Shell-Based Authentication of VPDN Users

Contents

- Feature Overview, page 1
- Supported Platforms, page 6
- Supported Standards, MIBs, and RFCs, page 7
- Configuration Tasks, page 8
- Command Reference, page 34
- Glossary, page 36

Feature Overview

The Shell-Based Authentication of VPDN Users feature provides terminal services for VPDN users to support rollout of wholesale dial networks. Terminal services (shell login or exec login) on the network access server (NAS) provide the following capabilities:

- Enabling a dial-in user session to be terminated at the access server.

Feature History for Shell-Based Authentication of VPDN Users

<table>
<thead>
<tr>
<th>Release</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1(3)XL1</td>
<td>This feature was introduced on the Cisco AS5800 universal access server.</td>
</tr>
<tr>
<td>12.2(2)T</td>
<td>This feature was integrated into Cisco IOS Release 12.2(2)T and support was added for the Cisco 2600 series, Cisco 3600 series, and Cisco 7200 platforms.</td>
</tr>
<tr>
<td>12.2(8)T</td>
<td>Support was added for the Cisco 806, Cisco 828, Cisco 1710, Cisco SOHO 78, Cisco 3631, Cisco 3725, Cisco 3745, and Cisco URM for IGX8400 platforms.</td>
</tr>
<tr>
<td>12.2(11)T</td>
<td>Support was added for the Cisco AS5300 and Cisco AS5800 platforms.</td>
</tr>
<tr>
<td>12.2(27)SBA</td>
<td>This feature was integrated into Cisco IOS Release 12.2(27)SBA.</td>
</tr>
</tbody>
</table>
Feature Overview

- Authenticating the user with a character-mode login dialog such as username/password or username/challenge/password, Secure ID, Safeword, and so on.
- Initiating PPP and tunneling it to a home gateway (HGW).

With the terminal services, user authentication methods other than PAP and CHAP can be applied to PPP users. With the Shell-Based Authentication of VPDN Users feature, PPP authentication data is preconfigured or entered before PPP starts. Authentication is completed without any further input from the user.

Terminal services provided by Exec-VPDN add the following functionality:

- An enhancement to an existing AAA configuration command which enables a user to be authenticated at a remote network determined by the DNIS number. This enhancement supports login in addition to ppp:

  aaa dnis map dnis-number authentication { ppp | login } group name

  If a proxy AAA server is used by the NAS to authenticate an exec login, this command is not needed. Shell-based authentication then uses the DNIS or domain name to decide which AAA server should authenticate the user.

- The new feature supports L2F and L2TP without PPP user authentication.

Figure 1  Typical Network Setup for Shell-Based Exec-VPDN

Benefits

With this feature, clients dial in, are authenticated in character mode, start PPP, and are tunneled based on either DNIS or domain—this feature allows dial-up users to be authenticated in a character-mode connection and then be switched to PPP and tunneled to a remote home gateway.

A character-mode login dialog is provided before PPP starts, and the login dialog supports schemes such as token-card synchronization and initialization, challenge-based password, and so on. After a user is authenticated in this way, the connection changes from character mode to PPP mode to connect the user to the desired destination. The AAA server that authenticates the login user can be selected based on the dialed DNIS or the domain-name part of the user name.

VPDN profiles can be kept by a Resource Pool Manager Server (RPMS), RADIUS-based AAA server, or on the NAS.
Restrictions

- Per-user virtual profile on a HGW is not supported.
- Call back is not supported.
- Only those login schemes supported by the NAS exec-login features are supported.
- If VPDN fails to get established (for example, RPMS denies the session), the dial-up call is terminated. An exec-PPP session is not terminated locally on the NAS if the desired VPDN session fails to get established because the user was presumed authenticated by an AAA server at the remote enterprise.
- While an exec-VPDN HGW accepts a tunneled PPP session without authenticating the PPP clients, the tunnel itself must be mutually authenticated by both the NAS and the HGW. To further reduce security risks, a separate VPDN group with a distinct local name should be created on the HGW so that only the exec-VPDN sessions are accepted without authentication.

Order of Precedence

AAA is extremely flexible; each of the three definitions of AAA services can be configured on the same network access server simultaneously. Because all three definitions of AAA services can be configured simultaneously, Cisco has established an order of precedence to determine which server or groups of servers provide AAA services. The precedence is in the following order:

- Per DNIS—If you have configured the network access server to use DNIS to identify or determine which server group provides AAA services, then this method has the highest priority and takes precedence over any additional AAA selection method configured.
- Per interface—If you have configured the network access server per interface to use access lists to determine how a server provides AAA services, this method takes precedence over any global configuration AAA access lists you might have configured.
- Globally—If you have configured the network access server by using global AAA access lists to determine how the security server provides AAA services, this method has the lowest priority.
Figure 2  Event Sequence Illustration for Shell-Based Exec-VPDN

Table 1  Event Sequence Description Table for Shell-Based Exec-VPDN

<table>
<thead>
<tr>
<th>Step</th>
<th>Client</th>
<th>NAS</th>
<th>HGW</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Calls in character mode to an asynchronous interface on a NAS</td>
<td>—</td>
<td>—</td>
<td>To identify the AAA server to use on the HGW network, the line is configured with a DNIS for the dialed line, or a domain name.</td>
</tr>
<tr>
<td>2.</td>
<td>—</td>
<td>Consults with RPMS if configured, on number calls limit on the DNIS group and call type (async or V.120).</td>
<td>—</td>
<td>If no AAA server can be decided or the call type is not async/V.120, then the NAS takes the usual action as with non-exec VPDN cases.</td>
</tr>
<tr>
<td>3.</td>
<td>—</td>
<td>Accepts the call if RPMS is not configured or RPMS says OK; and starts a login terminal service for the line.</td>
<td>—</td>
<td>If RPMS denies the call, it gives the call an appropriate call treatment specified by the customer RPMS configuration.</td>
</tr>
</tbody>
</table>
### Feature Overview

<table>
<thead>
<tr>
<th>Step</th>
<th>Client</th>
<th>NAS</th>
<th>HGW</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.</td>
<td>—</td>
<td>Retrieves AAA server information for the DNIS or domain name.</td>
<td>—</td>
<td>For exec-VPDN, the AAA server is presumed to be at the HGW network. It is a misconfiguration if no RADIUS or TACACS+ server groups are defined for AAA authentication (for example, only “local” defined).</td>
</tr>
<tr>
<td>5.</td>
<td>Enters user ID, password, and so on, as prompted.</td>
<td>Acts as the AAA client to authenticate the login user, then prompts the user based on the NAS conversation with the AAA server.</td>
<td>The AAA server in the HGW network serves the AAA requests from the NAS.</td>
<td>A Cisco NAS supports extended SDI login dialog in conjunction with a AAA server, with retry handling. It is a misconfiguration if the AAA is not at the HGW network while the DNIS is mapped to the HGW.</td>
</tr>
<tr>
<td>6.</td>
<td>—</td>
<td>Drops the character mode connection, and switches to PPP mode. Flags the PPP session as “exec-PPP”.</td>
<td>—</td>
<td>The NAS configures “autocommand ppp” on the line interface. The NAS performs active PPP open, with user=the exec-login user ID and PPP authentication method=none.</td>
</tr>
<tr>
<td>7.</td>
<td>Enters PPP mode.</td>
<td>—</td>
<td>—</td>
<td>The client enters PPP mode either manually or automatically, passively or actively.</td>
</tr>
<tr>
<td>8.</td>
<td>LCP is UP, starts NCP negotiation.</td>
<td>LCP is UP. Tries to forward the PPP session.</td>
<td>—</td>
<td>With no PPP authentication, NCP starts immediately. The NAS must buffer the NCP packets.</td>
</tr>
<tr>
<td>9.</td>
<td>—</td>
<td>Finds VPDN information based on the DNIS or domain name if VPDN is enabled.</td>
<td>—</td>
<td>If not enabled or not found, the PPP terminates at the NAS. It is a misconfiguration if a DNIS is mapped to a remote AAA but without a corresponding VPDN configuration or “vpdn enabled”.</td>
</tr>
<tr>
<td>10.</td>
<td>—</td>
<td>Consults RPMS, if configured, on limits of the number of VPDN-sessions, MLP-bundles, and links-per-bundle.</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>11.</td>
<td>—</td>
<td>Starts DNIS or domain-based VPDN as triggered by the PPP, if RPMS is not configured or RPMS indicates connection is OK.</td>
<td>—</td>
<td>If RPMS denies the connection, the NAS tears down the exec-PPP connection (flagged as such by exec PPP), for instance, no local terminated PPP is allowed if exec PPP fails to tunnel because of resource pool limits.</td>
</tr>
<tr>
<td>12.</td>
<td>—</td>
<td>—</td>
<td>Accepts the VPDN session without authenticating the user again.</td>
<td>This is a normal VPDN session to the HGW with no PPP authentication negotiated.</td>
</tr>
</tbody>
</table>
Supported Platforms

13. — Forwards LCP proxy data to HGW.
14. Negotiates NCP with the HGW.

Negotiates NCP with the client. Normal course of a tunneled PPP session follows.

Related Documents

- *Cisco IOS Security Configuration Guide*; Cisco IOS Release 12.1
- *Cisco IOS Security Command Reference*; Cisco IOS Release 12.1
- *Cisco IOS Dial Services Command Reference*, Cisco IOS Release 12.1
- *Selecting AAA Servers Using DNIS Numbers* Cisco IOS Release 12.0(2)T feature module
- *AAA Server Groups* Cisco IOS Release 12.0(5)T feature module
- *Cisco AAA Implementation Case Study*

Supported Platforms

- Cisco 806
- Cisco 828
- Cisco SOHO 78
- Cisco 1710
- Cisco 2600 series
- Cisco 3600 series
- Cisco 3631
- Cisco 3725
- Cisco 3745
- Cisco AS5300
- Cisco AS5800
- Cisco 7200
- Cisco URM for IGX8400

**Table 2**  
*Cisco IOS Release and Platform Support for this Feature*

<table>
<thead>
<tr>
<th>Platform</th>
<th>12.1(3)XL1</th>
<th>12.2(2)T</th>
<th>12.2(8)T</th>
<th>12.2(11)T</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco 806</td>
<td>Not supported</td>
<td>Not supported</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Cisco 828</td>
<td>Not supported</td>
<td>Not supported</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Cisco SOHO 78</td>
<td>Not supported</td>
<td>Not supported</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Cisco 1710</td>
<td>Not supported</td>
<td>Not supported</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
Table 2  Cisco IOS Release and Platform Support for this Feature

<table>
<thead>
<tr>
<th>Platform</th>
<th>12.1(3)XL1</th>
<th>12.2(2)T</th>
<th>12.2(8)T</th>
<th>12.2(11)T</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco 2600 series</td>
<td>Not supported</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Cisco 3600 series</td>
<td>Not supported</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Cisco 3631</td>
<td>Not supported</td>
<td>Not supported</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Cisco 3725</td>
<td>Not supported</td>
<td>Not supported</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Cisco 3745</td>
<td>Not supported</td>
<td>Not supported</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Cisco AS5300</td>
<td>Not supported</td>
<td>Not supported</td>
<td>Not supported</td>
<td>X</td>
</tr>
<tr>
<td>Cisco AS5800</td>
<td>X</td>
<td>Not supported</td>
<td>Not supported</td>
<td>X</td>
</tr>
<tr>
<td>Cisco 7200</td>
<td>Not supported</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Cisco URM for IGX8400</td>
<td>Not supported</td>
<td>Not supported</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

Supported Standards, MIBs, and RFCs

**Standards**
No new or modified standards are supported by this feature.

**MIBs**
No new or modified MIBs are supported by this feature.
To obtain lists of MIBs supported by platform and Cisco IOS release and to download MIB modules, go to the Cisco MIB web site on Cisco Connection Online (CCO) at http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml.

**RFCs**
No new or modified RFCs are supported by this feature.

Prerequisites

This feature requires virtual private dialup network (VPDN), wide area networking (WAN), and authentication, authorization, and accounting (AAA) configurations to be set up before it is implemented. Resource Pool Manager Server (RPMS) configuration can also be used, if needed. Before you configure your NAS or HGW for AAA, you must configure the remote security servers associated with each AAA server group. Refer to the applicable documentation listed in the “Related Documents” section for these other configuration requirements.

If you are not familiar with basic as well as advanced VPDN, and the difference between legacy VPDN and this feature, refer to the applicable documents in the “Related Documents” section.

The exec-VPDN configuration consists of basic configurations of existing technologies:
- Normal user information configuration: local or AAA
- Normal AAA server configuration for login if a AAA server is used for login
- Normal dial-in access interface configuration (serial async, V.120)
- Normal (non-tunnel) PPP configuration with no PPP user authentication
- Normal AAA server configuration for PPP if AAA is used for PPP
- Normal configuration of `autocommand ppp` on the dial-in access interface to start PPP
- Normal VPDN configuration: local or in a AAA profile
- Proxy AAA configuration (for instance, GRS)
- `aaa dnis map` command (new)

**Note**
Verify that all of the separate components mentioned previously are operating correctly—by testing them individually—before implementing the Exec-VPDN feature.

---

**Configuration Tasks**

To use the `aaa dnis map authentication group` `aaa-server-group` configuration command, you must first enable AAA, define a AAA server group, and enable DNIS mapping.

The following sections provide the steps for configuring Exec-VPDN:

- **Configuring the Network Access Server to Support Exec-VPDN**
- **Configuring the Home Gateway Server**

### Configuring the Network Access Server to Support Exec-VPDN

#### Configuring the NAS for AAA

To configure the NAS for AAA, use the following commands, starting in global configuration mode:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong>&lt;br&gt;<code>Router(config)# aaa new-model</code></td>
<td>Enables the AAA access control model. In addition to starting the AAA access control system, this step immediately locks down login and PPP authentication.</td>
</tr>
<tr>
<td><strong>Step 2</strong>&lt;br&gt;<code>Router(config)# radius-server host ip-address auth-port auth-port-number acct-port acct-port-number</code></td>
<td>Specifies a list of AAA servers for the NAS to use. For exec VPDN, the list of server hosts is the list of remote AAA servers on the HGW network. They must be accessible to the NAS.</td>
</tr>
<tr>
<td><strong>Step 3</strong>&lt;br&gt;<code>Router(config)# aaa authentication login name group group-name</code></td>
<td>Configures a AAA for the login, if doing VPDN based on domain name without proxy AAA to the remote AAA on the HGW network.</td>
</tr>
</tbody>
</table>

The following example maps DNIS number 7777 to the RADIUS server group called ExecVPDN-Login-Servers. Server group ExecVPDN-Login-Servers will use RADIUS server 172.30.0.0 for authentication requests for users dialing in with DNIS 7777.

```bash
aaa new-model
radius-server host 172.30.0.0 auth-port 1645 key cisco1
```
aaa group server radius ExecVPDN-Login-Servers
  server 172.30.0.0
aaa dnis map enable
aaa dnis map 7777 authentication ppp group ExecVPDN-Login-Servers
aaa dnis map 7777 authentication login group ExecVPDN-Login-Servers

The AAA servers in the ExecVPDN-Login-Servers server group should reside in the home gateway network that the exec VPDN user intends to tunnel to.

  server 171.69.71.85
aaa authentication login ExecVPDN-Login group ExecVPDN-Login-Servers

line 1 8
!assuming all logins on lines 1-8 is to be authen’ed at 171.69.71.85
login authentication ExecVPDN-Login
autoselect during-login
autocommand ppp
modem InOut
transport input all
transport output none
stopbits 1
speed 115200

When a user logs in by typing client_guy@company1.com at the login prompt, the 171.69.71.85 server is consulted for the authentication. If the authentication succeeds, the autocommand starts PPP immediately without letting the user access the exec shell.

Configuring PPP to Skip User Authentication

To configure the PPP to skip user authentication, use the following command, starting in global configuration mode:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Configuration Tasks</td>
</tr>
<tr>
<td>Router(config)# aaa authentication ppp NAME if-needed</td>
<td>Configures PPP so that it skips user authentication if a user has been authenticated at the login prompt.</td>
</tr>
</tbody>
</table>

The following example uses the global RADIUS server definition list for PPP authentication if authentication is needed.

aaa authentication ppp ExecVPDN-ppp if-needed group radius
PPP config for line 1
int async 1
ip unnumbered e0
encap ppp
async mode interactive
ppp authentication pap ExecVPDN-ppp
Configuring DNIS for Locating a AAA Server

To configure DNIS for locating a AAA server, use the following commands, starting in global configuration mode:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1: <code>Router(config)# aaa dnis map enable</code></td>
<td>Enables DNIS mapping for locating a AAA server.</td>
</tr>
<tr>
<td>Step 2: <code>Router(config)# aaa dnis map dnis-number</code></td>
<td>Maps a Dialed Number Identification Services (DNIS) number to a particular authentication server group (this server group is used for AAA authentication).</td>
</tr>
</tbody>
</table>

The following example (Again, this configuration is directed to the AAA on the HGW network):

```
aaa group server radius eV-login-serv-dnis-1
   server 171.69.71.85
aaa authentication login eVpdn-login-dnis-1 group eVpdn-login-serv-dnis-1
aaa dnis map enable
aaa dnis map 3335555 authentication login group eVpdn-login-dnis-1
aaa dnis map 3335555 authentication ppp group eVpdn-login-dnis-1
```

Enabling VPDN

To enable VPDN, use the following command, starting in global configuration mode:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1: <code>Router(config)# vpdn enable</code></td>
<td>Enables VPDN.</td>
</tr>
</tbody>
</table>

Alternatively, a static **vpdn-group** configuration on the NAS can be defined, for instance:

```
vpdn-group 1
   request-dialin
   protocol l2tp
   domain company1.com
   initiate-to ip 10.0.3.155
   local name host1_no_authen
```

Both Layer 2 Forwarding Protocol (L2F) and Layer 2 Tunneling Protocol (L2TP) are supported. On the dial-up line interface, configure **autoselect during-login** to allow smooth login terminal services. On the dial-up line interface, configure **autocommand ppp**. This denies the PPP user access to the exec shell, but allows entry to (tunnelled) PPP.

The Resource Pool Manager Server (RPMS) can be optionally configured. Multilink PPP Protocol (MLP) can be optionally configured.
Configuring the Home Gateway Server

The HGW must be configured to accept a tunneled PPP session without authenticating the PPP client (this requirement conforms to the L2TP and L2F RFCs). To do this, use the following commands, starting in global configuration mode:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Router(config)# vpdn group number</td>
</tr>
<tr>
<td>Step 2</td>
<td>Router(config-vpdn)# l2tp tunnel authentication</td>
</tr>
<tr>
<td>Step 3</td>
<td>Router(config-vpdn)# local name name</td>
</tr>
<tr>
<td>Step 4</td>
<td>Router(config-vpdn)# l2tp password password</td>
</tr>
</tbody>
</table>

The following example shows no PPP authentication configured:

```
vpdn-group 1
  accept-dialin
  protocol l2tp
  virtual-template 1
  terminate-from hostname host1_no_authen
  l2tp tunnel authentication
  l2tp password no_authen_secret
  local name host2_no_authen

! interface Virtual-Template1
  ip unnumbered Ethernet0/0
  no keepalive
  ppp authorization no_author

!```

The following example shows PPP authentication enabled:

```
vpdn-group 2
  accept-dialin
  protocol l2tp
  virtual-template 2
  terminate-from hostname authen_on
  l2tp tunnel authentication
  l2tp password no_authen_secret
  local name host2_authen_on

! interface Virtual-Template1
  ip unnumbered Ethernet0/0
  no keepalive
  ppp authentication pap
```

Cisco IOS Release: Multiple releases (see the Feature History table)
Verifying Shell-Based Authentication

To verify that a user can log in and get either an L2TP or L2F tunnel established and to see who is connected, use the `show users` command.

To see the L2F tunnels and to verify that the number of L2X tunnels and sessions are correctly used, the `show vpdn` command.

NAS Configuration

The following example shows a NAS configuration for a Cisco AS5300 domain-based exec-VPDN asynchronous call with L2X and RADIUS AAA:

```
st-5300-c2#sh run
Building configuration...

Current configuration:
!
version 12.1
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname st-5300-c2
!
no logging buffered
aaa new-model
aaa group server radius Exec-VPDN-Login-Servers
    server 171.69.69.72 auth-port 1645 acct-port 1646
!
aaa authentication login Exec-VPDN-login group Exec-VPDN-Login-Servers
aaa authentication ppp Exec-VPDN-ppp if-needed group Exec-VPDN-Login-Servers
aaa authorization network default group Exec-VPDN-Login-Servers
enable password lab
!
!<snip>
!
spe 1/0 1/7
    firmware location system:/ucode/mica_port_firmware
    resource-pool disable
!
ip subnet-zero
ip ftp source-interface Ethernet0
ip ftp username root
ip ftp password lab
no ip domain-lookup
!
vpdn enable
no vpdn logging
vpdn search-order domain
!
isdn switch-type primary-5ess
cns event-service server

mta receive maximum-recipients 0
!
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
clock source line secondary 2
linecode b8zs
pri-group timeslots 1-24
!
controller T1 3
framing esf
clock source line secondary 3
linecode b8zs
pri-group timeslots 1-24
!
controller T1 4
framing esf
clock source line secondary 4
linecode b8zs
pri-group timeslots 1-24
!
controller T1 5
framing esf
clock source line secondary 5
linecode b8zs
pri-group timeslots 1-24
!
controller T1 6
framing esf
clock source line secondary 6
linecode b8zs
pri-group timeslots 1-24
!
controller T1 7
framing esf
clock source line secondary 7
linecode b8zs
pri-group timeslots 1-24
!
interface Loopback0
ip address 1.1.1.1 255.255.255.0
!
interface Ethernet0
ip address 1.1.2.1 255.255.255.0
no ip route-cache
no ip mroute-cache
no cdp enable
!
interface Virtual-Template1
no ip address
!
interface Virtual-Template5
no ip address
!
interface Serial0
no ip address
shutdown
no fair-queue
clockrate 2015232
no cdp enable
!
interface Serial1
no ip address
shutdown
no fair-queue
clockrate 2015232
no cdp enable
!
interface Serial2
no ip address
shutdown
no fair-queue
clockrate 2015232
no cdp enable
!
interface Serial3
no ip address
shutdown
no fair-queue
clockrate 2015232
no cdp enable
!
interface Serial0:23
ip unnumbered Ethernet0
encapsulation ppp
ip mroute-cache
isdn switch-type primary-5ess
isdn incoming-voice modem
no peer default ip address
no fair-queue
no cdp enable
ppp authentication pap Exec-VPDN-ppp
ppp authorization no_author
ppp multilink
!
interface Serial1:23
no ip address
encapsulation ppp
ip mroute-cache
isdn switch-type primary-5ess
isdn incoming-voice modem
no peer default ip address
no fair-queue
no cdp enable
!
interface Serial2:23
no ip address
encapsulation ppp
ip mroute-cache
isdn switch-type primary-5ess
isdn incoming-voice modem
no peer default ip address
no fair-queue
no cdp enable
!
interface Serial3:23
no ip address
encapsulation ppp
ip mroute-cache
isdn switch-type primary-5ess
isdn incoming-voice modem
no peer default ip address
no fair-queue
no cdp enable
!
interface Serial4:23
no ip address
encapsulation ppp
ip mroute-cache
dialer-group 1
isdn switch-type primary-5ess
isdn incoming-voice modem
no peer default ip address
no fair-queue
no cdp enable
!
interface Serial5:23
no ip address
encapsulation ppp
ip mroute-cache
dialer-group 1
isdn switch-type primary-5ess
isdn incoming-voice modem
no peer default ip address
no fair-queue
no cdp enable
!
interface Serial6:23
no ip address
encapsulation ppp
ip mroute-cache
dialer-group 1
isdn switch-type primary-5ess
isdn incoming-voice modem
no peer default ip address
no fair-queue
no cdp enable
!
interface Serial7:23
no ip address
encapsulation ppp
ip mroute-cache
dialer-group 1
isdn switch-type primary-5ess
isdn incoming-voice modem
no peer default ip address
no fair-queue
no cdp enable
!
interface FastEthernet0
no ip address
no ip route-cache
no ip mroute-cache
no keepalive
shutdown
duplex auto
speed auto
no cdp enable
!
interface Group-Async1
ip unnumbered Ethernet0
encapsulation ppp
async mode interactive
no peer default ip address
no fair-queue
ppp authentication pap Exec-VPDN-ppp
ppp authorization no_author
ppp multilink
group-range 1 48
!
interface Dialer1
ip unnumbered Loopback0
capsulation ppp
no ip route-cache
do ip mroute-cache
dialer in-band
dialer idle-timeout 2147483
dialer-group 1
peer default ip address pool default
no fair-queue
no cdp enable
ppp authentication pap Exec-VPDN-ppp
ppp authorization no_author
ppp multilink
!
interface Dialer13
ip address 8.8.10.8 255.255.255.0
capsulation ppp
no ip route-cache
do ip mroute-cache
dialer remote-name useless_remote13
dialer pool 2
dialer idle-timeout 2147483
dialer string 4085211002
dialer load-threshold 1 either
dialer max-call 4096
dialer-group 2
pulse-time 0
no cdp enable
ppp chap hostname user1@hoki10.com
ppp chap password 7 09404F0B
ppp multilink
ppp timeout multilink link add 3
!
interface Dialer25
ip address 8.8.11.8 255.255.255.0
capsulation ppp
no ip route-cache
do ip mroute-cache
dialer remote-name useless_remote25
dialer pool 3
dialer idle-timeout 2147483
dialer string 4085211003
dialer load-threshold 1 either
dialer max-call 4096
dialer-group 2
pulse-time 0
no cdp enable
ppp chap hostname user1@hoki11.com
ppp chap password 7 020A0559
ppp multilink
ppp timeout multilink link add 3
!
interface Dialer37
ip address 8.8.12.8 255.255.255.0
capsulation ppp
no ip route-cache
do ip mroute-cache
dialer remote-name useless_remote37
dialer pool 4
dialer idle-timeout 2147483
  dialer string 4085211004
  dialer load-threshold 1 either
  dialer max-call 4096
  dialer-group 2
  no cdp enable
  ppp chap hostname user1@hoki12.com
  ppp chap password 7 03085A09
  ppp multilink
  ppp timeout multilink link add 3

interface Dialer49
  ip address 8.8.13.8 255.255.255.0
  encapsulation ppp
  no ip route-cache
  no ip mrout-cache
  dialer remote-name useless_remote49
  dialer pool 5
  dialer idle-timeout 2147483
  dialer string 4085211101
  dialer load-threshold 1 either
  dialer max-call 4096
  dialer-group 2
  no cdp enable
  ppp chap hostname user1@hoki13.com
  ppp chap password 7 0703204E
  ppp multilink
  ppp timeout multilink link add 3

interface Dialer61
  ip address 8.8.14.8 255.255.255.0
  encapsulation ppp
  no ip route-cache
  no ip mrout-cache
  dialer remote-name useless_remote61
  dialer pool 6
  dialer idle-timeout 2147483
  dialer string 4085211102
  dialer load-threshold 1 either
  dialer max-call 4096
  dialer-group 2
  no cdp enable
  ppp chap hostname user1@hoki14.com
  ppp chap password 7 11051807
  ppp multilink
  ppp timeout multilink link add 3

interface Dialer73
  ip address 8.8.15.8 255.255.255.0
  encapsulation ppp
  no ip route-cache
  no ip mrout-cache
  dialer remote-name useless_remote73
  dialer pool 7
  dialer idle-timeout 2147483
  dialer string 4085211103
  dialer load-threshold 1 either
  dialer max-call 4096
  dialer-group 2
  no cdp enable
  ppp chap hostname user1@hoki15.com
  ppp chap password 7 00081204
  ppp multilink
  ppp timeout multilink link add 3
Configuration for a Cisco 3640 HGW

```
 Configuration for a Cisco 3640 HGW

st-3640-n3#show running
Building configuration...
```
Current configuration:
!
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname st-3640-n3
!
no logging buffered
enable password <snip>
!
<snip>
!
ip subnet-zero
ip ftp source-interface FastEthernet3/0
ip ftp username root
ip ftp password lab
ip domain-list nlab.cisco.com
ip domain-list cisco.com
ip domain-list .
ip domain-name cisco.com
ip name-server 172.21.200.3
ip name-server 171.69.2.133
ip name-server 198.92.30.32
!
vpdn enable
no vpdn logging
!
vpdn-group 1
accept-dialin
protocol l2tp
virtual-template 1
terminate-from hostname nas
local name hgw
l2tp tunnel password 7 14191D340D113E2321260C262710151317
!
vpdn-group 2
accept-dialin
protocol l2tp
virtual-template 2
terminate-from hostname nas1
local name hgw
l2tp tunnel password 7 151C0433053F3F2C2D3D0A311604040615
!
vpdn-group 3
accept-dialin
protocol l2tp
virtual-template 3
terminate-from hostname nas2
local name hgw
l2tp tunnel password 7 045504390E3458460C173A0417081E013E
!
isdn switch-type primary-5ess
cns event-service server
!
controller T1 1/0
framing esf
linecode b8zs
pri-group timeslots 1-24
!
controller T1 1/1
framing esf
linecode b8zs
Configuration Tasks

```
pri-group timeslots 1-24
!
interface Loopback0
  ip address 2.2.2.2 255.255.255.0
!
interface Ethernet0/0
  no ip address
  shutdown
!
interface Ethernet0/1
  no ip address
  shutdown
!
interface Ethernet0/2
  no ip address
  shutdown
!
interface Ethernet0/3
  no ip address
  shutdown
!
interface Serial1/0:23
  no ip address
  ip mroute-cache
  isdn switch-type primary-5ess
  fair-queue 64 256 0
  no cdp enable
!
interface Serial1/1:23
  no ip address
  ip mroute-cache
  isdn switch-type primary-5ess
  fair-queue 64 256 0
  no cdp enable
!
interface BRI2/0
  ip address 10.1.1.1 255.255.255.0
  dialer string 4085210801
  dialer-group 1
  isdn switch-type basic-5ess
!
interface BRI2/1
  ip address 100.1.1.1 255.255.255.0
  dialer string 4085210801
  dialer-group 1
  isdn switch-type basic-ni
!
interface BRI2/2
  no ip address
  shutdown
  isdn switch-type basic-ni
!
interface BRI2/3
  no ip address
  shutdown
  isdn switch-type basic-ni
!
interface BRI2/4
  no ip address
  shutdown
  isdn switch-type basic-ni
!
interface BRI2/5
  no ip address
```
shutdown
isdn switch-type basic-ni
!
interface BRI2/6
no ip address
shutdown
isdn switch-type basic-ni
!
interface BRI2/7
no ip address
shutdown
isdn switch-type basic-ni
!
interface FastEthernet3/0
ip address 1.1.2.2 255.255.255.0
no keepalive
duplex auto
speed auto
!
interface Virtual-Template1
ip unnumbered FastEthernet3/0
ip mroute-cache
no keepalive
peer default ip address pool default
ppp authorization no_author
ppp multilink
!
interface Virtual-Template2
ip unnumbered FastEthernet3/0
ip mroute-cache
no keepalive
peer default ip address pool default
ppp authorization no_author
ppp multilink
!
interface Virtual-Template3
ip unnumbered FastEthernet3/0
ip mroute-cache
no keepalive
peer default ip address pool default
ppp authorization no_author
ppp multilink
!
interface Virtual-Template5
ip unnumbered Ethernet0/0
ip mroute-cache
no keepalive
peer default ip address pool default
ppp authentication chap
!
interface Group-Async1
physical-layer async
no ip address
!
interface Dialer1
do ip address
dialer in-band
dialer idle-timeout 5
dialer wait-for-carrier-time 5
dialer hold-queue 5
dialer-group 1
no cdp enable
!
interface Dialer2
no ip address
encapsulation ppp
dialer remote-name router
dialer pool 2
dialer idle-timeout 5
dialer wait-for-carrier-time 5
dialer string 5551212
dialer hold-queue 5
dialer max-call 3

ip local pool default 50.0.0.1 50.0.0.10
ip default-gateway 1.1.2.254
ip nat translation timeout never
ip nat translation tcp-timeout never
ip nat translation udp-timeout never
ip nat translation finrst-timeout never
ip nat translation syn-timeout never
ip nat translation dns-timeout never
ip nat translation icmp-timeout never
ip classless
ip route 0.0.0.0 0.0.0.0 1.1.2.254
ip route 10.1.4.2 255.255.255.255 10.1.2.254
ip route 171.69.0.0 255.255.0.0 1.1.2.254
ip route 172.21.0.0 255.255.0.0 1.1.2.254
no ip http server

dialer-list 1 protocol ip permit
terminal-queue entry-retry-interval 124

!!
line con 0
  exec-timeout 0 0
  transport input none
line aux 0
line vty 0 4
  exec-timeout 0 0
  password cisco
!
end

st-3640-n3#

NAS Configuration

Sample configuration on the NAS for a DNIS-based exec-VPDN asynchronous call using RADIUS AAA:

st-5300-c2#sh run
Building configuration...

Current configuration:
!
version 12.1
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname st-5300-c2
!
no logging buffered
aaa new-model
aaa group server radius Exec-VPDN-Login-Servers
  server 171.69.71.85 auth-port 1645 acct-port 1646
!
aaa authentication login Exec-VPDN-login group Exec-VPDN-Login-Servers
aaa authentication ppp Exec-VPDN-ppp if-needed group Exec-VPDN-Login-Servers
aaa authorization network default group Exec-VPDN-Login-Servers
aaa authorization network no_author none
aaa dns map enable

aaa dnis map 56114 authentication login group Exec-VPDN-Login-Servers
  enable password <snip>
!
<snip>
!
spe 1/0 1/7
  firmware location system:/ucode/mica_port_firmware
!
resource-pool disable
!
ip subnet-zero
ip ftp source-interface Ethernet0
ip ftp username root
ip ftp password lab
no ip domain-lookup
!
vpdn enable
no vpdn logging
!
isdn switch-type primary-5ess
cns event-service server
!
mta receive maximum-recipients 0
!
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
  clock source line secondary 2
  linecode b8zs
  pri-group timeslots 1-24
!
controller T1 3
  framing esf
  clock source line secondary 3
  linecode b8zs
  pri-group timeslots 1-24
!
controller T1 4
  framing esf
  clock source line secondary 4
  linecode b8zs
  pri-group timeslots 1-24
!
controller T1 5
  framing esf
clock source line secondary 5
linecode b8zs
pri-group timeslots 1-24
!
controller T1 6
framing esf
clock source line secondary 6
linecode b8zs
pri-group timeslots 1-24
!
controller T1 7
framing esf
clock source line secondary 7
linecode b8zs
pri-group timeslots 1-24
!
interface Loopback0
ip address 1.1.1.1 255.255.255.0
!
interface Ethernet0
ip address 1.1.2.1 255.255.255.0
no ip route-cache
no ip mroute-cache
no cdp enable
!
interface Virtual-Template1
no ip address
!
interface Virtual-Template5
no ip address
!
interface Serial0
no ip address
shutdown
no fair-queue
clockrate 2015232
no cdp enable
!
interface Serial1
no ip address
shutdown
no fair-queue
clockrate 2015232
no cdp enable
!
interface Serial2
no ip address
shutdown
no fair-queue
clockrate 2015232
no cdp enable
!
interface Serial3
no ip address
shutdown
no fair-queue
clockrate 2015232
no cdp enable
!
interface Serial0:23
ip unnumbered Ethernet0
encapsulation ppp
ip mroute-cache
isdn switch-type primary-5ess
isdn incoming-voice modem
no peer default ip address
no fair-queue
no cdp enable
ppp authentication pap Exec-VPDN-ppp
ppp authorization no_author
hold-queue 20 in
hold-queue 20 out
!
interface Serial1:23
no ip address
encapsulation ppp
ip mroute-cache
isdn switch-type primary-5ess
isdn incoming-voice modem
no peer default ip address
no fair-queue
no cdp enable
!
interface Serial2:23
no ip address
encapsulation ppp
ip mroute-cache
isdn switch-type primary-5ess
isdn incoming-voice modem
no peer default ip address
no fair-queue
no cdp enable
!
interface Serial3:23
no ip address
encapsulation ppp
ip mroute-cache
isdn switch-type primary-5ess
isdn incoming-voice modem
no peer default ip address
no fair-queue
no cdp enable
!
interface Serial4:23
no ip address
encapsulation ppp
ip mroute-cache
dialer-group 1
dialer-group 1
isdn switch-type primary-5ess
isdn incoming-voice modem
no peer default ip address
no fair-queue
no cdp enable
!
interface Serial5:23
no ip address
encapsulation ppp
ip mroute-cache
dialer-group 1
dialer-group 1
isdn switch-type primary-5ess
isdn incoming-voice modem
no peer default ip address
no fair-queue
no cdp enable
!
interface Serial6:23
no ip address
encapsulation ppp
ip mroute-cache
dialer-group 1
isdn switch-type primary-5ess
isdn incoming-voice modem
no peer default ip address
no fair-queue
no cdp enable
!
interface Serial7:23
no ip address
encapsulation ppp
ip mroute-cache
dialer-group 1
isdn switch-type primary-5ess
isdn incoming-voice modem
no peer default ip address
no fair-queue
no cdp enable
!
interface FastEthernet0
no ip address
no ip route-cache
no ip mroute-cache
no keepalive
shutdown
duplex auto
speed auto
no cdp enable
!
interface Group-Async1
ip unnumbered Ethernet0
encapsulation ppp
async mode interactive
no peer default ip address
no fair-queue
ppp authentication pap Exec-VPDN-ppp
ppp authorization no_author
group-range 1 48
hold-queue 20 in
hold-queue 20 out
!
interface Dialer1
ip unnumbered Loopback0
encapsulation ppp
no ip route-cache
no ip mroute-cache
dialer in-band
dialer idle-timeout 2147483
dialer-group 1
peer default ip address pool default
no fair-queue
no cdp enable
ppp authentication pap Exec-VPDN-ppp
ppp authorization no_author
ppp multilink
!
interface Dialer13
ip address 8.8.10.8 255.255.255.0
encapsulation ppp
no ip route-cache
no ip mroute-cache
dialer remote-name useless_remote13
dialer pool 2
dialer idle-timeout 2147483
dialer string 4085211002
dialer load-threshold 1 either
dialer max-call 4096
dialer-group 2
pulse-time 0
no cdp enable
ppp chap hostname user1@hoki10.com
ppp chap password 7 09404F0B
ppp multilink
ppp timeout multilink link add 3
!
interface Dialer25
ip address 8.8.11.8 255.255.255.0
encapsulation ppp
no ip route-cache
dialer remote-name useless_remote25
dialer pool 3
dialer idle-timeout 2147483
dialer string 4085211003
dialer load-threshold 1 either
dialer max-call 4096
dialer-group 2
pulse-time 0
no cdp enable
ppp chap hostname user1@hoki11.com
ppp chap password 7 020A0559
ppp multilink
ppp timeout multilink link add 3
!
interface Dialer37
ip address 8.8.12.8 255.255.255.0
encapsulation ppp
no ip route-cache
dialer remote-name useless_remote37
dialer pool 4
dialer idle-timeout 2147483
dialer string 4085211004
dialer load-threshold 1 either
dialer max-call 4096
dialer-group 2
no cdp enable
ppp chap hostname user1@hoki12.com
ppp chap password 7 03085A09
ppp multilink
ppp timeout multilink link add 3
!
interface Dialer49
ip address 8.8.13.8 255.255.255.0
encapsulation ppp
no ip route-cache
dialer remote-name useless_remote49
dialer pool 5
dialer idle-timeout 2147483
dialer string 4085211101
dialer load-threshold 1 either
dialer max-call 4096
dialer-group 2
no cdp enable
ppp chap hostname user1@hoki13.com
ppp chap password 7 0703204E
ppp multilink
ppp timeout multilink link add 3
!
interface Dialer61
ip address 8.8.14.8 255.255.255.0
capsulation ppp
no ip route-cache
no ip mroute-cache
dialer remote-name useless_remote61
dialer pool 6
dialer idle-timeout 2147483
dialer string 4085211102
dialer load-threshold 1 either
dialer max-call 4096
dialer-group 2
no cdp enable
ppp chap hostname user1@hoki14.com
ppp chap password 7 11051807
ppp multilink
ppp timeout multilink link add 3
!
interface Dialer73
ip address 8.8.15.8 255.255.255.0
capsulation ppp
no ip route-cache
no ip mroute-cache
dialer remote-name useless_remote73
dialer pool 7
dialer idle-timeout 2147483
dialer string 4085211103
dialer load-threshold 1 either
dialer max-call 4096
dialer-group 2
no cdp enable
ppp chap hostname user1@hoki15.com
ppp chap password 7 00081204
ppp multilink
ppp timeout multilink link add 3
!
interface Dialer85
ip address 8.8.16.8 255.255.255.0
capsulation ppp
no ip route-cache
no ip mroute-cache
dialer remote-name useless_remote85
dialer pool 8
dialer idle-timeout 2147483
dialer string 4085211104
dialer load-threshold 1 either
dialer max-call 4096
dialer-group 2
no cdp enable
ppp chap hostname user1@hoki16.com
ppp chap password 7 03085A09
ppp multilink
ppp timeout multilink link add 3
!
ip local pool default 50.0.0.1 50.0.0.10
ip default-gateway 1.1.2.254
ip classless
ip route 0.0.0.0 0.0.0.0 1.1.2.254
ip route 171.69.0.0 255.255.0.0 1.1.2.254
ip route 172.21.0.0 255.255.0.0 1.1.2.254
no ip http server
!
dialer-list 1 protocol ip permit
dialer-list 2 protocol ip permit
no cdp run

radius-server host 171.69.71.85 auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server key cisco

line con 0
  exec-timeout 0 0
  transport input none
line 1 48
  exec-timeout 0 0
  autoselect during-login
  login authentication Exec-VPDN-login
  modem InOut
  autocommand ppp
  transport input all
  transport output lat pad mop telnet rlogin udlptn v120 lapb-ta nasi
line aux 0
line vty 0 4
  exec-timeout 0 0
  password cisco
  login authentication Exec-VPDN-login

! scheduler interval 1000
end

HGW Configuration

On HGW:
st-3640-n3#sh run
Building configuration...

Current configuration:
!
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hosname st-3640-n3
!
no logging buffered
aaa new-model
aaa group server radius Exec-VPDN-Login-Servers
  server 171.69.71.85 auth-port 1645 acct-port 1646
!
aaa authentication login Exec-VPDN-login group Exec-VPDN-Login-Servers
aaa authentication ppp Exec-VPDN-ppp if-needed group radius
aaa authentication ppp Exec-VPDN-login if-needed
aaa authorization network default group radius
aaa authorization network no_author none
enable password <snip>
!
! ip subnet-zero
ip ftp source-interface FastEthernet3/0
ip ftp username root
ip ftp password lab

Cisco IOS Release: Multiple releases (see the Feature History table)
ip domain-list nlab.cisco.com
ip domain-list cisco.com
ip domain-list .
ip domain-name cisco.com
ip name-server 172.21.200.3
ip name-server 171.69.2.133
ip name-server 198.92.30.32
!
vpdn enable
no vpdn logging
!
vpdn-group 1
  accept-dialin
  protocol l2tp
  virtual-template 1
  terminate-from hostname nas
  local name hgw
!
isdn switch-type primary-5ess
cns event-service server
!
controller T1 1/0
  framing esf
  linecode b8zs
  pri-group timeslots 1-24
!
controller T1 1/1
  framing esf
  linecode b8zs
  pri-group timeslots 1-24
!
interface Loopback0
  ip address 2.2.2.2 255.255.255.0
!
interface Ethernet0/0
  no ip address
  shutdown
!
interface Ethernet0/1
  no ip address
  shutdown
!
interface Ethernet0/2
  no ip address
  shutdown
!
interface Ethernet0/3
  no ip address
  shutdown
!
interface Serial 1/0:23
  no ip address
  ip mroute-cache
  isdn switch-type primary-5ess
  fair-queue 64 256 0
  no cdp enable
!
interface Serial 1/1:23
  no ip address
  ip mroute-cache
  isdn switch-type primary-5ess
  fair-queue 64 256 0
  no cdp enable
!
interface BRI2/0
  ip address 10.1.1.1 255.255.255.0
dialer string 4085210801
dialer-group 1
  isdn switch-type basic-5ess
!
interface BRI2/1
  ip address 100.1.1.1 255.255.255.0
dialer string 4085210801
dialer-group 1
  isdn switch-type basic-ni
!
interface BRI2/2
  no ip address
  shutdown
  isdn switch-type basic-ni
!
interface BRI2/3
  no ip address
  shutdown
  isdn switch-type basic-ni
!
interface BRI2/4
  no ip address
  shutdown
  isdn switch-type basic-ni
!
interface BRI2/5
  no ip address
  shutdown
  isdn switch-type basic-ni
!
interface BRI2/6
  no ip address
  shutdown
  isdn switch-type basic-ni
!
interface BRI2/7
  no ip address
  shutdown
  isdn switch-type basic-ni
!
interface FastEthernet3/0
  ip address 1.1.2.2 255.255.255.0
  no keepalive
duplex auto
speed auto
!
interface Virtual-Template1
  ip unnumbered FastEthernet3/0
  ip mroute-cache
  no keepalive
  peer default ip address pool default
  ppp authorization no_author
!
interface Virtual-Template2
  ip unnumbered FastEthernet3/0
  ip mroute-cache
  no keepalive
  peer default ip address pool default
  ppp authorization no_author
!
interface Virtual-Template3
  ip unnumbered FastEthernet3/0
ip mroute-cache
no keepalive
peer default ip address pool default
ppp authorization no_author
!
interface Virtual-Template5
ip unnumbered Ethernet0/0
ip mroute-cache
no keepalive
peer default ip address pool default
ppp authentication chap
!
interface Group-Async1
physical-layer async
no ip address
!
interface Dialer1
no ip address
dialer in-band
dialer idle-timeout 5
dialer wait-for-carrier-time 5
dialer hold-queue 5
dialer-group 1
no cdp enable
!
interface Dialer2
no ip address
encapsulation ppp
dialer remote-name router
dialer pool 2
dialer idle-timeout 5
dialer wait-for-carrier-time 5
dialer string 5551212
dialer hold-queue 5
dialer max-call 3
!
ip local pool default 50.0.0.1 50.0.0.254
ip default-gateway 1.1.2.254
ip nat translation timeout never
ip nat translation tcp-timeout never
ip nat translation udp-timeout never
ip nat translation finrst-timeout never
ip nat translation syn-timeout never
ip nat translation dns-timeout never
ip nat translation icmp-timeout never
ip classless
ip route 0.0.0.0 0.0.0.0 1.1.2.254
ip route 10.1.4.2 255.255.255.255 10.1.2.254
ip route 171.69.0.0 255.255.0.0 1.1.2.254
ip route 172.21.0.0 255.255.0.0 1.1.2.254
no ip http server
!
dialer-list 1 protocol ip permit
terminal-queue entry-retry-interval 124
!
radius-server host 171.69.71.85 auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server key cisco
!
line con 0
exec-timeout 0 0
transport input none
line aux 0
line vty 0 4
exec-timeout 0 0
password cisco
!
end

st-3640-n3#

Troubleshooting Tips

- If a DNIS is mapped to a AAA server (for example, a `dnis map` command is used instead of the proxy AAA). The DNIS should also be mapped to a corresponding HGW in the VPDN configuration.

- The AAA server and the HGW, both of which can be mapped to by either a DNIS or domain name, must belong to the same enterprise and must be accessible to the NAS.

- No “local” clause should be used in the command.

```
aaa authentication login default group group-name
```

This prevents an end user from being locally authenticated and then tunneling to a remote HGW.

- The AAA server group mapped to by the DNIS is intended to authenticate users to be connected to the HGW network, and thus must not be used for authenticating local users.

- The `ppp dnis` command must not be used on the Exec-VPDN dial-up interface.

- For increased security, configuring IPSec for L2TP/L2F is recommended. See the Cisco IOS Security Configuration Guide for more information.

To ensure that the AAA parameters are correct, turn on debugging for AAA servers as listed below:

- `debug resource-pool`—To view resource pool management parameters.

- `debug aaa authentication`—To display information on AAA/Terminal Access Controller Access Control System Plus (TACACS+) authentication such as what methods of authentication are being used and what the results of these methods are.

- `debug aaa authorization`—To display information on AAA/TACACS+ authorization such as what methods of authorization are being used and what the results of these methods are.

- `debug radius`—To display information associated with the Remote Authentication Dial-In User Server (RADIUS).

- `debug modem`—To observe modem line activity on an access server.

- `debug modem csm`—To view Call Switching Module (CSM) activity and to troubleshoot call switching problems by tracing the complete sequence of switching incoming and outgoing calls. The CSM connects calls on the modem.

- `debug dialer event`—To display debugging information about the packets received on a dialer interface.

- `debug isdn event`—To display Integrated Services Digital Network (ISDN) events occurring on the user side (on the router) of the ISDN interface. The ISDN events that can be displayed are Q.931 events (call setup and teardown of ISDN network connections).

- `debug isdn q931`—To display information about call setup and teardown of ISDN network connections (layer 3) between the local router (user side) and the network.

- `debug vpdn`—To display debug traces for the Virtual Private Dialup Network (VPDN) feature, which provides PPP tunnels using the Layer 2 Forwarding (L2F) protocol.
- **debug ppp**—To display information on traffic and exchanges in an internetwork implementing the Point-to-Point Protocol (PPP).

- **debug ppp error**—To display protocol errors and error statistics associated with PPP connection negotiation and operation.

- **debug ppp multilink events**—To display information about events affecting multilink groups established for BACP.

- **debug vtemplate**—To display cloning information for a virtual access interface from the time it is cloned from a virtual template to the time the virtual access interface comes down when the call ends.

- **debug v120 event**—To display information on V.120 activity. V.120 is an ITU specification that allows for reliable transport of synchronous, asynchronous, or bit transparent data over ISDN bearer channels.

- **debug v120 packet**—To display general information on all incoming and outgoing V.120 packets and to determine whether incompatibilities exist between Cisco's V.120 implementation and other vendors' V.120 implementations

---

**Command Reference**

This section documents a new and modified command only.

- **aaa dnis map authentication group**
aaa dnis map authentication group

To map a Dialed Number Identification Service (DNIS) number to a particular authentication server group (this server group will be used for AAA authentication), use the **aaa dnis map authentication group** aaa-server-group configuration command. To remove the DNIS number from the defined server group, use the **no** form of this command.

```
aaa dnis map dnis-number authentication {ppp | login} group server-group-name

no aaa dnis map dnis-number authentication {ppp | login} group server-group-name
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dnis-number</td>
<td>Number of the DNIS.</td>
</tr>
<tr>
<td>ppp</td>
<td>Enables PPP authentication methods.</td>
</tr>
<tr>
<td>login</td>
<td>Enables character-mode authentication.</td>
</tr>
<tr>
<td>server-group-name</td>
<td>Character string used to name a group of security servers associated in a</td>
</tr>
<tr>
<td></td>
<td>server group.</td>
</tr>
</tbody>
</table>

**Defaults**

Disabled

**Command Modes**

AAA-server-group configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(7)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.1(3)XL1</td>
<td>This command was modified with the addition of the <strong>login</strong> keyword to</td>
</tr>
<tr>
<td></td>
<td>include character-mode authentication.</td>
</tr>
<tr>
<td>12.2(2)T</td>
<td>This command was integrated into Cisco IOS Release 12.2(2)T and support was</td>
</tr>
<tr>
<td></td>
<td>added for the Cisco 2600 series, Cisco 3600 series, and Cisco 7200 platforms.</td>
</tr>
<tr>
<td>12.2(8)T</td>
<td>Support was added for the Cisco 806, Cisco 828, Cisco 1710, Cisco SOHO 78,</td>
</tr>
<tr>
<td></td>
<td>Cisco 3631, Cisco 3725, Cisco 3745, and Cisco URM for IGX8400 platforms.</td>
</tr>
<tr>
<td>12.2(11)T</td>
<td>Support was added for the Cisco AS5300 and Cisco AS5800 platforms.</td>
</tr>
<tr>
<td>12.2(27)SBA</td>
<td>This command was integrated into Cisco IOS Release 12.2(27)SBA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the **aaa dnis map authentication group** aaa-server-group configuration command to assign a DNIS number to a particular AAA server group, so that the server group can process authentication requests for users dialing in to the network using that particular DNIS. To use the **aaa dnis map authentication group** aaa-server-group configuration command, you must first enable AAA, define a AAA server group, and enable DNIS mapping.
The following example maps DNIS number 7777 to the RADIUS server group called *group1*. Server group *group1* uses RADIUS server 172.30.0.0 for authentication requests for users dialing in with DNIS 7777.

```bash
aaa new-model
radius-server host 172.30.0.0 auth-port 1645 key cisco1
aaa group server radius group1
    server 172.30.0.0
    aaa dnis map enable
    aaa dnis map 7777 authentication ppp group group1
    aaa dnis map 7777 authentication login group group1
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa new-model</td>
<td>Enables the AAA access control model.</td>
</tr>
<tr>
<td>aaa dnis map accounting network group</td>
<td>Maps a DNIS number to a particular accounting server group.</td>
</tr>
<tr>
<td>aaa dnis map enable</td>
<td>Enables AAA server selection based on DNIS.</td>
</tr>
<tr>
<td>aaa group server</td>
<td>Groups different server hosts into distinct lists and distinct methods.</td>
</tr>
<tr>
<td>radius-server host</td>
<td>Specifies a RADIUS server host.</td>
</tr>
</tbody>
</table>

### Glossary

AAA—authentication, authorization, and accounting.


EAP—PPP Extensible Authentication Protocol.

Exec PPP—A feature of Cisco NASs that allows an end user to login to a NAS in character mode (exec mode, or shell mode), get authenticated, and then start PPP from the Exec session to establish a PPP connection between the end user and the NAS.

GRS—Global Roaming Service.

HGW—Home gateway—A router or access server that terminates L2F tunnels and PPP sessions.

IPCP—IP Control Protocol. Establishes and configures IP over PPP.

L2F—Layer 2 Forwarding Protocol. Protocol that supports the creation of secure virtual private dial-up networks over the Internet.

L2TP—Layer 2 Tunneling Protocol. Protocol that supports the creation of secure virtual private dial-up networks over the Internet.

L2X—Either L2F or L2TP or both.

LCP—Link Control Protocol.

MLP—Multilink PPP Protocol.

NCP—Network Control Protocol.

NAS—Network access server.

OTP—One-time password.
PAP—Password Authentication Protocol. Protocol that allows PPP peers to authenticate one another. The remote router attempting to connect to the local router is required to send an authentication request. Unlike CHAP, PAP passes the password and hostname or username in clear (unencrypted). PAP does not itself prevent unauthorized access, but merely identifies the remote end. The router or access server then determines if that user is allowed access.

PPP—Point-to-Point Protocol. Provides router-to-router and host-to-network connections over synchronous and asynchronous circuits. PPP was designed to work with several network layer protocols such as IP, IPX, and ARA. PPP also has a built-in security mechanism, such as CHAP or PAP. PPP relies on two protocols: LCP and NCP.

PPP client—A PPP user who dials up to a NAS.


ISP—Internet service provider.

SDI—Security Dynamics ID card.

VPDN—Virtual private dialup network.