Administração de Sistemas (ASIST)

Redes privadas virtuais

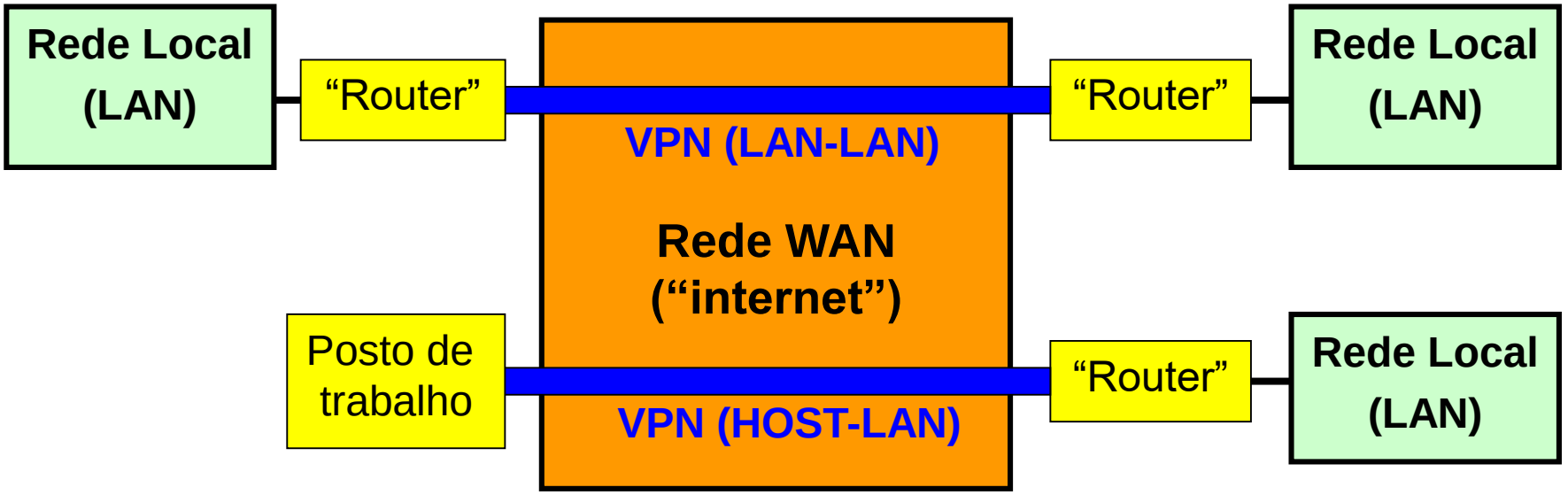
Novembro de 2014

Rede privada virtual ("VPN – Virtual Private Network")

Uma VPN é um túnel seguro (autenticação, confidencialidade e integridade) criado através de uma infra-estrutura de rede existente (WAN), usado para simular uma ligação física dedicada entre dois pontos.

Criado o túnel, os nós encaminham a informação através dele como se tratasse de uma ligação física ponto-a-ponto. O endereçamento usado na VPN e nas LAN interligadas é totalmente independente do endereçamento na rede WAN.

As VPN são uma forma económica de interligar de forma privada dois locais fisicamente distantes, mas acessíveis através da "internet".



VPN LAN-LAN e VPN HOST-LAN

Embora utilizando os mesmos protocolos podem classificar-se as VPN em:

- LAN-LAN – este tipo de VPN é criada pelo administrador por configuração dos dois nós nos extremos da ligação, tipicamente a VPN é permanente, sendo automaticamente estabelecida e mantida quando os nós arrancam. O administrador define regras de encaminhamento ("routing") para que o tráfego entre as duas LANs passe pela VPN em lugar de usar diretamente a WAN.

Os utilizadores das duas LAN utilizam a VPN de forma totalmente transparente como qualquer outra ligação física da infra estrutura de rede.

Uma vez que ambas as extermidades da VPN são administradas pela mesma entidade, a autenticação e confidencialidade recorre normalmente a certificados de chave pública ou uma chave pré-partilhada.

- HOST-LAN – também designada VPN de utilizador, é criada por iniciativa de um utilizador dirigindo um pedido a um servidor VPN, após autenticação o posto de trabalho recebe um endereço e dados de configuração (por exemplo via DHCP) correspondentes à LAN remota. No posto de trabalho é criada uma interface de rede virtual que é equivalente a uma interface física colocada na LAN remota.

“Layer 2 Tunneling Protocol” - L2TP

O L2TP apresenta todas as funcionalidades necessárias à implementação de redes privadas virtuais, contudo carece de garantias de autenticação e confidencialidade. Para implementar uma VPN o L2TP tem de ser aliado a um protocolo que garanta a comunicação segura, frequentemente o IPsec.

Os nós extremos dos túneis L2TP são designados LCCE (“L2TP Control Connection Endpoint”) de acordo com o tipo de dados transportados assumem outras designações mais específicas:

L2TP Access Concentrator (LAC) – quando são transportadas tramas de nível 2, opera como um comutador de rede.

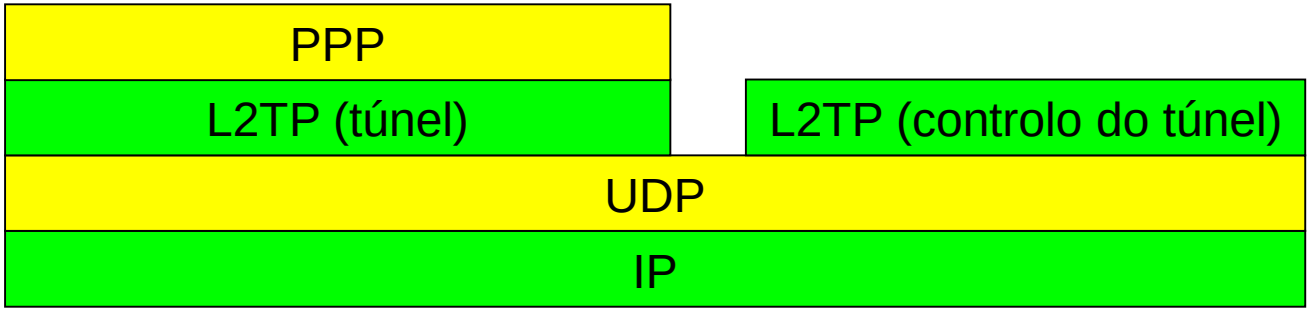
L2TP Network Server (LNS) – quando são transportados pacotes de nível 3, opera como um encaminhador de rede (“router”).

“Layer 2 Tunneling Protocol” - L2TP

O L2TP permite criar túneis para encaminhamento de dados através de redes existentes, na atual versão 3 (L2TPv3) pode encapsular a informação diretamente em “datagramas” IP ou em “datagramas” UDP.

Embora a utilização direta de IP seja mais eficiente, causa problemas quando existem dispositivos NAPT, por essa razão o UDP é mais usado.

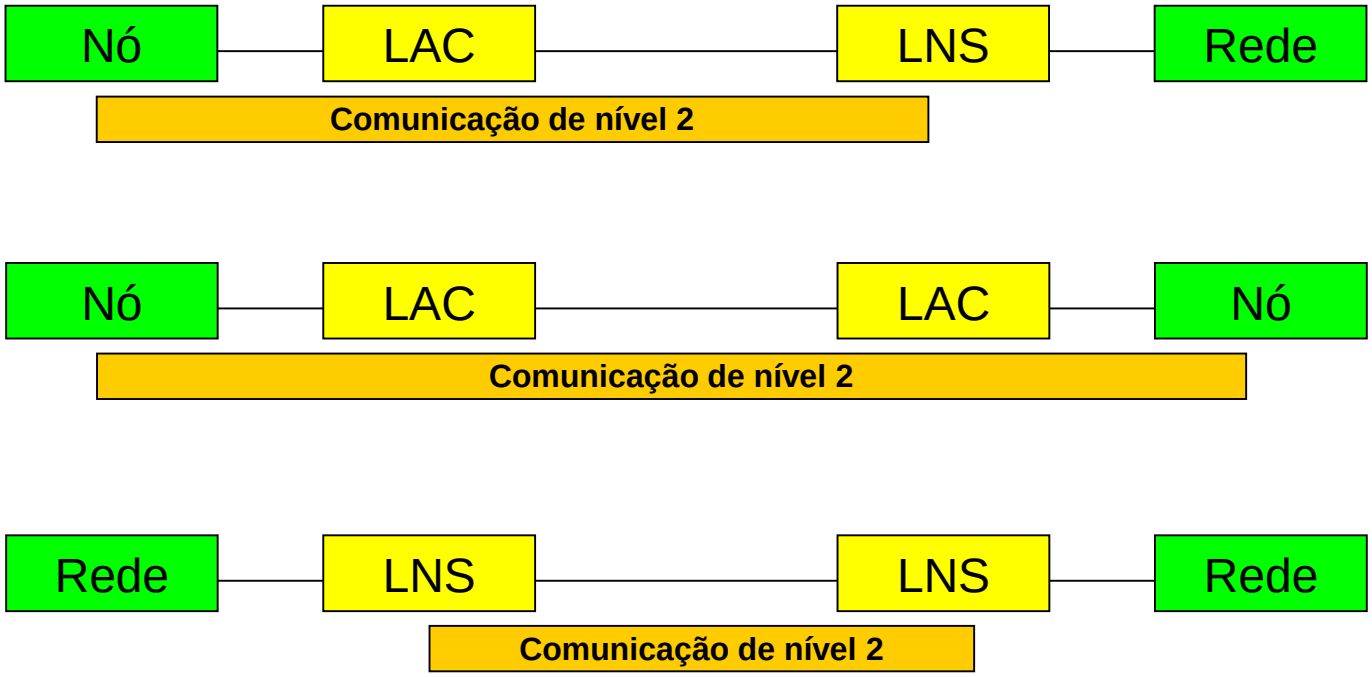
Tipicamente o objetivo do túnel é o transporte de pacotes, nesse caso opta-se por estabelecer uma sessão PPP através dele para controlar esse processo.



L2TP – sessões e topologias

Um túnel L2TP pode comportar múltiplas sessões, cada uma funcionando como um canal independente, um LCCE pode por isso ser simultaneamente LAC e LNS (em sessões distintas).

A topologia das sessões L2TP podem adotar 3 modelos de referência: LAC-LNS, LAC-LAC e LNS-LNS.



Um nó de rede ligado a um LAC pode ser um encaminhador de rede (“router”), nesse caso o conjunto torna-se equivalente a um LNS.

VPN L2TP/IPsec

O L2TP assegura a gestão túneis de comunicação independentes usados para transportar dados, possui todas as funcionalidades para implementar uma VPN desde que seja aliado a mecanismos que garantam a confidencialidade e autenticação.

O IPsec em modo de transporte ou túnel é um dos mecanismos mais usado para garantir a confidencialidade e a autenticação de dos túneis L2TP, mas pode ser complementado com a utilização do PPP através dos túneis:

1 – Utilização do IKE para negociar as SA

2 – Criação das SA e estabelecimento da ligação segura IPsec

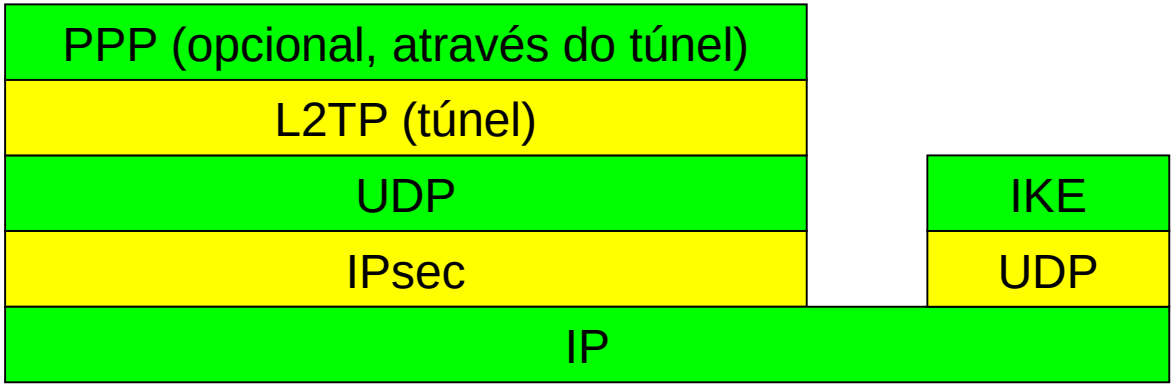
3 – Negociação e estabelecimento do túnel L2TP

4 – Autenticação de utilizador via PPP (opcional, VPN HOST-LAN)

VPN L2TP/IPsec

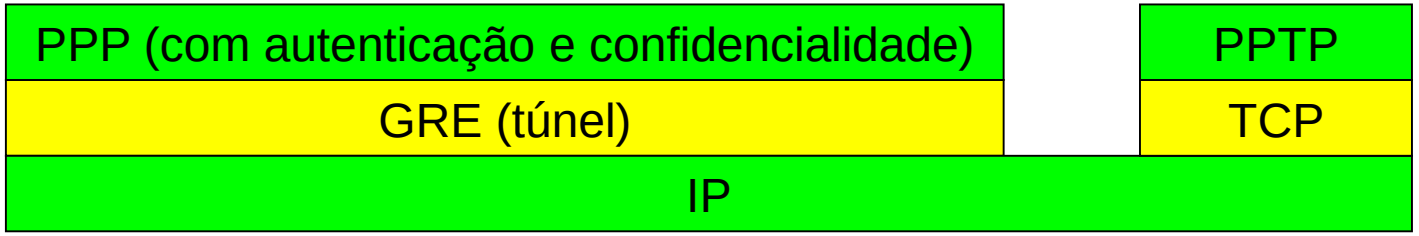
Embora o IPsec garanta a autenticação dos nós e a confidencialidade, não é muito adequado para autenticação de utilizadores (no contexto das VPN HOST-LAN).

Nesse caso muitas vezes opta-se por estabelecer uma ligação PPP através de um túnel L2TP permitindo então a autenticação segura do utilizador através de "password", por exemplo usando CHAP, ou mesmo PAP (uma vez que o túnel está protegido pelo IPsec.



PPTP – “Point-to-Point Tunneling Protocol”

O PPTP é um protocolo de VPN considerado menos seguro do que o L2TP/IPsec usa uma ligação de controlo TCP e os dados são encapsulados em pacotes GRE (“Generic Routing Encapsulation”) para criar um túnel através do qual se estabelece uma sessão PPP.



PPTP – “Point-to-Point Tunneling Protocol”

O facto de usar pacotes GRE, que não possuem números de porto cria problemas com “routers” que efetuam NAPT, tal como acontece com o IKE usado no IPsec.

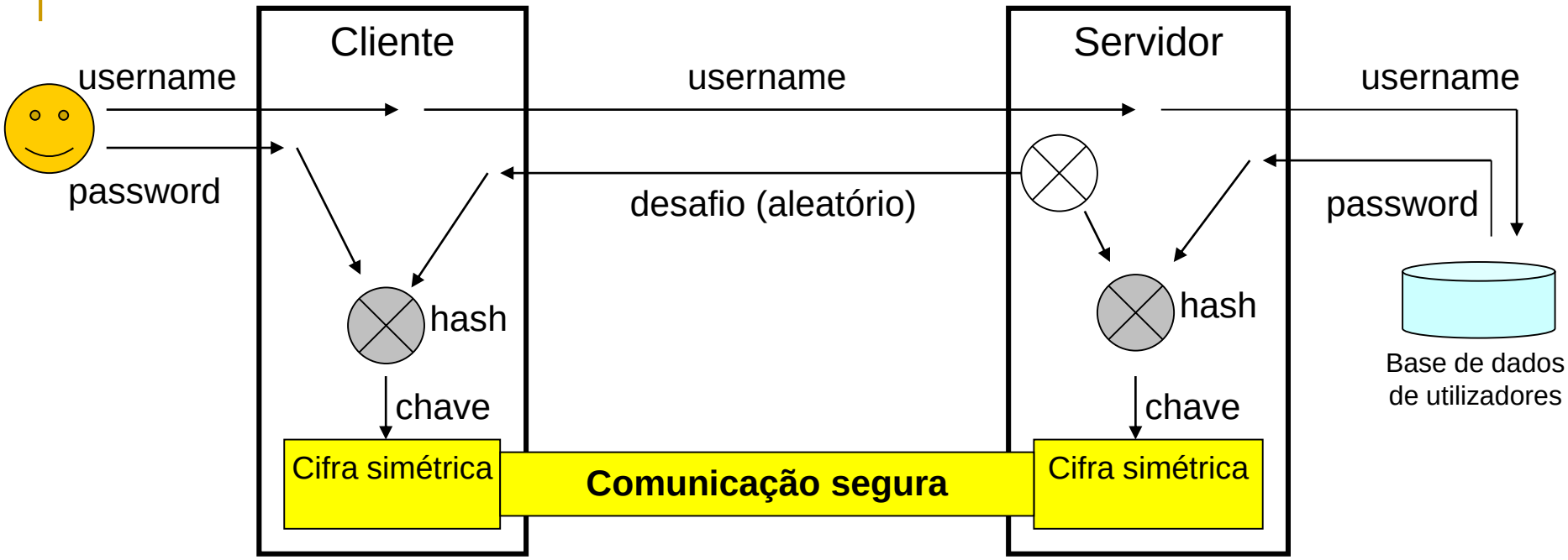
Os mecanismos de autenticação e confidencialidade são assegurados pelo PPP, o PPTP isoladamente não implementa confidencialidade nem autenticação.

Por ser simples garante uma boa performance e não exige certificados de chave pública, pelo que é popular, particularmente nas implementações HOST-LAN.

Uma das implementações mais divulgadas usa a autenticação MS-CHAPv2 para produzir a partir da “password” do utilizador uma chave simétrica para a cifra MPPE (“Microsoft Point-to-Point Encryption”). O MPPE é uma variante do RC4 que suporta chaves de 40, 80 e 128 bits.

Usando esta técnica consegue-se validar a autenticidade tanto do utilizador como do servidor. A sua fraqueza reside nas eventuais debilidades da “password” do utilizador.

PPTP + PPP + CHAP + MPPE (RC4)

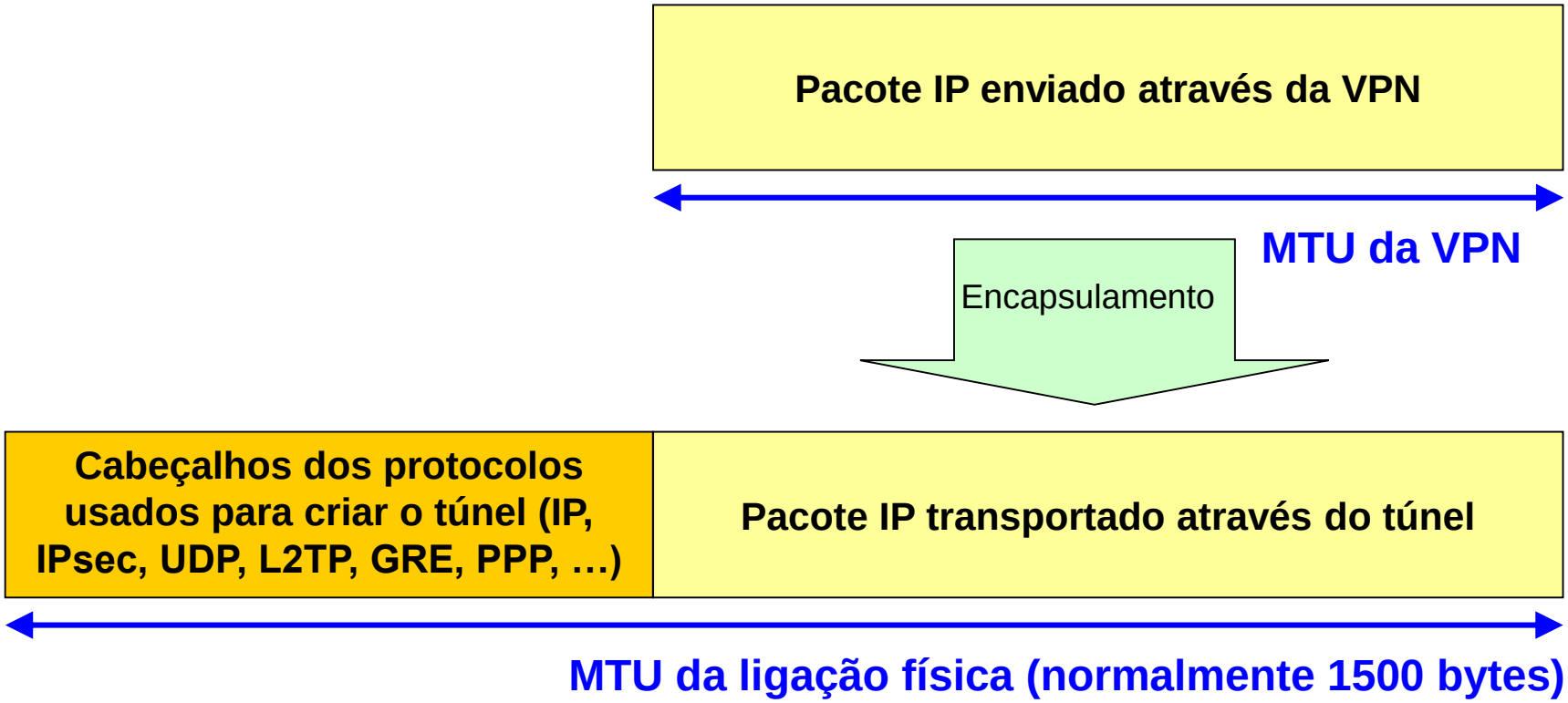


A chave deriva da “password” em conjunto com o desafio, uma vez que o desafio é acessível por “sniffing” um atacante precisa apenas de descobrir a “password” do utilizador.

O atacante tenta de forma massiva várias “passwords” (ataque de dicionário), procurando desta forma produzir a chave correta. Com as várias chaves que vai produzindo tenta desencriptar a informação que obteve da rede, se conseguir obter um resultado coerente é possível que tenha conseguido adivinhar a “password”.

Ligações VPN – MTU ("Maximum Transmission Unit")

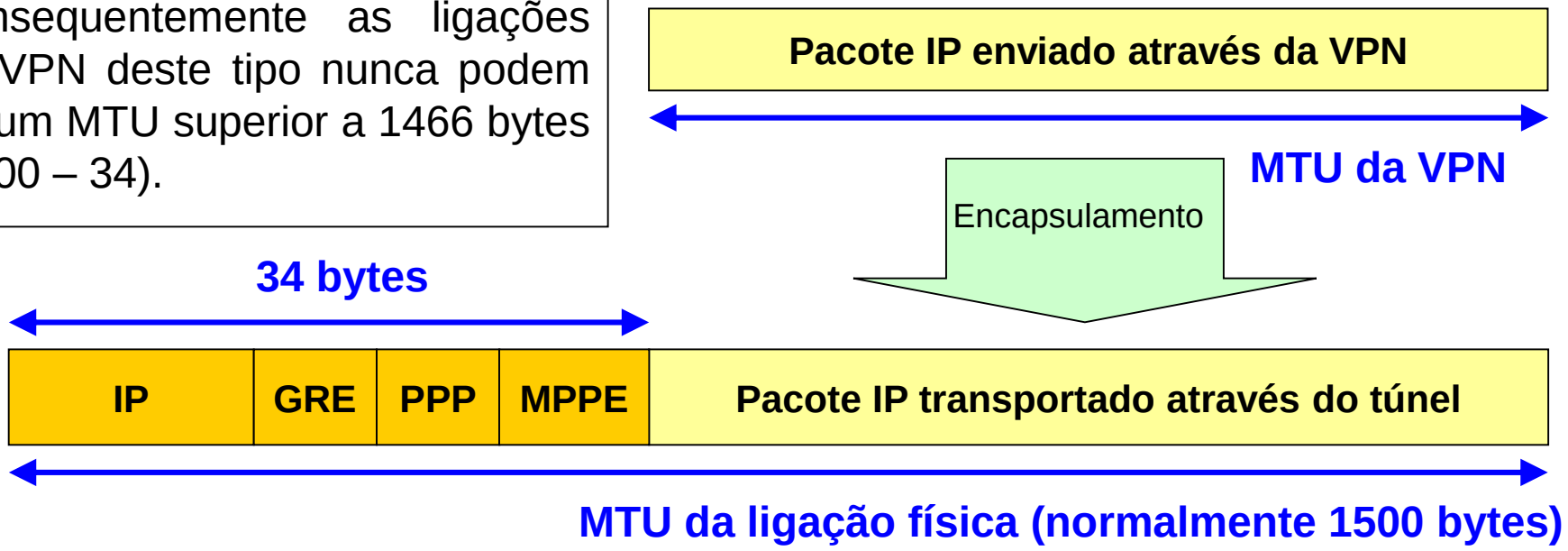
Os pacotes IP que atravessam uma VPN são transportados no interior de pacotes de outros protocolos (encapsulamento). Para não haver necessidade de fragmentação (pouco eficiente e nem sempre suportada) o MTU da ligação de VPN tem de ser inferior ao MTU da ligação física (normalmente 1500 bytes).



Exemplo PPTP – MTU

Tomando com exemplo as implementações mais comuns do PPTP, para criar o túnel são usados os seguintes protocolos com cabeçalhos das seguintes dimensões: IP (20 bytes) + GRE (4 bytes) + PPP (8 bytes) + MPPE (2 bytes)

Consequentemente as ligações de VPN deste tipo nunca podem ter um MTU superior a 1466 bytes (1500 – 34).



Nas extremidades da VPN o MTU deve ser definido de forma adequada, nas implementações HOST-LAN este dado é fornecido pelo servidor ao cliente.

MTU – fragmentação de pacotes na VPN

Desde que se defina os MTU corretos nas interfaces das extremidades da VPN e se permita a operação normal do protocolo PMTUD (deixar passar as respetivas mensagens ICMP) o facto de o MTU ser ligeiramente inferior a 1500 bytes não tem qualquer inconveniente.

Uma outra abordagem ao problema é garantir na VPN o MTU de 1500 bytes recorrendo à fragmentação. Algumas implementações de VPN (por exemplo da CISCO) baseadas em GRE, IPsec e L2TP suportam esta funcionalidade. Os pacotes demasiado grandes são fragmentados antes de serem enviados através da VPN e são reagrupados no extremo oposto.

Mesmo sendo aplicada apenas entre os dois “routers” nas extremidades da VPN, a fragmentação tende a tornar a ligação mais lenta por sobrecarga dos “routers” e é normalmente preferível definir os valores de MTU adequados nas interfaces e confiar no funcionamento do PMTUD.

Referências bibliográficas

[1] Lhamas A. (2010-2011). Aulas Teóricas de ASIST.

(…)