



Cisco AAA Case Study Overview

This chapter summarizes the technology behind AAA security solutions, outlines typical network definitions and network assumptions adopted for this case study, and lists tasks associated with implementing, verifying, and troubleshooting the AAA environment presented. Specific sections provided here are:

- 1.1 AAA Technology Summary
- 1.2 TACACS+ Overview
- 1.3 RADIUS Overview
- 1.4 Comparison of TACACS+ and RADIUS
- 1.5 Differences in Implementing Local and Server AAA
- 1.6 Scenario Description
- 1.7 Planning Your Network
- 1.8 Network Service Definitions
- 1.9 Security Implementation Policy Considerations
- 1.10 Network Equipment Selection
- 1.11 Task Check List

1.1 AAA Technology Summary

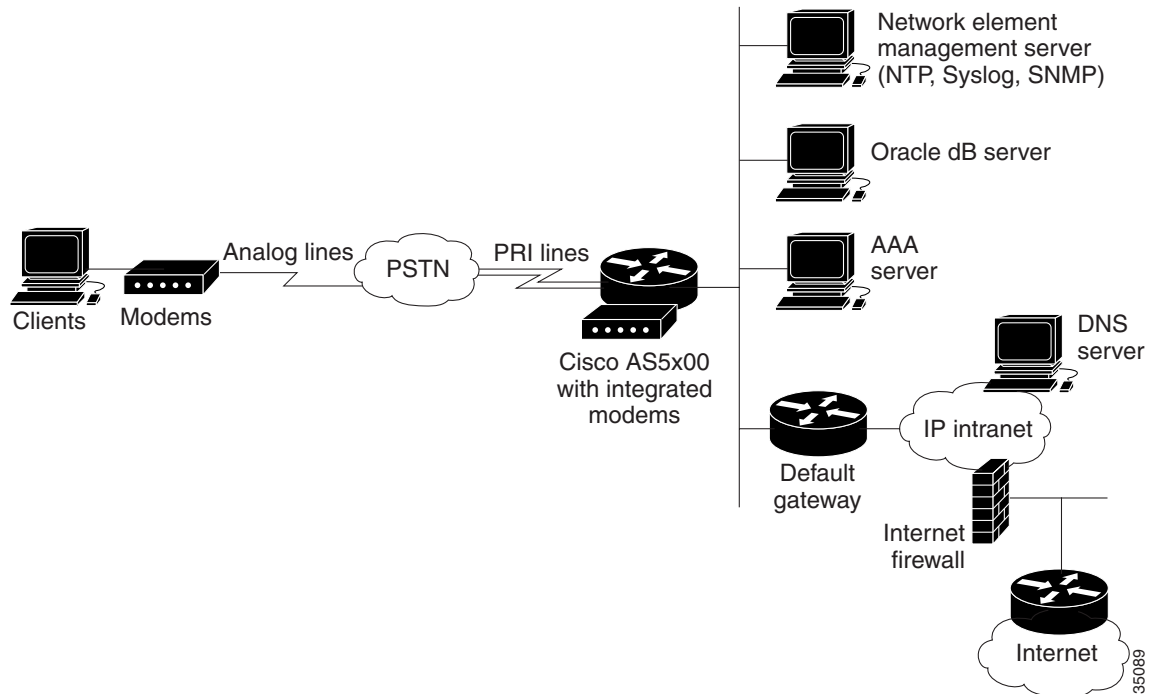
Dial access presents a challenge to network managers entrusted with network security. This case study illustrates essential steps in planning and implementing authentication, authorization, and accounting (AAA) technologies based on Cisco product capabilities.

For the purposes of this case study, the following generic definitions apply:

- *Authentication:* The process of validating the claimed identity of an end user or a device, such as a host, server, switch, router, and so on.
- *Authorization:* The act of granting access rights to a user, groups of users, system, or a process.
- *Accounting:* The methods to establish who, or what, performed a certain action, such as tracking user connection and logging system users.

Figure 1-1 illustrates a generalized view of a Cisco-based AAA environment, featuring a network access server (NAS) and AAA server. This basic arrangement forms the foundation for this case study.

Figure 1-1 AAA-Based, Secure Network Access Scenario



In the context of the Cisco-based AAA environment addressed here, the key operational elements are network access servers (NASs), routers, and CiscoSecure Access Control Server for UNIX servers (referred to in this document as *AAA servers*). Depending on the conventions and requirements of your particular design, you can select a security environment which utilizes *Terminal Access Controller Access Control System Plus (TACACS+)* or *Remote Authentication Dial-in User Service (RADIUS)*. This case study addresses implementation of both environments.

1.1.1 AAA RFC References

Requests for Comments (RFCs) play a crucial role in defining the behavior of devices in complex networking environments. The following RFCs are useful references for TACACS+ and RADIUS:

- TACACS+: <http://www.cisco.com/warp/public/459/tac-rfc.1.76.txt>
- TACACS: <http://www.ietf.org/rfc/rfc1492.txt>
- MD5: <http://www.ietf.org/rfc/rfc1321.txt>
- RADIUS: <http://www.ietf.org/rfc/rfc2138.txt>

1.2 TACACS+ Overview

Key TACACS+ features:

- TACACS+ separates AAA into three distinct functions (Authentication, Authorization and Accounting).
- TACACS+ supports router command authorization integration with advanced authentication mechanisms, such as Data Encryption Standard (DES) and One-Time Password (OTP) key.
- TACACS+ supports 16 different privilege levels (0-15).

- TACACS+ permits the control of services, such as Point-to-Point Protocol (PPP), shell, standard log in, enable, AppleTalk Remote Access (ARA) protocol, Novell Asynchronous Services Interface (NASI), remote command (RCMD), and firewall proxy.
- TACACS+ permits the blocking of services to a specific port, such as a TTY or VTY interface on a router.

The most common services supported by TACACS+ are PPP for IP and router EXEC shell access using console or VTY ports. EXEC shell allows users to connect to router shells and select services, such as PPP, Telnet, TN3270, or manage the router itself.

Many TACACS+ servers are available on the market today; however, the AAA server is designed specifically to be scalable and compatible with Cisco's broad line of routers, access servers, and switches. Hence, this case utilizes the Cisco AAA server as the TACACS+ server of choice.

When configured correctly, the AAA server validates AAA and responds to requests from routers and access servers with a pass or fail signal. The AAA server contains an internal database sized to 5000 users; therefore, an external Oracle database is used in our case study for user account attributes and billing information.

The AAA server acts as a proxy server by using TACACS+ to authenticate, authorize, and account for access to Cisco routers and network access servers.

1.3 RADIUS Overview

The RADIUS protocol was developed by Livingston Enterprises, Inc., as an access server authentication and accounting protocol. The RADIUS specification (RFC 2138) is a proposed standard protocol and RADIUS accounting standard (RFC 2139) is informational.

Although TACACS+ is considered to be more versatile, RADIUS is the AAA protocol of choice for enterprise ISPs because it uses fewer CPU cycles and is less memory intensive.

Communication between a network access server (NAS) and a RADIUS server is based on the User Datagram Protocol (UDP). Generally, the RADIUS protocol is considered a connectionless service. Issues related to server availability, retransmission, and timeouts are handled by the RADIUS-enabled devices rather than the transmission protocol.

RADIUS is a client/server protocol. The RADIUS client is typically a NAS and the RADIUS server is usually a daemon process running on a UNIX or Windows NT machine. The client passes user information to designated RADIUS servers and acts on the response that is returned. RADIUS servers receive user connection requests, authenticate the user, and then return the configuration information necessary for the client to deliver services to the user. A RADIUS server can act as a proxy client to other RADIUS servers or other kinds of authentication servers.

1.4 Comparison of TACACS+ and RADIUS

Table 1-1 summarizes the differences between RADIUS and TACACS+.

Table 1-1 Comparison of RADIUS and TACACS+

RADIUS	TACACS+
RADIUS uses UDP.	TACACS+ uses TCP.
RADIUS encrypts only the password in the access-request packet; less secure.	TACACS+ encrypts the entire body of the packet; more secure.
RADIUS combines authentication and authorization.	TACACS+ uses the AAA architecture, which separates authentication, authorization, and accounting.
Industry standard (created by Livingston).	Cisco Proprietary.
RADIUS does not support ARA access, Net BIOS Frame Protocol Control protocol, NASL, and X.25 PAD connections.	TACACS+ offers multiprotocol support.
RADIUS does not allow users to control which commands can be executed on a router.	TACACS+ provides two ways to control the authorization of router commands: on a per-user or per-group basis.

1.4.1 UDP and TCP

RADIUS uses UDP while TACACS+ uses TCP. TCP offers several advantages over UDP. TCP offers a connection-oriented transport, while UDP offers best effort delivery. RADIUS requires additional programmable variables, such as retransmit attempts and time-outs to compensate for best-effort transport, and it lacks the level of built-in support that reliable transport offers:

- Using TCP provides a separate acknowledgment that a request has been received, within (approximately) a network RTT, regardless of bandwidth. (TCP ACK).
- TCP provides immediate indication of a crashed (or not running) server (RST packets). You can determine when a server has crashed and come back up if you use long-lived TCP connections. UDP cannot tell the difference between a server that is out-of-service, slow, or non-existent server.
- By using TCP keepalives, you can detect server crashes out-of-band with actual requests. Connections to multiple servers can be maintained simultaneously, and you only need to send messages to the servers that are known to be up and running.
- TCP is more scalable than UDP.

1.4.2 Packet Encryption

RADIUS encrypts only the password in the access-request packet from the client to the server. The remainder of the packet is in the clear. Other information, such as username, authorized services, and accounting, can be captured by a third party.

RADIUS can use encrypted passwords by using the UNIX */etc/password* file; however, this process is slow because it involves a linear search of the file.

TACACS+ encrypts the entire body of the packet but leaves a standard TACACS+ header. Within the header is a field that indicates whether the body is encrypted or not. For debugging purposes, it is useful to have the body of the packets in the clear. However, normal operation fully encrypts the body of the packet for more secure communications.

1.4.3 Authentication and Authorization

RADIUS combines authentication and authorization. The access-accept packets sent by the RADIUS server to the client contain authorization information, making it difficult to decouple authentication and authorization.

TACACS+ uses the AAA architecture, which separates authentication, authorization, and accounting. This architecture allows separate authentication solutions that can still use TACACS+ for authorization and accounting. For example, with TACACS+, it is possible to use Kerberos authentication and TACACS+ authorization and accounting. After a NAS passes authentication on a Kerberos server, it requests authorization information from a TACACS+ server without having to re-authenticate the NAS by using the TACACS+ authentication mechanism. The NAS informs the TACACS+ server that it has successfully passed authentication on a Kerberos server, and the server then provides authorization information.

During a session, if additional authorization checking is needed, the access server checks with a TACACS+ server to determine if the user is granted permission to use a particular command. This provides greater control, compared to RADIUS, over the commands that can be executed on the access server while decoupling the authorization process from the authentication mechanism.

1.4.4 Multiprotocol Support

RADIUS does *not* support the following protocols (which are supported by TACACS+):

- AppleTalk Remote Access (ARA) protocol
- Net BIOS Frame Protocol Control protocol
- Novell Asynchronous Services Interface (NASI)
- X.25 PAD connection

1.4.5 Router Management

RADIUS does not allow users to control which commands can be executed on a router and which cannot; therefore, when compared with TACACS+, RADIUS is not as useful for router management and is not as flexible for terminal services.

TACACS+ provides two ways to control the authorization of router commands on a per-user or per-group basis. The first way is to assign privilege levels to commands and have the router verify with the TACACS+ server whether or not the user is authorized at the specified privilege level. The second way is to explicitly specify in the TACACS+ server, on a per-user or per-group basis, the commands that are allowed.

1.4.6 Interoperability

The RADIUS standard does not guarantee interoperability. Although several vendors implement RADIUS clients, this does not ensure they are interoperable. There are approximately 45 standard RADIUS ATTRIBUTES. Using standard ATTRIBUTES improves the likelihood of interoperability. Using proprietary extensions reduces interoperability.

1.4.7 Attribute-Value Pairs (AVPs)

Throughout this case study, implementation tasks and diagnostic procedures refer to *attribute-value pairs* (AVPs). Each AVP consists of a type identifier associated with one or more assignable values. AVPs specified in user and group profiles define the authentication and authorization characteristics for their respective users and groups. TACACS+ and RADIUS implement an array of AVPs, each with separate type definitions and characteristics. Table 1-2 and Table 1-3 illustrate several typical AVPs.

Table 1-2 Examples of RADIUS AVPs

Attribute	Type of Value
User-Name	String
Password	String
CHAP-Password	String
Client-Id	IP address
Login-Host	IP address
Login-Service	Integer
Login-TCP-Port	Integer

Table 1-3 Examples of TACACS+ AVPs

Attribute	Type of Value
Inacl	Integer
Addr-pool	String
Addr	IP address
Idletime	Integer
protocol	Keyword
timeout	Integer
Outacl	Integer

1.5 Differences in Implementing Local and Server AAA

AAA requirements differ between local-based and server-based environments. Throughout this case study, procedures and examples refer to scenarios based on this important distinction.

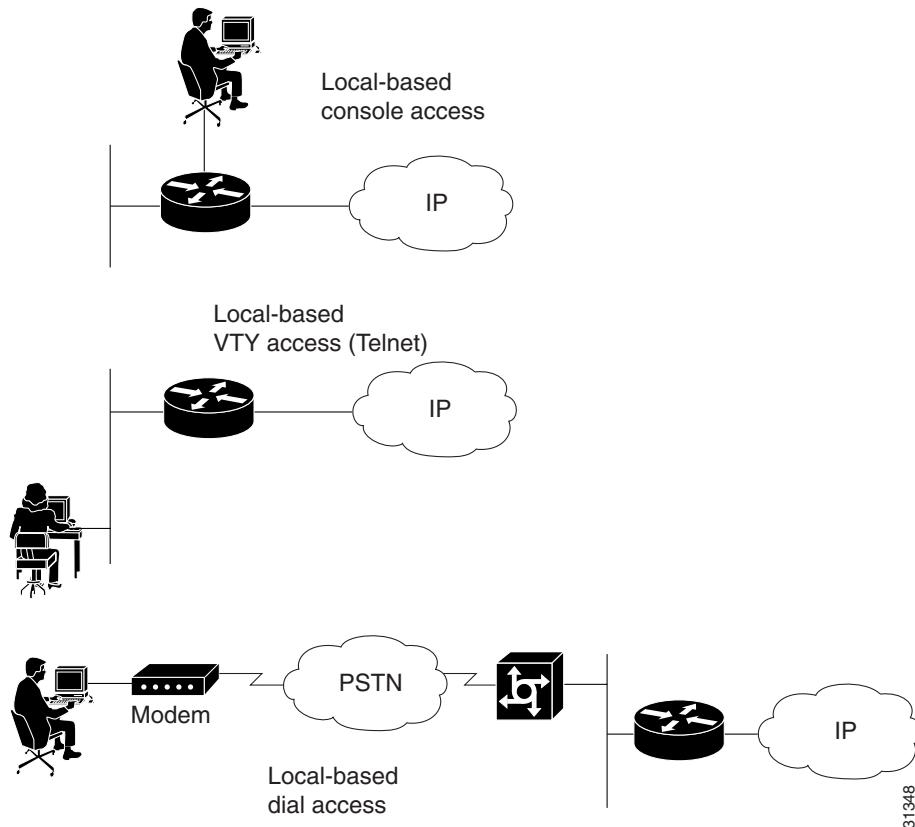
In *local-based* AAA access, users are permitted or denied access based on local AAA IOS account configuration. For the purposes of this case study, local-based AAA access features these attributes:

- User accounts are stored in router or NAS configurations.
- AVPs only are supported from EXEC shell terminal access.
- Limited set of AVPs are supported.
- AAA negotiation is performed internally by the Cisco IOS and is not protocol specific.

Figure 1-2 illustrates three local-based connectivity situations to consider:

- Local-based console access
- Local-based virtual terminal type (VTY) connections
- Local-based dial access

Figure 1-2 Local-Based Access Options



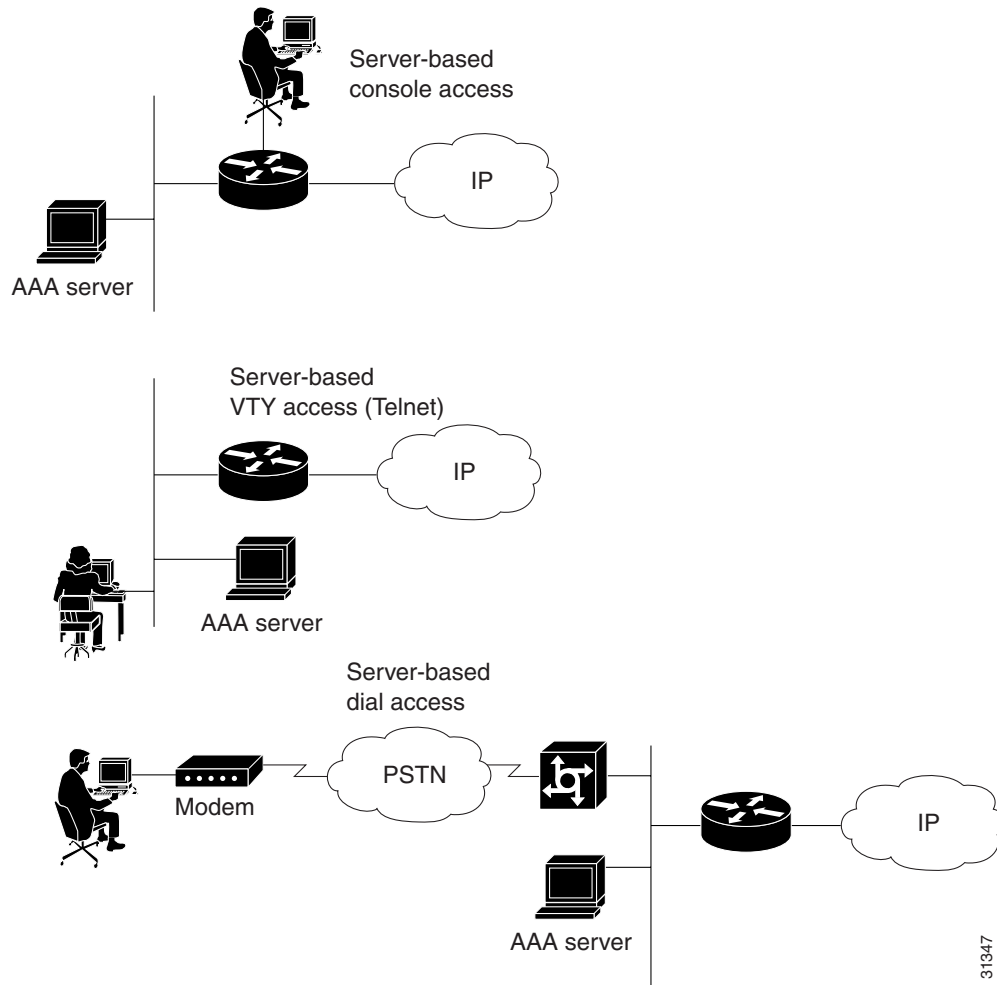
In *server-based* AAA access, users and groups are permitted or denied access based on AAA negotiations between a router or NAS and the AAA server. See the following attributes of server-based AAA access features:

- User or group profiles and accounting records stored in an internal or external database
- AVPs supported on both standard and EXEC shell-initiated PPP sessions
- Wide array of AVPs supported, including vendor-specific (non-Cisco) AVPs

Figure 1-3 illustrates the three server-based connectivity situations:

- Server-based console access
- Server-based VTY connections
- Server-based dial access

Figure 1-3 Server-Based Access Options



31347

Each connectivity scenario illustrated in Figure 1-2 and Figure 1-3 involves situation-specific requirements. As a result, each scenario also contains situation-specific implementation and troubleshooting considerations. The diagnostic chapters that follow present a series of implementation steps (configuring, verifying, and testing) symptoms, problems, and suggested diagnostic processes that reflect both these differences and similarities.

1.6 Scenario Description

The baseline network environment for a hypothetical access network scenario is used as a foundation for assessing the application of various security and management features available from Cisco. Figure 1-1 (presented in “1.1 AAA Technology Summary”) illustrates the underlying network environment and relationship between AAA components. The high-level AAA objectives:

- Enable secure dialup service to access an intranet and the Internet by using the public switched telephone network (PSTN).
- Build a manageable, redundant, and secure access strategy that supports large dialup access implementations.
- Provide versatile means of controlling administrative access to routers.

- Account for configuration changes in routers.

1.7 Planning Your Network

A network design engineer meets with each company to complete the following tasks:

- Complete a needs assessment dial questionnaire.
- Create a user-network service definition.
- Recommend a network implementation and operation strategy.

The following tables present two checklists that were completed for this case study. Table 1-4 focuses on general networking issues. Table 1-5 focuses on AAA implementation issues. Both checklists apply to a hypothetical network referred to in this case as *Access Network*.

Table 1-4 General Service Definition Checklist

General Access Network Checklist Questions	Access Network Policy
What media do you want to use to provide dialup service?	Plain old telephone service (POTS) analog modems ISDN
How many dial-in users does the new equipment need to support over the next 3 months, 1 year, and 5 years?	3 months: 2000 users 1 Year: 5,000 users 5 Years: 10,000 users
What kind of remote nodes do you want to support?	Modems, terminal adapters, ISDN modems
When users connect to modems, what will they be allowed to do?	Support EXEC shell sessions (async terminal service) Support PPP sessions
Will you allow users to change their own passwords? If yes, how?	Yes EXEC shell (character-mode session)
What kind of dialup operating systems do you want to support?	Windows, UNIX, Macintosh
Do you want to support remote routers?	Asynch DDR or multiple B-channel access
Do you want to use an external authentication database such as Windows NT or Novel NDS?	Yes, Oracle
Do you want to support per user protocol and attribute definitions?	Yes
Do you want to support dial out?	No
Do you want to support PPP timeouts?	No
Do you want to work with an existing accounting system?	Yes
Do you have an existing network element server?	Yes

Table 1-5 AAA Service Definition Checklist

Access Network AAA Checklist Questions	Access Network Policy
What AAA protocols do you plan to deploy?	RADIUS and TACACS+
Where do you want the users' passwords to be stored?	External Oracle database
Do you plan to support one-time passwords? If so, what tool do you plan to use to support this requirement?	No
Do you intend to implement database replication?	No
Do you require support for token caching?	No
What type of accounts currently exist?	UNIX, NT
Do you plan to implement an AAA server? If so, on which product?	Yes, CiscoSecure for UNIX
What database do you plan to use?	External, Oracle

1.8 Network Service Definitions

Based on the checklist information provided in Table 1-4 and Table 1-5, the following service definitions (stated as *policies*) can be asserted for this environment.

Dialup and router shell access AAA requirements are characterized in the following sections:

- 1.8.1 Authentication Policy
- 1.8.2 Authorization Policy
- 1.8.3 Accounting Policy

1.8.1 Authentication Policy

Separate the authentication policy into two distinct sections: router administration and dialup PPP.

Policies relating to router administration involve creating support for the following two authentication elements:

- DES passwords stored in external database
- Local user if connection to AAA server is down

Policies relating to dialup PPP involve creating support for the following two authentication elements:

- Password Authentication Protocol (PAP) for dialup PPP authentication
- Challenge Handshake Authentication Protocol (CHAP) for remote ISDN devices

1.8.2 Authorization Policy

Separate the authorization policy into two distinct sections: router administration and dialup PPP.

Policies relating to router administration involve creating support for the following authorization elements:

- Privilege level 15 command authorization
- Three levels of router administration command control (low, medium, and high)
- Privilege level 15 assigned to local users, which is valid only if an AAA server is down

Policies relating to dialup PPP involve creating support for the following authorization elements:

- Apply **autocommand ppp negotiate** to all groups other than router administrators
- Access control list filtering as required
- AVP support for all dial access devices

1.8.3 Accounting Policy

Accounting records are exported from an Oracle database using SQL queries. Separate the accounting policy into two distinct sections: router administration and dialup PPP.

Policies relating to router administration involve creating support for the following accounting elements:

- Failed log in attempts
- Privilege level 15 commands
- Failed command authorization
- Start, stop, and elapsed times of sessions
- Source IP address of routers

Policies relating to dialup PPP involve creating support for the following accounting elements:

- Failed log in attempts
- Start, stop, and elapsed time of sessions
- Disconnect cause codes
- Caller ID if applicable

1.9 Security Implementation Policy Considerations

Table 1-6 present checklists summarizing the key security policy elements of this case.

Table 1-6 AAA Security Checklist

Access Network AAA Checklist Questions	Access Network Policy
What is the current security policy for passwords?	PAP for dial-in PPP users CHAP passwords for dialup routers DES passwords for router administrators
What services will be denied?	Concurrent sessions for dial-in users EXEC shell access for dial-in PPP users Access to specific hosts within the corporate intranetwork Access to specific network services, such as Telnet, FTP, and rlogin
What type of mechanism will exist if AAA server is down?	Local privilege level 15 account Authentication and authorization disabled on console port
Are local accounts allowed in routers and NASs?	Yes
What accounting information is required?	Username Privilege level of clients Session start and stop times Elapsed time Privilege level 15 command usage Configuration changes Failed log in attempts Failed command authorizations
What type of accounting mechanism will be used?	Customer written SQL query to Oracle database
Who is responsible for reviewing daily logs?	Network managers
Will users be allowed concurrent sessions?	Dialup PPP = No Dialup router = Yes Router administrator = Yes
What type of administrative access will be assigned to router administrators?	Full control assigned to senior router administrators Basic control assigned to junior router administrators Customized command control for mid-level router administrators
Support for Multilink?	Yes

In addition to these considerations, security-related attributes addressed in this case include:

- Per-User Static IP Address Policy—Static IP addresses are assigned to required personnel to access specific areas within the internetwork.
- Password Authentication and Command Authorization Policy—DES password support is segregated into two elements: privilege level and command authorization. Within that context, three levels of privilege are supported in this case: low, medium, and high, with high having full control assigned. Command authorization at privilege level 15 is enforced. A local user with privilege level 15 is used in the event that the connection to the AAA server is down.

1.10 Network Equipment Selection

Figure 1-1 (presented in “1.1 AAA Technology Summary”) shows the specific devices used in the dialup access environment. Based on the requirements detailed in Table 1-4, Table 1-5, and Table 1-6, the following network entities were selected for this case study:

- Remote clients using modems to access the IP intranet and IP Internet through the public switched telephone network (PSTN).
- An AAA server.
- An password authentication server.
- An external Oracle database server acts as the repository for all user profile information.
- An element management server performs basic dial access system management by using the network time protocol (NTP), system logs (syslog), and simple network management protocol (SNMP).
- A remote AAA server performs basic user authentication.
- A default gateway forwards packets to the IP intranet and IP Internet.

1.11 Task Check List

Table 1-7 summarizes AAA management implementation and operation activities for the hypothetical network in this case study. This case focuses on illustrating implementation of specific AAA-related security and management options over an Access Path implementation. Refer to *Cisco AS5x00 Case Study for Basic IP Modem Service* for specifics regarding commissioning Cisco access servers to support modem services at the following URL:

<http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/as5xipmo/index.htm>

Table 1-7 AAA Task Checklist

Task	Topic
Chapter 2, “Implementing the Local AAA Subsystem”	2.1 Implementing Local Dialup Authentication 2.2 Implementing Local Dialup Authorization 2.3 Implementing Local Router Authentication 2.4 Implementing Local Router Authorization 2.5 Implementing Local Router Accounting
Chapter 3, “Implementing Cisco AAA Servers”	3.1 Installing CiscoSecure for UNIX with Oracle
Chapter 4, “Implementing the Server-Based AAA Subsystem”	4.1 Implementing Server-Based TACACS+ Dialup Authentication 4.2 Implementing Server-Based TACACS+ Dialup Authorization 4.3 Implementing Server-Based RADIUS Dialup Authentication 4.4 Implementing Server-Based RADIUS Dialup Authorization 4.5 Implementing Server-Based TACACS+ Router Authentication 4.6 Implementing Server-Based TACACS+ Router Authorization

Table 1-7 AAA Task Checklist

Task	Topic
Chapter 5, “Implementing Server-Based AAA Accounting”	5.1 Implementing Server-Based RADIUS Dial Accounting 5.2 Implementing Server-Based TACACS+ Router Accounting
Chapter 6, “Diagnosing and Troubleshooting AAA Operations”	6.1 Overview of Authentication and Authorization Processes 6.2 Troubleshooting AAA Implementation <ul style="list-style-type: none">• 6.2.1 Troubleshooting Methodology Overview• 6.2.2 Cisco IOS Debug Command Summary 6.3 AAA Troubleshooting Basics 6.4 Troubleshooting Scenarios

