UNIP
UNIVERSIDADE PAULISTA

Interativa

Redes I – Longa Distância e Alto Desempenho

Autor: Prof. Ataide Pereira Cardoso Junior
Colaboradoras: Profa. Elisângela Mônaco de Moraes
Profa. Iza Melão

Professor conteudista: Ataide Pereira Cardoso Junior

Graduado em Administração de Empresas, com especialização em Análise de Sistemas, possui diversas certificações profissionais na área de Redes de Computadores, entre elas, Cisco, HP, Novell, VMWare e Microsoft. É professor especialista da Universidade Paulista (UNIP) no curso Redes de Computadores desde 2004 e também professor instrutor da Cisco Network Academy da UNIP.

Dados Internacionais de Catalogação na Publicação (CIP)

C268r Cardoso Junior, Ataíde Pereira.

Redes I: Longa Distância e Alto Desempenho/ Ataíde Pereira Cardoso Junior. – São Paulo: Editora Sol, 2021.

240 p., il.

Nota: este volume está publicado nos Cadernos de Estudos e Pesquisas da UNIP, Série Didática, ISSN 1517-9230.

1. Redes. 2. Longa distância. 3. Alto desempenho. I. Título.

CDU 681.324

U510.20 – 21

Sumário

Redes I – Longa Distância e Alto Desempenho

Unidade III

Unidade IV

Unidade V

Unidade VI

Unidade VII

Unidade VIII

APRESENTAÇÃO

O objetivo deste livro-texto é apresentar aos estudantes os conceitos básicos das tecnologias de redes de computadores, sobretudo aquelas empregadas aos serviços de longa distância e de alto desempenho, com um forte apelo aos conceitos usados na telecomunicação e na transmissão de dados, que pertencem à categoria dos assuntos de extrema importância para a formação profissional em redes de computadores.

Percorrendo o caminho da evolução da tecnologia dos computadores, exploramos as primeiras tecnologias voltadas para a comunicação de longa distância. Embora algumas pessoas possam entender que essas tecnologias não fazem parte do contexto da atualidade, a resposta a essa dúvida é de simples compreensão: elas formam a base do conhecimento das tecnologias de longa distância e de alto desempenho, envolvendo protocolos que são empregados nos dias de hoje. Esse conhecimento acumulado traz uma forte compreensão dos conceitos e dos valores aplicados à tecnologia das redes de comunicação e faz parte do conteúdo necessário ao aprendizado.

Este material é apoiado com enfoque fortemente tecnológico, remetendo essa tecnologia para o futuro e trazendo a certeza de que esse caminho ainda deve percorrer um longo trajeto.

A abordagem desse conteúdo faz uma clara referência aos conceitos do modelo padrão OSI, com uma expressiva comparação às tecnologias aqui abordadas. Esses conceitos nos ajudam a compreender os mecanismos e as argumentações necessárias às referências nele expostas.

Na parte final do material, poderemos contemplar as principais tecnologias que propiciam o alto desempenho e que servem tanto às redes de longa distância quanto às redes locais, o que, mais uma vez, fundamenta claramente a necessidade do conhecimento da técnica e de suas aplicabilidades.

INTRODUÇÃO

Este material tem a responsabilidade de colocar nas mãos dos estudantes de redes de computadores conceitos e fatos sobre as tecnologias de comunicação de dados para as redes de longa distância, levando-os ao limite da tecnologia do alto desempenho. Alguns aspectos de grande relevância foram conceituados neste material envolvendo as soluções e a tecnologia predominantes no mercado de redes de computadores do Brasil. Provavelmente esses conceitos fazem parte do arcabouço de conhecimento de grande valia para todas as pessoas que se dedicam à tecnologia.

Nossa missão se inicia trazendo à pauta as tecnologias de rede que se iniciaram no final da década de 1960, passando por suas evoluções naturais, chegando aos dias de hoje com as aplicações de extraordinária capacidade de transporte de dados associado às redes públicas de comunicação e implementando altos níveis de confiabilidade e segurança. Nos apoiamos, sobretudo, nos protocolos de camada de rede de última geração, sem esquecer do legado dos protocolos da internet e das redes locais.

Entendemos que esses conceitos devem se fazer presentes para a capacitação do profissional de redes de computadores que trilha o caminho do conhecimento. Sabemos também que a abordagem deste

material precisa ter uma dose significativa de tecnologia e não apenas uma conceituação generalista a respeito do tema. Certamente, esse é o ponto central das preocupações dos profissionais de rede e dos docentes que propagam a tecnologia a seus alunos.

Ao fim desse material faremos abordagens específicas nas redes de alto desempenho de última geração, conceituando de forma firme e incisiva as tecnologias de redes ATM e MPLS – esta sim entendida como a tecnologia da atualidade para as redes de longa distância e que conta ainda com um grau de alto desempenho na excelência dos seus serviços para os usuários de redes públicas de dados.

Unidade I

1 O PROTOCOLO X-25 E O PONTO A PONTO

1.1 A tecnologia do protocolo X-25

1.1.1 Introdução ao X-25

O ITU criou e padronizou o protocolo X-25 para comunicação de redes WAN (*wide area network*), que provê o formato de como são estabelecidas e mantidas as conexões entre os equipamentos dos usuários da rede X-25. O uso das redes X-25 compreende a implementação de pacotes PSN (*packet switch network*) pelas empresas operadoras de telefonia. Sua forma de cobrança está relacionada ao consumo de banda do usuário. Em 1970, começou a ser desenvolvida a rede X-25, que hoje estabelece conectividade à rede SPDM rede pública de dados.

1.1.2 Operação dos equipamentos do protocolo X-25

Podemos dividir em três tipos de ativos a infraestrutura das redes X-25: ela é constituída inicialmente pelos DTE (*data terminal equipments*), pelos DCE (*data carrier equipments*) e pelos PSE (*packet switch equipments*).

1.1.2.1 Os DTE

Os DTE (*data terminal equipment*) são os equipamentos finais que comunicam os usuários às redes X-25. Eles são classificados como terminais computadores, impressoras, servidores e *notebooks* e localizam-se internamente na rede do usuário.

1.1.3 Os DCE

Os DCE (*data carrier equipment*) são os equipamentos de comunicação que fazem o perímetro da nuvem X-25. Exemplos: os *modems* de suítes, que são a interface entre os aparelhos DTE e os aparelhos PSE.

1.1.4 Os PSE

Os PSE (*packet switch equipment*) são *switches* que compõem a infraestrutura interna da nuvem da rede da operadora de telefonia para os serviços de 25. Têm uma função plástica de permitir a transferência dos dados entre os dispositivos DTEs para outros, através da rede X-25.

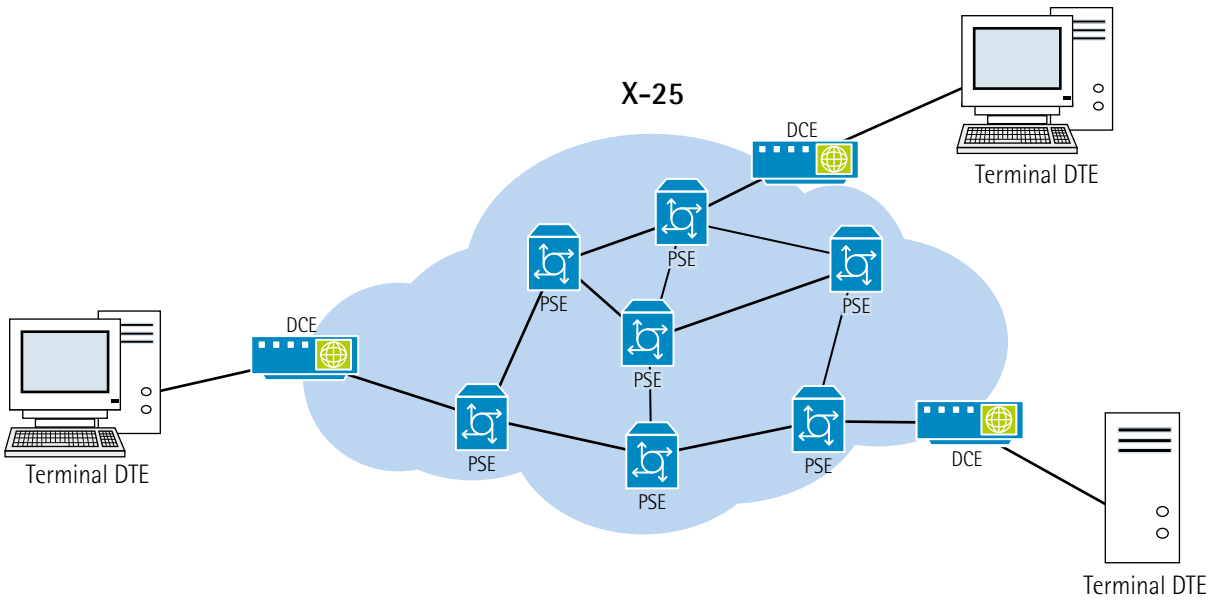

Figura 1 – Topologia da rede X-25

1.1.5 *Packet assembler/disassembler*

Um equipamento coadjuvante no processo de transmissão de dados da rede X-25 é o PAD (*packet assembler disassembler*), usado no momento que um equipamento de terminal de usuário não implementa completamente as funções do X-25. O PAD que fica localizado entre o terminal do usuário e o terminal de discagem possui três funções principais:

- bufferização;
- construção;
- desconstrução dos pacotes X-25.

A bufferização é uma área usada para gravar dados até que os equipamentos de terminal de usuário e de transmissão interna da rede estejam prontos a processar os dados. Sua função clássica é realizar o *packet assembler*, ou construção do pacote, e o *packet disassembler*, ou desconstrução do pacote.

Os dados do *buffer* do pacote são transmitidos e recebidos pelos equipamentos de terminal de usuário. Ele também constrói os dados da saída dos pacotes e os envia para o equipamento de discagem (DCE), sendo também responsável pela inclusão do cabeçalho X-25. Finalmente, o *packet disassembler* é responsável pela desconstrução dos pacotes recebidos antes de enviar o equipamento do usuário na ponta remota.

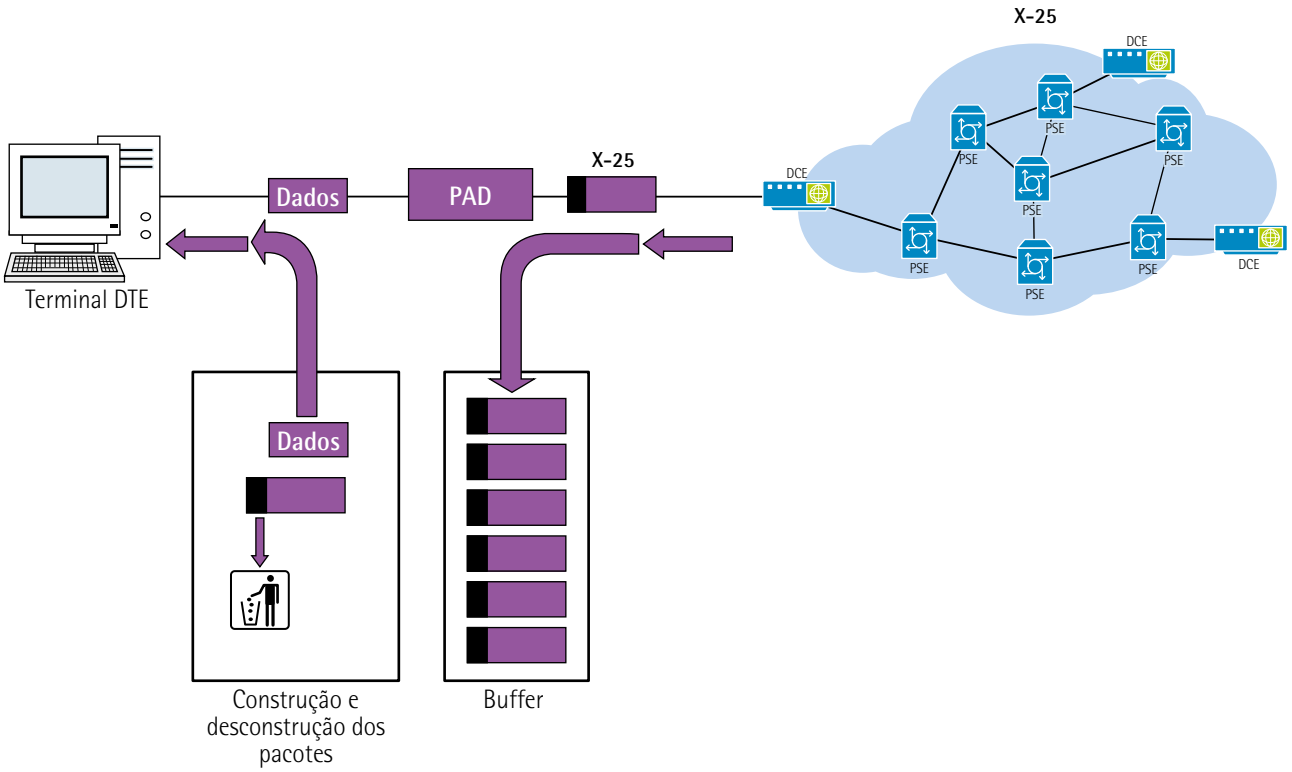

Figura 2 – Construção e desconstrução do PAD em redes X-25

1.1.6 Estabelecimento das sessões X-25

Invariavelmente, as sessões X-25 são estabelecidas quando o equipamento de usuário terminal contrata outro e solicita uma sessão para sua transmissão de dados. Os equipamentos terminais de usuário recebem essa solicitação e podem, nesse momento, aceitar ou recusar a conexão. Se tal solicitação é aceita, os dois sistemas iniciam o processo de transferência de informações no formato *full duplex*. A qualquer instante, qualquer um dos dois equipamentos envolvidos na transmissão pode encerrar a sessão. Depois que a sessão é encerrada, uma nova comunicação é necessária para o restabelecimento de uma nova transmissão de dados.

1.1.7 Os circuitos X-25

O circuito virtual é uma conexão lógica que é criada para possibilitar a comunicação entre dois equipamentos dentro de uma rede. Ele compreende a existência de um caminho lógico bidirecional dentro da nuvem da operadora que permite a comunicação de dados de um comunicando, um terminal de usuário para outro, no formato da rede X-25.

Se observarmos a estrutura física de uma rede X-25, podemos perceber que a comunicação e os circuitos passam por diversos nós intermediários compostos de *modems*, retransmissores e *switches* que são usados como encaminhadores de dados. Múltiplos circuitos virtuais ou conexões lógicas podem ser multiplexados em um único circuito físico ou uma única conexão física, então os circuitos virtuais são demuplexados na ponta remota, e os dados serão enviados aos usuários terminais em seu destino. Observe, na figura a seguir, o exemplo de demuplexação e multiplexação dos circuitos para os X-25.

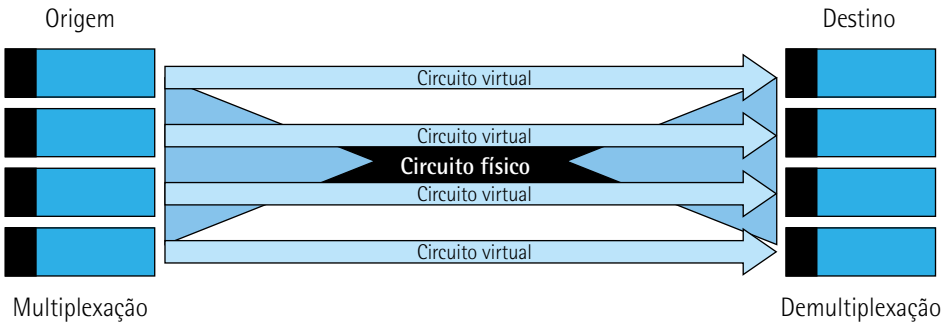

Figura 3 – Multiplexação e demuplexação sobre circuitos X-25

Existem dois tipos virtuais: os dinâmicos e os permanentes. Os virtuais dinâmicos, chamados de SVC (*switched virtual circuit* ou circuito virtual comutado), são circuitos temporários usados na transferência de dados de forma esporádica. Seu funcionamento depende de dois equipamentos de terminal de usuário que estabeleçam, mantenham e encerrem sua sessão toda vez que houver a necessidade de enviar dados de um lado a outro. Já os circuitos permanentes são conexões estabelecidas permanentemente, usadas para transferência dos dados de uma forma constante. Eles são chamados de PVC (*permanent virtual circuit* ou circuitos virtuais permanentes) e, ao contrário dos dinâmicos, não precisam estabelecer ou iniciar uma sessão e também não precisam terminar uma sessão ao fim da transferência dos dados, pois estarão sempre ativos.

A transferência básica em formato X-25 começa quando um equipamento terminal de usuário, de uma origem específica, acionar um circuito virtual, que deve ser usado como cabeçalho, integrado a cada pacote de dados, ao enviar esse pacote para o equipamento de discagem (DCE) no qual ele está conectado. A partir desse ponto, o equipamento (DCE) examina esse cabeçalho para determinar em qual circuito virtual ele será enviado.

Nesse ponto, o PSE interno da nuvem recebe o datagrama vindo do terminal de discagem da borda da nuvem (DCE), examina o cabeçalho e o encaminha ao devido circuito até o próximo equipamento PSE X-25. Esse datagrama, então, passa por todos os equipamentos (PSEs) envolvidos do circuito, até chegar ao destino final. Quando ele chega ao destino final, o último equipamento de discagem tem a tarefa de desconstruir o datagrama X-25 e entrega ao terminal DTE de destino.

1.1.8 O protocolo X 25

Apenas as três primeiras camadas do modelo OSI – a camada física, a camada de enlace e camada de rede – são operáveis na tecnologia X-25. Podemos identificar na camada física os seguintes protocolos que atuam no X-25.

- X-21;
- RS-232;
- EIA-449;

- EIA-530;
- G-703.

Podemos, também, identificar que na camada 2, camada de enlace, existe a presença apenas do protocolo LAPB.

Já na camada 3, camada de rede, o protocolo atuante para as redes X-25 é o PLP.

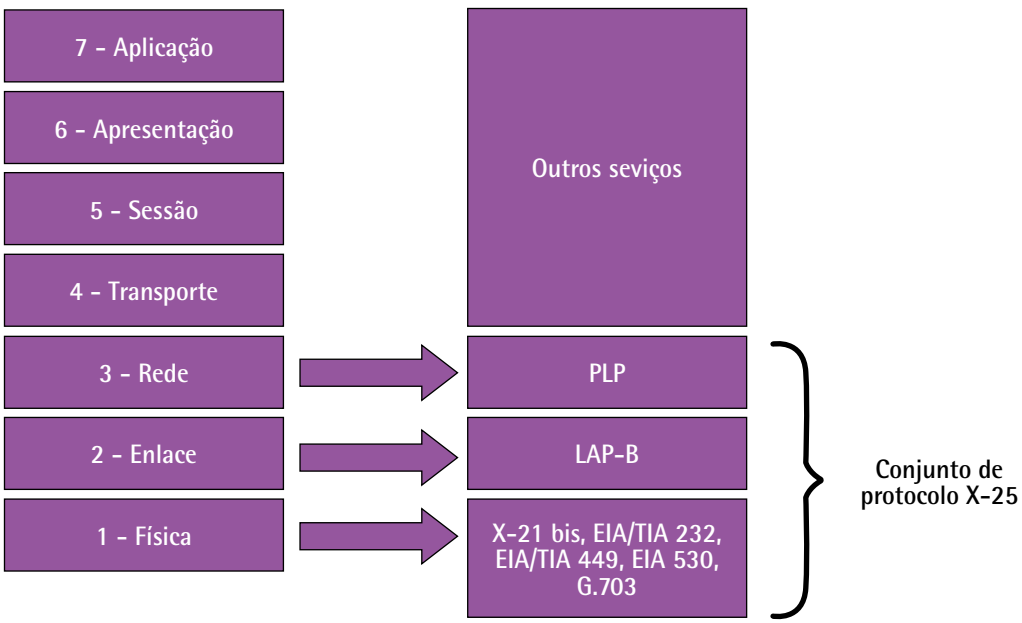

Figura 4 – Comparação do modelo OSI e as camadas para o X-25

1.1.9 O PLP

O PLP é a camada de rede existente no protocolo X-25. Ele gerencia a troca de pacotes entre os equipamentos terminais de usuário orientado pelos circuitos virtuais. O PDP também pode existir sobre a implementação do LLC2 (*logical link control*) em redes locais e sobre a interface dos serviços digitais de redes integradas ISDN (*integrated services digital network* ou rede digital de serviços integrados), rodando sobre a camada 2 do protocolo LAPB.

O PLP possui cinco modos de operação:

- *call setup*;
- *data transfer*;
- *idle*;

- *call clearing*;
- *restarting*.

O PLP também integra quatro tipos de campos para o pacote de dados:

- GFI (*general format identifier*): identifica os pacotes, se há dados de usuário, dados de controle, tipos de janelas e se é necessária a confirmação do pacote.
- LCI (*logical channel identifier*): identifica o circuito virtual através da interface local DTE/DCE.
- PTI (*packet type identifier*): identifica o pacote como um dos 17 tipos diferentes de pacotes PLP.
- *User data*: contém dados de usuário das camadas superiores.

1.1.10 O LAPB

O LAPB é um protocolo de camada de 2. Essa camada de dados é responsável pelo gerenciamento e comunicação entre os equipamentos de terminal de usuário (DTE) e os equipamentos terminais de discagem (DCE) da borda da nuvem. O LAPB é um protocolo orientado a conexão que deve identificar se os datagramas estão corretamente ordenados e livres de erros.

Existem três tipos de quadros usados no LAPB: o *information*, o *supervisor* e o *unnumbered*.

O quadro *information* transporta as informações das camadas superiores e também algumas informações do controle à função do campo. Esse quadro ainda inclui a sequência, o controle de fluxo, a detecção de erros e sua eventual correção. O canto informação também envia os cremes de dados sequenciais enumerados.

O quadro *supervisor* transporta as informações da rede, tais como requisição e suspensão de transmissão. Ele faz o relatório de *status* e a confirmação do recebimento dos quadros de informação e dos números sequenciais recebidos.

O quadro *unnumbered* transporta as informações do controle da rede, como *setup* do *link*, desconexão e relatório de erros. Ele não trafega números sequenciais.

Saiba mais

Você pode explorar mais conteúdo sobre o protocolo X-25, acessando o website do ITU-T:

<https://www.itu.int/en/ITU-T/Pages/default.aspx>.

1.1.11 O protocolo X-21 Bis

O protocolo X-21 é um protocolo da camada física usado com frequência nas conexões para definir os procedimentos elétricos e mecânicos usados especificamente para o meio físico, ou seja, para a ativação e desativação das conexões junto ao meio físico.

Responsável pela conexão dos equipamentos terminais de usuário e os equipamentos terminais de discagem, ele suporta conexões do tipo ponto a ponto. Sua velocidade é de 19,2 quilômetros por segundo no formato 5; na transmissão dos dados, é *full-duplex* e opera sobre quatro fios ou dois pares de fios metálicos.

A figura a seguir mostra um comparativo do protocolo RFB em relação ao protocolo físico X-21 Bis.

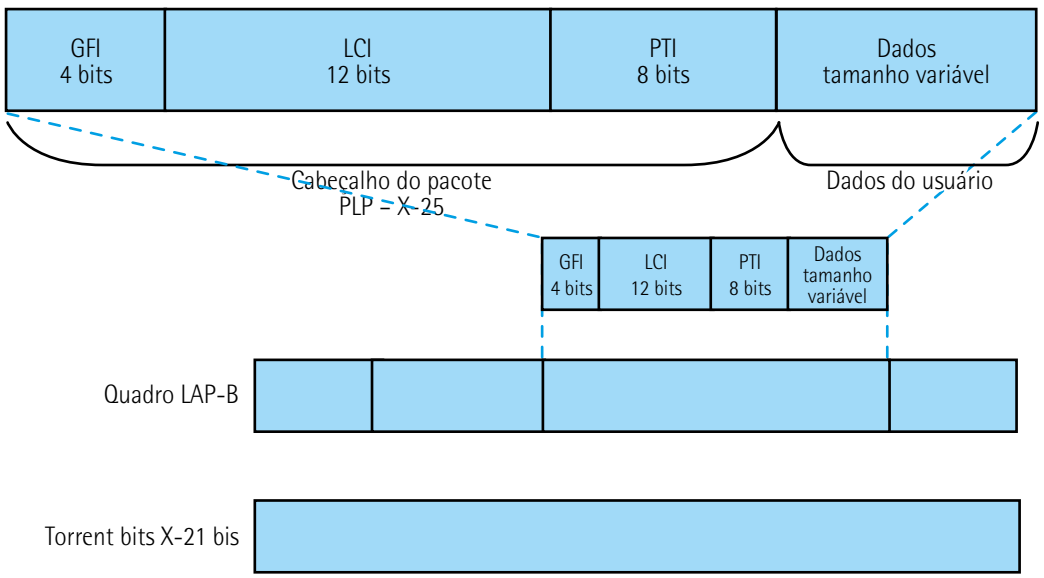

Figura 5 – Trailer do datagrama X-25

1.1.11.1 O formato do quadro LAPB

O quadro LAPB possui um cabeçalho (*header*), dados encapsulados e elementos de demarcação (*flags*) de início e de fim. A ilustração que segue mostra o formato do frame LAPB e a sua relação com o pacote PLP e o frame X-21 Bis.

Os campos LAPB:

- *Flag*: delimita o começo e o fim do frame LAPB.
- *Address*: indica se o *frame* transporta um comando ou uma resposta.
- *Control*: qualifica *frame* de resposta e comando e indica se o *frame* é um I-frame (dados), S-frame ou U-frame, ambos de controle. Esse campo também contém o número de sequência e a sua função (por exemplo, se é um *disconnect*).

- *Data*: contém dados da camada superior em formato de um pacote PLP encapsulado.
- FCS: verifica erro e garante integridade dos dados transmitidos.

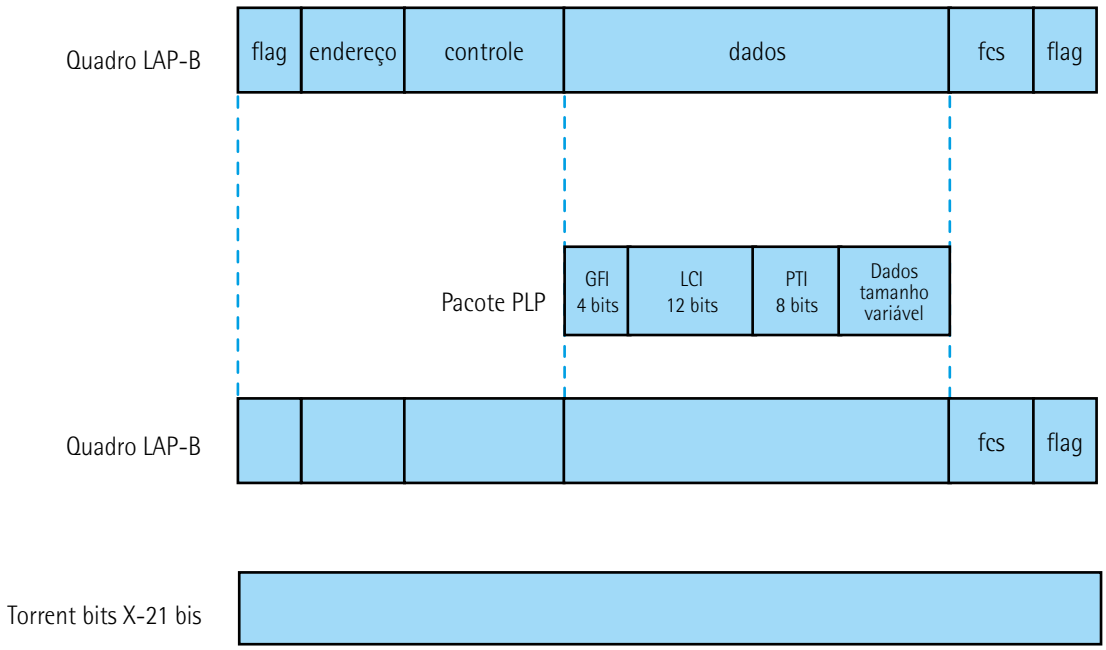

Figura 6 – Campos do pacote LAP-B

1.1.11.2 Endereço: o formato X-121

Os endereços X-121 são usados pela camada PLP do protocolo X-25, mais precisamente no *setup* da chamada para estabelecer SVCs (*switched virtual circuit* ou circuito virtual dinâmico). A ilustração a seguir mostra o formato do endereço X-121.

O campo do endereço X-121 inclui o IDN (*international data number*), que consiste em dois campos: o DNIC (*data network identification code*) e o NTN (*national terminal number*).

O DNIC é um campo opcional que identifica o valor correto para o PSN, que mostra a localidade do equipamento DTE de destino.

Já o NTN identifica o exato equipamento DTE no PSN para o qual o pacote é destinado.

Lembrete

O modelo X-25 foi baseado no conceito de telefonia tradicional para estabelecer circuitos confiáveis por meio de uma rede compartilhada, mas usando *software* para criar "chamadas virtuais" através da rede. Essas chamadas interconectam equipamentos de terminal de dados (DTE)

fornecendo pontos de extremidade aos usuários, que se assemelham a conexões ponto a ponto. Cada ponto de extremidade pode estabelecer muitas chamadas virtuais separadas para diferentes pontos.

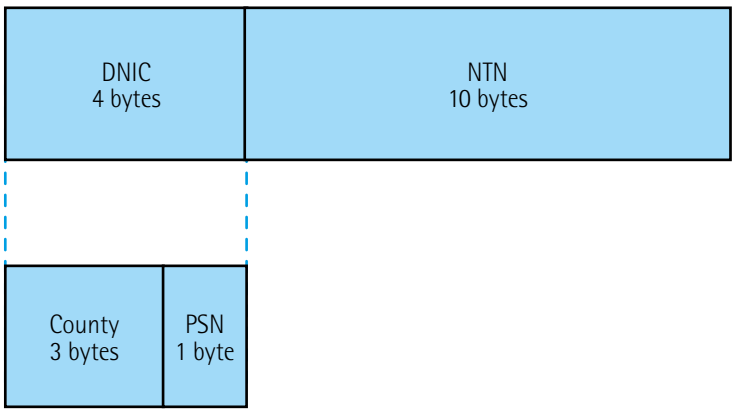

Figura 7 – Detalhe do pacote NTN

1.2 A tecnologia de rede ponto a ponto

1.2.1 A rede ponto a ponto

No fim da década de 1980, o protocolo SLIP (*serial line internet protocol*) promovia uma limitação do crescimento da internet. O protocolo PPP (ponto a ponto ou *point per point*) chegou para resolver problemas de conectividade remota com a internet. Ainda, o ponto a ponto foi um importante meio para a atribuição de endereços IP de forma dinâmica a distância e ainda permite o uso de vários protocolos adjacentes.

O ponto a ponto atribui conexões de roteador para roteador e conexões de *host* para rede por circuitos síncronos e assíncronos.

O ponto a ponto é um protocolo da WAN muito popular e abrangente, porque oferece todos os seguintes recursos:

- Controle de configuração de enlace de dados.
- Atribuição dinâmica de endereços IP.
- Multiplexação do protocolo de rede.
- Configuração de *link* e teste de qualidade do *link*.
- Detecção de erros.
- Opções de negociação para recursos como a negociação de endereços da camada de rede e as negociações de compactação de dados.

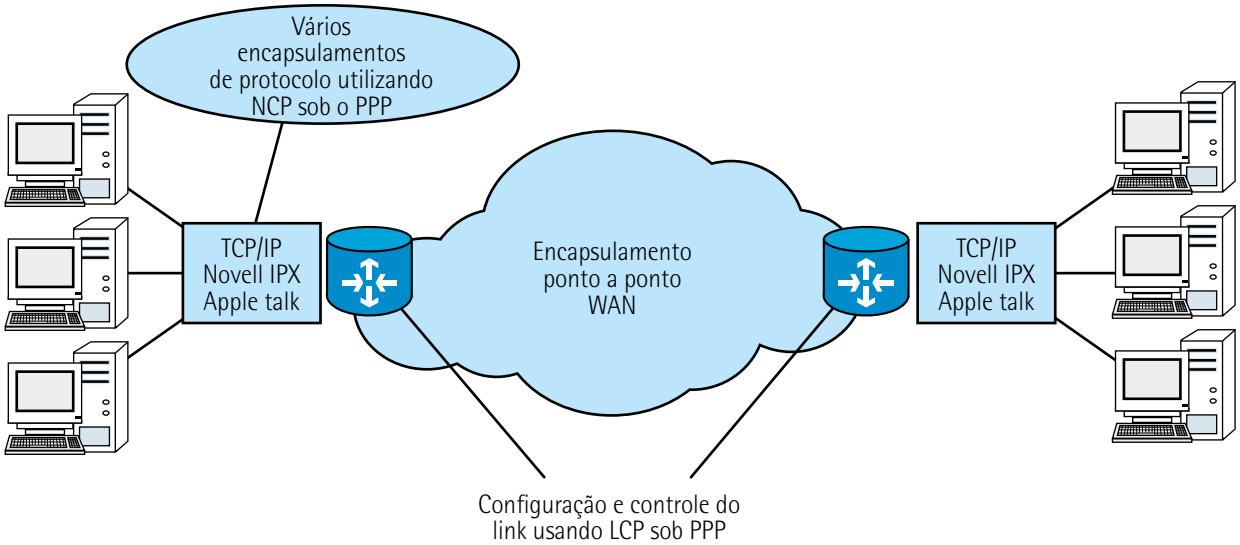

Figura 8 – Arquitetura de protocolos ponto a ponto

O ponto a ponto usa uma arquitetura em camadas. Com suas funções de nível inferior, o ponto a ponto pode usar:

- Meios físicos síncronos: como os que conectam redes ISDN (*integrated services digital network*).
- Meios físicos assíncronos: como os que usam o serviço básico de telefonia para conexões *dial-up* de *modem*.

Com suas funções de nível superior, o ponto a ponto suporta ou ainda encapsula vários protocolos da camada de rede usando placas de rede. Esses protocolos de camada superior incluem:

- BCP (*bridge control protocol*).
- IPCP (*internet protocol control protocol*).
- IPXCP (*internetwork packet exchange control protocol*).

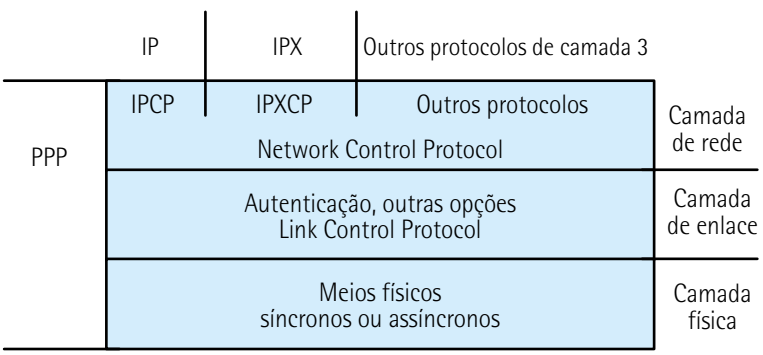

Figura 9 – Arquitetura ponto a ponto

A seguir, temos um diagrama da aplicação dos campos funcionais que contém códigos padronizados, sobretudo para indicar o tipo do protocolo da camada de rede que o ponto a ponto encapsula:

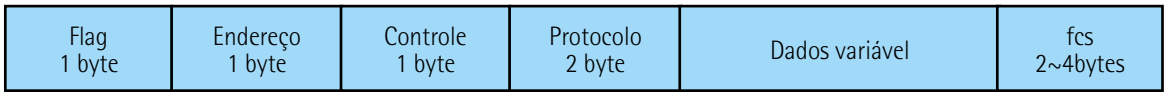

Figura 10 – *Trailer* do datagrama do protocolo LAP-D

Definição dos campos:

- *Flag*: indica o começo ou o fim de um quadro e consiste na sequência binária 01111110.
- Endereço: consiste no endereço de *broadcast* padrão, que é a sequência binária 11111111.
- Controle: 1 *byte* que consiste na sequência binária 00000011, que requer a transmissão de dados do usuário em um quadro sem sequência. É oferecido um serviço de *link* sem conexão similar ao do LLC (*logical link control*) Tipo 1.
- Protocolo: 2 *bytes* que identificam o protocolo encapsulado no campo de dados do quadro.
- Dados: 0 ou mais *bytes* que contêm o datagrama para o protocolo especificado no campo de protocolo. Ao final do campo de dados encontramos uma sequência de *flags* de fechamento, sendo deixados 2 *bytes* para o campo FCS (*frame check sequence*). O tamanho máximo padrão do campo de dados é de 1.500 *bytes*.
- FCS (*frame check sequence* ou quadro de checagem da sequência): normalmente, 16 *bits* (2 *bytes*). É recomendável observar a presença de caracteres extras adicionados a um quadro para fins de controle de erros.

1.2.2 As fases do protocolo ponto a ponto

O protocolo ponto a ponto atende a requisitos do método de estabelecimento, configuração, manutenção e encerramento de uma conexão ponto a ponto. Para estabelecer comunicações mediante um *link* ponto a ponto, o ponto a ponto passa por quatro fases distintas:

- Negociação da configuração e estabelecimento do *link*: um nó ponto a ponto de origem envia quadros LCP para configurar e estabelecer o enlace de dados.
- Determinação da qualidade do *link*: o *link* é testado para determinar se sua qualidade é suficiente para ativar os protocolos da camada de rede. Observe que essa é uma fase opcional.
- Negociação da configuração do protocolo da camada de rede: o nó ponto a ponto de origem envia quadros NCP para escolher e configurar protocolos da camada de rede. Os protocolos da camada de rede escolhidos, como IP, Novell IPX e AppleTalk, são configurados, e os pacotes de cada protocolo da camada de rede podem ser enviados.

- Encerramento do *link*: o *link* permanece configurado para as comunicações até que os quadros LCP ou NCP fechem o *link* ou até que ocorra algum evento externo (por exemplo, um *timer* de inatividade atinja o tempo limite ou um usuário intervenha).

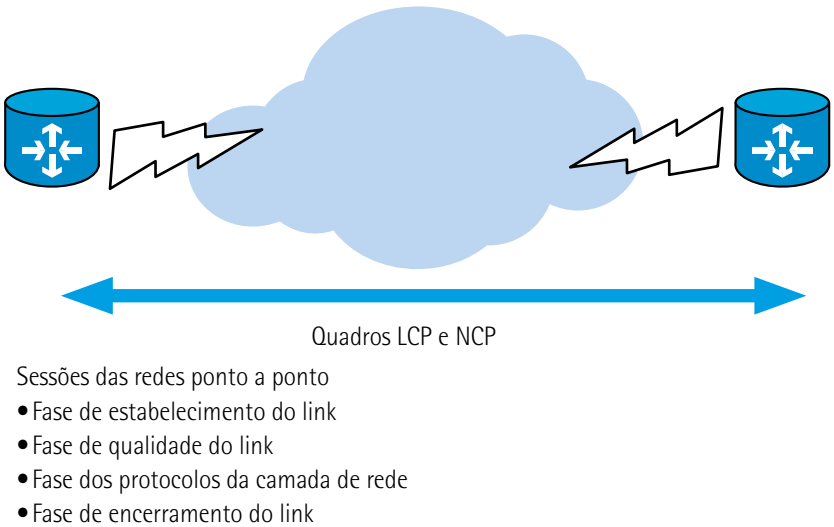

Figura 11 – Fases do estabelecimento de conexões ponto a ponto

1.2.2.1 As três classes dos quadros LCP

O LCP (*logical control protocol* ou controle lógico de protocolo) possui três classes de enquadramento para atender às fases de operação do protocolo ponto a ponto, que são:

- Quadros de estabelecimento de *link*: usados para estabelecer e configurar um *link*.
- Quadros de encerramento de *link*: usados para encerrar um *link*.
- Quadros de manutenção de *link*: usados para gerenciar e fazer o *debug* de um *link*.

Estes quadros LCP são usados para realizar o trabalho de cada uma das fases LCP:

1. Estabelecimento do *link*.
2. Qualidade do *link*.
3. Protocolo da camada de rede.
4. Encerramento do *link*.

Na fase de negociação da configuração e estabelecimento do *link*, cada elemento/dispositivo ponto a ponto envia pacotes LCP para configurar e estabelecer o enlace de dados.

1.2.3 O encadeamento das fases de LCP

Os pacotes LCP possuem um campo de opção de configuração que dá permissão de os dispositivos negociarem o uso de opções, como MTU (*maximum transmission unit*), compactação de determinados campos ponto a ponto e protocolo de autenticação de *link*.

Caso uma das opções de configuração não esteja incluída em um pacote LCP, consideramos o valor padrão para essa opção de configuração.

Ainda, antes que qualquer datagrama da camada de rede (por exemplo, IP) seja trocado, o LCP deve, primeiro, verificar a conexão e negociar os parâmetros de configuração.

Essa fase deverá estar concluída quando um quadro de confirmação da configuração for enviado ou recebido. O LCP permite a existência de uma fase de determinação da qualidade do *link*, em caráter opcional, após a fase de estabelecimento do *link* e negociação da configuração.

Na fase de determinação da qualidade do *link*, ele é testado para determinar se a sua qualidade é suficiente para ativar os protocolos da camada de rede.

Ainda, após o estabelecimento do *link* e o protocolo de autenticação ser escolhido, a estação de trabalho do usuário ou cliente pode ser autenticada. A autenticação, se usada, ocorre antes do início da fase de configuração do protocolo da camada de rede.

O LCP pode atrasar a transmissão das informações do protocolo da camada de rede até essa fase ser concluída.

1.2.4 A autenticação do protocolo ponto a ponto

O ponto a ponto suporta dois protocolos de autenticação: PAP (*password authentication protocol*) e Chap (*challenge handshake authentication protocol*). Esses protocolos estão detalhados no RFC 1334 – PPP Authentication Protocols, na fase de negociação da configuração e estabelecimento do *link*.

As opções de autenticação solicitam que o lado do *link* que faz a chamada inicie com informações de autenticação, para reforçar a garantia de que o usuário tenha a permissão do administrador de rede para fazer a chamada. Os roteadores pares trocam mensagens de autenticação.

Na fase de autenticação, o protocolo ponto a ponto poderá selecionar o PAP ou o Chap. Em geral, o Chap é o protocolo preferencial.

Lembrete

O PPP é comumente usado como um protocolo de camada de enlace de dados para conexão em circuitos síncronos e assíncronos, onde ele predominou sobre o antigo protocolo de linha serial internet (SLIP) e as normas mandatadas pelas operadoras de telefonia, como o protocolo de acesso à ligação, equilibrada (LAPB) no conjunto de protocolos X-25. O único requisito para PPP é que o circuito fornecido deve ser duplex. O PPP foi projetado para funcionar com inúmeros protocolos de camada de rede, incluindo protocolo de internet (IP), pacotes Novell (IPX), NBF, DECnet e AppleTalk. Como SLIP, esta é uma conexão de internet completa através de linhas telefônicas via *modem*. É mais confiável nas questões de tráfego e segurança porque ele verifica duas vezes a passagem dos pacotes, para se certificar de que os pacotes de internet cheguem intactos. Ele promove o reenvio de todos os pacotes incompletos ou danificados.

1.2.4.1 O protocolo PAP

O protocolo PAP fornece um método simples para que a entidade de um nó remoto estabeleça sua identidade, usando o *handshake* duplo. No final da fase de estabelecimento do *link* ponto a ponto, uma sequência par nome do usuário/senha é enviada repetidamente pelo nó remoto pelo *link* até que ocorra a confirmação da autenticação ou a conexão seja encerrada.

O PAP não é um protocolo de autenticação eficiente. O motivo principal é que as senhas são enviadas pelo *link* em texto claro e não existe qualquer tipo de proteção contra reprodução ou contra ataques sucessivos de tentativa e erro. O nó remoto controla a frequência e a temporização das tentativas de *logon*, então o LCP deve, primeiro, abrir a conexão. Essa fase será concluída quando um quadro de confirmação da configuração tiver sido enviado ou recebido. O LCP permite haver uma fase de determinação da qualidade do *link* opcional após a fase de estabelecimento do *link* e negociação da configuração.

O Chap é usado para verificar periodicamente a identidade do nó remoto, usando um *handshake* triplo. Isso é feito no momento do estabelecimento inicial do *link* e pode ser repetido a qualquer momento depois que o *link* tiver sido estabelecido. O Chap oferece recursos como a verificação periódica para melhorar a segurança, o que torna o Chap mais eficiente do que o PAP. O PAP só faz a verificação uma vez, o que o torna vulnerável à reprodução de *modem* e à ação de *hackers*. Além disso, o PAP permite que o usuário que faz a chamada tente obter a autenticação quando desejar (sem antes receber um desafio), tornando-o vulnerável aos ataques violentos, enquanto o Chap não permite que o usuário que faz a chamada tente obter uma autenticação sem um desafio.

Após a conclusão da fase de estabelecimento do *link* ponto a ponto, o *host* envia uma mensagem de desafio ao nó remoto. O nó remoto responde com um valor, e o *host* compara a resposta com seu próprio valor. Se o valor corresponde, a autenticação é confirmada. Do contrário, a conexão é encerrada.

1.2.4.2 O protocolo Chap

O protocolo Chap é uma versão mais requintada do protocolo PAP. Ele oferece proteção contra ataques de reprodução mediante o uso de um valor de desafio variável que é exclusivo e imprevisível.

O uso de desafios repetidos visa limitar o tempo de exposição a qualquer ataque. O roteador local (ou qualquer outra entidade de autenticação, como o Netscape Commerce Server), entidade que detém, na camada de aplicação, o controle do desafio de autenticação, determina a frequência e a temporização dos desafios.

1.2.4.3 O cenário de autenticação PAP/Chap

Aqui temos o registro do uso do protocolo PAP/Chap na negociação e na autenticação de entidades em ambiente ponto a ponto. Esses registros mostram as evidências do processo de autenticação em momento/fase na negociação da autenticação que ocorre na camada enlace e também o desdobramento da continuidade de transmissão de mensagens usando o protocolo em questão.

Seguem exemplos de transações na fase de autenticação do protocolo ponto a ponto.

Registro de chamada

O roteador identificado como 766-1 inicia uma chamada discada ao receptor 3640-1:

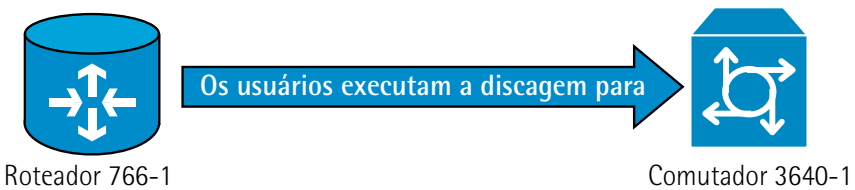

Figura 12 – Fases do estabelecimento do *dial-in*

O diagrama mostra essas etapas:

- A chamada é recebida em 3640-1. A interface de entrada é configurada com o comando ppp authentication chap.
- O LCP negocia Chap e MD5 para obter mais informações sobre como determiná-la.
- Um desafio da Chap de 3640-1 para o roteador de chamada é necessário nessa chamada.

Registro de desafio

Segue a atribuição do desafio proposto neste diagrama entre as entidades 766-1 e 3646-1:

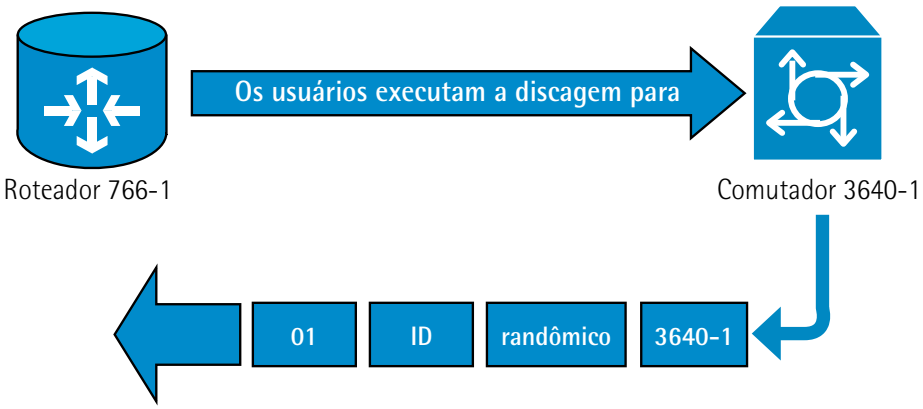

Figura 13 – Desafio Chap

A figura apresentada nos mostra as etapas na autenticação de Chap entre os dois roteadores:

- Um pacote de desafio de Chap é criado com as seguintes características:
  - 01: identificador do tipo de pacote de desafio.
  - ID: o número sequencial que identifica o desafio.
  - *Random*: um número razoavelmente aleatório gerado pelo roteador.
  - 3640-1: o nome de autenticação do desafiante.
- A identificação e os valores aleatórios são mantidos no roteador chamado.
- O pacote de desafio é enviado para o roteador de chamada. Uma lista dos desafios mais importantes é mantida.

Registro de resposta

Interceptação do procedimento de cifra no formato MD5 no intercâmbio de mensagens dos pares 766-1 e 3640-1:

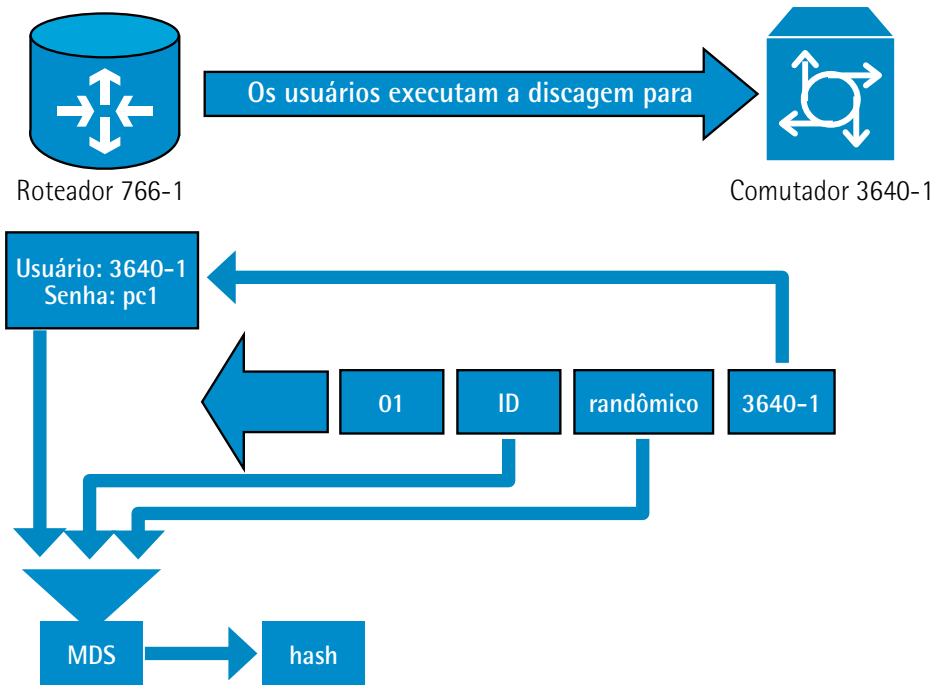

Figura 14 – Formação da cifra MD5 para um pacote Chap em redes ponto a ponto

A figura apresentada nos mostra como o pacote de desafio é recebido do "ponto" e como é processado pela cifra (MD5). O roteador processa o pacote de desafio de Chap de entrada da seguinte maneira:

- O valor ID é colocado no gerador de *hash* MD5.
- O valor *random* é colocado no gerador de *hash* MD5.

O nome 3640-1 é usado para procurar a senha. O roteador procura uma entrada que corresponda ao nome de usuário no desafio.

Nesse exemplo, ele procura:

- username 3640-1 password pc1.

A senha é alimentada no gerador de *hash* MD5.

O resultado é o desafio de Chap com *hash* MD5 unidirecional que é enviado novamente na resposta de Chap.

Resposta: próxima fase de autenticação

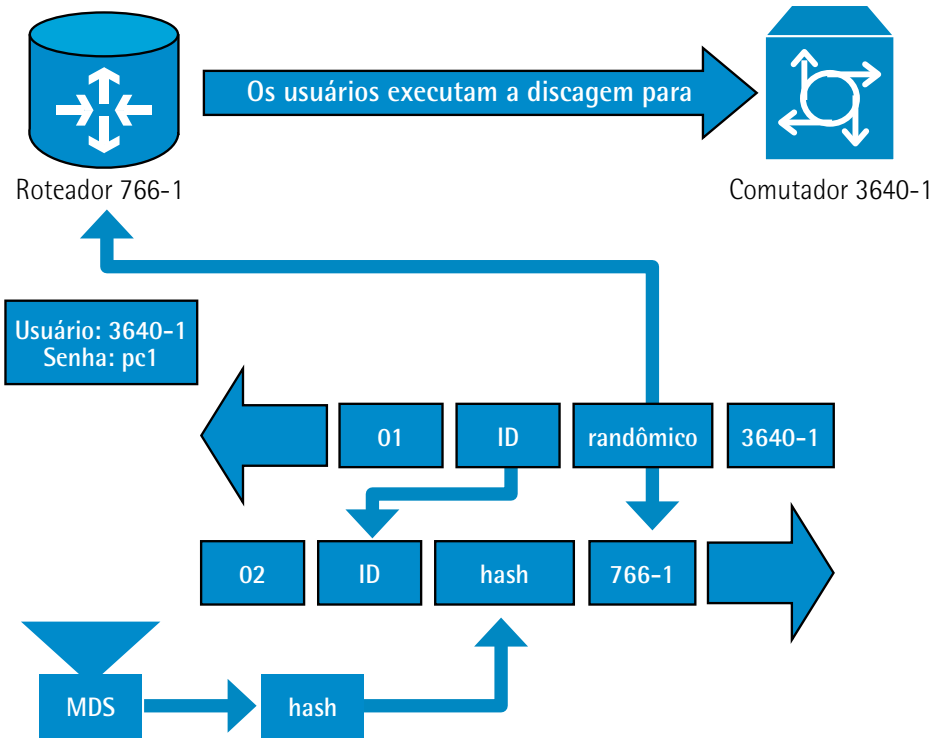

Figura 15 – A formação da cifra MD5 para um pacote Chap fase 2 em redes ponto a ponto

A figura apresentada nos mostra como o pacote de resposta de Chap enviado ao autenticador é criado.

- O pacote de resposta é montado a partir destes componentes:
  - 02: identificador de tipo de pacote de resposta Chap.
  - ID: copiada do pacote de desafio.
  - *hash*: a saída do gerador de *hash* MD5 (as informações misturadas do pacote de desafio).
  - 766-1: o nome de autenticação desse dispositivo. Isso é necessário para que o *peer* procure a entrada de nome de usuário e a senha necessária para verificar a identidade.
- O pacote de resposta é então enviado ao desafiante.

Saiba mais

Você pode conhecer um pouco mais sobre a aplicação do protocolo PAP/Chap em conexões ponto a ponto no *site* de suporte da Cisco Systems:

ENTENDENDO e configurando a autenticação de PPP Chap. *Cisco*. Setembro, 2014. Disponível em: <https://www.cisco.com/c/pt_br/support/docs/wan/point-to-point-protocol-ppp/25647-understanding-ppp-chap.html>. Acesso em: 9 jan. 2018.

Registro de verificação Chap

Modo da verificação do desafio de autenticação do par de entidades 766-1 e 3640-1:

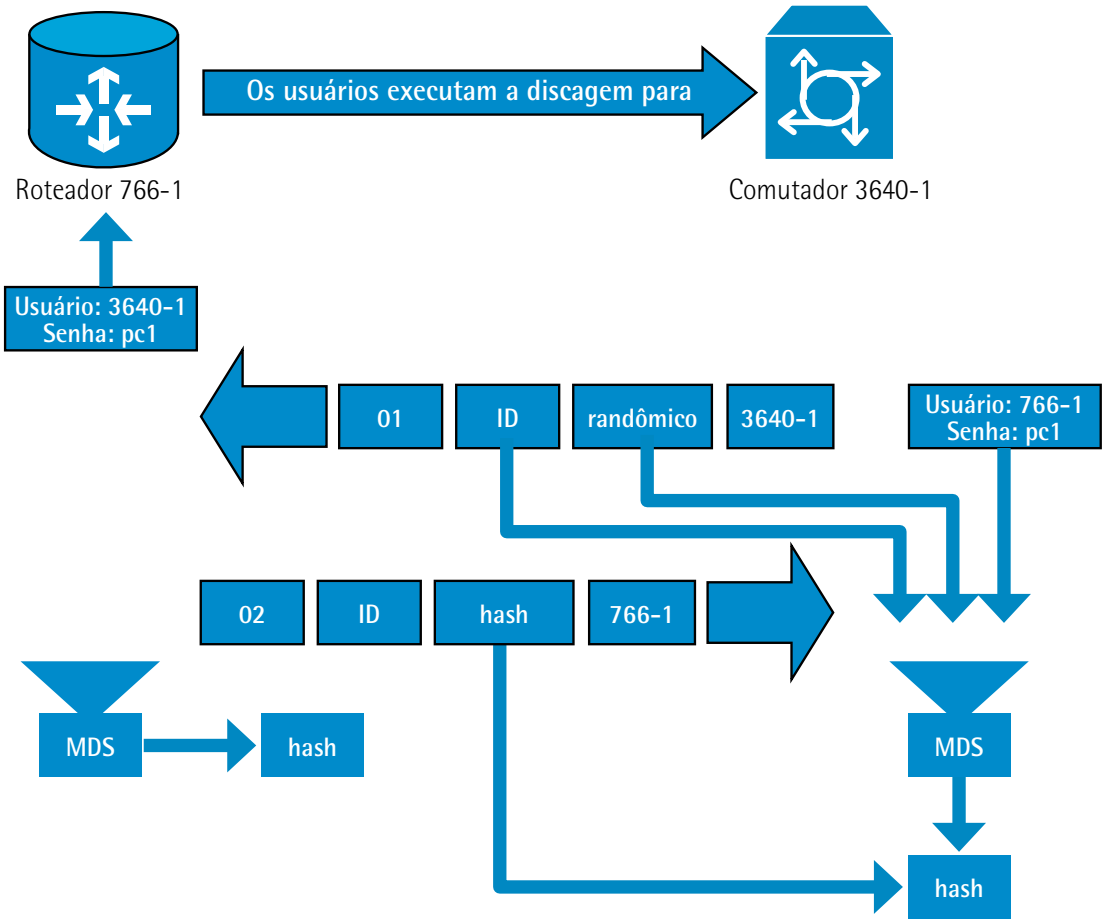

Figura 16 – A formação da cifra MD5 para um pacote Chap fase 3 em redes ponto a ponto

A figura apresentada nos mostra a maneira que o desafiante processa o pacote de resposta. Essas são as etapas envolvidas quando o pacote de resposta de Chap é processado (no autenticador):

- O ID é utilizado para localizar o pacote de desafio original.
- O ID é alimentado no gerador de mistura MD5.
- O valor aleatório do desafio original é alimentado no gerador de *hash* do MD5.

- O nome 766-1 é utilizado para procurar a senha de uma das seguintes fontes:
  - Banco de dados de nome de usuário e senha local.
  - Servidor RADIUS ou TACACS+.
- A senha é alimentada no gerador de *hash* MD5.
- O valor de *hash* recebido no pacote de resposta é comparado ao valor de *hash* MD5 calculado. A autenticação do Chap será bem-sucedida se o valor calculado e o valor de *hash* recebido forem iguais.

Registro de resultado

A imagem a seguir mostra o registro de sucesso na negociação de autenticação Chap entre as entidades 766-1 e 3640-1:

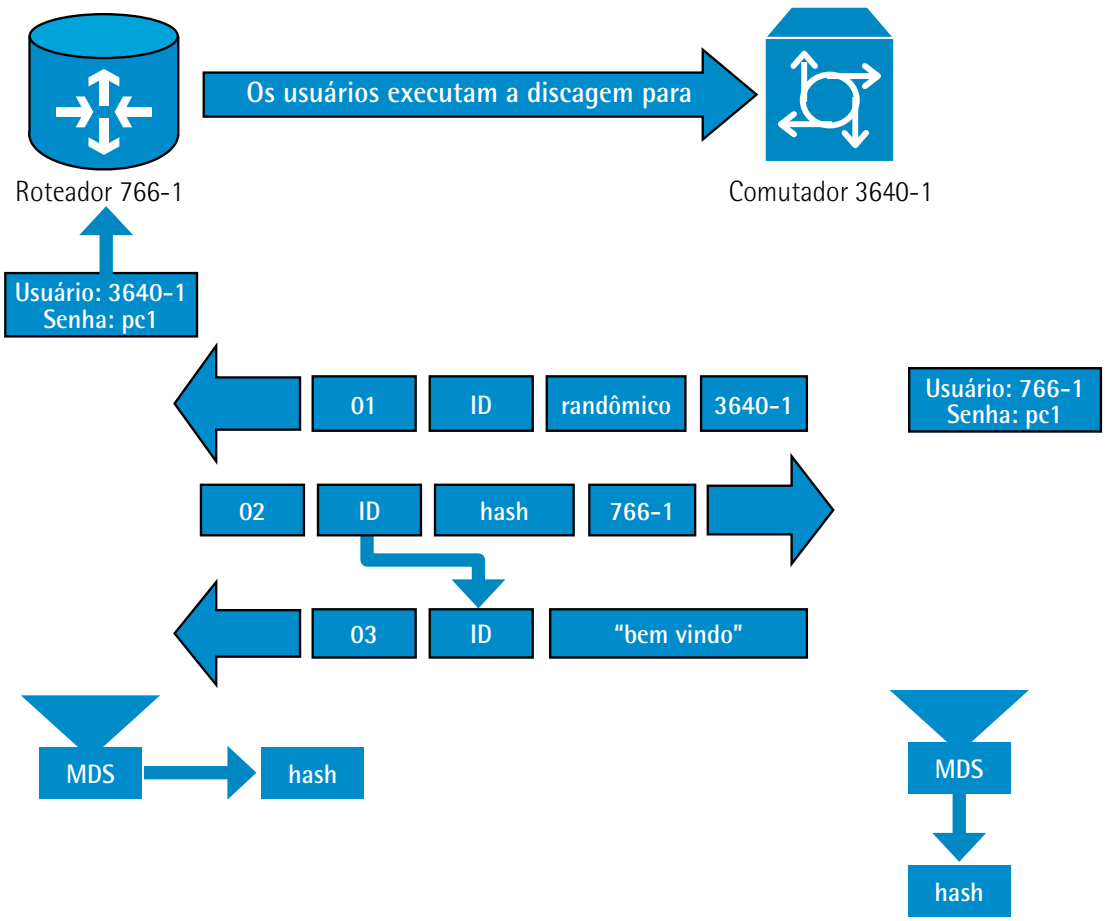

Figura 17 – A formação da cifra MD5 para um pacote Chap fase 4 em redes ponto a ponto

A imagem apresentada nos mostra a mensagem de sucesso enviada ao roteador de chamada. Ela envolve estas etapas:

- Se a autenticação for bem-sucedida, um pacote de sucesso de Chap será criado a partir destes componentes:

  – 03: tipo de mensagem de êxito de Chap.

  – ID: copiada do pacote de resposta.

- O campo da mensagem dá boas-vindas à entidade correspondente. Trata-se de simplesmente uma mensagem de texto que forneça uma explicação legível por usuário.

- Se a autenticação falhar, um pacote de falha de Chap será criado a partir destes componentes:

  – 04: tipo de mensagem de falha de Chap.

  – ID: copiada do pacote de resposta.

  – O campo nos mostra uma falha da autenticação da entidade correspondente, o que nos fornece uma explicação transparente por usuário.

- O pacote com êxito ou com falha é, em seguida, enviado ao roteador de chamada.

Esse exemplo nos mostra uma autenticação unidirecional. Em uma autenticação bidirecional, todo esse processo é repetido. Porém, o roteador de chamada começa o desafio inicial.

Resumo

Observamos nesta unidade a profundidade dos conceitos das redes X-25, que não devem, de forma alguma, serem entendidos como tecnologias do passado. A alta carga de conhecimento da tecnologia da construção dos *trailers* e dos PDUs, sem esquecer os conceitos absorvidos pela formulação dos circuitos virtuais, sejam eles permanentes ou dinâmicos, nos traz informações relevantes para entender os novos momentos da tecnologia da atualidade.

A tecnologia X-25 é um dos mais antigos serviços de comutação de pacotes disponíveis. Foi desenvolvida antes do modelo de referência OSI. O conjunto de protocolos é projetado como três camadas conceituais, que correspondem estreitamente às três camadas inferiores do modelo OSI – este, de sete camadas. O protocolo X-25 foi desenvolvido no grupo VII de estudo ITU-T (anteriormente estava a cargo do CCITT) baseado em vários projetos de rede de dados emergentes.

Várias atualizações e adições foram trabalhadas no padrão e, eventualmente, registradas na série ITU, referenciada em livros técnicos

que descrevem os sistemas de telecomunicações. A especificação X-25 é apenas parte do conjunto maior de especificações da série X em redes de dados públicos. A rede de dados públicos era o nome comum dado à coleção internacional de provedores X-25. Sua rede combinada teve grande cobertura global durante a década de 1980 e 1990. As redes X-25 publicamente acessíveis (CompuServe, Tymnet, Euronet, PSS, Datapac, Datanet 1 e Telenet) foram estabelecidas, na maioria dos países, durante as décadas de 1970 e 1980, para reduzir o custo de acesso a vários serviços *on-line*.

A partir do início da década de 1990, na América do Norte, o uso de redes X-25 (predominantes por Telenet e Tymnet) passaram a ser substituídas por *frame relay*, serviço atual oferecido pelas companhias telefônicas nacionais. A maioria dos sistemas que exigem X-25 atualmente usam TCP/IP, porém é possível transportar X-25 sobre TCP/IP quando necessário. As redes X-25 ainda estão em uso em todo o mundo. Uma variante chamada AX-25 também é amplamente utilizada por rádio amador em formato de redes de pacotes.

As redes ponto a ponto aprimoram nossos conceitos sobre conectividade de longa distância, principalmente na atribuição de circuitos que conectam redes de computadores a outras redes de computadores, em qualquer parte do planeta. Ao aplicar valiosos conceitos das camadas físicas, enlace e redes, podemos materializar cenários complexos e extremamente funcionais, agregando segurança e alta disponibilidade com essa nova formulação de redes.

Exercícios

Questão 1. (AOCP, 2012) O protocolo de autenticação do tipo desafio/resposta, que usa o esquema de *hash* MD5 para criptografar a resposta e requer o uso de uma senha criptografada reversível, é conhecido como:

A) Kerberos.

B) MS-Chap.

C) Tacacs.

D) Chap.

E) NAT.

Resposta correta: alternativa D.

Análise das alternativas

A) Alternativa incorreta.

Justificativa: a Kerberos é um protocolo desenvolvido para fornecer poderosa autenticação em aplicações usuário/servidor, que funciona como a terceira parte nesse processo, oferecendo autenticação ao usuário.

B) Alternativa incorreta.

Justificativa: o MS-Chap é o protocolo Chap (*challenge handshake authentication protocol*) da Microsoft que é baseado em senha e amplamente usado como um método de autenticação nos VPNs baseados em PPTP (*point to point tunneling protocol*).

C) Alternativa incorreta.

Justificativa: o TACACS (*terminal access controller access-control system*) é um protocolo de autenticação remota usado para comunicação com servidores de autenticação, comumente em redes UNIX. TACACS permite que um servidor de acesso remoto se comunique com um servidor de autenticação para verificar se o usuário tem acesso à rede.

D) Alternativa correta.

Justificativa: o Chap (*challenge handshake authentication protocol*) é um protocolo de autenticação de desafio-resposta que usa o esquema de *hash* MD5 (Message Digest 5) padrão da indústria para criptografar a resposta.

E) Alternativa incorreta.

Justificativa: o NAT (*network address translation*) faz a tradução dos endereços IP e portas TCP da rede local para a internet.

Questão 2. (FCC, 2009) O equipamento que proporciona a montagem e desmontagem de pacotes entre redes de transmissão assíncrona e de comutação de pacotes é o:

A) MUX.

B) PSN.

C) PLP.

D) PAD.

E) NAP.

Resolução desta questão na plataforma.