

Entendendo o VPDN

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Conventions](#)

[Glossário](#)

[Visão geral do processo de VPDN](#)

[Protocolos de túneis](#)

[Configurando o VPDN](#)

[Informações Relacionadas](#)

Introduction

Uma Rede Virtual Privada de Discagem (VPDN) permite que um serviço de discagem de rede privada se estenda até os servidores de acesso remoto (definidos como o L2TP Access Concentrator [LAC]).

Quando um cliente do Point-to-Point Protocol (PPP) disca para um LAC, o LAC determina que deve encaminhar a sessão PPP para um Servidor de Rede de L2TP (LNS, L2TP Network Server) do cliente. O LNS então autentica o usuário e começa a negociação PPP. Uma vez que a instalação do PPP esteja concluída, todas os quadros são enviados pelo LAC para o cliente e o LNS.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. All of the devices used in this document started with a cleared (default) configuration. Se você estiver trabalhando em uma rede ativa, certifique-se de que entende o impacto potencial de qualquer comando antes de utilizá-lo.

Conventions

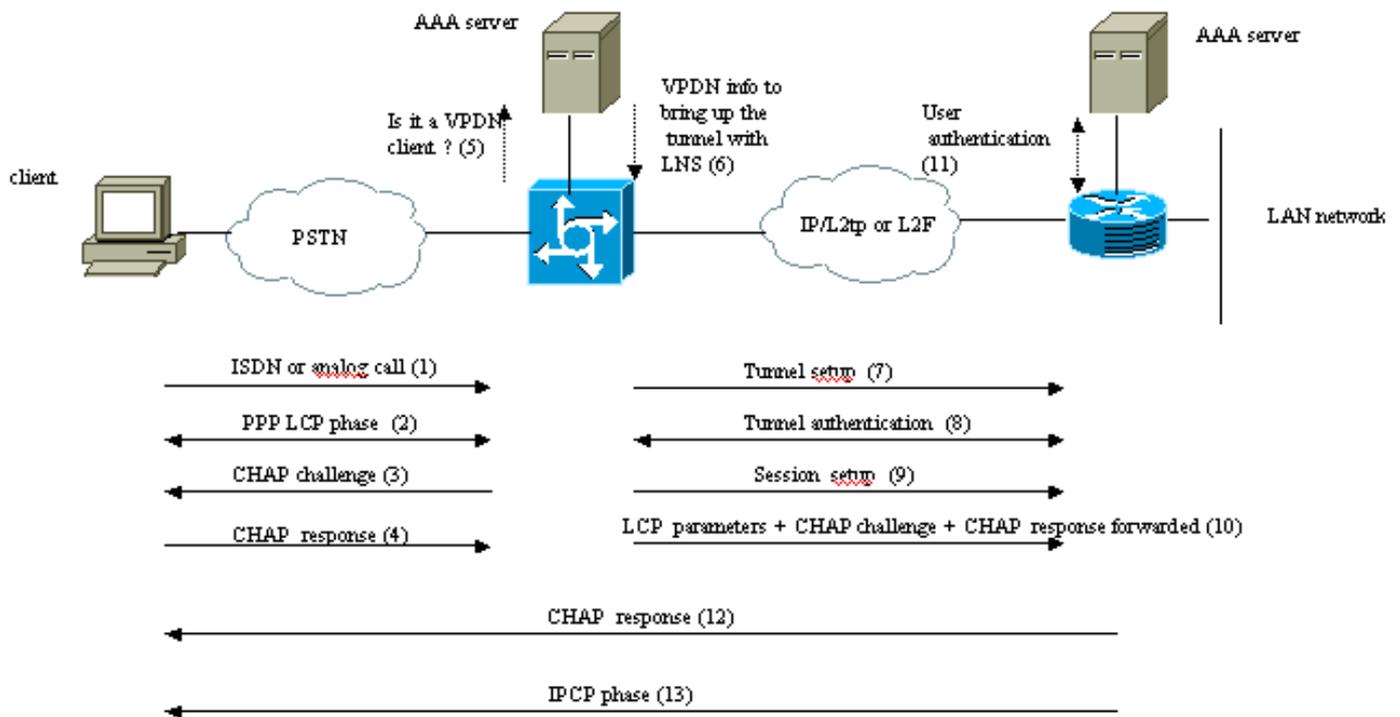
For more information on document conventions, refer to the [Cisco Technical Tips Conventions](#).

Glossário

- **Cliente:** PC ou roteador conectado a uma rede de acesso remoto, que é o iniciador de uma chamada.
- **L2TP:** Layer 2 Tunnel Protocol. O PPP define um mecanismo de encapsulamento para transportar pacotes multiprotocolo através de links ponto a ponto da camada 2 (L2, layer 2). Em geral, o usuário obtém uma conexão L2 a um Servidor de Acesso à Rede (NAS, Network Access Server) usando uma técnica como o serviço telefônico básico (POTS, dialup plain old telephone service), ISDN ou a Linha Digital Assimétrica de Assinante (ADSL, Asymmetric Digital Subscriber Line). Então o usuário executa o PPP em tal conexão. Nessa configuração, o ponto de encerramento da L2 e o ponto de extremidade da sessão PPP estão no mesmo dispositivo físico (o NAS). O L2TP estende o modelo PPP permitindo que os pontos finais L2 e PPP residam em dispositivos diferentes interconectados por uma rede. Com L2TP, o usuário tem uma conexão L2 a um concentrador de acesso, que envia quadros PPP individuais pelo túnel até o NAS. Isso permite que o processamento real de pacotes PPP seja separado da terminação do circuito L2.
- **L2F:** Layer 2 Forwarding Protocol. O L2F é um protocolo de tunelamento mais antigo do que o L2TP.
- **LAC:** Concentrador de Acesso L2TP. Um nó que atua como um lado de um ponto de extremidade do túnel L2TP e é um peer do LNS. O LAC está localizado entre um LNS e um cliente, e envia pacotes entre eles. Os pacotes enviados do LAC para o LNS necessitam de encapsulamento com o protocolo L2TP. A conexão do LAC ao cliente é geralmente realizada por ISDN ou sinal analógico.
- **LNS:** Servidor de Rede L2TP. Um nó que age como um lado de um ponto final do túnel L2TP e é um peer para o LAC. O LNS é o ponto de encerramento lógico de uma sessão PPP que está sendo colocada em túnel a partir do cliente pelo LAC.
- **Gateway Local:** Mesma definição que LNS na terminologia L2F.
- **NAS:** A mesma definição que LAC em terminologia L2F.
- **Túnel:** Na terminologia de L2TP, existe um túnel entre um par LAC-LNS. O túnel consiste em uma conexão de controle e zero ou mais sessões L2TP. O Túnel carrega datagramas PPP encapsulados e mensagens de controle entre o LAC e o LNS. O processo é o mesmo que para L2F.
- **Sessão:** O L2TP é orientado para conexão. O LNS e o LAC mantêm um estado para cada chamada que é iniciada ou respondida por um LAC. Uma sessão L2TP é criada entre LAC e LNS quando uma conexão PPP de ponta a ponta estiver estabelecida entre um cliente e o LNS. Os datagramas relacionados à conexão PPP são enviados pelo túnel entre o LAC e o LNS. Existe um relacionamento um para um entre as Sessões L2TP estabelecidas e suas chamadas associadas. O processo é o mesmo que para L2F.

Visão geral do processo de VPDN

Na descrição do processo de VPDN abaixo, utilizamos a terminologia L2TP (LAC e LNS).



..... These phases can be performed locally on the router or by the AAA server

1. O cliente faz uma chamada para o LAC (geralmente usando um modem ou um cartão ISDN).
2. O cliente e o LAC iniciam a fase PPP por meio da negociação das opções LCP (método de autenticação PAP [Protocolo de Autenticação de Senha] ou CHAP [Challenge Handshake Authentication Protocol], PPP multilink, compactação etc.).
3. Suponhamos que CHAP tenha sido negociado na etapa 2. O LAC envia uma desafio de CHAP ao cliente.
4. O LAC obtém uma resposta (por exemplo, username@DomainName e senha).
5. Com base no nome do domínio recebido na resposta CHAP ou no DNIS recebido na mensagem de configuração ISDN, o LAC verificar se o cliente é um usuário VPDN ou não. Faz isso usando sua configuração de VPDN local ou contatando um servidor de Autenticação, Autorização e Auditoria (AAA, Authentication, Authorization, and Accounting).
6. Como o cliente é um usuário VPDN, o LAC obtém informações (de sua configuração de VPDN local ou de um servidor AAA) que utiliza para ativar um túnel L2TP ou L2F com o LNS.
7. O LAC ativa um túnel L2TP ou L2F com o LNS.
8. Com base no nome recebido na solicitação do LAC, o LNS verifica se o LAC pode abrir um túnel (o LNS verifica sua configuração VPDN local). Além disso, o LAC e o LNS autenticam cada um (usam o banco de dados local ou entram em contato com um servidor AAA). O Túnel está ativo entre os dois dispositivos. Neste túnel, várias sessões de VPDN podem ser transportadas.
9. Para o cliente nomeusuário@NomedoDomínio, uma sessão de VPDN é disparada do LAC para o LNS. Há uma sessão VPDN por cliente.
10. O LAC encaminha as opções de LCP que ele negociou para o LNS com o cliente, junto ao

username@DomainName e senha recebidos do cliente.

11. O LNS clona um acesso virtual a partir de um molde virtual especificado na configuração do VPDN. O LNS usa as opções LCP recebidas do LAC e autentica o cliente localmente ou entrando em contato com o servidor AAA.
12. O LAC envia uma resposta CHAP ao cliente.
13. A fase do IP Control Protocol (IPCP) é executada e a rota é instalada: a sessão PPP está ativa e executando entre o cliente e o LNS. O LAC apenas encaminha os quadros PPP. Os quadros PPP são enviados pelo túnel entre o LAC e o LNS.

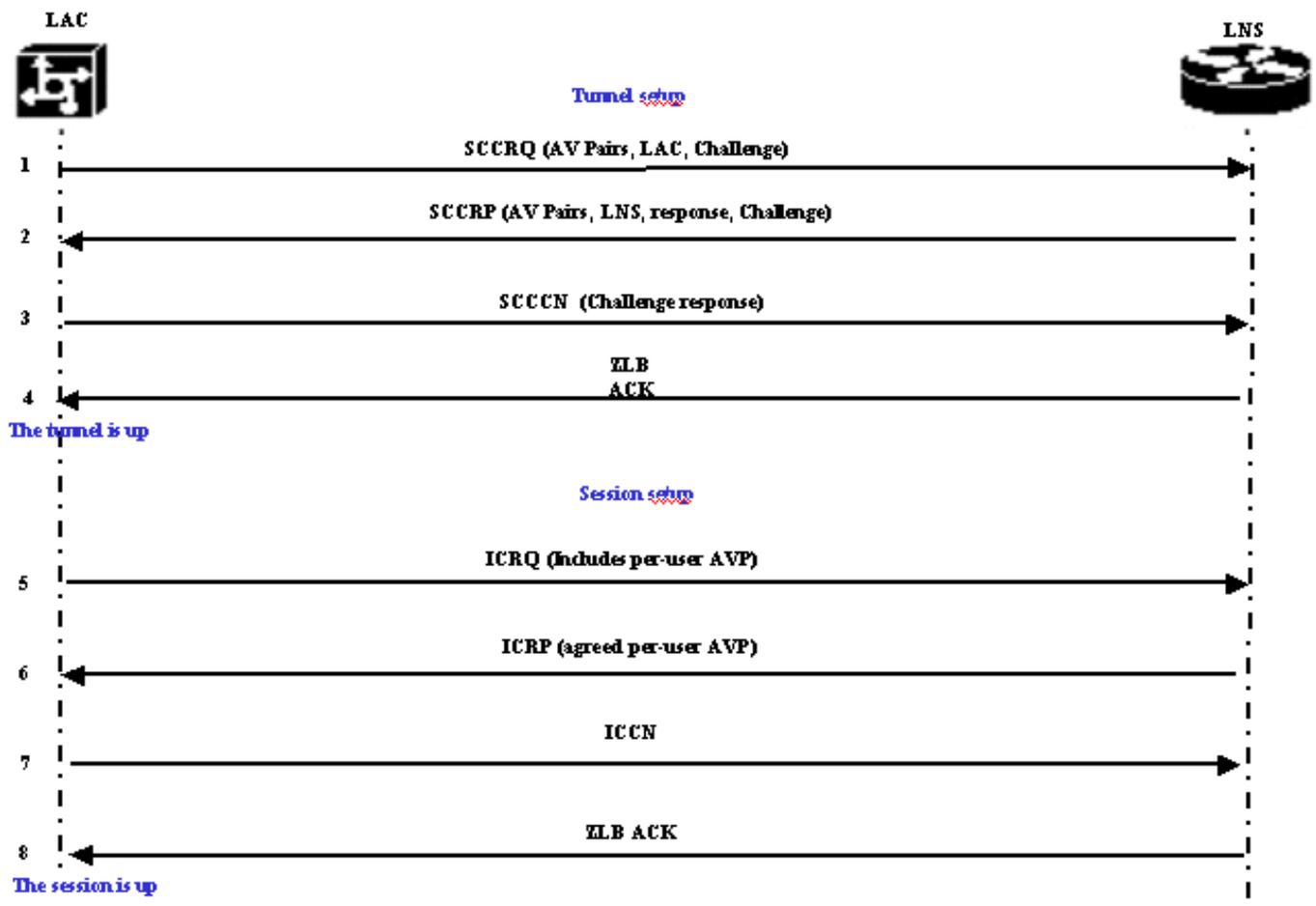
Protocolos de túneis

Um túnel VPDN pode ser construído usando o Layer-2 Forwarding Protocol (L2F) ou o Layer-2 Tunneling Protocol (L2TP).

- O L2F foi apresentado pela Cisco no RFC 2341 e também é usado para encaminhar sessões PPP para PPP de Multilink de Multibase.
- O L2TP, introduzido no RFC 2661, combina o melhor do protocolo Cisco L2F e do protocolo de tunelamento ponto a ponto (PPTP) Microsoft. Além disso, o L2F suporta apenas VPDN de discagem de entrada, enquanto o L2TP suporta VPDN de discagem de entrada e de saída.

Ambos os protocolos usam a porta UDP 1701 para criar um túnel pela rede IP de forma a encaminhar quadros de camada de link. Para o L2TP, a configuração para o tunelamento de uma sessão PPP consiste em duas etapas:

1. Estabeleça um túnel entre o LAC e o LNS. Essa fase ocorre apenas quando não há túnel ativo entre os dois dispositivos.
2. Estabelecimento de uma sessão entre o LAC e o LNS.



O LAC decide se um túnel deve ser iniciado do LAC para o LNS.

1. O LAC envia uma SCCRQ (Start-Control-Connection-Request, Iniciar solicitação de conexão de controle). Um desafio CHAP e pares AV estão incluídos nessa mensagem.
2. O LNS responde com uma mensagem Start-Control-Connection-Reply (SCCRP). Um desafio CHAP, a resposta ao desafio do LAC e os pares AV são incluídos nesta mensagem.
3. O LAC envia uma Start-Control-Connection-Connected (SCCCN). A resposta de CHAP é incluída nesta mensagem.
4. O LNS responde com um ZLB ACK (Zero-Length Body Acknowledgement). Esse reconhecimento pode ser transportado em outra mensagem. O túnel está ativado.
5. O LAC envia uma Solicitação de Chamada de Entrada (ICRQ) para o LNS.
6. O LNS responde com uma mensagem de resposta de chamada recebida (ICRP).
7. O LAC envia um ICCN (Incoming-Call-Connected).
8. O LNS responde com um ZLB ACK. Tal reconhecimento também pode ser realizado em outra mensagem.
9. A sessão está ativa.

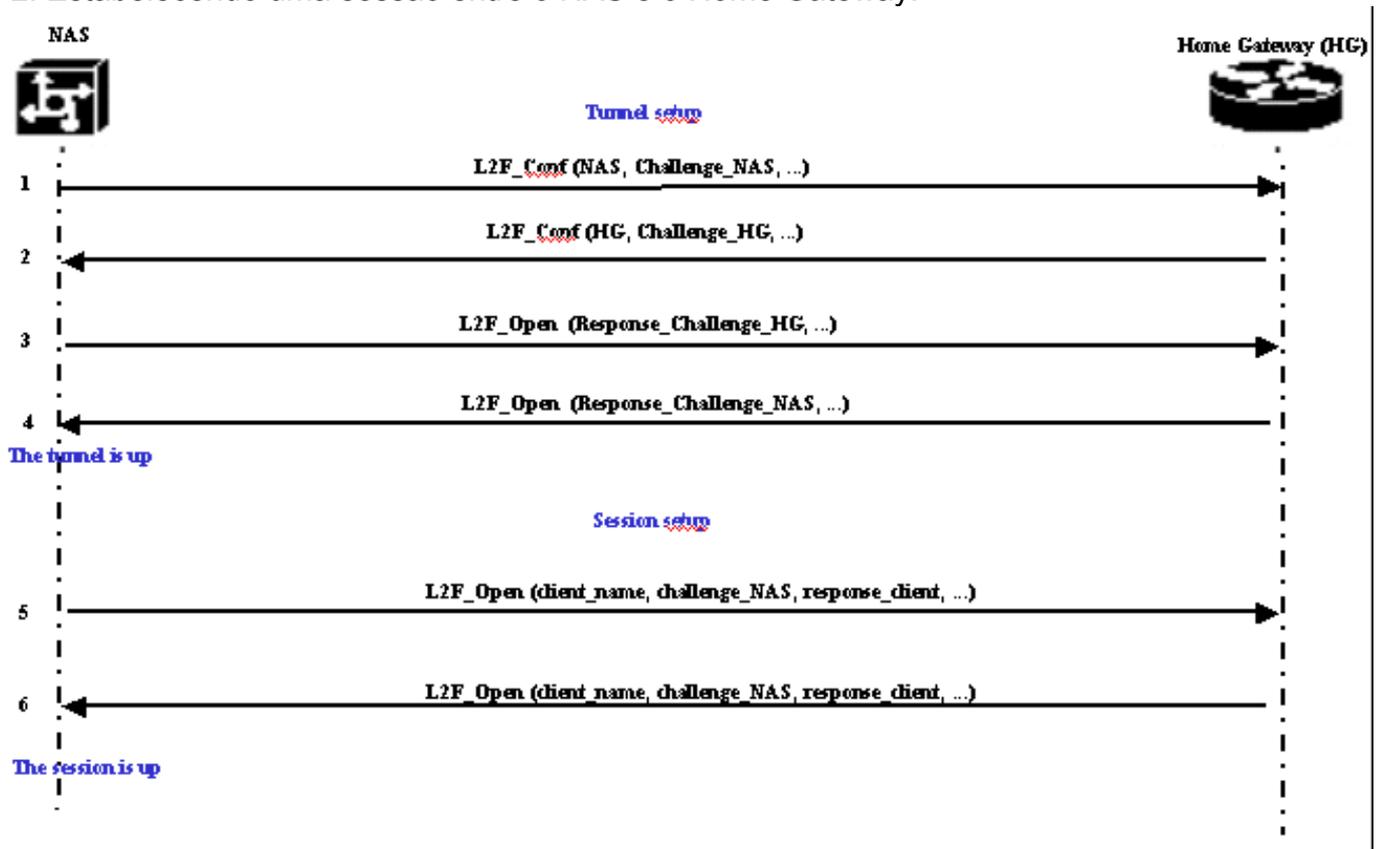
Observação: as mensagens acima usadas para abrir um túnel ou uma sessão transportam Pares de Valor de Atributo (AVPs) definidos no RFC 2661. Descrevem propriedades e informações (como cobertura da portadora, nome de host, nome de fornecedor e tamanho de janela). Alguns pares AV são obrigatórios e outros são opcionais.

Observação: um ID de túnel é usado para multiplexar e desmultiplexar túneis entre o LAC e o LNS. Um ID de sessão é usado para identificar uma sessão específica com o túnel.

A configuração de tunelamento de uma sessão PPP para L2F é igual à configuração para L2TP.

Ela envolve:

1. Estabelecendo um túnel entre o NAS e o Home Gateway. Essa fase ocorre apenas quando não há túnel ativo entre os dois dispositivos.
2. Estabelecendo uma sessão entre o NAS e o Home Gateway.



O NAS decide que é necessário iniciar um túnel entre ele e o Home Gateway.

1. O NAS envia um L2F_Conf para o Gateway Local. Um desafio de CHAP foi incluído nesta mensagem.
2. O Gateway Local responde com um L2F_Conf. Um desafio de CHAP foi incluído nesta mensagem.
3. O NAS envia um L2F_Open. A resposta CHAP da desafio de Gateway Doméstico está inclusa nesta mensagem.
4. O Gateway Local responde com um L2F_Open. A resposta CHAP ao desafio NAS é incluída nessa mensagem. O túnel está ativado.
5. O NAS envia um L2F_Open ao Gateway Local. O pacote inclui o nome de usuário do cliente (nome_cliente), o desafio CHAP enviado pelo NAS ao cliente (desafio_NAS) e sua resposta (resposta_cliente).
6. O Home Gateway, ao enviar de volta o L2F_OPEN, aceita o cliente. O tráfego está agora livre para fluir em qualquer direção entre o cliente e o Gateway Local.

Observação: um túnel é identificado com um CLID (ID do cliente). O ID de multiplexação (MID, Multiplex ID) identifica uma conexão específica do túnel.

[Configurando o VPDN](#)

Para obter informações sobre a configuração de VPDN, consulte o manual [Configuração de Redes Privadas Virtuais](#) e veja a [seção sobre Configuração de VPN](#).

Informações Relacionadas

- [Páginas de suporte à tecnologia de discagem e acesso](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)