

# Inbelconfiguratie met VPDN-groepen en TACACS+

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Conventies](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Netwerkdigram](#)

[Configuraties](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Opdrachten voor probleemoplossing](#)

[Gerelateerde informatie](#)

## [Inleiding](#)

Dit document biedt een voorbeeldconfiguratie voor inbel-Virtual Private Dialup Networks (VPDN), met gebruik van VPDN-groepen en Terminal Access Control System Plus (TACACS+).

## [Voorwaarden](#)

### [Vereisten](#)

Zorg er voordat u deze configuratie probeert voor dat u aan deze vereisten voldoet:

U moet beschikken over:

- Een Cisco-router voor clienttoegang (NAS/LAC) en een Cisco-router voor netwerktoegang (HGW/LNS) met IP-connectiviteit tussen deze routers.
- Host namen van de routers, of lokale namen die u in de VPDN-groepen wilt gebruiken.
- Het te gebruiken tunneling protocol. Dit kan een Layer 2 Tunneling (L2T)-protocol zijn of een Layer 2 Forwarding (L2F)-protocol.
- Een wachtwoord voor de routers om tunnels te authenticeren.
- Een tunneling-criterium. Dit kan de domeinnaam zijn, of de Dited Number Identification Service (DNIS).
- Gebruikersnaam en wachtwoorden voor de gebruiker (client inbellen).

- IP-adressen en -toetsen voor uw TACACS+-servers.

## Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

## Conventies

Raadpleeg voor meer informatie over documentconventies de [technische Tips](#) van [Cisco](#).

## Achtergrondinformatie

Zie [VPDN-begrip voor](#) een gedetailleerde inleiding tot Virtual Private Dialup Networks (VPDN's) [en](#) VPDN-groepen. Dit document breidt de VPDN-configuratie uit en voegt terminaal toegangscontrolesysteem voor controllers toe (TACACS+).

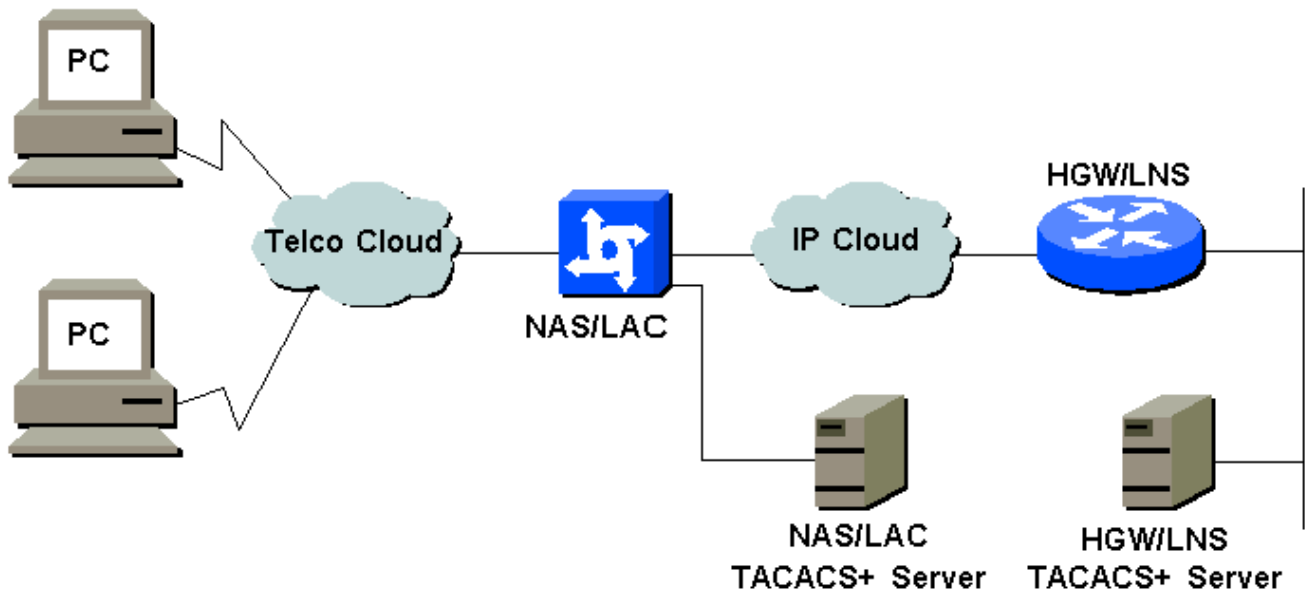
## Configureren

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

**N.B.:** Als u aanvullende informatie wilt vinden over de opdrachten in dit document, gebruikt u het [Opdrachtplanningprogramma](#) (alleen [geregistreerd](#) klanten).

## Netwerkdigram

Het netwerk in dit document is als volgt opgebouwd:



## Configuraties

Dit document gebruikt deze configuraties:

- NAS/LAC
- HGW/LNS
- NAS/LAC-bestand tegen TACACS+ configuratie
- HGW/LNS-bestand voor TACACS+ configuratie

### 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
```

## NAS/LAC-bestand tegen TACACS+ configuratie

```
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
}
```

## HGW/LNS-bestand voor TACACS+ configuratie

```
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 { }
}
```

## Verifiëren

Deze sectie verschaft informatie die u kunt gebruiken om te bevestigen dat uw configuratie correct werkt.

Bepaalde opdrachten met **show** worden ondersteund door de tool [Output Interpreter \(alleen voor geregistreerde klanten\)](#). Hiermee kunt u een analyse van de output van opdrachten met **show** genereren.

- **toon vpdn tunnel all**—toont details van alle actieve tunnels.
- **toon gebruiker**—geeft de naam weer van de aangesloten gebruiker.
- **laat de interface virtuele toegang zien #**—waardoor u de status van een bepaalde virtuele interface op de HGW/LNS kunt controleren.

## Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

## Opdrachten voor probleemoplossing



**Opmerking:** Voordat u **debug**-opdrachten afgeeft, raadpleegt u [Belangrijke informatie over Debug Commands](#).

- **debug vpdn l2x-gebeurtenissen**—geeft het dialoogvenster weer tussen NAS/LAC en HGW/LNS voor het maken van een tunnel of sessie.
- **debug van PPP-authenticatie** - stelt u in staat te controleren of een client authenticatie passeert.
- **debug PPP onderhandeling**-stelt u in staat om te controleren of een client PPP onderhandeling passeert. U kunt zien welke opties (zoals callback, MLP, enzovoort) en welke protocollen (zoals IP, IPX, enzovoort) worden onderhandeld.
- **debug van PPP**: toont protocol fouten en foutstatistieken, geassocieerd met PPP verbindingsonderhandeling en -handeling.
- **debug Vsjabloon**—geeft het klonen van virtuele access interfaces op de HGW/LNS weer. U kunt zien wanneer de interface wordt gemaakt (gekloond vanuit de virtuele sjabloon) aan het begin van de dialoogvensterverbinding, en wanneer de interface wordt vernietigd wanneer de verbinding wordt afgesloten.
- **debug a authenticatie** - stelt u in staat om te controleren of de gebruiker of tunnel geauthentiseerd wordt door de authenticatie, autorisatie en accounting (AAA) server.
- **debug a autorisatie** - stelt u in staat te controleren of de gebruiker is geautoriseerd op de AAA server.
- **debug a per-gebruiker** - stelt u in staat te controleren wat er op elke gebruiker wordt toegepast die echt is bevonden. Dit is niet hetzelfde als de hierboven genoemde algemene uitzettingen.

## [Gerelateerde informatie](#)

- [Pagina's voor technische ondersteuning - Dialoogvenster](#)
- [Technische ondersteuning - Cisco-systemen](#)