de meio utilizado. Por outro lado, o meio é geralmente partilhado por um conjunto de estações que são obrigadas a seguir regras por forma a poderem comunicar. Esta secção visa introduzir, de forma sucinta, os problemas associados à modulação e à transmissão do sinal.

2.4.1 Suporte Físico

O cobre é um dos meios físicos mais adequados para o transporte de sinais eléctricos. Além disso, o seu preço é inferior ao de outras tecnologias, como a fibra óptica, pelo que constitui uma opção atractiva para redes locais de comunicação de dados. Actualmente, o cobre constitui a base de grande número de sistemas de comunicação de dados. A sua oferta é apresentada tipicamente em cabos coaxiais ou de oares entrançados.

Por outro lado, a fibra óptica, tem vindo a assumir uma importância crescente na transmissão digital. A imunidade ao ruído eléctrico, a grande largura de banda que disponibiliza e a fraca atenuação com que afecta os sinais são características essenciais em redes de alta qualidade e de alta velocidade [Jain94]. A fibra óptica é, geralmente, utilizada para ligações ponto-a-ponto, o que a torna adequada em configurações do tipo anel ou estrela. É ainda possível a utilização de fibra óptica

segundo uma topologia linear, recorrendo a uma de duas técnicas de ligação de estações: baixadas activas e passivas.

As baixadas activas funcionam numa base de ligações ponto-a-ponto (Figura 2.14). O sinal óptico recebido é convertidos num sinal eléctrico (Detector Óptico) e descodificado (Descodificador), sendo da responsabilidade do DTE copiar e retransmitir para a ligação de saída (Codificador e Transmissor Óptico).

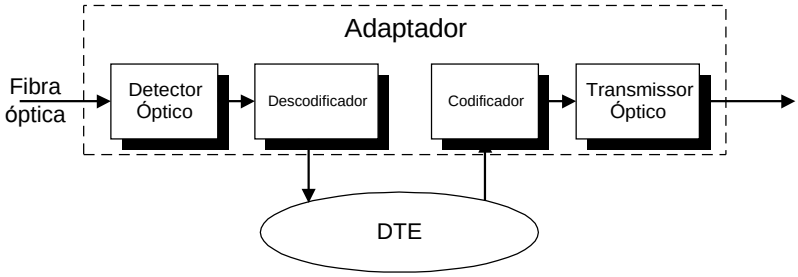


Figura 2.14 – Baixada activa.

No caso de uma baixada passiva (Figura 2.15), o adaptador retira um pouco da energia óptica na recepção limitando o número de terminais e o comprimento do meio [Stallings94].

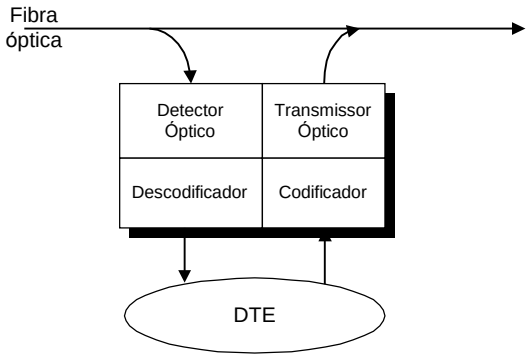


Figura 2.15 – Baixada passiva.

Devido ao carácter unidireccional dos transmissores ópticos são necessários dois caminhos para a troca de mensagens: um caminho "para baixo" e um caminho "para cima". Duas técnicas foram desenvolvidas com capacidade de resolverem o problema da unidireccionalidade do meio: meio único e meio duplo (Figura 2.16). No meio único, a transmissão é feita no troço "para baixo" e a recepção no troço "para cima".

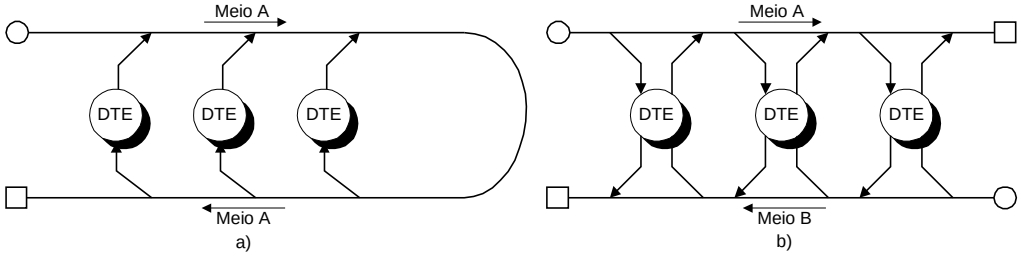


Figura 2.16 – Meio de transmissão unidireccional: a) meio único; b) meio duplo.

Os dados transmitidos são canalizados para o troço de recepção pela ligação feita entre os dois troços.

No meio duplo a transmissão é feita simultaneamente em dois meios distintos, com sentidos de transmissão contrários, permitindo abranger a totalidade de terminais conectados.

2.4.2 Tipo de Transmissão

Os dados podem ser transmitidos usando duas técnicas de modulação: Banda base (*Baseband*) e Banda larga (*Broadband*). Cada uma das técnicas possui vantagens e desvantagens relativamente à outra.

A tecnologia de transmissão em banda base usa sinais digitais (impulsos de tensão) na transmissão da informação. Toda a largura de banda do meio é usada na transmissão do sinal que é afectado por ruído e por atenuação, particularmente na gama das altas frequências. Este facto tem como consequência uma possível perda de informação, pelo que o comprimento do meio encontra-se limitado, na melhor das hipóteses, a alguns quilómetros. O cabo coaxial, tem um melhor comportamento às altas frequências que o cabo de pares entrançados, pelo que o efeito causado sobre o sinal é menor. O par entrançado, por sua vez, tem as vantagens de ser mais barato e de ser mais simples de manipular.

A possibilidade de modular a fase ou a frequência de uma portadora com um sinal digital introduz possibilidades inexistentes na transmissão em banda base. O uso de frequências diferentes para a portadora permite realizar multiplexagem na frequência de secções ou canais diferentes. Estes podem ser utilizados para transmitir diversos tipos de informação: dados, voz, vídeo, etc. Os sinais analógicos em causa podem percorrer grandes distâncias sem que o ruído e atenuação afectem, de modo significativo, o sinal modulado. Num sistema deste tipo, várias dezenas de quilómetros podem separar os terminais.

De uma forma geral, os sistemas deste último tipo são unidireccionais devido à impraticabilidade de construir amplificadores bidireccionais para a mesma frequência. Assim sendo, apenas as estações a jusante da estação emissora seriam capazes de receber a transmissão. Uma forma de transpor este facto passa pelo uso de meios físicos de transmissão com sentidos diferentes, um ascendente e outro descendente.

A tecnologia usada em sistemas de banda base é mais simples e mais barata que a utilizada em sistemas de banda larga. A simplicidade e o custo reduzido tornam os sistemas em banda base como a opção natural. Se houver necessidade de comunicação em distâncias relativamente longas, será de ponderar a utilização de um sistema em banda larga (Tabela 2.1).

Tabela 2.1 - Comparação entre Banda base e Banda larga.

	Banda Base	**Banda Larga**
Codificação	Sinal digital	Sinais analógicos
Largura de banda	Usa a totalidade de largura de banda	Multiplexagem em frequência
Direcção	Bidireccional	Unidireccional
Distância	Alguns quilómetros	Algumas dezenas de quilómetros

2.5 Estratégias de Controlo de Acesso ao Meio

O meio de transmissão é, de uma forma geral, partilhado entre inúmeras estações. Este facto torna imperativa a utilização de um método de controlo de acesso ao meio, isto é, de uma estratégia comum que regule a forma como o meio será utilizado por todos os sistemas.

O tipo de controlo de acesso ao meio depende de duas características: 1) onde o controlo é realizado e 2) como é realizado. A primeira indica se o controlo é realizado de forma centralizada ou distribuída. O controlo centralizado é regulado por um sistema com autoridade suficiente para garantir ou proibir o acesso ao meio. As estações têm de aguardar autorização de transmissão por parte do controlador. No controlo distribuído, as estações disputam entre si a ordem de acesso ao meio.

O controlo centralizado apresenta algumas vantagens em relação ao controlo distribuído:

- A possibilidade de criar esquemas de prioridades.
- A lógica de acesso encontra-se concentrada num único ponto, possibilitando a utilização de nós menos complexos.
- Resolver mais facilmente problemas de coordenação, manutenção e administração.

No entanto, é possível identificar igualmente algumas desvantagens:

- As comunicações assentam numa só entidade que, por estar sujeita a falhas, pode comprometer o bom funcionamento da rede.
- O controlador pode ser responsável por congestionamentos se o seu desempenho não for adequado.

A característica do "como realizar" está fortemente dependente da topologia usada e é resultado de um compromisso entre factores como o custo, desempenho e complexidade. De um modo geral, podem distinguir-se as técnicas de controlo de acesso em técnicas síncronas e técnicas assíncronas. As primeiras não são muito apropriadas para serviços de tráfego assíncrono, que tem sido característica dominante das redes de dados. Só mais recentemente, com o aparecimento de aplicações multimédia, surge a necessidade de garantir tráfego em tempo real. As técnicas assíncronas garantem potencialmente um melhor aproveitamento do meio de transmissão. Esta técnica pode ser subdividida em três categorias:

- Condicionado (***Round Robin***) –a oportunidade de transmissão é dada sucessivamente a cada estação, podendo esta rejeitar ou transmitir um volume máximo de informação. Como foi já referido, a coordenação entre estações pode ser feita de um modo centralizado ou distribuído. Para taxas de ocupação elevada o processo revela-se mais eficaz que para taxas de ocupação reduzidas. Nesta situação, o ***overhead*** imposto pelo mecanismo de passagem de testemunho reduz geralmente a eficácia de transmissão.

- Fixo (reserva) – funciona de modo semelhante ao TDM (*Time Division Multiplexing*). Uma estação que deseje transmitir necessita de reservar troços de tempo no meio para seu uso exclusivo. Esta técnica é mais adequada a tráfego intenso, como tráfego de voz, transferência de ficheiros, telemetria. Para tráfego curto (transmissões esporádicas) não é uma técnica muito eficaz.
- Contenda (disputa) – neste último método as estações disputam entre si por observação o privilégio de acesso ao meio de uma forma necessariamente distribuída. As principais vantagem são uma implementação mais simples e uma maior eficácia para tráfego pouco elevado. À medida que o tráfego aumenta o desempenho tende a ser cada vez mais baixo.

2.6 Protocolos de acesso

As redes locais de comunicação de dados sofreram, na década de 80, uma grande expansão que obrigou a um esforço de normalização em relação a toda a tecnologia emergente. O *Institute of Electrical and Electronics Engineers* (IEEE) foi uma das instituições que contribuiu para este esforço e do qual resultou a arquitectura IEEE 802. Esta arquitectura engloba três subcamadas correspondentes às camadas um e dois do modelo OSI.

2.6.1 Arquitectura IEEE 802

O grupo responsável pelas normas IEEE 802.x centrou nas camadas física e lógica do modelo OSI todo o trabalho de normalização (Figura 2.17).

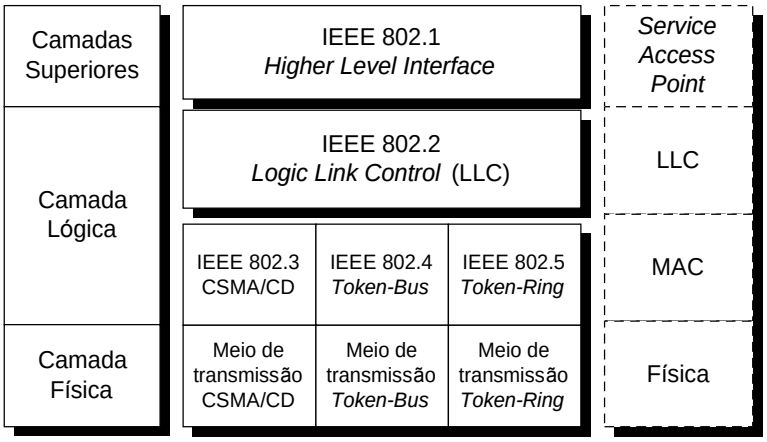


Figura 2.17 – Normas IEEE 802.

A norma IEEE 802.1 (*Higher Level Interface*) tem, por função, a especificação da interface com as camadas protocolares superiores.

A camada dois - lógica - foi subdividida em duas partes de modo a garantir na parte superior, (por intermédio da camada LLC – *Logical Link Control*) um acesso comum aos métodos de acesso ao meio definidos na parte inferior. Os dados do utilizador são passados à subcamada LLC, onde é acrescentada informação particular desta camada. Na subcamada inferior (MAC – *Medium Access Control*) é acrescentada a informação necessária à sincronização de tramas.

Encontram-se previstos alguns métodos de controlo de acesso ao meio de transmissão, entre os quais o método de acesso por contenda (IEEE 802.3 - CSMA/CD – *Carrier Sense Multiple Access with Colision Detection*) e método de acesso condicionado (IEEE 802.4 - *Token Bus* e IEEE 802.5 - *Token Ring*) (Tabela 2.2).

Tabela 2.2 - Técnicas de acesso ao meio.

Acesso	Linear	Anel
Condicionado	Token Bus (IEEE 802.4)	Token Ring (IEEE 802.5); FDDI
Fixo	DQDB (IEEE 802.6)	
Disputa	CSMA/CD (IEEE 802.3)	

2.6.2 Norma IEEE 802.2

Basicamente, o protocolo LLC deriva do HDLC (*High-Level Data Link Control*) [ISO4335]. Apesar de se basear em funções semelhantes, apresenta algumas diferenças [Stallings90a]:

- O LLC usa o modo de operação balanceado assíncrono do HDLC (ABM - *Asynchronous Balanced Mode*), ou seja, qualquer estação pode começar a transmissão sem autorização de outra estação. Este tipo de operação é referido como tipo 2 e destina-se a suportar ligações orientadas à conexão. Os outros modos de funcionamento do HDLC não são utilizados (NRM - *Normal Response Mode* e ARM - *Asynchronous Response Mode*).
- O LLC suporta a operação do tipo datagrama, conhecido como tipo 1.
- O LLC suporta um modo datagrama com confirmação, conhecido por operação de tipo 3.

Estas características do protocolo LLC permitem a prestação de três tipos de serviço:

- Datagrama sem confirmação - trata-se de um serviço simples que não envolve qualquer tipo de controlo de erros e não garante a recepção dos dados. Estas funções passam a ser da responsabilidade das camadas de nível superior.
- Orientada à conexão - este é um serviço semelhante ao disponibilizado pelo HDLC. Antes da troca de informação é estabelecida uma ligação lógica, na qual já existe controlo de erros e controlo de fluxo de informação.
- Datagrama com confirmação - intermédio entre os serviços anteriores. A informação é trocada em forma de datagramas com confirmação de recepção, o que permite um certo controlo de erros e de fluxo de informação.

De um modo geral, estes serviços são fornecidos de acordo com as necessidades de comunicação. O datagrama sem confirmação requer um mínimo de lógica (devido à sua simplicidade). É aplicável como suporte de protocolos que realizam, só por si, o controlo de erros e de fluxo de informação ou ainda em aplicações em que não é crítica a perda de uma ou mais tramas (monitorização, sensores).

A orientação à conexão pode ser usada em aplicações simples, dotados de uma pilha protocolar reduzida. O controlo de erros e fluxo de informação que este serviço disponibiliza permitem o seu uso por sistemas com pouco *software* acima deste nível, como controlo de terminais.

O serviço datagrama com confirmação encontra aplicação em inúmeros contextos. Um exemplo pode ser indicado num controlador de produção de um ambiente fabril. Devido à importância que os dados têm, é conveniente não perder nenhuma trama (confirmação de chegada) e, devido à urgência que alguns sinais podem ter, pode não ser conveniente o *throughput* acrescentado no estabelecimento de uma ligação.

2.6.3 Norma IEEE 802.3

A norma IEEE 802.3 especifica a escolha da topologia para meios de transmissão partilhados, como a linear, árvore ou estrela. Por sua vez, o protocolo de acesso escolhido é o CSMA/CD (*Carrier Sense Multiple Access with Colision Detection*) [ANSI802.3]. Este protocolo segue uma regra assíncrona distribuída de acesso aleatório. Por outras palavras, as estações partilham o meio (acesso múltiplo – MA) e disputam pela oportunidade de transmitir (Figura 2.18).

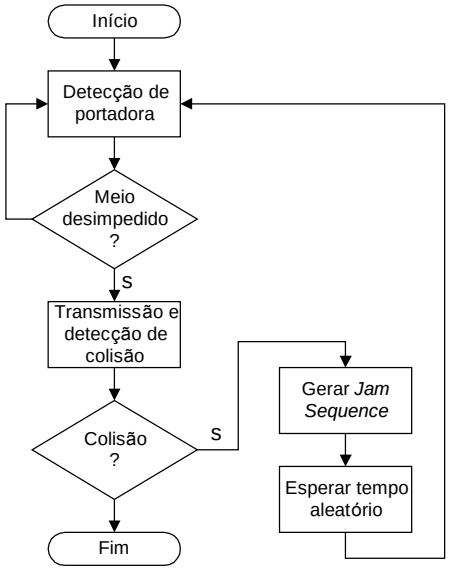


Figura 2.18 – Funcionamento do CSMA/CD.

Quando uma estação dispõe de dados para enviar é seguida uma ordem de operações:

- A disponibilidade do meio é testada, com a detecção de portadora (*carrier sense* - CS).
- Se o canal estiver ocupado, a transmissão é adiada, voltando a disponibilidade do meio a ser testada.
- Se o canal estiver desimpedido a estação inicia o acesso, transmitindo a trama sob a forma de uma sequência de bits. Esta trama transporta informação de endereçamento de destinatário, bem como de remetente, para as respostas serem correctamente encaminhadas.

- Devido à democracia do processo e a atrasos provenientes do tempo de propagação no meio podem ocorrer colisões (duas ou mais estações a transmitir ao mesmo tempo). Quando uma colisão é detectada (*Colision Detection* - CD) uma sequência de bits aleatória (*jam sequence*) é gerada, reforçando a colisão. Todas as operações são interrompidas. As estações responsáveis pela colisão esperam um período de tempo aleatório antes de recomeçarem a transmissão (início).

A norma define cinco tipos de meio de transmissão [ANSI802.3a] [ANSI802.3e] [ANSI802.3b] (Tabela 2.3).

Tabela 2.3 - Tipos de meio de transmissão.

Designação	Descrição
10BASE5	Usa cabo coaxial grosso (ϕ_E 10,26mm) de 50 Ohm com um comprimento máximo de 500 m entre repetidores. A distância mínima entre nós é de 2,5 m, suportando no máximo 100 nós por segmento. Entre dois nós o número máximo de repetidores é quatro. A velocidade de transmissão é de 10 Mbps, em banda base.
10BASE2	Semelhante ao 10BASE5 embora use cabo coaxial fino (ϕ_E 6,35mm) com um comprimento máximo de 185 m entre repetidores. A distância mínima entre nós é de 0,5 m, suportando no máximo 30 nós por segmento.
1BASE5	Também conhecida por ***StarLAN***, usa cabo de pares entrançados (UTP-3). As estações encontram-se ligadas numa configuração estrela passiva.
10BASE-T	Semelhante ao ***StarLAN***, embora a velocidade de operação se situe nos 10 Mbps.
10BROAD36	Usa cabo coaxial (75 Ohm) com um comp. máximo de 3600 m entre estações. As ligações são ponto a ponto entre um concentrador e a estação. A velocidade de transmissão é de 10 Mbps, em banda larga.
10BASE-F	Semelhante ao 10BASE-T, usa cabos de fibra óptica, o que lhe dá um comprimento máximo de segmento de 2 km.

2.6.4 Desempenho do CSMA/CD

O problema central deste protocolo é o atraso sofrido na propagação do sinal no meio de comunicação. Uma transmissão demora tempo a percorrer o canal, tempo este que pode ser suficiente para uma outra estação considerar o canal livre e iniciar a comunicação. Neste caso ocorre uma colisão. Durante a ocupação do canal, qualquer outra estação pode dispor de dados para enviar. Quando o canal é libertado, todas as estações em espera iniciam a transmissão.

O atraso na propagação tem o mesmo efeito tanto no fim da transmissão como no início. As estações apercebem-se do canal livre a diferentes instantes, dependendo da posição relativa ao longo deste. O tempo de propagação médio num canal de cobre é de cerca de 5,2 μs por quilómetro [Boisseau94]. Este valor aumenta ligeiramente na presença de repetidores.

Uma expressão vulgarmente aceite como indicadora da taxa máxima absoluta de transmissão é dada por [Dutton95]:

$$\text{TaxaMax} = \frac{1}{1+6.44\,r}\text{, onde } r = \frac{\text{atraso sofrido}}{\text{tempo de transmissão}} \qquad \text{[Eq. 2.1]}$$

Aplicando a expressão a uma rede local de 10 Mbps, com uma trama de 1000 *bits* (125 *bytes*) de comprimento (1000/10M=100 μs de tempo de transmissão) e um comprimento de 2 km (atraso de 10,4 μs) obtemos um rendimento de 59%, o que significa utilizar 5,9 Mbps dos 10 Mbps disponíveis à partida. Note-se que segundo [Eq. 2.1] o rendimento é tanto maior quanto maior for o comprimento das tramas e menor for o comprimento do segmento (Figura 2.19 – a). Por exemplo, para os mesmos valores anteriores mas alterando a taxa de transmissão para 100 Mbps (menor tempo de transmissão) o valor do rendimento desce para 13% (Figura 2.19 – b).

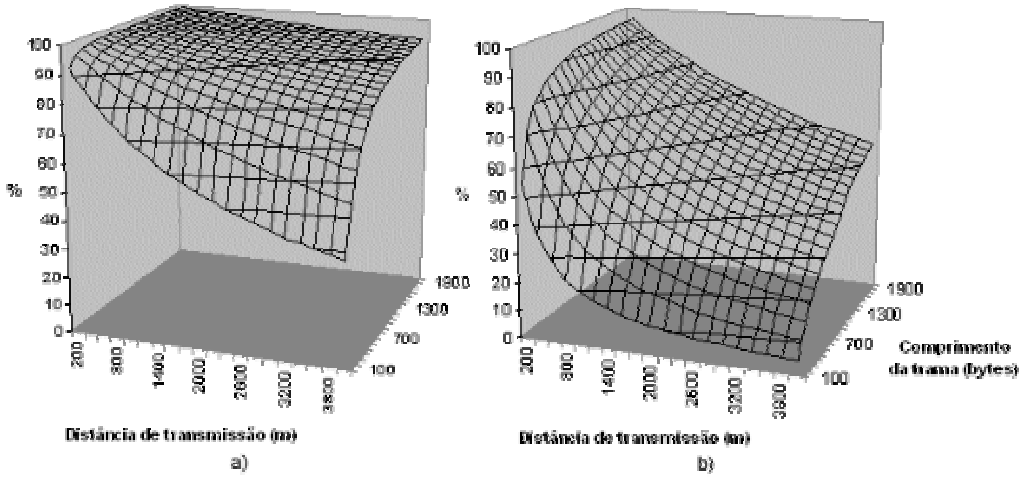


Figura 2.19 – Taxa de transmissão máxima de uma LAN CSMA/CD em função da distância de transmissão e do comprimento da trama:
a) 10 Mbps; b) 100 Mbps.

Embora este cenário possa parecer negativista, na prática, a taxa é consideravelmente superior. Este facto deve-se à característica do tráfego em que, para blocos relativamente longos (cerca de 1000 *bytes* – 8000 *bits*) e distâncias reduzidas (cerca de 200 m), o sistema apresenta uma taxa de transmissão de 92%.

Segundo [Dutton95], a expressão não é exacta em todas as situações mas serve para ilustrar o rendimento máximo de uma rede CSMA/CD relativamente à velocidade de transmissão e do comprimento das tramas.

O valor calculado por [Eq. 2.1] deve ser visto apenas como a velocidade máxima efectiva do meio. O rendimento encontra-se dependente de outros factores, como o número de colisões que afectam a transmissão.

Neste cenário, vários utilizadores tentam obter serviços de um recurso limitado seguindo uma ordem específica. Este caso pode ser estudado matematicamente segundo a teoria das filas de espera. Em resumo, quando a taxa de utilização de um recurso se aproxima de 100% a fila tende para infinito (Figura 2.20).

No caso de redes CSMA/CD o tempo de espera para um determinado utilizador ser servido aumenta exponencialmente, até que a comunicação deixa de se poder realizar devido ao elevado número de colisões. A conjugação dos dois factores implica um rendimento de 15% a 40% em redes CSMA/CD.

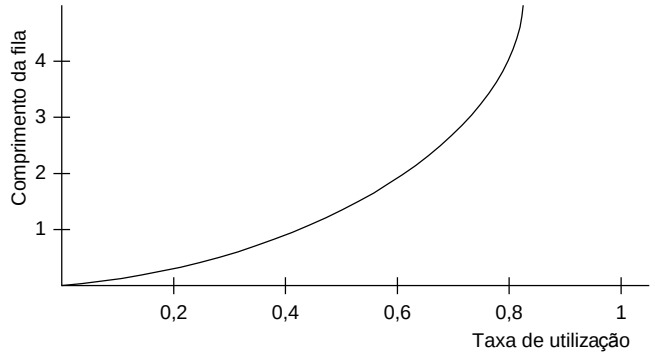


Figura 2.20 – Comprimento da fila relativamente à taxa de utilização do recurso.

2.6.5 Norma IEEE 802.4

Tal como o IEEE 802.3, o *Token Bus* [Stallings90b], usa como meio de transmissão as topologias em meio partilhado linear, árvore e estrela (Figura 2.21).

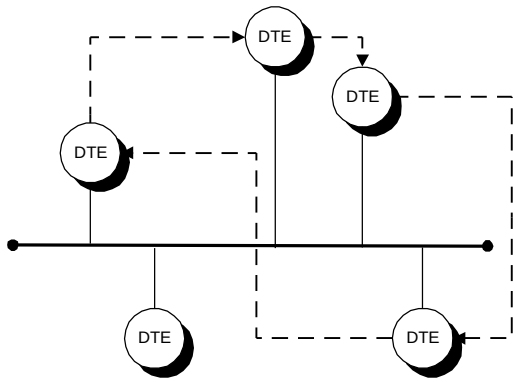


Figura 2.21 - Anel virtual em *Token-Bus.*

A regra de acesso ao meio é assíncrona de acesso condicionado (passagem de testemunho). O testemunho é representado por uma trama do nível da subcamada MAC (invisível nos níveis superiores), que é passada de estação em estação segundo uma configuração lógica em Anel. O acesso ao meio é garantido de uma forma condicional, por passagem de testemunho à máquina que se segue.

Cada estação só pode transmitir para o meio quando na posse do testemunho, sendo obrigada a passar o testemunho para a estação seguinte após a transmissão de uma trama de dados.

A sequência de operações é a seguinte:

- Um anel lógico é criado, sendo a sua ordenação baseada nos endereços das diferentes estações. Um testemunho é criado, enviado da estação de menor endereço para a sua sucessora.
- O testemunho percorre o anel lógico de estação para estação até ser recebido por uma disposta a enviar dados. Esta técnica concede um acesso determinístico ao meio partilhado: todas as estações dispõem de oportunidade para transmitir.

- A estação captura o testemunho e envia a trama de dados para o meio de transmissão, após a qual liberta o testemunho para a próxima estação do anel lógico.

Um problema desta arquitectura é a necessidade de um sistema complexo de controlo distribuído que possa detectar as perdas de testemunho bem como a duplicação do mesmo. O sistema de controlo reúne mecanismos com funções de estabelecimento e manutenção do anel lógico:

- Activação do testemunho.
- Inicialização dos endereços das estações intervenientes.
- Reposição do bom funcionamento em caso de falha ou erros (perda de testemunho ou testemunhos múltiplos).
- Reconfiguração dinâmica do anel lógico - admissão de novas estações no anel ou remoção das existentes sem interrupção do funcionamento normal dos restantes intervenientes.

O controlo da coordenação entre as estações é feito por intermédio de tramas de controlo ao nível da subcamanda MAC.

Todas as tramas trocadas necessitam de informação de endereço, quer de destino quer de origem, de modo semelhante ao CSMA/CD, uma vez que usam o mesmo tipo de meio.

A norma IEEE 802.4 prevê três tipos de meios de transmissão (Tabela 2.4):

- Banda larga com velocidades de 1, 5 e 10 Mbps, ocupando uma largura de banda de 1.5, 6, e 12 MHz, respectivamente.
- Banda larga de canal único (*carrierband*), que tem a vantagem de necessitar de electrónica mais simples do que a banda larga. Tem velocidades de 1, 5 e 10 Mbps.
- Fibra óptica numa configuração Estrela com velocidades de 5, 10 e 20 Mbps.

Tabela 2.4 - Meios de transmissão da norma IEEE 802.4.

	Meio transmissão	Codificação	Taxa de transferência	Comprimento max. do segmento
Banda larga	Coaxial 75 Ω	AM / PSK	1, 5, 10 Mbps	Não especificado
Carrierband	Coaxial 75 Ω	FSK	1, 5, 10 Mbps	7600 m
Fibra óptica	fibra óptica	ASK-Manchester	5, 10, 20 Mbps	Não especificado

2.6.6 Norma IEEE 802.5

O *Token Ring* [Haugdahl87] é um protocolo de acesso ao meio utilizado para configurações em anel. Todo o funcionamento assenta numa trama especial (o testemunho) que circula no anel. Quando não existe necessidade de transmissão o testemunho entra na condição de "livre". Uma estação que necessite transmitir aguarda a passagem do testemunho "livre" que modifica para "ocupado". A estação transmite a informação logo após o testemunho. As outras estações são, deste modo,

obrigadas a esperar. O testemunho dá a volta e regressa à estação que o modificou onde é destruído. Esta liberta um testemunho "livre" se:

- a estação completou a transmissão do pacote;
- o testemunho "ocupado" regressou à estação.

No caso de o comprimento do anel ser inferior ao do pacote (em termos de bits) a primeira condição implica a segunda.

À semelhança do *Token Bus*, o *Token Ring* requer mecanismos de recuperação em caso de erro. As condições de erro mais frequentes são a ausência de testemunho e testemunho "ocupado" persistente. Uma estação é designada como monitora para, continuamente, manter o bom estado de funcionamento do anel. A perda de um testemunho é detectada por intermédio de uma contagem finda a qual é considerado perdido. A recuperação passa pela eliminação de quaisquer dados que circulem e pela libertação de um testemunho "livre". Para detectar a permanência de um testemunho "ocupado", o monitor modifica um bit para o estado '1' no testemunho "ocupado". Se o testemunho passar novamente com o bit a '1' então ele assume que a estação emissora falhou na libertação do testemunho "livre", pelo que o "ocupado" é destruído e um "livre" é libertado.

Um esquema com 8 níveis de prioridade é acrescentado, com a finalidade de ordenação de pedidos, diminuindo o tempo de espera às estações que necessitem de transmitir dados prioritários.

2.7 Conclusões

Este capítulo teve início com uma pequena apresentação de conceitos e de equipamento elementar de rede. Foi feita uma descrição das configurações mais usadas em redes de comunicação de dados, terminando com uma apresentação das estratégias e protocolos de acesso mais conhecidos.

O compreensão destes conceitos básicos permite ir além da tecnologia actual e facilitar a aquisição de conhecimentos que, de outra forma, não seria tão imediata.

3 REDES DE ALTA VELOCIDADE

3.1 Introdução

Actualmente um grande número de organizações depende da sua rede local de comunicações de dados para a troca de informação. Com o aumento do volume de tráfego, a largura de banda disponível depressa se torna inadequada na manutenção de um nível de desempenho aceitável. A evolução para redes mais rápidas ou mais eficientes surge, muitas vezes, como inadiável. A migração para rede com débitos elevados passa pela opção entre dois tipos de soluções: baseadas em Ethernet ou soluções não Ethernet.

De entre as tecnologias de LANs capazes de débitos mais elevados, as baseadas em Ethernet são as mais prováveis de dominar o mercado. Estima-se que cerca de 80% de todas as redes instaladas usam o método de controlo de acesso ao meio CSMA/CD [Gigabit96], pelo que o impacto de evolução pela introdução de velocidades elevadas é reduzido.

As soluções baseadas em Ethernet não se apresentam eficientes para taxas de ocupação relativamente elevadas, pelo que nem sempre são uma escolha acertada em termos de desempenho [Lopes97a]. Este tipo de situações sugere a necessidade de outro tipo de tecnologia, capaz de fazer face ao tráfego elevado. O FDDI (*Fibber Data Distributed Interface*), apesar de conseguir débitos de 100 Mbps ainda é uma solução muito cara. Devido a esta característica, outras soluções surgem com base em métodos de controlo de acesso ao meio diferentes do CSMA/CD, como o 100VG-AnyLAN.

3.2 Soluções baseadas em Ethernet

A rede Ethernet assenta na tecnologia de controlo de acesso ao meio universalmente mais utilizada – o CSMA/CD (*Carrier Sense Multiple Access with Collision Detection*). Esta rede apresenta algumas vantagens:

- Tecnologia mais que comprovada - com milhões de utilizadores.
- Infra-estrutura de apoio numerosa e bastante treinada – os técnicos associados a este tipo de rede possuem, potencialmente, alguns anos de experiência e, por isso, acumularam já conhecimentos necessários para manter bons níveis de funcionamento.
- Facilidade de migração - a actualização pode ser periódica e sem grandes gastos.
- Informação - a vulgarização da tecnologia permite que a informação que lhe está associada chegue mais facilmente ao gestor.

Este tipo de soluções contém, de igual modo, alguns inconvenientes que permitem o aparecimento de novas tecnologias:

- Não houve uma evolução significativa ao nível do controlo de acesso ao meio, o que torna a tecnologia inadequada para certas aplicações e para determinado nível de tráfego.
- O aumento do número de utilizadores, geralmente, implica uma redução na eficiência da rede [Shock80].

Independentemente destes inconvenientes, a Ethernet é uma solução comprovada e plenamente testada, o que permite o desenvolvimento de soluções evolutivas tais como as que serão apresentadas nas secções seguintes.

3.2.1 100BASE-T (*Fast Ethernet*)

De entre todas as tecnologias actualmente disponíveis, que suportam larguras de banda elevadas, a *Fast Ethernet* tem vindo a tornar-se líder em termos de mercado. Baseada na norma IEEE 802.3, surge como uma evolução directa do 10BASE-T. Neste tipo de norma, as estações partilham o mesmo meio, havendo contenção (disputa) pela ocupação do meio. Qualquer transmissão é recebida por todas as estações, sendo processada apenas pelo destinatário. O protocolo de controlo de acesso ao meio continua a ser o CSMA/CD (*Carrier Sense Multiple Access with Collision Detection*).

A norma CSMA/CD a 100 Mbps foi desenvolvida de modo a possibilitar uma evolução natural do 10BASE-T [Melatti94]. O protocolo deveria:

- Ser barato. De outra forma seria preferível optar por FDDI.
- Preservar a lógica de acesso existente (MAC 802.3). Este ponto possibilitaria o uso continuado do *software* existente.
- Usar cabos de par entrançado (UTP). A maior parte dos utilizadores da norma IEEE 802.3 usa este tipo de suporte.
- Facilitar a migração a partir da norma anterior.

A operação a 100 Mbps faz-se em banda-base, tal como na norma anterior. A camada de MAC (*Medium Access Control*) é a mesma, havendo apenas diferenças ao nível do meio de transmissão (Figura 3.1).

Todos os pontos anteriores se encontram satisfeitos à excepção de um. Não é possível a simples operação sobre cabos UTP categoria 3 de dois pares, por apresentarem capacidades eléctricas e magnéticas insuficientes. A solução consiste em utilizar quatro pares. Para além deste facto, a grande diferença entre as duas normas (100 Mbps vs 10 Mbps) encontra-se a nível do número de repetidores ou concentradores entre duas estações. Para 10 Mbps são permitidos quatro, enquanto que para 100 Mbps não é autorizado o uso de mais de dois.

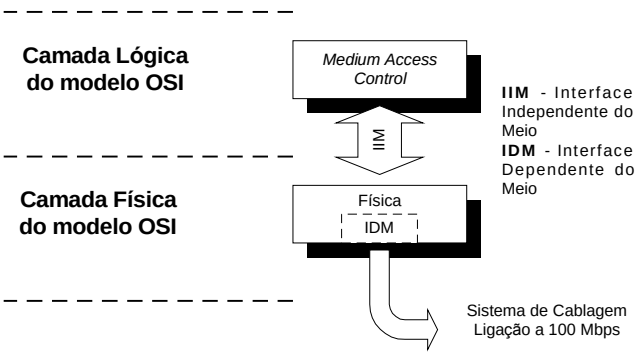


Figura 3.1 - 100BASE-T: Componentes básicos.

Os tipos de meio previstos em redes *Fast Ethernet* podem ser consultados na Tabela 3.1 [IEEE802.3u].

Tabela 3.1 - Tipos de meio para 100BASE-T.

Camada Física	Tipo de meio de transmissão
100BASE-TX	2 Pares de UTP-5 ou 2 pares de STP de 150 Ohm. Definidos na norma ISO/IEC 11801. A distância entre terminal e concentrador é de 100 m.
100BASE-T4	4 Pares de UTP-3, 4 ou 5. Definidos na norma ISO/IEC 11801. A distância entre estações é de 100 m.
100BASE-FX	2 Fibras ópticas multimodo. Definidas na norma ISO 9314. A distância entre estações é de 500 m.

Encontra-se previsto o uso de cabos UTP de Categoria 5 ou STP de 150 Ohm. Estes tipos de suporte encontram-se especificado na norma ISO/IEC 11801. O modo de operação é semelhante ao 10BASE-T, usando apenas dois pares. Um dos pares é usado para transmitir enquanto que o outro é usado na detecção de colisões. As propriedades físicas do cabo têm uma maior influência para velocidades elevadas, de modo que cabos de alta qualidade e técnicas diferentes de codificação são usados. O método de transmissão usa uma codificação 4B/5B (originária do FDDI) necessitando uma largura de banda efectiva de 125 MHz.

Devido à grande dificuldade em conseguir velocidades elevadas em pares simples de categoria 3, esta solução usa vários pares a velocidades mais baixas.

As normas especificam o funcionamento sobre UTP-3 de quatro pares. As características mais importantes deste tipo de ligação podem ser resumidas como se segue:

- Todas as ligações são ponto-a-ponto, entre as estações e um repetidor (concentrador - *HUB*).
- Por razões de tempo de propagação e de temporização a distância máxima entre o concentrador e as estações é de 100 m.
- O protocolo deve operar tanto a 100 Mbps como a 10 Mbps. As placas de rede devem detectar o tipo de concentrador a que estão ligadas e seleccionar o modo de funcionamento de acordo.
- As ligações são *half-duplex*. Todos os pares são usados pela estação transmissora e não é possível a operação em *full-duplex*.

O sistema funciona da seguinte forma:

- Um par é usado para detecção do modo de funcionamento (10/100 Mbps) e nunca é usado para transmitir dados. Este par também funciona para detecção de colisão.
- Os 3 pares restantes são usados em paralelo para transmitir dados: cada par transmite a 33,33 Mbps, conseguindo-se a totalidade de largura de banda.
- A codificação usada é a 8B6T (8 binário - 6 ternário). A velocidade de transmissão correspondente a esta codificação é de 25 Mbaud $\left(\frac{33{,}33}{8/6}\right)$, com uma frequência dominante de 12,5 MHz (2 baud por ciclo).

- Os bytes de dados são enviados para os pares seguindo uma ordenação *round-robin*. Um cabeçalho e um rodapé independentes são adicionados a cada par, de modo a facilitar a sincronização e reconstrução dos dados enviados.
- O comprimento máximo de trama é limitado a 1518 bytes, como no Ethernet clássico.

A transmissão de dados sobre fibra óptica segue as características do 100BASE-TX. São usadas duas fibras ópticas multimodo (tal como no FDDI), com codificação de 4B/5B e largura de banda efectiva de 125 MHz.

3.2.1.1 Repetidores

Os repetidores são componentes essenciais em redes Ethernet. Estes regeneram o sinal permitindo aumentar a distância entre estações. A norma 100BASE-T pode usar cabos UTP-3, UTP-5 ou fibra óptica, de modo que um repetidor pode ser construído de modo a suportar apenas um, ou mais destes tipos de meio. Em 10BASE-T o número máximo de repetidores entre duas estações é de quatro. Para 100 Mbps o atraso na propagação do sinal tem uma maior influência face à frequência de transmissão, pelo que a distância entre estações é, obrigatoriamente, menor. A especificação 100BASE-T classifica os repetidores em duas classes:

- **Classe I** - Repetidor de cujo tipo apenas um pode existir entre duas estações no mesmo domínio de colisão.
- **Classe II** - Repetidor especificado tal que, no máximo, apenas dois repetidores podem existir entre duas estações num domínio de colisão.

A distância máxima entre estações fica, deste modo, reduzida a 300 m (100 + 100 + 100). Se houver necessidade de aumentar este valor é necessário empregar uma ponte (*bridge*), para segmentar o meio de transmissão em domínios de colisão diferentes.

3.2.1.2 Estratégia de migração para 100BASE-T

As semelhanças entre as especificações 100BASE-T e 10BASE-T permitem várias estratégias de migração. Esta flexibilidade é boa para o cliente, uma vez que permite a escolha da melhor estratégia caso a caso. As considerações mais importantes incluem:

- Que componentes necessitam ser comprados?
- Como ligar à rede 10 Mbps existente?
- Como alargar a topologia a um maior número de utilizadores?

Na migração para 100BASE-T são necessários novos repetidores e novas placas de rede. Em alguns casos será necessário substituir a cablagem. A melhor estratégia de migração passa pela manutenção de troços a 10 Mbps e adquirir material adequado a 100 Mbps apenas para novos utilizadores.

A protecção do investimento passa pela aquisição de placas de rede e cabos que suportem ambos as especificações: 10 e 100 Mbps. Desta forma, os novos postos criados estarão adequados à migração quando esta for necessária. A invasão gradual da rede de 10 Mbps pela de 100 Mbps pode ser suportada pela aquisição de pontes ou encaminhadores. As pontes são mais rápidas, baratas e fáceis de instalar. Os encaminhadores constituem equipamento caro, difícil de instalar e requerem pessoal

treinado para a sua manutenção. O plano deve conter apenas um repetidor por domínio de colisão. O uso de pontes para segmentar o tráfego desvia o tráfego local de outros segmentos. Com redes Ethernet pequenas, o número de colisões decresce, aumentando o rendimento.

3.2.2 Gigabit Ethernet

A adopção do 100BASE-T na ligação a clientes começa a criar a necessidade de maior largura de banda nos servidores e no ***backbone*** da rede. O caminho natural a seguir passa pela evolução do ***Fast Ethernet***, num passo semelhante ao que o 10BASE-T sofreu.

A tecnologia do gigabit por segundo não é propriamente nova. Existem já soluções que apresentam velocidades da ordem do gigabit por segundo, como o ATM (*Asynchronous Transfer Mode*), o HIPPI (*HIgh Performance Parallel Interface*) ou o *Fiber Channel*, embora não ofereçam um caminho de evolução lógico a partir do 100BASE-T.

A evolução, ainda em desenvolvimento, é a *Gigabit Ethernet* (IEEE 802.3z). Esta fornecerá uma largura de banda de 1 Gbps para redes locais de comunicação de dados com a simplicidade de instalação de qualquer rede Ethernet. Os objectivos são:

- Oferecer um caminho de evolução natural, mantendo toda a infra-estrutura de apoio já existente para redes Ethernet.
- Preço reduzido quando comparado com tecnologias de largura de banda semelhantes.
- Manter o mesmo formato e comprimento de trama usada nas redes Ethernet originais.

O protocolo de controlo de acesso ao meio continua a ser o CSMA/CD, pelo que não há necessidade de formação ao nível de pessoal nem de aquisição de ferramentas de adaptação ou compatibilização.

Estas características tornam a tecnologia emergente adequada à interligação de comutadores 10/100Base-T, criando um meio de transmissão de alto desempenho para servidores e para estações com requisitos de largura de banda superior aos 100 Mbps.

3.2.2.1 Configurações de rede

Tal como as tecnologias anteriores, 10BASE-T e 100BASE-T, a *Gigabit Ethernet* admite configurações em que há partilha do meio de transmissão, como a topologia em Árvore, Estrela ou Linear. O uso de componentes de interligação como repetidores, concentradores ou pontes, tornam perfeitamente flexível a configuração das ligações. O uso de comutadores traz benefícios em termos de velocidade, pela criação de um maior número de domínios de colisão.

A estratégia de migração é simples e flexível, semelhante à da Ethernet para *Fast Ethernet*.

3.2.2.2 Tecnologia

O *Gigabit Ethernet* é uma extensão às normas IEEE 802.3. A largura de banda oferecida é de 1000 Mbps, mantendo-se a compatibilidade com as normas anteriores.

A tecnologia usada em fibra óptica deriva de uma norma já existente, a *Fibre Channel*.

O *Gigabit Ethernet* suporta modos de operação *full-duplex* em ligações entre comutadores e entre comutador e estação. Para ligações em meio partilhado, o modo de operação é *half-duplex*. O meio de transmissão previsto à partida é fibra óptica, havendo também a possibilidade de funcionar sobre UTP-5 e cabo coaxial (Figura 3.2).

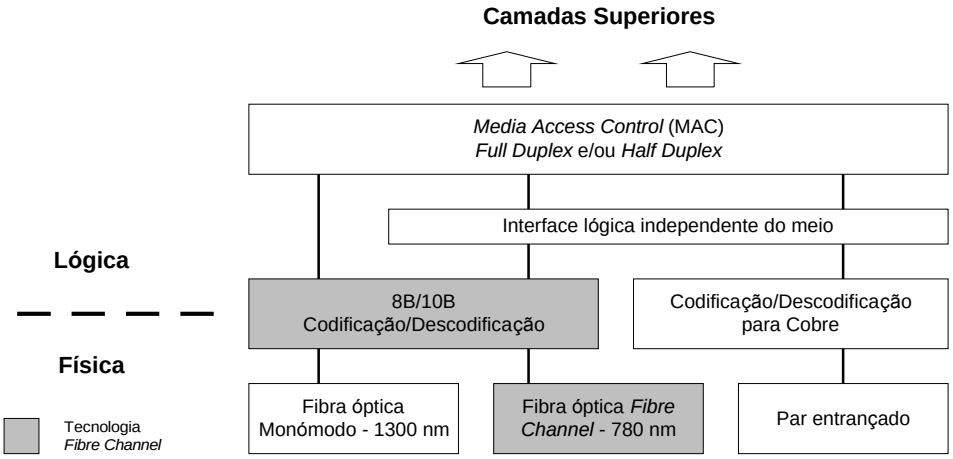


Figura 3.2 - Estrutura de funcionamento do *Gigabit Ethernet*.

O desenvolvimento inicial do Gigabit Ethernet empregou fibra óptica de 780 nm com a codificação 8B/10B (proveniente do *Fiber Channel*). A distância entre estações neste caso encontra-se limitada a cerca de 500 m. O uso de fibra óptica monomodo, com luz de comprimento de onda de 1300 nm, permite distâncias superiores (cerca de 2 km).

Avanços tecnológicos ao nível do silício e de processamento digital do sinal possibilitarão a operação sobre cabo UTP-5: numa primeira fase, em 1998, a aliança *Gigabit Ethernet* espera completar uma norma sobre UTP-5, para comprimentos máximos de 25 m. Espera-se que numa futura norma este atinja os 100 m para cabos com 4 pares [Gigabit96].

3.2.2.3 Cenários de aplicação do Gigabit Ethernet

O *Gigabit Ethernet* terá relevância acrescida em *campus* ou edifícios onde é necessária maior largura de banda entre encaminhadores, comutadores, concentradores, repetidores e servidores. Em todos os cenários, os sistemas operativos, aplicações e APIs serão mantidos, devido ao facto não haver modificação no método de controlo de acesso ao meio. Os cinco cenários mais prováveis serão:

- Ligações entre comutadores - obter pontes de 1000 Mbps entre comutadores 100/1000 Mbps. O aumento de velocidade na transferência de dados entre comutadores (100 Mbps para 1000 Mbps em comutadores 100/1000 Mbps) permite aumentar o número total de segmentos mantendo níveis de funcionamento elevados (Figura 3.3).

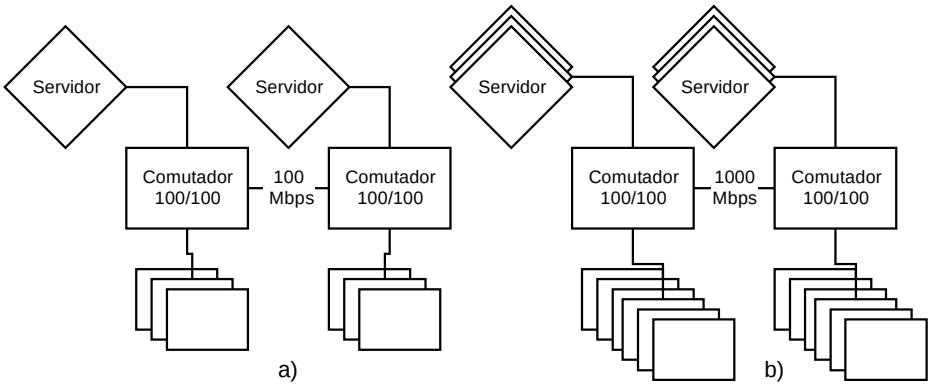


Figura 3.3 - Actualização das ligações entre comutadores.

- Ligações entre servidores e comutadores - alta velocidade no acesso a ficheiros e aplicações (Figura 3.4).

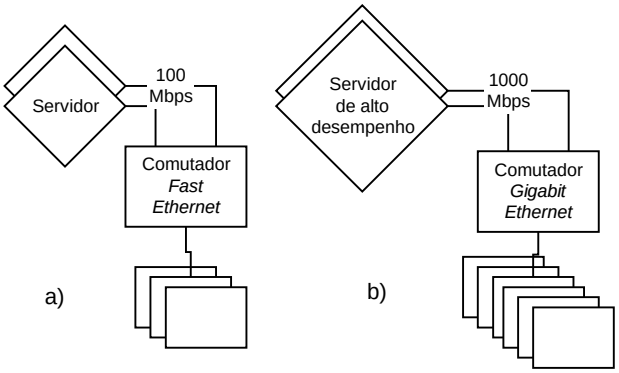


Figura 3.4 - Actualização das ligações entre servidores e comutadores.

- *Backbone Fast Ethernet* – dotar redes *Fast Ethernet* de comutadores e *backbone Gigabit Ethernet* (Figura 3.5).

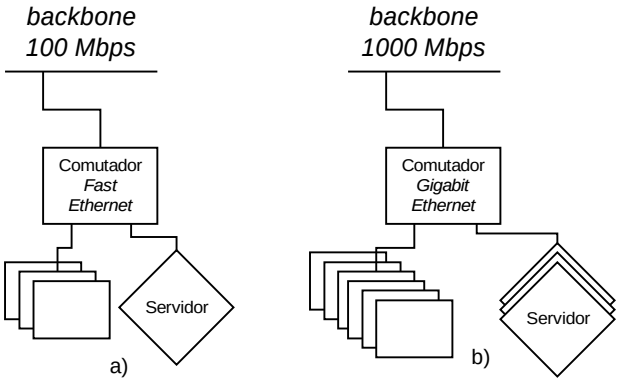


Figura 3.5 - Actualização de um *backbone Fast Ethernet*.

- *Backbone* FDDI - instalar tecnologia *Gigabit Ethernet* em redes FDDI. A substituição de concentradores FDDI por comutadores ou repetidores *Gigabit Ethernet* possibilita um aumento de largura de banda neste tipo de redes (Figura 3.6).

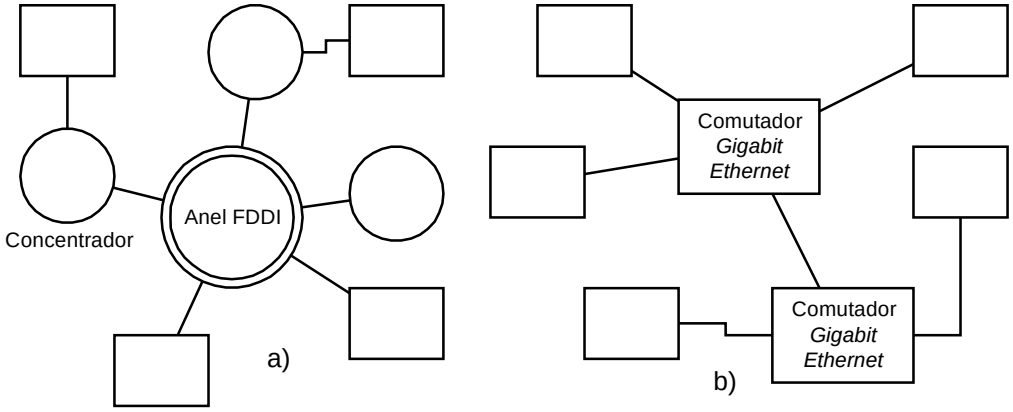


Figura 3.6 - Actualização de um *backbone* FDDI.

- Estações de trabalho de alto desempenho - cartas *Gigabit Ethernet* para ligação a redes da mesma tecnologia. Em fases posteriores da evolução do *Gigabit Ethernet*, à medida que as estações ligadas à rede local por intermédio de cartas *Fast Ethernet* ou FDDI, necessitem de maior largura de banda, cartas de interface (NICs - *Network Interface Cards*) podem ser usadas para interligar aquelas a um comutador ou repetidor *Gigabit Ethernet* (Figura 3.7).

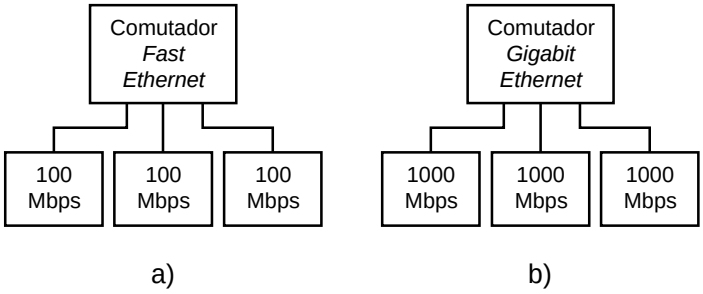


Figura 3.7 - Actualização de estações de trabalho de alto desempenho.

3.2.3 Limites de Segmentos e Repetidores na Norma IEEE 802.3

Como resumo, apresentam-se na Tabela 3.2 os comprimentos e velocidades máximos para as diferentes normas Ethernet.

3.3 Soluções não Ethernet

O fértil campo das comunicações de dados não se resume ao uso de apenas um protocolo de controlo de acesso ao meio. Um sem número de tecnologias, quer recentes quer já relativamente antigas, prolifera no sentido de possibilitar a troca de informação a ritmos elevados. Várias são as diferenças relativamente ao tipo de soluções Ethernet. Estas podem ser ao nível do protocolo de controlo de acesso ao meio, ou diferenças absolutamente radicais. O uso de pequenos pacotes (células) de informação (ATM) ou normas de ligações paralelas a interfaces de alto desempenho (HIPPI) possibilita o envio de informação a ritmos superiores ao gigabit por segundo.

Tabela 3.2 - Comprimentos máximos para as normas IEEE 802.3.

		Ethernet	Fast Ethernet	Gigabit Ethernet (esperado)
Taxa		10 Mbps	100 Mbps	1 Gbps
Cabo	UTP-5	100 m	100 m	25-100 m
	Repetidores	4	2	1
	STP	500 m	100 m	25-100 m
	Repetidores	4	2	1
	Coaxial	500 m	100 m	25-100 m
	Repetidores	4	2	1
	FO Multimodo	2 km	412 m	500 m
	FO Monomodo	25 km	20 km	2 km

3.3.1 100VG-ANYLAN

O grupo de trabalho IEEE 802 aprovou uma norma, conhecida por IEEE 802.12 (*Demand Priority Access Method*) [IEEE802.12] que visa a normalização de um método de controlo de acesso ao meio com um rendimento superior ao do CSMA/CD [Costa95]. Além de fornecer uma alternativa ao 100BASE-T, a proposta original foi estendida de modo a ser compatível com o formato de tramas do *Token-Ring*. A norma especifica uma topologia em Árvore, com ligações ponto a ponto entre cada estação e um concentrador (*HUB*). Na realidade, este concentrador não funciona como um repetidor, mas sim como um comutador de circuitos. O acesso ao meio também não segue os moldes do CSMA/CD, mas sim uma sequência de pedido e consequente disponibilização de canal (acesso condicionado centralizado).

O funcionamento do 100VG-AnyLAN assenta em três conceitos [VGAnyLAN]:

- Cada estação encontra-se ligada a um concentrador (ponto-a-ponto). Este concentrador agrupa funções de um comutador de circuitos.
- A transmissão à velocidade de 100 Mbps sobre um par de fios UTP de categoria 3 é cara e complexa, de modo que a proposta recomenda 4 pares de UTP-3, com transmissão simultânea em todos eles. Cada par transmite informação a 30 Mbps, com frequência fundamental de 15 MHz (Codificação NRZ, 5B6B). Como resultado, o preço e a complexidade dos adaptadores de rede reduz-se consideravelmente.
- Os formatos das tramas Ethernet ou *Token-Ring* mantêm-se. É alterado apenas o protocolo MAC. Não há possibilidade de adaptar o cabeçalho Ethernet para *Token-Ring* e vice versa; a comunicação é possível apenas entre estações que usam o mesmo formato.

Ao contrário do IEEE 802.3, o 100VG não impõe limites tão rígidos à distância entre estações [Rauch95]. Este facto resulta do abandono do CSMA/CD que, como se viu, perde rendimento com o aumento de distância e com o aumento de estações. As vantagens da eliminação do CSMA/CD são:

- Total eliminação de colisões. A largura de banda do meio é aproveitada de uma forma mais eficiente.
- A atribuição de prioridades permite que tráfego sensível a atrasos, como voz e vídeo em tempo real, não seja prejudicado. Este facto torna o 100VG adequado a aplicações multimédia.

O sistema de cabos permitido pelo 100VG-AnyLAN encontra resumido na Tabela 3.3.

Tabela 3.3 – Cablagem usada na norma IEEE 802.12.

Tipo de Cabo	Número de Pares	Comprimento
UTP-3, UTP-4, UTP-5	4	100 m
STP	2	150 m
Fibra multimodo	2 fibras	2000 m

A escolha deste tipo de rede implica a aquisição de novos adaptadores de rede, novos componentes de rede, nomeadamente, concentradores e equipamento de teste e instalação. O preço é comparável aos componentes 100BASE-T e consideravelmente inferiores a componentes ATM. A compatibilidade entre as propostas 100BASE-T e 100VG torna a estratégia de migração comparável.

As redes do tipo 100VG usam uma configuração de ligações em árvore (Figura 3.8).

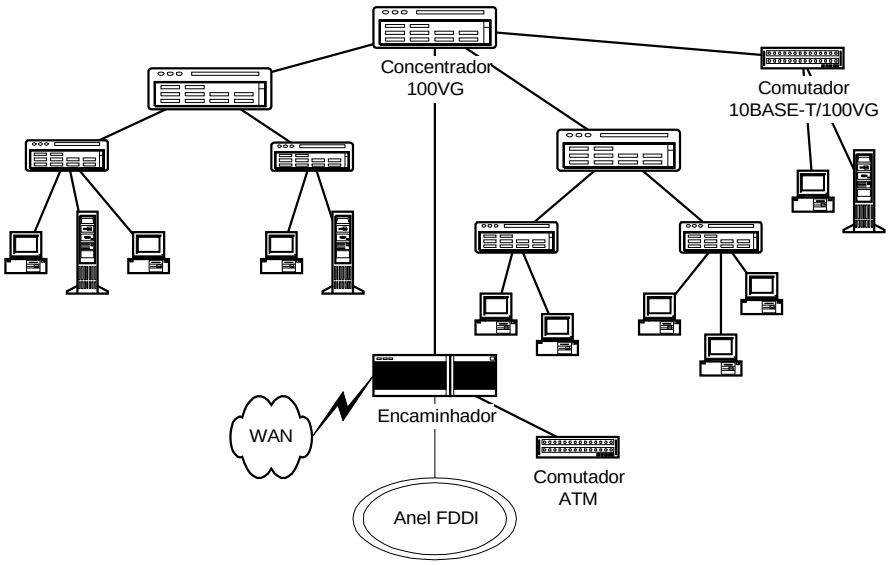


Figura 3.8 - 100vg-AnyLAN: Topologia em árvore.

Desde que todos os concentradores na mesma rede usem o mesmo tipo de tramas (Ethernet ou *Token-Ring*), uma estrutura 100VG pode conter até 7 níveis hierárquicos sem haver necessidade de uma ponte. Cada concentrador 100VG pode ser configurado para tramas Ethernet ou *Token-Ring*, embora não possa haver os dois tipos de trama numa única rede.

Cada nível adicional reduz a distância entre a raiz e a estação em 1,1 km [Costa95] (Tabela 3.4).

Tabela 3.4 – Distância máxima vs níveis hierárquicos.

Número de concentradores entre a raiz e a estação	Número de níveis	Distância máxima entre a raiz e a estação
1	2	6 km
2	3	4,9 km
3	4	3,8 km
4	5	2,7 km
5	6	1,6 km
6	7	500 m

Um nível hierárquico é definido pela existência de um concentrador. Por exemplo, uma rede com três níveis (dois concentradores entre a estação e a raiz) tem um comprimento máximo de 4,9 km (Figura 3.9).

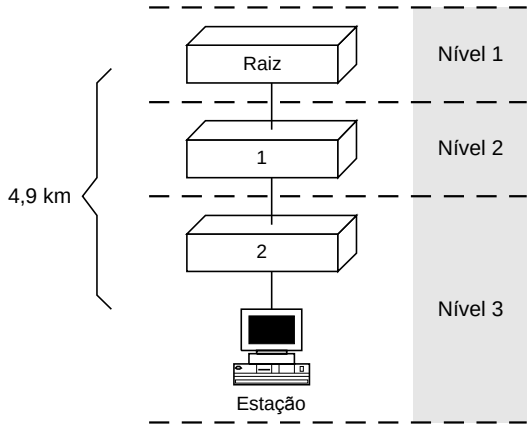


Figura 3.9 – Distância máxima entre a raiz e uma estação no nível 3.

No máximo, entre a raiz e o concentrador mais próximo da estação, são admitidos 6 concentradores em cascata. Por outro lado, o aumento do número de níveis hierárquicos implica, como consequência do atraso introduzido por cada concentrador, a diminuição da distância total entre a estação e a raiz.

A maior inovação introduzida no 100VG-AnyLAN é o protocolo MAC. Definido pela norma IEEE 802.12 (*Demand Priority*), o seu funcionamento não passa pelo uso de testemunhos e não existe qualquer tipo de colisão. O *Demand Priority* usa uma técnica baseada em convites (*polling*). Cada concentrador convida as estações a ele ligadas, segundo uma ordem *round-robin*, a ocuparem o canal de transmissão. Este esquema, concentra a inteligência no comutador ou no concentrador, simplificando a lógica em cada estação. Por outro lado, como cada estação encontra total disponibilidade do meio, não há ocorrência de colisões.

Quando uma estação necessita enviar algo para a rede, coloca um pedido no concentrador ou comutador. Este, por sua vez, serve cada estação em sequência. Se a estação tem dados para enviar, o acesso ao meio é garantido, em caso contrário, passa-se à estação seguinte. Em cada ciclo, cada estação pode transmitir um pacote, pelo que todas as estações são servidas. Em configurações com mais que um grau hierárquico, existem concentradores que necessitam de pedir acesso ao nível

imediatamente superior. Quando o acesso é garantido, este pode transmitir um pacote por cada estação ligada (Figura 3.10).

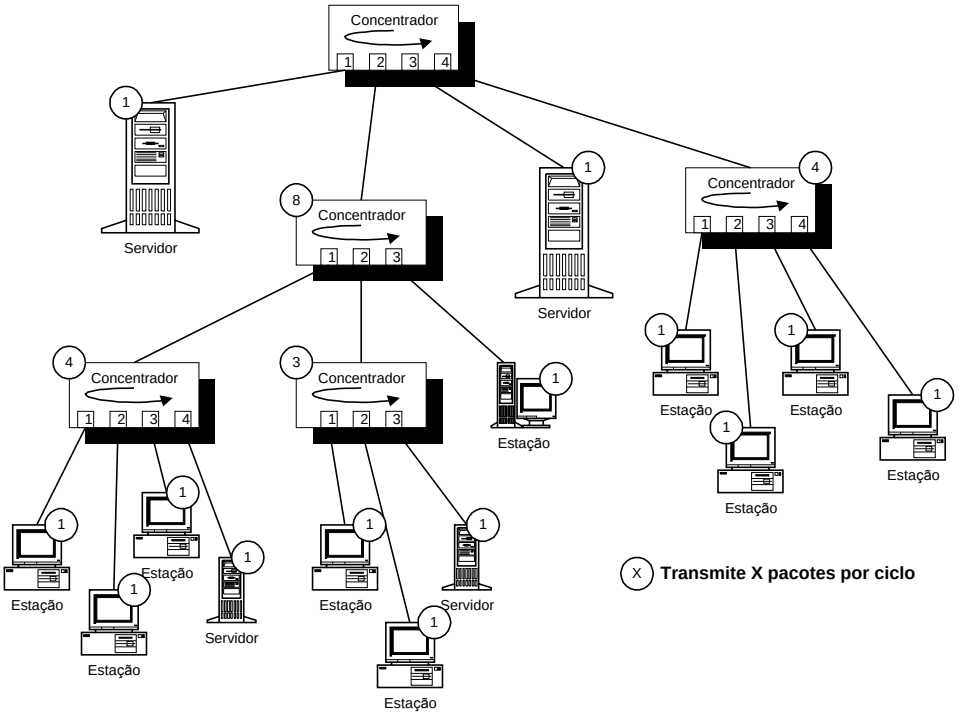


Figura 3.10 - Acesso *round-robin.*

Além da democratização do pedido de transmissão, foi implementado um sistema de prioridades. Para o efeito, são admitidos dois tipos de pacotes: alta prioridade e prioridade normal, que definem o respectivo nível de prioridade. O concentrador efectua o convite às estações com início na porta de menor ordem (*round-robin*). Se mais de uma estação deseja transmitir, o concentrador determina a ordem de transmissão com base em dois critérios:

- A prioridade (normal ou alta) do pedido.
- O número de ordem da porta respectiva.

Esta medida foi tomada com o objectivo de diminuir o tempo de atraso na transmissão de tráfego mais sensível a atrasos, como o vídeo ou a voz.

3.3.2 ATM (*Asynchronous Transfer Mode*)

O ATM surgiu, inicialmente, como a tecnologia de comutação base para a B-ISDN (*Broadband Integrated Services Digital Network*). Como sucessora da ISDN convencional, a B-ISDN é uma rede de telecomunicações adequada ao transporte de vários tipos de informação, gerada por uma multiplicidade de aplicações multimédia.

O transporte da informação é realizada de uma forma assíncrona, como o próprio nome indica. Técnicas de transporte síncronas são utilizadas em sistemas de transmissão de alto rendimento, como o SDH (*Synchronous Digital Hierarchy*) ou o seu equivalente americano, o SONET (*Synchronous Optical Network*). Os sistemas plesiócronos simulam a existência de um técnica síncrona pela reserva de recursos dedicados ao controlo de erros.

Em técnicas de transferência assíncronas, as tramas de informação são enviadas apenas quando for necessário. Se não houver informação a enviar, o meio é libertado para outras aplicações.

3.3.2.1 Transporte de Informação

A tecnologia ATM usa comutação de células (*cell relay switching*), uma técnica de multiplexagem estatística, na transmissão de informação.

Sendo uma evolução das técnicas de comutação de pacotes, como o X.25, o ATM possui a capacidade de transporte de informação sensível a atrasos, como a voz ou o vídeo. Ao contrário da comutação de circuitos, a multiplexagem estatística evita ocupar largura de banda com informação não relevante, como períodos de silêncio. No intervalo de tempo em que a ausência de informação ocorre, a capacidade do meio de transmissão é aproveitada por outros serviços/utilizadores.

O nome multiplexagem estatística provém da característica dos multiplexadores, que se baseiam na improbabilidade de todos os canais a eles ligados aguardarem transmissão. Nos casos em que o tráfego excede a capacidade de escoamento do multiplexador, por breves períodos de tempo, este envia a informação prioritária e armazena a excedente numa memória temporária (*buffer*). Se a situação se mantiver por períodos de tempo consideráveis, pode haver perda de informação.

Numa rede de comutação de pacotes "clássica", como o X.25 ou o *frame relay*, o tamanho do pacote encontra-se normalmente entre 128 e 4096 octetos. No ATM, cada célula (pacotes de dimensão reduzida) possui apenas 48 octetos de dados e 5 no cabeçalho. A pequena dimensão da célula permite diminuir o tempo de atraso na recepção de células consecutivas. Como consequência, o nível médio de qualidade de serviço aumenta (o tempo de espera por células consecutivas diminui).

O cabeçalho, embora impeça a utilização do canal com um rendimento de 100%, é fundamental para garantir o encaminhamento de cada célula (Figura 3.11).

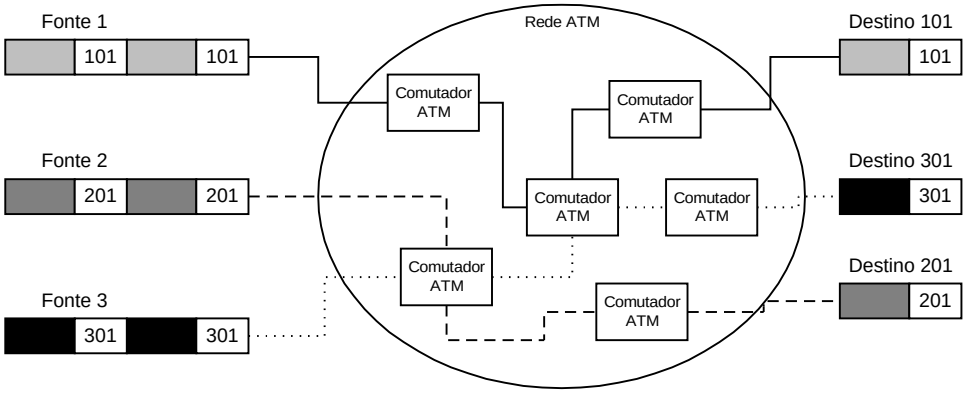


Figura 3.11 – Encaminhamento de células numa rede ATM.

O endereço dos intervenientes na comunicação é definido apenas quando a ligação é efectuada. Consegue-se, desta forma, um melhor aproveitamento da capacidade de endereçamento de uma rede ATM: este não é feito com base no número de ligações na rede, que podem ser milhões, mas sim com base no número de ligações activas, um número sempre inferior.

As ligações numa rede ATM são criadas como canais virtuais. Estas, por sua vez, são decompostas em secções denominadas ligações de caminho virtual.

3.3.2.2 Formato da Célula

Os vários canais e caminhos definidos no início da ligação, são identificados por números no cabeçalho (Figura 3.12) das células de ligações activas. Cada número é denominado identificador de canal virtual (VCI – *Virtual Channel Identifier*) e identificador de caminho virtual (VPI – *Virtual Path Identifier*).

8	7	6	5	4	3	2	1	bit / octeto
VPI (entre comutadores)				VPI				1
VPI				VCI				2
VCI								3
VCI				PT			CLP	4
HEC								5

Figura 3.12 – Estrutura do cabeçalho de uma célula ATM.

O cabeçalho de uma célula ATM ocupa 40 bits, dos quais 28 são usados na identificação de caminhos e canais virtuais (campo de encaminhamento). Outros campos, como o PT (*payload type*) assinala o tipo de informação da célula. O campo CLP (*Cell Loss Priority*) define o "tempo de vida" da célula. O campo HEC (*Header Error Control*) é usado na detecção e/ou correcção de erros no cabeçalho da célula.

3.3.2.3 Arquitectura

As normas ATM especificam a arquitectura protocolar de rede como composta por um conjunto de camadas, cada qual com a sua função (Figura 3.13) [Clark96].

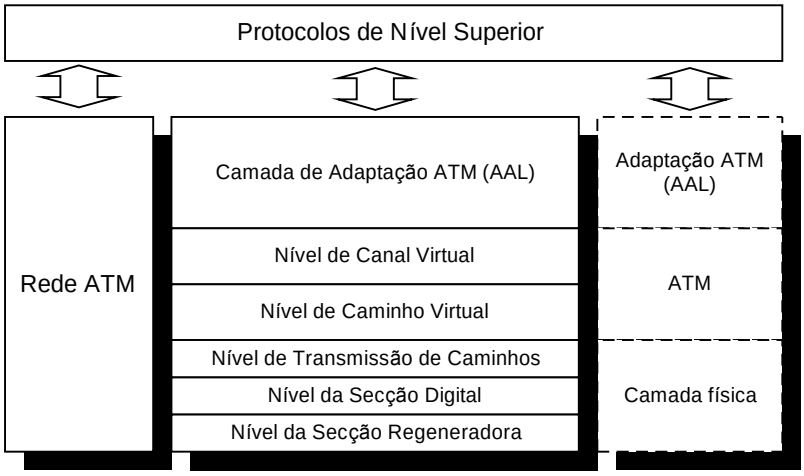


Figura 3.13 – Estrutura hierárquica de uma rede ATM.

A camada física define as características eléctricas, ópticas e de transmissão que a camada ATM usa. Esta, por sua vez, define o formato da célula e a metodologia seguida na transmissão de células sobre a rede. A camada AAL, ou seja, de adaptação, especifica como as células são usadas por forma a criar ligações adequadas ao tipo de

serviço (transporte de voz, transmissão de dados, fluxo contínuo de dados, etc.) [Schröder94].

3.3.2.4 ATM em Redes Locais

Existe, actualmente, uma necessidade de maior largura de banda ao serviço de estações de trabalho, servidores de ficheiros, servidores de impressão ou mesmo alguns sistemas terminais.

Uma das principais razões que tornam o ATM atractivo em redes locais reside nas taxas de transferência de informação conseguidas. O ATM encontra-se especificado para velocidades que vão desde as poucas dezenas de Mbps até aos 100, 155 ou 622 Mbps. Prevê ainda velocidades de 1,2 Gbps e 2,4 Gbps. Estas taxas encontram-se acima das mais utilizadas em redes locais, como os 10 Mbps do Ethernet ou 100 Mbps do FDDI. A própria rede ATM pode integrar tráfego proveniente de qualquer fonte, como por exemplo, voz proveniente do telefone de secretária e o tráfego de dados proveniente da estação de trabalho.

Em termos de topologia, as comunicações ATM podem ser de dois tipos [Stallings95]:

- Ponto-a-ponto: Este tipo de ligações é normalmente utilizado para interligar equipamento ATM, podendo operar em modo unidireccional ou bidireccional.
- Ponto-a-multiponto: As comunicações deste tipo são utilizadas para a interligação de um equipamento central a vários sistemas terminais. A replicação de células é realizada ao nível dos comutadores ATM.

Ao contrário do que acontece em redes Ethernet, o ATM é uma tecnologia orientada à conexão. Estabelece ligações virtuais entre duas (ponto-a-ponto) ou mais (ponto-a-multiponto) entidades. Cada ligação é identificada pelos campos VCI (*Virtual Channel Identifier*) e VPI (*Virtual Path Identifier*) no cabeçalho de cada célula. Uma vez que, de forma geral, as redes locais não são orientadas à conexão (*connectionless*) e usam um protocolo específico para identificar cada estação (MAC), há necessidade de um mecanismo que relacione os endereços MAC com os identificadores ATM [Black95].

3.3.3 FDDI (*Fibre Data Distributed Interface*)

A publicação da norma em que se baseia o FDDI remonta já ao ano de 1987. A sua principal utilização tem sido como suporte de ***backbone*** de algumas instituições, principalmente devido aos 100 Mbps que disponibiliza. Em adição, devido ao facto de usar cabos de fibra óptica numa configuração em anel, permite abranger uma extensa área geográfica. Por outro lado, a tecnologia óptica é relativamente cara, o que torna difícil, a curto prazo, a sua extensão directamente a todas as estações de trabalho. Nestas situações, o 100VG-AnyLAN ou o ***Fast Ethernet*** apresentam um preço substancialmente inferior para um desempenho semelhante em termos de velocidade.

O esquema de passagem de testemunho sobre uma topologia em anel é em tudo semelhante ao ***Token-Ring***. O FDDI é composto por quatro componentes [ANSIX3.139] (Figura 3.14):

- Camada MAC (*Medium Access Control*) – define informação de endereçamento, calendarização e encaminhamento. Fornece serviços a protocolos de nível superior, como o IP, IPX ou DECnet. Aceita tramas com comprimento até 9000 octetos.
- Camada PHY (*Physical*) – realiza a codificação e descodificação da trama MAC numa sequência de símbolos que entrega à camada inferior. É responsável pelo sincronismo no anel.
- Camada PMD (*Physical Media Dependent*) – realiza a transmissão sobre um de dois meios: fibra ou cobre.
- Camada SMT (*Station Management*) – ocupa-se da gestão efectiva do anel. As suas funções incluem: identificação da estação vizinha, detecção de anomalias, reconfiguração, detecção de inserção e remoção de estações do anel e monitorização de estatística de tráfego.

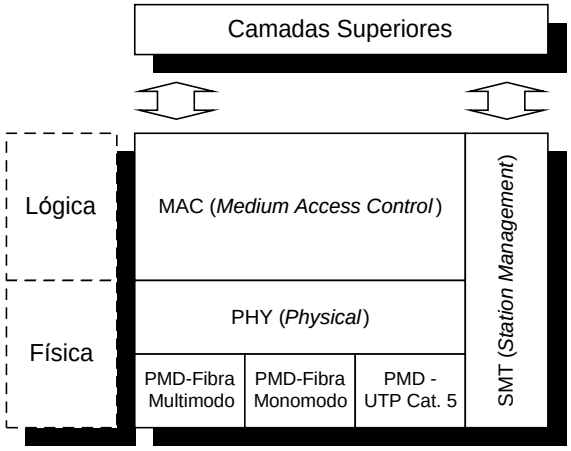


Figura 3.14 – Componentes chave da arquitectura FDDI.

O FDDI pode ser instalado sob a forma de um anel duplo e/ou baseado em concentradores [Jain94]. No primeiro caso, as estações encontram-se directamente interligadas. Em caso de anomalia, a comunicação é realizada com o auxílio da segunda via. Se, eventualmente, acontecer uma segunda anomalia, o anel é segmentado em dois anéis distintos, não sendo possível a comunicação entre eles. No segundo caso, cada estação encontra-se ligada a um concentrador, que isola a estação afectada em caso de anomalia. Os concentradores tornam a rede mais robusta, além de permitir uma melhor gestão.

O diâmetro de uma rede refere-se à distância máxima que separa duas estações sem necessidade de encaminhadores ou pontes. No caso do FDDI, o uso de fibra óptica permite ter anéis com um diâmetro máximo de 200 km. O número de estações ligadas pode atingir as 500. Para meio em cobre, a distância entre estações reduz-se a cerca de 100 m [Mills95].

3.3.3.1 FDDI-II

O FDDI não mostrou ser adequado para o transporte de informação sensível a atrasos. Para o efeito, a organização responsável pelo FDDI decidiu criar uma norma mais adequada a tráfego multimédia, a que se deu o nome de FDDI-II [Jayasumana94].

A afirmação do ATM é já uma realidade e revela-se mais flexível no transporte de voz, vídeo e dados que o FDDI-II. Este facto tem levado ao sucessivo abandono do FDDI-II [Restivo95].

3.3.4 Fibre Channel

O *Fibre Channel* é uma tecnologia que permite o transporte de informação a alta velocidade [FibreChannel]. É desta que o *Gigabit Ethernet* herda a tecnologia de transmissão para velocidades elevadas. O *Fibre Channel* estabelece uma base de suporte a uma multiplicidade de protocolos de rede. A tecnologia emprega velocidades de transferência de informação desde os 100 Mbps até ao 1 Gbps, esperando-se para breve velocidades superiores. Sobre fibra óptica, pode unir dois pontos com 10 km de separação.

3.3.4.1 Arquitectura

O *Fibre Channel* encontra-se estruturado em cinco camadas, cada uma com a sua responsabilidade [Frymoyer95] (Figura 3.15).

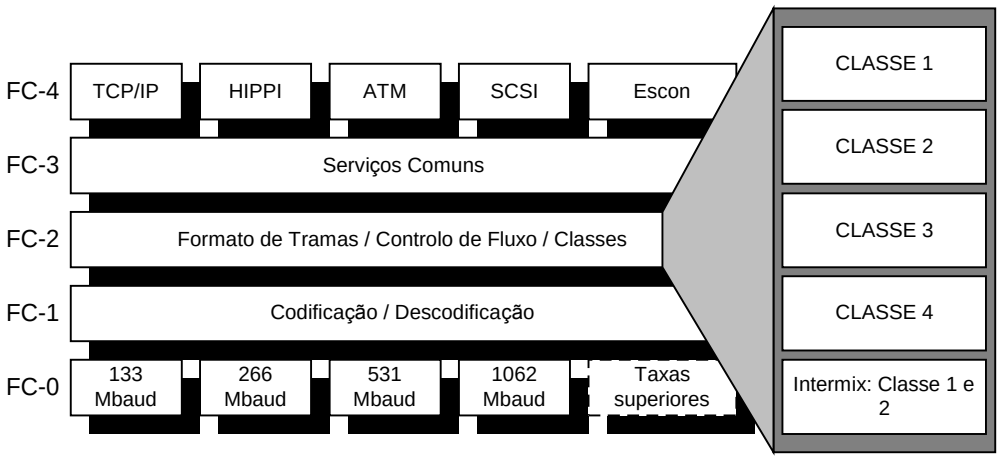


Figura 3.15 – Cinco camadas do *Fibre Channel*.

- FC-0: define taxas de transmissão.
- FC-1: codificação e descodificação dos dados. Usa uma codificação 8B/10B.
- FC-2: efectua sinalização essencial, formatação de tramas e define o mecanismo de transporte para os dados entregues pela camada superior e vice-versa. Efectua, ainda, funções de gestão tais como controlo de fluxo, gestão de ligações, memória e detecção de erros.
- FC-3: define mecanismos e funções de organização e divisão de dados provenientes de um conjunto de fontes diferentes.
- FC-4: define interfaces com vários protocolos de nível superior.

A camada FC-2 é onde grande parte do processamento é realizado. Os serviços de transporte fornecidos por esta camada encontram-se divididos em classes, o que permite satisfazer uma multiplicidade de requisitos de comunicação. Cada classe define os serviços seguintes:

- **Classe 1**: Comutação de circuitos – específica para transmissão de dados muito sensíveis a atrasos.
- **Classe 2**: Comutação de pacotes com confirmação – não há ligação estabelecida a não ser ao nível de pacotes.
- **Classe 3**: Comutação de pacotes sem confirmação – semelhante à Classe 2 mas, se uma transmissão não chega ao receptor, o pacote não é retransmitido.
- **Classe 4**: Orientada à conexão – define um caminho virtual com uma largura de banda garantida e um tempo de latência fixo.
- **Intermix**: Em adição, o *Fibre Channel* pode usar uma combinação entre as Classes 1 e 2. Essencialmente, a Classe 1 é usada excepto quando não há transmissão de pacotes. Neste caso, é usada a Classe 2.

3.3.4.2 Topologia

As ligações podem ser ponto-a-ponto, em meio partilhado ou comutado. O tipo de ligação é perfeitamente transparente para os componentes interligados. As ligações em meio partilhado fornecem um meio barato de interligação sem necessidade de concentradores ou comutadores. A largura de banda pode ser partilhada por uma máximo de 127 estações. Quando uma delas quer transmitir, é reservado o meio, escolhida a classe adequada e a transmissão efectuada. No fim de transmissão o meio é libertado [ANSIX3.230].

O uso de comutadores oferece grande versatilidade e desempenho. O tipo de comutação depende da classe designada, podendo ser efectuada a comutação de circuitos, em que há definição de uma ligação dedicada entre estações, ou comutação de pacotes, em que cada trama é processada e encaminhada de forma individual.

A arquitectura modular e os diferentes serviços disponibilizados pelo *Fibre Channel* permitem o transporte de diferentes protocolos, quer antigos, quer recentes com altas taxas de transferência.

3.3.5 HIPPI (*High Performance Parallel Interface*)

O sistema HIPPI surgiu como uma norma de comunicação de débitos elevados entre supercomputadores e respectivos periféricos [ANSIX3.183]. As velocidades de comunicação encontram-se especificadas para os 800 Mbps e 1,6 Gbps sobre cobre ou fibra óptica.

A distância máxima entre estações depende do tipo de meio e da velocidade de transmissão, podendo atingir os 50 m sobre cobre, 300 m sobre fibra multimodo e 10 km sobre fibra monomodo [HIPPI].

Actualmente existe um esforço por parte das entidades normalizadoras para introduzir o HIPPI no domínio das redes locais. A simplificação da gestão, com a criação de uma HIPPI MIB e a integração do HIPPI em ferramentas como o **Openview** da HP ou o **Netview** da IBM e o desenvolvimento de métodos de adaptação entre o HIPPI e outras tecnologias de LAN ou WAN, como o ATM, o *Fibre Channel* ou SONET (*Synchronous Optical Network*) são vertentes que não foram descuidadas.

3.3.5.1 Arquitectura

As características mais importantes do HIPPI podem ser resumidas nos seguintes pontos [Tolmie95]:

- Taxas de transferência elevadas: 800 Mbps ou 1,6 Gbps, tanto *simplex* como *duplex*.
- Sequências de sinalização simples: uma ligação HIPPI necessita apenas três mensagens – `REQUEST`, `CONNECT` e `READY`.
- Ligações baseadas em comutação de circuitos: cada comutador mantém um número de ligações independentes a velocidades de 800 Mbps ou 1,6 Gbps.
- Compatibilidade com cobre e fibra: HIPPI usa cabo STP de 50 pares para um comprimento máximo de 25 m. Admite fibra óptica multimodo ou monomodo para áreas metropolitanas ou SONET para comunicação a longas distâncias.

A topologia usada é uma estrela, com um comutador HIPPI como nó central. O número máximo de comutadores em cascata é de oito, pelo que se conseguem comprimentos máximos de 200 m sobre cobre.

3.3.5.2 Aplicação em LAN

A sinalização usada em HIPPI permite a criação e destruição de ligações em menos de 1 μs. Este tempo, apesar de representar uma comutação de circuitos é perfeitamente desprezável face ao tempo que as estações demoram a processar a trama recebida. O uso de HIPPI em LANs encontra-se especificado em [RFC2067].

Tráfego gerado por aplicações multimédia não sofre qualquer tipo de atraso, uma vez que lhe é atribuído um canal inteiramente dedicado.

3.3.6 Estudo Comparativo de Soluções Não Ethernet

Apresenta-se, na Tabela 3.5, um estudo comparativo entre as diferentes tecnologias apresentadas. Para cada tipo de cabo, são apresentados o número máximo de nós, a velocidade de transferência e a distância entre nós.

3.4 Conclusões

O Ethernet constitui uma tecnologia relativamente antiga. Desde a sua origem sofreu actualizações e melhoramentos que tornaram possível a sua utilização até aos dias de hoje. É provável que o rumo seguido pelo mercado das redes locais de comunicação de dados privilegie este modelo.

No entanto, o método de controlo de acesso ao meio CSMA/CD não se apresenta adequado a certas aplicações. As tecnologias alternativas geralmente oferecem excelentes soluções alternativas. O 100VG-AnyLAN apresenta um custo comparável ao *Fast Ethernet* e admite um maior numero de concentradores em cascata, assim como um maior afastamento entre as extremidades da rede. O ATM, o *Fibre Channel* e o HIPPI revelam-se mais eficientes na transmissão de tráfego multimédia, com tempos de atrasos consideravelmente inferiores. Como pontos desfavoráveis apresentam o custo elevado e o parque de utilização reduzido.

Toda esta diversidade tecnológica apresenta um vasto leque de escolha ao utilizador, que deve orientar a sua opção de acordo com a situação particular que visa resolver.

Tabela 3.5 – Resumo soluções não Ethernet.

Cabo	100VG	ATM	FDDI	Fibre Channel	HIPPI
UTP – 5	7 concentradores	Comutador*	500 nós	127 concent.	-
	100 m (4 pares)	100 m	100 m	24 m	-
	100 Mbps	25 – 155 Mbps	100 Mbps	1 Gbps	-
STP	7 concentradores	Comutador*	500 nós	127 concent.	8 comutadores
	150 m (2 pares)	100 m	100 m	1 Gbps	25 m (50 pares)
	100 Mbps	25 – 622 Mbps	100 Mbps	24 m	0,8 – 1,6 Gbps
Coaxial	-	-	-	24 m	-
FO Multim.	7 concentradores	Comutador*	500 nós	127 concent.	8 comutadores
	2000 m	300 m	2000 m	1 Gbps	1000 m
	100 Mbps	25 – 622 Mbps	100 Mbps	300 m	0,8 – 1,6 Gbps
FO Monom.	7 concentradores	Comutador*	500 nós	127 concent.	8 comutadores
	2000 m	15 km	40 - 60 km	1 Gbps	10 km
	100 Mbps	25 – 622 Mbps	100 Mbps	10 km	0,8 – 1,6 Gbps

* Não há limite para o número de nós.

4 ARQUITECTURAS DE GESTÃO

4.1 Introdução

A instalação de uma rede local de comunicação de dados segue um conjunto de etapas que visam o estabelecimento de uma infra-estrutura que permita efectuar, de forma eficiente, a troca de informação entre diversos utilizadores. A primeira etapa é constituída por uma fase de estudo seguida do planeamento da infra-estrutura. A respeito da infra-estrutura, é necessário considerar os aspectos físicos de transmissão, tais como o tipo de cabos e o tipo de topologia a utilizar. No Apêndice A apresenta-se um estudo que visa esclarecer possíveis dúvidas e auxiliar a normalização da estrutura de comunicações. Segue-se a instalação de equipamento e de aplicações que permitam operar a rede de comunicação. Após instalação a rede fica apta a prestar serviços de comunicação de dados aos seus utilizadores. Decorrente deste estudo, foi feita uma proposta de actualização de rede do Departamento de Electrónica e Telecomunicações da Universidade de Aveiro (Apêndice B).

Os rápidos avanços tecnológicos aliados ao crescimento das necessidades de comunicação tornam essencial a actualização da rede de comunicação. Por outro lado, o número de utilizadores não se mantém constante ao longo do tempo e as aplicações, tal como a tecnologia, sofrem uma evolução constante. Em resumo, uma rede de comunicação de dados constitui um sistema dinâmico e, como tal, é natural o aparecimento de problemas de funcionamento que podem afectar ou mesmo interromper o fluxo de informação.

Face a este problema, surge a necessidade de reduzir ao mínimo o tempo em que a rede se encontra inoperacional. Esta constitui a fase de manutenção/administração e consiste na monitorização do estado de funcionamento, detecção de problemas e consequente correcção. À medida que a rede vai crescendo e estabilizando a importância relativa da administração face à instalação resulta num maior esforço de desenvolvimento e instalação de aplicações de gestão (Figura 4.1).

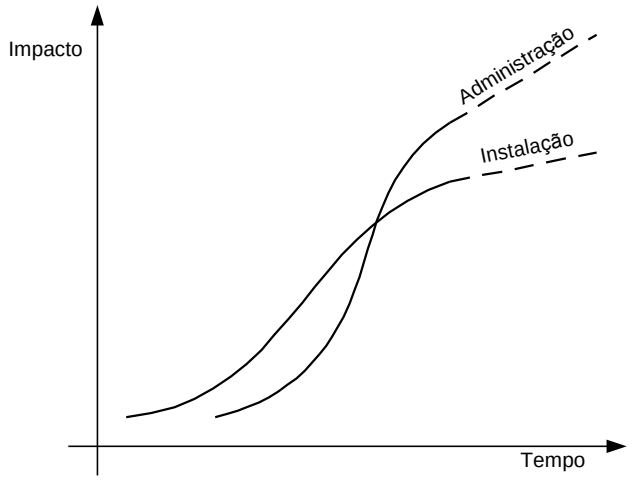


Figura 4.1 - Impacto relativo Instalação/Administração.

A administração casualmente baseada apenas no esforço humano deu lugar a sistemas de gestão proprietários. As estratégias comuns a fabricantes dos sistemas resultaram na formulação de normas.

Actualmente, as arquitecturas de gestão de redes estão fortemente polarizadas em torno de três soluções que serão discutidas neste capítulo: gestão OSI (*Open Systems Interconnection*), gestão SNMP (*Simple Network Management Protocol*), gestão TMN (*Telecommunications Management Network*).

4.2 Modelo de Gestão

A administração, ou gestão, de uma rede local é efectuada de forma a prever, identificar e corrigir falhas de funcionamento. As operações básicas efectuadas por um sistema deste tipo podem ser agrupadas em:

- Recolha de informação de gestão.
- Processamento de informação de gestão.
- Realização de acções correctivas.

O modelo típico de um sistema de gestão é constituído por várias entidades com funções distintas (Figura 4.2). Uma das entidades previstas pelo modelo desempenha funções de instrumentação, no sentido em que recolhe parâmetros de funcionamento de um componente, de um conjunto de componentes ou da própria infra-estrutura de comunicação. Esta entidade é tradicionalmente denominada Agente. Os agentes são dotados de mecanismos de recepção e resposta a comandos, gerados por uma outra entidade. Em certas ocasiões têm a possibilidade de gerar notificações de forma autónoma, reflectindo algum acontecimento anómalo.

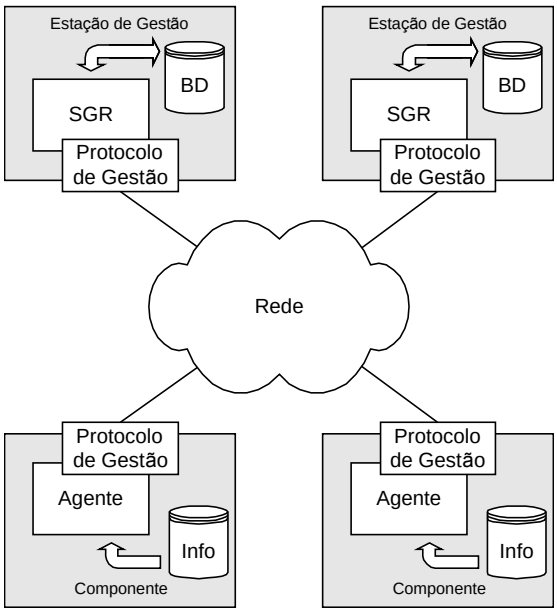


Figura 4.2 – Modelo simplificado de um sistema de gestão de redes.

A informação recolhida pelos agentes é geralmente processada por uma outra entidade gestora (ou entidades), denominada muitas vezes Sistema de Gestão de Redes (SGR) ou *Network Management System* (NMS). O SGR reflecte o estado de

funcionamento da rede numa interface, que pode ser gráfica, e apresenta ferramentas que permitem a visualização, de forma abstracta, da rede em análise. O SGR apresenta, tipicamente, mecanismos de geração de comandos e de recepção de notificações.

A troca de notificações e de comandos entre entidades de gestão é efectuada segundo um protocolo específico, o protocolo de gestão. Por outro lado, a informação trocada representa vários parâmetros de funcionamento, relativos a uma entidade específica, um conjunto de entidades ou à própria infra-estrutura de comunicação.

Este modelo simplificado é partilhado pelas três arquitecturas seguintes.

4.3 Modelo de Gestão OSI

A ISO (*International Standards Organisation*), com a colaboração do ITU-T (*International Telecommunications Union Telecommunication Standardisation Sector*, ex-CCITT), desenvolveu um trabalho pioneiro na normalização de redes locais de comunicação de dados. Um dos resultados deste trabalho foi o modelo de referência de redes OSI (*Open Systems Interconnection*) [ISO7498].

As directivas de gestão foram estabelecidas por [ISO7498-4], mais tarde complementadas por [ISO10040]. Um resumo dos documentos normativos enquadrados no trabalho de gestão OSI pode ser encontrado em [Langsford94]. Os documentos propõem uma divisão das tarefas de gestão nas seguintes áreas funcionais:

- Gestão de Falhas – agrupa os mecanismos que permitem detectar, isolar e corrigir funcionamentos anómalos.
- Contabilização e Gestão de Recursos – contém mecanismos que permitem o estabelecimento de custos de utilização de recursos da rede.
- Gestão de Configuração – mecanismos de controlo, identificação e consulta de dados necessários à operação dos dispositivos de ligação.
- Gestão de Desempenho – mecanismos de avaliação de comportamento e de eficiência da comunicação.
- Gestão de Segurança – segurança genérica dos sistemas de comunicação.

4.3.1 Modelo de Informação

A estrutura de informação de gestão (SMI – *Structure of Management Information*) é definida seguindo uma metodologia orientada ao objecto. Consegue-se, desta forma, utilizar os conceitos de classe, objecto, herança, encapsulamento, método, atributo na definição dos objectos de gestão. A ISO estabeleceu um conjunto de formalismos, conhecidos por GDMO (*Guidelines for the Definition of Managed Objects*) [ISO10165] com a finalidade de especificar os objectos de gestão. Esta consiste numa linguagem com a função de especificar classes de objectos, o seu comportamento, atributos e herança. Apesar de semelhante ao SMI do SNMP, o formato GDMO não é derivado do ASN.1, embora o utilize para a definição da sintaxe e codificação dos atributos.

Os objectos de gestão são representações lógicas de entidades físicas ou recursos associados a um sistema ou subsistema. Estes são organizados por classes, que definem as características comuns de um conjunto de objectos. Cada objecto reflecte continuamente o estado de uma determinada entidade, por intermédio dos valores armazenados nos seus atributos. Por outras palavras, os objectos de gestão definem uma fronteira lógica entre a entidade em causa e os mecanismos de gestão (Figura 4.3).

A identificação de cada objecto de gestão é efectuado por intermédio de um identificador de objecto (OID – *Object Identifier*). Este especifica todos os aspectos inseridos no modelo de gestão OSI (tais como classes, objectos, atributos, operações, notificações e documentos).

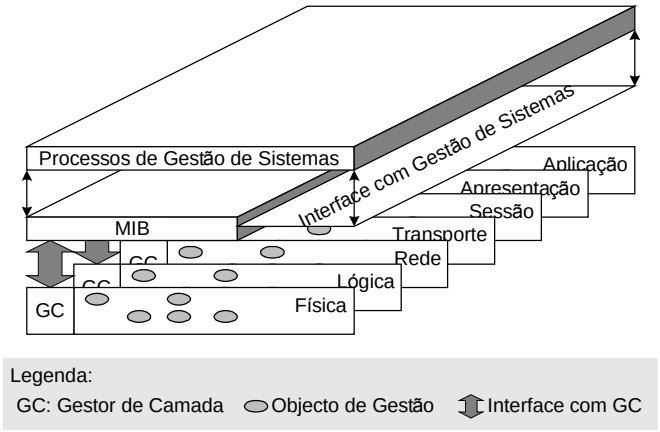


Figura 4.3 – Modelo da Informação de Gestão.

4.3.2 Modelo de Comunicações

O protocolo de gestão encontra-se especificado na camada de aplicação do modelo OSI e define conjunto de regras para a transferência de informação entre sistemas (Figura 4.4).

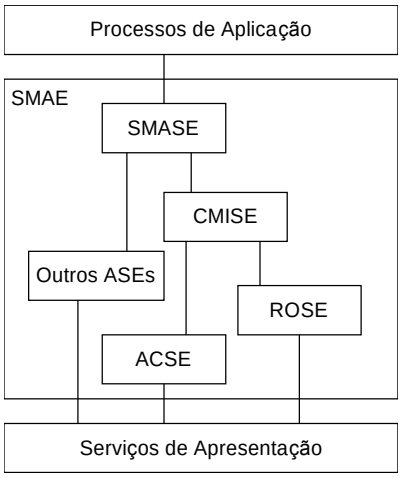


Figura 4.4 – Modelo de Comunicação.

O protocolo de gestão no contexto OSI é o *Common Management Information Protocol* (CMIP) [Stallings93]. Os serviços de informação de gestão são utilizados para troca de informação e de comandos que sejam relevantes para a gestão do sistema. Neste cenário, os serviços comuns de informação de gestão (CMIS) podem ser de dois tipos: de operação e de notificação de eventos (`M-EVENT-REPORT`). A notificação de eventos pode ser confirmada ou não confirmada (Tabela 4.1).

Tabela 4.1 – Serviços comuns de informação de gestão.

Serviço CMIS	Tipo
M-GET	Confirmado
M-CANCEL-GET	Confirmado
M-SET	Ambos
M-ACTION	Ambos
M-CREATE	Confirmado
M-DELETE	Confirmado
M-EVENT-REPORT	Ambos

4.4 SNMP

O crescimento da Internet em termos de equipamento interligado, diversidade de protocolos e aplicações tornou indispensável a criação de mecanismos organizados de gestão. A comunidade Internet, seguindo um caminho diferente do adoptado pela ISO, decidiu normalizar soluções só depois de suficientemente testadas e aceites.

No final da década de 80, a necessidade de manter bons níveis de funcionamento em qualquer rede local de comunicação de dados fomentou o aparecimento de algumas soluções de gestão. Exemplos são o HEMS/HEMP (*High-level Entity Management System* [RFC1021] / *High-level Entity Management Protocol* [RFC1022]), o CMOT (CMIP over TCP/IP) [RFC1189] e o SNMP [RFC1157]. Este último foi escolhido como uma solução provisória, sendo prevista a sua substituição pelo CMOT assim que possível. Na realidade, os atrasos sucessivos aliados à falta de aceitação que o modelo de gestão OSI sofreu levaram o CMOT ao abandono.

O SNMP é, hoje em dia, a escolha preferencial para a gestão de redes locais de comunicação de dados. Três documentos constituem a base do Sistema de Gestão de Redes da Internet (*Internet-standard Networking Management Framework*). Estes documentos definem os seguintes mecanismos essenciais:

- Um conjunto de regras que descrevem a informação de gestão [RFC1155].
- Um conjunto inicial de agentes de gestão [RFC1156].
- O protocolo usado na troca de informação [RFC1157].

O total de páginas não chega a 150, embora seja suficiente para permitir o desenvolvimento imediato de produtos nesta área.

A experiência adquirida no desenvolvimento de aplicações e agentes mostrou detalhes pouco claros ou mesmo ausentes nos vários documentos apresentados. Quanto mais implementações do SNMP apareciam, mais variações de interpretação surgiam. Esta situação tornou desejável uma evolução, evolução esta que nem sempre se revelou

isenta de controvérsia. Por outro lado, a falta de assentimento em torno do modelo de gestão OSI abria caminho à consolidação das soluções baseada em SNMP. Até agora, o termo SNMP acabou por vingar como designação genérica para o modelo de gestão.

Desde 1990 foram desenvolvidas diversas versões do SNMP:

- SNMPv1 - (*full*) a versão original e que continua a ser, em termos de mercado, a mais utilizada [RFC1157].
- SNMPsec - (*historic*) foi uma primeira tentativa de adicionar mecanismos de segurança ao SNMPv1 [RFC1351], [RFC1352], [RFC1353]. Foi posteriormente abandonada (historic).
- SNMPv2p - (*historic*) introdução de novos métodos de acesso e nova tentativa de dotar o SNMP de medidas de segurança, com base no conceito de perfis (*party-based*) [RFC1441], [RFC1445], [RFC1446], [RFC1448], [RFC1449].
- SNMPv2c - (*experimental*) tentativa de combinação das operações do SNMPv2 com o modelo de segurança do SNMPv1 (conceito de comunidade) [RFC1901], [RFC1905], [RFC1906].
- SNMPv2u - (*experimental*) segurança baseada na identificação de utilizadores (*user-based*) aliada às operações disponibilizadas pelo SNMPv2 [RFC1905], [RFC1906], [RFC1909], [RFC1910].
- SNMPv2* - (*experimental*) tentativa de unificar as características do SNMPv2p e do SNMPv2u [SNMPv2*].
- SNMPv3 - (*proposed*) resulta numa combinação da segurança baseada em utilizadores e as operações definidas para o SNMPv2p. A segurança é baseada numa actualização do SNMPv2u e SNMPv2* [RFC2271], [RFC2272], [RFC2273], [RFC2274], [RFC2275].

Desde a primeira versão, as versões que lhe seguiram nunca atingiram o grau de aceitação desejado (Figura 4.5).

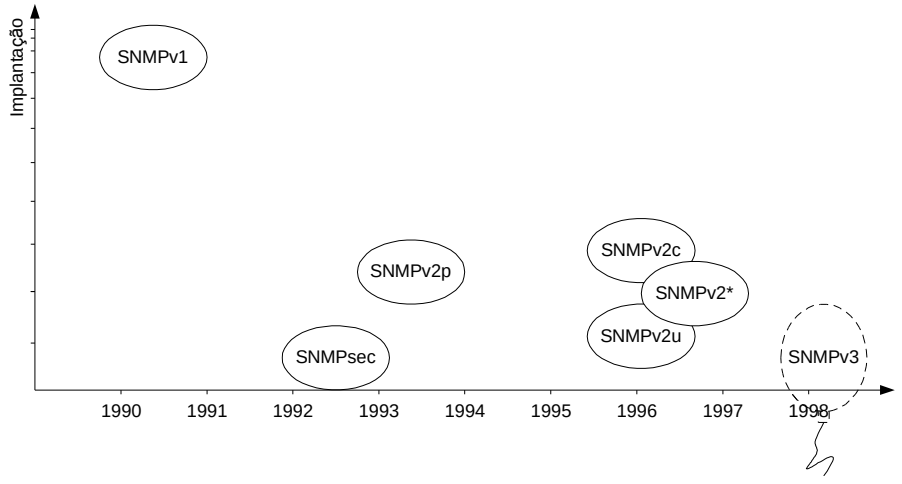


Figura 4.5 – Impacto das diferentes versões do SNMP.

O modelo de gestão SNMP especifica uma estrutura de informação de gestão (SMI – *Structure of Management Information*), que define um formato para objectos de

gestão acedidos por intermédio de um protocolo (SNMP). Actualmente há duas versões do SMI: SMIv1 [RFC1155], [RFC1212], [RFC1215] e SMIv2 [RFC1902], [RFC1903], [RFC1904].

4.4.1 Representação da Informação

O formato de representação digital de uma estrutura de dados depende fortemente da linguagem de programação usada, do compilador e da arquitectura da máquina. Com a finalidade de tornar a comunicação independente destes parâmetros, a troca de informação entre sistemas é feita com base em dois conceitos [Rose96]:

- Representação abstracta: cada tipo de dados da camada de aplicação é descrito segundo uma notação independente do sistema.
- Representação concreta: a representação abstracta é codificada de acordo com regras predefinidas e que são do conhecimento dos interlocutores da comunicação.

A notação utilizada para representar de forma abstracta tipos de dados numa rede Internet é um subconjunto da *Abstract Syntax Notation One* (ASN.1) [ISO8824]. Por sua vez, esta descrição é codificada segundo um conjunto de regras, as *Basic Encoding Rules* (BER) [ISO8825], definidas para a ASN.1, de modo a permitir a transmissão inequívoca de informação. As BER são aplicadas sob a forma de um algoritmo recursivo que produz uma codificação em octetos para cada valor ASN.1.

Cada tipo ASN.1 é codificado em três campos (Figura 4.6):

- Etiqueta, indicadora do tipo ASN.1.
- Comprimento, indicador do tamanho da codificação do valor ASN.1 que segue.
- Valor, contendo a codificação do valor ASN.1.

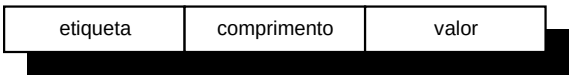


Figura 4.6 - Campos existentes numa codificação BER de um tipo de dados ASN.1.

Existe uma certa controvérsia quanto ao uso das BER. Geram, tipicamente, codificações compactas mas pouco eficientes em termos computacionais. O uso de BER e ASN.1 implica dotar os agentes de uma maior sobrecarga de processamento.

4.4.2 Estrutura da Informação de Gestão

A informação transmitida é armazenada em bases de informação de gestão (MIB - *Management Information Base*) [RFC1156], armazém virtual de informação de gestão. A MIB encontra-se estruturada segundo a SMI (*Structure of Management Information*) [RFC1155]. A sua função é permitir a descrição da informação de gestão de uma forma independente dos detalhes de implementação. Esta é definida usando ASN.1 mas permite apenas quatro tipos de variáveis: `INTEGER`, `OCTET STRING`, `SEQUENCE`, `SEQUENCE OF`. Os objectos, descritos segundo um conjunto de parâmetros [RFC1212], estão divididos em grupos e associados a identificadores (OID - *Object Identifier*). Este identificador é construído por associação dos números dos diversos nós de uma hierarquia em árvore (Figura 4.7).

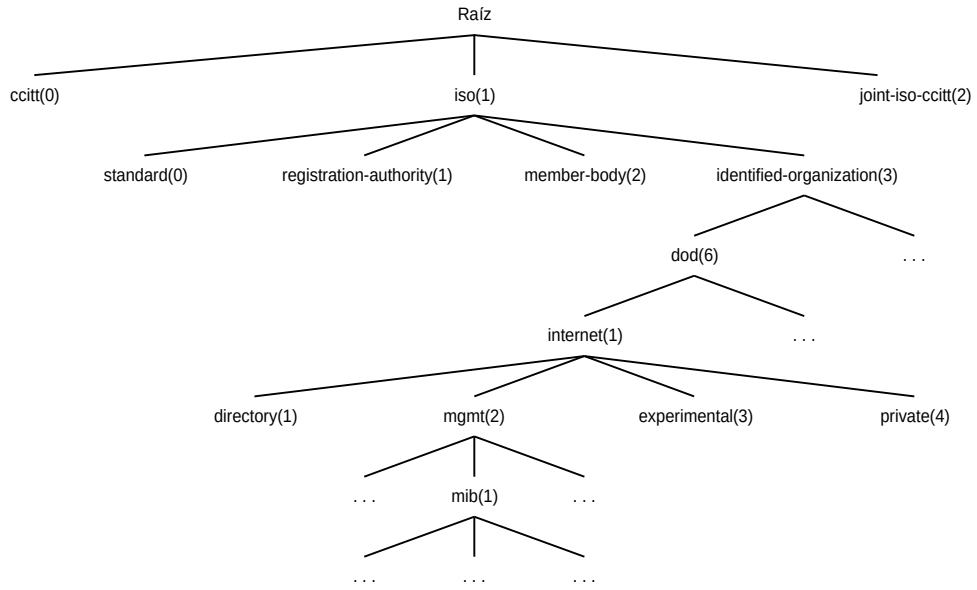


Figura 4.7 - Árvore de identificadores.

O OID é formado pela junção do nome do objecto e um sufixo. A forma do sufixo depende do tipo do objecto e é calculado de acordo com as seguintes regras:

- Apenas instâncias de objectos base podem ser identificadas. Tabelas e objectos do tipo linha não podem ser manipulados.
- Se um objecto não é uma coluna de uma tabela o sufixo é zero (0). A identificação de uma instância do objecto `sysDescr` [RFC1158] é, simplesmente, `sysDescr.0` ou 1.3.6.1.2.1.1.1.0 (Figura 4.8).
- O OID que identifica um determinado elemento de uma tabela é obtido através do OID correspondente à coluna e um valor que indica a linha.

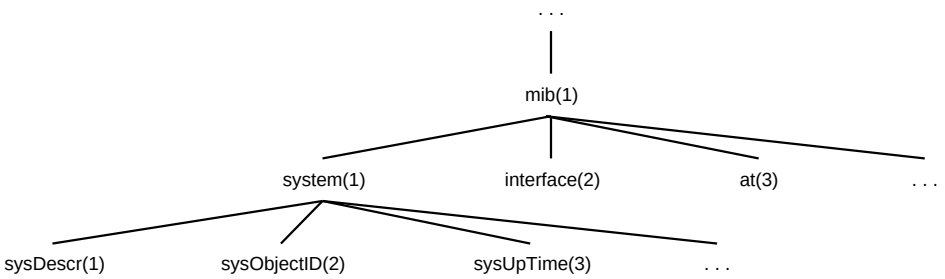


Figura 4.8 - Árvore de valores do grupo `system` da Internet MIB.

Como exemplo, suponha-se que se deseja ler a coluna de `ipRouteNextHop` de uma `ipRoutingTable` correspondente à linha `ipRouteDest`=192.92.133.0 (Tabela 4.2).

A estação gestora efectua uma operação de leitura ao parâmetro identificado como `ipRouteNextHop.192.92.133.0`. O agente visado devolve o valor `ipRouteNextHop.192.92.133.2`.

Tabela 4.2 - `ipRoutingTable` de uma MIB.

ipRouteDest	IpRouteifIndex	IpRouteNextHop	IpRouteType	ipRouteMask
0.0.0.0	2	192.92.133.254	4 (remote)	0.0.0.0
127.0.0.1	3	127.0.0.1	3 (direct)	255.255.255.0
192.92.133.0	2	192.92.133.2	3 (direct)	255.255.255.0
193.136.80.0	2	192.92.133.254	4 (remote)	255.255.255.0
193.136.82.0	2	192.92.133.2	3 (direct)	255.255.255.0

4.4.3 Operações/Protocolo

O SNMP (*Simple Network Management Protocol*) [RFC1157] consiste num protocolo simples que permite a uma estação gestora inspeccionar e modificar a informação de gestão de um elemento remoto de rede (agente), bem como o transporte de notificações geradas por estes. O protocolo especifica os seguintes tipos de operações:

- Operação de leitura (`GET`) – permite consultar um determinado parâmetro de um agente.
- Operação de actualização (`SET`) – permite modificar um determinado parâmetro de um agente.
- Operação transversal (`GET-NEXT`) – permite consultar parâmetros de um determinado agente sem necessidade de conhecer a MIB que o agente implementa. A selecção do objecto a consultar é feita sobre a instância imediatamente posterior à indicada.
- Operação de notificação (`TRAP`) – permite que cada agente notificar a ocorrência de eventos extraordinários.

Das quatro operações apresentadas, três delas são confirmadas e têm origem no gestor (`GET`, `GET-NEXT` e `SET`) enquanto que a outra (`TRAP`) é gerada pelo agente e não tem confirmação (Figura 4.9).

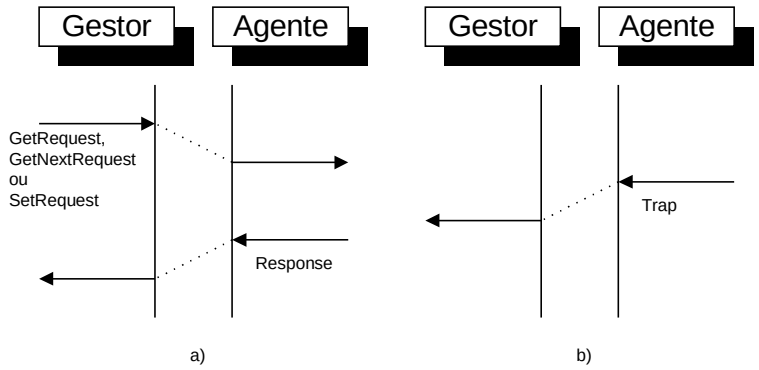


Figura 4.9 - Primitivas básicas do funcionamento do SNMP:
a) confirmadas e iniciadas pelo gestor; b) não confirmadas e iniciadas pelo agente.

O SNMP tem cinco PDUs (*Protocol Data Units*) na base das suas operações:

- `GetRequest` e `GetNextRequest`, utilizados na leitura de informação.
- `SetRequest`, utilizado na modificação de valores.

- `Response`, trama de resposta aos comandos anteriores.
- `Trap`, utilizado pelo agente na notificação de eventos anormais.

O uso de operações de notificação reveste-se de alguma controvérsia. Existem algumas desvantagens na escolha deste tipo de operação: se o evento causador de interrupção se propagar, o tráfego gerado pelos múltiplos pedidos pode agravar a situação e reduzir a largura de banda disponível. Uma opção de compromisso é o uso de níveis de disparo (*threshold*) associados a uma única interrupção. A consola, após interrupção, deve recorrer a uma técnica de convite (*polling*) para a leitura da informação considerada relevante para a análise do evento. O gestor, por sua vez, não se deve basear por inteiro nas interrupções mas sim verificar, periodicamente, o estado do agente (*low frequency polling*).

A especificação do SNMP apresenta o UDP [RFC768] como o protocolo principal ao transporte de mensagens de gestão. A codificação das estruturas de gestão são inseridas num único datagrama (Figura 4.10).

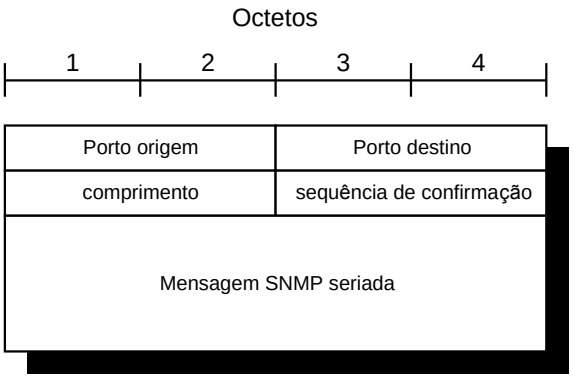


Figura 4.10 – Trama SNMP sobre UDP.

O endereço de cada trama consiste num endereço IP e no número de um porto de transporte. Todos os agentes SNMP esperam comandos no porto UDP 161. As notificações são recebidas no porto UDP 162.

4.4.4 Segurança no Contexto do SNMP

Um dos aspectos fundamentais na administração de uma rede de comunicações consiste na manutenção de um grau adequado de segurança. No contexto do SNMP, a questão de segurança resume-se à decisão de autorizar a realização de determinadas operações. O estabelecimento de autorizações adequadas implica a resposta às seguintes perguntas:

- A mensagem que especifica uma determinada operação foi alterada ou atrasada?
- Quem gerou a mensagem?
- Que objectos são acedidos na operação?
- Que direitos de acesso possui o emissor relativamente aos objectos visados pela operação?

Neste cenário há quatro aspectos que devem ser considerados:

- Sigilo: A informação transmitida deve ser protegida da leitura por parte de entidades não autorizadas.
- Autenticidade: A origem da mensagem deve ser inequivocamente identificada (“Tu és quem dizes que és?”).
- Integridade: A manutenção da integridade de uma determinada mensagem obriga a que apenas entidades autorizadas a possam modificar. A modificação inclui as operações de escrita, alteração, eliminação e criação.
- Disponibilidade: A informação deve estar permanentemente disponível.

Estes são os aspectos e ameaças que podem prejudicar o bom funcionamento, em termos de segurança, de uma rede de comunicação de dados. Um protocolo de gestão, tal como o SNMP, CMIP ou outros, devem disponibilizar meios de evitar qualquer um destes ataques de modo a tornar a rede menos vulnerável a invasões indesejáveis.

O SNMP original (versão 1) providencia mecanismos de segurança muito limitados, definindo apenas uma política de autenticação e de controlo de acesso. Para o efeito, introduz o conceito de comunidade [Stallings93], responsável por implementar uma política de autenticação. Cada comunidade é identificada por um nome, único em cada agente, e define uma relação entre um agente e um conjunto de estações gestoras. As estações gestoras pertencentes a uma comunidade necessitam indicar o nome da comunidade para todas as operações de consulta ou actualização.

Adicionalmente, cada agente define um perfil, o qual em associação com a comunidade, definem a política de acesso. O perfil é constituído por:

- Um conjunto de objectos pertencentes à MIB – a vista da MIB.
- O modo de acesso `READ-ONLY` ou `READ-WRITE`.

4.5 SNMPv2

A primeira versão do SNMP detém muitas deficiências, principalmente ao nível da segurança e das operações. Visando a eliminação destas deficiências, foi publicada uma actualização do SNMP, conhecido como SNMPv2.

4.5.1 Operações/Protocolo

O SNMPv2 encontra-se enriquecido com duas novas operações:

- Operação de informação – permite a troca de informação entre estações gestoras (`INFORM`).
- Operação de consulta múltipla – é semelhante à operação transversal (`GET-NEXT`) mas torna possível a especificação de múltiplos parâmetros (`GET-BULK`).
- `GET` não atómico –a falha de consulta a uma variável não impede o comando de prosseguir com outras consultas.

Ambas as operações requerem confirmação (Figura 4.11).

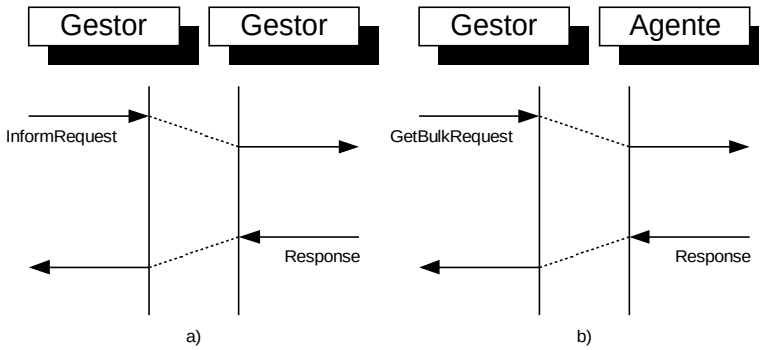


Figura 4.11 – Primitivas adicionadas ao SNMPv2:
a) entre estações gestoras; b) entre estação gestora e agente.

A PDU `GetBulkRequest` foi criada com o objectivo de minimizar o número de mensagens trocadas na consulta de uma grande quantidade de informação. A selecção de objectos segue os moldes da utilizada no `GetNextRequest`, ou seja, a selecção é feita sobre a instância imediatamente posterior à indicada.

Uma mensagem `GetBulkRequest` inclui (N+R) identificadores de variáveis e um valor (M). Para cada um dos primeiros N identificadores, a operação é efectuada de forma em tudo semelhante ao `GetNextRequest`. Os R identificadores seguintes especificam a recuperação de variáveis múltiplas. O valor M indica o número de variáveis sucessoras recuperadas para cada um dos R identificadores (Figura 4.12).

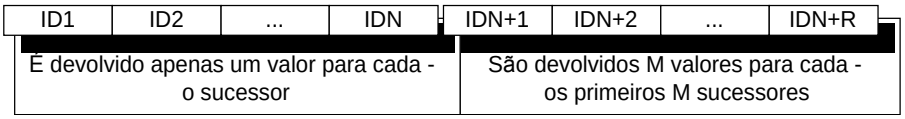


Figura 4.12 – Interpretação dos Campos do `GetBulkRequest`.

4.5.2 Segurança no Contexto SNMPv2

O modelo administrativo proposto pelo SNMPv2 não teve uma aceitação pacífica no seio da comunidade Internet. A controvérsia gerada resultou no aparecimento de três modelos distintos:

- SNMPv2p – baseado no conceito de perfis (***parties***) e contextos (***contexts***).
- SNMPv2c – baseado no conceito de comunidade, semelhante ao utilizado no SNMPv1 [RFC1901].
- SNMPv2u – baseado em nomes de utilizadores (***user-names***).

Por definição, um perfil SNMP é definido como o contexto de execução de uma operação SNMP. Cada mensagem SNMPv2p, contém o nome de dois perfis, o perfil da fonte e o perfil do destinatário. Estes permitem definir mecanismos de criptografia e de controlo de acesso. Em adição ao conceito de perfil, o modelo administrativo do SNMPv2p introduz o conceito de contexto. Este é definido como uma colecção de objectos de gestão, acessíveis por uma entidade SNMPv2 [RFC1445].

Uma mensagem SNMPv2u é identificada pelo nome de utilizador do emissor, nome este que deve ser reconhecido pelo destinatário. Cada utilizador define um conjunto

de atributos que permitem a sua inequívoca identificação em cada entidade [RFC1909]:

- `userName` – uma sequência de octetos que representam o nome do utilizador.
- `authProtocol` – uma indicação de que as mensagens enviadas por este utilizador podem ser autenticadas e, se for caso disso, o tipo de autenticação utilizada.
- `authPrivateKey` – indica a chave privada de autenticação.
- `privProtocol` – uma indicação de que a privacidade das mensagens se encontra protegida e, se for caso disso, o tipo de protocolo de privacidade utilizado. A chave de autenticação pode ser diferente em agentes diferentes.
- `privPrivateKey` – indica a chave privada usada pelo protocolo de privacidade. A chave de privacidade pode ser diferente em agentes diferentes.

Em adição, o modelo de segurança SNMPv2u define:

- `agentID` – identificador único entre todos os agentes de um domínio de gestão.
- `agentBoots` – contador de reinicializações desde que o agentID foi configurado.
- `agentTime` – número de segundos desde que o agentBoots foi incrementado.

O nível de segurança pretendido para uma determinada mensagem encontra-se descrito de acordo com a Qualidade de Serviço (QoS):

- sem autenticação (`noAuth`) e sem privacidade (`noPriv`).
- com autenticação (`auth`) e sem privacidade (`noPriv`).
- com autenticação (`auth`) e com privacidade (`priv`).

Cada mensagem contém a QoS no cabeçalho.

Em resumo, este modelo define um utilizador e tem um funcionamento semelhante ao paradigma utilizador/palavra chave usado para aceder a uma área particular numa estação de trabalho [Waters96]. Cada utilizador é identificado por um `userName` e autenticado com uma chave (`key`) – a palavra chave. Pode ser utilizada uma segunda chave para assegurar a privacidade.

4.6 SNMPv3

As versões 1 e 2 do SNMP apresentam uma grande rigidez em termos de extensão de funcionalidade. A actualização ou redefinição do formato das mensagens, do protocolo de segurança, ou de qualquer outra característica só se revela possível pela redefinição integral do modelo de gestão. Para que um sistema deste tipo seja viável a médio ou a longo prazo é necessário que apresente uma funcionalidade perfeita. É público a grande dificuldade (impossibilidade) em desenvolver um sistema perfeito.

Os objectivos do grupo de trabalho responsável pelo desenvolvimento do SNMPv3 apresentam-se mais realistas. O sistema não necessita ser perfeito à partida, basta permitir a correcção posterior de erros sem comprometer a globalidade do modelo. Além disso, deverá ser desenvolvido rapidamente, ser simples, funcional e prático.

Por outro lado, todo o trabalho despendido no desenvolvimento e normalização das versões anteriores não deve ser desprezado, pelo que o ponto de partida do desenvolvimento do SNMPv3 assenta no trabalho efectuado em torno do SNMPv2, nomeadamente, do SNMPv2u e SNMPv2* [Harrington97].

4.6.1 Documentação

De acordo com [RFC2026], um documento candidato a norma da Internet evolui segundo um conjunto de níveis de maturidade:

- Norma proposta (*proposed standard*).
- Norma provisória (*draft standard*).
- Norma (*standard*).

Documentos ultrapassados ou que não se encontrem classificados de acordo com um dos três níveis anteriores podem ser classificados como: experimental (*Experimental*), histórico (*Historic*) ou informativo (*Informational*). Estes documentos não constituem normas.

Uma proposta a norma passa inicialmente por uma fase de discussão pública (*Internet draft*) antes de ser submetida a aprovação pelo *Internet Engineering Steering Group* (IESG). Se for aprovada, a especificação e publicada como norma proposta, onde ficará pelo menos 6 meses. A norma sera provisória durante pelo menos 4 meses, antes de se tornar definitiva.

No momento, as especificações do SNMPv3 foram aprovadas pelo IESG como normas propostas em 5 de Dezembro de 1997, onde ficarão durante os 6 meses seguintes:

- D. Harrington, R. Presuhn, B. Wijnen, "An Architecture for Describing SNMP Management Frameworks", *Internet Request for Comments 2271*, Janeiro 1998.
- J. Case, D. Harrington, R. Presuhn, B. Wijnen, "Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)", *Internet Request for Comments 2272*, Janeiro 1998.
- D. Levi, P. Meyer, B. Stewart, "SNMPv3 Applications", Internet Request for Comments 2273, Janeiro 1998.
- U. Blumenthal, B. Wijnen, "User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)", *Internet Request for Comments 2274*, Janeiro 1998.
- B. Wijnen, R. Presuhn, K. McCloghrie, "View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)", *Internet Request for Comments 2275*, Janeiro 1998.

4.6.2 Modelo

Um protocolo de gestão deve ser seguro, particularmente em operações de actualização (SET). Deve admitir a extensão posterior de funcionalidade à medida que novos mecanismos ou protocolos surjam. Estes foram alguns dos objectivos patentes no desenvolvimento do SNMPv3. Acima de tudo, o SNMPv3 não deve apresentar rotura com o SNMPv2 ou o SNMPv1 facilitando a transição dos sistemas já instalados.

A proposta apresenta um modelo extensível, baseado no SNMPv2, mas que o suplementa ao nível do:

- Formato da mensagem.
- Modelo de segurança.
- Modelo de controlo de acesso.

A arquitectura SNMPv3 define um mecanismo, responsável pelas operações ao nível do modelo de gestão e uma ou mais aplicações, com a responsabilidade de recolha e/ou processamento de informação (Figura 4.13).

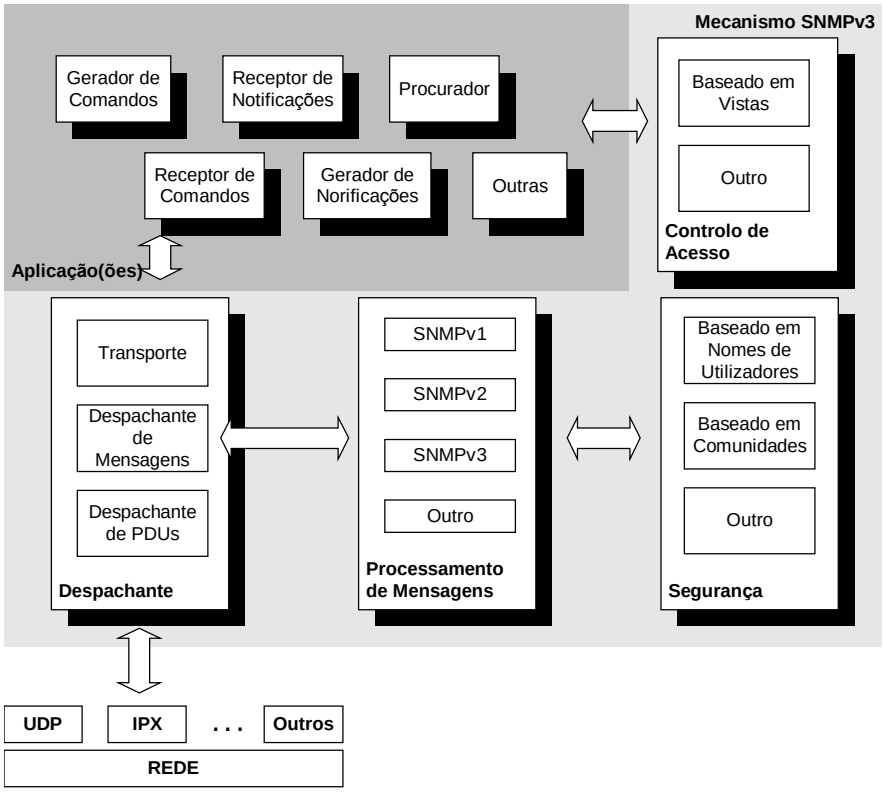


Figura 4.13 – Entidade SNMPv3.

A(s) aplicação(ões) utilizam os serviços prestados pelo mecanismo SNMPv3 para o envio e a recepção de mensagens, autenticação, criptografia e controlo de acesso aos objectos de gestão [RFC2271].

O despachante, subsistema pertencente ao mecanismo SNMPv3, coordena a comunicação entre subsistemas e distingue os módulos pertencentes ao mesmo

subsistema. Determina, com base no PDU, que aplicação deve ser invocada e coordena todos as correspondências sobre a camada de transporte.

A imutabilidade do formato da mensagem do SNMPv2 obriga à definição de um novo conjunto de documentos caso seja necessária a sua alteração. A concentração da tarefa de processamento de mensagens num único subsistema permite a alteração do formato da mensagem por substituição de apenas um módulo. Além disso, torna possível a coexistência de vários formatos num único modelo, sendo invocado o processador adequado sempre que for necessário [RFC2272].

Uma filosofia idêntica é seguida para o aspecto de segurança relativamente à mensagem. A mensagem deve ser autenticada, de forma a não haver execução de comandos por parte de entidades não autorizadas, protegida quanto à leitura indevida e validada segundo informação temporal. Este último aspecto visa proteger a mensagem quanto à duplicação e/ou o atraso propositado de comandos. A duplicação e atraso de um comando de reinicialização (*reboot*), por exemplo, pode ser desastroso quando efectuado de forma indevida.

Um dos pontos polémicos na definição do SNMPv2 foi, precisamente, que modelo usar para a segurança das mensagens. O SNMPv3 apresenta um subsistema responsável pelas tarefas de segurança tornando mais simples a substituição de um modelo de segurança e conseguindo simultaneamente a coexistência de várias soluções.

A entidade SNMPv3 pode conter uma ou mais aplicações de acordo com as necessidades de gestão. De forma resumida, as aplicações podem ser receptoras ou geradoras de comandos, notificações ou de um outro tipo como, por exemplo, aplicações com funções de procurador [RFC2273].

Num cenário real de funcionamento, quando uma mensagem é emitida, o despachante verifica a versão e tipo de protocolo seleccionado (Figura 4.14).

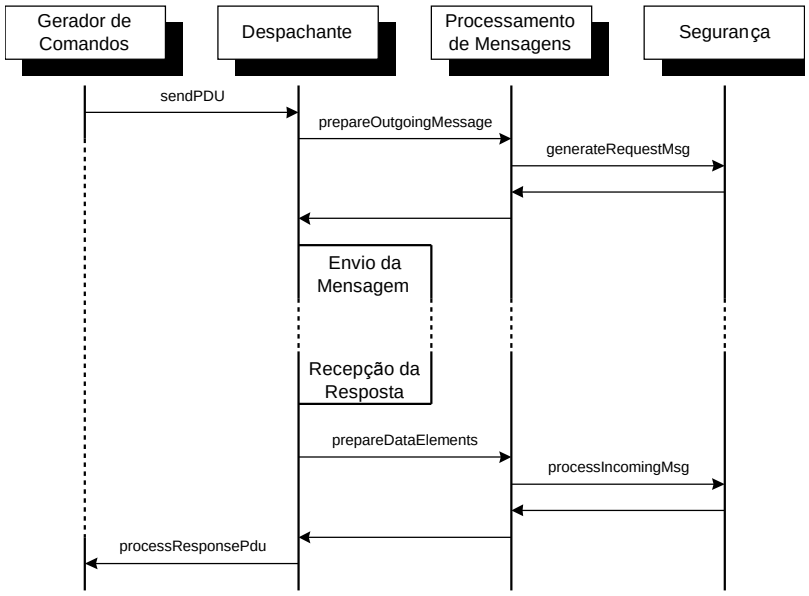


Figura 4.14 – Geração de um comando.

De acordo com esta informação é invocado o processador de mensagens adequado que, por sua vez, inclui informação acerca do modelo de segurança a utilizar. A

mensagem é, de seguida, entregue ao módulo de segurança para depois ser enviada. A recepção de uma mensagem segue o processo inverso: o despachante verifica a versão e tipo de protocolo indicado pela mensagem e invoca o processador de mensagens respectivo. Segue-se a etapa de autenticação, de descodificação e de verificação de atrasos. Se este processo terminar com sucesso a mensagem regressa ao despachante que a encaminha para a aplicação adequada.

A aplicação, dependendo do tipo de comando, pode necessitar de serviços de autorização de acesso a objectos de gestão. Estes são fornecidos pelo subsistema de controlo de acesso pertencente ao mecanismo SNMPv3. O subsistema de controlo de acesso contém pelo menos um mecanismo de autorização de acesso, havendo, também aqui, a possibilidade de coexistência de vários modelos distintos.

4.6.3 Identificação de Informação de Gestão

Um agente tradicional inclui o mecanismo SNMPv3 a aplicação de recepção de comandos, a aplicação geradora de notificações e, eventualmente, uma aplicação de procuração (Figura 4.15).

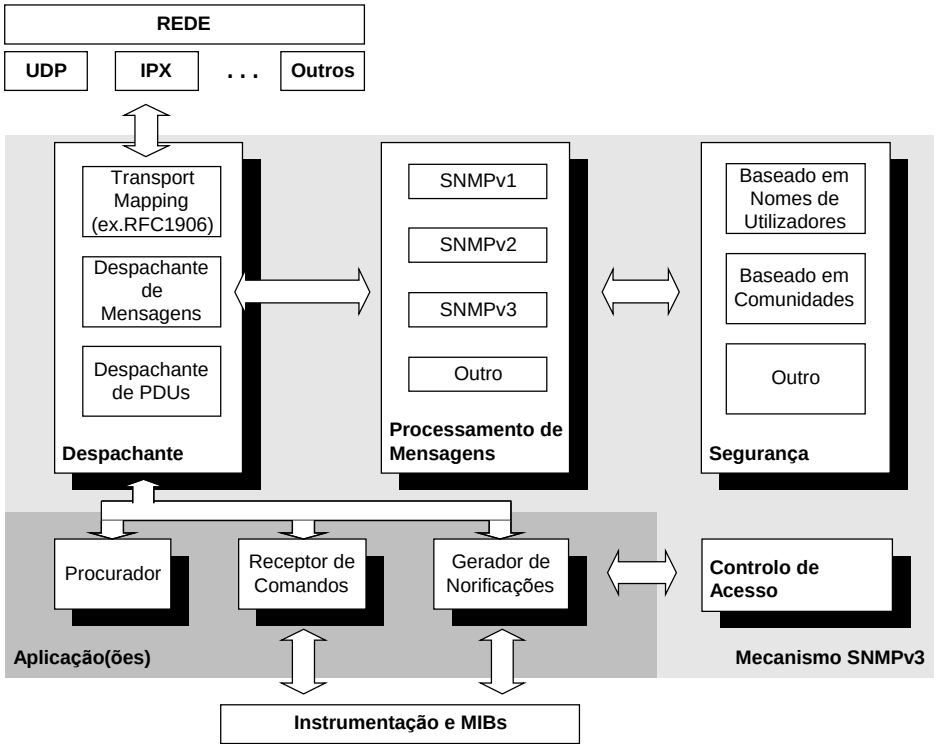


Figura 4.15 – Agente tradicional.

Cada agente tem mecanismos de instrumentação associados, ou seja, mecanismos de aquisição de informação e controlo de componentes de rede. A informação reside numa entidade SNMP e, à partida, será acedida pelo receptor de comandos. Este terá acesso a, potencialmente, múltiplos contextos, de acordo com o tipo de informação (Figura 4.16).

De forma geral, um conjunto de informação é acedida de acordo com um determinado contexto que, por sua vez, representa uma entidade física (como uma ponte ou um servidor), uma entidade lógica (um serviço) ou um conjunto de entidades. Cada

contexto é válido apenas no domínio de uma entidade SNMPv3. Não é possível que um contexto se distribua por várias entidades SNMPv3.

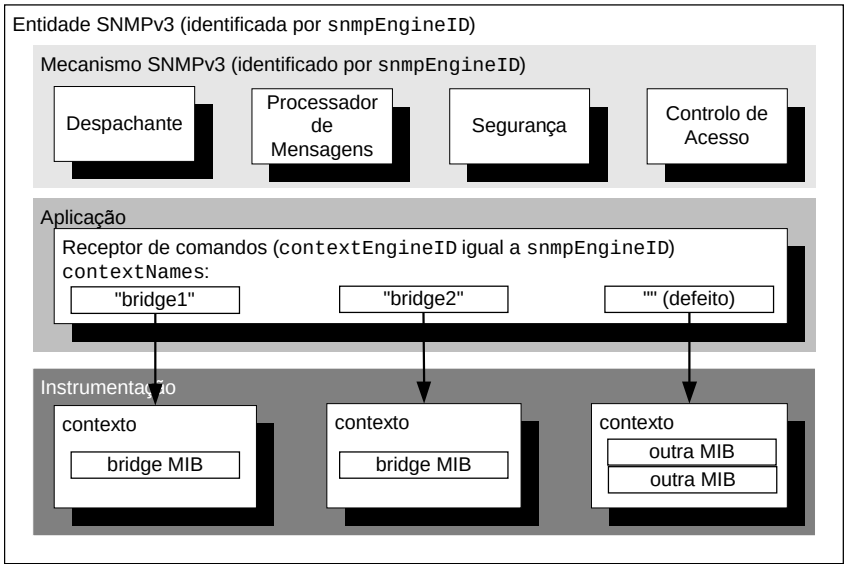


Figura 4.16 – Contextos e acesso e identificação de informação.

Para identificar cada objecto são necessários quatro identificadores: o identificador do mecanismo SNMPv3 (`snmpEngineID`), o nome do contexto (`contextName`), o identificador de objecto (OID – ex. `ifDescr`) e o identificador de instância (ex. "1"). No caso do SNMPv1, a consulta é efectuada apenas indicando o identificador de objecto (OID) e o identificador de instância, o que resulta numa maior simplicidade de acesso mas numa menor flexibilidade.

4.6.4 Segurança

O SNMPv3 admite, como foi já referido, vários modelos de segurança. Estes são identificados por um campo no cabeçalho de uma mensagem SNMPv3. O grupo de trabalho definiu um modelo de segurança baseado em nomes de utilizadores, denominado *User-based Security Model* (USM) [RFC2274].

O USM define um "chefe" (*principal*), que representa um utilizador e é identificado por um nome (`userName`). O "chefe" tem a responsabilidade de armazenar chaves e outro tipo de informação de segurança, como o tipo de algoritmo criptográfico utilizado. As chaves são sequências de octetos, utilizadas pelos protocolos de autenticação e privacidade.

É da responsabilidade do modelo de segurança prevenir ataques de autenticação, privacidade e manter o condicionalismo temporal das mensagens. A autenticação de mensagens é conseguida por intermédio de um Código de Autenticação de Mensagem (MAC – *Message Authentication Code*), único para cada mensagem [Blumenthal97]. Estes códigos funcionam como as "impressões digitais" da mensagem e são enviados juntamente com esta. A identidade do emissor é verificada com o auxílio do MAC e das chaves indicadas pelo "chefe".

A privacidade das mensagens é assegurada por intermédio de algoritmos de criptografia baseados nas chaves indicadas pelo "chefe" e pelo MAC.

O condicionalismo temporal tem a responsabilidade de detectar mensagens duplicadas e propositadamente atrasadas. Para o conseguir cada mensagem transporta uma marca temporal que pode ser examinada pelo receptor. Se a diferença entre a marca e o valor de relógio local exceder um certo limite a mensagem é rejeitada. O problema que se levanta reside na necessidade de sincronização entre os relógios do emissor e do receptor [RFC2274]. O cabeçalho de uma mensagem USM contém campos com informação acerca do número de vezes que um mecanismo SNMPv3 foi reinicializado (`engineBoots`) e com o número de segundos decorridos desde a última reinicialização (`engineTime`). A transmissão de uma mensagem não é instantânea, pelo que é definida uma "janela de oportunidade" (150 segundos) que define o limite de atraso de uma mensagem:

- Se o `engineBoots` indicado na mensagem for maior que a noção do receptor, a mensagem é aceite e a noção local de `engineBoots` e engineTime são actualizados.
- Se o `engineBoots` indicado na mensagem for menor que a noção do receptor, a mensagem é descartada, uma vez que apresenta sinais de atraso.
- Se o `engineBoots` for igual à noção do receptor, o `engineTime` é comparado com a noção local respectiva. Se a diferença for inferior a 150 s ("janela de oportunidade") esta será aceite, caso contrário, será rejeitada. Sempre que a mensagem é aceite, a noção local das marcas temporais são actualizados.

O mecanismo tal como foi apresentado permite a duplicação de mensagens ocorridas dentro da "janela de oportunidade", de modo que surge a necessidade de o complementar com um método adicional de protecção. Este método assenta num campo de identificação único de cada mensagem (`msgID`): se aparecerem dois `msgID` iguais dentro da mesma "janela de oportunidade", a mensagem é desprezada.

4.6.5 Implementações

No momento da escrita deste documento encontravam-se já várias implementações do SNMPv3 desenvolvidas por alguns fornecedores e centros de investigação:

- ACE*COMM (http://www.acecomm.com/).
- BMC Software (http://www.bmc.com/).
- Epilogue/ISI (http://www.epilogue.com/).
- IBM Research (http://www.watson.ibm.com/).
- SNMP Research (http://www.snmp.com/).
- Technical University of Braunschweig (http://www.ibr.cs.tu-bs.de/). - http://www.ibr.cs.tu-bs.de/projects/snmpv3/tcpdump.shtml ou http://www.ibr.cs.tu-bs.de/projects/snmpv3/scotty.shtml.
- University of Quebec in Montreal (http://www.teleinfo.uqam.ca/) - http://atm.teleinfo.uqam.ca/snmp/index.htm.

Após a fraca aceitação das versões SNMPv2u e SNMPv2*, a comunidade de gestão Internet aguarda pelas implementações do SNMPv3 para o desenvolvimento de

sistemas de gestão de redes mais seguros e capazes de fazer frente às necessidades mais prementes das redes actuais.

4.7 TMN – *Telecommunications Management Network*

A TMN providencia operações e mecanismos de gestão para redes de telecomunicações. Em particular, o sistema foi desenvolvido de forma a realizar o controlo e monitorização de redes de telecomunicações, incluindo funções de monitorização de falhas, análise de desempenho, controlo de encaminhamento e de configuração, taxação e controlo de acesso. A TMN pode ser vista como uma rede paralela à rede da operadora, em perfeita concordância com esta, por intermédio de um conjunto de pontos de acesso normalizados (Figura 4.17).

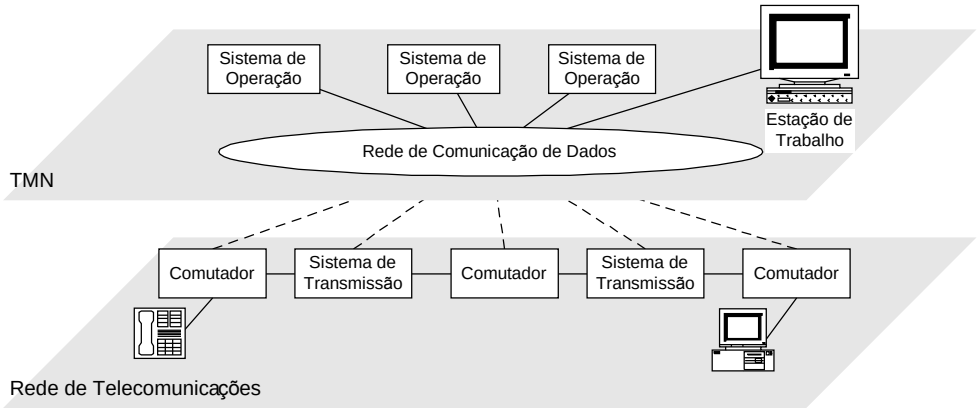


Figura 4.17 – Relação da TMN com a rede de telecomunicações.

O processo de normalização do TMN teve início em 1985 pelo grupo de estudo IV do CCITT. Até 1992 este grupo produziu um conjunto de normas, apresentadas de forma sucinta em [Cohen94].

As recomendações TMN apresentam três arquitecturas distintas [Cohen94]:

- Arquitectura Funcional – descreve os blocos funcionais e os pontos de acesso aos blocos funcionais.
- Arquitectura Física – descreve as interfaces e os componentes físicos de uma TMN.
- Arquitectura de Informação – descreve a aplicação dos princípios de gestão OSI em TMN.

4.7.1 Arquitectura Funcional TMN

A arquitectura funcional TMN define seis componentes, denominados blocos funcionais (Figura 4.18).

O bloco OSF tem como função o processamento de informação de gestão. As funções de mediação (MF) realizam um preprocessamento sobre a informação proveniente dos elementos de rede (NE). A informação trocada entre blocos é transportada pelo bloco DCF (comunicação de dados). NEF representa a entidade a gerir, na rede TMN. A comunicação entre um bloco funcional e o utilizador é efectuada por intermédio de das funções WSF. O QAF (adaptador) é utilizado na interligação com entidades que

não suportam TMN. Neste contexto, o QAF é semelhante ao conceito de entidade procuradora do SNMP.

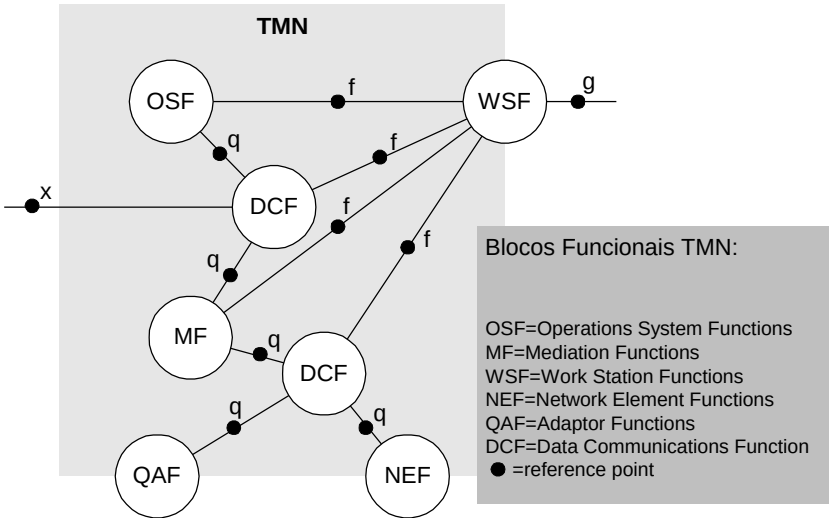


Figura 4.18 – Pontos de Referência e Blocos Funcionais TMN.

4.7.2 Arquitectura Física

A arquitectura física especifica a forma como são efectuadas as funções de gestão TMN sobre sistemas os de rede. Para o efeito, define os seguintes blocos em que cada um dos quais implementa as funções com o mesmo nome:

- Elemento de Rede (NE).
- Sistema de Mediação (MD).
- Adaptador Q (QA).
- Sistema de Operação (OS).
- Estação de Trabalho (WS).
- Rede de Comunicação de Dados (DCN).

Estes blocos são referidos como os blocos físicos TMN para contrastar com os blocos funcionais.

As interfaces são um aspecto chave da arquitectura física do TMN. Estas representam a implementação dos pontos de referência, assim como os protocolos constituem a implementação dos serviços das camadas OSI. Actualmente, as interfaces TMN são: F (entre TMN e as Estações de Trabalho), Q3 (entre sistemas TMN) e X (entre componentes de diferentes redes TMN). Em adição, existem as interfaces Qx, entre elementos de rede e sistemas de mediação, e G, entre as estações de trabalho e o utilizador.

4.7.3 Modelo de Informação TMN

O modelo de informação TMN utiliza o mesmo modelo das normas da ISO/ITU-T, em que se segue uma metodologia orientada ao objecto. Os objectos são definidos a

partir de um conjunto de regras sintáxicas (GDMO) e representam os dispositivos físicos a serem geridos.

4.8 Conclusões

Todas as arquitecturas discutidas neste capítulo apresentam características comuns, como a dualidade gestor/agente, uma estrutura de informação de gestão e um protocolo específico de transferência de informação. Apesar do esforço normativo que cada solução reúne, o mercado dita regras nem sempre são favoráveis à implantação de algumas delas. Por outro lado, o impacto causado por soluções largamente divulgadas é elevado, havendo tendência a tornarem-se *standards de facto* em detrimento de outras soluções normalizadas.

O processo de normalização OSI teve sucessivos atrasos e resultou num modelo complicado, que encarece as aplicações e dificulta a tarefa de desenvolvimento. Por estes motivos, o modelo OSI não apresenta um número de utilizadores suficiente para modo a fomentar a sua utilização.

A arquitectura TMN, apesar de ser desenvolvida segundo o modelo OSI tem uma grande fatia de mercado – o mercado das telecomunicações – que a podem impulsionar de forma diferente.

A gestão Internet, ou o SNMP, é a prova de que as soluções mais simples são mais fáceis de serem aceites relativamente às mais complicadas e poderosas. Praticamente todo o equipamento de gestão instalado em redes locais é baseado no modelo de gestão SNMP. A acumulação de equipamento mantém a tendência em seguir o modelo e assim sucessivamente.

5 GESTÃO BASEADA NA WWW

5.1 Introdução

As redes locais de comunicação de dados são intrinsecamente heterogéneas. É comum a coexistência de componentes de diversos fabricantes, derivada da implementação de diversas soluções tecnológicas ou dos contínuos avanços tecnológicos. A gestão de uma rede deste tipo é normalmente efectuada com o auxílio de ferramentas proprietárias, produzidas pelo fabricante para cada componente. O administrador de uma rede deste tipo necessita utilizar toda uma panóplia de ferramentas, de acordo com a diversidade existente, ou adquirir uma solução de aspecto geral. Este tipo de ferramentas é geralmente caro e requer *hardware* poderoso, pelo que a sua aquisição não se encontra ao alcance das instituições mais modestas.

O desenvolvimento de normas de gestão procura fomentar o estabelecimento de uma plataforma comum sobre diferentes recursos de rede, de forma a providenciar uma certa consistência sobre os métodos de gestão para a globalidade da rede. Segundo o que foi apresentado no capítulo anterior, as normas mais conhecidas no seio das redes locais de comunicação de dados são as relativas ao modelo de gestão da Internet – SNMP, ao modelo de gestão OSI – CMIP.

Os serviços baseados na WWW (*World Wide Web*), como resultado da sua crescente popularidade, apresentam uma interface bem conhecida (*web browser*) e ainda a capacidade de serem executados em várias plataformas. A vulgaridade dos chamados *browsers* e a tendência actual para a integração de múltiplos serviços possibilita a coexistência de vários tipos de informação, de uma forma local ou distribuída. Estas características tornam a tecnologia adequada para a integração de diversas soluções de gestão normalizadas ou proprietárias. A integração pode ser efectuada de várias formas, não exclusivas:

- Pela definição de um esquema de equivalência entre o *HyperText Transfer Protocol* (HTTP) [RFC1945] e o(s) protocolo(s) de gestão respectivo(s).
- Utilizando linguagens de programação interpretadas, do tipo Java [Arnold96], no desenvolvimento de aplicações de gestão.
- Pela extensão da tecnologia de WWW de modo a suportar operações de gestão.
- Utilizando a arquitectura CORBA (*Common Object Request Broker*) [Corba97] como núcleo de reunificação de diferentes soluções tecnológicas.

5.2 HyperText Transfer Protocol

A *World Wide Web* foi desenvolvida inicialmente pelo CERN (*Centre Européen de la Recherche Nucléaire*) e permite a organização e o acesso a uma variedade de formatos de informação, incluindo texto, imagens e som. O acesso é efectuado com base na activação de ligações hipermédia sobre uma interface apropriada – o *browser*. O protocolo nativo da WWW é o HTTP (*Hypertext Transfer Protocol*). Este é um protocolo genérico com a possibilidade de negociação de tipos de dados e da sua representação, característica esta que permite desenvolver sistemas independentes do tipo de dados transferidos.

A *HyperText Markup Language* (HTML) [Graham96] é um formato de dados, com base em etiquetas, que permite definir documentos hipermédia independentes da plataforma. Os documentos publicados na Internet são descritos em HTML e colocados num servidor de HTTP. Quando um utilizador deseja efectuar uma consulta, um programa cliente (*browser*) é utilizado para efectuar a ligação. Depois de conseguida, o documento é interpretado e visualizado. Cada documento é identificado com base num *Uniform Resource Locator* (URL) que contém informação acerca do endereço do servidor e do documento específico a consultar.

5.2.1 Common Gateway Interface

Os documentos HTML são geralmente estáticos. Para se modificar a informação apresentada no *browser* é necessário reeditar o documento. Uma técnica associada, que veio dar um grande dinamismo, permite adaptar as entradas e saídas de qualquer programa a um *browser* HTML. Este processo é designado por *Common Gateway Interface* (CGI) [Rowe96] e permite realizar a adaptação entre uma aplicação externa e o servidor HTTP, pelo que se torna possível a construção dinâmica de documentos HTML, de acordo com os resultados da execução de uma determinada aplicação (Figura 5.1).

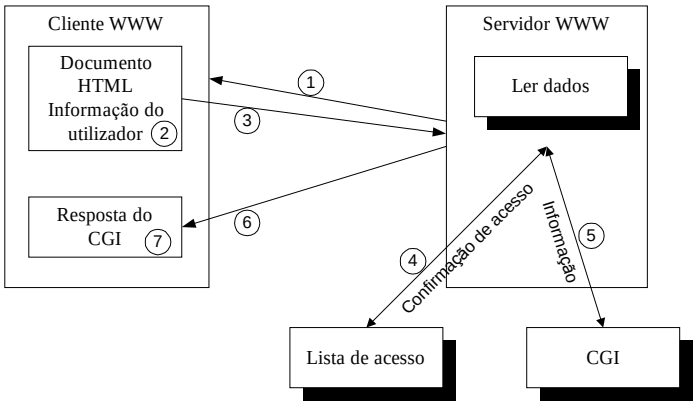


Figura 5.1 – Funcionamento de uma CGI.

Na prática, vários passos são seguidos antes de o *browser* poder mostrar os resultados:

1. Carregar a página que permite especificar os parâmetros de entrada da CGI, caso existam.
2. O utilizador acciona o CGI por intermédio de um evento (selecção de um botão ou de uma ligação).
3. O *browser* contacta o servidor pedindo permissão para correr o CGI.
4. O servidor executa um procedimento de controlo de acesso, com a finalidade de verificar se o utilizador tem a autorização necessária.
5. O servidor verifica se o CGI existe e executa-o.
6. Os resultados produzidos pelo CGI são devolvido ao *browser*.
7. O *browser* apresenta os resultados.

O código não necessita ser portável, uma vez que a execução do programa é sempre realizada no servidor, independentemente do local onde o utilizador se encontre.

A utilização de CGIs permite desenvolver soluções de gestão baseadas em tecnologia da *Web*. Em tal cenário, a CGI interage directamente com o agente de gestão, convertendo os pedidos HTTP em funções específicas de gestão. É da responsabilidade do agente a execução das operações e, se for caso disso, gerar as respectivas respostas, que entregará ao *browser* por intermédio do CGI/servidor HTTP.

5.2.2 Procurador HTTP

A intercalação de uma aplicação com funções de procurador (*proxy*) entre o *browser* e o agente permite converter os pedidos HTTP provenientes do cliente em mensagens específicas do modelo de gestão considerado (Figura 5.2).

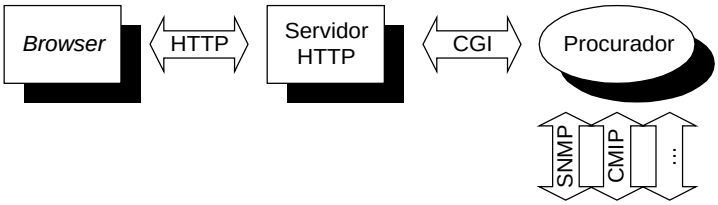


Figura 5.2 – Procurador HTTP.

Neste caso, dependendo do tipo de pedidos efectuados pelo *browser*, estes são convertidos num protocolo específico de gestão. A operação a realizar é identificada com base no URL enviado pelo *browser*. De modo a não haver inequívocos, o URL necessita conter informação sobre o agente específico, sob a forma de um endereço, o tipo de protocolo (SNMP ou CMIP, por exemplo) e a operação (`get` ou `set`, por exemplo). Em adição, sempre que for necessário, pode conter parâmetros necessários à operação [Deri96], tais como a lista de variáveis a consultar ou os valores a modificar.

5.3 Java

A linguagem de programação Java tem vindo a modificar a forma como as aplicações são desenvolvidas e executadas na Internet. A Java foi desenvolvida tendo em vista o suporte de aplicações em rede, composta por uma variedade de sistemas e arquitecturas. Para o conseguir, o compilador gera código objecto específico de uma máquina virtual, criando um ambiente homogéneo. Este código é executado em qualquer sistema que tenha instalado o respectivo interpretador. As aplicações são portáveis entre plataformas, desde que estas suportem a máquina virtual Java [Lindholm96], e podem ser acedidas por *browsers* de WWW. O problema com esta abordagem resulta da perda de desempenho na pela necessidade de interpretação.

Podem ser desenvolvidos dois tipos de programas: *applets* – programas destinados a serem armazenados num servidor HTTP e executados num *browser*, e aplicações – programas armazenados em disco e executados localmente.

Muito resumidamente, a Java é uma linguagem orientada ao objecto, apresentando características semelhantes às do C++. As principais diferenças relativamente a este reside na ausência de aritmética de ponteiros, na eliminação de algumas características como a sobrecarga de operadores (*operator overloading*) e a herança múltipla. Em adição foi criado um mecanismo de gestão dinâmica de memória (*garbage collection*), o que vem simplificar o desenvolvimento.

A Java contém uma extensa biblioteca de funções de suporte aos protocolos da Internet como o TCP, UDP, HTTP ou o *File Transfer Protocol* (FTP), cuja utilização simplifica o desenvolvimento de aplicações cliente/servidor.

5.4 Java Management API

A linguagem de programação Java, como foi já referido, providencia um ambiente comum sobre diversos sistemas operativos e protocolos de rede. Da forma a explorar este ambiente, um consórcio de empresas produtoras de componentes e soluções de rede em conjunto com a Sun, desenvolveu uma API orientada à criação de objectos e métodos de gestão. A *Java Management API* (JMAPI) [Jmapi96a, Jmapi96b] consiste num conjunto de classes para o desenvolvimento de soluções de gestão em redes heterogéneas. A filosofia da API segue o modelo genérico: a responsabilidade de recolha de informação é atribuída a pequenas aplicações (agentes), espalhadas por diversos componentes de rede. A informação proveniente dos agentes é recolhida, armazenada e modificada por módulo(s) de controlo e administração.

O objectivo é fornecer meios que simplifiquem o desenvolvimento de aplicações de gestão, tirando partido, ao mesmo tempo, das características multiplataforma e multiprotocolo.

5.4.1 Arquitectura

A um nível mais elevado, a arquitectura consiste na Interface com o Utilizador (*Browser User Interface*), Módulo de Execução (*Admin Runtime Module*) e nos agentes (*Appliances*) (Figura 5.3).

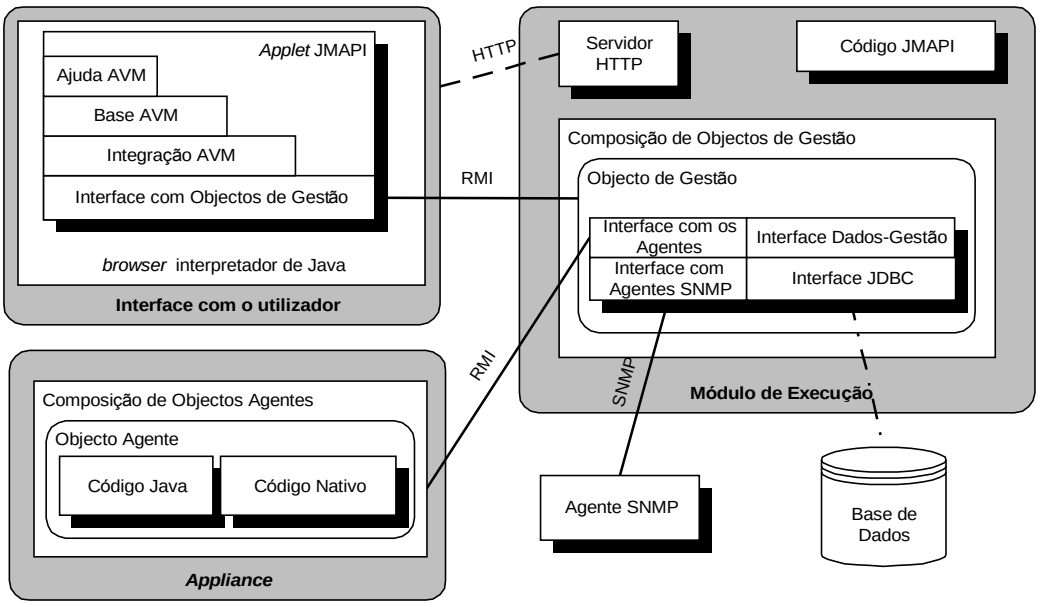


Figura 5.3 - Componentes da arquitectura JMAPI.

A arquitectura global da JMAPI apresenta um carácter distribuído, não sendo necessário que os componentes residam na mesma máquina. Os componentes usam o mecanismo RMI (*Remote Method Invocation*) [Rmi96] para comunicarem. Desenvolvido em Java, o RMI não impõe restrições ao nível de sistema operativo, arquitectura, protocolo ou máquina, dando possibilidade de comunicação a

componentes residentes em máquinas diferentes. Este mecanismo permite realizar a invocação remota de métodos, de modo semelhante à invocação remota de procedimentos (RPC – *Remote Procedure Calls*).

5.4.2 Interface com o Utilizador – BUI (*Browser User Interface*)

A Interface com o Utilizador (BUI) constitui o mecanismo a partir do qual o administrador gera comandos de gestão. Estas operações podem ser invocadas a partir de um *browser* ou de uma aplicação independente.

Vários recursos podem ser consultados e modificados, independentemente do local e da máquina onde se encontre, desde que seja usado um *browser* compatível com Java ou uma aplicação com essa função específica. O *applet* proveniente do ARM é constituído por módulos, cada um com uma responsabilidade particular. Desta forma consegue-se que as operações a realizar sejam estanques, tornando o desenvolvimento mais simples e livre de erros. Os módulos constituintes do BUI são o AVM (*Admin View Module*), as interfaces com os objectos de gestão (*Manager Object Interfaces*) e o *browser*.

O papel principal do AVM é fornecer os meios necessários para o diálogo com o utilizador. A arquitectura, inteiramente desenvolvida em Java, em particular sobre o AWT (*Abstract Window Toolkit*) [Nagaratnam96], é composta por classes responsáveis pela apresentação e recolha de acções do utilizador. Além dos objectos gráficos de interacção clássicos, como caixas de texto, janelas de diálogo, árvores hierárquicas, entre outras, reúne classes para a apresentação de páginas de ajuda sensível ao contexto, visualizadas sob a forma de páginas HTML (Figura 5.4).

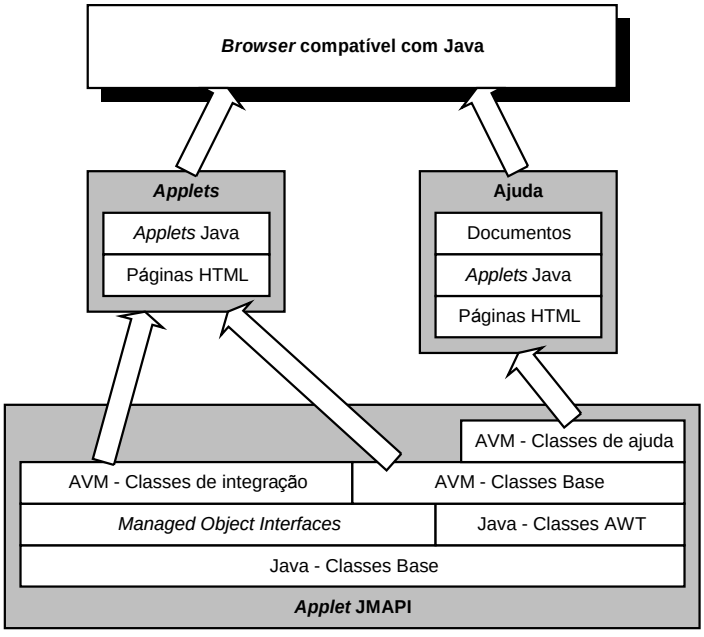


Figura 5.4 - Arquitectura AVM.

As classes AVM estão divididas em três módulos: classes de ajuda, classes base e classes de integração.

- Classes de Ajuda – o objectivo principal das classes de ajuda é tornar disponível um ambiente de ajuda generalizado. É possível que várias aplicações de gestão diferentes partilhem o mesmo bloco de ajuda, com índice, glossário e navegador comuns. Os documentos de ajuda são escritos em HTML pelo que não é necessária qualquer conversão adicional.
- Classes Base – as classes base do AVM são uma extensão do AWT de forma a permitir a criação de um ambiente de navegação semelhante ao hipertexto.
- Classes de Integração – este tipo de classes tem por função principal realizar uma integração entre as classes base AVM e as Interfaces com Objectos de Gestão. Estas classes são usadas para agrupar propriedades a partir de objectos de gestão. Para o efeito, providenciam a seguinte funcionalidade: registo e eliminação de *applets* de gestão, registo e eliminação de páginas de gestão, registo e eliminação de ligações de gestão e registo e eliminação de extensões às Interfaces com Objectos de Gestão.

Os métodos pertencentes à Interface com Objectos de Gestão usam RMI para executar métodos remotos de gestão. Objectos deste tipo fornecem uma abstracção de recursos, simplificando o acesso à informação de gestão.

5.4.3 Módulo de Execução – ARM (*Admin Runtime Module*)

O Módulo de Execução (ARM) constitui o servidor de aplicações. Este bloco é responsável por enviar os módulos BUI para os clientes HTTP e os agentes (*appliances*) para os diversos componentes de rede. O ARM reúne um conjunto de referências para os objectos de gestão distribuídos pela rede, de modo providenciar um mecanismo de comunicação entre as aplicações de gestão e os agentes. Entre estes objectos encontram-se as Interfaces com os agentes (*Agent Object Interfaces*) e Interfaces Dados-Gestão (*Managed Data Interfaces*).

O ARM centraliza todas as operações de administração, desde a gestão da base de dados à resposta a acções do utilizador. Para ultrapassar as limitações de segurança impostas aos *applets*, relativas ao acesso ao disco local e a ligações via rede, todas as comunicações entre a interface com o utilizador e as *appliances* são feitas por intermédio do ARM. De lembrar que um *applet* só pode realizar ligações ao servidor de origem. O ARM providencia três serviços básicos: o servidor HTTP, a composição de objectos de gestão e a interface com a base de dados.

O envio do *applet* ao *browser* é efectuado por intermédio do servidor HTTP. O ficheiro HTML inicial contém as indicações necessárias para carregar e executar o código. Quando o *applet* e os objectos JMAPI são executados, a comunicação passa a ser efectuada por RMI pelo que o servidor de HTTP passa a segundo plano. O módulo de Composição de Objectos de Gestão permite a criação de novos objectos ou a consulta de objectos armazenados em base de dados. Os objectos de gestão são parte constituinte das *appliances* (agentes), referenciados remotamente pelo AVM. Para todos os efeitos, a invocação dos métodos dos agentes é feita como se estes residissem no sistema local.

5.4.4 Componentes de Gestão (*Appliances*)

Os agentes (*appliances*) representam os componentes de rede a serem geridos. A estratégia consiste em colocar agentes próximos dos componentes, através de actualização dinâmica. Um componente inicia a recuperação do agente com um pedido ao ARM. Este, por sua vez, envia o módulo de uma forma segura.

De um ponto de vista lógico, as *appliances* são receptáculos de aplicações de instrumentação fornecidas pelo ARM e registadas na base de dados. O código necessário é enviado dinamicamente (Java ou nativo, dependente da plataforma). A recuperação de código em cada *appliance* é iniciada por intermédio de um pequeno programa que pode ser único para todos os sistemas existentes. As *appliances* são diferenciadas apenas pelo código carregado. Este facto simplifica a manutenção de *software*, principalmente em grandes redes.

5.4.5 Conclusões

Relativamente a outras arquitecturas de gestão, nomeadamente o SNMP, a JMAPI apresenta alguma lacunas. Não há continuidade do modelo de informação definido pelo SNMP, pelo que não vai ser fácil a sua aceitação de imediato. A segurança, em termos de autenticação e privacidade, é um assunto que fica ainda por resolver.

Por outro lado, o desenvolvimento de aplicações de gestão simplifica-se, devido à existência de uma camada homogénea sobre os recursos a gerir.

Por avaliação do tráfego gerado nas listas de correio electrónico, a adesão não tem sido muito elevada. Os utilizadores continuam a preferir o modelo de gestão SNMP, com particular ênfase no SNMPv3.

5.5 WBEM – *Web-Based Enterprise Management*

A divulgação da Internet levou a considerar a aplicação daquele tipo de ferramentas em sistemas de administração mais simples, baratos e eficazes. Seguindo um caminho alternativo ao do JMAPI, a comunidade de gestão desenvolve actualmente uma solução que visa uniformizar toda uma panóplia de protocolos, modelos de dados e sistemas de gestão. A iniciativa WBEM (*Web-Based Enterprise Management*) [WBEM] estabelece uma arquitectura de gestão compatível com os protocolos de gestão existentes, como o SNMP e CMIP. O objectivo da iniciativa é consolidar e unificar a informação gerada pelas tecnologias de gestão existentes, normalizando, deste modo, o ambiente de gestão de uma rede de comunicação de dados actual. A arquitectura WBEM define os seguintes componentes:

- *Hypermedia Management Schema* (HMMS) – define um esquema de descrição de dados de gestão.
- *Hypermedia Management Protocol* (HMMP) – usado como veículo de mensagens de gestão. As mensagens, tal como em qualquer protocolo de gestão, são usadas na inquisição e manipulação de informação mantida no componente de rede a ser gerido.
- *Hypermedia Object Manager* (HMOM) – uma definição genérica para aplicações de gestão que agregam informação e usam um ou mais protocolos de forma a obter uma representação uniforme num *browser* de *web*.

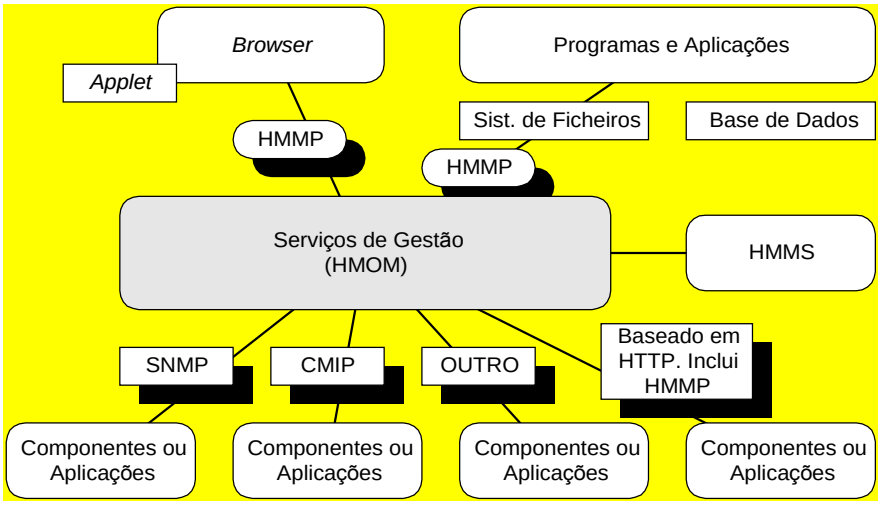


Figura 5.5 – Arquitectura proposta do WBEM.

5.5.1 Hypermedia Management Schema

O modelo de informação é usado para representar objectos reais segundo um paradigma orientado ao objecto, usando conceitos de classes e instâncias. Do ponto de vista lógico, o HMMS é semelhante a uma base de dados orientada ao objecto.

A classe é a definição básica de uma unidade de gestão. Esta descreve um armazém de funções e de campos de informação individuais denominados propriedades ou atributos. Cada atributo (ou propriedade) descreve aspectos particulares do componente descrito pela classe. Uma classe define um modelo para um objecto de gestão. Com base no modelo é possível definir objectos específicos criando instâncias da classe. Como exemplo, uma hipotética classe `Disco` poderia ter instâncias `disco_C` e `disco_D`.

As propriedades são os campos individuais descritos numa classe. Estas armazenam informação individual e particular a essa classe ou objecto. Normalmente, as propriedades não são acedidas directamente, mas por intermédio de qualificadores.

Um qualificador é um modificador de elementos básicos do esquema definido, como classes, instâncias e propriedades. A sua presença não é indispensável, embora tornem mais clara a operação a realizar.

O HMMS encontra-se estruturado em três níveis. O primeiro nível contém o esquema base, que consiste no conjunto de classes base, as suas propriedades e as suas associações (Figura 5.6). O segundo nível define um esquema comum. Trata-se de um conjunto de classes específicas mas independente da plataforma (`REDE`, `SISTEMA` ou `APLICAÇÃO`). O terceiro nível contém extensões que representam plataformas, aplicações ou serviços específicos (`WINDOWS_NT`, `UNIX` ou `FTPD`).

Relativamente ao nível base, cada classe agrupa métodos específicos de um determinado tipo de componente:

- A classe `CIM_ManagedSystemElement` é a base da hierarquia. Qualquer componente de um sistema é candidato a ser descrito por esta classe.

- `CIM_System` representa uma colecção de objectos que são vistos como um todo.
- `CIM_PhysicalElement` representa qualquer componente físico. Por exemplo, um ficheiro não pode ser um objecto `CIM_PhysicalElement` mas a placa de rede já pode.
- `CIM_LogicalDevice` representa qualquer componente que não é um sistema nem um `CIM_PhysicalElement`.
- `CIM_Service` e `CIM_ServiceAccessPoint` representam os serviços dependentes do `CIM_Service`.

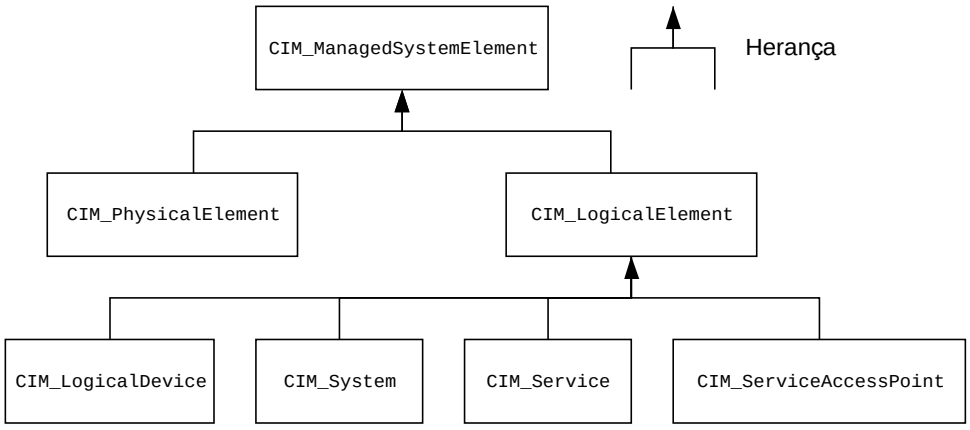


Figura 5.6 – O esquema base.

Cada esquema é descrito segundo dois modelos:

- O modelo ***meta*** – descreve que tipo de entidades formam o esquema (como classes, instâncias e propriedades) e como podem ser combinados de forma a representar componentes reais.
- O modelo ***standard*** – é um conjunto de classes normalizadas e publicadas que representam um conjunto vasto de ***hardware*** e de objectos de gestão. Se uma classe pertencer ao esquema ***standard***, a definição desta deve ser universal e imutável.

5.5.2 Hypermedia Management Protocol

Os objectos definidos num HMMS são acedidos e manipulados por intermédio do HMMP. A filosofia seguida assenta no modelo cliente/servidor e distingue cada processo segundo as seguintes categorias:

- Cliente – executa pedidos de forma a realizar uma determinada operação de gestão. Podem ser simples processos de monitorização de componentes de rede ou aplicações complexas de âmbito geral, capazes de gerir qualquer objecto HMMP.

- Servidor – satisfaz o pedido do cliente e devolve uma resposta adequada. Os servidores, na sua forma mais complexa, podem ser executados em estações de trabalho poderosas, com capacidade de armazenamento de uma grande quantidade de informação e funcionando como procurador de vários e distintos objectos geridos. Podem, por outro lado, ser simples processos sem capacidade de armazenamento de informação e implementando apenas um conjunto reduzido de rotinas.
- Produtor – tem como função a geração de Notificações HMMP. As notificações reportam eventos extraordinários de forma semelhante ao TRAP do SNMP.
- Consumidor – tem a função de executar acções de gestão HMMP em resposta às Notificações HMMP. O produtor gera notificações que envia para um determinado consumidor. Se for caso disso, o consumidor envia uma Resposta de Notificação HMMP ao produtor.

Os papéis cliente e servidor podem ser combinados de forma a conseguir um modelo hierárquico e distribuído. Um cliente executa um pedido a um servidor que, por sua vez, pode ser visto como um cliente por outro servidor (Figura 5.7).

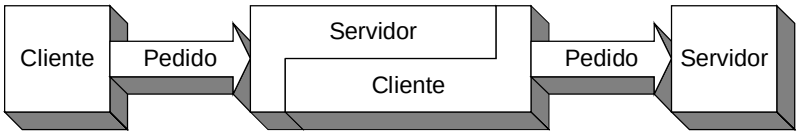


Figura 5.7 - Hierarquia de cliente/servidor.

O HMMP visa as interacções com o modelo de dados definido e prevê um conjunto extenso de operações tais como: criação, actualização, eliminação, leitura de classes e instâncias e a realização de consultas.

O HMMP encontra-se definido sobre TCP/IP, para o caso de operações remotas (Figura 5.8).

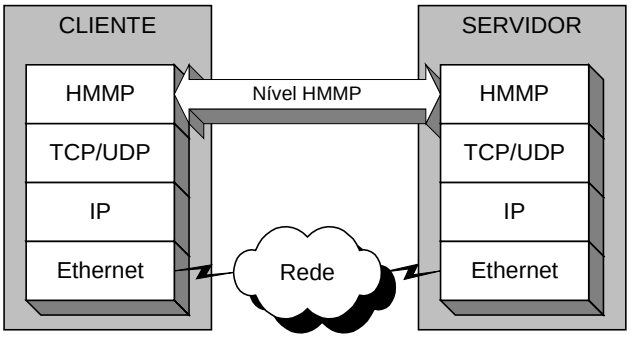


Figura 5.8 - Ligação HMMP em sistemas distribuídos.

Em situações em que o cliente e o servidor partilham a mesma máquina não há necessidade de implementar a pilha protocolar de comunicações. É suficiente um mecanismo de comunicação entre processos (IPC) que preenche as funções de transporte do pacote HMMP (Figura 5.9).

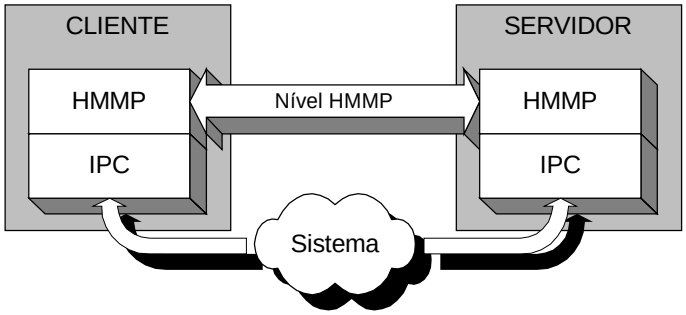


Figura 5.9 - Ligação HMMP em espaço comum.

As diversas mensagens HMMP são representadas por PDUs de quatro tipos diferentes:

- `HMMP_PDU_OP_REQUEST` – enviado pelo cliente para um servidor para iniciar uma operação.
- `HMMP_PDU_OP_RESPONSE` – enviado pelo servidor para um cliente em resposta à operação indicada.
- `HMMP_PDU_IND_REQUEST` – enviado por um produtor para um consumidor alertando-o de algum evento extraordinário.
- `HMMP_PDU_IND_RESPONSE` – enviado pelo consumidor para o produtor confirmando a recepção do evento extraordinário.

5.5.3 Hypermedia Object Manager

Em terminologia HMMP, um servidor que implementa um vasto conjunto de rotinas HMMP e que acumula funções de procurador é denominado *Hypermedia Object Manager* (HMOM). Os servidores HMMP que fornecem apenas um pequeno conjunto de primitivas HMMP e que funcionam apenas como servidores são denominados *Producers*.

Num ambiente típico, os clientes lidam directamente com um HMOM que se responsabiliza por satisfazer o pedido directamente ou tornar-se, por sua vez, num cliente e enviar o pedido ao fornecedor respectivo (Figura 5.10).

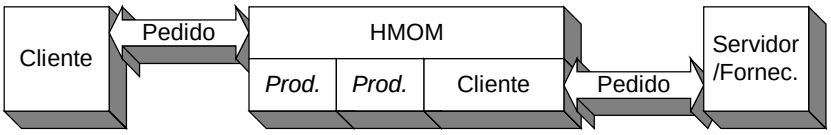


Figura 5.10 - Gestor de objectos.

Esta filosofia permite abstrair um conjunto de componentes em cada HMOM, reduzindo a complexidade dos clientes. Este, simplesmente, envia pedidos gerais ao HMOM que, por sua vez, distribui os pedidos por fornecedores adequados. Os fornecedores fazem a conversão do pedido para mecanismos proprietários ou normalizados, como o SNMP ou CMIP (Figura 5.11).

Um fornecedor pode devolver um valor específico obtido directamente do *hardware* ou realizar uma monitorização exaustiva de um conjunto de componentes semelhantes, como encaminhadores ou concentradores.

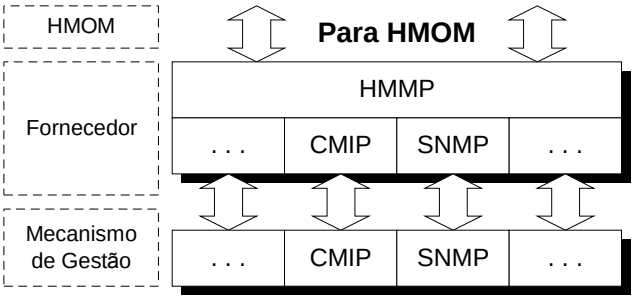


Figura 5.11 - Conversão HMMP/Mecanismos de gestão.

5.6 CORBA – *Common Object Request Broker Architecture*

A *Common Object Request Broker Architecture* (CORBA) [Corba97] surge como uma resposta à interoperabilidade entre diferentes produtos, sejam eles *software* ou *hardware*. A utilização de CORBA permite aceder a informação de forma transparente, sem haver necessidade de conhecer a sua localização, a plataforma ou protocolo de transporte. A arquitectura define objectos servidores, objectos clientes e um *Object Request Broker* (ORB), que estabelece as relações entre eles. O ORB intercepta a invocação e assume a responsabilidade de encontrar o objecto visado, efectuar a passagem de parâmetros, invocar o método e devolver os resultados. Neste contexto, o objecto cliente pode, de forma transparente, invocar um método definido pelo objecto servidor, que pode residir na própria máquina ou numa máquina remota.

A interoperabilidade entre a CORBA e a Internet permite que os *browsers* explorem as características da CORBA mantendo as suas próprias, nomeadamente, uma interface bem conhecida e grande simplicidade de utilização.

5.6.1 Arquitectura

A CORBA visa a gestão de objectos distribuídos e, para o efeito fornece mecanismos que possibilitam:

- A troca de mensagens entre objectos – para o efeito é necessário um protocolo ou interface que descreva as mensagens aceites por cada objecto.
- Uma forma de criação dos objectos – por exemplo, um construtor.
- A gestão de memória – plataforma de suporte e tempo de vida do objecto.

Em adição, são necessárias ferramentas e serviços de apoio ao desenvolvimento e execução de aplicações distribuídas. Entre estas encontram-se:

- O *Object Request Broker* (ORB) – providencia a base de apoio e as operações fundamentais para a gestão dos objectos distribuídos.
- Serviços usados no desenvolvimento de aplicações distribuídas e na gestão dos seus objectos.
- Serviços comuns a diferentes aplicações.
- As próprias aplicações distribuídas.

A troca de mensagens é um processo essencial para o desenvolvimento de uma aplicação distribuída baseada em objectos. As mensagens são trocadas sob a forma de invocações de métodos pertencentes a outros objectos e consequente recepção de resultados.

Em CORBA, cada mensagem é descrita mediante a construção de uma interface que define o tipo de pedidos que o objecto está disposto a receber. Desde que o objecto se comporte como indicado pela interface, não é necessário conhecer os pormenores de implementação. A interface é definida segundo uma especificação independente da linguagem, a *Interface Definition Language* (IDL).

Em adição à interface, é necessário um protocolo, utilizado no processo de invocação de métodos. Este protocolo actua entre as interfaces, pelo que se torna necessário definir a ligação entre as interfaces e os objectos cliente e servidor. A ligação passa pela geração de correspondências entre as implementações dos objectos e o ORB: os *stubs* e os *skeletons*. Os *stubs* constituem a terminação dos clientes, enquanto que os *skeletons* realizam a correspondência entre objectos servidores e o ORB.

Em resumo e de forma simplificada, a troca de mensagens entre dois objectos por intermédio de um ORB segue o seguinte procedimento (Figura 5.12):

1. O cliente invoca um método por intermédio do *stub*.
2. O *stub* invoca o ORB.
3. O ORB passa o pedido à implementação por intermédio do *skeleton.*
4. A implementação devolve o resultado ou uma excepção ao cliente por intermédio do ORB.

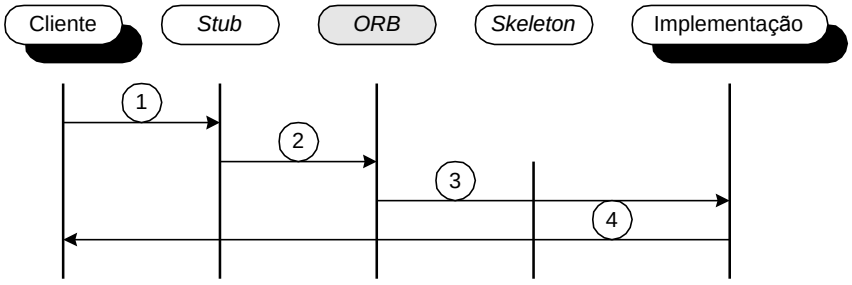


Figura 5.12 – Invocação de métodos por intermédio do ORB.

A invocação por intermédio do ORB segue os padrões usados nas *Remote Procedure Calls* (RPCs) [Bloomer92] que disfarça uma invocação remota como a chamada a um procedimento local. O compilador de RPCs é usado para traduzir a especificação dos procedimentos como um par de *stubs* (cliente e servidor). A grande diferença entre as RPCs e a CORBA reside no facto de as primeiras funcionarem numa base procedimental e a CORBA definir uma base OO.

A interoperabilidade sugere que diferentes implementações possam comunicar. Para o efeito é necessário um protocolo comum. O OMG define um protocolo geral – o *General Inter-ORB Protocol* (GIOP) – que deve ser implementado por todas os ORBs de modo a assegurar a interoperabilidade. Por outro lado, deve ser definida uma correspondência entre o GIOP e o protocolo de transporte utilizado (TCP ou IPX, por exemplo). Uma destas correspondências definida pelo OMG é o *Internet Inter-ORB Protocol* (IIOP), usado em redes TCP/IP (Figura 5.13).

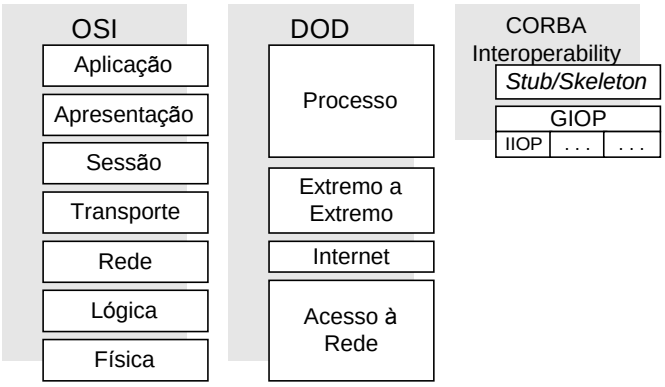


Figura 5.13 – Interoperabilidade ORB.

5.6.2 Gestão de Redes Baseada em CORBA

À partida, é possível considerar dois cenários: a gestão baseada em CORBA e a integração de tecnologia. No caso da gestão baseada em CORBA, o comportamento dos agentes é definido por interfaces IDL, invocadas pelo SGR por intermédio de um ORB. As operações realizadas, tal como no modelo genérico, incluem operações de consulta (`GET`) e modificação (`SET`) do estado do agente. Cada agente implementa um modelo de informação específico que serve de apoio à instrumentação realizada. Este modelo segue uma filosofia orientada ao objecto definido em IDL. O agente constitui, portanto, o servidor CORBA. O agente assim definido não possui capacidade de geração de notificações (`TRAP`), pelo que se torna necessário dotá-lo de um Serviço de Notificações (Figura 5.14).

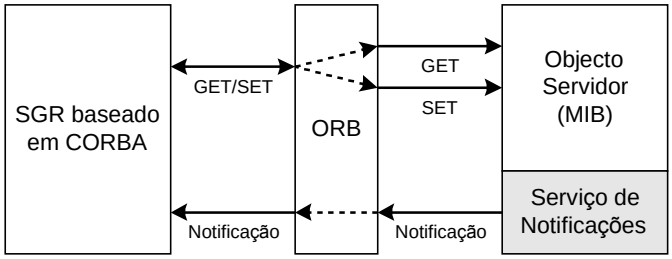


Figura 5.14 – Interacção entre o SGR e agente baseados em CORBA.

Por outro lado, algumas arquitecturas de gestão, nomeadamente o SNMP, tem já uma grande aceitação, reunindo características que tornam a sua substituição difícil a curto prazo. Uma destas características é o modelo de informação que constitui um dos pontos valiosos do SNMP, pelo que não é desejável a sua eliminação. Nestes casos, o método a seguir passa pela integração de da tecnologia com a CORBA. Algumas propostas nesta área [Mazumdar96] [Hong97] sugerem o desenvolvimento de uma interface SNMP/CORBA, com a definição de uma correspondência entre MIBs e interfaces IDL. A interface tem como função a conversão de pedidos CORBA para PDUs SNMP e vice-versa. Uma desvantagem desta abordagem passa pela necessidade de utilizar múltiplos pedidos CORBA para um único PDU SNMP, mais concretamente um para cada variável.

5.6.3 Integração de Tecnologia

A CORBA permite a interoperabilidade entre diversas tecnologias de gestão (JMAPI, WBEM, OSI ou SNMP) e entre diversas ferramentas de comunicação entre processos (RMI ou DCOM). A utilização de interfaces e ORBs permite o desenvolvimento de um arquitectura diversificada com núcleo comum, aproveitando as melhores características de cada tecnologia.

5.7 Conclusões

A associação entre a WWW e a gestão de redes é já uma realidade. Várias são as soluções que associam as duas vertentes tecnológicas mas nenhuma se revela consensual. Por avaliação do tráfego gerado nas listas de correio, há algum interesse em acompanhar as arquitecturas JMAPI e WBEM mas com a preocupação de manter uma ligação com o SNMP.

Fazendo uso da máquina virtual de Java, a JMAPI promete trazer compatibilidade universal em qualquer sistema. A complexidade do SNMP seria substituída pelo desenvolvimento de aplicações em Java, cobrindo sistemas diferentes com uma camada uniforme.

O WBEM apresenta um modelo de informação orientado ao objecto e forma a criar uma representação lógica do sistema a gerir. O protocolo HMMP assenta no HTTP, de forma a poder ser utilizado um ***browser*** para a gestão do sistema.

As duas soluções anteriores apresentam uma rotura com o modelo de informação SNMP, nomeadamente com a grande diversidade de MIBs que se encontram especificadas. Este é um dos motivos que dificulta a aceitação das arquitecturas. Neste sentido, a CORBA pode realizar a integração de tecnologia de forma independente da plataforma, de protocolos e de linguagens de programação. Começam a surgir compiladores que visam realizar a correspondência das MIBs SNMP/OSI para IDL que visam recuperar o trabalho realizado naquela área.

Em termos gerais o SNMP continua a ser a arquitectura de eleição, não se prevendo a sua substituição a curto prazo. Por outro lado, a sua sobrevivência a médio/longo prazo está dependente da aceitação geral do SNMPv3.

6 GESTÃO DE UMA REDE LOCAL DE COMUNICAÇÃO DE DADOS

6.1 Introdução

As abordagens anteriores sobre os sistemas de gestão, nomeadamente o SNMP e o modelo de gestão OSI, privilegiaram os mecanismos relacionados com a organização e transferência de informação, que servem de base à construção das aplicações de gestão. Algumas novas arquitecturas para gestão, como o WBEM e a JMAPI, incluem ferramentas que permitem a sua operação no ambiente distribuído da Internet. Em contrapartida, apresentam uma rotura com os modelos SNMP e OSI, principalmente ao nível do modelo de informação. Não é previsível a substituição a curto prazo dos sistemas de gestão já instalados, pelo que as abordagens mais recentes terão de conviver com os sistemas de gestão "clássicos".

Devido ao carácter dinâmico de uma rede de comunicação de dados não é fácil definir a funcionalidade que um SGR deve ter. De igual forma, o tipo de tarefas exigido depende do utilizador que, de forma geral, necessitará de um conjunto de ferramentas diversificado. A divisão em módulos permite criar níveis crescentes de funcionalidade, dotando o SGR de um modelo flexível de processamento de informação.

A quantidade de informação gerada é, de modo geral, suficientemente elevada para rapidamente fugir ao controlo do utilizador. O desenvolvimento de abstracções mais eficiente sobre esta informação permitirá reduzir o volume de informação e criar interpretações mais relevantes da mesma.

Num ambiente cada vez mais complexo, o papel desempenhado pelo utilizador em certas operações de gestão deverá tender para o de um espectador activo. Este cenário pressupõe a integração de ferramentas automáticas, tais como a detecção e correcção de certos problemas conhecidos pelo sistema. O primeiro passo em direcção à gestão automática passa pela definição de acções agendáveis no tempo, diminuindo o fardo causado pelas tarefas repetitivas. O passo seguinte passa pelo desenvolvimento de sistemas de gestão de redes inteligentes, baseados numa camada de abstracção sobre a informação de gestão.

A arquitectura apresentada descreve um sistema de gestão de redes que tem por base a integração de modelos de gestão "clássicos" com a tecnologia da Internet.

6.2 Generalidades

De acordo com o modelo genérico, um sistema de gestão de redes contém vários agentes acedidos por uma consola de gestão. A informação é vista como uma colecção de objectos, organizados segundo uma MIB. Cada agente pode implementar uma ou mais MIBs. Em particular, cada objecto tem um nome, uma sintaxe, e uma codificação. Cada MIB especifica variáveis necessárias para a monitorização e controlo dos vários componentes de rede. Potencialmente, representa uma vasta colecção de objectos, pelo que, numa rede relativamente grande, a quantidade de informação de gestão produzida pode ser enorme.

Apesar de não ser redundante, muita da informação apresenta-se de pouca utilidade para certas operações. Por outro lado, a forma em que se apresenta nem sempre é a mais adequada. Como exemplo, o número de datagramas de entrada perdidos devido a

erros no cabeçalho IP (1.3.6.1.2.1.4.4 – `ipInHdrErrors`, na MIB-II [RFC1213]) perde relevância face à sua derivada relativamente ao tempo: a taxa de erro.

6.2.1 Meta-Variáveis

O conceito de meta-variáveis não é novo [Oliveira95]. Por definição, uma meta-variável apresenta-se como uma função sobre um conjunto de objectos de uma ou mais MIBs. Consegue-se, desta forma, uma representação mais adequada da informação de gestão.

Entre o SGR e os agentes, propriamente ditos, encontra-se um mecanismo intermediário com a responsabilidade de realizar o cálculo de expressões predefinidas e exportar o resultado para um SGR - o processador de meta-variáveis (Figura 6.1). O processador de meta-variáveis é um processo independente do SGR. Estrategicamente colocados, apresentam, de forma mais relevante, a informação de gestão. Como extensão do conceito, uma meta-variável pode representar qualquer número de agentes, como, por exemplo, a média do `ifInErrors` (1.3.6.1.2.1.2.2.1.14 – MIB-II) num determinado segmento de rede.

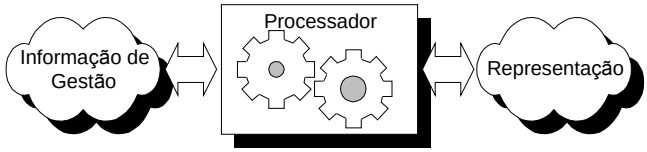


Figura 6.1 – Processador de meta-variáveis.

Um sistema de gestão, intrinsecamente distribuído, pode ser visto como uma base de dados distribuída (Figura 6.2).

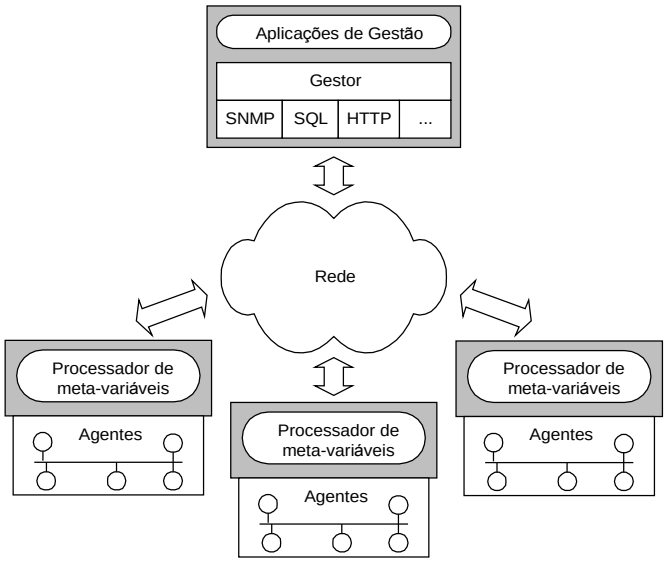


Figura 6.2 – Base de dados distribuída.

A informação provém de todas as meta-variáveis e agentes da rede. A base de dados pode ser acedida segundo uma multiplicidade de métodos com um mínimo de alterações na arquitectura:

- Por intermédio um agente procurador, usando SNMP.
- Por um cliente HTTP, associado a um servidor de WWW e uma CGI.
- Por intermédio de uma invocação remota, providenciada por mecanismos como CORBA, RMI ou DCOM.
- Por intermédio de uma interface SQL [ANSIX3.135], considerando a informação de gestão como uma base de dados virtual [Oliveira95].

A arquitectura do sistema aqui apresentado é suficientemente flexível para comportar um conjunto, ou mesmo a totalidade, dos métodos apresentados. No momento foi utilizado apenas SNMP, apenas por uma questão de divulgação.

6.3 Arquitectura

No momento em que foi iniciado o desenvolvimento do SGR aqui descrito, o SNMPv3 não se encontrava ainda disponível, além de não existirem APIs disponíveis em domínio público. Por outro lado, os sistemas que formam o ambiente sobre o qual foi desenvolvido o sistema implementam, essencialmente, agentes SNMPv1, pelo que esta foi a versão adoptada no desenvolvimento do SGR. Esta opção não inviabiliza de forma alguma a integração futura de diferentes versões ou mesmo de diferentes arquitecturas, tais como OSI ou TMN. Existe já trabalho realizado nesta área, com integração de TMN e CORBA [Chen96] e ATM e CORBA [Rixon97] para a gestão distribuída de redes.

A linha de orientação seguida no desenvolvimento do sistema visa a integração do SNMP com tecnologia Internet. Para o efeito a linguagem de desenvolvimento utilizada foi a Java, essencialmente devido ao extenso conjunto de funções de que dispõe e da característica particular que lhe permite ser executada num *browser* compatível com aquela linguagem.

Uma das preocupações principais foi manter a arquitectura modular, de forma a ser possível a adição de novas ferramentas e funcionalidades com um mínimo impacto sobre o sistema. A arquitectura pode ser dividida em três grandes blocos: o *applet* NMS, o Servidor e o Pré-processador de Informação (Figura 6.3).

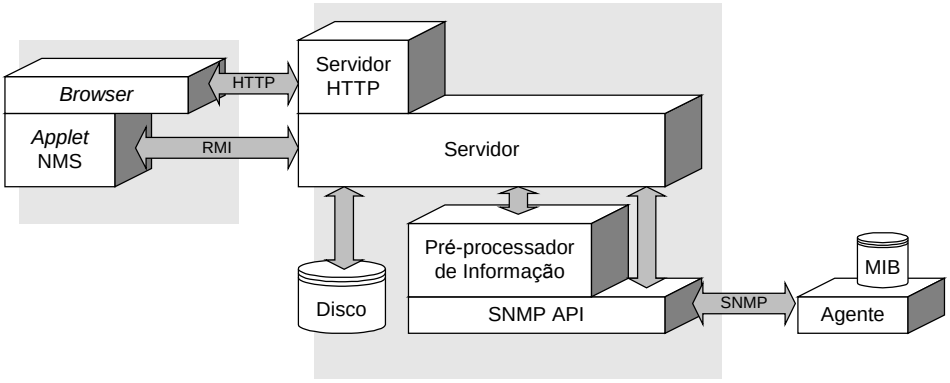


Figura 6.3 - Diagrama de blocos.

O *applet* NMS realiza funções de interface com o utilizador e pode ser executado num *browser* que contenha a máquina virtual de Java. O servidor é acompanhado por um servidor HTTP e um mecanismo de comunicação com os agentes (SNMP API). É da

responsabilidade do servidor realizar a ponte entre o *applet* e os agentes, armazenar a informação e receber notificação de eventos extraordinários (`TRAP`).

Em termos funcionais, o sistema necessita de ferramentas que permitam realizar a detecção de máquinas e agentes na rede. A informação resultante da etapa de detecção é armazenada numa estrutura de dados para posterior utilização. Devido a restrições de segurança, os *applets* não têm acesso directo ao disco, pelo que é necessário providenciar um módulo que sirva de interface entre o *applet* e o disco e entre o *applet* e a rede (Figura 6.4).

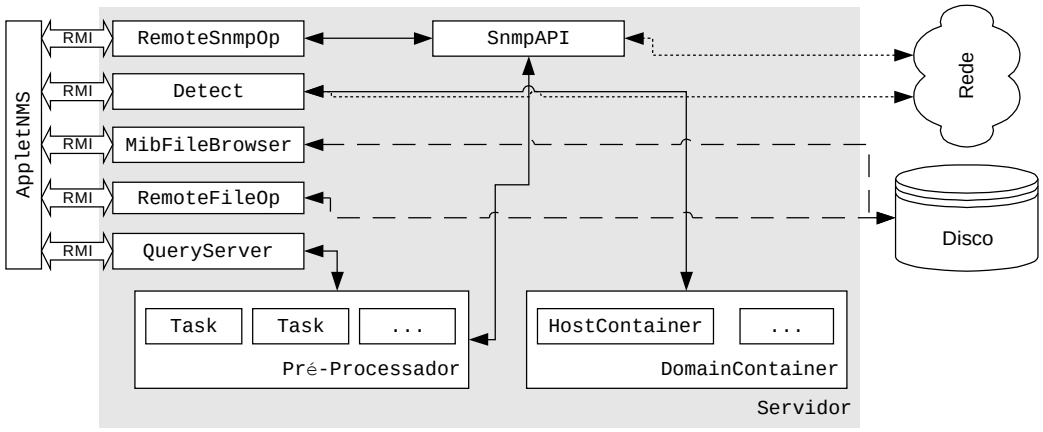


Figura 6.4 - Esquema resumido do servidor NMS.

O servidor apresenta um conjunto de módulos que servem de porta entre o *applet* e as operações a realizar no servidor:

- O módulo `RemoteSnmpOp` converte os pedidos RMI em pedidos SNMP.
- O módulo `Detect` é responsável por realizar a detecção de máquinas e actualizar o `DomainContainer` de acordo com os resultados.
- O objecto `DomainContainer` pode ser gravado e lido do disco do servidor por intermédio do `RemoteFileOp`.
- O `MibFileBrowser` faz a descodificação de ficheiros que definem as MIBs, definidas em ASN.1.
- O `QueryServer` realiza a interface entre a camada de abstracção de dados e o NMS.

6.3.1 Estrutura de Dados

As máquinas conhecidas pelo sistema encontram-se representadas numa estrutura do tipo lista ligada (Figura 6.5).

Um objecto `DomainContainer` serve como armazém de uma lista de objectos do tipo `HostContainer`. Cada objecto `HostContainer` representa um domínio ou um grupo de máquinas, distinguidos por intermédio do campo `domain`. Desta forma conseguem-se representar domínios lógicos bem como grupos específicos de funcionalidade (servidores, encaminhadores ou estações de trabalho, por exemplo). Um objecto `HostContainer`, representativo de um domínio, é distinguido de objecto

representativo de um grupo por intermédio do indicador `isDomain`. Os grupos servem para facilitar a realização de operações de gestão semelhantes em componentes de rede com as mesmas características.

Cada elemento pertencente a um `HostContainer`, ou seja, um objecto do tipo `Host`, representa uma determinada máquina, respectivamente, o seu endereço (`hostIp`), nome (`hostName`) e o estado actual (`status`) – acessível/não acessível. Se a máquina for dotada de um agente, a informação relativa a este é armazenada nas variáveis `community`, `port` e `mibs`. A detecção e/ou adição de novas máquinas implica a criação de um novo objecto `Host` e a sua adição a um `HostContainer` específico.

Esta estrutura permite representar de uma forma simplificada a topologia de uma rede local bem como criar grupos específicos de máquinas.

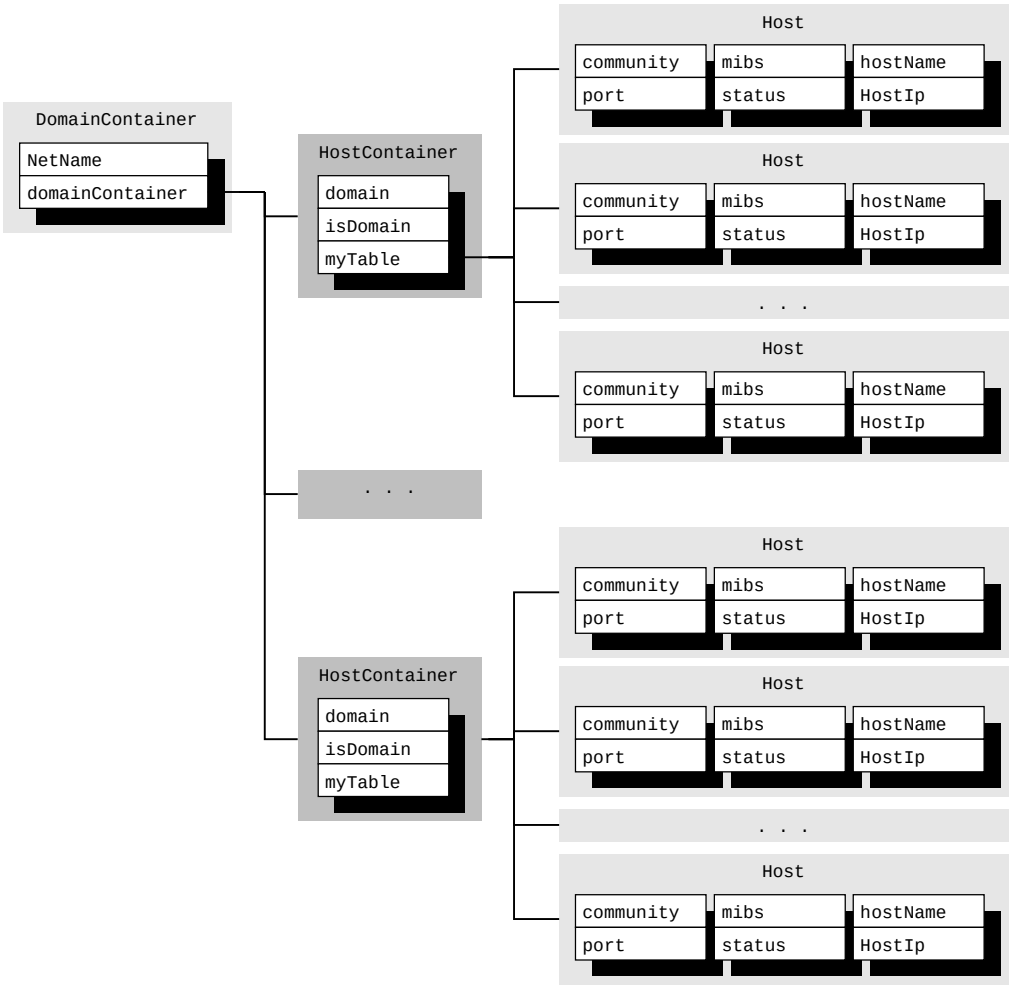


Figura 6.5 - Estrutura de armazenamento de máquinas.

6.3.2 Estrutura de Comunicação

De acordo com o diagrama de blocos apresentado na Figura 6.3, o sistema utiliza diferentes métodos para comunicar com os diferentes módulos. O *browser* utiliza o HTTP para carregar documentos, imagens e *applets* directamente do servidor WWW.

O *applet* NMS, mal é executado pelo *browser*, invoca métodos residentes no servidor como se residissem na própria máquina.

A invocação remota de métodos pressupõe, à partida, a existência de objectos clientes, que realizam as chamadas, objectos servidores, que fornecem a implementação dos métodos e um mecanismo de registo (`RMIRegistry`) (Figura 6.6).

O comportamento do objecto servidor é descrito por uma interface específica. Quando este é criado, efectua o seu registo com base num nome (*string*) de modo a ser reconhecido quando o cliente o requisitar. Em adição, é criado um objecto *Skeleton* que tem a responsabilidade de encaminhar a chamada para o objecto servidor.

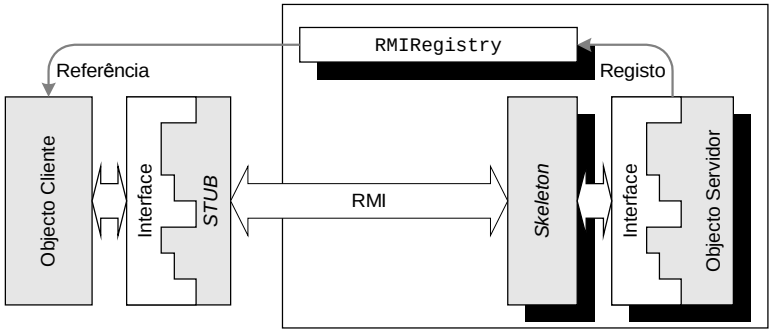


Figura 6.6 - Mecanismo de invocação remota de métodos.

No lado do cliente, é criado um objecto *Stub*, que define a mesma interface que rege o comportamento do objecto servidor. O *Stub* constitui um espelho local do servidor. O objecto cliente consulta a referência ao objecto remoto no `RMIRegistry` e invoca os métodos directamente sobre o *Stub* que, por sua vez, encaminha para o *Skeleton* correspondente. Os valores devolvidos seguem o caminho inverso.

Para o caso particular do NMS, as chamadas RMI são efectuadas sempre que é necessário gravar ou ler uma estrutura `DomainContainer` ou sempre que é efectuada uma consulta a um agente, caso em que a invocação é convertida em mensagens SNMP. Em resumo, o mecanismo RMI permite circundar as limitações de segurança de que os *applets* são alvo simulando a sua execução directamente no servidor.

A comunicação entre o servidor e os agentes é efectuada por SNMP, mais particularmente, por SNMPv1. A API utilizada foi desenvolvida pela *Advent Network Management, Inc*. [Advent97], uma empresa especializada no desenvolvimento de soluções de gestão em ambiente WWW. A API é de domínio público sem quaisquer restrições relativamente à sua utilização.

A API permite dotar as aplicações desenvolvidas com suporte de SNMP. Para o efeito apresenta módulos específicos para lidar com os diferentes aspectos da comunicação, nomeadamente a construção de PDUs, a interpretação de ficheiros descritivos de MIBs e o mecanismos de controlo da comunicação. Em traços gerais, o controlo de várias sessões de comunicação é efectuado por um objecto do tipo `SnmpAPI`, que, por intermédio de `Threads` pode monitorar várias sessões em simultâneo. Cada sessão é representada por um objecto do tipo `SnmpSession`. É por intermédio deste objecto que se enviam e recebem PDUs. Cada PDU é construído pela instanciação de um objecto do tipo `SnmpPDU`. Este contém informação acerca do endereço, comunidade, porto, versão e os objectos de gestão.

De forma simplificada, o NMS apresenta os seguintes tipos de comunicação:

- HTTP – efectua o arranque do sistema com o envio do *applet* para o *browser*.
- RMI – a comunicação entre o *applet* e o servidor é efectuada segundo um mecanismo de invocação remota de métodos específico da plataforma de execução Java.
- SNMP – a consulta e manipulação de informação de gestão é efectuada por SNMP, não inviabilizando a possibilidade de utilização de outros protocolos ou arquitecturas.

6.3.3 Interface NMS

A correcta utilização do SGR depende fortemente da interface com o utilizador. Se esta não for simples, intuitiva e extensível não haverá vantagens na utilização do sistema, pelo que muito do esforço de desenvolvimento incidiu sobre a interface com o utilizador.

A interface com o utilizador, neste caso o gestor da rede, deve reflectir o estado da rede e dos componentes que a formam, além de representar a forma como estes se encontram organizados. A organização pode apresentar diversas formas e segue geralmente algum agrupamento lógico – informação topológica. Algumas plataformas de gestão optam por uma representação esquemática de ligações, onde são visualizadas linhas entre diversos componentes. Alguns autores apresentam diferentes soluções para a interface, por exemplo baseada numa folha de cálculo [Sethi94]. No caso do sistema aqui apresentado foi adoptada uma filosofia tipo Explorador de Ficheiros [Vieira97] (Figura 6.7).

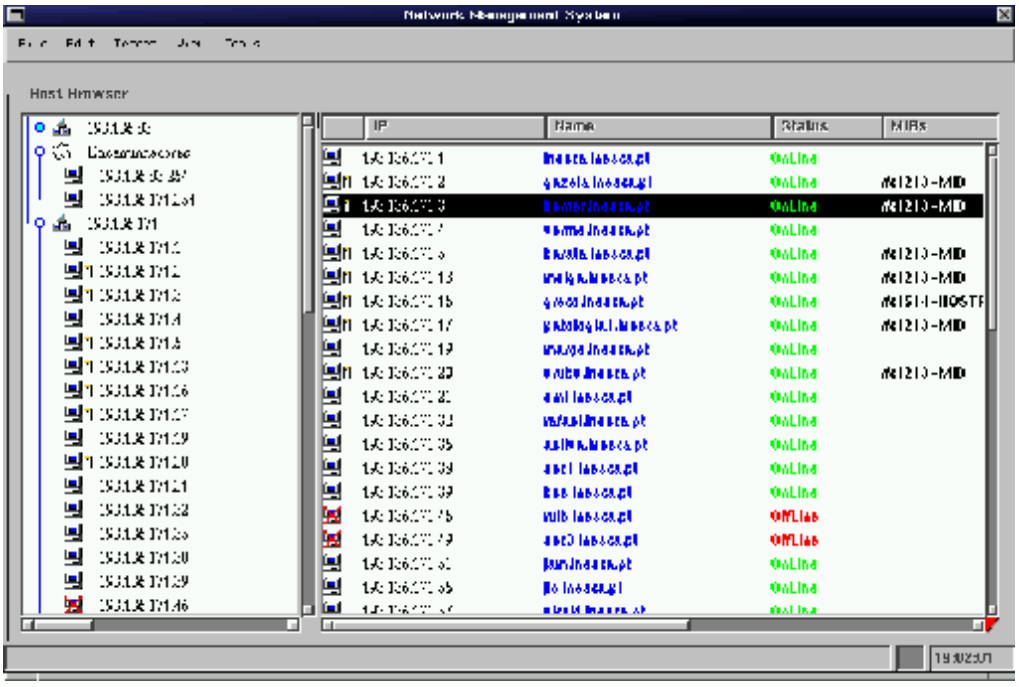


Figura 6.7 - Interface baseada no conceito de Explorador.

De entre as vantagens de uma interface deste tipo, apresentadas por [Moreau94], podem-se indicar a facilidade de operação e a visualização intuitiva de uma estrutura hierárquica.

O elemento raiz consiste num objecto do tipo `DomainContainer`, que pode conter diversas ramificações.

Cada uma das ramificações representa um domínio () ou um grupo (). Estes, por sua vez, contém ramificações para cada um dos componentes () que o constituem.

O sistema mantém uma monitorização periódica do estado de conectividade (acessível/não acessível) de cada uma das máquinas. O estado é representado graficamente por intermédio de um X () se a máquina não se encontrar acessível, ou por se encontrar desligada ou por existirem problemas de ligação.

6.3.4 Operação

O sistema é iniciado por intermédio de uma ligação ao servidor WWW. O *applet* é carregado (Figura 6.8) e a janela de operação surge (Figura 6.7).

Figura 6.8 – Carregamento do *applet*.

No momento de instalação, o sistema não conhece as máquinas que fazem parte da rede. O passo inicial é detectar um determinado domínio ou conjunto de domínios. Opcionalmente, o utilizador pode desejar detectar a presença de agentes SNMP (Figura 6.9).

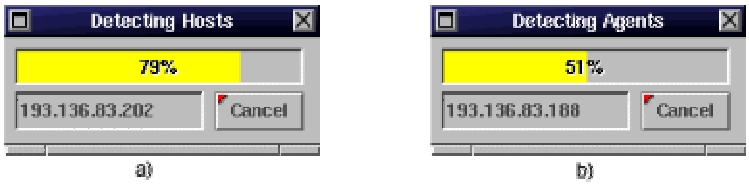


Figura 6.9 – Detecção de:
a) máquinas; b) agentes.

Neste caso, o sistema tenta realizar uma ligação SNMP e, em caso de sucesso, descobrir que tipo de MIBs se encontram presentes. No caso de ser detectado um agente, a figura é complementada com um pequeno cilindro ( ).

A informação gerada na fase de descoberta da rede é armazenada em objectos do tipo `Host`.

O lado direito da janela principal apresenta informação acerca dos componentes visualizados, nomeadamente, o seu endereço, o nome, o estado e as MIBs que o agente define.

Uma das ferramentas que acompanha o sistema é o clássico *browser* de MIBs (Figura 6.10).

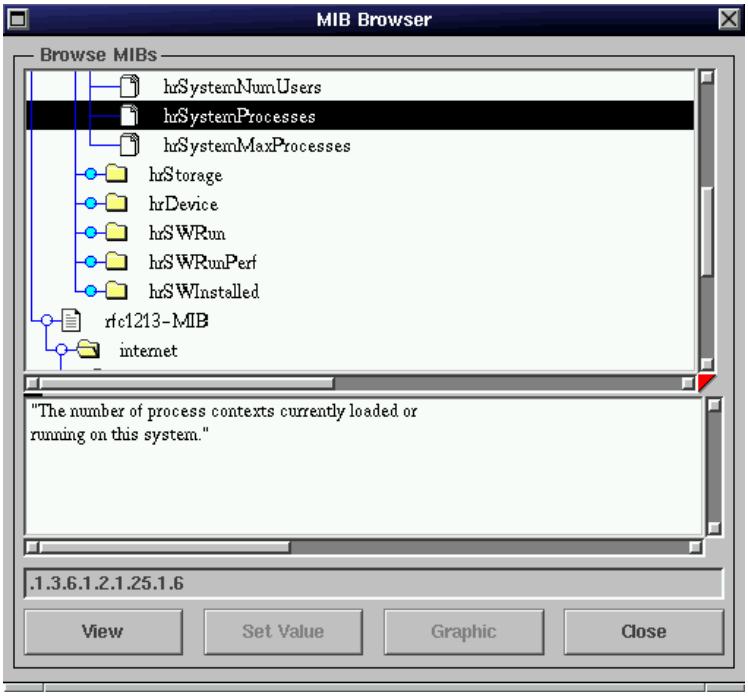


Figura 6.10 – *Browser* de MIBs.

O *browser* de MIBs permite seleccionar um objecto e, de acordo com o tipo ASN.1, visualizar o seu valor (*View*), ajustar o seu valor (*Set Value*) ou construir um gráfico (*Graphic*). A janela apresenta-se dividida em três partes principais: a árvore de objectos na parte superior, a descrição do objecto seleccionado na parte intermédia e um painel de controlo na parte inferior. Neste painel é possível visualizar o OID do objecto e seleccionar o tipo de operação a realizar.

O tipo de objecto é representado de acordo com as seguintes figuras:

- - Ficheiro MIB. Representa o ficheiro usado na interpretação.
- - Nó da MIB. Cada nó contém mais nós, tabelas ou objectos.
- - Objecto de gestão.
- - Tabela.

Dependendo do tipo de dados do objecto seleccionado (numérico ou não numérico), a tecla *Graphic* fica activa, permitindo visualizar um gráfico com amostras tiradas periodicamente (Figura 6.11). O período de amostragem e o período total de visualização podem ser configurados por acção nas teclas *Setup PoolTime* e *Setup Axis*.

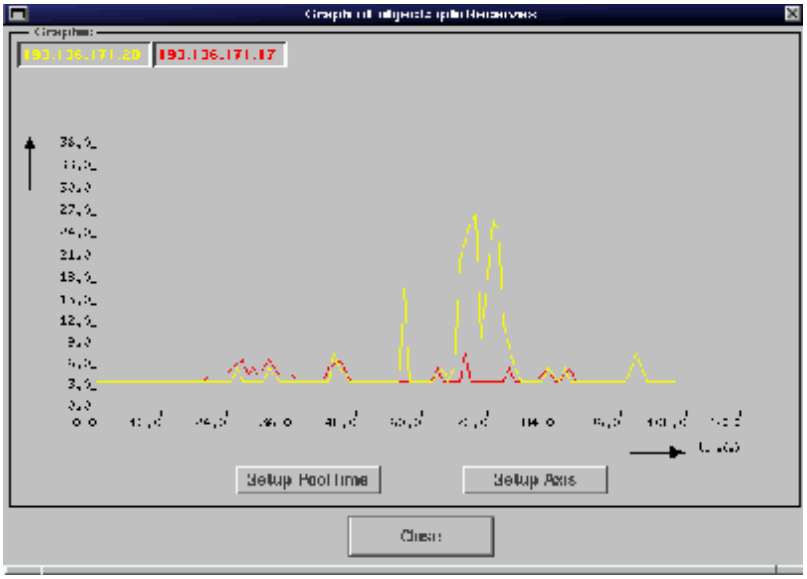


Figura 6.11 – Gráfico de `ipInReceives` de duas máquinas.

Os objectos com acesso de leitura e escrita (`RWRITE`) ou só de escrita (`WONLY`) activam a tecla *Set Value* que permite ajustar parâmetros (Figura 6.12).

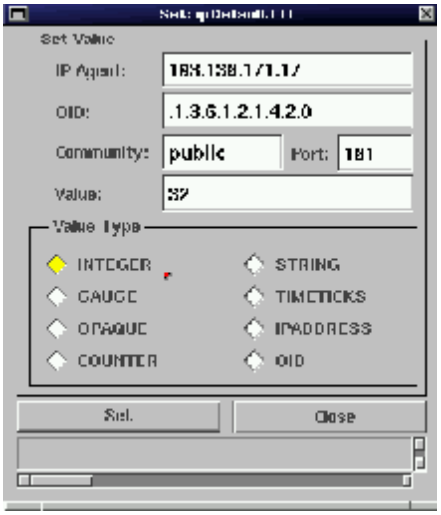


Figura 6.12 – Ajuste do valor `ipDefaultTTL` no agente 193.136.171.17.

6.3.5 Camada de Abstracção de Informação

A informação proveniente dos agentes é filtrada pelo pré-processador de informação. Este tem como objectivo providenciar um conjunto de mecanismos capazes de construir diferentes formas de ver a informação de gestão.

A camada de abstracção de informação assenta no conceito de tarefas. Cada tarefa é definida por um objecto do tipo `Task` que encapsula a seguinte informação:

- `Name` – nome pelo qual é identificada a tarefa.
- `Function` – referência para um objecto do tipo `Function`.
- `Start` – define o instante temporal em que a tarefa inicia a sua operação. Este apresenta-se como uma cadeia de caracteres (`String`) com o formato "yyyy.MM.dd.hh.mm.ss" onde yyyy define o ano, MM define o mês, dd representa o dia e hh, mm, ss definem a hora, minutos e segundos, respectivamente.
- `Period` – define o período de repetição da tarefa. O formato é o mesmo usado para o `Start`.
- `End` – instante a partir do qual a tarefa deixa de ser executada.
- `Status` – estado de execução da tarefa. Pode assumir os valores `RUNNING` ou `STTOPED`.

A definição da operação passa pela construção de funções matemáticas sobre a informação de gestão. Para o efeito, são criadas funções básicas que podem ser encadeadas para criar funções mais complexas. As funções básicas são classificadas em três categorias:

- Funções algébricas simples: soma, subtracção, divisão e multiplicação.
- Funções algébricas complexas: média, derivada, etc.
- Funções gerais: ***threshold***, correio, aviso, gráfico, registo, etc.

Cada função define uma interface específica (`AgentQuery`) que permite encadear qualquer função como argumento de outra e, consequentemente, definir funções mais complexas. A interface `AgentQuery` é definida como se segue:

```
package pt.ua.nms.query;
import java.util.NoSuchElementException;

/** Every query operation must implement AgentQuery. This maintains
 * consistency over Query Filters.*/

public interface AgentQuery {
/** Each AgentQuery must return a String value
 * associated to an OID */

public Object getValue(String oid) throws NoSuchElementException;
public void query() throws AgentException;

/** Make a query to an SNMP Agent. The results are stored and returned
 * by getValue(String).*/
public void query(String[] oids) throws AgentException;
}
```

Na prática, cada função é derivada (em termos de OO) de uma classe comum (Figura 6.13). As funções definidas pela classe comum permitem definir um comportamento idêntico para todas as classes derivadas. Este facto permite encadear um número de funções de modo a tornar possível a construção de funções complexas com base nas existentes.

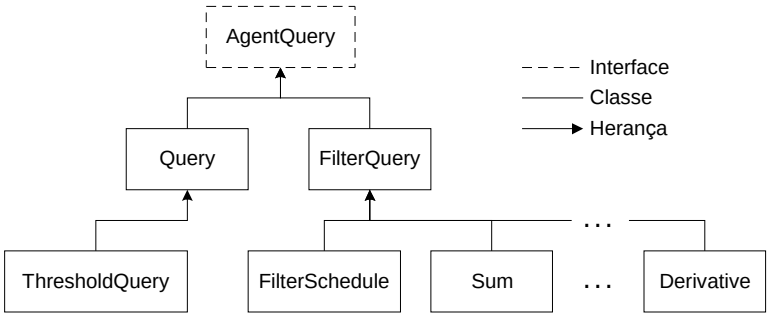


Figura 6.13 – Árvore de herança das classes de funções.

A definição de uma operação com base numa função mais complexa é definida encadeando objectos da seguinte forma:

```
...
agentObject = new Query(...);  // Generic Query
schedule = new Schedule(...);  // Sheduling definition
AgentQuery query = new FilterSchedule(schedule,
  new ThresholdQuery( boundListener,
  lowerLimit, upperLimit, agentObject));
...
```

No exemplo anterior, o objecto `query` representa uma consulta periódica (`FilterSchedule`) sobre o `agentObject` (que, por sua vez, representa uma consulta genérica). Se o valor exceder os limites definidos por `lowerLimit` e `upperLimit` será enviada uma notificação ao objecto `boundListener` que, em termos de implementação define um método – `actionPerformed()` – invocado se determinado evento acontecer (Figura 6.14).

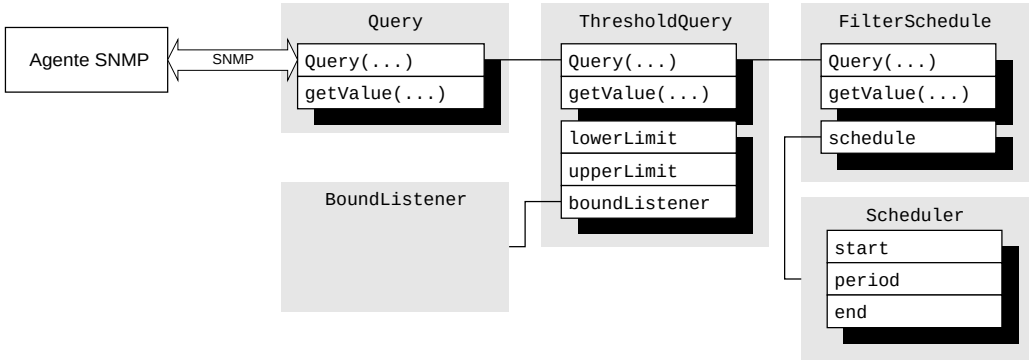


Figura 6.14 – Encadeamento de funções.

Este processo permite associar qualquer número de funções em qualquer ordem e, consequentemente, definir uma operação mais complexa.

Para o utilizador, o desenvolvimento de uma tarefa de gestão é efectuada graficamente, com o auxílio de um assistente. A primeira fase consiste na selecção da função (Figura 6.15).

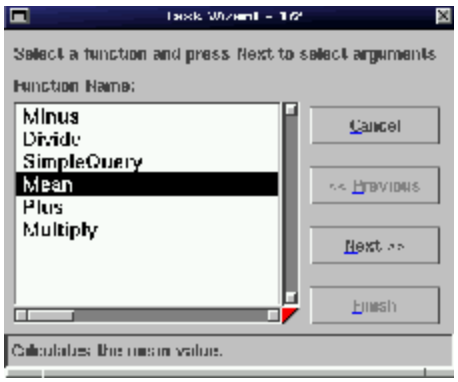


Figura 6.15 – Assistente de funções 1/2.

O passo seguinte passa pela selecção dos argumentos da função (Figura 6.16).

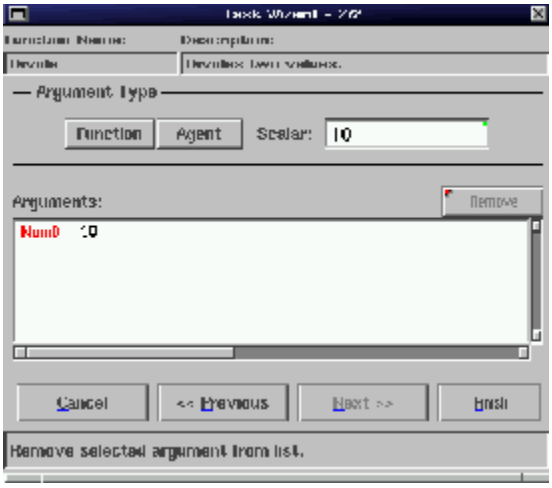


Figura 6.16 – Assistente de funções 2/2.

Os argumentos, dependendo da função, podem ser:

- O resultado de uma outra função (encadeamento).
- Uma constante.
- Um OID.

Após a definição da função é necessário definir a calendarização, onde se indica o tempo de início, o período e o instante a partir do qual a operação deixa de ser realizada. No caso de estar definido apenas o início, a operação será executada apenas uma vez. Se não for definido apenas o fim, a operação será executada periodicamente, terminando quando o gestor o desejar.

A calendarização é definida graficamente na janela *Task Planner* (Figura 6.17). O lado esquerdo da janela apresenta um calendário que permite seleccionar o ano, mês e dia, bem como a hora, minuto e segundo.

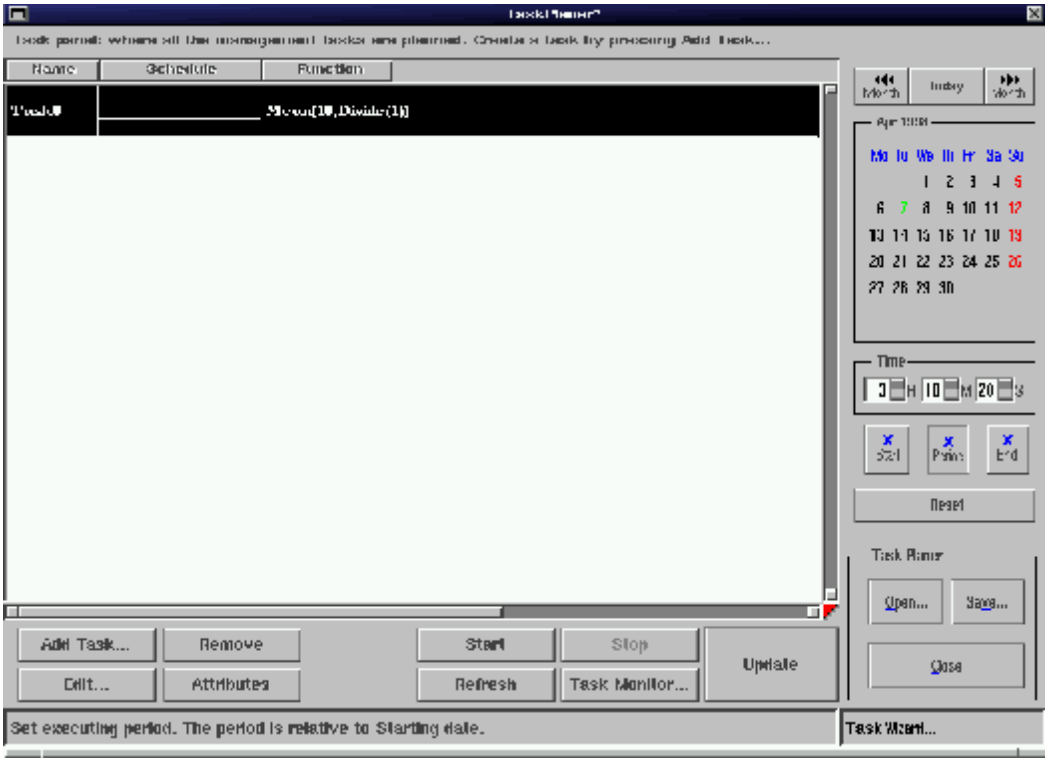


Figura 6.17 – Janela de definição de tarefas.

Após a definição da tarefa é necessário actualizar o servidor onde esta vai ser executada. O conjunto de tarefas define uma camada de abstracção de informação de gestão.

6.4 Conclusões

O trabalho desenvolvido traduz um primeiro passo para o desenvolvimento de um sistema simples mas suficientemente poderoso para coadjuvar na gestão de uma rede local de comunicação de dados. Existem alguns pormenores que merecem nova e melhorada abordagem.

Ao nível de interface falta comprovar se o conceito utilizado na abstracção de dados é sugestivo e eficaz num cenário de gestão de redes e, em caso afirmativo, avançar para o desenvolvimento de novas ferramentas que permitam tomar decisões sem intervenção directa do utilizador.

O mecanismo de procura inicial prevê apenas descoberta de máquinas por consulta e eco (*ping*). Este processo está actualmente a ser reforçado por uma ferramenta de consulta de DNS (*Domain Name Server*). Futuramente, prevê-se a integração de ferramentas de descoberta mais eficientes, baseadas na consulta de tabelas de encaminhadores ou na utilização de agentes específicos de descoberta de topologia [Ptopo98].

Um aspecto importante a considerar é a definição de perfis de trabalho, ou seja, soluções pré-definidas para sub-grupos de utilizadores. O objectivo é especificar uma estrutura que permita definir o acesso a um determinado tipo de informação e a determinados serviços de acordo com um perfil (por exemplo, impressoras ou

servidores WWW). Neste sentido é importante considerar quais as MIBs, que tipo de informação e que meta-variáveis interessam a um determinado perfil.

O desenvolvimento e integração de ferramentas de decisão automática permitirá aliviar o gestor de tarefas repetitivas e monótonas. Neste sentido, a utilização de tecnologia de inteligência artificial ou de mecanismos de controlo baseados em *fuzzy logic* deverão ser investigados para o desenvolvimento de um paradigma que permita resolver de forma automática alguns problemas de funcionamento que possam surgir.

7 CONCLUSÕES E PERSPECTIVAS FUTURAS

As dificuldades iniciais do projecto e da instalação de uma rede de comunicação de dados podem ser minimizadas por um conhecimento sólido e actualizado da variedade de equipamento e configurações existentes. Esta dissertação principiou com a apresentação e a discussão das principais topologias de rede, das suas vantagens e das suas lacunas, com o objectivo de propor configurações que permitam tirar o melhor partido do equipamento. Os componentes de rede representam um papel fundamental no desempenho de uma rede pelo que foi feito um estudo no qual se discutem as principais características de funcionamento de vários componentes de extensão e interligação.

A crescente dependência dos utilizadores de computadores face às redes de comunicação de dados, bem como o desenvolvimento de novas aplicações suscitam a necessidade de maiores velocidades de transferência de informação. Neste sentido, a variedade de escolha justifica um estudo sobre tecnologia capaz de aumentar a velocidade de transferência de informação. A *Fast Ethernet* e a *Gigabit Ethernet* ameaçam prolongar o sucesso do Ethernet, embora o método de acesso apresente algumas lacunas para velocidades de transferência elevadas. Várias são as suas concorrentes, pelo que a opção deve passar pela análise dos requisitos e correlaciona-los com as características particulares de cada solução. Como complemento foi feito um estudo das tecnologias mais divulgadas com método de acesso diferente do CSMA/CD.

A instalação de uma rede não termina na instalação de equipamento, pelo que a dissertação continua com a apresentação de várias arquitecturas de gestão "clássicas". Os protocolos e arquitecturas de gestão não são compatíveis a nível de protocolo nem a nível de modelo de informação. No caso do SNMP, a versão mais utilizada remonta já há cerca de 10 anos. As versões posteriores não alcançaram a popularidade esperada, pelo que os avanços nesta área estiveram bastante limitados. Em relação à versão mais recente (SNMPv3) espera-se que venha vencer a inércia e o descontentamento de que algumas versões anteriores foram alvo.

Os serviços baseados na WWW (*World Wide Web*) apresentam uma interface bem conhecida (*web browser*) e ainda a capacidade de serem executados em várias plataformas. Estas são, em parte, as características responsáveis pela sua grande divulgação. A vulgaridade dos chamados *browsers* e a tendência actual para a integração de múltiplos serviços possibilita a coexistência de vários tipos de informação, de uma forma local ou distribuída. Estas características tornam a tecnologia igualmente adequada para a integração de diversas soluções de gestão normalizadas ou proprietárias. Nesta área a linguagem Java apresenta-se como uma excelente opção para o desenvolvimento de aplicações com execução em *browsers*, aliando o poder do WWW com a flexibilidade de uma linguagem de programação.

O planeamento de uma rede local de comunicação de dados deve apresentar soluções que visem auxiliar a gestão de falhas que possam ocorrer durante o período de utilização. Com este objectivo encontra-se em desenvolvimento uma aplicação distribuída de gestão de redes baseada na linguagem Java e na arquitectura SNMP. Resultante do meio académico, o sistema constitui uma plataforma de gestão para o desenvolvimento e o estudo de soluções e ferramentas de gestão. O sistema foi construído tendo em vista a simplicidade de utilização e a independência de plataforma. A sua instalação foi efectuada com sucesso em qualquer plataforma dotada de um servidor HTTP e de um interpretador Java.

Durante a fase de desenvolvimento algumas dificuldades surgiram, nomeadamente as restrições de segurança que incidem sobre as *applets* (resolvidas por intermédio de uma aplicação servidora) e a ausência de possibilidade de acesso a alguns recursos específicos, tais como o ICMP (utilizado para o teste de conectividade).

Existem conceitos e ferramentas que se procuram testar no sistema de gestão. Actualmente está a ser integrada uma ferramenta de descoberta de máquinas por intermédio de consultas ao servidor de nomes. Adicionalmente, estão a ser investigadas soluções de gestão automáticas que visam aliviar a sobrecarga causada por algumas tarefas repetitivas, com base na agendagem de operações. Futuramente poderá ser investigada a integração de ferramentas de decisão automática baseadas em redes neuronais ou em algoritmos de controlo *fuzzy*.

O cenário actual de desenvolvimento de aplicações distribuídas encontra-se dividida em duas frentes: CORBA, suportada por mais de 800 empresas e DCOM, solução proprietária da Microsoft. Em comum apresentam a possibilidade de distribuir objectos por ambientes heterogéneos (começam a existir versões do Windows/DCOM para diferentes plataformas). Os acessos via CGI/HTTP começam a ser substituídos por chamadas remotas a métodos, uma evolução dos RPCs para objectos. A tecnologia de componentes de *software* parece começar a ter bases sólidas para se consolidar. As aplicações de gestão, pela sua natureza distribuída, poderão tirar proveitos com a integração destes processos.

Apêndice A Estrutura de Cabos

A.1 Introdução

O envio de informação de um emissor para o respectivo receptor implica, obrigatoriamente, a existência de um canal de transmissão. A voz percorre o espaço livre da atmosfera destinada ao ouvido de um receptor, assim como o papel serve de suporte para estas linhas de texto. No caso particular de uma rede local de comunicação de dados, o canal de transmissão é constituído por cabos de cobre ou fibra óptica, mais adequados a suportar informação digital.

A estrutura de cabos é a espinha dorsal e a base de suporte de qualquer rede local de comunicação de dados. Um sistema devidamente projectado, instalado e administrado reduz os custos de cada uma das fases do ciclo de vida de qualquer rede de comunicações: instalação, actualização, manutenção e administração.

O canal de transmissão, como parte integrante da rede, reúne grande parte da responsabilidade de bom funcionamento:

- Uma rede de comunicação de dados nunca é mais rápida ou mais segura do que o permitido pelo sistema de cablagem.
- O sistema de cablagem é o componente mais duradouro de uma rede de comunicação de dados.

Uma boa estrutura de cabos permite assegurar o investimento sobre os avanços da tecnologia, aumentado o ciclo de vida útil daquela.

A.2 Documentos e Normas

A inexistência de normas regulamentares da estrutura de cabos de comunicação de dados antes de 1991, levou a que esta fosse controlada pelos fabricantes de material informático. Os clientes, apanhados entre conflitos comerciais, eram obrigados a pagar preços elevados de instalação e administração de sistemas proprietários. A indústria de telecomunicações apercebeu-se da necessidade de um sistema que pudesse suportar o maior número possível de aplicações e equipamento. A *Electronic Industries Association* (EIA), *Telecommunications Industry Association* (TIA) e um grande número de empresas do ramo trabalharam sobre um documento que viria a normalizar o sistema de cablagens de telecomunicações para edifícios comerciais: ANSI/EIA/TIA-568-1991. Desde essa altura que novos documentos e normas se foram acumulado, levando à revisão da ANSI/EIA/TIA-568-1991 no ano de 1995, sendo agora referida por ANSI/EIA/TIA-568-A. Nesse mesmo ano, a *International Standards Organisation* (ISO) em conjunto com o *International Electrotechnical Committee* (IEC) completou um conjunto de normas sobre o mesmo assunto, o ISO/IEC 11801. Um sumário das normas de cablagem para redes locais de comunicação de dados pode ser encontrado em [Microtest97].

O objectivo destas normas é definir uma "cablagem estruturada": um sistema de cabos de telecomunicações que possa suportar qualquer tipo de aplicação que o utilizador escolha, seja ela a transmissão de voz, imagens ou dados. As normas EIA/TIA 586A e ISO/IEC 11801 acabaram com o debate sobre a impedância e a blindagem para as distribuições vertical e horizontal até aos 100 MHz. Estão, também, normalizados os cabos de par entrançado blindado (STP) até aos 300 MHz. Existem já cabos de par

entrançado que suportam frequências até 600 MHz, com vista a servirem de suporte ao ATM a 622 Mbps. Estes cabos aguardam ainda normalização [Kish97].

Existem mais alguns pontos de regulamentação de cablagem de telecomunicações: compatibilidade electromagnética e especificações de ordem mecânica e ambiental. A Comunidade Económica Europeia (CEE) emitiu directivas respeitantes a perturbações electromagnéticas e a imunidade a essas perturbações sobre um conjunto de materiais, englobando as redes de distribuição e transporte de energia eléctrica, as redes de telecomunicações e o *hardware* de processamento de informação. Uma delas é a directiva 89/336/CEE de 3 de Maio de 1989 [Cee89]. Entrou em vigor dia 1 de Janeiro de 1996, dando algum tempo aos fabricantes para vender produtos já desenvolvidos e dando-lhes tempo para conceberem novas ofertas capazes de responder às directivas de Compatibilidade Electromagnética (CEM).

As especificações de ordem mecânica e ambiental regulamentam os aspectos de segurança relativos a incêndios e ao meio ambiente onde se inserem, seja ele interior ou exterior.

A.3 Tipos de cabos

Os tipos de cabos mais utilizados na transmissão de dados em edifícios comerciais ou particulares são de três tipos: coaxial, par entrançado e fibra óptica.

A.3.1 Coaxial

O cabo coaxial é constituído por um condutor central rodeado por um isolador e por uma malha de blindagem concêntrica (Figura A.1).

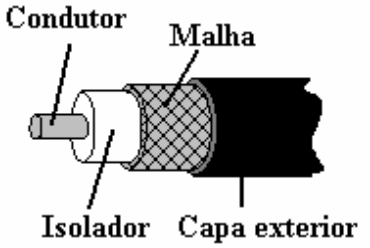


Figura A.1 – Cabo coaxial.

O condutor central, geralmente, é de cobre, bem como a malha. O isolador pode ser de qualquer tipo, inclusive ar. Normalmente, os cabos utilizados na comunicação de dados usam polietileno de vinilo. Este é, de igual modo, o material usado no fabrico da capa exterior que protege o cabo das condições adversas do meio envolvente.

Grande parte das redes Ethernet, com topologia linear, usam cabos coaxiais de 50 Ohm, que podem ser de dois tipos: grosso ou fino. O cabo coaxial grosso (ϕ_E=10,26mm) conheceu os seus tempos de glória com o aparecimento das redes Ethernet, actualmente pouco utilizado. O fino (ϕ_E =6,35mm) veio em sua substituição para distâncias até 180m. Actualmente encontra-se ameaçado pelo crescimento da fatia de mercado do par entrançado.

A.3.2 Par entrançado

Na actualidade, praticamente toda a estrutura de telecomunicações dos edifícios tem, como suporte, cabos do tipo par entrançado. Regra geral, grande parte dos edifícios

construídos actualmente incorpora, de origem, vários pares livres que podem ser utilizados em troços de uma rede local de transmissão de dados. Devido à sua configuração, este torna-se mais adequado à passagem em condutas saturadas que o cabo coaxial, difícil de dobrar e moldar. O preço de comercialização é consideravelmente mais baixo que a fibra óptica ou mesmo o coaxial. Este conjunto de características coloca os cabos de pares entrançados num ponto favorável de decisão para projecto e instalação de redes locais de comunicação de dados.

O cabo de pares entrançados é constituído por vários condutores interlaçados, rodeados por um isolador (Figura A.2). Em caso de ausência de blindagem o cabo é identificado por UTP - *Unshielded Twisted Pair*. Se existir uma fita de blindagem para cada par (normalmente em alumínio) e uma global (normalmente em cobre) (Figura A.2 - direita) o cabo é denominado STP - *Shielded Twisted Pair*.

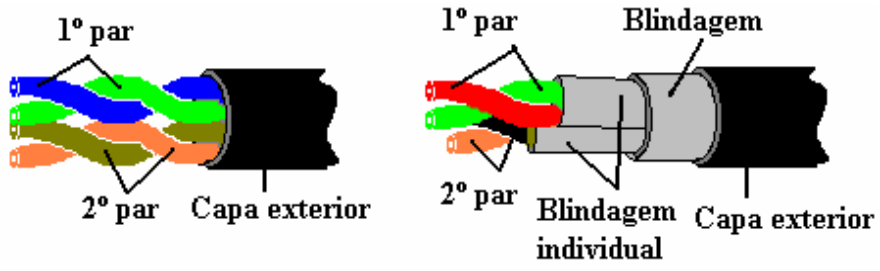


Figura A.2 – Cabo de pares entrançados:
esquerda: UTP; direita: STP.

É ainda fabricado um intermédio entre os dois tipos apresentados, em que os pares existentes são protegidos por uma blindagem global, denominado *Screened Twisted Pair* (Figura A.3).

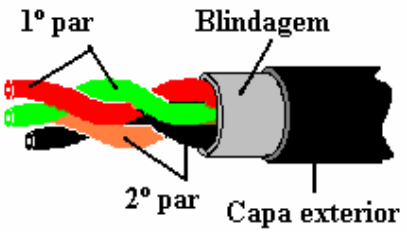


Figura A.3 – *Screened Twisted Pair*.

A torcedura que caracteriza cada par de condutores é efectuada de forma a atenuar influências electro-magnéticas, que resultam em diafonia ou paradiafonia. A diafonia é um fenómeno que afecta um canal de transmissão - como um par entrançado - e traduz-se em ruídos que perturbam a comunicação, seja ela de voz, dados ou imagem. A paradiafonia é a medida de diafonia entre dois pares. Tanto a diafonia como a paradiafonia são medidos em decibéis (dB). Os pares são identificados segundo um código de cores bem definido [Derfler93].

O cabo UTP, usado na comunicação de dados, pode ser especificado segundo uma de três categorias de capacidade de transmissão:

- Categoria 5: Características de transmissão especificadas até 100 MHz.

- Categoria 4: Características de transmissão especificadas até 20 MHz.
- Categoria 3: Características de transmissão especificadas até 16 MHz.

A.3.3 Fibra óptica

O cabo de fibra óptica é constituído por um ou mais condutores ópticos. Estes são construídos com base em minúsculas fibras de vidro. Cada fibra do guia de luz é constituída por duas espécies de vidro, com índices de refracção diferente. Os diferentes índices de refracção asseguram que, quando se faz incidir luz numa extremidade, esta ziguezagueie ao longo de todo o comprimento da fibra, mesmo quando o cabo estiver dobrado (Figura A.4).

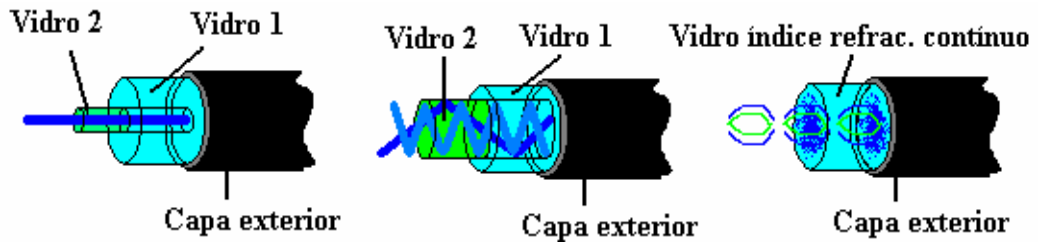


Figura A.4 – Cabos de fibra óptica:
esquerda: monomodo, centro e direita: multimodo.

Em telecomunicações, as fibras ópticas são reunidas num cabo, no qual estão envolvidas por materiais de protecção e de enchimento, reforçados por uma alma de nylon ou aço. Nas fibras de índice de refracção descontínuo (Figura A.4 – esquerda e centro), um núcleo com elevado índice de refracção é envolto por uma camada de outra espécie de vidro, com índice de refracção inferior. Nas fibras de índice de refracção contínuo (Figura A.4 – direita), o índice de refracção varia de uma forma contínua radial, sendo máximo no centro e mínimo na periferia. Os raios luminosos efectuam, então, trajectórias curvas.

Actualmente, fabricam-se fibras de dois tipos diferentes: monomodo e multimodo. Na transmissão multimodo uma fibra espessa dá espaço para que a luz passe ao longo dela segundo mais de 1000 padrões diferentes de ondas, com tempos de propagação diferente. Na transmissão monomodo, o fino núcleo - apenas oito vezes mais largo que o comprimento de onda da luz infravermelha utilizada - impõe à luz um padrão único e regular de onda.

O comprimento de onda da luz transportada mais utilizada é de 850 nm e 1300 nm. Comprimentos de onda de 1550 nm também são comuns em telecomunicações, mas apenas para ligações de longa distância (cerca de 100 km), portanto, menos utilizada em LANs.

Para a transmissão em monomodo temos os valores de atenuação apresentados no Figura A.5 [Dutton95].

Presentemente já se fabricam cabos de fibras ópticas construídas com base em plástico, substituindo a fibra de vidro. Estes cabos têm um preço significativamente inferior mas atenuações bastante superiores.

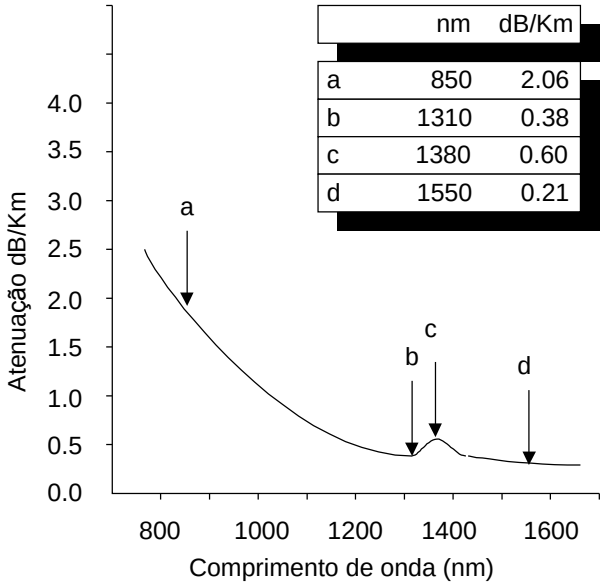


Figura A.5 – Atenuação espectral (fibra monomodo típica).

Para a transmissão em multimodo os valores de atenuação são superiores, comprovando a menor distância percorrida pelos sinais (Figura A.6).

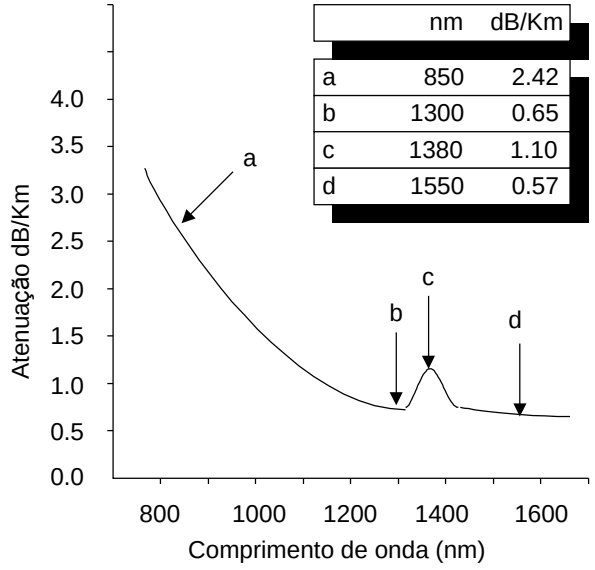


Figura A.6 – Atenuação espectral (fibra multimodo típica).

A.4 Estrutura de cabos

As normas EIA/TIA 568A e a ISO/IEC 11801, além de ditar as opções e características físicas inerentes ao meio de transmissão, distâncias máximas e mínimas para os segmentos, também cobrem opções topológicas. A estrutura é dividida em duas áreas principais: as ligações horizontais e as verticais [Derfler93] (Figura A.7).

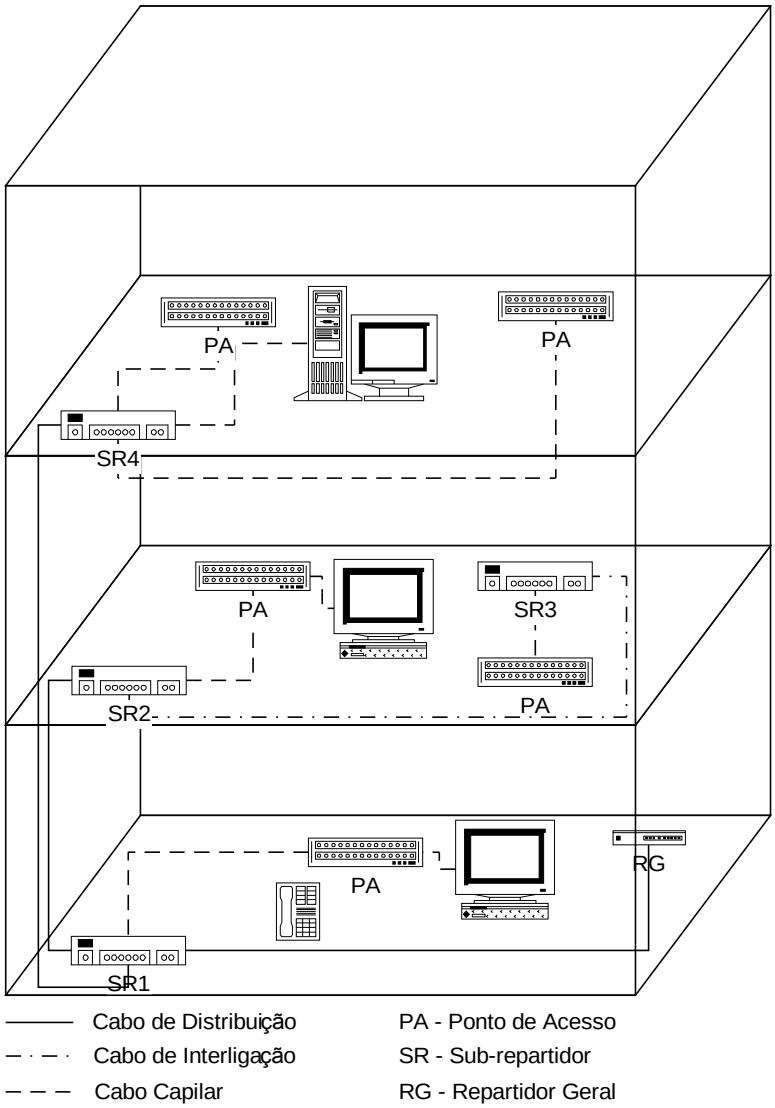


Figura A.7 – Arquitectura geral de um sistema de cablagem estruturada.

A.4.1 Cablagem Vertical

O sistema de ligações verticais especifica os troços de comunicação entre armários, salas e locais de entrada (Figura A.7 – Cabo de distribuição e Cabo de interligação). Este pode ser constituído por cabos coaxiais, de par entrançado UTP, STP ou de fibra óptica. As distâncias envolvidas são, geralmente, superiores a 500 m. O *backbone* também se pode estender a ligações entre edifícios num *campus*. Os cabos especificados para ligações verticais são os seguintes:

- Coaxial grosso, usado no 10BASE5, com 500 m de comprimento máximo.
- UTP de 100 Ω. A quantidade de pares depende da área a abranger, sendo comuns cabos de 25 pares ou mais. A distância máxima admitida é de 500 m.
- STP de 150 Ω. A distância máxima admitida é de 700 m.

- Fibra óptica multimodo 62,5/125 μm. Tipicamente são usados cabos com 6 ou 12 fibras. As fichas devem ser de cor bege. A distância máxima admitida é de 2 km.
- Fibra óptica monomodo 10/125 μm. Tipicamente são usados cabos com 6 ou 12 fibras. As fichas devem ser de cor azul. A distância recomendada é de 10 km.

As ligações verticais devem seguir uma configuração em estrela ou árvore, desde que não haja mais que dois níveis hierárquicos. Devem ser sempre respeitadas distâncias mínimas a fontes de interferência electromagnética. Para ligações entre edifícios com potenciais de terra diferentes a fibra óptica é recomendada.

A.4.2 Cablagem horizontal

O sistema de cablagem horizontal estende-se do armário de telecomunicações até ao local de trabalho (Figura A.7 – Cabo Capilar). Este pode ser constituído por cabos coaxiais, de par entrançado UTP, STP ou de fibra óptica. A distância máxima recomendada é de 90 m. Os cabos especificados são os seguintes:

- UTP de 100 Ω de 4 pares. Recomenda-se categoria 5.
- STP de 150 Ω de 2 pares.
- Cabo com duas fibras ópticas multimodo 62,5/125 μm.

As ligações horizontais devem seguir uma configuração em estrela, onde cada local de trabalho é ligado a uma armário de telecomunicações. As vantagens deste tipo de configuração resumem-se à facilidade que existe em fazer alterações na disposição de componentes sem afectar a globalidade da rede e a maior imunidade a problemas. Um problema que afecte um troço não é propagado a outros componentes.

A.5 Fibra versus Cobre

A instalação de cabo coaxial não é recomendado para sistemas modernos. As ligações de longas distâncias são efectuadas em fibra óptica. Actualmente, um grande número de redes usam cabo de pares entrançados, no entanto, as normas de CEM (Compatibilidade Electromagnética) e a migração actual para velocidades mais elevadas fazem prever um aumento significativo de utilização de fibra óptica relativamente ao par entrançado. Os preços da fibra tendem a descer, tornando a utilização desta uma opção a considerar.

Os cabos de fibra óptica, devido ao facto de suportarem uma portadora de frequência muito elevada, apresentam uma série de características invejáveis face a cabos baseados em cobre:

- Largura de banda virtualmente ilimitada.
- Capacidade de suporte para todos os protocolos actuais e futuros.
- Grau de confiança inatingível por outros meios de transmissão.

Por outro lado:

- A tecnologia ainda é muito cara.
- Difícil de instalar.
- As soluções em cobre cobrem as necessidades actuais e futuras.

Os avanços no campo da fibra óptica, o aumento de produção, a descida de preço de componentes e sistemas opto-electrónicos e um aumento do número de técnicos de instalação e teste de fibra levou à redução de inconvenientes, aproximando substancialmente a fibra dos cabos de cobre. Por outro lado, a rigidez das normas obrigam a um maior dispêndio de capital na instalação e teste de sistemas de cobre, que poderão levar à total extinção do fosso entre as duas tecnologias.

É perfeitamente possível o suporte a protocolos de débitos elevados sobre cobre, mas não sobre os cabos que frequentemente se encontram já instalados. As recomendações aconselham a instalação de UTP de categoria 5, juntamente com os painéis, armários e fichas adequadas. Muito do cabo instalado é o UTP de categoria 3. Mesmo seguindo todas as recomendações para o cobre, não há garantias de que toda a estrutura suporte protocolos de elevados débitos, como o ATM, *Fiber Channel* ou HIPPI, por exemplo.

A largura de banda disponível dá à fibra capacidade de suporte a todos os protocolos existentes ou futuros, havendo uma salvaguarda ao investimento feito. Imune a interferências electromagnéticas, a taxa de erros na comunicação de dados em fibra é consideravelmente inferior à taxa de erros da comunicação em cobre. A baixa atenuação da fibra permite uma extensão dos limites de comprimento na interligação de sistemas, dando uma maior flexibilidade ao dimensionamento da rede.

Apêndice B Proposta para a organização da Rede de Dados do DETUA

B.1 Introdução

A rede de dados do Departamento de Electrónica e Telecomunicações da Universidade de Aveiro (DETUA) é um exemplo típico de herança de equipamento e acumulação de tecnologia, por vezes, ultrapassada. No cenário actual surgem vários problemas de qualidade de serviço e de segurança. O meio académico, principalmente na área da informática/electrónica, é bastante sensível em termos de segurança, em parte devido à curiosidade dos alunos.

A rede existente é constituída por uma percentagem significativa de ligações em par entrançado (UTP), mas mantém vários troços equipados com cabo coaxial fino (10Base2). O *backbone* do departamento tem como suporte cabo coaxial grosso (10Base5). Este encontra-se ligado ao *backbone* da universidade por um encaminhador Cisco. O *backbone* da universidade tem como base o FDDI, através de uma ligação SAS (*single attachment station*).

Os problemas mais comuns na rede do DETUA podem ser classificados em três tipos:

- Físicos –ligações e estrutura de cabos.
- Serviços –DNS, servidor de *Mail*, servidor de *Web* e segurança.
- Administração e operação – gestão de equipamento e organização.

B.2 Rede Física

Os problemas físicos a atacar de início passam pelo aumento da capacidade da rede e da robustez nas conexões, no sentido de dificultar a propagação de problemas de ligação. O primeiro passo a seguir será a substituição dos troços em cabo coaxial (10Base2) por ligações em árvore. Em adição, é de prever a segmentação de determinados troços pela introdução de troços comutados, o que possibilita um aumento de largura de banda disponível.

Em termos de serviços, o equipamento de rede pode ser classificado em três níveis de acesso: acesso elevado, acesso médio e acesso baixo. Como exemplo, pode incluir-se o servidor de correio electrónico e o DNS como equipamento de acesso elevado. O equipamento de acesso médio pode incluir servidores específicos de ficheiros ou de impressão, enquanto que o equipamento de acesso baixo representa as estações de trabalho individual. Obviamente, as ligações efectuadas a cada um dos tipos de equipamento apresenta características diferentes (Figura B.1).

Um outro aspecto a considerar no projecto de uma rede é o custo dos componentes em geral. No caso do DETUA, o orçamento disponível não é elevado, pelo que interessa minimizar o mais possível o custo total de actualização. Este facto elimina, à partida, soluções baseadas em fibra óptica (FDDI), devido ao elevado preço dos componentes no mercado português. Outra tecnologia que é colocada à margem é o ATM, devido ao preço elevado das interfaces de rede e dos comutadores ATM. As soluções de elevada velocidade, da ordem do gigabit por segundo, tais como o *Gigabit Ethernet*, ou o *Fibre Channel*, não são para já necessárias, tendo em conta o tráfego actual no DETUA.

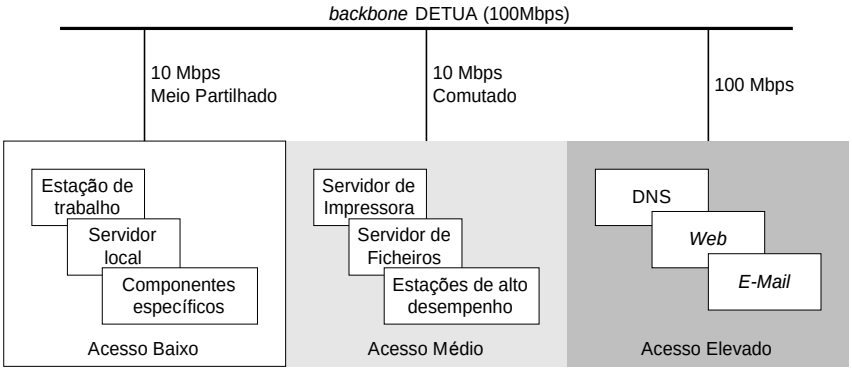


Figura B.1 – Tipo de ligações de acordo com as características do equipamento.

O equipamento de herança é uma outra variável a considerar. Grande parte dos componentes existentes baseiam-se em Ethernet a 10 Mbps, pelo que a introdução de um método de acesso diferente tornaria necessária a substituição de equipamento ou de interfaces de rede.

A janela de opções restringe-se, portanto, ao *Fast Ethernet*, Ethernet comutado e ao 100VG-AnyLAN (Tabela B.1).

Tabela B.1 – Ethernet, 100VG-AnyLAN e *Fast Ethernet*.

		10Base-T	**100VG-AnyLAN**	**100Base-T**
Topologia	Diâmetro	2500 m	4000 m	200 a 370 m
	Níveis hierárquicos	3	5	3
Cablagem	UTP 3,4	100 m	100 m	100 m
	UTP 5	150 m	150 m	100 m
	Fibra óptica	1000 m	2000 m	400 m
Desempenho	100 m	80 % (teórico)	95 %	80 % (teórico)
	2500 m	80 % (teórico)	80 %	-
Aplicações	Sensíveis a atrasos	Não	Sim	Não

Uma grande parte da rede do DETUA é baseada em Ethernet, pelo que a introdução de uma tecnologia diferente iria obrigar à aquisição de componentes de adaptação. Os componentes de adaptação (*transceivers*) vêm aumentar o orçamento de actualização, pelo que é de considerar a hipótese de não introduzir uma nova tecnologia, apesar de ter um desempenho superior.

O 100VG-AnyLAN ultrapassa em desempenho o *Fast Ethernet*, mais notavelmente em situações de tráfego sensível a atrasos e em redes congestionadas. O DETUA não apresenta uma especial necessidade, para já, de escoar tráfego sensível a atrasos (voz e vídeo em tempo real) e não se encontra extremamente congestionada, além de alguns picos esporádicos. A opção recomendável será optar pela via Ethernet comutada/*Fast Ethernet*, sem eliminar a possibilidade de actualização futura.

Um primeiro esboço da rede pode ser efectuado, com base no estudo anterior (Figura B.2).

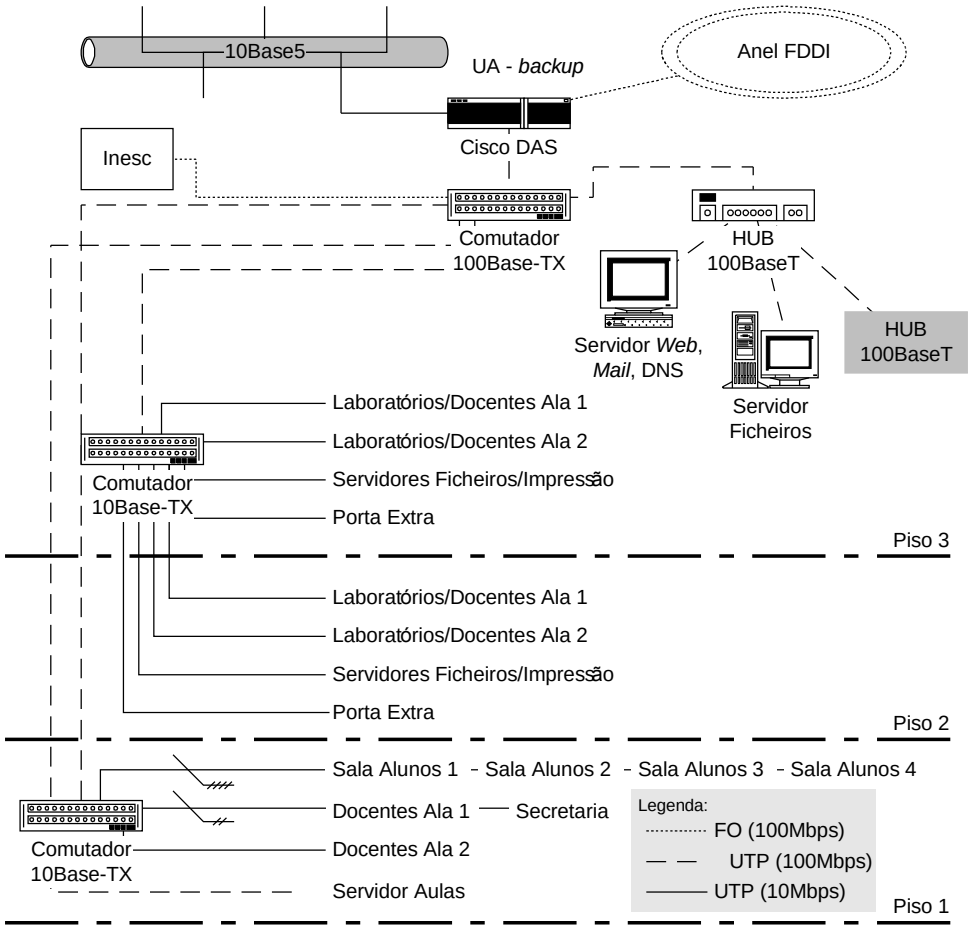


Figura B.2 – Estrutura geral da rede do DETUA.

As ligações denominadas horizontais, ou seja, aos Laboratórios, Gabinetes, Salas, etc., não devem ter mais de dois HUBs em cascata (segundo a norma ANSI/EIA/TIA-568A-1995). Todas as ligações não devem exceder os 100 m de comprimento à excepção da ligação em fibra ao INESC, que pode atingir os 500 m de comprimento.

A lista de material necessário, em adição ao existente, encontra-se especificado na Tabela B.2, juntamente com o preço médio de venda ao público.

Tabela B.2 – Relação de material.

Componente	Preço Unitário	Quantidade	Total
Transceiver DAS para Cisco		1	0,00 Esc.
Transceiver 100Base-TX para Cisco		1	0,00 Esc.
Comutador 100Base-TX de 8 portas	365.000,00 Esc.	1	365.000,00 Esc.
HUB 100Base-TX de 8 portas	137.500,00 Esc.	1	137.500,00 Esc.
Comutador 10Base-TX 8/10 + 1/100	281.500,00 Esc.	2	563.000,00 Esc.
Adaptadores de rede 100Base-TX	15.900,00 Esc.	3	47.700,00 Esc.
		Total	1.113.200,00 Esc.

O HUB 100Base-TX pode não ser necessário no caso de o DNS, o servidor de *Web* e o servidor de correio electrónico residirem na mesma máquina.

A estrutura horizontal tipicamente apresenta uma topologia em árvore com, no máximo, dois níveis hierárquicos (Figura B.3). A distância entre o comutador e a estação mais longínqua reduz-se a 300 m.

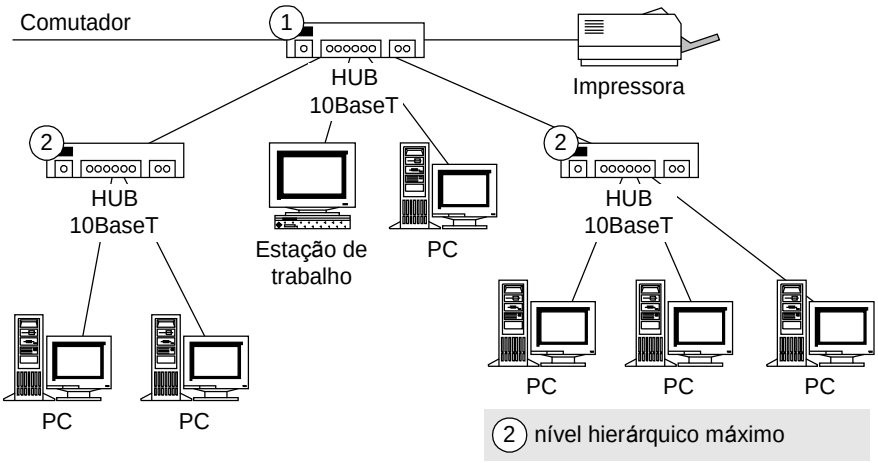


Figura B.3 – Estrutura horizontal típica.

Os servidores de alto acesso, como o servidor de ficheiros de aulas, servidor de correio electrónico e o DNS são dotados de um adaptador de rede 100Base-TX, com a finalidade de dar resposta adequada a inúmeros pedidos simultâneos.

B.3 Serviços

O servidor de DNS do DETUA reside numa estação de trabalho Decserver, já com alguns anos. Neste momento, a máquina encontra-se ultrapassada em termos de fiabilidade. O servidor de correio electrónico do DETUA padece dos mesmos problemas que o DNS. A imagem de *Web* do DETUA é praticamente inexistente, em parte devido à inexistência de um suporte adequado. Do ponto de vista de segurança, a criptografia, bem como medidas de autenticação eficientes, são praticamente inexistentes.

A proposta de melhoria de serviços passa pela instalação de uma máquina Linux dedicada aos serviços de *Web*, correio electrónico e DNS, equipada com um adaptador 100Base-TX. A escolha do Linux assenta nas seguintes considerações:

- O sistema operativo é gratuito.
- Os servidores (*Web*, DNS, *E-Mail*) são gratuitos.
- A administração remota é efectuada de forma semelhante à local.
- É um sistema robusto e continuamente actualizado.

Do ponto de vista de segurança, a criptografia é indispensável, pelo que se recomenda a implementação de SSH (*Secure SHell*) em todos os computadores da rede.

Sente-se a falta de um mecanismo que permita a realização de cópias de segurança para todos os utilizadores, compatível com UNIX e Windows. Propõe-se a instalação de um mecanismo deste tipo na máquina Linux supracitada, dotada com métodos de acesso por Samba (compatível com Windows), SCP (*Secure Copy*), FTP (*File Transfer Protocol*). Este serviço permite ter acesso aos trabalhos pessoais a partir de qualquer local e em qualquer altura.

B.4 Operação e Administração

A operação e administração de uma rede deste tipo, quer a nível de serviços, quer a nível físico, deve ser tarefa de um organismo interno específico. Esse organismo deverá ter a responsabilidade de atribuição de endereços, extensão da rede e gestão dos servidores globais do DETUA.

Em adição, há falta de ferramentas de gestão. Pode-se indicar à partida a necessidade de uma sonda RMON em pontos chaves da rede, bem como aplicações gestoras adequadas à tecnologia actual. Há também falta de equipamento de teste e análise.

REFERÊNCIAS

Advent97 — Advent Network Management Inc., *Advent SNMP 1.1*, http://www.adventnet.com/, 1997.

ANSI802.3 — "Carrier Sense Multiple Access with Colision Detection (CSMA/CD) Access Method and Physical Layer Specifications", American National Standards Institute, ANSI/IEEE 802.3 (ISO 8802/3).

ANSI802.3a — "Medium Attachement Unit and Baseband Medium Specifications, Type 10BASE2", American National Standards Institute, ANSI/IEEE 802.3a.

ANSI802.3b — "Broadband Medium Attachement Unit and Broadband Medium Specifications, Type 10BROAD36", American National Standards Institute, ANSI/IEEE 802.3b.

ANSI802.3e — "Physical Signaling, Medium Attachement, and Baseband Medium Specifications, Type 1BASE5", American National Standards Institute, ANSI/IEEE 802.3e.

ANSIX3.135 — "The Database language SQL", American National Standards Institute, ANSI X3.135, 1996.

ANSIX3.139 — "Information Systems - Fiber Distributed Data Interface (FDDI) – Token Ring Media Access Control (MAC)", American National Standards Institute, ANSI X3.139, 1997.

ANSIX3.183 — "High-Performance Parallel Interface - Mechanical, Electrical, and Signalling Protocol Specification (HIPPI-PH)", ANSI X3.183, 1991.

ANSIX3.230 — "Information Technology - Fibre Channel - Physical and Signaling Interface (FC-PH)", ANSI X3.230, 1994.

Arnold96 — K. Arnold, J. Gosling, *The Java Programming Language*, Addison-Wesley, 1996.

Beauchamp88 — R. G. Beauchamp, *Computer Communications*, Van Nostrand Reinhold, 1988, pp. 113-114, ISBN 0-278-00012-6.

Black95 — Uyless D. Black, *ATM Foundation for Broadband Networks*, Prentice Hall, 1995, ISBN 0-13-297178-X.

Bloomer92 — J. Bloomer, *Power Programming with RPC*, O'Reilly & Associates, Inc., 1992.

Blumenthal97 — U. Blumenthal, B. Wijnen, "Security Features of SNMPv3", *The Simple Times*, Vol. 5, N. 1, Dezembro 1997.

Boisseau94 — M. Boisseau, M. Demange, J. Munier, *High Speed Networks*, John Wiley & Sons, 1994, ISBN 0-471-95109-9.

Cee89 — "Directiva do Conselho de 3 de Maio de 1989 relativa à aproximação das legislações dos estados-membros respeitantes à compatibilidade electromagnética (89/336/CEE)", *Jornal Oficial das Comunidades Europeias*, 23 de Maio de 1989, pp. 139/19-139/23.

Chen96 — Graham Chen, Michael Neville, Quinzheng Kong, "Distributed Network Management Using CORBA/TMN", *Proc. of the 7th IFIP/IEEE International Workshop on Distributed Systems Operation and Management (DSOM)*, 1996.

Clark96 — Martin P. Clark, *ATM Networks: Principles and Use*, Wiley-Teubner, 1996, ISBN 0-471-96701-7.

Cohen94 — Roberta S. Cohen, "The Telecommunications Management Network", *Network and Distributed Systems Management*, Morris Sloman, Addison-Wesley, 1994.

Corba97 — OMG, *The Common Object Request Broker: Architecture and Specification, v.2.1*, http://www.omg.org, Agosto 1997.

Costa95 — Janis Furtek Costa, *High Speed Networks Using 100VG-AnyLAN – 2nd Edition*, Prentice Hall, 1995, ISBN 0-13-439092-X.

Derfler93 — Frank J. Derfler, Jr., Les Freed, *Get a Grip on Network Cabling*, Ziff-Davis Press, 1993, ISBN 1-56276-057-2.

Deri96 — L. Deri, "Surfin' Resources across the Web", IBM Zurich Research Laboratory, University of Berne, 1996.

Dutton95 — H. Dutton, P. Lenhard, *High-Speed Networking Technology: An Introductory Survey - Third Edition*, Prentice Hall, 1995, ISBN 0-13-242421-5.

Gigabit96 — "Gigabit Ethernet - White Paper", Gigabit Ethernet Alliance, Agosto 1996.

Graham96 — I. Graham, *The HTML sourcebook : a complete guide to HTML 3.0 - 2nd ed*, John Wiley, 1996.

FibreChannel — *Fibre Channel*, *http://www.fibrechannel.com*, 1997.

Frymoyer95 — Edward M. Frymoyer, "Fibre Channel Fusion: Low Latency, High Speed", Hewlett-Packard Co., *Data Communications*, Fevereiro, 1995, pp. 107-112.

Halsall92 — F. Halsall, *Data Communications, Computer Networks and Open Systems - Third Edition*, Addison-Wesley, 1992, ISBN 0-201-56506-4.

Harrington97 — D. Harrington, "The Evolution of Architectural Concepts in the SNMPv3 Working Group", *The Simple Times*, Vol. 5, N. 1, Dezembro 1997.

Haugdahl87 — J. Scott Haugdahl, *Inside the Token-Ring*, North-Holland, 1987, ISBN 0-444-70139-7.

HIPPI — "High Performance Parallel Interface – HIPPI", *http://www.cern.ch/HIS/hippi/hippi.html*, 1997.

Hong97 — James Won-Ki Hong, Ji-Young Kong, Tae-Hyoung Yun, Jomg-Seo Kim, "Web-Based Intranet Services and Network Management", *IEEE Communications Magazine*, Vol. 35, N. 10, Outubro, 1997.

Huitema95 — Christian Huitema, *Routing in the Internet*, Prentice-Hall, 1995, ISBN 0-13-132192-7.

IEEE802.3u — "Local and Metropolitan Area Networks-Supplement - Media Access Control MAC) Parameters, Physical Layer, Medium Attachment Units and Repeater for 100Mb/s Operation, Type 100BASE-T", IEEE 802.3u – 1995.

IEEE802.12 — "Standard for Demand Priority Access Method Physical Layer and Repeater Specification for 100 Mb/s Operation", IEEE 802.12 – 1995.

ISO4335 — ISO/IEC 4335 Information Technology - Telecommunications and Information Exchange Between Systems - High-level Data Link control (HDLC) Procedures - Elements of Procedures 1993.

ISO7498 — ISO 7498, Information Processing Systems – Open Systems Interconnection – Basic Reference Model.

ISO7498-4 — ISO/IEC 7498-4, Information Processing Systems – Open Systems Interconnection – Basic Reference Model – Part 4: Management Framework.

ISO10040 — ISO/IEC 10040, Information Processing Systems – Open Systems Interconnection – Systems Management Overview.

ISO10165 — ISO/IEC 10165, GDMO – Guidelines for Definition of Managed Objects.

ISO8824 — ISO/IEC 8824, Information Processing Systems - Open Systems Interconection - Specification of Abstract Syntax Notation One.

ISO8825 — ISO/IEC 8825, Information Processing Systems - Open Systems Interconection - Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1).

Jain94 — Raj Jain, *FDDI Handbook: High-speed Networking using Fiber and Other Media*, Addison-Wesley, 1994, pp. 9-13, ISBN 0-201-56376-2.

Jayasumana94 — Bernhard Albert, Anura P. Jayasumana, *FDDI and FDDI-II: Architecture, Protocols, and Performance*, Artech House, 1994, ISBN 0-89006-633-7.

Jmapi96a — Sun Microsystems, Inc., *Java Management API Programmer's Guide*, Developer's Releas, Junho, 1996.

Jmapi96b — Sun Microsystems, Inc., "Java Management API Architecture", Junho, 1996.

Kish97 — Paul Kish, "Cable-bodied", *Communications International*, Vol. 24, N. 12, Dezembro, 1997.

Langsford94 — Alwyn Langsford, "OSI Management Model and Standards", *Network and Distributed Systems Management*, Morris Sloman, Addison-Wesley, 1994.

Lindholm96 — T. Lindholm, F. Yellin, *The JavaTM Virtual Machine Specification*, Setembro, 1996.

Lopes97a — Rui Pedro Lopes, José Luís Oliveira, "Ethernet: de 1 Mbps a 1 Gbps", *Revista do Departamento de Electrónica e Telecomunicações da Universidade de Aveiro*, Vol.2, Nº1, Setembro, 1997, pp. 47-56.

Mazumdar96 — Subrata Mazumdar, "Inter-Domain Management between CORBA and SNMP: WEB-based Management – CORBA/SNMP Gateway Approach", *Proc. Of DSOM'96, L'Aquila, Itália*, Outubro 28-30, 1996.

Melatti94 — L. Melatti, "Fast Ethernet: 100 Mbit/s Made Easy", National Semiconductor Corp., *Data Communications*, Novembro, 1994.

Mills95 — A. Mills, *Understanding FDDI*, Prentice Hall, 1995.

Microtest97 — Microtest, Inc. , "Microtest LAN Cabling Standards Summary", http://www.microtest.com/html/wire_stds_summary.html, 1997.

Moreau94 — Jean-Jaques Moreau, Kave Eshghi, Adrian Pell, Simon Towers, "Beyond the File Manager: Towards an Object Manager and its Use for Networked Systems Management", *Proc. of 5th IFIP/IEEE International Workshop on Distributed Systems: Operations & Management (DSOM'94)*, Toulouse, França, 1994.

Nagaratnam96 — N. Nagaratnam, *Java Networking and AWT API SuperBible*, Waite Group Press, 1996.

Oliveira95 — José Luís Oliveira, *Arquitectura para Desenvolvimento e Integração de Aplicações de Gestão*, Tese de Doutoramento, Universidade de Aveiro, Setembro 1995.

Peterson96 — Larry L. Peterson, Bruce S. Davie, *Computer Networks: a System Approach*, Morgan Kaufman, 1996, pp. 210-217, ISBN 1-55860-368-9.

Ptopo98 — Andy Bierman, Keith McCloghrie, "PTOPO Discovery Protocol and MIB", <*draft-ietf-ptopomib-pdp-02.txt*>, Março, 1998.

Rauch95 — Peter Rauch, Scott Lawrence, "100VG-AnyLAN: The Other Fast Ethernet", Thomas-Conrad Corp., *Data Communications*, Março, 1995, pp. 129-134.

Restivo95 — Ken Restivo, "The Boring Facts About FDDI", Interphase Corp., *Data Communications*, Janeiro, 1995.

RFC1021 — C. Partridge, G. Trewitt, "High-level Entity Management System HEMS", *Internet Request for Comments 1021*, Outubro, 1987.

RFC1022 — C. Partridge, G. Trewitt, "High-level Entity Management Protocol HEMP", *Internet Request for Comments 1022*, Outubro, 1987.

RFC1155 — K. McCloghrie, M. Rose, "Structure and Identification of Management Information for TCP/IP-based Internets", *Internet Request for Comments 1155*, Maio 1990.

RFC1156 — K. McCloghrie, M. Rose, "Management Information Base for Network Management of TCP/IP-based internets", *Internet Request for Comments 1156*, Maio 1990.

RFC1157 — J. Case, M. Fedor, M. Schoffstall, J. Davin, "A Simple Network Management Protocol (SNMP)", *Internet Request for Comments 1157*, Maio 1990.

RFC1158 — M. Rose, "Management Information Base for Network Management of TCP/IP based internets: MIB-II", *Internet Request for Comments 1158*, Maio 1990.

RFC1189 — L. Besaw, B. Handspicker, L. LaBarre, U. Warrier, "The Common Management Information Services and Protocols for the Internet", *Internet Request for Comments 1189*, Outubro 1990.

RFC1212 — K. McCloghrie, M. Rose, "Concise MIB Definitions", *Internet Request for Comments 1212*, Março 1991.

RFC1213 — K. McCloghrie, M. Rose, "Management Information Base for Network Management of TCP/IP-based internets: MIB-II", *Internet Request for Comments 1213*, Março 1991.

RFC1215 — M. Rose, "A Convention for Defining Traps for use with the SNMP", *Internet Request for Comments 1215*, Março 1991.

RFC1351 — J. Davin, J. Galvin, K. McCloghrie, "SNMP Administrative Model", *Internet Request for Comments 1351*, Julho 1992.

RFC1352 — J. Galvin, K. McCloghrie, J. Davin, "SNMP Security Protocols", *Internet Request for Comments 1352*, Julho 1992.

RFC1353 K. McCloghrie, J. Davin, J. Galvin, "Definitions of Managed Objects for Administration of SNMP Parties", *Internet Request for Comments 1353*, Julho 1992.

RFC1441 J. Case, K. McCloghrie, M. Rose, S. Waldbusser, "Introduction to version 2 of the Internet standard Network Management Framework", *Internet Request for Comments 1441*, Maio 1993.

RFC1445 J. Galvin, K. McCloghrie, "Administrative Model for version 2 of the Simple Network Management Protocol (SNMPv2)", *Internet Request for Comments 1445*, Maio 1993.

RFC1446 J. Galvin, K. McCloghrie, "Security Protocols for version 2 of the Simple Network Management Protocol (SNMPv2)", *Internet Request for Comments 1446*, Maio 1993.

RFC1448 J. Case, K. McCloghrie, M. Rose, S. Waldbusser, "Protocol Operations for version 2 of the Simple Network Management Protocol (SNMPv2)", *Internet Request for Comments 1448*, Maio 1993.

RFC1449 J. Case, K. McCloghrie, M. Rose, S. Waldbusser, "Transport Mappings for version 2 of the Simple Network Management Protocol (SNMPv2)", *Internet Request for Comments 1449*, Abril 1993.

RFC1901 J. Case, K. McCloghrie, M. Rose, S. Waldbusser, "Introduction to Community-based SNMPv2", *Internet Request for Comments 1901*, Janeiro 1996.

RFC1902 J. Case, K. McCloghrie, M. Rose, S. Waldbusser, "Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2)", *Internet Request for Comments 1902*, Janeiro 1996.

RFC1903 J. Case, K. McCloghrie, M. Rose, S. Waldbusser, "Textual Conventions for Version 2 of the Simple Network Management Protocol (SNMPv2)", *Internet Request for Comments 1903*, Janeiro 1996.

RFC1904 J. Case, K. McCloghrie, M. Rose, S. Waldbusser, "Conformance Statements for Version 2 of the Simple Network Management Protocol (SNMPv2)", *Internet Request for Comments1904*, Janeiro 1996.

RFC1905 J. Case, K. McCloghrie, M. Rose, S. Waldbusser, "Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)", *Internet Request for Comments 1905*, Janeiro 1996.

RFC1906 J. Case, K. McCloghrie, M. Rose, S. Waldbusser, "Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2)", *Internet Request for Comments 1906*, Janeiro 1996.

RFC1909 K. McCloghrie, "An Administrative Infrastructure for SNMPv2", *Internet Request for Comments 1909*, Fevereiro 1996.

RFC1910 G. Waters, "User-based Security Model for SNMPv2", *Internet Request for Comments 1910*, Fevereiro 1996.

RFC1945 T. Berners-Lee, R. Fielding, H. Frystyk, "Hypertext Transfer Protocol - HTTP/1.0", *Internet Request for Comments 1945*, Maio 1996.

RFC2026 S. Bradner, "The Internet Standards Process - Revision 3", *Internet Request for Comments 2026*, Outubro 1996.

RFC2067 J. Renwick, "IP over HIPPI", *Internet Request for Comments 2067*, Janeiro, 1997.

RFC2271 D. Harrington, R. Presuhn, B. Wijnen, "An Architecture for Describing SNMP Management Frameworks", *Internet Request for Comments 2271*, Janeiro 1998.

RFC2272 J. Case, D. Harrington, R. Presuhn, B. Wijnen, "Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)", *Internet Request for Comments 2272*, Janeiro 1998.

RFC2273 D. Levi, P. Meyer, B. Stewart, "SNMPv3 Applications", *Internet Request for Comments 2273*, Janeiro 1998.

RFC2274 U. Blumenthal, B. Wijnen, "User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)", *Internet Request for Comments 2274*, Janeiro 1998.

RFC2275 B. Wijnen, R. Presuhn, K. McCloghrie, "View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)", *Internet Request for Comments 2275*, Janeiro 1998.

RFC768 J. B. Postel, "User Datagram Protocol", *Internet Request for Comments 768*, Agosto 1980.

Rixon97 Jeremy Rixon, "ATM Management Using HP DM CORBA and Java", *Proc. of the International Open View Forum* Conference, Anaheim, USA, Junho, 1997.

Rmi96 Sun Microsystems, Inc., "Remote Method Invocation Specification", http://java.sun.com/products/jdk/rmi/, 1996.

Rose96 M. Rose, *The Simple Book: An Introduction to Networking Management - 2nd edition*, Prentice-Hall, 1996.

Rowe96 J. Rowe, *Building Internet Database Servers with CGI*, New Riders, 1996.

Schröder94 Rainer Händel, Manfred N. Huber, Stefan Schröder, *ATM Networks: Concepts, Protocols, Applications*, Addison-Wesley, 1994, ISBN 0-201-42274-3.

Sethi94 Adarshpal S. Sethi, Pramod Kalyanasundaram, "A Spreadsheet Paradigm for Network Management and Control", *Proc. of 5th IFIP/IEEE International Workshop on Distributed Systems: Operation and Management (DSOM'94)*, Toulouse, França, 1994.

Shock80 John F. Shock, Jon A. Hupp, "Measured Performance of an Ethernet Local Network", *The Ethernet Sourcebook*, Fevereiro, 1980.

Smythe95 Colin Smythe, *Internetworking: Designing the Right Architectures*, Addison-Wesley, 1995, pp. 203-226, ISBN 1-55860-368-9.

SNMPv2* SNMP Research Inc., http://www.snmp.com/v2star.html, 1997.

Stallings90a W. Stallings, *Computer Organization and Architecture, Second Edition*, Macmillan, 1990.

Stallings90b W. Stallings, *Local Networks, Third Edition*, Macmillan, 1990.

Stallings93 W. Stallings, *SNMP, SNMPv2 and CMIP, The Practical Guide to Network Management Standards*, Addison-Wesley, 1993, ISBN 0-201-63331-0.

Stallings94	W. Stallings, *Data and Computer Communications - Fourth Edition*, MacMillan, 1994.
Stallings95	W. Stallings, *ISDN and Broadband ISDN with Frame Relay and ATM, Third Edition*, Prentice-Hall, 1995, ISBN 0-13-180944-X.
Tanenbaum96	A. Tanenbaum, *Computer Networks - 3rd edition*, Prentice-Hall, 1996.
Tolmie95	Don Tolmie, Don Flanagan, "HIPPI: It's Not Just for Supercomputers Anymore", *Data Communications*, Maio, 1995, pp. 107-112.
Vieira97	Gabriel Vieira, Orlando Sá Morais, *Bancada de Gestão de Redes*, Universidade de Aveiro, Setembro, 1997.
VGAnyLAN	"100VG-AnyLAN Training", *http://www.iol.unh.edu/training/vganylan/*, 1997.
Waters96	Glenn W. Waters, "The User-based Security Model", *The Simple Times*, Vol. 4, N. 1, Janeiro, 1996.
WBEM	WBEM Consortium, *http://wbem.freerange.com/*, 1997.

APONTADORES VÁRIOS

CORBA

OMG Home Page

http://www.omg.org/
Endereço do ***Object Management Group***. Um bom sitio para iniciar o contacto com CORBA, particularmente na secção "*CORBA for Beginners*" onde são indicados apontadores vários, exemplos e documentação geral. A última especificação pode ser carregada a partir deste endereço.

The Free CORBA Page

http://adams.patriot.net/~tvalesky/freecorba.html
Página dedicada a uma vertente gratuita da CORBA. Podem ser encontrados ORBs gratuitos para diversas plataformas e linguagens.

Gestão de Redes

The Simple Times http://www.simple-times.org/
Publicação dedicada à promoção do SNMP. Em cada número são apresentados artigos técnicos, uma lista de recursos Internet e um sumário de normas.

The SimpleWeb - University of Twente

http://wwwsnmp.cs.utwente.nl/
Informação acerca de várias arquitecturas de gestão, desde a Internet passando pelo OSI e o TMN. Contem ligações para centros de investigação, *software*.

DMTF The Desktop Management Task Force

http://www.dmtf.org/
Normas e especificações associadas à DMI (*Desktop Management Interface*) bem como à sua correspondência com SNMP. Um bom ponto de partida para o estudo de normas de gestão de estações de trabalho.

About TMN http://www.isrglobal.com/tmnpage.htm
Informação genérica sobre TMN, incluindo uma vasta coleccao de MIBs definidas pelo ITU-T em GDMO e ASN.1. Contem aplicações de demonstração como um *browser* de MIBs e comutação móvel.

GDMO - Guidelines for Definition of Managed Objects
http://www.dg-tech.com/gdmo.htm
Página interessante sobre GDMO. Orientada ao desenvolvimento de aplicações para TMN e OSI.

SNMP Research International

http://www.snmp.com/
Um fabricante de tecnologia e soluções SNMP. Apresenta várias soluções de gestão Internet baseadas nas arquitecturas SNMPv1, SNMPv2 e SNMPv3. Contém informação e especificações para o SNMPv2*.

SNMP version 3 (SNMPv3) Charter

http://www.ietf.org/html.charters/snmpv3-charter.html
Página do grupo responsável pela edição dos RFCs específicos do SNMPv3.

SNMP Version 3 (SNMPv3)

http://www.ibr.cs.tu-bs.de/projects/snmpv3/
Página do grupo de trabalho SNMPv3. Contém ligações a documentação e implementações de SNMPv3.

Gestão Baseada em WWW

The Web Based Management Page

http://www.mindspring.com/~jlindsay/webbased.html
Um bom ponto de partida para o estudo de gestão baseada em tecnologia Internet. Contém um conjunto bastante completo de ligações para várias arquitecturas, implementações e tecnologia de gestão baseada em WWW.

Java Management Home Page

http://java.sun.com:80/products/JavaManagement/index.html
Documentação e implementação da JMAPI.

Advent Network Management Inc.

http://www.adventnet.com/
Empresa de desenvolvimento de soluções de gestão baseadas em Java e SNMP. Disponibilisa gratuitamente excelentes APIs Java que implementam SNMPv1 e SNMPv2c.

Introduction to JUMP(tm)

http://www.outbackinc.com/products/jump/intro.html
Arquitectura baseada em Java, SNMP, DMI e CORBA para a gestão de redes.

Network Management Laboratory - Java Connection Network Management Laboratory - Java Connection

http://www.sce.carleton.ca/netmanage/Java.shtml
Página de recursos relacionados com Java, aplicações distribuidas e gestão de redes baseada em WWW.

Java Network Management Resources

http://www.adventnet.com/java-nm-resources.html
Página de redursos relacionados com Java e gestão de redes. Um excelente ponto de partida para o desenvolvimento de aplicações de gestão baseadas na linguagem Java.

Subrata Mazumdar's Home Page at Bell Laboratories

http://www.bell-labs.com/~mazum/
Artigos e referências a trabalho desenvolvido com CORBA e SNMP/OSI.

Distributed Network Management Using CORBA/TMN

http://www.citr.com/02.TechnicalJournal/02.Volume_2/01.Papers/P2_DSOM96.html
Artigo sobre integração de CORBA/TMN.

Mobile Agents and CORBA in Network Management

http://www.witrans.uni-frankfurt.de/WiTrans/messe/aktuell/cebit98_ex6e.html
Exportação de agentes com base em CORBA.

Web-Based Enterprise Management

http://wbem.freerange.com/
Documentação variada sobre WBEM. Em adição, contém o pacote de desenvolvimento de WBEM.

Links to WBEM http://www.ki.com/WBEM/links.html
Lista de colaboradores para o desenvolvimento da norma WBEM.

WBEM - Home Page

http://www.microsoft.com/management/wbem/default.htm
Descrição da arquitectura WBEM, com particular ênfase sobre o modelo de informacao.

Java

Java Home Page http://www.javasoft.com/
Endereço de Java na Sun. Referências, documentação, ferramentas de desenvolvimento e APIs Java.

JavaShareware.com http://www.JavaShareware.com/
Arquivo de programas desenvolvidos em Java.

Gamelan: Earthweb's Java Directory

http://www.developer.com/
Arquivo bastante completo com diversos programas desenvolvidos em Java e ActiveX entre outros. Por vezes conseguem-se código fonte bastante útil.

The Java Tutorial http://www.javasoft.com/docs/books/tutorial/index.html
Um excelente documento de introdução à linguagem de programação Java. É constantemente actualizado.

RFCs

Linked RFCs http://www.pmg.lcs.mit.edu/rfc.html
Motor de pesquisa de RFCs por número ou por ocorrência.

Internet Standards Archive

http://sunsite.cnlab-switch.ch/cgi-bin/search/standard/nph-findstd/
Motor de pesquisa de RFCs por número ou ocorrência. Bastante completo.

RFCs in HTML format

http://rfc.fh-koeln.de/rfc.html
Índice de RFCs em formato HTML.

Tecnologia

As seguintes referências apresentam normas, documentação e ferramentas específicas. Fornecem um bom ponto de partida para o estudo de várias soluções tecnológicas de rede.

FastEthernet

Fast Ethernet Consortium

http://www.iol.unh.edu/consortiums/fe/index.html

Fast Ethernet Whitepaper

http://www.lantronix.com/htmfiles/whitepapers/lfrwp.htm

Quick Reference Guide to 100BASE-FX

http://www.ots.utexas.edu/ethernet/100quickref/ch11qr_1.html

Asanté 100 Megabit Fast Ethernet White Paper

http://www.asante.com/Press/wpfast.html

100VG-AnyLAN

Compaq.com - Network Technology Information

http://www.compaq.com/support/techpubs/whitepapers/407a0796.html

100VG-AnyLAN Training

http://www.iol.unh.edu/training/vganylan/index.html

100VG-AnyLAN Technology

http://www.100vg.com/

100VG AnyLan WEB FAQ / Home Page

http://www.io.com/~richardr/vg/

FibreChannel

Fibre Channel Loop Community Homepage

http://www.fcloop.org/

Fibre Channel Association

http://www.fibrechannel.com/

CERN Fibre Channel homepage

http://www.cern.ch/HSI/fcs/fcs.html

Fibre Channel Consortium

http://www.iol.unh.edu/consortiums/fc/index.html

GigabitEthernet

Gigabit Ethernet Alliance

http://www.gigabit-ethernet.org/

Gigabit Ethernet on the Horizon

http://www.3com.com/0files/strategy/600220.html

ATM

Welcome to the ATM Forum

http://www.atmforum.com/

The Cell Relay Retreat

http://cell-relay.indiana.edu/cell-relay/

Demo of (Java-powered) UNI 3.1 Signalling Package

http://www.ultranet.com/~dhudek/junidemo1.shtml

A Brief Tutorial on ATM

http://juggler.lanl.gov/lanp/atm.tutorial.html

High Speed Networks and Asynchronous Transfer Mode

http://www.npac.syr.edu/users/mahesh/homepage/atm_tutorial/

FDDI

FDDI Consortium

http://www.iol.unh.edu/consortiums/fddi/index.html

ANSI X3T12 FDDI FAQ

http://sholeh.nswc.navy.mil/x3t12/fddifaq.html

FDDI Technology

http://jmazza.shillsdata.com/tech/fddi/

HIPPI

HIPPI Networking Forum

http://www.esscom.com/hnf/index.html

HIPPI: It's Not Just for Supercomputers Anymore

http://www.cic-5.lanl.gov/lanp/HIPPI_Data_Comm.html

HIPPI Standards Activities

http://www.noc.lanl.gov/~det/Welcome.html

HNF-gigabit to gigabyte and beyond

http://www.hnf.org/menubar1.htm