Redes de Computadores

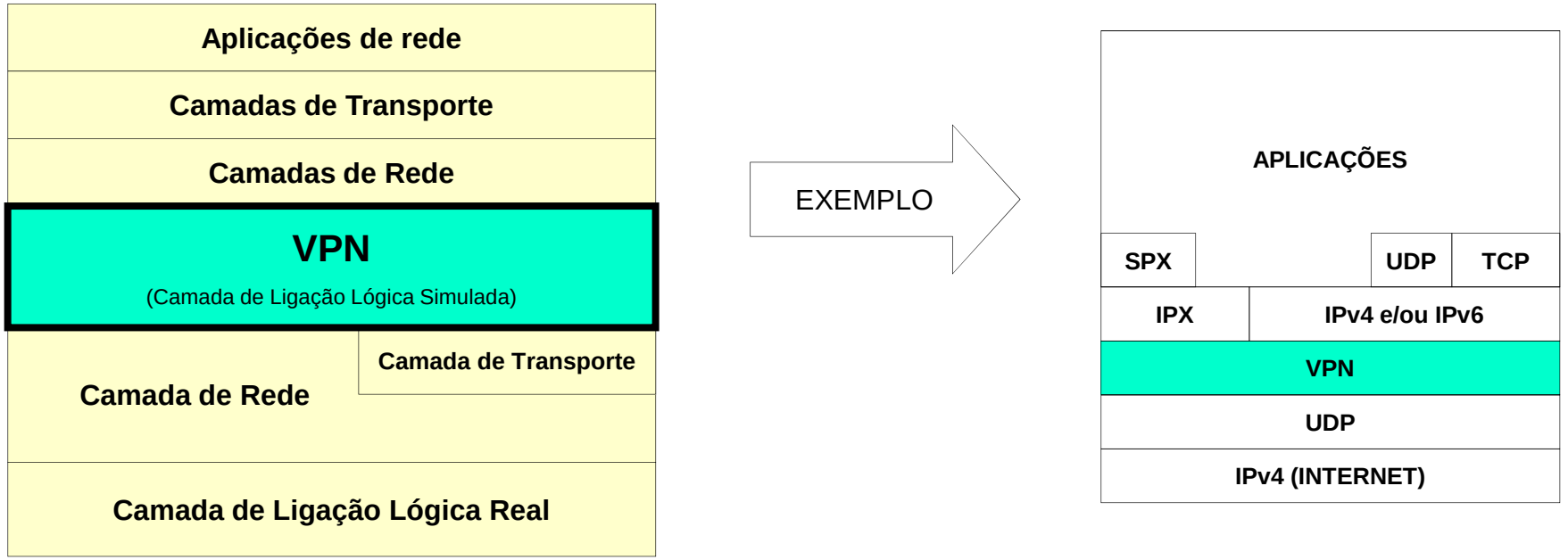
(RCOMP – 2015/2016)

Redes Privadas Virtuais (VPN)

Protocolo PPP

Virtual Private Network (VPN)

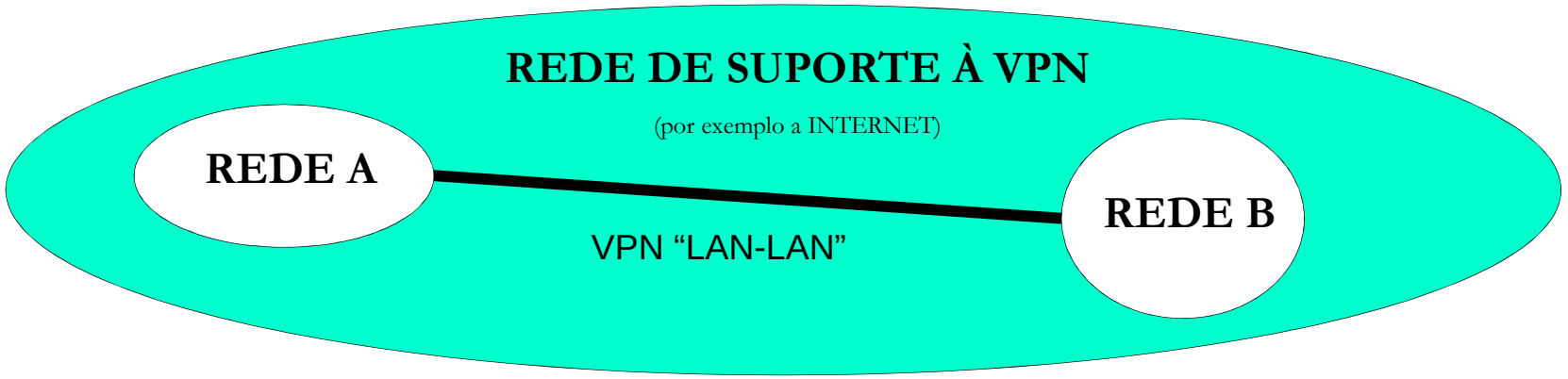
Uma VPN é uma infraestrutura de comunicação de nível 2 (camada de ligação lógica) que é simulada sobre uma outra rede, tipicamente uma infraestrutura de nível 3 (Camada de rede).



A designação VIRTUAL tem origem no facto de se tratar de uma infraestrutura simulada (não real), normalmente uma ligação “ponto-a-ponto”; PRIVADA advém do facto de serem usados mecanismo de segurança que garantem a confidencialidade dos dados que circulam na VPN.

VPN LAN-LAN (“Site-to-Site VPN”)

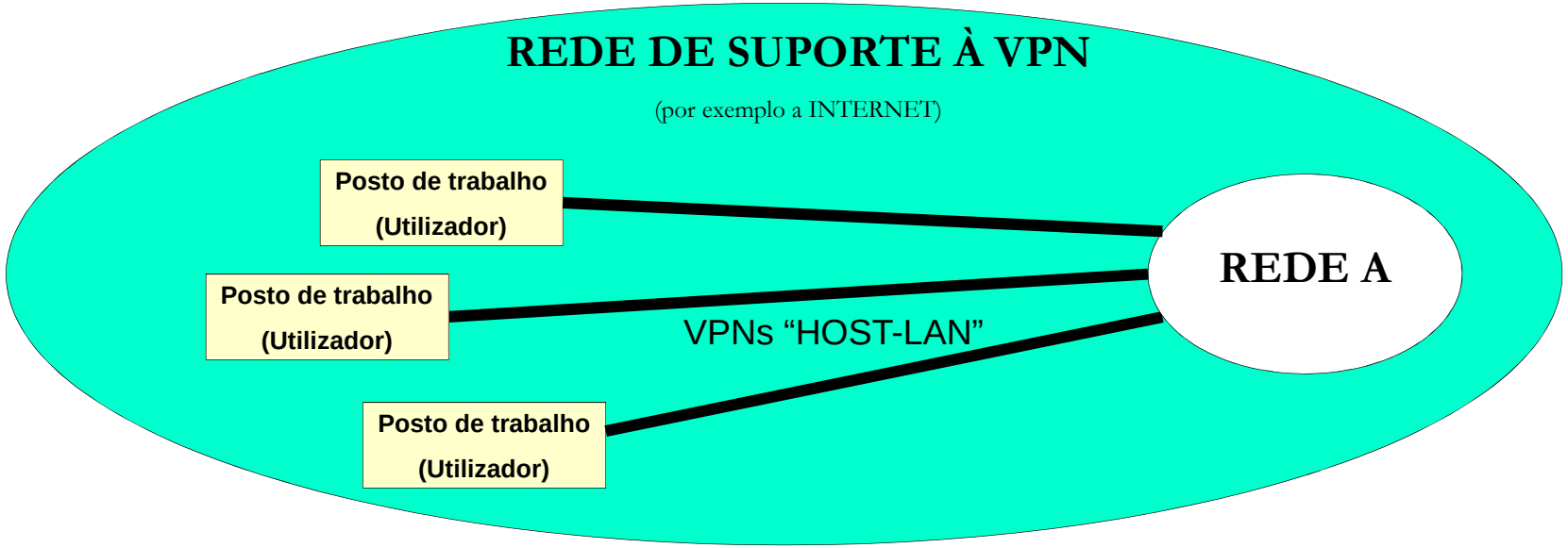
Embora idênticas sob o ponto de vista de funcionamento, podem considerar-se dois tipos de aplicação diferente das VPN: LAN-LAN e HOST-LAN.
As VPN LAN-LAN destinam-se a interligar redes, são implementadas pelos administradores das redes como outro qualquer tipo de ligação entre duas redes.



Os utilizadores das redes usufruem desta ligações VPN sem necessidade de conhecerem a sua existência. Dadas as suas características devem ter um carácter permanente, podendo ser estabelecidas e recuperadas automaticamente sem intervenção manual.

VPN HOST-LAN (“Remote-Access VPN”)

As VPN HOST-LAN servem para ligar nós individuais a uma rede remota. Tipicamente uma VPN deste tipo é criada por iniciativa do utilizador de um posto de trabalho, recorrendo a uma aplicação cliente instalado no posto local que comunica com um servidor na rede remota.

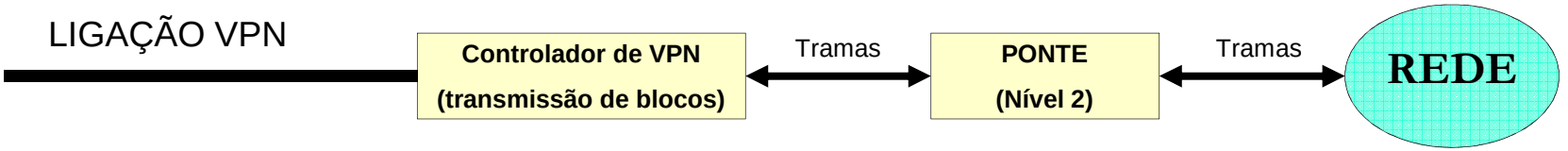


Neste tipo de VPN, o controlo de acesso baseia-se na autenticação do utilizador, após esse processo o posto de trabalho recebe um endereço de rede pertencente à rede remota que lhe permite operar como se estivesse diretamente ligado a essa rede.

Interligação de redes por VPN – Nível 2

Uma VPN tem como objetivo simular uma ligação física "ponto-a-ponto". A forma como esta ligação pode ser usada para interligar redes remotas depende dos objetivos e muitas vezes das restrições impostas pelo próprio protocolo da VPN.

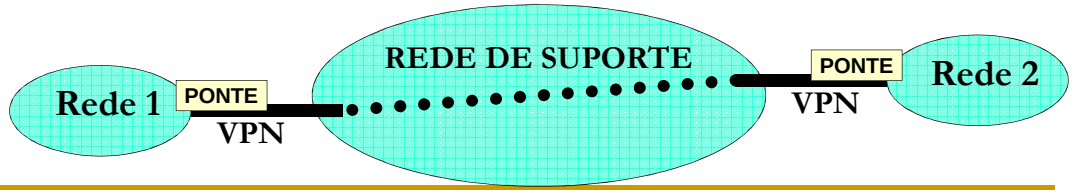
A interligação por VPN no nível 2 consiste na retransmissão de tramas de nível 2 através da VPN, a VPN comporta-se então como uma ponte (*bridge*).



Todos os dados que circulam em tramas numa das redes propagam-se até à rede remota, independentemente do protocolos em causa. As duas redes interligadas são obrigatoriamente do mesmo tipo, caso contrário os formatos de trama seriam diferentes. Sob o ponto de vista das camadas superiores, as duas redes passam a ser apenas uma única.

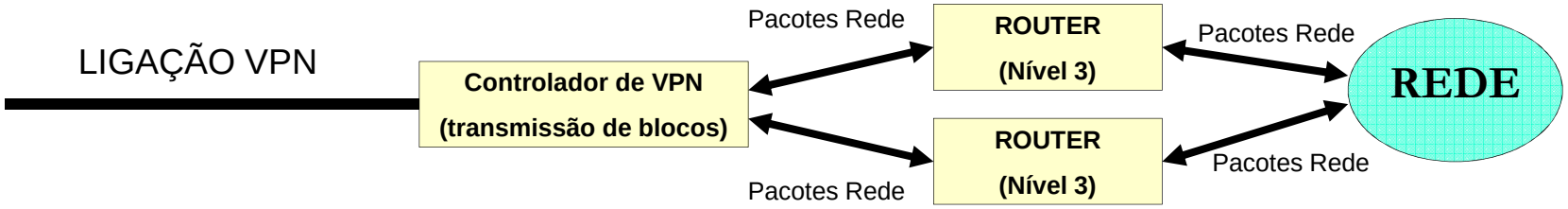
O tráfego de *broadcast* de nível 2 propaga-se através da VPN, permitindo o funcionamento de protocolos tais como o ARP.

A "Rede 1" e a "Rede 2" funcionam como dois segmentos de uma mesma rede local, interligados por uma ponte. Por exemplo sob o ponto de vista IP, são apenas uma rede.



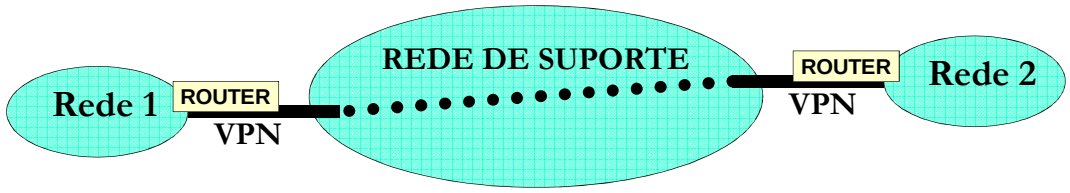
Interligação de redes por VPN – Nível 3

A interligação por VPN no nível 3 consiste na retransmissão de pacotes de rede através da VPN, a VPN comporta-se então como um encaminhador (*router*).
Se houver necessidade de suportar vários protocolos de rede serão necessários vários encaminhadores em paralelos (*router* multiprotocolo).



Como as redes não estão ligadas no nível 2 o tráfego em *broadcast* não passa através da VPN. As redes interligadas mantêm-se separadas no nível 2 e irão por isso constituir redes distintas sob o ponto de vista dos protocolos de nível 3.

Por exemplo, sob o ponto de vista IP, a "Rede 1" e a "Rede 2" são duas redes distintas, cada uma exigindo o seu espaço de endereçamento independente.
No exemplo a própria ligação VPN pode exigir endereços de rede para a ligação ponto a ponto entre os dois encaminhadores.



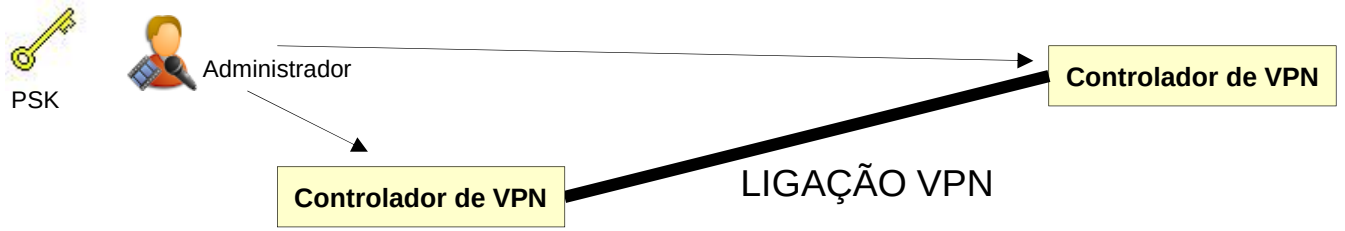
Segurança das VPN

Tratando-se transferências de dados que usam infraestruturas potencialmente inseguras e nas quais é possível todo tipo de intervenções de terceiros, a introdução de mecanismos de segurança é fundamental.

Autenticação
Garantir a autenticidade dos intervenientes (nós da VPN) ou seja, máquinas/servidores ou utilizadores.

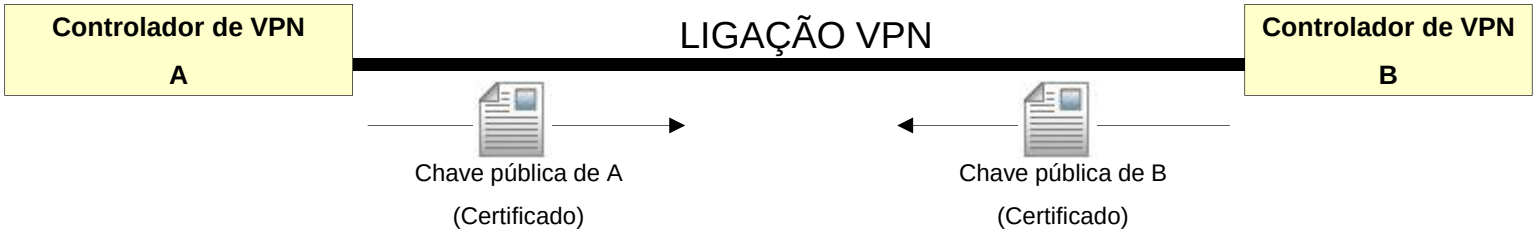
Privacidade
Garantir que os dados que são transferidos pela VPN não serão acessíveis e terceiros. Dado que se trata de redes públicas não é possível controlar o acesso, logo é necessário recorrer à cifragem.

A técnica de cifragem convencional é conhecida por criptografia simétrica e implica a partilha entre os dois envolvidos de uma chave secreta (PSK – *Pre Shared Key*).
Sendo um segredo pré-partilhado, este é um bom mecanismo de autenticação. Se uma das partes não possui a chave correta não vai poder comunicar. A operação de distribuição da chave pode ser complicada, na sua versão mais simples é realizada pelo administrador das duas extremidades da VPN.

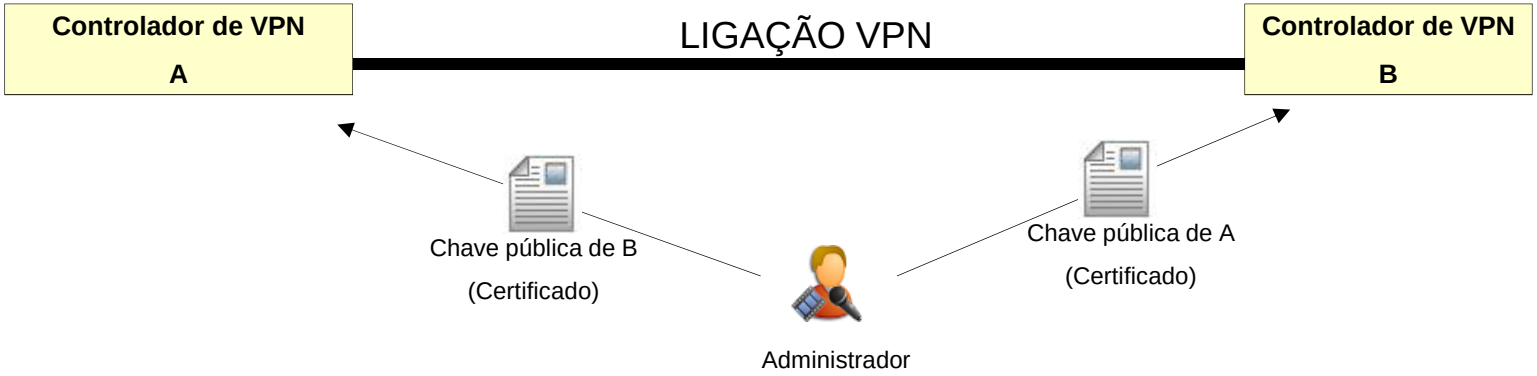


VPN – Chaves públicas

A técnica de cifragem conhecida por criptografia de chave pública veio resolver de forma radical as dificuldades na distribuição das chaves. Ao contrário dos algoritmos simétricos anteriores, em que existe uma única chave que tem de ser mantida secreta a todo o custo, agora a chave usada para cifrar é pública, mas não serve para decifrar, isso é conseguido com uma outra chave designada de privada. A vantagem é que a chave privada nunca tem de ser transferida.

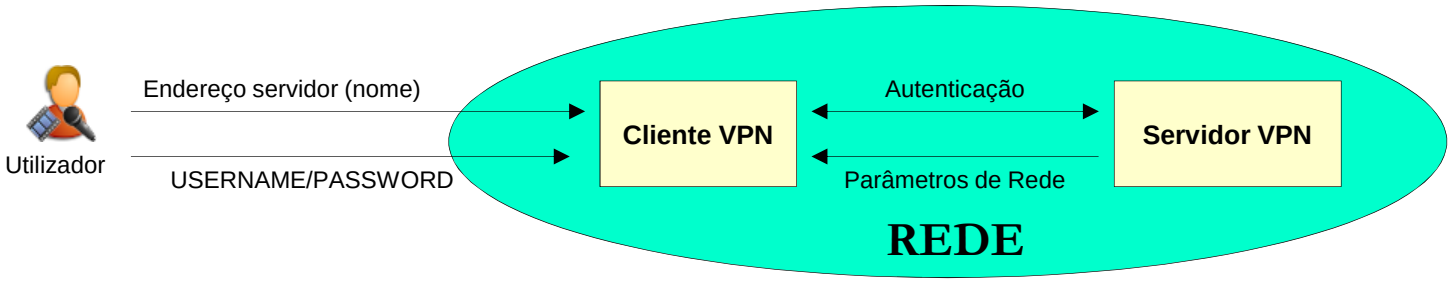


Os certificados são um elemento importante porque garantem a autenticidade dos intervenientes, se os nós forem controlados pelo mesmo administrador (VPN LAN-LAN) os certificados podem ser instalados manualmente para maior segurança.



VPN de utilizador

Uma VPN de utilizador é tipicamente uma VPN HOST-LAN e caracteriza-se por ser criada por iniciativa do utilizador. Para esse efeito os dois nós da VPN assumem mais claramente uma relação cliente – servidor. O cliente contacta o servidor no endereço de rede fornecido pelo utilizador, será então exigido ao utilizador elementos de autenticação, habitualmente constituídos pelo par "NOME-DE-UTILIZADOR + PASSWORD". Posteriormente o servidor fornece ao cliente os parâmetros de configuração de rede para o cliente poder funcionar.



O par "NOME-DE-UTILIZADOR + PASSWORD" serve como autenticação do utilizador perante o servidor VPN que faz assim o controlo de acesso ao serviço.
Se para o servidor é importante verificar a autenticidade do cliente (utilizador), também para o utilizador do serviço é importante ter algumas garantias, não convém que a PASSWORD seja entregue ao "primeiro servidor que aparecer".

VPN de Utilizador – Autenticação com chave pública

As VPN de utilizador caracterizam-se por:

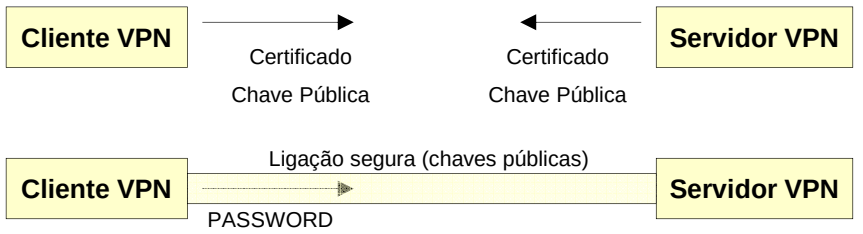
- Autenticação de utilizador por USERNAME/PASSWORD
- Servidor sem conhecimento prévio da existência do cliente.
- Número elevado de clientes/utilizadores para cada servidor.

Sendo a autenticação do utilizador garantida por PASSWORD, também é necessário garantir a autenticidade do servidor e um manuseamento seguro da PASSWORD do utilizador. Dadas as características particulares alguns métodos não são praticáveis, é o caso do PSK devido ao elevado número de clientes/utilizadores. Embora possam ser combinados de várias formas existem duas abordagens em uso: com chave pública e com chave secreta.

CHAVE PÚBLICA

Nesta abordagem começa-se por criar uma ligação segura e autenticada com base em certificados de chave pública que cada um envia ao parceiro. É particularmente importante a validação do certificado de chave pública do servidor por parte do cliente.

Através da ligação segura criada é possível então enviar a PASSWORD para autenticação do utilizador.

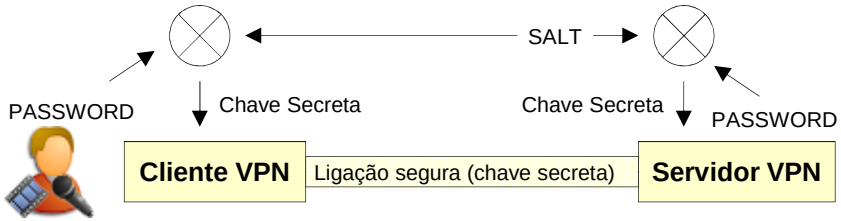


VPN de Utilizador – Autenticação com chave secreta

Para se conseguir distribuir uma chave secreta por cliente e servidor e simultaneamente autenticar ambos pode-se lançar mão de um segredo que mais ninguém conhece: “a PASSWORD do utilizador”.

Um algoritmo produz uma chave secreta usando a PASSWORD, então reproduzindo o processo nos dois pontos temos uma chave secreta:

CHAVE SECRETA = HASH (SALT + PASSWORD)

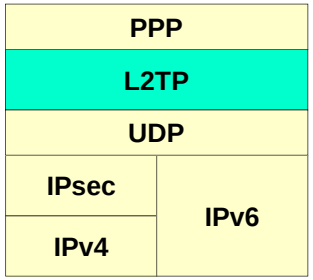


Como a chave é secreta, tal como acontecia no PSK, o simples facto de a ligação segura funcionar autentica os intervenientes. Note-se que a PASSWORD nunca é transmitida.

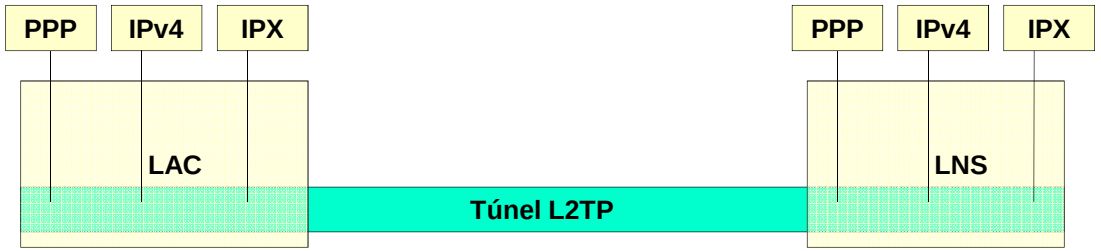
O sistema é de uma forma geral seguro, contudo baseia-se na PASSWORD do utilizador, esse é o seu ponto fraco, se a PASSWORD do utilizador é deficiente tudo pode ficar comprometido para esse utilizador.
O protocolo CHAP (*Challenge-Handshake Authentication Protocol*) baseia-se nestes princípios de funcionamento.
A necessidade de o servidor conhecer a PASSWORD do utilizador pode ser um obstáculo à sua implementação em alguns tipos de sistema, como por exemplo os da família Unix.

L2TP - Layer 2 Tunneling Protocol

O L2TP é um dos tipos de VPN com mais utilização, foi desenvolvido pela Microsoft e pela Cisco, mas está normalizado em várias RFC's.
O L2TP é um protocolo de túnel simples, não implementa mecanismos de autenticação nem de privacidade. Normalmente a autenticação é assegurada pelo protocolo PPP e a confidencialidade é assegurada pelo IPsec.
O IPsec, parte integrante do IPv6 e um protocolo extra no IPv4, permite criar ligações seguras e autenticadas, baseadas quer em chaves secretas pré-partilhadas (PSK), quer em certificados de chave pública. A missão do L2TP é criar os túneis e transferir o respetivo tráfego.



O L2TP cria os túneis usando o modelo cliente/servidor, o LNS (*L2TP Network Server*) é contactado no porto UDP 1701 pelo LAC (*L2TP Access Concentrator*) para se estabelecer o túnel. Cada túnel é ainda dividido em sessões, para cada protocolo acima do L2TP será usada uma sessão diferente.

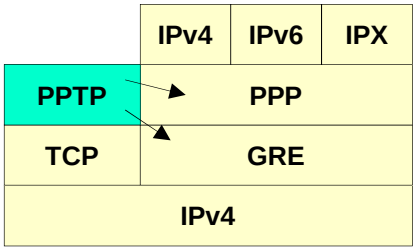


Para implementar autenticação de utilizador é necessário recorrer ao protocolo PPP.

PPTP - Point-to-point tunneling protocol

O protocolo PPTP é um predecessor do L2TP, mas ainda é bastante usado pela Microsoft e também pela Cisco. Uma vez que não usa IPsec, o PPTP acaba por ser mais simples de configurar porque não exige chaves pré partilhadas (PSK) ou certificados de chave pública.

O PPTP usa uma ligação TCP (porto 1723) para controlar a o túnel de dados que funciona sobre o protocolo GRE (*Generic Routing Encapsulation*). O protocolo GRE foi desenvolvido pela Cisco para criar túneis sobre o protocolo IP, tem o identificador de protocolo número 47.



O protocolo GRE não foi desenvolvido para uso direto pelas aplicações (não define números de porto), isso causa grandes problema na tradução de endereços (NAT) nas redes privadas.
Nem o PPTP, nem o GRE implementam mecanismos de segurança, tanto a privacidade como a autenticação são asseguradas pelo protocolo PPP.

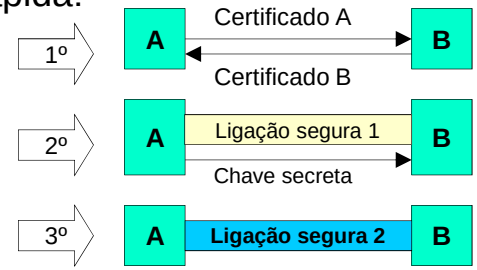
O protocolo PPP pode suportar diversos mecanismos de autenticação e privacidade, no contexto atual a Microsoft usa o protocolo de autenticação MSCHAPv2 (CHAP = *Challenge-Handshake Authentication Protocol*) que além da autenticação do utilizador via PASSWORD permite gerar uma chave secreta para o protocolo MPPE (*Microsoft Point-to-Point Encryption*) baseado no RC4 (*Rivest Cipher 4*).
Juntamente com o MPPE a Microsoft usa ainda o MPPC (*Microsoft Point-to-Point Compression*).

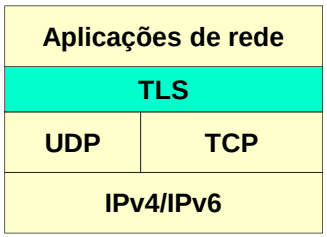
Outros protocolos de VPN

Existe uma grande variedade de protocolos de VPN, alguns proprietários, outros de domínio público, com clara vantagem destes últimos sob o ponto de vista de inter operacionalidade. Tal como o protocolo L2TP se baseia e usa o protocolo IPsec, também existem alguns tipos de VPN apoiadas no protocolo SSL/TLS.

O protocolo SSL – *Secure Sockets Layer* (nome original da Netscape), atualmente em fase final de normalização com a designação TLS - *Transport Layer Security* tem como finalidade proporcionar segurança, quer sob o ponto de vista de privacidade, quer sob o ponto de vista de autenticação dos interlocutores.

Embora seja bastante flexível e modular, nas aplicações mais correntes usa certificados de chave pública para autenticação e distribuição de uma chave secreta e de seguida transfere os dados usando criptografia convencional que é muito mais rápida:





Tal como a sigla TLS indica, situa-se na camada de transporte (o IPsec encontra-se na camada de rede), assim sendo pode usar ligações TCP ou pacotes UDP. Os protocolos de aplicação podem tornar-se seguros sem grandes modificações se passarem a usar a camada TLS, atualmente quase todos os protocolos de aplicação dispõem de uma versão segura ("s") que usa TLS: http/https; pop3/pop3s; smtp/smtps; etc. Não sendo uma implementação de VPN a camada TLS pode ser usada para esse efeito.

Uma VPN sobre TLS - OpenVPN

O OpenVPN é uma das implementações *Open Source* de VPN sobre TLS que mais se destaca atualmente.
A privacidade pode ser assegurada pelo método “habitual” para o TLS, ou seja criptografia de chave pública para distribuir a chave secreta, seguida de criptografia convencional com a chave que foi distribuída, mas também são suportadas chaves pré partilhadas (PSK).

A autenticação pode usar vários métodos de acordo com os intervenientes, desde logo certificados de chave pública, esta é a técnica ideal para uma VPN LAN-LAN. Outra possibilidade em configurações LAN-LAN é usar PSK. Quando há utilizadores envolvidos (VPN HOST-LAN) é possível a autenticação por PASSWORD.

Neste tipo de configuração a PASSWORD é enviada diretamente ao servidor através de uma ligação segura já estabelecida. Nesta fase é fundamental que o servidor já se tenha autenticado perante o cliente, caso contrario corremos o risco de estar a entregar a PASSWORD a um desconhecido.
A autenticação do servidor perante o cliente deve ser feita através do certificado de chave pública do servidor, instalado manualmente no cliente.

O OpenVPN pode funcionar (porto 1194) tanto sobre UDP como TCP, a preferência vai para o UDP pois a implementação de VPN sobre TCP é problemática (TCP sobre TCP):

Uma vez que o TCP faz a retransmissão de segmentos quando não recebe o respetivo ACK, isso significa que quando há uma perda de conectividade o TCP faz retransmissões constantes, normalmente isso não é problema porque estas retransmissões perdem-se, mas se forem efetuadas sobre um VPN a funcionar sobre TCP não se vão perder a vão acumular-se sucessivamente e pode provocar uma falha.

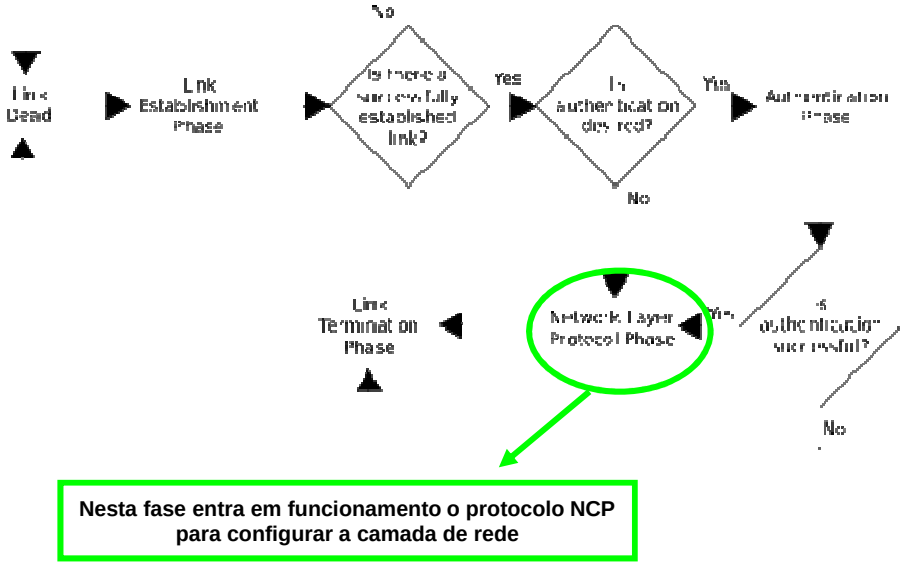
PPP – Point to Point Protocol

O protocolo PPP, deriva diretamente do protocolo HDLC e assegura de forma bastante eficiente e completa o transporte de dados de nível 2 através de uma ligação dedicada ponto a ponto. Possui diversos mecanismos apropriados aos estabelecimento da ligação lógica entre os dois pontos, incluindo por exemplo mecanismos de autenticação.

Marcador (7E)	Endereço (FF)	Controlo (03)	Protocolo	DADOS		FCS	Marcador (7E)

O campo "protocolo" serve para identificar os dados que são transportados, alguns protocolos são usados pelo próprio PPP. O identificador de protocolo 0xC021 é usado pelo protocolo LCP (Link Control Protocol).

O protocolo LCP é o responsável pelo estabelecimento e manutenção da ligação nível 2. O LCP lida com a autenticação, por exemplo usando o *Challenge Handshake Authentication Protocol* (CHAP), e com a configuração da ligação de dados, negociando por exemplo o MTU.



PPP – NCP (*Network Control Protocol*)

Depois de o LCP estabelecer o funcionamento do nível de ligação de dados o processo segue no nível de rede, para cada um dos protocolos de rede pretendidos.
O protocolo NCP (*Network Control Protocol*) usa os identificadores de protocolo “0x8???”, o NCP é o responsável pela interação com os protocolos de nível 3, por exemplo trata de definição dos parâmetros necessários a cada protocolo em particular.

Para cada protocolo de rede existe um NCP especifico, por exemplo para o IPv4 é o protocolo NCP é o IPCP (*Internet Protocol Control Protocol* – 0x8021) entre outras funcionalidades o IPCP é o responsável pela configuração automática dos parâmetros de rede nos nós ao estilo DHCP.
Os identificadores de protocolo “0x0???” São usados para transportar os dados dos protocolos de rede propriamente ditos, para o IPv4 usa-se o identificador 0x0021.

A figura apresenta alguns dos protocolos usados sobre a camada **ppp** e os respetivos identificadores de protocolo em notação hexadecimal.