UNIVERSIDADE DO PORTO
FACULDADE DE ENGENHARIA
Departamento de Engenharia Electrotécnica e de Computadores

Estudo Comparativo de protocolos de nível de transporte em redes rápidas XTP versus TCP e TP4

Nuno Jorge Gonçalves de Magalhães Ribeiro

Abril de 1993

INESC Instituto de Engenharia
de Sistemas e Computadores

Parecer

Confirmo tanto o empenho revelado no estágio pelo Licº **Nuno Jorge Gonçalves de Magalhães Ribeiro**, como a qualidade técnica do trabalho realizado "Estudo comparativo de protocolos de nível de transporte em redes rápidas XTP versus TCP e TP4".

Porto e INESC, 14 de Maio de 1993

José Manuel da Costa Correia
Investigador do INESC

Largo Mompiller 22 • Apartado 4433 • 4007 Porto Codex • Portugal • Tel. 351.2.321006 • Fax. 351.2.318692 • Tlx. 23023 INESC P
Pessoa Colectiva n.º 501107169 • Associação Privada sem fins lucrativos, declarada de Utilidade Pública • C.R.C. de Lisboa n.º 72

FACULDADE DE ENGENHARIA DA UNIVERSIDADE DO PORTO
Departamento de Engenharia Electrotécnica e de Computadores
Rua dos Bragas, 4099 Porto Codex, PORTUGAL
Telef. 351-2-317105/107/412/457 · Telex 27323 FEUP P · Telefax 351-2-319280

Parecer

Confirmo tanto o empenho revelado no estágio pelo Licº **Nuno Jorge Gonçalves de Magalhães Ribeiro**, como a qualidade e o interesse científico do trabalho realizado e intitulado "Estudo comparativo de protocolos de nível de transporte em redes rápidas XTP versus TCP e TP4".

Porto e FEUP, 14 de Maio de 1993

Raul Fernando Almeida Moreira Vidal
Professor Associado da FEUP

INESC - Instituto de Engenharia de Sistemas e Computadores

Estudo Comparativo de protocolos de nível de transporte em redes rápidas XTP versus TCP e TP4

Nuno Jorge Gonçalves de Magalhães Ribeiro

Porto, 1993

Índice

Estudo Comparativo de protocolos de nível de transporte em redes rápidas XTP versus TCP e TP4

Abstract. Este trabalho consiste num estudo comparativo dos mecanismos de transporte de três protocolos: **ISO TP4, DARPA TCP** e **XTP.** O objectivo fundamental é realçar a necessidade deste novo protocolo, dando particular ênfase aos melhoramentos funcionais e de desempenho introduzidos. Este estudo é desenvolvido tendo em conta duas áreas fundamentais do nível de transporte: na primeira, foca.-se os aspectos relacionados com a **gestão da ligação** (i.e. estabelecimento e libertação da ligação); na segunda, analisa-se os mecanismos utilizados durante a fase de **transferência de dados** através de uma ligação. O objectivo a atingir no estudo da primeira área, onde se compara os mecanismos de gestão da ligação, é determinar a adequação de cada um dos três protocolos a ambientes **HSLANs** (redes locais de alta velocidade) que são caracterizados, sob este ponto de vista, por um desempenho elevado e um grande número de requisitos aplicacionais em relação aos tipos de comunicação que serão fornecidos. O objectivo a atingir na análise da segunda área é realçar as limitações e incovenientes dos mecanismos de transferência de dados dos protocolos TP4 e TCP no que diz respeito à sua aplicação nos mesmos ambientes HSLANs que são caracterizados, sob este ponto de vista, por uma elevada largura de banda e uma taxa de erros diminuta. Deste modo, pretende-se identificar a área onde o emergente **XTP** contribui para um melhoramento da situação passada. Este trabalho baseia-se num estudo apresentado na revista de telecomunicções EET e nos temas aí explanados. Dado o interesse deste estudo comparativo, cada tema é também aqui explorado e explicado recorrendo às normas do XTP e ao livro 'XTP: The Express Transfer Protocol'. Foi ainda consultada outra bibliografia como apoio aos conceitos relacionados com o TP4 e o TCP. A realização deste estudo insere-se no âmbito de um estágio efectuado em 1993 no INESC - Instituto de Engenharia de Sistemas e Computadores, orientado pelo Professor Doutor Raul Moreira Vidal e apoiado pelo PRODEP através da concessão de uma bolsa de estágio.

1. Introdução

O protocolo **TCP** (DARPA Transmission Control Protocol) e o protocolo **TP4** (ISO Transport Protocol class 4) surgiram na altura em que a infraestrutura comum de comunicação era conseguida com base em linhas comutadas, linhas alugadas e também WANs de comutação de pacotes baseadas em tecnologia telefónica e nós de comutação baseados em computadores de baixo desempenho. A largura de banda do meio com a sua elevada taxa de erro, o espaço de *buffer* do nó e o poder de processamento do nó eram então os recursos críticos. A concepção do TCP e do TP4 foi condicionada pela preocupação de obter um serviço sem erros neste tipo de ambientes.

A tecnologia de redes é, neste momento, consideravelmente diferente nas LANs baseadas em serviços sem estabelecimento de ligação (*connectionless)* até ao nível de rede, no entanto, o TCP e o TP4 continuam a ser os dois protocolos de transporte orientados à ligação (*connection-oriented)* mais utilizados nos ambientes das LANs.

Hoje em dia a existência de taxas apreciáveis de carga efectivamente transportada (throughput) , pelo menos na LANs, é geralmente reconhecida. No entanto, para manter *troughputs* elevados na interface do serviço de transporte, os atrasos de processamento e as latências na camada de transporte devem ser estritamente controlados.

Para além da evolução no sentido de infraestruturas de rede mais eficientes, há uma evolução no sentido da diversificação das necessidades das aplicações no que diz respeito à comunicação através das redes, devida ao advento dos sistemas distribuidos.

Além disso, o advento dos serviços *multimedia*, para além de oferecer novas possibilidades aos utilizadores, requer novos serviços da camada de transporte.

Como a camada de transporte é a "camada-chave" que se pretende que sirva como junção entre as necessidades da aplicação e as possibilidades oferecidas pelas redes, as evoluções acima mencionadas sugerem que o critério de concepção adoptado para os protocolos de transporte na década passada deve ser revisto.

Um protocolo implica sempre três aspectos: **mecanismos** para implementar o conjunto de funções pretendidas, uma **sintaxe** que descreva o formato da Unidade de Dados do protocolo (PDU-Protocol Data Unit) e, por fim, uma **implementação**. No que diz respeito à implementação, pode-se argumentar que uma má implementação dá origem a mau desempenho, no entanto, nem mesmo boas implementações são capazes de corrigir a influência nefasta de mecanismos mal concebidos e de funcionar de forma eficiente com formatos das PDUs mal concebidos.

Entre os novos protocolos de nível de transporte, o **X**press **T**ransfer **P**rotocol (XTP) representa uma nova tendência na concepção de protocolos. Na realidade, o protocolo XTP não é apenas um protocolo de transporte, é um *protocolo de transferência* porque possui, para além de uma parte de transporte, uma outra parte de encaminhamento que pertence à camada três OSI e que tenta melhorar o controle de congestionamento.

O objectivo deste estudo é efectuar uma comparação dos mecanismos de transporte do TP4 e TCP com os do XTP. A análise comparativa destes três protocolos centrar-se-á exclusivamente nos seus mecanismos numa perspectiva qualitativa, ignorando por completo todos os aspectos relacionados com a sintaxe ou a implementação.

Os mecanismos do TP4 e do TCP serão examinados em detalhe de modo a realçar todas as suas limitações e incovenientes no que diz respeito à sua adequação na área da largura de banda elevada com baixas taxas de erro. Paralelamente, efectua-se uma análise profunda dos mecanismos de transporte do XTP, de modo a identificar distintamente o modo como este protocolo contribui para melhorar a situação existente. Deste modo, cada mecanismo de transporte do XTP será devidamente descrito e posteriormente comparado com o seu equivalente no TP4 e no TCP (nos casos em que existe nestes protocolos !). Significa isto que os mecanismos do TP4 e do TCP serão tomados como pontos de referência para o estudo dos mecanismos de transporte do XTP.

O estudo encontra-se estruturado da seguinte forma: na **primeira** secção faz-se uma pequena introdução onde se descreve os objectivos e se situa o XTP no contexto actual das redes locais; na **segunda** secção define-se as bases para o estudo comparativo; na **terceira** secção cobre-se a primeira grande área em análise - a *gestão da ligação*, onde se discute os vários mecanismos de estabelecimento e libertação da ligação, terminando com as conclusões referentes ao estudo analítico desta área; na **quarta** secção aborda-se a segunda grande área em análise - os *mecanismos de transferência de dados*, começando por classificar esses mecanismos para posteriormente os analisar em detalhe. Esta secção termina com as conclusões que apresentam sumáriamente os pontos mais importantes a retirar deste estudo.

2. Base para o estudo comparativo

Neste estudo estamos interessados em observar o comportamento do TP4, TCP e XTP em ambientes LANs (redes locais). Desta forma, assume-se que a rede é uma LAN isolada ou um conjunto de LANs interligadas.

2.1 TP4 nas LANs

Originalmente, a possibilidade de fazer com que o standard ISO TP4 operasse sobre um serviço de nível de rede *connectionless* não estava especificado nas normas da ISO. Posteriormente essa hipótese foi considerada e o serviço de rede então especificado foi designado ISO CLNS (ConnectionLess Network Service), sendo fornecido pelo protocolo ISO CLNP (ConnectionLess Network Protocol). O CLNP é um protocolo Internet que fornece o standard ISO CLNS apoiando-se no standard ISO CLSNS (ConnectionLess SubNetwork Service).

Em ambientes LAN, este standard (ISO CLSNS) pode ser obtido por aplicação das Funções de Convergência Dependentes do Sub-nível de Rede (SNDCFs) directamente sobre o serviço *connectionless* de tipo um do sub-nível de Controlo da Ligação Lógica (sub-nível LLC) da camada dois OSI como se pode verificar na figura 1. A presença de um protocolo LLC é obrigatória no contexto da pilha protocolar OSI. As funções SNDCFs são apenas funções locais de mapeamento, pelo que não se exige nenhum protocolo no sub-nível de rede (sub-nível SubNetwork)do nível três OSI.

Neste estudo, o termo '*router*' refere-se a uma *gateway* de interligação que executa uma função de retransmissão com regeneração (*relay*) no sub-nível Internet do nível três OSI. Nos casos em que se considerem LANs interligadas por meio de *routers*, o protocolo CLNP (ou um seu subconjunto adequado - NonSegmenting Protocol Subset) deve ser utilizado.

Nos casos em que se considerem LANs isoladas ou um conjunto de LANs interligadas por *bridges* que executam uma função de *relay* no sub-nível MAC, o protocolo CLNP pode ser substituido por outro seu subconjunto que não é mais do que um conjunto vazio de funções (Inactive Network Layer Protocol Subset).

2.2 TCP nas LANs

Na pilha protocolar DARPA, o protocolo de transporte TCP é associado com o protocolo do nível inferior - IP (Internet Protocol) e com o protocolo ICMP (Internet Control Message Protocol).

Normalmente, o TCP não pode correr sem o IP, pelo que esta combinação (TCP/IP) é sistemáticamente instalada em todos os sistemas, independentemente das LANs serem interligadas por *routers* ou *bridges*.

As duas pilhas protocolares DARPA são apresentadas na figura 2.

A figura 2 a) está relacionada com o standard Ethernet-DIX (**D**igital, **I**ntel e **X**erox), no qual o TCP/IP se encontra instalado directamente acima do serviço *connectionless* MAC sem qualquer protocolo LLC intermédio.

A figura 2 b) corresponde à série de standards IEEE 802.x, i.e. o 802.3 (CSMA/CD), o 802.4 (Token Bus) e o 802.5 (Token Ring), bem como ao standard FDDI, nos quais o protocolo LLC de tipo 1 deve ser incluido na pilha protocolar entre o protocolo MAC e o TCP/IP. O protocolo LLC de tipo 1 tem como objectivo oferecer um serviço de interface de ligação de dados uniforme, seja qual for o protocolo utilizado no sub-nível MAC, bem como uma facilidade de endereçamento. Na figura 2 b) pode-se verificar que o encapsulamento de pacotes IP no sub-nível LLC segue as normas estabelecidas já que utiliza o protocolo SNAP (SubNetwork Acces Protocol) para identificar protocolos públicos e/ou privados que pretendem aceder ao serviço LLC do tipo 1. A figura 3 ilustra o encapsulamento de pacotes IP no sub-nível LLC por utilização do SNAP.

O Cabeçalho SNAP é simplesmente uma extensão do cabeçalho básico LLC tipo 1. Quando o campo de três bytes <código de organização> do cabeçalho SNAP contém o valor zero (i.e. o valor atribuido à Xerox), o campo de dois bytes seguinte, nomeadamente o campo <tipo>, irá ser interpretado exactamente da mesma forma que o campo de dois bytes <tipo> no cabeçalho Ethernet-DIX MAC, e o resto do pacote deve estar em conformidade com as convenções respeitantes a esse tipo. Ou seja, o cabeçalho SNAP com um código de organização igual a zero, colocado imediatamente atrás do cabeçalho LLC, existe apenas para oferecer um serviço semelhante ao Ethernet-DIX sobre uma LAN IEEE 802 ou FDDI, permitindo aceder aos vários tipos de protocolos Ethernet-DIX já definidos.

2.3 XTP nas LANs

O emergente XTP foi concebido tendo em mente os ambientes LANs. O XTP é mais do que um protocolo de transporte: o XTP é um **protocolo de transferência** que derivou de um standard Francês para uma LAN militar de tempo real, propondo um arquitectura que cobre as camadas três e quatro OSI. De facto, o XTP possui uma parte de transporte e uma parte de encaminhamento (*routing*) que pertence claramente à camada três OSI. Os seus autores decidiram combinar as funções comuns da camada de transporte com várias funções da camada de rede num único protocolo e, por conseguinte, numa única estrutura de dados protocolar-PDU. Deste modo, as unidades de dados do serviço (SDUs) apresentadas ao fornecedor de serviços XTP (*provider*) são encapsuladas uma vez com informação de controle relacionada com a parte de transporte e informação de controle relacionada com a parte de encaminhamento do XTP.

Verificando que, conceptualmente, o XTP combina a camada de transporte com o sub-nível internet da camada três de rede, conclui-se que o XTP deveria comportar-se de forma semelhante à combinação de um protocolo de transporte clássico com um protocolo internet clássico. Ou seja, o XTP deveria funcionar correctamente em cima da camada dois OSI (DLL-Data Link Layer). De facto, esta afirmação verifica-se para uma LAN isolada ou para um conjunto de LANs interligadas por *bridges*. Mais ainda, continua a verificar-se afirmativamente no caso de LANs interligadas por *routers*, desde que a função de encaminhamento do XTP esteja instalada em **todos** os *routers*, substituindo a função de encaminhamento do protocolo internet clássico.

Um problema interessante levanta-se quando tentamos fazer com que a parte de transporte do XTP opere sozinha sobre um protocolo internet clássico como o IP ou o CLNP, em vez de operar sobre a sua parte de encaminhamento.

Desde o início da sua concepção, o XTP tem sido desenvolvido na linha do TCP/IP. Isto explica que a interface com a camada DLL inferior seja conseguida exactamente da mesma forma que a interface do TCP/IP com a camada DLL. Deste modo, no caso de LANs Ethernet-DIX, o XTP é instalado directamente sobre o serviço MAC *connectionless* tal como é descrito na figura 4 a). Por outro lado, a figura 4 b) mostra que, nas LANs 802 e FDDI, o XTP assenta no serviço LLC do tipo 1 por meio de um protocolo SNAP. Aqui, o código de tipo para o protocolo XTP é: ox817D (hexadecimal).

2.4 Pressupostos utilizados na análise comparativa

O contexto da análise comparativa dos diversos mecanismos deve ser descrito precisamente, pelo que são apresentados a seguir os pressupostos nos quais essa análise se baseia:

1. *Assume-se uma LAN isolada ou um conjunto de LANs interligadas ao sub-nível MAC por bridges*, para que não seja necessária qualquer interligação no sub-nível internet. Este pressuposto permite-nos focar a nossa atenção na parte de encaminhamento do XTP.

2. *Assume-se que os protocolos TP4 e XTP acedem ao serviço LLC do tipo1:*
- *através de um protocolo SNAP para o XTP,tal como se vê na figura b);*
- *através do subconjunto do protocolo CLNP- Inactive Network Layer Protocol Subset e as funções SNDCFs para o TP4, como está ilustrado na figura 1.*

2.5 Convenções

Nos casos em que não cause confusão, o termo genérico **ligação de transporte** será utilizado para designar qualquer uma das seguintes ligações específicas:
- uma ligação de transporte OSI (TC),
- uma ligação XTP
- uma ligação TCP.

Da mesma forma, o termo genérico **entidade do protocolo de transporte** será utilizado para designar qualquer uma das seguintes entidades protocolares específicas:
- uma entidade de transporte OSI,
- uma entidade XTP,
- uma entidade TCP.

Adicionalmente, o termo **TPDU (Transport Protocol Data Unit),** que é um termo OSI, deve ser utilizado com o standard ISO TP4. No entanto, ao longo do estudo, ele será utilizado também com o TCP, mesmo sendo o TCP um protocolo pre-OSI. Os criadores do XTP

preferiram o termo **pacote** para designar uma PDU que é trocada entre um par de entidades XTP. Assim, utilizar-se-á o termo **TPDU** de uma forma genérica, sendo no entanto substituido por **pacote XTP** sempre que o XTP for discutido.

3. Mecanismos de Gestão da ligação

3.1 Generalidades sobre Gestão da ligação

Todos estes protocolos: TP4, TCP e XTP são protocolos orientados à ligação (*connection oriented*) e, por isso, lidam com transferência de dados sobre ligações de transporte.

Uma ligação de transporte é uma ligação lógica full-duplex. Na vida de cada ligação existem sempre três fases distintas:

1. A fase de estabelecimento da ligação (*connection establishment*),
2. A fase de transmissão de dados através da ligação,
3. A fase de libertação da ligação (*connection release*).

Uma ligação gerida por duas entidades protocolares existe durante o intervalo de tempo em que ambas as entidades mantém informação de estado em relação à comunicação com o parceiro. O termo **informação de estado** refere-se a um registo de características e eventos que estão relacionados com a comunicação entre o par de entidades protocolares. A informação de estado deve ser suficiente, de modo que permita uma transferência de dados fiável sobre a ligação. Não se consegue obter fiabilidade completa sem que se mantenha informação de estado em ambos os terminais da ligação.

Para efectuar a ligação, todos estes protocolos utilizam sinalização *in-band* (**sinalização** significa troca de informação entre o par de entidades protocolares com o objectivo de gerir a ligação). Com a utilização de sinalização *in-band*, a informação de controle e os dados do utilizador são multiplexados na mesma associação. Por isso, as entidades protocolares que efectuam o transporte dos dados do utilizador devem analisar cada PDU recebida para determinar se existe informação de sinalização presente. Este procedimento aumenta a quantidade de processamento necessária a cada PDU de dados normal, o que constitui um comportamento indesejável num ambiente de alta velocidade.

Por outro lado, com sinalização *out-of-band*, a informação de sinalização e os dados do utilizador são transmitidos em associações separadas. No entanto, não se pode transferir dados durante a fase inicial de sinalização.

3.2 Mecanismos de Estabelecimento e Libertação da ligação

A gestão do estabelecimento e libertação da ligação é conseguida através de dois tipos de mecanismos:

- os mecanismos baseados em **handshake**,
- os mecanismos **implícitos** ou controlados por um temporizador **(timer-driven)**

Os esquemas baseados em *handshake* necessitam de uma troca explícita de PDUs entre as entidades protocolares intervenientes na comunicação. Os esquemas implícitos abrem ligações quando a primeira PDU é recebida e fecham essas ligações por controle de um temporizador.

3.2.1 Mecanismo de Estabelecimento da ligação

Os protocolos de transporte orientados à ligação das classes 0 a 3, normalizados pela ISO (TP0 a TP3), assumem que existe um serviço de rede orientado à ligação sobre o qual se apoiam. Este serviço é suposto possuir, pelo menos, uma taxa de erros residual. Esta é a razão pela qual a abertura de uma ligação de transporte (TC) é baseada num *handshake* de duas vias, portanto numa troca de duas TPDUs (i.e. uma TPDU **connection request** e uma outra TPDU **connection confirm**. Este esquema de *handshake* de duas vias tem como objectivo fornecer um serviço de negociação de qualidade na altura do estabelecimento da ligação de transporte (TC).

No entanto, este esquema não é apropriado para o TP4 visto que este assume que as camadas inferiores ou fornecem um serviço de rede orientado à ligação com uma taxa de erros residual inaceitável, ou assume o serviço CLNS, sendo este o caso em análise neste estudo.

3.2.1.1 Mecanismo de Estabelecimento da ligação de transporte no TP4

O mecanismo utilizado no TP4 deriva do mecanismo antes concebido para o TCP. Tal como o TCP, o TP4 assenta num *handshake* clássico de três vias para efectuar a abertura de

uma ligação:

- em primeiro lugar, a entidade **A** envia uma TPDU com um **pedido de abertura de ligação** a uma entidade **B** com quem deseja estabelecer uma ligação,

- em segundo lugar, a entidade **B** responde com uma TPDU de **confirmação** cujo papel é duplo: por um lado, confirma a recepção do pedido de ligação e por outro lado pede a confirmação à entidade **A** que o seu pedido não é um duplicado de um pedido anterior,

- em terceiro lugar, a entidade **A** efectiva o estabelecimento da ligação confirmando (*acknowledge*) a recepção da TPDU de confirmação da entidade **B**.

Quando uma entidade de **sessão** faz um pedido ao fornecedor do serviço de transporte (*TS provider*) para estabelecer uma ligação de transporte (TC) com uma outra entidade, via uma primitiva de pedido de serviço **T-CONNECT**, a entidade de transporte na camada imediatamente abaixo constrói uma TPDU de pedido de ligação (TPDU CR) e envia-a à entidade de transporte do outro lado.

Quando a TPDU CR chega à entidade de transporte remota, esta entidade tem que interactuar com a entidade de sessão remota através de uma primitiva de serviço de indicação **T-CONNECT**. Então, a entidade de sessão remota decide se vai aceitar ou recusar o pedido de estabelecimento de uma ligação de transporte:

- Se a entidade de sessão remota indicar à entidade de transporte remota, através de uma primitiva de resposta **T-CONNECT**, que o estabelecimento de uma ligação de transporte foi aceite, é construida uma TPDU de confirmação de ligação (TPDU CC) e enviada à entidade de transporte que efectuou o pedido. Quando esta TPDU CC for recebida, a entidade de transporte envia uma primitiva de confirmação **T-CONNECT** à entidade de sessão que efectuou o pedido de ligação.

- Se a entidade de sessão remota rejeita o pedido de estabelecimento de uma ligação de transporte, envia uma primitiva de pedido **T-DISCONNECT** à entidade de transporte remota que, por sua vez, constrói e envia uma TPDU de pedido de terminação da ligação (TPDU DR) à entidade de transporte que enviou o pedido. Quando esta TPDU DR for recebida, causa o envio de uma primitiva de indicação **T-DISCONNECT** à entidade de sessão que efectuou o pedido.

No TP4, a entidade de transporte que efectua o pedido considera que a ligação de transporte está aberta logo que a TPDU CC for por si recebida, mas a entidade de transporte remota só o considera no momento em que receber a confirmação de sua TPDU CC. Esta é a razão pela qual o mecanismo de estabelecimento de ligação do TP4 é realmente baseado num *handshake* de três vias, tal como está ilustrado na figura 7.

Como se assume que as entidades de transporte operam sobre um serviço não fiável CLNS, a TPDU CR e a TPDU CC, entre outras, são retidas até que seja recebida uma confirmação (ack) e são retransmitidas no fim do *timeout*.

Se uma entidade de transporte envia uma TPDU CR para pedir o estabelecimento de uma ligação de transporte e se, antes de receber esta TPDU CR, a entidade de transporte remota enviar também um pedido TPDU CR de estabelecimento de uma ligação de transporte entre as mesmas entidades de sessão, então serão eventualmente abertas duas ligações de transporte separadas. Como é evidente, estas duas ligaçoes de transporte possuirão dois pontos de ligação de transporte (TCEPs) distintos em cada ponto de acesso ao serviço de transporte (TSAP).

As entidades de transporte mencionam os endereços TSAPs completos de origem e destino apenas na TPDU CR e possivelmente na TPDU CC. O que realmente acontece é que durante a fase de estabelecimento da ligação de transporte, cada uma das duas entidades de transporte que irá gerir a ligação atribui-lhe um número de referência. Os números de referência são atribuidos independentemente em cada um dos lados da ligação de transporte e são comunicados à outra entidade através de um campo <SRC-REF> no cabeçalho de transporte da TPDU CRe da TPDU CC. Logo que estas duas TPDUs tenham sido trocadas, as duas entidades de transporte que gerem a ligação assinalam essa ligação nas TPDUs por meio do número de referência atribuido pela outra entidade. Deste modo, a atribuição de cada TPDU recebida (excepto a TPDU CR) a uma das ligações de transporte abertas baseia-se no número de referência do destino que é escrito no campo <DST-REF> do cabeçalho de transporte da TPDU.

A identificação de uma ligação de transporte entre uma entidade de transporte e uma entidade de sessão adjacente é efectuada por meio do identificador TCEP. O procedimento de identificação TCEP, que deve ser fornecido na interface do serviço de transporte (TS), que serve para distinguir entre várias ligações de transporte no mesmo ponto de acesso ao serviço de transporte (TSAP), é uma questão local, logo não faz parte das especificações ISO.

3.2.1.2 Diferenças com o mecanismo de Estabelecimento da ligação no TCP

Existem básicamente quatro diferenças significativas entre o mecanismo de estabelecimento de ligação do TP4 e o correspondente no TCP:

1. O TP4 utiliza TPDUs específicas de controle(i.e. a TPDU CR e a TPDU CC) para efectuar a abertura da ligação de transporte ao passo que no TCP só existe um formato de TPDU. Uma TPDU de controle TCP tem exactamente o mesmo formato duma TPDU de dados com a única diferença de não transportar dados do utilizador. A TPDU que efectua o pedido de abertura da ligação no TCP é uma TPDU na qual a flag de sincronização SYN foi colocada a 1 (valor lógico verdadeiro). A TPDU de confirmação gerada em resposta a esta TPDU que efectua o pedido também contém a mesma flag SYN colocada a 1 e contém uma confirmação para a flag SYN presenta na TPDU que efectua o pedido. Finalmente, uma terceira TPDU que contém a confirmação para a flag SYN que está presente na segunda TPDU (de confirmação) é enviada pelo iniciador da ligação.

2. A entidade TCP remota que é chamada não precisa de interactuar com o utilizador remoto após a recepção da primeira TPDU para decidir se aceita ou recusa o pedido de estabelecimento de uma ligação activa. O que se verifica é que o pedido de estabelecimento de uma ligação activa é aceite pela entidade TCP remota apenas se o endereço de destino da primeira TPDU for igual ao endereço de um socket local, e se o endereço de origem desta primeira TPDU for aceite por um pedido de estabelecimento de ligação que está à espera associado ao socket local de destino A interacção entre a entidade TCP remota e o utilizador remoto após a recepção da primeira TPDU não é necessária visto que o utilizador remoto indicou à entidade TCP qual o pedido de estabelecimento de ligação que está disposto a aceitar, porque está, de facto, à escuta desses pedidos.

3. Uma ligação não é referenciada da mesma forma no TP4 e no TCP após o estabelecimento da ligação. No TP4, para referenciar ligações de transporte abertas, utiliza-se números de referência que são trocados entre entidades de transporte comunicantes, enquanto que identificadores TCEP atribuidos localmente são utilizados na interface do serviço de transporte (TS). Contrariamente, o TCP continua a referenciar as ligações abertas

utilizando, em todas as TPDUs trocadas, o endereço completo dos sockets de origem e de destino. Consequentemente, é possível estabelecer várias ligações de transporte entre o mesmo par de TSAPs enquanto que só é permitida uma única ligação TCP entre o mesmo par de sockets.

4. No caso de existirem pedidos de ligação cruzados, o TP4 estabelece ligações de transporte distintas enquanto que o TCP estabelece uma única ligação, já que é impossível estabelecer duas ligações distintas entre o mesmo par de sockets.

3.2.1.3 Comentários ao Estabelecimento da ligação baseado em "handshake"

O esquema de *handshake* de três vias para efectuar a abertura de uma ligação apresenta um incoveniente muito importante nos ambientes das redes locais de alta velocidade. De facto, um protocolo orientado à ligação com um mecanismo de estabelecimento de ligação baseado em *handshake* de três vias desperdiça uma ida-e-volta (RTD-round trip delay) para estabelecer uma ligação.

Tomando o TP4 como exemplo, passa-se um RTD, pelo menos, entre o momento em que a TPDU CR é enviada pela entidade de transporte e o momento em que a correspondente TPDU CC é recebida por esta entidade, atendendo a que estas duas primeiras TPDUs trocadas só são utilizadas para abrir a ligação de transporte e não transportam quaisquer dados.

O RTD gasto meramente no estabelecimentoda ligação de transporte funciona como um travão sobre a realização eficiente de trocas de duas mensagens sobre uma ligação de transporte. Como as duas primeiras TPDUs que são trocadas só são utilizadas para abrir a ligação de transporte e não transportam dados, a TPDU que contém a mensagem de pedido não pode ser enviada antes de um RTD. Por isso, desde o momento em que a primeira TPDU é enviada, demora-se pelo menos dois RTDs (pelo menos o dobro do tempo óptimo) antes que a mensagem de resposta seja recebida.

Para além disso, o RTD gasto apenas para estabelecer a ligação de transporte pode degradar severamente o desempenho de uma transferência de dados unidireccional (por exemplo uma transferência de ficheiros). Numa rede caracterizada por um produto { **Throghput * Round Trip Delay** } elevado, este RTD que é desperdiçado inicialmente pode vir a representar uma parte significativa do tempo total necessário para transmitir todo o bloco

de dados, mesmo no caso de blocos de dados bastante grandes.

Durante este RTD inicial, enquanto a entidade de transporte que efectua o pedido se encontra à espera da confirmação que o pedido de estabelecimento de ligação foi aceite, já poderia ter sido enviada uma quantidade de dados dada pelo produto { **Throghput * Round Trip Delay** }.

Hoje em dia, as redes apresentam para este produto um valor várias ordens de gandeza mais elevado do que as redes existentes na altura em que o TCP e o TP4 foram concebidos. Nas redes locais actuais, o produto { **Throghput * Round Trip Delay** } é igual a um valor da ordem das várias centenas de Kbit. Por exemplo:

10 Mbit/s * 60 ms = 600 Kbit.

Isto explica que nos protocolos de transporte emergentes, a tendência seja óbviamente tentar entrar na fase de transmissão o mais rápidamente possível. Um estabelecimento de ligação rápido permite ao protocolo levar a cabo vários tipos de comunicações mais eficientemente e com latências mais baixas. O mecanismo de estabelecimento de ligação utilizado no XTP ilustra muito bem esta tendência: o XTP assenta num esquema ímplicito para estabelecer a ligação.

3.2.1.4 Mecanismo de Estabelecimento da ligação no XTP

Na especificação do XTP, o registo de informação de estado relacionado com uma ligação XTP num dos seus terminais é designado por **contexto**. Assim, se dois utilizadores implementados em dois sistemas terminais A e B, comunicam por intermédio de uma ligação XTP, a entidade XTP de cada sistema terminal possui um contexto activo para a ligação.

Um pacote XTP é representado recorrendo à seguinte notação: **[B,A,K,R](tipo_de_pacote, flags_opções,campo=valor)**. Neste tipo de representação os símbolos utilizados têm um significado que se descreve a seguir:

B - endereço MAC do sistema B, interpretado como o endereço MAC de destino do pacote na LAN em causa,

A - endereço MAC do sistema A interpretado como o endereço MAC de origem do pacote na LAN em causa,

K - chave utilizada para identificar o contexto,

R - variável de percurso.

A informação colocada entre parêntesis tem o seguinte significado:

* **tipo_do_pacote,**

* **flags_opções** - lista de flags (bits) seleccionadas a partir de um conjunto de opções de comando do cabeçalho XTP que são colocadas a um (valor lógico 1) no pacote,

* **campo=valor** - lista de valores atribuidos aos campos de controle especificados.

A notação parêntesis rectos -[ ]- contém variáveis utilizadas para identificação do pacote, ao passo que a notação parêntesis curvos -( )- descreve o restante do pacote onde apenas as flags e campos relevantes a um dado tópico são especificadas. Este tipo de notação mistura informação de controle relacionada com o XTP com informação de controle relacionada com protocolo MAC. Os endereços MAC de origem e de destino do pacote não são colocados nos campos de controle do XTP. Se considerarmos os pressupostos de que se partiu para o XTP (descritos na secção 2.3), os endereços MAC são colocados nos campos apropriados do cabeçalho (*header*) MAC na altura em que se efectua o encapsulamento do pacote XTP (um SDU - MAC) com um cabeçalho MAC e um apêndice (*trailer*) MAC. Por outro lado, a chave que identifica o contexto (**K**) e a variável de percurso (**R**) são colocadas respectivamente nos campos **<chave>** e **<percurso>** do header XTP. Por último, o **tipo_de_pacote** é colocado no campo **<cmd>** do header XTP.

Como foi afirmado na secção 2, assume-se uma LAN isolada ou um conjunto de LANs interligadas apenas ao nível MAC por *bridges*, de modo que não seja necessária nenhuma função de *relay* internet. A parte de encaminhamento do XTP que deve lidar com o encaminhamento por um percurso ao nível internet pode ser ignorada, de modo que a parte dos mecanismos de transporte XTP possa ser analisada independentemente. A variável de percurso pertence à informação de controle da parte de encaminhamento do XTP. Por isso, a sua função não será ainda analisada (refira-se à seccção 4 para o desenvolvimento deste tópico).

Neste momento, pode-se descrever o mecanismo de estabelecimento de ligação do XTP. Uma ligação XTP é aberta **implicitamente** entre dois utilizadores implementados em dois

sistemas terminais distintos A e B, quando um pacote do tipo **FIRST** (primeiro pacote) é enviado de uma entidade XTP iniciadora da ligação (A) para uma entidade receptora (B). Quando um utilizador no sistema A pede ao fornecedor de serviços XTP para estabelecer uma ligação XTP com um utilizador no sistema B, a entidade XTP em A cria um contexto local activo para a nova ligação, atribui uma chave (KA) a este contexto e transmite um pacote **[B,A,KA,RA](FIRST)** para a entidade XTP remota em B. O segmento de informação deste pacote FIRST (i.e. o segmento intermédio entre o cabeçalho XTP e o respectivo apêndice) é dividido em dois segmentos:

- um **segmento de endereço** que contém informação de endereçamento sobre o utilizador chamado em B e o utilizador emissor em A,

- um **segmento de dados** que pode conter dados do utilizador emissor em A.

Quando um pacote do tipo FIRST, proveniente de A, é recebido em B, deve existir um contexto de escuta local em B para aceitar este pacote recém-chegado. De outro modo, o pedido de estabelecimento de ligação é imediatamente recusado. Assim, uma ligação XTP é estabelecida por transmissão de um pacote FIRST de um contexto activo num terminal para um contexto de escuta correspondente no outro terminal, contexto esse que passa ao estado activo. Na revisão 3.6 do protocolo XTP um utilizador que pede à entidade XTP para criar um contexto de escuta, através de uma operação de escuta, pode elegê-lo para supervisionar o estabelecimento da ligação. Se o utilizador se decidir a supervisionar esse estabelecimento ele mesmo, deve ser notificado pela entidade XTP da chegada de um pacote do tipo FIRST com um endereço de transporte de destino que corresponde ao endereço associado ao contexto de escuta. Neste caso, cabe ao utilizador instruir a entidade XTP para aceitar ou rejeitar o pacote FIRST que chegou entretanto.

Os pacotes enviados de B para A e relacionados com a ligação XTP que foi aberta implicitamente pelo pacote FIRST possuirão todos a seguinte forma: **[A,B,KA',RA']** onde a chave **KA'** representa uma chave de retorno que é idêntica à chave KA excepto no bit mais significativo que é colocado a um em KA'. Assim, durante todo o tempo em que a ligação existir, a entidade XTP em B deve colocar a chave de retorno KA' no campo <chave> de qualquer pacote que envie para A, de modo a referenciar correctamente o contexto de ligação em A.

A entidade XTP em B pode forçar a entidade XTP em A a alterar a chave no campo <chave> dos pacotes enviados para B. Após a recepção do pacote FIRST, a entidade XTP em B pode impôr a utilização da chave de retorno **KB'** na entidade XTP em A, sendo KB a chave

atribuida ao contexto de ligação em B na altura em que este é criado como contexto de escuta. Esta chave pode ser comunicada à entidade XTP em A no campo **<xkey>** (troca de chave) de um pacote de controlo **CNTL**. Logo que este pacote for recebido em A com a forma seguinte: **[A,B,KA',RA'](CNTL, xkey=KB')** , a entidade XTP em A começa a utilizar a chave KB' que irá ser colocada no campo <chave> dos pacotes enviados para B. A partir deste instante, A e B irão utilizar apenas as chaves de retorno nos pacotes relacionados com a ligação XTP estabelecida: A coloca a chave de retorno KB' no campo <chve> do pacote que enviar para B enquanto que B coloca a chave de retorno KA' nos pacotes enviados para A.

A entidade XTP em A não tem forma de saber se a ligação XTP foi estabelecida com sucesso até que receba um pacote de B relacionada com essa ligação. Em cicunstâncias normais, cabe à entidade XTP que procede ao envio do pacote a determinação da política de confirmação. Significa isto que normalmente a entidade XTP em B irá enviar um pacote CNTL **se e só se** a entidade XTP em A pedir por esse envio quando coloca a 1 a flag **SREQ** ou a fag **DREQ** no cabeçalho XTP do pacote transmitido para B.

Se o estabelecimento da ligação falhar, a notoficação da falha enviada ao iniciador da ligação em A corresponde ao envio de um pacote de diagnóstico do tipo **DIAG** que indica a razão da falha que pode ser:

- contexto inválido,
- contexto recusado,
- destino desconhecido

entre outras.

As figuras 6,7 e 8 ilustram o mecanismo de estabelecimento de ligação do XTP. A figura 6 demosntra que uma ligação XTP é estabelecida como efeito da recepção de um pacote FIRST. A figura 7 revela que a flag SREQ deve ser colocada a 1 no pacote FIRST para pedir o envio de um pacote CNTL por parte de B como resposta ao seu pacote FIRST. A figura 7 demosntra ainda que os dados podem ser enviados em pacotes do tipo **DATA** antes da recepção de qualquer pacote de resposta (no caso um pacote CNTL). Se o pacote FIRST é perdido ou destruido, estes pacotes de dados devem ser retransmitidos. A figura 8 ilustra a forma como um pacote DIAG é enviado se o pacote FIRST for rejeitado em B. Este pacote DIAG tem a forma **[A,B,KA',RA'](DIAG, código=1 para contexto inválido)** se não for encontrado um contexto de escuta correspondente ao pedido em B, e toma a forma **(A,B,KA',RA'](DIAG, código=2 para contexto recusado)** se a razão da recusa do pacote FIRST for de outro género. Quando o pacote FIRST é rejeitado, os pacotes de dados enviados

atrás do pacote FIRST são simplesmente ignorados em B.

No que respeita ao procedimento de troca da chave de contexto, a entidade XTP em A comunica a sua chave de contexto KA no pacote FIRST, ao passo que, mais tarde, a entidade XTP em B comunica a sua chave de contexto KB num pacote CNTL por meio de um procedimento de troca de chaves. As duas chaves de contexto que são trocadas no XTP possuem a mesma função que os dois números de referência que são trocados através da CR TPDU e da CC TPDU no TP4. As chaves de contexto não são nada mais que números de referência atribuidos às ligações XTP por entidades XTP. Após a troca de chaves numa ligação XTP, cada uma das entidades que gerem a ligação colocam a chave de retorno (i.e a chave que foi atribuida pela entidade XTP remota) no campo <chave> dos pacotes enviados, exactamente da mesma forma que duas entidades de transporte que gerem uma ligação de transporte (TC) no TP4 se referem a esta TC no campo <DST-REF> das TPDUs enviadas por meio do número de referência que foi atribuido pela entidadede transporte remota. A maior diferença é que, como o XTP utiliza um mecanismo de estabelecimento de ligação rápido, os pacotes do tipo DATA podem ser transmitidos pela entidade XTP em A antes da troca de chaves. Por isso, a entidade XTP em A não tem outra alternativa senão escrever a sua própria chave KA no campo <chave> dos pacotes enviados até à altura em que ocorre a troca de chaves, ficando então obrigada a utilizar a chave KB'.

A utilização de chaves de retorno é um truque que permite à entidade XTP identificar prontamente, nos pacotes recebidos, as chaves atribuidas por si e as chaves atribuidas pela outra entidade. Claro está que não basta à entidade XTP em A colocar a chave KA no campo <chave> dos pacotes enviados para B de forma a identificar correctamente o contexto de ligação adequado em B, pois a entidade XTP em B poderia receber vários pacotes FIRST com a mesma chave KA.

Se a entidade XTP em A envia um pacote **[B,A,KA,RA](FIRST, SREQ)** à entidade XTP em B de modo a estabelecer uma ligação entre um utilizador A e um utilizador B e se, antes da recepção deste pacote FIRST a entidade XTP em B transmitir um pacote **[B,A,KB;RB](FIRST, SREQ)** de modo a estabelecer uma ligação XTP entre o mesmo par de utilizadores, irão ser estabelecidas implicitamente duas ligações distintas .

Quando um pacote FIRST recebido contém no seu subsegmento de endereço um endereço de transporte de destinoque corresponde ao endereço de um ponto de acesso local válido ao serviço fornecido pelo XTP e quando este pacote FIRST encontra um contexto de escuta correspondente a este ponto de acesso, a entidade XTP receptora cria uma associação entre o tuplo **(id_origem, chave, percurso)** e o contexto de escuta. A seguir, o contexto de escuta transita para um estado activo. No tuplo, o **id_origem** é um identificador de baixo nível que identifica a última entidade XTP que transmitiu um pacote, por isso normalmente utiliza-

se o endereço MAC da origem. Os restantes **chave** e **percurso** são a chave de contexto e a variável de percurso contidas respectivamente nos campos <chave> e <percurso> do pacote FIRST. **Chave** é um valor seleccionado pela entidade XTP que originou o pacote e **percurso** é um valor seleccionado pala última entidade XTP que transmitiu um pacote, que também é a entidade XTP que originou o pacote se considerarmos o caso de uma LAN isolada ou um conjunto de LANs interligadas apenas por *bridges*. Sempre que um pacote de uqalquer tipo excepto FIRST chegar, a entidade XTP examina a chave que ele contém. Se a chave for uma chave de retorno o contexto de ligação local apropriado pode ser localizado muito rápidamente mediante a utilização desta chave de retorno. Isto acontece porque a entidade XTP de cada sistema terminal nunca pode atribuir a mesma chave a contextos de ligação locais distintos, mesmo que estes contextos locais se relacionem com ligações XTP que são estabelecidas com entidades XTP diferentes. A utilização da chave de retorno permite uma localização rápida e directa do contexto de ligação local correcto. Por outro lado, se a chave contida no pacote recebido não for uma chave de retorno (pacote recebido antes da troca de chaves), então a entidade XTP necessita de comparar o tuplo completo que construiu a partir deste pacote com os tuplos associados com os contextos locais activos de modo a localizar correctamente o contexto de ligação local.

Um processo de localização do contexto de ligação correcto que seja rápido é um factor muito importante para atingir os objectivos de desempenho. Isto explica a razão pela qual a troca de chaves deve ser efectuada o mais cedo possível sempre que for necessária.

3.2.2 Mecanismos de Libertação da ligação

Como foi mencionado na secção 3.1, uma ligação de transporte é uma ligação lógica full-duplex. Por isso, associados com cada ligação full-duplex existem dois fluxos (*streams)* simplex entre as duas entidades protocolares de transporte que gerem a ligação. Um **fluxo simplex** consiste de um fluxo simplex de dados (para dados do utilizador) em paralelo com um fluxo simplex de controle (para informação de controle). No caso de sinalização *in-band*, os dois fluxos simplex de dados relacionados com a ligação de transporte full-duplex e os dois fluxos simplex de controle correspondentes são multiplexados na mesma associação. A informação de controle transferida num fluxo de controle diz respeito ao fluxo de dados do mesmo **fluxo simplex** ou ao fluxo de dados do **fluxo simplex inverso** relacionado com a mesma ligação.

A filosofia da libertação da ligação é bastante diferente no TP4 e no XTP.

No TP4, os dois fluxos de dados simplex relacionados com uma ligação de transporte (TC) são sempre libertados simultâneamente. O TP4 liberta a TC incondicionalmente e abruptamentepor meio de um mecanismo baseado num *handshake* de duas vias.

O esquema básico de término de ligação do XTP foi inspirado no esquema utilizado no TCP. Os dois fluxos de dados simplex relacionados com uma ligação XTP podem ser libertados separadamente e graciosamente, cada um através de um *handshake* de duas vias. Adicionalmente, o XTP pode libertar um fluxo de dados simplex graciosamente e o inverso abruptamente, ou pode libertar ambos os fluxos de dados simplex abruptamente.

3.2.2.1 Mecanismos de Libertação da ligação no TP4

Os dois fluxos de dados simplex relacionados com uma ligação de transporte (TC) full-duplex nunca podem ser libertados separadamente. Quando uma entidade de sessão de um dos lados da TC decide libertar esta TC, a entidade de sessão do outro lado deve aceitar o término da ligação imediatamente. A libertação da TC é **incondicional** porque é permitida em qualquer altura, independentemente da fase actual da TC: um pedido de libertação **não** pode ser rejeitado. Para além disso, a libertação da TC é possivelmente destrutiva porque a entrega fiável de dados que ainda está a decorrer nos dois fluxos de dados simplex deixa automáticamente de ser assegurada uma vez que o procedimento de libertação da TC foi despoletado por uma das duas entidades de sessão que comunicam entre si.

A figura 9 ilustra o mecanismo baseado num *handshake* de duas vias que é utilizado pelo TP4 para libertar a TC.

Quando uma entidade de sessão pede o término de uma ligação de transporte(TC) ao fornecedor de serviços de transporte através de uma primitiva de serviço de pedido T-DISCONNECT, a entidade de transporte abaixo constrói uma TPDU de pedido de libertação (**TPDU DR**) e envia-a imediatamente à entidade remota. A partir deste momento, todas as TPDUs que não sejam uma TPDU DR ou uma TPDU de confirmação de libertação (**TPDU DC**) são rejeitadas pela entidade de transporte.

Quando uma TPDU DRchega à entidade de transporte, esta entidade responde com uma TPDU DC para confirmar a TPDU DR e envia uma indicação do tipo primitiva T-DISCONNECT à sua entidade de sessão. Logo que a TPDU DC for enviada, a TC considera-se libertada e a informação de estado é destruida deste lado da ligação.

Quando a TPDU DC for recebida, a TC também se considera libertada e a informação de estado é também destruida daquele segundo lado da ligação. Se for necessário, a TPDU DRé

retransmitida no fim do *timeout*.

Se uma entidade de transporte que enviou uma TPDU DR para libertar uma TC receber uma TPDU DR relacionada com a mesma TC proveniente da entidade de transporte com quem comunica, então a TC é considerada libertada e a informação de estado é destruida sem ser necessário esperar por uma TPDU DC.

3.2.2.2 Mecanismos de Libertação da ligação no TCP

Como já se referiu, existe apenas um formato de TPDU no TCP. A mesma informação de controle é colocada em todos os cabeçalhos de todas as TPDUs (as que contém dados e as que não contém dados). Por isso, ao contrário do TP4, o TCP não recorre a TPDUs específicas de controle para libertar uma ligação.

No TCP, também existe um esquema incondicional de libertação da ligação e que também é possivelmente destrutivo. Os dois fluxos de dados simplex relacionados com uma ligação TCP são libertados simultâneamente e abruptamente mediante o envio de uma única TPDU na qual a flag RST (ReSeT) é colocada a 1. Esta TPDU não necessita de ser confirmada como no caso correspondente no TP4.

No entanto, o esquema de libertação da ligação mais utilizado no TCP é um esquema de libertação gracioso. Os dois fluxos de dados simplex relacionados com uma ligação TCP podem ser libertados separadamente e graciosamente. A libertação graciosa de um fluxo de dados simplex implica que todos os dados ainda em trânsito neste fluxo de dados sejam correctamente entregues antes do término da ligação.

Quando uma entidade TCP deseja libertar graciosamente um fluxo de dados simplex que é utilizado para transmitir dados para a outra entidade, coloca a flag FIN a 1 na próxima TPDU que irá enviar e que contém os últimos dados a ser transmitidos. Após algumas possíveis retransmissões (se necessárias), a libertação graciosa deste fluxo de dados de saida é confirmada por meio de uma confirmação (ACK) à flag FIN. A libertação graciosa de um fluxo de dados simplex é, por isso, baseada num *handshake* de duas vias. Este esquema de duas vias pode no entanto ser reduzido a um único *handshake* de três vias se os dois fluxos de dados forem libertados simultâneamente. Para isso, a TPDU que contém a confirmação para a primeira flag FIN pode conter também a sua flag FIN colocada a 1.

3.2.2.3 Mecanismos de Libertação da ligação no XTP

O mecanismo de libertação da ligação utilizado pelo XTP é ainda mais rico do que o do TCP. Permite que os dois fluxos de dados simplex relacionados com uma ligação XTP full-duplex sejam libertados separadamente. No entanto, permite também uma libertação graciosa bem como uma libertação abrupta de fluxos de dados simplex.

Existem três flags do cabeçalho XTP que estão envolvidas no mecanismo de libertação: as flags **END, WCLOSE** e **RCLOSE.** Todos os pacotes XTP possuem os mesmos formatos de cabeçalho e apêndice independentemente do seu tipo. Isto permite uma rápida descodificação do seu conteúdo. Assim, as três flags estão presentes no cabeçalho XTP de cada pacote seja qual for o seu tipo. Isto implica que no XTP pode-se utilizar pacotes diferentes para libertar um ou ambos os fluxos de dados simplex relacionadso com uma ligação de transporte, ao contrário do TP4 que possui TPDUs de controle específicas (a TPDU DR e a TPDU DC) para o mesmo efeito.

Quando a flag **WCLOSE** é colocada a 1 num pacote XTP, significa que a entidade XTP que enviou o pacote **deseja libertar o seu fluxo de escrita de dados** (ou o fluxo de saida). Quando a flag **RCLOSE** é colocada a 1 num pacote XTP, isso significa que a entidade que o enviou **já libertou o seu fluxo de leitura de dados** (ou fluxo de entrada de dados) e não aceitará mais dados nesse fluxo de dados. Por último, quando a flag **END** é colocada a 1 num pacote XTP, significa que o contexto de ligação na entidade que enviou esse pacote **está a ser libertado**, eliminando qualquer possibilidade de prosseguir com a comunicação.

A libertação graciosa de um fluxo de dados simplex ocorre quando todos os dados estipulados para um determinado fluxo de dados foram correctamente enviados pela entidade XTP que transmite no fluxo de dados e correctamente entregues pela entidade XTP remota ao respectivo utilizador. A entrega fiável de todos os dados em trânsito neste fluxo de dados implica que a entidade XTP receptora, ao detectar uma flag WCLOSE colocada a 1 num pacote que recebeu, tenha oportunidade de pedir retransmissão se necessário antes de colocar a flag RCLOSE a 1 num pacote que envie na mesma ligação XTP.

Desta forma, cada fluxo de dados simplex relacionada com uma ligação XTP pode ser libertado graciosamente e independentemente do fluxo inverso por meio de um esquema de *handshake* de duas vias. Para libertar graciosamente o fluxo de dados simplex estabelecido de A para B, a entidade XTP de A começa por colocar a flag WCLOSE a 1 no último pacote que enviar para B. De seguida, quando todos os dados destinados ao utilizador B forem correctamente entregues, a entidade XTP em B responde à entidade XTP em A com um pacote cuja flag RCLOSE é colocada a 1. Se existirem erros de transmissão, a entidade XTP

em A deve retransmitir os dados que não foram recebidos por B, até que a entidade XTP em B responda com um pacote no qual a flag RCLOSE esteja a 1. Um segundo esquema *handshake* de duas vias é necessário mais tarde para libertar graciosamente o fluxo simplex inverso de B para A.

Como se pode verificar na figura 10, devem ser trocados dois pacotes com flags especiais colocadas a 1 entre as duas entidades XTP comunicantes para libertar cada fluxo de dados simplex relacionado com uma ligação XTP: um pacote **(WCLOSE + SREQ)** que é confirmado por um pacote **(CNTL, RCLOSE)** para libertar o primeiro fluxo de dados, e um pacote **(WCLOSE+RCLOSE+SREQ)** confirmado por um pacote **(CNTL, WCLOSE+RCLOSE+END)** para libertar o fluxo de dados simplex inverso. A flag END significa que o contexto de ligação na entidade XTP emissora foi libertado. Normalmente, uma entidade protocolar XTP não se pode desfazer do seu contexto de ligação local até que envie ou receba a flag END.

O esquema gracioso que envolve dois *handshakes* de duas vias, como se pode apreciar na figura 10, pode ser reduzido a um esquema gracioso que envolve um único *handshake* de três vias como se descreve na figura 11, se os dois fluxos de dados simplex forem libertados simultâneamente.

Para além destes esquemas graciosos o XTP permite o término forçado de um ou ambos os fluxos de dados simplex relacionados com uma dada ligação XTP. A libertação forçada de um fluxo de dados implica que a entrega fiável de dados ainda em trânsito deixa de ser garantida a partir deste instante.

Uma libertação forçada deste género pode ocorrer quando um dos seguintes eventos ocorrer:

1] Uma entidade XTP detecta uma flag RCLOSE com valor 1 num pacote recebido antes de ter enviado um pacote com a flag WCLOSE colocada a 1. Esta sequência impede que a entidade XTP transmita mais dados no seu fluxo de escrita da dados. Assim, uma entidade XTP pode libertar o seu fluxo de leitura de dados abruptamente colocando a flag RCLOSE a 1 num pacote que envie sem necessitar de esperar pela recepção de um pacote onde a falg WCLOSE estivesse a 1,

2] Uma entidade XTP recebe um pacote com a flag END colocada a 1 embora este pacote não seja o último de um esquema gracioso basedado num *handshake* de duas vias nem o último de um esquema gracioso baseado num único *handshake* de três vias. De facto, a flag END suprime toda e qualquer possibilidade de comunicações posteriores,

3] Uma entidade XTP recebe um pacote **(DIAG, código=contexo inválido)**. Esta mensagem indica que o contexto de ligação da entidade XTP remota deixou de existir.

Como exemplo, a figura 12 mostra um esquema específico de libertação da ligação baseado num único *handshake* de duas vias. Dado que o fluxo de dados simplex, orientado de A para B é libertado graciosamente, ao passo que o fluxo inverso é libertado abruptamente (devido à flag END), este esquema é indicado para uma transmissão fiável de uma mensagem.

Note-se que a libertação de um fluxo de dados simplex não provoca a libertação do correspondente fluxo de controle simplex. De facto, como um fluxo de controle simplex consiste de informação de controle que diz respeito ao fluxo de dados do mesmo fluxo simplex e do fluxo simplex inverso relacionado com a mesma ligação XTP, os dois fluxos de controle simplex ainda são necessários, mesmo que apenas um dos dois fluxos de dados simplex ainda se mantenha aberto.

No XTP, considera-se que os fluxos de controle de entrada e saida são libertados simultâneamente de uma forma implícita por uma entidade XTP quando esta envia ou recebe uma flag END, i.e. quando destrói o seu contexto de ligação local.

Se estabelecermos um paralelo entre os mecanismos de libertação da ligação no TCP e no XTP, concluimos que a flag WCLOSE do XTP corresponde à flag FIN do TCP. A flag RCLOSE do XTP é equivalente à confirmação da flag FIN no TCP apenas quando esta flag RCLOSE age como confirmação de um pedido WCLOSE prévio. Para além disto, a flag END do XTP é equivalente à flag RST do TCP. Por outro lado, o TCP não possui equivalente para a flag RCLOSE quando esta flag é utilizada noutras circusntâncias que não para confirmar um pedido WCLOSE prévio.

3.3 Conclusões do estudo dos mecanismos de Gestão da ligação

O desenvolvimento dos protocolos TCP e TP4 começou há mais de uma década, baseado nas características das infraestruturas de comunicação e nas aplicações existentes nessa altura. A concepção de protocolos de transporte contemporâneos deveria ser fortemente influenciada pela enorme evolução tecnológica nas comunicações através de redes, bem como pelo alargamento das necessidades das aplicações que ocorreu desde então.

O emergente XTP representa uma abordagem interessante à concepção de protocolos para a geração presente e para a próxima geração de redes. A vontade de conceber o XTP

como um protocolo adaptado às vovas infraestruturas de comunicação e às novas aplicações è notória se examinarmos com atenção os seus mecanismos de gestão da ligação.

Para conseguir que o XTP seja um protocolo melhor adaptado às novas aplicações, os seus autores concentraram esforços significativos num mecanismo implícito de estabelecimento de ligação. Este mecanismo permita ao XTP uma realização eficiente de trocas genéricas de duas mensagens em ligações XTP de curta duração.

Para o tornar ainda mais eficiente, a realização deste tipo de trocas exige um mecanismo de libertação da ligação que não necessite de PDUs específicas de controle para libertar a ligação logo que a troca de dados esteja completa. Além disso, a libertação da ligação na qual a troca dessas mensagens decorre exige um esquema gracioso de libertação de ambos os fluxos de dados simplex relacionados com a ligação, enquanto que a libertação de uma ligação na qual decorre uma transmissão não fiável de apenas uma mensagem exige idealmente a libertação graciosa de um dos dois fluxos de dados, podendo ser a libertação do fluxo inverso do tipo abrupto. O mecanismo de libertação da ligação do XTP possui as propriedades que respondem a estas necessidades. Em contraste, o TP4 utiliza sempre duas TPDUs específicas de controle para libertar uma ligação de transporte (TC).

O intervalo de tempo que decorre desde o início de uma troca genérica de duas mensagens e a recepção da mensagem resposta é certamente tão importante como o número de pacotes trocados. No XTP, este intervalo de tempo ronda um RTD (Roud Trip Delay). Claramente, o XTP está melhor adaptado às trocas genéricas de duas mensagens do que o TP4 que constitui o pior dos três protocolos analisados.

Adicionalmente, o XTP é apropriado para transmitir datagramas. Estes podem ser vistos como o envio de pacotes do tipo FIRST com a flag END colocada a 1.

O mecanismo implícito de estabelecimento de ligação do XTP também vai de encontro ao objectivo de o tornar num protocolo melhor adaptado que o TP4 e o TCP aos requisitos impostos pela elevada largura de banda com baixa taxa de erros. O mecanismo implícito pode conduzir a um melhoramento significativode desempenho de uma transferência de dados unidireccional, tal como uma transferência de ficheiros, porque não desperdiça um RTD inicial apenas para abrir a ligação.

No entanto, um mecanismo implícito de estabelecimento de ligação no protocolo seria inútil se não existisse o suporte apropriado na especificação do serviço fornecido. Embora o servoço a ser fornecido pelo XTP não esteja ainda definido, pode-se antecipar que será bastante diferente do standard ISO modo de ligação TS (Serviço de transporte). De facto, à primeira vista parece que o serviço a fornecer acima do XTP deve possuir características particulares que explorem ao máximo os melhoramentos potenciais desencadeados nos mecanismos de gestão de ligação do XTP.

4. Mecanismos de Transferência de dados

4.1 Classificação dos principais mecanismos de Transporte

Tanto o TP4 como o TCP e o XTP são protocolos orientados à ligação. Os principais mecanismos de transporte utilizados nas LANs durante a fase de transferência de dados numa ligação podem classificar-se em cinco categorias principais enumeradas nas próximas secções:

1 - Mecanismos de mapeamento de Unidades de dados,
2 - Mecanismos de controle de erro,
3 - Mecanismos de controle de fluxo de extremo-a-extremo (*end-to-end*),
4 - Mecanismos de controle de congestionamento,
5 - Mecanismo "Multicast".

4.1.1 Mecanismos de mapeamento de Unidades de dados

As entidades protocolares de transporte comunicam com o seu par mediante uma troca de TPDUs. Estas TPDUs são mapeadas **em** NSDUs (Unidades de dados do Serviço de Rede) do lado da entidade emissora e são mapeadas a **partir de** NSDUs do lado da entidade receptora. São possíveis vários mecanismos distintos de mapeamento entre as TPDUs e as NSDUs na **interface do serviço de rede**.

As TPDUs que transportam dados do utilizador são mapeadas **a partir de** TSDUs (Unidades de dados do Serviço de Transporte) do lado da entidade emissora e são mapeadas **em** TSDUs do lado da entidade receptora. Também aqui são possíveis vários mecanismos distintos de mapeamento entre TPDUs e NSDUs na **interface do serviço de transporte**.

4.1.2 Mecanismos de Controle de erro

Considerando que um protocolo de transporte orientado à ligação tem como objectivo assegurar a transmissão fiável de dados com controle de extremo-a-extremo, as entidades protocolares de trasnporte devem implementar mecanismos de controle de erros para detectar e recuperar de erros que possam ocorrer durante a troca de TPDUs.

4.1.3 Mecanismos de Controle de fluxo de extremo-a-extremo

Um mecanismo de controle de fluxo de extremo-a-extremo ao nível de transporte é aquele que permite a uma entidade protocolar de transporte receptora controlar o fluxo de chegada de dados por cada ligação de transporte a ela associada, actuando nas entidades protocolares de transporte emissoras.

4.1.4 Mecanismos de Controle de congestionamento

Se duas LANs forem interligadas através de um *router* e se este fôr o único elemento de junção entre as duas LANs, os pacotes de rede que transportam as TPDUs relacionadas com as múltiplas ligações de transporte estabelecidas entre os diversos sistemas terminais associados a ambas as LANs terão que atravessar o *router*. Assim, torna-se possível que uma situação de estrangulamento ocorra no *router*, ao passo que cada entidade protocolar de transporte receptora é perfeitamente capaz de suportar a taxa de transmissão imposta pela entidade emissora.

Ao contrário co controle de fluxo de extremo-a-extremo no nível de transporte que é uma função de prevenção da chegada de dados que não tém espaço disponível na entidade receptora, o controle de congestionamento é uma função que combate o congestionamento interno ao serviço de rede. Esta função, que diz respeito às camadas de rede e de transporte, pode ser fornecida numa das duas camadas ou não ser fornecida em nenhuma, dependendo das famílias de protocolos utilizadas.

4.1.5 Mecanismo de Multidifusão

Nas LANs, os mecanismos de difusão (*broadcast*) e multidifusão (*multicast)* são disponibilizados pelos vários serviços sem ligação MAC e pelo serviço sem ligação LLC do tipo 1. Tanto um como o outro estão a ser desenvolvidos também ao nível internet, pelo que será de prever a sua extensão para cima até ao nível de transporte.

4.2 Mecanismos de mapeamento de Unidades de dados

Parte-se do princípio que o protocolo de transferência XTP tem acesso directo ao serviço LLC do tipo 1 através do protocolo SNAP. Os conceitos de Serviço de Rede e particularmente

de NSDU são, por isso, descabidos neste contexto. As SDUs (Unidades de Dados de Serviço), de e para as quais são mapeados os pacotes XTP (ou seja as PDUs-XTP), são directamente as LSDUs (Unidades de Dados do Serviço de Controle de Ligação Lógica).

Por sua vez no TP4, o conceito de NSDU também é descabido visto que o TP4 assenta no serviço CLNS (ISO) no contexto OSI escolhido para os ambientes LAN.

Nesta secção investiga-se os mecanismos de mapeamento de Unidades de Dados a dois níveis:

1 - mecanismos de mapeamento entre TPDUs e TSDUs,

2- mecanismos de mapeamento entre TPDus e SDUs (NSDUs para o TP4 e LSDUs para o XTP).

O procedimento normal de mapeamento entre as SDUs e as PDUs, tal como está definido no modelo de referência OSI da ISO, é de um para um. Estão definidos ainda três procedimentos de mapeamento especiais no mesmo modelo de referência. Este procedimentos serão analisados com detalhe nas secções seguintes:

- procedimentos de segmentação/reconstrução,
- procedimentos de agregação/desagregação em blocos,
- procedimentos de concatenação/separação.

4.2.1 Mecanismo de Segmentação/Reconstrução - delimitação da mensagem

Nas LANs, está sempre estipulado um tamanho máximo para as LSDUs. Por outro lado, geralmente não existe limite superior para o tamanho máximo das TSDUs. Por isso, os protocolos de transporte e internet devem possuir um mecanismo que evite apresentar LSDUs com um tamanho superior ao máximo autorizado pelo fornecedor de serviços LLC.

o TP4 implementa um mecanismo de segmentação/reconstrução obrigatório porque não existe limite para o tamanho máximo das TSDUs e porque na subcamada internet nem sempre se encontra um mecanismo deste género. Na realidade, os dois subconjuntos do CLNP não efectuam a segmentação/reconstrução das NSDUs.

No XTP, a situação é mais complexa porque não está explicitamente definido nenhum mecanismo deste tipo para a parte de transporte, embora esta parte possua um mecanismo cujo objectivo é o de preservar os limites de uma mensagem do utilizador.

4.2.1.1 Mecanismo de Segmentação/Reconstrução no TP4

Na especificação standar da ISO para o Serviço de Transporte, não existe limite para o tamanho máximo das TSDUs normais. Pelo contrário, o tamanho máximo das TSDUs relacionadas com uma dada TC é negociado durante a fase de estabelecimento da TC. Assim, mesmo que o tamanho das TPDUs não seja limitado à priori pelo protocolo de transporte, ele pode ser limitado porque o fornecedor de serviços de rede impõe um limite máximo ao tamanho das NSDUs. Por isso, sempre que uma TSDU fôr muito grande para caber numa única TPDU DT (TPDU de dados), a TSDU é segmentada em unidades mais pequenas.

No cabeçalho de transporte da última TPDU DT uma sequência de TPDUs DT provenientes da segmentação da mesma TSDU, o bit EOT (fim de transmissão) é colocada a 1 para assinalar o fim da TSDU. A entidade de transporte receptora pode assim reconstruir a TSDU antes de a entregar à entidade de sessão receptora.

4.2.1.2 Mecanismo de Segmentação/Reconstrução no TCP

Uma entidade TCP pode pedir a outra entidade TCP com quem estabeleceu uma ligação de transporte para enviar apenas TPDUs com um tamanho menor ou igual a um determinado valor. No caso contrário, o tamanho máximo das TPDUs relacionadas com uma dada ligação TCP é de 64 Kbytes. A segmentação numa entidade TCP ocorre apenas para mensagens do utilizador que são maiores do que o tamanho máximo de uma única TPDU. A fragmentação necessária para enviar dados do utilizador em pacotes de rede é efectuada pelo IP.

4.2.1.3 Mecanismo de Segmentação/Reconstrução no XTP

Não existe ainda uma definição de serviço para o XTP. Consequentemente, as unidades de dados que vão ser submentidas ao fornecedor de serviços do XTP ainda não forma muito bem definidas. No entanto, de acordo com a especificação actual, o XTP pode manusear mensagens do utilizador que constituem blocos de bytes bem delimitados que podem ser vistos como TSDUs.

Os dados do utilizador que são submentidos ao fornecedor de serviços XTP para transmissão, são enviados em subsegmentos de dados. Apenas o pacote FIRST e de seguida os pacotes DATA contém subsegementos de dados no seu subsegmento de informação. O procedimento de mapeamento entre mensagens do utilizador e os subsegementos de dados

dos referidos pacotes também não foi ainda especificado. No entanto, prevê-se que uma mensagem do utilizador submentida ao fornecedor de serviços XTP poderá ser colocada pela entidade XTP emissora no subsegmento de dados de um único pacote ou pode ser dividida e colocada em subsegmentos de dados de vários pacotes consecutivos, o que corresponde a um procedimento de segmentação.

De qualquer maneira, o XTP fornece um mecanismo que preserva os limites da mensagem do utilizador. A flag EOM (fim da mensagem) que pode ser colocada a 1 no cabeçalho XTP de qualquer pacote, assinala o fim da mensagem num dado fluxo. Esta flag é análoga ao bit EOT do TP4. Graças a esta flag, a mensagem do utilizador que é enviada em vários pacotes consecutivos pode ser reconstruida na recepção.

4.2.2 Mecanismos de Agregação/Desagregação em blocos e Concatenação/ Separação

Os mecanismos deste género são utilizados para poupar largura de banda. Quando se agrupam várias SDUs de nível N numa PDU de nível N, a entidade do nível N reduz o número de encapsulamentos necessários na camada N. Assim, quando o agregação/desagregação em blocos é efectuado por entidades do nível N, o número de PDUs do nível N a processar, equivalente ao número de SDUs de nível (N-1) a submeter ao fornecedor de serviços do nível (N-1), diminui. No entanto, o tempo de processamento gasto em cada PDU do nível N aumenta.

Concatenando várias PDUs de nível N numa única SDU de nível (N-1), uma entidade de nível N diminui o número de SDUs de nível (N-1) a processar pelo fornecedor de serviços do nível (N-1), apesar de não diminuir o número de PDUs de nível N a processar. No entanto, o tempo de processamento por cada SDU de nível (N-1) aumenta quando a concatenação/ separação é executada pelas entidades do nível N.

4.2.2.1 Mecanismos de Agregação/Desagregação em blocos e Concatenação/ Separação no TP4

Este tipo de mecanismos não existe no TP4. Por isso, os dados provenientes de várias TSDus consecutivas relacionadas com a mesma TC não podem ser agrupados numa única TPDU.

Uma entidade de transporte pode cocatenar várias TPDUs numa única NSDU. Esta

concatenação de TPDUs pode estar relacionada com a mesma TC ou con TCs diferentes, mantendo no entanto a ordem das TPDUs para uma dada TC. A especificação do TP4 impõe algumas condições à concatenação válida de TPDUs. Uma entidade de transporte receptora deve aceitar qualquer conjunto válido de TPDUs concatenadas que, posteriormente, separa e processa ordenadamente.

4.2.2.2 Mecanismos de Agregação/Desagregação em blocos e Concatenação/ Separação no TCP

Ao contrário do TP4, o TCP não possui qualquer mecanismo de concatenação/separação. Por isso, uma entidade TCP não pode agrupar várias TPDUs num único pacote IP. No entanto, uma entidade TCP pode decidir-se a não enviar imediatamente a mensagem que lhe é submetida pelo utilizador. Na realidade, uma entidade TCP pode considerar que a quantidade de dados à espera de transmissão numa dada ligação TCP não é suficiente para justificar o envio de uma nova TPDU de dados. Por isso, os dados de uma determinada mensagem podem ser combinados com dados de mensagens subsequentes relacionadas com a mesma ligação TCP. Esta possibilidade apresenta semlhanças com o mecanismo de agregação em blocos OSI.

4.2.2.3 Mecanismos de Agregação/Desagregação em blocos e Concatenação/ Separação no XTP

O XTP não possui nenhum destes dois mecanismos. Na realidade, estes mecanismos vão no sentido oposto à evolução no sentido de redes de alta e muito alta velocidade porque os objectivos a atingir com a utilização destes mecanismos pretendem a otpimização da largura de banda disponível em detrimento dos atrasos na camada onde estão implementados, ao passo que a tendência nas HSLANs onde existe por natureza uma elevada largura de banda (em fibra óptica até 100Mbit/s no sentido de atingir a ordem dos gigabit/s) é tentar diminuir os atrasos. Isto explica a razão pela qual a maior parte dos novos protocolos, em particular o XTP, não fornece estes dois mecanismos.

4.3 Mecanismos de Controle de erro

Geralmente, os erros que afectam a troca de TPDUs entre entidades protocolares de transporte que operam sobre um serviço sem ligação são os seguintes:

- TPDUs corrompidas
- TPDUs perdidas
- TPDUs duplicadas
- chegada desordenada de TPDUs .

A detecção e correcção de erros nos protocolos aqui estudados só se aplica nos seguintes casos:

- às TPDUs DT no TP4,
- aos TPDUs de dados no TCP,
- aos pacotes do tipo FIRST no XTP.

4.3.1 Mecanismos de detecção de TPDUs corrompidas

O mecanismo utilizado pelos três protocolos para a detecção de TPDUs ou pacotes XTP corrompidas é uma soma de verificação - *checksum*. Ao nível de transporte, esta soma tem o objectivo de proporcionar uma verificação de integridade de extremo-a-extremo.

Quando o cálculo da *checksum* é incorrecto, a entidade de transporte receptora destrói os pacotes recebidos. Isto é aceitável se considerarmos as baixas taxas de erros apresentadas pelas LANs - tipicamente 10^{-9} ou menos.

4.3.1.1 Mecanismos de detecção de TPDUs corrompidas no TP4

No TP4, a utilização da *ckecksum* de transporte de extremo-a-extremo é opcional. Na verdade, é na fase de estabelecimento da ligação de transporte (TC) que se negoceia a utilização ou não deste mecanismo. A *checksum* é colocada na zona das variáveis do cabeçalho de transporte de cada TPDU quando é utilizadao na ligação. A *checksum* é calculada para toda a TPDU, sendo o campo correspondente à *ckecksum* colocado a zero durante o cálculo.

4.3.1.2 Mecanismos de detecção de TPDUs corrompidas no TCP

Aqui, a utilização deste mecanismo é obrigatória. O valor da *checksum* é colocado no cabeçalho TCP da cada TPDU. O seu cálculo é efectuado para toda a TPDU (i.e. cabeçalho

+ dados), mas também cobre um pseudo-cabeçalho que é prefixado ao cabeçalho TCP. De novo, enquanto o cálculo se efectua, o campo correspondente é colocada a zero.

4.3.1.3 Mecanismos de detecção de pacotes XTP corrompidos

O XTP utiliza duas *checksums* complementares de integridade. A checksum **Dcheck** cobre o segmento intermédio do pacote entre o cabeçalho e o apêndice XTP: o segmento de informção ou de controle. Este campo <Dcheck> é o único campo presente no apêndice XTP.

Por outro lado, a checksum **HT check** é calculada sobre o cabeçalho XTP de comprimento fixo, excluindo os seguintes campos: <route>, <ttl> e o próprio <HT check> que é o último campo encontrado no cabeçalho.

Se é encontrado um cálculo da checksum errado na recepção, o pacote é destruido. Se o cálculo do HT check estiver correcto e o cálculo do Dcheck estiver errado, a entidade XTP receptora consegue identificar a entidade emissora com toda a segurança. Neste caso, pode-se enviar imediatamente um pacote CNTL de controle à entidade emissora para avisar que ocorreu um erro. Isto só ocorre se a entidade emissora pediu a emissão de pacotes CNTL, caso contrário, o pacote é simplesmente destruido sem envio do pacote CNTL.

A utilização da checksum HT check é obrigatória, ao passo que a Dcheck é opcional. A flag NOCHECK é colocada a 1 no campo <options> do header XTP do pacote para indicar que o cálculo do campo Dcheck não é efectuado sobre este pacote.

4.3.2 Mecanismos de detecção e recuperação de TPDUs perdidas

A perda de TPDUs DT no TP4, de TPDUs de dados no TCP e de pacotes tipo FIRST ou DATA no XTP é efectuado utilizando um mecanismo de numeração. O TP4 utiliza uma numeração baseada na TPDU DT ao passo que o TCP e o XTP utilizam uma numeração baseada no byte. Este mecanismo de numeração dos dados permite que uma entidade de transporte emissora poporcione à entidade receptora informação sobre as TPDUs que transmitiu. A entidade receptora por sua vez deve comunicar à entidade emissora informação sobre as TPDUs que recebeu com sucesso. Para isso, estes três protocolos utilizam um mecanismo de **confirmação positiva** para este efeito, associado com o mecanismo de numeração.

Em todos estes protocolos, as confirmações positivas são **cumulativas**, ou seja cada confirmação positiva traz de volta o maior número de sequência para o qual todas as TPDUs

com números inferiores forma correctamente recebidas. Uma vatagem importante deste mecanismo de confirmações cumulativas é que elas fornecem uma informação de controle de erro redundantem reduzindo os prblemas causados pela perda de confirmações. Por outro lado, este mecanismo tem um problema que está relacionada com a perda de uma TPDU de ordem i. A partir da altura em que essa TPDU se perde todas as confirmações subsequentes contém o número de sequência da TPDU perdida (i) até que essa TPDU chegue ao seu destino. O problema é que estas confirmações não contém qualquer informação sobre o número de sequência da TPDU que os originou.

Ao contrário do TP4 e do TCP, uma entidade XTP pode ainda implementar um mecanismo adicional selectivo de confirmações positivas, sendo este mecanismo combinada com o mecanismo cumulativo de confirmações positivas.

Quer no TP4 quer no TCP, a estratégia escolhida para as confirmações positivas é da responsabilidade da entidade receptora, já que a entidade emissora não precisa de as pedir explicitamente.

No XTP, cabe à entidade emissora escolher a estratégia mais adequada para as respostas que trazem confirmações. Normalmente, a entidade XTP receptora só envia uma confirmação se foi explicitamente pedida pela entidade emissora. Existe no entanto uma condição extraordinária sob a qual pode a entidade emissora autorizar a entidade receptora a enviar confirmações, mesmo quando não foram pedidas.

Como tivemos oportunidade de ver, a perda de TPDUs DT no TP4, de TPDUs de dados no TCP e de pacotes tipo FIRST ou DATA no XTP conduz a uma recuperação que é conseguida por meio de retransmissão. Deste modo, sempre que a entidade emissora recebe uma confirmação, actualiza a sua informação de estado e, no caso de uma confirmação positiva, também destrói os dados do utilizador que estavam retidos para uma possível retransmissão. Como as confirmações positivas no TP4 e no TCP informam da recepção correcta de TPDUs mas não se referem explicitamente às TPDUs perdidas, as retransmissões efectuadas pela entidade emissora são sempre baseadas em *timeout*.

4.3.2.1 Mecanismos de detecção e recuperação de TPDUs perdidas no TP4

O número de sequência da TPDU DT está contido no campo <TPDU-NR> do cabeçalho de transporte da TPDU DT.

Não existe nenhum mecanismo de "piggy-back" controlado no TP4. Significa isto que são necessárias TPDUs AK específicas para confirmar as TPDUs DT. O campo <YR-TU-NR> na TPDU AKcontém o número de sequência do próximo pacote esperado, isto é da próxima TPDU DT relacionada com a ligação de transporte. É uma confirmação positiva

cumulativa.

Cada TPDU DT é retida até que seja confirmada por uma TPDU AK e retransmitida no fim do *timeout*. A especificação do TP4 não exige nenhuma estratégia de confirmações particular:

1] A entidade de transporte receptora pode decidir-se a confirmar cada TPDU DT separadamente, ou confirmar um conjunto de TPDUs DT com uma simples TPDU.AK, já que as confirmações positivas são cumulativas.

2] Uma entidade de transporte emissora pode gerir os temporizadores numa base por ligação ou numa base por TPDU. Se fôr efectuada por ligação (TC), são possíveis dois métodos de retransmissão quando o temporizador expira para uma TC na qual o número de sequência mais elevado que foi recebido numa TPDU AK é (i). Um método é transmitir a TPDU DT que possui o número de sequência (i) e depois esperar pela próxima TPDU AK. Outro método mais agressivo é transmitir todas as TPDUs DT cujos números de sequência se situem entre o número (i) recebido e a TPDU DT que estava a ser transmitida quando o temporizador expirou. O segundo método corresponde a uma retransmissão "go-back-N".

O valor do *timeout* pode ser fixo pela implementação ou pode ser ajustável dinâmicamente. Geralmente, ele é ajustado dinâmicamente em função do tempo *round-trip* de modo a obter um desempenho razoável.

Se a utilização do mecanismo selectivo de confirmações positivas fôr escolhido para uma dada TC, a entidade de transporte receptora pode enviar confirmações selccionadas em complemento das confirmações cumulativas nas TPDUs AK de resposta.

Se a utilização de um mecanismo de pedido de confirmação fôr escolhido para uma dada TC, a entidade de transporte emissora pode pedir uma TPDU AK imediata colocando a 1 a flag ROA (pedido de confirmação) no cabeçalho de transporte de uma TPDU DT que esteja pronta para ser enviada.

No TP4, a detecção de TPDUs perdidas e os mecanismos de recuperação foram concebidos para lidar com redes de altas taxas de erro. Cada TPDU DT que é enviada deve ser confirmada por uma TPDU AK, ou alternativamente uma TPDU AK pode confirmar um conjunto de TPDUs DT. A transmissão de um conjunto de TPDUs AK degrada o desempenho pois a entidade de transporte que envia as TPDUs AK de resposta é obrigada a interromper a sua transmissão normal de TPDUs DT para transmitir cada TPDU AK de resposta e também porque a entidade de transporte que recebe as TPDUs AK vê-se também obrigada a interromper a sua transmissão normal de TPDUs DT de modo a conseguir processar recém chegada TPDU AK.

No TP4 não existe nenhum mecanismo selctivo de retransmissões. Por isso, quando se passa um *timeout*, ou só é necessário retransmitir a TPDU DT com o menor número de sequência que ainda não foi confirmado ou então será necessário todas as TPDUs DT que não foram ainda confirmadas. Se cairmos no primeiro caso, gasta-se um intervalo de tempo igual a um tempo de ida e volta (Round Trip Time) à espera da próxima TPDU AK. Por outro lado, retransmitir todas as TPDUs também não é uma boa solução. Na verdade, nas HSLANs com baixas taxas de erros, a perda de uma TPDU é indicativo de um congestionamento local. A retransmissão de todas as TPDUs ainda não confirmadas só contribui para piorar o problema em vez de o resolver.

4.3.2.2 Mecanismos de detecção e recuperação de TPDUs perdidas no XTP

No XTP, o controle de erros é dividido entre a entidade XTP emissora remota e a entidade XTP receptora local. Na figura 13 está descrito o estado da fila de entrada de uma entidade XTP receptora. Esse estado é caracterizado por três variáveis de estado: a **dseq**, a **rseq** e a **hseq**. Estas variáveis pertencem ao contexto de ligação local, i.e. ao registo de informação local relacionada com a ligação.

O valo de **dseq** é dado pelo número de sequência do próximo byte de dados a ser entregue ao utilizador na recepção. Todos os bytes de dados que possuem um número de referência menor ou igual ao valor de **dseq** foram já transferidos para o utilizador. O valor de **rseq** é uma unidade somada ao número de sequência mais elevado para o qual todos os bytes com número de sequência inferior foram correctamente recebidos neste fluxo de dados. O valor de **hseq** é uma unidade superior ao número de sequência do byte de dados mais alto de todos os bytes recebidos. Existem alguns buracos intermédios devidos a erros de transmissão ou pacotes destruidos. Se todos os bytes de dados recebidos consecutivamente sem erros já foram entregues ao utilizador então **dseq=rseq**. Se não existirem buracos então **rseq=hseq**. O valor de **dseq** é colocado no campo <Dseq> do cabeçalho XTP de todos os pacotes, ou seja os pacotes DATA (controle de "piggt-back") e os pacotes não DATA, transmitidos no fluxo simplex inverso realcionado com a mesma ligação XTP. O valor de **rseq** é colocado apenas no campo <Rseq> do segmento de controle dos pacotes CNTL (sem controle de "piggy-back").

O estado da fila de entrada da entidade receptora local é gravado por um pacote CNTL que é enviado de volta para a entidade emissora em dois casos a seguir descritos:

1] No caso de um pedido da entodade XTP remota, quando a flag SREQ ou a flag DREQ

é recebida no campo <flags> do cabeçalho XTP de um pacote recebido,

2] No caso em que a entidade local receptora detecta um buraco na sequência do seu fluxo de entrada, desde que o modo agressivo (negativo) de confirmação tenha sido seleccionado pela entidade emissora remota. Este modo é seleccionada quando a flag FASTNACK é colocada a 1 no campo <options> do cabeçalho XTP dos pacotes que chegam da entidade XTP emissora.

Se a entidade XTP emissora não seleccionar o modo negativo de confirmação, a entidade receptora local não tem permissão para enviar de volta um pacote CNTL quando detecta um buraco na sequência do seu fluxo de entrada. A entidade emissora é responsável por colocar as flags SREQ ou DREQ a 1 no cabeçalho XTP de um pacote que envie para a entidade receptora.

Sempre que uma entidade receptora local encontre uma flag SREQ colocada a 1 num pacote recebido, envia imediatamente um pacote CNTL de resposta que contém a gravação do estado actual da sua fila de entrada.

Sempre que a entidade receptora local detecta uma flag DREQ colocada a 1 num pacote recebido, coloca um indicador DREQ na sua fila de entrada após os dados do utilizador que extraiu do pacote recebido. À medida que os dados do utilizador da fila de entrada são movidos para os buffers, os indicadores DREQ vão sendo encontrados, e para cada um deles é gerado um pacote CNTL de resposta. Deste modo a entidade XTP emissora remota pode pedir a confirmação de dados quando são recebidos (flag SREQ) ou quando são entregues ao utilizador (flag DREQ).

O XTP possui um esquema de sincronização: *handshake* de sincronização. Cada contexto de ligação possui uma variável de sincronização de estado e uma variável de eco de estado. A variável de sincronização de estado é um contador local que é incrementado para cada pacote DATA enviado. Alternativamente, a variável de sincronizaçãopoderia ser incrementada sempre que a transmissão mudasse de pacotes de controle para pacotes de dados, criando uma nova época. O valor da variável de eco é o valor da última comunicação do valor da variável de sincronização pertencente à entidade com a qual se estabeleceu a ligação XTP. O valor actual da variável de sincronização é colocado no campo <sync> do cabeçalho XTP de cada pacote enviado. O valor de eco é colocado no campo <echo> do segmento de controle de cada pacote enviado. Um *handshake* sincronizado consiste na troca de dois pacotes CNTL:

1] Em primeiro lugar envia-se um pacote (**CNTL,SREQ**), que regista os valores actuais das variáveis locais (de eco e de sincronização). Quando este pacote CNTL chega à entidade receptora remota, o valor da variável de eco remota é actualizado com o valor que está

colocado no campo <sync> do pacote.

2] Em segundo lugar, é recebido um pacote CNTL em resposta ao pedido SREQ contendo um valor no campo <echo> que corresponde ao valor local da variável de sincronização.

O *handshake* sincronizado permite medir o tempo de ida e volta graças aos campos de controle do segmento de controle dos pacotes CNTL: <time> e <techo> (echo de tempo). O valor contido no campo <time> do pacote (**CNTL,SREQ**) é simplesmente replicado no campo <techo> do pacote CNTL de resposta.

A entidade XTP emissora utiliza um temporizador, WTIMER, um por cada ligação XTP para detectar a altura em que um pacote CNTL pedido não foi recebido dentro do período de tempo esperado. O temporizador WTIMER é reiniciado sempre que um pacote com a flag SREQ ou a flag DREQ colocada a 1 seja enviado. O valor de *timeout* do temporizador WTIMER deve ser ajustado em função do valor actual do tempo de ida e volta.

Quando o temporizador é iniciado, verificar-se-á uma das seguintes condições:

1] Um pacote CNTL é recebido em resposta antes que o *timeout* expire e não são encontrados quaisquer erros. Neste caso não é efectuada nenhuma acção em especial. O temporizador é simplesmente parado.

2] Um pacote CNTL é recebido em resposta antes do *timeout* expirar mas são encontrados erros. Neste caso, o pacote CNTL indica quais os números de sequência de saida que é necessário retransmitir. O temporizador é parado.

3] Não é recebido qualquer pacote CNTL durante o intervalo do *timeout*. Neste caso, a entidade XTP emissora começa a enviar pacotes (**CNTL,SREQ,sync=valor)** até que seja recebido um pacote CNTL com um valor no campo <echo> que corresponda ao valor local da variável de sincronização. Quando o protocolo entra num ciclo repetitivo na tentativa de de completar o *handshake* de sincronização, o intervalo de tempo entre tentativas aumanta exponencialmente. Este aumento exponencial é importante para minimizar o tráfego de tentativas repetidas, dando assim uma oportunidade de recuperação a sistemas congestionados.

O mecanismo de encaminhamento da parte de encaminhamento do XTP garante que os pacotes (pacotes do tipo DATA em particular) relacionados com a mesma ligação XTP cheguem sempre por ordem à entidade XTP receptora. Esta é uma característica essencial do XTP. Na realidade, os pacotes relacionados com a mesma ligação XTP não podem ser re-ordenados no caso de uma LAN isolada ou no caso de uma configuração de LANs interligadas por *bridges*. Quando as LANs são interligadas por *routers*, os pacotes só podem

ser re-ordenados se a parte de encaminhamento do XTP estiver presente em todos os *routers*.

No XTP, as retransmissões são baseadas na recepção e interpretação da pacotes CNTL , ao contrário do TP4 que é baseado em *timeouts*. Os três modos de operação para controle de erros são os seguintes:

1] modo **NOERR,**

2] **retransmissão go-back-N,**

3] **retransmissão selectiva.**

O modo mais simples é o **NOERR**. Cada retransmissão é anulada pela flag NOERR do cabeçalho XTP. A entidade XTP receptora assume sempre que recebeu toda a informação e, por isso, coloca sempre **hseq** e **rseq** a 1, escondendo os furos que possivelmente existiriam na sua fila de entrada. Assim, a entidade XTP emissora não se apercebe de erros, mas continua a observar o controle de fluxo. No caso contrário, o controle de erro no XTP permite duas estratégias de retransmissão: **go-back-N** e **retransmissão selectiva** que assentam na mesma estrutura básica protocolar. O mecanismo **fo-back-N** utiliza apenas o campo <Rseq> de segmento de controle de um pacote CNTL para indicar qual o ponto do fluxo de dados onde a retransmissão se deve iniciar. Para além disso, o mecanismo da **retransmissão selectiva** utiliza ainda os campos <nspan> e <spans> do segmento de controle de um pacote CNTL. O campo <nspan> contém o número de pares de números de sequência activos ("spans") que estão presentes no campo de comprimento variável <spans>. Estes pares de números de sequência são utilizados para identificar os pacotes que foram recebidos correctamente no fluxo de dados para além do valor de **rseq**. Uma entidade XTP emissora retém sempre os dados transmitidos até que eles sejam confirmados pela entidade XTP receptora que ajusta o conteúdo do campo <Dseq> de um pacote CNTL que envia como resposta à entidade emissora.

A técnica de **retransmissão selectiva** melhora o *throughput* em casos de taxas de erro elevadas com largura de banda pequena ou ainda atrasos elevados. Nas HSLANs, a largura de banda é imensa e as taxas de erro são baixas, logo não existem muitas diferenças, do ponto de vista do desempenho, entre retransmitir uma sequência inteira de pacotes ou retransmitir simplesmente os pacotes destruidos. Por isso, o procedimento **go-back-N**, que é mais simples, pode ser melhor. Assim, o XTP define a retransmissão **go-back-N** como um subconjunto compatível do mecanismo de **retransmissão selectiva**. Deste modo, fica assegurada a comunicação entre sistemas terminais que implementaram níveis de controle de erros diferentes.

O mecanismo de confirmação do XTP é melhor adaptado às HSLANs que o do TP4. Se existe ume transmissão sem erros, a taxa a que uma entidade XTP emissora recebe pacotes

CNTL de resposta é igual à taxa a que esta entidade XTP emissora envia pedidos de pacotes CNTL por colocação a 1 das flags SREQ ou DREQ nos pacotes que envia. Se forem removidos os espaços entre pedidos SREQ ou DREQ, os pacotes CNTL de resposta também serão removidos de espaços e cada pacote CNTL confirmará um grande grupo de pacotes DATA.

4.3.3 Mecanismos de detecção e recuperação de TPDUs duplicadas ou desordenadas

Para detectar a duplicação e a chegada desordenada de TPDUs DT no TP4, de TPDUs de dados no TCP e de pacotes do tipo FIRST ou DATA no XTP, todos estes protocolos utilizam o mecanismo de numeração de dados. Um duplicado é simplesmente destruido.

Quando a recepção ordenada de pacotes XTP é garantida, pacotes duplicados ou desordenados só ocorrem quando existem retransmissões.

4.4 Mecanismos de Controle de fluxo de extremo-a-extremo

O mecanismo de controle de fluxo de extremo-a-extremo na camada de transporte permite que uma entidade de transporte receptora controle o fluxo de dados que chegam numa base por ligação de transporte, actuando directamente nas entidades de transporte emissoras.

Todos estes protocolos utilizam um mecanismo conhecido por **janela deslizante(sliding-window)** associado com o mecanismo de numeração utilizado para o controle de erros. O TP4 utiliza uma numeração baseada nas TPDUs DT , ao passo que o XTP eo TCP utilizam uma numeração baseada no byte, como já foi visto.

4.4.1 Mecanismos de Controle de fluxo de extremo-a-extremo no TP4

Aqui, o tamanho da janela é expresso em TPDUs DT. O limite inferior e o tamanho da janela são comunicados pela entidade de transporte receptora no campo <YR-TU-NR> e no campo <CDT> das TPDUs AK (portanto sem controle de "piggy-back") que são enviadas no fluxo simplex inverso da mesma ligação de trnasporte.

De uma forma geral, o TP4 assume que o fornecedor de serviços de rede pode entregar TPDUs AK desordenadas. Uma entidade de transporte receptora pode controlar a sequência

de TPDUs AK recebidas. Esta TPDUs contém todas o mesmo número de confirmação no seu campo <YR-TU-NR>. O mecanismo que permite este controle utiliza um parâmetro de subsequência que está contido nas mesmas TPDUs AK. Quando a entidade de transporte emissora detecta uma TPDU AK desordenada, ela é simplesmente ignorada e destruida.

Uma TPDU AK que contém infirmação actualizada sobre o estado da janela deve ser enviada imediatamente quando é recebida uma TPDU DT que esteja fora da janela alocada dado que isso indica a perda de uma TPDU AK enviada préviamente. Para além disso, existe um limite superior imposto máximo que uma entidade de transporte pode esperar antes de transmitir informação actualizada sobre o estado da janela. Este limite é um dos parâmetros a ajustar na implementação.

A estratégia para o ajustamento do tamanho da janela de transmissão não foi especificada no TP4. Na prática, o tamanho da janela é ajustado com base numa heurística pela entidade receptora.

A utilização de opção expedita de dados é negociada entre o par de entidades de sessão durante a fase de estabelecimento da ligação de transporte (TC). Se esta opção fôr oferecida para uma TC, uma entidade de sessão pode escolher entre enviar dados numa TSDU expedita ou numa TSDU normal. O tamanho de uma TSDU expedita não pode ser superior a 16 bytes. O fornecedor de serviços de transporte assegura que uma TSDU expedita não seja entregue á entidade de sessão receptora após qualquer TSDU normal subsequente ou mesmo uma TSDU expedita susequente.

Assim, o TP4 só permite que uma única TPDU expedita de dados (TPDU ED) permaneça não confirmada em qualquer altura para cada fluxo simplex relacionado com uma TC. O TP4 também interrompe o fluxo normal de TPDUs DT até que a TPDU ED seja confirmada por uma TPDU de confirmação expedita (TPDU EA). Quando a TPDU EA é recebida, é retomado o fluxo normal de TPDUs DT , excepto no caso em que ainda haja TPDUs ED à espera de envio. Uma TPDU ED é retida até que seja confirmada e é retransmitida ao fim do *timeout* tal como uma TPDU DT. As TPDUs ED possuem uma numeração prórpia, logo não estáo sujeitas às restrições impostas pelo controle de fluxo de extremo-a-extremo. Por isso, podem ser enviadas mesmo que a janela de transmissão esteja completamente fechada.

4.4.2 Mecanismos de Controle de fluxo de extremo-a-extremo no XTP

Aqui, o tamanho da janela é expresso em bytes. A entidade XTP receptora comunica o seu limite inferior à entidade XTP emissora no campo <Dseq> do cabeçalho XTP de todos os pacotes (ou seja, aqui há controle de "piggy-back") que são enviados no fluxo simplex

inverso relacionadao com a mesma ligação XTP. O limite superior da janela é transmitido no campo campo <alloc> do segmento de controle apenas nos pacotes CNTL (i.e. sem controle de "piggy-back").

Todos os pacotes relacionados com uma ligação XTP, e em particular os pacotes CNTL que contém informação relevante da janela, são sempre entregues à entidade XTP receptora ordenadamente nos casos em que não há encaminhamento internet ou nos casos em que esse encaminhamento é efectuado pela parte de encaminhamento do XTP. Por tudo isto, assegura-se que a última informação referente ao estado da janela que é recebida é a mais recente.

Dado que o limite superior da janela só pode ser comunicado por intermédio de pacotes CNTL, uma entidade XTP emissora tem que pedir pacotes CNTL à entidade XTP remota por meio de SREQ ou DREQ, para obter as informações mais recentes sobre o estado da janela (nomeadamente o seu limite superior). Por isso, nas redes com um produto **T*RTD** elevado, o tamanho alocado à janela é um factor fundamental do ponto de vista do desempenho. Geralmente, uma entidade XTP receptora copia o valor **alloc** para a direita de **dseq** com base numa heurística ou num deslocamento constante.

O XTP proporciona ainda um **modo explícito de reserva** para transferência de grandes volumes de dados. Neste modo, a flag RES é colocada a 1 no cabeçalho XTP dos pacotes para pedir à entidade receptora a alocação de uma janela de transmissão cujo tamanho represente exactamente o número de bytes disponíveis nos *buffers* de leitura atribuidos pelo utilizador à ligação XTP. No **modo de reserva**, deve ser enviado de volta um pacote CNTL com informação actualizada sobre o estado da janela sempre que seja atribuido à entidade XTP receptora um espaço de *buffer* superior.

A entidade XTP que inicia a ligação pode indicar que não vai obedecer ao controle de fluxo baseado nas janelas, colocando a 1 a flag NOFLOW do cabeçalho XTP dos pacotes enviados. Este modo destina-se a ser utilizado nas ligações controladas pela taxa (*rate-controlled*) ou em situações onde se deseja operar sem restrições. A entidade XTP que recebe o pacote FIRST pode recusar-se a aceitar o modo NOFLOW se rejeitar o pacote FIRST e responder com um pacote DIAG.

Normalmente, o acesso às filas de pacotes de entrada e de saida numa entidade XTP obedece a uma disciplina FIFO (First In First Out). De qualquer maneira, o XTP pode utilizar uma disciplina baseada numa fila com prioridades: *preemptive priority queue*. Na realidade, cada contexto activo tem uma vlor actual de ordenação fornecido pelo utilizador. As implementações XTP não são obrigadas a suportar ordenação/prioridade, no entanto, numa entidade XTP que as suporte, todos os pacotes que possuem uma prioridade mais elevada para transmissão devem ser enviados antes dos pacotes que se situam num nível de prioridade inferior.

No XTP, não existe nenhuma forma de evitar o fluxo de controle, mesmo quando o mecanismo da fila prioritári é utilizado. Esta situação é bastante diferente no TP4 e no TCP onde o envio de dados expeditos ou urgentes não é restringido pelo controle de fluxo.

Nas HSLANs que são caracterizadas por produtos **T*RTD** elevados, um mecanismo expedito de dados que bloqueia o envio de dados normais durante pelo menos um tempo de ida e volta para transmitir dados expeditos, pode ter um impacto negativo no desempenho global de uma troca de dados sobre uma ligação de transporte. Esta é a razão que justifica o seu reduzido interesse no futuro das comunicações.

4.5 Mecanismos de Controle de congestionamento

A taxa a que os dados são transmitidos numa dada ligação de transporte deveria ser condicionada pela taxa a que a entidade de transporte receptora recebe e processa as TPDUs de dados e depois as dirige para o utilizador. No entanto, a taxa a que os dados podem ser transmitidos numa dada ligação de transporte está condicionada à taxa suportada pelo serviço de rede.

O controle de fluxo de extremo-a-extremo não resolve problemas de congestionamento que podem ocorrer no interior do próprio serviço de rede, ouseja, congestionamentos locais nos *routers*. A função de controle de congestionamento foi concebida para lidar com congestionamentos internos ao serviço de rede.

A partir de agora, abandona-se o pressuposto que tomamos até aqui e que restringia a análise a uma LAN isolada ou um conjunto de LANs interligadas por *bridges*. Agora, inclui-se também na análise as configurações onde as LANs são interligadas por *routers*.

Neste último caso, o TP4 tem acesso ao serviço LLC do tipo 1 através do conjunto completo CLNP adicionadao com as funções SNDCFs. O encaminhamento está portanto a cargo do CLNP.

O XTP acede o serviço LLC do tipo 1 através o ponto de acesso SNAP. Quando o XTP é utilizado em LANs interligadas por *routers*, deve ser instalado em todos os sistemas terminais bem como em todos os *routers*.

4.5.1 Mecanismos de Controle de congestionamento no TP4

A especificação do TP4 não proporciona um mecanismo de controle de congestionamento. Esta limitação terá de ser removida de modo que assegure a viabilidade dos standards OSI nos ambientes HSLANs.

4.5.2 Mecanismos de Controle de congestionamento no TCP

No seu início, o TCP/IP não possuia nenhum mecanismo de controle de congestionamento, e os problemas deste tipo começaram a surgir com frequência. A cause deste tipo de problemas está na incapacidade do IP em realizar um controle adequado de congestionamentos. Na realidade, o algoritmo utilizado pelo TCP para ajustar o valor do *timeout* dos temporizadores de retransmissão conta com o pressuposto que as perdas de TPDUs que contém dados são aleatórias e muito raras (uma percentagem de 1 a 2%). No entanto, este pressuposto torna-se inválido quando o IP tenta resolver o congestionamento ao colocar sistemáticamente pacotes atrás de pacotes no *router* congestionado. Por seu lado, o TCP não pode ajudar o IP a resolver os problemas de congestionamento internos à rede se quer obter bons níveis de desempenho, a não ser que o TCP inclua o seu próprio mecanismo de controle de congestionamentos.

Foram desenvolvidos vários mecanismos de controle de congestionamento baseados em *timeout* que podem ser aplicados ao TCP/IP. Estes mecanismos contam com a ideia básica que afirma que, nas redes actuais com baixas taxas de erros, a perda de um pacote é geralmente um bom indicador da ocorrência de um congestionamento. Por isso, sempre que o *timeout* associado com uma dada TPDU expira, a carga na rededeve ser eduzida. Mais tarde, se não ocorrerem mais oerdas, a carga deve ser aumentada lentamente. Os mecanismos disponíveis diferem nas estratégias que escolhem para diminuir e de seguida aumentar o tráfego apresentado à rede. Os mecanismos de controle de congestionamento baseados em *timeout* são caracterizados por um arranque lento ("slow start") e por reinicios lentos após congestionamentos ("slow restarts"). Por isso, não são realmente adequados às redes actuais e futuras, que são promissoras do ponto de vista de cargas efectivamente transportadas (*throughput*), porque conduzem a um subaproveitamento da largura de banda disponível em cada inicio ou reinicio. No entanto, estes mecanismos possuem uma vantagem inegável: a sinalização de um congestionamento é implícita, logo não aumenta o tráfego durante o congestionamento. O mecanismo de controle de congestionamento implementado no XTP pertence à parte de encaminhamento do XTP e não à parte de transporte.

4.5.3 Breve descrição da parte de encaminhamento do XTP

Os dois mecanismos básicos que são implementados na parte de encaminhamento do XTP são:

- o mecanismo de encaminhamento propriamente dito e
- o mecanismo de controle da taxa de transmissão.

4.5.3.1 Mecanismo de encaminhamento no XTP

Quando uma ligação XTP é estabelecida entre dois sistemas terminais A e B que se situam em LANs diferentes interligadas por *routers*, o encaminhamento está a cargo da parte de encaminhamento do XTP. O pacote FIRST enviado para estabelecer a ligação XTP é obrigado a travessar um ou mais *routers* para atingir o seu destino. Este pacote assinala deste modo um percurso na rede. Todos os pacotes subsequentes que circulem em ambos os fluxos simplex relacionados com esta ligação XTP irão seguir o mesmo percurso seguida pelo pacote FIRST. è por isso que a função de encaminhamento do XTP assegura sempre a chegada ordenada de pacotes pertencentes à mesma ligação XTP. Na rede, um pacote não pode ultrapassar outro pacote já transmitido na mesma ligaçãoXTP, a não ser que a disciplina utilizada para aceder às filas de entrada e saida de pacotes não seja do tipo FIFO.

A relação existente entre os conceitos de **'percurso'** (que pertence à parte de encaminhamento do XTP) e de **'ligação'** (que pertence à parte de transporte) não é de um-para-um. Na realidade, uma ligação XTP está sempre associada a um único percurso na rede mas o mesmo percurso pode ser partilhado por várias ligações XTP estabelecidas entre os mesmos sistemas terminais. Por conseguinte, ligações XTP distintas estabelecidas entre os mesmos sistemas terminais podem utilizar percursos diferentes ou o mesmo percurso na rede.

A selecção de um percurso na altura em que se estabelece a ligação é baseada nas variáveis de percurso utilizadas no campo <percurso> do cabeçalho XTP dos pacotes.

4.5.3.2 Mecanismo de Controle da taxa de transmissão no XTP

O XTP possui um mecanismo de controle de congestionamento baseado no controle da taxa de transmissão. Este mecanismo pertence à parte de encaminhamento do XTP visto que o controle da taxa de transmissão é efectuado pelas entidades XTP terminais e pelos *routers* XTP intermédios.

O controle da taxa de transmissão é efectuado numa base por-percurso e não numa base por-ligação, logo é necessário recorrer à distinção entre os dois conceitos como foi referido atrás. Assim, um percurso que seja partilhado por muitas ligações XTP implica uma partilha de taxa de transmissão por essas mesmas ligações. As taxas de saida podem ser controladas separadamente em ambas as direcções do percurso.

Uma entidade XTP receptora pode controlar a taxa de transmissão na direcção da

recepção se proporcionar informação respeitante a esse controle por intermédio dos campos <rate> e <burst> do segmento de controle dos pacotes CNTL que envia como resposta à entidade XTP emissora. O valor contido no campo <rate> especifica a taxa de transmissão de dados máxima em bytes por segundo. O valor contido no campo <burst> especifica o número máximo de bytes a ser transmitidos num conjunto de pacotes. Deste modo, o valor do campo <rate> dividido pelo valor do campo <burst> dá o número de transmissões de conjuntos de pacotes com o tamanho <burst> por segundo autorizadas.

Qualquer *router* XTP intermédio ao longo do percurso possui autorização para diminuir os valores dos campos <rate> e <burst> do pacote CNTL quando este o atravessa. Para além disso, um *router* XTP não precisa de esperar por uma pcote CNTL para enviar infirmação de controle da taxa de transmissão a uma entidade XTP emissora. O *router* pode decidir-se a enviar um pacote RCNTL (pacote CNTL gerado pelo *router*) com os valores <rate> e <burst> adequados.

Teóricamente, o mecanismo de controle da taxa de transmissão no XTP permite prevenir os fenómenos de congestionamento nos *routers* XTP visto que um *router* pode memorizar e também alterar os valores das variáveis <rate> e <burst> realcionados com todos os percursos que o atravessam. Na prática, o mecanismo de controle da taxa de transmissão acarreta alguns problemas tais como a medida correcta de recursos postos à disposição de um *router* XTP. Para além disso, mesmo que o mecanismo de controle da taxa de transmissão permita evitar os congestionamentos locais nos *routers* XTP, as *bridges* que interligam as LANs ao nível MAC não podem participar no controle da taxa de transmissão. Por isso, o mecanismo de controle da taxa de transmissão no XTP é impotente para resolver os problemas de congestionamento numa rede onde existem várias LANs interligadas por *bridges*.

4.6 Mecanismo de Multidifusão

4.6.1 Mecanismo de Multidifusão no TP4

O TP4 foi desenvolvido na altura em que as infraestruturas de comunicações eram dominadas por linhas comutadas, linhas alugadas e WANs (Wide Area Networs) de comutação de pacotes. O fornecedor de serviços de rede não oferecia facilidades de difusão ou multidifusão. Por isso, a inclusão de um mecanismo de multidifusão no nível de transporte não era estritamente necessário.

Uma ligação de transporte (TC9 é estabelecida entre dois pontos de acesso ao serviço de

transporte (TSAPs) e permite a transferência de TSDUs apenas entre as duas entidades de sessão associadas por esta ligação.

4.6.2 Mecanismo de multidifusão no XTP

O XTP proporciona um mecanismo de multidifusão. O serviço abaixo deve suportar pelo menos a capacidade de difusão. A filtragem de endereços do XTP pode ser utilizada para estabelecer uma camada com uma arquitectura de endereços de multidifusão em cima da transmissão por difusão.

Graças a este mecanismo de multidifusão, a facilidade de multidifusão nas LANs pode ser estendida até à interface do serviço fornecido pelo XTP. Esta extensão tem muito interesse numa LAN isolada ou num conjunto de LANs interligadas por *bridges*. Esta facilidade continua a ser atractiva num conjunto de LANs interligadas por *routers* XTP, desde que não afecte o desempenho global. É de notar que na maior parte das vezes os *routers* constituem os elementos críticos do ponto de vista do desempenho.

O mecanismo de multidifusão no XTP é um mecanismo que permite emviar pacotes multidifundidos a partir de uma única entidade XTP multidifusora para um conjunto de entidades XTP multidifundidas. O controle de erros pode permanecer ou pode ser inibido colocando a 1 a flag NOERR no cabeçalho XTP de todos os pacotes enviados.

Os pacotes multidifundidos abedecem às mesmas regras de sintaxe dos pacotes normais: o cabeçalho XTP, o apêndice XTP e os segmentos de controle ou de informação são idênticos.

Os pacotes multidifundidos diferem dos pacotes normais apenas nas seguintes características:

- todos os pacotes multidifundidos possuem a flag MULTI colocada a 1 no seu campo <options> do cabeçalho XTP enquanto que os pacotes normais não possuem esta flag colocada a 1,

- os pacotes FIRST multidifundidos utilizam endereços de grupo em vez de endereços individuais no seu subsegmento de endereços,

- os pacotes multidifundidos utilizam sempre a flag SREQ e nunca a flag DREQ,

- a flag SREQ pode ser colocada a 1 apenas nos pacotes de controle CNTL e nunca nos pacotes de dados DATA.

Quando um utilizador instrui a entidade XTP para utilizar o modo de multidifusão através de parâmetros de configuração, a flag MULTI é colocada a 1 por esta entidade XTP no cabeçalho XTP de todos os pacotes que enviar. Os outros aspectos da transmissão permanecem inalterados: o pacote inicial será do tipo FIRST enquanto que os pacotes subsequentes serã do tipo DATA e todos os bits (flags) do cabeçalho XTP que comandam as opções funcionam normalmente.

Um utilizador que deseja receber transmissões multidifundidas estabelece um contexto de escuta que corresponda a qualquer endereço de multidifusão e passa ao estado activo. Quando activo, este contexto aceita a transmissão multidifundida e entrega os dados ao utilizador respectivo.

Existem dois métodos de controle de erros disponíveis no modo de multidifusão do XTP:

1] **Sem controle de erro:**

A flag NOERR é colocada a 1 em todos os pacotes. As entidades XTP receptoras destroem os dados de entrada que chegarem danificados e entregam aos seus utilizadores apenas os dados correctos. Não são tomadas mais acções.

2] **Retransmissão go-back-N de pacotes danificados:**

A multidifusão que emprega este método é utilizada sempre que não seja inibida pela flag NOERR. A entidade XTP receptora monitoriza os números de sequência utilizando o mesmo mecanismo descrito na secção 4.3.2.2.

No entanto, no modo de multidifusão, se se desjar um fluxo de saida contínuo,uma entidade XTP emissora deve associar positivamente os pacotes CNTL de resposta com eventos passados. Isto só pode ser conseguido fazendo corresponder os valores <echo> retornados nos pacotes CNTL aos valores locais <sync>. Este procedimento requer que uma entidade XTP multidifusora coloque a flag SREQ a 1 apenas nos pacotes CNTL, e nunca nos pacotes FIRST e DATA. Os pacotes CNTL que são enviados pelas entidades XTP receptoras em resposta à flag SREQ recebida são multidifundidos ao grupo de entidades XTP que participam na multidifusão bem como à entidade XTP multidifusora. Este comportamento é necessário para a utilização de algoritmos de **amortecimento** (*damping*) e de **escatelamento** (*slotting*). No primeiro caso, uma entidade XTP receptora não envia o pacote CNTL se este fôr um duplicado de um pacote já observado a circular na rede. Este algoritmo reduz o número total de pacotes CNTL que são trasnmitidos, subtraindo o número de pacotes duplicados. No entanto, torna-se necessário que todas as entidades receptoras leiam todos os pacotes CNTL.

A técnica de escatelamento impõe um atraso aleatório antes de enviar pacotes CNTL pedidos através da flag SREQ. Os resultados obtidos por esta técnica são dois:

- em primeiro lugar, o número de pacotes CNTL é distribuido no tempo em vez de ser concentrado no tempo,

- em segundo lugar, a distribuição de pacotes CNTL no tempo aumenta a probabilidade de uma implementação praticar a primeira técnica -amortecimento.

A geração e a interpretação de pacotes CNTL necessita de considerações especiais no modo de multidifusão. No modo normal, um valor **dseq** que é recebido no campo <Dseq> de um pacote CNTL enviado como resposta à entidade XTP emissora, indica que os dados recebidos foram correctamente entregues ao utilizador na recepção. Mas no modo de multidifusão, um valor **dseq** retornado apenas indica que uma das entidades receptoras que participam na multidifusão recebeu correctamente os dados. O algoritmo *bucket* proporciona a estratégia adequada ao envio de pedidos SREQ, interpretando os pacotes CNTL retornados e libertando os *buffers* de saida.

Este esquema de multidifusão não funciona eficientemente em todas as circustâncias e em todos os ambientes. Se existirem muitos receptores XTP de multidifusão numa rede com propensão a erros, esistirão muitos pacotes CNTL de erros multidifundidos e consequentemente pouco progresso nesta área. Nesta circusntâncias é aconselhável a utilização da estratégia NOERR.

4.7 Conclusões do estudo dos mecanismos de transferência de dados

Do que ficou exposto, conclui-se que o XTP é um protocolo melhor adaptado que o TP4 e o TCP às novas infraestruturas das comunicações e às novas aplicações, particularmente as que exigem ambientes *multimedia*.

Para atingir estes objectivos, os autores do XTP concentraram esforços no desenvolvimento de um mecanismo de multidifusão e num mecanismo selccionável de controle de erros.

O objectivo de tornar o XTP num protocolo melhor adaptado que o TP4 e o TCP às condições de elevada largura de banda com reduzidas taxas de erroinfluenciou a maior parte dos mecanismos de transferência de dados.

A parte de transporte do XTP não inclui nenum mecanismo similar ao mecanismo de

concatenação/separação do TP4 que é considerado obsoleto nos dias que correm.

Conclui-se através de simulações que o controle de erros e o controle de fluxo são as funções de transporte que mais afectam o desempenho. Neste ponto, o XTP difere dos protocolos clássicos (TCP e TP4) apenas na forma como utiliza esses mecanismos. Os mecanismos de controle de erros e de fluxo no XTP estão melhor adaptados às propriedades das redes de alta velocidade com baixas taxas de erro, e em particular às HSLANs.

Na parte de encaminhamento do XTP, o maior melhoramento introduzido foi um mecanismo de controle da taxa de transmissão que evita congestionamentos nos *routers*. Uma propriedade importante de mecanismo de encaminhamento do XTP é a de conseguir que todos os pacotes relacionados com a mesma ligação XTP sigam o mesmo percurso na rede, o que assegura a sua entrega ordenada à entidade XTP receptora.

5. Conclusão do estudo desenvolvido

O estudo das normas XTP bem como dos artigos referidos e dos livros consultados permitiu concluir que o XTP é um protocolo em rápido desenvolvimento que promete vir a aproveitar de uma forma eficiente os novos conceitos e tecnologias na área das comunicações. O surgimento de redes de fibras ópticas que conduziu ao crescimento de aplicações *multimedia*, introduziu a necessidade de funcionalidades flexíveis em altas velocidades de transmissão que são fornecidas no XTP. Por outro lado, o XTP foi especificado de forma a permitir a sua fácil implementação em *hardware* utilizando a tecnologia VLSI actual.

Por tudo isto, a análise dos estudos efectuados e a realização deste trabalho com base nesses estudos reveste-se de um interesse particular no que diz respeito à análise da evolução dos protocolos de transporte e ao conhecimento do que serão os ambientes de redes de comunicações da próxima década.

Bibliografia

Protocol Engines, Inc. : XTP Protocol Definition - Revision 3.6
Ref.: PEI 92 -10, Jan. 11,1992

Y. Baguette, A. Danthine, «Comparison of TP4, TCP and XTP »
ETT, Vols. 3 and 4

W. Timothy Strayer, Bert J. Dempsey, Alfred C. Weaver, « XTP: The XpressTransfer Protocol »
Addison-Wesley Publishing Company, Inc.,1992

William Stallings, Ph D., « Data and Computer Communications »
Macmillan Publishing Company, 1985

Andrew S. Tanenbaum, « Computer Networks »
3rd Ed. Englewood Cliffs,
Prentice-Hall International, Inc., 1988

Anexo: Figuras

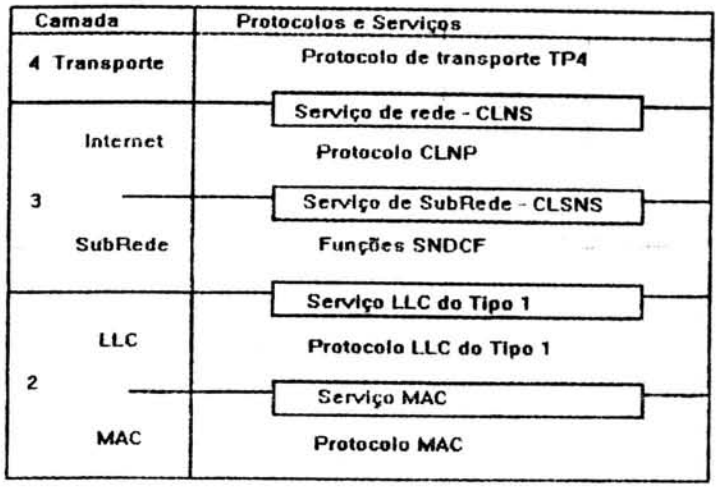


Figura 1. Pilha Protocolar ISO para as camadas 2 a 4 em ambientes LAN

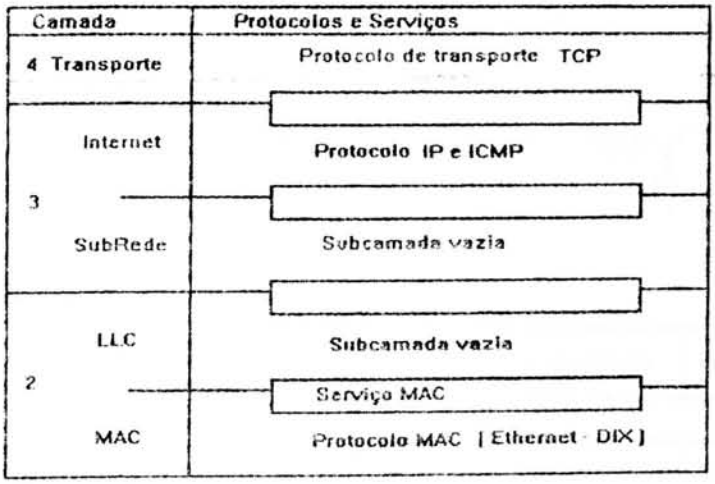


Figura 2 (a) Pilha protocolar DARPA para as camadas 2 a 4 quando o TCP/IP é utilizado sobre uma LAN Ethernet - DIX

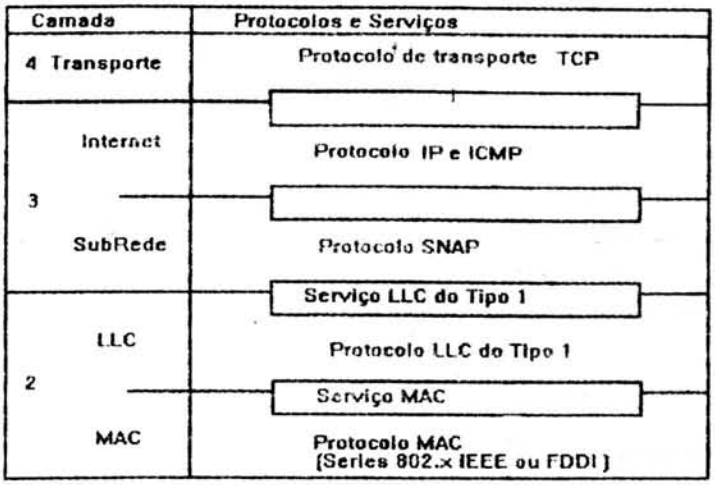


Figura 2 (b) Pilha protocolar DARPA para as camadas 2 a 4 quando o TCP/IP é utilizado sobre uma LAN IEEE 802 ou uma LAN FDDI.

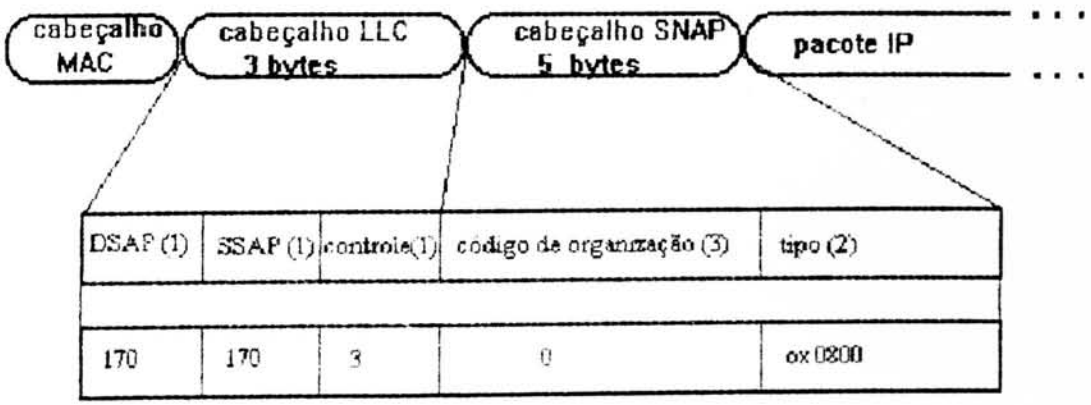


Figura 3. Encapsulamento de pacotes IP utilizando o protocolo SNAP

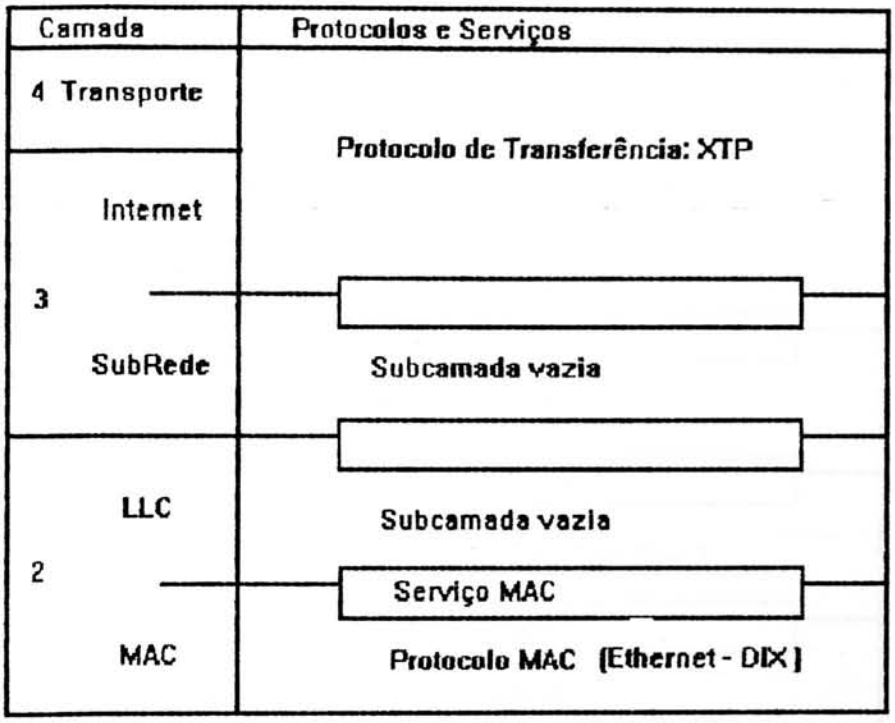


Figura 4 (a) Pilha protocolar para as camadas 2 a 4 em ambientes LAN quando o XTP é utilizado sobre uma LAN Ethernet - DIX.

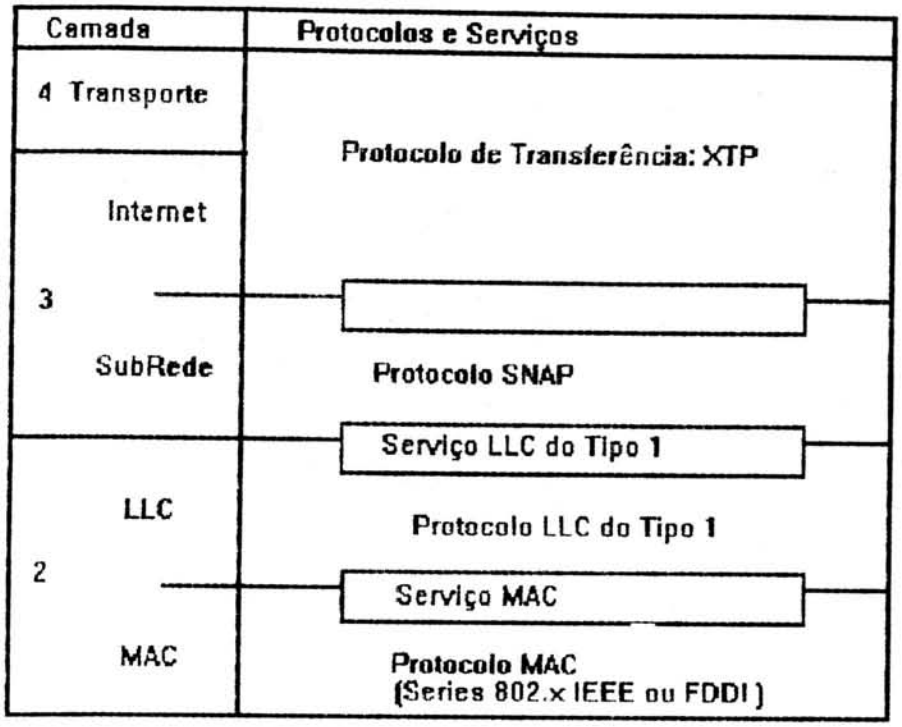


Figura 4 (b) Pilha protocolar para as camadas 2 a 4 em ambientes LAN quando o XTP é utilizado sobre uma LAN IEEE 802 ou sobre uma LAN FDDI.

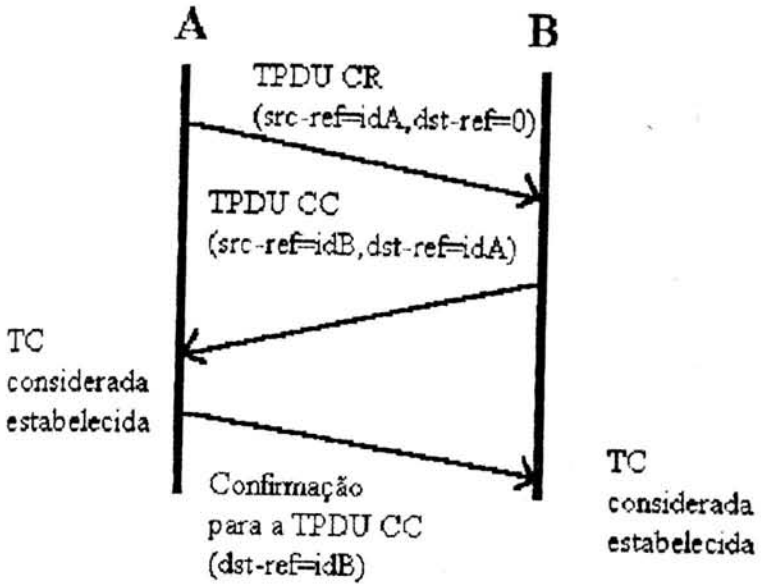


Figura 5. Mecanismo de Estabelecimento da ligação de transporte (TC) baseado num handshake de três vias no TP4.

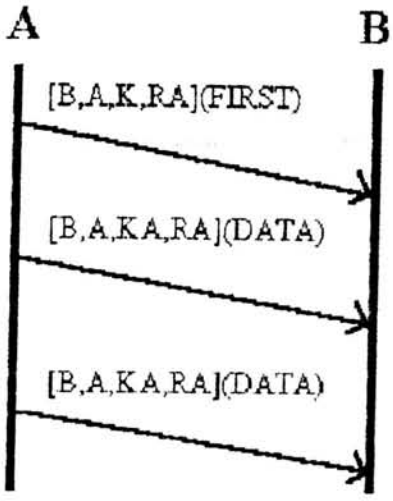
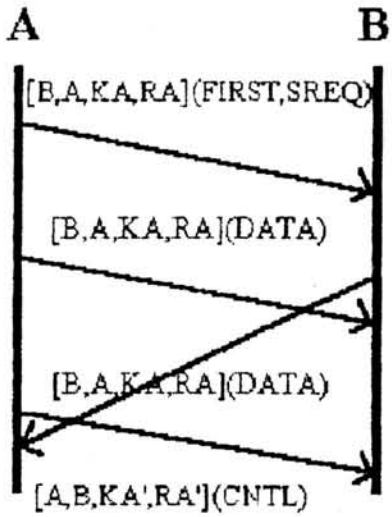
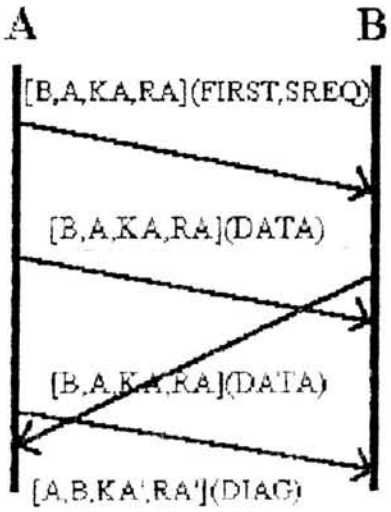


Figura 6. Mecanismo implícito de Estabelecimento da ligação no XTP.



Os pacotes DATA podem ser enviados antes do pacote CNTL de resposta chegar à entidade emissora (A).

Figura 7. Mecanismo implicito de Estabelecimento da ligação no XTP: aceitação da ligação.



Os pacotes de dados são destruidos em (B) porque a ligação foi recusada.

Figura 8. Mecanismo implicito de Estabelecimento da ligação no XTP : Ligação recusada.

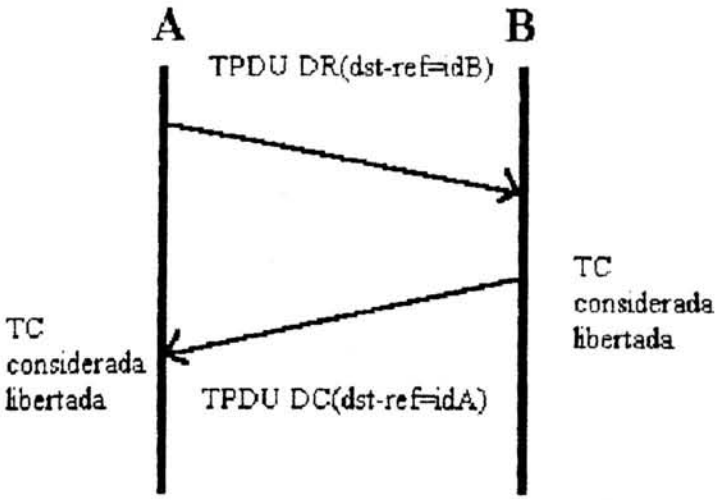


Figura 9. Mecanismo de libertação da ligação de transporte no TP4 baseado num handshake de duas vias.

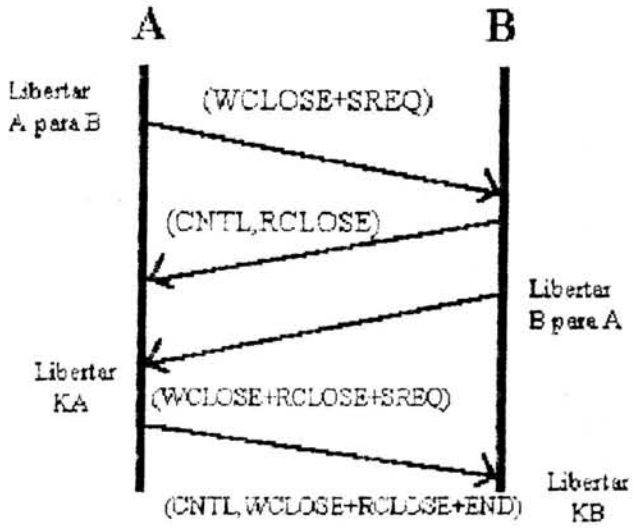


Figura 10. Mecanismo de libertação da ligação no XTP: baseado num handshake duplo de duas vias: dois handshakes de duas vias cada um.

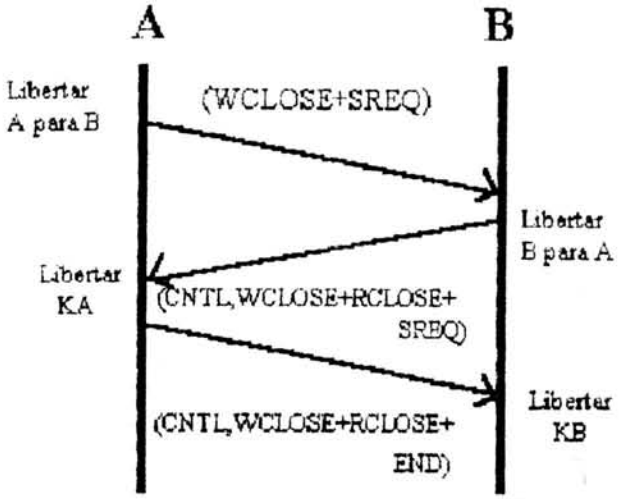


Figura 11. Mecanismo de libertação da ligação no XTP baseado num único handshake de três vias

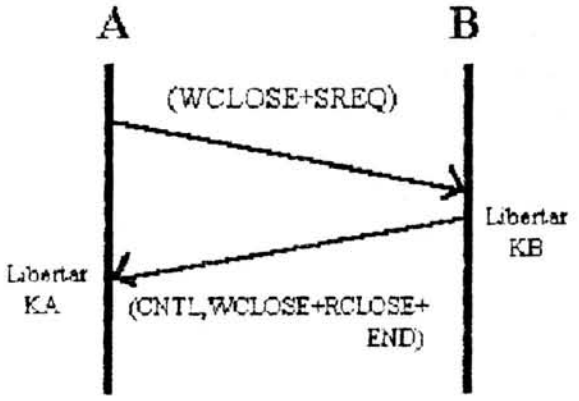


Figura 12. Mecanismo de libertação da ligação no XTP baseado num handshake de duas vias.

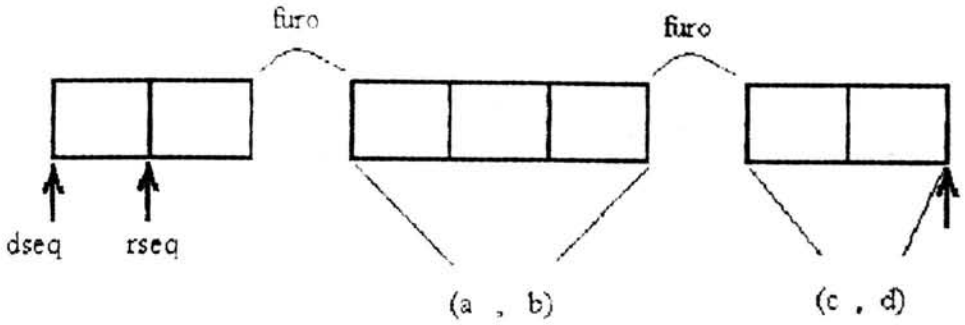


Figura 13. Descrição do estado da fila de entrada duma entidade XTP.