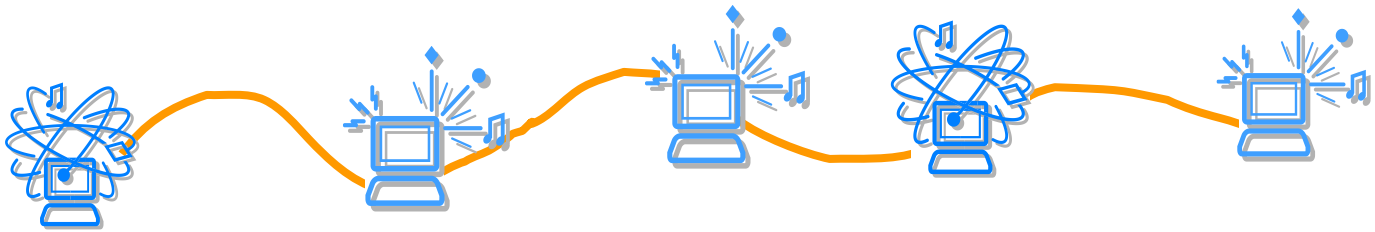
VPN – PPTP (*Point to Point Tunneling Protocol*)



Redes de Comunicação
Departamento de Engenharia da Electrónica e Telecomunicações e de Computadores
Instituto Superior de Engenharia de Lisboa

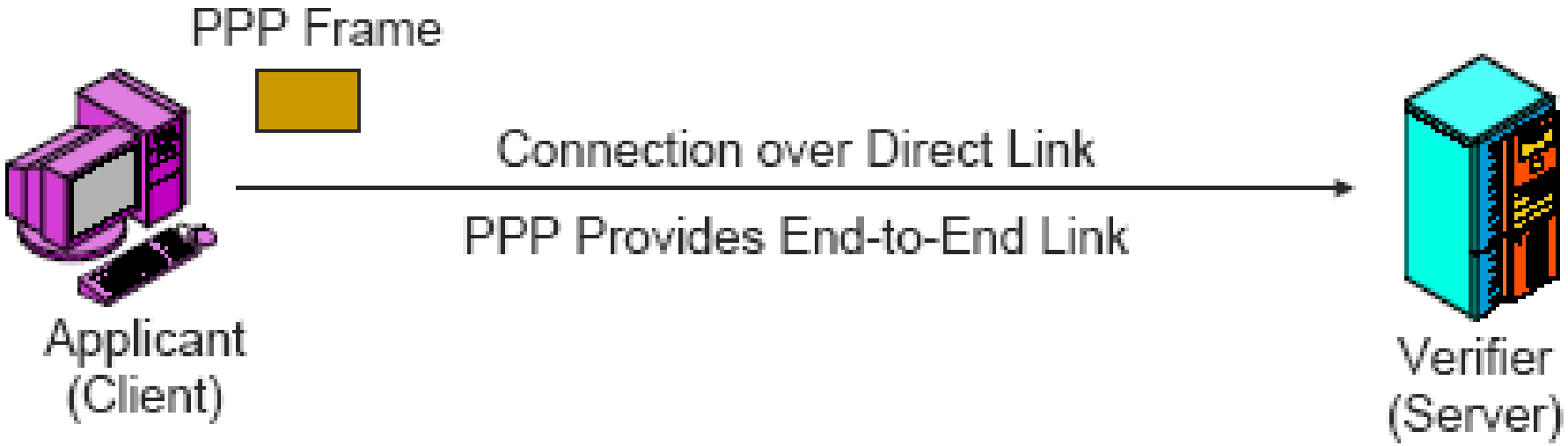
Baseado em:

- "*VPNs A Beginner's Guide*", John Mairs, McGraw-Hill
- *M.Sc. in Information Security* - Royal Holloway, University of London
- Prof. Dr. Andreas Steffen - Zürcher Hochschule Winterthur
- Pascal Meunier, Symantec Corporation, Purdue Research Foundation
- Henric Johnson, Blekinge Institute of Technology, Sweden
- Fred Baker, VPNs

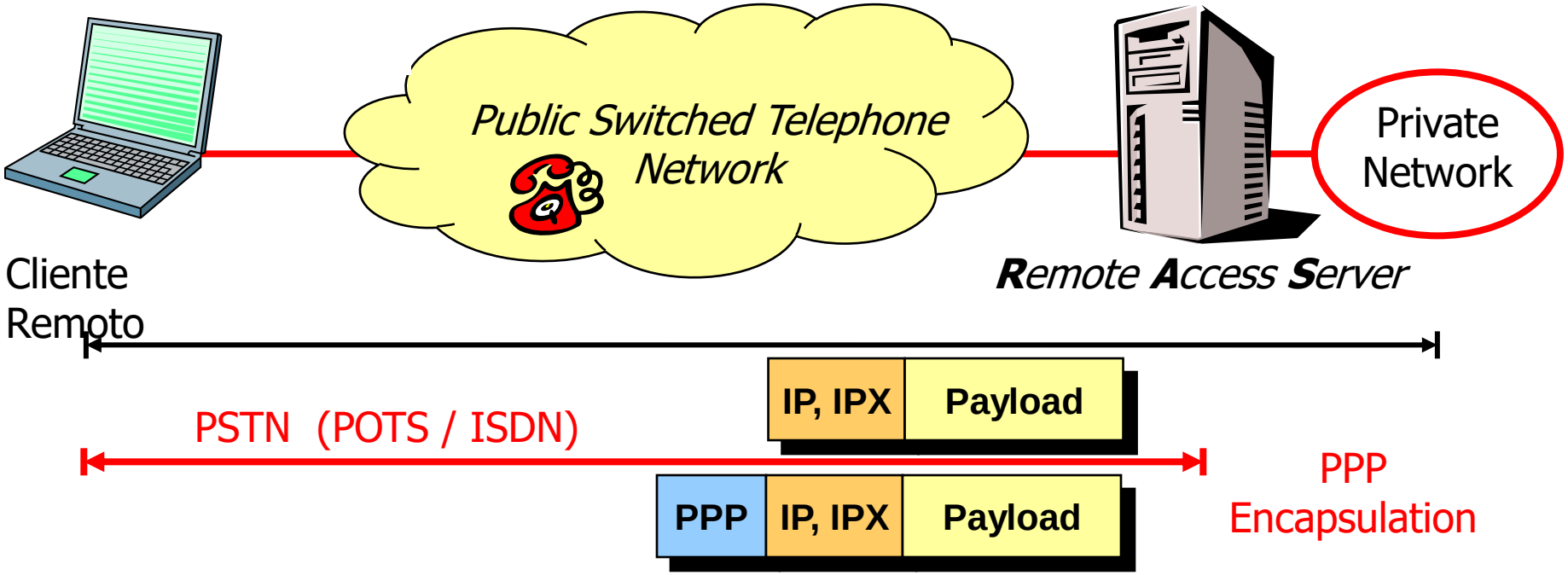
PPTP

- O ***Point-to-Point Tunneling Protocol*** (PPTP), foi desenvolvido pela Microsoft
- O PPTP é, basicamente, uma extensão do PPP para correr através de *internets*
  - O PPP trabalha na camada de ligação e não pode atravessar múltiplos troços entre *routers*
- Os mecanismos definidos para o PPP são utilizados aqui no PPTP, nomeadamente os ligados à segurança e à compressão de dados
- O PPTP está disponível nos seguintes sistemas operativos, entre outros:
  - Windows XP, NT, 98 e Linux

PPP em ligações directas e Internet



PPP–Acesso remoto baseado em Dial–In



- **Autenticação** utilizando PAP (*password*), CHAP (*challenge/response*), ou outro protocolo sobre o *Extensible Authentication Protocol* (EAP) suportando e.g. *token cards*
- Opcional: **cifra** de pacotes PPP (ECP) utilizando segredos pré-partilhados
- Pacotes individuais PPP não são autenticados
- O *Link Control Protocol* (LCP), tal como o EAP e o ECP, não é protegido!!

PPTP

- Estabelece um túnel, não cifrado
- Usa o *Microsoft Point-to-Point Encryption* (MPPE) se for necessário cifrar, este usa o RC4
- Suporta vários métodos de autenticação, nomeadamente: MS-CHAPv2 e EAP
- *Extensible Authentication Protocol* - EAP
  - Uma extensão ao PPP. O EAP é um protocolo geral para autenticação que também suporta múltiplos mecanismos de autenticação, tais como *token cards*, Kerberos, *one-time passwords*, certificados, autenticação por chave pública e *smart cards*.

PPTP - Segurança

- A parte da segurança do PPTP utiliza os mecanismos definidos para o PPP, nomeadamente:
  - Para autenticação o MS-CHAPv2 ou EAP
  - Para cifrar o MPPE (RFC 3078 - *Microsoft Point-To-Point Encryption (MPPE) Protocol*).
- O PPTP/MPPE utiliza chaves de sessão para cifrar os dados com o algoritmo RSA RC4
- A autenticação e a chave de sessão são obtidos a partir de *passwords* cujo *hash* foi calculado com SHA

(http://www.schneier.com/paper-pptpv2.html - "Cryptanalysis of Microsoft's PPTP Authentication Extensions (MS-CHAPv2) ")

PPTP – Porquê a sua utilização?

- Um servidor RAS (*Remote Access Server*) está ligado normalmente à PSTN, RDIS ou rede X.25 permitindo a utilizadores remotos acederem ao servidor através dessas redes. Pode também estar ligado através de ligações permanentes (ADSL, cabo). O RAS permite aos utilizadores remotos acederem através da Internet utilizando *Point-to-Point Tunneling Protocol* (PPTP).

PPTP – Porquê a sua utilização?

- O PPTP é um protocolo de rede que suporta VPN multiprotocolo permitindo a utilizadores remotos acederem a redes empresariais de forma segura através da Internet ligando através da rede telefónica para o ISP ou ligando-se directamente à Internet (e.g. ADSL). O PPTP oferece as seguinte vantagens:
  - **Menores custos de transmissão:** O PPTP utiliza a Internet como suporte da ligação em vez de uma ligação telefónica de longa distância. Isto pode reduzir muito o custo das transmissões
  - **Custos de hardware mais baixos:** O PPTP permite que os *modems* e as cartas ISDN sejam separadas dos servidores RAS. Em vez disso podem ser localizdos num *pool* de *modems* ou num servidor de comunicações (resultando em menos *hardware* para um administrador adquirir e gerir)
  - **Menos custos administrativos:** Com o PPTP os administradores da rede podem gerir centralmente e manter seguros os acessos remotos aos seus RAS. Necessitam gerir apenas contas de utilizadores em vez de terem de dar suporte a configurações complexas de hardware
  - **Segurança melhorada:** Acima de tudo, a ligação PPTP através da Internet é cifrada e segura e funciona com qualquer protocolo (incluindo IP, IPX, e NetBEUI).

PPTP

- O PPTP tem alguns problemas por utilizar o MD4 na derivação das chaves devido a este já ter sido quebrado e ter sido provado que não é unidirecional, por isso nas propostas mais recentes (RFC 3079 - Deriving Keys for use with Microsoft Point-to-Point Encryption (MPPE)) é proposto o SHA como algoritmo de *hash*.

- O PPTP, apesar de tudo, é um dos tipos de VPN mais difundidos porque foi um dos primeiros protocolos disponíveis.

As funções do PPTP

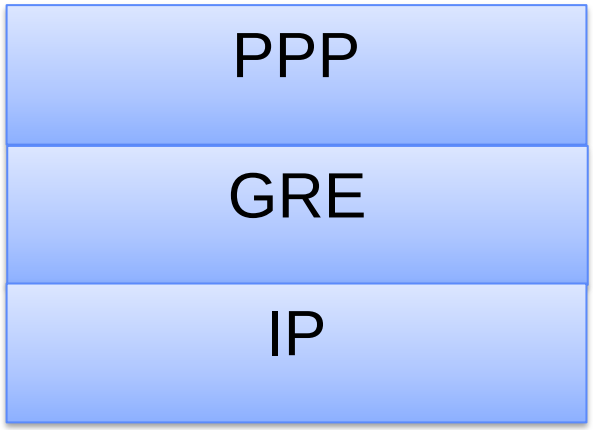
1. Fornecer um túnel

2. Usar a segurança construída no PPP para dar segurança à comunicação no túnel
   - Autenticação inicial do PPP

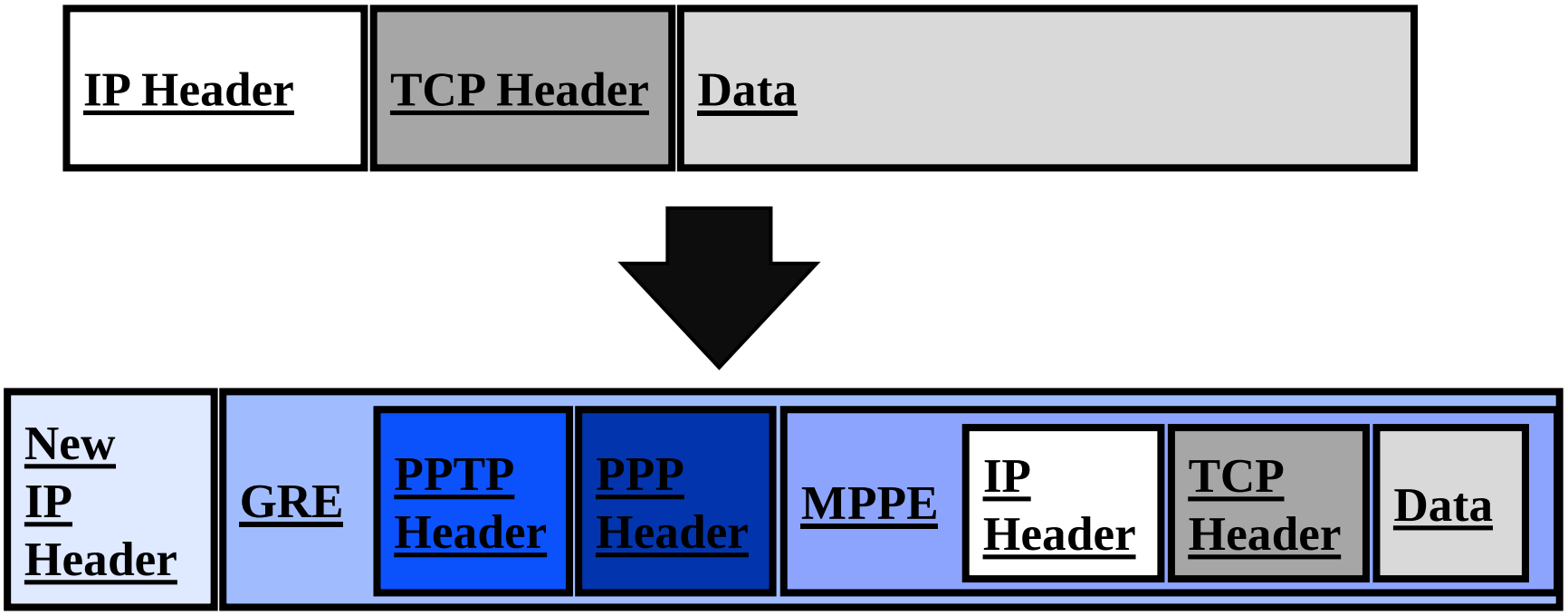
3. Confidencialidade nas trocas de dados sobre PPP usando o MPPE

PPTP

- **Protocolo**
  - Canal de dados: PPP sobre GRE sobre IP
  - Encapsula a camada de ligação (PPP), comunica ao nível da camada de rede (IP)
  - O *Call setup* é realizado num canal de controlo separado (TCP).



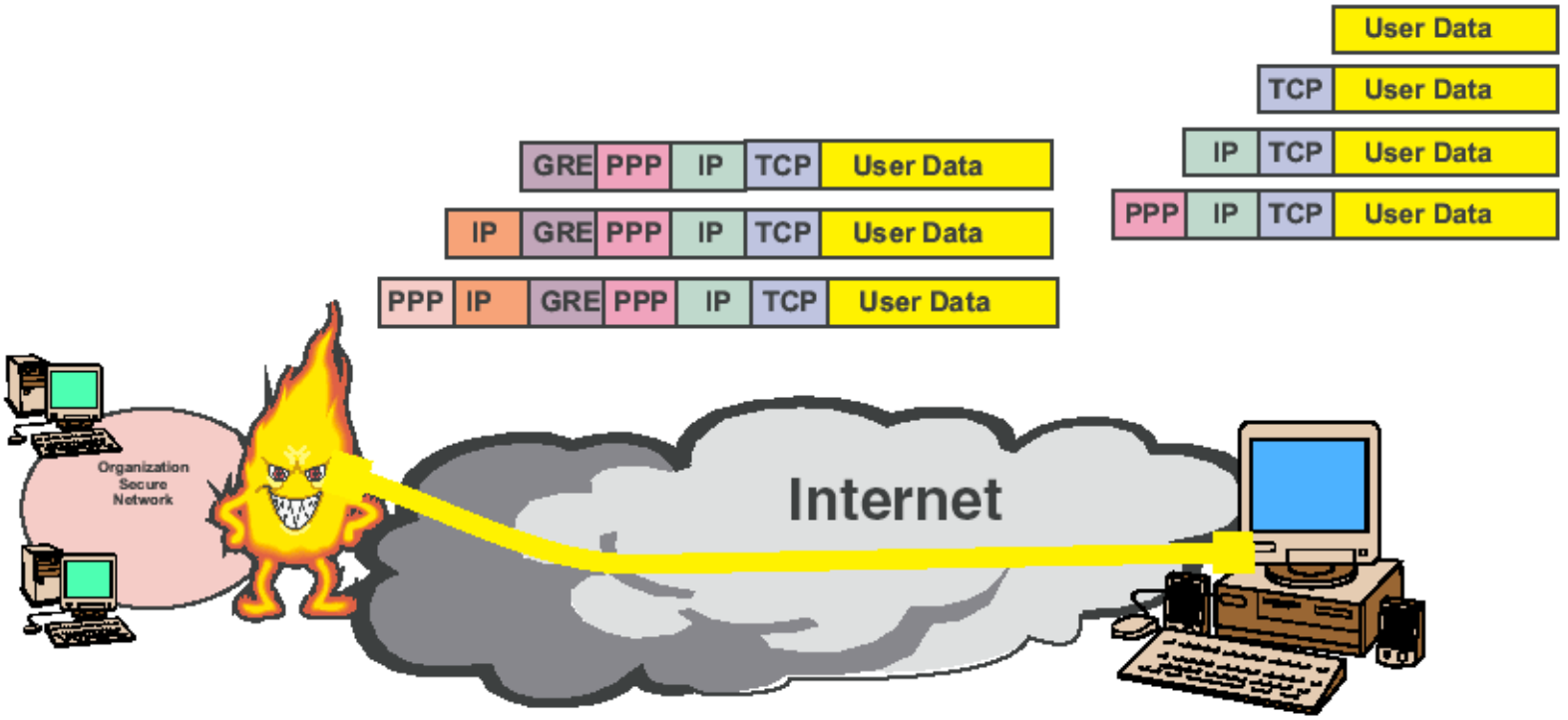
Datagrama IP transportando PPTP



Resumo da arquitectura PPTP

- A comunicação segura conseguida ao utilizar-se o protocolo PPTP tipicamente envolve três processos em que cada um deles requer que o anterior finalize com sucesso:
  - **Ligação PPP**: Um cliente PPTP utiliza PPP para se ligar a um ISP utilizando uma ligação telefónica normal ou uma linha ISDN. Esta ligação utiliza o protocolo PPP para estabelecer a ligação e cifrar os pacotes de dados.
  - **Controlo de ligação PPTP**: Utilizando a ligação à Internet estabelecida pelo protocolo PPP, o protocolo PPTP cria uma ligação de controlo desde o cliente PPTP até ao servidor PPTP no destino. Esta ligação usa o TCP para estabelecer a ligação e é designada por túnel PPTP.
  - **PPTP *data tunneling***: Finalmente o protocolo PPTP cria datagramas IP contendo pacotes PPP cifrados os quais são então enviados através do túnel PPTP para o servidor PPTP. O servidor PPTP desfaz o datagrama IP e decifra o pacote PPP e envia então o pacote decifrado para a rede final.

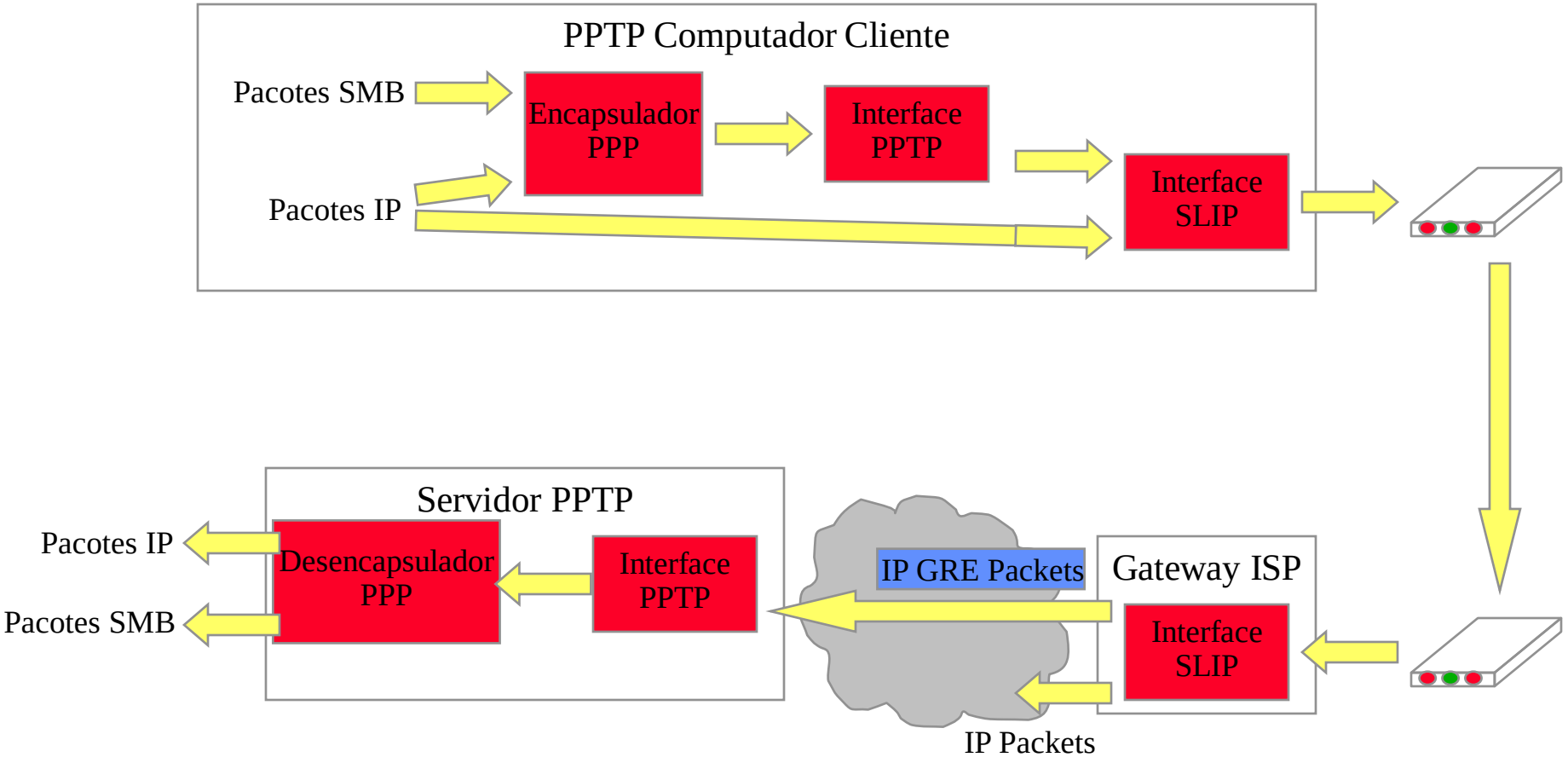
PPTP



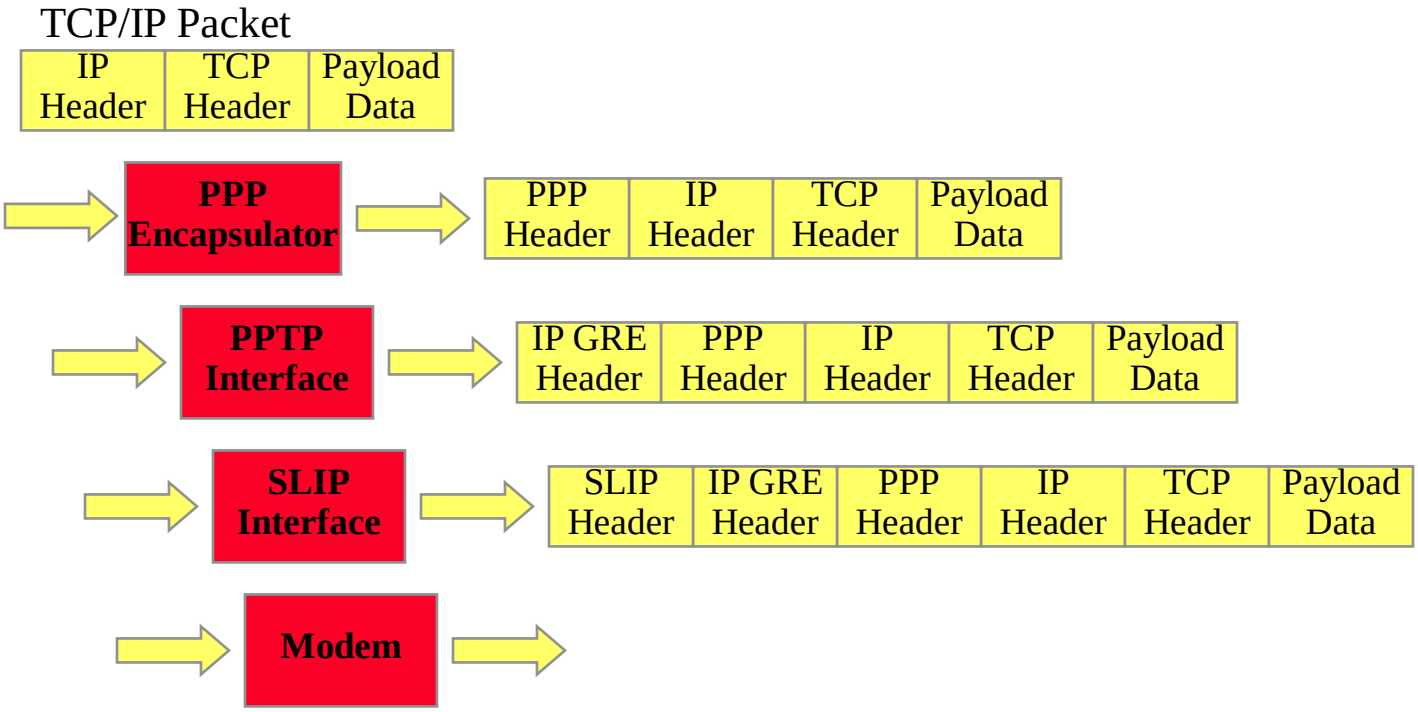
PPTP

- PPoE is Point-Point protocol over Ethernet
- Single tunnel between end-points : single device support (GRE = generic routing encapsulation)
- 6 bytes of overhead when compression used
- No tunnel authentication
- With RADIUS server supports authentication and accounting
- CHAP V2 fixes password, masquerading, and encryption weakness
- 40 or 128 bit RC4 packet encryption

PPTP: Exemplo dum túnel

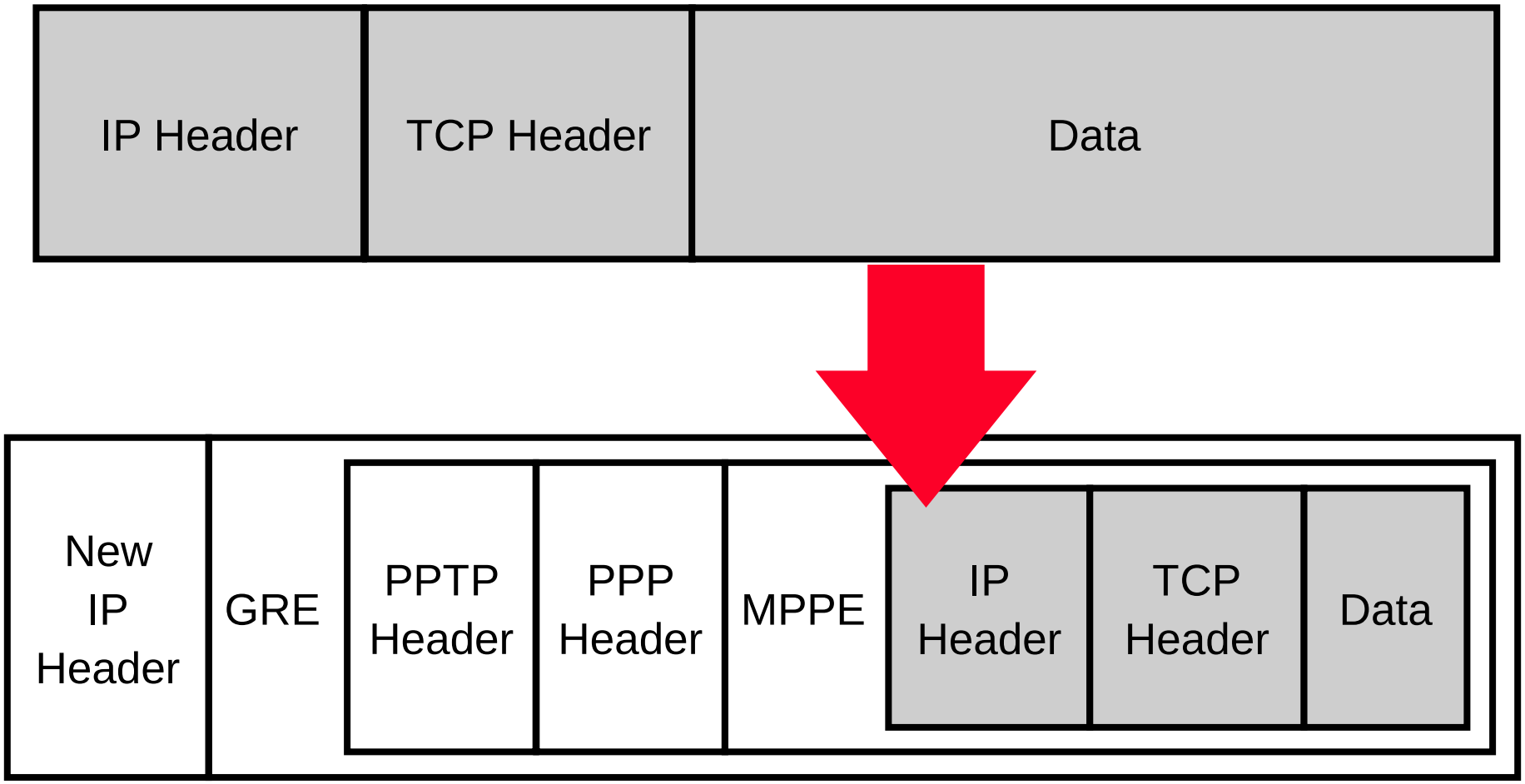


PPTP: Exemplo dum túnel

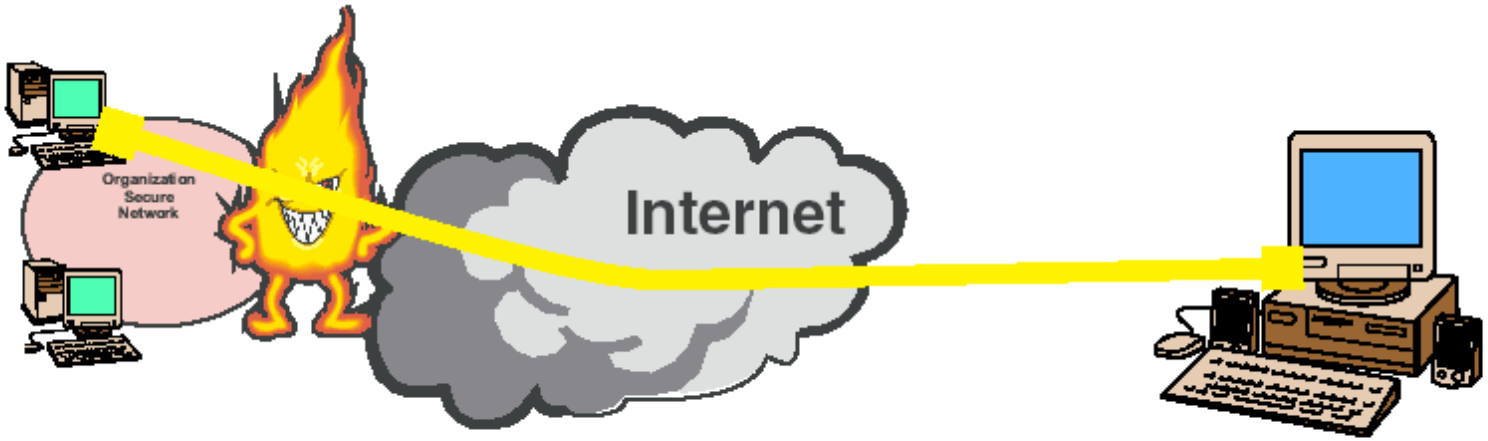


IP GRE tem problemas em muitos *firewalls*

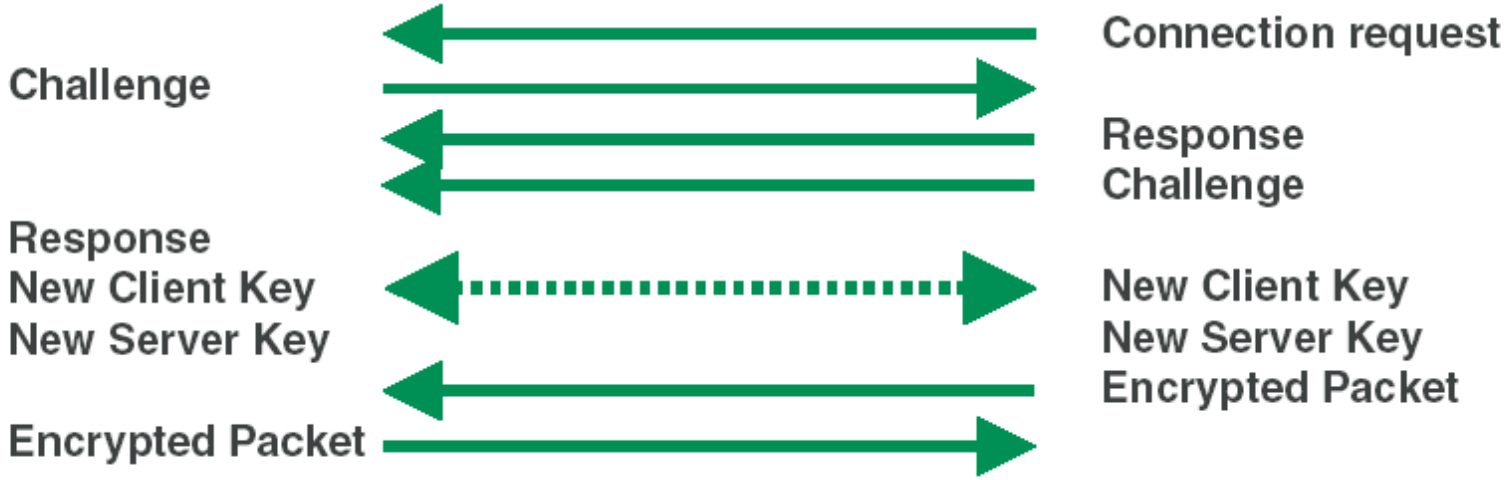
Encapsulamento PPTP



PPTP: Segurança



CHAP V2 Authentication with 40 or 128 bit RC4 encryption



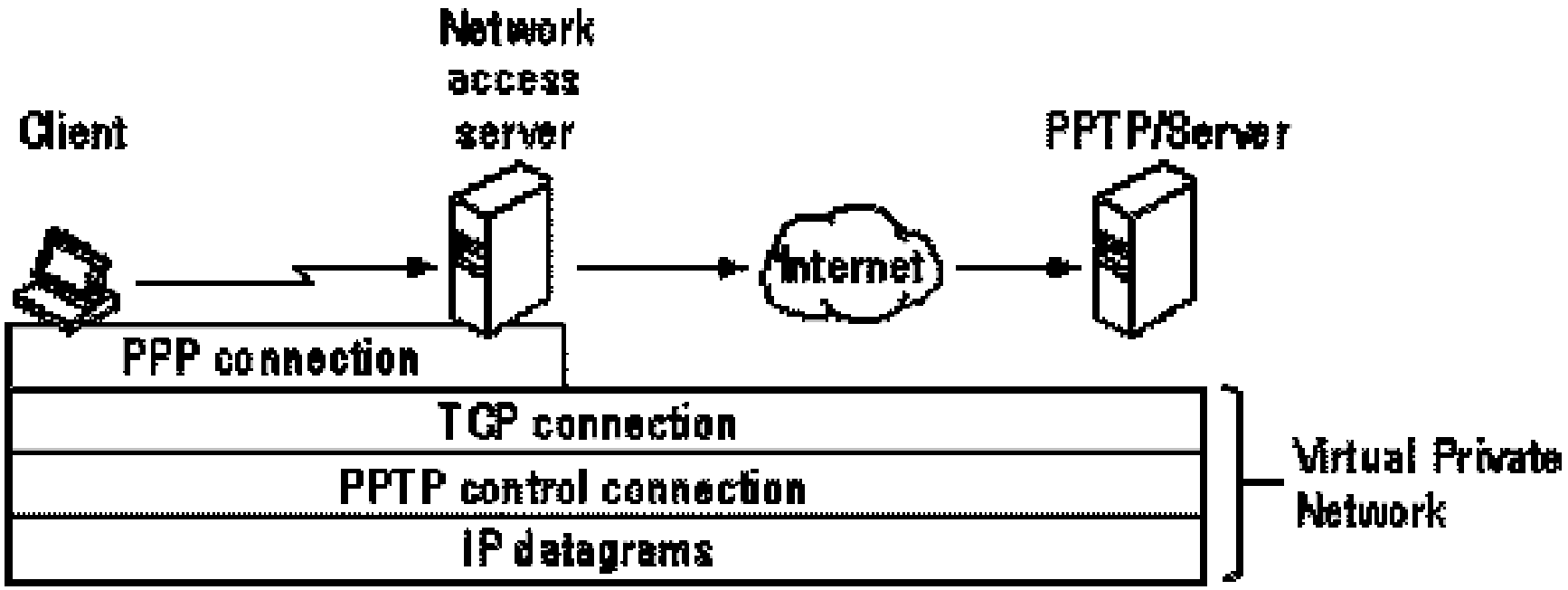
Estabelecimento da ligação

O estabelecimento da ligação inclui três fases básicas:

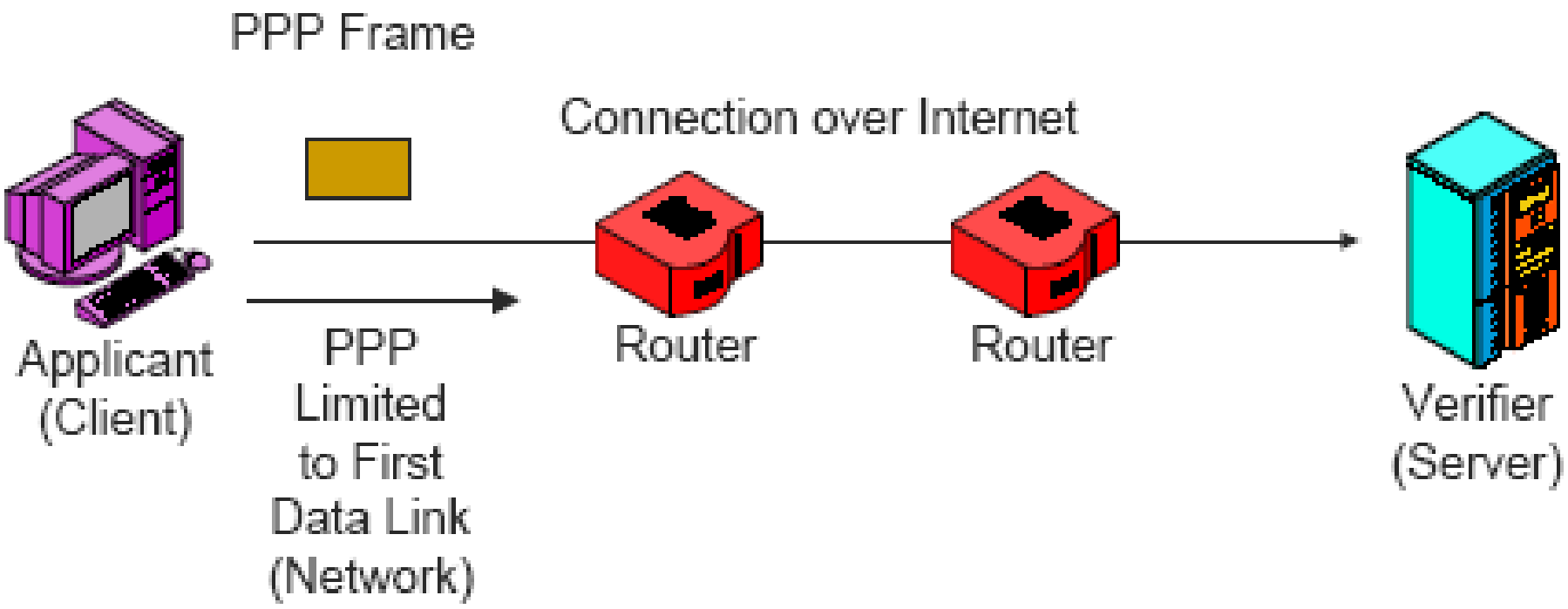
1. Estabelecer a ligação *dial-up* do cliente

2. Estabelecer a ligação de controlo PPTP (**TCP, porto 1723**)

3. Encapsulamento dos dados via protocolo IP (47 – *Generic Routing Encapsulation* (GRE))


Network
access
server
Client
PPTP/Server
Internet
PPP connection
TCP connection
PPTP control connection
IP datagrams
Virtual Private
Network

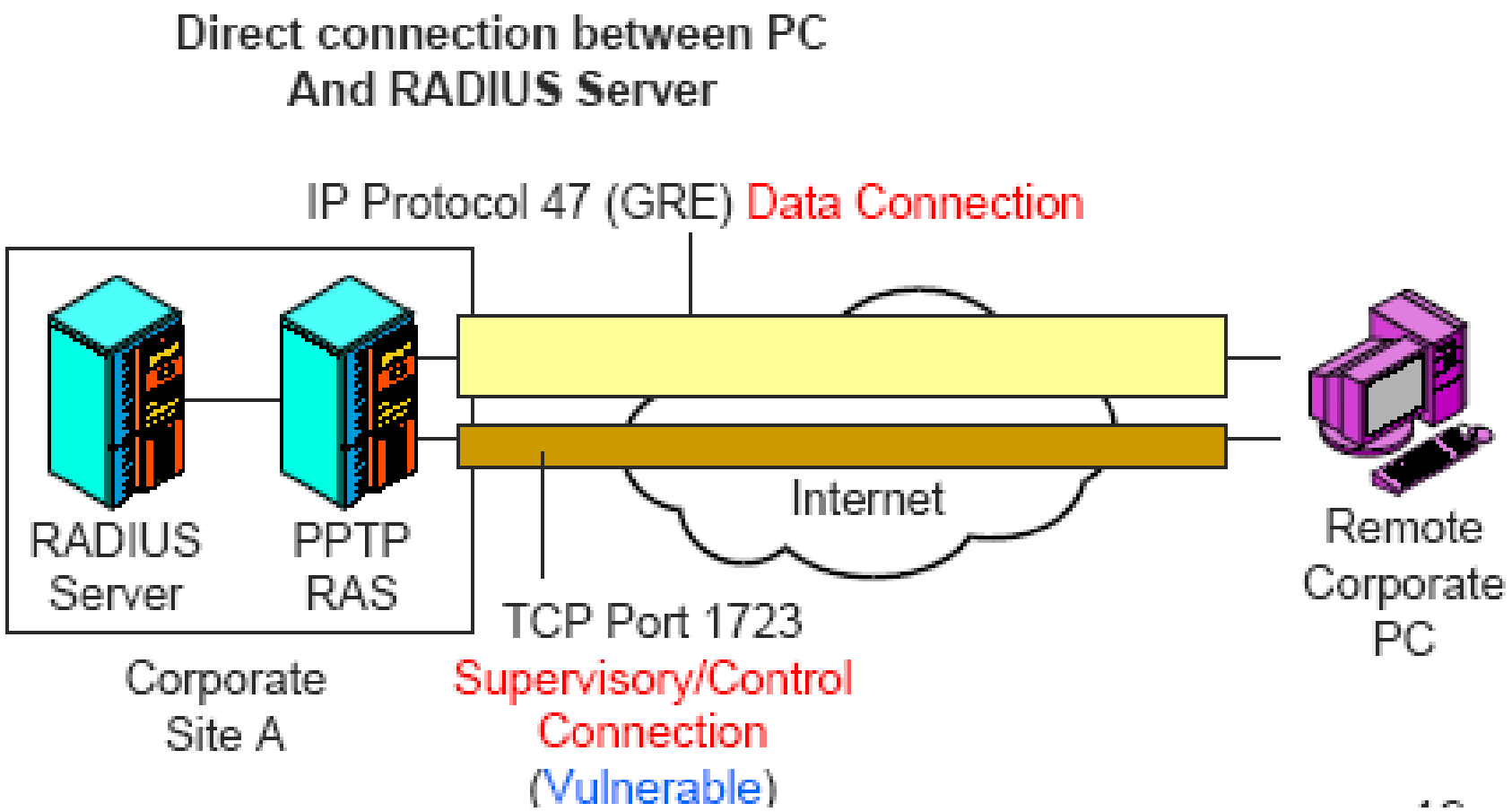
PPP em ligações directas e Internet



PPP em ligações directas e Internet

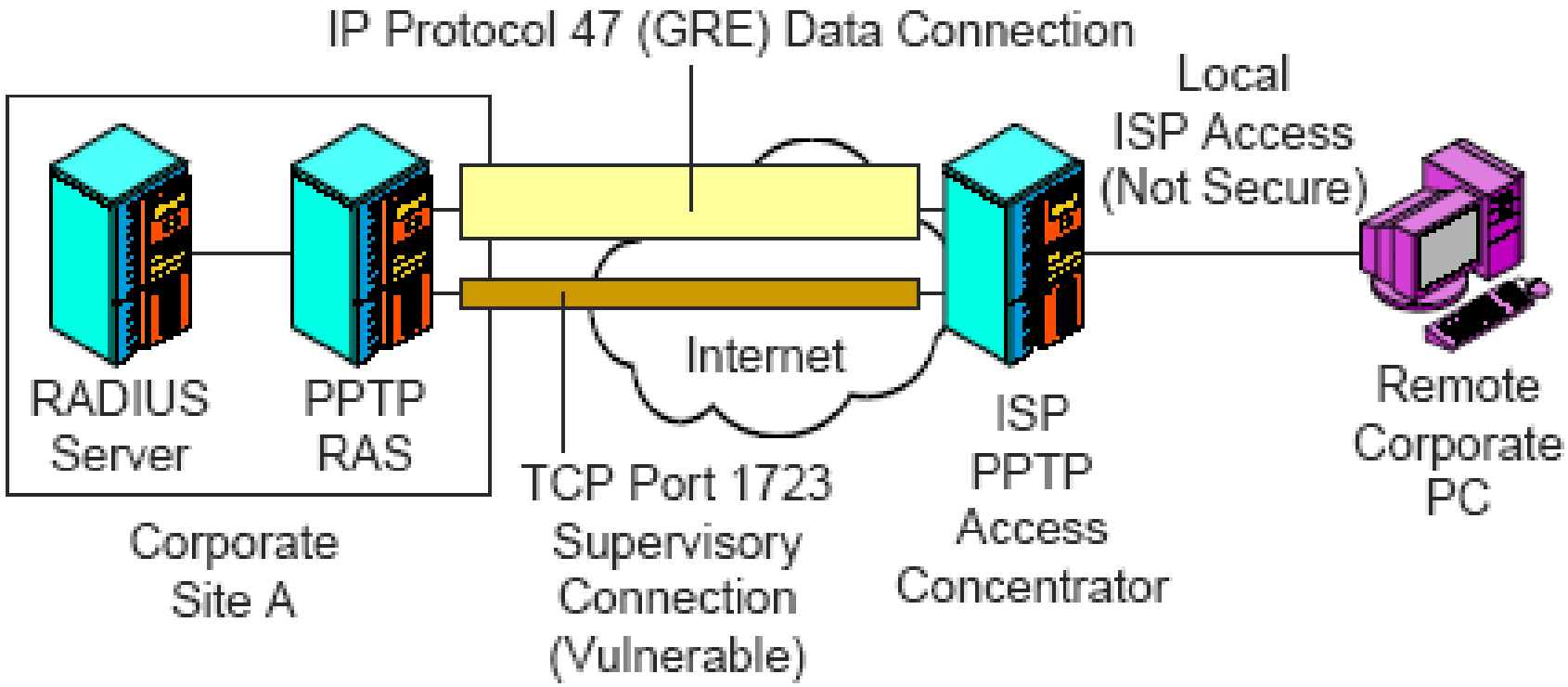
- **Nota:**
  - A utilização de túneis é realizada através da colocação de tramas PPP em datagramas IP, o qual entrega a trama. De facto o PPP é colocado num pacote GRE que é colocado num datagrama IP
  - Para o receptor é como se fosse uma ligação directa do PPP
  - Permite a uma empresa continuar a utilizar a segurança baseada no PPP tal como autenticação e cifra.

PPTP: Cliente *dial-in* remoto



- **Perspectiva de uma ligação directa (VPN de acesso remoto)**
  - A segurança extrêmo-a-extrêmo entre PC remotos e um RAS PPTP
  - O cliente tem de ser configurado para correr PPTP.

PPTP: Usando ISP



- **Perspectiva usando um ISP (VPN extremo-a-extremo)**
  - Nada tem de ser realizado no cliente, o qual se liga como se não houvesse segurança.
  - O concentrador de acessos PPTP faz todo o trabalho.
  - O túnel pode ser tornado obrigatório para se ter a certeza que é utilizado.
  - Não existe segurança na ligação entre o cliente e o ISP.

Vantagens

Vantagens:

- Oferece segurança média
- Ainda é muito usado porque está muito disponível
- O Windows nas suas várias versões dá suporte ao PPTP
  - Não é necessário adicionar software aos clientes dado este já vir incluído no sistema operativo
- Com a implementação no ISP não é necessário configurar o PPTP nos clientes.

Problemas

- A **negociação de parâmetros é feita sem qualquer** protecção ⇒ é possível **obter ou modificar dados.**
- As mensagens do **canal de controle** são transmitidas sem qualquer protecção de autenticidade ou integridade ⇒ **sequestro da ligação.**
  - Canal de controlo separado e não protegido utilizando o porto 1723 do TCP
- Não faz autenticação mensagem-a-mensagem.
- Problemas específicos do PPTP da Microsoft:
  - Formato de armazenamento de senhas **LanMan**
    - caracteres convertidos para *uppercase*
    - 14 caracteres = 2 cadeias de 7 caracteres
  - Chaves criptográficas baseadas na senha do utilizador.
- Fragilidades conhecidas do MS-CHAPv2