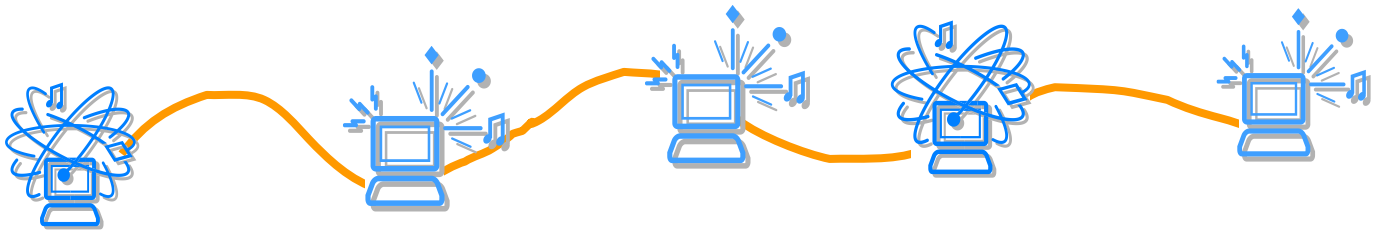
VPN (*Virtual Private Networks*) - Introdução



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

Definição

Uma VPN é um canal seguro (túnel) que usa recursos de uma rede pública (normalmente a Internet) para interligar redes privadas ou utilizadores remotos a redes privadas.

Em vez de uma ligação fisica dedicada, uma VPN utiliza ligações virtuais estabelecidas através da rede pública entre a máquina de um colaborador remoto ou uma rede privada e outra rede privada.

Definição (cont.)

- **VPN** – Rede "virtual" que, apesar de normalmente utilizar uma rede pública, como a Internet, é mantida privada através do transporte de dados em **túneis** através da infra-estrutura pública.

- Uma VPN utiliza a Internet ou outro serviço de rede pública como todo ou parte do seu "*backbone*" WAN
- As VPN possibilitam:
  - **Utilizadores remotos –** Substituir as ligações *dial-up* e ISDN, por vezes a longas distâncias, por ligações locais a ISP (*Internet Service Providers*), menos dispendiosas.
  - **LAN** – Substituir linhas privadas dispendiosas (tais como E1, ATM e *Frame Relay*) entre LAN remotas

Conceito de “canal seguro”

- Garante a **confidencialidade, integridade e autenticidade (CIA) dos dados** que viajam através de redes inseguras.
- Não apenas na Internet, nas LAN e WAN também.
- Algumas aplicações das VPN:
  - Ligação de redes remotas da mesma empresa
  - Ligação entre redes remotas de parceiros de negócio
  - Acesso remoto de colaboradores
  - Protecção dos números de cartão de crédito em transacções bancárias e outras no *e-commerce, ...*

Nota: Nem todas as VPN asseguram um canal seguro.

Conceito de “canal seguro”

- Oferta típica:
  - Confidencialidade
  - Autenticação da origem de dados (do quê? Máquina? Aplicação? Utilizador?)
  - Integridade de dados
- Oferta menos usual:
  - Não-repudiação (negar a responsabilidade de uma acção depois de feita)
  - Maior eficiência (MPLS)

Pré-requisitos de uma VPN

- **Segurança**, eficiência e **custo menor** do que as soluções tradicionais
  - VPN devem dar suporte a mecanismos de confidencialidade, mas nem todas o têm de fazer (e.g. MPLS)
  - VPN devem suportar autenticação
  - Ninguém externo à VPN deve poder alterar a VPN ou os conteúdos que lá passam (integridade)
  - Todas as partes associadas à VPN devem acordar sobre as propriedades de segurança.

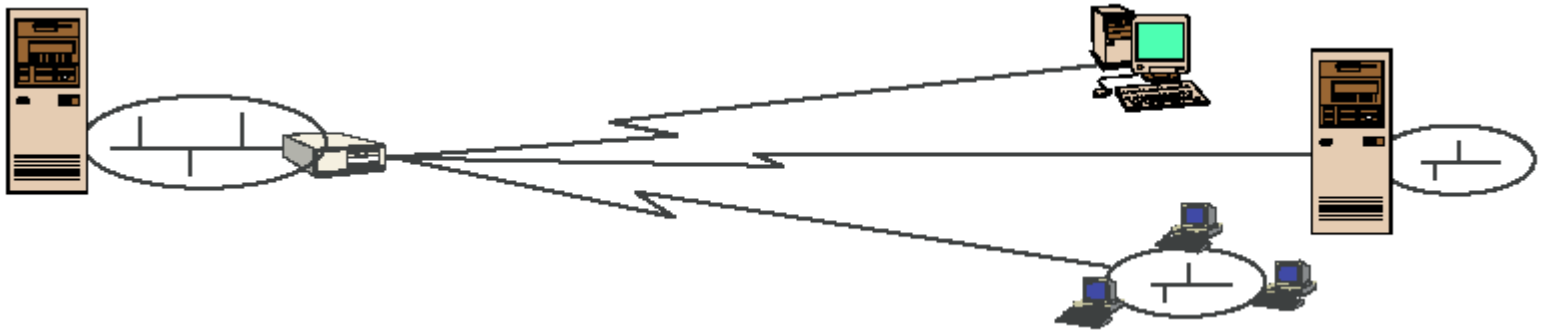
Porquê usar VPN?

- Expandir a abrangência geográfica
- Aumentar a segurança
- Reduzir os custos operacionais das WAN tradicionais
- Reduzir o tempo de trânsito e custo de transporte para os utilizadores remotos
- Aumentar a produtividade
- Simplificar a topologia da rede
- Melhorar as oportunidades de utilização da rede global
- Fornecer suporte ao trabalho remoto
- Melhorar a utilização e a compatibilidade com a rede de banda larga
- Fornecer um ROI (*return on investment*) mais rápido que uma WAN

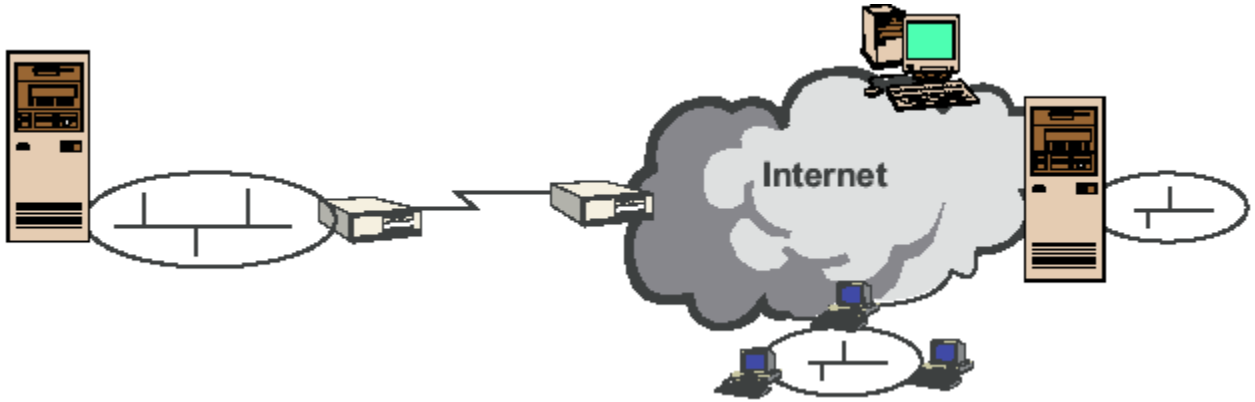
Quais as opções criticas?

- Segurança
- Fiabilidade
- Escalabilidade
- Gestão da rede
- Gestão de politicas

VPN porquê?



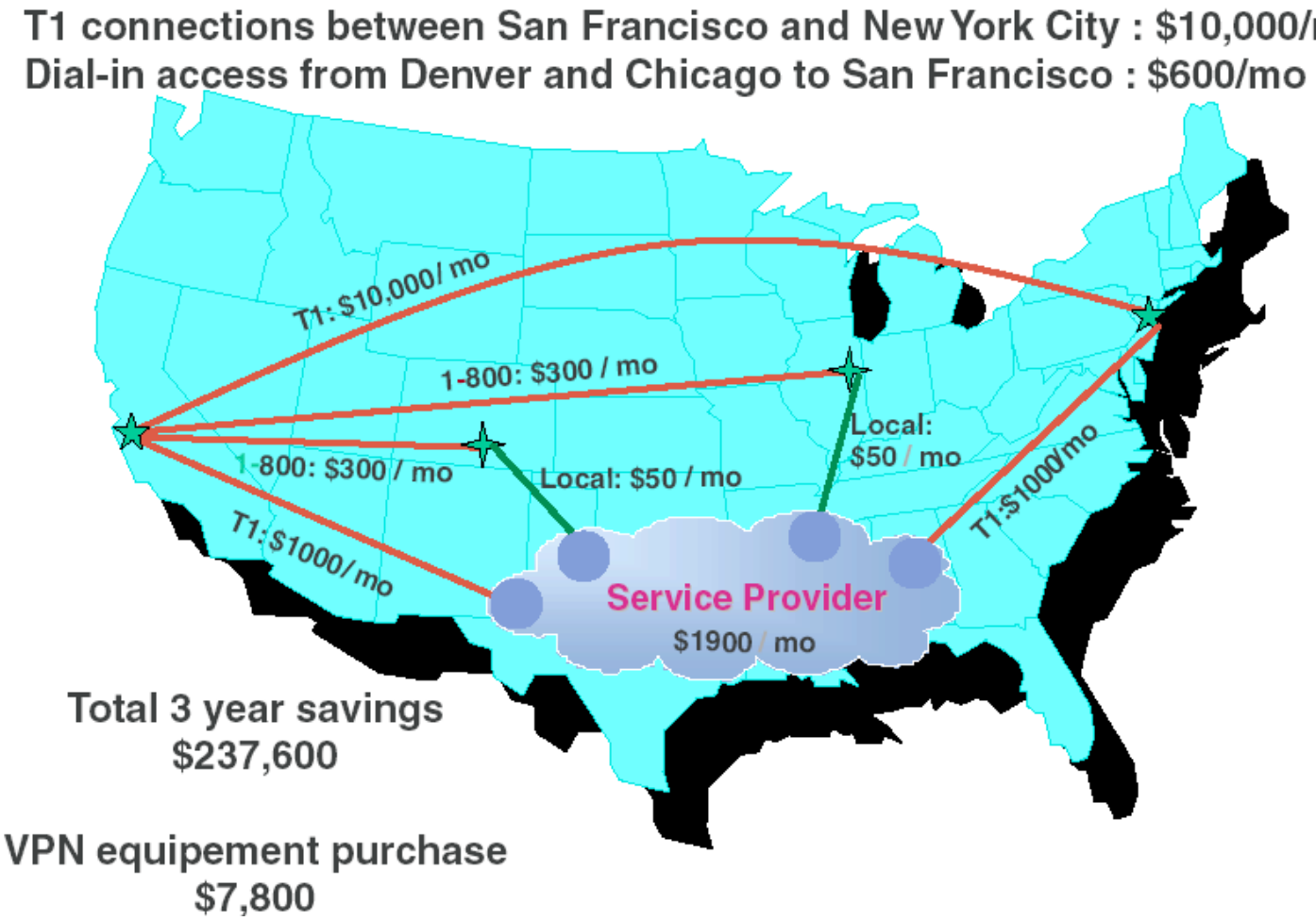
As redes públicas são utilizadas para passarem informação entre redes de confiança, utilizando recursos partilhados como *Frame Relay* ou ATM.



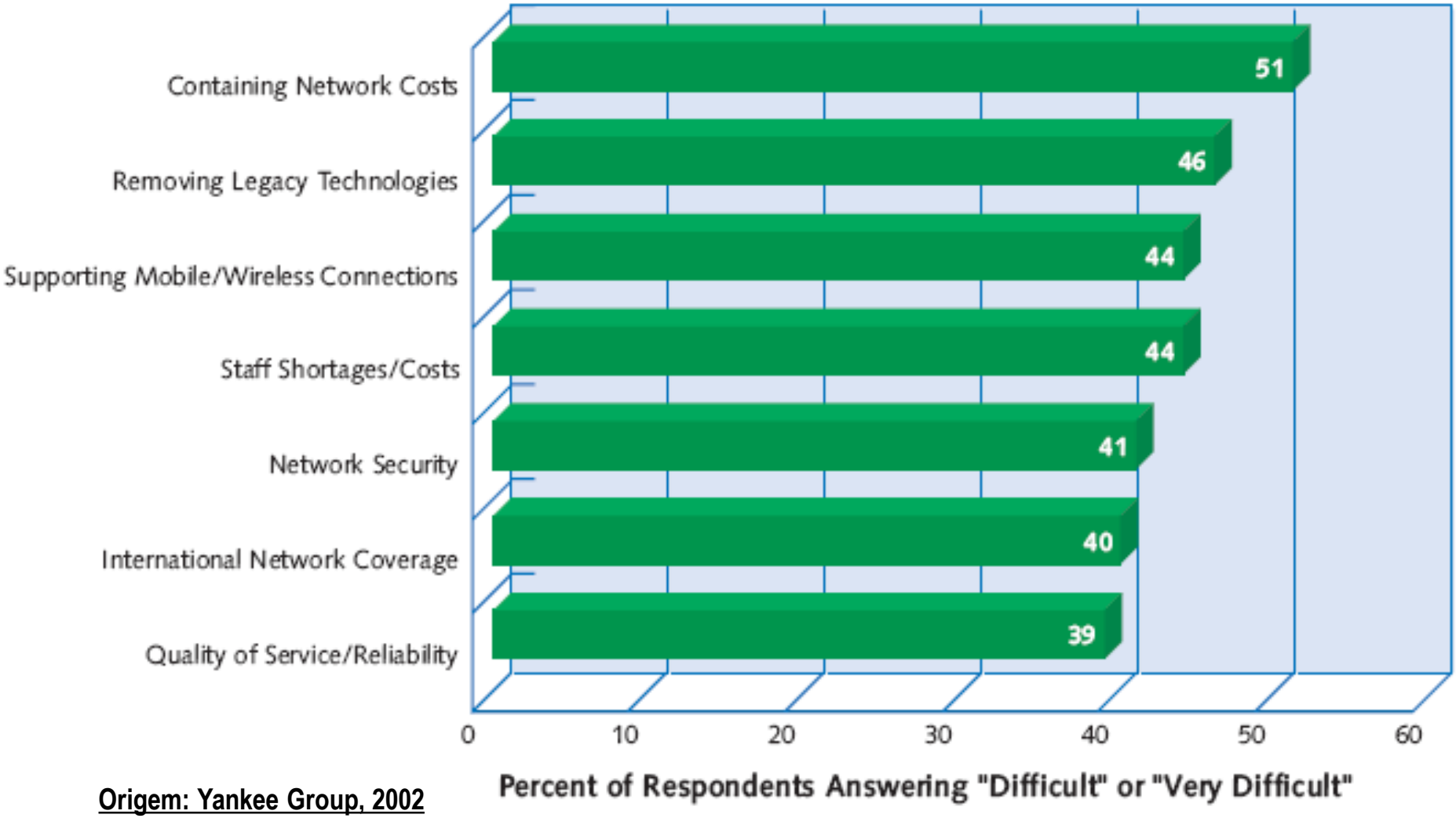
Uma "***V**irtual **P**rivate **N**etwork*" pode substituir as anteriores utilizando a Internet.

VPN porquê?

Poupança, mantendo ou aumentando a segurança e **versatilidade**

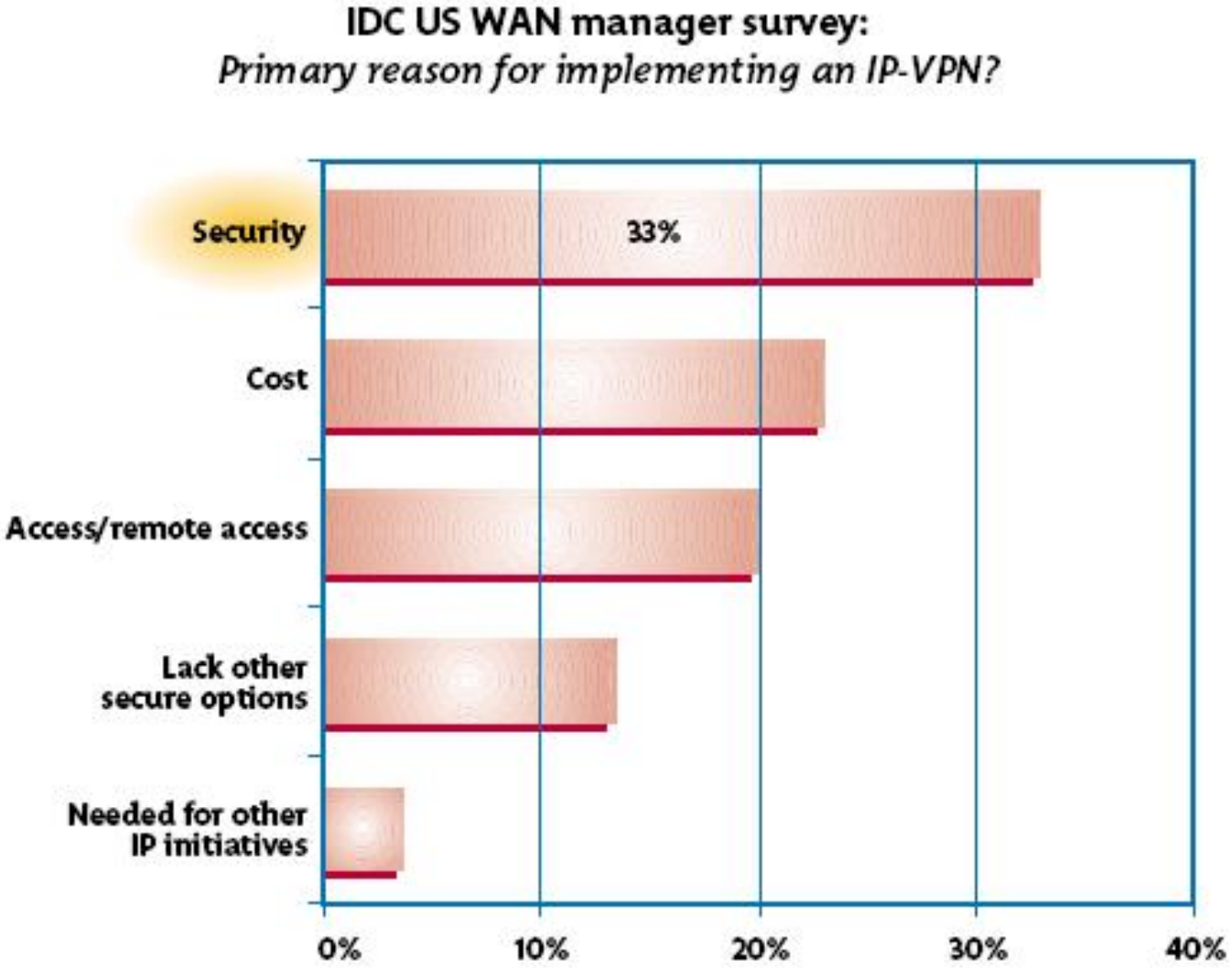


Problemas das organizações na gestão das suas redes



Origem: Yankee Group, 2002

Razões principais da opção por VPN IP



Conceito de “canal seguro”

- Canal seguro funciona da seguinte maneira:
  - **Protocolo de estabelecimento de chaves de sessão**
    - Durante este uma ou ambas as partes são autenticadas
    - São estabelecidas novas chaves de sessão
    - As chaves de sessão podem ser criadas a partir dum segredo partilhado
  - **Fase de derivação de chaves**
    - As chaves de sessão podem dar origem a chaves independentes de cifra e autenticação
  - **O tráfego que se seguir é cifrado usando as chaves derivadas**
- Opcionalmente: Reutilização da sessão, mudança rápida de chaves (*session re-use*, *fast re-keying*, …)

Primitivas criptográficas típicas utilizadas

- **Algoritmos de cifra simétrica**.
  - Para velocidade na cifra e decifra.
- **Algoritmos de cifra assimétrica**
  - Para a autenticação de entidades e troca de chaves
- **Algoritmos de autenticação e integridade**
  - MAC (*Message Authentication Code*) usualmente construído com funções de *hash*
- **Funções de geração de números pseudo-aleatórios** (com chave)
  - Derivação da chave.
- **Outros contributos para a segurança**
  - Números de sequência, protegidos por MACs, utilizados para prevenir ataques por repetição
  - "*Nonces*" e "*timestamps*" utilizados para garantir a "frescura" nas trocas para autenticação entre entidades

Vantagens das VPN

- Fornece um canal seguro: Confidencialidade, autenticação e integridade
- Fácil de estabelecer dado utilizar a mesma infra-estrutura das redes existentes
- Fácil de terminar
- Interliga locais (por exemplo, escritórios) de maneira segura através de uma rede com custos mais razoáveis do que métodos mais tradicionais tais como, por exemplo, as linhas alugadas.

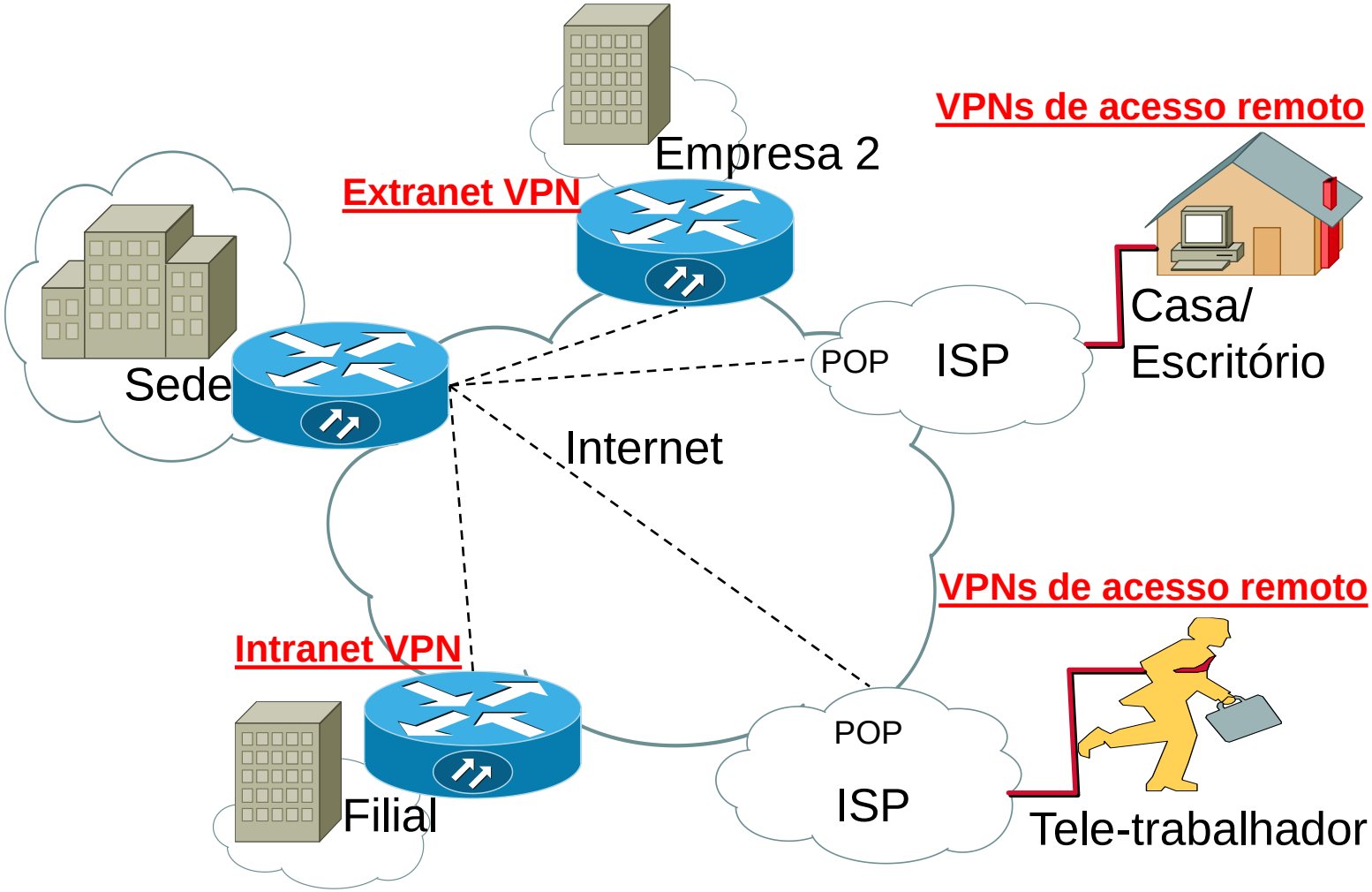
Desvantagem das VPN (face às linhas alugadas)

- *Overhead* devido aos mecanismos para garantirem a confidencialidade, autenticação e integridade
- Possibilidade da velocidade da VPN limitada pela velocidade do troço com débito menor na Internet
- Possibilidade de uma única falha no caminho desligar toda a VPN
- Difícil detectar problemas dado parte do tráfego ser cifrado
- IDS (*Intrusion Detection System*) é menos eficaz dado a cifra dos conteúdos
- Integração difícil com o NAT.

Tipos de VPN

- Podemos classificar as VPN de acordo com a sua funcionalidade em:
  - VPN de acesso remoto
  - VPN intranet
  - VPN extranet
- Também podemos classificar as VPN quanto à sua função enquanto emuladoras de outro tipo de redes:
  - *Virtual Leased Lines* (VLL)
  - *Virtual Private Routed Networks* (VPRN)
  - *Virtual Private LAN Segment* (VPLS)
  - *Virtual Private Dial Networks* (VPDN)

Tipos de VPN


VPNs de acesso remoto
Empresa 2
Extranet VPN
Sede
POP
ISP
Casa/
Escritório
Internet
VPNs de acesso remoto
Intranet VPN
POP
ISP
Filial
Tele-trabalhador

VPN de acesso remoto

- Ligação de equipamentos móveis
- Ligações de muitos para um
- Computador remoto (cliente VPN) e gateway da VPN de acesso remoto (servidor VPN)
- Software de cliente
- Acesso ao recursos privados internos da rede

VPN extremo a extremo (entre redes)

- Ligação *router* a *router*
- Ligação de um para um
- Lida com os assuntos do encaminhamento
- Utiliza IP públicos estáticos

- Podemos incluir nesta classificação as VPN *intranet* e *extranet.*

Tipos de VPN

Use	Application	Alternative To	Benefits
Remote Access VPN	Remote Connectivity	Dedicated Dial ISDN	Ubiquitous Access Lower Cost
IntranetVPN	Site-to-Site Internal Connectivity	Leased Line	Extend Connectivity Lower Cost
ExtranetVPN	Business-to-Business External Connectivity	Fax, Mail, EDI	Facilitates E-Commerce

Tipos de VPN (2)

- As VPN podem ser implementadas de várias formas :
  - Soluções baseadas em equipamentos dos clientes (*Customer Premises Equipment* (CPE))
  - Soluções baseadas na rede, equipamentos dos operadores

VPN baseadas em CPE *vs* rede

- A maioria das implementações de VPN actuais são **baseadas em dispositivos CPE (equipamentos dos clientes)**:
  - *Firewalls*
  - *Routers* de fronteira de WAN
  - Dispositivos especializados de terminação de VPN

- Soluções **baseadas em rede**: A VPN é implementada na rede pelo *Internet Service Provider* (ISP)
  - Alguns mecanismos disponibilizam ferramentas poderosas que são apenas aplicáveis aos ISP em vez de clientes individuais que utilizam dispositivos CPE especiais

Tipos de VPN (emulação de outras redes)

- *Virtual Leased Lines (VLL)*
- *Virtual Private Routed Networks (VPRN)*
- *Virtual Private LAN Segment (VPLS)*
- *Virtual Private Dial Networks (VPDN)*

Tipo I: *Virtual Leased Lines* (VLL)

- **VLL = Túnel IP formando uma ligação ponto-a-ponto de maneira a emular uma ligação através de uma linha alugada ou dedicada**

- Requer um mecanismo para dar suporte a um túnel IP
  - O envio é disjunto dos campos de endereço dos pacotes encapsulados, permite o transporte opaco de tramas como carga dos pacotes
  - e.g. IP/IP, túneis GRE, L2TP (pacotes PPP), MPLS e IPSec

VLL: Requisitos do protocolo de suporte dos túneis

- Suporte de **multiplexagem de VLLs**
  - e.g. *tunnel-id* & *call-id* para o L2TP, *labels* MPLS
- Suporte de um **protocolo de sinalização**
  - Para negociar os atributos do túnel tais como nível de segurança, endereço IP dos pontos remotos (e.g. LDP no MPLS).
- Suporte de **segurança de dados**
  - Permitir aos clientes especificar os níveis de segurança
- Suporte de **múltiplos protocolos de transporte**
- Suporte de **sequenciação de tramas**
  - Requerido para garantir entrega por ordem dos pacotes

VLL: Requisitos do protocolo de suporte dos túneis

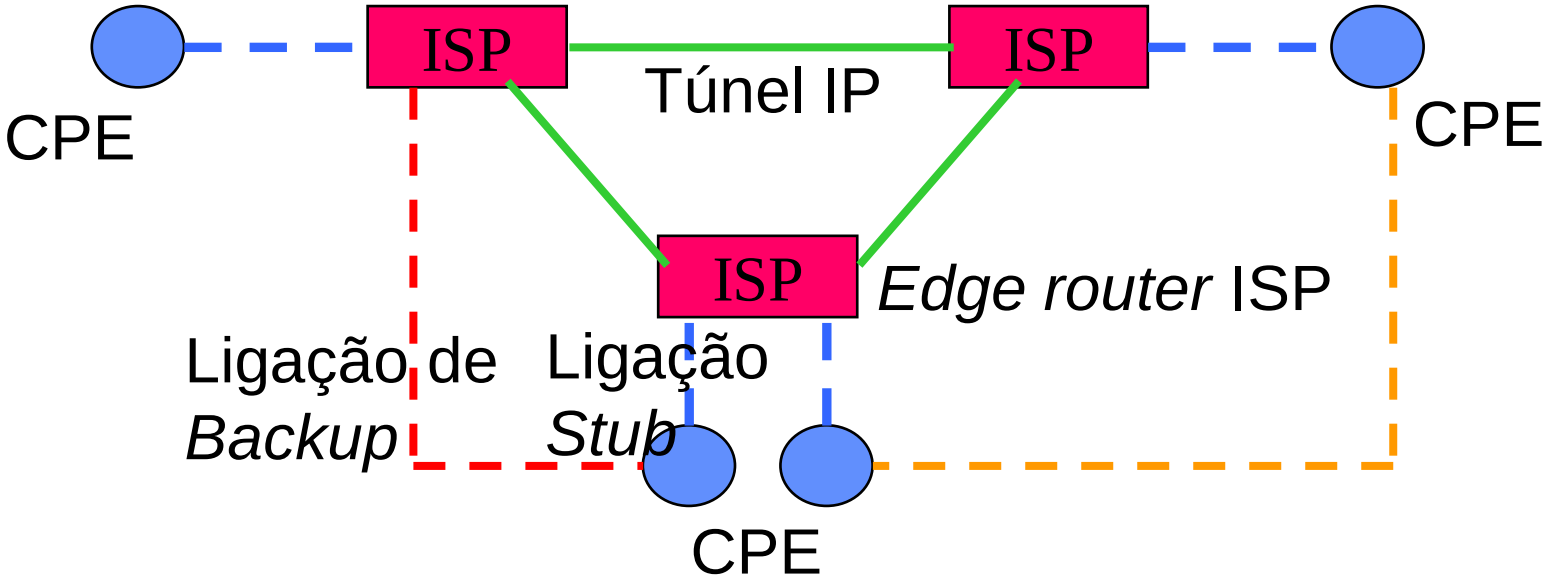
- Suporte de **manutenção do túnel**
  - Estabelecer, manter e terminar instâncias de túneis
- Suporte de **MTU grandes**
  - Deve permitir fragmentação de tramas, quer ao nível do IP ou dentro do túnel (número de sequência no túnel)
- **Minimização do *overhead*** devido ao túnel
  - Importante para tráfego sensível a pequenos *jitter* e latência
- Formas de **controlo de congestão e de fluxo**
  - Actualmente apenas o L2TP faz isto, ainda em fase de experiência
- Formas de **gestão do tráfego**
  - Garantia de entrega e.g. taxa de perdas, latência e largura de banda

VLL: Recomendações

- Uma modificação do IKE/IPSec pode ser uma escolha óptima como norma para um mecanismo de túnel VLL
  - Tem capacidades bem definidas de multiplexagem e de sinalização
  - Tem suporte de segurança
  - Compete com: MPLS
- Usar um único protocolo de sinalização e o encapsulamento de dados associado é melhor do que ter múltiplos protocolos em paralelo.

Tipo II: *Virtual Private Routed Networks* (VPRN)

- Uma VPRN emula uma rede IP com múltiplos sítios com possibilidade de encaminhar entre eles
  - Uma mistura de túneis IP entre *routers* de ISPs e *routers* do cliente
  - Ligações "*stub*" a interligar os *routers* CPE aos *routers* dos ISPs



VPRN (continuação)

- **Benefício**: A configuração dos *routers* CPE é simplificada. O *router* de fronteira do ISP aparece como um *router* "vizinho".
- A complicação do estabelecimento do túnel, manutenção e encaminhamento está do lado do ISP. O encaminhamento é realizado ao nível de rede (nível 3)

- Cada *router* CPE do lado do cliente está ligado a um *router* de fronteira do ISP através uma ou mais ligações "*stub*" (linhas alugadas, ATM ou *Frame Relay*)
- Cada VPRN suporta apenas um único protocolo da camada de rede.

VPRN (continuação)

- Assuntos que necessitam ser abordados:
  - Configuração inicial/topologia: Necessidade de determinar o conjunto de *routers* que têm membros em VPRN
  - Os *routers* CPE necessitam determinar o conjunto de prefixos dos endereços IP a serem enviados para um *router* de fronteira do ISP
  - *Routers* de fronteira do ISP
    - Necessidade de determinar o conjunto de prefixos de endereços IP que estão disponíveis através de cada ligação "*stub*"
    - Necessidade de aprender e disseminar informação entre eles da maneira de atingir as várias sub-redes
    - Necessidade de mecanismos de envio da VPN para o envio de tráfego de chegada das ligações "*stub*" para o próximo *router* e para enviar o tráfego de saída da rede para as ligações "*stub*"
  - Nota: Assuntos semelhantes aplicados a VPLS.

VPRN: Requisitos genéricos

- Identificador único de VPN para se referir a uma VPN em particular
  - Único através de diferentes AS (Sistemas Autónomos)
- Membros da VPRN
  - configuração
  - disseminação (*lookup* de directorias, configuração de gestão explícita, *piggybacking* em protocolos de *routing*).
- Informação de acesso às ligações "*stub*"
  - Os *routers* de fronteira devem aprender conjuntos de endereços/prefixos de endereços atingíveis via cada ligação "*stub*"
  - Cada *router* CPE necessita aprender os destinos atingíveis por cada ligação "*stub*"

VPRN: Requisitos genéricos

- Informação de encaminhamento intra-VPRN
  - Necessita ser disseminada para outros *routers* de fronteira de uma das seguintes formas:
    - *Lookup* em directorias
    - Configuração explicita
    - Instanciações de encaminhamento intra-VPRN local
    - Protocolo "*link reachability*"
    - *Piggybacking* de protocolos de *routing* no *backbone* IP
- Mecanismo de túnel (como em VLL)
  - Os *routers* de fronteira devem construir os túneis necessários para os outros *routers* na VPRN, encapsular/desencapsular e enviar/receber pacotes através do túnel

VPRN: Suporte de *multicast*

O tráfego de *multicast* e *broadcast* pode ser suportado por:

- Replicação na fronteira:
  - O *router* de fronteira replica o tráfego de *multicast* para a transmissão através de cada ligação da VPRN
- Suporte de *multicast* nativo
  - Os *routers* de fronteira VPRN mapeiam o tráfego *multicast* intra-VPRN em mecanismo de distribuição IP *multicast* através do *backbone*.

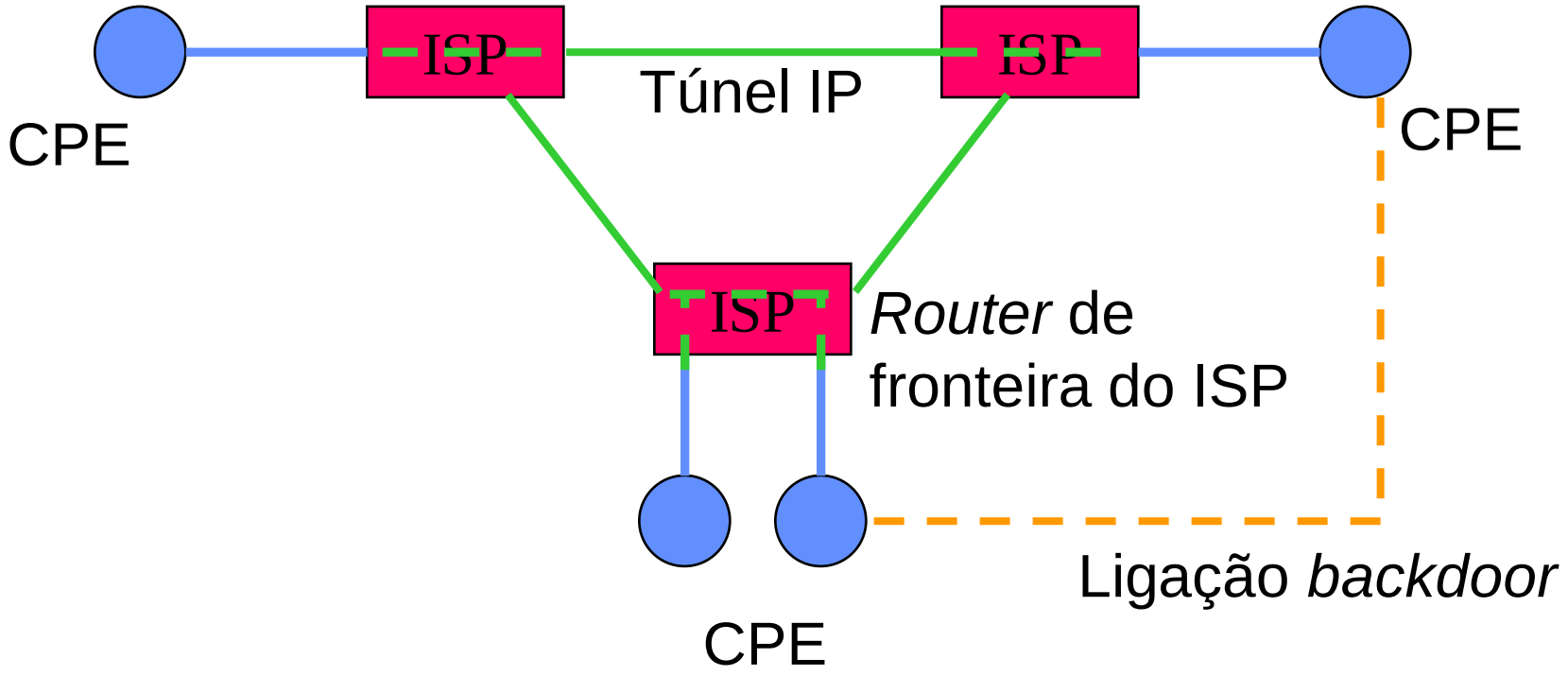
VPRN: Recomendações

- Existem propostas para adaptar protocolos de *routing* para transportarem informações de VPN para suportarem mecanismos de *piggybacking* de *routers* (e.g. MPLS)

- **Contra**: Alguns ISP preferem não associar "*membership*" e "*reachability*" com os protocolos de *routing* do *backbone*.

Tipo III: *Virtual Private LAN Segment* (VPLS)

- Uma VPLS emula um segmento de uma LAN sobre IP.
  - Equivalente às VPRN, excepto que agora os túneis estendem-se até aos *routers* CPE e os *routers* de fronteira do ISP fornecem ligações ao nível da camada de ligação (*bridging*) (apenas ligação ao nível 2).



VPLS: Requisitos e recomendações

- Muito semelhante às VPRN
- Ao contrário das VPRN, os nós CPE podem ser *bridges* ou *routers*
  - A natureza dos CPE (*bridge* vs *router*) tem impacto na natureza da encapsulação, endereçamento, envio e acessibilidade dos protocolos na VPLS.
- Vantagem: Transparência do protocolo.

- A parceria entre VPRN e VPLS pode ser explorada de forma a diminuir a complexidade.

Tipo IV: *Virtual Private Dial Networks* (VPDN)

- Uma VPDN permite a utilizadores remotos ligarem-se a pedido através de túneis:
  - Ex. Ligações PPP a NAS (*Network Access Server*)
- Uma relação forte entre o utilizador e a rede central requer segurança.
- L2TP (*Layer 2 Tunneling Protocol*) permite uma sessão PPP entre um utilizador de um concentrador de acessos L2TP (LAC) e um servidor de rede remoto (LNS) L2TP.

VPDN (continuação)

- Suporte compulsivo de túneis
  - Um servidor de acessos (LAC), estende uma sessão PPP através do *backbone* usando L2TP até um LNS remoto

- Outros assuntos:
  - *Call Routing*
  - Mecanismos de segurança
  - Gestão de tráfego
  - Multiplexagem de chamadas
  - Gestão de endereços
  - Suporte de MTU grandes

VPDN (continuação)

- Túneis voluntários
  - Um *host* individual liga-se a um local remoto utilizando um túnel com origem no *host*, sem envolvimento de nós da rede intermédios.

- Suporte de *hosts* na rede
  - O modelo existente do PPP assume uma ligação a uma rede de acesso
  - Se se quiser acomodar a infra-estrutura AAA entre os fornecedores de serviços
    - Estender o PPP a *hosts* através do L2TP
    - Estender directamente o PPP até aos *hosts*
    - Usar IPSec

VPDN

- As especificações do L2TP foram complementadas para suportarem VPDN usando túneis compulsórios
- São necessários mais estudos para determinar a melhor solução para dar suporte aos túneis voluntários:
  - Solução baseada em PPP ou
  - Mecanismo baseado em IPSec.

Protocolos de suporte a VPN

- PPTP (*Point to Point Tunneling Protocol*)
- L2TP (*Layer 2 Tunneling Protocol*)
- IPSec (*Internet Protocol Security*), IKEv2
- SSL/TLS (*Secure Socket Layer / Transport Layer Security*)
- SSH + PPP (*Secure Shell* + *Peer-to-Peer Protocol*)
- SSTP
- OpenVPN
- SoftEther VPN
- MPLS

Lista não exaustiva

Segurança *versus* camadas de rede

- **Em que camada da rede devemos implementar a segurança?**

- A segurança pode ser aplicada em qualquer das camadas de rede:
  - Mesmo na física é por vezes possível aplicar segurança (técnicas de "*spread spectrum*", por exemplo)

- **Quais os prós e os contras de aplicar a segurança numa ou noutra camada?**

VPN – Camadas de rede

Camada do modelo	Protocolos
Camada de aplicação	SoftEther VPN, OpenVPN, SSH
Camada de transporte	SSL/TLS
Camada de rede	IPSec
Camada de ligação	PPTP, L2TP, MPLS
Camada física	*Scrambling, Hopping, Quantum Communications*

Segurança e camadas da rede

- **Camada *Data Link* (*Network Interface*):**
  - ✓ Cobre todo o tráfego nessa ligação (*link*), independentemente dos protocolos acima
  - ✘ Protecção de apenas um troço ("*hop*")

- **Camada *Network* (*Internet*):**
  - ✓ Pode cobrir todo o tráfego, extremo-a-extremo
  - ✓ Transparente para as aplicações
  - ✘ Pouco controlo das aplicações
    - As aplicações não têm visibilidade da camada Internet
  - ✘ Não natural dado que a camada de rede não tem estado (*stateless*) e não é fiável
    - A ordem dos dados num canal seguro pode ser crucial
    - Difícil de manter se os datagramas IP forem descartados ou jogados fora, …

Segurança e camadas da rede

- **Camada de Transporte**:
  - ✓ Extrêmo-a-extrêmo, cobre todo o tráfego que use o protocolo de transporte protegido
  - ✓ As aplicações podem controlar quando é usado
    - As aplicações têm uma maior visibilidade da camada de transporte.
  - ✓ A camada de transporte pode naturalmente ter noção de estado (*statefull*), e.g. TCP
  - ✗ As aplicações têm de ser modificadas (se não se usarem *proxies*)

- **Camada de Aplicação**:
  - ✓ A segurança pode ser ajustada às necessidades da carga
    - Aplicações diferentes podem ter necessidades radicalmente diferentes
    - E.g. aplicação VoIP versus transferência de dados sensíveis.
  - ✗ Cada aplicação deve gerir a sua própria segurança.

VPN Nível 2 vs. Nível 3 – Prós e Contras

- **Nível 2 – L2TP**
  - ↗ Os mesmos procedimentos de que o PPP (segredos pré-partilhados, RADIUS, etc.)
  - ↗ Mesma informação auxiliar que o PPP (*virtual IP, DNS/WINS servers*)
  - ↘ Sem segurança forte, o protocolo de controlo da ligação fica sujeita a ataques e pode ser enganado para estabelecer um cifra fraca ou nenhuma.
  - ↘ Os pacotes L2TP não são autenticados e estão sujeitos a ataques por repetição

- **Nível 3 – IPSec**
  - ↗ Cifra forte criptograficamente e autenticação do túnel VPN
  - ↗ Pode negociar e forçar politicas de controlo complexas de acesso à VPN
  - ↗ DHCP-over-IPSec e autenticação oferecem facilidades tipo PPP
  - ↘ Não permite enviar pelo túnel protocolos não-IP (IPX, etc.)
  - ↘ Estabelecimento da ligação complexo, *overhead* da gestão PKI

VPN Nível 4/5

- **Nível 2 – SSL/TLS**
  - Possibilidade de utilizar inúmeros algoritmos criptográficos, incluindo cifras simétricas, assimétricas, hashes e certificados digitais
  - Possibilidade de negociar os algoritmos criptográficos a utilizar em cada caso
  - Mais «pesado» do que os protocolos implementados em camadas OSI inferiores
- **Nível 4/5 – OpenVPN e SoftEther VPN**
  - Baseados no SSL/TLS
  - Pode negociar e forçar politicas de controlo complexas de acesso à VPN
  - Pode oferecer serviços nível 2 OSI (SoftEther VPN)
  - Não têm uma abrangencia tão grande como os outros protocolos de suporte de VPN referidos anteriormente
  - Normalmente mais «pesados» do que os protocolos de VPN de camadas inferiores apesar da sua implementação utilizando facilidades relacionadas com o kernel, etc. Permitam melhorar o desempenho

VPNs Nível 2 vs. Nível 3– Prós e Contras

- **L2TP sobre IPsec**
  - ↗ Fornece serviços de nivel 2 OSI de modo seguro
  - ↗ A encapsulação IPSec adiciona cifra e autenticação fortes
  - ↗ Permite o envio pelo túnel de protocolos não-IP (IPX, etc.)
  - ↘ Pacotes grandes devido à sobrecarga da múltipla encapsulação

PPTP

- *Point-to-Point Tunneling Protocol* (PPTP), desenvolvido pela Microsoft
- Estabelece um túnel, não fornece encriptação
- Usado com o *Microsoft Point-to-Point Encryption* (MPPE) se se pretender confidencialidade
- Usado nas VPN de acesso remoto (cliente)
- Utiliza o MS-CHAPv2 para autenticação, ou utiliza *o* EAP (*Extensible Authentication Protocol*) para melhorar o suporte de mecanismos de autenticação

  O EAP, criado inicialmente como uma extensão do PPP, é um protocolo de suporte à autenticação que dá suporte a múltiplos métodos de autenticação, tal como *token* cards, Kerberos, one-time passwords, certificados digitais, autenticação com chave pública e smart cards.

L2TP

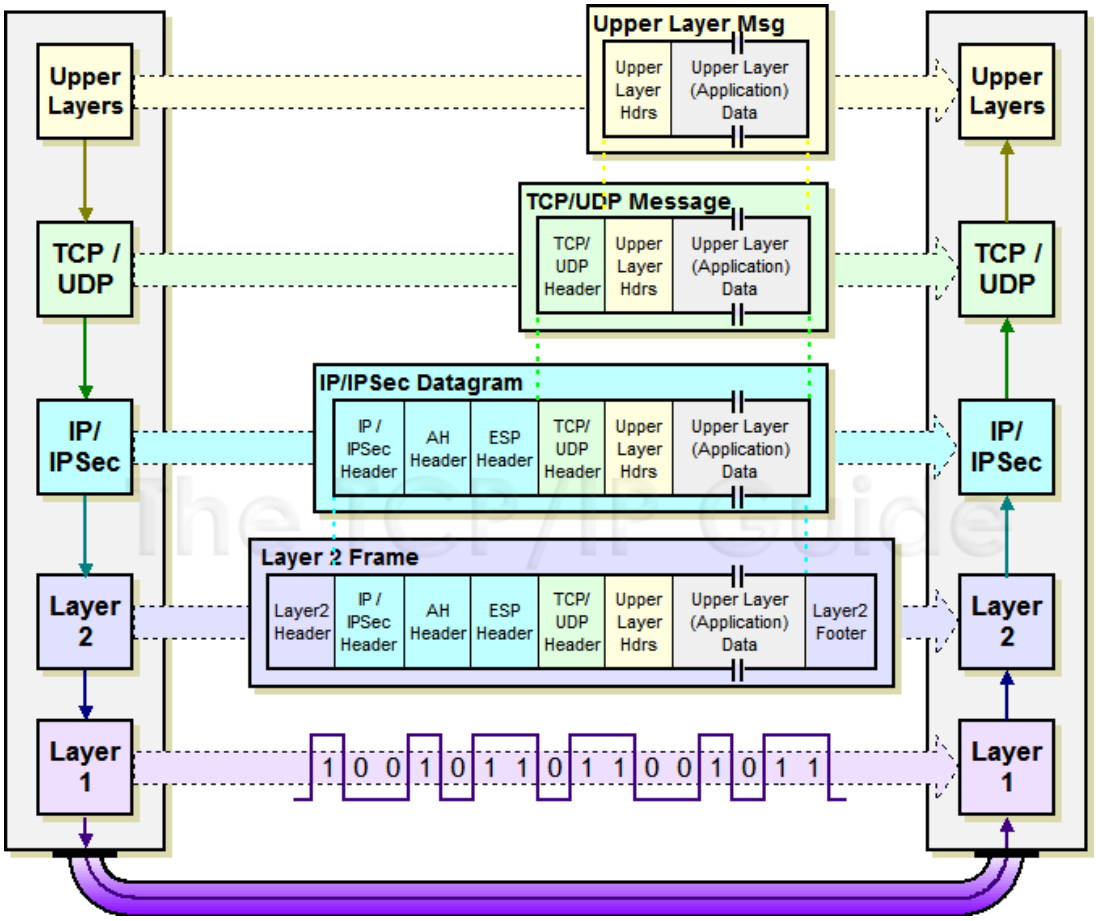
- *Layer 2 Tunneling Protocol* (PPTP + L2P, Layer 2 Forwarding)
- É independente do IP (nível 2 OSI)
- Requer certificados digitais
- Vantagens relativa ao PPTP
  - Não-repudiação

IPSec

- Utilizado também pelo L2TP para cifrar os túneis
- Nível 3 do OSI
- Pode funcionar em modo transporte ou em modo túnel
- Autenticação via *Internet Key Exchange* (IKE)
  - Certificados digitais
  - Chaves pré-partilhadas

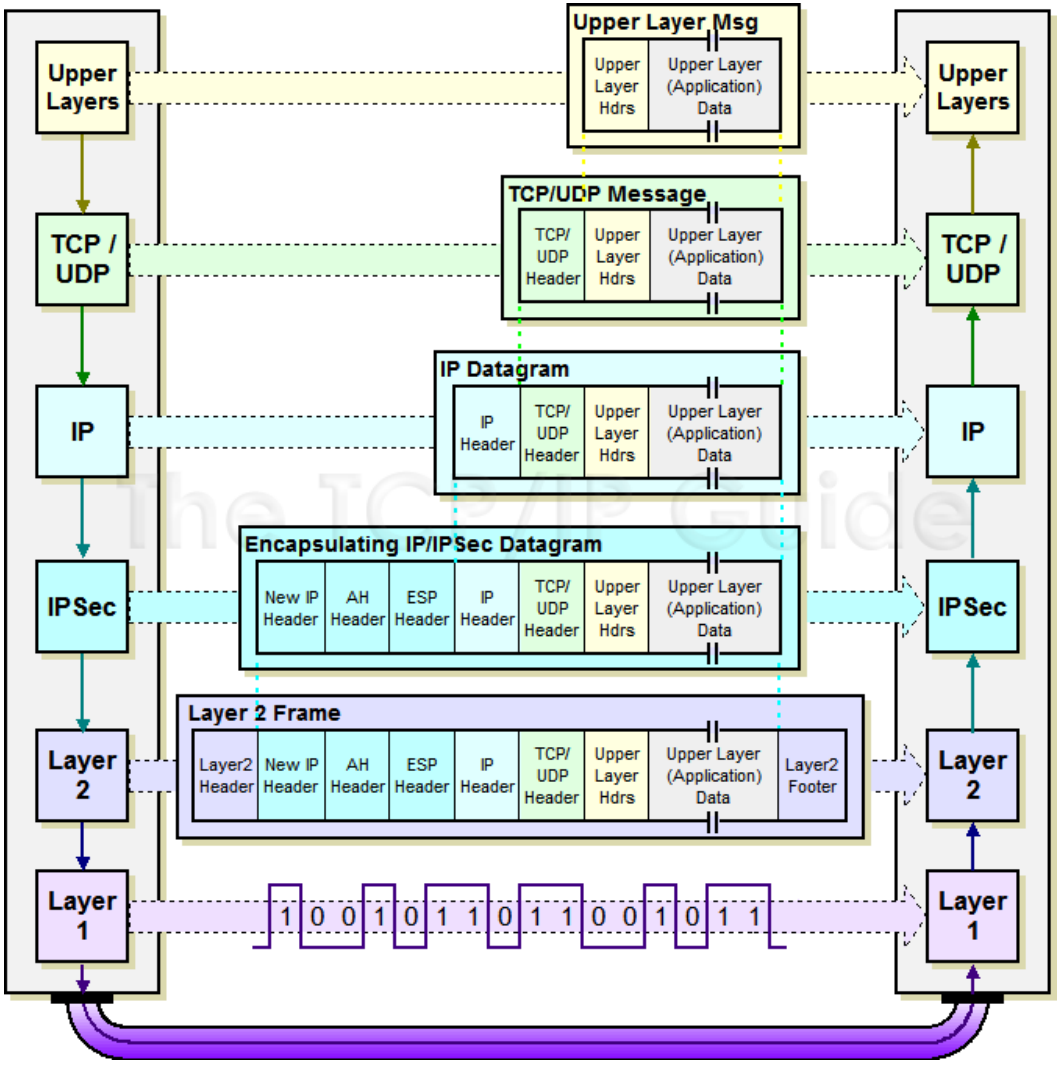
Modo transporte

Como o nome sugere, no modo transporte o protocolo IPSec protege apenas a mensagem recebida da camada de transporte.



Modo túnel

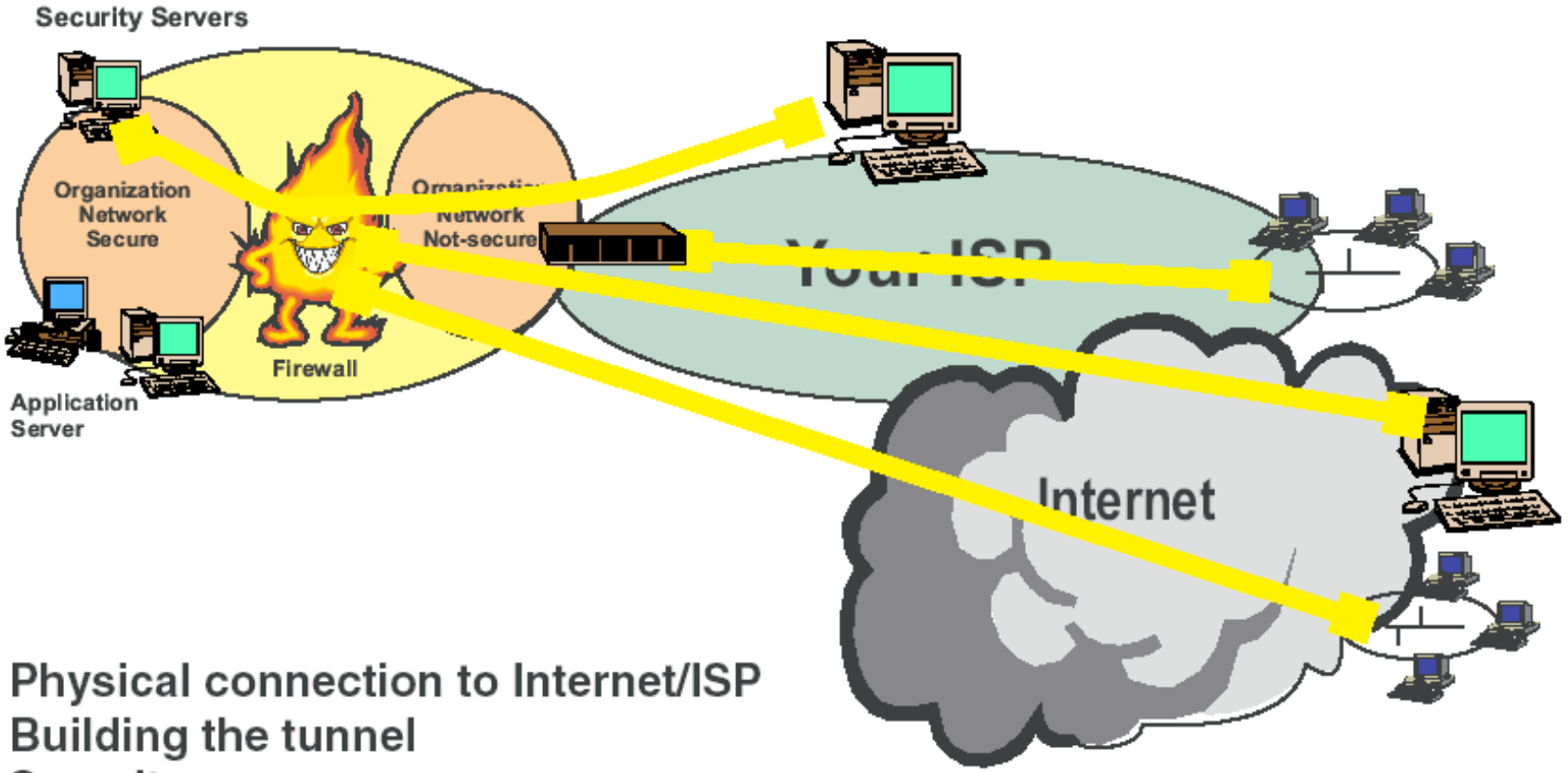
Neste modo o IPSec é utilizado para proteger um datagrama IP completo que é encapsulado dentro de outro datagrama IPSec.



SSL

- Utilizado principalmente para a criação de VPNs de acesso remoto a servidores Web
- Utiliza certificados digitais

Partes a considerar numa VPN



Physical connection to Internet/ISP
Building the tunnel
Security servers
Management
Provisioning
Quality of Service (QoS)