

# Configuração de VPDN de discagem usando grupos de VPDN e TACACS+

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Conventions](#)

[Informações de Apoio](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações](#)

[Verificar](#)

[Troubleshoot](#)

[Comandos para Troubleshooting](#)

[Informações Relacionadas](#)

## [Introduction](#)

Este documento fornece uma configuração de exemplo para VPDN (Virtual Private Dialup Networks) de discagem, usando grupos VPDN e TACACS+ (Terminal Access Controller Access Control System Plus).

## [Prerequisites](#)

### [Requirements](#)

Antes de tentar esta configuração, verifique se estes requisitos são atendidos:

Você precisa ter:

- Um roteador Cisco para acesso de cliente (NAS/LAC) e um roteador Cisco para acesso à rede (HGW/LNS) com conectividade IP entre eles.
- Nomes de host dos roteadores ou nomes locais a serem usados nos grupos de VPDN.
- O protocolo de tunelamento a ser usado. Pode ser o protocolo L2T (Layer 2 Tunneling, Encapsulamento de Camada 2) ou o protocolo L2F (Layer 2 Forwarding, Encaminhamento de Camada 2).
- Uma senha para que os roteadores autentiquem o túnel.
- Um critério de tunelamento. Esse pode ser o nome de domínio ou o DNIS (Serviço de

identificação de número discado).

- Nomes de usuário e senhas para o usuário (discagem do cliente).
- Endereços IP e chaves para os servidores TACACS+.

## Componentes Utilizados

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## Conventions

Para obter mais informações sobre convenções de documento, consulte as [Convenções de dicas técnicas Cisco](#).

## Informações de Apoio

Para obter uma introdução detalhada sobre redes de discagem privada virtual (VPDN) e grupos de VPDN, consulte [Entendendo a VPDN](#). Este documento é expandido na configuração do VPDN e adiciona o Terminal Access Controller Access Control System Plus (TACACS+).

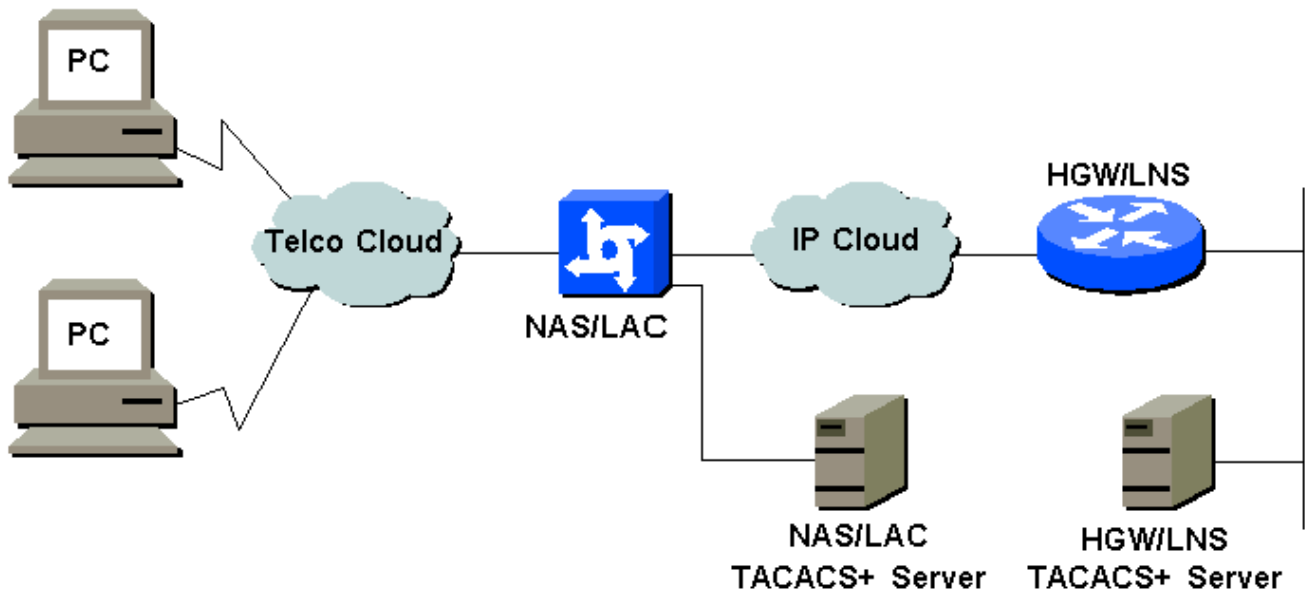
## Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

**Observação:** para encontrar informações adicionais sobre os comandos usados neste documento, use a [ferramenta Command Lookup Tool](#) (somente clientes [registrados](#)).

## Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



## Configurações

Este documento utiliza as seguintes configurações:

- NAS/LAC
- HGW/LNS
- Arquivo de configuração NAS/LAC TACACS+
- Arquivo de configuração TACACS+ HGW/LNS

### NAS/LAC

```

!
version 12.0
service timestamps debug datetime msec
service timestamps log datetime msec
!
hostname as5300
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authentication ppp default if-needed group tacacs+
aaa authorization network default group tacacs+
enable password somethingSecret
!
username john password 0 secret4me
!
ip subnet-zero
!
vpdn enable
!
isdn switch-type primary-5ess
!
controller T1 0
 framing esf
 clock source line primary
 linecode b8zs
 pri-group timeslots 1-24
!

```

```
controller T1 1
  framing esf
  clock source line secondary 1
  linecode b8zs
  pri-group timeslots 1-24
!
controller T1 2
  framing esf
  linecode b8zs
  pri-group timeslots 1-24
!
controller T1 3
  framing esf
  linecode b8zs
  pri-group timeslots 1-24
!
interface Ethernet0
  ip address 172.16.186.52 255.255.255.240
  no ip directed-broadcast
!
interface Serial023
  no ip address
  no ip directed-broadcast
  encapsulation ppp
  ip tcp header-compression passive
  dialer rotary-group 1
  isdn switch-type primary-5ess
  isdn incoming-voice modem
  no cdp enable
!
interface Serial123
  no ip address
  no ip directed-broadcast
  encapsulation ppp
  ip tcp header-compression passive
  dialer rotary-group 1
  isdn switch-type primary-5ess
  isdn incoming-voice modem
  no cdp enable
!
interface Serial223
  no ip address
  no ip directed-broadcast
  encapsulation ppp
  ip tcp header-compression passive
  dialer rotary-group 1
  isdn switch-type primary-5ess
  isdn incoming-voice modem
  no cdp enable
!
interface Serial323
  no ip address
  no ip directed-broadcast
  encapsulation ppp
  ip tcp header-compression passive
  dialer rotary-group 1
  isdn switch-type primary-5ess
  isdn incoming-voice modem
  no cdp enable
!
interface FastEthernet0
  no ip address
  no ip directed-broadcast
  shutdown
```

```
!  
interface Group-Async1  
  ip unnumbered Ethernet0  
  no ip directed-broadcast  
  encapsulation ppp  
  ip tcp header-compression passive  
  async mode interactive  
  peer default ip address pool IPAddressPool  
  no cdp enable  
  ppp authentication chap  
  group-range 1 96  
!  
interface Dialer1  
  ip unnumbered Ethernet0  
  no ip directed-broadcast  
  encapsulation ppp  
  ip tcp header-compression passive  
  dialer-group 1  
  peer default ip address pool IPAddressPool  
  no cdp enable  
  ppp authentication chap  
!  
ip local pool IPAddressPool 10.10.10.1 10.10.10.254  
no ip http server  
ip classless  
ip route 0.0.0.0 0.0.0.0 172.16.186.49  
!  
tacacs-server host 172.16.171.9  
tacacs-server key 2easy  
!  
line con 0  
  login authentication CONSOLE  
  transport input none  
line 1 96  
  autoselect during-login  
  autoselect ppp  
  modem Dialin  
line aux 0  
line vty 0 4  
!  
end
```

## HGW/LNS

```
!  
version 12.0  
service timestamps debug uptime  
service timestamps log uptime  
!  
hostname access-9  
!  
aaa new-model  
aaa authentication login default local  
aaa authentication login CONSOLE none  
aaa authentication ppp default if-needed group tacacs+  
aaa authorization network default group tacacs+  
enable password somethingSecret  
!  
ip subnet-zero  
!  
vpdn enable  
!
```

```
vpdn-group DEFAULT
! Default L2TP VPDN group
accept-dialin
  protocol any
  virtual-template 1
local name LNS
lcp renegotiation always
l2tp tunnel password 0 not2tell
!
vpdn-group POP1
accept-dialin
  protocol l2tp
  virtual-template 2
terminate-from hostname LAC
local name LNS
l2tp tunnel password 0 2secret
!
vpdn-group POP2
accept-dialin
  protocol l2f
  virtual-template 3
terminate-from hostname NAS
local name HGW
lcp renegotiation always
!
interface FastEthernet0/0
 ip address 172.16.186.1 255.255.255.240
 no ip directed-broadcast
!
interface Virtual-Template1
 ip unnumbered FastEthernet0/0
 no ip directed-broadcast
 ip tcp header-compression passive
 peer default ip address pool IPAddressPool
 ppp authentication chap
!
interface Virtual-Template2
 ip unnumbered Ethernet0/0
 no ip directed-broadcast
 ip tcp header-compression passive
 peer default ip address pool IPAddressPoolPOP1
 compress stac
 ppp authentication chap
!
interface Virtual-Template3
 ip unnumbered Ethernet0/0
 no ip directed-broadcast
 ip tcp header-compression passive
 peer default ip address pool IPAddressPoolPOP2
 ppp authentication pap
 ppp multilink
!
ip local pool IPAddressPool 10.10.10.1 10.10.10.254
ip local pool IPAddressPoolPOP1 10.1.1.1 10.1.1.254
ip local pool IPAddressPoolPOP2 10.1.2.1 10.1.2.254
ip classless
no ip http server
!
tacacs-server host 172.16.186.9
tacacs-server key not2difficult
!
line con 0

login authentication CONSOLE
```

```
transport input none
line 97 120
line aux 0
line vty 0 4
!
!
end
```

## Arquivo de configuração NAS/LAC TACACS+

```
key = 2easy

# Use L2TP tunnel to 172.16.186.1 when 4085555100 is
dialed
user = dnis:4085555100 {
    service = ppp protocol = vpdn {
        tunnel-id = anonymous
        ip-addresses = 172.16.186.1
        tunnel-type = l2tp
    }
}

# Password for tunnel authentication
user = anonymous {
    chap = cleartext not2tell
}

###

# Use L2TP tunnel to 172.16.186.1 when 4085555200 is
dialed
user = dnis:4085555200 {
    service = ppp protocol = vpdn {
        tunnel-id = LAC
        ip-addresses = 172.16.186.1
        tunnel-type = l2tp
    }
}

# Password for tunnel authentication
user = LAC {
    chap = cleartext 2secret
}

###

# Use L2F tunnel to 172.16.186.1 when user authenticates
with cisco.com domain
user = cisco.com {
    service = ppp protocol = vpdn {
        tunnel-id = NAS
        ip-addresses = 172.16.186.1
        tunnel-type = l2f
    }
}

# Password for tunnel authentication
user = NAS {
    chap = cleartext cisco
}

# Password for tunnel authentication
```

```
user = HGW {
    chap = cleartext cisco
}
```

## Arquivo de configuração TACACS+ HGW/LNS

```
key = not2difficult

# Password for tunnel authentication
user = NAS {
    chap = cleartext cisco
}

# Password for tunnel authentication
user = HGW {
    chap = cleartext cisco
}

user = santiago {
    chap = cleartext letmein

    service = ppp protocol = lcp { }
    service = ppp protocol = ip { }
}

user = santiago@cisco.com {
    global = cleartext letmein

    service = ppp protocol = lcp { }
    service = ppp protocol = multilink { }
    service = ppp protocol = ip { }
}
```

## Verificar

Esta seção fornece informações que você pode usar para confirmar se sua configuração está funcionando adequadamente.

A [Output Interpreter Tool \(somente clientes registrados\) oferece suporte a determinados comandos show](#), o que permite exibir uma análise da saída do comando show.

- **show vpdn tunnel all** — exibe detalhes de todos os túneis ativos.
- **show user** — exibe o nome do usuário conectado.
- **show interface virtual-access #**—permite verificar o status de uma interface virtual específica no HGW/LNS.

## Troubleshoot

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

## Comandos para Troubleshooting



**Observação:** antes de inserir o comando **debug**, consulte [Informações importantes sobre os comandos debug](#).

- **debug vpdn l2x-events** — exibe o diálogo entre NAS/LAC e HGW/LNS para criação de túneis ou sessões.
- **debug ppp authentication** — permite verificar se um cliente está passando a autenticação.
- **debug ppp negotiation** — permite verificar se um cliente está passando a negociação PPP. Você pode ver quais opções (como retorno de chamada, MLP e assim por diante) e quais protocolos (como IP, IPX e assim por diante) estão sendo negociados.
- **debug ppp error** — exibe erros de protocolo e estatísticas de erro, associados à negociação e à operação da conexão PPP.
- **debug vtemplate** — exibe a clonagem de interfaces de acesso virtual no HGW/LNS. Você pode ver quando a interface é criada (clonada do modelo virtual) no início da conexão de discagem e quando a interface é destruída quando a conexão é encerrada.
- **debug aaa authentication** — permite verificar se o usuário ou túnel está sendo autenticado pelo servidor de autenticação, autorização e contabilização (AAA).
- **debug aaa authorization** — permite verificar se o usuário está sendo autorizado pelo servidor AAA.
- **debug aaa per-user** — permite verificar o que é aplicado a cada usuário autenticado. Isso é diferente das depurações gerais listadas acima.

## [Informações Relacionadas](#)

- [Páginas de suporte de tecnologia - Discar](#)
- [Suporte Técnico - Cisco Systems](#)