

VPN

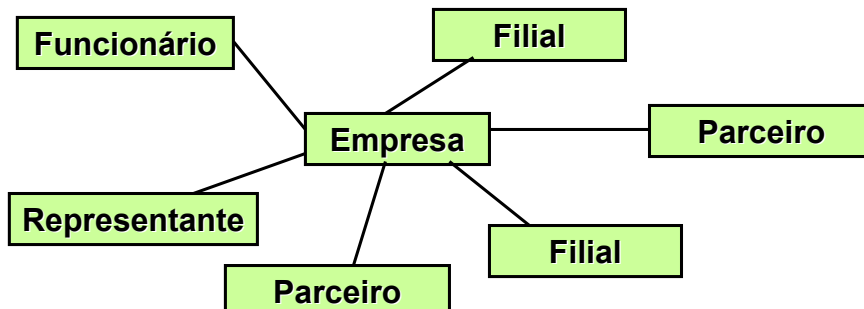
Virtual Private Networks

Universidade Santan Cecília

Prof. Hugo Santana

Motivação para as VPN's

- PROBLEMA:
 - Como construir sistemas de informação de grande amplitude geográfica sem arcar com custos excessivos com a infra-estrutura de comunicação.

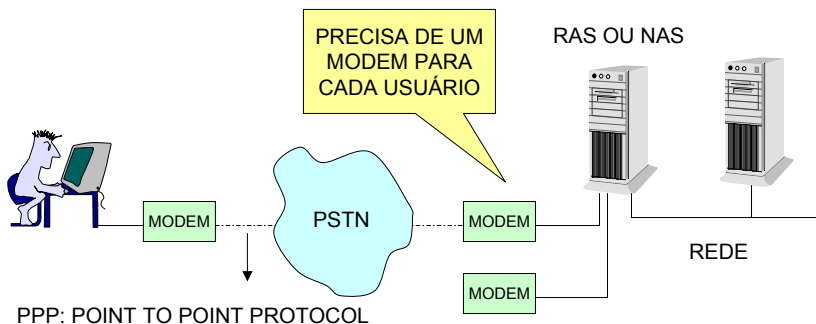


Soluções Usuais

- Utilizar os enlaces de comunicação temporários
 - LINHAS DISCADAS:
 - sistema público de telefonia
- Utilizar enlaces de comunicação permanentes
 - LINHAS DEDICADAS ou PRIVATIVAS:
 - Serviços disponibilizados por empresas de telecomunicação.

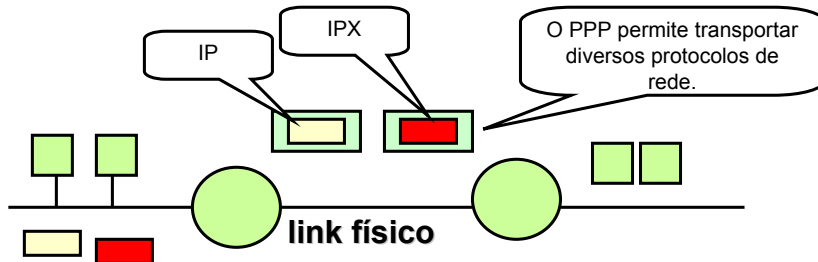
Acesso por linha discada

- Serviço de Acesso Remoto:
 - Implementado pelos sistemas operacionais comerciais mais difundidos.
 - Permite que um usuário acesse um servidor por linha discada.

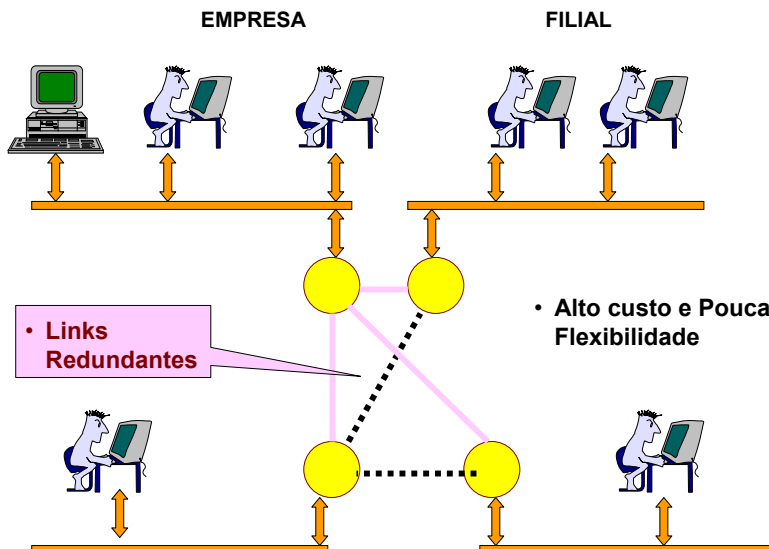


PPP: Point to Point Protocol

- Permite criar conexão de rede através de links ponto a ponto.
 - O PPP é um protocolo do nível de enlace destinado a transportar mensagens ponto a ponto.
 - O PPP supõem que o link físico transporta os pacotes na mesma ordem em que foram gerados.



Acesso por linhas privadas

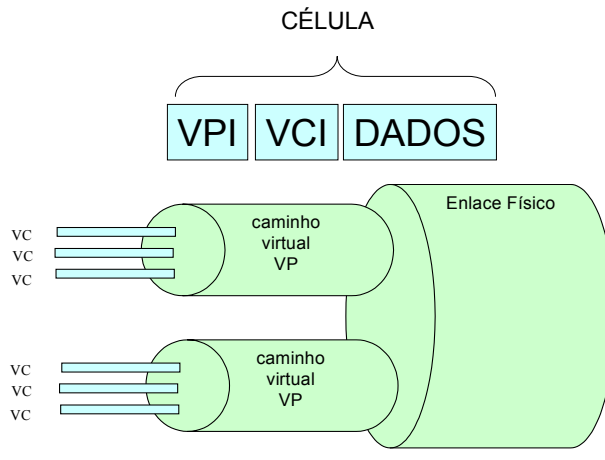


Tecnologias para Linhas Privativas

- Linhas privadas podem ser implementadas com:
 - ATM ou Frame-Relay
 - Comunicação Orientada a Conexão
 - Connection-Oriented
- Ambas as tecnologias permitem dividir a banda de um enlace físico através de circuitos virtuais.
- ATM:
 - VPI e VCI
- FRAME RELAY
 - DLCI

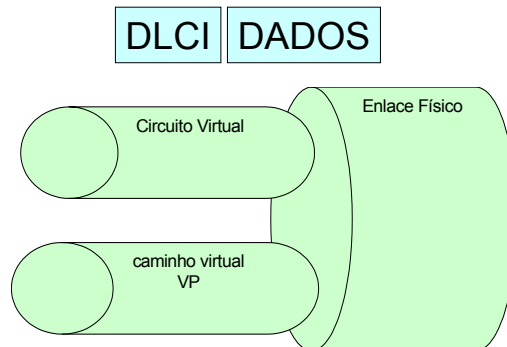
Circuitos Virtuais ATM

- ATM utiliza uma estrutura hierárquica para criar circuitos virtuais.

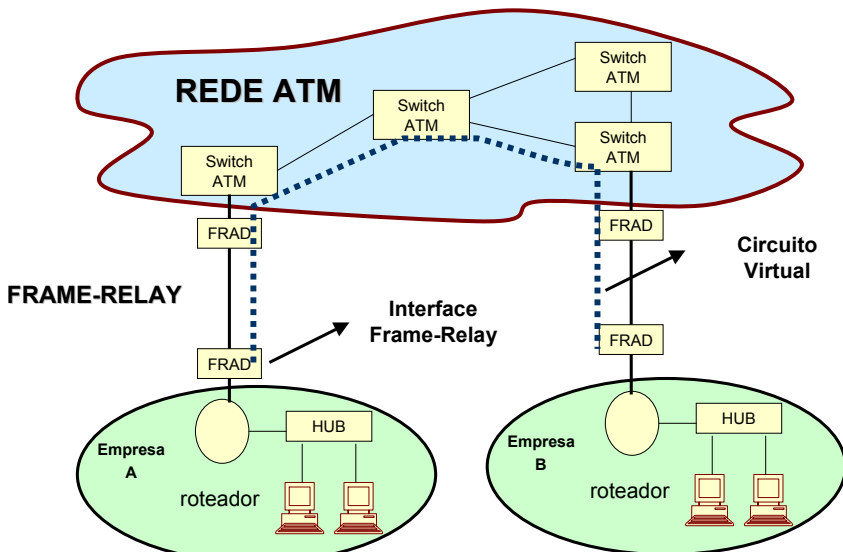


Frame-Relay

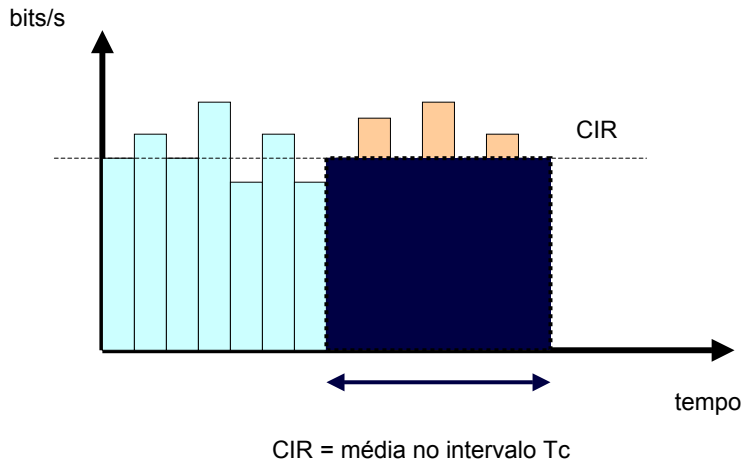
- Frame-relay utiliza uma estrutura simples para criação de circuitos virtuais.



Rede Frame Relay



CIR - Committed Information Rate



SLA: Service Level Agreement

- SLA define as métricas usadas para descrever o desempenho de um serviço Frame Relay.
- Essas métricas pode ser usadas para estabelecer um contrato entre o provedor de serviço e um usuário ou entre provedores de serviço.
 - Frame Transfer Delay
 - Frame Delivery Ratio
 - Data Delivery Ratio
 - Service Availability
 - **Segurança?**

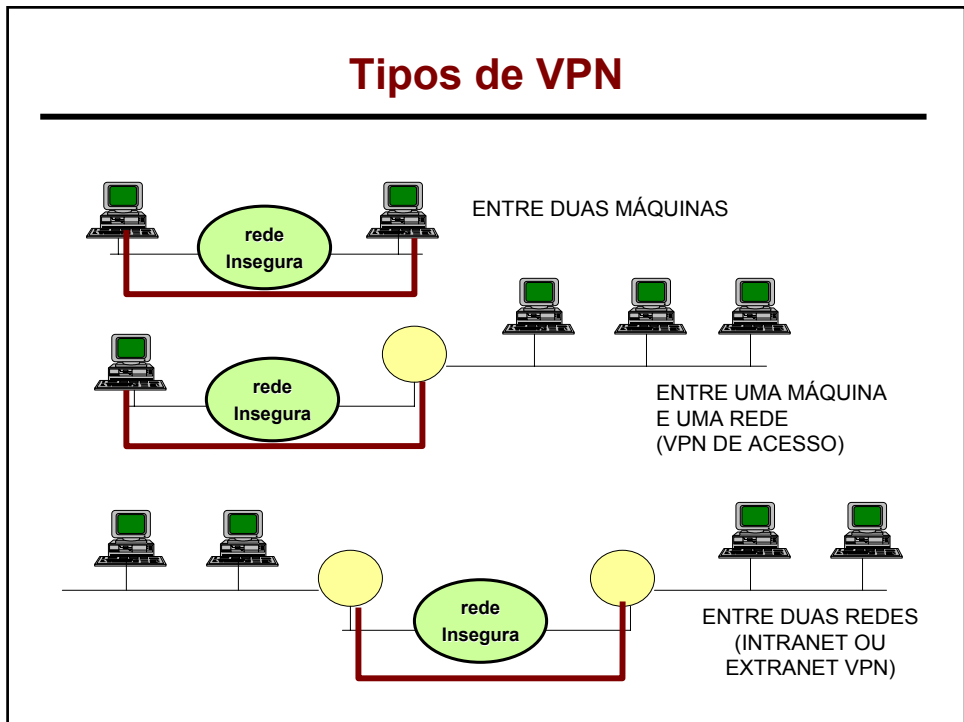
VPN X Circuitos Virtuais

- Circuitos Virtuais ATM ou Frame Relay
 - **Objetivo:**
 - Garantia de Qualidade de Serviço (QoS).
 - **Princípio:**
 - Criam canais com QoS controlado.
 - **Limitação:**
 - Depende do provedor de serviço.

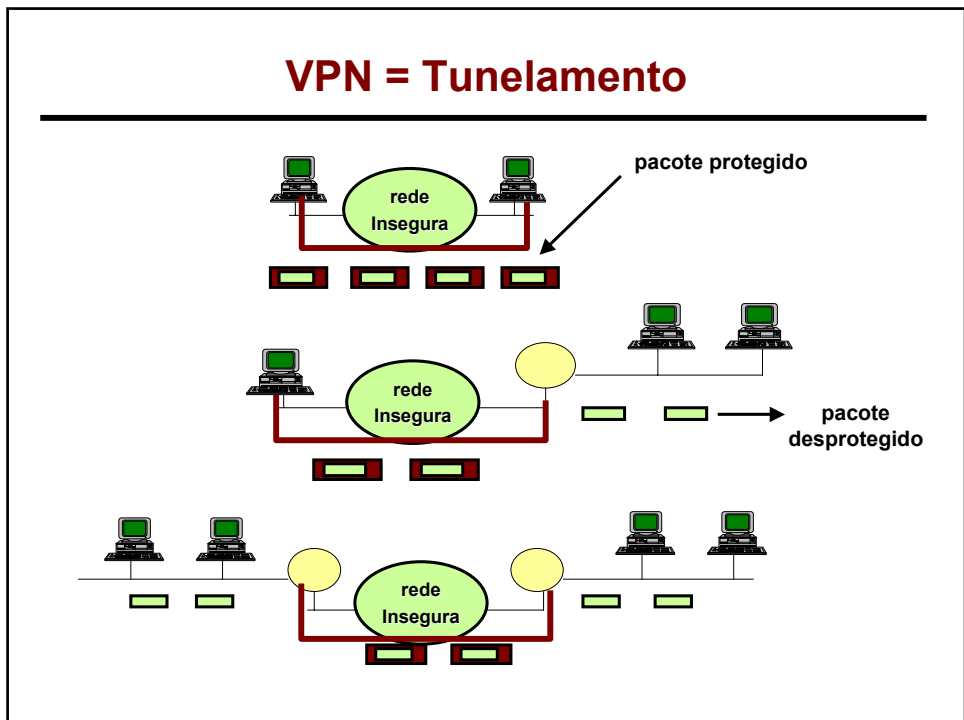
VPN X Circuitos Virtuais

- VPN: Virtual Private Networks
 - **Objetivos:**
 - Oferecer segurança através de redes IP potencialmente inseguras.
 - Permitir o transporte de outros protocolos de rede sobre a Internet.
 - **Princípios:**
 - Encapsulamento adicional de quadros e pacotes.
 - **Limitação:**
 - Não oferece qualidade de serviço

Tipos de VPN

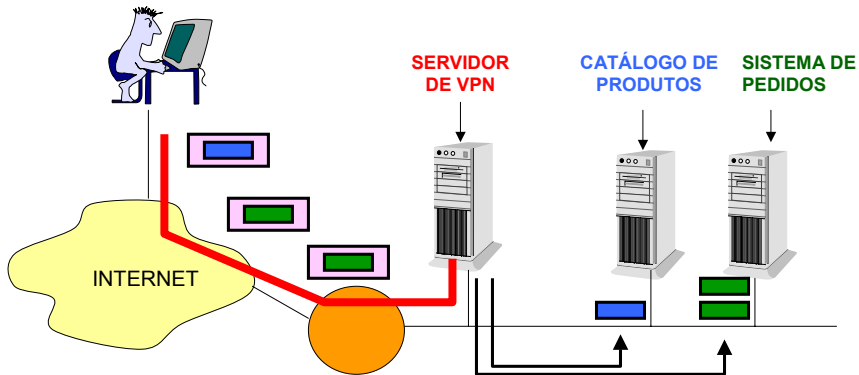


VPN = Tunelamento



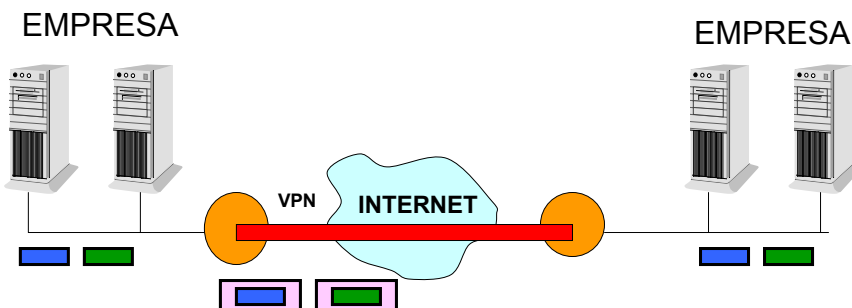
Exemplo: VPN de Acesso

- Vendedor que precisa acessar a rede corporativa de um ponto remoto.



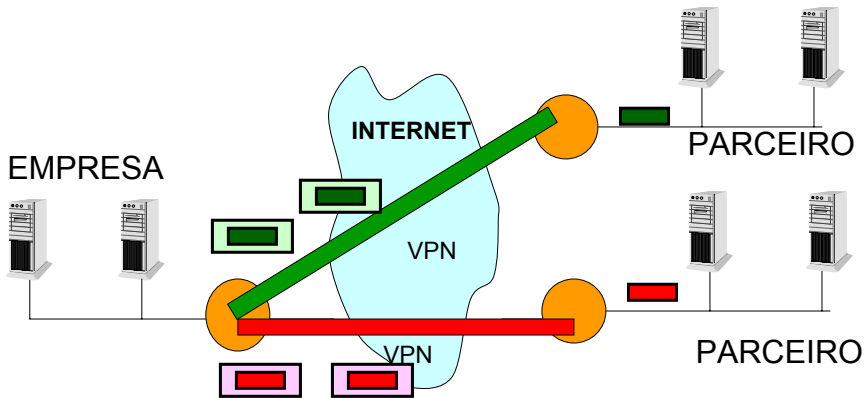
Intranet VPN

- Permite construir uma intranet utilizando recursos de uma infra-estrutura de comunicação pública (e.g. Internet).



Extranet VPN

- Permite construir uma rede que compartilhe parcialmente seus recursos com empresas parceiras (fornecedores, clientes, parceiros, etc.).

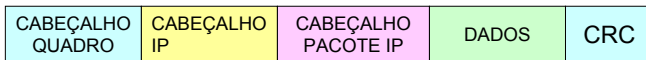
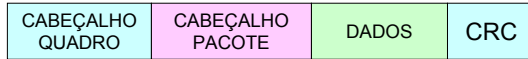


Conceitos Básicos de uma VPN

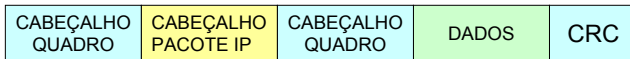
- TUNELAMENTO:
 - Permite transportar pacotes com IP privado ou com outros protocolos de rede através da Internet.
- AUTENTICAÇÃO:
 - Permite controlar quais usuários podem acessar a VPN
 - Reduz o risco de ataques por roubo de conexão e spoofing.
- CRIPTOGRAFIA:
 - Garante a confidencialidade dos dados transportados através da VPN.

TUNELAMENTO

- **TUNELAR:** Significa colocar as estruturas de dados de um protocolo da mesma camada do modelo OSI dentro do outro.
- Existem dois tipos de Tunelamento:
 - **Camada 3:** Transporta apenas pacotes IP
 - **Camada 2:** Permite transportar outros protocolos de rede: IP, NetBEUI, IPX.

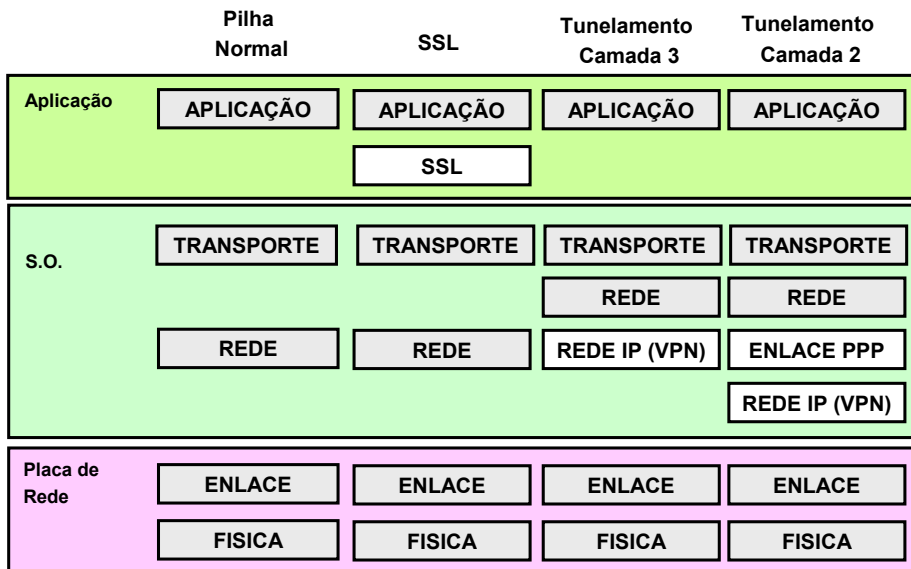


TUNELAMENTO DA CAMADA 3

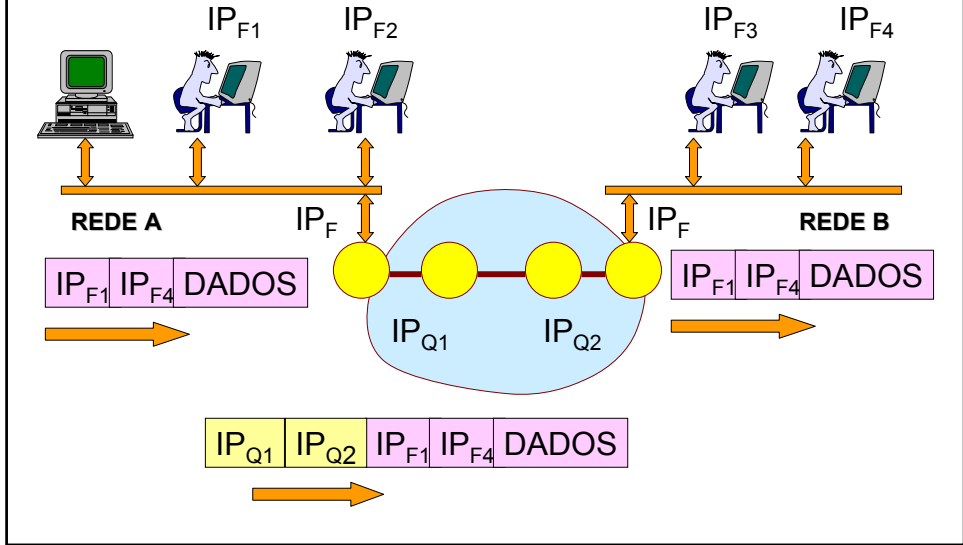


TUNELAMENTO DA CAMADA 2

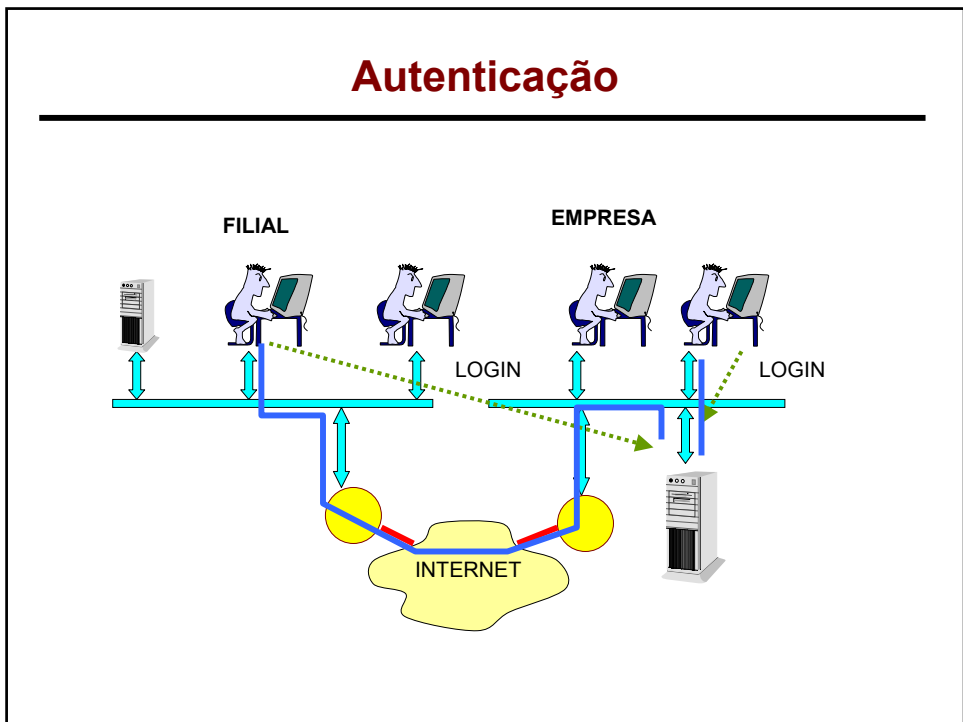
TUNELAMENTO



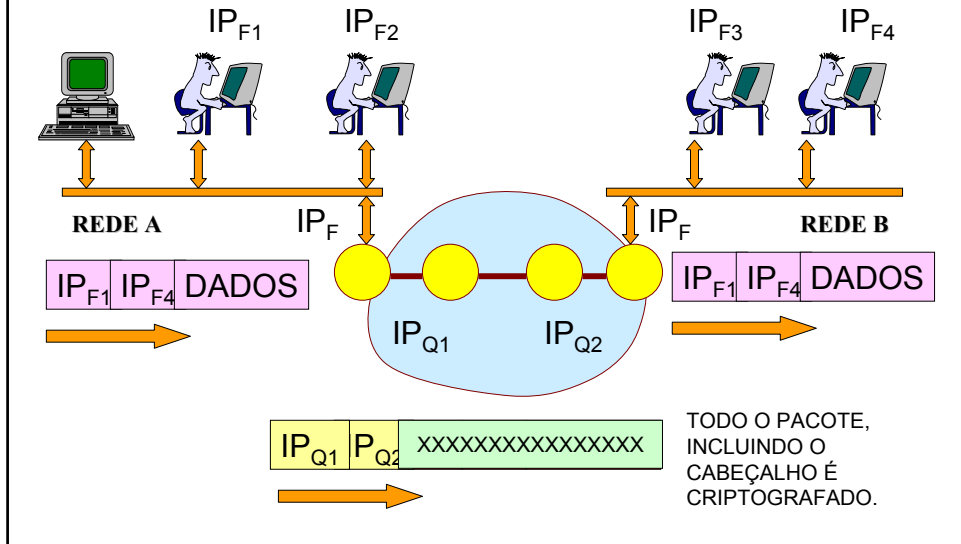
Exemplo



Autenticação



Criptografia



PROCOLOS PARA VPN

- **L2F:**
 - Layer 2 Forwarding Protocol (Cisco)
 - Não é mais utilizado.
- **PPTP:**
 - Tunelamento de Camada 2
 - Point-to-Point tunneling Protocol
- **L2TP:**
 - Tunelamento de Camada 2
 - Level 2 Tunneling Protocol (L2TP)
 - Combinação do L2F e PPTP
- **IPSec:**
 - Tunelamento de Camada 3
 - IETF (Internet Engineering Task Force)

Protocolos para VPN

Protocolo	Tunelamento	Criptografia	Autenticação	Aplicação
PPTP	Camada 2	Sim	Sim	VPN de Acesso Iniciada no Cliente
L2TP	Camada 2	Não	Sim	VPN de Acesso Iniciada no NAS Intranet e Extranet VPN
IPsec	Camada 3	Sim	Sim	VPN de Acesso Intranet e Extranet VPN
IPsec e L2TP	Camada 2	Sim	Sim	VPN de Acesso Iniciada no NAS Intranet e Extranet VPN

PPTP: Point-to-Point tunneling Protocol

- Definido pelo PPTP Forum:
 - Ascend Communication, U.S. Robotics, 3Com Corporation, Microsoft Corporation e ECI Telematics
 - Formalizado por RFC
- Requisitos para Utilização:
 - Os sistemas operacionais do cliente e do servidor devem suportar PPTP
 - PPTP é o protocolo de tunelamento mais difundido no mercado:
 - Windows, Linux, Roteadores, etc...

Cenários de Utilização do PPTP

- Cenários:

- A) Acesso por modem:

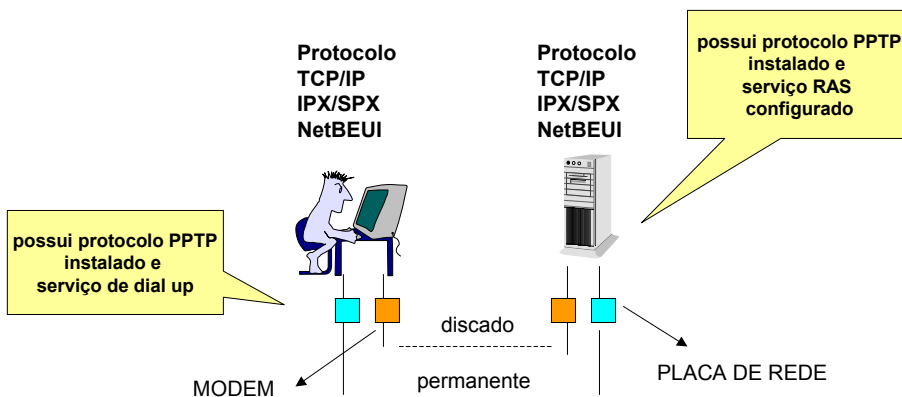
- O cliente estabelece uma conexão com um provedor (ISP) e depois com o servidor de VPN.

- B) Acesso por placa de rede:

- O cliente já está na Internet, ele se conecta diretamente ao servidor de VPN.
 - O cliente e o servidor da VPN se encontram na mesma rede corporativa.

Tipos de Conexão

- O cliente tem acesso direto ao servidor, seja via linha discada, seja via rede.



Opções de Configuração

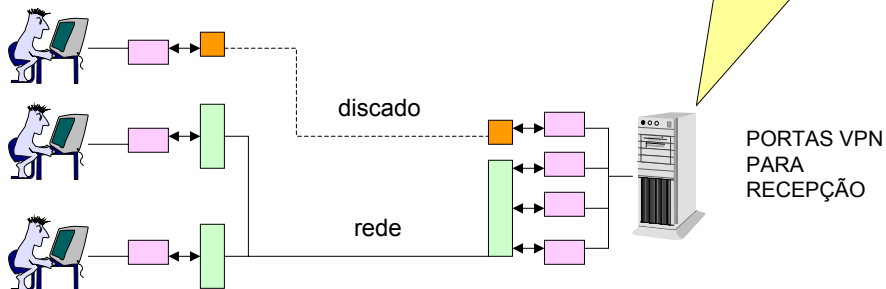
Opção no Cliente:

- Conexões Virtuais Simultâneas (1 no WINDOWS 95/98).
- Criptografia
- Método de Autenticação

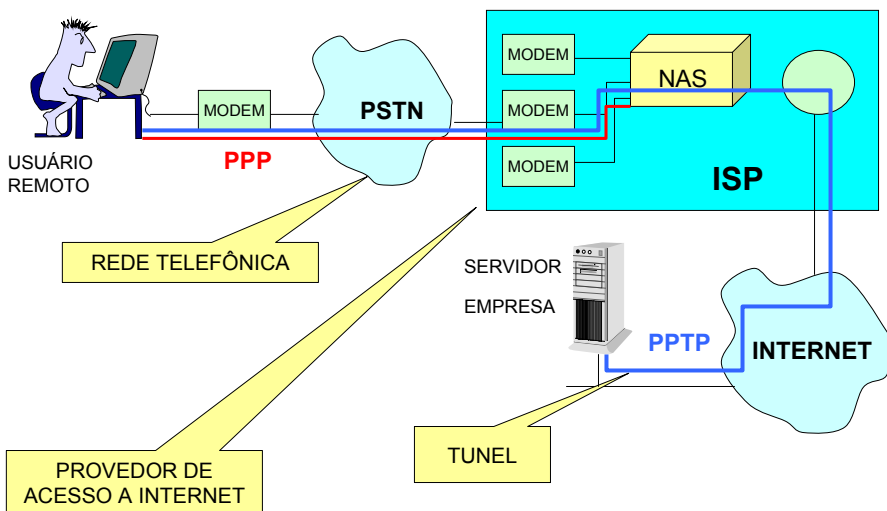
Opções no Servidor:

- Número de portas VPN
- DHCP ou RAS
- O cliente pode especificar seu IP (S/N)
- Range de IP's
- Tipo de Autenticação
- Criptografia de Dados (S/N)
- Acesso ao servidor ou a toda rede.

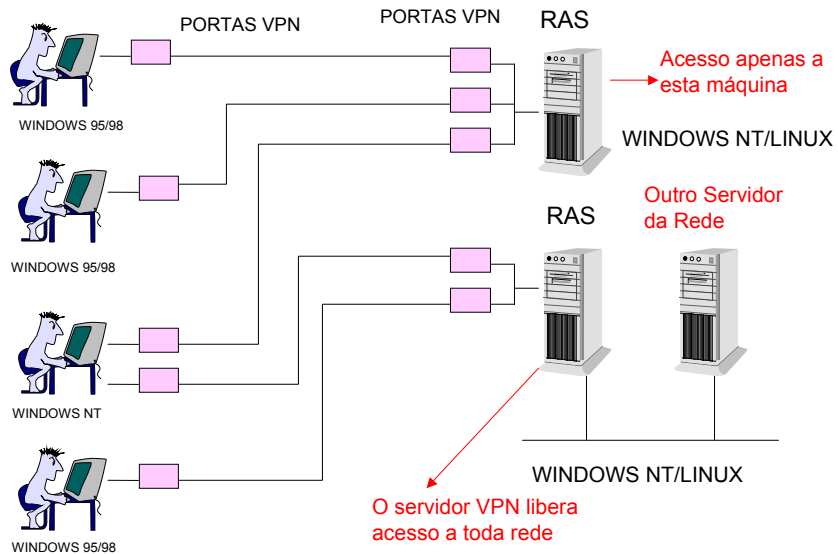
PORTAS VPN
PARA DISCAGEM



Conexão PPTP

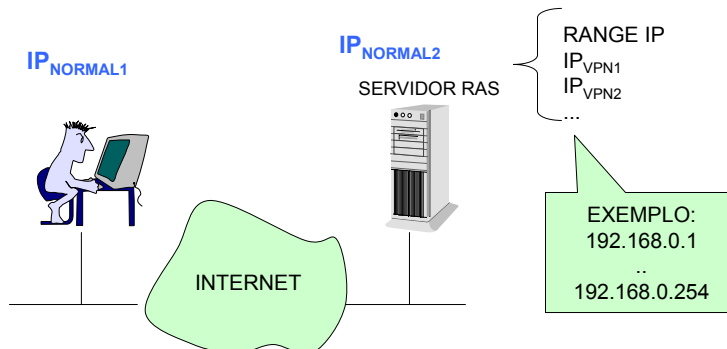


Topologias de Conexão



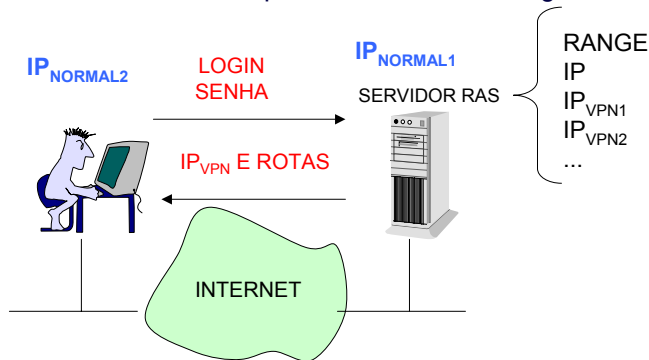
Exemplo

- 1) Situação Inicial
 - Considere um cliente e um servidor conectados por uma rede TCP/IP.
 - Ambos possuem endereços pré-definidos.



Estabelecimento da Conexão PPTP

- 2) O cliente disca para o endereço IP do servidor.
 - Nesse processo, o cliente deve fornecer seu login e senha.
 - A conta do usuário deve existir no servidor, e ele deve ter direitos de acesso via dial up.
 - O servidor atribui um IP para o cliente, e reconfigura suas rotas.

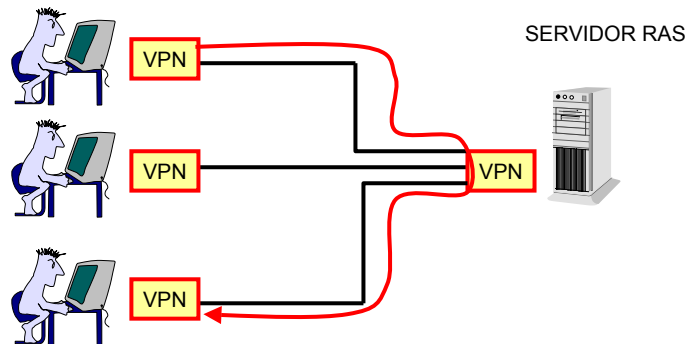


IP's de tunelamento

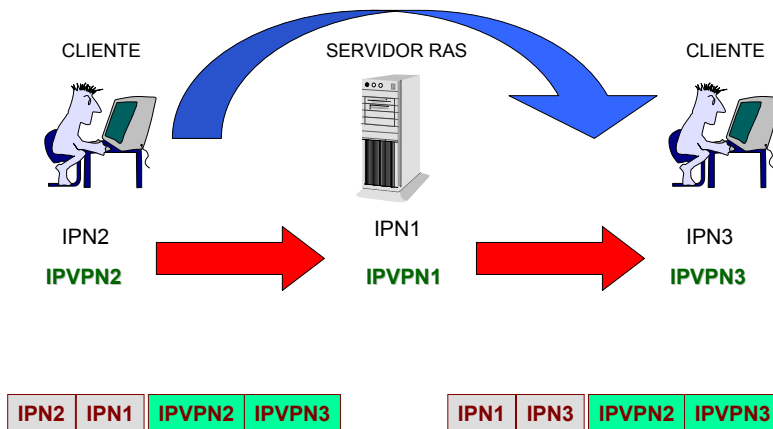
- Uma conexão PPTP que encapsula protocolos TCP/IP em outro datagrama IP envolve a utilização de 2 pares de IP:
 - **IP sem tunelamento**
 - cliente: $IP_{NORMAL2}$ (e.g. 210.0.0.1)
 - servidor: $IP_{NORMAL1}$ (eg. 200.0.0.1)
 - **IP com tunelamento**
 - cliente: IP_{VPN2} (192.168.0.2)
 - servidor: IP_{VPN1} (192.168.0.1)

Rede Virtual

- Os clientes conectados a rede virtual utilizam o servidor RAS como roteador.

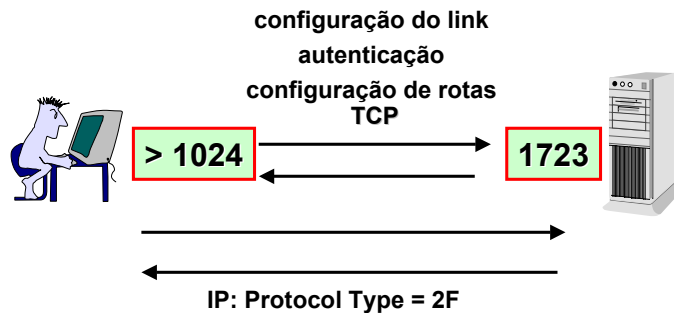


Comunicação com Tunelamento

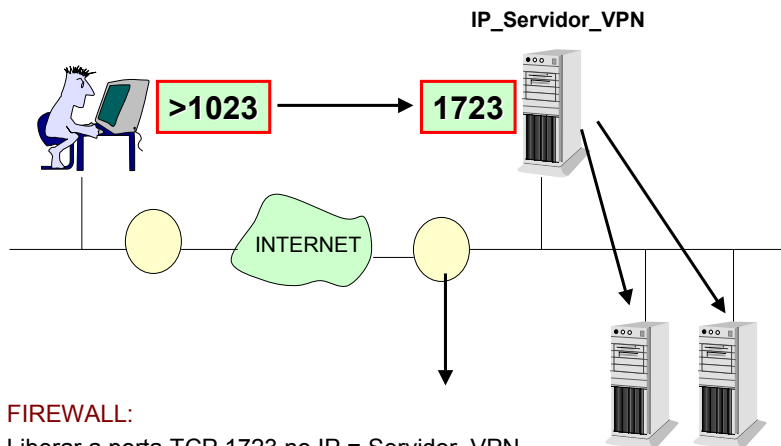


Porta de Controle

- O estabelecimento de uma conexão PPTP é feito pela porta de controle TCP 1723.
- Esta porte precisa ser liberada no firewall para implantar uma VPN de acesso.



Exemplo de VPN com Firewall



Segurança do PPTP

- PPTP fornece dois serviços de segurança:
 - Autenticação
 - Criptografia de Dados
- Diversos tipos de autenticação podem ser utilizadas:
 - CHAP: Standard Encrypted Authentication
 - MS-CHAP: Microsoft Encrypted Authentication
 - Único Método que Permite Criptografia
 - PAP: Password Authentication Protocol
 - Autenticação Sem Criptografia

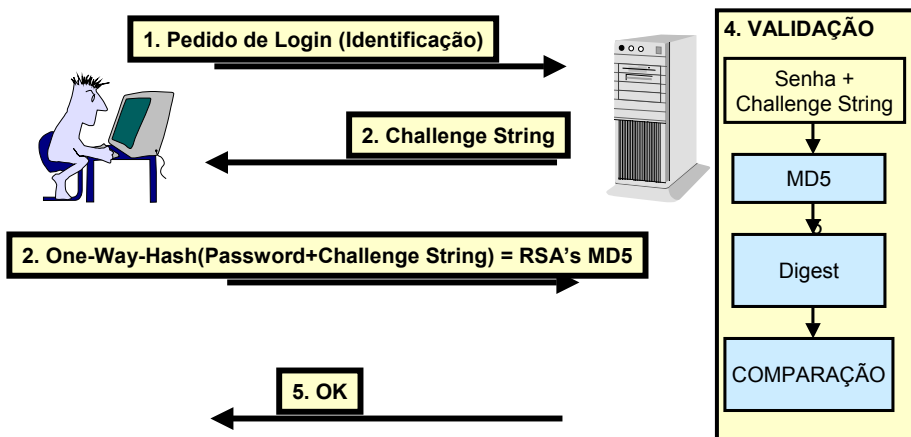
Autenticação por CHAP

- CHAP: Challenge Handshake Authentication Protocol
 - Definido pela RFC 1994 como uma extensão para PPP
 - Não utiliza passwords em aberto
 - Um password secreto, criado apenas para a sessão, é utilizado para o processo de autenticação.
 - CHAP permite repetir o processo de validação da senha durante a conexão para evitar ataques por roubo de conexão.

Autenticação CHAP

- O processo utilizado é do tipo challenge-response:
 - a) O cliente envia sua identificação ao servidor (mas não a senha)
 - b) O servidor responde enviando ao cliente uma “challenge string”, única, criada no momento do recebimento do pedido.
 - c) O cliente aplica um algoritmo RSA’s MD5 (one-way hashing), e combinado-se password e a string recebida.
 - d) O servidor compara a senha criptografada recebida pelo usuário aplicado a mesma operação na senha armazenada localmente.

Autenticação no CHAP



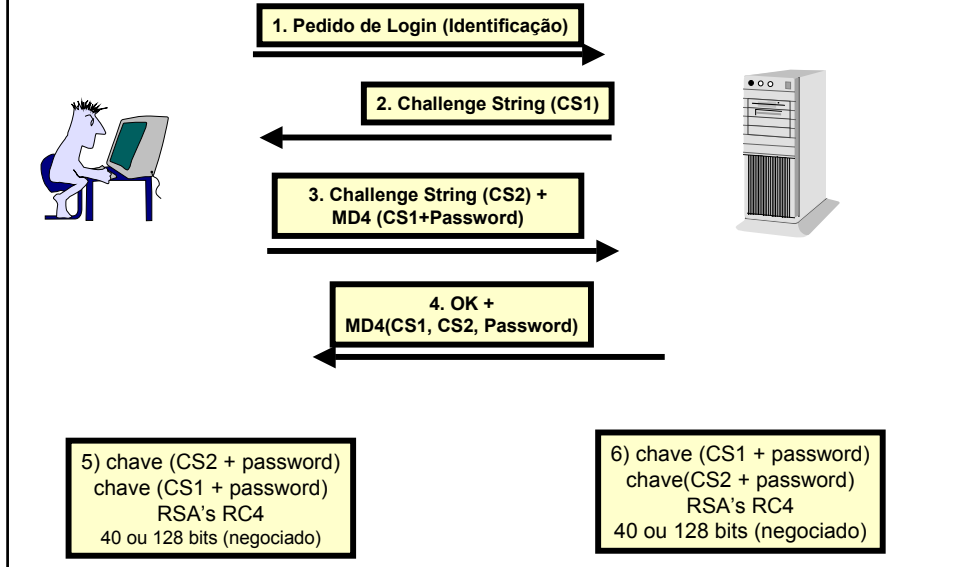
MD4 e MD5

- O Algoritmo MD5:
 - Aceita uma mensagem de entrada de tamanho arbitrário e gera como resultado um “fingerprint” ou “message digest” de tamanho fixo (128 bits).
 - Probabilidade de duas mensagens gerarem o mesmo digest: “computationally infeasible”
 - Definido na RFC 1321.
- O Algoritmo MD4:
 - Versão anterior do MD5, menos segura e mais rápida.
 - Probabilidade de duas mensagens gerarem o mesmo digest: 2^{64}
 - Definido na RFC 1320.
 - O site do RSA (www.rsasecurity.com) indica que o MD4 deve ser considerado quebrado (1999).

Autenticação por MS-CHAP

- MS-CHAP: Microsoft - Challenge HandShake Authentication Protocol
- Duas versões:
 - Versão 1:
 - gera chaves criptográficas a partir apenas do password, por isso a chave não muda de uma sessão para outra.
 - a autenticação é one-way: o cliente prova a identidade para o servidor, mas não o contrário.
 - a mesma chave de criptografia é utilizada para enviar e receber dados.
 - Versão 2 (RFC 2759):
 - gera chaves criptográficas a partir do password e da challenge string, por isso a chave muda a cada sessão.
 - a autenticação é two-way (mutual authentication).
 - gera uma chave de criptografia diferente para transmitir e para receber dados.

Autenticação no MS-CHAP



L2TP: Layer Two Tunneling Protocol

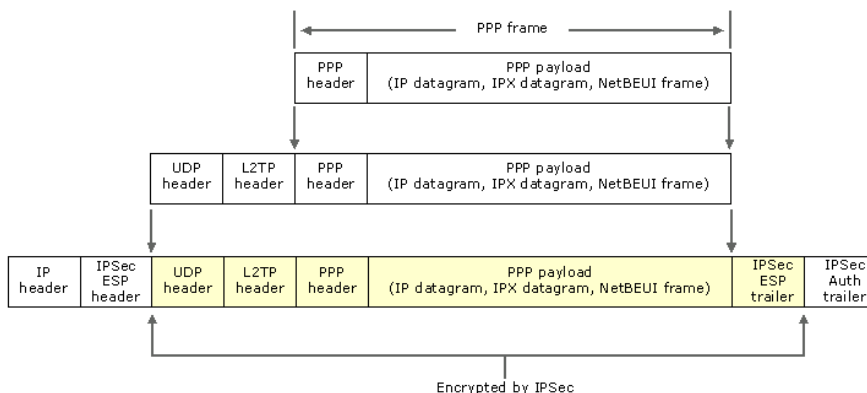
- Baseado nos Protocolos:
 - PPTP
 - L2F
- As mensagens do protocolo L2TP são de dois tipos:
 - Mensagens de controle:
 - Utilizadas para estabelecer e manter as conexões
 - Mensagens de dados:
 - Utilizadas para transportar informações

PPTP e L2TP

- PPTP:
 - Utiliza uma conexão TCP para negociar o túnel, independente da conexão utilizada para transferir dados.
 - Não possui mecanismos fortes de integridade dos pacotes (baseia-se apenas no PPP).
 - Túneis são usualmente criados pelo cliente.
- L2TP:
 - Envia tanto as mensagens de controle quanto os dados encapsulados em datagramas UDP.
 - No Windows 2000, por exemplo, o cliente e o servidor utilizam a porta UDP 1701 para negociar os túneis L2TP.
 - Túneis são usualmente criados automaticamente pelo NAS.

Tunelamento L2TP

- O tunelamento no L2TP é feito com o auxílio do protocolo UDP.
- Observe como o L2TP é construído sobre o protocolo PPP.



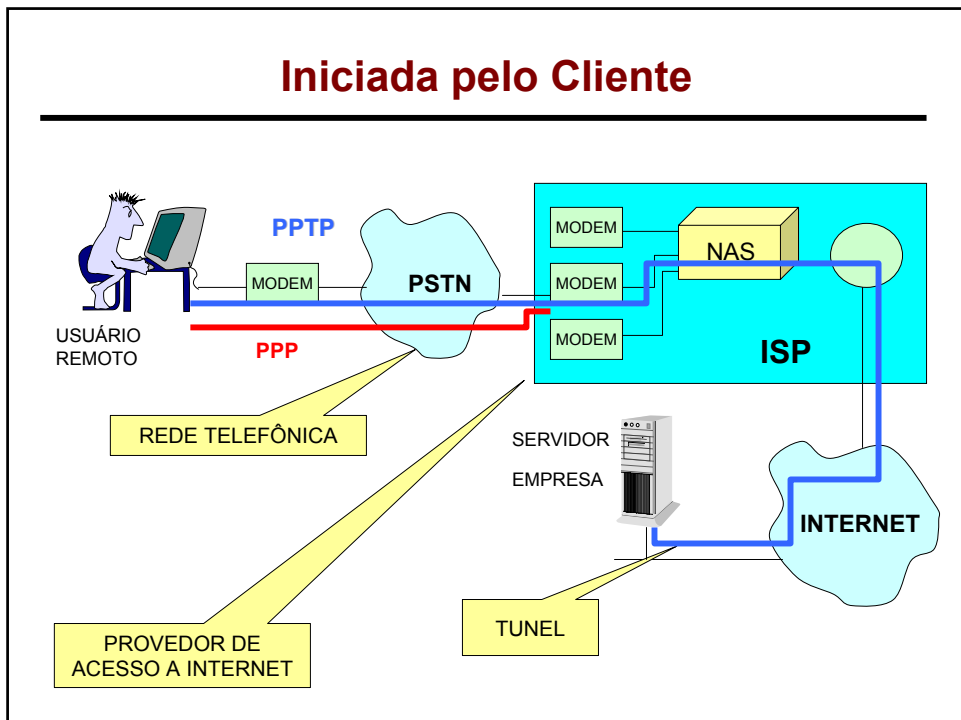
Tipos de VPN de Acesso

- As VPNs de acesso podem ser de dois tipos, dependendo do ponto onde começa a rede segura:

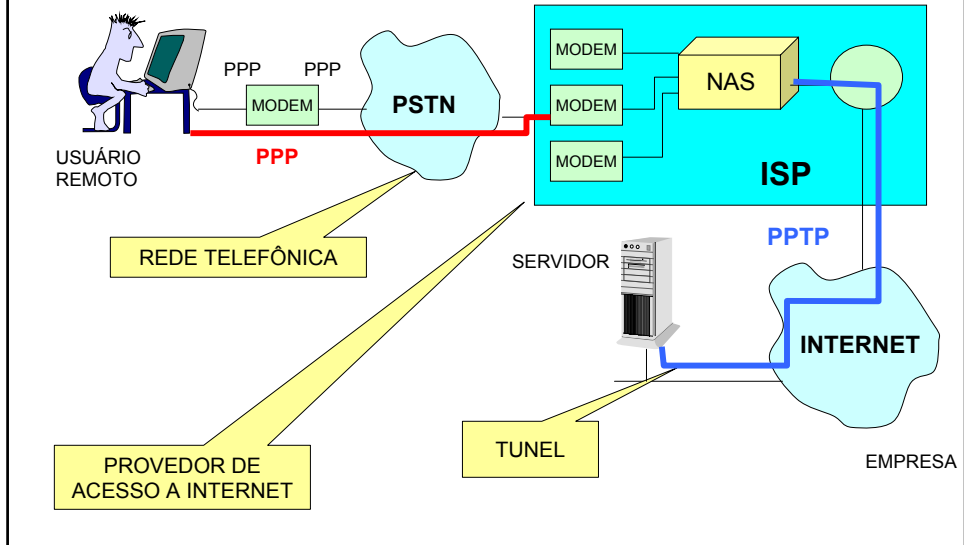
A) Iniciada pelo Cliente

B) Iniciada pelo Servidor de Acesso a Rede (NAS)

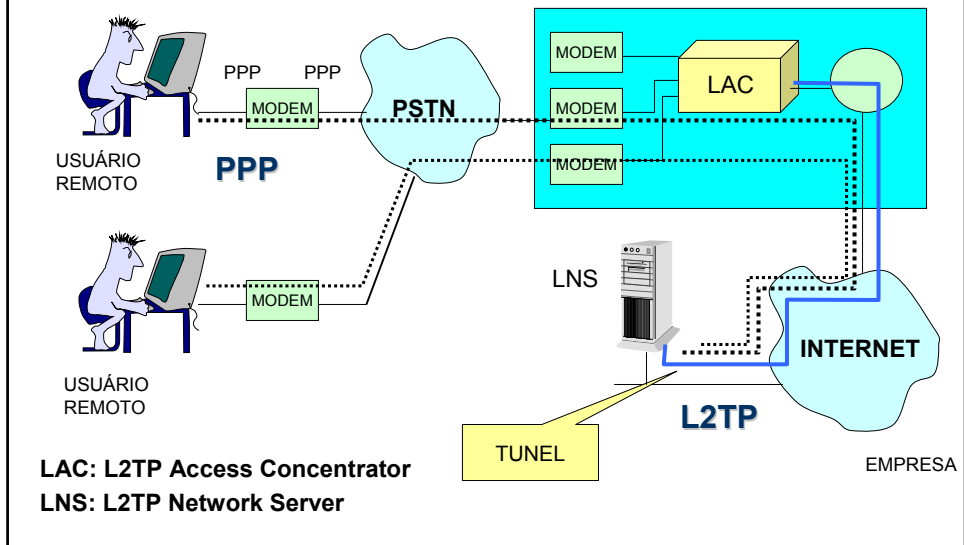
Iniciada pelo Cliente



Iniciada pelo Servidor de Acesso a Rede (NAS)



Conexão L2TP Típica



L2TP

- Possui suporte as seguintes funções:
 - Tunnelamento de múltiplos protocolos
 - Autenticação
 - Anti-spoofing
 - Integridade de dados
 - Certificar parte ou todos os dados
 - Padding de Dados
 - Permite esconder a quantidade real de dados Transportados
- **Não possui suporte nativo para criptografia.**
- Para se obter criptografia, o L2TP deve ser combinado com o IPsec.

Conclusão

- SSL:
 - Segurança fim-a-fim entre aplicações.
 - Necessita que as aplicações sejam reescritas.
 - Protege a camada de aplicação e os dados.
- VPN:
 - Segurança implementada pela rede.
 - É transparente para as aplicações.
 - Protege as camadas de rede, transporte e aplicação.
 - Cria um único ponto de entrada para acesso de usuários externos na rede.