



Diagnosing and Troubleshooting AAA Operations

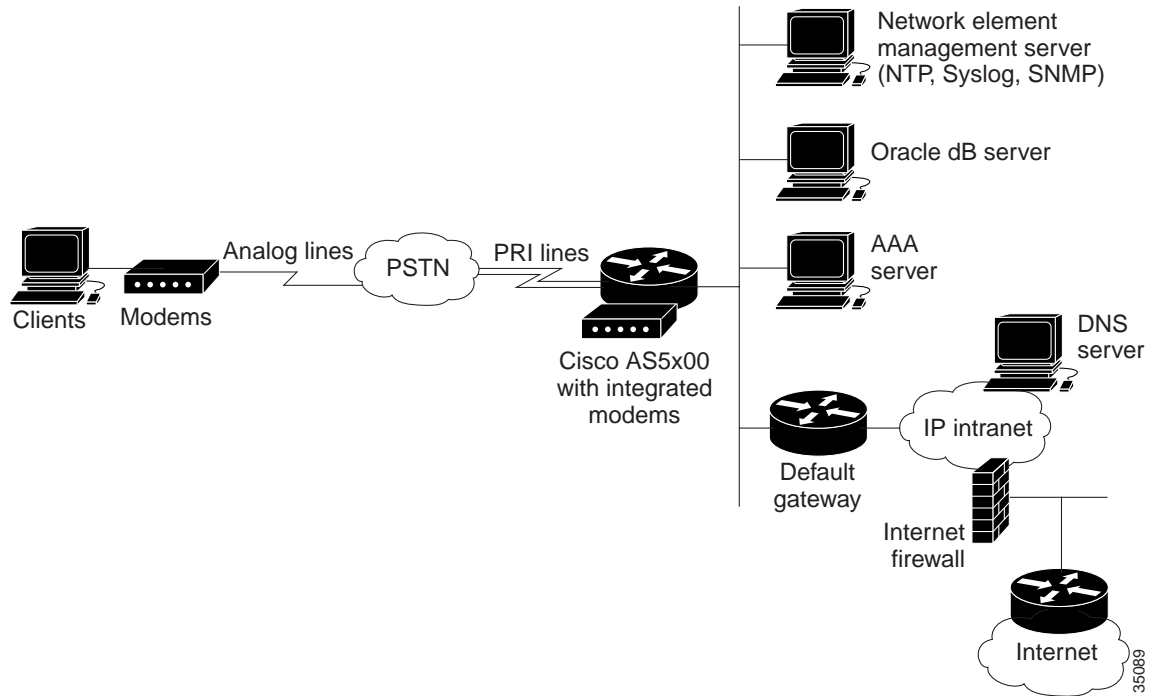
This chapter focuses on diagnosing and troubleshooting negotiations between AAA devices. This section reviews the case study environment and outlines the protocol flows associated with AAA negotiations in the context of this network environment. The subsequent sections focus on specific troubleshooting techniques as follows:

- 6.1 Overview of Authentication and Authorization Processes
- 6.2 Troubleshooting AAA Implementation
- 6.3 AAA Troubleshooting Basics
- 6.4 Troubleshooting Scenarios

6.1 Overview of Authentication and Authorization Processes

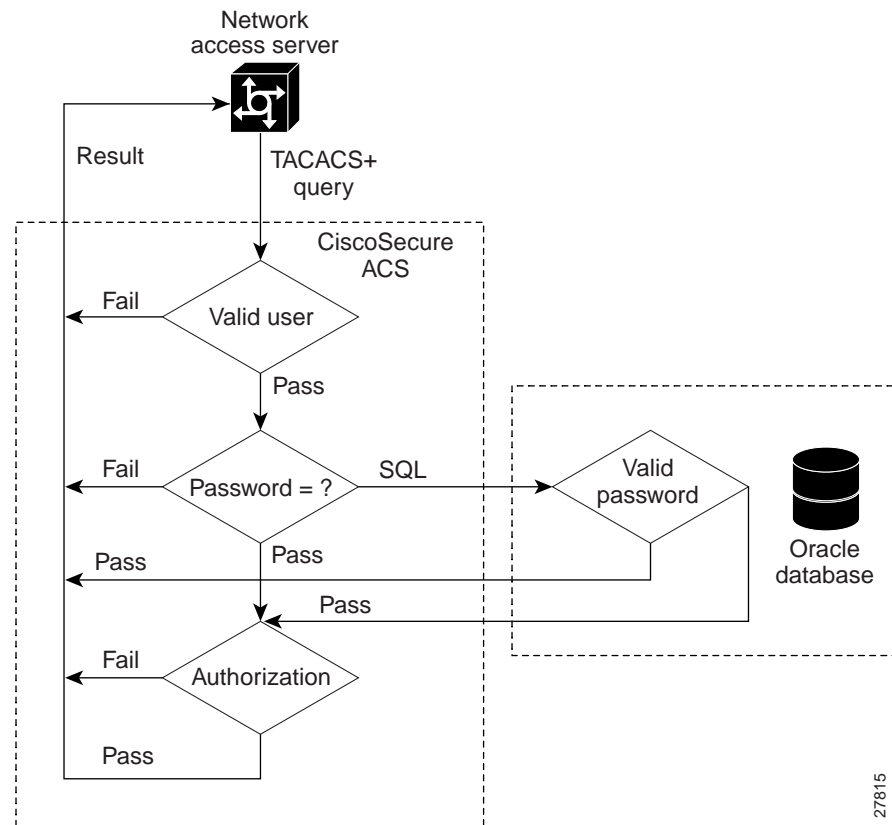
Before jumping immediately into troubleshooting AAA problems, it is useful to review authentication and authorization processes. Figure 6-1 provides the general scenario this case study is built around. The primary elements of this environment are the AAA server, the AAA database, and the NAS.

Figure 6-1 Basic AAA Case Study Environment



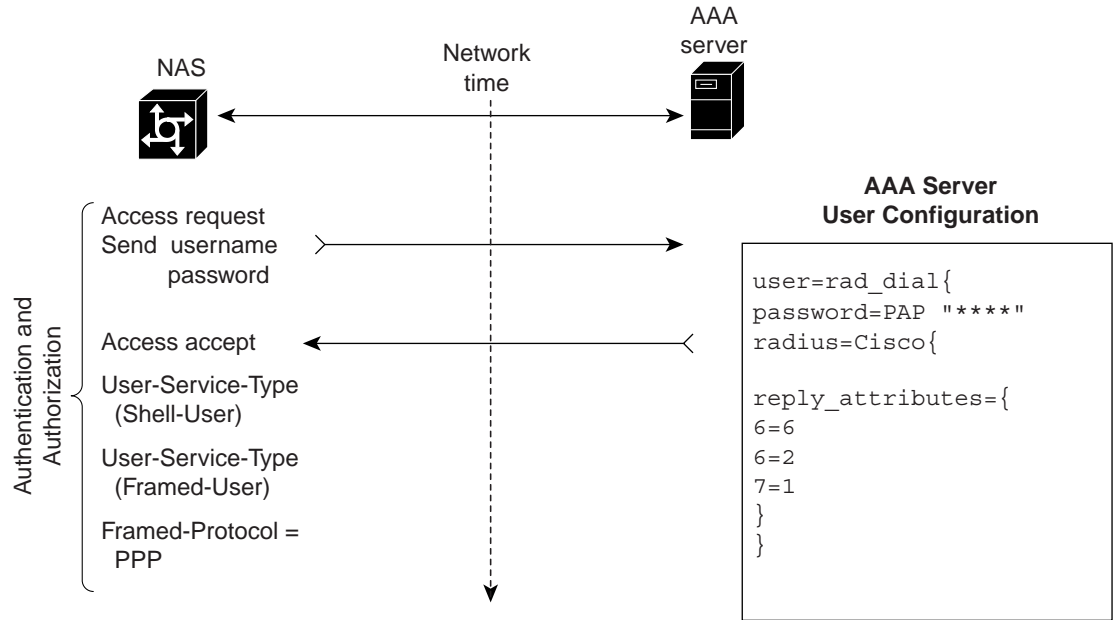
The negotiation suggested in Figure 6-1 is expanded in Figure 6-2 which presents the logical flow of the authentication and authorization processes and illustrates the relationship between the elements within the TACACS+ based AAA negotiation. While the network access server (NAS) communicates directly with the AAA server, the AAA server in turn exchanges information with the Oracle database server.

Figure 6-2 Dial Access Authentication and Authorization Flow Diagram



The RADIUS dial-access authentication and authorization illustrated in Figure 6-3 describes RADIUS negotiation between the NAS and the AAA server. User *rad_dial* is permitted PPP access through EXEC shell (character mode) or autoselect PPP (packet mode).

Figure 6-3 RADIUS Dial Access Authentication and Authorization Process

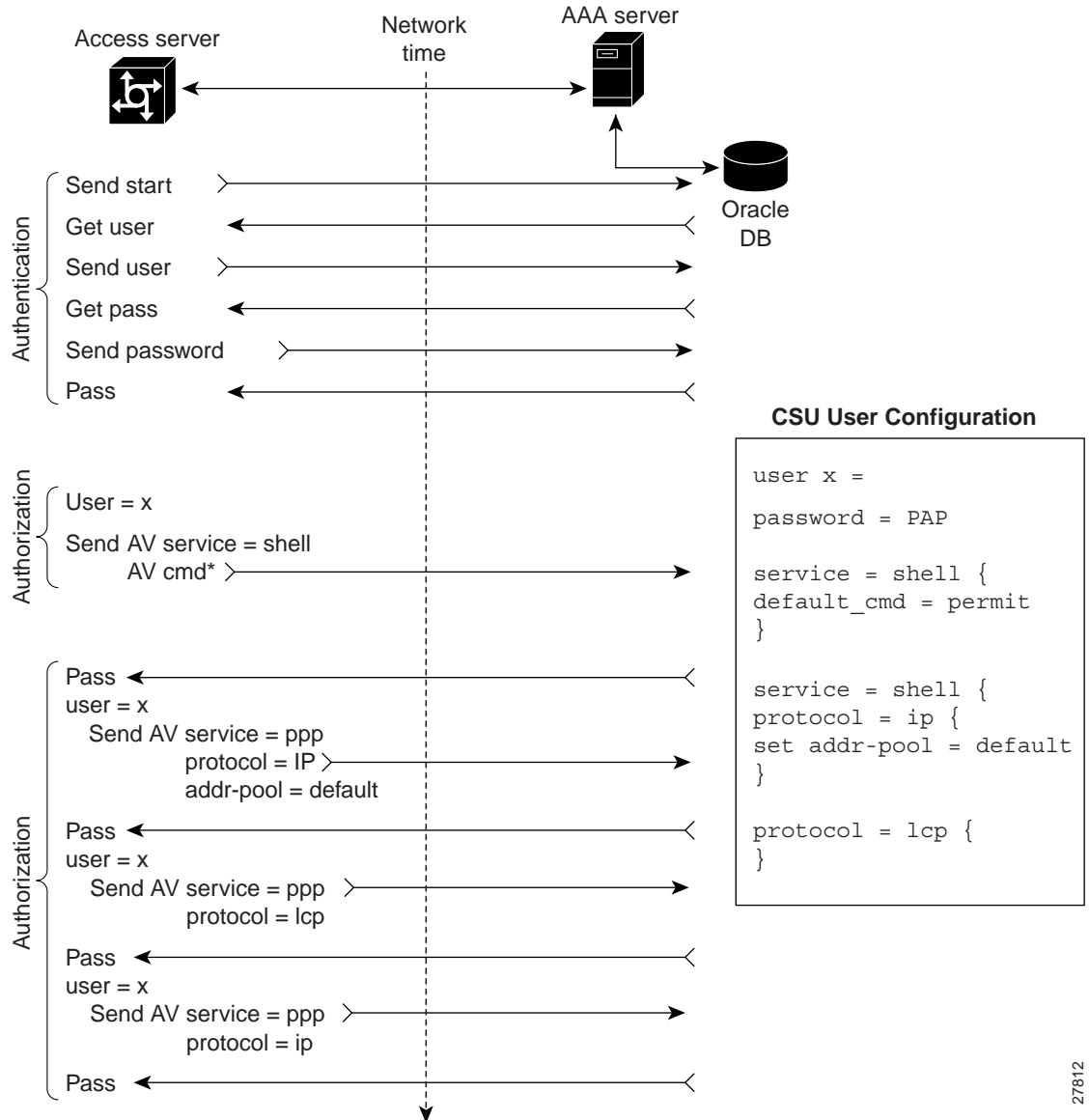


Note

Unlike TACACS+, the authentication and authorization processes are not handled as separate stages in RADIUS-based AAA access control.

Figure 6-4 and Figure 6-5 expand on the basic negotiation flow depicted in Figure 6-2 by illustrating the specific TACACS+ negotiation process associated with particular users, as defined in their respective CSU profiles.

Figure 6-4 TACACS+ Dial Access Authentication and Authorization Session (EXEC Enabled)



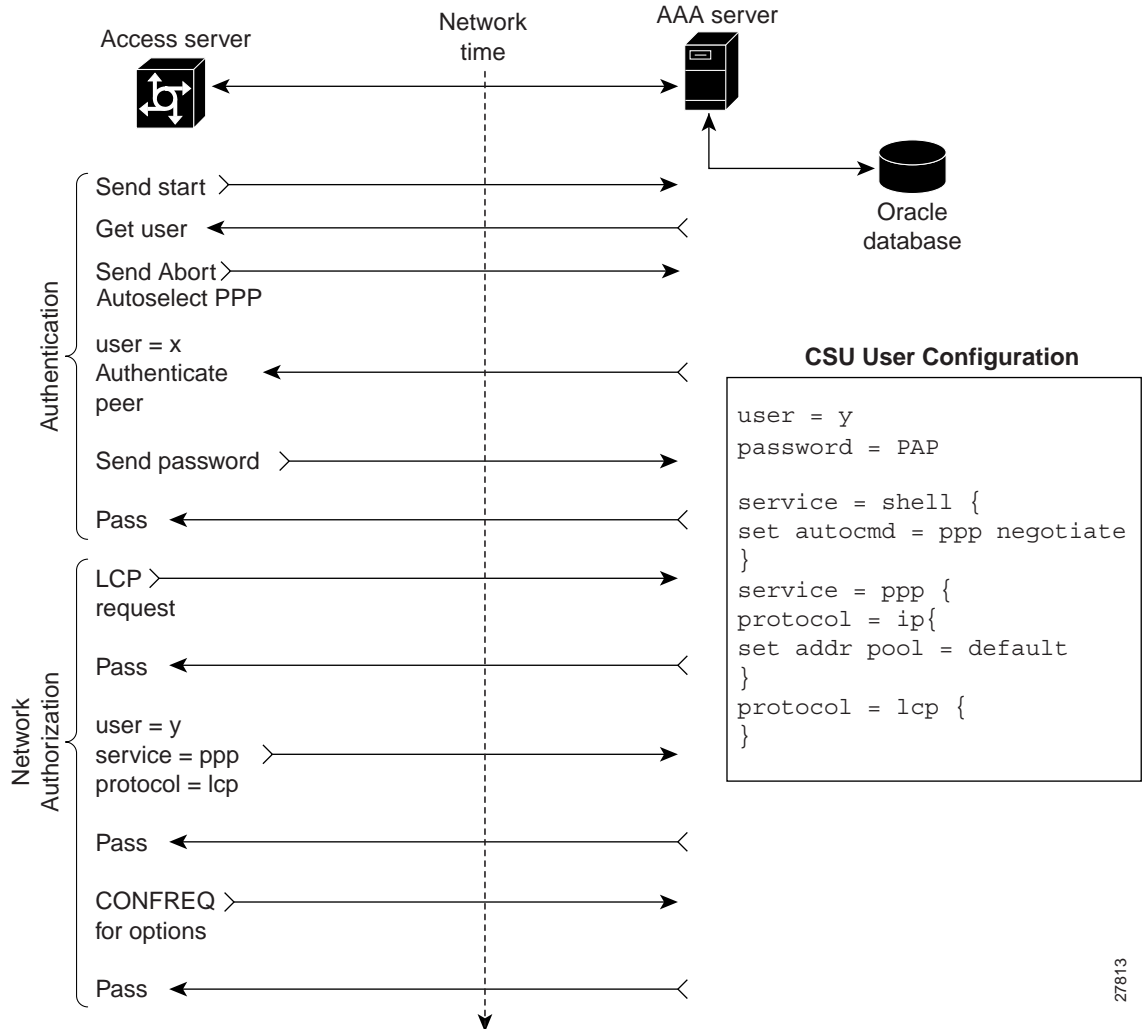
27812

The difference in authorization behavior stems from the use of two commands in the AAA server user configurations. The **default_cmd=permit** command included in the example in Figure 6-4 enables default privilege level 15 commands for user x.

As configured in Figure 6-4, the session for user x depicts a process that involves either a shell initiated or a standard PPP session. The same negotiations are used in initiating shell access to a router.

Both figures depict the stages of dial access authentication and authorization sessions between an access server and an AAA server. The key difference is defined in the CSU user configuration (profiles) included in each illustration. In Figure 6-4, EXEC shell access authorization is permitted while it is not permitted in the illustration depicted in Figure 6-5.

Figure 6-5 TACACS+ Dial Access Authentication and Authorization Session (EXEC Shell Disabled)



The example session illustrated in Figure 6-5 omits the **default_cmd=permit** AVP and instead includes the **autocmd=ppp negotiate** AVP disabling EXEC shell access to IOS devices. User y fails any attempt to access the router and receives the message `PPP not allowed on this interface` as a result of the PPP configuration statement. This distinction provides an element of security, blocking access to routers.

6.2 Troubleshooting AAA Implementation

These sections help you to accomplish the following tasks:

- 6.2.1 Troubleshooting Methodology Overview
- 6.2.2 Cisco IOS Debug Command Summary

6.2.1 Troubleshooting Methodology Overview

The troubleshooting methodology adopted in this chapter follows these general steps:

1. Isolating the problem.
 - Gathering detailed information about trouble.
 - Determining the starting point and fault isolation procedures.
2. Correcting the problem.
 - Making appropriate hardware, software, or configuration changes to correct the problem.
3. Verifying that the trouble is corrected.
 - Performing operational tests to verify that trouble is corrected.

The troubleshooting tables presented in “6.3 AAA Troubleshooting Basics” and the example scenarios presented in “6.4 Troubleshooting Scenarios” generally follow this methodology in listing typical symptoms, and provide associated problems and diagnostics measures.

6.2.2 Cisco IOS Debug Command Summary

Output from Cisco IOS **debug** commands provide a valuable source of information and feedback concerning state transitions and functions within the AAA subsystem environment.

Use the **debug** commands that follow for capturing AAA-related transitions and functions:

- **debug condition user *username***
Enabling this **debug** command sets conditional debugging for a specific user and generates output debugs related to the user. This command is helpful in an enterprise environment for troubleshooting.
- **debug aaa authentication**
Enabling this **debug** command displays authentication information with TACACS+ and RADIUS client/server interaction.
- **debug aaa authorization**
Enabling this **debug** command displays authorization information with TACACS+ and RADIUS client/server interaction.
- **debug aaa accounting**
Enabling this **debug** command displays accounting information with TACACS+ and RADIUS client/server interaction.
- **debug tacacs**
Enabling this **debug** command displays TACACS+ interaction between IOS client and AAA Server.
- **debug radius**

Enabling this **debug** command displays RADIUS interaction between the IOS client and the AAA server.

In addition to **debug** command output gathered directly from devices running Cisco IOS, a Cisco AAA server can be configured to collect important operational diagnostics.

Go to the following link for information regarding configuring and using CSU ACS logs:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/cs_unx/cs23rg/troubles.htm

6.3 AAA Troubleshooting Basics

AAA operational diagnostic activity for access environments is divided into the following basic areas:

- Dial-based versus router-based access
- Local versus server access
- Authentication and authorization processes

These three areas can be associated with eight underlying diagnostic situations which are addressed in the following subsections:

- 6.3.1 Troubleshooting Dial-Based Local Authentication
- 6.3.2 Troubleshooting Dial-Based Server Authentication
- 6.3.3 Troubleshooting Dial-Based Local Authorization
- 6.3.4 Troubleshooting Dial-Based Server Authorization
- 6.3.5 Troubleshooting Router-Based Local Authentication
- 6.3.6 Troubleshooting Router-Based Server Authentication
- 6.3.7 Troubleshooting Router-Based Local Authorization
- 6.3.8 Troubleshooting Router-Based Server Authorization

The following sections address each of the diagnostic topics separately. Detailed scenarios are provided in “6.4 Troubleshooting Scenarios.”

The diagnostics summaries address the troubleshooting process using three basic stages:

1. Identifying symptoms
2. Isolating problems
3. Resolving problems

Each diagnostic table includes suggestions for identifying and isolating problems. Diagnostic information is provided in “6.4 Troubleshooting Scenarios.” Specific diagnostic output is included to illustrate how network entities react to failures and how to discern specific failures.



Note

Some of the symptoms described in the following tables can be caused by a variety of problems other than AAA issues. Because this case study focuses on AAA-based security topics, the problems and diagnostics provided here focus on AAA issues.

6.3.1 Troubleshooting Dial-Based Local Authentication

The following symptoms are addressed in separate tables in this section:

- Single User Failure; Individual Dial-in User Connection Fails
- Multiple User Failure; All Dial-in Users Unable to Connect to NAS

Table 6-1 *Single User Failure; Individual Dial-in User Connection Fails*

Problem	Suggested Diagnostic Steps
User entered invalid username or password.	<ol style="list-style-type: none"> To verify local account, enter: <pre><NAS>#debug aaa authentication</pre> Test login with username/password. Look for “user not found” or “password validation” failure. If user is not found, add the user. If password validation failure, reenter login with username and password combination.

Table 6-2 *Multiple User Failure; All Dial-in Users Unable to Connect to NAS*

Problem	Suggested Diagnostic Steps
AAA behavior configured incorrectly in NAS.	<ol style="list-style-type: none"> Enter this diagnostic command in NAS: <pre><NAS>#debug aaa authentication</pre> To verify local authentication is configured correctly, enter: <pre><router>#show running-config</pre> Verify inclusion of one of these commands: <pre>aaa authentication login default local</pre> or <pre>aaa authentication login ppp default local</pre>
Shell initiated PPP session passes, but is torn down.	<ol style="list-style-type: none"> Enter this diagnostic command in NAS: <pre><NAS>#debug aaa authentication</pre> To verify AAA is configured correctly in NAS, enter: <pre><NAS>#show running-config</pre> Verify inclusion of this command: <pre>aaa authentication ppp default if-needed local</pre>

6.3.2 Troubleshooting Dial-Based Server Authentication

The following symptoms are addressed in separate tables in this section:

- Single User Failure; Individual User Unable to Make Connection (RADIUS and TACACS+)
- Multiple User Failure; All Dial-in Users Unable to Connect to NAS (RADIUS and TACACS+)

Table 6-3 Single User Failure; Individual User Unable to Make Connection (RADIUS and TACACS+)

Problem	Suggested Diagnostic Steps
User name not in server database.	<ol style="list-style-type: none"> To verify user is in database, enter: <pre><CSUser>\$/opt/ciscosecure/CLI/ViewProfile -p 9900 -u username</pre>
User entered password incorrectly.	<ol style="list-style-type: none"> Verify password case-sensitivity. Monitor user activity in AAA server: <pre><CSUser>\$tail -f /var/log/csuslog grep username</pre> Review csuslog file for errors (for example, if user is configured for OTP, verify PASSCODE is accepted from OTP server. Reset user password or synchronize PASSCODE if needed.
User profile configured incorrectly. The error message “bad method for user” reported in <i>csuslog</i> file.	<ol style="list-style-type: none"> To verify user profile is programmed with correct password type, enter: <pre><CSUser>\$/opt/ciscosecure/CLI/ViewProfile -p 9900 -u username</pre> Verify user profile privilege is sufficient to perform task. Verify profile is configured for correct password type. For example, PAP for OTP.
User account disabled due to too many failed logins.	<ol style="list-style-type: none"> To view user profile, enter: <pre><CSUser>\$/opt/ciscosecure/Utils/bin/ViewProfile -p 9900 -u username</pre> Verify that the profile is not disabled. If it is disabled, compare set server current-failed-login counters to max failed login setting in <i>CSU.cfg</i> file. If these attributes are the same, reset user profile status to enabled and reset the set server current-failed-login counter by using the web-based administration utility.

Table 6-3 Single User Failure; Individual User Unable to Make Connection (RADIUS and TACACS+)

Problem	Suggested Diagnostic Steps
User account password or profile expired.	<ol style="list-style-type: none"> 1. To view profile, enter: <pre><CSUser>\$ /opt/ciscosecure/CLI/ViewProfile -p 9900 -u username</pre> 2. For TACACS+: Look for expiration in profile, such as: <p>expires = "24 Jan 2000"</p> 3. For RADIUS: Look for expiration in profile, such as: <p>Password-Expiration = "24 Jan 2000"</p>
User workstation configured incorrectly.	<ol style="list-style-type: none"> 1. Review user dialup networking setup. 2. To review user profile, enter: <pre><CSUser>\$ /opt/ciscosecure/CLI/ViewProfile -p 9900 -u username</pre> 3. Check for setup for parameter such as "Requires encrypted password."
User exceeded the maximum number of concurrent sessions.	<p>To review user profile, enter:</p> <pre><CSUser>\$ /opt/ciscosecure/CLI/ViewProfile -p 9900 -u username</pre> <p>For TACACS+, look for this AVP:</p> <p>max-sessions</p> <p>For RADIUS, look for this AVP:</p> <p>Maximum-Channels</p>

Table 6-4 Multiple User Failure; All Dial-in Users Unable to Connect to NAS (RADIUS and TACACS+)

Problem	Suggested Diagnostic Steps
Connection between NAS and AAA server is down.	Verify network connectivity between NAS and AAA server. Enter these diagnostic commands in NAS: <pre data-bbox="964 474 1295 579"> <NAS>#show tacacs <NAS>#debug tacacs <NAS>#debug radius <NAS>#ping CSU-server-name </pre>
TACACS+ or RADIUS key incorrect in NAS or AAA server.	Review NAS and CSU configurations for shared secret. <p data-bbox="964 667 1122 695">In NAS, enter:</p> <pre data-bbox="964 716 1284 743"><NAS>#show running-config</pre> <p data-bbox="964 768 1203 795">In AAA server, enter:</p> <pre data-bbox="964 816 1360 915"> <CSUserver>\$grep NAS-IP-Address /opt/ciscosecure/config/CSU.cfg <CSUserver>\$tail -f /var/log/csuslog </pre>
Maximum number of users exceeded.	<ol data-bbox="922 957 1455 1220" style="list-style-type: none"> 1. Verify license key is entered correctly in AAA server. Enter the following commands at the CSUserver: <pre data-bbox="964 1068 1360 1117"> <CSUserver>\$grep license-key /opt/ciscosecure/config/CSU.cfg </pre> 2. To review expiration date of license key, enter: <pre data-bbox="964 1243 1325 1285"> <CSUserver>\$grep license-key /var/log/csuslog </pre>

Table 6-4 Multiple User Failure; All Dial-in Users Unable to Connect to NAS (RADIUS and TACACS+)

Problem	Suggested Diagnostic Steps
Group profile password type does not match type specified in NAS group-async or dialer interface configuration (for example, PPP authentication PAP).	<ol style="list-style-type: none"> To review NAS configuration, enter: <code><NAS># show running-config</code> Verify group-async or dialer interface is configured with correct password type. For example, for OTP, PAP must be specified. Verify group profile matches group-async or dialer interface configuration in NAS.
Shell initiated PPP session passes, but is torn down.	<ol style="list-style-type: none"> Enter this diagnostic command in NAS: <code><NAS>#debug aaa authentication</code> To verify correct AAA configuration is configured in NAS, enter: <code><NAS>#show running-config</code> Verify these commands are included in the NAS configuration: aaa authentication ppp default if-needed tacacs+ or aaa authentication ppp default if-needed radius

6.3.3 Troubleshooting Dial-Based Local Authorization

The following symptoms are addressed in separate tables in this section:

- User Cannot Start PPP
- Network Authorization Fails
- Unable to Access Specific Host or Network Service
- Multilink Fails

Table 6-5 User Cannot Start PPP

Problem	Suggested Diagnostic Steps
User client configuration error.	<p>Refer to MS troubleshooting chapter:</p> <p>http://support.microsoft.com/support/kb/articles/Q130/0/79.asp?LNG=ENG&SA=ALLKB</p>

Table 6-6 Network Authorization Fails

Problem	Suggested Diagnostic Steps
Attribute-value pairs (AVPs) not assigned ¹ .	<ol style="list-style-type: none"> 1. Enter this diagnostic command in NAS: <pre><NAS>#debug aaa authorization</pre> 2. To verify AAA is configured correctly in NAS, enter: <pre><NAS>#show running-config</pre> 3. Verify inclusion of this command: <pre>aaa authorization exec default local</pre>

1. AAA authorization only supported on shell sessions with local accounts.

Table 6-7 Unable to Access Specific Host or Network Service

Problem	Suggested Diagnostic Steps
Access list assigned to user.	<ol style="list-style-type: none"> 1. Verify local account not restricted with access-class AVP: <pre><NAS>#show running-config</pre> 2. Enter these NAS commands to determine whether access list is assigned to user: <pre><NAS>#show caller user userid detail <NAS>#show line</pre> 3. To review access list with this NAS command, enter: <pre><NAS>#show access-list ACL-number</pre>

Table 6-8 Multilink Fails

Problem	Suggested Diagnostic Steps
User profile restricted.	<p>To verify user account is not restricted by inclusion of max-links AVP, enter:</p> <pre><CSUserver>\$/opt/ciscosecure/CLI/ViewProfile -p 9900 -u username</pre>

6.3.4 Troubleshooting Dial-Based Server Authorization

The following symptoms are addressed in separate tables in this section:

- Multiple Users Cannot Start PPP (RADIUS and TACACS+)
- Network Authorization Fails (RADIUS and TACACS+)
- User or Group Members Unable to Access Specific Host or Network Service (RADIUS and TACACS+)
- Multilink Fails (TACACS+)
- Multilink Fails (RADIUS)
- Session Fails to Disconnect After Expected Idle Timeout (TACACS+)
- Session Fails to Disconnect After Expected Idle Timeout (RADIUS)
- No EXEC Shell for TACACS+
- No EXEC Shell for RADIUS
- Cannot Start Concurrent Sessions (TACACS+)
- Cannot Start Concurrent Sessions (RADIUS)

Table 6-9 Multiple Users Cannot Start PPP (RADIUS and TACACS+)

Problem	Suggested Diagnostic Steps
AAA authorization configured incorrectly in NAS.	<ol style="list-style-type: none"> <li data-bbox="922 329 1463 405">1. Enter this diagnostic command in NAS: <code><NAS>#debug aaa authorization</code> <li data-bbox="922 428 1463 533">2. To verify AAA is configured correctly in NAS, enter: <code><NAS>#show running-config</code> <li data-bbox="922 556 1463 835">3. Verify inclusion of this command: aaa authorization network default group tacacs+ or aaa authorization network default group radius
Does not have PPP service assigned.	<ol style="list-style-type: none"> <li data-bbox="922 842 1463 947">1. To view group profile, enter: <code><CSUserver>\$/opt/ciscosecure/CLI/ViewProfile -p 9900 -g groupname</code> <li data-bbox="922 970 1463 1213">2. For TACACS+, verify the following commands are assigned to group: service=ppp protocol=lcp protocol=ip <li data-bbox="922 1257 1463 1444">3. For RADIUS, verify the following commands are assigned to group: Service-Type=Framed Framed-Protocol=ppp
Group lacks shell service assigned (EXEC shell-initiated PPP session only).	<ol style="list-style-type: none"> <li data-bbox="922 1451 1463 1556">1. To view group profile, enter: <code><CSUserver>\$/opt/ciscosecure/CLI/ViewProfile -p 9900 -g groupname</code> <li data-bbox="922 1579 1463 1684">2. For TACACS+, verify the following command is assigned to group: service=shell <li data-bbox="922 1728 1463 1841">3. For RADIUS, verify the following command is assigned to group: User-Service-Type (Shell-User)

Table 6-10 Network Authorization Fails (RADIUS and TACACS+)

Problem	Suggested Diagnostic Steps
AVPs not assigned.	<ol style="list-style-type: none"> 1. Enter this diagnostic command in NAS: <pre><NAS>#debug aaa authorization</pre> 2. To verify AAA is configured correctly in NAS, enter: <pre><NAS>#show running-config</pre> 3. Verify inclusion of this command: <pre>aaa authorization network default group tacacs+</pre> <p>or</p> <pre>aaa authorization network default group radius</pre>

Table 6-11 User or Group Members Unable to Access Specific Host or Network Service (RADIUS and TACACS+)

Problem	Suggested Diagnostic Steps
Access list assigned to user.	<ol style="list-style-type: none"> 1. To view group profile, enter: <pre><CSUserver>\$/opt/ciscosecure/CLI/ViewProfile -p 9900 -g groupname</pre> <p>Verify group account not restricted with inac AVP.</p> 2. Enter these NAS commands to determine whether access list is assigned to user: <pre><NAS>#show caller user userid detail</pre> <pre><NAS>#show line</pre> 3. Review access list with this NAS command: <pre><NAS>#show access-list ACL-number</pre>

Table 6-12 Multilink Fails (TACACS+)

Problem	Suggested Diagnostic Steps
User or group profile lacks proper AVP.	<ol style="list-style-type: none"> To verify group account includes protocol=multilink AVP assigned, enter: <pre><CSUserver>\$/opt/ciscosecure/CLI/ViewPr ofile -p 9900 -g groupname</pre> Review profile for load-threshold AVP and whether it is configured properly.
User or group profile restricted.	To verify group account not restricted with max-links AVP, enter: <pre><CSUserver>\$/opt/ciscosecure/CLI/ViewPr ofile -p 9900 -g groupname</pre>

Table 6-13 Multilink Fails (RADIUS)

Problem	Suggested Diagnostic Steps
User or group profile lacks proper AVP.	To verify group account includes framed-protocol=multilink AVP assigned, enter: <pre><CSUserver>\$/opt/ciscosecure/CLI/ViewPr ofile -p 9900 -g groupname</pre>
User or group profile restricted.	To verify group account not restricted with max-links AVP, enter: <pre><CSUserver>\$/opt/ciscosecure/CLI/ViewPr ofile -p 9900 -g groupname</pre>

Table 6-14 Session Fails to Disconnect After Expected Idle Timeout (TACACS+)

Problem	Suggested Diagnostic Steps
The idletime AVP not configured on group profile.	To verify group account includes idletime AVP assigned, enter: <pre><CSUserver>\$/opt/ciscosecure/CLI/ViewPr ofile -p 9900 -g groupname</pre>

Table 6-15 Session Fails to Disconnect After Expected Idle Timeout (RADIUS)

Problem	Suggested Diagnostic Steps
The Idle-Timeout AVP not configured on group profile.	To verify group account includes Idle-Timeout AVP assigned, enter: <pre><CSUserver>\$/opt/ciscosecure/CLI/ViewPr ofile -p 9900 -g groupname</pre>

Table 6-16 No EXEC Shell for TACACS+

Problem	Suggested Diagnostic Steps
User or group lacks service=shell AVP assigned.	To verify service=shell is assigned to user or group, enter: <pre><CSUser>\$/opt/ciscosecure/CLI/ViewProfile -p 9900 -g groupname</pre> <pre><CSUser>\$/opt/ciscosecure/CLI/ViewProfile -p 9900 -u username</pre>

Table 6-17 No EXEC Shell for RADIUS

Problem	Suggested Diagnostic Steps
User or group does not have User-Service-Type AVP assigned.	To verify User-Service-Type (Shell-User) is assigned to user or group, enter: <pre><CSUser>\$/opt/ciscosecure/CLI/ViewProfile -p 9900 -g groupname</pre> <pre><CSUser>\$/opt/ciscosecure/CLI/ViewProfile -p 9900 -u username</pre>

Table 6-18 Cannot Start Concurrent Sessions (TACACS+)

Problem	Suggested Diagnostic Steps
User exceeds the maximum number of concurrent sessions.	1. To review the user profile, enter: <pre><CSUser>\$/opt/ciscosecure/CLI/ViewProfile -p 9900 -u username</pre> 2. Look for the following AVP: server max sessions

Table 6-19 Cannot Start Concurrent Sessions (RADIUS)

Problem	Suggested Diagnostic Steps
User exceeds the maximum number of concurrent sessions.	1. To review the user profile, enter: <pre><CSUser>\$/opt/ciscosecure/CLI/ViewProfile -p 9900 -u username</pre> 2. Look for the following AVP: Maximum-Channels

6.3.5 Troubleshooting Router-Based Local Authentication

The following symptoms are addressed in separate tables in this section:

- Single User Failure; Individual Dial-in User Connection Fails
- Multiple User Failure; All Dial-in Users Unable to Connect to Router
- Users Can Access Router by Using Console or VTY, but Not Both

Table 6-20 Single User Failure; Individual Dial-in User Connection Fails

Problem	Suggested Diagnostic Steps
User entered invalid username or password.	<ol style="list-style-type: none"> 1. To verify local account, enter: <code><router>#debug aaa authentication</code> 2. Test login with username/password. 3. Look for user not found or password validation failure.

Table 6-21 Multiple User Failure; All Dial-in Users Unable to Connect to Router

Problem	Suggested Diagnostic Steps
AAA behavior configured incorrectly in router.	<ol style="list-style-type: none"> 1. Enter this diagnostic command in router: <code><router>#debug aaa authentication</code> 2. To verify local authentication is configured correctly, enter: <code><router>#show running-config</code> 3. Verify inclusion of this command: aaa authentication login/ppp default local

Table 6-22 Users Can Access Router by Using Console or VTY, but Not Both

Problem	Suggested Diagnostic Steps
Incorrect AAA configuration in router.	<ol style="list-style-type: none"> 1. Enter this diagnostic command in router: <pre><router>#debug aaa authentication</pre> 2. To verify AAA is configured correctly in router, enter: <pre><router>#show running-config</pre> 3. Verify method used for console authentication matches VTY method. <p>For example:</p> <ul style="list-style-type: none"> • AAA configuration: <pre>aaa authentication login listname group tacacs+</pre> • Console line configuration: <pre>line con 0 login authentication listname</pre> • VTY line configuration: <pre>line vty 0 4 login authentication listname</pre>

6.3.6 Troubleshooting Router-Based Server Authentication

The following symptoms are addressed in separate tables in this section:

- Single User Failure; Individual User Unable to Make a Connection
- Multiple User Failure; All Dial-In Users Unable to Connect to the Router
- Users Pass Authentication on Console or VTY, but Not Both

Table 6-23 Single User Failure; Individual User Unable to Make a Connection

Problem	Suggested Diagnostic Steps
User name not in server database.	<ol style="list-style-type: none"> To verify user is in database, enter: <pre><CSUserver>\$/opt/ciscosecure/CLI/ViewProfile -p 9900 -u username</pre>
User entered password incorrectly.	<ol style="list-style-type: none"> Verify password case sensitivity. To monitor user activity in AAA server, enter: <pre><CSUserver>\$tail -f /var/log/csuslog grep username</pre> Review <i>csuslog</i> file for errors.
User profile configured incorrectly. The error message “bad method for user” reported in <i>csuslog</i> file.	<ol style="list-style-type: none"> To verify user profile is programmed with correct password type, enter: <pre><CSUserver>\$/opt/ciscosecure/CLI/ViewProfile -p 9900 -u username</pre> Verify user profile privilege is sufficient to perform task. Verify profile is configured for correct password type. For example, DES or clear text.
User account disabled due to too many failed logins.	<ol style="list-style-type: none"> To view user profile, enter: <pre><CSUserver>\$/opt/ciscosecure/utlils/bin/ViewProfile -p 9900 -u username</pre> Verify that the profile is not disabled. If it is disabled, compared set server current-failed-login counters to max failed login setting in <i>CSU.cfg</i> file. If these attributes are the same, reset user profile status to enabled and reset the set server current-failed-login counter by using the web-based administration utility.
User account password or profile expired.	<ol style="list-style-type: none"> To view profile, enter: <pre><CSUserver>\$/opt/ciscosecure/CLI/ViewProfile -p 9900 -u username</pre> Look for expiration in profile, such as: expires = "24 Jan 2000"
User exceeds the maximum number of concurrent sessions.	<ol style="list-style-type: none"> To review the user profile, enter: <pre><CSUserver>\$/opt/ciscosecure/CLI/ViewProfile -p 9900 -u username</pre> Look for the following AVP: server max sessions

Table 6-24 Multiple User Failure; All Dial-In Users Unable to Connect to the Router

Problem	Suggested Diagnostic Steps
Connection between router and AAA server down.	Verify network connectivity between router and AAA server. Enter these diagnostic commands in router: <pre data-bbox="1011 447 1369 546"> <router>#show tacacs <router>#debug tacacs <router>#debug radius <router>#ping CSU-IP-address </pre>
TACACS+ key incorrect in router or AAA server.	Review router and CSU configurations for shared secret. <p data-bbox="1011 638 1227 663">In the router, enter:</p> <pre data-bbox="1011 684 1369 709"> <router>#show running-config </pre> <p data-bbox="1011 737 1292 762">In the AAA server, enter:</p> <pre data-bbox="1011 783 1446 831"> <CSUserver>\$grep router-IP-address /opt/ciscosecure/config/CSU.cfg </pre>
Maximum number of users exceeded.	<ol data-bbox="971 848 1503 1155" style="list-style-type: none"> 1. Verify license key is entered correctly in AAA server. Enter the following commands at the CSUserver: <pre data-bbox="1011 957 1406 1005"> <CSUserver>\$grep license-key /opt/ciscosecure/config/CSU.cfg </pre> 2. To review the expiration date of the license key, enter: <pre data-bbox="1011 1115 1369 1163"> <CSUserver>\$grep license-key /var/log/csuslog </pre>

Table 6-25 Users Pass Authentication on Console or VTY, but Not Both

Problem	Suggested Diagnostic Steps
Incorrect AAA configuration in router.	<ol style="list-style-type: none"> 1. Enter this diagnostic command in router: <pre><router>#debug aaa authentication</pre> 2. To verify AAA is configured correctly in router, enter. <pre><router>#show running-config</pre> 3. Verify method used for console authentication matches VTY method. <p>For example:</p> <ul style="list-style-type: none"> • AAA configuration: <pre>aaa authentication login listname group tacacs+</pre> • Console line configuration: <pre>line con 0</pre> <pre>login authentication listname</pre> • VTY line configuration: <pre>line vty 0 4</pre> <pre>login authentication listname</pre>

6.3.7 Troubleshooting Router-Based Local Authorization

The following symptoms are addressed in separate tables in this section:

- User Fails Router Command
- User Disconnected After Entering a Password
- Users Access Incorrect Privilege Level Commands
- Router User Receives Error Message Stating “This Line Not Allowed to Run PPP and is Disconnected”

Table 6-26 User Fails Router Command

Problem	Suggested Diagnostic Steps
AAA configuration error.	<ol style="list-style-type: none"> 1. Enter this diagnostic command in router to determine method of authorization and failure: <pre><router>#debug aaa authorization</pre> 2. To verify AAA is configured correctly in router, enter: <pre><router>#show running-config</pre> <p>Example: If aaa authorization commands is used, ensure method specified is local.</p>
User profile lacks appropriate privilege level to perform command.	<p>To review privilege configuration in router, enter: <pre><router>#show running-config</pre> </p> <p>Example: Cisco IOS command aaa authorization commands 15 default local is used, but user does not have a corresponding privilege level assigned.</p>
User profile lacks appropriate enable level to perform command.	<p>To review enable privilege level configuration in router, enter: <pre><router>#show running-config</pre> </p> <p>Example of relevant Cisco IOS commands:</p> <pre>aaa authentication enable default local enable 15 secret enable 10 secret2</pre> <p>In this example, users at enable level 10 cannot perform privilege level 15 commands.</p>

Table 6-27 User Disconnected After Entering a Password

Problem	Suggested Diagnostic Steps
Authorization failed service. Looks like an authentication problem, but is an authorization failure.	<p>To review AAA configuration, enter: <pre><router>#show running-config</pre> </p> <p>If aaa authorization exec command specifies method other than local, user fails shell access. For example, aaa authorization exec default tacacs+ results in local user failing authorization.</p>

Table 6-28 Users Access Incorrect Privilege Level Commands

Problem	Suggested Diagnostic Steps
AAA behavior incorrectly configured.	<ol style="list-style-type: none"> 1. Enter this diagnostic command in router to determine level of command authorization: <pre><router>#debug aaa authorization</pre> 2. To review AAA configuration in router, enter: <pre><router>#show running-config</pre> 3. Verify AAA configured properly in router. <p>For example:</p> <pre>aaa authorization commands 15 default local</pre>

Table 6-29 Router User Receives Error Message Stating “This Line Not Allowed to Run PPP and is Disconnected”

Problem	Suggested Diagnostic Steps
The autocommand ppp negotiate command assigned to user.	<ol style="list-style-type: none"> 1. To review correct configuration is configured in router, enter: <pre><router>#show running-config</pre> <p>Look for autocommand ppp negotiate command assigned to user.</p> 2. Delete autocommand ppp negotiate if appropriate.

6.3.8 Troubleshooting Router-Based Server Authorization

The following symptoms are addressed in separate tables in this section:

- User Fails Router Command
- User Disconnected After Entering Password
- Users Access Incorrect Privilege Level Commands
- Router User Receives Error Message Stating “This Line Not Allowed to Run PPP and is Disconnected”
- Router User Unable to Initiate Shell Session with Router
- AVPs Not Working on Console Port

Table 6-30 User Fails Router Command

Problem	Suggested Diagnostic Steps
AAA configuration error.	<ol style="list-style-type: none"> 1. Enter this diagnostic command in router to determine method of authorization and failure: <pre><router>#debug aaa authorization</pre> 2. To review AAA configuration in router, enter: <pre><router>#show running-config</pre> <p>Example: If aaa authorization commands is used, ensure method specified is tacacs+.</p>
User profile lacks appropriate privilege level to perform command.	<p>To view user profile for appropriate priv-lvl=x AVP, enter:</p> <pre><CSUser>\$/opt/ciscosecure/utlils/bin/ViewProfile -p 9900 -u username</pre>
User profile lacks appropriate enable privilege level to perform command.	<p>To view user profile for appropriate enable privilege level, enter:</p> <pre><CSUser>\$/opt/ciscosecure/utlils/bin/ViewProfile -p 9900 -u username</pre> <p>For example: privilege = des "*****" 15</p>

Table 6-31 User Disconnected After Entering Password

Problem	Suggested Diagnostic Steps
Authorization failed service.	<p>To review AAA configuration, enter:</p> <pre><router>#show running-config</pre> <p>If aaa authorization exec command specifies method other than TACACS+, user fails shell access.</p> <p>For example, aaa authorization exec default local results in TACACS+ user failing authorization.</p>

Table 6-32 Users Access Incorrect Privilege Level Commands

Problem	Suggested Diagnostic Steps
AAA behavior incorrectly configured.	<ol style="list-style-type: none"> 1. Enter this diagnostic command in router to determine level of command authorization: <pre><router>#debug aaa authorization</pre> 2. To verify AAA is configured correctly in router, enter <pre><router>#show running-config</pre> <p>Example of relevant Cisco IOS command: aaa authorization commands 15 default group tacacs+</p>
User profile configured incorrectly.	<p>To view user profile for appropriate priv-lvl=x AVP, enter:</p> <pre><CSUser>\$/opt/ciscosecure/utlils/bin/ViewProfile -p 9900 -u username</pre>

Table 6-33 Router User Receives Error Message Stating “This Line Not Allowed to Run PPP and is Disconnected”

Problem	Suggested Diagnostic Steps
The autocommand ppp negotiate AVP assigned to user.	<ol style="list-style-type: none"> 1. To view user profile for inclusion of autocommand ppp negotiate AVP assigned to user, enter: <pre><CSUser>\$/opt/ciscosecure/utlils/bin/ViewProfile -p 9900 -u username</pre> 2. Delete autocommand ppp negotiate if appropriate.

Table 6-34 Router User Unable to Initiate Shell Session with Router

Problem	Suggested Diagnostic Steps
Lack of service=shell AVP; user sees “Authorization failed service” error message.	<p>To view user profile for inclusion of service=shell AVP, enter:</p> <pre><CSUser>\$/opt/ciscosecure/utlils/bin/ViewProfile -p 9900 -u username</pre>

Table 6-35 AVPs Not Working on Console Port

Problem	Suggested Diagnostic Steps
Feature is not supported on console ports.	None. Feature not supported.

6.4 Troubleshooting Scenarios

The following example troubleshooting scenarios elaborate the process of diagnosing, correcting, and testing several problems addressed in “6.3 AAA Troubleshooting Basics”:

- 6.4.1 Isolating Incorrect TACACS+ Key in NAS or AAA Server (TACACS+ Dial-Based Server Authentication)
- 6.4.2 Isolating Invalid User Password (TACACS+ Dial-Based Server Authentication)
- 6.4.3 Isolating Non-Existent User (TACACS+ Dial-Based Server Authentication)
- 6.4.4 Isolating Missing PPP Service Definition (TACACS+ Dial-Based Server Authorization)
- 6.4.5 Isolating Defined AVPs not Being Assigned (TACACS+ Dial-Based Server Authorization)
- 6.4.6 Isolating Missing Shell Service Definition (TACACS+ Dial-Based Server Authorization)
- 6.4.7 Isolating Incorrect PPP Reply Attributes (RADIUS Dial-Based Server Authorization)

6.4.1 Isolating Incorrect TACACS+ Key in NAS or AAA Server (TACACS+ Dial-Based Server Authentication)

This scenario focuses on a server-authentication failure for a dial-based connection and provides a statement of a symptom, suggests a specific problem, and summarizes diagnostic steps. Diagnostics include output from relevant **debug** commands and other troubleshooting tools. See Table 6-4 for additional related problems.

Symptom Multiple user failure; all dial-in users unable to connect to NAS. See Table 6-4.

Possible Cause TACACS+ key incorrect in NAS or AAA server. See Table 6-4.

Action Complete troubleshooting steps to isolate and resolve this possible cause.

Step 1 Gather general **debug** command information from the NAS. The following output is from a **debug aaa authentication** command executed on a NAS. The last line of this **debug** output shows the failure expressed for user *dial_tac*.

```
088189: Jan 27 18:37:22.972 CST: AAA/MEMORY: create_user (0x61D7A2E0) user='' ruser=''
port='tty51' rem_addr='172.22.2.3' authen_type=ASCII service=LOGIN priv=1
088190: Jan 27 18:37:22.976 CST: AAA/AUTHEN/START (953379418): port='tty51' list= =30356
25154
088203: Jan 27 18:37:26.216 CST: TAC+: ver=192 id=3035625154 received AUTHEN status =
GETPASS
088204: Jan 27 18:37:26.216 CST: AAA/AUTHEN (3035625154): status = GETPASS
088205: Jan 27 18:37:30.337 CST: AAA/AUTHEN/CONT (3035625154): continue_login
(user='dial_tac')
088206: Jan 27 18:37:30.337 CST: AAA/AUTHEN (3035625154): status = GETPASS
088207: Jan 27 18:37:30.337 CST: AAA/AUTHEN (3035625154): Method=ADMIN (tacacs+)
088208: Jan 27 18:37:30.337 CST: TAC+: send AUTHEN/CONT packet id=3035625154
088209: Jan 27 18:37:30.637 CST: TAC+: ver=192 id=3035625154 received AUTHEN status =
FAIL
```

Step 2 Enter the following command to assess warnings and errors reported in the AAA server log file:

```
<CSUserver>$tail -f /var/log/csuslog
```

The AAA server log file reports the following warning when no key is specified (indicating that there is no encryption key):

```
Jan 27 18:35:17 coachella CiscoSecure: WARNING - Insecure configuration: No encryption
key for NAS <default>
```

Step 3 Review NAS configurations for shared secret configuration. To obtain the NAS configuration, enter:

```
<NAS>#show running-config
```

The following configuration fragment specifies the TACACS+ server and key. In this case, the key is *bobbit*.

```
tacacs-server host 172.22.53.201 key bobbit
```

Review the AAA server configuration for the corresponding server shared secret configuration. View the CSU.cfg file with **vi** (or a similar tool):

```
<CSUserver>$vi /opt/ciscosecure/config/CSU.cfg
```

Find the key configuration in the *CSU.cfg* AAA server configuration file and review it for the NAS specification. In this example, this configuration is missing.

```
NAS config_nas_config =
    {
        {
            "172.22.53.201",
            "",
```

If the key is properly configured, it appears between the quotation marks following the IP address specification. In this case, the key is missing. Because it is not specified in the AAA server configuration file, users' access is blocked.

Step 4 Update key specifications and restart the AAA server. Verify successful dialup operation.

6.4.2 Isolating Invalid User Password (TACACS+ Dial-Based Server Authentication)

This scenario focuses on a server-authentication failure for a dial-based connection and provides a statement of a symptom, suggests a specific problem, and summarizes diagnostic steps. Diagnostics include output from relevant **debug** commands and other troubleshooting tools. See Table 6-3 for additional related problems.

Symptom Single user failure; individual dial-in user unable to connect to NAS. See Table 6-3.

Possible Cause User enters invalid password. See Table 6-3.

Action Complete troubleshooting steps to isolate and resolve this possible cause.

Step 1 Gather general **debug** command information from the NAS. The following output is from a **debug aaa authentication** command executed on a NAS. This command results in a stream of diagnostic output.

The last line in the following output shows the AAA authentication request sent to AAA server for user *dial_tac*:

```
092852: Jan 27 22:19:06.713 CST: AAA/AUTHEN (543609479): status = GETPASS
092853: Jan 27 22:19:07.985 CST: AAA/AUTHEN/CONT (543609479): continue_login
(user='dial_tac')
```

The NAS receives FAIL from AAA server for user:

```
092854: Jan 27 22:19:07.985 CST: AAA/AUTHEN (543609479): status = GETPASS
092855: Jan 27 22:19:07.985 CST: AAA/AUTHEN (543609479): Method=ADMIN (tacacs+)
092856: Jan 27 22:19:07.985 CST: TAC+: send AUTHEN/CONT packet id=543609479
092857: Jan 27 22:19:08.185 CST: TAC+: ver=192 id=543609479 received AUTHEN status = FAIL
092858: Jan 27 22:19:08.185 CST: AAA/AUTHEN (543609479): status = FAIL
```

The user session is torn down and AAA process is freed:

```
092859: Jan 27 22:19:10.185 CST: AAA/MEMORY: free_user (0x61D87A70) user='dial_tac'
ruser='' port='tty51' rem_addr='172.22.2.3' authen_type=ASCII service=LOGIN
priv=1
```

Step 2 Enter the **tail** command to assess warning and errors reported in the AAA server log file:

```
<CSUserver>$tail -f /var/log/csuslog
```

In this case, the AAA server log reports an incorrect password for user *dial_tac*:

```
Jan 27 22:19:08 coachella CiscoSecure: NOTICE - Authentication - Incorrect password; [NAS
= 172.22.63.1, Port = tty51, User = dial_tac, Service = 1, Priv = 1]
Jan 27 22:19:08 coachella CiscoSecure: INFO - Profile: user = dial_tac {
Jan 27 22:19:08 coachella set server current-failed-logins = 1
```



Note Following the failure, the **current-failed-login** counter increments. This counter is described in Table 6-3.

Step 3 If the user does not exist in the database (but should), create a new user, or provide feedback if password or login were entered incorrectly by the user.

6.4.3 Isolating Non-Existent User (TACACS+ Dial-Based Server Authentication)

This scenario focuses on a server-authentication failure for a dial-based connection and provides a statement of a symptom, suggests a specific problem, and summarizes diagnostic steps. Diagnostics include output from relevant **debug** commands and other troubleshooting tools. See Table 6-3 for additional related problems.

Symptom Single user failure; individual dial-in user unable to connect to NAS. See Table 6-3.

Possible Cause User does not exist in the database. See Table 6-3.

Action Complete troubleshooting steps to isolate and resolve this possible cause.

Step 1 Gather general **debug** command information from the NAS. The following output is from a **debug aaa authentication** command executed on a NAS.

The following output fragment shows the AAA process starting on NAS.

```
092794: Jan 27 22:15:39.132 CST: AAA/MEMORY: create_user (0x61D87A70) user='' ruser=''
port='tty51' rem_addr='172.22.2.3' authen_type=ASCII service=LOGIN priv=1
092795: Jan 27 22:15:39.132 CST: AAA/AUTHEN/START (3576082779): port='tty51'
list='INSIDE' action=LOGIN service=LOGIN
```

GETPASS is sent to AAA server for verification for user *dial_test*:

```
092806: Jan 27 22:15:41.132 CST: AAA/AUTHEN/START (3285027777): Method=ADMIN (tacacs+)
092807: Jan 27 22:15:41.132 CST: TAC+: send AUTHEN/START packet ver=192 id=32850=27777
092808: Jan 27 22:15:41.936 CST: TAC+: ver=192 id=3285027777 received AUTHEN status =
GETPASS
092809: Jan 27 22:15:41.936 CST: AAA/AUTHEN (3285027777): status = GETPASS
092810: Jan 27 22:15:43.340 CST: AAA/AUTHEN/CONT (3285027777): continue_login
(user='dial_test')
092811: Jan 27 22:15:43.340 CST: AAA/AUTHEN (3285027777): status = GETPASS
092812: Jan 27 22:15:43.340 CST: AAA/AUTHEN (3285027777): Method=ADMIN (tacacs+)
```

The NAS then receives the authentication FAIL message from the AAA server:

```
092813: Jan 27 22:15:43.340 CST: TAC+: send AUTHEN/CONT packet id=3285027777
092814: Jan 27 22:15:43.540 CST: TAC+: ver=192 id=3285027777 received AUTHEN status =
FAIL
092815: Jan 27 22:15:43.540 CST: AAA/AUTHEN (3285027777): status = FAIL
```

The session is torn down and AAA process is freed:

```
092816: Jan 27 22:15:45.540 CST: AAA/MEMORY: free_user (0x61D87A70) user='dial_test'
ruser='' port='tty51' rem_addr='172.22.2.3' authen_type=ASCII service=LOGIN priv=1
092817: Jan 27 22:15:45.540 CST: AAA: parse name=tty51 idb type=-1 tty=-1
092818: Jan 27 22:15:45.540 CST: AAA: name=tty51 flags=0x11 type=5 shelf=0 slot
```

Step 2 Enter the following command to assess warning and errors reported in the AAA server log file:

```
<CSUser>$tail -f /var/log/csuslog
```

AAA server log file shows that the AAA server did not find user *dial_test* in cache (profile caching is enabled):

```
Jan 27 22:15:41 coachella CiscoSecure: DEBUG - Profile USER = dial_test not found in
cache.
```

The AAA server log file also shows that AAA server did not find user in the database; next, the AAA server conducts a search for the *unknown_user* account:

```
Jan 27 22:15:41 coachella CiscoSecure: WARNING - User dial_test not found, using
unknown_user
```

AAA server finally again reports user not found after exhausting its search:

```
Jan 27 22:15:41 coachella CiscoSecure: DEBUG - Password:
Jan 27 22:15:43 coachella CiscoSecure: DEBUG - AUTHENTICATION CONTINUE request (c3cd8bc1)
Jan 27 22:15:43 coachella CiscoSecure: DEBUG - Authentication - User not found;
[NAS = 172.22.63.1, Port = tty51, User = dial_test, Service = 1]
```

Step 3 Enter the following command to view a user profile in the database:

```
<CSUser>$ /opt/ciscosecure/CLI/ViewProfile -p 9900 -u dial_test
Error: Unable to find profile
RC = 3
```

- Step 4** If the user does not exist in the database (but should), create a new user, or provide feedback if password or login were entered incorrectly by the user.
-

6.4.4 Isolating Missing PPP Service Definition (TACACS+ Dial-Based Server Authorization)

This scenario focuses on a server-authorization failure for a dial-based connection and provides a statement of a symptom, suggests a specific problem, and summarizes diagnostic steps. Diagnostics include output from relevant **debug** commands and other troubleshooting tools. See Table 6-9 for additional related problems.

Symptom Multiple users cannot start PPP. See Table 6-9.

Possible Cause Group does not have **service=ppp** AVP assigned. See Table 6-9.

Action Complete troubleshooting steps to isolate and resolve this possible cause.

- Step 1** Gather general **debug** command information from the NAS. The following output is from a **debug aaa authentication** command executed on a NAS. The following output fragment shows the PPP service authorization request being initiated for user *dial_tac*; then, being denied by the AAA server:

```
111802: Feb  3 20:48:53.015 CST: As2 AAA/AUTHOR/LCP (153050196): send AV service=ppp
111803: Feb  3 20:48:53.015 CST: As2 AAA/AUTHOR/LCP (153050196): send AV protocol=lcp
111804: Feb  3 20:48:53.015 CST: As2 AAA/AUTHOR/LCP (153050196): found list "default"
111805: Feb  3 20:48:53.015 CST: As2 AAA/AUTHOR/LCP (153050196): Method=tacacs+(tacacs+)
111806: Feb  3 20:48:53.015 CST: AAA/AUTHOR/TAC+: (153050196): user=dial_tac
111807: Feb  3 20:48:53.015 CST: AAA/AUTHOR/TAC+: (153050196): send AV service=ppp
111808: Feb  3 20:48:53.015 CST: AAA/AUTHOR/TAC+: (153050196): send AV protocol=lcp
111809: Feb  3 20:48:53.219 CST: As2 AAA/AUTHOR (153050196): Post authorization status = FAIL
111810: Feb  3 20:48:53.219 CST: As2 AAA/AUTHOR/LCP: Denied
```

- Step 2** Enter the following command to assess warning and errors reported in the AAA server log file:

```
<CSUserver>$tail -f /var/log/csuslog
```

AAA server log file shows that the AAA server successfully authenticated the user, but that the PPP service request was denied due to an authorization failure:

```
Feb  3 20:48:58 coachella CiscoSecure: DEBUG - Authentication - LOGIN successful; [NAS = 172.22.63.1, Port = Async2, User = dial_tac, Priv = 1]
Feb  3 20:48:58 coachella CiscoSecure: DEBUG - AUTHORIZATION request (468d69de)
Feb  3 20:48:58 coachella CiscoSecure: DEBUG - Authorization - Failed service; [NAS = 172.22.63.1, user = dial_tac, port = Async2, input: service=ppp protocol=lcp output: ]
```

- Step 3** Add **service=ppp** and related AVPs **protocol=ip** and **protocol=lcp**.
-

6.4.5 Isolating Defined AVPs not Being Assigned (TACACS+ Dial-Based Server Authorization)

This scenario focuses on a server-authorization failure for a dial-based connection and provides a statement of a symptom, suggests a specific problem, and summarizes diagnostic steps. Diagnostics include output from relevant **debug** commands and other troubleshooting tools. See Table 6-10 for additional related problems.

Symptom Network authorization fails. See Table 6-10.

Possible Cause AVPs not assigned. See Table 6-10.

Action Complete troubleshooting steps to isolate and resolve this possible cause.

Step 1 Review the group profile. In this case, the group profile shows **inacl=110** is assigned to the *aaa_test_group* profile:

```
<CSUserver>$/opt/ciscosecure/CLI/ViewProfile -p 9900 -g aaa_test_group
Group Profile Information
group = aaa_test_group{
  profile_id = 64
  profile_cycle = 7
  service=ppp {
  protocol=ip {
  inacl=110
  }
  protocol=lcp {
  }
  }
}
```

Step 2 Gather general **debug** command information from the NAS. The following output is from a **debug aaa authentication** command executed on a NAS. The following output fragment shows that no AAA authorization for **service=net** taking place.

```
112037: Feb  3 21:18:04.994 CST: AAA/MEMORY: create_user (0x61DF0AE8) user='dial_tac'
ruser='' port='Async5' rem_addr='async/81560' authen_type=PAP service=PPP priv=1
```

Step 3 Enter the following command to assess warning and errors reported in the AAA server log file:

```
<CSUserver>$tail -f /var/log/csuslog
```

The following log file fragment confirms that access is permitted with no AAA authentication.

```
Feb  3 21:18:05 coachella CiscoSecure: DEBUG - Authentication - LOGIN successful; [NAS =
172.22.63.1, Port = Async5, User = dial_tac, Priv = 1]
Feb  3 21:18:05 coachella CiscoSecure: INFO - Profile: user = dial_tac {
Feb  3 21:18:05 coachella          set server current-failed-logins = 0
Feb  3 21:18:05 coachella profile_cycle = 12
Feb  3 21:18:05 coachella }
```

Step 4 Add **aaa authorization network default group tacacs+** global command to the NAS configuration.

6.4.6 Isolating Missing Shell Service Definition (TACACS+ Dial-Based Server Authorization)

This scenario focuses on a server-authorization failure for a dial-based connection and provides a statement of a symptom, suggests a specific problem, and summarizes diagnostic steps. Diagnostics include output from relevant **debug** commands and other troubleshooting tools. See Table 6-16 for additional related problems.

Symptom No EXEC shell (terminal window after dial). See Table 6-16.

Possible Cause User or group does not have **service=shell** AVP assigned. See Table 6-16.

Action Complete troubleshooting steps to isolate and resolve this possible cause.

- Step 1** Gather general **debug** command information from the NAS. The following output is from a **debug aaa authentication** command executed on a NAS. The following output fragment shows the request sent to AAA server to start **service=shell**:

```
092730: Jan 27 21:57:41.355 CST: tty52 AAA/AUTHOR/EXEC (3818889333): Port='tty52'
list='INSIDE' service=EXEC
092738: Jan 27 21:57:41.355 CST: tty52 AAA/AUTHOR/EXEC (3818889333): Method=ADMIN
(tacacs+)
092739: Jan 27 21:57:41.355 CST: AAA/AUTHOR/TAC+: (3818889333): user=dial_tac
092740: Jan 27 21:57:41.355 CST: AAA/AUTHOR/TAC+: (3818889333): send AV service=shell
```

The following output fragments illustrate notification of the failure from AAA server for **service=shell**:

```
092741: Jan 27 21:57:41.355 CST: AAA/AUTHOR/TAC+: (3818889333): send AV cmd*
092742: Jan 27 21:57:41.559 CST: AAA/AUTHOR (3818889333): Post authorization status =
FAIL
```

The following fragment illustrates the Authorization FAILED message being detected by the **debug aaa authentication** process:

```
092743: Jan 27 21:57:41.559 CST: AAA/AUTHOR/EXEC: Authorization FAILED
092744: Jan 27 21:57:43.559 CST: AAA/MEMORY: free_user (0x61D87A70) user='dial_tac'
ruser='' port='tty52' rem_addr='172.22.2.3' authen_type=ASCII service=LOGIN priv=1
```

- Step 2** Enter the following command to assess warning and errors reported in the AAA server log file:

```
<CSUserver>$tail -f /var/log/csuslog
```

In this case, the authentication succeeds for user *dial_tac*, as illustrated in the following *csuslog* file fragment:

```
Jan 27 21:57:40 coachella CiscoSecure: DEBUG - Authentication - LOGIN successful; [NAS =
172.22.63.1, Port = tty52, User = dial_tac, Priv = 1]
```

However, the *csuslog* file also shows that the authorization failed service for user *dial_tac* because the **service=shell** AVP is not assigned:

```
Jan 27 21:57:40 coachella CiscoSecure: DEBUG -
Jan 27 21:57:41 coachella CiscoSecure: DEBUG - AUTHORIZATION request (e39fa075)
Jan 27 21:57:41 coachella CiscoSecure: DEBUG - Authorization - Failed service; [NAS =
172.22.63.1, user = dial_tac, port = tty52, input: service=shell cmd* output: ]
```

- Step 3** Enter the following command to review the user profile. This profile shows that the AVP **service=shell** is not assigned to user *dial_tac*:

```
<CSUser>$ /opt/ciscosecure/CLI/ViewProfile -p 9900 -u dial_tac
User Profile Information
user = dial_tac{
profile_id = 63
profile_cycle = 4
member = aaa_test_group
password = des "*****"
password = pap "*****"
}
```

- Step 4** Assign **service=shell** AVP.

6.4.7 Isolating Incorrect PPP Reply Attributes (RADIUS Dial-Based Server Authorization)

This scenario focuses on a server-authorization failure for a dial-based connection using the RADIUS protocol and provides a statement of a symptom, suggests a specific problem, and summarizes diagnostic steps. Diagnostics include output from relevant **debug** commands and other troubleshooting tools. See Table 6-9 for additional related problems.

Symptom PPP session is not established. See Table 6-9.

Possible Cause User or group does not have correct PPP reply attributes. See Table 6-9.

Action Complete troubleshooting steps to isolate and resolve this possible cause.

- Step 1** Gather general **debug** command information from the NAS. The following output is from a **debug aaa authentication** command executed on a NAS. The following fragment illustrates the Authorization FAILED message being detected by the **debug aaa authentication** process:

```
*Apr  5 23:12:28.228: AAA/AUTHOR/EXEC: Authorization FAILED
*Apr  5 23:12:30.228: AAA/MEMORY: free_user (0x612311BC) user='rad_dial' ruser=''
port='tty4' rem_addr='408/3241933' authen_type=ASCII service=LOGIN priv=1
*Apr  5 23:12:30.936: %ISDN-6-DISCONNECT: Interface Serial0:0 disconnected from unknown
, call lasted 61 seconds
*Apr  5 23:12:30.980: %LINK-3-UPDOWN: Interface Serial0:0, changed state to down
```

- Step 2** Enter the **tail** command to assess warning and errors reported in the AAA server log file:

```
<CSUser>$ tail -f /var/log/csuslog
```

In this case, the authorization fails for user *rad_dial*, as illustrated in the following *csuslog* file fragment:

```
Apr  6 15:14:03 sleddog CiscoSecure: INFO - RADIUS: Servicing requests from NAS
(172.23.84.35), sending host <172.23.84.35>
```

However, the csuslog file also shows that the authorization failed service for user *dial_tac* because the **service=shell** AVP is not assigned:

```
Jan 27 21:57:40 coachella CiscoSecure: DEBUG -  
Jan 27 21:57:41 coachella CiscoSecure: DEBUG - AUTHORIZATION request (e39fa075)  
Jan 27 21:57:41 coachella CiscoSecure: DEBUG - Authorization - Failed service; [NAS =  
172.22.63.1, user = dial_tac, port = tty52, input: service=shell cmd* output: ]
```

Step 3 Enter the following command to view a user profile in the database:

```
<CSUserver>$/opt/ciscosecure/CLI/ViewProfile -p 9900 -u rad_dial
```

```
User Profile Information  
user = rad_dial{  
profile_id = 23  
set server current-failed-logins = 0  
profile_cycle = 4  
password = pap "*****"  
radius=Cisco {  
reply_attributes= {  
7=1  
9,1="ip:inacl=110"  
}  
}  
}
```



Note In this profile, the missing reply_attribute is **6=2**.

Step 4 Add the following RADIUS AVP: **Frame-Protocol=ppp** (entered as **6=2** in **AddProfile** command input).
