INTERCONEXÃO DE REDES DE COMPUTADORES: INTERDEPENDÊNCIA DOS MÉTODOS DE CONTROLE DE FLUXO, DE CONTROLE DE ROTAS E DE FRAGMENTAÇÃO

Antônio Eugênio Ramos Gadelha

TESE SUBMETIDA AO CORPO DOCENTE DA COORDENAÇÃO DOS PROGRAMAS DE PÓS-GRADUAÇÃO DE ENGENHARIA DA UNIVERSIDADE FEDERAL DO RIO DE JANEIRO COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE MESTRE EM CIÊNCIAS (M.Sc.)

Aprovada por:

Prof. Gerhard Schwarz

Dr. Pierre Jean Lavelle

Prof. Daniel Schwabe

Profa. Sueli Mendes dos Santos

RIO DE JANEIRO, RJ - BRASIL
DEZEMBRO DE 1982

GADELHA, ANTONIO EUGENIO RAMOS

Interconexão de Redes de Computadores: Interdependencia dos métodos de Controle de Fluxo, de Rotas e de Fragmentação (Rio de Janeiro) 1982.

XIII, 290 p. 29,7 cm (COPPE-UFRJ, M.SC), Engenharia de Sistemas, 1982)

Tese - Universidade Federal do Rio de Janeiro, Faculdade de Engenharia.

1. Redes de Computadores, 2. Controle de Fluxo, 3. Controle de Rotas, 4. Fragmentação, 5. Interconexão de Redes, I. COPPE/UFRJ II. Título (série)

Agradecimentos:

Agradeço a meus pais, sem os quais este trabalho não seria possível de ser realizado.

Agradeço ao Professor Gerhard Schwarz pela orientação e, principalmente pela compreensão, dedicação e paciência demonstradas.

Agradeço ao Núcleo de Computação Eletrônica (NCE-UFRJ), nas pessoas de Jayme L. Szwarcfiter e Miguel Aranha Borges (in memorian) pela oportunidade e confiança demonstradas.

Agradeço a COBRA - Computadores e Sistemas Brasileiros S.A. - na pessoa de Eduardo Lessa Peixoto de Azevedo pelo apoio fornecido.

Agradeço, finalmente, a todos que, diretamente ou indiretamente, contribuíram para tornar realidade este trabalho.

Sinopse

O objetivo principal deste trabalho é o de propor uma metodologia de estudo dos problemas causados pela Interconexão de Redes de Computadores.

Esta metodologia propõe que este estudo seja efetuado a partir dos estudos das redes simples de computadores. Para comprovar esta metodologia foi adaptado um modelo matemático, aplicado no caso de redes simples, para o caso de redes interconectadas.

Com o intuito de validar este modelo, são analisados os problemas relacionados aos Controles de Rota e de Fluxo e processo de compatibilização do tamanho dos pacotes. Discute-se a necessidade de que ao se implementar uma estrutura de redes interconectadas, atenção especial deve ser dedicada a esta três componentes conjuntamente, já que são interdependentes.

ABSTRACT

The main goal of this work is the proposal of a study problem methodology caused by the Computer Network Interconnection.

This methodology proposes that this study must be done using the studies of the common computer networks. A mathematical model, that usually was applied to the common networks, was used in the case of the interconnected networks.

The problems related with Routing and Flow controls and with the process of packet size compatibilization were analysed aiming to validade this model. It is discussed the need of having special carefulness to these threee components together, since they are independent, when it is being implemented an interconnected network structure.

RESUMEN

El principal objetivo deste trabajo és proponer una metodologia de estudio de los problemas ocasionados por la Interconeccion de Redes de Ordenadores.

Esta metodologia propone que el estudio relativo a redes interconectadas sea realizado a partir de los estudios de las redes simples de ordenadores. Para comprobar esta metodologia fué adaptado un modelo matemático, aplicado en el caso de redes simples, para el caso de redes interconectadas.

Con la intención de validar este modelo son analisados los problemas relacionados con los Controles de Rota, de Flujo e proceso de compatibilizacion del tama~no de los paquetes. Discute-se la necessidad de que al implantar-se una estructura de redes interconectadas, un cuidado especial deve dedicar-se a estas tres componentes conjuntamente, una vez que son interdependentes.

INDICE GERAL

I - Introdução:

O desenvolvimento de técnicas de interconexão de redes de computadores tem sido motivado pelo desejo de se possibilitar a comunicação entre os, geograficamente dispersos, recursos computacionais que estejam interconectados por uma variedade de tecnologias de redes de computadores. A pesquisa neste campo possui como grandes forças motivadoras:

- o surgimento da tecnologia de redes locais que permite uma melhor relação custo/desempenho na utilização dos recursos da rede;

- a existência de redes que apresentam um determinado tipo de serviço não fornecido pelas outras redes.

Como exemplo da importância das redes locais de computadores podemos citar os seguintes esforços que estão sendo realizados no Rio de Janeiro: a rede local do NCE-UFRJ (Núcleo de Computação Eletrônica da Universidade Federal do Rio de Janeiro), a REDPUC a rede local da Pontificia Universidade Católica e a rede local do CEPEL (Centro de Pesquisas da Eletrobrás). Estas redes devem fornecer os serviços desejados por cada uma das entidades e com a possibilidade de se interconectarem à rede pública da Embratel ou a uma outra rede local, fornecendo uma gama maior de serviços, contribuindo para um maior desenvolvimento na área da Telemática e para uma maior interação entre os diversos orgãos de pesquisa e uma maior disseminação do conhecimento. Estas considerações por si só justificam e validam esta pesquisa, que pretende estabelecer critérios e metodologias que possibilitem a realização deste plano de interconectar as diversas redes existentes no Brasil.

Por causa destes pontos, a adoção de uma estrutura de redes interconectadas nos parece irreversível, podendo ser considerada como um dos pontos principais a ser desenvolvido na Telemática na década de 80.

Uma das grandes dificuldades que surge ao se procurar

estudar a interconexão de redes é pouca disponibilidade de referências deste assunto, talvez, por ele ser recente. Neste trabalho procuramos desenvolver uma metodologia de estudo para as redes interconectadas através do estabelecimento de uma série de analogias com as redes de computadores, permitindo com isto que os estudos e modelos desenvolvidos para o caso de redes simples pudessem ser adaptados e aplicados ao caso de redes interconectadas.

Para validar esta metodologia procurou-se analisar três pontos considerados importantes em um ambiente de INTERCONEXÃO DE REDES que são:

- Controle de Fluxo;

- Controle de Rotas;

- Fragmentação.

Estes pontos são analisados indepentemente, não procurando estabelecer critérios de dependência entre os mesmos. Neste trabalho, procura-se estabelecer as relações de dependência entre estes parâmetros e estudá-las através de um modelo matemático conhecido e aplicado ao caso de redes simples.

Inicialmente, procurou-se estabelecer um conhecimento e uma terminologia comum a respeito das Redes de Computadores, destacando-se os pontos julgados principais e que estão relacionados com os três pontos acima mencionados.

Posteriormente, apresenta-se um resumo qualitativo dos aspectos relacionados à INTERCONEXÃO, procurando estabelecer analogias sempre que possível.

Finalmente, um modelo matemático é proposto, com a intenção de comprovar a validade da metodologia empregada e de se comparar as diversas opções para a estrutura de Redes Interconectadas.

II - Redes de Computadores:

II.1 - Introdução:

As redes atuais de comunicação de dados originaram-se no meio da década de 1960, quando os usuários começaram a utilizar os recursos computacionais remotamente, através da utilização de linhas telefônicas. Para possibilitar estes serviços foram construídas redes primitivas,o que aumentou a eficiência na utilização dos recursos, mas não apresentando uma eficiência análoga no que se relacionava às facilidades de comunicação. Os custos devido a comunicações começaram a crescer exponencialmente, forçando os pesquisadores a desenvolver novas técnicas para aumentar o desempenho das redes.

Um dos métodos desenvolvido foi o do compartilhamento de uma linha de comunicação por vários terminais, por causa do fato da quantidade média de dados transmitidos por um terminal típico ser inferior à capacidade da linha. Entretanto, para haver o compartilhamento efetivo da linha de comunicação foi necessário desenvolverem-se protocolos a fim de solucionar os problemas causados pelo compartilhamento, aumentando, consequentemente, a complexidade do processador central e do planejamento necessário. Uma das consequências deste desenvolvimento não padronizado foi o surgimento de vários tipos de protocolos, dificultando ainda mais a decisão de uma estratégia.

Em paralelo com estes desenvolvimentos surgiu o processador frontal ('front-end') que tem como função o de reduzir a sobrecarga de processamento no computador central pela absorção de algumas funções de controle da rede.

Outros desenvolvimentos resultaram na introdução de multiplexadores e concentradores como um meio de redução dos custos de comunicação. Estes equipamentos diminuem o custo de transmissão dos dados por tirar vantagem da economia de escala

das concessionárias e dos fabricantes de modem, permitindo que vários terminais de baixa velocidade compartilhem um número reduzido de linhas de comunicação, aumentando, em consequência a eficiência na utilização da capacidade das linhas e diminuindo o custo médio por bit transmitido.

A estrutura atual da maior parte das redes de comunicação contém vários níveis de concentração, variando desde as linhas multiponto até esquemas complexos de multiplexação. Estas redes possuem uma variedade enorme de equipamentos, incluindo, por exemplo, terminais, interfaces, modems, multiplexadores, processadores frontais, processadores de mensagem e computadores.

Com o aumento da necessidade de se acessar os diversos computadores e os bancos de dados, novas técnicas tiveram que ser desenvolvidas para facilitar a comunicação entre os computadores.

O primeiro método desenvolvido para esta finalidade foi o transporte de uma fita magnética de um computador para o outro. Um outro meio de se transferir informação entre os computadores surgiu com o desenvolvimento de sistemas de comutação de mensagens que permitiam a ligação dos computadores em linhas de baixa velocidade.

Inicialmente, surgiu o sistema de teleprocessamento clássico do tipo centralizado, que consiste de um processador conectado por linhas telefônicas ou privadas a vários terminais. Na década de 70, esta estrutura evoluiu com a adoção de novas técnicas, como por exemplo: processadores frontais, multiplexadores, unidades satélites de processamento remoto, unidades de controle e terminais. Esta rede, ainda classificada como centralizada, é na verdade um sistema distribuído. Entretanto, atualmente, o termo distribuído, quando utilizado no contexto de redes de computadores, se refere à COMUTAÇÃO POR PACOTES.

A comutação por pacotes combina várias técnicas de

manipulação de dados com a tecnologia atual de computadores a fim de aumentar a eficiência da rede. A comutação de pacotes funciona pela divisão das mensagens a serem transmitidas em segmentos, denominados pacotes. Estes pacotes contem a informação necessária para chegar ao destino e que possibilite a reconstituição das mensagens originais. Estes pacotes podem ser transmitidos de uma forma independente, não havendo necessidade de todos os pacotes seguirem o mesmo caminho.

A idéia da comutação de pacotes surgiu em 1964 no trabalho ' On distributed Communications' preparado por Paul Baran da 'Rand Corporation'. Um trabalho pioneiro desenvolvido nesta área foi o realizado pela ' Advanced Research Projects Agency' (ARPA) do Departamento de Defesa dos Estados Unidos na rede denominada ARPAnet (ver /ROBEL78/).

Uma das características da rede de pacotes é a possibilidade de vários computadores se comunicarem através da utilização de uma linguagem comum, seguindo determinados protocolos. Por exemplo, os nós da rede contêm um protocolo de terminal virtual no qual os diferentes tipos de terminais encontram uma base para se comunicar. Os processadores do sistema permitem a conversão da linguagem do terminal local para a linguagem da rede e vice-versa.

Uma outra característica deste tipo de rede é a possibilidade de se obter altos índices de utilização das linhas de comunicação por causa da capacidade de multiplexação dos comutadores ou nós, que desta forma realizam as mesmas funções de um concentrador.

Estas duas características, aliadas com a possibilidade do direcionamento dos pacotes ser adaptativo permitem um acréscimo na confiabilidade e na disponibilidade, justificando com isto a grande aceitação e evolução deste tipo de tecnologia nos últimos anos.

Nas seções seguintes serão apresentados algumas características relativas às redes de comutação de pacotes,

que serão úteis no desenvolvimento deste trabalho e que possibilitarão uma melhor compreensão do comportamento de uma rede de computadores.

Inicialmente, será apresentado uma classificação de redes de computadores por vários critérios julgados importantes.

O critério de escolha dos pontos analisados deveu-se aos assuntos principais que são os CONTROLES de ROTAS e de FLUXO e por causa destes estudar a estrutura de NOMES e ENDEREÇOS. Como exemplo de comportamento de um protocolo são apresentados vários tipos de protocolo e as aplicações de cada um destes.

II.2 - Classificação das Redes de Computadores:

II.2.1 - quanto à topologia (/SCHWG78/,/SCHWM77/):

As redes podem ser distinguidas quanto à sua topologia da seguinte forma:

- Ponto a ponto:

A mais simples das topologias. Neste caso, temos somente ligados dois pontos, como por exemplo: um terminal e um computador, dois computadores. No sentido restrito de redes de computadores esta é uma topologia muito pouco utilizada, ficando mais como um tipo de ligação entre dois pontos, um computador ao nó da rede (por exemplo), do que uma rede propriamente dita. (Vide fig. II.1.(a)).

- Estrela:

Neste caso, podemos ter vários terminais utilizando-se da mesma linha de comunicação através da adoção de mecanismos que permitam o selecionamento de um determinado terminal ou conjunto de terminais ligados a um ponto comum, o denominado CONCENTRADOR REMOTO (vide fig. II.1.(b)). Convém ressaltar que os terminais conectados aos respectivos concentradores se comunicam diretamente com um único computador.

- Arvore:

Similar a anterior, diferindo somente que neste caso temos concentradores localizados em determinados pontos concentrando outros concentradores. Em outras palavras, nem todos os concentradores estão diretamente conectados ao computador central (vide fig. II.1.(c)). Um bom exemplo para esta estrutura são os COMPUTADORES FRONTAIS ('front-end').

- Anel /CAMB*78/:

Neste caso, cada computador está conectado a um outro constituindo um anel (vide fig. II.1.(d)). Este tipo de topologia é bastante simplificadora de certos pontos, como por exemplo o direcionamento de mensagens, que serão detalhados nas próximas seções.

- Anel com Cordas /ARDEB8Ø/:

Uma rede deste tipo é uma rede estruturada em anel na qual permite-se a cada nó possuir uma ligação adicional, denominada CORDA, com outro nó não consecutivo da rede (vide fig. II.1.(e)).

O número de nós da rede é assumido ser par sendo que os nós são numerados de Ø a n - 1, onde n é o número de nós da rede. Cada nó impar, i (i= 1, 3, ... n - 1), é conectado ao nó (i+w) módulo n. Analogamente cada nó par, j (j= Ø, 2,... n - 2) é conectado ao nó (j-w) módulo n. O item "w" é denominado tamanho da corda, de valor impar e positivo.

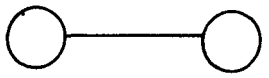
Para um número dado de nós, n, uma variedade de redes deste tipo podem ser obtidas através da utilização de diferentes valores para o tamanho da corda. Observe que a estrutura deste tipo de rede permite o acréscimo de outros nós na configuração original, só que quando isto ocorre o tamanho ótimo do tamanho de corda que irá fornecer o diâmetro mínimo será alterado.

- Barra:

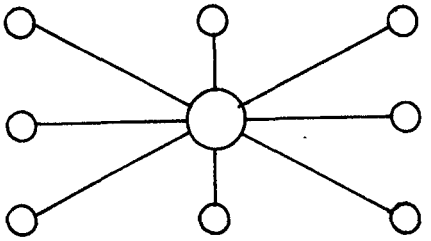
Neste caso, todos os componentes da rede estão conectados através de um meio 'broadcast'. Este meio pode ser um cabo coaxial ou até mesmo o ar (através do rádio). Esta topologia (vide fig. II.1.(f)) apresenta uma série de simplificações no que concerne ao controle de rotas.

- Malhada:

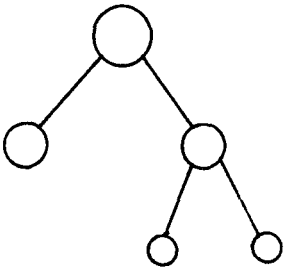
Pode ser considerada como sendo o caso geral de topologia (ver figura II.1(g)).



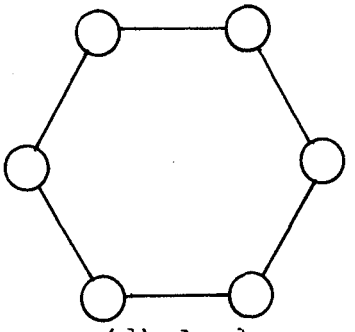
(a) Ponto a ponto



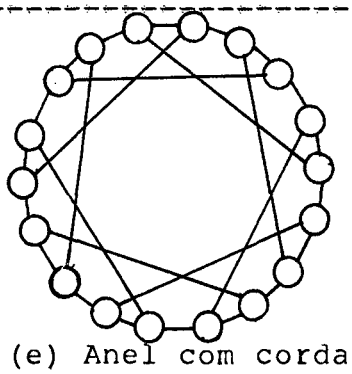
(b) Estrela



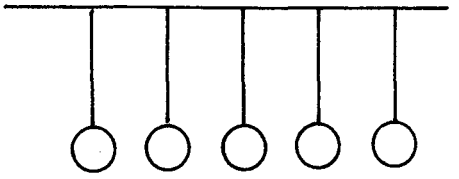
(c) Arvore



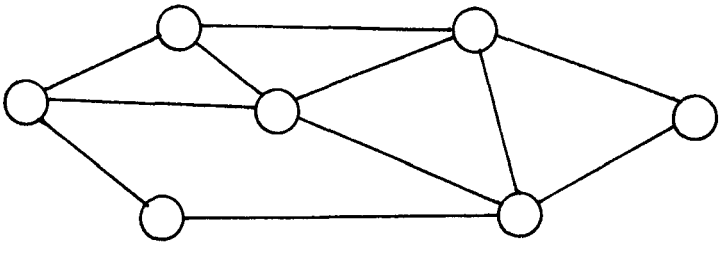
(d) Anel



(e) Anel com cordas



(f) Barra



(g) Malhada

Fig. II.1 - Classificação quanto à topologia

II.2.2 - quanto à estrutura /GIENM79/:

As maneiras pelas quais podemos definir a estrutura de uma rede de computadores são as seguintes:

- multiplexação;
- chaveamento;
- cascateamento;
- envolvimento;
- camadas.

Detalhando estas técnicas temos:

- Multiplexação:

Em qualquer tipo de rede os recursos são compartilhados concorrentemente entre os diversos usuários ou, em termos mais gerais, entre os diversos processos. A multiplexação trata de distribuir os recursos entre os diferentes processos que os necessitam (vide fig. II.2.(a)). No caso mais simples a multiplexacao é local , ou seja, é um processo não distribuído, tratando somente do compartilhamento dos recursos locais baseando-se somente nas informações disponíveis localmente, como por exemplo, a alocação das linhas de transmissão. Além das vantagens econômicas fornecidas pelo compartilhamento a multiplexação permite que os processos se comportem como se fossem independentes.

- Chaveamento:

Quando um recurso ou, de uma forma geral, qualquer entidade lógica está sendo compartilhada entre várias atividades (atraves da multiplexação) esta entidade deve ser capaz de identificar qual das atividades está relacionada com

as suas posteriores ações (vide fig. II.2.(b)), devendo deduzir para onde deverá dirigir ou responder os pedidos (por exemplo, conduzir um pacote para a saida correta em nó de chaveamento de uma rede de pacotes ou enviar uma mensagem para determinado processo). Como já deve ter sido observado o chaveamento implica na interpretação de endereços e rotas que devem estar de alguma forma implícitos na mensagem recebida ou transmitida.

- Cascateamento:

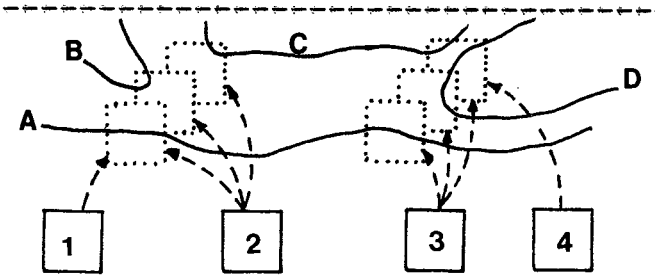
Consiste na formação de uma cadeia linear de entidades (vide fig. II.2.(c)) cuja função será a de servir como geradoras de pedidos ou simplesmente como um meio de propagação dos pedidos de funções . O cascateamento é o único meio pelo qual se pode efetuar a comunicação entre entidades que não estão diretamente conectadas.

- Envolvimento:

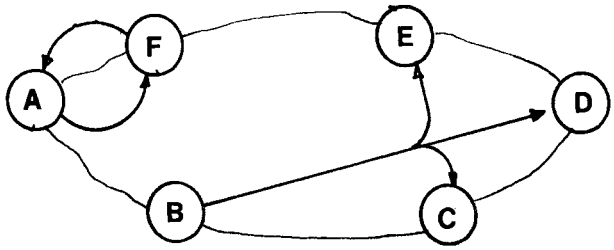
Quando as funções realizadas por um conjunto de entidades não são exatamente aquelas requeridas pelos usuários, uma camada de entidades pode ser acrescentada, envolvendo o conjunto inicial. As entidades desta camada envoltória se comunicam através do conjunto inicial e realizam as funções adicionais ou modificadas. Esta técnica oferece a vantagem de não modificar o conjunto inicial (vide figura II.2.(d)).

- Camadas:

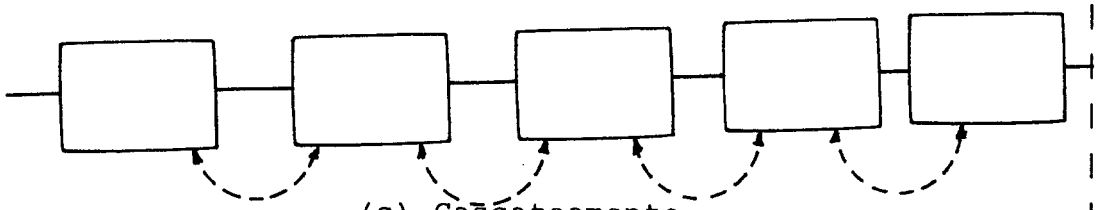
A estrutura de camadas é a técnica que a maioria dos sistemas distribuídos utilizam. Estes sistemas estão logicamente divididos em camadas de tal forma que uma camada intermediária presta serviços para a de nível superior e utiliza o serviço da camada imediatamente inferior, permitindo que sejam identificadas e localizadas em uma única camada determinadas características (vide /ZIMMH8Ø/). A estrutura de camadas está ilustrada na figura II.2.(e).



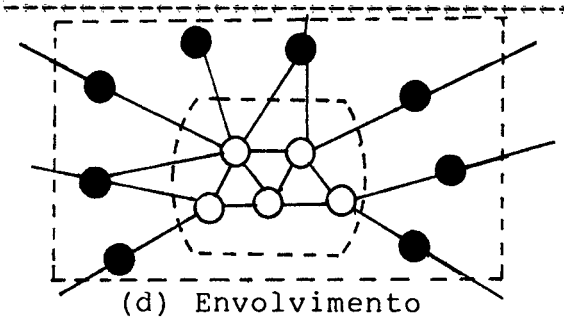
(a) Multiplexação



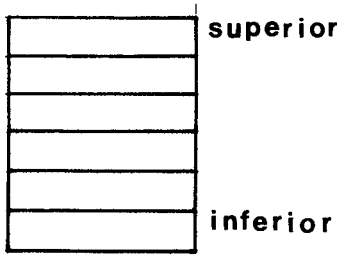
(b) Chaveamento



(c) Cascateamento



(d) Envolvimento



(e) Camadas

Fig. II.2 - Classificação quanto à estrutura

II.2.3 - quanto à forma de funcionamento /KIMBS75/:

As redes neste caso podem ser classificadas de três maneiras:

- Redes de Acesso Remoto ('Remote Access Networks' - RAN);

- Redes Valorizadas ('Value Added Networks' - VAN);

- Redes Orientadas para a Aplicação ('Mission Oriented Networks' - MON).

Detalhando:

- Redes de Acesso Remoto (RAN):

São as redes projetadas para suportar a interação entre um usuário e um determinado computador anfitrião. Os serviços disponíveis ao usuário por este tipo de rede podem ser divididos em duas categorias:

- acesso por terminal: possibilita o acesso pelo usuário de recursos localizados no computador central, além de permitir o funcionamento em tempo compartilhado ('time-sharing');

- entrada remota de trabalhos: possibilita a submissão de trabalhos para o computador central ('remote job entry').

- Redes Valorizadas (VAN):

Contrastando com a anterior na qual existia somente comunicação de um terminal com um computador central este tipo de rede possibilita a comunicação entre os computadores anfitriões. Consegue-se com isto que a potencialidade de utilizaçao da rede seja bastante ampliada, possibilitando a inclusão de novas tarefas, tais como a transferência de

arquivos, a utilização de bancos de dados remotos, o multiprocessamento geograficamente disperso . Podemos observar que a RAN é um caso mais restrito da VAN.

Em redes deste tipo, tanto a sub-rede de comunicação quanto o conjunto de computadores podem pertencer a várias organizações, trazendo como consequência a necessidade de se implementar acordos que possibilitem a interação entre os computadores.

- Redes Orientadas a Aplicação (MON):

Por definição, uma rede deste tipo é uma VAN na qual os computadores, e talvez até a sub-rede de comunicações, estão sôbre o controle de uma única organização. Esta distinção permitirá a alocação e o controle dos recursos e a sua interação na rede possibilitando com isto uma melhoria acentuada na eficiência da rede.

O desenvolvimento das atividades necessárias para se obter uma eficiência máxima irá requerer um conhecimento profundo das relações computação e comunicação.

II.2.4 - quanto ao método de comutação:

As redes podem ser classificadas de acôrdo com o método de comutação adotado em:

- comutação por circuitos ('Circuit switching');

- comutação por mensagens ('Message switching');

- comutação por pacotes ('Packet switching');

- comutação híbrida.

- Comutação por circuitos /MCQUJ78b/, /SCHWG78/:

Uma rede deste tipo fornece serviços pela alocação de um caminho físico dedicado entre dois usuários de comunicação. O circuito completo é alocado através de uma mensagem especial de sinalização. Esta mensagem passa por todo o caminho através da rede, retornando um sinal que irá informar ao nó origem que a transmissão de dados pode ser iniciada. Esta alocação do caminho a ser percorrido é da ordem de segundos (vide fig. II.3(a)) , sendo que o caminho permanecerá alocado para a transferência de informação até que seja liberado. Esta é a técnica utilizada pelos serviços telefônicos.

Este tipo de comutação aplica-se aos usuários que necessitam se comunicar com pouca frequência por um longo período de tempo e possuem equipamentos idênticos não necessitando por causa disto de uma compatibilização de código ou de velocidade.

Este tipo de comutação apresenta como VANTAGENS:

- o atraso é devido somente a propagação do sinal;
- a mensagem chega ao destino na mesma ordem que foi enviada;
- nenhuma identificação ou endereçamento dos dados é necessária.

E como DESVANTAGENS:

- o canal fica ocupado, mesmo se não estiver ocorrendo transmissão de dados;
- demora no estabelecimento do circuito.

- Comutação por mensagens:

Em uma rede deste tipo somente um canal é utilizado de

cada vez para uma dada transmissão. A mensagem é uma unidade lógica de dados que inicialmente é dirigida do nó origem para o próximo nó no caminho. Cada nó seguinte deste caminho armazena a mensagem enviando-a para o proximo nó. Este processo irá se repetir de uma maneira armazena e envia, causando com isto um atraso devido ao enfileiramento em cada nó quando o canal selecionado estiver ocupado (vide fig. II.3.(b)). Este sistema foi desenvolvido para se otimizar a utilização das linhas de comunicação além de se retirar do usuário a responsabilidade do estabelecimento da ligação.

Apresenta como VANTAGENS:

- boa utilização dos canais;

- o meio de comunicação é transparente para o usuário.

E como DESVANTAGEM apresenta grandes tempos de tráfego, geralmente, da ordem de minutos.

- Comutação por pacotes:

Similar a anterior, exceto que o armazenamento secundário não é utilizado na rede. As mensagens são divididas em unidades menores, denominadas PACOTES, que são direcionados independentemente em uma forma armazena-e-envia ('store-and-forward') através da rede. Com isto, torna-se possível que vários pacotes da mesma mensagem possam estar trafegando simultaneamente. Isto constitui uma das principais vantagens da comutação por pacotes. Este método de comutação oferece uma tecnologia de comutação mais dinâmica pelo fato de utilizar efetivamente o canal. Garante-se com este tipo de rede uma resposta mais rápida, da ordem de frações de segundos. (vide fig. II.3.(c)).

Este tipo de comutação apresenta as seguintes VANTAGENS:

- uso efetivo do canal;

- tempo de resposta pequeno para as transações interativas;

- proteção contra erro;

- conversões de código, velocidade e protocolos.

E como DESVANTAGEM a ineficiência para determinadas aplicações, como por exemplo:

- transferência de arquivos;

- tráfego de mensagens em tempo real;

- suporte de terminais assíncronos.

- Comutação Híbrida:

O PACUIT, método de comutação, híbrido dos métodos de comutação por pacotes e circuitos (PACket-cirCUIT) foi projetado para fornecer as características de tempo de resposta das transações interativas da comutação por pacotes com a transparência de dados da comutação de circuitos.

Esta necessidade surgiu de estudos da eficiência da comutação por pacotes que mostraram que esta, embora forneça uma utilização eficiente do canal, requer um conjunto de técnicas sofisticadas de controle de fluxo, além das limitações já expostas.

A estrutura básica de uma rede deste tipo é uma estrutura de multiplexação por tempo que permite a utilização de vários circuitos em um mesmo canal. Uma ligação de capacidade conhecida é estabelecida pela descoberta de um caminho com capacidade extra maior do que a desejada e pela reserva deste caminho nos nós ao longo do percurso.

A maneira mais óbvia de se implementar a comutação por pacotes em uma rede TDM ('Time Division Multiplexing' -

Multiplexação por Divisão de Tempo) é a de derivar circuitos permanentes de largura de banda fixa entre alguns dos nós estabelecendo um protocolo de pacotes entre estes nós. Desta forma obtemos uma rede de pacotes que é uma subrede da rede TDM original.

O fluxo de dados em uma rede deste tipo é feito na base de pacotes. Cada pacote multiplexa vários usuários, isto é, cada pacote contém vários campos, cada um dos quais corresponde a um determinado sub-canal.

Os pacotes são construídos no nó de origem a intervalos regulares (tipicamente, 100 mseg.). Os dados provenientes do usuário são buferizados até que a próxima oportunidade de construção de um pacote ocorra. Neste instante, o pacote é montado e destinado para a fila de saída. Os dados do usuário são transmitidos pelos canais sem esperar a completa reconstituição da mensagem. Para maiores detalhes a respeito do PACUIT recomenda-se a leitura das seguintes referências: /SMETJ76/, /GERLM78/ e /GERML78b/.

Este tipo de rede apresenta como VANTAGENS:

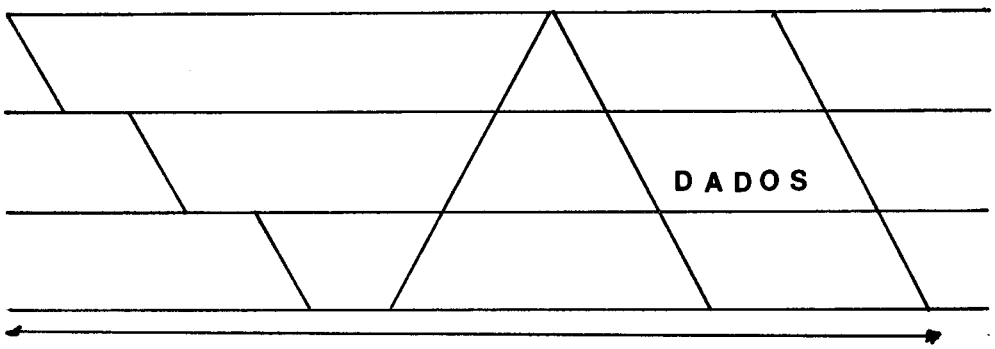
- não existe a necessidade de checagem de erros ou armazenamento dos pacotes nos nós intermediários;

- as mensagens são confirmadas em uma base fim a fim.

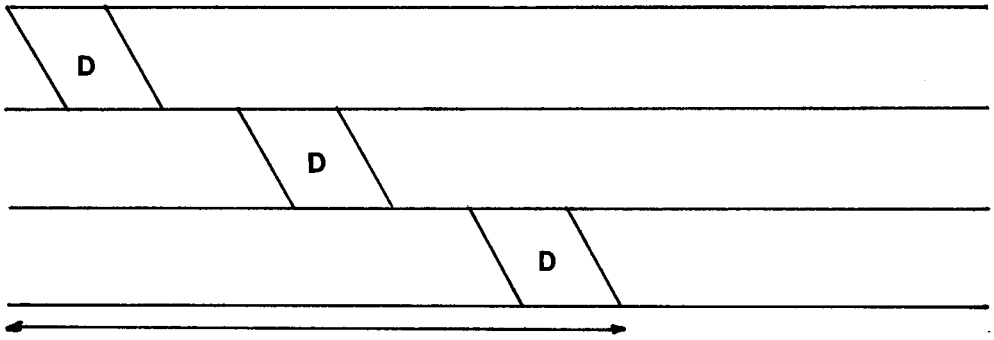
Como DESVANTAGEM, pode-se citar a dificuldade de se estabeler um direcionamento dinâmico de mensagens.

Apenas como referência deve-se mencionar um outro tipo de comutação híbrida que é denominada 'VIRTUAL CUT-THROUGH'. Este sistema de comutação é similar à comutação de mensagens, com a diferença de que quando uma mensagem chega a um nó intermediário e o canal de saída selecionado se encontrar disponível (após ter sido recebido completamente o cabeçalho da mensagem), esta mensagem é imediatemente transmitida para o nó seguinte, antes mesmo de ter sido completamente recebida.

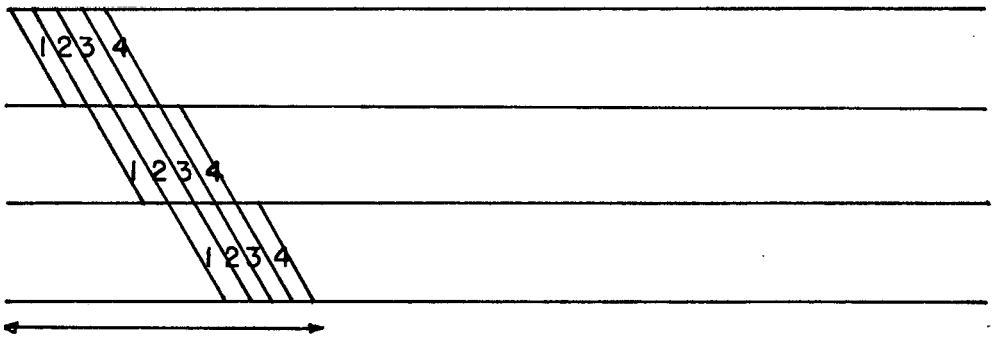
No caso do canal se encontrar bloqueado a mensagem é armazenada no nó intermediário para uma posterior transmissão. Para maiores detalhes a respeito deste tipo de comutação, aconselha-se a leitura de /KERMP79/ e /KERMP80/.



(a) Atraso da Comutação de Circuitos



(b) Atraso da Comutação de Mensagens



(c) Atraso da Comutação de Pacotes

Fig. II.3 - Métodos de Comutação

II.2.5 - quanto ao tipo de interface:

Uma interface entre um computador anfitrião e uma rede do tipo COMUTACAO POR PACOTES pode ser classificada da seguinte forma:

- datagrama;
- circuito virtual;
- emuladora de terminal.

Detalhando temos:

- Datagrama:

A característica que distingue o pacote transmitido pelo anfitrião neste caso é o fato dele ser auto-suficiente, isto é, possui a informação de controle para a rede e o endereço completo do destinatário desejado. A rede manipula cada datagrama ou pacote independentemente de tal forma que este seja entregue em um tempo mínimo mas sem garantir a duplicação, perda ou o sequenciamento relativo, isto é, a ordem original pela qual os pacotes foram transmitidos. Logo, o anfitrião receptor será responsável pelas seguintes tarefas:

- identificação da origem do datagrama;
- detecção e recuperação dos datagramas perdidos;
- pela ordenação dos datagramas visando a recomposição da mensagem original.

- Circuito Virtual:

Com uma interface deste tipo, o anfitrião observa um fluxo de dados mais organizado. Como o nome sugere, a rede

parece fornecer um circuito ponto a ponto dedicado entre os computadores anfitriões origem e destino. Ao invés de tratar cada bloco de dados que está sendo transmitido de uma maneira isolada, a rede assume que a comunicação entre os dois pontos é caracterizada pelo sequenciamento destas transmissões. Logo, um circuito é mantido pela rede através de uma associação entre os nós origem e destino.

Com o datagrama a rede é estritamente um meio de transmissão, enquanto que com a interface do tipo circuito virtual a rede também recupera os dados que foram perdidos , elimina os dados duplicados, ordenando os dados que porventura cheguem fora de sequência.

Um anfitrião pode possuir mais de um circuito virtual estabelecido em um determinado instante pela associação de um número de canal-lógico a cada destino , utilizando-o para identificar os dados trocados. Em oposição ao datagrama o pacote transmitido só necessita conter como informação de endereçamento somente o número do canal lógico ao invés de toda a informação de endereçamento.

- Emuladora de Terminal:

Este tipo de interface é a extensão lógica da idéia do circuito virtual, na qual a rede assume toda a responsabilidade do anfitrião, tais como a monitoração do canal lógico e o controle do fluxo de dados. O anfitrião meramente envia e recebe um fluxo serial de caracteres, como se fôsse um simples terminal com teclado e impressora. Por isto mesmo, esta mesma interface pode ser utilizada para terminais não inteligentes: surgindo daí a denominação emulação de terminais. O computador anfitrião aparece para a rede - analogamente a rede aparece para o computador - como um simples terminal.

A manutenção de várias interfaces deste tipo simultaneamente é análoga a manutenção de vários circuitos virtuais. Entretanto, uma diferença importante é que com a

interface deste tipo cada circuito virtual é dividido pela rede em canais de acesso fisicamente separados.

Por causa da rede emular terminais para os quais o anfitrião já possui suporte de 'software', o anfitrião pode rápida e facilmente acessar à rede. Em comparação com uma interface circuito virtual a interface deste tipo é mais cara e menos eficiente, mas podendo ser atrativa no contexto comercial.

Como já se deve ter percebido, uma interface deste tipo não chega a ser considerada um tipo predominante em uma rede de computadores pois necessita que a rede possua um outro tipo de funcionamento, isto é, seja do tipo datagrama ou circuito virtual.

II.3 - Títulos, Endereços e Rotas:

II.3.1 - Introdução:

Apesar de algumas referências a respeito deste assunto tratarem como sendo uma única entidade, TÍTULOS, ENDEREÇOS e ROTAS são entidades distintas, embora, principalmente, as duas primeiras estejam bastante relacionadas. Estes termos podem ser definidos a partir de seus valores intrínsecos, isto é, a partir do que queremos dizer quando nos referimos a eles, da seguinte forma:

- o NOME de um recurso identifica o que procuramos;

- o ENDEREÇO indica onde ele se localiza;

- a ROTA indica o caminho que deve ser percorrido para que se atinja o recurso desejado (/SHOCJ78/,/CERFV78/).

Em uma definição mais detalhada /SHOCJ78/:

O NOME é um símbolo - geralmente legível - que identifica algum recurso ou conjunto de recursos. Estes símbolos não necessitam ter significado para todos os usuários e nem pertencer a um espaço uniforme de nomes. Deverá existir algum tipo de mecanismo disponível ao usuario que transforme o nome desejado em um endereço, isto é, onde está o recurso desejado. Logo, o nome (o que queremos) não necessita ter junto a si o endereço (onde ele está) até que esta transformação ocorra. Com isto, o endereço (ou endereços) associado(s) com um determinado nome pode ser alterado com o tempo sem que isto implique em grandes modificações.

O ENDEREÇO é uma estrutura de dados cujo formato deve ser reconhecido por todos os elementos do domínio, definindo fundamentalmente o objeto endereçado. Podemos destacar como características do endereço o seguinte:

- o endereço deve ter significado para todos no domínio considerado;

- se um nome puder produzir diferentes endereços para um recurso em particular, alguma forma de informação a priori deve ser fornecida para que se possa chegar ao endereço desejado;

- no momento da comunicação com um determinado endereço deve existir algum tipo de mecanismo que transforme este endereço em uma rota apropriada;

- logo, o endereço (onde está) não necessita estar ligado à rota (como chegar lá) até que esta transformação ocorra, pois a escolha da rota apropriada pode ser alterada com o tempo.

A ROTA é a informação específica necessária para conduzir uma peça de informaçao para o endereço especificado.

Observa-se que um nome pode ser utilizado para encontrar-se um endereço e este,por sua vez, pode ser utilizado para encontrar-se uma rota. Existe uma certa similaridade desta estrutura e os mecanismos utilizados em outras áreas da computação:

- a compilação e a carga de um programa, onde os símbolos são mapeados (transformados) do espaço de nomes do programa em sucessivos espaços de endereçamento;

- ao executar-se um programa quando um valor é atribuido a uma variável;

- memória virtual, que liga temporariamente um endereço real a um virtual.

Cabe aqui uma observaçao: como já se deve ter percebido os têrmos TITULO e NOME são utilizados de uma

forma equivalente. A denominação TÍTULO, adotada pela ISO no seu trabalho ' OPEN SYSTEMS INTERCONNECTION' /ZIMMH8Ø/, possui um significado mais geral do que NOME. Usaremos neste trabalho de uma maneira livre os dois têrmos, embora deva-se preferir TÍTULO.

II.3.2 - Título:

Os TÍTULOS são utilizados em sistemas de computação para identificar os seus recursos. Os TÍTULOS podem ser de tamanho variável ou fixo, de acôrdo com a convenção adotada pelo sistema para a sua formação, convenção esta que varia de sistema para sistema.

No nosso caso, de redes de computadores, esta falta de uniformidade na geração dos títulos é problemática. Uma forma de resolvê-la é a possibilidade de se uniformizar as convenções adotadas através da proposição de uma convenção única que será válida para todos os sistemas componentes da rede.

Analisando-se esta sugestão verificamos que ela é, na prática, impossível de ser implementada devido ao trabalho que isto irá causar dado que a convenção de nomes está normalmente entranhada no projeto do sistema operacional, tornando impraticável qualquer modificação.

Verifica-se também que a adoção de um esquema único de nomes não se faz necessário pois os nomes dos recursos só necessitam ter significado para o sistema onde estes recursos se encontram. Agora, o problema que surge é o seguinte:

Como poderemos então identificar os recursos dentro da rede?, ou formulando de outra maneira: Como poderemos obter um nome, que identificará o recurso desejado, que seja único no universo considerado?

Para melhor podermos responder a esta pergunta, precisaremos das seguintes definições:

- TÍTULO LOCAL: é o título adotado no sistema local;

- TÍTULO COMUM: é o título adotado no universo considerado, ou seja pela rede.

Os métodos adotados para resolver este problema são:

- Concatenação hierárquica;

- Alocação;

- Mapeamento;

II.3.2.a - Concatenação hierárquica /POUZL78/:

Imaginemos que cada sistema possua um conjunto de títulos locais Lj. A cada um destes conjuntos é atribuído um único título comum Ci.

Estes títulos comuns devem ser únicos no universo considerado não podendo referenciar mais de um conjunto de títulos locais para se evitar ambiguidades, embora um mesmo conjunto de títulos locais possa ser referenciado por mais de um título comum.

Visto isto, o espaço de títulos da rede de computadores será obtido pela concatenação dos títulos locais com o título comum, isto é, o universo de títulos a ser considerado será <Ci x Lj>.

Exemplo:

- Títulos locais no sistema AZUL:

ARQUIVO.DO.JOAO
CARTAS.PARA.MARIA

← Títulos locais no sistema BRANCO:

ABCDEFGHIJ/ZYXWVUTSRQ
ANEURAGA

← Títulos locais no sistema VERDE:

534Ø9
4321Ø

Os títulos comuns seriam:

AZUL ARQUIVO.DO.JOAO
AZUL CARTAS.PARA.MARIA
BRANCO ABCDEFGHIJ/ZYXWVUTSRQ
BRANCO ANEURAGA
VERDE 534Ø9
VERDE 4321Ø

Os nomes AZUL, BRANCO, VERDE são os nomes comuns que identificam os conjuntos de nomes locais pertinentes a cada um dos sistemas.

O esquema acima é similar ao adotado pelo DDD (Discagem Direta à Distância) ou pelo DDI (Discagem Direta Internacional) aonde o número telefônico de outro sistema (no caso internacional, país) é obtido pela concatenação do número do país com o número atribuído à região do país e com o número local do telefone.

II.3.2.b - Alocação:

São alocados permanentemente títulos comuns sòmente a

poucos recursos (processos), como por exemplo, ao processo que autoriza o acesso do usuário remoto ao sistema desejado.

Um outro conjunto de títulos comuns é alocado para cada sistema local para que se faça uma associação dinâmica aos processos locais. Pelo menos um processo de cada sistema deve ter um nome conhecido e a responsabilidade de atribuir dinamicamente os outros títulos locais destinados ao sistema local aos processos desejados.

Por exemplo:

Suponhamos que os títulos comuns são números inteiros de 1 a 9999. Para o uso do sistema "A" foram reservados os títulos comuns 6100 a 6199 e para o sistema "B" os títulos comuns 4300 a 4399. No sistema "B" o processo de controle do acesso a rede tem como título comum o número 4301 e no sistema "A" existe um processo cujo título comum é 6192 tentando acessar um recurso no sistema "B" cujo título local neste sistema é ZOOM (fig. II.4)

O processo que deve ser seguido para que isto se torne possivel é o seguinte:

O processo 6192 deve enviar um pedido para o processo de controle de acesso a rede no sistema "B" (4301) a fim de tornar possível o acesso ao recurso "ZOOM".

O processo 4301 executará então as seguintes funções:

- colocar disponível ao processo requisitante o recurso ZOOM no sistema "B";

- alocar um título comum não utilizado ao recurso ZOOM (no caso, 4327);

- responder ao processo 6192 (o requisitante) que o recurso desejado esta' disponível e associado ao título comum 4327.

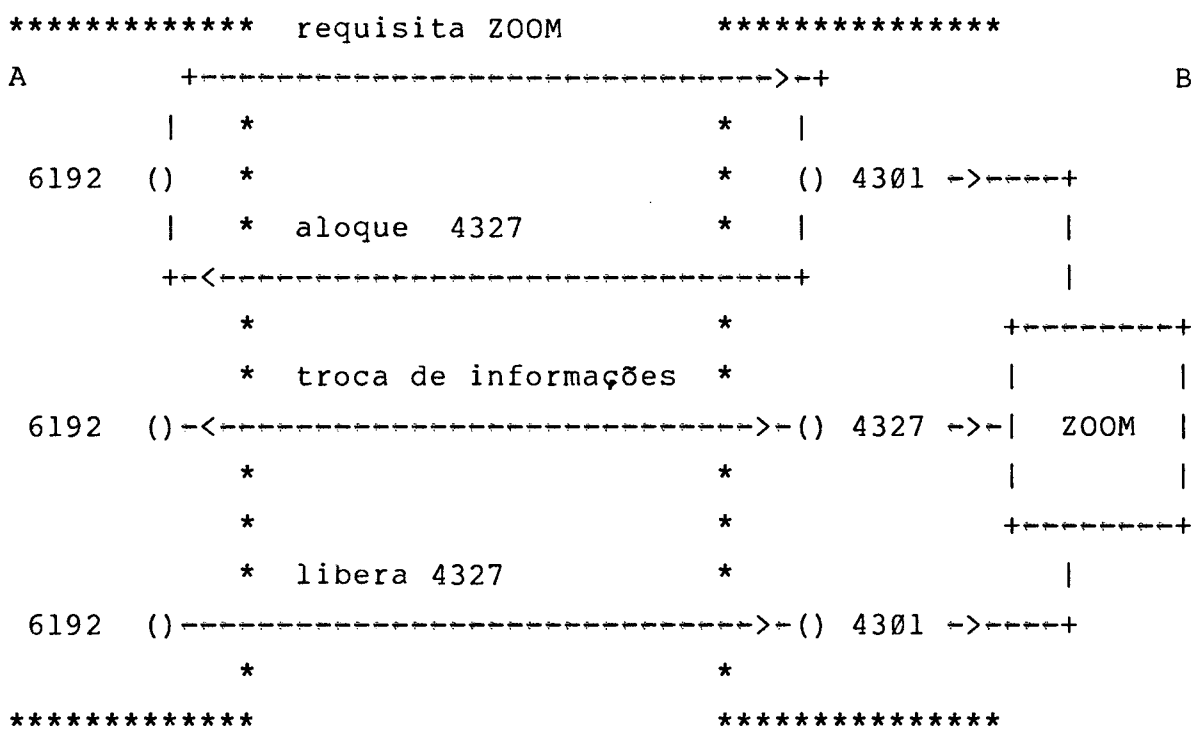


Fig. II.4- Exemplo de alocação de Nomes

Ao receber esta informação o processo 6192 estará apto a realizar as tarefas desejadas com o recurso ZOOM. Ao terminar estas tarefas o processo 6192 deverá enviar ao processo de controle de acesso do sistema "B", no caso, 4301 que está liberando o título comum 4327, ou seja o recurso ZOOM.

Esta estratégia está intimamente relacionada ao protocolo de conexão inicial da ARPANET associada com o protocolo de controle da rede que constituem a camada de transporte do protocolo.

II.3.2.c - Mapeamento:

Uma alternativa à concatenação é criar-se um conjunto de títulos comuns Ci atribuindo-os estàticamente aos recursos que podem ser acessados pela rede. Os nomes comuns associados são

então mapeados por cada sistema local no respectivo título local (vide figura II.5) Esta é a estratégia adotada pela rede CYCLADES.

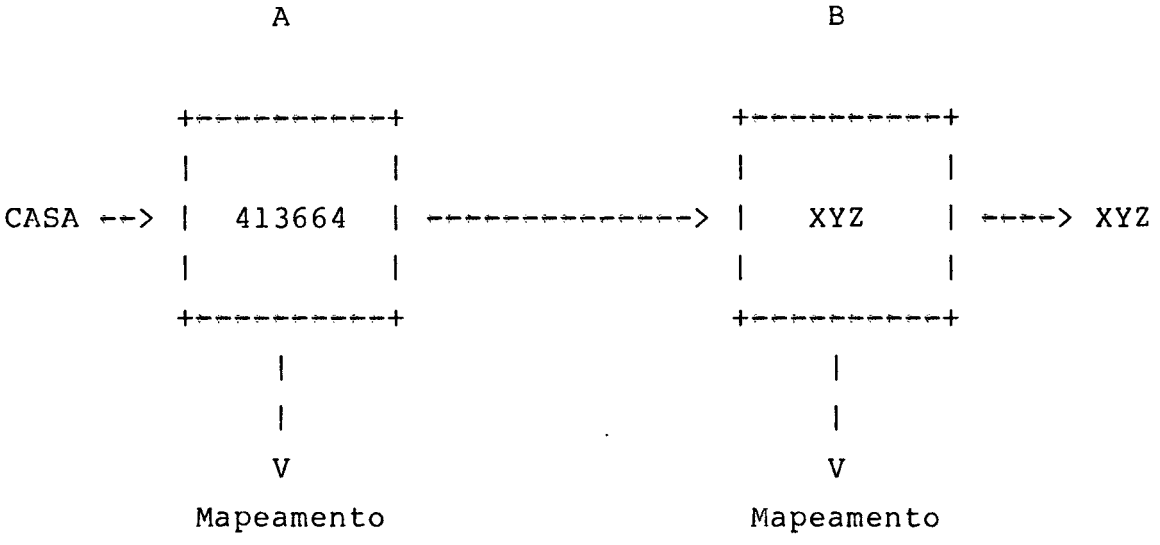


Fig. II.5 - Mapeamento

Existe um processo no sistema "A" que deseja alocar o recurso de título CASA no sistema "B". Este pedido, alocar o recurso CASA, é mapeado para se alocar o recurso de título comum 413664. Ao receber este pedido o processo de controle do acesso ao sistema "B" realiza o mapeamento transformando o título comum para o título local XYZ sendo então efetivada a alocação.

II.3.2.d - Comparação entre os métodos:

- Concatenação hierárquica:

Aparentemente o método mais simples por que o título comum é gerado a partir do nome do sistema e dos títulos locais. Porém, na prática, isto só se torna possível quando os

títulos locais são homogêneos. No caso de não serem, os títulos comuns possuem diferentes formatos, tornando o protocolo de tratamento adotado grande e ineficiente, por causa da necessidade deste de conhecer todos os formatos possíveis de nomes da rede. No caso da inclusão de mais um conjunto de nomes locais, ou seja de mais um sistema, poderá ocorrer a necessidade de se alterar os protocolos de controle de acesso a rede.

- Alocação:

  - Vantagens:

    - facilidade de implementação, pois a maioria dos sistemas operacionais existentes foram projetados para possuir entidades centralizadoras das funções críticas do Sistema Operacional;

    - facilidade na sua utilização, tornando transparente ao usuário a existência da rede;

    - ao se utilizar um conjunto menor de títulos comuns, sòmente para os processos ativos, diminui-se a sobrecarga causada pelo acesso à rede.

  - Desvantagens:

    - os recursos são rigidamente associados aos sistemas específicos, criando com isto uma verdadeira rede de recursos ao invés de uma rede de computadores;

    - mais complexo de ser implementado, por requerer um gerenciamento das mudanças de associações entre os títulos comuns e locais.

- Mapeamento:

  - Vantagens:

    - fornece um espaço de nomes homogêneos para acesso a qualquer recurso da rede

    - método mais flexível porque:

      - os usuários podem escolher os títulos locais de acordo com o seu simbolismo;

      - vários títulos locais podem ser mapeados em um único título comum;

      - como os títulos locais não precisam ser conhecidos remotamente, não irão ocorrer ambiguidades quando títulos locais idênticos forem utilizados pelos diversos sistemas.

  - Desvantagens:

    - sobrecarga causada na pesquisa da tabela de títulos comuns.

II.3.3 - ENDEREÇOS /MCQUJ78/:

II.3.3.a - Introdução:

A intenção desta seção é a de identificar os diversos tipos de endereçamento que podem ser utilizados para que se possa oferecer uma interface da rede com os usuários e uma operação eficiente, em especial, para redes de COMUTAÇÃO DE PACOTES. Será feita uma distinção entre o tipo de endereçamento, como o usuário identifica a mensagem, e a

implementação do endereçamento, como a rede processa a mensagem, por que a primeira é a interface entre o usuário e a rede e a outra é o protocolo da rede.

Para prosseguirmos devemos conceituar o que seja endereço físico. ENDEREÇO FISICO é o número do nó (ECD) ou o número da porta, por onde é feita a comunicação entre o assinante (ETD) e o nó (ECD); logo, é a informação utilizada pela rede para localizar o destinatário.O endereço é especificado como parte do cabeçalho que é acrescentado pelo ETD origem. No modo de funcionamento básico da maioria das redes atuais, o assinante apresenta a mensagem à rede com o endereço correspondente à localização física do assinante destinatário (vide Fig. II.6.(a)) Embora esta forma seja simples e efetiva, ela também é restritiva, porque exige que os assinantes tenham conhecimento das localizações físicas dos outros assinantes, não assimilando novos conceitos, tais como:

- atribuição de múltiplas conexões a um mesmo assinante;

- envio de mensagens para mais de um assinante.

Mc Quillan propôs que para solucionar os problemas de endereçamentos fôssem adotados três modos de endereçamento:

- ENDEREÇAMENTO LÓGICO: no qual atribui-se de uma forma permanente endereços lógicos que denotarão um ou mais endereços físicos (vide Fig. II.6(b)). O remetente não necessita conhecer a localização física do destinatário, possibilitando que esta seja modificada sem a alteração do endereço lógico correspondente. Desde que um endereço lógico pode referenciar vários endereços físicos, os assinantes poderão se conectar a rede por LIGAÇOES MÚLTIPLAS ('multiple homing') aumentando com isto a sua disponibilidade e capacidade (vide fig. II.6.(c));

- ENDEREÇAMENTO POR DIFUSAO ('BROADCAST'): no qual a mensagem e endereçada para todos os outros nós ou assinantes (Fig. II.7.(a)). Se implementado de uma forma

eficiente, poderá reduzir significantemente o tráfego na rede quando comparado com o envio de mensagens endereçadas separadamente, uma para cada assinante;

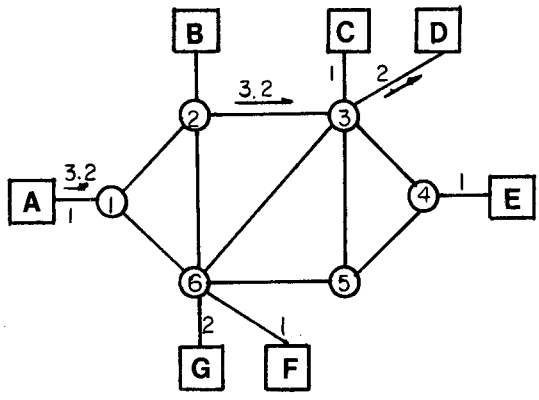
- ENDEREÇAMENTO DE GRUPO (Fig. II.7.(b)) e ENDEREÇAMENTO MULTI-DESTINO (Fig. II.7.(c)) nos quais as mensagens contêm o nome de uma lista de endereços ou a própria lista. Aumenta a performance da rede, principalmente nas aplicaçoes de mala eletrônica, conferências, etc.

Passaremos agora a descrever as consideraçôes envolvidas no projeto e implementação dos três modos apresentados.

II.3.3.b - Endereçamento lógico:

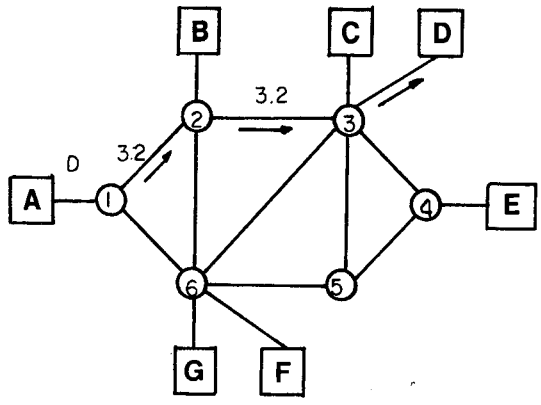
Uma estrutura geral de endereçamento lógico pode traduzir vários endereços físicos em um simples endereço lógico e um endereço físico em vários lógicos. Em uma rede do tipo CIRCUITO VIRTUAL o endereço lógico é traduzido pelo nó origem uma única vez para cada conexão, permitindo que todas as mensagens de um determinado circuito virtual fluam até o endereço físico desejado, no caso o destino. Em uma rede do tipo DATAGRAMA, por outro lado, os endereços das mensagens são traduzidos um de cada vez , as mensagens fluindo para qualquer endereço físico. O nó origem pode realizar a tradução (modificando o campo de endereçamento do cabeçalho do pacote), ou poderá deixar que esta ocorra em cada nó intermediário (sem modificar o campo de endereço lógico do cabeçalho do pacote) .

A envia uma mensagem
para D, endereçada 3.2
(nó 3, canal 2)



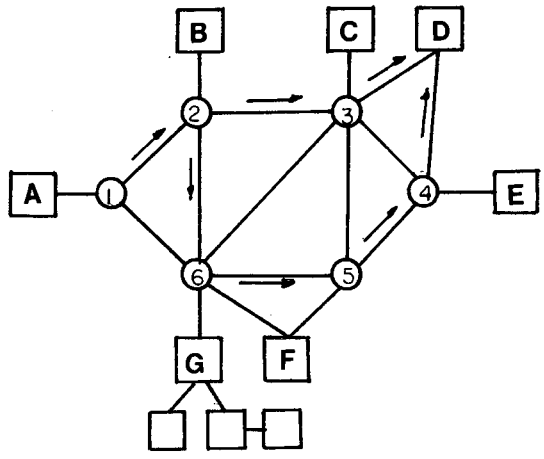
(a) Endereçamento Físico

A envia uma mensagem
para D, endereçada "D"



(b) Endereçamento Lógico

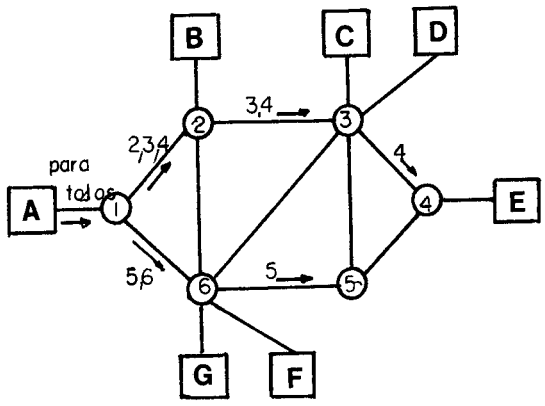
Os assinantes D, E e F
são 'Multiple homed'.
Indicado o tráfego
possível de A para D.
D tem vários endereços
físicos e um lógico.
G,G1,G2,G3 tem um
endereço físico,
vários lógicos



(c) Ligações Múltiplas

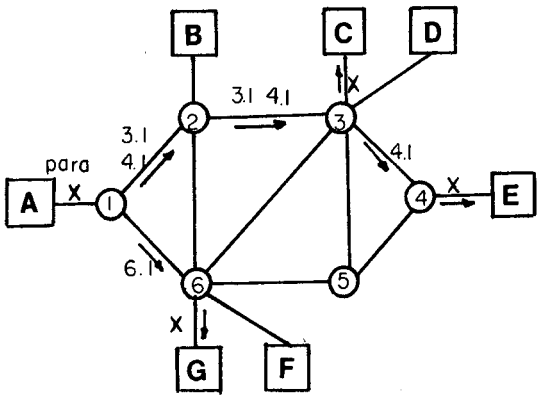
II.6 - Tipos de Endereçamento /MCQUJ78/

A envia uma mensagem para todos os nós

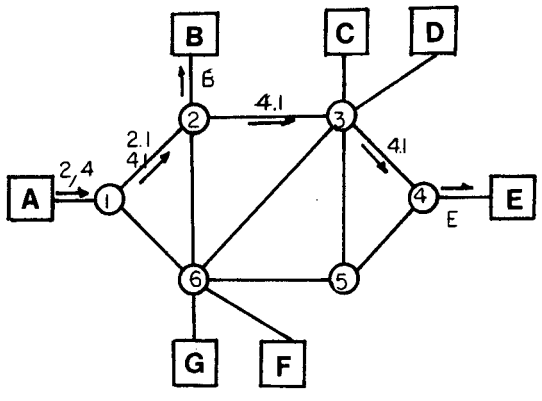


(a) Endereçamento 'broadcast'

O assinante A envia uma mensagem para o grupo X: (C,E,F)



(b) Endereçamento de Grupo



(c) Endereçamento Multi-destino

II.7 - Tipos de Endereçamento (cont.) /MCQUJ78/

O endereçamento lógico também permite o 'MULTIPLE HOMING' dos assinantes para as portas da rede e o uso de uma porta para a rede por vários assinantes distintos. Para que isto ocorra se torna necessário que o assinante origem se identifique por meio de seu endereço no cabeçalho da mensagem, assim como estipulando o endereço lógico de destino, se fôr desejável um mapeamento completamente geral.

Endereços físicos representam um ponto no espectro de endereçamento de mensagens. Uma dificuldade que surge com a adoção deste tipo de endereçamento é quando surgem modificações nos endereços físicos, pois estas devem ser divulgadas por todos os assinantes com todos os problemas operacionais inevitáveis que tais modificações causam. Os endereços lógicos representam o ponto oposto neste espectro. Neste caso, a rede de comunicação é responsável pela manutenção da localização de cada assinante e pela tradução dos endereços lógicos utilizados pelos usuários nos respectivos endereços físicos utilizados pelos algoritmos de direcionamento.

- Considerações de implementação:

O endereçamento lógico dos assinantes necessita de algum tipo de mapeamento para que a tradução dos endereços lógicos em físicos e vice-versa se realize. Estas tabelas podem estar localizadas em um ou mais lugares sendo atualizadas quando as modificações ocorrerem. O custo da manutenção desta tabela depende do tamanho da rede e a forma de implementação do endereçamento lógico escolhida. As formas de implementação podem ser:

- ENDEREÇAMENTO LÓGICO E FÍSICO: esta é uma forma híbrida que pode ser utilizada quando uma rede projetada somente para endereçamento físico está sendo modificada para permitir o endereçamento lógico. Nesta fase de transição o usuário escolhe qual o tipo de endereçamento que quer

utilizar. O mapeamento do endereço lógico para o físico é realizado no nó origem;

- MAPEAMENTO COMPLETO: fornece um endereçamento lógico para todos os assinantes da rede, ou seja é a extensão do método anterior;

- MAPEAMENTO PARTICIONADO: Uma estrutura diferente para a tabela de endereços pode ser desenvolvida tirando-se vantagem do fato de que, para propósitos de direcionamento, o nó origem necessita somente da informação relativa ao nó destino, enquanto que o nó destino necessita somente a informação para que porta deverá seguir a mensagem recebida. A tabela de mapeamento do nó "X" constitui-se-á de duas partes: a primeira com K entradas contendo os endereços dos nós e a outra com M entradas contendo o endereço das portas, onde K é o numero total de endereços lógicos, exceto os endereços dos assinantes conectados ao nó "X", e M é o número total de endereços lógicos dos assinantes conectados ao nó "X";

- CENTRO DE INFORMAÇOES: baseia-se na existência de um ou mais centros de informações na rede. Cada um destes centros deve manter a informação de mapeamento necessária para que o mapeamento dos endereços ocorra. A informação é fornecida aos nós através de pedidos. Este é o método utilizado na rede SNA da IBM. Este método é de utilidade em grandes redes nas quais existam poucos nós com grande capacidade e muitos nós de capacidade reduzida, porque evita que cada nó de capacidade reduzida possua a informação completa dos endereços físicos, possibilitando que estes nós possuam apenas o conjunto das transformações dos endereços utilizadas mais recentemente, junto com o das conexões ativas no momento, ou até outras como por exemplo, as informações que certamente serão utilizadas para que possa evitar o acesso ao centro de informação para cada mensagem.

- Considerações de eficiência:

Para uma rede de circuito virtual, o endereçamento lógico pode ser implementado pela troca de informação apropriada de mapeamento na fase de conexão. O resultado desta troca é que os nós origem e destino lembrar-se-ão cada um dos endereços físico e lógico do assinante no outro extremo. Estes poderão ser utilizados sem necessidade de se referenciar a tabela de mapeamento durante a conexão lógica; esta é uma vantagem que a rede do tipo datagrama não possui.

Especificamente, em uma rede circuito virtual os pacotes que fluem pela rede podem ser endereçados pelo endereço físico do assinante destinatário somente, sendo que o cabeçalho da mensagem para o assinante destino pode ser construído no nó destino, pois este cabeçalho deverá conter os endereços lógicos dos assinantes origem e destino. Em uma rede datagrama, o cabeçalho do pacote tem que conter tanto a informação do endereço para os assinantes quanto o endereço físico para efeitos de direcionamento.

Visto isto chega-se a conclusão de que os circuitos virtuais, uma vez estabelecidos, são mais eficientes para o endereçamento lógico do que os datagramas.

II.3.3.c - Endereçamento por Difusão ('Broadcast'):

Este tipo de endereçamento significa a capacidade de um nó enviar uma única mensagem para todos os nós ao invés de enviar várias mensagens separadas, uma para cada nó.

Também pode ser utilizado para a propagação de informações pela rede para todos os nós, como por exemplo, a atualização das tabelas de rotas dos nós (vide Seção II.4).

O maior problema que surge na adoção deste tipo de endereçamento é quanto ao direcionamento das mensagens.

- Considerações quanto à implementação:

Existem dois tipos de estratégias para o problema de transmitir-se uma mensagem para todos os endereços possíveis que são:

- DIFUSÃO ('BROADCASTING') : dirigir uma única mensagem para todos os endereços possíveis;

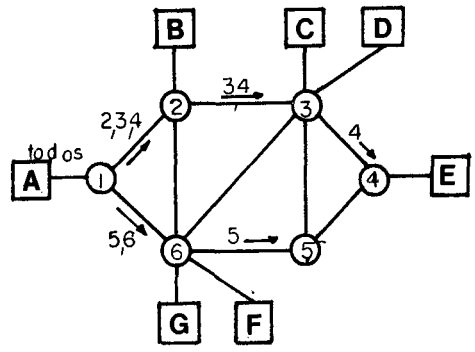
- ENCHENTE ('FLOODING'): enviar uma cópia da mensagem para cada linha da rede.

DIFUSÃO é o sistema no qual a origem explicitamente endereça a mensagem para todos os nós, enviando uma ou mais cópias com os endereços apropriados para cada uma de suas linhas de saida, dirigindo-as para cada nó. (Vide Fig. II.8.(a)). Tal esquema irá requerer N-1 passos para o 'broadcast' que é ótimo, onde N é o número de nós da rede.

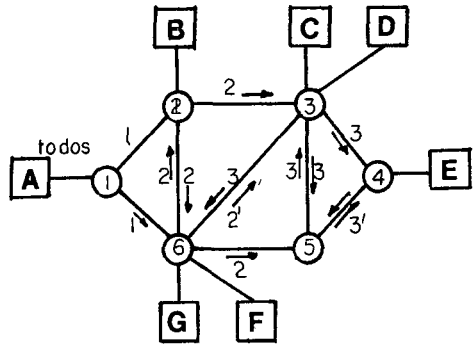
ENCHENTE é um método no qual cada um dos nós envia uma nova cópia da mensagem recebida por todos os canais, com exceção do canal pelo qual foi recebida a mensagem (vide figura II.8(b)). Este método irá requerer L-N+1 passos para o 'broadcast' (onde, L é igual ao número de canais na rede, contando cada direção separadamente).

II.3.3.d - Endereçamento de grupo e multi-destino:

Por razões de conveniência e eficiência, é desejável fornecer a facilidade de se endereçar mensagens com o nome de um grupo de endereços (endereços físicos dos assinantes 'singly homed' e 'multiply homed'). Este grupo pode, por exemplo, corresponder a uma convocação para uma conferência, ou um grupo de trabalho distribuído, ou a uma simples lista de distribuição de certas mensagens (Vide Fig. II.9).



(a) Por difusão



(b) Por enchente

A sequência do fluxo de mensagens é indicado pelos números (1 antes do 2, antes do 2' , antes do 3', antes do 4)

Figura II.8: Métodos de Endereçamento por Difusão

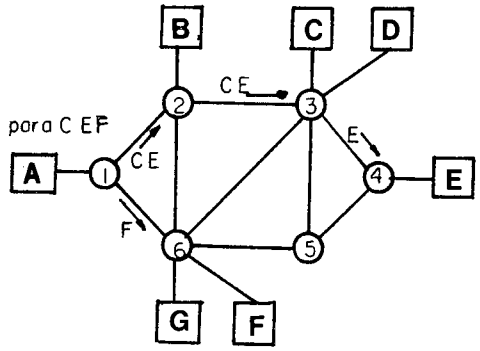


Figura II.9: Endereçamento de Grupo e Multi-destino

- Considerações de implementação:

Em uma rede de circuito virtual estes tipos de endereçamento são inadequados: por que ambos são ineficientes e de difícil controle. As duas alternativas básicas para este caso são:

- estabelecer (a)x(a) circuitos virtuais , quando (a) endereços estiverem presentes no grupo;

- modificar o cabeçalho do pacote para se permitir vários números de mensagens, confirmações e alocações de fluxo pelo circuito virtual multi-destino.

Os métodos acima parecem ser tão complexos que tornam difícil justificar a sua implementação. Em contrapartida, para um datagrama com vários endereços o problema se resume em simplesmente direcionar os pacotes eficientemente até os respectivos destinos.

II.3.4 - Rotas:

- Classificação dos Algoritmos:

Os algoritmos de direcionamento podem ser classificados baseados em três variáveis:

- o LUGAR aonde a decisão de qual caminho que deverá ser seguido é tomada;

- a constante do TEMPO: fornece o tipo de comportamento do algoritmo com o transcorrer do tempo;

- o TIPO de controle adotado.

Detalhando temos:

- de acôrdo com o lugar de decisão:

- DIRECIONAMENTO EM UM PONTO FIXO: o nó origem deve especificar todo o caminho a ser percorrido pelo pacote; esta informação deverá ser incluída aos dados que estão sendo transmitidos. Neste caso, o nó origem deve obter esta informação no próprio nó ou em ponto centralizador pré-determinado. Este ponto deve possuir informações bastante detalhadas a respeito do estado da rede. Os pontos de chaveamento não necessitam possuir as tabelas de direcionamento, já que nenhuma decisão de mudança de rota será efetivada;

- DIRECIONAMENTO PASSO-A-PASSO ou INCREMENTAL: o nó origem especifica somente o endereço do nó destino, cabendo aos nós intermediários a tarefa de direcionamento do pacote. O nó origem só precisa conhecer o caminho que deverá ser seguido para se atingir o proximo nó. Obviamente, cada nó intermediário precisará possuir as tabelas de

direcionamento pois as rotas serão traçadas passo-a-passo;

- DIRECIONAMENTO HÍBRIDO: combinação dos métodos acima. Neste caso, o nó origem só especifica determinados pontos, ditos principais, permitindo que o trajeto entre estes pontos seja decidido pelos nós intermediários.

- de acordo com o tempo envolvido:

- DIRECIONAMENTO FIXO OU DETERMINÍSTICO: as tabelas de rotas são criadas uma única vez, permanecendo inalteradas durante grandes intervalos de tempo. Estas tabelas só deverão sofrer alterações quando ocorrer modificações no sistema, como por exemplo, a inclusão de mais um nó;

- DIRECIONAMENTO DINÂMICO OU ADAPTATIVO: as tabelas de rotas são alteradas com frequência, refletindo as modificações sofridas pela rede decorrente das condições de funcionamento.

- de acôrdo com o mecanismo de controle:

(Esta classificação só tem sentido no caso do direcionamento ser adaptativo).

- DIRECIONAMENTO ISOLADO: os nós, isoladamente, tentam atualizar as suas tabelas pela observação da performance das suas tentativas de transmissão dos pacotes, utilizando-se somente dos dados locais para se adaptarem as mudanças de condições;

- DIRECIONAMENTO CENTRALIZADO: as modificações sofridas pela rede, tais como a perda de conectividade ou

modificações na performance de determinados nós, são enviadas para um ponto centralizador que é responsável pela atualização das tabelas de direcionamento. Esta informação, as tabelas atualizadas, será então difundida para os pontos de origem (no caso de direcionamento na origem) ou para todos os nós (no caso de direcionamento passo-a-passo);

- DIRECIONAMENTO DISTRIBUÍDO: o processo de controle da atualização das tabelas é distribuído por todos os nós; para que esta forma de direcionamento seja viável torna-se necessário uma cooperação entre os nós, isto é, uma troca de informações sobre a sua performance e das suas ligações com os outros nós.

II.4 - CONTROLE DE ROTAS

II.4.1 - Introdução:

Para que uma rede de comunicações de dados opere com sucesso é necessário que ela possua uma previsão para um algoritmo adequado para traçado de rotas. Em uma rede de comutação por circuitos o algoritmo de direcionamento atua durante a fase de estabelecimento da ligação, enquanto que no caso de uma rede de comutação por pacotes o algoritmo poderá determinar a rota para cada pacote ou para uma determinada sequência de pacotes.

Qualquer procedimento de controle de rotas do tipo adaptativo possui as seguintes funções:

- medição dos parâmetros da rede pertinentes a estratégia de direcionamento;

- envio desta informação ao(s) ponto(s) (Centro de controle da rede ou nós) nos quais o cálculo do direcionamento tem lugar;

- cálculo das tabelas de direcionamento;

- conversão das tabelas de direcionamento em decisões de direcionamento.

O problema do direcionamento em redes cresce, em complexidade, diretamente com a complexidade de sua topologia. Em uma rede do tipo ESTRELA com ligações 'full-duplex' (fig. II.1Ø.(a)) cada nó da rede é conectado a um nó central para o qual todo tráfego deve ser dirigido. Somente o nó central necessita possuir a definição da topologia da rede; a cada nó destino é associado um canal ('link') distinto e a tabela de rotas a ser utilizada simplesmente relaciona o destino com determinado canal. Logo, o algoritmo de direcionamento é bastante simplificado.

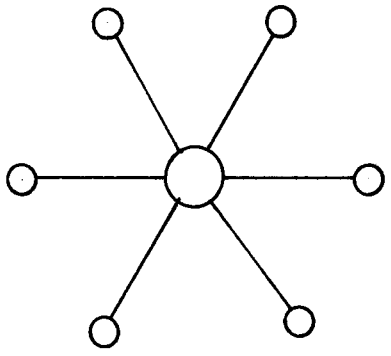
Uma outra topologia bastante simples é a rede do tipo

anel. Neste caso, se os canais forem duplex, o tráfego pode atingir qualquer destino a partir de qualquer origem simplesmente percorrendo o anel. Novamente o algoritmo de direcionamento é bastante simples, não necessitando essencialmente da tabela de rotas. Esta seria necessária quando quisermos determinar a rota mínima a ser percorrida para se atingir um determinado nó, por exemplo.

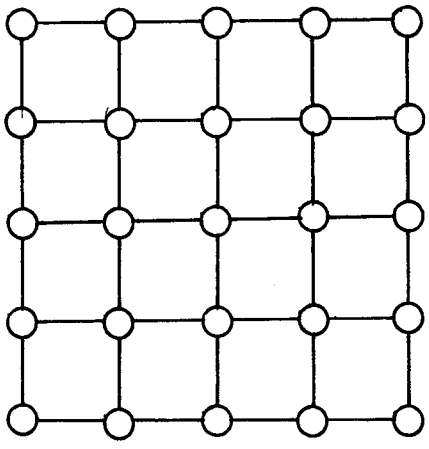
Uma outra topologia na qual o algoritmo é simples é a rede MALHADA REGULAR RETANGULADA (vide fig. II.1Ø.(b)) que utiliza um sistema de numeração dos nós. Neste caso, existem pelo menos duas rotas mínimas de igual comprimento de um nó origem a um nó destino (exceto no caso de nós adjacentes). A numeração dos nós é feita de tal forma que indica a linha e a coluna ocupadas por cada nó na malha. Cada nó necessitará conhecer o procedimento de direcionar o tráfego para os números de linhas e colunas maiores (ou menores). Esta informação pode ser armazenada em uma tabela de rotas bastante simplificada.

Como exemplo final de redes que possuem algoritmos bastante simplificados de direcionamento mencionaremos a rede completamente conectada (fig II.1Ø.(c)). Neste caso, cada nó possui uma ligação direta com todos os outros nós, possuindo uma tabela de direcionamento que define a única ligação para se atingir o outro nó.

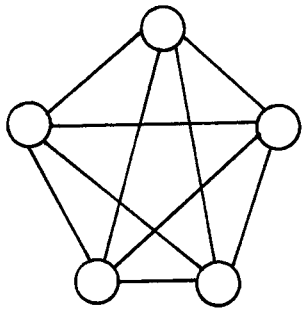
Estas topologias de redes que conduzem a uma simplificação nos algoritmos de direcionamento são difíceis de serem encontradas na prática, pois a maioria das redes existentes possuem topologias bastante complexas. Isto geralmente ocorre porque a localização dos nós é fornecida pelas necessidades do usuário e as ligações entre os nós dependem das rotas, da capacidade disponível e considerações de custo. Um exemplo prático deste tipo de redes é a rede telefônica de uma cidade.



(a) Estrela



(b) Malhada Retangular



(c) Rede Completamente Conectada

Figura II.10: Exemplos de Direcionamento

II.4.2 - Projeto de um algoritmo de Controle de Rotas: /MCQUJ78/

Uma dúvida que ocorre ao projetista de uma rede de computadores é: Como projetar um algoritmo de controle de rotas? Quais os cuidados que deverei tomar ?. Nesta seção tentaremos responder a estas perguntas.

O projeto de um algoritmo de controle de rotas pode ser dividido em duas fases (vide figura II.11)

- uma FASE DE ESPECIFICAÇÃO: na qual estuda-se as alternativas possíveis, quais devem ser os dados de entrada e saida, como deve proceder o algoritmo;

- uma FASE DE AVALIAÇÃO: na qual estuda-se o comportamento do algoritmo, se ele está realmente cumprindo os seus objetivos.

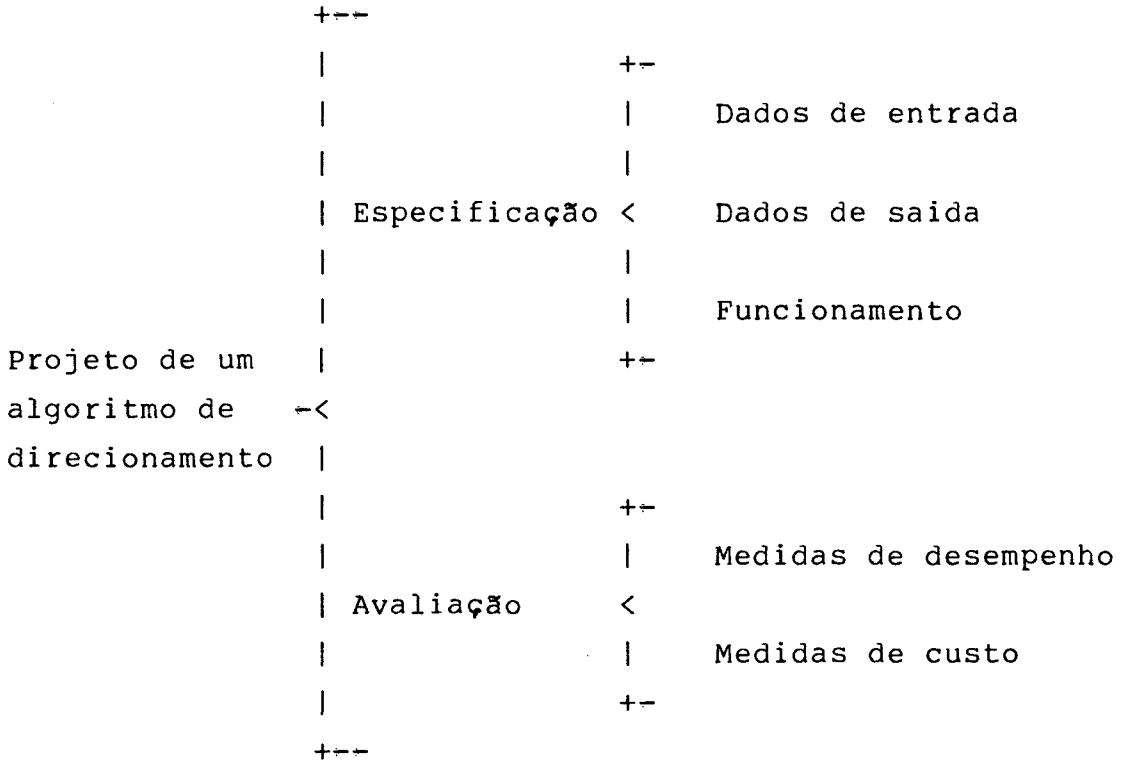


Fig. II.11 - Fases de um Algoritmo de Roteamento

Analisando-se cada estágio temos:

- Dados de entrada e saida:

Os dados podem ser divididos em:

- INFORMAÇÃO SOBRE A ADJACÊNCIA: a identificação dos nós adjacentes a um determinado nó constitui um ponto fundamental para o algoritmo. O algoritmo deverá determinar se o canal que conecta os nós está funcionando e, talvez, se os próprios nós estão em funcionamento. Outros aspectos da conectividade tais como a largura de banda e o atraso dos circuitos poderão ser considerados;.

- NECESSIDADE DE TRÁFEGO: Os dois tipos básicos de dados a serem medidos ou estimados são o atraso e a taxa de vazão ('throughput') obtida pelo tráfego que chega a cada nó. O fluxo dos dados em cada linha da rede poderá ser derivado a partir destes dados;

- ALCANCE: a necessidade de qualquer algoritmo de direcionamento é de que cada nó deve conhecer se existe um caminho para um outro nó. O cálculo deve determinar se é possível atingir a um determinado nó baseado somente nas informações sobre os nós adjacentes;

- ATRIBUIÇÃO DE TRÁFEGO: A seguir, o algoritmo deve atribuir o tráfego para cada nó por um conjunto de caminhos. Isto significa a escolha do melhor caminho ou caminhos para um determinado destino baseado no critério de otimalidade. Dois critérios importantes são o de destinar o tráfego interativo para os caminhos de atrasos pequenos e o de destinar o tráfego pesado (transferência de arquivos) para os caminhos de altas taxas de vazão;

- FUNCIONAMENTO: para alcançar o seu pleno funcionamento o algoritmo deve satisfazer a seis objetivos que estão

relacionados ao desempenho que são:

- simplicidade;
- confiabilidade;
- solução a um estado fixo;
- adaptação a modificações;
- otimalidade global;
- rapidez.

O objetivo da simplicidade assume particular importância no caso em que novas exigências são acrescentadas ao algoritmo implicando em um aumento em sua complexidade. O algoritmo deve ser simples o suficiente para que se possa compreender o seu funcionamento em todas as condições possíveis, implicando na facilidade de se descobrir erros e de desenvolvimento de melhorias. Isto implica que técnicas sofisticadas, tais como as técnicas heurísticas, não determinísticas, são indesejáveis. Um outro ponto em que a simplicidade se aplica é quanto à estrutura do programa, pelo fato de que este deverá rodar em vários pontos, nos nós, de uma forma contínua, por causa disto prefere-se que o programa seja pequeno e bastante simples.

O algoritmo deve ser seguro e confiável no caso de falhas dos nós e das linhas, pois estas devem ser esperadas, causando com isto o funcionamento correto do programa muito importante. Em consequência um mau funcionamento momentâneo ou prolongado de qualquer componente da rede não deve interferir com o direcionamento mesmo se o programa de direcionamento em um nó ou os dados de direcionamento transmitidos forem afetados. Deve-se tomar muito cuidado com o programa de direcionamento porque este é intrinsicamente vulnerável pois se um nó começar a transmitir informações de direcionamento errôneas toda a rede poderá ser afetada.

Uma exigência básica do algoritmo de direcionamento é que este deve chegar a uma solução fixa baseado em um conjunto de dados estáticos, isto é, as opções feitas devem ser corretas, não devendo oscilar.

A necessidade anterior é trivial quando comparada com o fato de que o algoritmo tem que se adaptar as modificações verificadas na topologia da rede e nas condições de tráfego. Este fato influencia o projeto de várias maneiras:

- o programa deve ser eficiente o suficiente para rodar em tempo real de acordo com as modificações sofridas pela rede;

- deve ter uma prioridade mais alta do que a do processo de manipulação de dados;

- a rede pode ficar congestionada se o programa demorar a se ajustar as mudanças observadas tais como: tráfego pesado, acréscimo rápido no tráfego em uma determinada linha, quebra de uma determinada linha.

- Medidas de desempenho:

Passaremos agora a considerar o projeto em sua segunda fase: a avaliação de seus méritos em têrmos de desempenho e custos.

O desempenho de um algoritmo de direcionamento pode ser medido de acordo com quatro fatores de fundamental importância:

- ATRASO : o atraso mínimo teórico é determinado pelas condições da rede em um ponto específico. O programa deverá chegar a resultados os mais próximos possíveis do mínimo teórico;

- VAZÃO: idêntica a anterior. Existe uma vazão máxima que deve ser alcançada pela aplicação do algoritmo. Existe

uma relação muito grande entre o atraso e a vazão, por que nem sempre é desejável obter-se a melhor vazão pois altas taxas de vazão devem ser destinadas para as grandes transferências de dados;

- CUSTOS: o algoritmo pode afetar os custos de utilização da rede pela sua demanda da capacidade das linhas dos nós e de armazenamento nos nós;

- CONFIABILIDADE: o processo de direcionamento está também relacionado com a conectividade da rede. A decisão de que um nó pode ser acessado deve ser correta.

Estes quatro fatores são sentidos principalmente por uma modificação no custo de manutenção da rede, por causa disto devemos orientar o nosso projeto para que possamos diminuir estes custos. Podemos definir cinco tipos de custos que influenciam diretamente o projeto, por que seus efeitos deverão ser balanceados a fim de se obter um melhor desempenho da rede, que são:

- CAPACIDADE DOS NÓS: o cálculo das melhores rotas representa uma demanda de tempo de processamento nos nós, um fator que reduz a capacidade destes para o processamento dos dados;

- ATRASO NOS NÓS: enquanto o cálculo das rotas é efetuado, o fluxo de dados através do nó é interrompido representando um custo direto;

- ARMAZENAMENTO NOS NÓS: o algoritmo de direcionamento necessita de espaço para armazenar as informações utilizadas no direcionamento, como por exemplo o próprio programa, os dados de entrada e saida. Tudo isto representa espaço não disponível para o 'pool' de buffers utilizados pelas mensagens reduzindo com isto a capacidade do nó e causando a necessidade de mais um tipo de controle, o CONTROLE DE FLUXO.(vide seção II.5);

- CAPACIDADE DAS LINHAS: a utilização das linhas pelo controle de rotas depende do tamanho das mensagens de direcionamento que são enviadas para os nós atualizarem as suas tabelas, da frequência destas mensagens e da própria capacidade da linha. Convém observar que ao se utilizar uma linha de comunicação para transportar informações de controle da rede estamos diminuindo com isto a sua capacidade e aumentando o custo;

- ATRASO NA LINHA: os atrasos aumentam linearmente com a frequência das mensagens de direcionamento, quadraticamente com o tamanho da mensagem e com o decréscimo da capacidade da linha.

II.4.3 - Algoritmos utilizados para o controle de rotas: /SCHWM8Ø/, /JOHND77/:

Os algoritmos de controle de rotas baseados nas informações medidas atribuem "custos" a cada caminho possível entre um nó e um destino. Estas atribuições podem ser baseadas em dois princípios:

- atribuição a um único caminho entre um dado par origem/destino;

- o tráfego para um determinado par origem/destino é distribuido por vários caminhos.

Ao se pensar em termos de direcionamento por um único caminho é natural escolher-se o "menor" ou, em termos mais gerais, o caminho de menor custo sempre que os caminhos alternativos existam, é claro. Os custos das ligações que são calculados utilizando-se funções de custo, possuem uma propriedade essencial que é a seguinte: o custo de uma ligação é calculado como sendo a soma dos custos dos canais que pertencem a esta ligação, ou em outras palavras, o custo de uma ligação entre dois nós origem/destino é o somatório dos

custos mínimos calculados para cada nó intermediário da rede. Neste caso, o problema de direcionamento é equivalente ao de se achar um menor caminho de um grafo, no qual o "comprimento" do arco é dito ser o "custo" da ligação. O conjunto de caminhos mínimos de todos os nós origens para um nó destino comum forma uma árvore na qual o nó destino é a raiz. Logo, é claro que se o direcionamento do caminho único for utilizado em uma base origem/destino o caminho do pacote será unicamente determinado pelo nó destino.

Passaremos agora a discutir dois dos muitos algoritmos que são utilizados em redes de computadores sendo considerados casos gerais. Um destes algoritmos, o de Ford-Fulkerson, denominado algoritmo "A", aplica-se ao caso em que o cálculo é centralizado enquanto que o outro, o de Dijkstra, denominado "B", aplica-se ao direcionamento distribuído.

Considere a figura II.12.(a) na qual os números associados as ligações são os custos de cada uma. Por efeito de simplificação as ligações são consideradas bi-direcionais com o mesmo custo em cada uma das direções, embora os algoritmos possam trabalhar com custos diferentes.

Para melhor podermos definir os algoritmos devemos considerar a seguinte notação:

N ..... conjunto de nós

l(i,j).. comprimento da ligação do nó i ao nó j. (infinito no caso de não haver nenhuma ligação entre estes dois nós)

D(n) ... distância da origem até ao nó n obtida através do menor caminho restritos aos nós pertencentes ao conjunto N

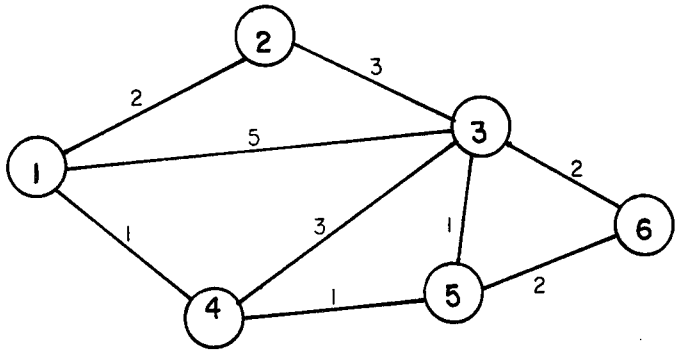
O funcionamento em têrmos gerais do algoritmo A é o seguinte:

- Inicio: atribuir N= { 1 }, e para cada nó v que não esteja no conjunto N faça D(v)=l (1,v);

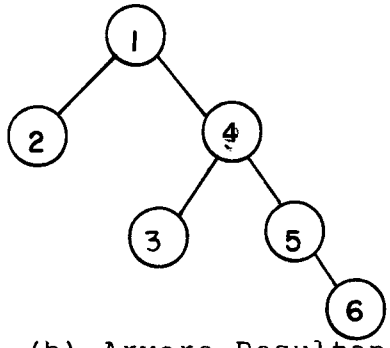
- nos próximos passos encontra-se um nó w que não esteja em N para o qual D(w) é mínimo colocando-o em N. Atualize as distâncias D(v) para os nós restantes que não estão em N pelo cálculo :

$$D(v) = \min(D(v), D(w) + l(w,v)).$$

A aplicação do algoritmo para a rede acima é mostrada na figura II.13 e a árvore resultante dos caminhos mínimos aparece na fig II.12.(b) junto com a tabela de direcionamento para o nó 1, indicando qual a ligação de saida que deve ser tomada pelo tráfego que chega a este nó.



(a) Rede Considerada



(b) Arvore Resultante

Figura II.12: Topologia considerada

Passo	N	D(2)	D(3)	D(4)	D(5)	D(6)
Inicial	{1}	2	5	1	-	-
1	{1,4}	2	4	1	2	-
2	{1,2,4}	2	4	1	2	-
3	{1,2,4,5}	2	3	1	2	4
4	{1,2,3,4,5}	2	3	1	2	4
5	{1,2,3,4,5,6}	2	3	1	2	4

Figura II.13: Aplicação do algoritmo A

Consideremos agora o algoritmo B, que é um procedimento iterativo que será utilizado no mesmo caso para se encontrar os caminhos mínimos de todos os nós até o nó 1, considerado como sendo o destinatário comum. Para se ter um registro dos caminhos mínimos cada nó "v" será identificado por um par de valores (n,D(v)) onde D(v) representa o valor corrente desta iteração para a distância mínima deste nó até ao destinatário e n é o número do próximo nó ao longo deste caminho mínimo que está sendo calculado. Em linhas gerais este algoritmo comporta-se da seguinte forma (vide fig. II.14):

- Início: atribuir D (1) = Ø, e a todos os outros nós o valor (-,-) isto é, o nó está inatingível;

- Passo 2: atualizar D(v) para cada nó v não-destinatário pelo exame do valor corrente D(w) para cada nó adjacente w efetuando a seguinte operação:

$$D(v) := \min (D(w) + l(v,w)).$$

A atualização do nó v é completada pela troca do primeiro argumento pelo número do nó adjacente que minimiza a expressão acima. A operação de atualização é repetida para cada nó até que nenhuma modificação a mais ocorra; neste momento o algoritmo termina. A árvore de caminhos mínimos é naturalmente igual à mesma gerada pelo algoritmo anterior. Observa-se também que embora o algoritmo tenha atualizado os nós pela sua ordem numérica o algoritmo funciona a partir de qualquer ordem dos nós. Para cada nó não-destinatário o primeiro argumento indica o proximo nó pertencente ao caminho mínimo que deverá ser seguido, logo suprindo a informação de direcionamento necessária para se atingir o destinatário.

Ciclo	No' ->	2	3	4	5	6
Inicial		(-,-)	(-,-)	(-,-)	(-,-)	(-,-)
1		(1,2)	(2,5)	(1,1)	(4,2)	(5,4)
2		(1,2)	(5,3)	(1,1)	(4,2)	(5,4)

Figura II.14 - Aplicação do algoritmo B

- Comparação dos Algoritmos:

A construção das tabelas de direcionamento baseada no algoritmo A necessita do cálculo da árvore de caminhos mínimos para cada um dos nós. Esta arvore é construída a partir das informações globais da rede (i.e., as modificações sofridas pela rede) e da escolha de um determinado nó para servir de raiz da árvore. A informação de direcionamento gerada a partir desta árvore é utilizada para se construir a tabela de rotas para este nó escolhido.

A construção das tabelas de rotas no caso do algoritmo B requer uma aplicação repetida do algoritmo para cada nó destinatário resultando na formação de um conjunto de dados para cada um dos nós. Estes dados são utilizados como informação para o direcionamento (próximo nó) e da distância até um determinado destinatário. Observe que neste caso este algoritmo pode ser convenientemente implementado em uma forma distribuída na qual cada nó necessita somente obter informações dos nós vizinhos.

A avaliação dos méritos dos dois algoritmos para efeito de comparação depende de uma série de fatores a saber:

- sobrecarga causada pela transmissão dos dados medidos

para os pontos nos quais o cálculo é realizado;

- volume de dados a ser armazenado;

- complexidade do cálculo;

- velocidade com que o algoritmo responde às modificações sofridas pela rede.

Estas comparações podem somente serem realizadas ao se estudar uma rede específica. Passaremos agora a descrever como o problema de controle de rotas é enfrentado em uma das redes já em funcionamento.

II.4.4 - Exemplo da aplicação do Controle de Rotas :

- ARPANET: /MCQUJ79/,/SCHWM8Ø/

Cada nó da rede mantém informações que descrevem a topologia da rede e os atrasos das linhas. Utilizando estas informações cada nó calcula independentemente o melhor caminho para todos os outros nós, direcionando os pacotes desta forma. Por causa da possibilidade do tráfego na rede variar, cada nó mede periodicamente os atrasos ocasionados nas suas linhas de saida, enviando esta informação (na forma de uma atualização de direcionamento) para todos os outros nós. Uma mensagem deste tipo gerada por um determinado nó será pequena e seu tamanho independente do tamanho da rede. Uma mensagem deste tipo é dirigida inalterada para todos os nós da rede (ao invés de serem enviadas somente para os nós vizinhos, como outros algoritmos de direcionamento utilizados). Como as atualizações não precisam ser processadas antes de serem despachadas elas se propagam rapidamente pela rede de tal forma que possibilitam aos nós atualizarem as suas informações e a continuarem a direcionar o tráfego de uma maneira eficiente e consistente com o estado atual da rede.

O algoritmo utilizado é o denominado 'Shortest Path First', SPF, (Primeiro o menor caminho), basicamente uma variação do algoritmo B.

O algoritmo SPF básico utiliza as informações que descrevem a rede para gerar uma árvore que representa os caminhos de atrasos mínimos, de um dado nó raiz para todos os outros nós da rede. A fig. II.15 mostra um fluxograma simplificado do algoritmo. A árvore consiste inicialmente somente do nó raiz. A árvore é aumentada para conter o nó que está mais próximo (em termos de atraso) da raiz e que seja adjacente a um nó que já esteja na árvore. O processo continua pela repetição deste último passo. LISTA denota uma estrutura de dados que contém os nós que ainda não foram colocados na ARVORE, mas que são vizinhos dos nós que já estão na ARVORE. A ARVORE é construída com os menores caminhos inicialmente, daí o nome deste algoritmo.

Eventualmente o último nó é colocado na árvore terminado o algoritmo.

As outras duas componentes importantes do procedimento de direcionamento são os mecanismos de medida dos atrasos e o esquema de propagação desta informação.

Na ARPANET cada nó mede o atraso real de cada pacote que passa através de cada uma de suas linhas de saída, calculando o atraso médio a cada 10 segundos. Se este atraso for significantemente diferente do anterior ele deverá notificar os outros nós.

O procedimento de atualização das informações de atrasos na propagação é de suma importância porque deve-se assegurar que cada atualização foi realmente recebida por todos os nós, para que as informações mantidas por estes sejam as mais atualizadas, refletindo o estado da rede. Cada nova atualização recebe um número de sequência, sendo então transmitida para todos os nós pelo método mais simples e confiável de transmissao, isto é, transmiti-la por todas as

linhas. Quando um nó recebe uma atualização verifica se já foi processada esta atualização; se isto ocorrer esta informação não é considerada. Em caso contrário, ela é imediatamente transmitida para os nós adjacentes. Desta forma se garante que a atualização atinge todo o universo da rede de uma forma rápida.

Como pudemos verificar o algoritmo de direcionamento da ARPANET pode ser classificado como sendo : distribuído e adaptativo.

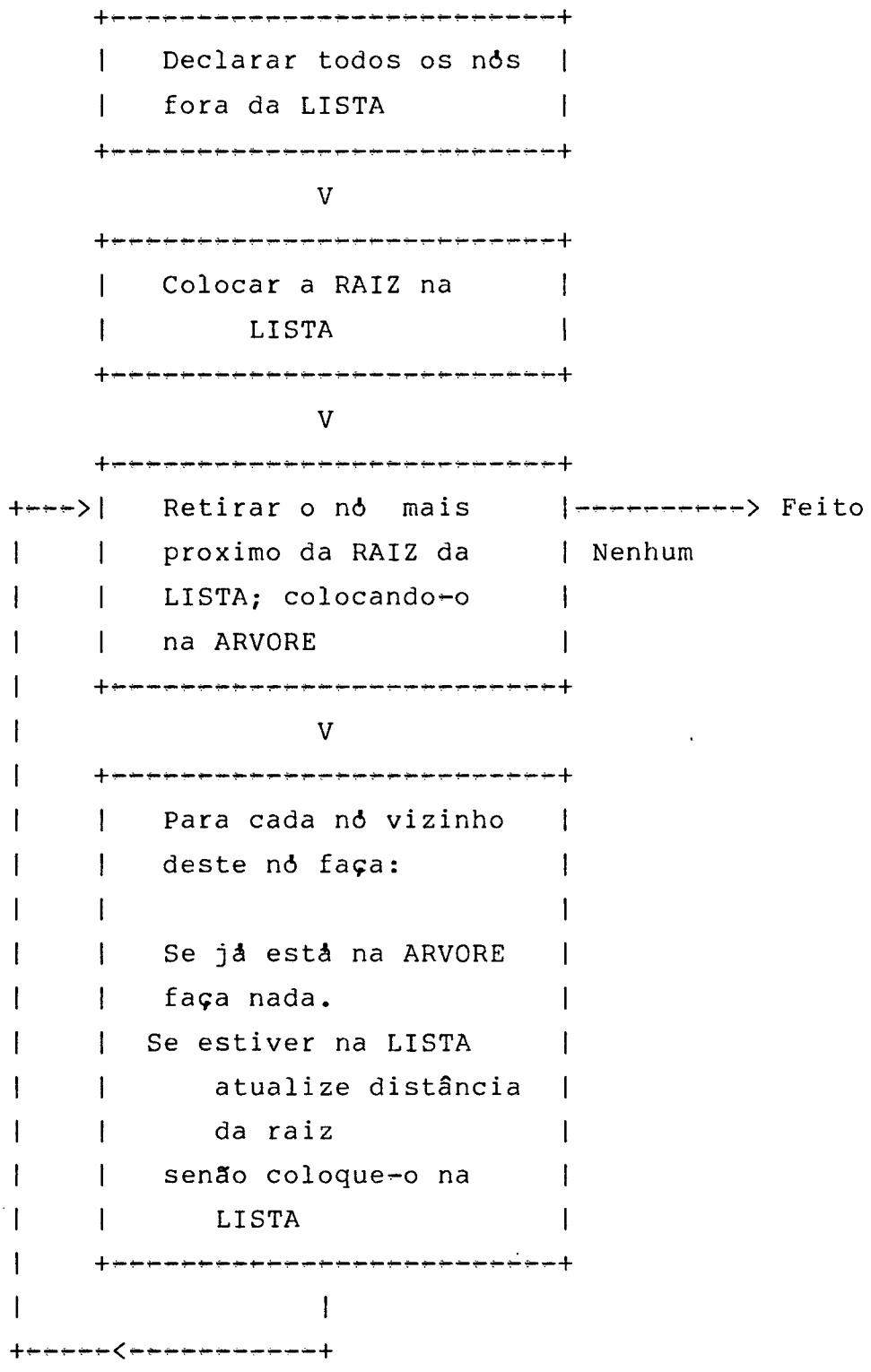


Figura II.15: Fluxograma do Controle de Rotas

II.5 - Controle de Fluxo:

II.5.1 - Introdução:

Uma rede de comutação de pacotes pode ser vista como sendo um conjunto distribuído de recursos (canais, buffers e processadores de comutação) cuja capacidade deve ser dinamicamente compartilhada por vários usuários (ou para ser mais geral, processos) que desejam se comunicar. O compartilhamento dinâmico dos recursos é que distingue a comutação de pacotes da comutação de circuitos, na qual os recursos são dedicados a cada um dos usuários por longos períodos de tempo. As seguintes vantagens do compartilhamento dinâmico podem ser destacadas:

- maiores velocidades de transmissão;

- flexibilidade no estabelecimento de conexões;

- uso mais eficiente dos recursos da rede.

Entretanto, estas vantagens do compartilhamento dinâmico vêm acompanhadas de um certo risco que é a possibilidade dos usuários abusarem dos recursos da rede no caso de não haver um controle rígido. De fato, não havendo o controle da demanda o abuso dos usuários pode conduzir rapidamente a rede a um estado desagradável de congestionamento, neutralizando, consequentemente, as vantagens mencionadas. Então, deve-se adotar mecanismos de monitoração e de controle da carga oferecida para que se evite o congestionamento. Estes mecanismos, denominados de Controle de Fluxo, possuem como funções principais:

- prevenção da degradação da vazão e perda de eficiência devido à sobrecarga;

- prevenção de bloqueios ('deadlocks');

- equidade na alocação dos recursos para os diferentes usuários;

- compatibilização da velocidade da rede com a dos usuários.

A degradação da vazão e os bloqueios ocorrem no caso do tráfego que já foi aceito pela rede (isto é, o tráfego que já está alocandomos recursos da rede) exceder a capacidade nominal da rede. Existem várias possibilidades de ocorrer a degradação e os bloqueios, como será visto a seguir.

II.5.2 - Problemas e Funções do Controle de Fluxo:

II.5.2.a - Degradação:

Definida como sendo uma redução da eficiência da rede (os bloqueios são considerados um caso extremo de degradação). A eficiência de uma rede pode ser medida de várias maneiras possíveis, como por exemplo o tempo de retardo e a vazão.

Distinguem-se os seguintes tipos de degradação:

- 'LOOPING': ocorre por causa do fato das decisões de direcionamento dos pacotes serem independentes e efetuadas pelos diversos nós, possibilitando ao tráfego retornar a um nó previamente visitado ou, em uma definição mais geral, o tráfego percorrer um caminho desnecessariamente longo. A ocorrência destes 'loops' causa o surgimento de grandes retardos no tráfego, retardos estes inaceitáveis em determinadas aplicações. Naturalmente, qualquer procedimento de direcionamento adaptativo deve detectar estes 'loops' a fim de evitá-los e direcionar o tráfego diretamente para o seu destino. Um outro método, mais drástico, é o de se destruir o pacote quando este já passou por um número pré-determinado de nós.

- VAZIOS NO FLUXO DE MENSAGENS: estes vazios são devidos a uma limitação no número de mensagens em trânsito permitido pela rede. Assuma que entre um par de nós origem-destino seja permitido que n mensagens estejam em trânsito em um determinado instante. Se n mensagens estiverem em trânsito, a próxima mensagem terá que esperar a chegada de uma confirmação do nó destino para qualquer uma das n mensagens enviadas. Observa-se que, se o tempo necessário para se enviar uma mensagem pela rede e esperar pela sua confirmação ('round trip delay') for maior que o tempo que se leva para gerar n mensagens, então o nó origem ficará bloqueado esperando as confirmações chegarem, a fim de poder enviar mais mensagens. Estes vazios introduzidos no fluxo de mensagens resulta em um decréscimo na vazão.

- TURBULÊNCIA CAUSADA POR UM SIMPLES PACOTE: Observou-se na rede ARPA que as mensagens de pacote único não eram aceitos pelo nó destino se elas chegavam fora de ordem, sendo encaradas como um pedido de alocação de um buffer para o reempacotamento. No caso de uma cadeia de mensagens constituídas de um único pacote, o pacote p chegar fora de ordem (isto é, chegar após o pacote p + 3, por exemplo), os pacotes p+1, p+2 e p+3 serão descartados pelo nó destino, e somente após a chegada do pacote p é que seria alocado um buffer para a mensagem p+1. Esta alocação retornaria na confirmação fim a fim do pacote p, autorizando a retransmissão pelo nó origem do pacote p+1. Obviamente, todos os pacotes, que chegarem ao nó destino no intervalo da chegada do pacote p+3 e a nova chegada do pacote p+1, serão descartados. Quando o pacote p+1 finalmente chegar, pela segunda vez, ao nó destino ele é aceito pois está em ordem, causando, consequentemente, a alocação do buffer para o pacote p+2, continuando assim o funcionamento normal da rede. O resultado disto é que somente um pacote será entregue ao destinatário por tempo de 'round-trip' ao longo deste caminho; no caso de não ocorrerem pacotes fora de sequência a rede estaria sendo alimentada a uma taxa de

n pacotes por 'round-trip'. Observa-se que no instante que um pacote chegou fora de ordem neste fluxo, a degradação de n para 1 pacotes por 'round-trip' persistirá até que algum tipo de ação supervisora seja tomada ou até que o fluxo de tráfego cesse;

- DEFASAGEM: em uma rede típica, mais que um recurso é normalmente necessário antes que uma mensagem possa ser transmitida. Alguns destes recursos são: o número de mensagem, espaço de armazenamento no destinatário e na origem. Estes recursos podem ser distribuídos pela rede através de mensagens denominadas 'tokens'. O fenômeno da defasagem ocorre quando os 'tokens' livres se encontram disponíveis na rede a fim de possibilitar o fluxo de mensagens mas o conjunto de 'tokens', necessários para que isto ocorra, não se encontra sempre disponível em todos os locais da rede. O atraso em obter estes 'tokens' representa uma degradação.

II.5.1.b - Bloqueios:

Bloqueio ('deadlock') pode ser definido como sendo uma situação desagradável na qual dois (ou mais) processos competidores possuem, cada um deles, um subconjunto de seus recursos necessários; nenhum pode prosseguir até que um deles possua algum recurso adicional que está, atualmente, alocado ao outro processo e nenhum dos processos envolvidos está disposto a liberar algum recurso que esteja alocando. O bloqueio é um dos problemas mais sérios de uma rede devendo se tomar vários cuidados que permitam evitá-los.

Passaremos agora a discutir alguns dos tipos possíveis de bloqueios ocorridos nas redes de comutação.

- BLOQUEIO DIRETO DO ARMAZENA-E-ENVIA: Ocorre no caso em que dois nós adjacentes de uma rede estão com seus conjuntos de buffers completamente lotados com pacotes

que esperam ser enviados para o nó adjacente;

- BLOQUEIO INDIRETO DO ARMAZENA-E-ENVIA: ocorre quando situações desfavoráveis de tráfego em uma topologia de anel - apesar deste tipo de bloqueio poder ocorrer em outras topologias - cada um dos nós está com seu conjunto de buffers completamente lotado com pacotes que devem ser enviados para um nó dois ou mais nós a frente (ver /GERLM80/)

- BLOQUEIO CAUSADO PELO REEMPACOTAMENTO: ocorre quando as mensagens multi-pacotes não podem ser recompostas no nó de destino devido a rede estar congestionada impedindo que os pacotes restantes que compõem a mensagem cheguem ao nó onde está se realizando o reempacotamento. Pode-se reconhecer neste tipo de bloqueio duas situações. A primeira, é causada pela adoção de uma estratégia falha para a alocação dos buffers, pode causar que o conjunto inteiro de buffers seja preenchido com mensagens multi-pacotes incompletas à espera de reempacotamento. Esta deficiência pode ser eliminada pela adoção de um esquema de pré-alocação ou de reserva dos buffers utilizados para o reempacotamento. A segunda situação ocorre quando a tarefa de reempacotamento das mensagens multi-pacotes em um determinado nó não pode ser completada porque todos os buffers destinados a esta tarefa no nó N estão ocupados ou reservados à espera dos pacotes restantes. Os nós vizinhos a N estão ocupados com pacotes que devem ser enviados para o nó N, mas estão impedidos de prosseguir pois não existe espaço ou reserva neste nó. Nesta situação, os nós vizinhos ao considerado evitam que os pacotes restantes, necessários para o término da tarefa de reempacotamento, cheguem ao seu destino.

- BLOQUEIO DEVIDO À CONFIRMAÇÃO POR CARONA: ocorre quando é adotado um procedimento de se transmitir a confirmação dos pacotes recebidos junto com os pacotes a serem transmitidos, isto é, de carona ('piggybacking'). Neste

caso, a seguinte condição pode ocorrer: uma cadeia de pacotes dirigida para um determinado nó N com as confirmações de recebimento dos pacotes anteriormente transmitidos por N, está impedida de chegar ao nó N por não haver buffer disponível no nó N, porque todos os buffers estão ocupados com pacotes que estão à espera da chegada das confirmações a fim de serem liberados.

- BLOQUEIO DEVIDO A UM ESQUEMA RÍGIDO DE PRIORIDADES DE TRÁFEGO: ocorre quando o procedimento de armazena-e-envia adota um esquema rígido de prioridades na escolha do pacote a ser transmitido. Exemplificando: os pacotes de uma determinada rede são divididos quanto a prioridade em duas classes: uma de maior prioridade - os pacotes de diálogo - e uma outra de menor prioridade - os pacotes normais. No caso da rede transmitir preferencialmente os pacotes de maior prioridade, pode levar a uma falta de transmissão dos pacotes normais e, no caso extremo, conduzir a um bloqueio dos pacotes de maior prioridade. Isto ocorre, porque estes não podem ser enviados para os nós vizinhos, devido ao fato destes estarem ocupados com os pacotes normais que só deverão ser liberados após a chegada de mais pacotes normais, (por exemplo, pacotes remanescentes de uma mensagem multi-pacote). Medidas razoáveis para se solucionar este problema são a de se evitar o esquema de prioridades ou a de se reservar buffers destinados para estas mensagens de maior prioridade.

- BLOQUEIO NO INSTANTE DO ESTABELECIMENTO DO CIRCUITO VIRTUAL: este é um tipo especial de bloqueio do armazena-e-envia que só ocorre em redes que fornecem circuitos virtuais como serviço. Estas redes necessitam alocar os recursos necessários para uma determinada chamada virtual em todos os nós envolvidos neste circuito. Se os circuitos virtuais forem estabelecidos no instante da geração do sistema, não há problemas. Mas, no caso deles serem estabelecidos dinamicamente, pode ocorrer uma situação similar a um bloqueio que

ocorre na fase de transmissão de dados. Neste caso, deve-se adotar a rejeição do pedido de estabelecimento da conexão, pura e simplesmente, por falta de disponibilidade de recursos.

- BLOCAGEM ESTATISTICA: não chega a ser um bloqueio no sentido restrito da palavra mas, os seus efeitos são similares. Um exemplo típico ocorre quando são dispensados todos os métodos de controle de fluxo e de congestionamento em favor de um esquema de rejeição e de retransmissão dos pacotes quando não houver buffers disponíveis. Foi confirmado por estudos de simulação que a vazão total da rede decresce rapidamente, se ela estiver com um número excessivo de pacotes destinados a todos os nós. Embora, estes não estejam bloqueados, o efeito é similar porque eles provavelmente estariam bloqueados se não fossem descartados.

II.5.2.c - Alocação de buffers:

Os buffers utilizados por uma transmissão de um pacote podem ser controlados por quatro métodos que serão descritos a seguir.

- DESCARTAR: neste caso, o nó origem mantém uma cópia de cada pacote enviado para a rede e esta cópia é utilizada para controlar o fluxo nó a nó. Sempre que um nó intermediário encontrar um estado de congestionamento (por exemplo, descobre que não possui buffers disponíveis para o pacote que chega) ele simplesmente descarta o pacote, cabendo ao nó de origem providenciar a retransmissão. A principal vantagem desta técnica é o fato dela dissipar completamente o congestionamento pela remoção de todos os pacotes bloqueados da área congestionada, eliminando com isto a possibilidade de regressão do congestionamento (isto é, que o congestionamento passe a afetar os nós anteriores) que

irá causar um problema global mais sério, provavelmente um bloqueio. Dois problemas específicos podem ocorrer ao se utilizar esta técnica: os bloqueios diretos e indiretos do armazena-e-envia. Existem várias desvantagens na utilização deste método relacionadas principalmente com a eficiência da rede. Se o nó origem necessitar retransmitir o pacote ele estará usando duas ou mais vezes a capacidade do canal do que normalmente. Comparado com o método Recusar, o próximo a ser visto, este método utiliza a capacidade de todas as linhas até o ponto de congestionamento, ao invés de utilizar somente a capacidade do canal congestionado, além de utilizar mais buffers devido ao grande intervalo de tempo decorrido antes da chegada da confirmação. Além disto tudo, existe a questão do intervalo de tempo para a retransmissão ('timeout'), isto é, o nó origem deve determinar quando retransmitir a sua cópia. A retransmissão prematura pode ser desnecessária, pois o pacote ainda pode estar em trânsito, e a retransmissão após o tempo correto irá causar grandes e desordenados intervalos na entrega dos pacotes. Mesmo se o nó origem sabe que o pacote está bloqueado e que foi descartado (via uma mensagem de controle) não é desejável que o processo de retransmissão seja automático, porque o congestionamento pode persistir e o pacote não deve tentar reentrar na área congestionada imediatamente. Este método causará maiores sobrecargas (' overheads') na medida em que o congestionamento crescer. Esta opção deve ser utilizada raramente, cabendo aos mecanismos de roteamento prover o controle do congestionamento na maior parte do tempo.

- RECUSAR: similar ao anterior, somente que a cópia do pacote é mantida no nó adjacente. Ao invés de descartar o pacote, o nó intermediário não aceita o pacote de seu vizinho, cabendo a este nó a tarefa de retransmissão. A maior vantagem deste método sobre o anterior é que, o controle sendo local ao problema, possibilita que a resposta seja mais rápida e precisa. Os problemas

mencionados para o método anterior, especialmente a ineficiência da retransmissão e a dificuldade na atribuição do intervalo de tempo após o qual o pacote deve ser retransmitido, permanecem verdadeiras. Entretanto, os problemas são menores devido ao fato da retransmissão ser local, existindo uma variação menor no tempo. Por outro lado, é permitido ao tráfego retornar através da própria rede, podendo inclusive influenciar diretamente o congestionamento.

- ALOCAR: esta opção é baseada no princípio de se obter um buffer no próximo nó antes do envio do pacote se efetuar. Como o pacote deve ser mantido no primeiro nó até que o próximo buffer esteja alocado, esta técnica tende a utilizar mais buffers do que o método anterior. Este método pode ser generalizado para o conceito de pré-alocação do espaço para os buffers ao longo de todo o percurso. Este método não apresenta nenhuma vantagem quando comparado com os anteriores pois necessita manter uma cópia do pacote em um nó até que o buffer no nó adjacente seja alocado. Enquanto este tipo de técnica é útil no protocolo origem-destino ele não é apropriado para os protocolos nó-a-nó do tipo datagrama. Este método é utilizado em redes de circuito virtual como por exemplo a TYMNET.

- GARANTIR: uma solução diferente para o problema do congestionamento da rede é de se adotar uma quantidade infinita de buffers (por exemplo, através da utilização de uma unidade de armazenamento secundária) para que se possa manter os pacotes em momentos de congestionamento, cabendo ao controle de direcionamento da rede a tarefa de manter os níveis de tráfego de uma maneira tal que o espaço em disco seja necessário somente uma fração do tempo. Esta opção é atrativa se os nós possuirem unidades de armazenamento destinadas para uma outra função. Como o armazenamento secundário estaria desocupado a garantia de buffers eliminaria completamente o bloqueio tal como o método Descartar

mas, sem causar os problemas mencionados para o primeiro método. O controle do congestionamento seria local, já que seria resolvido no próprio nó, além da recuperação do congestionamento ser mais rápida. Esta opção não é prática para a maioria das redes atuais.

II.5.3 - Níveis de Controle de Fluxo:

Em uma rede de comutação de pacotes o controle de fluxo pode ser exercido em vários níveis:

- NÍVEL DO NÓ: este nível tem como objetivo o de manter um tráfego bem comportado entre dois nós adjacentes, evitando que ocorra o congestionamento dos buffers locais e a ocorrência de bloqueios;

- NÍVEL DE ENTRADA E SAÍDA DA REDE: geralmente implementado como um protocolo entre o nó de origem e o de destino, tendo o objetivo de prevenir o congestionamento dos buffers no nó de saída da rede;

- NÍVEL DE ACESSO À REDE: o objetivo deste nível é o de controlar o acesso à rede de novos pacotes baseando-se na observação do congestionamento interno da rede;

- NÍVEL DE TRANSPORTE: este nível de controle de fluxo está relacionado ao protocolo de transporte, isto é, o protocolo utilizado para se obter uma transferência confiável de dados entre os dois anfitriões. O seu objetivo principal é o de prevenir o congestionamento dos buffers dos usuários.

Passaremos a descrever cada um destes níveis de Controle de Fluxo, mencionando alguns métodos utilizados em cada um destes níveis.

II.5.3.a - Nível do Nó:

O objetivo deste nível de Controle de Fluxo é o de prevenir o congestionamento dos buffers nos nós e suas consequências, como por exemplo, a degradação da vazão e o surgimento dos bloqueios. Este nível de controle se aplica de uma forma local, pois deve monitorar a ocupação das filas de mensagens e dos buffers em cada um dos nós, rejeitando o tráfego que se destina para o nó quando alguns dos parâmetros pré-definidos são excedidos.

Esta localidade do controle não assume, entretanto, possíveis repercussões nos pontos terminais (origem) causados pelo efeito da propagação das condições do nó congestionado para os nós origens das mensagens ('backpressure').

- Classificação dos métodos:

O esquema de Controle de Fluxo ao nível do Nó realiza um papel de árbitro entre as várias classes de tráfego que estão competindo por um buffer em cada um dos nós.

Entende-se por classe de tráfego a sub-divisão que é efetuada no tráfego total que chega ao nó. Os métodos de Controle de Fluxo deste nível podem ser classificados pela maneira pela qual o tráfego é sub-dividido em classes. Estes podem ser classificados em:

- LIMITE DA FILA DO CANAL: distingue o tráfego que chega ao nó baseado na fila de saída para o qual este deve ser dirigido. Logo, o número de classes é igual ao número de filas de saída; o algoritmo de controle deve supervisionar a alocação dos buffers destinados para as diversas filas de saída. Algum limite de ocupação dos buffers deve ser definido para cada uma destas filas; este limite pode ser pré-fixado ou ajustado dinamicamente.

- CLASSES DE BUFFERS: distingue os pacotes que chegam ao nó baseados no contador de nós, isto é, o número de ligações da rede que foram percorridas até chegar ao nó considerado. Isto implica que cada nó deve controlar N-1 classes de tráfego (onde N é igual ao número de nós da rede), alocando um número de buffers, fixo ou ajustável, para cada uma das classes de buffers. Observe que nenhum caminho da rede pode passar por mais de N-1 nós.

- CIRCUITO VIRTUAL AO NÍVEL DO NÓ: aplicável em redes do tipo circuito virtual. Distingue o tráfego de acôrdo com o número do circuito a que está associado. Assume que cada nó pode distinguir os pacotes que chegam ao nó baseado no circuito virtual a que pertencem, mantendo um número de classes igual ao número de circuitos virtuais que estão atualmente passando pelo nó. Observe que o número de classes pode variar com o tempo, porque os circuitos virtuais são criados e liberados dinamicamente, diferentemente dos outros métodos onde o número de classes é função da topologia adotada. Após a criação de um determinado circuito virtual é alocado para este um conjunto de buffers (fixo ou variável) em cada um dos nós. Quando o conjunto de buffers de um determinado nó estiver sendo totalmente utilizado passa-se a rejeitar o tráfego proveniente deste circuito virtual até que a situação se normalize.

Detalhando-se os métodos tem-se:

II.5.3.a.1 - Limite da fila do Canal:

Nesta estratégia uma determinada classe de tráfego corresponde a uma determinada fila de saída do nó, havendo restrições quanto ao número de buffers que cada classe pode utilizar. Considerando que:

B = tamanho da área reservada para os buffers
N = número de filas de saída
n(i) = número de pacotes na i-ésima fila
Bmax = tamanho máximo permitido para a fila , tipicamente Bmax > B/N
Bmin = tamanho mínimo para a fila que é alocado e garantido para cada uma das filas, tipicamente: Bmin é menor ou igual a B/N

pode-se definir asseguintes estratégias:

1) Particionamento Completo:

A área de buffers é dividida igualmente entre as diversas classes, sendo que o tamanho da fila de saída não pode exceder a este limite. Isto é:

Ø <= n(i) <= B/N para qualquer i

2) Compartilhamento com filas máximas:

O conjunto de buffers é compartilhado pelas diversas filas com as seguintes restrições:

- o tamanho da fila de saída não pode exceder a Bmax;

- o somatório dos tamanhos das diversas filas de saída não pode exceder ao tamanho do 'pool' de buffers;

3) Compartilhamento com alocação mínima:

O conjunto de buffers é compartilhado pelas diversas filas com a restrição de que o somatório dos excessos de buffers ocupados por cada fila não exceda ao tamanho da área disponível de buffers. Isto é:

Somatório Máximo (Ø, n(i)-Bmin) <= B- N * Bmin

onde Máximo é a função que calcula o maior de 2 números.

4) Compartilhamento com alocação mínima e fila máxima:

Combinação dos métodos 2 e 3 acima descritos.

As opções acima assumem que os parâmetros de limitação de buffers são fixos no decorrer do tempo e os mesmos para todas as filas. Estas opções podem ser sofisticadas pela introdução da possibilidade dos parâmetros variarem dinamicamente no tempo e de fila para fila baseado na flutuação do tráfego.

Baseado em vários resultados publicados, pode-se afirmar que o controle de fluxo do tipo limite da fila do canal é necessário para se evitar a degradação na vazão, a má distribuição dos recursos e o bloqueios do armazena-e-envia pois todas as vistas fornecem a proteção mínima necessária.

O esquema mais seguro, por razões de melhor distribuição dos recursos, é o compartilhamento com alocação mínima e fila máxima utilizado na ARPAnet.

II.5.3.a.2 - Classes de buffers:

Nesta estratégia, também denominada de Conjunto Estruturado de Buffers, os pacotes, que chegam a um determinado nó, são divididos em classes de acôrdo com o número de ligações por eles atravessadas. Por exemplo, os pacotes que chegam a um nó provenientes do anfitrião pertencem a classe Ø (zero) deste nó, pois eles não percorreram nenhuma ligação. A classe mais alta, Hmax, corresponde aos pacotes que percorreram Hmax ligações, aonde Hmax é o número máximo de ligações que um pacote pode percorrer, sendo, portanto, uma função da topologia e do algoritmo de encaminhamento. Na classe Hmax estão também incluídos os pacotes que já chegaram a seu destino e estão sendo reagrupados em mensagens antes de

serem despachados para o anfitrião.

Cada classe de buffers tem o direito de utilizar um subconjunto bem definido do conjunto total de buffers. A classe Ø só pode acessar os buffers disponíveis no subconjunto reservado para esta classe. Este subconjunto deve ser grande o suficiente para armazenar a maior mensagem possível de ser transportada pela rede.

A classe i + 1 pode utilizar todos os buffers disponíveis da classe i mais um buffer adicional. Finalmente, a classe Hmax pode acessar todos os buffers disponíveis para a classe Hmax-1 mais um número suficiente de buffers para recomposição da maior mensagem que pode ser transportada pela rede.

Sob condições normais de tráfego somente o subconjunto Ø de buffers é utilizado. Quando a carga aumenta, os buffers são preenchidos progressivamente do nível Ø até o nível Hmax.

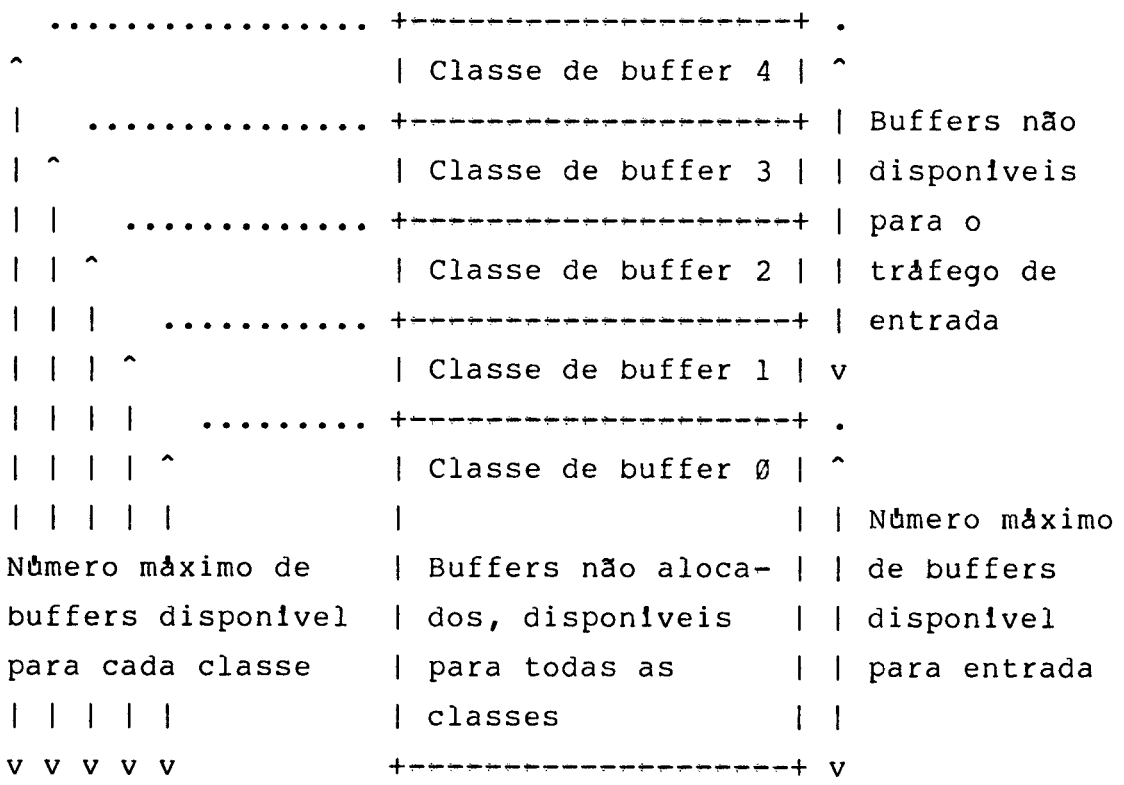


Figura II.16 - Conjunto estruturado de buffers

Quando em um determinado nó os buffers de níveis menores ou igual ao nível i estiverem ocupados, os pacotes que tiverem percorrido no máximo i nós são descartados. Logo, em caso de congestionamento, os pacotes mais recentes são rejeitados, dando-se preferência aos pacotes mais antigos, pois estes estão utilizando há mais tempo os recursos da rede.

Este método previne a ocorrência de bloqueios do tipo direto e indireto.

II.5.3.a.3 - Controle de Fluxo do tipo Circuito Virtual:

O princípio básico de operação desta estratégia é o de se fixar um limite, digamos Max, para o número máximo de pacotes para cada circuito virtual. Este limite pode ser fixado no momento da conexão do circuito virtual ou pode ser ajustado dinamicamente, baseado nas flutuações do tráfego. O limite de buffers Max é obedecido em cada nó pelo protocolo do circuito virtual ao nível do nó que controla a transmissão pela utilização de créditos, rejeitando os pacotes baseados na ocupação dos buffers.

A vantagem deste método sobre os anteriores é o de fornecer uma recuperação mais rápida e eficiente do congestionamento pela parada seletiva dos circuitos virtuais que estão influenciando diretamente a área congestionada. Esta parada é obtida pelo efeito já descrito de 'backpressure': o controle é transferido da área congestionada para todos os nós origens que estão contribuindo para o congestionamento, reduzindo, ou mesmo congelando, as entradas problemáticas, não perturbando as outras fontes de mensagens que não estão contribuindo para o congestionamento. Sem este controle, o congestionamento iria gradualmente se espalhar pela rede, afetando as fontes de tráfego que não são diretamente responsáveis pelo congestionamento original, causando, consequentemente, uma degradação na vazão e uma má utilização dos recursos da rede.

Como nos métodos anteriores, várias políticas de compartilhamento de buffers podem ser propostas. Em um dos extremos, Max buffers podem ser dedicados a cada um dos circuitos virtuais no instante do estabelecimento da conexão e no outro extremo, os buffers podem ser alocados de um conjunto de buffers por demanda na base de um compartilhamento total.

Observa-se, facilmente, que a dedicação dos buffers proposta no primeiro método pode conduzir a uma extraordinária sobrecarga de armazenamento, por causa da inexistência de um

limite superior no número de circuitos virtuais que podem coexistir em uma rede. Outro motivo para isto ocorrer é devido a característica do tráfego em cada um dos circuitos virtuais ser de rajadas, conduzindo a uma sub-utilização dos buffers alocados.

A política de compartilhamento, quando comparada com a política de buffers dedicados, pode causar um impacto nas propriedades de prevenção de bloqueios deste esquema. Com a dedicação dos buffers, este esquema se torna livre de bloqueios, o que não ocorre no método de compartilhamento total.

II.5.3.b - Nível de entrada e saída da rede:

O principal objetivo do controle de fluxo do fim a fim é o de prevenir o congestionamento dos buffers no nó de saída da rede devido ao fato dos nós origens estarem gerando um tráfego em taxas superiores as que podem ser aceitas pelos destinatários. A causa do engarrafamento pode ser devido à sobrecarga das linhas locais que conectam o nó de saída aos anfitriões ou a uma baixa taxa de aceitação dos computadores anfitriões. O problema da prevenção do congestionamento no nó de saída se torna mais complexo quando este nó deve também realizar a tarefa de reconstituição dos pacotes nas mensagens originais e/ou resequenciamento das mensagens. De fato, os bloqueios devido ao reempacotamento e resequenciamento podem ocorrer, requerendo medidas especiais de prevenção.

Vários esquemas podem ser utilizados para prevenir estes tipos de bloqueios. Na ARPAnet, por exemplo, os bloqueios causados pelo reempacotamento são evitados pela necessidade de haver uma reserva de espaço para os buffers destinados a esta tarefa, válida para cada mensagem multi-pacote que entra na rede; o bloqueio devido ao resequenciamento é evitado pela rejeição das mensagens fora de sequência no destinatário. Outras redes, por exemplo TELENET, possuem um espaço nodal

suficiente para permitir que as mensagens fora de sequência possam ser aceitas, apesar de poderem ser descartadas posteriormente no caso de haver um congestionamento de buffers (pode-se agir desta maneira por causa da existência de uma cópia da mensagem na origem).

Embora o principal objetivo deste nível de controle de fluxo seja o de proteger o nó de saída do congestionamento, obtem-se com este nível de controle um importante sub-produto que é a prevenção do congestionamento global, isto é, interno à rede.

Basicamente, todos os tipos de controle neste nível são baseados no método da janela, descrito a seguir. Suponha que o campo do cabeçalho Número de Sequência (utilizado para se identificar cada um dos pacotes transmitidos) permita que a variação deste número seja de Ø a n-1. Assume-se que o transmissor não pode enviar mais de w pacotes sem ter recebido a confirmação dos pacotes anteriormente transmitidos. Estes w pacotes definem uma janela (vide figura II.17). Logicamente w tem que ser menor do que n.

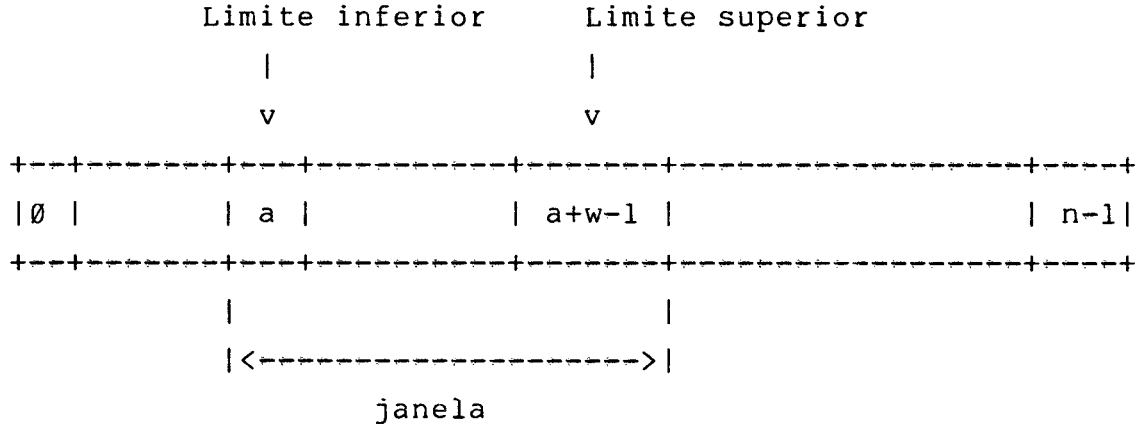


Figura II.17 - Conceito de janela

As regras que ditam o comportamento do transmissor e do receptor são as seguintes:

- Transmissor:

  - Seja L o número de sequência associado com o limite inferior da janela;

  - o transmissor envia os pacotes de número de sequência L até L+w-1;

  - após um determinado intervalo de tempo ('timeout'), ocorre a retransmissão dos pacotes não confirmados;

  - na recepção da confirmação do pacote de número de sequência igual ao limite inferior, o transmissor atualiza este limite (e consequentemente o superior).

- Receptor:

  - os pacotes que estão sendo recebidos e cujos números de sequência coincidirem com o limite inferior da janela são confirmados através do envio para a origem do próximo número de sequência esperado, podendo haver a confirmação simultânea de vários pacotes. O limite inferior é atualizado para o próximo número de sequência esperado;

  - os pacotes que estão chegando ao receptor com um número inferior ao limite inferior da janela (isto é, fora do espaço da janela) são descartados, sendo retornado para o transmissor o limite inferior atual;

  - os pacotes recebidos cujos números de sequência estão dentro dos limites da janela mas não coincidem com o limite inferior, podem ser mantidos ou descartados, conforme a implementação, mas não podem ser confirmados. Este é o caso em que os pacotes chegam fora de ordem.

As seguintes observações podem ser feitas a respeito deste método:

- todos os cálculos com números de sequência e com os limites da janela devem ser feitos módulo n (isto é, o pacote Ø segue o pacote n-1);

- o tamanho da janela (w) deve ser menor do que n/2, senão uma retransmissão pode aparecer para o receptor como uma nova transmissão, por exemplo, no caso em que o receptor tenha aceito uma janela completa de pacotes mas, todas as confirmações foram perdidas;

- o receptor pode armazenar ou descartar os pacotes que estão chegando com números de sequência que não coincidirem com o limite inferior. Logo, na implementação mais simples, o receptor não necessita armazenar mais que um pacote por fluxo de mensagens quando o espaço reservado para os buffers for crítico;

- pode haver a confirmação simultânea de vários pacotes;

- se o receptor aceitar os pacotes com número de sequência válido, isto é, estão contidos na janela mas, não coincidem com o limite inferior, o envio de uma confirmação com o número de sequência igual ao limite inferior pode estimular a retransmissão desnecessária do pacote.

O método da janela pode ser considerado como sendo uma variante do método Isarítmico, no caso em que este controle não é aplicado na rede como um todo, mas sim, entre dois anfitriões ou entre dois processos.

O método de créditos previne o congestionamento dos buffers do destinatário, além de fornecer indiretamente uma proteção global contra o congestionamento da rede.

II.5.3.c - Nível de acesso à rede:

O objetivo deste nível de controle de fluxo é o de congelar as solicitações de acesso à rede externas baseado em medições do congestionamento interno da rede. Estas medições podem ser locais (por exemplo, ocupação dos buffers), globais (por exemplo, o número total de buffers disponíveis em toda a rede) ou seletivos (por exemplo, o congestionamento dos caminhos que vão até um determinado destino). A condição de congestionamento é determinada (ou informada) pelos pontos de acesso à rede sendo utilizada para regularizar o acesso à rede do tráfego externo.

Este nível de controle de fluxo difere dos anteriores no aspecto dele estrangular o tráfego externo com o intuito de prevenir o congestionamento total dos buffers internos, enquanto que o controle de fluxo ao nível do nó limita o acesso a um nó específico com a intenção de prevenir o congestionamento local e os bloqueios do armazena-e-envia. O controle de fluxo fim-a-fim limita o fluxo entre um par origem e destino específico a fim de prevenir o congestionamento e os bloqueios causados pelo reempacotamento no destino.

Como foi mencionado anteriormente, os controles de fluxo ao nível do nó e o fim-a-fim atuam indiretamente como uma forma de controle de acesso à rede. Isto se deve ao fato destes reportarem aos pontos de acesso o estado de congestionamento da rede, através do mecanismo, já visto, de 'backpressure' (nos esquemas ao nível do nó) ou pelo retardo do crédito causado por grandes atrasos internos (fim a fim).

As seguintes implementações podem ocorrer:

- Isarítmico: esquema de prevenção global do congestionamento baseado na circulação pela rede de um número fixo de permissões para a transmissão;

- Limite de buffers de entrada: esquema local de prevenção

do congestionamento que atribui um limite no número de novos pacotes em cada um dos nós;

- 'Choke packet': esquema seletivo de prevenção do congestionamento baseado no envio de pacotes especiais de controle do nó congestionado para os nós origens.

Detalhando estes métodos temos:

II.5.3.c.1 - Isarítmico:

Desde que a principal causa do congestionamento de uma rede é o número excessivo de pacotes nela armazenados, um método intuitivo de prevenção do congestionamento é o de se limitar o número total de pacotes que podem circular pela rede em um determinado instante.

Este esquema é baseado no conceito de permissão para transmitir, isto é, um "bilhete" que autoriza um pacote ir de um determinado ponto de acesso até o seu destino. Dentro deste conceito, a rede inicialmente possui um número de permissões ou créditos distribuídos pelos diferentes nós. Como o tráfego é oferecido por um anfitrião à rede, cada pacote deve assegurar uma permissão antes que sua admissão seja autorizada. Cada pacote que é aceito causa uma redução unitária no estoque de permissões disponíveis no nó que aceitou este pacote. O pacote que foi aceito pela rede está apto para percorrer a rede. Quando o pacote estiver sendo manipulado pelo destinatário, a permissão que o acompanhou se torna livre, aumentando com isto o estoque de permissões neste nó.

Para se obter um sistema viável, no qual as permissões não fiquem acumuladas em certas partes da rede, prejudicando outras regiões da rede, se torna necessário estabelecer um limite no número de permissões que podem ser mantidas em estoque por cada um dos nós. Se por causa deste limite uma

permissão recentemente liberada não puder ser estocada no nó, ela deve ser enviada para algum outro nó, através do envio desta permissão por uma mensagem de dados ou de controle. Somente na ausência de outro tipo de tráfego será necessário criar-se um pacote especial para o transporte da permissão.

Simulações efetuadas pelo 'National Physical Laboratory', com o intuito de avaliar a eficiência deste esquema em várias configurações de redes, demonstraram que este método é um mecanismo simples de prevenção do congestionamento, funcionando muito bem em condições uniformes de tráfego, mas podendo conduzir a um decréscimo na vazão e a uma eficiência inferior no caso de haver padrões de tráfego não uniformes e variantes com o tempo. Em particular, na presença de transferência de dados em altas taxas existe a possibilidade das permissões não retornarem rapidamente ao ponto de origem do tráfego, impedindo por isto a plena utilização dos recursos da rede. Isto ocorre quando o nó destinatário redistribui os créditos de uma forma randômica pela rede. Se por outro lado, o destinatário sistematicamente retorna para o nó de origem os créditos recebidos, este par origem e destino pode ficar com a maioria dos créditos, resultando em uma má distribuição dos recursos.

Apesar destas restrições, o esquema isarítmico provou ser bastante efetivo em redes fracamente controladas (basicamente, redes sem o tipo de controle ao nível da ligação), eliminando o congestionamento e os bloqueios que teriam ocorrido sem a presença de um controle. Em redes fortemente controlada (redes com o controle de fluxo ao nível da ligação, especialmente o LFC) e com uma forma simples de controle do acesso (um buffer em cada uma das filas de saída foi reservado para o tráfego do armazena-e-envia), observou-se que as redes não apresentavam sinais de congestionamento, mesmo no caso de não haver o controle isarítmico e o encaminhamento ser fixo.

Quando a disciplina de encaminhamento foi modificada para adaptativa, observou-se que a rede se tornava facilmente

congestionada porque o controle implementado não prevenia o fato de que o tráfego externo poder ocupar todas as filas no nó de entrada. Com a introdução do esquema isarítmico, eliminou-se o congestionamento neste caso.

Os parâmetros críticos no esquema isarítmico são:

- número total de créditos ou permissões -P- na rede;

- número máximo de permissões -L- que podem ser acumulados em um determinado nó (fila de permissões).

Resultados experimentais mostram que a eficiência ótima é obtida com P=3N, onde N é igual ao número total de nós e com L igual a 3. Um número excessivo de créditos na rede conduzem ao congestionamento; e um número excessivo de créditos que podem ser acumulados em um nó conduz a uma má distribuição de recursos.

II.5.3.c.2 - Limite do buffer de entrada:

Este método é baseado na diferenciação entre o tráfego proveniente de pontos externos à rede e o tráfego interno à rede. O controle do tráfego externo é feito baseado na ocupação dos buffers no nó de entrada. Este é um método de controle de acesso à rede local porque monitora o congestionamento local ao nó de entrada ao invés do congestionamento global, como acontece no método isarítmico. O nível de congestionamento no nó de entrada à rede é um bom sinal do nível de congestionamento global por causa dos efeitos de 'backpressure' que propagam as condições de congestionamento interno da rede para os nós origens de tráfego.

A função deste controle é o de bloquear o tráfego que chega à rede quando certos limites de utilização dos buffers foram atingidos no nó de acesso à rede. Este método de

controle de fluxo favorece claramente o tráfego em trânsito em detrimento do tráfego que chega à rede. Aceita-se este fato em razão de já ter-se destinado uma parte dos recursos da rede para o tráfego em trânsito.

Várias versões deste controle podem ser propostas. Passaremos a discutir algumas destas versões.

O têrmo Limite de Buffer de Entrada foi inicialmente introduzido pelo GMD (GMD- Gesellschaft fur Mathematik und Datenverarbeitung, instituto de pesquisas alemão). O esquema adotado para a GMDNET é um subproduto do método de controle de fluxo ao nível do nó do tipo Conjunto de Buffers Estruturado. Recordando este método, a i-ésima classe de tráfego consiste de todos os pacotes que já percorreram i nós. A classe zero (nenhum nó percorrido) é destinada ao tráfego que chega à rede. Esta classe de tráfego utiliza os buffers da classe zero que é um subconjunto do 'pool' de buffers do nó (geralmente, para a i-ésima classe são destinadas todas as classes de buffers menor ou igual a i). Quando a classe zero estiver ocupada, o tráfego que chega à rede passa a ser descartado. A definição do tamanho destinado aos buffers da classe zero -denominado limite do buffer de entrada- tem um impacto significante na eficiência em têrmos de vazão em condições de saturação da rede. Simulações demonstraram que para uma dada topologia e um dado padrão de tráfego existe um limite do buffer de entrada ótimo, que maximiza a vazão.

Uma outra versão mais simples deste método foi proposto por Lam. Nesta versão somente duas classes de tráfego -de entrada e em trânsito- são consideradas. Seja N(T) o número total de buffers no nó e N(I) o limite do buffer de entrada (obviamente N(I) menor ou igual a N(T)). As seguintes restrições podem ser impostas a cada um dos nós:

- o número de pacotes que chega à rede tem que ser menor ou igual a N(I);

- o número de pacotes em trânsito tem que ser menor ou

igual a N(T).

II.5.3.c.3 - Pacote de Congestionamento ('Choke Packet'):

O esquema de pacote de congestionamento, proposto para a rede Cyclades, é baseado na noção de congestionamento da ligação e do caminho. Uma ligação é dita congestionada se a sua utilização exceder a um determinado limite (por exemplo, 80% da capacidade). Um caminho está congestionado se qualquer uma de suas ligações está congestionada. A informação de congestionamento do caminho é propagada pela rede junto com as informações de direcionamento, permitindo que cada um dos nós conheça o estado de congestionamento de cada uma de suas ligações.

Quando um nó recebe um pacote, que deve ser dirigido para o destino através de um caminho que esteja congestionado, as seguintes ações podem ser tomadas:

- se o pacote fôr um pacote de entrada (isto é, proveniente do anfitrião), então o pacote é abandonado;

- se o pacote é um pacote em trânsito, ele é enviado pelo caminho, mas um pacote de congestionamento (pacote de controle) é enviado para o nó origem, informando que o caminho para o destinatário está congestionado, requerendo que os pacotes subsequentes de entrada para este destinatário sejam bloqueados. O caminho é gradualmente liberado se nenhum pacote de congestionamento for recebido durante um determinado intervalo de tempo.

Observe que este método tenta beneficiar o tráfego em trânsito em detrimento do tráfego de entrada, da mesma maneira que o método do Limite de Buffers de Entrada. A diferença básica entre estes métodos é o fato do método Limite de Buffers utilizar somente medidas locais de congestionamento,

enquanto que o método do pacote de congestionamento utiliza a medida do congestionamento do caminho, possibilitando um controle de fluxo seletivo do tráfego de entrada que é dirigido para os vários usuários.

II.5.3.d - Nível de Transporte:

O protocolo de transporte (ver seção II.6.5) é um conjunto de regras que governam as transferências de controle e de dados entre os anfitriões da rede. As funções principais deste protocolo são a de transmitir as informações de uma forma confiável e eficiente e o compartilhamento dos recursos da rede pelas várias sessões de usuários.

Para uma reconstituição das mensagens eficiente e confiável no anfitrião de destino, o protocolo de transporte deve assegurar que as mensagens que estão chegando ao destinatário disponham de um espaço adequado para os buffers. A função do protocolo de transporte que previne o congestionamento dos buffers no destinatárioa é conhecida como o Controle de Fluxo do nível de Transporte.

Geralmente, este tipo de controle é baseado em um sistema de créditos (ou janela) já discutido anteriormente. Em resumo, o receptor envia os créditos de transmissão para a origem, assim que os buffers utiliados para o reempacotamento sejam liberados. Após a recepção de um crédito o transmissor está autorizado a transmitir uma mensagem de tamanho pré-determinado. Quando os buffers destinados ao reempacotamento ficarem completos, nenhum crédito será enviado para o transmissor, parando, temporariamente, a transmissão de novas mensagens.

O esquema de créditos descrito acima é vulnerável a perdas de mensagens, pois basta a perda de um crédito para paralisar uma conexão. De fato, o transmissor pode esperar indefinidamente por um crédito perdido, enquanto que o

receptor está esperando por uma mensagem. Um método de controle de fluxo melhor é obtido pela numeração dos créditos relativos às mensagens que estão sendo enviadas para a direção oposta. Neste caso, cada crédito carrega um número de sequência, N, e o tamanho da janela, w. Ao receber o crédito, o transmissor é autorizado a enviar mensagens até o número de sequência N+w. Com o crédito numerado, se uma mensagem de crédito fôr perdida não ocorre o efeito anteriormente descrito, pois a próxima mensagem de crédito restaurará a situação.

Além de prevenir o congestionamento dos buffers do destinatário, o esquema de crédito também contribui, ainda que indiretamente, para fornecer uma proteção contra o congestionamento global da rede. De fato, o congestionamento dos buffers do armazena-e-envia nos nós intermediários causarão um atraso na chegada de créditos para o transmissor, retardando com isto o envio de novas mensagens.

II.5.4 - Interações entre os controle de Rota e de Fluxo /MCQUJ79/, /GERLM80b/:

II.5.4.a - Influências do controle de rota sobre o de fluxo:

Ao se projetar um algoritmo para controle de rotas, uma das perguntas que devem respondidas inicialmente é a seguinte: Qual será o objetivo do Controle? ou, O que se espera obter com o controle de rotas?.

Dentre os objetivos possíveis de serem escolhidos, destacam-se:

- maximizar a vazão;

- minimizar o atraso;

- minimizar a probabilidade de ocorrência de bloqueios;

- maximizar a relação vazão/atraso;

- maximizar a função da média ponderada da vazão e do atraso.

Qualquer um dos critérios de otimalidade usado no algoritmo (por exemplo, minimizar o atraso) pode ser visto como um mecanismo de se evitar o congestionamento.

Qualquer função objetivo, que preferir taxas baixas de tráfego em uma determinada ligação ao invés de taxas mais altas, contribui para se evitar o congestionamento no canal considerado, mas não necessariamente na rede como um todo. Entretanto, medidas simples, tais como a minimização do atraso médio, podem não levar em conta os altos níveis de congestionamento que podem persistir por pequenos períodos de tempo no caso de haver uma sobrecarga no tráfego. Observa-se que as funções que crescem exponencialmente, ao invés de linearmente, com o atraso, podem ser efetivas para se evitar o congestionamento, mas insuficientes para controlá-lo.

Uma outra decisão importante no desenvolvimento de algoritmos para o controle de rota diz respeito à garantia que o direcionamento conduzirá a um fluxo estável sob as mais diversas condições.

Geralmente, quanto menos estável fôr um método de roteamento mais difícil será o desenvolvimento e implementação do controle de fluxo. Discutiremos a seguir alguns problemas ocasionados pelo controle de fluxo.

Na utilização das opções de Descarte ou de Alocação para o controle do congestionamento, a decisão mais importante que deve ser tomada é como distinguir o tráfego que está contribuindo para o congestionamento e o fluxo que está sendo afetado pelo congestionamento, a fim de possibilitar a rejeição, prioritariamente, do tráfego que está causando o

problema. Em outras palavras, é essencial para o algoritmo de controle de fluxo identificar quais os fluxos de dados que diminuídos ou mesmo parados resultariam em um acréscimo geral no fluxo ou em um decréscimo no atraso ou um outro tipo de melhoria em têrmos de eficiência.

Uma possível solução para este problema é a verificação dos pacotes que se encontram enfileirados no nó, quando fôr necessário tomar-se a decisão de descartar ou rejeitar um pedido de alocação. Contudo, se torna bastante dificil decidir-se acertadamente, baseado somente na informação local, pois se a maioria dos pacotes pertencem a uma determinada ligação, isto não implica necessariamente que esta ligação esteja congestionada, mas que esta ligação está sofrendo retenções devido ao tráfego de menor frequência. Logo, um sistema puramente local não pode considerar, em têrmos globais, as causas e os efeitos do congestionamento na rede.

Pode-se concluir desta argumentação que o melhor método de direcionamento é aquele que possui informações, em cada um dos nós, que dizem respeito ao estado do tráfego entre os vários nós origens e destinos, e um procedimento que distribua esta informação de um determinado nó para os nós restantes.

II.5.4.b - Influências do controle de fluxo sobre o de rotas:

Um dos pontos principais de interação entre estes dois tipos de controle é o fornecimento da informação da rejeição de um pacote para o controle de rotas.

Uma outra ligação mais estreita entre estes dois controles ocorre quando uma sobrecarga de tráfego é detectada pelo controle de fluxo, cabendo ao controle de rotas determinar uma rota alternativa. Um outro tipo de ligação, mais frouxa, existe quando o algoritmo de roteamento estabelece uma determinada rota, cabendo ao controle de fluxo atuar, simplesmente, controlando o tráfego aceito para este

canal.

No caso do roteamento ser adaptativo, o controle de rotas pode auxiliar o controle de fluxo no cumprimento de suas tarefas, simplesmente pela divisão do tráfego por várias rotas.

Deve-se observar que para não sobrecarregar o texto dos capítulos relativos aos Controles de Rota e de Fluxo com o excesso de referências, procurou-se não explicitar as referências consultadas, cabendo ao interessado consultar a Bibliografia.

II.6 - Protocolos /TANEA81/:

II.6.1 - Introdução:

Durante os últimos dez anos, várias redes de computadores foram projetadas, implementadas e colocadas em funcionamente em praticamente todas as regiões do mundo. Da experiência obtida com estas redes vários princípios de projeto surgiram, que podem ser aplicados no desenvolvimento de novas redes, permitindo que estes projetos tenham uma forma mais estruturada do que os anteriores. O mais importante destes princípios é o de se estruturar a rede como tendo uma hierarquia de camadas, cada uma com uma função pré-determinada e utilizando os serviços das camadas inferiores a fim de prestar serviços aos níveis superiores. A International Organization for Standardization' (ISO) desenvolveu um modelo denominado ' OSI - Open Systems Interconnection' com o objetivo de constituir uma base comum para a coordenação do desenvolvimento de padrões para a interconexão de sistemas, permitindo, também, que os padrões já existentes fôssem encaixados no modelo.

Um outro propósito do modelo é o de se identificar áreas que se prestam para o desenvolvimento ou aperfeiçoamento de padrões, fornecendo uma referência comum para manter a consistência dos vários padrões relacionados.

Embora o modelo OSI possa ser utilizado em qualquer tipo de rede, algumas de suas considerações (como o roteamento) só são aplicadas em redes de grande porte. O modelo OSI desenvolveu uma estrutura hierárquica de camadas, cada uma com funções pré-determinadas e com protocolos específicos entre as camadas de mesmo nível.

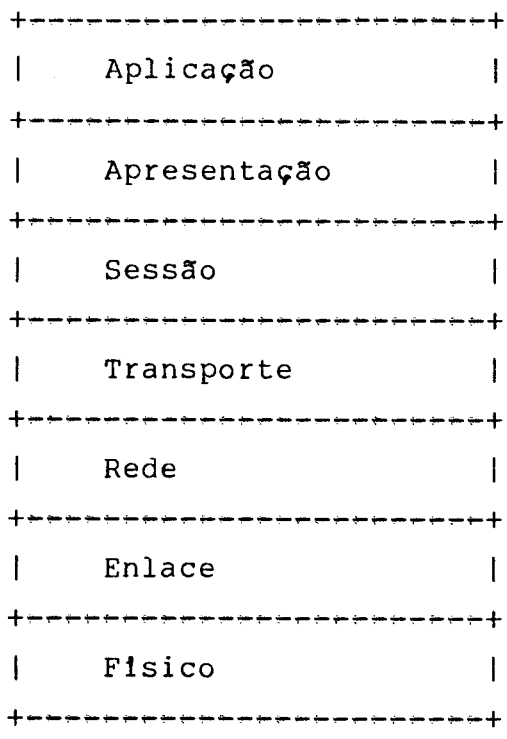


Fig. II.18 - Modelo OSI

Neste modelo são identificados sete níveis ou camadas de protocolo (vide figura II.18):

- NÍVEL FÍSICO ('Physical Layer'): define as características mecânicas, elétricas, funcionais e de procedimentos que possibilitam o estabelecimento. manutenção e liberação das conexões físicas;

- NÍVEL DE ENLACE ('Data Link Layer'): o propósito deste nível é o de fornecer os meios pelos quais seja possível converter um canal de comunicações não confiável em um meio de comunicação confiável. Isto é feito pela divisão da mensagem a ser transmitida em quadros ('frames') que são transmitidos até que sejam confirmados pelo receptor;

- NÍVEL DE REDE ('Network Layer'): também denominado de nível da subrede de comunicações, tem como tarefa o gerenciamento das operações efetuadas pela sub-rede de

comunicações. Entre outras coisas, especifica as características principais da interface anfitrião-nó e como os pacotes são encaminhados pela sub-rede;

- NÍVEL DE TRANSPORTE ('Transport Layer'): responsável pela comunicação confiável entre dois anfitriões, a de possibilitar a comunicação de processos de níveis superiores. Este nível fornece uma transferência confiável de dados, transparente aos níveis superiores, não necessitando que estes níveis conheçam de que maneira são obtidos os serviços prestados, de tal forma que uma ligação ponto-a-ponto possa ser substituída por uma ligação de satélite sem o conhecimento dos níveis superiores;

- NÍVEL DE SESSÃO ('Session Layer'): o objetivo deste nível é o de gerenciar as interações entre os processos de usuário. Para que isto seja possível, o nível de sessão fornece para os níveis superiores dois tipos de serviço: o serviço de administração da sessão que fornece os meios de união e de separação de dois processos e o serviço de diálogo que controla, delimita e sincroniza as operações de transferência de dados entre os processos;

- NÍVEL DE APRESENTAÇÃO ('Presentation Layer'): realiza as transformações (como por exemplo a compressão de dados) desejadas pelo usuário antes que estes sejam transmitidos. Efetua também as conversões necessárias que permitem a um programa interativo manipular qualquer tipo de terminal ou de arquivo;

- NÍVEL DE APLICAÇÃO (Application Layer'): constitui o nível mais alto do modelo OSI estando diretamente relacionado com o usuário final, prestando os serviços apropriados para a distribuição de informações, o gerenciamento da aplicação e do sistema. É a razão de ser dos níveis inferiores, pois estes só se justificam pelos serviços prestados a este nível.

Observa-se que o modelo OSI descreve o conceito de camadas com detalhes, introduzindo uma terminologia uniforme que permite identificar as várias entidades envolvidas. Finalmente, especifica as sete camadas já mencionadas através de uma descrição de suas funções e objetivos. Apesar disto, o modelo OSI não deve ser considerado como sendo uma definição de um protocolo mas, sim como uma metodologia para se dividir as funções executadas por uma rede e para se localizar possíveis áreas de padronização.

No restante deste sub-capítulo, baseando-se no modelo OSI, serão apresentados alguns protocolos que se aplicam em cada um dos níveis já mencionados.

II.6.2 - Nível Físico:

A função do nível físico é a de permitir que um anfitrião possa transmitir um conjunto de bits pela rede. Este nível não está relacionado à maneira pela qual os bits são organizados para formar as mensagens e nem com o significado associado a cada um dos bits enviados, não se preocupando com a possibilidade de que determinados bits sejam perdidos ou alterados, deixando os procedimentos de deteção e recuperação dos erros para os níveis superiores.

Neste nível são analisados vários aspectos relacionados à sub-rede de comunicações, tais como:

- método de comutação: circuitos ou pacotes;

- meio de transmissão: sistema telefônico, cabo coaxial, satélite, etc.;

- formas de transmissão do sinal: analógica ou digital.

Provavelmente o padrão atualmente mais conhecido para este nível é o EIA-RS-232-C que especifica o significado de

cada um dos 25 pinos do conector do terminal e os procedimentos a serem seguidos a fim de se possibilitar a transferência. Entretanto um novo padrão o EIA-RS-449 foi desenvolvido para substituir ao antigo. Este padrão é inteiramente compatível com o RS-232-C embora utilize um conector de 37 pinos.

- X.21 - Exemplo de protocolo do nível físico:

Atualmente a maioria dos padrões existentes para o nível físico utilizam a sinalização analógica, mas no futuro interfaces digitais serão necessárias. Reconhecendo esta necessidade, o CCITT desenvolveu uma interface completamente digital denominada X.21. Esta é aplicada no caso de se conectar um anfitrião a uma rede. Esta conexão permanece estabelecida enquanto o anfitrião desejar comunicar-se com a sub-rede. Consequentemente, o X.21 é um protocolo de comutação de circuitos, embora a conexão anfitrião-anfitrião possa se realizar em um canal de comutação de circuitos ou de pacotes.

Na terminologia do X.21 o anfitrião é identificado como ETD - Equipamento Terminal de Dados (DTE - 'Data Terminal Equipment') - e o nó da rede como ECD - Equipamente de Terminação do Circuito de Dados (DCE - 'Data Circuit-terminating Equipment'). A interface ETD-ECD consiste de oito linhas cada uma com os seus significados e funções associados.

Para maiores detalhes a respeito dos protocolos de nível físico recomenda-se as seguintes referências: /BERTH80/, /FOLTH80/, /TANEA81/.

II.6.3 - Nível de Enlace:

Como já foi mencionado, o nível físico não se preocupa com a detecção ou correção dos erros de transmissão. Nenhum destes protocolos preocupa-se com a possibilidade do receptor

não poder aceitar os dados da mesma forma que o trasnsmissor os está enviando. Estes problemas são resolvidos pelo Nível de Enlace.

A forma em que o nível de Enlace implementa as suas funções é baseada na divisão da cadeia de bits a serem transmitidos em quadros de tal forma que o recebimento de um quadro possa ser confirmado ou não. Uma questão óbvia que surge é a seguinte: Como delimitar os quadros?. Em outras palavras, como o receptor pode identificar o início e o término de um quadro. Este problema pode ser resolvido de três maneiras:

- contador de caracteres;

- enchimento de caracteres ('byte stuffing');

- enchimento de bits ('bit stuffing').

Com o método CONTADOR DE CARACTERES cada um dos quadros começa com um cabeçalho de formato fixo que especifica o número de caracteres que estão contidos no quadro. Logo, pelo simples processo de contagem dos caracteres recebidos o receptor pode detectar o fim do quadro corrente e o início do seguinte. Este método apresenta como desvantagens o fato de ser insensível aos erros de transmissão não detectados que por acaso afetem o cabeçalho e pela fixação de uma tamanho constante para o caractere. A tendência deste método é cair em desuso.

O segundo método, o ENCHIMENTO DE CARACTERES, delimita o fim do quadro pela presença de um caractere especial indicativo de fim de quadro. A solução para o problema da presença de um caractere indicativo de fim de quadro no meio da informação a ser transmitida é a de precedê-lo por um caractere especial (DLE) que serve para indicar que o caractere seguinte é dado e não controle. No caso deste caractere especial constar dos dados o procedimento é análogo. Este método tende a ficar obsoleto.

Os protocolos mais recentes utilizam o terceiro método: o ENCHIMENTO POR BITS. Neste método os quadros são delimitados pelo padrão de bits Ø1111110, denominado de 'flag'. Sempre que cinco bits 1 consecutivos aparecerem na mensagem um bit Ø é adicionado na cadeia de bits a ser transmitida (normalmente isto é feito pelo próprio 'hardware'). O receptor ao receber uma cadeia de 5 bits 1 consecutivos deve verificar se o bit seguinte para achar o 'flag' (no caso deste bit ser 1) ou não considerar este bit (no caso deste ser zero). Procedendo-se desta maneira impede-se que os dados do usuário interfiram na transmissão, não impondo nenhuma limitação no tamanho dos caracteres.

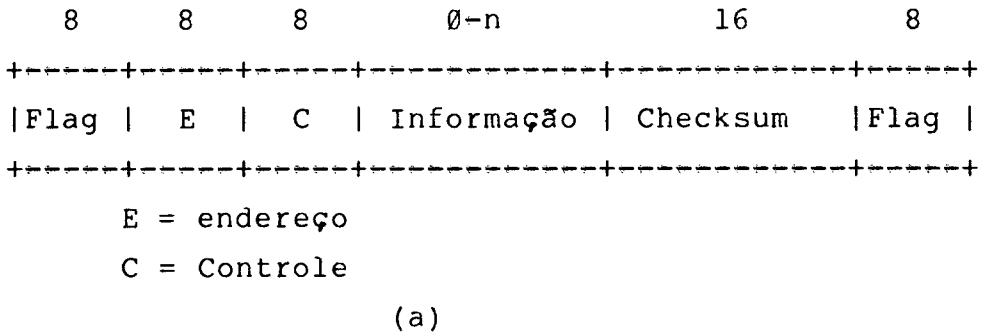
Em redes locais pode-se aplicar outro método para se detectar o início dos quadros. Isto é feito pela presença ou não de um sinal no meio de transmissão (por exemplo, cabo coaxial).

Geralmente, todos os protocolos deste nível incluem um 'checksum' no cabeçalho e/ou no final do quadro que serve para detectar os erros de transmissão. A correção normalmente não é feita porque o processo para se corrigir os dados necessitaria utilizar mais bits do que o procedimento de detecção e por causa disto é mais eficiente detectar o quadro errado e pedir a sua retransmissão. Entretanto com o crescimento do uso de satélites como meio de transmissão isto não se aplica. Neste caso, como uma das características do satélite é o grande tempo de propagação, as técnicas de correção (como o código de Hamming, ver /MUSCE79/) devem ser adotadas.

- HDLC - Exemplo de um protocolo do nível de Enlace:

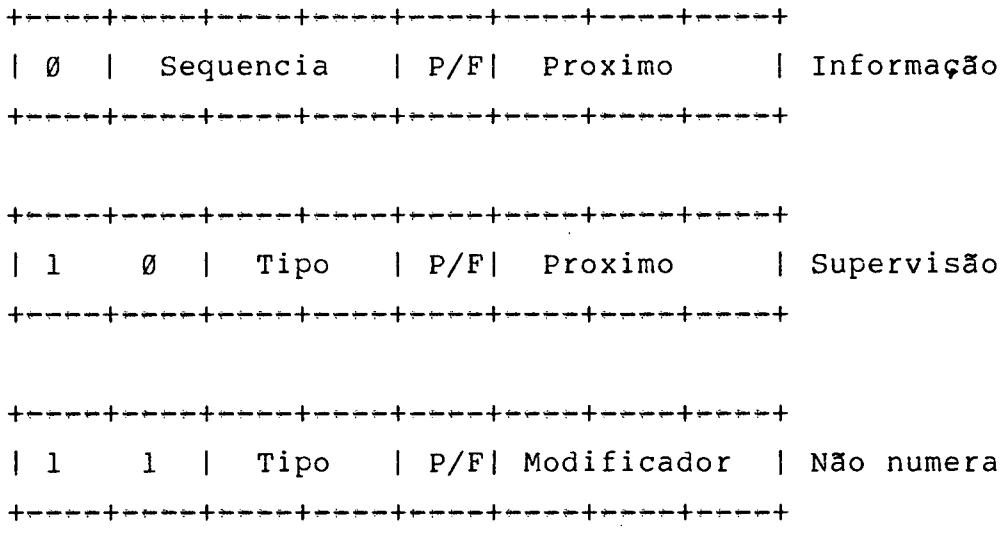
Como exemplo de um protocolo deste nível será utilizado o HDLC ('High-level Data Link Control') que é o protocolo mais usado neste nível quer pela sua utilização direta ou indireta no caso de serem adotados subconjuntos deste protocolo, como por exemplo: SDLC ('Synchronous Data Link Control'), LAP ('Link Access Protocol') e LAPB ('Link Acess Protocol Balanced').

Todos os protocolos mencionados utilizam a técnica de 'bit stuffing' para delimitar os quadros. O formato do quadro no HDLC (para maiores detalhes vide /ISO**77/, /TANEA81/) é apresentado na figura II.19.(a).



E = endereço
C = Controle

(a)



(b)

Figura II.19 -(a): Formato do Quadro
(b): Caractere de controle para os três tipos de quadro

O campo de Endereço é utilizado para identificar o destinatário da mensagem em uma linha multi-ponto. O campo de Controle é diferente para cada uma das três classes de quadro (ver figura II.19.b). Nos quadros de Informação os campos de Sequência e Próximo correspondem ao número de sequência do quadro corrente e do próximo quadro esperado, respectivamente. Quando A envia um quadro para B o campo "Sequência" é o número

do quadro que está sendo transmitido e o campo "Próximo" é a confirmação enviada para B de que A recebeu corretamente todos os quadros anteriores ao valor de "Próximo". Esta técnica é conhecida como envio da confirmação de carona ('piggybacking') que serve para aumentar a capacidade do canal por causa da transmissão de menos quadros além, de melhorar a eficiência dos nós, pois a transmissão de um menor número de mensagens significa a recepção de um menor número de mensagens e consequentemente um menor número de interrupções no receptor.

Quando não existir nenhum tráfego no sentido inverso para servir de transporte da confirmação utiliza-se para isto um quadro de Supervisão de tipo Ø. Os outros quadros de supervisão são utilizados nos casos de confirmação negativa, rejeição seletiva e de receptor não pronto temporariamente.

O bit P/F, abreviação de 'POLL'/FINAL possui os seguintes usos: indicar o último quadro de uma sequência de quadros e para "pollar" em uma linha multi-ponto.

Os quadros não numerados correspondem a uma combinação de quadros de controle, constituindo-se nas maiores diferenças dos protocolos anteriormente mencionados. A maioria destes quadros é utilizada para indicar condições de anormalidade e para o estabelecimento de ligações entre o par origem e destino.

II.6.4 - Nível de Rede:

Quando um quadro chega a um determinado nó, o nível de enlace separa do quadro a parte referente ao campo de informações, transferindo-o para o nível de Rede que é responsável pela decisão de qual caminho o pacote deve seguir para atingir o seu destino. Esta tarefa seria bem simplificada se tal decisão pudesse ser realizada sem se preocupar com a carga existente nos canais e na possibilidade de haver áreas da rede congestionadas. Estes pontos já foram apresentados em

sub-capitulos anteriores (ver II.4 e II.5).

Duas filosofias opostas podem ser aplicadas neste nível. Na maioria das redes locais e em algumas redes de longo alcance, o nível de rede presta o serviço de entrega dos pacotes da origem para o destino com uma alta probabilidade de sucesso (logicamente inferior a 1.Ø). Cada pacote é independente dos outros pacotes, devendo possuir o endereço de seu destino completo. Estes pacotes são denominados DATAGRAMAS.

A outra filosofia, seguida pelas redes públicas, necessita que a transmissão de um pacote de estabelecimento da ligação ('setup') ocorra antes que a transferência de dados se inicie. Este pacote ao percorrer a rede determina uma rota que será percorrida pelos demais pacotes e reserva os recursos necessários ao longo deste caminho. O usuário escolhe, ou lhe é fornecido, um número de identificação do circuito virtual que será utilizado para identificar o caminho a ser seguido, devendo constar de todos os pacotes subsequentes. Nesta filosofia os pacotes pertencentes a um mesmo circuito virtual não são independentes, pois devem percorrer o mesmo caminho anteriormente selecionado, possuindo como única identificação de seu destino o número do circuito virtual.

A vantagem do circuito virtual é o fato dele garantir que os pacotes serão entregues em ordem e que a prevenção do congestionamento é otimizada pela possibilidade de haver a pré-alocação de recursos e a do datagrama é por facilitar a utilização de bancos de dados. Para maiores comparações destas filosofias consulte seção II.2.5.

- X.25 - Exemplo de um protocolo do nível de Rede:

Para auxiliar a padronização das redes públicas de computadores o CCITT desenvolveu um protocolo constituído de três camadas denominado X.25 (vide nível físico consistindo na adoção do X.21, o segundo nível, o nível de enlace, é constituído de duas variantes do HDLC (LAP e LAPB) e o

terceiro nível, o de rede, será resumido a seguir.

O X.25 é um protocolo originalmente orientado para circuito virtual, embora tenha sofrido algumas extensões (/FOLTH80b/). Para se estabelecer um circuito virtual, um anfitrião (ETD) envia um pacote do tipo 'CALL REQUEST' através da rede para o destinatário remoto. Este pode aceitar ou rejeitar este pedido; em caso de aceitação é considerado estabelecida a ligação.

A figura II.20.(a) mostra o formato do pacote 'CALL REQUEST'. Os 4 primeiros bits são 0001 e os 12 seguintes constituem o número do circuito virtual determinado pelo anfitrião origem. O terceiro caractere é o código de controle do 'CALL REQUEST'. O próximo byte fornece o número de digitos dos endereços de origem e de destino, seguido de no máximo 30 caracteres contendo os endereços representados em decimal binário. O campo de Facilidade é utilizado para especificar o tipo de serviço desejado, podendo ser de tamanho variável, tamanho este especificado no campo correspondente. Finalmente, o campo de dados do usuário pode ser utilizado de qualquer maneira, como por exemplo, indicar qual é o processo no anfitrião que está esperando esta chamada.

Quando o pacote de 'CALL REQUEST' chega ao seu destino, este pedido pode ser aceito ou rejeitado. Isto é feito pelo envio do pacote mostrado na figura II.20.(b). A aceitação ou recusa do pedido é indicada pelo campo TIPO. Uma vez o circuito virtual estando estabelecido, ambos os lados estão capacitados a trocar mensagens. Qualquer um dos lados pode terminar a chamada pelo envio de um pacote 'CLEAR REQUEST' que é confirmado pelo envio do pacote 'CLEAR CONFIRMATION'.

Um pacote de dados é mostrado na figura II.20.c. Os campos de SEQUÊNCIA e de PRÓXIMO possuem o mesmo significado visto no HDLC. O bit M pode ser utilizado pelo anfitrião para indicar que serão transmitidos mais dados após este, de certa forma particionando o fluxo de pacotes em unidades multi-pacotes.

O significado do bit Q não é especificado, podendo ser utilizado pelo nível de transporte para distinguir os seus pacotes de dados dos seus de controle. O bit D é utilizado pela confirmação de entrega ('Delivery Confirmation'). Se um anfitrião atribuir-lhe o valor 1 em todos os pacotes transmitidos por um determinado circuito virtual, o campo PRÓXIMO conterá uma confirmação legítima do anfitrião remoto, fornecendo uma confirmação fim-a-fim. Se o valor deste bit for igual a Ø(zero), significa que o ECD local recebeu o pacote especificado e não o anfitrião remoto.

Como as camadas 2 e 3 do X.25 possuem muitos pontos de superposição, é conveniente destacar que os números de sequência e as confirmações do nível 2 referem-se ao tráfego entre o anfitrião e o nó para todos os circuitos virtuais combinados. Se um anfitrião envia para o nó sete pacotes, cada um para circuitos diferentes, o anfitrião deve parar de transmitir até que uma confirmação seja recebida. O nível 2 de protocolo previne que o anfitrião sobrecarregue o nó. Em contraste, no nível 3, os números de sequência são aplicados para cada circuito virtual, servindo para controlar o fluxo de cada conexão isoladamente.

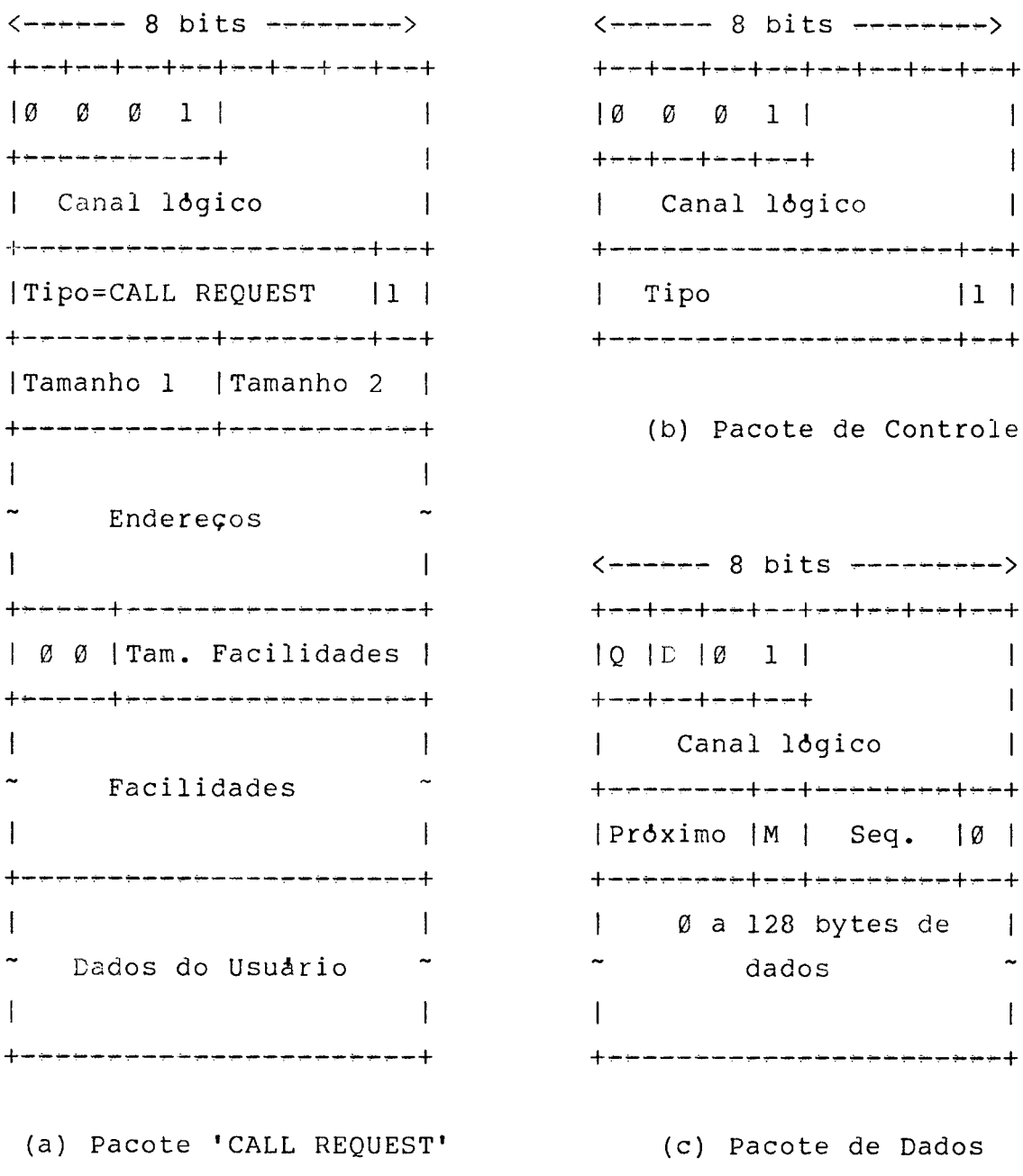


Figura II.2Ø - Cabeçalhos do X.25

O nível 3 do X.25 possui poucos pacotes de controle. Nestes estão incluídos os pacotes de 'RESET' e de 'RESET CONFIRMATION' que são utilizados para se reiniciar um circuito virtual; os pacotes de 'RESTART' e 'RESTART CONFIRMATION', utilizados para reiniciar todos os circuitos virtuais após uma falha do anfitrião ou do nó; os pacotes de 'RECEIVER READY', utilizados para o envio de confirmações; os pacotes de

'RECEIVER NOT READY', usados para inidicar problemas temporários no receptor, devendo o transmissor parar de transmitir até que a situação se normalize, mesmo se a sua janela de transmissão assim o permitir; e os pacotes 'INTERRUPT' e 'INTERRUPT CONFIRMATION', utilizados para enviar mensagens fora do esquema de circuito virtual. Todos estes pacotes de controle utilizam o formato da figura II.2Ø.b, sendo que em alguns casos, o formato possui um ou mais caracteres de informações adicionais.

Para uma descrição detalhada do X.25 recomenda-se a leitura das referências /JACOT77/ e /IMPE*78/.

II.6.5 - Nível de Transporte:

O nível de Rede não assegura, necessariamente, que os pacotes enviados pela origem cheguem intactos ao destinatário. Os pacotes podem ser perdidos ou reordenados devido, por exemplo, a falhas no funcionamento de um nó intermediário. O padrão X.25 coloca à disposição da rede mecanismos (pacotes de 'RESET' e 'RESTART') que permitem comunicar ao anfitrião que ele está com problemas e perdeu as informações correntes a respeito dos números de sequência e a respeito dos pacotes que por acaso estejam ainda em trânsito. Para fornecer ao usuário um serviço fim-a-fim (isto é, anfitrião a anfitrião), realmente confiável, necessita-se criar uma nova camada a fim de suprir esta falha: a camada de transporte.

Uma outra maneira de se definir o nível de transporte é dizer que ele é responsável pelo fornecimento de um serviço de transporte independente das carcterísticas da sub-rede utilizada. O nível de Sessão não deve se preocupar com qualquer detalhe de implementação da rede, cabendo esta responsabilidade ao nível de transporte.

O processo no anfitrião, que implementa o nível de transporte é denominado de Estação de Transporte ('Transport

Station'), possuindo as seguintes funções: gerenciar o estabelecimento e destruição da conexão, controle de fluxo, alocação de buffers e multiplexação. Embora, uma estação de transporte deva apresentar uma interface para os usuários do tipo datagrama, algumas implementações não tomam este procedimento, enfatizando o seu funcionamento tipo circuito virtual. Discutiremos a seguir algumas das funções do nível de Transporte.

- Gerenciamento das Conexões:

Como já foi visto anteriormente, uma consequência do roteamento adaptativo é a possibilidade dos pacotes entrarem em 'loop' por um tempo determinado, atrasando com isto a sua chegada ao destinatário. Se a confirmação de recebimento não chegar após um determinado intervalo de tempo, o pacote será retransmitido, gerando uma duplicata do pacote que ainda está em trânsito. Se a duplicata seguir por um caminho livre de empecilhos e com isto chegando antes do pacote original, ocorrerá uma duplicação do pacote e o recebimento de uma duplicata poderá gerar problemas. Imagine, por exemplo, o que aconteceria se uma mensagem que ordene a um banco transferir alta soma de dinheiro for atendida e logo após ter terminado esta transação a duplicata é recebida. O que fazer com esta duplicata?. A resposta a esta pergunta é feita pela inclusão no protocolo de transporte de mecanismos que permitam detectar a duplicação ou a ausência de uma determinada mensagem, que serão discutidos a seguir.

O primeiro passo a ser dado para resolver este problema é o de se limitar a quantidade de tempo que um pacote pode existir na rede. Isto é feito, por exemplo, pela adoção de um contador localizado no cabeçalho do pacote. Cada vez que o pacote passar por um nó este contador é decrementado e quando atingir o valor zero o pacote é simplesmente destruído. Uma outra hipótese seria a de se utilizar no cabeçalho do pacote a hora de geração do pacote e, após ter decorrido um determinado intervalo de tempo, o pacote é descartado.

O passo seguinte a ser adotado é de se exigir que as estações de transporte utilizem um espaço grande de sequenciamento de tal forma que nenhum pacote consiga sobreviver a um ciclo completo. A adoção desta medida possibilita a detecção do pacote duplicado pela observação do seu número de sequência.

Entretanto, se todas as novas conexões tiverem o mesmo número de sequência inicial (por exemplo, zero), os pacotes das conexões anteriores poderão ser confundidos com os da conexão corrente, principalmente no caso de se ter estabelecimentos de conexão consecutivos e em curtos intervalos de tempo. Logo, para resolver este problema, é necessário que cada nova conexão possua o seu próprio número de sequência de valor superior ao do maior número de sequência adotado para os pacotes anteriores.

Infelizmente, nem mesmo todas estas medidas são suficientes. Como cada anfitrião possui diferentes campos isolados de número de sequência, cada um deve especificar o número de sequência inicial que será utilizado pelos pacotes a serem transmitidos. Esta troca de informações é normalmente realizada durante a fase de estabelecimento de uma chamada. Por azar, a seguinte situação pode ocorrer quando A tenta estabelecer uma chamada com B, utilizando um número de sequência inicial igual a 100:

- A envia um pacote do tipo 'CALL REQUEST' para B com o número de sequência 100;

- o pacote é perdido;

- um pacote antigo de 'CALL REQUEST' que tinha sido enviado de A para B e que tinha se atrasado chega a B, tendo como número de sequência 50;

- a resposta de B para A é enviada por um pacote do tipo 'CALL ACCEPT' com um número de sequência 700 que por sua vez é perdido;

- um pacote antigo de 'CALL ACCEPT' com o número de sequência igual a 650 de repente é recebido por A.

Neste ponto, a conexão foi estabelecida com A pronto para enviar a mensagem de número de sequência 100 e B pronto para receber a mensagem de número 50. B, por sua vez, está pronto para transmitir a mensagem de número 700 mas A espera receber a de número 650. Resultado desta situação: BLOQUEIO.

Tomlinson propôs um protocolo de estabelecimento de conexão, que funciona mesmo na presença de pacotes atrasados, denominado Cumprimento de três modos ('three-way handshake'). Este protocolo está descrito em /SUNSC78/, /TANEA81/, /WATSR81b/. Como exemplo de seu funcionamento pode-se mostrar:

- A envia o pedido de estabelecimento de conexão com o número de sequência igual a 100;

- B envia a confirmação de recebimento deste pacote com o número de sequência 700 e informa também que está confirmando o recebimento do pacote de número 100;

- A, ao receber esta mensagem, envia a confirmação de recebimento do pacote 700 com o número de sequência 101.

Agora passemos a considerar o comportamento deste protocolo diante da situação descrita anteriormente, que conduziu a um bloqueio. Quando B recebe o 'CALL REQUEST' com o número de sequência 50 ele responde com o número de sequência 700, confirmando o recebimento do pacote de número 50. Ao receber esta mensagem, A reconhece a sua invalidade, rejeitando a conexão. A única maneira de A ser enganado por um 'CALL ACCEPT' antigo, é quando um pacote deste tipo surgir com o número de sequência 100. Tal pacote somente poderia ser gerado em resposta a um 'CALL REQUEST' anterior, que A deve ter enviado a algum tempo. Como pode-se observar, o procedimento de estabelecimento de uma conexão é bastante complexa, estando bem abordado em /SUNSC78/ e /WATSR81b/.

A situação inversa, o término de uma conexão, é também bastante complexa. Uma solução para este problema, aparentemente fácil, é a seguinte: A envia para B um pedido de término de conexão e B envia para A a confirmação do recebimento desta mensagem, resolvendo com isto o problema. Infelizmente, isto não é verdade. Como demonstração disto, considere a situação descrita a seguir.

Duas divisões do exército BRANCO estão localizadas em lados opostos de um vale ocupado pelo exército AZUL. Se estas divisões atacarem simultâneamente o exército AZUL a guerra está ganha e em caso contrário, a guerra está perdida. As divisões do exército BRANCO devem se sincronizar através da utilização de um meio de comunicação não confiável (por exemplo, um mensageiro). Suponha agora que a divisão A do exército BRANCO envie a mensagem informando que horas ela pretende atacar o exército AZUL. A após um determinado tempo recebe de B, a outra divisão, a confirmação da mensagem recebida. O problema que surge é o fato da divisão B não ter meios de se assegurar que a resposta foi recebida e no caso dela atacar e de A não ter recebido a confirmação, B será massacrada. Da mesma maneira, A aplicando o mesmo raciocínio teria dúvidas em atacar, mesmo após ter recebido a confirmação.

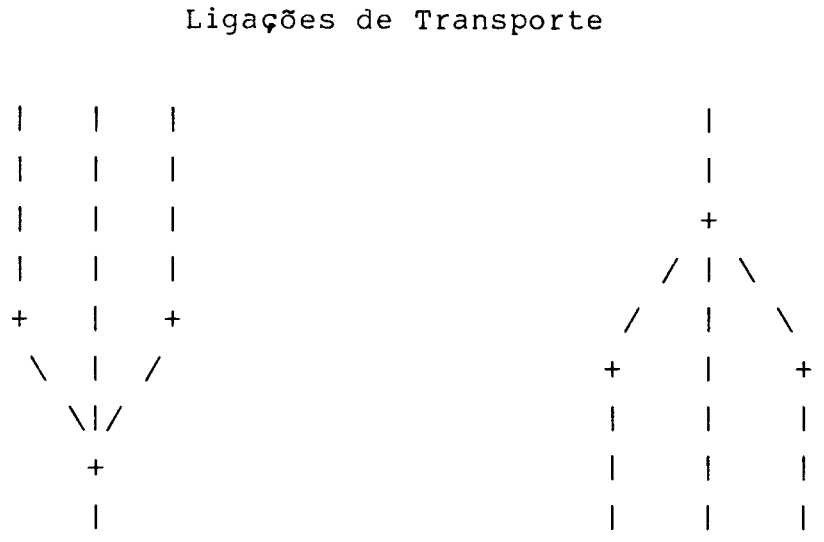
Aparentemente, a primeira solução que surge é a utilização do mesmo método utilizado para o estabelecimento da conexão ('three-way handshake'). Infelizmente, esta solução não funciona pois a mensagem de confirmação do recebimento da confirmação pode ser perdida, permanecendo a situação.

Então porque não adotar um esquema de Cumprimento de quatro modos ('four-way handshake'). Não funciona. E o esquema 'n-way handshake'?. Também não funciona, porque em todos os casos o transmissor da última mensagem não tem condições de afirmar se esta mensagem foi ou não recebida, tornando impossível para uma das divisões saber se a outra vai à guerra ou não.

A implicação disto tudo é que o protocolo utilizado para se fechar uma conexão no caso em que nenhum dos lados termina o seu procedimento enquanto não tiver certeza de que o outro lado está também pronto para terminar é bastante complexa, sendo analisado em /SUNSC78/ e /MCQUJ79/ com bastantes detalhes.

- Multiplexação das Conexões:

A multiplexação das conexões possui um papel importante em vários níveis de protocolo. Por exemplo, nas camadas inferiores, os pacotes e os quadros destinados para diferentes anfitriões são multiplexados no mesmo canal de saída. No nível de Transporte, dois tipos de multiplexação podem ocorrer. Na multiplexação ascendente (' upward multiplexing'), vista na figura II.21.(a), várias ligações de transporte são multiplexadas na mesma ligação de rede. A multiplexação deste tipo, geralmente, é melhor em termos de custos, porque pode-se adotar um esquema de cobrança baseado em números de circuitos virtuais utilizados e não por pacotes transmitidos.



(a) - Ascendente (b) Descendente

Figura II.21 - Tipos de Multiplexação

A outra forma, multiplexação descendente ('downward multiplexing'), pode ser vista na figura II.21.(b). Este método de multiplexação é interessante quando o usuário tem que transferir grandes quantidades de dados e está sendo limitado pela presença de pequenas janelas de transmissão. Adota-se, neste caso, a multiplexação descendente de tal forma que o usuário, baseado em algum critério, dividiria o tráfego pelos diversos canais.

Observa-se que estes tipos de multiplexação podem ser combinados no caso de haver n conexões e k circuitos virtuais com o tráfego sendo dinamicamente distribuído.

As funções de Controle de Fluxo e de Alocação dos Buffers, características deste nível, são descritas no sub-capítulo II.5.

- Exemplo de um protocolo de Transporte: NCP da ARPAnet:

No projeto original de transporte da ARPAnet assumia-se que a sub-rede de comunicações oferecia o serviço de circuito virtual (isto é, totalmente confiável). O primeiro protocolo de transporte desenvolvido foi o NCP ('Network Control Protocol') que foi projetado considerando-se a sub-rede confiável. Neste protocolo, o nível de Transporte passa as mensagens para o nível de rede, assumindo que elas serão entregues na mesma ordem ao destinatário. A experiência mostrou que este protocolo é satisfatório para o tráfego dentro da ARPAnet. Mas, com o passar do tempo o DARPA interessou-se em interconectar a rede ARPA a redes do tipo datagrama, essencialmente não confiáveis. Isto forçou a que modificações fossem efetuadas no protocolo NCP, que culminou com a introdução de um novo protocolo de transporte denominado TCP ('Transmission Control Protocol'), que foi desenvolvido para tolerar uma sub-rede não confiável. Associado com o desenvolvimento do TCP surgiu um novo nível de Rede denominado de nível de Datagrama ou Inter-redes que tem como funções principais o roteamento dos pacotes pela rede ou pelas redes, fragmentar e reconstituir os datagramas. As estações de transporte NCP e TCP podem coexistir no mesmo anfitrião. O NCP é apresentado a seguir, ficando a descrição do TCP para o capítulo III.

- NCP: 'Network Control Protocol':

O serviço de transporte básico prestado pelo NCP a seus usuários é o de fornecer uma ligação simplex sequenciada e livre de erros. Para se obter uma comunicação 'full-duplex', é necessário alocar-se duas ligações. Cada ligação conecta uma porta específica a uma outra específica, localizada em um outro anfitrião. As portas são identificadas por números de 32 bits, sendo reservadas as portas de número par para a recepção de dados e as de número impar para transmissão de dados.

Para se estabelecer uma conexão é necessário a troca de duas mensagens análogas ao 'CALL REQUEST' e 'CALL ACCEPTED' do

X.25. Estas mensagens são as seguintes: a RTS (Receptor para o transmissor - 'Receiver To Sender') e STR (transmissor para o receptor - 'Sender To Receiver'). A maioria dos anfitriões possui as primitivas do serviço de transporte LISTEN e INIT que permitem, respectivamente, aos usuários esperar passivamente por uma conexão ou tentar o estabelecimento de uma conexão de uma forma ativa. A primitiva LISTEN especifica uma porta local que deve ser escutada e opcionalmente um endereço de transporte remoto que identifica a porta que quer seja escutada. INIT deve especificar os dois endereços de transporte.

Quando o usuário fornece um INIT, a estação de transporte examina os endereços fornecidos a fim de determinar qual é a porta de entrada e qual é a porta de saída. De posse desta informação, ela envia para o anfitrião remoto as mensagens RTS e STR. Quando o pedido de estabelecimento de conexão chega no anfitrião remoto, a estação de transporte verifica se existe algum processo escutando na porta especificada. Se houver, os comandos STR e RTS são transmitidos para a origem. Em caso contrário, a estação de transporte pode optar em colocá-los em uma fila, por um determinado período de tempo, ou simplesmente recusar a tentativa de estabelecimento da conexão através do envio da mensagem CLS ('CLoSe'). No caso da ligação ter sido estabelecida, lhe é atribuída um número de 8 bits que serve para identificar esta ligação, tornando desnecessário o envio, nas mensagens trocadas, do endereço completo das portas envolvidas nesta ligação.

As mensagens de dados contém um cabeçalho de 40 bits constituídos de 4 campos dois dos quais devem ser sempre igual a zero. Os outros dois contém o número de bits em um caractere e o número de caracteres na mensagem. O número da ligação é passado como parâmetro para o nível de rede que deverá incluí-lo no cabeçalho da mensagem deste nível e passado como parâmetro para o NCP destinatário.

Observe, que o NCP não possui nenhum esquema de

confirmação de mensagens, pois ele assume que a sub-rede pode manipular todos os erros de uma forma transparente aos níveis superiores e que as mensagens são entregues em sequência, na mesma forma ordem em que foram transmitidas.

As conexões são desfeitas pelas estações de transporte a partir da troca de mensagens do tipo CLS. Como não existe distinção entre os comandos 'CLEAR' e 'CLEAR CONFIRMATION', como no X.25, não há problema de colisão de mensagens deste tipo. Se ambos os lados decidirem desfazer simultaneamente a conexão, cada um interpretará o pedido de CLS do outro como sendo uma resposta a seu pedido, terminando desta maneira a ligação.

Em contraste com outros protocolos deste nível, o NCP não utiliza o mecanismo de janela para controlar o fluxo de mensagens. Ao invés deste esquema, utiliza um esquema de alocação explícita de buffers, usando para isto três mensagens de controle: ALL (alocar - ALLocate'), GVB (dê-me de volta - 'GiVe Back') e RET (retôrno - 'RETurn'). Quando uma conexão é estabelecida o anfitrião transmissor fica impedido de transmitir até que seja recebido do anfitrião receptor uma mensagem de alocação (ALL) para esta conexão. A mensagem ALL, como todas as mensagens de controle, é transmitida pelo canal Ø (o de controle) e não pelo canal a que esta mensagem se aplica. Em outras palavras, a alocação dos buffers é feita em uma base anfitrião a anfitrião e não em uma base de conexão. A mensagem de alocação especifica o limite de mensagens e o limite de bits por mensagem.

Em algumas circunstâncias, o anfitrião pode requisitar os buffers previamente alocados por causa da ocorrência de falta de espaço. Isto é feito através da mensagem GVB. Quando o receptor pede ao transmissor que ele devolva alguma área alocada ele transmite a mensagem GVB para o transmissor. Espera-se que o transmissor concorde, utilizando para isto a mensagem RET.

Como o X.25, o NCP fornece mecanismos especiais que

podem ser utilizados em casos excepcionais como o INR (interrupção pelo receptor - INterrupt by Receiver') e o INS (interrupção pelo transmissor - INterrupt by Sender'). A mensagem ECO (EChO') pode ser utilizado para se verificar se o outro anfitrião está ativo ou para se tomar medidas de tempo.

Se algum anfitrião descobrir um erro, ele pode informar esta situação aos demais participantes utilizando para isto a mensagem ERR (ERRor').

As duas últimas mensagens deste protocolo são a RST (reinicio - ReSTart') e RRP (resposta ao reinicio - Resart RePly'), possuindo o mesmo significado das mensagens 'RESTART' e 'RESTART CONFIRMATION' do X.25.

II.6.6 - Nível de Sessão:

Na maioria das redes, o nível de transporte estabelece e mantem as conexões entre os anfitriões. O nível de Sessão estabelece e mantem as conexões, denominadas SESSOES, entre pares de processos. Por outro lado, existem redes que ignoram a presença do nível de Sessão, considerando que as ligações de processos se efetuam ao nível de transporte. O modelo OSI é vago neste ponto quando afirma que o nível de Sessão conecta entidades do nível de Apresentação e que o nível de Transporte conecta entidades do nível de Sessão. Neste trabalho assume-se que as ligações de transporte existe entre anfitriões e que as ligações de sessão ocorrem entre processos. Logo, quando um processo desejar comunicar-se com um outro processo, ele expressa o seu desejo ao nível de sessão que requisita os serviços do nível de transporte a fim de estabelecer uma ligação de transporte com o anfitrião remoto para possibilitar a comunicação entre os processos.

A principal tarefa do nível de sessão é a de conectar dois processos constituindo uma sessão. Como é incoveniente para os usuários lidar com os endereços de transporte, o nível

de sessão efetua o mapeamento do nome simbólico conhecido pelo usuário no endereço de transporte correspondente.

Quando uma sessão é iniciada, convenções a respeito da sessão podem ser estabelecidas. Exemplos destas convenções podem ser o tipo de transferência de dados ('half' ou 'full-duplex'), códigos dos caracteres, tamanho da janela a ser utilizada para controlar o fluxo, a presença ou não de mensagens criptografadas, compressão de textos e como agir no caso de haver falhas no nível de transporte.

Uma outra possível atribuição do nível de sessão é o controle do diálogo entre os processos. Este controle é feito pela manutenção do registro dos pedidos e respostas, reordenando-os se necessário, a fim de simplificar o desenvolvimento dos programas do usuário.

Outro aspecto do controle do diálogo é o de associar um grupo de mensagens em unidades atômicas. Exemplificando, em várias aplicações de banco de dados é altamente indesejável que uma transação seja feita parcialmente por causa da ocorrência de falhas na rede. Se as transações consistirem de um grupo de mensagens, o nível de sessão pode assegurar que o grupo em sua totalidade foi recebido no destinatárioa, antes mesmo de iniciar a transação.

A discussão sobre o nível de sessão se encerra aqui, pois a maioria das redes não fazem distinções entre o nível de transporte e o de sessão. Como não há nenhuma proposta internacional de um padrão para este nível, não mostraremos nenhum exemplo de protocolo para este nível.

II.6.7 - Nível de Apresentação:

A função deste nível é o de realizar transformações nos dados antes destes serem despachados para o nível de Sessão. As seguintes transformações nos dados podem ser mencionadas:

compressão de texto, criptografia e conversão de e para os padrões da rede dos arquivos e terminais.

- Compressão de Textos:

Deve-se observar que a transmissão de milhares de caracteres brancos para serem impressos é a mesma coisa que não fazer nada, além de ocupar o tempo de transmissão, tempo este que poderia ser utilizado para se transmitir outro tipo de informação, representando um custo que pode ser minimizado pela adoção de mecanismos que otimizem a transferência de dados pela compressão dos caracteres repetitivos, denominados métodos de Compressão de Textos.

Embora alguns projetistas considerem a compressão de textos comos sendo da responsabilidade do programa do usuário, é mais eficiente e conveniente incorporar estes procedimentos à arquitetura da rede, constituindo-se no padrão da rede para os serviços de Apresentação.

A compressão de textos é um assunto interessante, possuindo várias referências entre as quais pode-se citar /HELDG79/.

- Protocolo de Criptografia:

A informação na maioria das vezes possui um grande valor econômico e em alguns casos até estratégico. Por causa disto deve-se dotar a rede de mecanismos que permitam preservar a segurança e a integridade dos dados transmitidos, colocando-os a salvo de espiões e curiosos. Um destes mecanismos é a Criptografia.

A função da Criptografia é a de transformar os dados de entrada ('plaintext') em dados de saída ('ciphertext') que é incompreensível para qualquer pessoa que não possua a chave secreta utilizada para parametrizar esta transformação.

A definição de que nível de protocolo o processo de

criptografia deve ser aplicado é motivo de controvérsia. Alguns projetistas afirmam que esta é uma função do nível de transporte e outros afirmam, baseado no fato de que a compressão de textos é uma tarefa do nível de Apresentação, que a criptografia é uma função do nível de Apresentação, com os quais concordamos.

Não entraremos em detalhes a respeito dos processos de criptografia mas, recomenda-se a leitura de /HOFFL77/, /COUSW8Ø/, /HOWAJ8Ø/, /KENTS81/, /LENNR81/, /POPEG79/ e /STILR8Ø/.

- Terminais Virtuais:

Existem dezenas de tipos de terminais em uso, cada um com as mais variadas funções. Seria um fator negativo, para uma rede de computadores, impedir que um usuário utilize um terminal por ele não ser compatível com o seu programa. Para se evitar este problema foram desenvolvidos protocolos que tentam tornar transparentes para o programa do usuários as características do terminal. Estes protocolos são denominados de protocolo de Terminais Virtuais, porque tentam os terminais reais em um terminal virtual hipotético.

- Transferência de Arquivos:

Análogo ao caso anterior. Da mesma forma que um programa deve utilizar vários tipos de terminais, existe a necessidade destes programas serem capazes de acessar arquivos em diferentes máquinas, cada uma destas com as características próprias para os seus arquivos.

Em princípio, pode-se adotar o mesmo esquema seguido para os terminais, isto é, definir-se um formato padrão para os arquivos e mapear os diferentes formatos de arquivo para este padrão, viabilizando com isto um processo acessar a qualquer arquivo em qualquer máquina.

Na prática, este esquema não funciona porque as

diferenças entre os arquivos podem ser grandes, dificultando o mapeamento. Como exemplo pode-se citar o caso de um número de ponto flutuante ser representado em uma determinada máquina em 60 bits e em uma outra em 32 bits, agravando-se no caso dos números aparecerem aleatoriamente no arquivo.

Os arquivos são transferidos devido a quatro razões principais:

- armazenar o arquivo para uma posterior recuperação;

- imprimir um arquivo remoto em uma impressora local;

- submeter um arquivo como sendo uma tarefa remota ('remote job entry');

- utilizar um arquivo remoto como entrada ou saída de dados.

Cada uma destas categorias possui suas próprias características, podendo-se citar como exemplo:

- quando um arquivo é armazenado para ser utilizado posteriormente, é possível produzir-se uma cópia exata bit-a-bit deste arquivo. O número de bits no arquivo deve ser registrado no próprio arquivo a fim de permitir a transferência entre máquinas com diferentes tamanhos de caractere.

- quando um arquivo é transferido para ser impresso o problema que surge diz respeito às diferentes convenções adotadas para o processo de impressão.

Um outro aspecto da transferência de arquivos é a manipulação do arquivo. O usuário deve ser capaz de criar, deletar, copiar, renomear e gerenciar os arquivos remotos. A maioria dos protocolos de transferência de arquivos se concentra neste aspecto do problema, não se preocupando com as possíveis conversões. A referência /GIENM78/ descreve um

protocolo de transferência de arquivos em detalhes.

Como não existe um protocolo padrão para este nível não será dado nenhum exemplo de um protocolo deste nível, embora se aconselhe a consulta à referência /SCHIS81/ que é uma proposta de protocolo para este nível.

II.6.8 - Nível de Aplicação:

A fronteira entre o nível de Apresentação e o nível de Aplicação é uma fronteira conceitualmente importante, por separar o domínio de ação dos projetistas da rede do domínio dos usuários da rede.

Em princípio, muito pouco se pode dizer à respeito do conteúdo do nível de Aplicação porque cada usuário determina que procedimentos e protocolos serão utilizados, além de não haver padrões para este nível.

Por causa de estar fora do domínio da rede não será dado nenhum destaque para este nível neste trabalho, aconselhamos, porém, a leitura de /TANEA81/ e de /DAVID81/ a fim de obter maiores informações a respeito deste nível.

II.7 - Conclusão:

Neste capítulo procurou-se avaliar vários pontos de interesse deste trabalho no caso de redes de computadores de uma forma isolada. Os seguintes objetivos podem ser destacados:

- uniformização dos têrmos utilizados;

- avaliação dos pontos julgados relevantes para o trabalho;

- preparar uma base qualitativa que será utilizada nos capítulos seguintes.

Julgamos que o conteúdo deste capítulo se justifique por causa da importância dos pontos analisados no desenvolvimento desta pesquisa e também para efeitos didáticos.

III - Redes de Computadores Interconectadas:

III.1 - Introdução:

Como já foi observado no capítulo I, existe uma necessidade de se interconectar as redes de computadores, a fim de possibilitar o acesso do usuário a um conjunto maior de recursos, aumentando, consequentemente, a sua capacidade e a sua disponibilidade, contribuindo para a obtenção de um melhor desempenho.

Do ponto de vista do usuário, a exigência de se interligar as redes é independente das tecnologias adotadas pelas diversas redes. Do ponto de vista da implementação desta estrutura podem surgir alguns pontos complexos quando se interligam redes de diferentes tecnologias (como por exemplo, redes de comutação de circuitos e redes de comutação de pacotes do tipo datagrama). Neste trabalho será considerado, em particular, a interconexão de redes de comutação de pacotes, por ser a mais complexa e as hipóteses consideradas podem ser aplicadas em qualquer tipo de tecnologia.

Ao se interconectar duas ou mais redes de computadores surgem várias questões técnicas, legais e políticas. As questões técnicas dizem respeito aos mecanismos utilizados que possibilitam a ligação entre as redes e a avaliação do desempenho do conjunto de redes. As seguintes perguntas podem ser feitas neste caso:

- Como as redes podem ser conectadas, de tal forma que possibilite aos pacotes transitarem de uma maneira controlada pelas diversas redes?

- Todos os computadores de todas as redes devem ser capazes de se comunicarem uns com os outros? Como isto pode ser obtido?

- Qual o tipo de desempenho que pode ser esperado por um

conjunto de redes, no caso de cada uma das redes envolvidas possuirem tecnologias díspares?

- Como o usuário pode obter o acesso a um recurso localizado em uma outra rede?

- Quais os protocolos utilizados?

- Os procolos de uma rede devem ser traduzidos para os da outra rede ou deve-se adotar um protocolo comum a todas as redes?

- Que tipos de protocolos de comunicação se fazem necessários para o suporte eficiente e prático da interconexão?

- Quem deve ter a responsabilidade de definir um padrão a ser adotado por todas as redes?

As seguintes perguntas legais e políticas, que são mais simples do que as técnicas, podem ser levantadas:

- As redes privadas devem ou não se interconectar através de uma rede pública?

- Como garantir a privacidade e a confidência dos dados?

- Deve ou não existir algum tipo de controle sobre os dados que trafegam de uma rede para outra?

- Existe alguma convenção ou acôrdo internacional que seja afetado pela interconexão de redes de diferentes países?

- Qual deve ser o critério de cobrança a ser aplicado ao tráfego multi-rede?

- Como as falhas e os erros podem ser diagnosticados em um conjunto de redes? Quem deve ser o responsável pela correção destas falhas?

Não será possível responder a todas estas questões levantadas neste trabalho, embora a maior parte destas sejam analisadas.

- Conceito de Comporta:

Como pode-se observar, pela análise destas questões, um pacote ao passar de uma rede para outra passa por vários processos que vão desde o processo de uniformização de seu formato ao processo de taxação, passando por uma série de outros processos como por exemplo, o processo de compatibilização de tecnologias.

Considerando-se estes vários processos surgem as seguintes perguntas: Como e quem deve efetuar estas tarefas?

A resposta a estas perguntas é feita pela introdução do conceito de COMPORTA ('Gateway'). A comporta pode ser definida como sendo o conjunto de 'software' e 'hardware' necessários para se efetuar a interconexão de duas ou mais redes de dados, a fim de possibilitar-se o tráfego de dados de uma rede para outra. Em outras palavras, a função da comporta é o de converter os pacotes de um protocolo para o outro, de uma maneira análoga a de uma pessoa que traduz um texto do inglês para o português, e vice-versa.

Neste capítulo serão considerados diversos pontos relativos à interconexão de redes, procurando-se responder de uma forma qualitativa a todas questões levantadas.

Em uma primeira etapa, o conjunto de redes deve ser classificado de acôrdo com diversos critérios. Após esta fase, consideraremos o processo de compatibilização das diversas estruturas de Nomes e Endereços das diversas redes, estruturas estas apresentadas no capítulo II.3.

Posteriormente, serão avaliados os problemas relativos aos Controles de Rotas e de Fluxo, procurando-se traçar um

paralelo do caso de redes simples e determinar os pontos críticos de cada um deles.

Finalmente, serão considerados os procedimentos adotados para a compatibilização do tamanho dos pacotes (Fragmentação) e apresentados exemplos de protocolo desenvolvidos para o caso de Redes Interconectadas.

Em resumo, o objetivo deste capítulo é o de levantar os pontos críticos que se surgem ao se interconectar diferentes redes, realizando uma análise qualitativa destes pontos, procurando estabelecer uma analogia entre este caso e o caso de uma rede simples.

III.2 - Classificação de Redes Interconectadas:

III.2.1 - De acôrdo com as funções exercidas pela comporta:

As funções exercidas pela comporta podem ser divididas em dois grandes grupos:

- MAPEAMENTO: quando as funções e as entidades das redes são correspondentes;

- PONTE: quando não é possível estabelecer um mapeamento satisfatório entre as funções, tornando-se necessário criar mecanismos de compatibilização.

De acôrdo com os níveis de participação das comportas, ou seja, a porcentagem dos grupos acima nas funções exercidas pela comporta, podemos classificar as redes interconectadas no seguinte sentido:

- Tecnologia da Sub-rede Comum;

- Interfaces de acesso a rede comuns;

- Comportas do tipo anfitrião;

- Comportas conversoras de protocolo.

Estes níveis serão discriminados a seguir.

III.2.1.a - Tecnologia de Subrede Comum:

Aplicada no caso de interconexão de redes idênticas ao nível de pacote (vide figura III.1). Este nível de participação também é conhecido como nível de pacote.

Neste caso, a comporta pode se constituir de rotinas localizadas nos nós, realizando a contabilização do uso e possivelmente as funções de endereçamento.

O modelo de contôrno da camada do protocolo é útil porque mostra que níveis são comuns e quais são os que diferem. Essencialmente, as camadas que são terminadas pela comporta podem ser diferentes em cada uma das redes envolvidas, enquanto as que passam transparentemente pela comporta são assumidas serem comuns às redes.

Esta estratégia implica que a estrutura de endereçamento interno de todas as redes envolvidas seja comum, podendo implicar na modificação da estrutura de endereçamento de uma das redes.

Esta estratégia apresenta para o usuário uma nova rede composta da união de outras redes. Este método tem o seu uso restrito aos casos em que as redes a serem conectadas forem virtualmente idênticas, por causa da necessidade das comportas participarem diretamente em todos os protocolos da sub-rede de comunicações, apresentando a mesma interface de acesso à rede para todos os assinantes.

III.2.1.b - Interfaces comuns de acesso à rede:

No caso dos protocolos da sub-rede não serem idênticos, o próximo nível de participação das comportas na compatibilização é no nível de acesso à rede, ilustrado na figura III.2.

Neste caso, cada rede possui o seu próprio protocolo de sub-rede, embora apresentem a mesma interface externa para os assinantes. Isto é ilustrado ao se mostrar uma interface comum passando por todos os anfitriões, denominada de "interface de acesso comum à rede" (vide figura III.2).

Novamente, a comporta pode ser encarada como sendo um 'software' nos nós adjacentes às redes, composta de duas metades formadas pela ligação dos nós de duas redes. Neste caso, os protocolos da sub-rede das redes interconectadas são terminados pela comporta de tal forma que a troca de informações entre as redes é mais uma interação de acesso a rede do que uma troca de mensagens entre os nós. Esta é a estratégia adotada pelo CCITT em sua recomendação X.75 (ver seção III.7).

É importante observar-se que a interface entre comportas pode ser similar à interface padrão de acesso à rede, mas não necessitando ser a mesma.

III.2.1.c - Comportas do tipo Anfitrião:

Neste caso, a comporta não é diferente de qualquer anfitrião das redes, implementando sempre que necessário a interface anfitrião-rede que é exigida pelas redes as quais está interconectada (ver figura III.3).

O principal ponto de partida para este método é o seguinte: as redes são capazes de pelo menos transportar os pacotes em seu comprimento máximo, que varia de rede para rede. Não se assume, especificamente, que estes pacotes sejam entregues na mesma ordem, através das redes e comportas intermediárias, ao anfitrião destinatário.

O modelo básico deste nível, ilustrado na figura III.3, é que os datagramas entre-redes são transportados para e dos anfitriões e comportas e entre as comportas pela transformação dos datagramas em pacotes locais à rede (técnica denominada envelopamento).

Nesta estratégia, as funções básicas são as de envelopar e desenvelopar os datagramas, mapeando os endereços origem e destino em endereços locais e o direcionamento dos datagramas.

As comportas não precisam ter nenhum conhecimento dos protocolos de níveis superiores, pois é assumido que estes são mantidos comuns pelos anfitriões em comunicação.

A vantagem deste método é que qualquer tipo de rede pode participar, independente se a sua operação interna fôr orientada para datagrama ou circuito virtual.

III.2.1.d - Comportas Conversoras de Protocolo:

Neste caso, o pacote, que possui um formato ditado pelo protocolo adotado em uma das redes, é convertido para um outro formato que seja entendido pelos protocolos da rede subsequente. Por exemplo, se duas redes possuirem um conceito de circuito virtual, uma implementada na sub-rede e a outra nos protocolos fim-a-fim, é possível à comporta mapear um circuito virtual para o outro.

O sucesso desta estratégia (vide figura III.4) depende, em grande parte, da semelhança de conceitos dos protocolos adotados. Discrepâncias nestes conceitos podem fazer com que os serviços prestados pelo conjunto de redes seja um subconjunto dos serviços oferecidos de uma maneira isolada. A extensão da tradução por várias comportas pode ser bastante difícil, particularmente, se os protocolos possuirem um espaço de endereçamento comum para os pontos origem e destino.

Este caso é o mais geral, porque a comporta se torna um super computador frontal, já que uma das características do computador frontal é a de transformar os protocolos do anfitrião nos protocolos da rede.

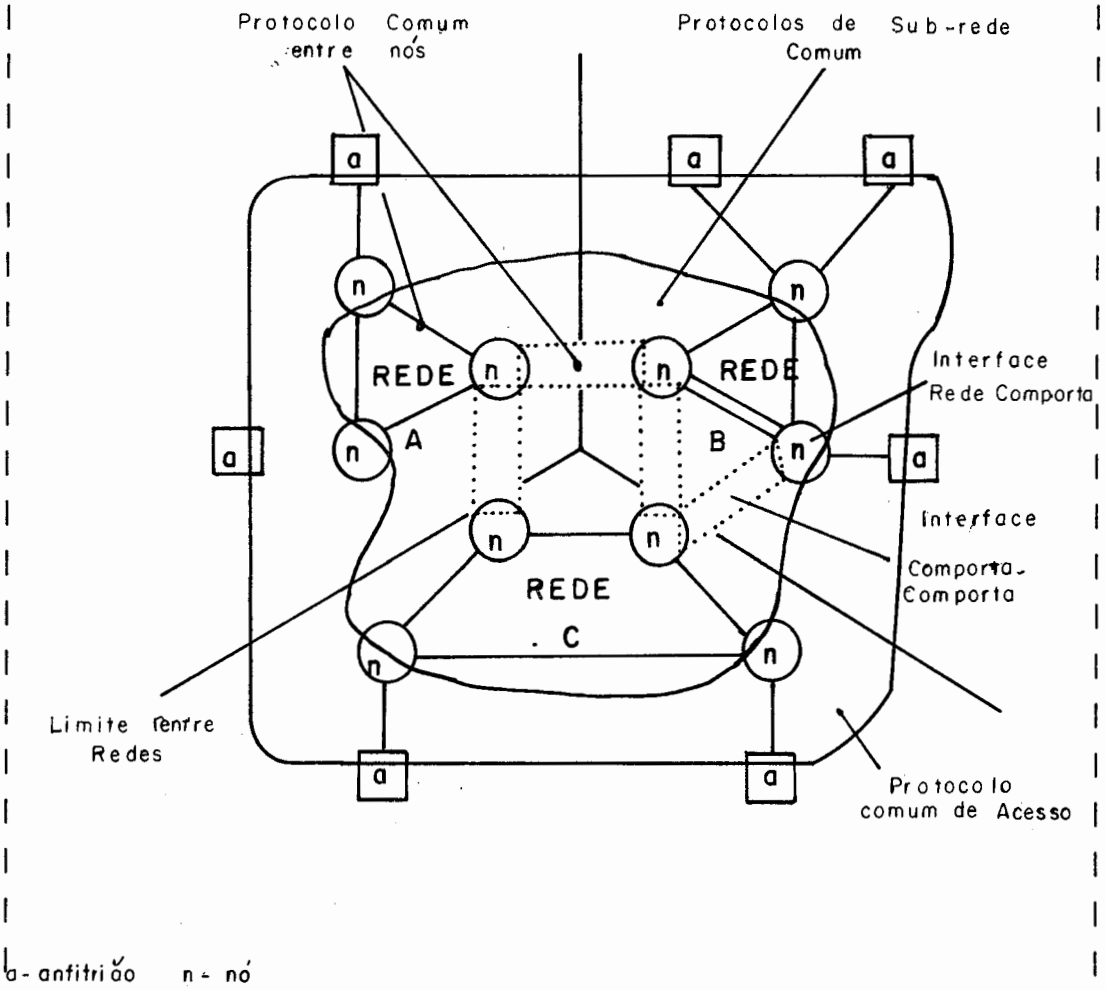


Figura III.1: Tecnologia da Sub-rede Comum /CERFV78/

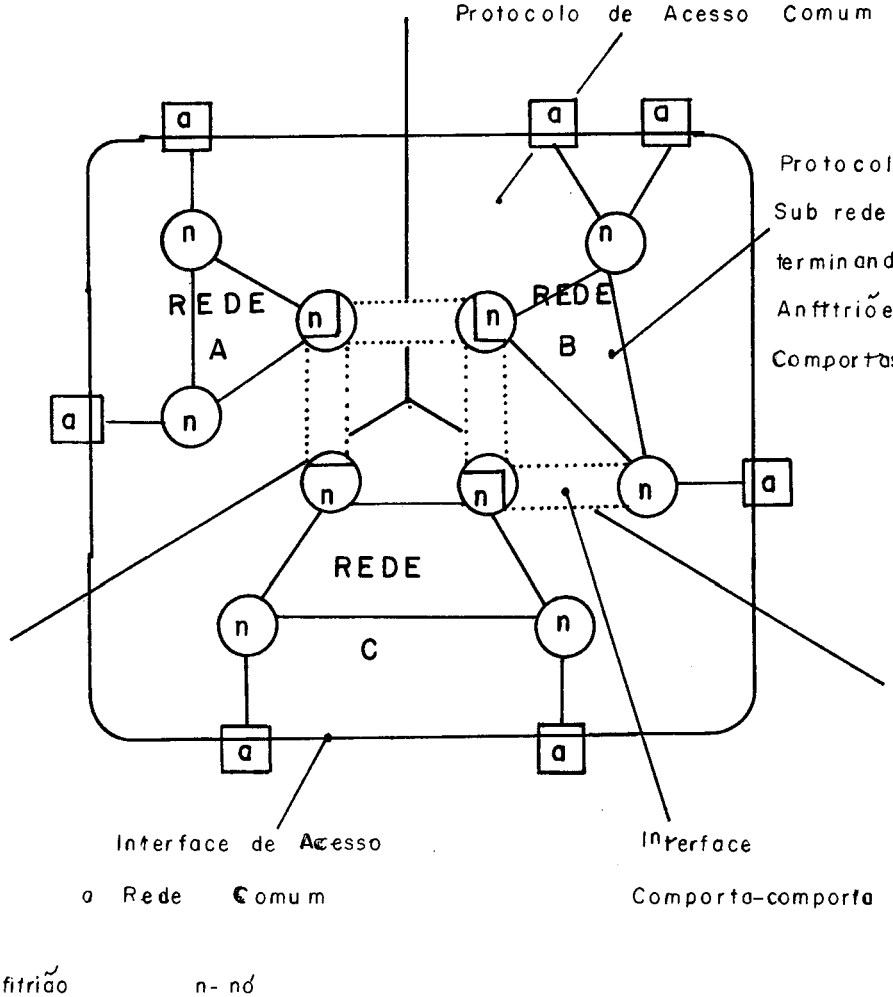


Figura III.2: Nível de Acesso Comum /CERFV78/

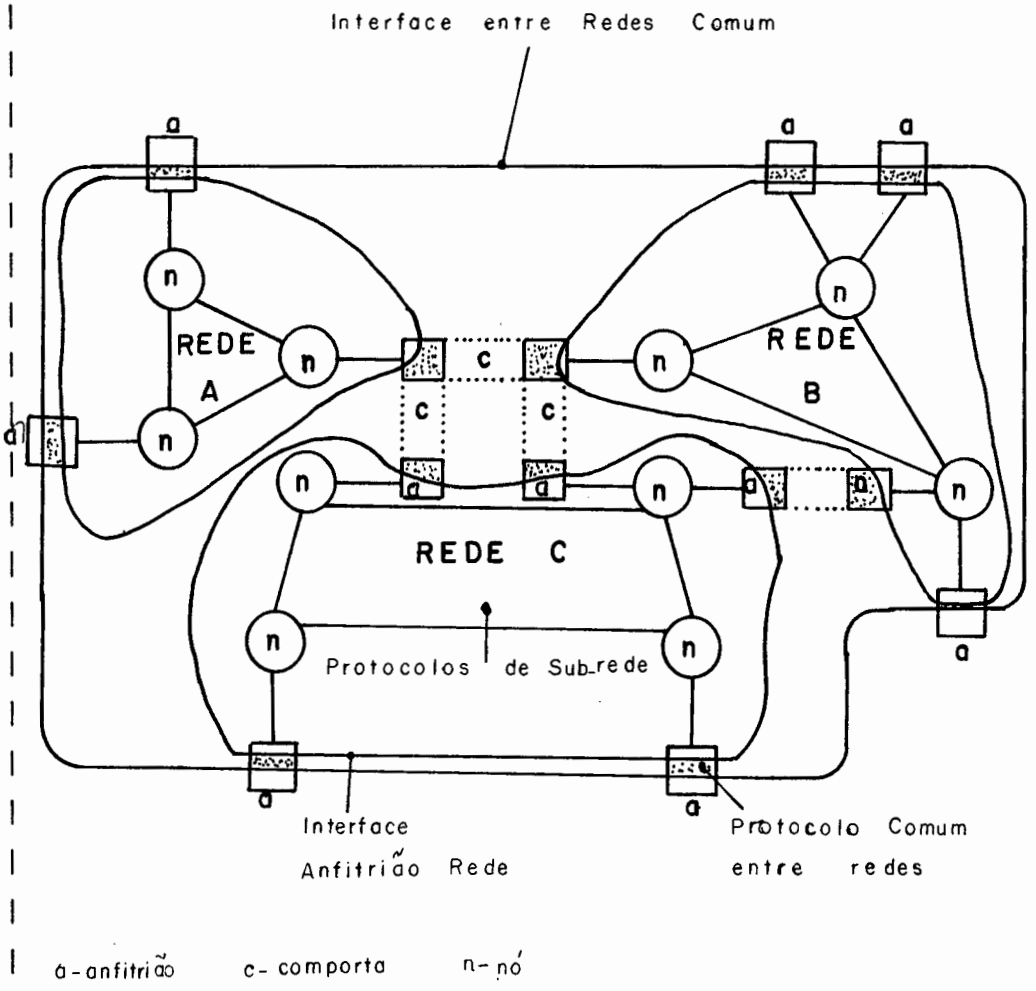


Figura III.3: Comportas do tipo Anfitrião /CERFV78/

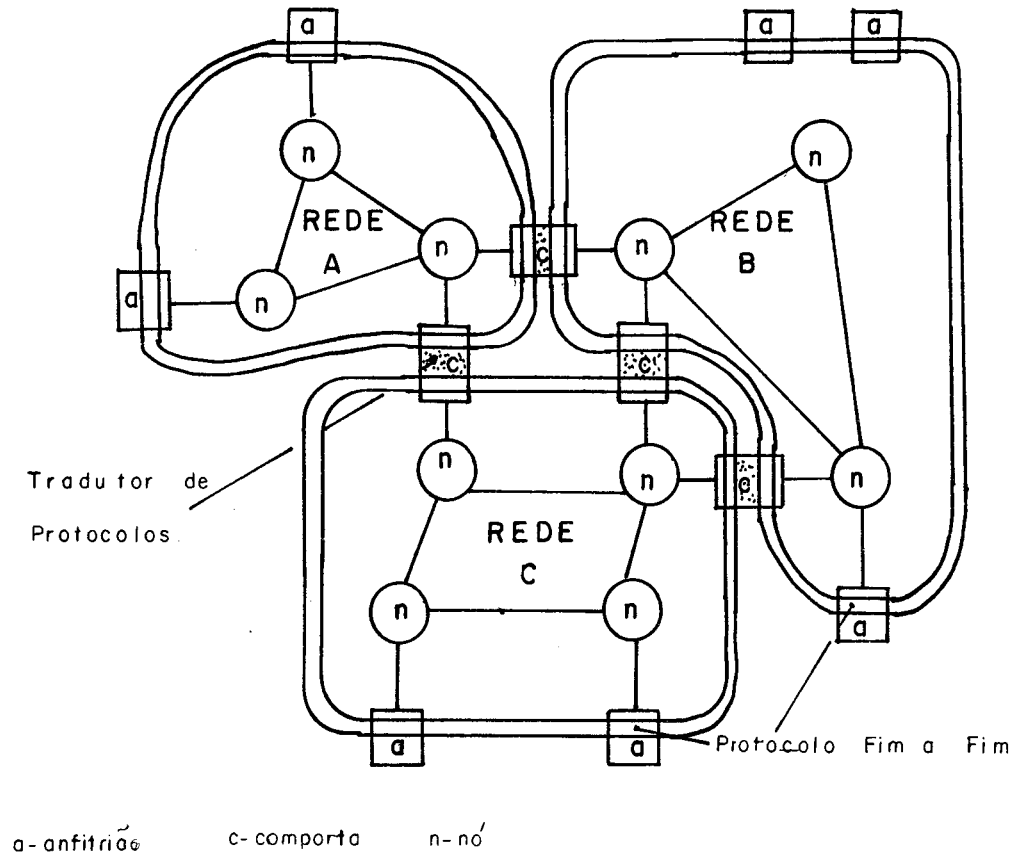


Fig.III.4: Comportas Conversora de Protocolo /CERFV78/

III.2.2 - Quanto à forma de implementação:

Ao se implementar uma estratégia para a interconexão de redes, pode-se optar por uma das seguintes alternativas:

- Pontos extremos (' endpoint') ou datagrama;

- Passo a passo ('hop-by-hop') ou circuito virtual.

A estratégia dos pontos extremos, como será visto a seguir, requer dos participantes a adoção de um protocolo de controle da comunicação comum e exige das redes envolvidas a prestação de um conjunto mínimo de serviços.

A outra alternativa utiliza os protocolos existentes em cada uma das redes para fornecer o nível de serviço desejado, mas necessitando que uma compatibilização, bastante complexa, ocorra nas comportas.

Estas alternativas serão descritas a seguir.

III.2.2.a - Pontos Extremos:

O funcionamento desta alternativa baseia-se na adoção de um protocolo padrão para o controle da comunicação, que deve ser implementado por todos os participantes. Este protocolo se aplica à comunicação entre os pontos origem e destino do pacote, servindo principalmente para o controle de fluxo e de erro. Detalhando o modo de agir da rede temos:

Os pacotes, que se destinam a um anfitrião localizado em uma outra rede que não a de origem, são transmitidos pelas redes subsequentes e pelas comportas de uma forma independente, não se exigindo que os pacotes saiam de uma rede pela mesma comporta. Este é o comportamento típico de uma rede do tipo Datagrama (vide figura III.5).

A possibilidade de haver várias rotas entre as redes é devida ao fato da comporta de saída não ter necessidade de realizar a tarefa de sequenciamento, que ocorrerá no destino, por causa dos pacotes serem independentes.

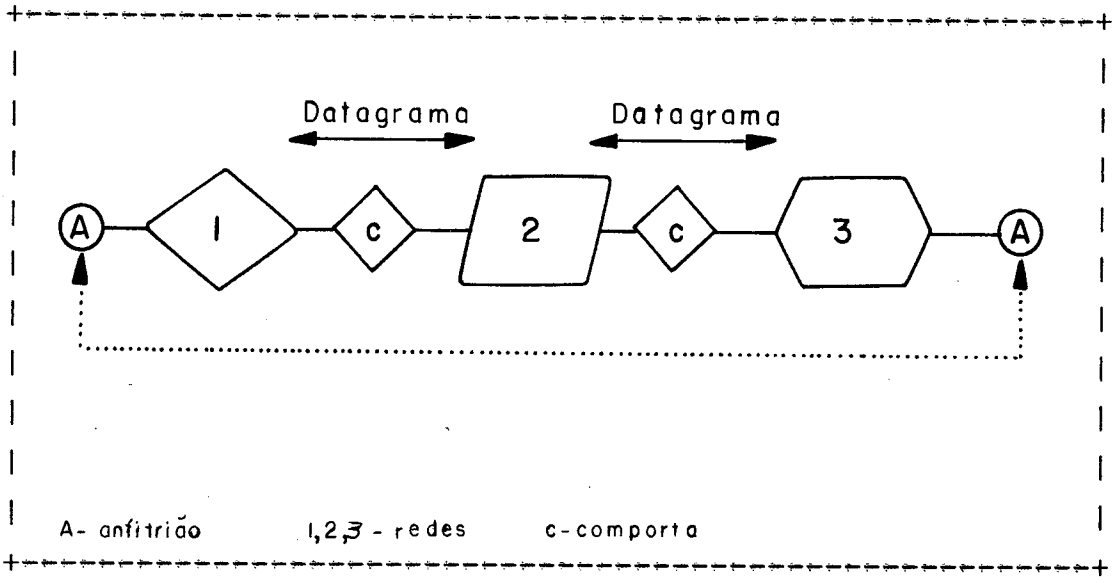


Figura III.5: Implementação dos Pontos Extremos.

Esta possibilidade é importante em termos de confiabilidade da ligação entre as redes, pois no caso de ocorrer uma falha em uma determinada comporta de saída, rotas alternativas podem ser determinadas automaticamente, não criando nenhum problema para o protocolo de comunicação fim-a-fim.

Esta estratégia apresenta como principais VANTAGENS:

- reduzir o ' overhead' causado por um pacote na passagem de uma rede para outra, pela não necessidade de se sequenciar os pacotes;

- as rotas entre redes podem ser dinamicamente alteradas, permitindo-se uma resposta rápida a falhas das redes ou a congestionamentos;

- simplificação das comportas.

Apesar destas vantagens, esta estratégia é DESVANTAJOSA nos seguintes pontos:

- necessidade de uma padronização nos protocolos de comunicação entre as redes em cada um dos anfitriões. Esta necessidade pode ser difícil de ser implementada devido ao alto custo e pela alteração no comportamento dos anfitriões. Esta desvantagem pode ser minimizada pela adoção de um Centro de Comunicações entre redes que é responsável pela comunicação entre redes e implementação dos serviços entre redes. Este Centro é acessado utilizando-se os protocolos da própria rede, não necessitando-se alterar os anfitriões;

- possibilidade de ocorrer grandes cabeçalhos entre redes, diminuindo com isto a eficiência de transmissão;

- duplicação desnecessária das tarefas fim-a-fim efetuada pela comporta, no caso em que o tráfego entre redes passa por uma rede do tipo circuito virtual.

III.2.2.b - Passo a passo:

Ao se implementar esta estratégia de interconexão não se exige a definição de nenhum protocolo padrão fim a fim, pois, ao utilizar os próprios protocolos das redes envolvidas, transfere-se para as comportas a tarefa de compatibilização dos serviços oferecidos pelas diversas redes. Embora , diversas funções universais oferecidas pelas redes possam ser identificadas, esta tarefa de compatibilização pode ser complexa e de difícil implementação, porque em alguns casos serviços equivalentes mas incompatíveis são fornecidos pelos diversos níveis de protocolo da rede, como, por exemplo, o Controle de Fluxo.

Neste caso, a comporta deve simular a concordância localmente, sem garantir a obtenção do serviço no destinatário. Geralmente, isto reduz os serviços entre-redes a um subconjunto oferecido pelas redes isoladamente, transferindo para o usuário o conhecimento dos serviços oferecidos pelo conjunto de redes. Observa-se que o serviço desejado não está sendo oferecido como fim a fim mas, sim como uma concatenação dos serviços prestados por cada uma das redes intermediárias e por causa disto dificultando o tratamento dos erros.

Uma outra exigência desta alternativa é a existência de um único caminho entre-redes, determinando com isto que todos os pacotes saiam da rede pelo mesmo ponto, por causa da necessidade de se manter a ordenação das mensagens. Deve-se observar que este método não exige que seja seguida a mesma rota internamente à rede mas que seja mantido o mesmo ponto de saída da rede.

Esta estratégia é implementada nas comportas, ao nível de circuito virtual, obtendo-se a interconexão das redes pelo encadeamento das diversas chamadas virtuais locais em cada uma das redes intermediárias (ver figura III.6)

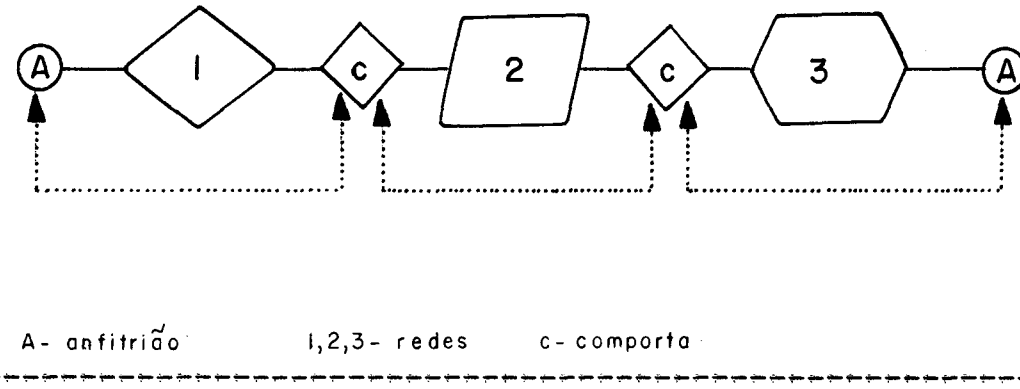


Figura III.6: Implementação Passo a passo

Pode-se destacar as seguintes VANTAGENS para esta estratégia:

- permite a utilização das chamadas virtuais para a constituição de uma ligação entre redes;

- utilização de cabeçalhos reduzidos pela adoção de cabeçalhos abreviados, sendo mantido nas comportas o cabeçalho completo;

- não há necessidade de se implementar um protocolo padrão;

- diminuição das tarefas executadas pelos anfitriões.

Apesar disto tudo as seguintes DESVANTAGENS podem ser mencionadas:

- complexidade das comportas pela necessidade da compatibilização dos protocolos;

- possibilidade de não ser viável o mapeamento de todas as funções de um serviço;

- se o comportamento de uma rede fôr do tipo datagrama, há necessidade de realizar na comporta as funções da chamada virtual.

III.3 - Títulos e Endereços em Redes Interconectadas:

III.3.1 - Títulos (/POUZL79/):

Conforme já foi visto no capítulo II.3 um projeto de Rede de Conputadores deve prever um método específico para se identificar os participantes de uma comunicação entre dois processos localizados em anfitriões distintos. Tipicamente, em uma Rede de Computadores coexistem vários níveis de identificação, como por exemplo: o nível da sub-rede de comunicações, o nível de acesso à rede, o nível correspondente ao sistema de arquivos. Em redes homogêneas de computadores, o esquema de identificação é consistente e hierárquico, resultando diretamente da definição dos níveis de protocolo e, no caso das redes heterogêneas, somente os níveis inferiores de protocolo possuem um esquema de identificação consistente, o que não ocorre nos níveis superiores que utilizam diferentes alternativas para cada um dos computadores da rede.

No caso de redes interconectadas, onde diversos esquemas de identificação são utilizados pelas diversas redes, precisa-se adotar mecanismos de compatibilização. Dois destes métodos se destacam: o método do Mapeamento Estático e o método da Alocação.

O método da Concatenação Hierárquica não é considerado em nossa análise por ser característico de sistemas homogêneos, sendo utilizado nas interconexões de redes homogêneas, não apresentando maiores dificuldades em sua implementação (vide Seção II.3.2.a).

- Mapeamento Estático (compare com a seção II.3.2.c):

Neste método, o recurso (digamos, b(j)) da rede B que pode ser acessado pela rede A, possui um título (digamos, a(i)) no espaço de nomes da rede A (ver Seção II.3). As mensagens que se destinam ao recurso b(j) são enviadas pelos processos da rede A como se fossem destinadas para o recurso a(i) e

despachadas para a comporta correspondente que deverá substituir o título a(i), que só tem significado para a rede A, pelo título correspondente b(j), específico da rede B.

Este método, para ser utilizado, exige que o conjunto de títulos a serem mapeados (o conjunto de títulos a(i) e os correspondentes b(j)) seja definido a priori, isto é, este conjunto de títulos deve ser finito, devendo possuir de uma forma permanente, tantas entradas quantos forem os recursos disponíveis em outras redes.

Uma das desvantagens deste método é a quantidade de memória que deve ser reservada nas comportas para o armazenamento e manutenção destas tabelas de mapeamento, podendo esta quantidade até ser proibitiva.

Uma outra desvantagem surge quando se precisa atualizar estas tabelas quando ocorrer a inclusão (ou deleção) de um novo recurso, pois será necessário atualizar todas as tabelas dispersas pela rede.

- Alocação (compare com a seção II.3.2.b):

Nesta alternativa, assume-se que os recursos, localizados em outras redes diferentes e que são alocados pelos usuários da rede A, não excedem a um determinado número pré-fixado em um determinado intervalo de tempo, sendo utilizados durante um certo período intervalo de tempo, denominado SESSÃO. Este é o comportamento típico de um sistema de tempo compartilhado.

A identificação de um recurso localizado em uma outra rede implica na execução de um procedimento que possui três fases distintas. Na primeira fase , o processo localizado na rede A requisita a uma determinada comporta a alocação de um título, a(i), que será utilizado posteriormente para identificar-se o recurso de nome b(j) localizado em uma outra rede. Este procedimento é denominado de Estabelecimento de Conexão. Após a primeira fase ter sido transcorrida, as mensagens enviadas para a(i) são transmitidas como se fossem destinadas ao

recurso b(j) para uma determinada comporta, que se encarregará de efetuar a substituição dos títulos locais. Finalmente, quando o processo terminar a utilização do recurso, esta associação temporária será desfeita, possibilitando-se com isto a utilização do identificador a(i) por outro processo.

Esta alternativa apresenta como desvantagem principal o fato de se permitir a alocação de um número reduzido de recursos extra-rede durante um determinado intervalo de tempo, embora este número possa ser definido de acôrdo com a necessidade dos usuários.

Ao comparar o esquema de alocação com o de mapeamento chega-se a conclusão de que o esquema de alocação deve ser recomendado quando se tem problemas de espaço nas comportas para se armazenar a tabela de mapeamento.

Por outro lado, o esquema de alocação praticamente exclui a troca de mensagens independentes, como por exemplo, as mensagens de controle. Isto ocorre devido ao ' overhead' causado pelo procedimento de estabelecimento de conexão.

O esquema de Alocação é bastante vulnerável no caso em que as informações sobre as alocações já efetuadas forem perdidas, devido a falhas em uma ou mais comportas.

Apesar de todos estes problemas o método de alocação é o mais utilizado por ser equivalente aos procedimentos seguidos para se alocar um arquivo, por exemplo. Cabe às comportas possuirem mecanismos de recuperação de falhas que evite a perda de informações acima descrita.

Recomenda-se, que ao projetar uma rede isolada de computadores que admita a possibilidade de ser interconectada, o método indicado para a atribuição de títulos comece pela definição de um espaço de nomes hierárquico pois isto reduzirá em muito as dificuldades encontradas.

III.3.2 - Endereços (compare com a seção II.3.3):

Após a obtenção do nome do recurso desejado deve-se obter o seu endereço, ou seja a localização deste recurso. Geralmente, o endereço é obtido através de uma função de mapeamento ou pela utilização do denominado endereço bem conhecido que serve para localizar os recursos mais utilizados.

Embora não existam regras gerais para se identificar os recursos, conforme já foi visto anteriormente, a identificação do recurso e a obtenção de seu endereço é normalmente realizada no anfitrião. Duas estratégias podem ser utilizadas para se definir o espaço de endereçamento dos diversos recursos, que são:

- Endereçamento Hierárquico;

- Endereçamento Único ou Global.

Relembrando, um usuário acessa um determinado recurso pelo seu título,que possui um determinado significado intrínseco, não pelo seu endereço. O anfitrião local a deve utilizar o nome fornecido pelo usuário para obter a localização deste recurso e a partir deste endereço deve ser definida qual será a rota a ser seguida por esta mensagem até o seu destino.

Especificando as diferentes estratégias temos aqui o seguinte:

- Endereçamento Hierárquico:

Neste caso, o endereço é composto de uma sequência de campos, cada um com seu significado associado. A divisão de um endereço em campos permite que o espaço de endereçamento seja constituído em grupos. Por exemplo, um esquema de endereçamento verdadeiramente universal deve ser constituído dos seguintes campos:

<Endereço> ::= <Galáxia> <Estrela> <Planêta> <País> <Rede> <Anfitrião> <Porta>

Como pode ser observado na análise deste endereço, no esquema hierárquico o conhecimento do endereço de um recurso é suficiente para se descobrir a sua localização, por causa da divisão do endereço em campos de significados conhecidos e pré-determinados.

Dentre as VANTAGENS do Endereçamento Hierárquico pode-se citar:

- facilita o roteamento (vide capítulo III.4);

- facilita a definição de novas portas de acesso, cada país podendo decidir internamente quais são os endereços das respectivas redes e por sua vez as redes decidindo os endereços dos anfitriões sem a necessidade de se consultar uma autoridade central normativa para se obter a permissão para se poder utilizar um determinado endereço;

- utilização de valores 'defaults' para os campos não definidos, permitindo com a utilização de endereços mais compactos, já que o tráfego dentro de uma determinada rede não precisar especificar o código da rede e o código do país.

Apesar disto, as seguintes desvantagens podem ser mencionadas:

- definição de endereços estáticos, já que no caso de um recurso migrar de uma rede para outra o endereço terá que ser modificado;

- este tipo de endereçamento aloca um determinado número de endereços para cada país, para cada rede e assim por diante. Este número pode ser restritivo, limitando a

definição de novas redes, por exemplo;

- super-especificação da rota a ser seguida. Por exemplo, considere a existência de um campo no endereço que serve para identificar o nó da rede em que está conectado o anfitrião. Ao especificar o endereço deste anfitrião está se indicando automaticamente o nó em que está conectado, não se considerando a possibilidade deste anfitrião possuir ligações com outros nós, podendo com isto sobrecarregar um determinado nó.

- Endereçamento Global:

Isto não ocorre no caso do endereçamento ser Global. Neste caso, define-se um endereço único para cada um dos recursos que pode ser acessado pelo conjunto de redes. O endereço não possui nenhum indicativo da localização do recurso. A geração de um endereço deste tipo pode ser feita pela utilização de um contador que é incrementado toda vez que se atribui um endereço a um novo recurso.

O esquema de Endereçamento Global pode ser encarado como sendo o caso inverso do Hierárquico. Por exemplo, o direcionamento das mensagens será dificultado, mas um recurso ao migrar leva consigo o seu endereço. A atribuição de novos endereços é mais dificil, pela necessidade de se garantir que este novo endereço é único dentro do espaço de endereçamento considerado, podendo necessitar-se da existência de uma Central de Atribuição de endereços.

- Diferenças entre as duas estratégias:

Para exemplificar a diferença entre os esquemas de Endereçamento Hierárquico e Global será feita uma analogia entre o número de telefone e o número do C.P.F. (Cadastro de Pessoas Físicas do Imposto de Renda). Neste exemplo, a partir do nome de uma pessoa, procuraremos obter o seu endereço utilizando-se os dois métodos.

O conjunto internacional de números telefônicos constitui um exemplo do Endereçamento Hierárquico. Por exemplo, o número de telefone 19Ø76543210 pode ser dividido em campos (1-9Ø7-654-321Ø), cada um com o seguinte significado:

1 - Código do país
9Ø7 - Código da área, ou do estado
654 - Código da estação ou central telefônica
321Ø - Código do assinante

Com este "endereço" do recurso pode-se perfeitamente descobrir a localização deste recurso. Agora, por sua vez, o número do CPF 9Ø422Ø447 não pode ser dividido em campos que tornem possível a localização do portador deste número. O conjunto de números que constitue o CPF é um exemplo de Endereçamento Global.

- Recomendação X.121:

A recomendação X.121 do CCITT regulamenta que as redes públicas de computadores devem utilizar um esquema de endereçamento hierárquico semelhante ao das redes telefônicas existentes. Nesta recomendação, cada anfitrião é identificado por um número decimal formado pelos seguintes campos:

- Código do País;

- Código da Rede;

- Um endereço específico para se identificar um recurso nesta rede.

O endereço completo possui até 14 digitos, dos quais os três primeiros servem para se identificar o país e o seguinte é indicativo da Rede, restando 1Ø digitos para se identificar o recurso da rede. A divisão destes 1Ø digitos não é regulamentada pela norma, cabendo a responsabilidade desta divisão à própria rede, seguindo um determinado critério. Um possível critério seria o de considerar-se os sete primeiros

digitos como identificação do anfitrião e os restantes para se identificar a porta ou o processo desejado.

III.4 - Controle de Rotas em Redes Interconectadas:

III.4.1 - Introdução:

Como foi visto no capítulo II.4 define-se o Controle de Rotas como sendo o conjunto de funções utilizadas para se determinar um caminho físico ou lógico de um ponto, denominado origem, para um outro ponto, denominado destino. No capítulo II.4 foram estudados diversos tipos de controle, sendo analisadas as várias hipóteses que devem ser assumidas no desenvolvimento de um algoritmo de controle de rotas.

No caso de se projetar um algoritmo de roteamento para redes interconectadas, vários outros itens devem ser considerados, dificultando com isto a definição do comportamento do algoritmo. Alguns destes podem ser apresentados:

- SEGURANÇA: por motivos de segurança uma determinada rota não pode ser considerada, devido às características do tráfego. Por exemplo, os Estados Unidos não vai querer que informações ultra-secretas relacionadas à sua segurança sejam enviadas para a Inglaterra passando por Cuba ao invés de ir pelo Canadá;

- LEGISLAÇÃO: um determinado país pode proibir por lei que determinados tipo de tráfego passem ou saiam do país. Por exemplo, a Suécia impede que informações de cidadãos suecos saiam do país, impedindo com isto que uma firma na Noruega possa transmitir a sua folha de pagamento para a Dinamarca passando pela Suécia;

- TAXAÇÃO: o usuário deseja que certas redes sejam evitadas por discordar do esquema de cobrança empregado, ou, de maneira inversa, que certas redes sejam consideradas por apresentar vantagens econômicas em detrimento dos aspectos de eficiência;

- O TAMANHO ÓTIMO de uma mensagem depende de uma série de características técnicas da rede (ver capítulo III.6); então o usuário pode desejar escolher uma rota que melhor se adapte às características de seu tráfego, evitando as redes que imponham limites inferiores para o tamanho do pacote manipulado, eliminando com isto a sobrecarga causada pela compatibilização do tamanho do pacote.

Como pôde ser observado no capítulo II.4, a estrutura básica de dados utilizada pelos algoritmos de direcionamento é a Tabela de Rotas (TR). Esta tabela contem uma entrada para cada ponto possível de destino. Cada uma destas possui as várias opções de caminhos a serem percorridos a fim de chegar ao destino. Estas opções são apresentadas em termos do custo que se terá para chegar ao destino quando se adotar esta rota. Estes custos podem ser definidos de acordo com os objetivos do algoritmo, podendo serem determinados a partir de um dos seguintes pontos:

- atraso mínimo;

- capacidade do canal;

- menor caminho;

- menor taxação;

- evitar certas redes;

- critérios de segurança.

A escolha do critério pode ser fixo, isto é característico do sistema, ou pode ser dinâmico, no caso do próprio pacote conter em seu cabeçalho o critério que deve ser adotado para se determinar qual é a melhor rota a ser seguida.

Como o tamanho da Tabela de Rotas cresce linearmente com o número de possíveis destinos, conclui-se que no caso de

redes interconectadas, e mesmo no caso de grandes redes, o espaço alocado nos nós para estas tabelas pode ser proibitivo. Também como consequência direta do tamanho das tabelas, o custo de atualização é alto, podendo, no caso do direcionamento ser adaptativo, representar uma parcela significativa no tráfego da rede, diminuindo, consequentemente, a capacidade efetiva dos canais de comunicação.

Por causa destes motivos, a adoção de um esquema de Endereçamento Global apresenta um desempenho inferior ao do Hierárquico em termos de Controle de Rotas, pois com a implementação deste esquema diminui-se as Tabelas de Rotas, otimizando com isto a pesquisa da rota a ser seguida, a alocação de memória nos nós e a troca de informações necessárias para a atualização destas tabelas.

A idéia principal para se reduzir o tamanho das Tabelas de Rotas é a de se manter, em cada um dos nós, a informação completa utilizada pelo direcionamento somente para os nós que estão próximos (definidos por algum critério) e informações reduzidas para os nós considerados distantes. Isto é conseguido pela reserva de uma entrada para cada destino considerado próximo e de uma entrada para um conjunto de destinatários considerados remotos. Este conjunto pode representar, por exemplo, uma rede ou até mesmo uma parte de uma rede. Desta forma, a Tabela de Rotas pode ser dividida em dois ou mais níveis, cada um destes níveis correspondendo a um determinado critério de divisão, com um número total de entradas reduzido para o número de grupos considerados remoto mais o número de anfitriões considerados pertencente ao mesmo grupo. Kleinrock e Kamoun em /KLEIL77/ estudam o comportamento e o desempenho de um controle de rotas hierárquico.

O direcionamento com um espaço de endereçamento hierárquico é considerado ótimo da origem até a comporta de saída da rede e da comporta de entrada da rede destino até o destinatário propriamente dito; porém, o algoritmo não será considerado ótimo na sua totalidade por que com a estrutura da

Tabela de Rotas não se consegue distinguir as rotas baseando-se somente na localização do anfitrião de destino na rede. Expressando de outra forma: o somatório das melhores rotas intermediárias não é necessariamente a melhor rota entre a origem e o destino.

Uma outra consequência do direcionamento hierárquico diz respeito à determinação da disponibilidade de um anfitrião localizado em uma outra rede. Como a tabela de Rotas possui uma entrada para cada rede é impossível determinar-se a priori se o anfitrião está ou não disponível. Então, a tarefa de se determinar a disponibilidade de um anfitrião é transferida para a comporta final, causando com isto uma série de transmissões desnecessárias.

III.4.2 - Estratégia de Controle:

No capítulo II.3.4 foram apresentados os diversos tipos de estratégia que podem ser adotados em um algoritmo de Controle de Rotas. Relembrando, a estratégia pode ser:

- FIXA ou DETERMINISTICA: a Tabela de Rotas é calculada uma única vez, não sofrendo alterações durante longos períodos de tempo;

- ADAPTATIVA ISOLADA: a Tabela de Rotas é atualizada a partir de informações obtidas da observação do comportamento do tráfego, de uma forma isolada, sem haver troca de informações entre os diversos nós;

- ADAPTATIVA CENTRALIZADA: existem Centros de Roteamento que têm como função a coleta das informações do comportamento do tráfego que são transmitidas pelos diversos nós para este centro, processar as informações assim obtidas e enviar as tabelas já atualizadas para os nós de comutação;

- ADAPTATIVA DISTRIBUÍDA: a atualização da Tabela de Rotas é feita pelo nó a partir da troca de informações que é realizada pelos diversos nós adjacentes.

Qualquer uma destas estratégias pode ser aplicada para o direcionamento entre-redes, sendo que o Direcionamento Determinístico é o mais fácil de ser implementado devido ao fato de não haver troca de informações, mas é bastante sensível a ocorrência de falhas. O Direcionamento Fixo, ainda que apresente a possibilidade de se considerar rotas alternativas, supre, de certa maneira, esta deficiência mas continua a ser ineficiente por não se adaptar às características de tráfego.

O Direcionamento Adaptativo Isolado é também ineficiente por que deve testar as diversas possibilidades de rotas alternativas a fim de poder detectar quaisquer modificações no comportamento da rede, adaptando-se se necessário. Se este teste for demorado, então os caminhos considerados ruins persistirão por longos períodos de tempo e se, por sua vez, o teste for rápido uma considerável parte do tráfego pode ser direcionado para caminhos mais lentos, podendo por causa disto gerar um congestionamento.

Os algoritmos de roteamento Centralizado concentram os cálculos de atualização das tabelas em um ou mais Centros de processamento possibilitando com isto uma determinação mais precisa das rotas. A centralização apresenta como principais desvantagens o fato de ser mais sensível a falhas, pois as informações sobre o estado da rede podem demorar a chegar a um destes centro, o processamento de atualização das tabelas será mais demorado, e haverá um acréscimo de tráfego nos canais adjacentes ao centro. Além destes pontos mencionados, considerações políticas e administrativas tornam esta alternativa difícil de ser aceita em um ambiente multi-rede (qual das redes deve determinar a rota multi-rede a ser percorrida?).

O Direcionamento Distribuído é o que apresenta a maior

confiabilidade e eficiência, embora uma possível falha no algoritmo possa conduzir a um congestionamento.

Um outra estratégia que pode ser aplicada em interconexão de redes é o Direcionamento na Origem, na qual o anfitrião de origem especifica a rota a ser seguida na sua totalidade ou especifica determinados pontos considerados principais por onde a mensagem deve passar (direcionamento hibrido). A adoção desta estratégia beneficia as Comportas pois elas não mais precisarão realizar o direcionamento e manter as tabelas de rotas. Porém prejudica a eficiência de transmissão devido ao formato do pacote e pelo aumento da sobrecarga causada pelo tamanho do cabeçalho.

Carl Sunshine, em /SUNSC77/, conclui que, para viabilizar a interconexão de redes, os seguintes padrões devem ser aceitos pelas redes participantes:

- um espaço de nomes global deve ser definido, devendo ser adotado o endereçamento hierárquico;

- direcionamento comum entre as diversas redes;

Complementando estas condições, ele recomenda que:

- para preservar a independência da rede local, a técnica de envelopamento dos pacotes multi-rede deve ser adotado, a fim de se possibilitar a transmissão dos pacotes pela rede local, cabendo a comporta desenvelopar, entender o significado do cabeçalho multi-rede e direcionar o pacote;

- o endereçamento hierárquico é preferível ao endereçamento global por manter, de certa forma, a independência das diversas redes;

- o direcionamento na origem é apropriado onde haja uma grande participação do processo de origem na determinação da rota, não levando-se em consideração se a rota escolhida é a melhor ou não.

III.5 - Controle de Fluxo em Redes Interconectadas:

III.5.1 - Introdução:

Como foi apresentado no capítulo II.5, o controle de fluxo consiste nos mecanismos disponíveis utilizados para regular o comportamento de um determinado par origem e destino, a fim de se evitar que o transmissor envie mais mensagens do que o receptor é capaz de processar. Possui como funções principais:

- prevenção da degradação na vazão e perda de eficiência devido à sobrecarga;

- evitar que os bloqueios ocorram;

- distribuição equitativa dos recursos entre os diversos usuários;

- compatibilização entre a capacidade de processamento dos usuários e da rede.

Nas implementações de redes interconectadas que estão ocorrendo (/DARPA80/, /DARPA80b/, /BOGGD80/, /POSTJ80/), o controle de fluxo adotado é o mais simples possível, consistindo de um esquema de janela entre os pontos origem e destino. No caso de uma comporta não ter condições de lidar com um determinado pacote, ela simplesmente destrói este pacote, podendo enviar uma mensagem de advertência para o nó de origem, transferindo desta forma a responsabilidade da manutenção da confiabilidade da comunicação entre as redes para os níveis superiores de protocolo.

Embora o controle de fluxo entre as redes seja relegado a um plano bem primário, ele é importante para o correto funcionamento das redes por permitir a otimização dos recursos da rede, e, por causa disto, necessita-se criar mais um nível

de controle de fluxo que seria relativo ao protocolo de comunicação entre as redes, podendo-se adaptar para este nível os métodos já existentes e aplicados em outros níveis.

Como já foi visto no capítulo II.5, a aplicação dos métodos de controle de fluxo é uma tarefa bastante complexa. Em um ambiente de redes interconectadas esta tarefa se torna bem mais complexa, devido às várias estratégias adotadas pelas diversas redes que constituem o conjunto de redes, dicultando a tarefa de compatibilização destas estratégias. Atualmente, poucas referências são encontradas na literatura especializada que aborde este assunto, embora a maioria das referências sobre controle de fluxo considere como evidente e necessário a criação de mecanismos que permitam às comportas e às redes controlar o fluxo, especialmente quando uma comporta interligar redes de capacidade bastantes diferentes, como no caso de uma conexão de uma rede local de alta capacidade com uma rede pública de capacidade inferior. Típicamente, a diferença de capacidade de uma rede local e de uma rede pública é da ordem de 30 vezes, justificando, por isto, a adoção de procedimentos que permitam controlar o tráfego entre duas comportas e entre a comporta e uma determinada rede.

Quando se exige que um serviço seja estendido por várias redes, novos fatores poderão ser incluídos de tal forma que prejudiquem a prestação do serviço de uma forma eficiente. Os seguintes fatores, que influenciam o controle de fluxo entre redes, podem ser destacados:

- DIFERENÇAS NO TAMANHO DO PACOTE (este fator será abordado com mais detalhes no capítulo III.6): as diversas redes de computadores possuem diferentes tamanhos de pacote e uma das tarefas da comporta é o de efetuar a compatibilização do tamanho dos pacotes através da adoção de mecanismos. Um destes mecanismos é a Fragmentação. Os pacotes de tamanho superior ao permitido pela rede devem ser divididos em pedaços menores denominados fragmentos. A criação destes fragmentos implica que cada um destes possui informações

de endereçamento, para reconstituição do pacote original, aumentando com isto a sobrecarga na transmissão (confirmação de recebimento, retransmissão, etc.). Em particular, a alocação de buffers e' necessária para o processo de fragmentação e para a reconstituição do pacote original. Conclui-se disto, que a maneira em que é implementado o processo de compatibilização do tamanho do pacote, afeta diretamente o controle de fluxo entre redes;

- DIFERENÇAS NAS CARACTERÍSTICAS DE SERVIÇO: as diferenças entre as redes adjacentes podem afetar o controle de fluxo, principalmente os seguintes fatores:

  - meio de comunicação utilizado pela rede;

  - dispersão geográfica;

  - mobilidade;

  - taxas de vazão;

  - atraso fim-a-fim;

  -taxas de ocorrência de erros.

- DIFERENÇAS NAS OPÇOES FORNECIDAS AO USUARIO: as redes podem possuir interfaces do tipo datagrama ou circuito virtual, e oferecer diferentes graus de confiabilidade. As redes do tipo datagrama, por exemplo, não garantem a ordenação das mensagens, implicando com isto que a comporta ou o destinatário reserve mais espaço para buffers a fim de efetuar esta tarefa;

III.5.2 - A função das Comportas no Controle de Fluxo:

Como já foi observado, a comporta é a responsável pela

compatibilização dos serviços entre as redes, servindo de árbitro entre as redes. Um modelo padrão para a interconexão considera a comporta no nível de anfitrião. Esta forma de visualização é a que nos parece mais viável de ser implementada no caso das redes serem heterogêneas, por conseguir definir mais claramente as responsabilidades e os serviços oferecidos. Nesta forma de implementação (ver capítulo III.2.2) a comporta dispõe de todos os serviços de cada uma das redes e também de todas as limitações que um anfitrião sofre ao se conectar a uma rede. Uma outra vantagem desta implementação é a de se poder considerar o controle de fluxo geral a todas a redes interconectadas como sendo o conjunto de todos os controles fornecidos pelas redes intermediárias. Neste caso, além do controle fim-a-fim efetuado pelos processos de origem e destino, poderia ser facilmente implementado o controle de fluxo ao nível de redes interconectadas que seria obtido parcialmente de rede a rede da seguinte forma:

- o controle de acesso da rede origem;

- o controle fim-a-fim do nó origem até a comporta de saída;

- o controle de acesso à rede subsequente dos fragmentos gerados pela comporta;

- e assim repetitivamente, sem precisar realizar a compatibilização dos controles de fluxo de cada uma das redes.

O grau de participação das comportas no controle de fluxo é determinado pelo ambiente multi-rede no qual estão conectadas. Por exemplo, no caso de não existir um protocolo multi-rede global, a comporta terá que se encarregar de efetuar o mapeamento dos protocolos em todos os níveis, limitado pela consequente sobrecarga e pela impossibilidade de se realizar o mapeamento. A segunda possibilidade é quando um protocolo ao nível de aplicação é definido, necessitando-se

efetuar o mapeamento no protocolo de transporte. Aqui, os problemas de mapeamento são simplificados, porque a comporta tem acesso às informações fornecidas pelo nível de aplicação ao nível de transporte.

A outra possibilidade é a integração total do sistema multi-rede em todos os níveis, isto é, existe um protocolo comum de transporte que suporta o protocolo de aplicação. Neste caso, a capacidade da comporta suportar os vários tipos de serviço é determinada pela natureza do protocolo de transporte e pelas suposições consideradas pelos níveis superiores.

Como se pode verificar as comportas tem um papel importante no gerenciamento do fluxo de uma maneira geral. Para obter um melhor desempenho no cumprimento de suas tarefas, a comporta deve considerar os seguintes pontos:

- suportar com um mínimo de sobrecarga os fragmentos: as comportas devem minimizar os efeitos da fragmentação e em casos efetuar a reconstituição intermediária dos pacotes;

- minimizar a perda de pacotes: a comporta deve escolher uma opção confiável para a transmissão dos pacotes a fim de minimizar as suas perdas e consequentemente as futuras retransmissões. As perdas devidas a problemas de congestionamento devem ser minimizadas pela utilização do método de alocação de buffers garantida (vide capítulo II.6), isto é, sempre aceita os pacotes por considerar a sua capacidade de memória infinita (pela presença de uma memória auxiliar);

- otimizar a disponibilidade de buffers: a comporta deve relacionar o número de buffers reservados à demanda de uma determinada aplicação. Isto só ocorre se a comporta tiver conhecimento do comportamento do protocolo de aplicação.

III.5.3 - Controle de Fluxo Fim a Fim:

O esquema utilizado por algumas implementações (PUP e IP) é o método da janela.

Quando a janela fôr pequena, isto é, o número de mensagens transmitidas sem confirmação tender a 1, este método se aproxima do método de confirmação pacote-a-pacote, característico do tráfego interativo. Quando grandes valores de janela são utilizados, a situação se modifica, a confirmação para grandes quantidades de dados só é enviada após ter decorrido um determinado intervalo de tempo, tornando este esquema praticamente insensível à entrega das mensagens fora de ordem, otimizando por causa disto a transmissão de grandes quantidades de dados, isto é a transferência de arquivos.

O valor da janela pode ser objeto de discussão entre os nós de origem e de destino. O valor obtido de comum acordo é de certa forma uma garantia de disponibilidade de recursos no receptor. Se for possível para a comporta conhecer as características de tráfego e a largura da janela, ela poderá destinar um conjunto de buffers especialmente para esta aplicação, e causando, consequentemente, uma influência reduzida nesta transferência.

III.5.4 - Controle de Fluxo Comporta-a-comporta:

Nas implementações atuais, este tipo de controle praticamente não existe, pois se uma comporta não puder aceitar um pacote ele é simplesmente abandonado. Como se trata de um pacote multi-rede a sua chegada ao destinatário só depende do protocolo fim-a-fim que deve detectar a sua ausência e acionar os mecanismos de retransmissão. Este procedimento é aceitável para o tráfego interativo, pois supõe-se que haverá tempo para a comporta se recuperar da

situação de congestionamento antes que o próximo pacote chegue. Entretanto, este procedimento é inaceitável no caso do tráfego ser de transferência de arquivos, porque ao rejeitar um pacote devido a um congestionamento significará a rejeiçao de vários pacotes posteriores antes que esta situação se modifique, envolvendo com isto grandes quantidades de dados e, como consequência direta, uma diminuição na vazão do sistema. O congestionamento costuma ocorrer com mais frequência quando se está transferindo grandes quantidades de dados do que em outros tipos de tráfego, mas a reserva antecipada de buffers só é possível se a comporta dispuser de mais informações a respeito do tráfego.

Na prática, a situação pode ser mais complicada do que a descrita. Como a comunicação comporta-a-comporta pode não ser confiável, a rede local deve garantir esta confiabilidade. Como em alguns casos pode não existir uma confirmação de comporta-a-comporta, a comporta é incapaz de reconhecer se o congestionamento está ocorrendo na rede local ou na comporta de saída, não podendo precisar quais são os pacotes que estão atrasados devido a este congestionamento. Esta situação pode ocorrer quando a comporta está tentando transmitir os pacotes que estão sendo retransmitidos por causa do protocolo fim-a-fim enquanto a rede está ainda tentando transmitir os pacotes anteriores.

Uma solução para este problema é a da comporta transmitir uma advertência para a origem informando que o tráfego deve ser diminuído a fim de solucionar o congestionamento. Esta estratégia elimina alguns dos problemas mencionados, mas pode incluir outros problemas causados principalmente pela má distribuição dos recursos, e pelos procedimentos seguidos quando as mensagens de advertência forem ignoradas ou perdidas.

No caso das comportas serem anfitriões da rede, o controle de fluxo comporta-a-comporta pode ser o mesmo utilizado para o controle fim-a-fim. Desta forma, só serão aceitos novos pacotes se forem satisfeitas as exigências do

controle de acesso e de fluxo fim-a-fim. Isto, certamente poderá aumentar a sobrecarga causada por um pacote multi-rede, apresentando como principal vantagem a possibilidade de se ter um tráfego mais bem comportado entre a origem e o destino.

III.5.5 - Controle de Fluxo Comporta-Rede local:

Neste caso, o controle se resume principalmente no controle de acesso à rede, mas a comporta, sabedora do tipo de tráfego, pode requisitar alguns serviços da rede, em particular se o tipo de tráfego fôr de transferência de arquivos.

Em resumo, a interconexão de redes cria um número enorme de problemas de fluxo, devidos principalmente ao fato de coexistirem vários tipos de controle, um para cada tipo de rede, e das diferentes características de tráfego que são suportadas.

Fazendo-se uma analogia com as redes simples, ao se considerar as alternativas para controle de fluxo, conclui-se da necessidade dos quatro níveis de controle (ver capítulo II.5) e de uma nova forma de controle que é o controle de fluxo comporta-a-comporta e comporta-destino que pode ser equivalente ao controle de fluxo ao nível de nó ou ao próprio controle de fluxo fim-a-fim de cada uma das redes.

Conclui-se também que a tarefa de compatibilização dos controles de fluxo, quando a implementação da comporta fôr ao nível do nó, é de difícil implementação no caso das redes possuirem diferentes métodos de controle. Como exemplo, pode-se mencionar no controle de fluxo ao nível do nó o seguinte: uma das redes é do tipo datagrama e a outra é a do tipo circuito virtual.

III.6 - Fragmentação:

III.6.1- Generalidades:

O tamanho máximo dos pacotes transmitidos por uma rede de computadores varia de rede para rede, podendo ir de 32 bits na rede de Cambridge (/CAMB*78/) até a 8192 bits na rede ARPA. Esta diversidade no tamanho dos pacotes é justificada por uma série de fatores que influenciam o funcionamento e a determinação das características de uma determinada rede de comunicações de dados. Os seguintes fatores podem ser destacados /SHOCJ79/:

- restrição do 'hardware', como por exemplo, o intervalo de tempo adotado pela multiplexação por divisão de tempo (TDM);

- limitações no protocolo utilizado pela rede, como exemplo pode-se citar a adoção de um número reduzido de bits alocados para se especificar o tamanho dos pacotes;

- limitações de 'software' (vide /PATEA8Ø/);

- problemas de alocação de espaço reservado para os buffers nos nós da rede;

- minimização dos intervalos de tempo do armazena-e-envia;

- controle de erros, já que a probabilidade de ocorrência de erros em uma transmissão de dados é proporcional ao tamanho do pacote;

- equidade, isto é a necessidade de se assegurar a utilização por igual dos canais;

- desempenho da rede, talvez o item mais importante, pois

de certa forma engloba os itens anteriormente mencionados;

- conformidade com algum padrão pré-estabelecido;

- arquitetura adotada para a rede;

- aplicação da rede, isto é, qual é o propósito ou destinação considerada para a rede na fase de projeto.

Como se pode observar pela análise dos itens acima, a escolha de um limite para o tamanho do pacote é baseada fundamentalmente no funcionamento interno da rede, precisando-se avaliar criteriosamente as características desejadas para a rede.

O ponto que será abordado nesta seção diz respeito aos procedimentos que podem ser adotados pelo conjunto de redes interconectadas a fim de se garantir a compatibilização do tamanho dos pacotes transmitidos neste ambiente multi-rede.

III.6.2 - Alternativas estratégicas de compatibilização:

III.6.2.a - Adoção de um limite comum para o tamanho dos pacotes multi-rede:

Uma das alternativas para se compatibilizar os tamanhos dos pacotes das diversas redes é o de se estabelecer um limite máximo mínimo para o tamanho dos pacotes que seriam adotados por todas as redes envolvidas no ambiente multi-rede considerado. Este limite pode ser, por exemplo, o Máximo Divisor Comum dos tamanhos limites das diversas redes.

A adoção deste limite pelas redes pode acarretar sérios problemas no desempenho das redes, tomadas isoladamente, pois pode ocorrer um acréscimo de pacotes transmitidos (informação

ou controle), causando com isto uma consequente sobrecarga na rede como um todo e um decréscimo no desempenho da rede devido principalmente a uma má utilização de seus recursos.

Analisando-se os critérios utilizados para a determinação do tamanho máximo dos pacotes para uma rede de computadores pode-se concluir que o estabelecimento de um limite padrão para todas as redes envolvidas não é uma boa solução. Ele é de difícil implementação, já que se faz necessário modificar o comportamento das redes já existentes e por não ser flexível, pois a evolução das técnicas de transmissão de dados viabilizará a adoção de tamanhos maiores para os pacotes.

Esta alternativa pode ser otimizada pelo estabelecimento de um limite máximo para o pacote a ser transmitido baseado no conhecimento das características das redes intermediárias que serão atravessadas pelo pacote, desde que o controle de rotas entre redes adotado seja fixo e efetuado na origem.

III.6.2.b - Evitar as redes "pequenas":

Como já foi visto no capítulo III.4, o algoritmo de rotas baseia-se principalmente na topologia das redes envolvidas e na observação do comportamento das transmissões dos pacotes a fim de se determinar qual é a melhor rota a ser seguida por um determindo pacote até o seu destino.

Nesta alternativa de compatiblização do tamanho dos pacotes o algoritmo de determinação da melhor rota deve também considerar como fator de opção a limitação do tamanho dos pacotes. O algoritmo, ao considerar as restrições impostas por determinadas redes aos tamanhos dos pacotes, evita que estas redes sejam atravessadas, determinando com isto uma rota livre de restrições. No caso de não conseguir determinar esta rota, uma outra alternativa deve ser considerada.

Esta estratégia apresenta como desvantagem principal a

necessidade de se alterar os algoritmos de roteamento, e no caso do algoritmo ser do tipo adaptativo, a propagação do parâmetro "Tamanho Máximo do Pacote" para todos os nós pode ser de difícil implementação.

Esta alternativa é vantajosa quando for adotado um esquema de direcionamento fixo e na origem, facilitando com isto a obtenção do parâmetro anteriormente mencinado.

III.6.2.c - Rejeitar o pacote:

Esta é a estratégia aparentemente a mais simples de ser implementada. Nesta alternativa o pacote que possui um tamanho superior ao permitido pela rede subsequente é simplesmente rejeitado pela comporta.

Esta estratégia apresenta como desvantagem o fato de transferir para os pontos de origem ou para os métodos de controle de fluxo e de rotas a responsabilidade de evitar a rede que rejeitou o pacote. No caso da impossibilidade de se evitar a rede que rejeitou o pacote o anfitrião deve limitar o tamanho do pacote ao tamanho permitido pela rede.

III.6.2.d - Utilizar a fragmentação específica para a rede:

Nesta estratégia o pacote de tamanho superior ao da rede subsequente ao chegar na comporta é dividido ou fragmentado em pacotes menores de tamanho condizente com o da rede subsequente, a fim de possibilitar o transporte destes da comporta de entrada até a próxima comporta ou até o anfitrião de destino, onde o pacote original é reconstituído. Estes pacotes menores são denominados de fragmentos.

Os critérios de divisão do pacote em fragmentos e como o transporte destes fragmentos até a comporta de saída podem ser específicas da rede, isto é, só precisam ser conhecidos pela

rede, não sendo necessário às outras redes saber se o processo de fragmentação ocorreu ou não, pois o pacote original é recomposto na comporta de saída (ver figura III.7).

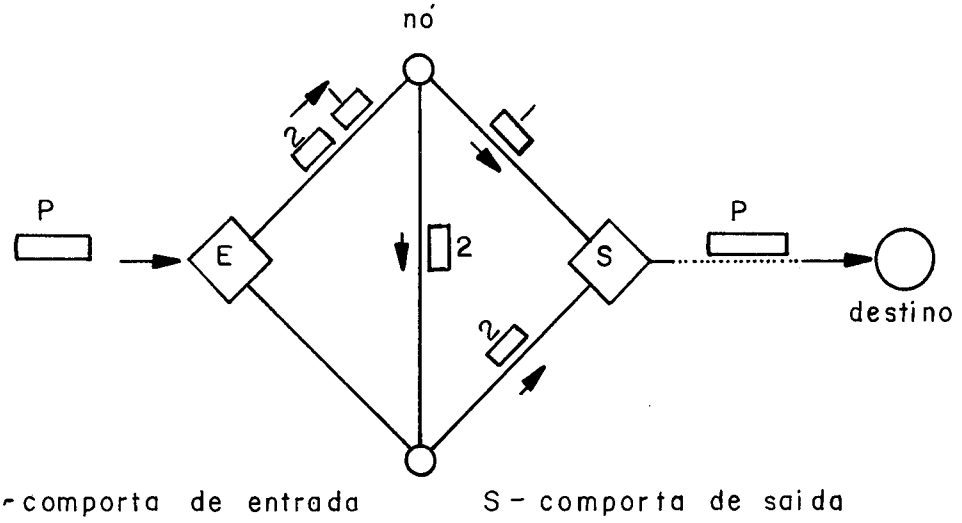


Figura III.7: Fragmentação Específica da Rede

Esta estratégia é a opção mais atrativa do ponto de vista político porque é a mais invisível para as demais redes. Esta invisibilidade é conseguida ao se transferir para as comportas a tarefa de compatibilização do tamanho.

Do ponto de vista técnico, esta opção é atrativa pois conduz a uma melhor utilização dos recursos da rede.

Esta estratégia também pode se aplicar nos casos em que pacotes de tamanho inferior ao limite máximo permitido pela rede subsequente ao, chegarem na comporta, sofram o processo inverso da fragmentação, isto é, o agrupamento de vários destes pacotes em um pacote maior visando com isto a uma melhor utilização dos recursos da rede.

III.6.2.e - Utilizar a Fragmentação Trans-rede:

Nesta opção o pacote de tamanho superior ao permitido pela rede subsequente, ao chegar na comporta, de entrada é dividido em fragmentos, de acôrdo com um critério pré-estabelecido, a fim de possibilitar que estes atravessem a rede. Cada um dos fragmentos gerados segue em sua rota de uma forma independente dos demais até o seu destino onde a reconstituição do pacote original se verificará (ver figura III.8).

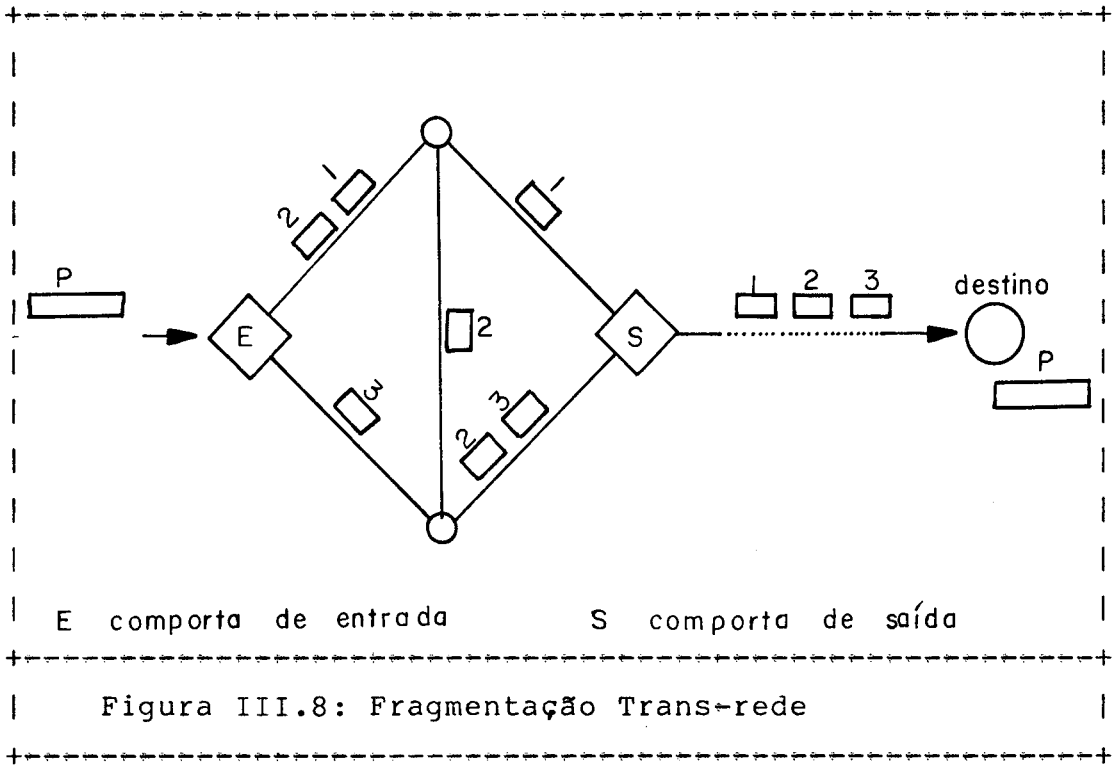


Figura III.8: Fragmentação Trans-rede

Nesta alternativa os fragmentos, por serem independentes, devem possuir um cabeçalho com as informações necessárias para a recomposição do pacote original e para a determinação da rota a ser seguida.

III.6.3 - As alternativas táticas de fragmentação disponíveis para a comporta:

A decisão de fragmentar ou não um determinado pacote ocorre geralmente nas comportas, pois estas, ao receber um pacote de tamanho superior ao que a rede subsequente pode manipular, tem a tarefa de enviar o pacote para o seu destino, ou tomar alguma atitude que contorne este problema. Estas alternativas serão descritas a seguir.

III.6.3.a - Abandonar o pacote:

A comporta se declara incapaz de lidar com o pacote, abandonando-o simplesmente. De certa forma este procedimento é aceitável desde que a informação de rejeição seja propagada até o nó de origem, possibilitando com isto que providências sejam tomadas.

Embora este procedimento seja aceitável, dependendo da estratégia geral adotada ele se torna indesejável pois não condiz com esta estratégia.

III.6.3.b - Fragmentação especifica da rede:

Nesta tática a comporta de entrada escolhe alguma forma de fragmentação especifica da rede, divide os pacotes em fragmentos, enviando-os para a comporta de saída onde ocorre a reconstituição do pacote original.

Esta tática apresenta como principais vantagens /SHOCJ79a/:

- o fato de ser invisível às demais redes;

- a rede pode utilizar um protocolo local eficiente para transportar os fragmentos, não necessitando reaplicar o cabeçalho inter-redes original em cada um dos fragmentos;

- se existir somente uma rede no caminho que necessita da fragmentação, todos os fragmentos gerados serão reunidos na comporta de saída, evitando com isto que eles cascateiem pelo resto do caminho.

Apesar destas vantagens esta tática possui as seguintes desvantagens:

- o fato de existir algum processamento a ser realizado nas comportas e da necessidade da comporta de saída acumular os diversos fragmentos a fim de poder reconstituir o pacote original;

- não se poder tirar partido do fato de existir comportas alternativas nas redes intermediárias, por causa da necessidade de que todos os fragmentos saiam da rede pela mesma comporta a fim de poderem ser reagrupados;

- se existirem várias redes subsequentes ao longo do caminho, então, existirá uma duplicação de tarefas pois o pacote de tamamho superior será sucessivamente fragmentado e recomposto dentro de cada uma destas redes.

Deve-se observar que este tipo de Fragmentação é sempre uma decisão aceitável, independendo se a estratégia adotada é a da Fragmentação Específica ou da Fragmentação Trans-rede. Esta tática é empregada na estratégia de Fragmentação Trans-rede quando o tamanho máximo da rede intermediária não suporta o cabeçalho inter-redes, necessitando-se então utilizar este tipo de fragmentação a fim de que seja possível transmitir este pacote pela rede.

III.6.3.c - Fragmentação Trans-rede:

Neste caso a comporta divide o pacote em fragmentos, tornando-os pacotes inter-redes independentes, necessitando por causa disto endereçá-los para o seu destino final a fim de poderem ser reconstituídos.

O cabeçalho destes fragmentos deve conter as informações a respeito de seu destino, do pacote que lhe deu origem, número de sequência, número do fragmento e de outras informações que possibilitem a reconstituição do pacote original no destinatário.

Este método apresenta como vantagens:

- não há necessidade da comporta de saída efetuar a reconstituição do pacote original;

- não há necessidade dos fragmentos saírem pelo mesmo ponto, possibilitando com isto a adoção de esquemas de rotas alternativas.

As seguintes desvantagens podem ser apontadas neste método:

- a comporta deve fragmentar o pacote de uma forma conhecida por todas as redes, ao invés de poder utilizar uma técnica de conhecimento específico da rede;

- a comporta deve conhecer detalhes dos pacotes inter-redes;

- o cabeçalho inter-redes deve ser aplicado em todos os fragmentos gerados;

- o destinatário tem a tarefa de reconstituir o pacote original.

III.6.4 - Algoritmos de Fragmentação:

Escolhidas a estratégia e a tática a serem adotadas na fragmentação surge a seguinte pergunta: Como deve ser o algoritmo de divisão do pacote cujo tamanho ultrapassar o limite imposto por uma rede?

Dois algoritmos podem ser utilizados para responder a esta pergunta: o da Fragmentação Máxima e o da Fragmentação Balanceada.

III.6.4.a - Fragmentação Máxima:

Considerando que o tamanho do pacote excedente seja L, que o tamanho máximo permitido pela rede seja LMAX e que o número de fragmentos gerados seja N.

Neste algoritmo serão gerados N-1 fragmentos de tamanho LMAX e um fragmento com o restante do pacote original. Explicando melhor, o algoritmo, baseado no tamanho máximo permitido pela rede, gera os fragmentos procurando criar o maior número possível de fragmentos com o tamanho máximo permitido.

III.6.4.b - Fragmentação Balanceada:

Este algoritmo procura gerar os fragmentos de tamanho próximo ao da média do pacote dividido pelo número de fragmentos gerados, isto é: L/N.

III.7 - Protocolos Utilizados em Interconexão de Redes:

III.7.1 - Protocolo de Interconexão PUP /BOGGD80/:

O nome PUP (Parc -Palo Alto Research Center- Universal Packet) serve para identificar um protocolo do tipo datagrama que pode ser aplicado na interconexão de redes. Este protocolo foi desenvolvido pela XEROX, sendo utilizado na ' Ethernet'.

Uma característica importante adotada pelo PUP é a de que os anfitriões constituem a própria super-rede (' internet'). As comportas são simplesmente anfitriões desta super-rede que desejam transmitir os pacotes por diversas redes.

Dois tipos de comporta são distinguidos: as comportas conversoras de protocolo e as conversoras de meio de comunicação. Estas são anfitriões que interfaceiam dois ou mais mecanismos de transporte de pacotes para os quais deverão ser enviados os pacotes multi-redes, constituindo o cerne da estrutura datagrama entre-redes.

As comportas conversoras de protocolo são anfitriões que entendem dois ou mais protocolos de alto-nível (funcionalmente similares, mas incompatíveis), sendo utilizadas para transportar a informação pelas diversas redes e de efetuar o mapeamento dos protocolos. Observa-se que a comporta conversora de meio está fazendo o mapeamento necessário nos níveis inferiores mas, a distinção é útil dada a importância dos datagramas entre-redes nesta arquitetura.

Nesta arquitetura, as comportas conversoras de meio são, por definição, bastantes simples, pois o processo necessário de conversão é o de se preservar a semântica dos datagramas. As comportas conversoras de protocolo são mais complexas, por causa da dificuldade de se compatibilizar os diversos protocolos de mais alto nível. Passaremos a considerar alguns pontos considerados importantes neste protocolo.

- Endereçamento:

Um processo envia ou recebe os PUP's através de uma porta identificada por um endereço, de estrutura hierárquica, constituído de três campos: o número da rede, o número do anfitrião e o número da interface neste anfitrião, consistindo de seis octetos.

- Direcionamento:

Esta implementação utiliza uma estratégia de roteamento distribuída e adaptativa. O processo origem só precisa especificar o endereço de destino. As comportas entre-redes direcionam os PUP's para a rede apropriada, estas roteam para o anfitrião apropriado e este finalmente os direciona para o soquete especificado.

- Controle de Fluxo:

O modelo entre-redes desenvolvido não requer que a super-rede entregue com sucesso os pacotes, pois uma comporta intermediária, que esteja congestionada, pode descartar um pacote embora o sistema deva ser projetado para tornar este acontecimento raro. Se uma comporta é forçada a descartar um pacote devido à presença de congestionamento, ela é obrigada a transmitir esta informação para a origem, cabendo a esta tomar os procedimentos que julgar necessário.

- Confirmação das mensagens:

É de responsabilidade dos processos origem e destino garantir a confiabilidade da transmissão, e as confirmações são utilizadas com o propósito de controle de fluxo e de erro.

- Recuperação de erros:

Como já foi mencionado, a rede PUP tem sempre a opção de rejeitar os pacotes com o intuito de diminuir o congestionamento embora esta não seja a estratégia mais

correta. As estratégias de gerenciamento que tentam garantir a confiabilidade da rede devem ser projetadas para o pior caso, o que não ocorre no caso considerado, já que esta só deve funcionar bem na maioria dos casos. Esta idéia de se sacrificar a garantia de uma entrega confiável dos pacotes se justifica pela simplicidade obtida. Esta consideração transfere para a origem a tarefa de recuperação dos erros.

- Segurança:

Não existe, embora os usuários sejam aconselhados a adotar algum esquema de segurança.

- Estrutura do Cabeçalho:

O cabeçalho é constituído de 20 octetos , incluindo as informações necessárias para o correto direcionamento do pacote. Não existe um estabelecimento de conexão equivalente ao do X.25.

- Fragmentação /BENNC82/:

Utiliza a estratégia de fragmentação específica da rede, exigindo com isto que os fragmentos sejam enviados para a mesma comporta de saída. Destacam-se as seguintes propriedades:

- os fragmentos gerados não são visíveis para as outras redes;

- a fragmentação é aplicada no pacote inteiro e toda vez que ocorrer um pacote de tamanho excessivo;

- não é necessário reaplicar nenhuma informação do pacote original nos fragmentos;

- um pacote não pode prosseguir viagem até que todos os seus fragmentos sejam recebidos.

Em resumo, a arquitetura PUP para redes interconectadas utiliza um protocolo do tipo datagrama, com um esquema de direcionamento distribuído e adaptativo (para maiores detalhes vide /BOGGD80/)

II.7.2 - Protocolo de Interconexão da rede ARPA /POSTJ80/,/DARPA80/:

Este protocolo consiste de dois níveis, que são: o protocolo entre redes (IP -'Internet Protocol') e o protocolo de controle da transmissão (TCP: 'Transmission Control Protocol').

O TCP é um protocolo de transporte, correspondendo ao nível 4 do modelo OSI (vide seção II.6). O IP é um protocolo que fornece o serviço de datagrama, correspondendo ao nível 3 do modelo OSI.

As redes utilizadas possuem os mais diferentes tipos de tecnologia e são referenciadas, impropriamente, de redes locais. A interface com uma rede local é feita através do protocolo da rede local (LNP: 'Local Network Protocol').

Neste protocolo as comportas possuem funções de anfitriões, sendo comuns a duas ou mais redes. Cada comporta é identificada pela rede local da mesma maneira que um anfitrião. A informação necessária para se direcionar o pacote até o seu destino consta do cabeçalho do pacote.

O protocolo IP não tem previsão para os controles de fluxo e para o controle de erros na parte relativa aos dados, simplificando com isto as comportas.

O IP não fornece um serviço equivalente ao do X.25/X.75 (mencionado a seguir), necessitando de que o TCP garanta a entrega ordenada e confiável dos dados.

O TCP utiliza os mecanismos fim a fim para assegurar esta entrega confiável. Para implementar esta função o TCP usa o controle de fluxo, a confirmação positiva das mensagens em um determinado intervalo de tempo. Observa-se que neste esquema, a comunicação gerenciada pelo protocolo entre-redes (IP) é baseada no datagrama e que o circuito virtual estabelecido entre os processos é fornecido pelo TCP. As seguintes características podem ser destacadas:

- Endereçamento:

O tamanho do campo de endereços é fixo. O protocolo entre redes utiliza um campo de 1 octeto para identificar a rede e um outro de 3 octetos para identificar o anfitrião, podendo-se também considerar como endereço o campo de 1 octeto do identificador do protocolo. O TCP utiliza um campo de 2 octetos para identificar a porta pela qual é feita a comunicação com o processo. Os tamanhos mínimos dos cabeçalhos, tanto para o IP quanto para o TCP, são de 20 octetos, podendo chegar a 60 octetos.

- Direcionamento:

Normalmente, o usuário não tem influência na determinação da rota entre redes, embora o usuário tenha a possibilidade de determinar pontos principais da rota a ser seguida. Não existe o procedimento de estabelecimento da conexão, permitindo também que a rota varie no tempo. Como o campo de endereços é grande, não é necessário armazenar muita informação na comporta.

- Controle de Fluxo:

Não existe nenhum mecanismo de controle de fluxo no protocolo entre redes. As comportas não controlam o fluxo porque são incapazes de determinar alguma relação entre as diversas mensagens. As comportas se precavêm do congestionamento pela destruição da mensagem e pelo envio de um aviso para a origem da mensagem rejeitada. O TCP utiliza o

controle de fluxo fim a fim do tipo janela, que é aplicado a cada uma das conexões, para gerenciar a transferência de informações.

- Confirmação das mensagens:

O protocolo entre redes não tem previsão de confirmação. O TCP utiliza as confirmações para controlar o fluxo e detecção de erros. Estas confirmações não estão disponíveis aos usuários.

- Recuperação de Erros:

Os erros na rede ou na comporta resultam do fato de uma mensagem ter sido destruída, podendo ou não o transmissor ter sido avisado. Esta não confiabilidade do IP permite que ele seja bastante simplificado embora exija a utilização de um protocolo fim a fim. O TCP presta as funções de recuperação fim a fim para qualquer mensagem que tenha sido perdida. O TCP utiliza a confirmação positiva, 'timeout' e a retransmissão para assegurar o envio dos dados. Por causa do potencial do direcionamento adaptativo a comunicação fim a fim pode continuar, mesmo com a falha da comporta.

- Segurança:

O IP fornece a opção de transportar as informações relativas à segurança, precedência e grupo de usuários compatível com a AUTODIN II. O TCP possui um esquema de checagem fim a fim que garante a integridade do cabeçalho.

- Estrutura do cabeçalho:

O cabeçalho do IP tem em média 2Ø octetos (podendo ser maior no caso de se utilizar os campos de opções), não necessitando haver o estabelecimento da conexão e a manutenção das informações na comporta. O cabeçalho do TCP possui normalmente 2Ø octetos, existindo um procedimento de estabelecimento de conexão e a manutenção de informações

relevantes nas comportas. Neste caso, existem cabeçalhos e tabelas de informações relativamente grandes.

- Fragmentação:

A fragmentação no DoD é um forma de fragmentação trans-rede, seguindo as seguintes regras:

- os fragmentos podem ser criados por qualquer comporta no caminho entre o transmissor e o receptor. A reconstituição da mensagem original só ocorre no destinatário;

- para cada fragmento criado uma cópia modificada do cabeçalho trans-rede deve ser feita;

- o tamanho de um fragmento é o número de octetos ocupados pelo cabeçalho e pelos dados do usuário.

II.7.3 - Recomendação X.75 do CCITT /POSTJ80/:

As redes públicas de comunicação de dados que seguem a recomendação X.25 do CCITT devem ser interconectadas segundo a recomendação X.75. Como já foi visto na seção II.6, o X.25 é um protocolo que especifica a interface entre o anfitrião (ETD) e o nó da rede (ECD). Este protocolo assume que a comunicação é feita utilizando-se os circuitos virtuais, fornecendo uma interface de circuito virtual para o nível de transporte.

A interface entre duas redes públicas, especificada na recomendação X.75, é bastante similar a do X.25. Os equipamentos utilizados nesta interface são denominados de Terminal de Sinalização (STE - 'Signalling TErminal'). A definição desta interface STE-STE tem aspectos muito parecidos com a interface X.25.

A comporta STE-STE definida pelo X.75 funciona no nível de nó, sendo constituída de duas partes, cada uma das quais é conectada a uma rede pública.

A interconexão de redes públicas utilizando o X.75 resulta em um encadeamento de circuitos virtuais. Cada seção é uma entidade distinta com os seus tipos de controle de fluxo, de recuperação de erros, controle de rotas, etc. Alguns aspectos importantes são analisados a seguir:

- Endereçamento:

Utiliza a recomendação X.121 com um campo de endereçamento de até 15 digitos com cada digito sendo codificado em 4 bits.

- Direcionamento:

O usuário não tem nenhuma influência na definição da rota a ser utilizada. O esquema de direcionamento utilizado é o híbrido, sendo a rota definida através de uma série de pedidos de estabelecimento de conexões. As informações que dizem respeito às chamadas devem ser mantidas nos ETD e ECD de origem e destino e em cada STE intermediário ao longo da rota.

- Controle de Fluxo:

Como já foi dito o caminho a ser percorrido é constituído de uma série de circuitos virtuais independentes, cada um possuindo controles de fluxo independentes, podendo inclusive serem diferentes uns dos outros. Existe, além destes controles independentes, o controle STE-STE que é feito em uma base de chamadas. Este controle de fluxo passo a passo pode introduzir um atraso significativo.

- Confirmação das mensagens:

Existe confirmações intermediárias, isto é, cada trecho do caminho tem a sua confirmação. O significado desta

confirmação é de que o pacote foi submetido à rede subsequente, não significando que ele tenha sido recebido pelo destinatário.

- Recuperação de Erros:

O X.25 e o X.75 não especificam como uma rede deve proceder internamente em caso de erros. Se ocorrer um erro irrecuperável, a rede sinaliza com um comando 'RESET', significando que o circuito virtual ainda existe, mas o controle de fluxo deve ser reiniciado, podendo, inclusive, terem sido perdidas algumas mensagens. No caso de haver um erro mais crítico a ligação virtual é desfeita. No caso de haver uma falha na comporta o circuito virtual é desfeito, por causa de não haver rotas alternativas.

- Segurança:

As recomendações X.25 e X.75 não estabelecem nenhum critério de segurança.

- Estrutura do Cabeçalho:

O cabeçalho do pacote de estabelecimento de conexão é grande, podendo variar de 2Ø até 166 octetos mas, após a conexão ter sido estabelecida o cabeçalho utilizado se reduz a 3 octetos. O cabeçalho reduzido implica na necessidade de se acumular informações a respeito do estado da conexão, nos diversos pontos, ao longo do caminho.

- Fragmentação:

O X.25 permite que os usuários submetam os dados em unidades de tamanho variável, como por exemplo 256 octetos. A recomendação X.75 estabelece como tamanho máximo suportado 128 octetos, significando que os pacotes de tamanho superior devem ser fragmentados pela utilização do esquema de fragementação específica da rede.

Em resumo, o aspecto mais importante da interconexão de redes públicas é que o serviço prestado ao usuário é do tipo circuito virtual com as mesmas propriedades essenciais da rede pública. Obtem-se o serviço pela concatenação de uma série de circuitos virtuais, fixando por isto a rota entre as diferentes redes.

III.8 - Conclusão:

Neste capítulo procurou-se avaliar os problemas que surgem ao se adotar um esquema de Interconexão de Redes e o de se criar uma metodologia que possibilite o estudo das redes interconectadas a partir dos estudos existentes na área de Redes de Computadores. Esta metodologia é justificada por causa da possibilidade de se traçar uma analogia entre as redes interconectadas e as redes simples, da mesma maneira que se pode fazer uma analogia entre o comportamento de uma rede e o de um computador.

O objetivo principal deste capítulo é o de se estabelecer uma base qualitativa que possibilite a posterior análise que será efetuada no próximo capítulo.

IV - Proposta de um modelo para redes interconectadas:

IV.1 - Introdução:

Neste capítulo analisaremos a Interconexão de Redes em seu aspecto analítico, procurando estabelecer uma dependência entre os métodos de Controle de Fluxo, de Controle de Rotas e de Fragmentação.

Esta estudo analítico é feito através da utilização de um modelo matemático. Dentro do enfoque deste trabalho, estabelecer uma analogia entre Redes e Redes Interconectadas, procurou-se avaliar vários modelos matemáticos existentes e aplicados no caso de redes simples, adaptando-os para o caso considerado.

Na primeira fase da modelagem é apresentado um modelo utilizado para se estudar o comportamento dos diversos métodos de fragmentação, obtendo como resultado o número de fragmentos gerados para cada uma das estratégias.

Na fase intermediária, é apresentada uma adaptação do modelo desenvolvido por Pujolle /PUJOG8Ø/ que estuda o comportamento do Controle de Fluxo em uma rede de comutação de pacotes. Este modelo possibilita o estudo de vários métodos de Controle de Fluxo Fim-a-fim e ao nível do nó, supondo que a sub-rede de comunicações não é confiável.

Finalmente, é apresentado a proposta para o modelo que será utilizado para analisar-se o comportamento de um conjunto de redes interconectadas, que é uma adaptação dos modelos anteriormente apresentados. Este modelo serve para estudar a interdependência dos parâmetros anteriormente mencionados. Esta interdependência é demonstrada pelos efeitos causados no comportamento do conjunto de redes ao se variar um destes parâmetros.

IV.2 - Modelagem isolada do processo de Fragmentação /BENNC82/:

Nesta seção estudar-se-á os aspectos necessários para o desenvolvimento de um modelo para a análise do processo de Fragmentação. Este modelo apresenta como resultados o número de fragmentos gerados e a quantidade de dados que está sendo entregue para cada um dos seguintes esquemas:

- Fragmentação Especifica da Rede;

- Fragmentação Trans-rede;

- Nenhuma fragmentação, por causa da determinação de um limite máximo mínimo.

Antes de prosseguir na análise deve-se considerar algumas hipóteses que serão adotadas na modelagem deste processo.

IV.2.1 - Hipóteses:

O PACOTE pode ser definido como sendo um conjunto de octetos consistindo de L(N) octetos relativos ao cabeçalho da rede local, podendo ser seguido de H octetos relativos ao cabeçalho trans-rede e de Ld octetos de dados do usuário.

O CABEÇALHO DA REDE LOCAL (L(N)) segue o formato especificado pela rede N que o pacote está percorrendo em determinado instante. Este cabeçalho deve ser entendido pela própria rede e pelos pontos (nós ou comportas) origem e destino deste pacote na rede considerada. Este cabeçalho pode ser diferente para diferentes redes mas, como no esquema proposto pelo CCITT, o mesmo cabeçalho local deve ser compreendido por todas as redes envolvidas, atuando como se fôsse o próprio cabeçalho trans-rede e assumindo um valor fixo L.

O CABEÇALHO TRANS-REDE (H) possui neste modelo um valor fixo para todos os pacotes trans-redes porém, na prática, alguns protocolos de interconexão permitam que o tamanho deste cabeçalho varie de acôrdo com os campos de opção e de facilidades do protocolo implementado. Para os casos em que o cabeçalho local se confunde com o cabeçalho trans-rede, H é definido como tendo o valor zero.

O TAMANHO DO PACOTE é definido como sendo o número de octetos transportados (isto é, H + Ld) pela rede e entregues ao destinatário na rede considerada. Para cada uma das redes envolvidas existe um TAMANHO MAXIMO PARA O PACOTE (Max(N)), que limita o tamanho dos pacotes transmitidos pela rede N.

O tamanho de um fragmento (excluindo o cabeçalho local mas considerando o cabeçalho trans-rede) é múltiplo da UNIDADE BÁSICA DE FRAGMENTAÇÃO (F) que é definida para cada um dos algoritmos. Logo, um fragmento é constituído de F octetos, embora o processo de fragmentação de um pacote possa gerar pelo menos um fragmento (o último) com um tamanho que não seja múltiplo de F.

Para facilitar o desenvolvimento do modelo isolado para a Fragmentação assume-se que o meio de comunicação é favorável, isto é, não existe perdas de dados trans-rede pelas redes intermediárias, pelo transmissor, pelo receptor ou pelas comportas, não havendo, por ser um meio favorável, retransmissões de pacotes.

Uma outra hipótese simplificadora assumida é o desconhecimento das características da interface trans-rede, isto é, se as redes envolvidas em um determinado caminho apresentam interfaces do tipo datagrama ou circuito virtual. Ao assumir esta hipótese considera-se que não há sobrecarga devido ao fato dos pacotes chegarem fora de ordem.

O objetivo considerado pelo modelo para os algoritmos de fragmentação é o de se produzir o menor número de fragmentos levando-se em consideração que todos os fragmentos são

inferiores ao tamanho máximo admitido pela rede.

IV.2.2 - Descrição do modelo:

IV.2.2.a - Observações básicas:

O processo de fragmentação ocorre se, e somente se, o tamanho do pacote transmitido fôr maior do que o tamanho máximo permitido pela rede, isto é:

$$Ld + H > Max(N). \qquad (iv.1)$$

No caso da estratégia escolhida ser a da Fragmentação Trans-rede é necessário que o tamanho do cabeçalho trans-rede seja inferior ao tamanho máximo permitido pela rede (isto é, H menor do que Max(N)). Se o cabeçalho trans-rede fôr maior ou igual ao tamanho máximo permitido o único método possível de fragmentação que pode ser adotado é o da Fragmentação Específica da Rede.

Para efeitos de medida de desempenho, cabe aqui definir o que vem a ser o TAMANHO MÁXIMO EFETIVO DO PACOTE (Ef(N)). Ef(N) é definido como sendo a quantidade de dados do usuário que pode ser transportada no maior fragmento possível de ser gerado na rede N, sujeito às restrições acima.

A definição exata do valor de Ef(N) depende do tratamento do cabeçalho trans-rede. Se as redes apresentarem uma interface comum para o usuário (por exemplo, X.25 e X.75) o tamanho máximo do pacote não inclui o cabeçalho trans-rede. Neste esquema, denominado Esquema do Cabeçalho Comum (vide figura IV.1(a)), o valor de Ef(N) é:

$$Ef(N) = \lfloor Max(N) / F \rfloor * F \text{ octetos}. \qquad (iv.2)$$

Deve-se observar que:

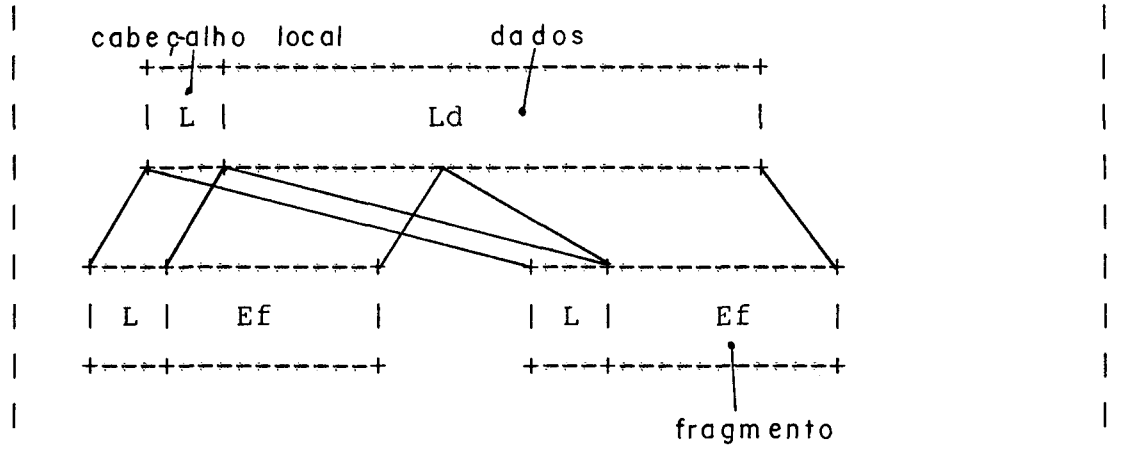
- a função $\lfloor x \rfloor$ significa o maior inteiro menor ou igual a x;

- a função $\lceil x \rceil$ significa o menor inteiro maior ou igual a x.

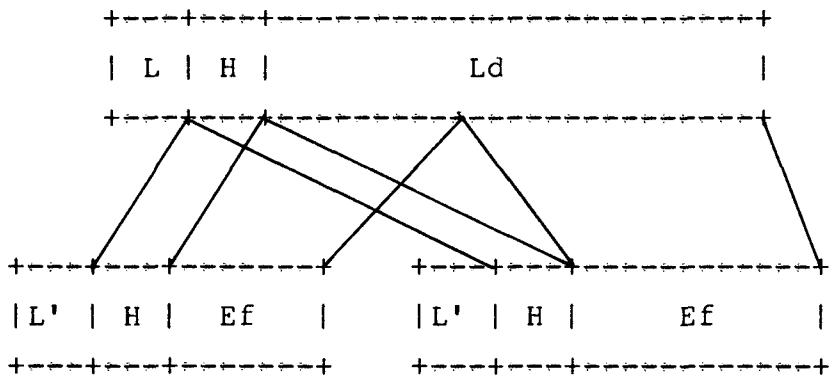
A segunda possibilidade surge quando o cabeçalho trans-rede (H) não é conhecido pelas redes intermediárias, sendo tratado como parte dos dados que estão sendo transmitidos, reduzindo com isto a quantidade de dados transmitidos. Neste caso existem duas alternativas que podem ser escolhidas. A primeira destas alternativas é a de reaplicar o cabeçalho trans-rede em cada um dos fragmentos gerados (vide figura IV.1(b)). Neste esquema, denominado Esquema do Cabeçalho Envelopado, o tamanho máximo efetivo é definido como sendo:

$$Ef(N) = \lfloor Max(N) / F \rfloor * F - H \text{ octetos.} \qquad \text{(iv.3)}$$

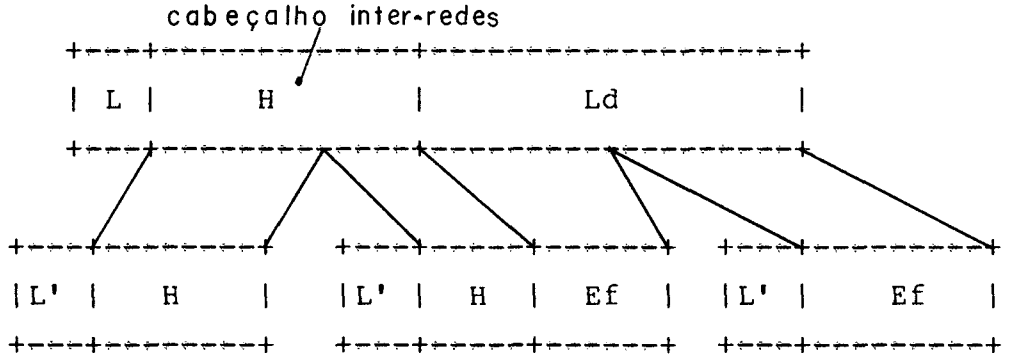
Observa-se que o esquema de cabeçalho comum é um caso particular deste esquema, pois foi convencionado que no caso do cabeçalho comum ser utilizado também como cabeçalho trans-rede o tamanho deste cabeçalho seria nulo (H=Ø).



(a) - Esquema do cabeçalho comum



(b) - Esquema do cabeçalho envelopado



(c) - Fragmentação Específica da Rede

Figura IV.1 - Alternativas de divisão do pacote

A outra alternativa é a da Fragmentação Específica da Rede (vide figura IV.1(c)). Nesta alternativa o cabeçalho trans-rede pode sofrer o processo de Fragmentação, sofrendo o mesmo tratamento dispensado aos dados do usuário. Uma forma de simplificação do tratamento é considerar o pacote como sendo constituído de S + H octetos de pseudos-dados do usuário; com isto, o tamanho máximo de cada fragmento, antes do acêrto do cabeçalho segue as regras do esquema do cabeçalho comum. Observa-se que os "dados do usuário" serão encarados da forma acima no esquema de fragmentação específica, isto é, todo pacote que chegar para ser fragmentado é encarado como sendo um pacote do tipo cabeçalho comum com pelo menos H octetos de tamanho.

Tem-se que o tamanho máximo efetivo do pacote fornece a quantidade de dados do usuário contida no maior fragmento que pode ser gerado. A partir disto o NÚMERO DE FRAGMENTOS GERADOS (Nf(Ld)) pode ser obtido da seguinte forma:

$$Nf\ (Ld) = \lceil\ Ld\ /\ Ef\ (N)\ \rceil. \qquad \text{(iv.4)}$$

Como já foi visto (seção III.6.4), existem pelo menos dois algoritmos de divisão de um pacote em fragmentos respeitando-se as restrições impostas. No primeiro algoritmo, denominado FRAGMENTAÇÃO MÁXIMA, serão gerados Nf(Ld) - 1 fragmentos cada um contendo Ef(N) octetos de dados do usuário. O último fragmento terá o restante dos dados, isto é, se o resto da divisão do tamanho dos dados do usuário (Ld) pelo tamanho máximo efetivo (Ef(N)) fôr maior do que zero o tamanho deste último fragmento será igual a este resto e em caso contrário o último fragmento conterá Ef(N) octetos de dados.

No segundo algoritmo, denominado FRAGMENTAÇÃO BALANCEADA, se são gerados Nf fragmentos, o tamanho de cada um deles é dado pela divisão do tamanho dos dados do usuário (Ld) pelo número de fragmentos gerados (Nf), isto é o tamanho dos fragmentos ficará próximo da média aritmética.

Os tamanhos dos fragmentos resultantes ficarão entre um tamanho operacional mínimo de fragmentos igual a:

$$e'(Ld) = \lfloor (Ld / Nf + H) / F \rfloor * F - H \qquad (iv.5)$$

e um tamanho operacional máximo de fragmento igual a:

$$e(Ld) = \lceil (Ld / Nf + H) / F \rceil * F - H. \qquad (iv.6)$$

O número de fragmentos recebidos pelo destinatário depende não só dos fatores analisados anteriormente mas também dos caminhos que os fragmentos gerados percorrerem no sistema multi-rede. Os efeitos da topologia multi-rede sobre a fragmentação passam a ser considerados.

IV.2.2.b - A Fragmentação ocorre em uma única rede:

Neste caso, os resultados já obtidos são suficientes para fornecer o número de fragmentos recebidos no destinatário. Na estratégia trans-rede o número de fragmentos é expresso por:

$$Nf = \lceil Ld / Ef \rceil. \qquad (iv.7)$$

Para a estratégia específica da rede o número de fragmentos é:

$$Nf = \lceil (Ld + H) / Ef \rceil. \qquad (iv.8)$$

O tamanho dos fragmentos depende dos limites operacionais discutidos anteriormente. Observa-se que, ao adotar a estratégia de fragmentação específica, o processo de fragmentação só vai ser visível para o receptor no seguinte caso: a rede que exige a fragmentação é a última do caminho percorrido, isto é, a rede na qual está conectado o

destinatário. O número de fragmentos recebido é independente da configuração da multi-rede neste aspecto.

IV.2.2.c - Fragmentação em várias redes:

Nesta seção será analisado o caso de haver várias redes intermediárias que necessitem da fragmentação, só existindo um único caminho multi-rede entre a origem e o destino. Como já foi observado, só as configurações trans-rede necessitam ser consideradas e o tratamento aqui desenvolvido é simplesmente uma iteração da discussão anterior.

Considere que o conjunto de redes interconectadas seja {REDE(i)}. As redes envolvidas em uma comunicação multi-rede são identificadas pelo indice i com i variando de Ø a k. Cada uma destas redes possui um tamanho máximo limite para os pacotes igual a Max(i).

Considere que um anfitrião localizado na REDE(Ø) gere um pacote multi-rede contendo Ld octetos de dados do usuário e H octetos relativos ao cabeçalho trans-rede, cujo destino é a REDE(k). Então, para cada uma das redes envolvidas pode-se definir um conjunto de tamanhos efetivos máximo para o pacote ({ Ef(i)}) e tamanho operacionais mínimos ({ ef (i)}) a partir da seguinte condição inicial:

$$ef\ (Ø) = Ef\ (Ø) = Ld \text{ octetos} \qquad \text{(iv.9)}$$

e pela aplicação repetitiva das definições do tamanho efetivo máximo e do tamanho operacional máximo.

A condição necessária para que a Fragmentação ocorra entre redes adjacentes é que um pacote contenha mais dados do usuário do que a capacidade de transporte da rede em seu maior fragmento, isto é, que :

$$ef\ (i) > Ef\ (i + 1). \qquad \text{(iv.1Ø)}$$

O limite no número atual de fragmentos criados pela REDE(i) a partir de cada um dos fragmentos que chega da REDE(i-1) é dado por:

$$Nf\ (i) <= \lceil\ ef\ (\ i - 1\ )\ /\ Ef\ (\ i\ )\ \rceil. \qquad \text{(iv.11)}$$

No caso de estar sendo adotado o algoritmo da fragmentação máxima, o tamanho máximo operacional da REDE(i) (ef(i)) é igual ao tamanho máximo efetivo (Ef(i)), e a fragmentação irá ocorrer se Ef(i) fôr maior do que Ef(i+1). Para o algoritmo balanceado, ef(i) é menor ou igual a Ef(i), causando com isto que este algoritmo produz, normalmente, mais fragmentos menores do que o outro algoritmo. À primeira vista, isto indica que a fragmentação balanceada diminui a probabilidade de ocorrência do processo de fragmentação nas redes subsequentes, o que pode não ser verdade. Esta afirmação é justificada porque o último fragmento gerado pelo algoritmo de fragmentação máxima pode ser suficientemente pequeno de tal forma que evite as fragmentações subsequentes. Isto é, se Nf fragmentos são gerados em um determinado ponto, somente Nf - 1 fragmentos são igualmente prováveis de sofrerem fragmentações futuras se eles tiverem sido gerados pelo algoritmo de fragmentação máxima e no caso do outro algoritmo os Nf fragmentos tem a mesma probabilidade de sofrer futuras fragmentações. O efeito acumulativo desta diferença pode ser considerável e o desempenho dos algoritmos fica bastante dependente da configuração multi-rede, pois podemos ter casos em que os Nf fragmentos gerados pelo algoritmos balanceado não sofram fragmentações subsequentes enquanto que todos os fragmentos gerados pelo outro algoritmos sofram.

A distribuição atual, tamanhos e o número total de fragmentos entregues ao receptor na REDE(k) pode ser determinado algoritmicamente, mas para efeitos do caso considerado os limites inferiores e superiores são suficientes. Os limites do número de fragmentos gerados pelo algoritmo balanceado é:

$$\prod \lceil ef'(i)/Ef(i+1) \rceil <= Nf <= \prod \lceil ef(i)/Ef(i+1) \rceil. \quad \text{(iv.12)}$$

Para o algoritmo de fragmentação máxima os limites seriam:

$$\prod Ef(i)/Ef(i+1) <= Nf <= \prod \lceil Ef(i)/Ef(i+1) \rceil \quad \text{(iv.13)}$$

isto e':

$$\lceil Ef(\emptyset)/Ef(k) \rceil <= Nf <= \prod \lceil Ef(i)/Ef(i+1) \rceil. \quad \text{(iv.14)}$$

Para os esquemas trans-rede $Ef(\emptyset) = Ld$ mas, com a definição de pseudo-dados do usuário, tem-se $E(\emptyset) = Ld + H$ aplicável no esquema de fragmentação especifica, este limite inferior é precisamente o número de fragmentos gerados por este tipo de fragmentação. Baseado nisto, pode-se concluir que a estratégia de fragmentação especifica da rede produz no máximo tantos fragmentos quanto qualquer esquema de fragmentação trans-rede para qualquer tamanho de pacote Ld tal que:

$$\lceil Ld/Ef(k) \rceil = \lceil (Ld + H)/Ef(k) \rceil. \quad \text{(iv.15)}$$

IV.2.2.d- Fragmentação em vários redes com caminhos alternativos:

Será analisado nesta seção o processo de obtenção do número de fragmentos gerados a partir de um pacote de tamanho Ld quando existe a possibilidade de haver rotas alternativas entre as diversas redes.

A obtenção do caminho será efetuada pelo algoritmo de Controle de Rotas, só existindo caminhos alternativos se o algoritmo fôr do tipo dinâmico, com o objetivo de balancear o tráfego entre as redes (para maiores detalhes ver capítulo II.4).

Para facilitar esta análise assume-se inicialmente que a rota escolhida é livre de 'loop', isto garante que existe somente um número finito de caminhos intermediários entre o par origem e destino, e por último assume-se que as probabilidades de se escolher um caminho em um determinado ponto é conhecida e fixa.

Em primeira instância cada possível caminho será analisado em separado, utilizando para isto as técnicas já desenvolvidas. Em cada uma das comportas do caminho, a possível distribuição dos tamanhos dos fragmentos que chegam a esta comporta pode ser determinada pelo conhecimento do caminho já percorrido e pela aplicação do algoritmo apropriado para este trecho.

O número de fragmentos esperado para um determinado tamanho de pacote é obtido pela multiplicação do número máximo possível pela probabilidade deste caminho ser escolhido. Logo, o número de fragmentos que se espera que sejam entregues para o receptor é fornecido por:

$$Nf(Ld) = \sum_{P(j)} \{ p(P(j)) * Nf(Ld, P(j)) \}. \qquad \text{(iv.16)}$$

onde P(j) é o j-ésimo caminho entre a origem e o destino e p(.) é a probabilidade de que um determinado caminho seja escolhido e Nf(.,.) é o número de fragmentos, calculado de acôrdo com o algoritmo apropriado.

IV.3 - Modelo isolado de Controle de Fluxo:

Nesta seção serão abordados os aspectos necessários para o desenvolvimento de um modelo para a análise do comportamento do Controle de Fluxo em uma rede de comutação de pacotes. O modêlo apresentado é uma adaptação do modelo descrito em /PUJOG80/. A adaptação feita neste modelo foi a introdução das características da sub-rede de comunicação, sendo analisados quatro tipos de técnicas utilizadas em redes locais de computadores.

IV.3.1 - Métodos de Contrôle de Fluxo:

- Controle por janela (WFC: 'window flow control'):

Este tipo de controle é utilizado em diversas redes de computadores, podendo ser considerado como sendo um caso particular do controle isarítmico. Neste controle o tamanho da janela (w) define o número máximo permitido de mensagens enviadas simultâneamente e não confirmadas entre dois computadores anfitriões. Quando a janela é fechada não se permite que sejam realizadas mais transmissões, até que seja recebido a confirmação de recebimento da outra máquina.

- Controle de fluxo por taxa (RFC: 'rate flow-control'):

Este tipo de controle é exercido pela limitação do número de pacotes que podem acessar a rede. Se o destinatário fôr capaz de lidar com todos os pacotes que estão sendo recebidos não há necessidade de se bloquear o anfitrião de origem. Porém, se houver um excesso de tráfego começarão a surgir filas de mensagens e eventualmente chegando a bloquear os nós. Para evitar esta possibilidade é conveniente que cada

anfitrião receba de cada nó a informação do número máximo de pacotes que ele pode aceitar. Baseado nesta informação os anfitriões podem então limitar as suas transmissões a um número ótimo de pacotes por unidade de tempo.

- Controle de fluxo induzido pela recomendação X.25 (XFC):

Como foi observado no capítulo II.6 a recomendação X.25 é composta de três níveis ou camadas; no nível 1 é definido a interface física, no nível 2 estão localizados os procedimentos de acesso ao canal e de controle de erro. O nível 3 implementa os circuitos virtuais que são, comparativamente, livres de erros, destinando-se principalmente para o controlar o fluxo. Relembrando, um circuito virtual se torna disponível pela troca de pacotes de controle antes que a troca de informações possa ocorrer, sendo utilizado um mecanismo de janela para cada um dos circuitos virtuais.

A recomendação X.25 não especifica como a informação de controle deve ser interpretada, isto é, se o nível 3 implementa o controle de fluxo fim-a-fim ou se implementa o controle entre o anfitrião e o nó.

Assume-se neste modelo que o X.25 implementa o controle de fluxo fim-a-fim, e que o pacote de 'set-up' utilizado no início do estabelecimento do circuito virtual reserva recursos quando em trânsito pela rede. No caso destes recursos serem buffers serão alocados tantos buffers quanto for o tamanho especificado para a janela. Em resumo, o controle de fluxo global induzido pela recomendação X.25 é baseado na autorização fornecida pela rede (enviada pelo Receptor) a fim de possibilitar a transmissão de um novo pacote. Esta autorização de transmissão de um pacote será fornecida somente se houver pelo menos um buffer disponível em cada um dos nós pelos quais o pacote deverá passar. Se uma super-alocação de buffers fôr permitida para os circuitos virtuais, novos

pacotes entrarão na rede até que o limite imposto seja atingido.

Uma observação queve de ser feita é que neste modelo, os tempos de estabelecimento e de liberação dos circuitos virtuais são considerados despreziveis, não sendo considerados para efeito de modelagem.

IV.3.2 - Especificação da rede de comutação de pacotes:

Antes de descrever o modelo, será considerada a estratégia de retransmissão dos pacotes rejeitados por causa de ' overflow' devido à limitação de buffers nos nós de comutação. Duas possibilidades serão analisadas:

- Retransmissão pelo nó, a técnica mais comum. Nesta técnica o pacote que não puder ser aceito por um determinado nó é rejeitado, cabendo ao nó imediatamente precedente retransmiti-lo a partir de uma cópia mantida neste nó, que deve ser mantida até que a transmissão tenha sucesso.

- Retransmissão pelo anfitrião, na qual o pacote é rejeitado ao chegar em um nó que esteja lotado, cabendo ao anfitrião de origem a responsabilidade de retransmissão deste pacote.

Além destas técnicas é necessário considerar-se os procedimentos de transmissão nó-a-nó, isto é, qual é o comportamento da transmissão dos pacotes entre dois nós consecutivos tomados isoladamente. Dois procedimentos são analisados neste modelo, descritos a seguir.

IV.3.2.a - Procedimento "Envia e Espera" (EE):

Neste procedimento o nó antes de transmitir um novo pacote deve esperar que o pacote anteriormente transmitido seja confirmado. Na figura IV.2 está representado os estados do transmissor e do receptor durante a transmissão de um pacote.

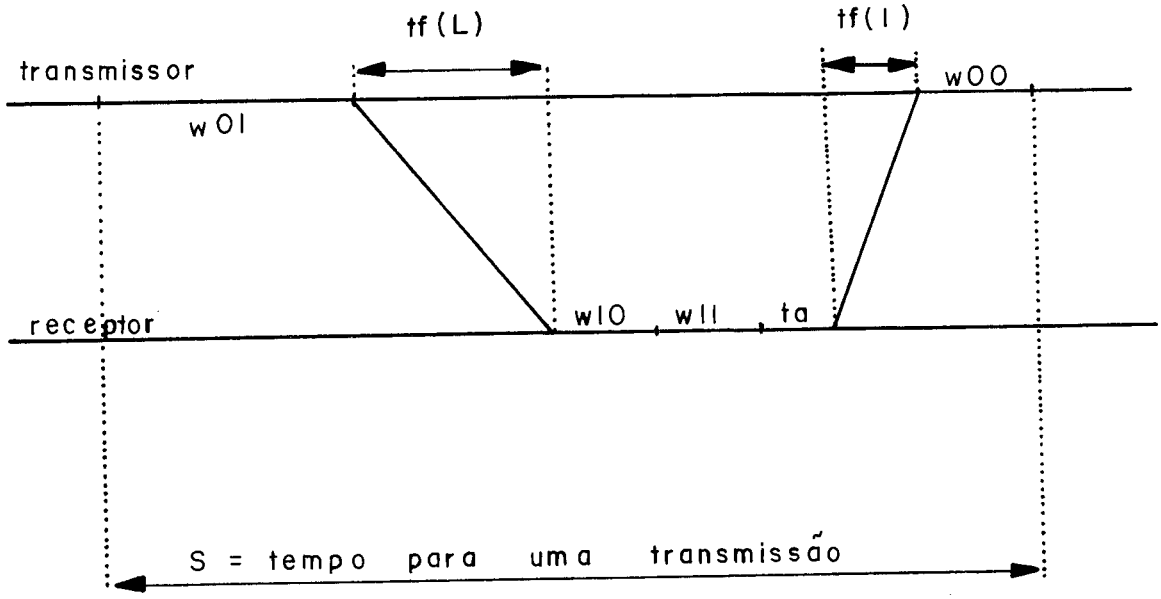
O tempo total necessário para a transmissão de um pacote é denotado por S. O tempo médio total é dado por:

$$S = w\emptyset\emptyset + w\emptyset 1 + tf(L) + w1\emptyset + w11 + ta + tf(1). \qquad (iv.17)$$

A variável ta representa o tempo gasto por um pacote anteriormente transmitido até que a sua transmissão termine. Este tempo varia de acordo com a carga existente nos canais. Se os canais estiverem com pouca carga este tempo será praticamente nulo. Em condições de sobrecarga o tempo médio gasto será equivalente à metade do tempo de transmissão de um pacote.

O comportamento do tráfego é considerado simétrico, isto é, existem quantidades iguais de tráfego em ambos os sentidos.

Denotando por RO a carga de um canal, tem-se que o tempo de serviço S será mínimo quando a carga fôr mínima (RO=Ø) e será máximo quando a carga for máxima (RO=1), assumindo-se que a variação do tempo de serviço de seu valor mínimo até o seu valor máximo é linear.



onde

w00,w10	:	tempos devidos ao procedimento de comutação e do 'software' utilizado para manipular o pacote;
w01,w11	:	atraso de escrita em ambos os sistemas;
L	:	tamanho médio dos pacotes a serem transmitidos;
l	:	tamanho do pacote de controle que retorna com a confirmação
ta	:	representa o tempo médio que o pacote anterior, se existir leva para terminar a sua transmissão;
tf	:	tempo de transferência.

Figura IV.2 - Comportamento do Envia e Espera

Considerando que:

$$Cb = w00 + w01 + w10 + w11 + tf(1), \qquad (iv.18)$$

a fórmula (iv.17) pode ser simplificada para:

$$S = tf(1) + Cb + tf(1) * RO / 2. \qquad (iv.19)$$

A variável S é definida como sendo o tempo necessário para transmitir com sucesso um determinado pacote. Agora, se ocorrer um erro durante a transmissão ou se o pacote for rejeitado por causa de um ' overflow' em um dos nós uma cópia terá que ser retransmitida após ter decorrido o intervalo de 'time-out'. Conforme foi demonstrado em /GELEE78/, o desempenho do procedimento nó-a-nó não é sensível à probabilidade da ocorrência de pacotes com erro para os valores usuais desta probabilidade, podendo ser desprezada para efeitos de modelagem. Logo, a retransmissão de um pacote só irá ocorrer para o caso de ' overflow', no receptor. A probabilidade de ocorrer um ' overflow' é representada pela variável p.

Se for utilizada a técnica de retransmissão pelo nó (rn) a cópia será retransmitida após o intervalo de tempo T com uma probabilidade p. Logo, o tempo médio real para uma transmissão, não considerando-se a retransmissão no caso do pacote ter sido perdido, é:

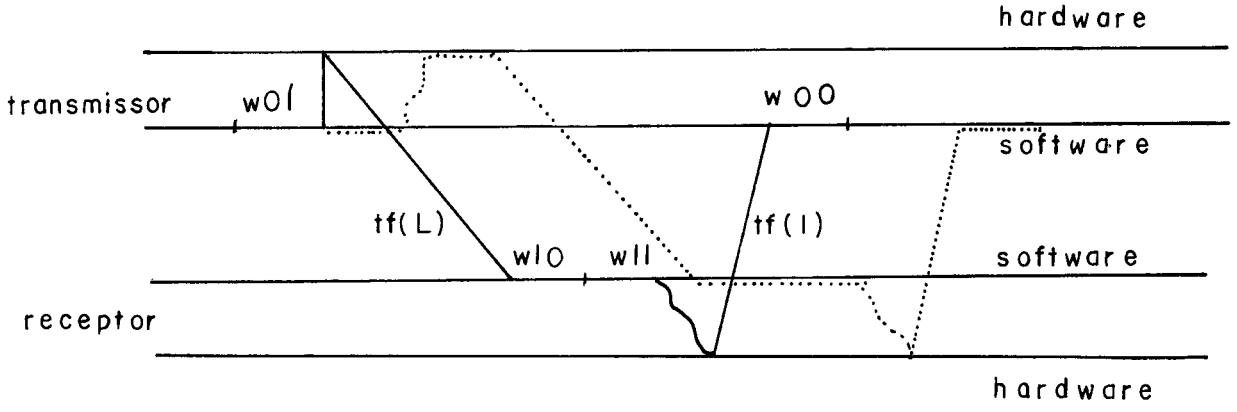
$$S.EE.rn\ (RO) = (tf(1) + Cb + tf(1)*RO/2) * (1 - p) + T*p. \qquad (iv.20)$$

No caso da retransmissão pelo anfitrião, o ' overflow' é detetado após o envio da confirmação (o óverflow' é detetado pelo nó), logo o tempo médio para uma transmissão é:

$$S.EE.ra\ (RO) = tf(L) + Cb + tf(L) * RO / 2. \qquad (iv.21)$$

IV.3.2.b - Procedimento do HDLC:

O procedimento sugerido pelo HDLC tem sido aceito como sendo um padrão internacional. Seu comportamento é mostrado na figura IV.3.



vide fig. IV.2

Figura IV.3 - Procedimento do HDLC

Uma janela é definida entre o transmissor e o receptor sendo que o tamanho da janela define o número máximo permitido de pacotes não confirmados simultâneamente em trânsito entre dois pontos.

Devido ao paralelismo dos processos o tempo efetivo necessário para a transmissão é difícil de ser calculado, sendo uma função do tamanho da janela. Entretanto, em /GELEE78/ mostrou-se que a vazão, neste caso, só é limitada pelos tempos de transmissão se a largura da janela não tiver sido escolhida adequadamente (a largura deve ser suficientemente grande para que não ocorra bloqueio do transmissor). Logo, o tempo médio de transmissão para esta estratégia é:

$$S.HDLC.rn\ (RO) = tf(1) * (1 - p) + T * p \qquad (iv.22)$$

e

$$S.HDLC.ra\ (RO) = tf(L) \qquad (iv.23)$$

IV.3.3 - Descrição do modelo:

Considerando que o roteamento seja fixo, o anfitrião transmite os pacotes para um determinado destino por um único caminho da rede, que consiste de uma série de nós intermediários conectados por canais de comunicação. Somando-se a estes pacotes, provenientes do anfitrião, deve-se considerar os pacotes provenientes de outros anfitriões, denominados pacotes externos, que passam pelo mesmo caminho utilizando os serviços providos pelos nós intermediários.

Ao assumir que a tráfego da rede é simétrico, está-se considerando que o número de pacotes externos que chegam a um determinado nó é igual ao número de pacotes externos que estão saindo do mesmo nó após ter decorrido o tempo de serviço. Em média, assume-se que é o mesmo pacote que está percorrendo a fila do tipo tandem. Esta afirmativa é correta devido ao fato da distribuição de entrada para cada uma das filas ser do tipo Poisson.

Logo, o caminho percorrido por um pacote é modelado como sendo uma rede de filas do tipo tandem, consistindo de k + 1 filas. O usuário (o pacote) percorre o sistema juntando a (i+1)-ésima fila após a i-ésima estação para i variando de 0 a k - 1.

A primeira estação, correspondente ao anfitrião, possui um número infinito de buffers, por hipótese. A capacidade destes buffers é de no máximo um e somente um pacote por

buffer considerado. Todas as outras estações possuem um conjunto finito (M(i)) de buffers, isto é, existe espaço em cada uma das estações para no máximo M(i) pacotes. Este tamanho limitado corresponde à capacidade de armazenamento dos canais e nós que fazem parte da rota considerada. O modelo pode ser visualizado na figura IV.4.

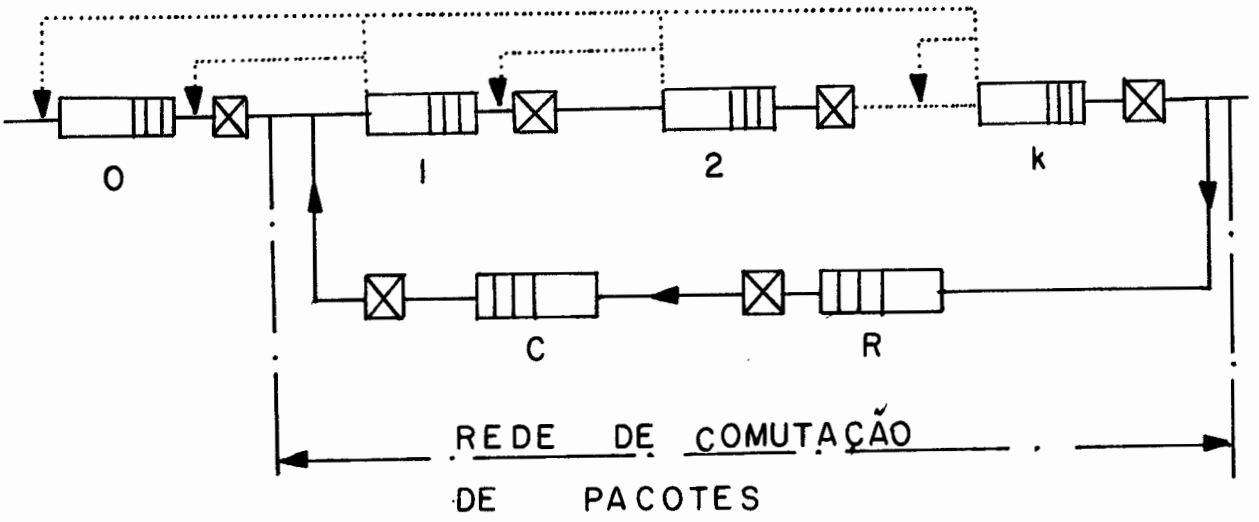


Figura IV.4 - Modelo Matemático Unificado

Analisando a figura IV.4, tem-se as técnicas de retransmissão representadas pelas linhas tracejadas e a estação C representa os créditos necessários para poder se transmitir um pacote. Se a fila desta estação estiver vazia o anfitrião deve esperar por um crédito antes de poder transmitir um pacote. O número de créditos na rede é denotado por N. Quando um pacote deixa a rede o crédito é retornado para o anfitrião; este retorno é representado no modelo pela estação R. Esta estação representa o tempo de retorno da confirmação dos pacotes anteriormente transmitidos contendo os créditos liberados. Quando um pacote vai da estação Ø (o anfitrião) para a estação 1 o crédito é retirado da estação C, voltando a ser considerado no instante da confirmação.

A análise das três estratégias de controle de flucxo

podem ser caracterizadas no modelo da seguinte forma:

No Controle de Fluxo por janela, o número total de créditos que estão circulando em uma determinada rota fim-a-fim representa a largura da janela. Observa-se que se o número de créditos fôr menor ou igual ao valor mínimo do número de buffers disponíveis em cada um dos nós, significando com isto que existe pelo menos um buffer disponível em cada um dos nós a fim de possibilitar-se a transmissão de um novo pacote. Esta consideração se aplica na estratégia XFC.

Se o número total de créditos fôr maior do que o somatório do número máximo de buffers disponíveis em cada um dos nós e assumindo-se que a estação R não exista, tem-se uma rede sem controle de fluxo.

Finalmente, no caso do controle de fluxo por taxa basta impor-se uma limitação no estudo de uma rede sem o controle de fluxo.

IV.3.4 - Solução do modelo:

Vários critérios podem ser utilizados para se avaliar o desempenho de modelos matemáticos aplicados a redes de computadores. Como se está lidando com Controle de Fluxo necessita-se de um indicador de desempenho a fim de se possibilitar a avaliação do sistema. Para este indicador pode ser escolhida a comparação da variação da vazão a partir da utilização do anfitrião, isto é, o comportamento do canal de transmissão entre o anfitrião transmissor e o primeiro nó de comutação. Este parâmetro foi escolhido por permitir a comparação dos diversos controles de fluxo apresentados de uma maneira unificada e por este ser um dos parâmetros utilizados para se controlar o tráfego que está acessando a rede.

A solução do modelo foi desenvolvida em duas etapas:

- O modelo sem as estações C e R;

- O modelo considerando estas estações.

Para se poder resolver o modelo, as seguintes hipóteses simplificadoras foram admitidas:

- Independência: em uma rede de comutação de pacotes, cada pacote transmitido mantem o seu tamanho quando está indo de um nó para outro e os tempos de serviço não são considerados independentes. Neste modelo assumiu-se a hipótese simplificadora da independência sugerida por Kleinrock /KLEIL76/ que supõe que toda vez que uma mensagem é recebida em um determinado nó um novo tamanho será determinado para o pacote, independentemente da função de distribuição;

- a distribuição dos tempos de serviço de todas as estações são idênticas e o valor médio é dado por S (RO), onde RO é a utilização do servidor no anfitrião. Supõe-se que todas as estações tem a mesma taxa de utilização, comportamento típico de redes balanceadas;

- o usuário ao deixar uma determinada fila vê o sistema em seu estado de equilíbrio, isto é, a probabilidade de um pacote ser rejeitado é considerada igual à probabilidade da próxima fila estar cheia.

Os cálculos desenvolvidos para este modelo estão apresentados no apêndice A , sendo somente apresentado nesta seção um resumo deste desenvolvimento.

A partir de uma dada utilização RO do anfitrião é calculada a probabilidade p de que um pacote seja rejeitado pela rede retornando ao anfitrião. Logo, o tempo de transmissão médio é obtido a partir de S (RO) cujo valor depende do protocolo de transmissão nó-a-nó e da estratégia de retransmissão adotados pela rede.

A partir da obtenção do tempo médio chega-se ao valor da taxa total de chegada (LAMBDA.T):

$$LAMBDA.T = RO / S(RO). \qquad (iv.24)$$

Esta taxa é o somatório dos pacotes que estão chegando à rede e dos pacotes reciclados, logo a vazão total do sistema será:

$$LAMBDA = LAMBDA.T * (1 - p). \qquad (iv.25)$$

IV.4 - Proposta de um modelo para redes interconectadas:

Convém aqui ressaltar que o objetivo deste trabalho é o de se propor um modelo matemático que permita estudar o comportamento de um conjunto de redes de computadores interligadas a partir dos modelos matemáticos existentes e aplicados ao caso de redes simples de computadores.

O modelo a ser analisado deve apresentar além das características internas de cada uma das redes que compõem o conjunto, aspectos considerados relevantes que só aparecem quando se considera o conjunto de redes na sua totalidade, que são o processo de fragmentação e o Controle de Fluxo entre redes.

Na literatura, foram encontrados poucos modelos matemáticos para o caso de redes interconectadas. Um destes modelos é o proposto por Kleinrock e Kermani em /KLEIL78b/. Neste modelo é introduzido o conceito de redes equivalentes, isto é, duas redes são consideradas equivalentes se a capacidade de tráfego e o atraso máximo de ambas as redes são idênticos. O estudo de um conjunto de redes se resume então no estudo da rede equivalente ao conjunto. O trabalho estuda duas configurações típicas de redes interconectadas: a ligação em série ou em tandem e a ligação em paralelo das redes. Cada uma das redes é caracterizada baseado em três parâmetros: a capacidade da rede, o número de nós da rede e o tamanho da janela que é utilizada para se controlar o fluxo. A partir destes parâmetros é desenvolvido um modelo que permite calcular o atraso e a vazão de uma rede isoladamente. A partir deste modelo isolado extrapola-se o modelo para o conjunto de redes.

Apesar de considerar este trabalho importante para a modelagem de redes interconectadas e também pela introdução do conceito de redes equivalentes achou-se que este modelo não correspondia ao objetivo do trabalho, além de apresentar as seguintes restrições:

- não considera a fragmentação;

- só analisa um tipo de controle de fluxo;

- não considera as características da sub-rede de comunicações;

- não considera a forma de implementação do protocolo entre redes (Extremo ou ' Endpoint' e Passo-a-passo ou 'hop-by-hop').

Por causa destas restrições procurou-se avaliar outras propostas, como a que foi apresentada por Carl Sunshine em seu trabalho, considerado como sendo um clássico desta área /SUNSC77/. Neste trabalho o conjunto de redes é visualizado como sendo uma super-rede de computadores. As comportas que interligam as diversas redes são consideradas como sendo super-nós desta super-rede e as redes isoladamente são consideradas como sendo, simplesmente, canais de comunicação que interligam os computadores anfitriões aos super-nós e super-nós a outros super-nós. Este modelo é apresentado na figura IV.5.

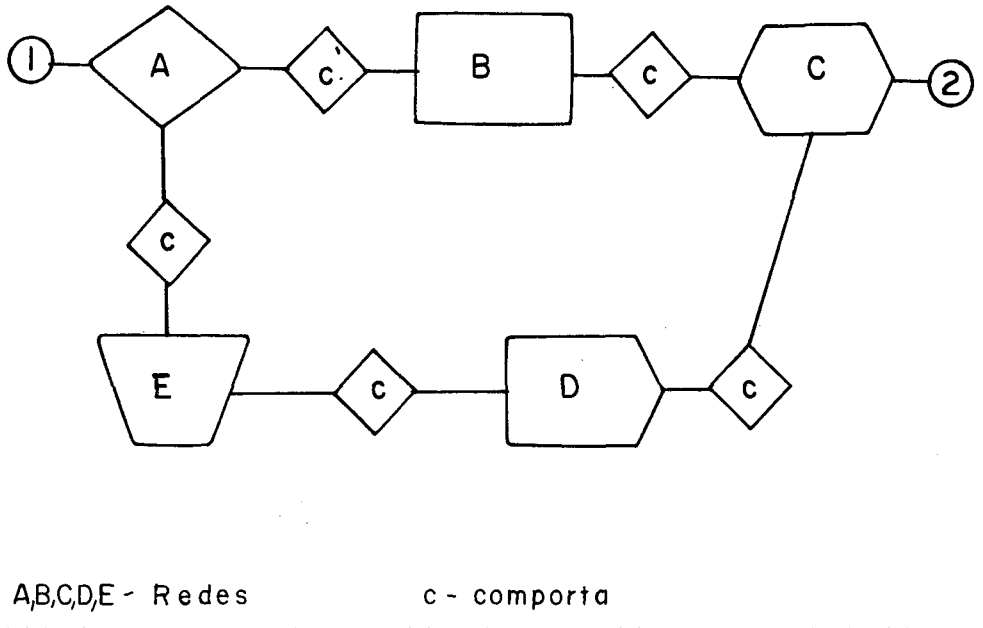


Figura IV.5: Modelo da Super-rede

Um aspecto interessante deste modelo é a possibilidade de cada um dos canais desta super-rede possuir diferentes protocolos de comunicação, exigindo com isto que os super-nós suportem o protocolo específico para este canal, isto é, em última análise para a rede que está interfaceando. Esta forma de visualização possibilita a análise da fragmentação e da compatibilização dos protocolos que porventura seja necessária.

Como as comportas são consideradas nós desta super-rede que, é constituída pela conexão de várias redes locais, devem também suportar funções típicas de um nó, tais como:

- controle de fluxo;

- alocação de buffers;

- controle de acesso;

- monitoração de desempenho;

- direcionamento das mensagens, etc.

Uma outra justificativa para a adoção deste modelo é a analogia que se pode fazer ao se considerar um conjunto de redes interconectadas como sendo uma super-rede, podendo-se por causa disto basear-se o estudo da interconexão em um estudo de redes de computadores, que é bastante desenvolvido. É isto o que será tentado demonstrar neste trabalho.

IV.4.1 - Apresentação do modelo:

Antes de começar a descrever o modelo deve-se considerar algumas hipóteses. A primeira destas hipóteses é a que a interconexão é realizada ao nível de anfitriões, isto é, a comporta é constituída de duas partes, cada uma das quais é um anfitrião que conhece bem o protocolo da rede ao qual está conectada. Considera-se que a comunicação entre estas partes é eficiente e o tempo gasto nesta comunicação desprezível. A forma de funcionamento destas comportas-anfitriãs é a seguinte: ao receber um pacote inter-redes ela deve realizar o processo de compatibilização do protocolo e o processo de fragmentação. Após ter executado estes processos a comporta deve submeter os fragmentos do pacote para a rede subsequente.

Uma outra consideração é a de que os pacotes multi-rede estão envelopados, isto é, os pacotes multi-rede que são constituídos de uma parte de dados e de uma parte relativa ao cabeçalho inter-redes são submetidos à rede como dados, devendo, por isto, serem acrescidos do cabeçalho da rede considerada.

Finalmente, considera-se que o tráfego entre as redes seja equivalente.

Para melhor apresentar o modelo, considerar-se-á uma

rota qualquer, determinada segundo algum critério, que ligue os anfitriões origem (1) e destino (2) das mensagens entre redes (vide figura IV.6)

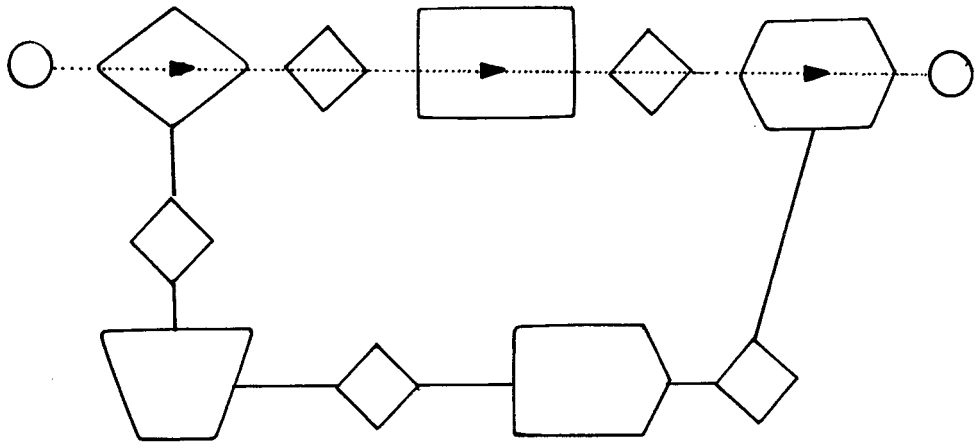
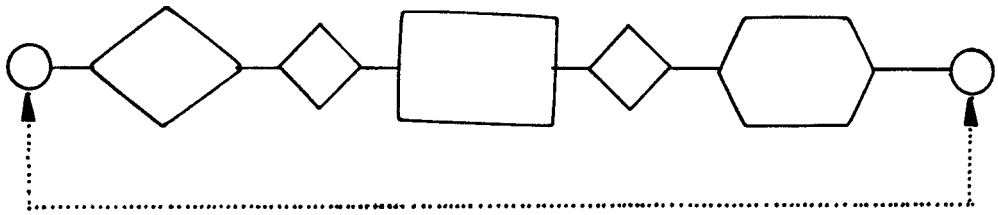


Figura IV.6: Determinação de uma rota

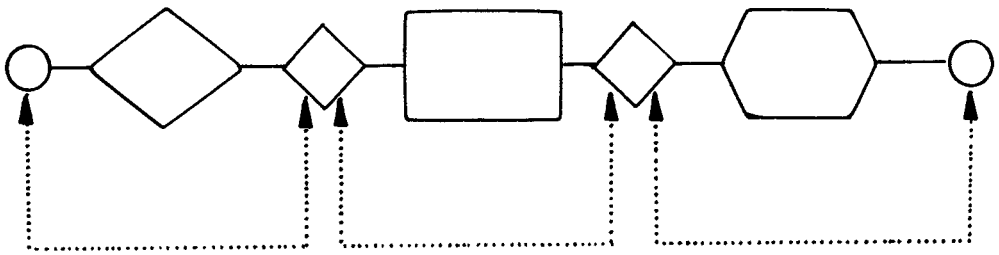
Isolando-se a rota escolhida tem-se:

Figura IV.7: Rota escolhida isolada

Como já foi visto no capítulo III.2, o conjunto de redes pode ser implementado de duas maneiras distintas: extremo (ver figura IV.8.(a)) e passo-a-passo (ver figura IV.8.(b)). Na primeira forma de implementação a ligação entre as redes é do tipo datagrama, não sendo necessário o gerenciamento das chamadas virtuais, podendo-se transferir os pacotes por uma rede utilizando-se a estrutura interna de datagrama. Possibilita a adoção de caminhos alternativos para os pacotes, não se exigindo que estes saiam pelo mesmo ponto da rede. Apresenta como principais desvantagens a necessidade de padronização do protocolo entre redes e pela utilização de grandes cabeçalhos para os pacotes.



(a) Extremo (' endpoint')



(b) Passo a passo ('hop by hop')

Figura IV.8: Métodos de Implementação

Na segunda forma de implementação, a ligação multi-rede é realizada pela concatenação de chamadas virtuais entre as diversas redes. No caso de uma das redes ser do tipo datagrama, deve-se exigir que todos os pacotes multi-rede saiam da rede pela mesma comporta, cabendo a esta realizar o gerenciamento da chamada virtual.

Para efeitos de retransmissão dos pacotes multi-redes

recusados ou por causa do controle de fluxo ou por causa da ocorrência de erros pode-se considerar que na forma de implementação Extremo a responsabilidade de retransmissão é do anfitrião de origem, enquanto que na outra forma de implementação a retransmissão ocorre nos pontos intermediários, possibilitando com isto um melhor desempenho no caso de uma das redes intermediárias possuir altas taxas de erro (se a rede fôr por rádio, por exemplo). Neste caso particular, pode-se dizer que, por analogia com as redes simples na implementação passo-a-passo, o esquema de retransmissão é o da retransmissão pelo nó, cabendo à comporta de entrada a tarefa de retransmitir o pacote e na outra implementação o esquema de retransmissão é o da retransmissão pelo anfitrião de origem, permanecendo válidas todas as considerações da seção IV.3.

Para facilitar a visualização do funcionamento do modelo proposto adotou-se a proposta de Edge de considerar o comportamento do conjunto de redes interconectadas como sendo realizado em três níveis /EDGES79/ (ver figura IV.9):

- o nível de protocolo fim-a-fim, entre os processos origem e destino;

- o nível das comportas, entre as diversas comportas de entrada e saída;

- o nível das redes individuais.

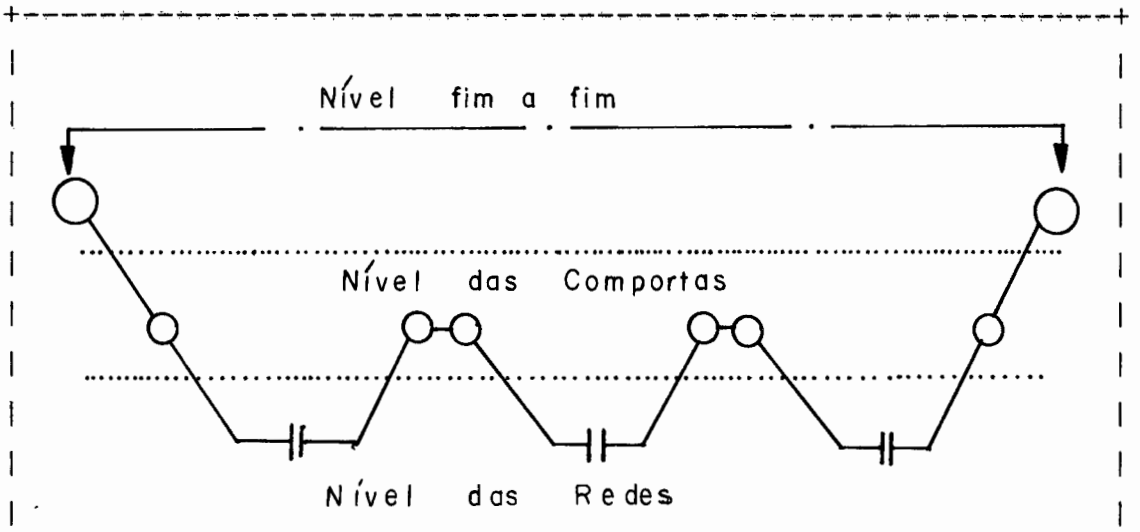


Figura IV.9: Divisão em Níveis da Super-rede.

IV.4.2 - Descrição do modelo:

O processo origem gera os pacotes multi-rede de acordo com uma distribuição geral de intervalos entre chegadas. Cada um destes pacotes possui um determinado tamanho que segue uma distribuição exponencial de média Mi.p. Esta distribuição pode variar de acôrdo com o tipo de tráfego, isto é, se o tráfego fôr interativo a média será inferior a média no caso do tráfego ser de transferência de arquivos, mas para este modelo esta possibilidade não será considerada.

O processo origem ao gerar um pacote multi-rede deve se comunicar com a entidade que deve envelopar os pacotes de acordo com o protocolo da rede e despachá-lo para o seu destino. Esta entidade pode ser considerada como sendo uma comporta degenerada, sendo representada no modelo pela entidade x.

Este pacote multi-rede, após sofrer os efeitos do controle de fluxo da primeira rede, chega à comporta de saída, após ter transcorrido um tempo t(1). Ao chegar na comporta, o pacote pode sofrer ou não o processo de fragmentação. No caso

do pacote ser fragmentado, os fragmentos obtidos de acordo com um determinado método serão submetidos à rede subsequente após um determinado intervalo de tempo representado por tfrag.

Após este intervalo de tempo (tfrag) ter decorrido é enviada a confirmação de recebimento do pacote para a comporta anterior. Os fragmentos são envelopados e submetidos à rede subsequente, sofrendo os processos de controle de acesso e de fluxo. Este processo é repetido até que os fragmentos do pacote multi-rede cheguem à comporta degenerada y que deve reconstituir o pacote original (se necessário) e encaminhá-lo para o processo de destino, que ao receber o pacote irá realizar a consistência da mensagem recebida e enviar para o anfitrião de origem. Esta mensagem de confirmação sofre os mesmos processos anteriormente descritos.

Como se pode observar o modelo apresentado é equivalente ao visto na seção IV.3, bastando para isto fazer-se algumas analogias:

- a rede considerada no modelo da seção IV.3 passa a ser a super-rede;

- os nós da rede simples equivalem às comportas;

- os canais da super-rede são as próprias redes de computadores simples

Esta analogia será agora discutida. Para tanto, considere a figura IV.1Ø, que mostra o comportamento do protocolo "Envia-e-espera", já discutido na seção IV.3.

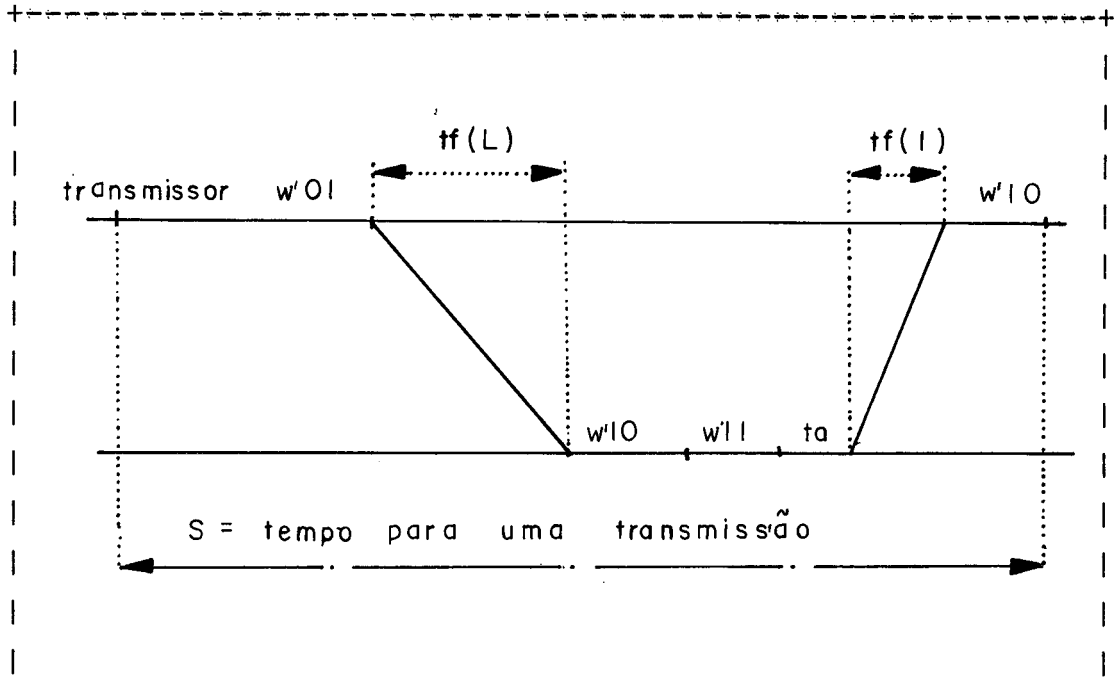


Figura IV.1Ø: Comportamento do Envia e Espera

O significado de cada uma destas variáveis será alterado, a fim de se poder demonstrar a equivalência entre os modelos.

w'Ø1, w'11: tempo gasto na geração e no envelopamento do pacote;
w'ØØ : tempo devido ao processamento da confirmação de recebimento;
w'1Ø : tempo devido ao processamento efetuado no recebimento do pacote, na possi'vel recomposição e no tempo gasto no processo de fragmentação;
L : tamanho médio dos pacotes transmitidos;
1 : tamanho do pacote de controle que retorna com a confirmação;
ta : representa o tempo que o pacote anterior, se existir, leva para terminar a sua transferência;
tf : tempo de transferência gasto pela transmissão de um pacote pela rede.

Neste caso são considerados quatro tipos de sub-rede de comunicação que podem ser utilizadas em redes locais de computadores. Estas tecnologias são:

- anel do tipo 'token' ('token ring')

- 'slotted ring'

- barra de acesso randômico ou de acesso múltiplo com deteção de colisão (CSMA/CD: 'carrier sense multiple access with collision detection');

- barra de acesso ordenado ou de acesso múltiplo multi-nível (MLMA: 'multiple level multiple access').

A expressão destes tempos de transferência pode ser obtida no apêndice B.2.

Considerando-se estas definições, o modelo, descrito na seção IV.3, pode perfeitamente ser adaptado para se estudar o comportamento de redes interconectadas, desde que se respeite a descrição dos níveis propostos por Edge, como será demonstrado a seguir.

Temos que o tempo total necessário para a transmissão de um pacote é denotado por S. Este tempo, para o caso de redes interconectadas, é igual ao somatório dos tempos parciais obtidos nas redes intermediárias multiplicado pelo número de fragmentos gerados para a rede em questão, como será demonstrado a seguir.

Fazendo as mesmas considerações efetuadas na seção IV.3.2.a, temos que o tempo médio total gasto na transmissão de um pacote pela REDE(i) é dado por:

$$S'(i) = w'00 + w'01 + tf(L) + w'10 + w'11 + ta + tf(1) \qquad \text{(iv.26)}$$

Considerando que:

$$C'b = w'00 + w'01 + w'10 + w'11 + tf(1), \qquad (iv.27)$$

a fórmula (iv.26) pode ser reescrita da seguinte forma:

$$S'(i) = tf(L) + C'b + tf(1) * RO / 2. \qquad (iv.28)$$

A variável tf(L) representa o tempo gasto na transferência de um pacote de tamanho L pela rede considerada. O seu cálculo varia de acordo com o tipo de tecnologia adotada pela rede (vide anexo B). A carga na rede considerada é representada por RO.

A variável S'(i) representa o tempo necessário para transmitir com sucesso um determinado pacote, não sendo considerada a hipótese de haver rejeição do pacote. Havendo esta possibilidade, o valor do tempo médio real para a transmissão com sucesso de um pacote é dado por:

$$S'(i) = (tf(L) + C'b + tf(1)*RO/2) * (1-p) + T*p \qquad (iv.29)$$

onde p: probabilidade de um pacote ser rejeitado
T: intervalo de tempo para ocorrer uma retransmissão.

Observa-se que o tempo S'(i) é o tempo gasto na transmissão de um pacote pela REDE(i). Considerando que estamos interessado na transmissão de um pacote por várias redes, devemos considerar os efeitos da fragmentação nesta tarefa. Considerando que um pacote original de tamanho L gere Nf(i) fragmentos na REDE(i) temos que, o tempo gasto na transmissão do pacote original é dado pela expressão Nf(i).S'(i).

Este tempo corresponde, também, ao tempo de ocupação de um buffer de tamanho L na comporta de entrada a esta rede, que só será liberado após a transmissão ter sido completada com êxito.

Desta forma, demostrou-se que o tempo total gasto na transmissão de um pacote trans-rede é dado pela fórmula:

S= Somatório { Nf(i).S'(i) } (iv.29)

para i variando de 1 até n.

Após ter-se determinado o tempo gasto na transmissão de um pacote pode-se determinar, da mesma forma que na seção IV.3, a taxa total de chegada dos pacotes:

LAMBDA.T = RO / S(RO). (iv.3Ø)

Como esta taxa é o somatório dos pacotes que estão chegando ao conjunto de redes e dos pacotes reciclados, a vazão total do sistema é determinada por:

LAMBDA= LAMBDA.T * (1-p) (iv.31)

Uma observação que deve ser feita é a de que a ocupação dos buffers na comporta de entrada se processa em dois níveis. O primeiro, corresponde ao nível entre redes, destinado para o procedimento de fragmentação e o outro relacionado aos fragmentos gerados. A liberação destes buffers é feita de uma forma independente. A partir da determinação do tempo gasto na ocupa,ão de buffers nestes dois níveis, pode-se, perfeitamente, determinar a quantidade de memória necessária para estes buffers, possibilitando com isto uma avaliação mais criteriosa deste problema.

Uma outra observação que deve ser ressaltada diz respeito à fragmentação. Os seguintes efeitos da fragmentação podem ser destacados:

- o número de fragmentos gerados por uma rede influencia diretamente o tempo de transmissão do pacote trans-rede;

- o tamanho do fragmento afeta diretamente o cálculo do tempo de transmissão deste pela rede;

- o consequente acréscimo de processamento devido às tarefas de compatibilização do tamanho dos pacotes.

V - Resumo e Conclusões:

Em resumo, apresentou-se neste trabalho um estudo relacionado a Interconexão de Redes de Computadores, abordando com mais detalhes a interdependência dos seguintes parâmetros:

- Controle de Fluxo;

- Controle de Rotas;

- Fragmentação.

Demonstrou-se que o estudo destes parâmetros deve ser feito em conjunto e não de uma forma isolada, como tem sido abordado na literatura.

Como foi observado o processo de Fragmentação pode ser evitado pelo Controle de Rotas a nível global, desde que os algoritmos de direcionamento considerem a limitação do tamanho máximo dos pacotes como um fator de decisão.

A escolha de uma estratégia de Fragmentação pode ser também influenciada pelo Controle de Rotas a nível de rede individual, por causa das características intrínsecas da estratégia adotada. A estratégia de Fragmentação específica da rede, por exemplo, necessita que todos os fragmentos saiam da rede pela mesma comporta, eliminando com isto a vantagem do Controle de Rotas adaptativo no caso da rede apresentar um comportamento do tipo datagrama.

A fragmentação afeta diretamente o Controle de Fluxo. Uma das primeiras causas é a necessidade de ocupação de espaço nas comportas a fim de que seja realizado o processo de Fragmentação, diminuindo com isto a disponibilidade de espaço nas comportas e aumentando, consequentemente, a possibilidade de congestionamento.

O tempo de ocupação deste espaço é função do controle de

acesso da rede subsequente. O método de Fragmentação cria, a partir de um pacote, vários fragmentos que devem ser submetidos à rede seguinte. Cada um destes fragmentos sofre o controle de acesso particular a esta rede, aumentando com isto o tempo de retardo do pacote e por conseguinte o tempo de ocupação do espaço de armazenamento nas comportas.

Com o surgimento dos fragmentos o Controle de Fluxo fim-a-fim aumenta a sua complexidade, por causa da necessidade de se acumular as várias confirmações dos fragmentos a fim de se poder confirmar o recebimento do pacote. Esta confirmação deve ecoar por todas as redes percorridas até chegar ao nó origem.

Para analisar-se o comportamento da Interconexão de Redes foi desenvolvida uma metodologia de estudo que permite avaliar os pontos críticos relativos a redes interconectadas através da comparação com o caso de uma rede simples de computadores, procurando-se distinguir os pontos principais em ambos os casos e traçar uma analogia que permitisse adaptar os estudos relativos a redes de computadores, já existentes e comprovados, ao caso de redes interconectadas.

Esta metodologia foi posta a prova no capítulo relativo a modelagem, no qual se procurou traçar este paralelo e pela proposta de um modelo que permitisse o estudo da interdependência dos métodos de Controle de Fluxo, de Rotas e de Fragmentação, a partir de modelos já existentes e aplicados ao caso de redes simples.

Concluímos que a analogia feita é satisfatória por cumprir os seus objetivos e permitir a adaptação de váris estudos já realizados a uma nova situação , que é a Interconexão de Redes.

Convem destacar que este trabalho é pioneiro, no sentido de se comparar os métodos de Fragmentação considerando-se os aspectos relativos ao controle de fluxo e de rotas (ver /BENNC82/).

Neste trabalho foram considerados somente três fatoras relativos a Interconexão de Redes. Uma possível extensão para este trabalho seria o de se estudar outros fatores importantes a fim de se fazer uma avaliação crítica de todos os componentes da Interconexão de Redes.

Uma outra possível extensão seria a de se propor um protocolo geral de interconexão de redes, no qual fossem considerados todos os pontos levantados e que fosse utilizado o modelo proposto para efetuar as análises quantitativas a fim de poder validar a proposta.

Uma outra extensão seria a de se realizar a interconexão de duas ou mais redes a fim de se avaliar a validade dos itens mencionados.

Cremos que este trabalho é importante por mostrar uma tendência e por levantar vários aspectos relativos à redes de computadores, advertindo aos projetistas das novas redes da necessidade de se, ao projetar uma nova rede, prever a possibilidade desta rede ser interconectada com outras redes.

VI - Bibliografia:

ABRAN77 - ABRAMSON, Norman; The Throughput of Packet Broadcasting Channels; IEEE Transactions on Communications, Vol COM-25, NO.1, Jan.1977, pp.117-128;

ALLEA78 - ALLEN, Arnold O.; Probability, Statistics, and Queueing Theory; Academic Press, Inc..

ARDEB80 - ARDEN, Bruce W., Hikyu Lee; Analysis of Chordal Ring Network; Proceedings of the Workshop on Interconnection Networks for Parallel and Distributes Processing 21-22 abril de 1980 - Editor: Howard Jay Siegel

AROKR76 - AROKIARAJ Richard, Shyam Johari; Design and Analysis of a Centralized Data Communications System; Proceedings of the IFIP Regional Conference, Singapore, 6-9 Setembro de 1976

AUER*77 - AUERBACH PUBLISHERS; Bit-oriented Data Link Control Protocols; Data Communications Management 53-01-10

BADEM75 - BADEL M., A.V.Y. Shum; Accuracy of an Approximate Computer System Model; IRIA Research Report 130, 1975.

BARBG80 - BARBERIS, Giulio; A Useful tool in the theory of Priority Queueing; IEEE Transactions on Communications, VOL.COM-28 NO.9 SEPT.80, PP.1757-1762

BASSC80 - BASS, Charlie,Joseph S. Kennedy, John M. Davidson; Local Networks gives new flexibility to Distributed Processing; ELECTRONICS , SEPT, 25 1980 PAG.114-122

BAUMD79 - BAUM, D., W. Lehmann-Barrefeld, R.Popescu-Zeletin e K. Ullmann; End-to-end Level Data Flow Analysis for

Communication Networks; Flow Control in Computer Networks;

BELLJ81 - BELL, James R.; Future Directions in Computing; COMPUTER DESIGN Março 1981,pp.95-102

BELSD77 - BELSNES, DAG, Ejvind Lynning; Some problems with the X.25 Packet level Protocol; Computer Communication Review - SIGCOMM - OCT 77 VOL.7 NO.4

BENNC79 - BENNET, C. J.; Supporting Transnet bulk data transfer; Flow Control in Computer Networks (79)

BENNC82 - BENNET, C.J.; The Overheads of Transnetwork Fragmentation; Computer Networks, 6(1982) pp.21-36;

BERGM80 - BERGAMO, M.A., A.S. Campos; REXPAC - A Brazilian Packet Switching Data Network; Proceedings of the Fifth International Conference on Computer Communications - ATLANTA, 27-30 OCT. 80

BERTD80 - BERTSEKAS, D. P.; A class of optimal routing algorithms for communication networks; Proceedings of the Fifth International Conference on Computer Communications - ATLANTA, 27-30 OCT. 80

BLACR80 - BLACKSHAM, R. E., I.M. Cunningham; Evolution of Open Systems Interconnection; Proceedings of the Fifth International Conference on Computer Communications - ATLANTA, 27-30 OCT.80

BLANR80 - BLANC R.P., J.F. Heafner The NBS program in Computer Network Protocol Standards Proccedings of the Fifth International Conference on Computer Communications - ATLANTA, 27-30 OCT. 80

BLEVJ80 - BLEVANUS J., G. Mitaut The use of X.75 in the TRANSPAC International Gateway Proccedings of the Fifth International Conference on Computer

Communications - ATLANTA, 27-30 OCT. 80

BOCHG80 - BOCHMANN G.V., P. Merlin; On the Construction of Communication Protocols; Proceedings of the Fifth International Conference on Computer Communications - ATLANTA, 27-30 OCT. 80

BOGGD80 - BOGGS, David R., John F. Shoch, Edward A. Taft, Robert M. Metcalfe; PUP: an Internetwork Architecture; IEEE Transactions on Communications , VOL. COM-28 APRIL 1980 PP. 612-624

BOORR77 - BOORSTYN, Robert R., Howard Frank; Large Scale Network topological optimization; IEEE Transactions on Communications Jan.77

BOORR81 - BOORSTYN, Robert R., Adam Livne; A technique for adaptive routing in networks; IEEE Transactions on Communications , VOL. COM-29 NO.4, APRIL 81 PP. 474-480

BOSER81 - BOSEN, Robert; A low-speed local net for under $100 per station; DATA COMMUNICATIONS - DEC.81, PP.81-83

BOZZM80 - BOZZETTI, M., P.C. Ravasio; Internetting among Local and Long Haul Networks: a case study; Proceedings of the Fifth International Conference on Computer Communications - ATLANTA, 27-30 OCT.80

BUX*W80 - BUX, Werner, Karl Kummerle, Hong Linh Truong; Balanced HDLC Procedures: a performance analysis; IEEE Transactions on Communications, VOL. COM-28 NO.11 NOV.80, PP.1889-1897

BUX*W81 - BUX, Werner; Local area subnetworks: a performance comparison; IEEE Transactions on Communications, VOL. COM-29 NO.10 OCT 81 PP. 1465-1473

CALOS81 - CALO, Seraphin S.; Message delay in repeated service

tandem connections; IEEE Transactions on Communications, VOL. COM-29 NO.5 MAY 81, PP. 670-678

CAMB*78 - Universty of Cambridge; Computer Laboratory; General Outline of Ring; 27/04/78

CARLD80 - CARLSON, David E.; Bit-oriented Data Link Control Procedures; IEEE Transactions on Communications, VOL COM-28 NO.4 APRIL-80 PP. 455-467

CERFV74 - CERF, Vinton G., Robert E. Kahn; A Protocol for Packet Network Intercommunication; IEEE Transactions on Communications, Maio 1974

CERFV75 - CERF, Vinton G.; An assesment of ARPANET Protocols; Proceedings of the Jerusalem Conference on Information Technology;

CERFV76 - CERF, V.G., A. McKenzie, R. Scantlebury, H. Zimmermann; Proposal for an International End to End protocol; Computer Communication Review, Jan.76

CERFV78 - CERF, Vinton G., Peter T. Kirstein; Issues in Packet Network Interconnection; Proceedings of the IEEE, VOL. 66 #11, NOV-78

CHANK79 - CHANDY, K.M., Victor Holmes, J.Misra; Distributed Simulation of Networks; Computer Networks 3(1979) PAG.105-113

CHOUW79 - CHOU W., J.D. Powell, A.W. Bragg Jr.; Comparative Evaluation of Deterministic and Adaptive Routing; Flow Control In Computer Networks

CHOUW81 - CHOU, W., Arnold W. Bragg, Arne A. Nilsson; The need for adaptive routing in the chaotic and unbalanced Traffic environment; IEEE Transactions on Communications, VOL. COM-29 NO.4, APRIL 81 PP. 481-490

CHU*W81 - CHU, Wesley W., Guy Fayolle, David G. Hibbits; An analysis of a Tandem Queueing System for Flow Control in Computer Networks; IEEE Transactions on Computers, Vol. C-30, No.5, May 1981, pp.318-323

CLARD78 - CLARK, DAVID, Kenneth T. Pogran, David P. Reed; An Introduction to Local Area Networks; Proceedings of the IEEE, VOL 66 NO.11, NOV-78 PAG. 1497-

COHED79 - COHEN Danny, Jonathan B. Postel; On Protocol Multiplexing; Sixth Data Communication Symposium, Nov.79

CONAJ8Ø - CONRAD, James W.; Character-oriented Data Link Control Protocols; IEEE Transactions on Communications, VOL COM-28 NO.4 APRIL-8Ø PP. 445-454

COSEB77 - COSELL, Bernard, Alan Nemeth, David Walden; X.25 Link Access Procedure; Computer Communication Review - SIGCOMM - OCT 77 VOL.7 NO.4

COTTI78 - COTTON, Ira W.; Computer Network Interconnection; Computer Networks 2(1978) PAG. 25-34

COURD8Ø - COURTOIS P.J., P.Semai; A Flow assignment algorithm based on the flow deviation method; Proceedings of the Fifth International Conference on Computer Communications - ATLANTA, 27-3Ø OCT.8Ø

COUSW8Ø - COUSINS, W.B.; Problems of Privacy in Data Networks: a European Perspective; Proceedings of the Fifth International Conference on Computer Communications - ATLANTA, 27-3Ø OCT.8Ø

COYNR81 - COYNE, Robert; Dynamic Reconfiguration by a Local Network's Operating System; Data Communications, DEC.81, PP.88-96

CRAVH81 - CRAVIS, Howard; Communications Network Analysis;

Arthur D. Little.

DAVID81 - DAVIES, D.W., E. Holler, E.D. Jensen, S.R. Kimbleton, B.W. Lampson. G. LeLann, K.J. Thurber, R.W. Watson; Distributed Systems - Architecture and Implementation; Lecture Notes in Computer Science no. 105, Editado por: B.W. Lampson, M.Paul e H.J. Siegert; Springer Verlag.

DARPA80 - DARPA - Defense Advanced Research Projects Agency; DoD Standard Internet Protocol; Computer Communication Review, Oct. 1980, Vol.10, No.4,pp.12-51;

DARPA80b- DARPA - Defense Advanced Research Projects Agency; DoD - Standard Transmission Control Protocol; Computer Communication Review, Oct.1980, Vol.10, No.4,pp.52-132.

DAVIJ77 - The ARPAnet TELNET protocol: its purpose, principles, implementation and impact on host operating system design; Proceedings of the Fifth Data Communications Symposium

DAVIJ81 - DAVIDSON,John M.; NET/ONE'S Answer to packet and circuit switching; Data Communications, Dez.81, PP.84-87

DAY*J79 - DAY, John D.; Resource Sharing Protocols COMPUTER Sept. 79

DEATG79 - DEATON, George A. JR.; Flow Control in Packet-switched Networks with Explicit Path Routing; FLOW CONTROL IN COMPUTER NETWORKS; Proceedings of the International Symposium on Flow Control in Computer Networks; Versailles, France, February 12-14, 1979; Edited by Jean-Louis Grangé and Michel Gien; North-Holland Publishing Company.

DELAJ79 - DELATTRE Jacques; Routing and Flow Control within a Message Switching Network; FLOW CONTROL IN COMPUTER NETWORKS; Proceedings of the International Symposium on Flow Control in Computer Networks; Versailles, France, February 12-14, 1979; Edited by Jean-Louis Grangé and Michel Gien; North-Holland Publishing Company.

DENIJ79 - DENIS, Jean-Jacques, Olivier Gibergues; Principes de Conversion entre les Protocoles CYCLADES et X.25 FLOW CONTROL IN COMPUTER NETWORKS; Proceedings of the International Symposium on Flow Control in Computer Networks; Versailles, France, February 12-14, 1979; Edited by Jean-Louis Grangé and Michel Gien; North-Holland Publishing Company.

DICCV79 - DI CICCIO, Vic, Carl A. Sunshine, James A. Field, Eric G. Manning; Alternatives for Interconnection of Public Packet Switching Data Networks; Sixth Data Communication Symposium, Nov. 79

DRIVH79 - DRIVER, Henry H., H. Lynn Hopewell, Joseph F. Iaquinto; How the Gateway Regulates Information Flow; Data Communications - Setembro 79 - PP. 61-70

DRIVH79b- DRIVER, Henry H., H. Lynn Hopewell, Joseph F. Iaquinto; What's the Best Approach to Gateway Design?; Data Communications - Outubro 79 - PP. 101-111

EASTM81 - EASTON, Malcon C.; Design Choices for Selective-repeat Retransmission Protocols; IEEE Transactions on Communications, VOL. COM-29 NO.7, JULY 81 PP. 944-953

EDGES79 - EDGE, Stephen William; Comparison of the Hop-by-hop and Endpoint Approaches to Network Interconnection; FLOW CONTROL IN COMPUTER NETWORKS; Proceedings of the International Symposium on Flow Control in

Computer Networks; Versailles, France, February 12-14, 1979; Edited by Jean-Louis Grangé and Michel Gien; North-Holland Publishing Company.

EDWAM81 - EDWARD, Morris; Universal Architecture Standard Brings Unity to Network Planning; Communications News - JULY 81 - PP. 86 -90

EGERJ81 - EGER, John M.; The International Information War; Computerworld, VOL. XV NO.11A MARCH 18,1981

ELIEM79 - ELIE, Michel; Traffic Control by Latency in a Packet Switching; FLOW CONTROL IN COMPUTER NETWORKS; Proceedings of the International Symposium on Flow Control in Computer Networks; Versailles, France, February 12-14, 1979; Edited by Jean-Louis Grangé and Michel Gien; North-Holland Publishing Company.

FAROA81 - FARO, A., G. Messina; Internetworking Analysis; Computer Communications, VOL.4, NO.4, AUG.81 PP. 169-173

FERRE81 - FERRARINI, Elizabeth; VIDEOTEX: The Race to Plug in; Computerworld, VOL. XV NO.11A March 18,1981

FOLTH79 - FOLTS, Harold C.; Status Report on New Standards for DTE/DCE Interface Protocols; COMPUTER Sept. 79

FOLTH81 - FOLTS, Harold C.; Coming of Age: A Long Awaited Standard for Heterogeneous Nets; Data Communications, JAN. 81, PP. 63-73

FRANH72 - FRANK, Howard, Wushow Chou; Topological Optimization of Computer Networks; Proceedings of the IEEE, VOL. 60 NO.11 NOV.72; PP.1385-1397

FRANH81 - FRANK, Howard; Telecommunications: 1970-1980; COMPUTERWORLD VOL. XV NO.11A MARCH 18,1981

GAFNE8Ø - GAFNI, E., D.P. Bertsekas; Distributed Algorithms for Generating Loopfree Routes in Networks with Frequently Changing Topology; Proceedings of the Fifth International Conference on Computer Communications - ATLANTA, 27-3Ø OCT. 8Ø;

GALLR77 - GALLAGER, Robert R.; A Minimum Delay Routing Algorithm Using Distributed Computation; IEEE Transactions on Communications, VOL. COM-25 NO.1 JAN.77, PP.73-85

GALLR8Ø - GALLAGER, R.G., S.J. Golestaani; Flow Control and Routing Algorithms for Data Networks; Proceedings of the Fifth International Conference on Computer Communications - ATLANTA, 27-3Ø OCT. 8Ø

GASSH8Ø - GASSMANN, H.R.; Privacy: the International Perspective; Proceedings of the Fifth International Conference on Computer Communications - ATLANTA, 27-3Ø OCT. 8Ø

GEORN8Ø - GEORGANAS; Nicolas D.; Modeling and Analysis of Message Switched Computer Communication Networks with Multilevel Flow Control; Computer Networks 4(198Ø) PP.285-294

GELEE75 - GELENBE, E; On Approximate Computer System Models; Journal of the ACM, No.22, pp.261-269, 1975.

GELEE76 - GELENBE, E, G. Pujolle; Approximation to a Single Queue in a Network; ACTA Informatica 7, pp.123-136, 1976.

GELEE78 - GELLENBE, Erol, J. Labetoulle, G. Pujolle; Performance Evaluation of The HDLC Protocol; Computer Networks Vol. 2, No. 4/5, Sept/Oct 1978, pp.4Ø9-415.

GERLM78 - GERLA, Mario, Doug Mason; Distributed Routing in

Hybrid Packet and Circuit Data Networks; Proceedings of Computer Communications Networks - COMPCOM 78

GERLM78b- GERLA, Mario, G. DE Stasio Integration of Packet and Circuit Transport Protocols in the TRAN Data Network; Proceedings of the Comp. Network Protocol Symposium; Universite' de Liege - Symposium - 13, 15 FEB. 78

GERLM8Ø - GERLA, Mario, Leonard Kleinrock; Flow Control: a Comparative Survey; IEEE Transactions on Communications, VOL COM-28 #4 APRIL 8Ø PAG. 553-574

GERLM8Øb- GERLA, Mario, P.O. Nilsson; Routing and Flow Control Interplay in Computer Networks; Proceedings of the Fifth International Conference on Computer Communications - ATLANTA, 27-3Ø OCT.8Ø

GIENM75 - GIEN, Michel, J. Laws., R. Scantlebury; Interconnection of Packet-switched Networks: Theory and Practice; INRIA - SCH 566 - MAY 75, também em, European Computing Conference on Communications Networks; Londres, 23-25 SEPT.75

GIENM78 - GIEN, Michel; A file transfer protocol; Computer Networks, vol.2, No. 4/5, Sept/Oct. 1978, pp.312-319.

GIENM79 - GIEN, Michel, H. Zimmermann Design Principles for Network Interconnection Sixth Data Communications Symposium, Nov.79

GIESA81 - GIESSLER, Alfred, Anne Marie Jagemann, Ellen Maser, Jurgen O. Hanle; Flow Control Based on Buffer Classes; IEEE Transactions on Communications, VOL. COM-29 NO.4, APRIL 81 PP. 436-443

GILLD81 - GILLETTE, Dean; Telematics: the Integration of Computing and Communications; Computerworld, VOL. XV

NO.11A MARCH 18,1981

GOMBG79 - GOMBERG G.R., I.H. Kerr, J. Richards; A Design Study of a Hierarchically Connected Packet-Switched Network Using Simulation Techniques; Computer Networks, 3(1979)

GRANJ73 - GRANGE, J.L., L. Pouzin; CIGALE, la Machine de Commutation de Paquets du Reseau CYCLADES; INRIA - MIT 536 - Maio 73

GRANJ79 - GRANGE, Jean Louis; Traffic Control in a Packet Switching Network; INRIA - SCH 618 - Maio 79.

GREEL81 - GREENHOUSE, Lee R.; Communications and Networking Invade the Home Front; Data Communications, FEB.81, PP.56-69

GUNTK81 - GUNTHER, Klaus D.; Prevention of Deadlocks in Packet-switched Data Transport Systems; IEEE Transactions on Communications, VOL. COM-29 NO.4, APRIL 81 PP. 512-524

HAEND81 - HAENSCHKE, Detlev, David A. Ketler, Eric Oberer; Network Management and Congestion in the U.S. Telecommunications; IEEE Transactions on Communications, VOL. COM-29 NO.4 APRIL 81 PP. 376-384

HAENJ78 - HAENLE, J.O., A. Giessler; Simulation of Data Transport Systems of Packet-switched Networks; Computer Networks and Simulation;

HELDG79 - HELD, Gilbert; Eliminating those Blanks and Zeros in Data Transmission; Data Communications - SEPTEMBER 79 - PP. 75-77

HIRSP81 - HIRSCH, Phil; VIDEOTEX in the U.S.: the Portland Project; Computerworld, VOL. XV NO.11A MARCH 18,1981

HOFFL77 - HOFFMAN, Lance J.; Modern Methods for Computer Security and Privacy; Prentice-Hall, Inc.; 255 páginas.

HOPPA78a- HOPPER, A.; Local Area Computer Networks - a Brief Survey; University of Cambridge; Computer Laboratory; 1978.

HOPPA78b- HOPPER, A.; Data Ring at Computer Laboratory; University of Cambridge - Computer Laboratory;

HOVER76 - HOVEY, Richard B.; Packet-switched Networks Agree on Standard Interface; Data Communications,

HOWAJ8Ø - HOWARD, J.R.,Jr.; Privacy: the U.S. Perspective; Proceedings of the Fifth International Conference on Computer Communications - ATLANTA, 27-3Ø OCT.8Ø

IGLED81 - IGLEHART, Donald L., Gerald S. Shedler; Regenerative Simulation of Responde Times in Networks of Queues: Statistical Efficiency; ACTA Informatica 15, PP.347-363 (1981)

IMPE*78 - IMPERIAL COLLEGE; An Explanation of the CCITT X.25 Recommendation for Accessing a Packet Switched Network; Publication # 78/34 (Research Report); Dept. of Computing and Control; London SW7 2BZ

INOSH78 - INOSE, Hiroshi, Tadao Saito; Theoretical Aspects in the Analysis and Synthesis of Packet Communications Networks; Proceedings of the IEEE, VOL 66 NO.11, NOV-78 PAG. 1409-1422

INWG*75 - INWG - 6.1 - IFIP - INWG General Note # 83; Basic Message Format for Inter-network Communication;

INWG*78 - IFIP - International Federation for Information Processing Working Group 6.1; Proposal for an Internetwork End-to-end Transport Protocol;

ISO**77 - International Organization for Standardization; High Level Data Link Control Procedures - Elements of Procedures; ISO/TC97/SC 6 N

ISO**81 - International Organization for Standardization; Data Processing - Open Systems Interconnection - Basic Reference Model; ISO/TC97/SC16; Computer Networks 5(1981) PP. 81-118

JACOT77 - JACOBSEN, Tom, Peter Thisted; CCITT Recommendation X.25 as Part of the ISO Reference Model of Open SYstems Interconnection;

JAFFJ8Ø - JAFFE, J.M.; A Decentralized, "Optimal", Multiple-user, Flow Control Algorithm; Proceedings of the Fifth International Conference on Computer Communications - ATLANTA, 27-3Ø OCT. 8Ø

JAFFJ81 - JAFFE, Jeffrey M; Bottleneck Flow Control; IEEE Transactions on Communications, VOL. COM-29 NO.7, JULY 81 PP. 954-962

JOHND77 - JOHNSON, Donald; Efficient Algorithms for Shortest Path in Sparse Networks; Journal of the ACM, VOL.24, NO.1, JAN.77 PP 1-13

KAMOF8Ø - KAMOUN, Farouk; Analysis of Shared Finite Storage in a Computer Network Node Environment Under General Traffic Conditions; IEEE Transactions on Communications, VOL.COM-28 #7, JULY 8Ø - PAG. 992-1ØØ3

KAMOF8Øb- KAMOUN, F., A. Belguith, J.L. Grange; Congestion Control with a Buffer Management Strategy Based on Traffic Priorities; Proceedings of the Fifth International Conference on Computer Communications - ATLANTA, 27-3Ø OCT.

KAMOF81 - KAMOUN, F.; A Drop and Throttle Flow Control Policy

for Computer Networks; IEEE Transactions on Communications, VOL. COM-29 NO. 4, APRIL 81 PP. 444-452

KANHR72 - KAHN, Robert E.; Resource Sharing Computer Networks; Proceedings of the IEEE, VOL.60 NO.11 NOV-72 PP. 1397-1407

KAR*S81 - KAR, Saroj K.; Closing the Gap: Compatibily with SNA Computerworld VOL. XV NO.11A MARCH 18,1981

KAUFL81 - KAUFMAN, LInda, B. Gopinath, Eberhard F. Wunderlich; Analysis of Packet Network Congestion Control Using Sparse Matrix Algorithms; IEEE Transactions on Communications, VOL. COM-29 NO.4, APRIL 81 PP. 453-465

KAWAT80 - KAWAOKA, T., S. Yoshitake, K. Morino; A Method for Verifying Layered Protocol Products and its Application to Data Communications Network Architecture Products; Proceedings of the Fifth International Conference on Computer Communications - ATLANTA, 27-30 OCT. 80

KELLP78 - KELLY, P.T.F.; Public Packet Switched Data Networks, International Plans and Standards; Proceedings of the IEEE, VOL 66 NO.11, NOV-78 PAG. 1539-1549

KENTS81 - KENT, Stephen; Security Requirements and Protocols for a Broadcast Scenario; IEEE Transactions on Communications, VOL. COM-29 NO. 6, JUNE 81 PP. 778-786

KERMP79 - KERMANI, Parviz, Leonard Kleinrock; Virtual Cut-through: a New Computer Communication Switching Technique; Computer Networks, 3(1979) pp. 267-286.

KERMP80 - KERMANI, Parviz, Leonard Kleinrock; A Tradeoff Study of Switching Systems in Computer Communication

Networks; IEEE Transactions on Computers, VOL C-29 NO.12 DEC.80 PP.1052-1060

KEYEN78 - KEYES, N. Mario Gerla; Report on Experience in Developing a Hybrid Packet and Circuit Network; ICC-78

KIMBS75 - KIMBLETON, Stephen , G. Michael Schneider; Computer Communication Networks: Approaches, Objectives and Performance Considerations; Computing Surveys, VOL. 7 # 3, SEPT. 75

KLEIL75 - KLEINROCK, Leonard; Queueing Systems, Vol. I: Theory; Wiley-Interscience.

KLEIL76 - KLEINROCK, Leonard; Queueing Systems, Vol. II: Computer Applications; Wiley-Interscience.

KLEIL77 - KLEINROCK, Leonard, Farouk Kamoun; Hierarchical Routing for Large Networks - Performance Evaluation and Optimization; Computer Networks 1(1977) PAG. 155-174

KLEIL77b- KLEINROCK, Leonard, Holger Opferbeck; Throughput in the ARPANET - Protocols and Measurements; IEEE Transactions on Communications, VOL.COM-25 NO.1 JAN.77 PP. 95-104

KLEIL78 - KLEINROCK, Leonard; Principles and Lessons in Packet Communications; Proceedings of the IEEE, VOL 66 NO.11, NOV-78 PAG. 1320-1329

KLEIL78b- KLEINROCK, Leonard, Parviz Kermani; A Network Algebra for the Performance Evaluation of Interconnected Computer Networks; NTC-78, Birminghan, Alabama, Dec. 3-6 1978.

KLEIL80 - KLEINROCK, L., C.W.Tseng; Flow Control Based on Limiting Permit Generations Rates; Proceedings of

the Fifth International Conference on Computer Communications - ATLANTA, 27-30 OCT. 80

KOBAH74 - KOBAYASHI, Hisashi; Application of the Diffusion Approximation to Queueing Networks; Journal of the ACM, No.21, pp.316-328, 1974

KOBAH77 - KOBAYASHI, Hisashi, Alan G. Konheim; Queueing Models for Computer Communications System Analysis; IEEE Transactions on Communications, Vol. Com-25, No.1, Jan.1977, pp.2-28;

KONHA80 - KONHEIM, Alain G.; A Queueing Analysis of Two ARQ Protocols; IEEE Transactions on Communications, VOL.COM-28 #7, JULY 80 - PAG. 1004-1014

KRUTT81 - KRUTSCH, Thomas E.; A User Speaks Out: Broadband or Baseband for Local Nets? Data Communications, DEC.81, PP.105-112

KRYSJ81a- KRYSKOW, J. Michael, C. Kenneth Miller; Local Area Networks Overview - Part 1: Definitions and Attributes; Computer Design - FEB.81, PP.22-35

KRYSJ81b- KRYSKOW, J. Michael, C. Kenneth Miller; Local Area Networks Overview - Part 2: Standards Activities; Computer Design - MARCH 81 - PP.12-20

KUMAK81 - KUMAR, Kadaba Bharath , Jeffrey M. Jaffe; A New Approach to Performance Oriented Flow Control; IEEE Transactions on Communications, VOL. COM-29 NO.4, APRIL 81 PP. 427-435

LABEJ79 - LABETOULLE, Jacques, Guy Pujolle; A Study of Flows in an X.25 Environment; FLOW CONTROL IN COMPUTER NETWORKS; Proceedings of the International Symposium on Flow Control in Computer Networks; Versailles, France, February 12-14, 1979; Edited by Jean-Louis Grangé and Michel Gien; North-Holland Publishing

Company.

LABEJ79b- LABETOULLE, J., G. Pujolle, N. Mikou; Performance of the HDLC Protocol; IRIA - Rapport de Recherche NO. 352 MAY 79

LABEJ81 - LABETOULLE, J., Guy Pujolle; A Study of Flows Through Virtual Circuits Computer Networks; Computer Networks 5(1981) PP. 119-126

LABEJ81b- LABETOULLE,J., Guy Pujolle; HDLC Throughput and Response Time for Bidirectional Data Flow with Nonuniform Frame Sizes; IEEE Transactions on Computers, VOL. C-30 NO.6 JUNE 81, PP.405-413

LAM*S80 - LAM, S.S., Y.L. Lien; An Experimental Study of the Congestion Control of Packet Communication Networks; Proceedings of the Fifth International Conference on Computer Communications - ATLANTA, 27-30 OCT. 80

LAVIA79 - LAVIA, A., D.J. Rhynas; A Virtual Circuit Based Transaction Service; Sixth Data Communication Symposium, NOV.79

LEMIC81 - LEMIEUX, Claude; Theory of Flow Control in Shared Networks and its Application in the Canadian Telephone Network; IEEE Transactions on Communications, VOL. COM-29 NO. 4, APRIL 81 PP. 399-413

LENNR81 - LENNON, Richard E., Stephen M. Matyas, Carl H. Meyer; Cryptographic Authentications of Time-incariant Quantities; IEEE Transactions on Communications, VOL. COM-29 NO. 6, JUNE 81 PP. 773-777

LICKJ78 - LICKLIDER, J.C.R., Albert Vezza; Applications of Information Networks; Proceedings of the IEEE, VOL 66 NO.11, NOV-78 PAG. 1330-1346

MAGOR79 - MAGOON R., D. Twyver; Flow and Congestion Control in SL-10 Networks; FLOW CONTROL IN COMPUTER NETWORKS; Proceedings of the International Symposium on Flow Control in Computer Networks; Versailles, France, February 12-14, 1979; Edited by Jean-Louis Grangé and Michel Gien; North-Holland Publishing Company.

MAJIJ79 - MAJITHIA, J.C., M. Irland, J.L. Grange, N. Cohen, C. O'Donnel; Experiments in Congestion Control Techniques; INRIA - MOD 550 - FEB. 79

MALOJ81 - MALONE, Joe; The Microcomputer Connection to Local Networks; Data Communications, DEC.81, PP.101-104

MARGI78 - MARGITICS, I.; Final Report on Scholarship on the CYCLADES Computer Network; INRIA - GAL 530 - SEPT. 78

MARUK80 - MARUYAMA, K., G. Markowsky; On the Generation of Explicit Routing Tables; Proceedings of the Fifth International Conference on Computer Communications - ATLANTA, 27-30 OCT. 80

MASOJ81 - MASON, Jeffrey, Gregory Shaw; Implementing ETHERNET from Soup to Nuts; Data Communications, DEC. 81, PP.74-80

MATSJ81 - MATSUMOTO, Jun, Hiromichi Mori; Flow Control in Packet Switched Networks by Gradual Restrictions of Virtual Call; IEEE Transactions on Communications, VOL. COM-29 NO.4, APRIL 81 PP. 466-473

MCQUJ75 - MCQUILLAN, J.M.; The Evolution of Message Processing Techniques in the ARPA Network;

MCQUJ77 - MC QUILLAN, John; Routing Algorithms for Computer Networks - a Survey; Conference Record, NTC 77, VOL. 2

MCQUJ78 - MC QUILLAN, John; Enhanced Message Addressing Capabilities for Computer Networks; Proceedings of the IEEE, VOL 66 NO.11, NOV-78 PAG. 1517-1527

MCQUJ78b- MC QUILLAN, John, Vinton G. Cerf; Tutorial: a Practical View of Computer Communications Protocols; IEEE Catalog NO. EHO 137-Ø

MCQUJ79 - MC QUILLAN, John, Ira Richer, Eric C. Rosen; An Overview of the New Routing Algorithm for the ARPANET Sixth Data Communications Symposium, NOV. 79

MCQUJ79b- MC QUILLAN, John; Interactions Between Routing and Congestion Control in Computer Networks; FLOW CONTROL IN COMPUTER NETWORKS; Proceedings of the International Symposium on Flow Control in Computer Networks; Versailles, France, February 12-14, 1979; Edited by Jean-Louis Grangé and Michel Gien; North-Holland Publishing Company.

MCQUJ8Ø - MC QUILLAN, John, Ira Richer, Eric C. Rosen; The New Routing Algorithm for the ARPANET IEEE Transactions on Communications, VOL COM-28, NO. 5, MAY-8Ø PP 711-719

MELLF79 - MELLOR, F., M.M. Matsubara; Flow Control of Access Services in SL-1Ø Networks; FLOW CONTROL IN COMPUTER NETWORKS; Proceedings of the International Symposium on Flow Control in Computer Networks; Versailles, France, February 12-14, 1979; Edited by Jean-Louis Grangé and Michel Gien; North-Holland Publishing Company.

MERLP8Ø - MERLIN, Philip M., Paul J. Schweitzer; Deadlock Avoidance in Store-and-Forward Networks - I: Store-and-Forward Deadlocks; IEEE Transactions on Communications, Vol.COM-28, No.3, March 198Ø, pp.345-354;

MERPL80b- MERLIN, Philip M., Paul J. Schweitzer; Deadlock Avoidance in Store-and-Forward Networks - II: Other Deadlock Types; IEEE Transactions on Communications, Vol.COM-28, No.3, March 1980, pp.355-360;

MITTK81 - MITTAL, Kumud K., Anastasios N. Venetsanopoulos; On the Dynamic Control of the Urn Scheme for Multiple Access Broadcast Communication Systems; IEEE Transactions on Communications, VOL. COM-29 NO. 7, JULY 81 PP. 962-

MOLDB81 - MOLDOW, Bert D.; Reality and the Proposed OSI Standard; Data Communications - JUNE 81 - PP. 77-80

MOLIG78 - MOLI, G. Le; On Networking; Computer Networks and Simulation - 78

MUSCE79 - MUSCELLACK, Erich; Proposta de um Padrão de Protocolo de Comunicação; COPPE-UFRJ - PTS-05/79.

NAFFN81 - NAFFAH, Najah; Le Projet Pilote KAYAK, Objectifs, Axes de Recherche et Conduite; INRIA - GAL 2.524 Fev. 1981.

ORNSS75 - ORNSTEIN, Severo M., David C. Walden; The Evolution of a High Performance Modular Packet Switch; International Conference on Communications, San Francisco Calif. JUNE 75

PATEA80 - PATEL, AHmed, Michel Purser; Systems Programming for Data Communications on Minicomputers; Software - Practice and Experience; VOL. 10, PAG. 283-305

PAWLP81 - PAWLITA, Peter T.; Traffic Measurements in Data Networks, Recent Measurement Results and some Implications; IEEE Transactions on Communications, VOL. COM-29 NO.4, APRIL 81 PP. 525-535

PETRA80 - PETRENKO, A.F.; On the Specification and

Verification of Protocols Using PETRI-NETS; Proceedings of the Fifth International Conference on Computer Communications - ATLANTA, 27-30 OCT. 80

POPEG79 - POPEK, Gerald S.; Encryption and Secure Computer Networks; Computing Surveys, VOL. 11 # 4 DEC-79

POSTJ80 - POSTEL, Jonathan B.; Internetwork Protocol Approaches; IEEE Transactions on Communications, VOL. COM-28 NO.4 APRIL-80 PP. 604-611

POSTJ81 - POSTEL, Jonathan B., Carl A. Sunshine, Danny Cohen; The ARPA Internet Protocol; Computer Networks, 5(1981) PP. 261-277

POUZL73 - POUZIN, Louis; Presentation and Major Design Aspects of the CYCLADES Computer Network; INRIA - SCH 511 Abril 1973, também em, 3RD. DATA COMM. SYMP., IEEE TAMPA (FLORIDA), NOV.73

POUZL75 - POUZIN, Louis; Congestion Control Based on Channel Load; INRIA - MIT 600 - AUG. 75

POUZL76 - POUZIN, Louis; Names and Objects in Heterogeneous Computer Networks; INRIA - SCH 585 - MAY 76

POUZL77 - POUZIN. Louis; A Restructuring of X25 into HDLC Computer Communication Review - JAN. 77 VOL. 7 NO.1

POUZL78 - POUZIN, Louis, Hubert Zimmermann; A Tutorial on Protocols; Proceedings of the IEEE, VOL. 66 # 11, NOV-78

POUZL79 - POUZIN, Louis; Internetworking; INRIA - SCH 626 - JUNE 79

POUZL81 - POUZIN, Louis; Methods, Tools and Observations on Flow Control un Packet Switched Data Networks; IEEE Transactions on Communications, VOL. COM-29 NO. 4,

APRIL 81 PP. 413-426

POWEG81 - POWER, Gerald; . A Survey of Distributed Network Architectures; Computerworld, VOL. XV NO.11A MARCH 18,1981

PRICW78 - PRICE, W.L.; Simulation of Routing Doctrines, Flow Control and Congestions Avoidance; Computer Network and Simulation - 78

PRICW79 - PRICE, W.L.; A Review of the Flow Control Aspects of the Network Simulation Studies of the National Physical Laboratory; FLOW CONTROL IN COMPUTER NETWORKS; Proceedings of the International Symposium on Flow Control in Computer Networks; Versailles, France, February 12-14,1979; Edited by Jean-Louis Grangé and Michel Gien; North-Holland Publishing Company.

PUJOG78 - PUJOLLE, Guy; Analysis of Flow COntrols in Switched Data Networks by an Unified Model; IRIA - Rapport de Recherche NO. 291; Abril 1978.

PUJOG79 - PUJOLLE, Guy, Christine Soula; A Study of Flows in Queueing Networks and an Approximate Method for Solution; IRIA - Rapport de Recherche NO. 340 Jan. 1979.

PUJOG79b- PUJOLLE, Guy; The Influence of Protocols on the Stability Conditions in Packet-Switching Networks; IEEE Transactions on Communications, Vol, Com-27, No.3, March 1979, pp. 611-619.

PUJOG80 - PUJOLLE, Guy; Comparison of some End-to-end Flow Control Policies in a Packet Switching Network; INRIA - Rapports de Recherche NO.1; Jan. 1980.

REISM74 - REISER, M., H. Kobayashi; Accuracy of the Diffusion Approximation for some Queueing Systems; IBM J. Res.

Develop. 18, 2, pp.110-124, 1974.

RINDJ79 - RINDI, Joseph, Arthur Caisse; Passive Flow Control Techniques for Distributed Networks; FLOW CONTROL IN COMPUTER NETWORKS; Proceedings of the International Symposium on Flow Control in Computer Networks; Versailles, France, February 12-14, 1979; Edited by Jean-Louis Grangé and Michel Gien; North-Holland Publishing Company.

ROBEL78 - ROBERTS, Lawrence; The Evolution of PAcket Switching; Proceedings of the IEEE, VOL 66 NO.11, NOV-78 PAG. 1307-1313

ROM*R81 - ROM, Raphael; Message Based Priority Functions in Local Multiaccess Communications Systems; Computer Networks 5(1981) PP. 273-286

ROSSS72 - ROSS, Sheldon M.; Introduction to Probability Models; Academic Press, Inc..

ROWAJ81 - ROWAN, James; A Look at a Popular Switching Technique; Data Communications - March 1981 - PP. 117-123

RUDIH79 - RUDIN, Harry, Heinrich Muller; On Routing and Flow Control; FLOW CONTROL IN COMPUTER NETWORKS; Proceedings of the International Symposium on Flow Control in Computer Networks; Versailles, France, February 12-14, 1979; Edited by Jean-Louis Grangé and Michel Gien; North-Holland Publishing Company.

RUDIH80 - RUDIN, Harry, Heinrich Muller; Dynamic Routing and Flow Control; IEEE Transactions on Communications, VOL.COM-28 #7, JULY 80 - PAG. 1030-1039

RYBCA76 - RYBCZYNSKI, A., B. Wessler, R. Despres, J. Wedlack; A New Communication Protocol for Accessing Data Networks - the International Packet-mode Interface;

Conference Proceedings, 1976 National Computer Conference, VOL.45

RYBCA8Ø - RYBCZYNSKI, A.M., J.D. Palframan, A. Thomas; Design of the DATAPAC X.75 Internetworking Capability; Proceedings of the Fifth International Conference on Computer Communications - ATLANTA, 27-3Ø OCT.8Ø

SARCR81 - SARCH, Ray; Protocol Conversion - Product of Profusion; Data Communications, - JUNE 81 - PP. 65-73

SCHIS81 - SCHINDLER, Sigram, Ute Flasche, Carsten Bormann; Open Systems Interconnection - the Presentations Service Model; Computer Communications, VOL. 4, NO.5, OCT.81 PP.227-241

SCHWG78 - SCHWARZ, Gerhard; Rede de Computadores - uma Análise Qualitativa; COPPE - PDD 11/78

SCHWG79 - SCHWARZ, Gerhard; Redes de Computadores - Programação Matemática e Simulação; COPPE-UFRJ - PDD-16/79.

SCHWG79b- SCHWARZ, Gerhard; Redes de Computadores - Um Estudo de Modelos Matemáticos; COPPE-UFRJ - PDD-13/79.

SCHWM72 - SCHWARTZ, Mischa, Robert R. Boorstyn, Raymond L. Pickholts; Terminal Oriented Computer Communication Networks; PROCEEDINGS OF THE IEEE, VOL.6Ø NO.11 NOV-72 PP.14Ø8-1423

SCHWM77 - SCHWARTZ, Mischa; Computer Communications Networks and Analysis; PRENTICE-HALL - 1977 CHAP. 2,3,4,5

SCHWM79 - SCHWARTZ, Mischa, Samir Saad; Analysis of Congestion Techniques in Computer Communication Networks; FLOW CONTROL IN COMPUTER NETWORKS; Proceedings of the International Symposium on Flow Control in Computer

Networks; Versailles, France, February 12-14, 1979; Edited by Jean-Louis Grangé and Michel Gien; North-Holland Publishing Company.

SCHWM8Ø - SCHWARTZ, M., Thomas E.Stern; Routing Techniques Used un Computer Communications Networks; IEEE Transactions on Communications, VOL COM-28 #4 APRIL 8Ø PAG. 539-552

SEGAA77 - SEGALL, Adrian; The Modeling of Adaptive Routing in Data-Communications Networks; IEEE Transactions on Communications, VOL. COM-25 NO.1, JAN. 77, PP.85-94

SEGAA79 - SEGALL, Adrian; Failsafe Distributed Algorithms for Routing in Communication Networks; FLOW CONTROL IN COMPUTER NETWORKS; Proceedings of the International Symposium on Flow Control in Computer Networks; Versailles, France, February 12-14, 1979; Edited by Jean-Louis Grangé and Michel Gien; North-Holland Publishing Company.

SEGAA81 - SEGALL, Adrian; Advances in Verifiable Fail Safe Routing Procedures; IEEE Transactions on Communications, VOL. COM-29 NO.4, APRIL 81 PP. 491-497

SEGAA81b- SEGALL, Adrian, Moshe Sidi; A Failsafe Distributed Protocol for Minimum Delay Routing; IEEE Transactions on Communications, VOL. COM-29, NO.5 MAY 81 PP.689-695

SEVCK77 - SEVCIK K.C.; Improving Approximations of Aggregated Queueing Network Subsystems; Proceedings of IFIP Working Group 7.3, Yorktown Heights, 1977.

SHOCJ78 - SHOCH, John F.; Inter-network Naming Addressing and Routing Proceedings of COMPCOM FALL 78, IEEE Computer Society.

SHOCJ79a- SHOCH, John F.; Packet Fragmentation in Inter-network Protocols; Computer Networks 3(1979) PAG. 3-8

SHOCJ79b- SHOCK, John F., Lawrence Stewart; Interconnecting Local Networks Via the Packet Radio Network; Sixth Data Communications Symposium, NOV.79

SHOCJ8Ø - SHOCH, John F., Jon A. Hupp; Measured Performance of an ETHERNET Local Network; CACM, DEC.198Ø, VOL.23, NO.12, PP.711-721

SHOCJ81 - SHOCH, John F., Danny Cohen, Edward A. Taft; Mutual Encapsulation of Internetwork Protocols; Computer Networks, 5(1981) PP. 287-3ØØ

SIMOJ79 - SIMON, J.M., A. Danet; Controle des Ressources et Principes du Routage dans le Réseau TRANSPAC FLOW CONTROL IN COMPUTER NETWORKS; Proceedings of the International Symposium on Flow Control in Computer Networks; Versailles, France, February 12-14, 1979; Edited by Jean-Louis Grangé and Michel Gien; North-Holland Publishing Company.

SLOAL79 - SLOAN, Lansing J.; Limiting the Lifetime of Packets in Computer Networks; Computer Networks, 3(1979) PAG. 435-445

SMETJ76 - SMET, Joe De, Ray W. Sanders; "PACUIT" Switching Combines Two Techniques in One Network; Computer Design - JUNE 76 PP.83-88

SMIDM81 - SMID, Miles E.; Integrating the Data Encryption Standard into Computer Networks IEEE Transactions on Communications, VOL. COM-29 NO. 6, JUNE 81 PP. 762-772

SPROD81 - SPROULE, Ronald E., Frank Mellor; Routing, Flow and Congestion Control in the DATAPAC Network; IEEE

Transactions on Communications, VOL. COM-29 NO. 4, APRIL 81 PP. 385-391

STERR81 - STERRY, Richard E.; Ring Nets:Passing the Token in Local Network Circles; Data Communications, DEC.81, PP.97-100

STILR80 - STILLMAN, Rona B., Casper Defiore; Computer Security and Networking Protocols: Technical Issues in Military Data Communications; IEEE Transactions on Communications, VOL.COM-28, NO.9, SEPT.80 PP.1472-1477

STRIE81 - STRITTER, Edward P., Leonard J. Shuster; Local Network Links Personal Computers in a Multiuser, Multifunction System; Electronics, JUNE 16, 1981;

SUNSC77 - SUNSHINE, Carl A.; Interconnection of Computer Networks; Computer Networks, 1(1977) PAG. 175-195

SUNSC77b- SUNSHINE, Carl A.; Source Routing in Computer Networks; SIGCOMM - JAN.77 VOL. 7 NO.1

SUNSC77c- SUNSHINE, Carl A.; Efficiency of Interprocess Communications Protocols for Computer Networks; IEEE Transactions on Communications, FEB.77, PP.287-293

SUNSC78 - SUNSHINE, Carl A., Yogen K. Dalal; Connection Management in Transport Protocols; Computer Networks, 2(1978) pp.454-473;

SUNSC79 - SUNSHINE, Carl A.; Formal Techniques for Protocol Specification and Verification; Computer - SEPT. 79

SUNSC80 - SUNSHINE, Carl A.; Current Trends in Computer Network Interconnection;

TANEA81 - TANENBAUM, Andrew S.; Computer Networks; Prentice-Halll.

TELFA81 - TELFER, A.R., J.C. Majithia; Design and Evaluation of an Interface for an Integrated Service Data Network; Computer Communications, VOL.4, NO.4, AUG.81, PP.155-164

THURK81 - THURBER, Kenneth J., Harvey A. Freeman; The Many Faces of Local Networking; Data Communications, DEC. 81 PP.62-69

TIMMM81 - TIMMONS, Michel L.; Distributed Communication Architecture Forms Framework for Network design; Computer Design - FEB. 81. PP 121-125

TOBAF78 - TOBAGI, Fouad, Mario Gerla, Richard W. Peebles, Eric G. Manning; Modeling and Measurement Techniques in Packet Communication Networks; Proceedings of the IEEE, VOL 66 NO.11, NOV-78 PAG. 1423-1447

TOBAF8Ø - TOBAGI, Fouad A.; Multiaccess Protocols in Packet Communication Systems; IEEE Transactions on Communications, VOL COM-28 NO.4 APRIL-8Ø PP. 468-488

TOWSD81 - TOWSLEY, Don; A Statistical Analysis of ARQ Protocols Operating in a Nonindependent Error Environment; IEEE Transactions on Communications, VOL. COM-29, NO.7, JULY-81 PP. 971-981

TROPC81 - TROPPER, Carl; Local Computer Network Technologies; Academic Press, Inc.

TYMEL81 - TYMES, La Roy W.; Routing and Flow Control in TYMNET; IEEE Transactions on Communications, VOL. COM-29 NO. 4, APRIL 81 PP. 392-398

VASCE82 - VASCONCELLOS, Eduardo de; Análise de desempenho de sub-sistemas de comunicação de dados: Aplicação de modelos de multifilas; Tese M.Sc. na COPPE-UFRJ, Rio de Janeiro, Brasil, Nov.82, 2Ø9 págs.

WALDD79 - WALDEN, David C., Alexander A. Mc Kenzie; The Evolution of Host-to-host Protocol Technology; Computer - SEPT. 79

WAY*D81 - WAY, Dale; Build a Local Network on Proven Software; Data Communications, DEC.81 PP.70-73

WECKS79 - WECKER, Stuart; Computer Network Architectures; Computer - SEPT. 79

WECKS79b- WECKER, Stuart; DNA: The DIGITAL Network Architecture; IEEE Transactions on Communications, VOL.COM-28 NO.4 APRIL-80 PP. 425-432

WEIRD80 - WEIR, D.F., J.B. Holmblad, A.C. Rothberg; An X.75 Based Network Architecture; Proceedings of the Fifth International Conference on Computer Communications - ATLANTA, 27-30 OCT. 80

WILLG81 - WILLIAMS, Gerald W.; Focus on Data terminal Equipment; Computerworld, VOL. XV NO.11A MARCH 18,1981

WINSP80 - WINSTON, Patrick H.; Learning and Reasoning by Analogy; CACM - DEC.80 - VOL.23 - NO.12, PP.689-703

WOLFB78 - WOLFINGER, B., O. Drobnik; Simulation of Protocol Layers of Communication in Computer Networks; Computer Networks and Simulation;

WUNDE80 - WUNDERLICH, E.F., L. Kaufman, B. Gopinath; The Control of Store and Forward Congestion in Packet Switched Networks; Proceedings of the Fifth International Conference on Computer Communications - ATLANTA, 27-30 OCT. 80 - ATLANTA, 27-30 OCT. 80

YU**W80 - YU, Wilfred, J.C. Majithia, J.W. Wong; Access Protocol for Circuit/Packet Switching Networks; Computer Networks 4(1980), PP.271-283

YUM*T81 - YUM, Tak-Shing P.; The design and analysis of a semidynamic deterministic routing rule; IEEE Transactions on Communications, VOL. COM-29 NO.4, APRIL 81 PP. 498-504

YUM*T81b- YUM, Tak-Shing P., Mischa Schwartz; The Join-biased-queue rule and its application to Routing in Computer Communication Networks; IEEE Transactions on Communications, VOL. COM-29 NO.4, Abril 81 PP. 505-511

ZIMMH75 - ZIMMERMANN, Hubert; The CYCLADES End-to-end Protocol INRIA - SCH 565 - OCT 75 ALSO, 4TH. DATA COMM. SYMP. QUEBEC (OCT.

ZIMMH80 - ZIMMERMANN, Hubert; OSI Reference Model - The ISO model of architecture for Open Systems Interconnection; IEEE Transactions on Communications, VOL.COM-28 NO.4 Abril-80 PP. 425-432

ANEXO A

A - Cálculo da Vazão como função da atividade do anfitrião:

O desenvolvimento do modelo é realizado em duas etapas, na primeira o modelo é estudado sem considerar-se as estações de créditos e de recebimento de confirmacções e na seguinte estas restrições são retiradas.

A.1 - O modelo sem as estações C e R:

Antes de apresentar a análise é conveniente recordar as hipóteses consideradas neste estudo:

- independência;
- as distribuições dos tempos de serviço de todas as estações são idênticas;
- um usuário (pacote) ao deixar uma fila encontra o sistema em seu estado de equilíbrio.

Na figura A.1 é apresentado o modelo a ser analisado. Na análise deste modelo serão utilizadas aproximações obtidas por processos de difusão (ver /KOBAH74/, /GELEE75/, /BADEM75/).

A distribuição de probabilidades dos tempos de serviço na estação n é denotada por f.n(x), que equivale a se definir a distribuição do tamanho dos pacotes conhecendo-se a capacidade do canal. Denota-se a média (Ms) de f(x) por E[f(x)], a variância por Var[f(x)] e o QCV (quadrado do coeficiente de variação) por Ks[f(x)].

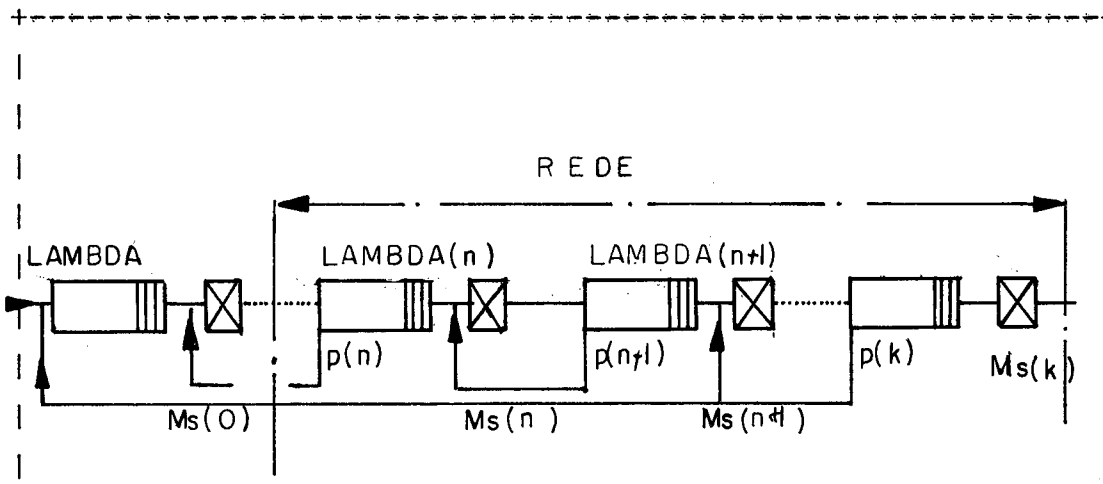
Para efeitos do modelo define-se que para a estação n

tem-se:

$$Ms\ (n) = 1\ /\ E[f.n(x)] \qquad (a.1)$$

$$Var\ (n) = Var[f.n(x)] \qquad (a.2)$$

$$Ks\ (n) = Ks[f.n(x)] \qquad (a.3)$$



LAMBDA = taxa de chegada
Ms = média
p = probabilidade de retransmissão

Figura A.1 - Modelo analisado

Denotando por LAMBDA(n), Ka(n) a taxa e o QCV dos intervalos entre chegadas, respectivamente, da estação n antes da rejeição ocorrer com probabilidade p(n). Assume-se que a chegada de novos usuários (pacotes) na primeira estação obedece a um processo geral de taxa LAMBDA.

Para se analisar o comportamento da estação n, esta será substituída por uma fila equivalente, onde não existe o efeito de realimentação. O novo tempo de serviço assim obtido é o

tempo total de residência na estação considerada do usuário. Considerando-se que h.n(x) seja a distribuição do tempo de serviço equivalente, pode-se definir que:

$$M's(n) = 1 / E[h.n(x)], \qquad (a.4)$$

$$K's(n) = Ks[h.n(x)]. \qquad (a.5)$$

Pode-se expressar h.n(x) da seguinte forma:

$$h.n(x) = (1-p(n+1)) * \text{Somatório } (p(n+1)^{**}(k-1) * f.n(x)), \qquad (a.6)$$

onde *k é o produto da convolação, correspondendo ao fato de que com a probabilidade (1-p(n+1))*p(n+1)**(k-1)) o usuário é atendido k vezes. A partir desta definição obtem-se:

$$M's(n) = Ms(n) * (1-p(n+1)) \qquad (a.7)$$

$$K's(n) = p(n+1) + Ks(n) * (1-p(n+1)) \qquad (a.8)$$

Necessita-se conhecer também a taxa LAMBDA(n) e o QCV dos tempos entre chegadas (Ka(n)). A taxa de chegada dos pacotes na estação n é definida como sendo:

$$LAMBDA(n) = LAMBDA / (1 - p(n)). \qquad (a.9)$$

O número de pacotes que vão da estação (n-1) para a estação (n) é o somatório das novas transmissões e do número de pacotes retransmitidos pela estação (n-1). Existem várias alternativas para se aproximar o valor de Ka(n) (/KOBAH74/, /REISM74/, /SEVCK77/), mas adotou-se a desenvolvida em /GELEE76/ que apresenta o seguinte valor para Ka(n):

$$Ka(n) = -1 + RO(n-1)^{**}2 * (Ks(n-1) + 1) + (2*RO(n-1) + 1 + Ka(n-1)) * (1 - RO(n-1)), \qquad (a.10)$$

onde:

$$RO(n) = LAMBDA(n) / M's(n). \qquad (a.11)$$

Cada uma das estações (n) é tratada como sendo um sistema G/G/1/M(n) com uma distribuição de tempo de serviço determinado por M's(n) e K's(n) e com uma distribuição de tempo entre chegadas determinado por LAMBDA(n) e Ka(n).

A probabilidade p(n) de que um pacote seja rejeitado pela estação (n) é igual à probabilidade de existirem M(n) pacotes na estação considerada. Obtem-se de /GELEE75/ o seguinte valor para esta probabilidade:

$$p(n) = (RO(n) * (1-RO(n))) / (Exp(a) - RO(n)**2), \qquad (a.12)$$

onde:

RO(n) = LAMBDA(n) / M's(n)
Exp = função exponencial
a = - b(n) * (M(n) - 1)
b(n) = 2 * b1(n) / b2(n)
b1(n) = LAMBDA(n) - M's(n)
b2(n) = LAMBDA(n) * Ka(n) + M's(n) * K's(n).

Observa-se que o valor de p(n) depende do valor de p(n+1) por causa de M's(n) e K's(n). Mas, se a solução das equações começar inicialmente pela última estação, tem-se que p(k+1) é igual a zero, possibilitando com isto a determinação iterativa de p(n) com n variando de k até 1.

Por assumir que a distribuição dos tempos de serviço de todas as estações são idênticas, pode-se supor que o tempo médio de serviço seja igual à unidade de tempo.

Deve-se observar que p(1) é uma função crescente da taxa de chegada normalizada (LAMBDA.N) (tempo de serviço igual a 1)

de tal forma que o valor da atividade do anfitrião determina um valor único para a taxa de chegada externa. Logo, para uma dada utilização RO do anfitrião, através de um método iterativo pode-se calcular os valores de LAMBDA.N e da probabilidade do primeiro nó rejeitar uma mensagem (p(1)).

Descrevendo este método, tem-se que para um dado valor de LAMBDA.N pode-se calcular passo a passo o valor de p(n) para n variando de k até 1. O valor exato de LAMBDA.N é obtido quando a igualdade RO = LAMBDA.N / (1-(p(1)) permanecer. O valor para S(RO), isto é, o tempo de serviço a partir de uma determinada carga, é calculado da seguinte forma:

$$S.EE.rn\ (RO) = (tf(L) + Cb + (tf(L)/2) * RO) * (1-p(1)) + T * p(1) \qquad (a.13)$$

$$S.HDLC.ra\ (RO) = tf(1) * (1-p(1)) + T * p(1), \qquad (a.14)$$

de acôrdo com a política de retransmissão. A taxa de chegada total (LAMBDA.T) é igual a:

$$LAMBDA.T = RO / S(RO). \qquad (a.15)$$

Como esta taxa é o somatório dos pacotes externos e reciclados, a vazão do sistema é dado por:

$$LAMBDA = LAMBDA.T * (1 - p(1)) \qquad (a.16)$$

A.2 - Análise do método de retransmissão pelo anfitrião:

A taxa de chegada na estação (n+1) é dada por:

$$LAMBDA(n+1) = LAMBDA(n) * (1-p(n)) \quad n=1 \text{ até } k-1. \qquad (a.17)$$

Se for convenientemente denotado por LAMBDA(k+1) a taxa de partida da última estação (k), então a equação precedente é válida para qualquer valor de (k). Como a retransmissão pelo anfitrião somente é utilizada com os tempos de serviço exponencialmente distribuído, a solução desenvolvida só se aplica para este caso em particular. A probabilidade de rejeição de um pacote é obtida pela aplicação do sistema clássico M/M/1/M(n):

p(n) = RO(n) ** M(n) * (1-RO(n)) / (1 - RO(n) ** M(n+1)).

(a.18)

Sabendo-se que a taxa de partida da última estação é igual a taxa de chegada externa na rede, isto é, LAMBDA(k+1) é igual a LAMBDA. Analogamente ao caso anterior, começando-se com a última estação pode-se calcular os valores para LAMBDA(n) e p(n) para (n) variando de k até 1.

O anfitrião é encarado como sendo um sistema M/M/1 com tempo de serviço S(RO) e uma taxa de chegada de:

LAMBDA.T = LAMBDA + Somatório (p(i) * LAMBDA(i)), (a.19)

com i variando de 1 até k.

Como já foi visto anteriormente o tempo de serviço (S(RO)) depende do protocolo utilizado:

S.EE.ra (RO) = tf(L) + Cb + tf(L) / 2 (a.2Ø)

S.HDLC.ra (RO) = tf(L). (a.21)

Logo, para uma dada taxa de utilização do anfitrião obtem-se a taxa de chegada total (LAMBDA.T) e a vazão do sistema é obtida por um método algoritmico que determina o valor de LAMBDA quando a seguinte igualdade fôr verdadeira:

LAMBDA = LAMBDA.T - Somatório (p(i) * LAMBDA(i)), (a.22)

para i variando de 1 até k.

A solução é única porque os valores de p(i) são crescentes com LAMBDA.

A.3 - O modelo considerando as estações C e R:

O modelo considerado é o que está apresentado na figura IV.2, sendo somente analisado o caso da política de retransmissão pelo nó. A solução proposta é a de se considerar uma estação equivalente. A rede fechada representando o modelo da rede de comutação de pacotes pode ser substituída por uma simples fila com uma taxa de estado dependente PSI(j) (para j variando de 1 até o número total de créditos, isto é, o número total de pacotes na rede mais os créditos livres). Logo, o problema se resume no estudo de uma rede de filas fechadas com um tamanho finito de buffers. Como não se conhece um método disponível para estudar este sistema, foi adotado uma simulação a fim de se calcular a utilização A(j,k) do k-ésimo servidor quando existem j usuários na rede. Gelenbe assumiu em seu estudo que o tempo de serviço da fila de créditos é igual ao tempo de serviço do anfitrião.

Assumindo-se que o tempo médio de serviço de cada estação é igual a unidade de tempo, obtem-se a taxa de serviço equivalente como sendo:

$$PSI(j) = A(j,k). \qquad (a.23)$$

O sistema equivalente pode ser visto na figura A.2

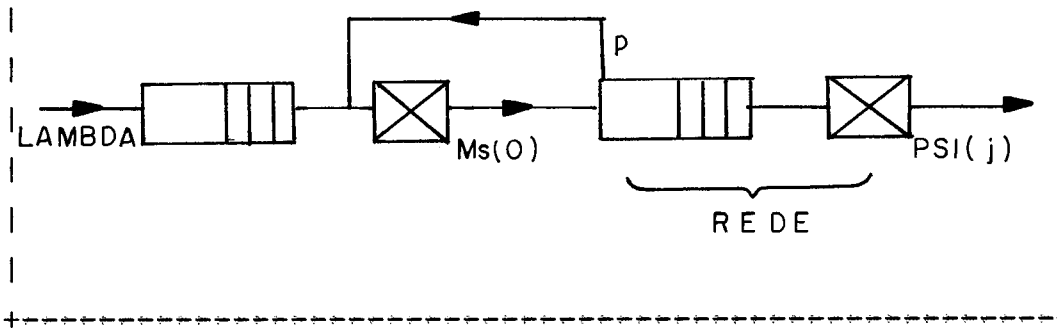


Figura A.2 - Modelo unificado equivalente

A probabilidade de rejeição p para um determinado nó é considerada como sendo a probabilidade da fila seguinte estar lotada, logo:

```
p = (RO / (PSI(1)*PSI(2)*...PSI(n)) /
    (1+RO/PSI(1) +...+ RO**N/PSI(1)*PSI(2)...PSI(N)), (a.24)
```

onde RO é a utilização do anfitrião, e
N é o número total de créditos.

A partir deste valor pode-se calcular o tempo de serviço que é igual ao S.EE.rn ou S.HDLC.rn seguindo o protocolo nó-a-nó. A taxa total de chegada é:

```
LAMBDA.T = RO / S(RO)                                    (a.25)
```

e a vazão do sistema é dada por:

```
LAMBDA = LAMBDA.T * (1 - p).                             (a.26)
```

ANEXO B

B - Cálculo do tempo de transferência /BUX*W81/:

B.1 - Considerações iniciais:

Neste anexo serão apresentados os modelos aplicados em quatro tipos de sub-rede de comunicação visando a determinar o tempo de transferência médio de um pacote. Esta análise é baseada em modelos analíticos que descrevem as várias tecnologias e os mecanismos de acesso com um sufuciente nível de detalhamento.

Os tipos de sub-rede de comunicação analisados são os que se aplicam às redes locais de computadores. Os tipos considerados são:

- Anel do tipo 'token' ('token ring');

- Anel particionado ('slotted ring');

- Barra de acesso randômico ou de Acesso múltiplo com percepção da portadora e detecção de colisão (CSMA/CD: 'carrier sense multiple-access with collision detection');

- Barra de acesso ordenado ou de Acesso múltiplo multinível (MLMA: 'multilevel multiple-acess').

O objetivo do modelo é o de se determinar as características de atraso e de vazão dos sistemas. O atraso é medido como sendo o tempo médio de transferência (tf) dos pacotes, sendo definido como o intervalo de tempo da geração do pacote na estação de origem até a sua recepção pelo destinatário. Isto significa que o tempo de transferência inclui o enfileiramento e os atrasos do transmissor, o tempo de transmissão do pacote e o tempo de propagação.

Para possibilitar a comparação dos resultados, as seguintes hipóteses foram assumidas e aplicadas nos modelos:

- os pacotes são gerados nas (n) estações de acôrdo com os processos de Poisson, com taxas LAMBDA(i) com (i) variando de 1 até (n). Denota-se por LAMBDA a taxa total de chegada à sub-rede, isto é, LAMBDA é igual ao somatório de todos os LAMBDA(i);

- O tamanho do pacote L pode ter uma distribuição geral, sendo consituído de uma parte constante relativa ao cabeçalho (Lh) e de uma parte variável relativa à informação (Ld).

Denota-se por v a velocidade de transmissão e por TAU o atraso máximo o atraso máximo de propagação fim a fim no caso de uma barra ou, o tempo de latência do 'round-trip' no caso de um sistema em anel.

O tempo de propagação é assumido ser constante e igual para todos os casos. Para efeitos do modelo, foi considerado que a distância máxima entre o transmissor e o receptor é igual à metade da distância máxima da barra ou do anel.

Uma outra observação importante é a de não se considerar, neste anexo, os efeitos relacionados aos erros de transmissão, aos procedimentos de recuperação de erros e aos aspectos de controle de fluxo.

B.2 - Anel do tipo 'token':

Neste tipo de sub-rede, o acesso ao canal de transmissão é controlado pela passagem de uma permissão ('token') pelo anel. Quando o sistema é colocado em funcionamento, uma estação previamente determinada gera uma permissão livre que percorre o anel até que uma estação que se encontra para transmitir, modifica o estado da permissão para ocupada,

transmitindo a seguir o pacote que pode ser de tamanho fixo ou variável. A estação geradora do pacote é também a encarregada de retirar o pacote do anel, liberando com isto a permissão.

Esta operação é mostrada na figura B.1 que apresenta o modelo apresentado para este caso.

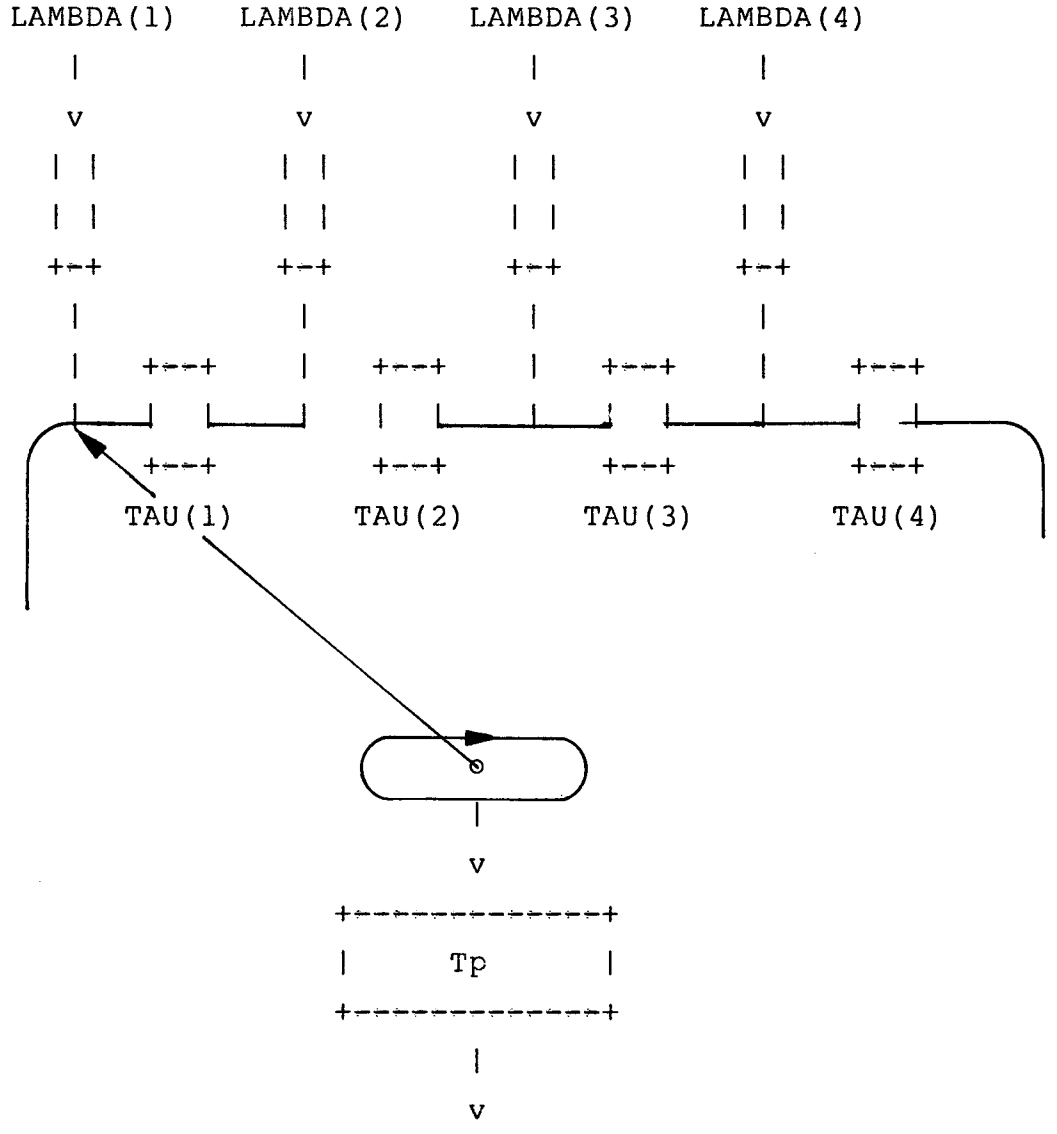


Figura B.1: Modelo do anel do tipo 'token'

O modelo analisado é um modelo de filas com um único servidor com tantas filas quantas forem as estações conectadas ao anel. As filas são atendidas de uma maneira cíclica, simbolizada pela chave rotativa que aponta para o 'token' livre. O tempo necessário para a passagem da permissão da

i-ésima estação para a estação (i+1) (atraso devido à propagação mais a latência adicional devido à manipulação da permissão na estação i) é denotado pela constante TAU(i).

No que diz respeito a ordem de atendimento das estações, várias táticas podem ser escolhidas (vide /VASCE82/), como por exemplo o atendimento de uma fila até que esta se esvazie (atendimento exaustivo) ou o atendimento de um número limitado de mensagens (por exemplo, uma) para cada possibilidade de acesso (atendimento não-exaustivo). Embora, existam diferenças em têrmos de desempenho entre estas táticas, assume-se que para os parâmetros de interesse em redes locais estas diferenças são ínfimas se o tráfego fôr uniformemente distribuído entre todas as estações.

Utilizando uma aproximação discreta em tempo, uma solução para o atraso médio de enfileiramento pode ser obtido, considerando-se a hipótese de taxas de chegada iguais (LAMBDA(i)) e atrasos iguais de comutação (TAU(i)). A fim de se limitar o impacto da consideração do tempo ser discreto na comparação foi considerado o caso do intervalo discreto de tempo tender a zero. Para este caso limite, obtem-se o seguinte resultado para o tempo de transferência médio:

```
tf =   RO * E[ Tp**2 ] / 2*(1-RO) * E[Tp] +
     + E[Tp] +
     + TAU * (1 - RO / n) / 2*(-RO) +
     + TAU / 2,                                    (b.1)
```

onde

$$RO = LAMBDA(i) * E [Tp] \qquad (b.2)$$

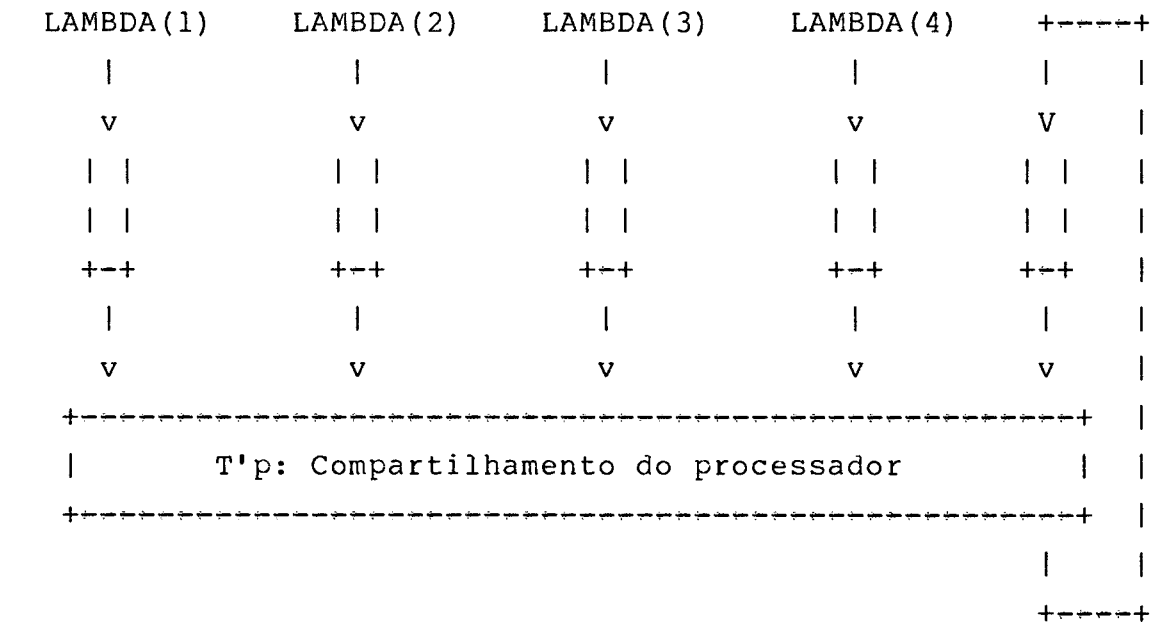
$$Tp = L / v. \qquad (b.3)$$

B.3 - Anel Particionado ('Slotted Ring'):

Neste tipo de sub-rede um número constante de vagões

('slots') de tamanho fixo circulam continuamente pela rede. O estado do vagão, isto é, se ele está cheio ou vazio, é indicado no cabeçalho do vagão. Qualquer estação que esteja pronta para transmitir ocupa o primeiro vagão vazio, pela alteração do indicador de estado para cheio, colocando a seguir a mensagem no vagão. Quando a estação transmissora receber de volta o vagão ocupado ela deve alterar o indicador de estado do vagão para vazio. Esta operação previne o bloqueio do anel, possibilitando um compoartilhamento equitativo do canal de comunicação por todas as estações.

O modelo de filas analisado possui (n+1) filas onde n é o número de estações conectadas ao anel. Os pacotes que estão esperando em uma determinada fila são atendidos em sequência durante um pequeno intervalo de tempo que corresponde ao tamanho do vagão. Entre duas possibilidades de acesso de uma estação o vagão livre completou exatamente um ciclo pelo anel. Como a latência do anel corresponde a duração do vagão, esta pode ser descrita pelo 'loop' fechado mostrado na figura B.2 que contém sempre um usuário fictício.



onde T'p = Tempo de serviço do pacote.

Figura B.2: Modelagem do anel particionado.

Por conveniência analítica, admite-se que o tempo de serviço (DELTA.T) tende a zero. O modelo resultante de compartilhamento do processador fornece uma boa aproximação para os resultados de intervalo de tempo finito se este intervalo fôr suficientemente pequeno quando comparado com o tempo de serviço médio. Como no ambiente considerado, os pacotes são, geralmente, 1Ø vezes maior do que o tempo do vagão, em média, esta condição é atendida.

Para se determinar o tempo de transferência médio, o modelo da figura B.2 pode ser concebido como uma simples rede de filas mistas com (n+1) classes de usuários. Se denotarmos por x(i) o número de pacotes na fila Q(i) pode-se determinar as probabilidades do estado de equilíbrio do modelo como:

$$p(x) = p(x(1),.....,x(n))$$

$$= (1-RO)^{**}2 * \binom{x(1)+...+ x(n) + 1}{x(1), ..., x(n)} *$$

$$* RO(1)^{**}x(1) * ... * RO(n)^{**}x(n) \qquad (b.4)$$

onde

$$RO(i) = LAMBDA(i) * E\,[T'p] \qquad (b.5)$$

$$RO = \text{Somatório}\,(RO(i)). \qquad (b.6)$$

Para se calcular o tempo de serviço médio do pacote E[T'p], deve-se notar que cada vagão consiste de um campo de dados de tamanho Ld e de um campo para o cabeçalho de tamanho Lh. Considerando-se estes pontos, o tempo de serviço médio do pacote é acrescido, sendo determinado da seguinte forma:

$$E[\,T'p\,] = ((\,Lh + Ld\,) \,/\, Ld) * (E[\,Lp\,] \,/\, v\,). \qquad (b.7)$$

A partir de (b.4) o número total de pacotes esperado

pode ser facilmente calculado pela aplicação do teorema de Little (/KLEIL76/), possibilitando determinar-se o tempo de transferência como sendo:

$$tf = (2 / (1-RO)) * E [T'p] + TAU / 2. \qquad (b.8)$$

B.4 - Acesso múltiplo com percepção da portadora (CSMA/CD):

Entre os vários tipos de acesso randômico o acesso múltiplo com percepção da portadora e detecção de colisão aparece como a solução mais atrativa. Neste esquema, toda estação que está esperando transmitir um pacote deve escutar a barra a fim de verificar se alguma transmissão está em curso. Se houver, a estação deve esperar pelo término desta transmissão. Apesar da percepção da portadora, as colisões não podem ser completamente evitadas, por causa do tempo de propagação na barra. Após a detecção de uma colisão a transmissão é abortada e a estação espera um intervalo de tempo randômico para tentar a nova transmissão.

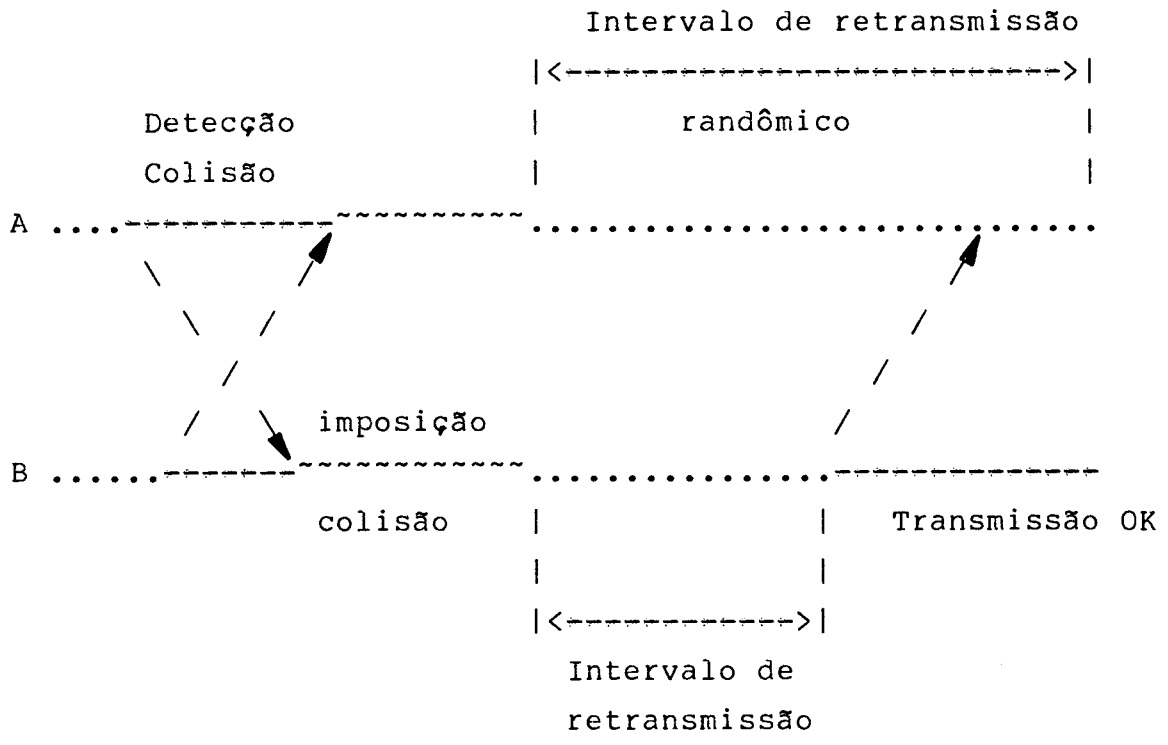


Figura B.3: Exemplo de Operação CSMA/CD

Análises de eficiência dos sistemas CSMA/CD foram realizados por /LAM*S8Ø/. O modelo foi desenvolvido supondo-se que o sistema é estabilizado pela utilização de um algoritmo adaptativo adequado. Por razões de simplificação analítica o canal particionado com tamanho de vagão 2*TAU é assumido em /LAM*S8Ø/. Como consequência desta hipótese tem-se que mesmo se a utilização tender a zero, os pacotes tem que esperar, em média, pelo tempo TAU antes de poderem ser transmitidos. Como o tempo de acesso não existe em um sistema não particionado, pode ser um possível fator para a má interpretação dos resultados. Com uma simples modificação na fórmula do atraso proposta por Lam, redução do atraso médio, o tempo médio de transferência para a barra CSMA/CD é:

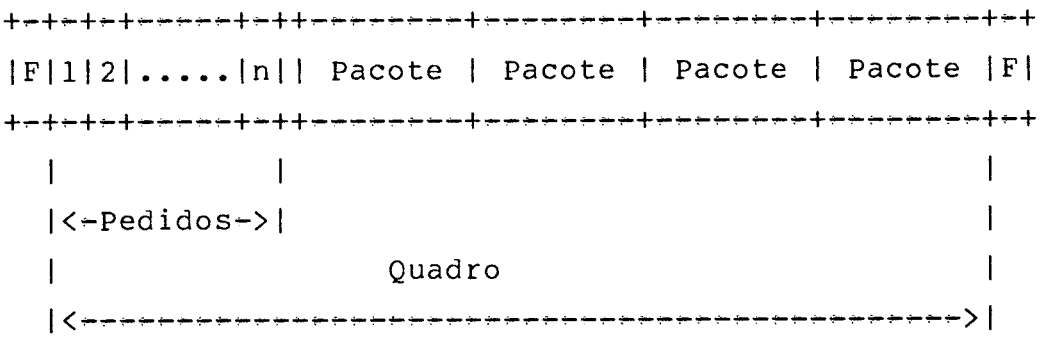
```
tf = LAMBDA * { E [ Tp**2 ] + (4*e + 2) * TAU * E[Tp] +
     + 5 * TAU**2 + 4*e*(2*e - 1) * TAU ** 2 } /
     / 2 * { 1 - LAMBDA * (E[Tp] + TAU + 2*e*TAU) } +
     + E [ Tp ] +
     + 2*TAU*e -
     - { (1 - e**(- 2 * LAMBDA * TAU )) *
     * (2/LAMBDA + 2 * TAU / e - 6 * TAU) } /
     / 2 * { F'p (LAMBDA) * e ** (-LAMBDA * TAU) * 1/e +
     + e ** (-2*LAMBDA*TAU) } +
     + TAU / 2.                                          (b.9)
```

O têrmo F'p corresponde a transformada de Laplace da função densidade de probabilidade do tempo de serviço do pacote (Tp=(Lh + Lp)/v).

B.5 - Barra de Acesso Ordenado:

Como exemplo de um sistema em barra que utiliza o acesso ordenado foi considerado o esquema de reserva MLMA ('MultiLevel Multiple Access') proposto por Rothauser e Wild /TROPC81/ que funciona da maneira descrita a seguir.

A transmissão da informação ocorre em quadros de tamanho variável (vide fig. B.4). O controlador da barra fornece em intervalos de tempo apropriados 'flags de início de quadro.



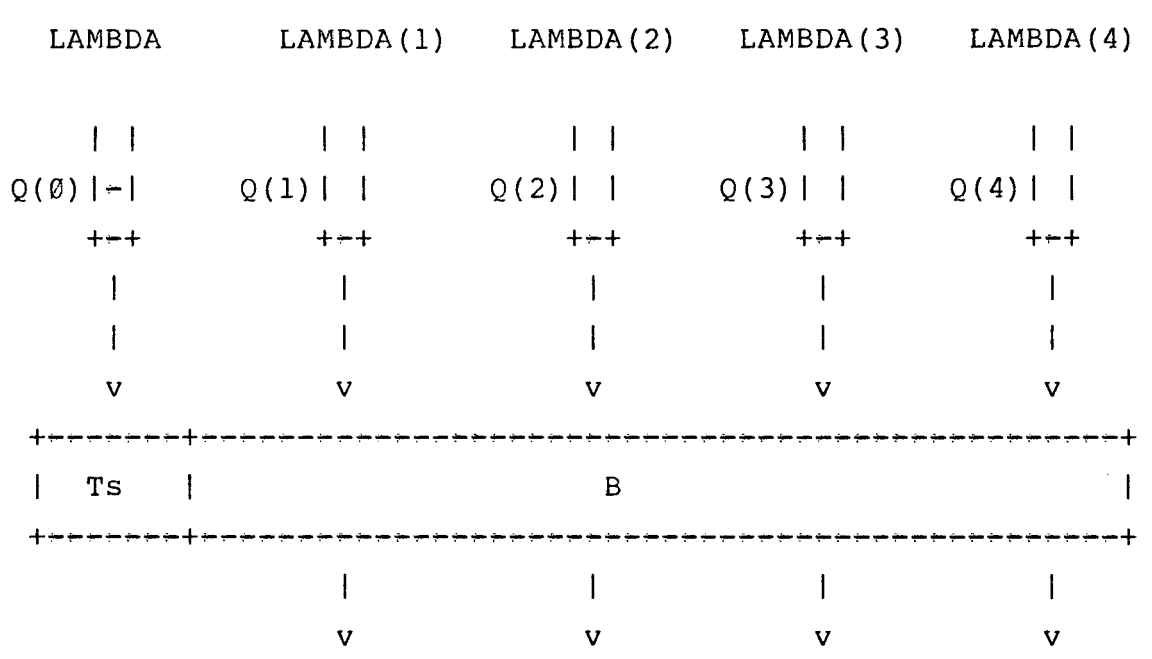
F = Flag

Figura B.4 - Estrutura do Quadro

O quadro é dividido em duas partes, uma relativa ao vagão de pedidos e a outra constituída de um número arbitrário de pacotes. Na versão considerada, cada estação possui um bit privativo dentro do vagão de pedidos. Este bit é utilizado para indicar o desejo de transmitir um pacote neste quadro. No final do ciclo de pedidos, todas as estações sabem quais as estações que utilizarão o quadro. A sequência de transmissão é dada por um esquema de prioridades conhecido por todas as estações.

O modelo que descreve este tipo de operação é mostrado na figura B.5. A barra é modelada como um sistema de servidor único. Os pacotes de todas as estações que foram gerados recentemente e que ainda não foram selecionados constituem a fila Q(Ø). De acôrdo com a operação da barra descrita anteriormente, estes pacotes não podem ser transmitidos no quadro atual, devendo esperar até que o novo quadro seja iniciado. Neste momento, todos os pacotes da fila Q(Ø) obtem simultaneamente a primeira fase de serviço, gastando um tempo Ts, que representa o tempo necessário para a seleção. Para assegurar que todas as estações conhecem os pedidos feitos o tempo Ts deve ser significantemente maior que o tempo de transmissão do vagão de pedidos. Neste caso o tempo de seleção é definido como sendo igual ao dôbro do tempo necessário para se transmitir n bits mais o dôbro do tempo de propagação

(TAU). Após este tempo Ts, os pacotes são colocados nas filas Q(1)-Q(n), onde Q(1) contém os pacotes da estação de maior prioridade e Q(n) a de menor prioridade. Quando todos os pacotes das filas Q(1)-Q(n) forem transmitidos, um novo quadro é iniciado.



LAMBDA(i) : taxa de chegada dos pacotes
LAMBDA : taxa de chegada total
B : tempo de serviço do pacote
Ts : tempo de seleção

Figura B.5 - Modelo da Barra Ordenada

O tempo médio de transferência neste caso é obtido pela seguinte expressão /BUX*W81/:

$$tf = \left(RO' * \{ E[Tp^{**}2] + TAU^* E [Tp] + TAU^{**}2 / 3 \} / / 2 * (1-RO') * \{ E [Tp] + TAU / 2 \} \right) + + E [Tp] + + (3-RO') / (1-RO') * Ts/2 + TAU/2 \qquad (b.1\emptyset)$$

onde:

$$RO' = LAMBDA * \{ E [Tp] + TAU / 2 \}$$

$$Tp = (Lh + Lp) / v.$$

C - Nomenclatura

C	fila de créditos
ef (.)	tamanho operacional mínimo para o pacote
Ef (.)	tamanho máximo efetivo para o pacote
E [f(x)]	média da função f(x)
e (.)	tamanho operacional máximo para o fragmento
e'(.)	tamanho operacional mínimo para o fragmento
F	unidade básica de fragmentação
f.n(x)	distribuição dos tempos de serviço na estação "n"
GMD	Gesellschaft fur Mathematik und Datenverarbeitung
H	número de octetos relativos ao cabecalho trans-rede
HDLC	High Data-Link Control
Ks [f(x)]	quadrado do coeficiente de variação da função f(x)
l	tamanho do pacote de controle que retorna com a confirmação
L	tamanho médio dos pacotes transmitidos
LAMBDA	vazão total do sistema de redes
LAMBDA.T	taxa total de chegada
Ld	número de octetos de dados do usuário
L(n)	número de octetos relativos ao cabeçalho da rede "n"
Max(n)	Tamanho máximo para o pacote na rede "n"
Ms	Média
Nf (.)	Número de fragmentos gerados
P (j)	j-ésimo caminho entre a origem e destino
p(.)	probabilidade de um determinado caminho ser escolhido
p(.)	probabilidade de retransmissão de um pacote
QCV	quadrado do coeficiente de variação
R	estação que representa o tempo de retorno dos créditos
REDE	conjunto de redes
RFC	controle de fluxo por taxa ('rate flow control')

RO	carga em um determinado canal
S	tempo total necessário para a transmissão de um pacote
S.EE.ra	tempo médio para uma transmissão no procedimento Envia e Espera com retransmissão pelo anfitrião
S.EE.rn	tempo médio para uma transmissão no procedimento Envia e Espera com retransmissão pelo nó
S.HDLC.ra	tempo médio para uma transmissão no procedimento HDLC com retransmissão pelo anfitrião
S.HDLC.rn	tempo médio para uma transmissão no procedimento HDLC con retransmissão pelo nó
ta	tempo gasto por um pacote anteriormente transmitido
tf	tempo de transferência
tfrag	tempo de processamento devido a fragmentação
Var [f(x)]	variância da função f(x)
XFC	controle de fluxo induzido pelo X.25
WFC	controle de fluxo por janela ('window flow control')
wØØ, wlØ	tempos devidos aos procedimentos de comutação e 'software'
wØl, wll	atraso de escrita nos sistemas
w'Øl, w'll	tempo gasto na geração e no envelopamento do pacote
w'ØØ	tempo devido ao processamento da confirmação de recebimento
w'lØ	tempo devido ao processamento no recebimento do pacote

D - Indice Alfabético