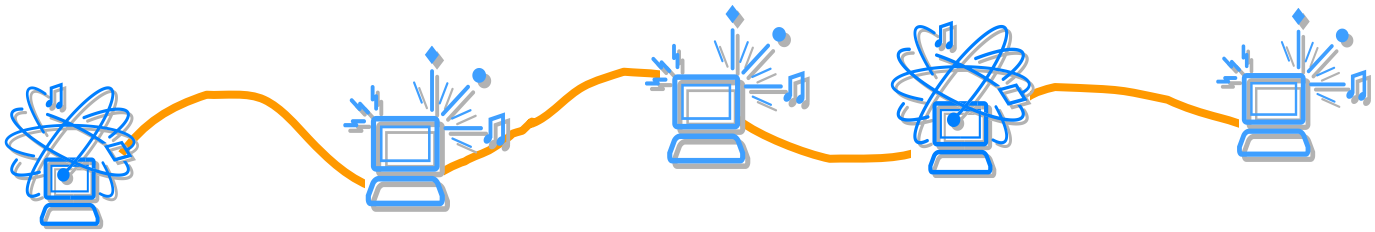
Protocolos de acesso remoto - PPP
PAP, CHAP



Segurança em Redes de Computadores

Redes de Comunicação

PPP – Point to Point Protocol

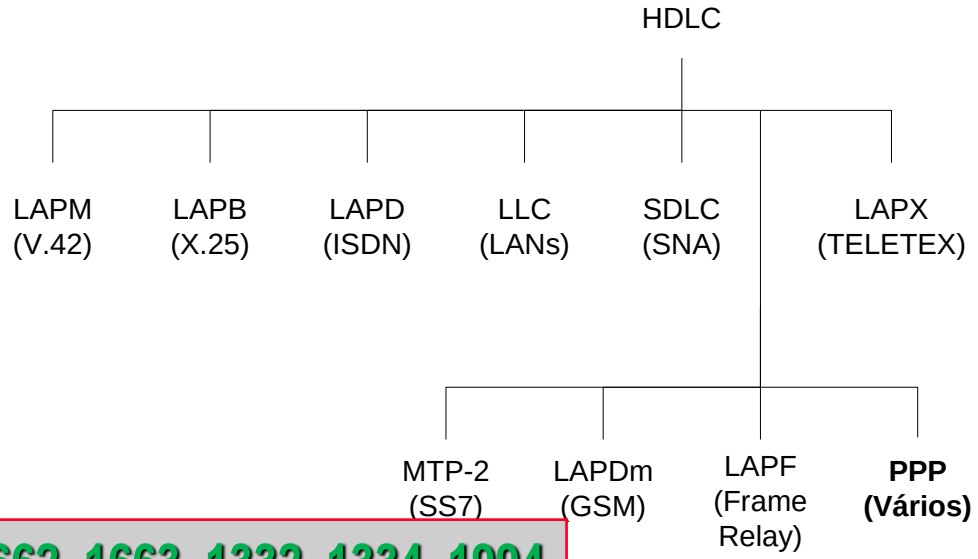
PPP provides three things:

- A framing method that unambiguously delineates the end of one frame and the start of the next one. The frame format also handles error detection.

- A link control protocol for bringing up lines, testing them, negotiating options, and bringing them down gracefully when no longer needed. This protocol is called Link Control Protocol (LCP).

- A way to negotiate network layer options in a way that is independent of the network layer protocol to be used. The method chosen is to have a different Network Control Protocol (NCP) for each network layer supported.

Protocolo PPP (*Point-to-Point Protocol*)

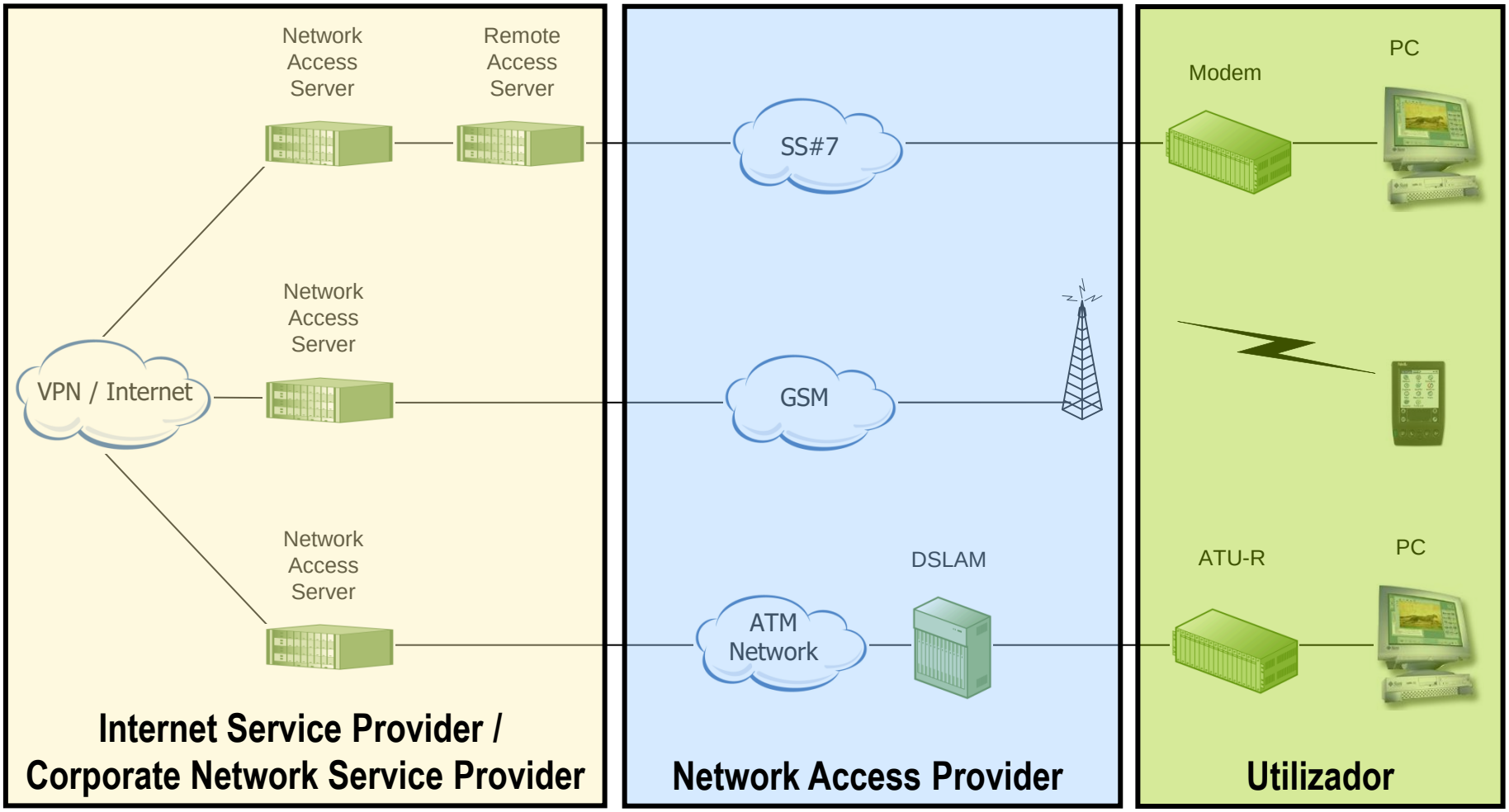


- Oferece um método para encapsular datagramas através de linhas série.
- Permite a comunicação ponto a ponto entre duas máquinas.

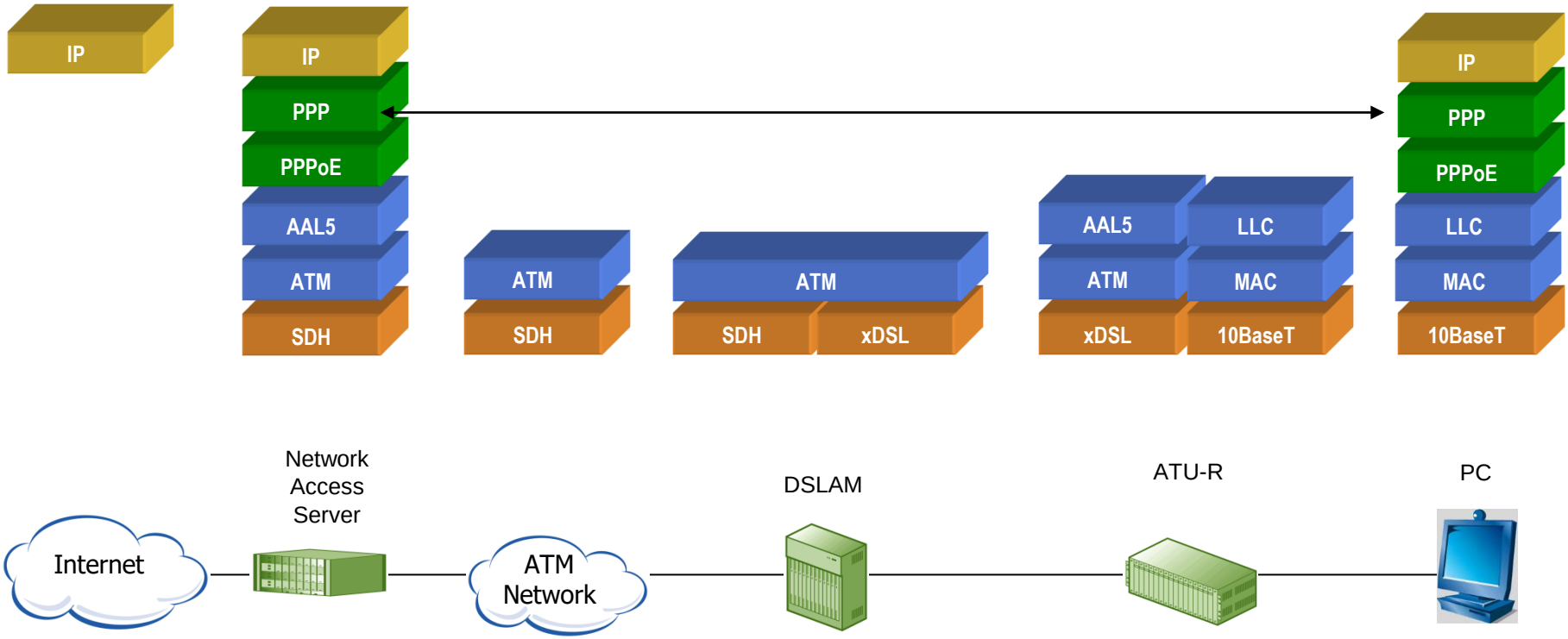
PPP: RFC1661, 1662, 1663, 1332, 1334, 1994

- Permite que as máquinas negoceiem parâmetros para configurar o nível 2 e o nível 3.
- Tipicamente as duas máquinas envolvidas são o terminal do utilizador e uma máquina (NAS – *Network Access Server*) que oferece acesso a uma determinada rede, mas também podem ser dois *routers*.

Acesso remoto a redes



Exemplo de utilização do PPP



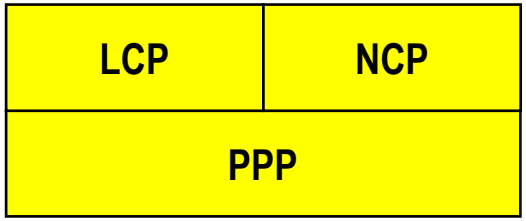
Funções do PPP

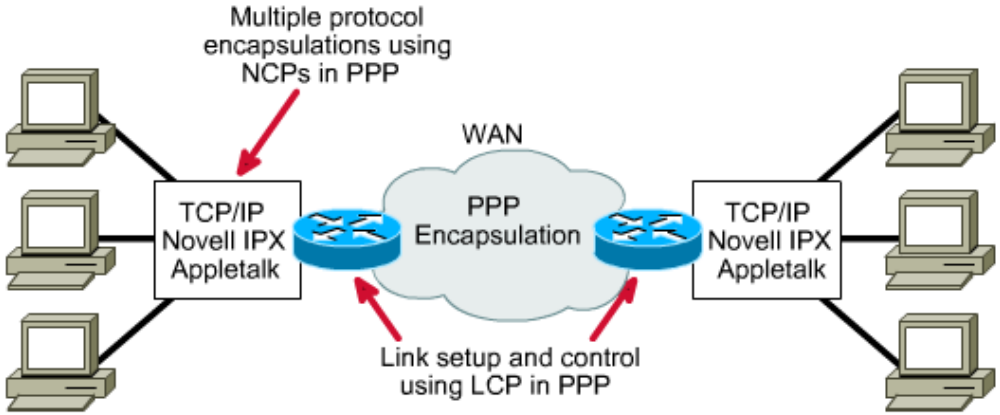
- Controlo do estabelecimento do nível de ligação.
- Multiplexagem de protocolos de rede.
- Configuração da ligação e teste à qualidade da ligação.
- Autenticação
- Compressão
- Deteção de erros
- Negociação de opções para capacidades como endereços do nível de rede e compressão de dados.
- Suporte de *multilink.*

Funções não suportadas pelo PPP

- Controlo de fluxo
  - Qualquer mensagem PPP que sobrecarregue os *buffers* do receptor será perdido.
- Correcção de erros
  - PPP, por omissão, inclui apenas um campo de CRC - não faz correcção de erros (por omissão não pede retransmissão). Pode ser negociado a correcção de erros a qual pode não ser suportada.
- Sequência
  - O PPP assume que todas as mensagens, enviados e recebidos, mantêm a sequência original.

Estrutura do PPP

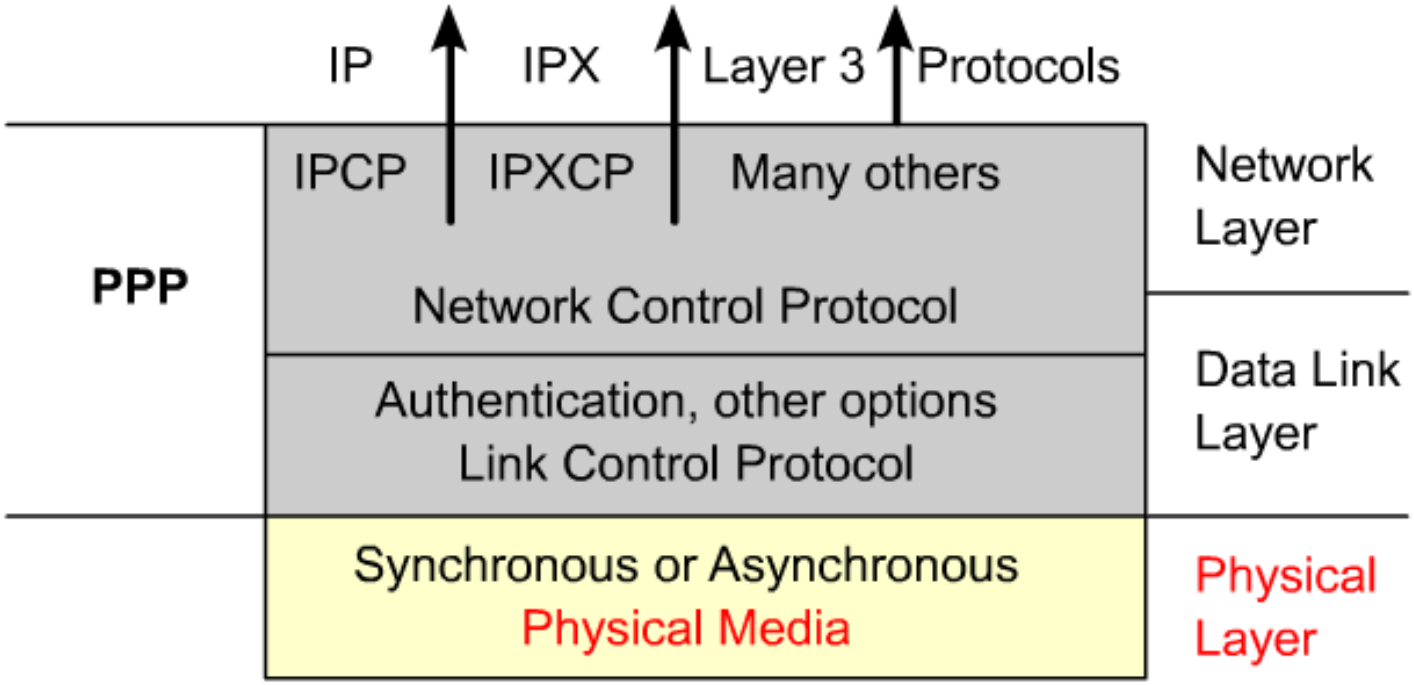




- ***Link Control Protocol*** (**LCP**): Para estabelecer, configurar e testar a ligação de dados de nível 2.

- ***Network Control Protocols*** (**NCPs**): Para estabelecer e configurar diferentes protocolos de nível 3. PPP foi concebido para suportar simultaneamente diferentes protocolos de nível de rede.
  - PPP suporta vários protocolos para além de IP, e.g. *Internetwork Packet Exchange* (IPX), *Appletalk*.

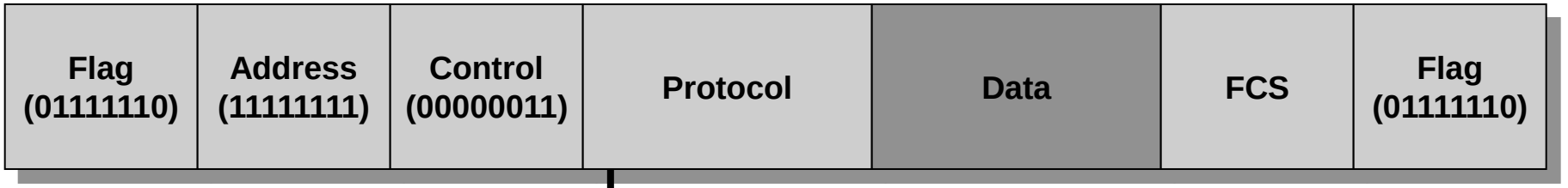
Stack PPP


IP
IPX
Layer 3
Protocols
IPCP
IPXCP
Many others
Network Control Protocol
PPP
Authentication, other options
Link Control Protocol
Synchronous or Asynchronous
Physical Media
Network Layer
Data Link Layer
Physical Layer

Network Access Server (NAS)

- Suporte para aceitar e estabelecer ligações de/para os utilizadores.
- *Tunneling* de tráfego de utilizador de/para outros nós da rede.
- Serviços AAA:
  - ***A**uthorization*, ***A**uthentication* e ***A**ccounting*.

Formato da mensagem PPP



UI – ***U**nnumbered **I**nformation* (03h)

Network protocols:
0021h – IP
0029h – Appletalk
002bh – Novell IPX

Network Control Protocols:
8021h – IP Control Protocol
8029h – Appletalk Control Protocol
802bh – Novell IPX Control Protocol

Link Control Protocols:
C021h – Link Control Protocol
C023h – PAP
C025h – Link Quality Report
C223h – CHAP
C227h – EAP (PPP Extensible Authentication Protocol)

Estabelecimento da sessão PPP

- O estabelecimento de uma sessão PPP progride através de três fases:
  - Fase de estabelecimento da ligação
  - Fase de autenticação (opcional)
  - Fase dos protocolos da camada de rede

Estabelecimento da sessão PPP (detalhe)

1. Estabelecimento da ligação (LCP)
2. Autenticação (opcional) (LCP)
3. Determinação da qualidade da ligação (LCP)
4. Configuração do protocolo da camada de rede (NCP)
5. Terminação da ligação (LCP)

```
Router#configure terminal
Router(config)#interface serial 0/0
Router(config-if)#encapsulation ppp
```

Fases PPP no estabelecimento de ligações

- **Fase 1**: O PC faz uma chamada ou pede o estabelecimento de uma ligação através do *modem.*
- **Fase 2**: *Modem* ligado ao *router* do ISP responde e estabelece a ligação física.
- **Fase 3**: Estabelecimento da ligação lógica.
- **Fase 4**: O PC cliente e o *router* trocam mensagens LCP para a configuração da ligação.
- **Fase 5**: Os dados de autenticação opcionais são analisados pelo ISP e em caso de sucesso são trocados uma série de mensagens NCP para configuração de parâmetros da camada de rede.
- **Fase 6**: São trocados dados.

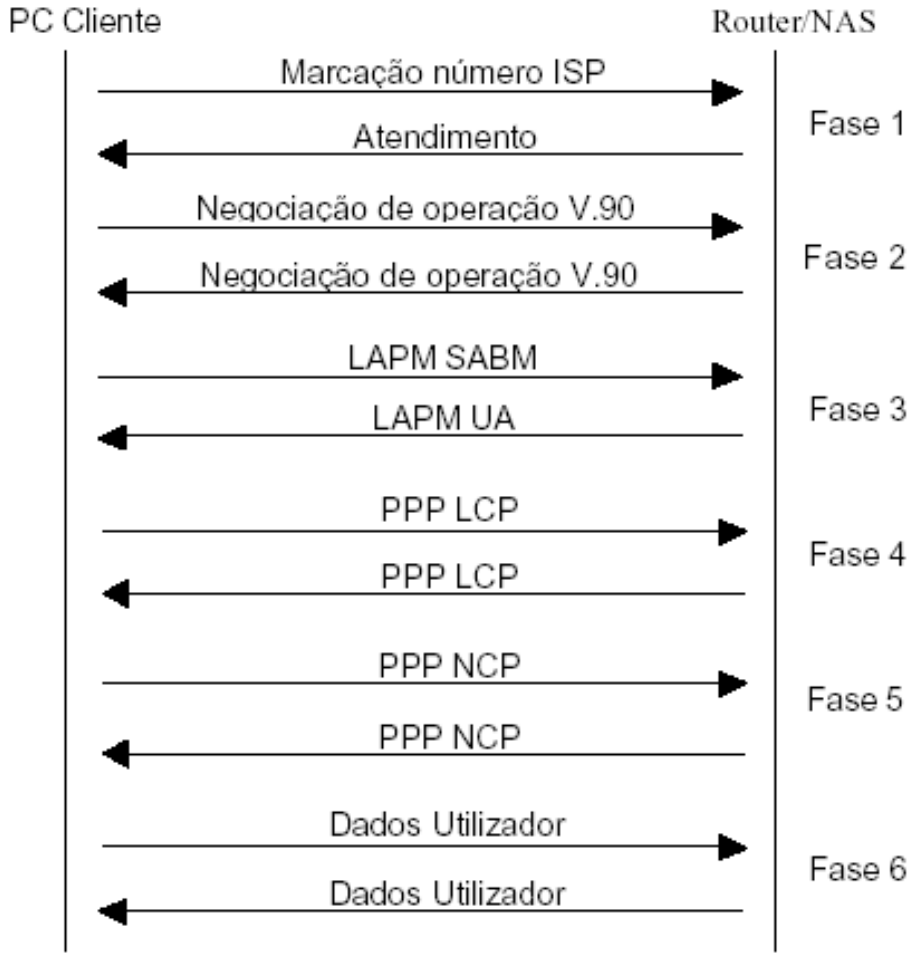
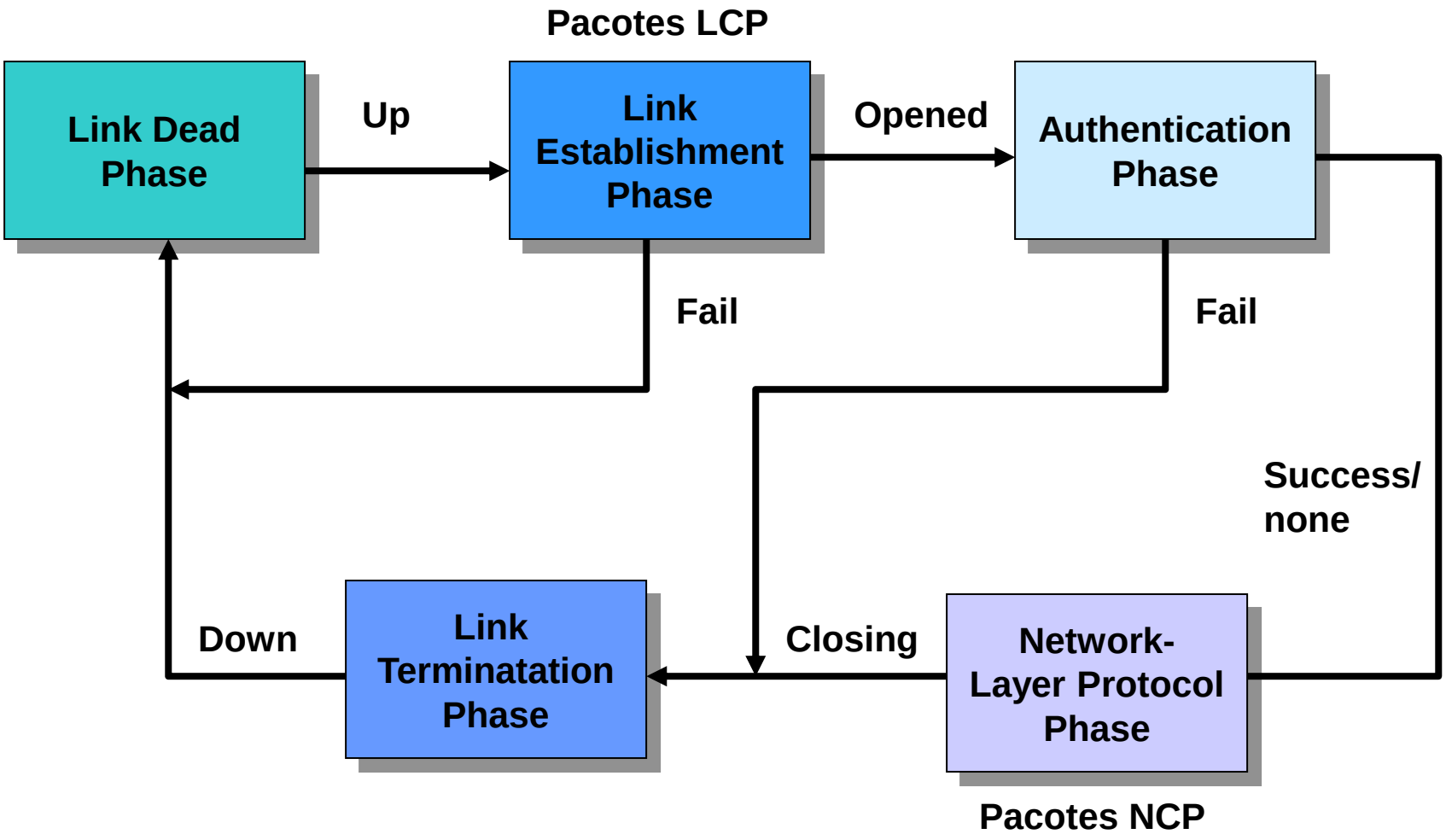


Diagrama de fases PPP



Fase inactiva (*idle*)

- A ligação começa e termina nesta fase.
- Um evento indicando que a camada física está disponível para ser usada, tem como consequência a transição para a fase de estabelecimento da ligação.
- Durante esta fase a máquina estados do LCP, estará nos estados *Initial* ou *Starting*. A fase Inactiva é retornada após a desconexão do Modem.

Fase de estabelecimento (*establishing*)

- O protocolo de controlo da ligação (LCP) é usado para estabelecer a conexão mediante a troca de mensagens de configuração. O estado *LCP-Opened* da máquina de estados é atingido depois da recepção e envio de mensagens *Configure-Ack*.
  - *LCP-Opened* é o último estado da máquina de estados da fase de estabelecimento.
- Nesta fase são negociadas as opções de configuração, independentes do tipo de protocolos de rede, a serem usados nas fases posteriores.
  - A recepção de uma mensagem *Configure-Request* LCP nas fases seguintes resultam no retorno à reconfiguração da ligação.
  - A recepção de mensagens que não sejam do tipo LCP nesta fase devem ser silenciosamente descartados.
- A configuração de protocolos da camada de rede é feita por protocolos independentes (NCPs).

Fase de estabelecimento (*establishing*)

- São trocadas tramas LCP para configurar e testar a ligação.
- As tramas LCP incluem os campos das opções de configuração que permitem aos dispositivos negociarem ouso de opções como:
  - Dimensão máxima da trama (MTU)
  - Compressão de alguns dos campos do PPP
  - Protocolo de autenticação
- Se uma opção não for incluída na trama LCP, é assumido o valor por omissão (por ex.: sem autenticação)
- Antes de se poderem trocar quaisquer mensagens da camada de rede o LCP deve **abrir a ligação e negociar os parâmetros de configuração**.
- Esta fase termina quando uma trama de *acknowledge* de configuração tiver sido enviada e recebida.

Fase de autenticação (*authentication*) (opcional)

- Em algumas ligações o extremo oposto pode desejar que o utilizador se autentique antes de prosseguir com a configuração dos protocolos de rede.
  - Nesta fase são negociadas opções através de mensagens LCP com base num protocolo de autenticação específico, daí que a autenticação não seja imperativa.
  - Esta fase só pode ser activada quando é recebido um sinal explícito de indicação do término da fase anterior de estabelecimento.
- Se a autenticação for obtida com sucesso a linha passa para fase de rede (*networking*), no caso de insucesso a ligação vai para a fase de terminação.
- Os protocolos permitidos nesta fase são o LCP, protocolos de monitorização de qualidade da linha e protocolos de autenticação (PAP e CHAP).

Fase de rede (*networking*)

- Uma vez terminada a fase precedente, cada protocolo de rede (tais como o IP, IPX e AppleTalk) deve ser configurado separadamente pelo protocolo NCP correspondente que, no caso do IP, é o IPCP.
- Quando termina a negociação na fase de rede, o protocolo de rede negociado é assumido para as fases seguintes.
  - Qualquer outro protocolo de rede diferente do configurado ao ser recebido deverá ser imediatamente descartado.
- Nesta fase qualquer combinação de mensagens como LCP, NCP ou outros protocolos de rede podem surgir
- Se o LCP terminar a ligação avisa os protocolos de rede para que eles procedam em conformidade.

Fase de finalização (*terminating*)

- O PPP pode terminar a ligação em qualquer altura.
  - E.g. devido a perda da portadora, falha na autenticação, fraca qualidade de ligação, um temporizador expirado por causa de um período longo de inactividade e ainda o encerramento por parte do operador.
- O LCP faz a troca de mensagens de terminação da ligação.
  - Quando a troca de mensagens de terminação da conexão chega ao fim é necessário forçar a camada física à desconexão, particularmente quando há falha de autenticação.
- O remetente da mensagem *Terminate-Request* deve desligar após receber uma mensagem *Terminate-Ack* ou depois do temporizador expirar.
- Finalmente o PPP prossegue para a fase inactiva, no caso de mensagens do tipo LCP serem recebidos devem ser imediatamente descartados.

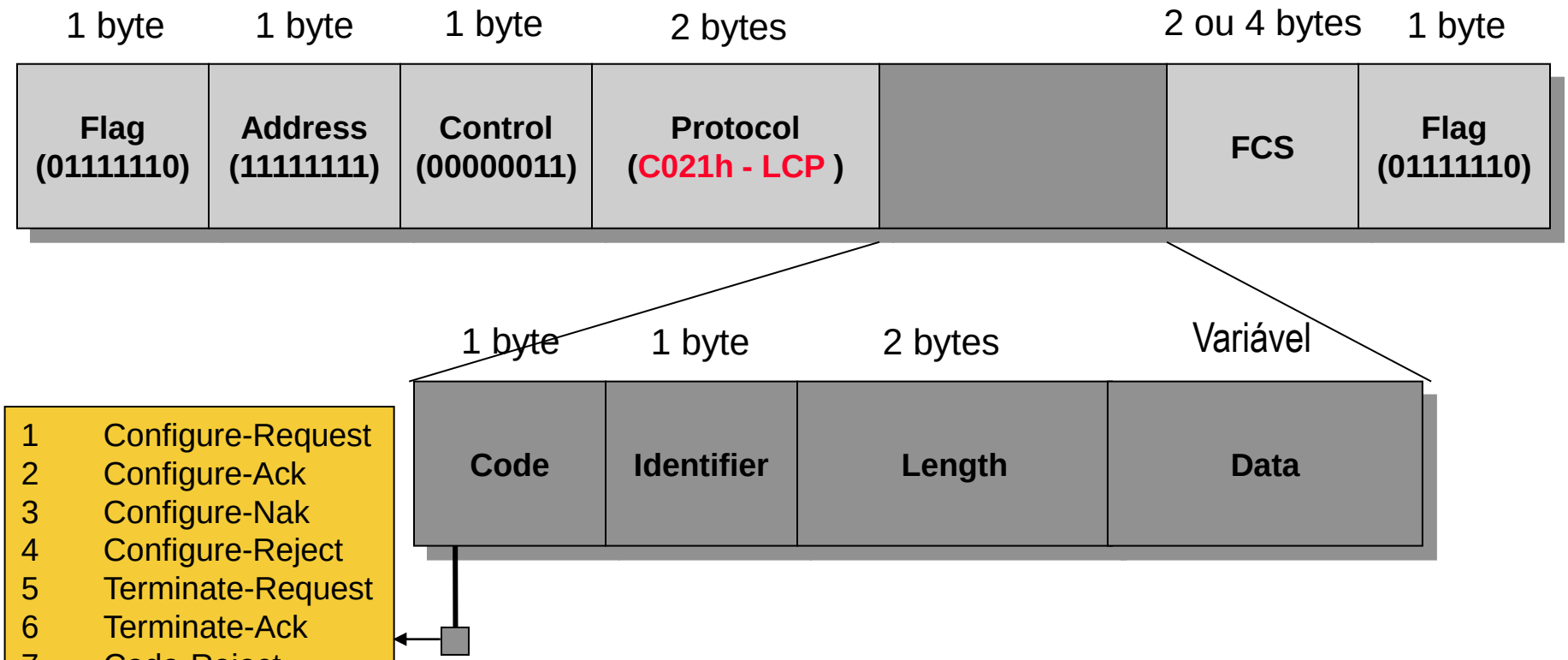
Protocolo LCP (*Link Control Protocol*)

- O protocolo de controlo de ligação LCP permite iniciar a ligação, testar a qualidade da linha, negociar opções de configuração (e.g. o tipo de protocolo a ser usado nas fases seguintes), e finalmente interromper a ligação quando esta já não for necessária.
  - Autenticação
  - Compressão
  - Detecção de erros
  - Suporte de *multilink*
  - Lidar com variações da dimensão dos PDUs
  - Detectar erros de configuração
  - Terminar a ligação
  - Determinar se a ligação está a funcionar bem ou se está a falhar

Protocolo LCP (*Link Control Protocol*)

- Existem três classes de mensagens LCP a saber:
  - **1. Mensagens de configuração da ligação**, que são usados para estabelecer e configurar a ligação *(**Configure-Request, Configure-Ack, Configure-Nak e Configure-Reject**)*.
  - **2. Mensagens terminadores de ligação**, que são usados para terminar a ligação *(**Terminate-Request, Terminate-Ack**)*.
  - **3. Mensagens para manutenção, controle e eliminação de erros da ligação *(Code-Reject, Protocol-Reject, Echo-Request, Echo-Reply e Discard-Request)***.

LCP: Formato da mensagem



LCP: Formato das mensagens

- ***Code*:** Ocupa um octeto e é preenchido com valores que variam de um a onze, para a identificação da mensagem LCP. No caso da mensagem ser recebido com o campo **Code** desconhecido é rejeitado com envio de uma mensagem *code-reject.*

- ***Identifier* (ID):** Relaciona a sequência das mensagens transmitidas com as mensagens recebidas.

- ***Length*:** Dois octetos, indicando o tamanho total da mensagem LCP incluindo o cabeçalho.

- ***Data*:** Tamanho variável, dependente do código da mensagem.

LCP: Mensagens de configuração

- ***configure-request***
  - Enviado pelo extremo que pretende estabelecer a ligação
  - Inclui uma lista de opções
- ***configure-ack***
  - Todas as opções foram aceites
- ***configure-nak***
  - Algumas opções foram omitidas ou revistas
  - O outro extremo deve enviar um novo pedido *configure-request*
- ***configure-reject***
  - Algumas opções não são reconhecidas
  - O outro extremo deve enviar um novo pedido *configure-request*

LCP: Mensagens de finalização da ligação

- ***terminate-request***
  - Quando um dos extremos pretende desligar a ligação

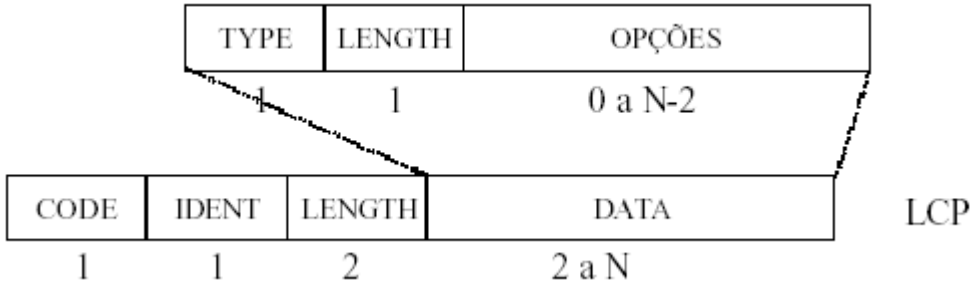
- ***terminate-ack***
  - O extremo que recebe o *terminate-request* deve responder com *terminate-ack*

LCP: Mensagens de monitorização e de *debug*

- ***code-reject***
  - Indica que uma mensagem desconhecido foi recebido
- ***protocol-reject***
  - Indica que foi recebido uma mensagem de um protocolo desconhecido
- ***echo-request***
  - Para verificar que a ligação está activa
- ***echo-reply***
  - Pacote enviado em resposta a um *echo-request*
- ***discard-request***
  - Para verificar condição de *loopback* no transmissor

LCP: Opções

- A configuração automática é conseguida graças a um mecanismo extensivo de negociação de opções, baseada numa máquina de estados.

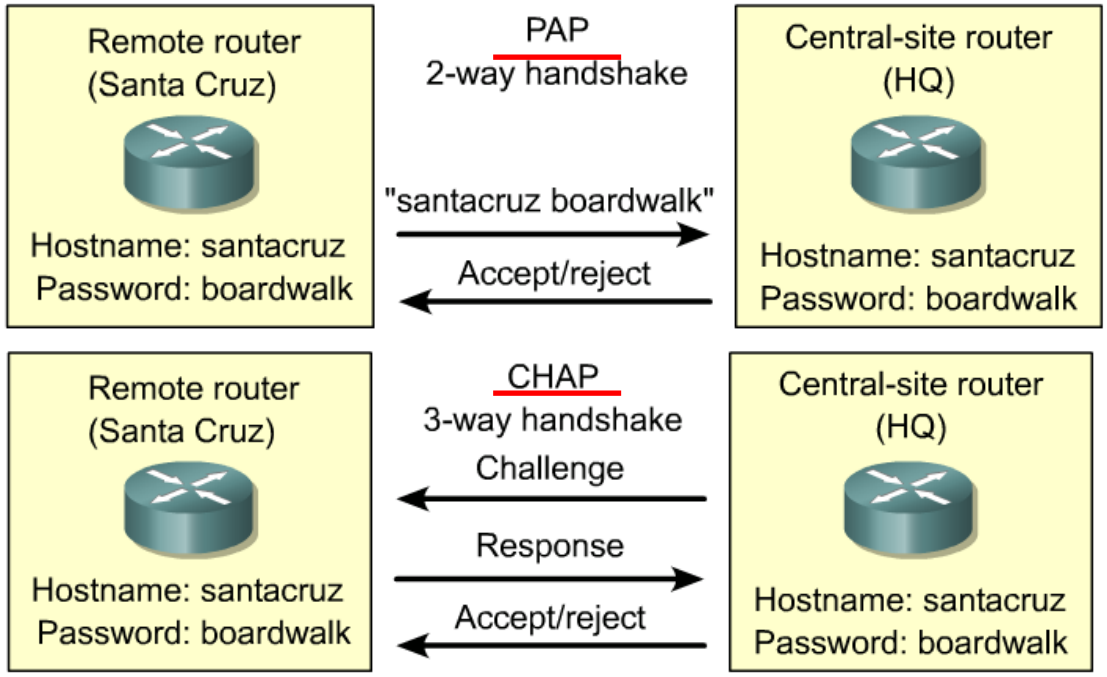


Tipo/ Type	Tipo	Comprimento [bytes]	Opções/Valor
0	***Vendor Specific***		
1	***Maximum Receive Unit***	4	1500
2	***Async-Control-Character Protocol***		
3	***Authentication-Protocol***	4	C023 (PAP) / C223 (CHAP)
4	***Quality Protocol Report***	4	C025
5	***Magic-Number***	>=4	Aleatório

LCP: Opções mais comuns

- **Autenticação (opção PPP 3):** Autenticação antes de iniciar a recepção e o envio de mensagens do nível três do modelo OSI. Uma vez que existem diferentes tipos de protocolos para autenticação, é negociado um protocolo específico de autenticação (PAP, CHAP, ...).
- **Monitorização da Qualidade da Ligação (opção PPP 4):** Permite monitorar durante a ligação eventuais perdas de dados.
- **Número Mágico (opção PPP 5):** Mecanismo de detecção de retorno de sinais emitidos permitindo que o *peer* saiba que não está a comunicar consigo próprio mas com a rede. Se o número mágico for pedido pelo *peer* deve-se responder com a escolha de um número aleatório garantindo uma elevada probabilidade de ser diferente do do *peer.*

Protocolos de autenticação do PPP

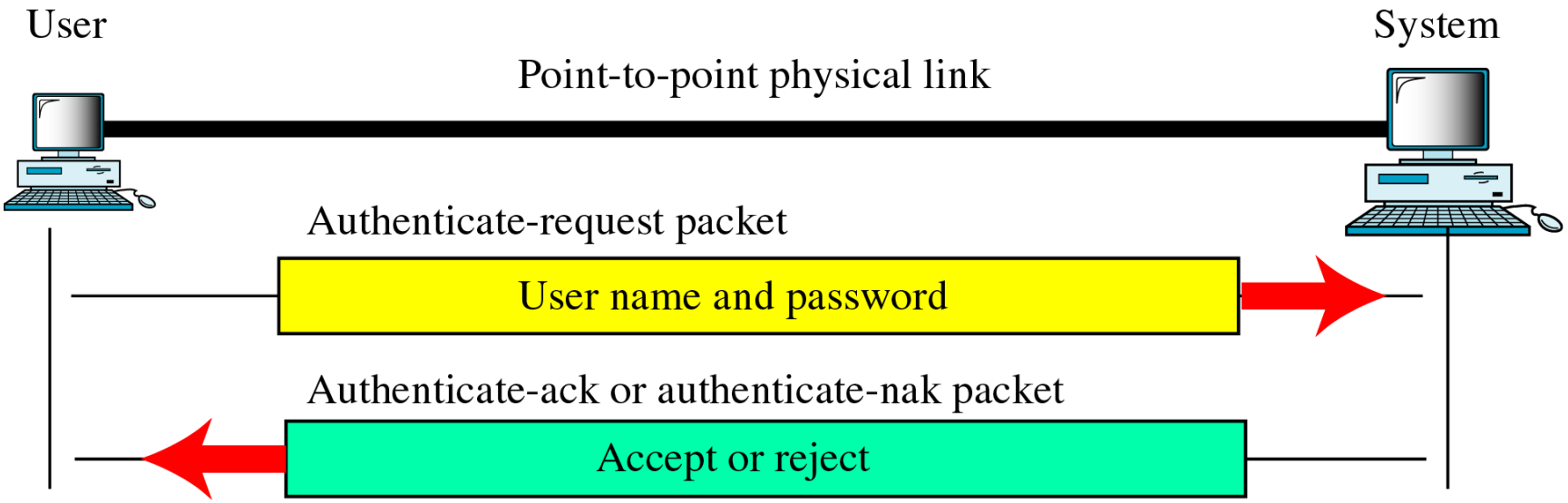


- Password sent in clear text
- Peer in control of attempts

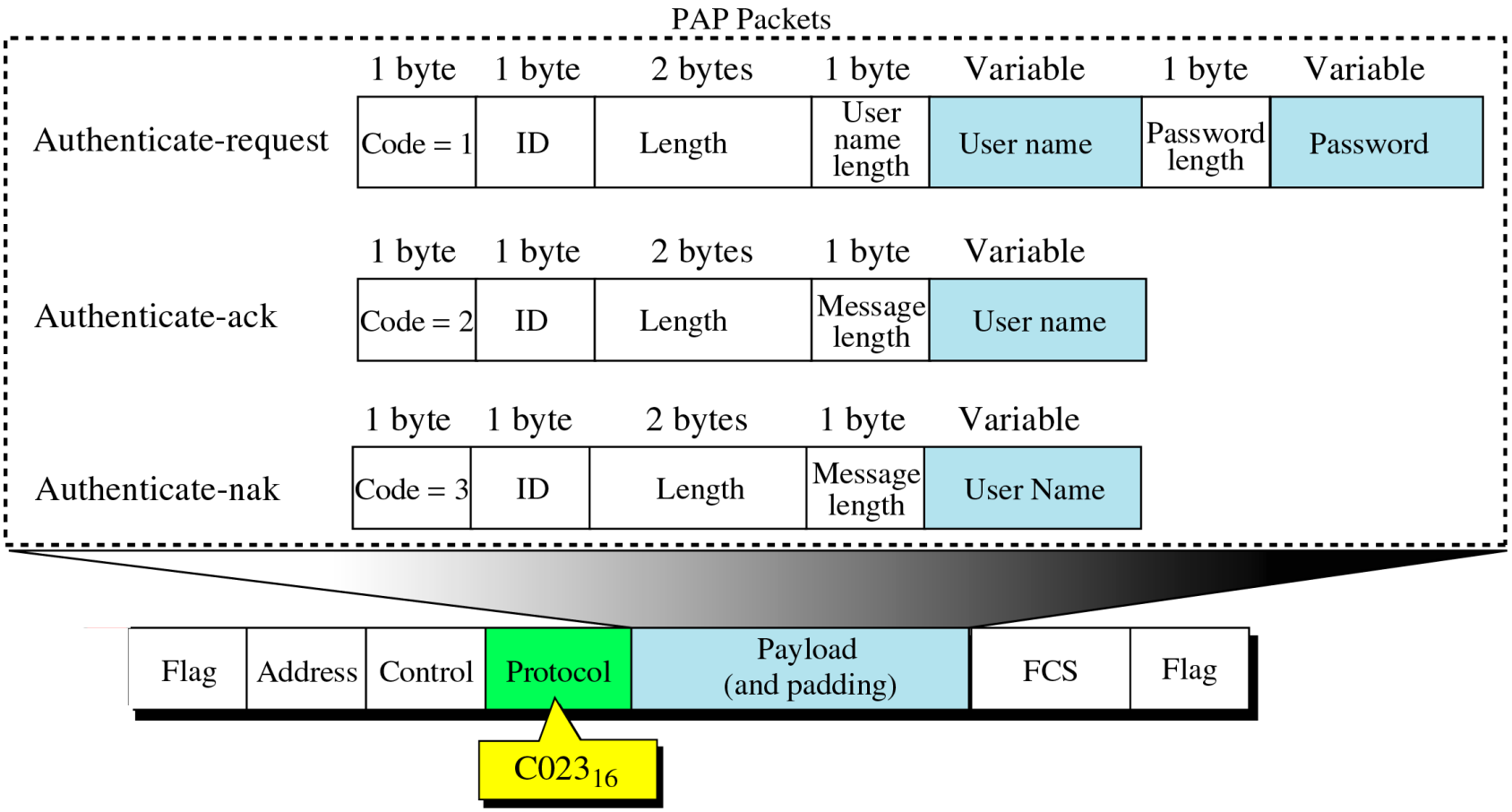
Encrypted password
Repeated challenges

PAP (*Password Authentication Protocol*)

- Método de autenticação em que a identificação é feita num sentido e no sentido de retorno aguarda-se uma única resposta de aceitação ou rejeição (*two-way handshake*).
  - Ocorre apenas no início do estabelecimento de uma ligação PPP.
  - O *user name* e a *password* (em claro) são enviados em claro repetidamente até vir um *acknowledge* ou a ligação ser terminada.



PAP: Formato da mensagem



PAP: Tipos de mensagens

- **Authenticate-request:** Pacote utilizado para iniciar o protocolo PAP, pode ser enviado repetidamente dentro de um número definido de tentativas ou então periodicamente até que seja recebida a resposta.

- **Authenticate-ack:** Confirmação da validade da combinação *username/password* recebido na mensagem *Authenticate-Request.*

- **Authenticate-nak:** Rejeição da combinação *username/password* recebido no *Authenticate-Request.*
  - O campo **Identifier** ocupa um octeto, e é preenchido por números que relacionam a sequência das mensagens transmitidas com as mensagens ou mensagens recebidos.

Configuração do PAP

DTE .2/S0 — 172.25.3.0/24 Serial — DCE .1/S0


```
hostname SantaCruz
username HQ password HQpass

interface Serial0
   ip address 172.25.3.2 255.255.255.0
   encapsulation ppp
   ppp authentication pap
   ppp pap sent-username SantaCruz
                password SantaCruzpass
```

```
hostname HQ
username SantaCruz password SantaCruzpass

interface Serial0
   ip address 172.25.3.1 255.255.255.0
   encapsulation ppp
   ppp authentication pap
   ppp pap sent-username HQ
                password HQpass
```

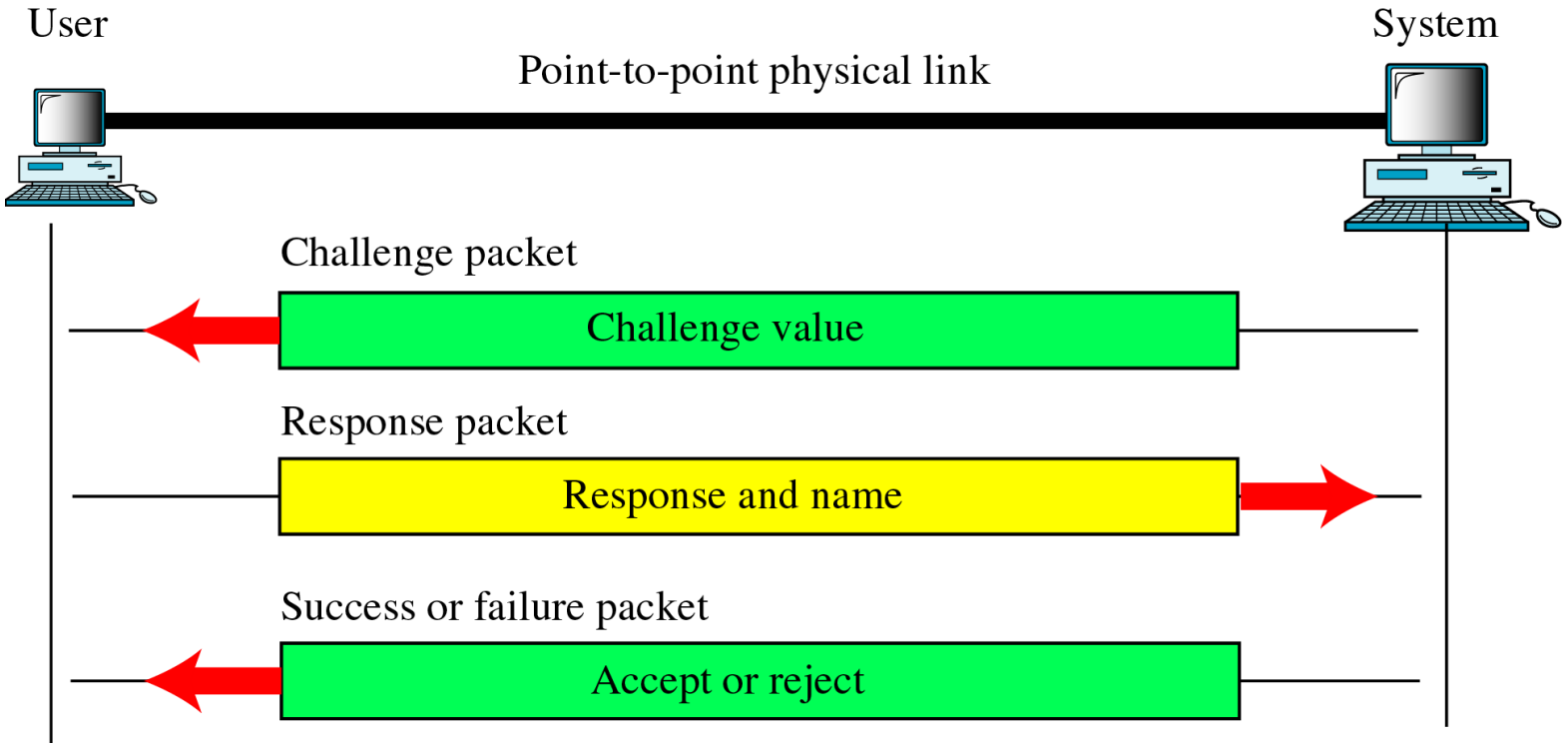
CHAP (*Challenge Handshake Authentication Protocol*)

O CHAP é utilizado para verificar a identidade dos pares. Utiliza *3-way handshake*. É realizado após o estabelecimento da ligação e PODE ser repetido a qualquer momento após a ligação ter sido estabelecida.

1. Após a fase de estabelecimento da ligação estar completa, o autenticador envia uma mensagem de desafio ("*challenge*") ao par.
2. O par responde com um valor calculado através de uma função de "*one-way hash*" protegida, tipicamente Message Digest 5 (MD5).
3. O autenticador verifica a resposta relativamente aos seus próprios cálculos do valor do *hash* e da *password* que conhece. Se o valor for igual a autenticação é considerada positiva; se o valor for diferente a autenticação é negativa e a ligação deve ser terminada.
4. A intervalos aleatórios o autenticador pode enviar novo "*challenge*" ao par e repetir os passos anteriores.

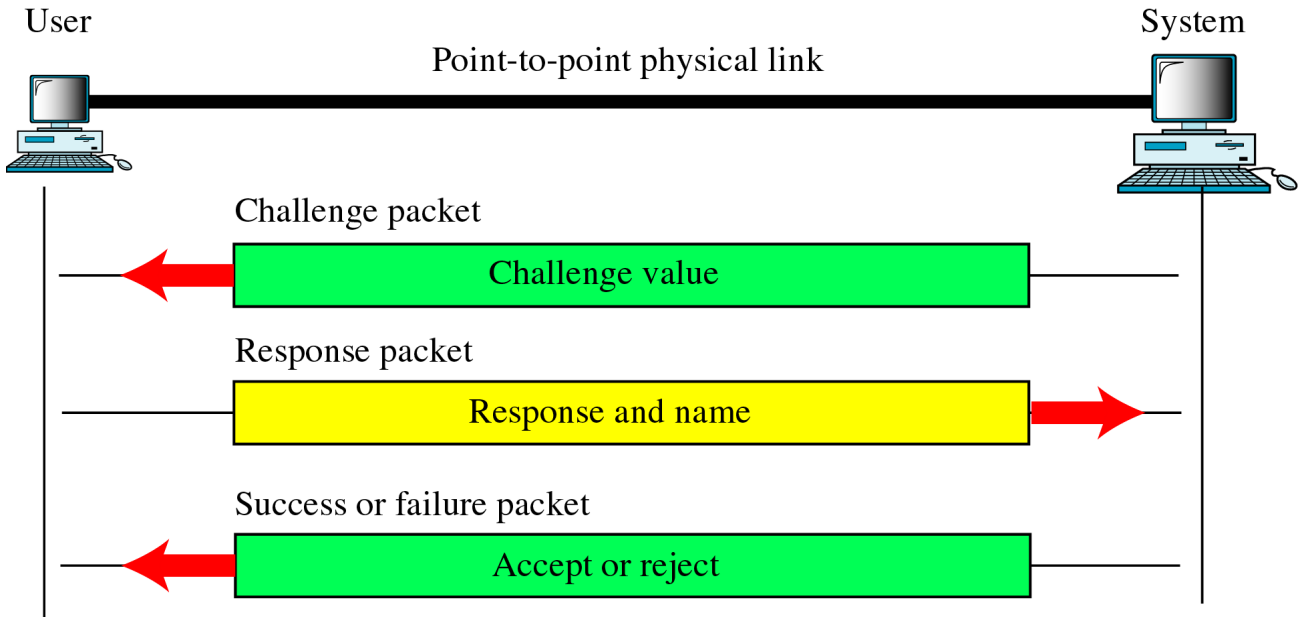
CHAP (*Challenge Handshake Authentication Protocol*)

- Protocolo de autenticação usado para a verificação periódica da identidade do *peer* remoto pelo método "***3-way handshake***" no início do estabelecimento da ligação e depois em qualquer altura depois do *link* estar estabelecido.

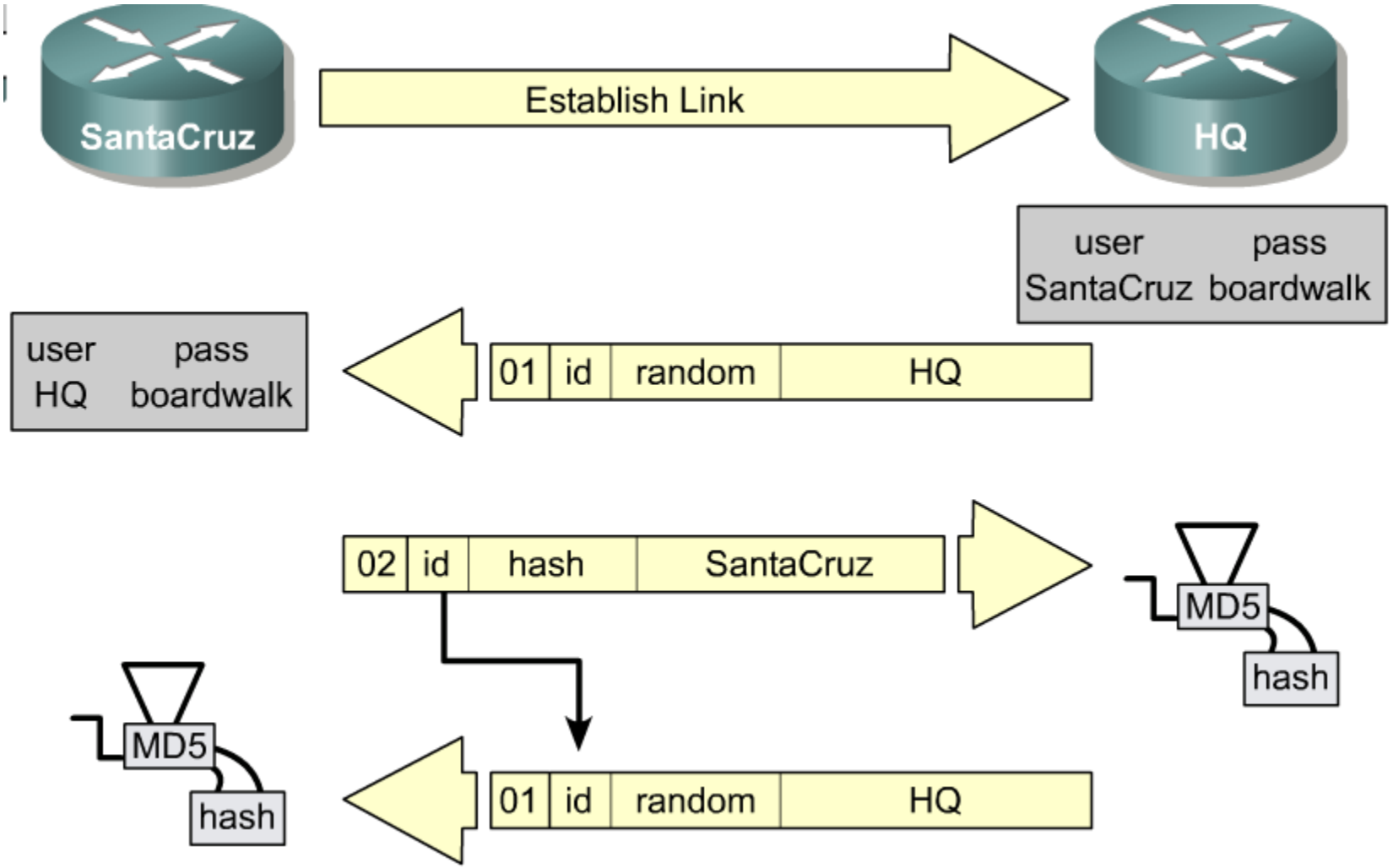


CHAP (*Challenge Handshake Authentication Protocol*)

- O CHAP fornece protecção contra ataques por repetição (*playback*) através do uso de um valor da variável de desafio única e aleatória.
- A utilização de desafios sucessivos destina-se a limitar o tempo de exposição a um único ataque.
- O NAS controla a frequência dos desafios.



CHAP (*Challenge Handshake Authentication Protocol*)



CHAP (*Challenge Handshake Authentication Protocol*)

Vantagens

- O CHAP fornece protecção contra ataques de repetição através do uso de um identificador que vai incrementando e a variável do valor do desafio ("*challenge*"). A utilização de repetição de desafios destina-se a limitar o tempo de exposição a um único ataque. É o autenticador é quem controla a frequência e a temporização dos desafios.
- Este método de autenticação depende de um "segredo" conhecido apenas pelo autenticador e pelo par. O segredo não é enviado através da ligação.
- Embora a autenticação seja apenas num sentido, ao negociar o CHAP em ambos os sentidos o mesmo "segredo" pode ser utilizado para autenticação mútua.
- Dado o CHAP poder ser utilizado para autenticar diferentes sistemas o campo *name* pode ser utilizado como um índice para uma tabela de "segredos". Isto também torna possível o suporte de mais de um par de nome/segredo por sistema e a alteração do segredo em uso a qualquer altura durante a sessão.

CHAP (*Challenge Handshake Authentication Protocol*)

Desvantagens

- O CHAP requer que o “segredo” esteja disponível na forma “plaintext”. *Passwords* cifradas de forma irreversível não podem ser utilizadas.

- Não é muito útil em grandes organizações dado os “segredos” terem de ser colocados em ambas os extremos de todas as ligações o que provoca um problema de gestão da segurança.

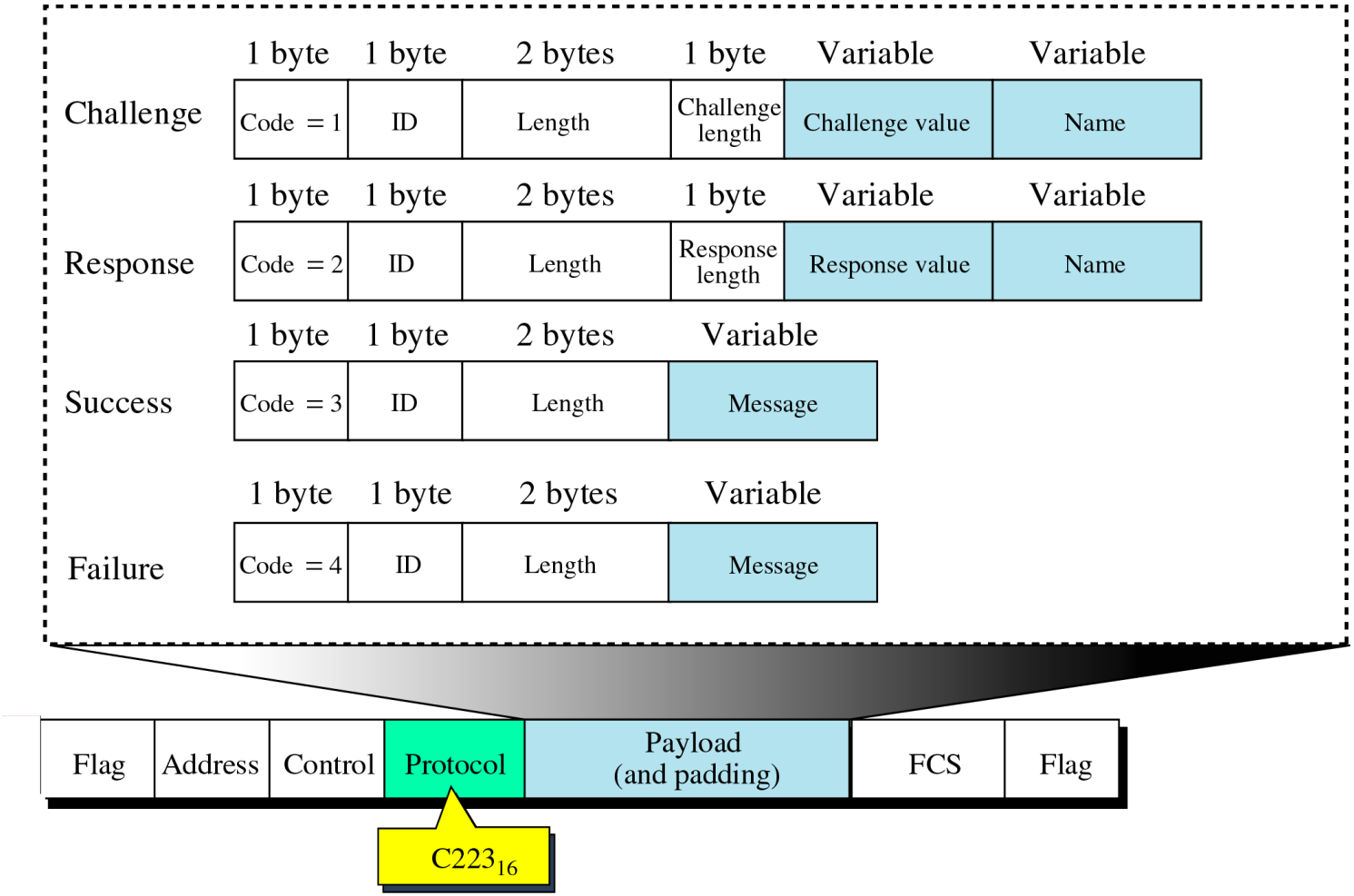
CHAP: Procedimento de autenticação

- O comprimento do segredo DEVE ser pelo menos de um octeto. O “segredo” DEVIA ser tão comprido e difícil de adivinhar como uma *password* bem escolhida. Seria preferível que tivesse o comprimento igual ao do resultado da função de *hash* utilizada (128 bits no MD5). Isto para dar protecção contra ataques por pesquisa exaustiva.

- Cada valor de “*challenge*” DEVE ser único dado que a repetição de desafios iguais e com o mesmo “segredo” leva a que um atacante possa utilizar respostas capturadas anteriormente.

- Cada valor de “*challenge*” deve ser imprevisível para evitar que um atacante, em vez de um par, possa responder a um futuro desafio. Utilizando a resposta para se fazer passar pelo par perante o autenticador.

CHAP: Formato da mensagem



CHAP: Formato da mensagem

- *Identifier*
  - O **Identifier** DEVE ser trocado cada vez que um Challenge for enviado. O Response Identifier DEVE ser copiado do campo Identifier recebido no Challenge que causa a resposta o Response.

- *Value*
  - O campo **Challenge Value** é uma *stream* de octetos de dimensão variável. O *Challenge Value* DEVE ser trocado cada vez que um *Challenge* é enviado. O comprimentos do *Challenge Value* depende do método usado para gerar os octetos, e é independente do algoritmo de *hash* utilizado.
  - O campo ***Response Value*** é um *hash* calculado a partir de uma *stream* de octetos consistindo no *Identifier*, concatenado com o "segredo", concatenado com o *Challenge Value*. O comprimento do *Response Value* depende do algoritmo de *hash* utilizado (128 bits para o MD5).

CHAP: Formato da mensagem

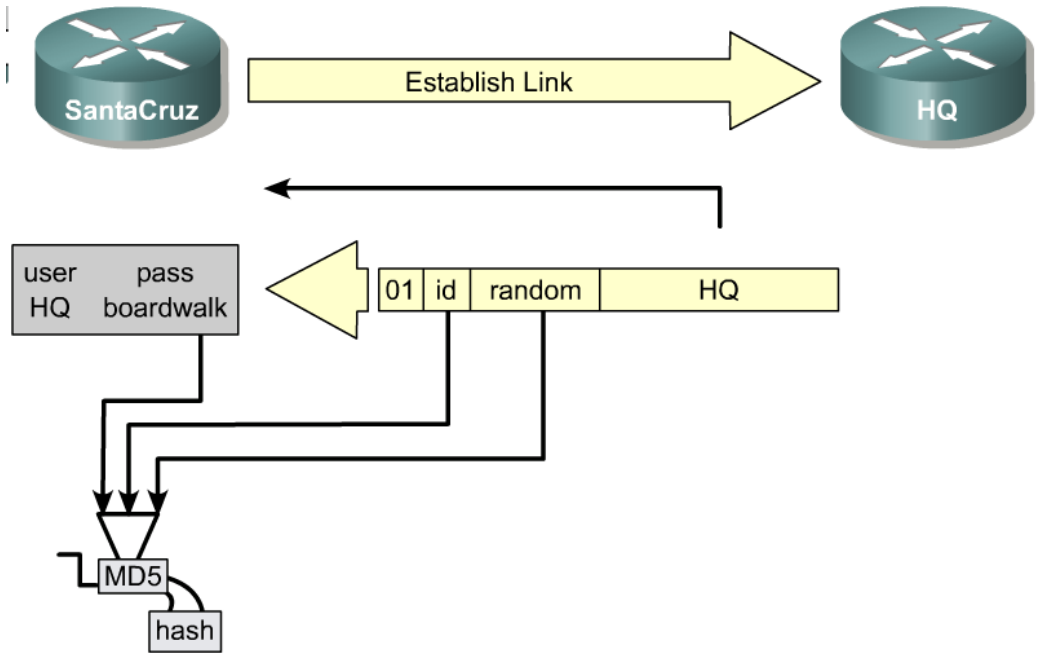
- *Name*
  - O campo ***Name*** é um ou mais octetos representando a identificação do sistema que transmitiu a mensagem.
  - Não há limitações ao conteúdo deste campo. Por exemplo, ele pode conter uma *string* de caracteres ASCII ou um identificador único em sintaxe ASN.1.
  - O campo *Name* não pode ser nulo ou terminado em CR/LF.
  - Dado que o CHAP pode ser utilizado para autenticar muitos sistemas diferentes, o conteúdo do campo *Name* pode ser utilizado para localizar o "segredo" numa base de dados de "segredos". Isto torna possível utilizar mais do que um par nome/segredo por sistema.

CHAP: Procedimento de autenticação

- Método "***3-way handshake***" consiste na seguinte sequência:
  - Envio de uma mensagem *challenge* (tipo 01) pelo equipamento autenticador ao equipamento remoto,
    1. A mensagem de *challenge* inclui o identificador do tipo da mensagem (01), o ID da mensagem, composto por um número sequencial que identifica o desafio, um valor aleatório (*challenge*) gerado pelo NAS e o nome de quem desafia.
    2. O ID e o valor aleatório (*challenge*) são mantidos pelo NAS.
    3. A mensagem de *challenge* é enviada pelo NAS. É mantida uma lista dos *challenges* enviados.

CHAP: Procedimento de autenticação

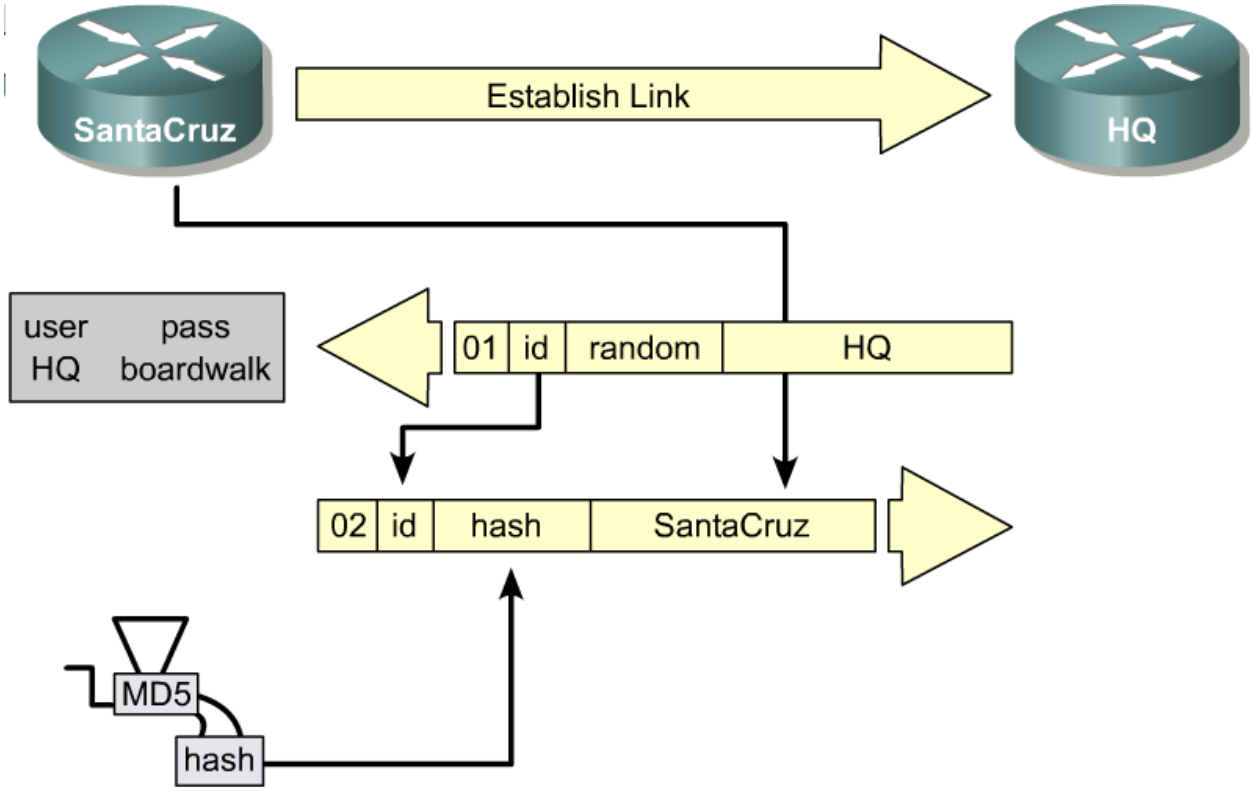
- O NAS responde com uma mensagem calculada na base de uma função de *hash*.
- A resposta é analisada pelo equipamento autenticador e, se os valores coincidirem, uma resposta de confirmação é enviada, caso contrário a ligação termina.



- Os "**segredos/ *passwords***" são únicos e secretos, e são apenas do conhecimento da entidade autenticadora e do equipamento remoto.

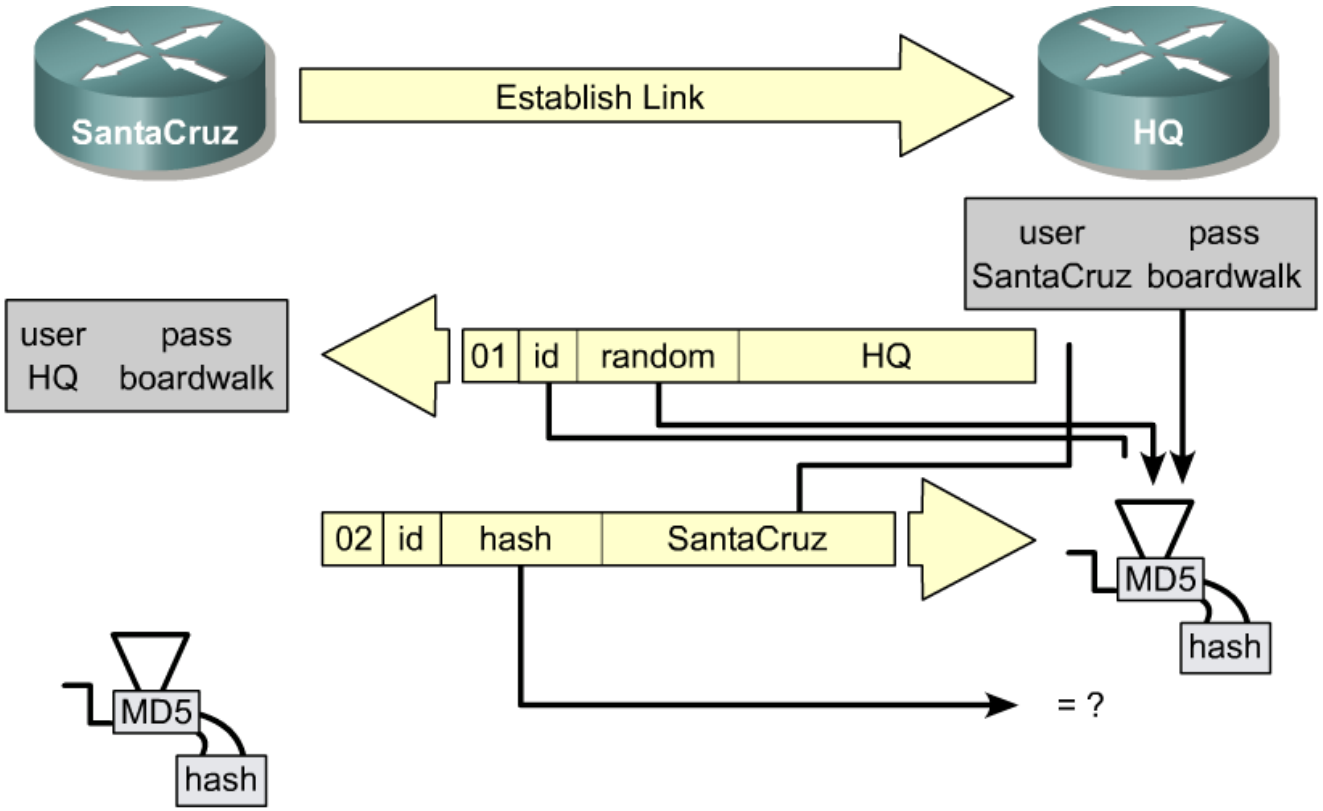
CHAP: Procedimento de autenticação

– O dispositivo que está a ser autenticado tem de responder com uma mensagem que inclui o *hash* calculado a partir da mensagem de *challenge* recebida e da password.



CHAP: Procedimento de autenticação

– Com base na mensagem de *challenge* (tipo 02) recebida o desafiador consulta a base de dados com nomes de utilizadores e senhas ou servidores de RADIUS para obter os dados para verificar se o desafio foi bem respondido.



Configuração do CHAP

DTE .2/S0 — 172.25.3.0/24 Serial — DCE .1/S0


```
hostname SantaCruz
username HQ password boardwalk
ppp chap hostname SantaCruz (optional)

interface Serial0
   ip address 172.25.3.2 255.255.255.0
   encapsulation ppp
   ppp authentication chap
```

```
hostname HQ
username SantaCruz password boardwalk
ppp chap hostname HQ (optional)

interface Serial0
   ip address 172.25.3.1 255.255.255.0
   encapsulation ppp
   ppp authentication chap
```

Compressão

- A Cisco suporta os seguintes tipos de compressão:
  - **Predictor** – Determina se os dados já estão comprimidos.
  - **Stacker** - Baseado no algoritmo de compressão de Lempel-Ziv (LZ)
  - **MPPC** – Suportado pela Microsoft (RFC 2118). Usa um algoritmo de compressão baseado no Lempel.Ziv
  - **TCP header compression** – comprime apenas os cabeçalhos do TCP.
    - `Router(config-if)#ip tcp header-compression`

Configurar a compressão

```
Router(config)#interface serial 0/0
Router(config-if)#encapsulation ppp
Router(config-if)#compress [predictor|stac|mppc]
```

- O PPP suporta compressão nas ligações ponto-a-ponto
- A compressão efectuada por software pode afectar o desempenho dos equipamentos.

Detecção de erros

- A monitorização de erros da ligação (LQM) é suportada em todas as ligações série a correrem PPP
- Monitoriza a qualidade da ligação e se a qualidade baixa abaixo de um certo valor a ligação é terminada
- As percentagens de erro são calculadas em ambas as direcções.

```
Router(config)#interface serial 0/0
Router(config-if)#encapsulation ppp
Router(config-if)#ppp quality percentage
```

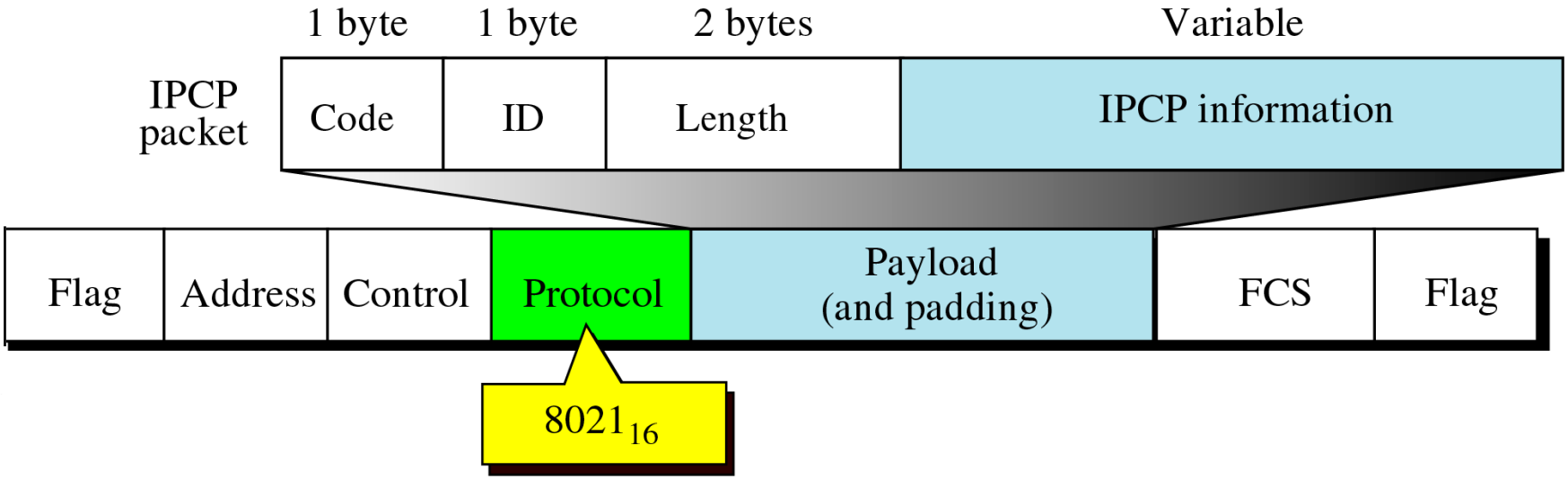
Protocolos NCP (*Network Control Protocol*)

- No estado rede, o PPP utiliza o NCP para encapsular dados de controlo dos protocolos das camadas de rede. Cada protocolo de rede define o seu conjunto de mensagens para configurar a sua ligação:
  - ***IP Control Protocol* (IPCP)**
    - Estabelece e termina uma ligação de rede para mensagens IP.
    - Após a configuração uma mensagem IP é transportado no campo de informação da mensagem PPP.
  - ***Internetwork Packet Exchange NCP* (IPXCP)**
  - ***AppleTalk NCP* (ATCP)**
  - ***Bridge Control Protocol* (BCP)**
  - ***Xerox Network Systems Internet Datagram NCP* (XNSCP)**
  - ***Banyan Vines Control Protocol* (BVCP)**

Protocolo IPCP (*IP Control Protocol*)

- as mensagens IPCP têm a mesma constituição que as mensagens LCP na sua estrutura de dados e funcionamento, com algumas excepções a considerar:
  - Ao nível de ligação de dados a mensagem IPCP é encapsulado no campo *Payload* da mensagem PPP onde o campo ***Protocol*** é preenchido pelo 0x8021.
  - O campo ***Code*** admite sete tipos de mensagens IPCP a saber: *configure-request, configure-ack, configure-nak, configure-reject, terminate-request, terminate-ack e code-reject*. Qualquer outro código deve ser rejeitado.
  - Só poderão ser trocadas mensagens IPCP após terminadas as fases de estabelecimento de linha e de autenticação.

Formato da mensagem IPCP



IPCP: Pacotes e Opções

Pacotes

Códigos / Code	Nome da mensagem
01	***configure-request***
02	***configure-ack***
03	***configure-nak***
04	***configure-reject***
05	***terminate-request***
06	***terminate-ack***
07	***code-reject***

Opções

Tipo	Opção	Comprimento	Valor
2	***IP Compression Protocol***	>=4	0x002d
3	***IP Address***	6	var
129	***Primary DNS***	6	var
130	***Secundary DNS***	6	var
131	***Primary NBNS***	6	var
132	***Secundary NBNS***	6	var

IPCP: Opções

- ***IP Address***
  - É uma opção que ocupa quatro octetos e possui uma forma de negociação de endereços IP a ser usado pelo utilizador remoto ao longo da ligação.
  - Permite que o remetente especifique que endereço IP deseja utilizar.
  - O requerente remoto pode sugerir um endereço IP ou pode enviar um endereço a zero, para que o *peer* atribua um endereço IP.
  - O *peer* pode responder com uma mensagem Configure-Nak com o valor IP válido a ser usado.

- ***IP Compression Protocol***
  - É uma opção que ocupa dois octetos e indica o tipo de compressão do protocolo desejado. Por opção a compressão não está activada.
  - A compressão de cabeçalho TCP/IP Van Jacobson (RFC 1144) permite reduzir o tamanho dos cabeçalhos TCP/IP de 40 octetos para 3 octetos, o que permite um aumento significativo da eficiência e do tempo de transmissão das mensagens.

IPCP: Opções

- ***Primary DNS*** (*Domain Name Server*)
  - Define o método de negociação do endereço do *Primary DNS* com o *peer* remoto a ser usado no terminal.
  - Se o *peer* local enviar um endereço ao servidor com valor falso (que normalmente é feito intencionalmente), o servidor retorna uma mensagem *Nak* que contem o valor *Primary DNS* correcto.

- ***Primary NBNS*** (*Netbios Name Server*)
  - Esta opção define o método de negociação do endereço do *Primary NBNS* com o *peer* remoto a ser usado no terminal.
  - Se o *peer* local enviar um endereço ao servidor com valor falso (que normalmente é feito intencionalmente), o servidor retornauma mensagem *Nak* que contém o valor *Primary NBNS* correcto.

PPP: Fases de operações e respectivos protocolos