6.4 - INTERCONEXÃO DE REDES LOCAIS.

A interconexão de redes locais é uma necessidade nos dias atuais. Esta é a tarefa mais importante da camada de rede em redes locais. Ela se faz necessária quando máquinas origem e destino estão em redes diferentes. Na execução da função de ligar rede locais entre si pode-se criar topologias parcialmente ligadas fazendo com que existam caminhos diferentes por redes intermediárias, com diferentes protocolos. O principal problema que decorre disto é que existem diversos tipos de redes com características próprias. Assim, a tarefa do nível de rede é compatibilizar as diferentes tecnologias e protocolos empregados nas redes a serem interconectadas.

Nem sempre a interconexão de redes exige alto grau de complexidade. Por vezes é apenas necessário ligar dois segmentos de rede exatamente iguais, ou que possuam apenas o meio físico diferente. Por exemplo, quando desejamos interconectar duas redes Ethernet com cabeamento diferente. Outro problema, um pouco mais complexo, seria interconectar duas redes com protocolos de acesso diferentes, porém com o mesmo protocolo de rede. Por exemplo, se desejarmos interconectar uma rede Ethernet com uma rede Token Ring.

As motivações que podem levar à necessidade de interconectar de redes entre si são:
1. de ordem econômica, por exemplo, para compartilhar uma interface de rede pública;
2. de ordem tecnológica, por exemplo, para interconectar várias redes locais em áreas ou prédios distintos;
3. para melhorar desempenho e confiabilidade, por exemplo, dividir uma rede local com grande número de estações em 2 ou mais redes;
4. de ordem funcional, por exemplo, para atender necessidades do usuário, tais como acesso a recursos como bancos de dados, disponíveis em outras redes.

Algumas questões a serem abordadas para a interconexão:
1. endereçamento e encaminhamento das mensagens;
2. fragmentação das mensagens;
3. detecção e recuperação de erros;
4. serviço com ou sem conexão;
5. nível de interconexão;
6. controle de fluxo;
7. controle de congestionamento;
8. segurança;
9. tarifação de serviços;
10. nomes e endereçamento.

A ligação entre equipamentos heterogêneos deve ter convenções para representação de nomes e endereços de processos que tenham significado em toda a rede. As referências às redes são feitas por nomes ou por endereços, e isto é importante para identificação de recursos na rede. A maneira mais comum é o endereçamento hierárquico, ou seja, o endereço do processo constituído de endereço da rede, endereço do equipamento hospedeiro (host) e endereço dentro do hospedeiro (porta). Há também uma alternativa, o endereçamento plano, ou não-hierárquico, onde há um endereço para cada recurso na rede.

É importante lembrar que a interconexão de duas redes exige a implementação, em cada rede, de um protocolo inter-redes que realize, pelo menos, as funções de tratamento de endereços. Os principais equipamentos para interconexão de redes são: repetidores, pontes e roteadores.

6.5 - A ARQUITETURA TCP/IP – INTERNET.

A arquitetura Internet é largamente utilizada para interconexão e interoperação de sistemas computacionais heterogêneos. Tal arquitetura foi lançada pelo Departamento de Defesa do governo americano e escolhida para ser o padrão obrigatório de comunicação entre os diversos sistemas daquela organização. Ela tornou-se um padrão de fato do mercado. Seus padrões não são definidos por entidades de padronização internacional como a ISO, por exemplo. As definições dos protocolos são encontradas em documentos denominados **RFC** (Request for Comments), os quais são elaborados pelo **IAB** (Internet Activities Board).

A arquitetura Internet também é organizada em camadas. Ela é composta por dois protocolos principais: o **IP (Internet Protocol)** e o **TCP (Transmission Control Protocol**). O IP é responsável pelo encaminhamento de pacotes de dados através das diversas sub-redes, desde a origem até o seu destino. O TCP tem por função o transporte fim-a-fim, confiável, de mensagens de dados entre dois sistemas.

O IP é um protocolo do tipo datagrama, operando, portanto, no modo não orientado à conexão, enquanto o TCP é um protocolo de transporte orientado à conexão.

O conjunto TCP/IP pode, desta forma, oferecer um serviço relativamente confiável. Para uso em redes de alta qualidade, onde o problema de confiabilidade não assume grande importância, foi definido o protocolo UDP (User Datagram Protocol) que opera no modo não orientado à conexão e possui funcionalidades bem mais simplificadas que o TCP.

Dentre os protocolos correspondentes de cada camada, o protocolo IP é que desempenha as atividades mais importantes de toda a arquitetura. O IP tem como função a fragmentação/desfragmentação e o roteamento de unidades de dados através dos equipamentos roteadores existentes no caminho a ser seguido até o destino da comunicação.

O IP atualmente se encontra na versão 4.0 que foi apresentada em 1978 e possui problemas para ser utilizado nos dias atuais, dentre os quais destacam-se a baixa quantidade de endereços de interfaces oferecido, a não hierarquização dos endereços e a falta de recursos de segurança e de controle de qualidade de serviço para a transmissão dos dados. Devido a esses e outros problemas, além da necessidade de inclusão de novos requisitos tecnológicos a este protocolo, está sendo criado uma nova versão do IP, o IPv6 (ou IPng).

A Internet cresceu muito além do que se podia imaginar. A Internet é hoje uma coleção de redes acadêmicas, militares e comerciais espalhadas pelo mundo, interconectadas através do protocolo TCP/IP.

Uma vez que toda a rede conectada à Internet deve falar o protocolo TCP/IP, é natural que o interesse comercial por este protocolo tenha crescido muito, ao ponto de hoje estar disponível em quase todas as plataformas. Além disso, é comum encontrarmos TCP/IP sendo utilizado em redes locais que não estão conectadas à Internet.

O sucesso e a popularidade do protocolo TCP/IP não se deve apenas à imposição das agências militares americanas, mas também ao fato der ter sido o primeiro protocolo a atingir a importante meta da comunicação de dados com abrangência mundial. Isto somente foi possível graças a algumas de suas características:

1. TCP/IP é um protocolo aberto, público e completamente independente de equipamentos e de sistemas operacionais;
2. TCP/IP não define protocolos para o nível físico, possibilitando sua implementação sobre uma grande variedade de protocolos já existentes, tais como: Ethernet, Token Ring e X.25;
3. O esquema de endereçamento do TCP/IP permite designar univocamente qualquer máquina, mesmo em redes globais como a Internet;
4. TCP/IP inclui protocolos do nível de aplicação que atendem muito bem à demanda de serviços imposta pelos usuários.

Uma vez que a padronização foi essencial para a definição do TCP/IP como o protocolo mais utilizado no mundo, é importante que se conheça como ele foi, e continua sendo, padronizado.

Originalmente, os protocolos básicos do TCP/IP foram padronizados através de Military Standards (MILSTD) e de Internet Engineering Notes (IEN). Atualmente, a maior parte da padronização do TCP/IP é feita através de Requests For Comments (RFC), que, além da especificação formal dos protocolos, inclui informações importantes sobre seu funcionamento e uso.

6.5.1 - AS CAMADAS DO TCP/IP.

A descrição da arquitetura do protocolo TCP/IP em camadas como as do modelo de referência OSI é controversa. As camadas OSI foram definidas por pesquisadores ao longo de anos, sempre com o compromisso acadêmico de ser um modelo de referência, enquanto que o protocolo TCP/IP não teve qualquer compromisso que não a funcionalidade. Assim sendo, tentar estabelecer uma relação precisa entre as camadas OSI e TCP/IP é algo praticamente impossível.

O modelo mais aceito para descrever a arquitetura TCP/IP é composto de quatro camadas: acesso à rede (ou camada de interface) , Internet (ou camada de rede), transporte e aplicação. Este modelo é apresentado na figura 6.9, em comparação ao modelo de referência OSI.

Da mesma forma que no modelo de referência OSI, os dados descem a pilha de protocolos para chegar a rede e sobem para chegar às aplicações. Cada camada da pilha de protocolos adiciona um cabeçalho com informações de controle e trata o que recebe da camada superior como sendo dados. Esta adição de informações de controle em cada nível é denominada encapsulamento e é ilustrada pela figura 6.10. O processo reverso acontece quando uma camada passa dados às superiores, ou seja, o cabeçalho é removido e o restante é passado para cima como dados.

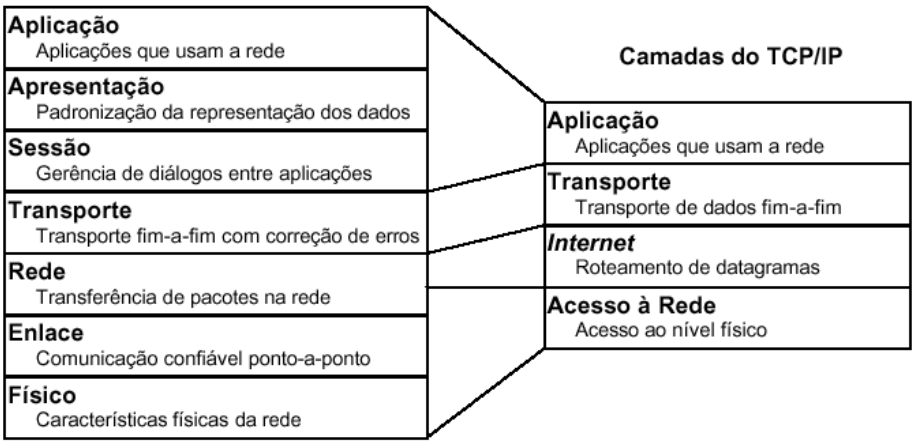


Figura 6.9 – Camadas da arquitetura TCP/IP em comparação com as camadas do RM-OSI

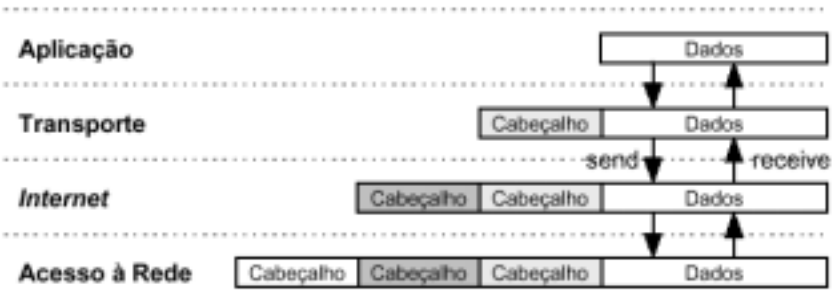


Figura 6.10 - Encapsulamento de dados na pilha TCP/IP.

Cada camada da pilha possui estruturas de dados próprias e independentes. Assim sendo, cada protocolo faz referência aos dados de forma específica. Por exemplo, aplicações que fazem uso do protocolo TCP se referem aos dados como streams, ao passo que aplicações que fazem uso do protocolo User Datagram Protocol (UDP) se referem aos dados como mensagens. O protocolo TCP, por sua vez, se refere aos dados como segmentos, enquanto que o UDP se refere aos dados como pacotes. O protocolo IP sempre se refere aos dados como datagramas, enquanto que os dados passados à camada de acesso à rede são referidos como frames ou quadros.

6.5.1.1 - A CAMADA DE ACESSO À REDE.

A **Camada de Acesso à Rede (ou Camada de Interface)** é a mais baixa na hierarquia de protocolos TCP/IP. Os protocolos nesta camada provêem meios para que os dados sejam transmitidos a outros computadores na mesma rede física. Esta camada pode abranger as três primeiras camadas do modelo de referência OSI: física, de enlace e de rede. Entretanto, a camada de acesso à rede do TCP/IP não define propriamente os protocolos para estes três níveis, mas sim como utilizar os protocolos já existentes para suportar a transmissão de um datagrama IP. À medida que novas tecnologias de rede vão surgindo, novos protocolos são acrescidos à camada de acesso à rede. As principais funções da camada de acesso à rede são: o encapsulamento de datagramas IP em *frames* para transmissão e a tradução de endereços IP em endereços físicos de rede. Estas duas funções apresentam implementações específicas para cada tipo de rede.

6.5.1.2 - A CAMADA INTERNET.

A **Camada Internet (ou Camada de Rede)** fica exatamente sobre a camada de acesso à rede. O *Internet Protocol* (IP), é o coração desta camada. Ele provê um serviço básico de datagrama sobre o qual as redes TCP/IP são implementadas. Todos os protocolos das camadas superiores a esta fazem uso do protocolo IP. As principais funções do protocolo IP são:

1. definir o datagrama IP, que é a unidade básica de transmissão de dados da arquitetura TCP/IP;
2. definir o esquema de endereçamento IP;

3. passar dados da camada de acesso à rede à camada de transporte;
4. rotear datagramas IP;
5. fragmentar e remontar datagramas IP.

O **IP** é um protocolo não orientado a conexão, ou seja, não existe negociação prévia de uma conexão para a transmissão de dados. Isto não impede a existência de protocolos orientados à conexão nas camadas superiores, mas eles deverão negociar o estabelecimento de conexões por si próprios. Além de ser não orientado à conexão, o protocolo IP também é não confiável, uma vez que não suporta mecanismos de detecção e recuperação de erros. Em outras palavras, o protocolo IP não verifica se um datagrama foi recebido corretamente, deixando esta responsabilidade para os protocolos das camadas superiores.

Outros protocolos da Camada Internet são o *Internet Message Control Protocol* (ICMP) e o *Address Resolution Protocol* (ARP).

O **ICMP** é utilizado para enviar alertas aos hosts sobre anormalias na rede. Também é utilizado para a obtenção de informações sobre a rede. O comando "PING", muito utilizado para verificar se um *host* está ativo, é uma aplicação do ICMP.

O **ARP** é um protocolo de resolução de endereços que permite a associação dos endereços físicos das interfaces de rede com a numeração promovida pelo endereçamento do protocolo IP.

6.5.1.3 - A CAMADA DE TRANSPORTE.

A **Camada de Transporte** fim-a-fim está localizada exatamente sobre a camada Internet na hierarquia TCP/IP. Os principais protocolos desta camada são: *Transmission Control Protocol* (TCP), o *User Datagram Protocol* (UDP).

O **TCP** é um protocolo orientado a conexão com detecção e correção de erros fim-a-fim. O **UDP** é um protocolo não orientado a conexão e não confiável, sendo portanto muito leve. Ambos os protocolos passam dados entre as camadas de aplicação e Internet. Cada aplicação é livre para escolher o protocolo que melhor se adapta a sua natureza.

O User Datagram Protocol (UDP) provê meios para que aplicações tenham acesso direto ao serviço de datagrama IP. Aplicações que usam este protocolo inserem pouco overhead na rede. Como o próprio IP, o protocolo UDP é não orientado a conexão e não confiável. Note que a expressão não confiável implica apenas a inexistência de mecanismos de confirmação do correto recebimento do datagrama. O protocolo UDP é utilizado principalmente por aplicações que transmitem dados em pequenas quantidades, de tal forma que o overhead de uma conexão é maior do que o da retransmissão dos dados em caso de erro. Além disto, as aplicações do modelo cliente/servidor freqüentemente fazem uso de protocolos do tipo requisição/resposta que são melhor implementados sobre UDP, uma vez que não existem conexões preestabelecidas entre clientes e servidores.

O Transmission Control Protocol (TCP) é um protocolo orientado a conexão e confiável. A transmissão de dados através de uma conexão, ou stream, se dá através de segmentos. De forma similar ao pacote UDP, cada segmento carrega informações sobre as aplicações origem e destino (ports).

Os protocolos da camada de transporte serão estudados com mais profundidade posteriormente.

6.5.1.4 - A CAMADA DE APLICAÇÃO.

A **Camada de Aplicação** fica no topo da pilha TCP/IP e inclui todos os processos que utilizam serviços das camadas inferiores para transmitir dados através da rede. Alguns protocolos desta camada são :

1. Telnet: serviço de terminal virtual que permite sessões remotas sobre a rede;
2. File Transfer Protocol (FTP): serviço de transferência de arquivos pela rede;
3. Simple Mail Transfer Protocol (SMTP): serviço de correio eletrônico;
4. Domain Name Service (DNS): serviço de tradução de nomes de hosts em endereços IP;
5. Routing Information Protocol (RIP): suporta a troca de informações de roteamento entre gateways;
6. Network File System (NFS): sistema de arquivos remotamente acessíveis.

A figura 6.11 demonstra o processamento de uma solicitação para transferência de arquivo entre 2 computadores através da arquitetura TCP/IP em uma aplicação baseada no FTP – "File Transfer Protocol". C.4, C.3,

C.2 e C.1 são as camadas de aplicação (no caso FTP), de transporte (o TCP), internet (o IP) e de acesso ao meio que varia conforme o enlace físico sendo, no caso,: PPP, Ethernet - ETH e "Asynchronous Transfer Mode" - ATM.

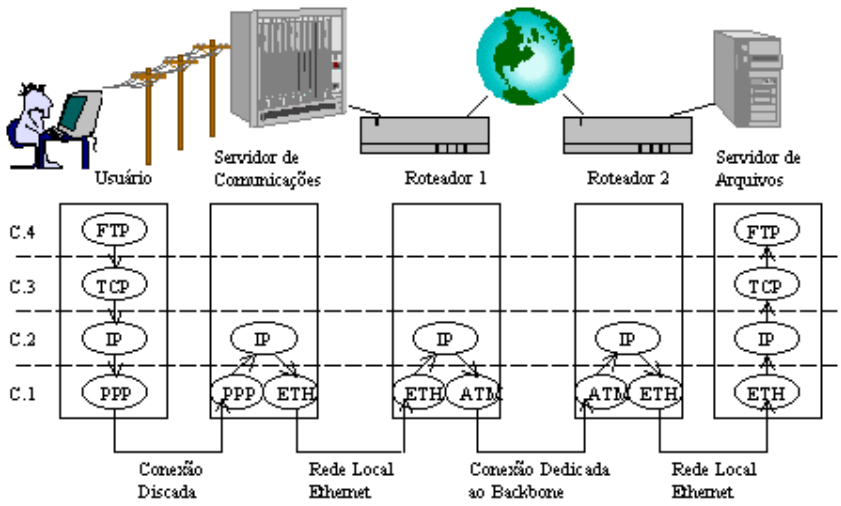


Figura 6.11 - Processamento de uma requisição FTP através da arquitetura TCP/IP

A figura 6.11 também ilustra uma das formas mais comuns de acesso à Internet:

1. O usuário utiliza um computador ligado a uma linha telefônica por um MODEM e conecta-se a um Provedor de Acesso, representado pelo Servidor de Comunicação e pelo Roteador 1.
2. O Provedor de Acesso recebe o usuário pelo servidor de comunicação e atribui ao seu computador um endereço para que as informações enviadas e recebidas possam trafegar pela arquitetura TCP/IP.
3. Uma vez conectado e com o endereço correto, a aplicação requisitada pelo usuário passa a trafegar através de roteadores e "backbones", representados pelo globo terrestre, até encontrar o seu destino.
4. No destino, sua requisição é atendida e enviada de volta, pelo mesmo principio de identificação de endereços de origem e destino.

6.5.2 – ENDEREÇAMENTO IP.

Como já vimos. o protocolo IP é responsável pelo **endereçamento** dos componentes ativos em uma rede de arquitetura TCP/IP. Ele atua na camada internet e sua unidade de informação é o datagrama (ou pacote) que, entre outras informações, possui o número identificador do equipamento origem da informação transportada e o número do equipamento de destino. O endereçamento baseado em um identificador, que independe da tecnologia de interconexão envolvida, é obtido em uma representação binária de 32 bits que deve ser único na rede. No caso da Internet, não existem dois equipamentos com o mesmo identificador em todo o mundo.

O formato de apresentação dos endereços IP é uma representação decimal em grupos de 4 dígitos separados por ponto. Teoricamente, esses endereços variam de 0.0.0.0 até 255.255.255.255 - pois 255_{10} é a representação decimal de 11111111_2 , valor máximo representado com 8 algarismos binários ou 1 byte. A figura 6.12 exemplifica a representação decimal de um endereço IP.

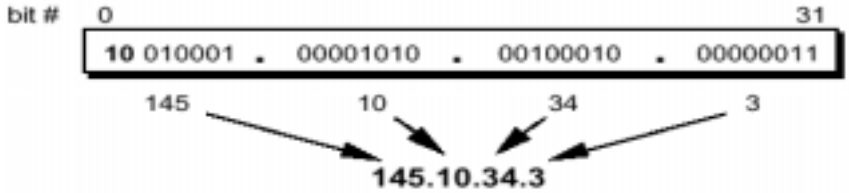


Figura 6.12 - Representação de um endereço IP.

As sequências numéricas que identificam redes e equipamentos a ela associados, são organizadas na forma de classes. Cada byte do endereço pode significar uma rede ou um host, dependendo da classe a qual o endereço pertence.

As classes definidas pelo InterNIC para a Internet são:

CLASSE A - o primeiro byte representa o número da rede e os três restantes são números de hosts.

CLASSE B - os dois primeiros bytes representam o número da rede e os dois restantes são números de hosts.

CLASSE C - o último byte representa números de hosts e os três primeiros identificam a rede.

CLASSE D - Especifica "multicast address" utilizados para transmissão simultânea de informação a um grupo de hosts identificados por um endereço especial de destino.

CLASSE E - Reservada para uso futuro.

A figura 6.13 detalha as faixas de endereçamento das classes A, B e C.

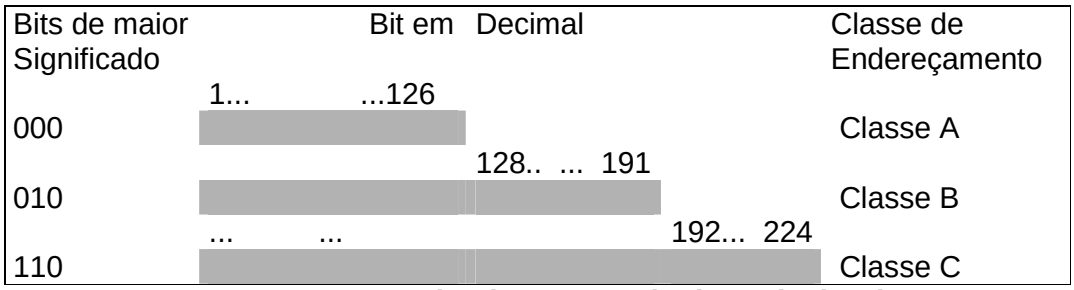


Figura 6.13 - Faixas de endereçamento IP das classes adotadas pelo InterNIC.

Pela convenção apresentada, é possível identificar a classe e, através dela, o endereço de rede e do host na rede IP. Como exemplos:

1 - O endereço 200.195.20.37 pertence à classe C - o primeiro byte é maior que 192. Portanto, o endereço de rede é composto dos 3 primeiros bytes, ou seja, 200.195.20 e o endereço do equipamento ligado a esta rede é .37.

2 - O endereço 128.127.50.112 pertence à classe B - o primeiro byte é maior que 127 e menor que 191. Portanto o endereço de rede é composto dos 2 primeiros bytes: 128.127 e o endereço do equipamento pertencente a esta rede é .50.112.

O InterNIC convencionou os seguintes endereços para redes internas, definidas no documento RFC1597, e que não estão disponíveis em redes ligadas à Internet :

10.0.0.1 até 10.255.255.255	Classe A
172.16.0.0 até 172.31.255.255	Classe B
192.168.0.0 até 192.168.255.255	Classe C

Alguns endereços são reservados para funções especiais:

1. **Endereço de Rede**: Identifica a própria rede e não uma interface de rede específica, representado por todos os bits de hostid com o valor ZERO.
2. **Endereço de Broadcast**: Identifica todas as máquinas na rede específica, representado por todos os bits de hostid com o valor UM.
3. **Endereço de Broadcast Limitado**: Identifica um broadcast na própria rede, sem especificar a que rede pertence. Representado por todos os bits do endereço iguais a UM = 255.255.255.255.
4. **Endereço de Loopback**: O endereço de rede 127.0.0.0 é reservado para o tráfego local da máquina. Normalmente o endereço 127.0.0.1 é definido para uma interface especial denominada interface local (loopback interface) ou local host, que atua como um circuito fechado. Qualquer pacote IP enviado para esta interface a partir dos protocolos TCP ou UDP será retornado ao próprio host que o enviou como se estivesse chegando da rede.

Desta forma, para cada rede A, B ou C, o primeiro endereço e o último são reservados e não podem ser usados por interfaces de rede.

As máquinas com mais de uma interface de rede (caso dos roteadores ou máquinas interligadas à mais de uma rede, mas que não efetuam a função de roteamento) possuem um endereço IP para cada uma, e podem ser identificados por qualquer um dos dois de modo independente. Um endereço IP identifica não uma máquina, mas uma conexão à

rede.

Para interligar uma rede à Internet, é necessário requisitar um bloco de endereços ao orgão responsável pelo controle da numeração IP designado como responsável para a área geográfica onde a rede se encontra. No Brasil, existem empresas, entidades e orgãos governamentais que oferecem backbone Internet. Esses provedores de backbone normalmente se incumbem de fornecer o bloco numérico de IP.

Os endereços de computadores e redes oferecidos pelo protocolo IP não são suficientes para localizar uma aplicação ou serviço na rede. Existe um outro identificador para serviços denominado "port" associado a um protocolo da camada de transporte (TCP ou UCP) para o estabelecimento de comunicação entre a aplicação que gera o serviço e o usuário que irá utilizá-la. O conjunto: IP + PORT + (TCP ou UDP), é denominado "socket". Existem "ports" convencionados na Internet para serviços utilizados em toda a rede. Os mais difundidos são:

Serviço:	"Port":	Protocolo:
FTP	21	TCP
TELNET	23	TCP
SMTP	25	TCP
POP3	110	TCP
DNS	53	UDP
HTTP	80	TCP

6.5.2.1 - REDES IP.

Redes IP estão estruturadas de uma forma similar aos Correios. Toda a Internet consiste em um número de redes próprias, denominadas sistemas autônomos. Cada sistema destes executa qualquer roteamento interno entre seus membros, porém a tarefa de entregar um datagrama resume-se em encontrar-se um caminho para a rede da máquina de destino. Isso significa que assim que o datagrama é enviado para qualquer máquina que esteja em uma rede, processos adicionais são executados exclusivamente pela rede de destino (como no caso dos correios locais).

Ao se escrever uma carta para alguém, deve ser colocado o endereço completo do destinatário no envelope, especificando-se o País, Estado, CEP, etc. Após isso ela é colocada em uma caixa de correio e os Correios a enviarão para o seu destino: a carta vai até o País indicado, onde o serviço de correio local a enviará para o estado indicado, para a cidade de destino, etc. A vantagem deste sistema hierárquico é óbvia: toda vez que uma carta for postada, o correio local saberá o endereço do destinatário, mas não tem que se preocupar em como a carta irá viajar até chegar ao seu destino Final. Assim funcionam as redes IP.

A figura 6.14 abaixo mostra exemplos de endereçamento de máquinas situadas na mesma rede e em redes diferentes. Pode ser observado que como o endereço começa por 200, eles são de classe C. Por isto, os três primeiros bytes do endereço identificam a rede. Como na primeira figura, ambas as estações tem o endereço começando por 200.18.171, elas estão na mesma rede. Na segunda figura, as estações estão em redes distintas e uma possível topologia é mostrada, onde um roteador interliga diretamente as duas redes.

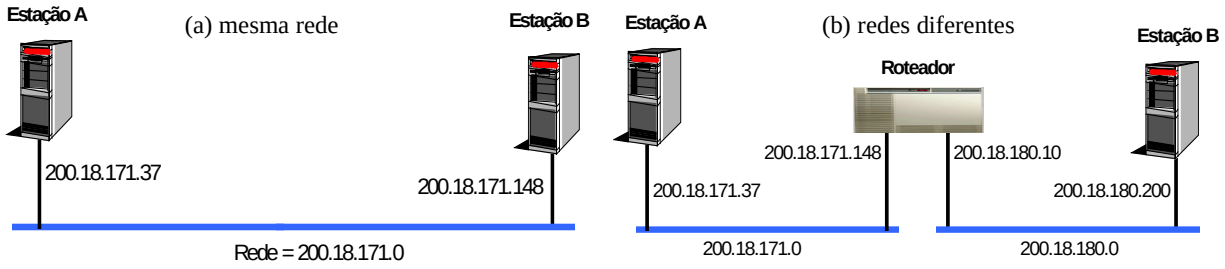


Figura 6.14 - Exemplos de endereçamento de máquinas situadas (a) na mesma rede e (b) em redes diferentes

6.5.2.2 - SUB-REDES IP.

A estrutura de sub-redes IP (*subnet*) é produzida através da divisão de um endereço IP em uma parte destinada à identificação da rede e outra parte destinada à máquina. Por padrão a rede de destino é derivada da parte do endereço

IP definida para redes. Obviamente, hosts com endereços IP de rede idênticos devem estar localizadas na mesma rede.

A RFC 950, de 1985, define o procedimento padrão de suporte à sub-redes e a divisão de redes classes A,B e C em partes menores.

O protocolo IP permite a divisão de uma rede IP em diversas sub-redes. Uma sub-rede assume a responsabilidade pela entrega de datagramas em uma determinada faixa de endereços IP de uma rede IP da qual ela faça parte. Assim como nas classes de rede A, B ou C, ela é identificada pela parte de rede do endereço IP. A parte de rede é porém expandida, incluindo-se alguns bits da parte de endereço de máquina. O número de bits que são interpretados como o número da sub-rede é definido pelo parâmetro denominado máscara de sub-rede, ou sub*net mask*. Esta é composta por um número de 32 bits que especifica a parte de rede do endereço IP. Os bits do endereço IP e da máscara de sub-rede têm correspondência em um para um. Para obter o endereço de rede, é realizada uma operação lógica AND entre os bits do endereço IP e os bits da máscara de sub-rede. Na máscara de sub-rede, o bit 1(um) indica endereço de rede e o bit 0 (zero) endereço de host. O exemplo seguinte demonstra a constituição de uma mascara de sub-rede.

	Notação Decimal	Notação Binária
Endereço IP	130.5.5.1	10000010.00000101.00000101.00000001
Máscara de sub-rede	255.255.0.0	11111111.11111111.00000000.00000000
	Operação AND para obter o endereço de rede	10000010.00000101.00000000.00000000
Endereço de rede IP	130.5.0.0	

A máscara de sub-rede 255.255.0.0 é característica da Classe B. Do mesmo modo, a Classe A é definida pela máscara 255.0.0.0 e a Classe C por 255.255.255.0.

Existe outro modo convencionado para representar máscaras de sub-rede. Elas podem ser representadas por um valor decimal correspondente ao número de bits 1 (um) utilizados para compor a máscara colocado logo após o endereço IP. Para separar o valor que representa a máscara de sub-rede do número IP utiliza-se uma barra (/). Exemplificando, no quadro acima o endereço IP 130.5.5.1 e sua máscara 255.255.0.0 podem ser descritos da seguinte maneira: 130.5.5.1/16, pois 16 é o número de bits 1 (um) utilizado na máscara de sub-rede.

É importante frisar que a definição de sub-rede é somente uma divisão interna da rede. Sub-redes são geradas pelos administradores locais das redes. Freqüentemente, sub-redes são criadas para redefinir limites existentes, sejam físicos (entre duas redes Ethernets), administrativos (entre dois departamentos) ou geográficos, sendo que a autoridade sobre essas sub-redes é delegada a alguma pessoa de contato. De qualquer forma, esta estrutura afeta somente o comportamento interno da rede e é completamente invisível para o mundo externo.

Para ilustrar a criação de sub-redes IP em uma rede IP de classe C, vamos dividir a rede IP 193.1.1.0/24 em oito sub-redes.

```
Base Net:  11000001.00000001.00000001.00000000 = 193.1.1.0/24

Subnet #0: 11000001.00000001.00000001.00000000 = 193.1.1.0/27
Subnet #1: 11000001.00000001.00000001.00100000 = 193.1.1.32/27
Subnet #2: 11000001.00000001.00000001.01000000 = 193.1.1.64/27
Subnet #3: 11000001.00000001.00000001.01100000 = 193.1.1.96/27
Subnet #4: 11000001.00000001.00000001.10000000 = 193.1.1.128/27
Subnet #5: 11000001.00000001.00000001.10100000 = 193.1.1.160/27
Subnet #6: 11000001.00000001.00000001.11000000 = 193.1.1.192/27
Subnet #7: 11000001.00000001.00000001.11100000 = 193.1.1.224/27
```

Podemos observar que a máscara utilizada para obter oito sub-redes é /27, porque a máscara padrão para uma rede IP classe C é 255.255.255.0 (24 bits com valor igual a 1) e além dela foram elevados para 1 (um) mais três bits (24 + 3 = 27). Em binário: 11111111.11111111.11111111.**11100000.** Convertendo-se 11100000_2 para decimal teremos o valor $224_{10.}$ Então esta máscara pode ser escrita também como sendo: 255.255.255.224.

Os endereços das sub-redes formadas pela aplicação da máscara serão os que resultam da aplicação da operação AND, como descrito acima. Assim, serão endereços de rede IP no exemplo acima: 193.1.1.0/27; 193.1.1.32/27; 193.1.1.64/27; 193.1.1.96/27; 193.1.1.128/27; 193.1.1.160/27; 193.1.1.192/27 e 193.1.1.224/27. O último endereço de cada conjunto de IPs formado é utilizado pela rede para *broadcasting*, ou seja, para acesso simultâneo a todos os endereços válidos do conjunto. Então, serão endereços de *broadcasting* no exemplo:

193.1.1.31/27; 193.1.1.63/27; 193.1.1.95/27; 193.1.1.127/27; 193.1.1.159/27; 193.1.1.191/27; 193.1.1.223/27 e 193.1.1.255/27.

Para saber quantos endereços poderão ser utilizados em cada sub-rede com a aplicação de uma determinada máscara basta aplicar a seguinte fórmula:

$$\text{número de endereços válidos} = 2^{(\text{número de bits iguais a zero da máscara de sub-rede})} - 2$$

Para saber quantss sub-redes serão geradas com a aplicação de uma determinada máscara basta aplicar a seguinte fórmula:

$$\text{número de sub-redes} = 2^{(\text{número de bits iguais a um da máscara de sub-rede})}$$

6.5.2.3 - RESOLUÇÃO DE ENDEREÇOS IP EM ENDEREÇOS DE REDE.

Os protocolos de rede compartilhada como Ethernet, Token-Ring e FDDI possuem um endereço próprio para identificar as diversas máquinas situadas na rede. Em Ethernet e Token-Ring o endereçamento utilizado é chamado endereço físico ou endereço MAC - Medium Access Control , formado por 6 bytes, conforme a figura 6.15 abaixo:

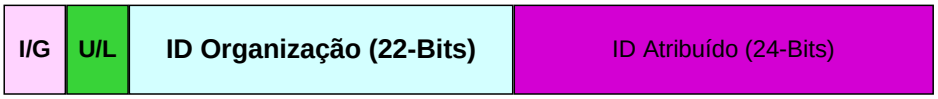


Figura 6.15 – Constituição do endereço MAC.

Este tipo de endereçamento só é útil para identificar diversas máquinas, não possuindo nenhuma informação capaz de distinguir redes distintas. Para que uma máquina com protocolo IP envie um pacote para outra máquina situada na mesma rede, ela deve se basear no protocolo de rede local, já que é necessário saber o endereço físico. Como o protocolo IP só identifica uma máquina pelo endereço IP, deve haver uma associação entre o endereço IP e o endereço de rede MAC. Esta associação, realizada pelo protocolo *Address Resolution Protocol* (ARP) é conhecida como mapeamento.

O mapeamento via protocolo ARP só é necessário em uma rede do tipo compartilhada como Ethernet, Token-Ring, FDDI, entre outras. Em uma rede ponto-a-ponto como, por exemplo, um enlace serial, o protocolo ARP não é necessário, já que há somente um destino possível.

A figura 6.16 mostra uma rede com 3 estações, onde uma máquina A com endereço IP 200.18.171.1 deseja enviar uma mensagem para a máquina B cujo endereço é 200.18.171.3. A mensagem a ser enviada é uma mensagem IP. No caso deste exemplo, antes de efetivamente enviar a mensagem IP, a estação utilizará o protocolo ARP para determinar o endereço MAC da interface cujo endereço IP é o destino da mensagem.

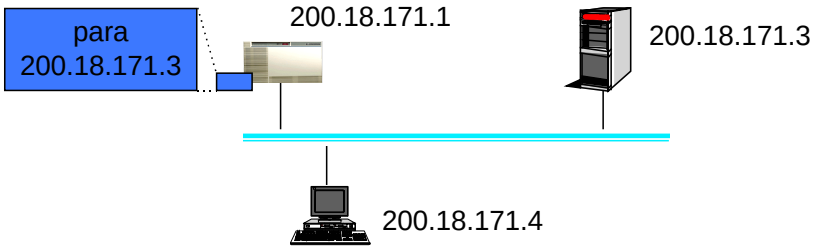


Figura 6.16 (a) – Exemplo do funcionamento do protocolo ARP. Inicio do envio da mensagem.

O funcionamento do protocolo ARP é descrito abaixo:

1. Estação A verifica que a máquina destino está na mesma rede local, determinado através dos endereços origem e

destino e suas respectivas classes.

2. O protocolo IP da estação A verifica que ainda não possui um mapeamento do endereço MAC para o endereço IP da máquina destino.

3. O protocolo IP solicita ao protocolo que o endereço MAC necessário

4. Protocolo ARP envia um pacote ARP (ARP Request) com o endereço MAC destino de broadcast (difusão para todas as máquinas)

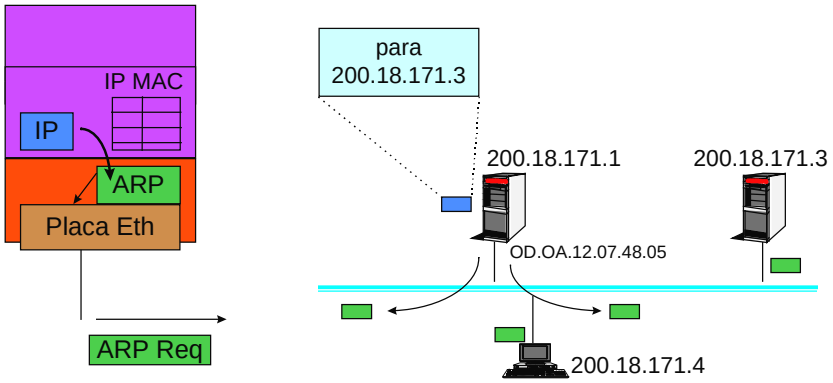
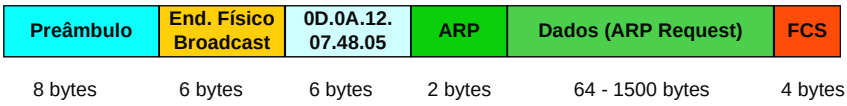


Figura 6.16 (b) – Exemplo do funcionamento do protocolo ARP. Envio de pacote ARP em difusão.

5. A mensagem ARP enviada é encapsulada em um pacote Ethernet conforme diagrama abaixo:



6. Todas as máquinas recebem o pacote ARP, mas somente aquela que possui o endereço IP especificado responde. A máquina B já instala na tabela ARP o mapeamento do endereço 200.18.171.1 para o endereço MAC de A.

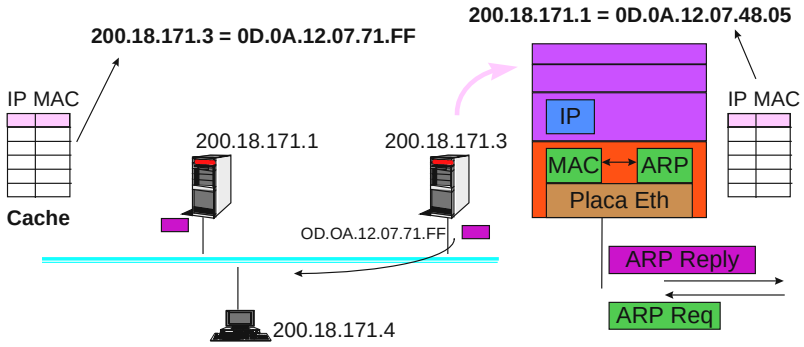
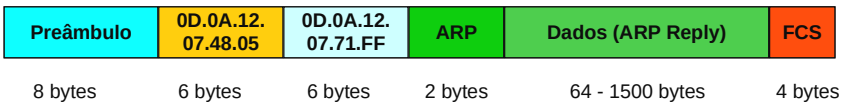


Figura 6.16 (c) – Exemplo do funcionamento do protocolo ARP. Resposta à requisição ARP.

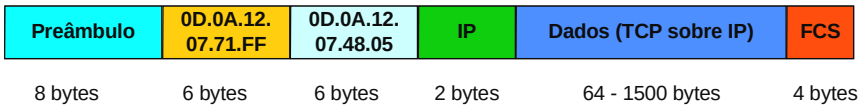
7. A resposta é enviada no pacote Ethernet, encapsulado conforme mostrado abaixo, através de uma mensagem ARP Reply endereçado diretamente para a máquina origem.



8. A máquina A recebe o pacote e coloca um mapeamento do endereço IP de B e seu endereço MAC respectivo. Esta

informação residirá em uma tabela que persistirá durante um certo tempo.

9. Finalmente a máquina A transmite o pacote IP inicial, após saber o endereço MAC da estação destino.



Os protocolos de nível de Rede como Ethernet possuem um identificador para determinar o tipo do protocolo que está sendo carregado no seu campo de dados. Um pacote Ethernet pode, por exemplo, carregar os protocolos ARP, IP, RARP, IPX, Netbios e outros. A figura 6.17 mostra o formato do quadro Ethernet. Note que o campo protocolo, de 2 bytes de tamanho identifica o protocolo sendo carregado no campo de dados. No caso de transporte de um pacote ARP, o valor é 0806h (hexadecimal), enquanto que no caso de IP este campo tem o valor 0800h.

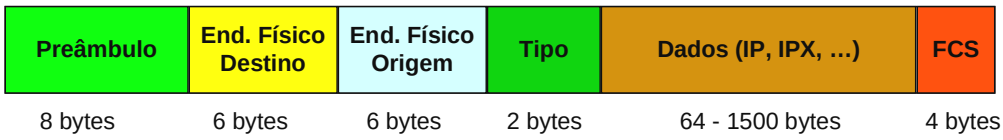


Figura 6.17 – Quadro (frame) Ethernet

6.5.3 – ROTEAMENTO IP.

O destino de um datagrama IP sendo enviado por um host pode ser a próprio host, um host situado na mesma rede ou um host situado numa rede diferente. No primeiro caso, o pacote é enviado ao nível IP que o retorna para os níveis superiores. No segundo caso, é realizado o mapeamento por meio de ARP e a mensagem é enviada por meio do protocolo de rede.

Quando um host deve enviar um pacote para outra rede, o protocolo IP deve enviá-lo para um roteador situado na mesma rede. O roteador por sua vez irá enviar o pacote para outro roteador, e assim sucessivamente até que o pacote chegue ao destino final. Este tipo de roteamento é chamado de *Next-Hop Routing*, já que um pacote é sempre enviado para o próximo roteador no caminho.

Neste tipo de roteamento, não há necessidade de que um roteador conheça a rota completa até o destino. Cada roteador deve conhecer apenas o próximo roteador para o qual deve enviar a mensagem. Esta decisão é chamada de decisão de roteamento. Um host situado em uma rede que tenha mais de um roteador deve também tomar uma decisão de roteamento para decidir para qual roteador deve enviar o pacote IP.

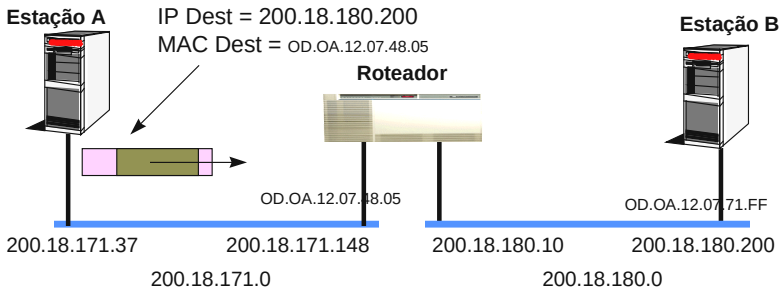
Quando uma estação deve enviar uma mensagem IP para outra rede, ela deve seguir os seguintes passos:

1. Determinar que o hist destino está em outra rede e por isto deve-se enviar a mensagem para um roteador.
2. Determinar, através da tabela de rotas da máquina origem, qual roteador é o correto para se enviar a mensagem.
3. Descobrir, através do protocolo ARP, qual o endereço MAC do roteador.
4. Enviar a mensagem IP com o endereço de nível de rede apontado para o roteador e o endereço IP (na mensagem IP) endereçado para a máquina destino.

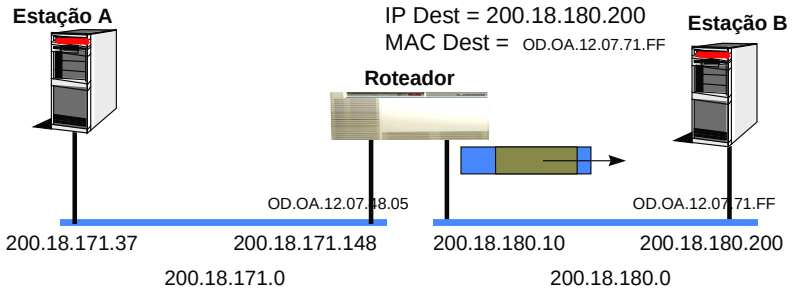
Uma questão importante no pacote roteado consiste no fato de que o pacote a ser roteado é endereçado fisicamente ao roteador (endereço MAC), mas é endereçado logicamente (endereçamento IP) à máquina destino. Quando o roteador recebe um pacote que não é endereçado a ele, tenta roteá-lo.

A decisão de roteamento é baseada em uma tabela, chamada de **tabela de rotas**, que é parte integrante de qualquer protocolo IP. Esta tabela relaciona cada rede destino ao roteador para onde o pacote deve ser enviado para chegar a ela.

A figura 6.18 ilustra o funcionamento do roteamento.



(a) A estação A envia um datagrama com destino a B



(b) O roteador recebe o pacote e transfere para o meio de transmissão que tem acesso à estação B.

Figura 6.18 – Roteamento de um datagrama IP por um roteador.

Na figura 6.18 o roteamento é realizado somente por um roteador. Caso houvesse mais de um roteador a ser atravessado, o primeiro roteador procederia de forma idêntica à Estação A, ou seja, determinaria a rota correta e enviaria a mensagem para o próximo roteador.

Os Algoritmos de transmissão e recepção de um pacote IP são descritos a seguir.

ALGORITMO DE TRANSMISSÃO

1. Datagrama pronto para ser transmitido

2. Caso:

2.1 Endereço Destino == Endereço Transmissor

2.1.1 Entrega datagrama pela interface loopback (127.0.0.1)

2.2.2 Fim

2.2 Endereço de rede do destino == endereço de rede local

2.2.1 Descobre o endereço físico do destino (ARP)

2.2.1 Transmite datagrama pela interface correta

2.2.2 Fim

2.3 Endereço de rede do destino != endereço de rede local

2.3.1 Verifica tabela de rotas

2.3.2 Descobre rota que se encaixa com a rede destino

2.3.3 Descobre o endereço físico do gateway (ARP)

2.3.4 Transmite o datagrama para o gateway

2.3.5 Fim

3. Fim

ALGORITMO DE RECEPÇÃO

1. Datagrama recebido da camada intra-rede, defragmentado e testado

2. Caso:

2.1 Endereço Destino = Endereço do Host, ou E.D. = outras interfaces do Host, ou E.D. = Broadcast

2.1.1 Passa datagrama para níveis superiores -> FIM

2.2 Caso:

2.2.1 Máquina que recebeu não é roteador

2.2.1.1 Descarta datagrama -> FIM

2.2.2 Máquina é roteador (possui mais de uma interface IP)

2.2.2 Caso:

2.2.2.1 Endereço IP destino = Rede IPcom interface direta

2.2.2.1.1 Descobre o endereço físico do destino (ARP)

2.2.2.1.2 Transmite datagrama pela interface respectiva -> FIM

2.2.2.2 Caso Endereço de rede do destino endereço de rede local

2.2.2.2.1 Verifica tabela de rotas

2.2.2.2.2 Descobre o endereço físico do gateway (ARP)

2.2.2.2.3 Transmite o datagrama para o gateway -> FIM

3. Fim

A figura 6.19 ilustra uma estrutura de redes. As tabelas de rotas de cada roteador são diferentes uma das outras. Note nestas tabela a existência de rotas diretas, que são informações redundantes para identificar a capacidade de acessar a própria rede na qual os roteadores estão conectados. Este tipo de rota apesar de parecer redundante é útil para mostrar de forma semelhante as rotas diretas para as redes conectadas diretamente no roteador.

Outra informação relevante é a existência de uma rota default. Esta rota é utilizada durante a decisão de

roteamento no caso de não existir uma rota específica para a rede destino da mensagem IP. A rota default pode ser considerada como um resumo de diversas rotas encaminhadas pelo mesmo próximo roteador. Sem a utilização da rota default, a tabela de rotas deveria possuir uma linha para cada rede que pudesse ser endereçada. Em uma rede como a Internet isto seria completamente impossível.

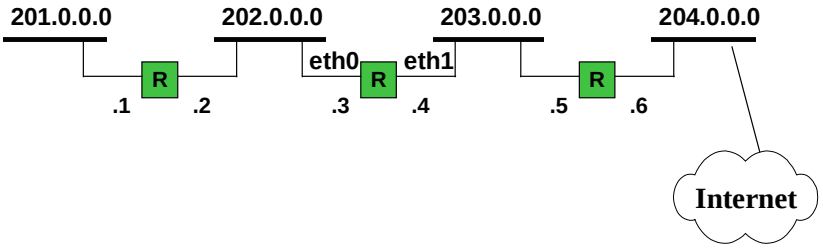


Figura 6.19 – Exemplo de estrutura de rede incluindo três roteadores (R).

A tabela de rotas para o roteador da esquerda na figura 6.19 é descrita abaixo:

Rede Destino	Roteador (Gateway)	Hops
201.0.0.0	eth0 (rota direta)	0
202.0.0.0	eth1 (rota direta)	0
203.0.0.0	202.0.0.3	1
204.0.0.0	203.0.0.3	2
Default	203.0.0.3	--

A tabela de rotas para o roteador central na figura 6.19 é descrita abaixo:

Rede Destino	Roteador (Gateway)	Hops
202.0.0.0	eth0 (rota direta)	0
203.0.0.0	eth1 (rota direta)	0
201.0.0.0	202.0.0.2	1
204.0.0.0	203.0.0.5	1
Default	203.0.0.5	--

A tabela de rotas para o roteador da direita na figura 6.19 é descrita abaixo:

Rede Destino	Roteador (Gateway)	Hops
203.0.0.0	eth0 (rota direta)	0
204.0.0.0	eth1 (rota direta)	0
202.0.0.0	203.0.0.4	1
201.0.0.0	203.0.0.4	1
Default	204.0.0.7**	--

** Não mostrado na figura.

A rota default geralmente é representada nos sistemas operacionais como a rede 0.0.0.0.

6.5.3.1 - ROTEAMENTO ESTÁTICO X ROTEAMENTO DINÂMICO

A alimentação das informações na tabela de rotas pode ser de modo estático ou dinâmico ou ambos. Na alimentação estática, as rotas são preenchidas manualmente, geralmente pela configuração inicial da máquina. Na alimentação dinâmica, protocolos como RIP, RIP2, OSPF ou BGP4 são responsáveis pela aquisição de informações sobre a topologia da rede e a publicação de rotas na tabela de rotas dos roteadores envolvidos.

6.5.4 – FRAGMENTAÇÃO DE PACOTES IP.

Um pacote IP pode ter um tamanho de até 64 Kbytes. Entretanto o nível de rede geralmente tem um tamanho máximo menor que 64K. Por exemplo, uma rede Ethernet pode transmitir uma mensagem de até 1500 bytes. Este valor

é chamado de MTU - Maximum Transmission Unit - para este tipo de rede. A camada IP deve então ser capaz de dividir um pacote IP maior que 1500 bytes em diversos fragmentos de até 1500 bytes cada um.

A fragmentação do pacote IP pode ocorrer na máquina origem ou em algum roteador que possua uma rede com MTU menor que o tamanho do pacote IP sendo roteado. Note que durante o percurso até o destino, um fragmento pode ser novamente fragmentado se o MTU da rede seguinte for ainda menor que o tamanho do fragmento. A remontagem do pacote só é realizada pela máquina destino, baseado nas informações de FRAGMENT OFFSET e bit MF. A perda de um fragmento inutiliza o datagrama inteiro.

O campo FRAGMENT OFFSET identifica a posição em Bytes do fragmento face ao pacote IP completo conforme pode ser visto na figura 6.20.

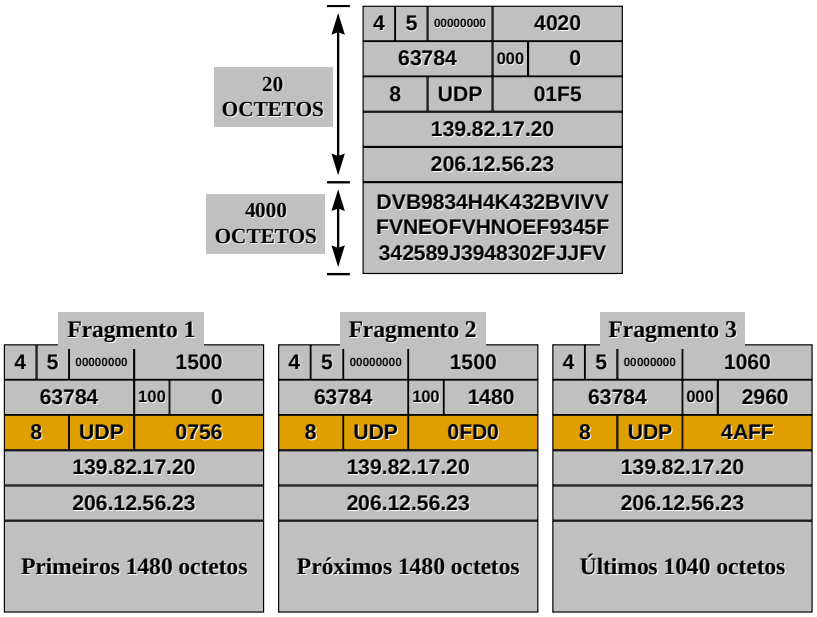


Figura 6.20 – Fragmentação do pacote IP.

A figura 6.21 demonstra a fragmentação de um pacote quando este passa para uma rede com MTU menor que o tamanho do pacote IP.

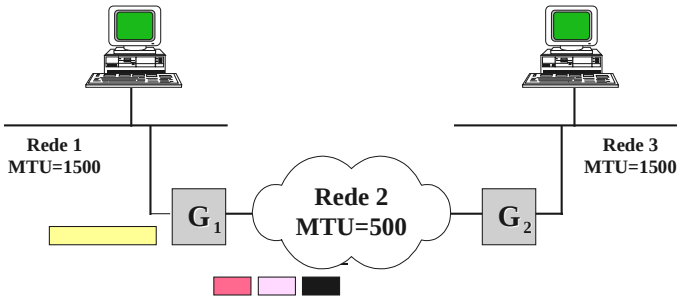


Figura 6.21 – Exemplo de fragmentação do pacote IP.

6.5.5 – PROTOCOLOS DA CAMADA DE TRANSPORTE

A camada de transporte do TCP/IP reúne os protocolos que realizam as funções de transporte de dados fim-a-fim, ou seja, considerando apenas a origem e o destino da comunicação, sem se preocupar com os elementos intermediários. A camada de transporte possui dois protocolos que são o UDP (User Datagram Protocol) e TCP (Transmission Control Protocol).

O protocolo UDP realiza apenas a multiplexação para que várias aplicações possam acessar o sistema de comunicação de forma coerente.

O protocolo TCP realiza além da multiplexação, uma série de funções para tornar a comunicação entre origem e destino mais confiável. São responsabilidades do protocolo TCP o controle de fluxo, o controle de erros, o sequenciamento e a multiplexação de mensagens.

A camada de transporte oferece para o nível de aplicação um conjunto de funções e procedimentos de acesso ao sistema de comunicação que permitem a criação e a utilização de aplicações de forma independente da implementação. Desta forma, as interfaces socket (ambiente Unix) e Winsock (ambiente Windows) fornecem um conjunto de funções-padrão para permitir que as aplicações possam ser desenvolvidas independentes do sistema operacional no qual serão executadas.

6.5.5.1 - PROTOCOLO UDP

O protocolo UDP fornece uma forma simples de acesso ao sistema de comunicação, provendo um serviço sem conexão, sem confiabilidade e sem correção de erros. A principal função do nível de transporte implementada em UDP é a capacidade de multiplexação de acesso ao sistema de comunicação. Esta função permite que vários processos ou programas executando em um computador possam acessar o sistema de comunicação e o tráfego de dados respectivo a cada um deles seja corretamente identificado, separado e utilize buffers individuais.

Um processo é o programa que implementa uma aplicação do sistema operacional, e que pode ser uma aplicação da camada de aplicação TCP/IP.

A forma de identificação de um ponto de acesso de serviço (SAP) do modelo OSI é a **porta** ou “port” de protocolo em TCP/IP. A porta é a unidade que permite identificar o tráfego de dados destinado a diversas aplicações. A identificação única de um processo acessando os serviços TCP/IP é, então, o endereço IP da máquina e a porta (ou portas) usada pela aplicação. Cada processo pode utilizar mais de uma porta simultaneamente, mas uma porta só pode ser utilizada por uma aplicação em um dado momento. Uma aplicação que deseje utilizar os serviços de comunicação deverá requisitar uma ou mais portas para realizar a comunicação. A mesma porta usada por uma aplicação pode ser usada por outra, desde que a primeira tenha terminado de utilizá-la.

A forma de utilização de portas mostra uma distinção entre a parte cliente e a parte servidor de uma aplicação TCP/IP. O programa cliente pode utilizar um número de porta qualquer, já que nenhum programa na rede terá necessidade de enviar uma mensagem para ele. Já uma aplicação do tipo servidor deve utilizar um número de porta convencionado ou “popular” (Well-known ports) de modo que um cliente qualquer que deseje utilizar os serviços do servidor, possa requisita-lo conhecendo apenas o endereço IP do host servidor.

Se não houvesse a utilização de um número de porta convencionado, a arquitetura TCP/IP deveria possuir um mecanismo de diretório para que um cliente pudesse descobrir o número da porta associado ao servidor.

Os números de porta de **1 a 1023 são números convencionados para serviços (aplicações) atribuídos pela IANA (Internet Assigned Numbers Authority)**. Os números de 1024 a 65535 podem ser atribuídos para outros serviços e são geralmente utilizados pelos programas-cliente de um protocolo. Este conjunto de números tem ainda a atribuição de alguns serviços de forma não oficial, já que os primeiros 1024 números não conseguem comportar todos os protocolos TCP/IP existentes.

A figura 6.22 ilustra a multiplexação/demultiplexação realizada pelo protocolo UDP na camada de transporte:

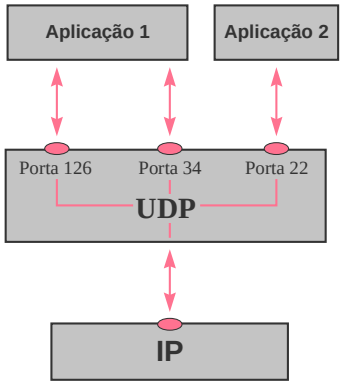


Figura 6.22 - Multiplexação/Demultiplexação realizada na camada de transporte

A mensagem UDP é representada pela figura 6.23. O dado carregado é o pacote de nível de aplicação. UDP acrescenta apenas mais 8 bytes que são a porta de protocolo origem a porta de protocolo destino, o tamanho da mensagem UDP e um checksum para averiguar a correção dos dados do cabeçalho UDP.

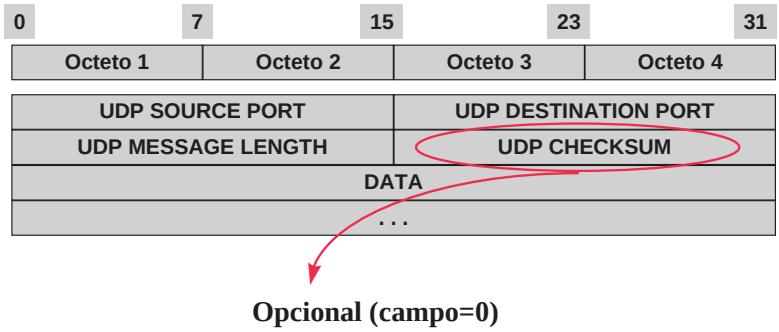


Figura 6.23 - Mensagem UDP

6.5.5.2 - PROTOCOLO TCP

O protocolo TCP trabalha no mesmo nível que o protocolo UDP, mas oferece serviços mais complexos, que incluem controle de erros e de fluxo, serviço com conexão e envio de fluxo de dados. O TCP utiliza o mesmo conceito de porta do UDP. Para o TCP, uma conexão é formada pelo par (Endereço IP de Origem, Porta de Origem) e (Endereço IP de Destino, Porta de Destino).

O protocolo TCP oferece as seguintes características:

1. Controle de Fluxo e Erro fim-a-fim.
2. Serviço confiável de transferência de dados.
3. Comunicação full-duplex fim-a-fim.
4. A aplicação necessita apenas enviar um fluxo de bytes.
5. Desassociação entre quantidade de dados enviados pela aplicação e pela camada TCP.
6. Ordenação de mensagens.
7. Multiplexação de IP, através de várias portas.
8. Opção de envio de dados urgentes.

A conexão TCP é ilustrada na figura 6.24 abaixo.

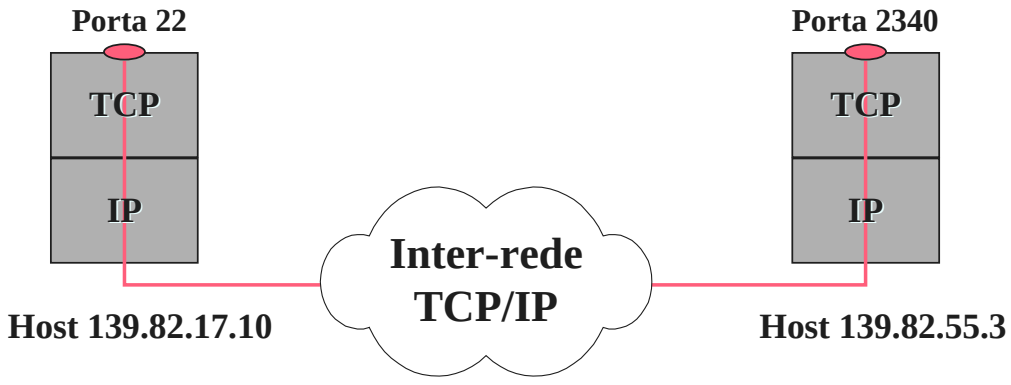


Figura 6.24 – Exemplo de conexão TCP.

Uma conexão TCP é formada por três fases: o estabelecimento de conexão, a troca de dados e a finalização da conexão, conforme ilustrado na figura 6.25.

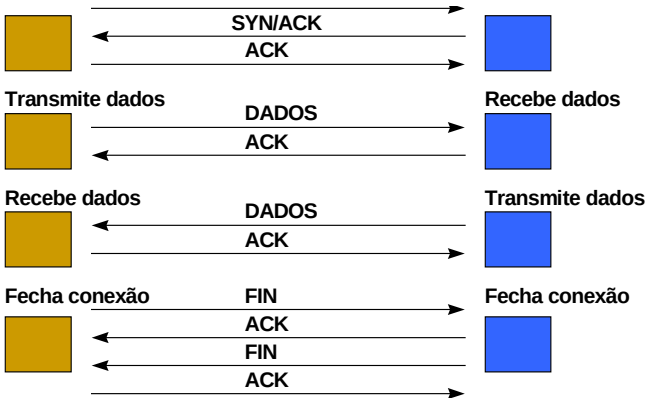


Figura 6.25 – Fases de uma conexão TCP.

O pacote TCP é formado pela mensagem mostrada na figura 6.26. Os campos do pacote são definidos da seguinte forma:

- TCP SOURCE PORT: Porta origem da mensagem

- TCP DESTINATION PORT: Porta destino da mensagem

- SEQUENCE NUMBER: número de sequência dos dados sendo transmitidos face ao conjunto total de dados já transmitidos. Este número indica a posição do primeiro byte de dados sendo transmitido em relação ao total de bytes já transmitidos nesta conexão. O primeiro número de sequência utilizado não é zero ou um, mas começa de um valor aleatório. Logo se um pacote está transmitindo do 1234º byte até o 2000º byte de uma conexão e o SEQUENCE NUMBER inicial utilizado nesta conexão foi 10000, o campo SEQUENCE NUMBER conterá o valor 11234. O sequence number em um sentido da conexão (máquina A para B) é diferente do sequence number do sentido inverso, já que os dados transmitidos por um e outro lado são distintos.

- ACKNOWLEDGE NUMBER: número que significa o reconhecimento dos dados recebidos até então no sentido inverso. O ACK de um sentido é transmitido em *piggy-backing* no outro sentido. O ACK contém o número do próximo byte do fluxo de dados recebido, que a origem deste pacote espera receber da outra máquina. Este valor leva em consideração o número de SEQUENCE NUMBER inicial praticado pela outra máquina. O valor de ACK informa sempre o próximo byte ainda não recebido do conjunto contíguo de bytes recebidos do transmissor.

- CODE BITS: São formados por seis bits, URG, ACK, PSH, RST, SYN e FIN, cuja utilização é mostrada abaixo:

- URG: bit de Urgência: significa que o segmento sendo carregado contém dados urgentes que devem ser lidos com prioridade pela aplicação. A aplicação origem é responsável por acionar este bit e fornecer o valor do URGENT POINTER que indica o fim dos dados urgentes. Um exemplo da utilização desta facilidade é o aborto de uma conexão (por exemplo por Control-C), que faz com que a aplicação destino examine logo o pacote até o fim da área de urgência, descubra que houve um Control-C e termine a conexão.

- ACK: bit de Reconhecimento: indica que o valor do campo de reconhecimento está carregando um reconhecimento válido.

- PSH: bit de PUSH: Este mecanismo que pode ser acionado pela aplicação informa ao TCP origem e destino que a aplicação solicita a transmissão rápida dos dados enviados, mesmo que ela contenha um número baixo de bytes, não preenchendo o tamanho mínimo do buffer de transmissão.

- RST: bit de RESET: Informa o destino que a conexão foi abortada neste sentido pela origem

- SYN: bit de Sincronismo: é o bit que informa os dois primeiros segmentos de estabelecimento da conexão.

- FIN: bit de Terminação: indica que este pacote é um dos pacotes de finalização da conexão

- WINDOW: Este campo informa o tamanho disponível em bytes na janela de recepção da origem deste pacote. Por meio deste valor, o TCP pode realizar um controle adequando de fluxo para evitar a sobrecarga do receptor. Quando este valor é igual a zero, o transmissor não envia dados, esperando receber um pacote com WINDOW maior que zero. O transmissor sempre vai tentar transmitir a quantidade de dados disponíveis na janela de recepção sem aguardar um ACK. Enquanto não for recebido um reconhecimento dos dados transmitidos e o correspondente valor de WINDOW > 0, o transmissor não enviará dados.

- OPTIONS: O campo de opções só possui uma única opção válida que é a negociação do MSS (Maximum Segment Size) que o TCP pode transmitir. O MSS é calculado através do MTU ou através do protocolo ICMP Path MTU Discovery.

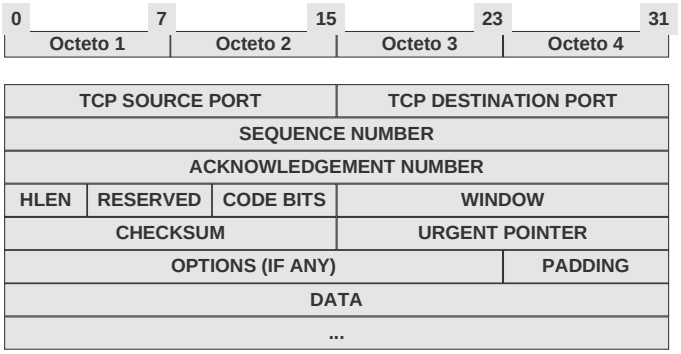


Figura 6.26 – Mensagem TCP.

6.5.6 – PROTOCOLOS DA CAMADA DE APLICAÇÃO.

Os protocolos de aplicação TCP/IP são aqueles que realizam as funções de alto nível e que utilizam os serviços da camada de transporte UDP ou TCP para a comunicação.

Os protocolos de aplicação podem realizar funções diretamente acessíveis pelo usuário como FTP, HTTP, SMTP, POP3, IMAP4, Finger, Telnet, Chat, NFS, TFTP, NNTP e outros. Além disto, podem também realizar funções mais próximas do sistema de comunicação, tais como os protocolos DNS, BOOTP, DHCP, SNMP, BGP4, e outros.

6.5.6.1 – PROTOCOLO DNS

Destacaremos em nosso estudo o protocolo DNS (Domain Name System), que especifica duas partes principais: regras de sintaxe para a definição de domínios e o protocolo utilizado para a consulta de nomes.

O DNS é basicamente uma associação entre endereços IP e nomes. A abordagem inicial para esta associação era a utilização de nomes simples, ou seja, sem hierarquia. Esta abordagem possui limitações intrínsecas quanto a escalabilidade e a manutenção. O sistema de nomes utilizado na Internet tem o objetivo de ser escalável, suportando a definição de nomes únicos para todas as redes e máquinas na Internet e permitindo que a administração seja descentralizada.

A estrutura de nomes na Internet tem o formato de uma árvore invertida onde a raiz não possui nome. Os ramos imediatamante inferiores à raiz são chamados de TLDs (Top-Level Domain Names) e são por exemplo .com, .edu., .org, .gov, .net, .mil, .br, .fr, .us, uk, etc. Os TLDs que não designam países são utilizados nos EUA. Os diversos países utilizam a sua própria designação para as classificações internas. No Brasil, por exemplo, temos os nomes .com .br., .gov.br, .net.br, .org.br e outros.

Cada ramo completo até a raiz como, por exemplo, fepesmig.br, empresa.com.br, nasa.gov, e outros são chamados de domínios. Um domínio é a área administrativa englobando ele próprio e os subdomínios abaixo dele. Por exemplo o domínio .br engloba todos os subdomínios do Brasil. O domínio empresa.com.br tem a responsabilidade por todos os domínios abaixo dele.

A hierarquia de domínios pode ser observada na figura 6.27.

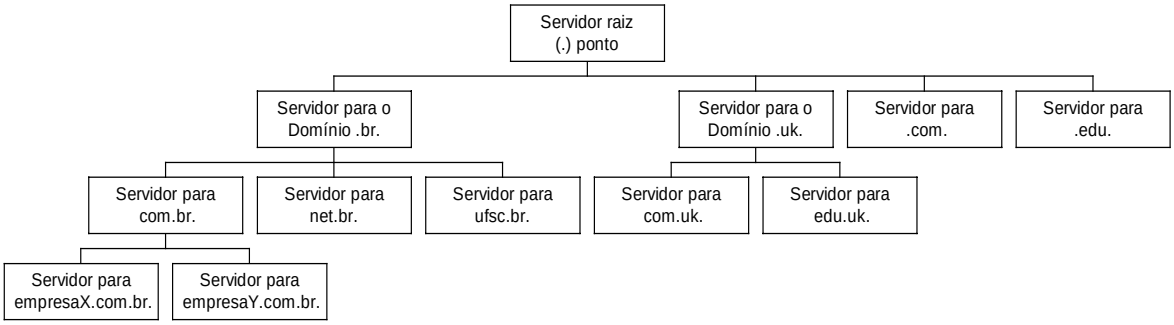


Figura 6.27 - Servidores DNS estruturados hierarquicamente

Os domínios principais genéricos, chamados de GTLDs (Generic Top Level Domain Names) que são .net, .com e .org são administrados pelo Internic (Internet Network Information Center) que também é responsável pela administração do espaço de endereçamento IP. Recentemente foram criados novos nomes de domínio genéricos que serão utilizado a partir de 98. São eles: .firm, .store, .web, .arts, .rec, .infor, .nom.

Os domínios são completamente independentes da estrutura de rede utilizada. Não existe, necessariamente, relacionamento entre eles. O DNS possui uma estrutura inversa para poder representar o endereçamento de rede, ou permitir que seja feita a associação do endereço IP correspondente a um nome. Esta estrutura possui como raiz principal a notação .ARPA e possui como único ramo o .in-addr. Abaixo deste são colocados em ordem os bytes do endereço IP.

6.6 - OUTROS EXEMPLOS DE ARQUITETURAS DE REDES.

Existe atualmente um número muito grande de redes em operação. Algumas são públicas, controladas por concessionárias de serviços de comunicação, outras são redes de pesquisa e outras ainda são redes corporativas ou comerciais. Todas elas apresentam diferenças em relação a sua história, administração, recursos oferecidos, projeto técnico e comunidade de usuários. A história e a administração de uma rede podem variar significativamente, de exemplos onde ela foi cuidadosamente planejada por uma organização até exemplos de redes cujas máquinas foram interconectadas no decorrer dos anos sem qualquer planejamento ou administração central. Os recursos disponíveis podem variar da arbitrária comunicação processo a processo até o correio eletrônico, à transferência de arquivos, ao *login* remoto e à execução remota. Os projetos técnicos podem diferir no tipo de meio de transmissão utilizado, nos algoritmos de roteamento e de denominação empregados, no número e no conteúdo das camadas presentes e nos protocolos usados. Por fim, a comunidade de usuários pode variar dos funcionários de uma empresa até todas as pessoas interessadas no mundo.

Muitos são os exemplos de redes disponíveis no mercado, principalmente para redes locais. Ainda podemos analisar algumas experiências de grandes redes tais como a ARPANET e a NSFNET, precursoras da Internet mundial, assim como das primeiras experiências até a gigabit. Um bom exemplo de rede local bastante popular é a Novel NetWare. Ela foi projetada para ser usada para empresas que estavam fazendo downsizing de mainframe para rede de PCs. Ela utiliza a filosofia cliente/servidor e está baseada numa pilha de protocolos proprietária ilustrada na figura 6.28. Ela é baseada na antiga XNS (Xerox Network System) com várias modificações. Esta arquitetura antecede o RM-OSI e se parece mais com a arquitetura TCP/IP.

As camadas física e de enlace podem ser escolhidas dentre vários padrões industriais. O IPX é um protocolo sem conexão não confiável e é funcionalmente semelhante ao IP, com diferenças no endereçamento, que é de 10 bytes.

O NCP (Network Core Protocol) é um protocolo de transporte orientado a conexão e não está restrito ao transporte de dados do usuário, sendo considerado o coração do Netware. O SPX (Sequence Packet Exchange) oferece apenas o transporte de mensagens. Ainda há a opção do TCP, que também pode ser utilizado. Por exemplo, o sistema de arquivos utiliza o NCP e o Lotus Notes utiliza o SPX.

Figura 6.28 – O modelo de referência da Novel NetWare.