AAA Protocols

This section contains the following topics:

Typical Use Cases

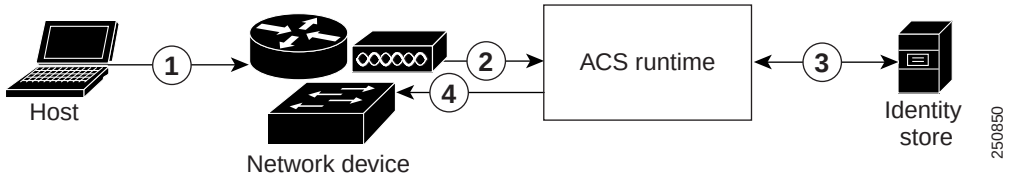
This section contains the following topics:

Device Administration (TACACS+)

Figure B-1 shows the flows associated with device administration. The two primary triggers are:

- Session Access Requests (Device Administration [TACACS+]), page B-1.
- Command Authorization Requests, page B-2.

Figure B-1 Device Administration Flow



Session Access Requests (Device Administration [TACACS+])

Note The numbers refer to Figure B-1Device Administration Flow, page B-1.

For session request:

Step 1 An administrator logs into a network device.

Step 2 The network device sends a TACACS+ access request to ACS.

Step 3 ACS uses an identity store to validate the user's credentials.

Step 4 ACS sends a TACACS+ response to the network device that applies the decision. The response includes parameters, such as the privilege level that determines the level of administrator access for the duration of the session.

Command Authorization Requests

Note The numbers refer to Figure B-1.

For command authorization:

Step 1 An administrator issues a command at a network device.

Step 2 The network device sends a TACACS+ access request to ACS.

Step 3 ACS optionally uses an identity store to retrieve user attributes for inclusion in policy processing.

Step 4 The TACACS+ response indicates whether the administrator is authorized to issue the command.

Network Access (RADIUS With and Without EAP)

For network access, a host connects to the network device and requests to use network resources. The network device identifies the newly connected host, and, using the RADIUS protocol as a transport mechanism, requests ACS to authenticate and authorize the user.

ACS 5.8.1 supports the following categories of network access flows, depending on the protocol that is transported over the RADIUS protocol:

- RADIUS-based protocols that do not include EAP:
  - PAP
  - CHAP
  - MSCHAPv1
  - MSCHAPv2

  For more information on RADIUS-based protocols that do not include EAP, see RADIUS-Based Flow Without EAP Authentication, page B-3.
- EAP family of protocols transported over RADIUS, which can be further classified as:
  - Simple EAP protocols that do not use certificates:

  EAP-MD5

  LEAP

– EAP protocols that involve a TLS handshake and in which the client uses the ACS server certificate to perform server authentication:

PEAP, using one of the following inner methods: PEAP/EAP-MSCHAPv2 and PEAP/EAP-GTC

EAP-FAST, using one of the following inner methods: EAP-FAST/EAP-MSCHAPv2 and EAP-FAST/EAP-GTC

– EAP protocols that are fully certificate-based, in which the TLS handshake uses certificates for both server and client authentication:

EAP-TLS

PEAP with inner method EAP-TLS

For more information on RADIUS-based flows with EAP authentication, see RADIUS-Based Flows with EAP Authentication, page B-3.

RADIUS-Based Flow Without EAP Authentication

This section describes RADIUS-based workflow without EAP authentication.

For RADIUS with PAP authentication:

Step 1 A host connects to a network device.

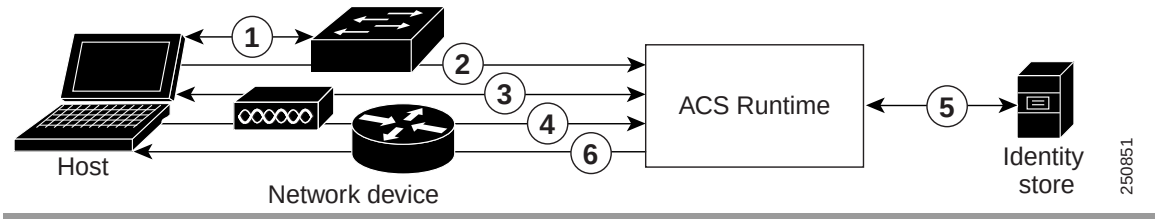
Step 2 The network device sends a RADIUS Access-Request to ACS, containing RADIUS attributes appropriate to the specific protocol that is being used (PAP, CHAP, MSCHAPv1, or MSCHAPv2).

Step 3 ACS uses an identity store to validate the user's credentials.

Step 4 The RADIUS response (Access-Accept or Access-Reject) is sent to the network device that will apply the decision.

Figure B-2 shows a RADIUS-based authentication without EAP.

Figure B-2 RADIUS-Based Flow Without EAP Authentication



RADIUS-Based Flows with EAP Authentication

EAP provides an extensible framework that supports a variety of authentication types. Among them, the specific EAP methods supported by ACS are:

- Simple EAP methods that do not use certificates:
  - EAP-MD5
  - LEAP
- EAP methods in which the client uses the ACS server certificate to perform server authentication:
  - PEAP/EAP-MSCHAPv2

  - PEAP/EAP-GTC
  - EAP-FAST/EAP-MSCHAPv2
  - EAP-FAST/EAP-GTC
- EAP methods that use certificates for both server and client authentication
  - EAP-TLS
  - PEAP/EAP-TLS

Whenever EAP is involved in the authentication process, it is preceded by an EAP negotiation phase to determine which specific EAP method (and inner method, if applicable) should be used.

For all EAP authentications:

Step 1 A host connects to a network device.

Step 2 The network device sends an EAP Request to the host.

Step 3 The host replies with an EAP Response to the network device.

Step 4 The network device encapsulates the EAP Response that it received from the host into a RADIUS Access-Request (using the EAP-Message RADIUS attribute) and sends the RADIUS Access-Request to ACS.

Step 5 ACS extracts the EAP Response from the RADIUS packet and creates a new EAP Request, encapsulates it into a RADIUS Access-Challenge (again, using the EAP-Message RADIUS attribute), and sends it to the network device.

Step 6 The network device extracts the EAP Request and sends it to the host.

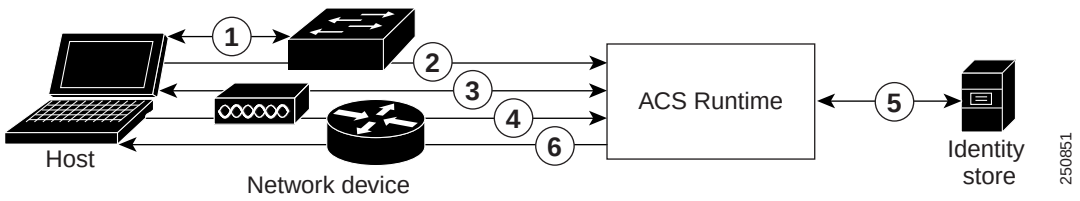
In this way, the host and ACS indirectly exchange EAP messages (transported over RADIUS and passed through the network device). The initial set of EAP messages that are exchanged in this manner negotiate the specific EAP method that will subsequently be used to perform the authentication.

The EAP messages that are subsequently exchanged are then used to carry the data needed to perform the actual authentication. If required by the specific EAP authentication method that is negotiated, ACS uses an identity store to validate the user's credentials.

After ACS determines whether the authentication should pass or fail, it sends either an EAP-Success or EAP-Failure message, encapsulated into a RADIUS Access-Accept or Access-Reject message to the network device (and ultimately also to the host).

Figure B-3 shows a RADIUS-based authentication with EAP.

Figure B-3 RADIUS-Based Authentication with EAP



For a list of known supplicant issues that might impact your ACS 5.8.1 experience, see *Release Notes for Cisco Secure Access Control System 5.8.1*.

Access Protocols—TACACS+ and RADIUS

This section contains the following topics:

ACS 5.8.1 can use the TACACS+ and RADIUS access protocols. Table B-1 compares the two protocols.

Table B-1 TACACS+ and RADIUS Protocol Comparison

Point of Comparison	TACACS+	RADIUS
Transmission Protocol	TCP—Connection-oriented transport-layer protocol, reliable full-duplex data transmission.	UDP—Connectionless transport-layer protocol, datagram exchange without acknowledgments or guaranteed delivery. UDP uses the IP to get a data unit (called a datagram) from one computer to another.
Ports Used	49	Authentication and Authorization: 1645 and 1812 Accounting: 1646 and 1813.
Encryption	Full packet-body encryption.	Encrypts only passwords up to 16 bytes.
AAA Architecture	Separate control of each service: authentication, authorization, and accounting.	Authentication and authorization combined as one service.
Intended Purpose	Device management.	User access control.

Overview of TACACS+

TACACS+ must be used if the network device is a Cisco device-management application, access server, router, or firewall. ACS 5.8.1 supports IPv6 addresses in TACACS+ protocols. ACS 5.8.1 supports Cisco device-management applications by providing command authorization for network users who are using the management application to configure managed network devices.

You provide support for command authorization for management application users by using unique command sets for each management application that is configured to use ACS for authorization.

ACS 5.8.1 uses TACACS+ to communicate with management applications. For a management application to communicate with ACS, you must configure the management application in ACS 5.8.1 as a AAA client that uses TACACS+.

You must also provide the device-management application with a valid administrator name and password. When a management application initially communicates with ACS, these requirements ensure the validity of the communication.

Except for the packet-headers, all information that the client and TACACS+ server communicate, which is contained in the packet-bodies are encrypted through the use of a shared secret (which is, itself, not sent over the network directly).

Additionally, the administrator that the management application uses must have the Command Set privilege enabled.

Overview of RADIUS

This section contains the following topics:

RADIUS is a client/server protocol through which remote access servers communicate with a central server to authenticate dial-in users, and authorize their access to the requested system or service. A company could use RADIUS to maintain user profiles in a central database that all remote servers can share.

This protocol provides better security, and the company can use it to set up a policy that is applied at a single administered network point.

To support the older and newer RFCs, ACS 5.8.1 accepts authentication requests on port 1645 and port 1812. For accounting, ACS accepts accounting packets on ports 1646 and 1813.

RADIUS IETF

ACS 5.8.1 provides a set of standard IETF RADIUS attributes with a set of predefined sub-attributes and values. You can not edit these RADIUS IETF attributes. You can use them in policy conditions. You can identify RADIUS IETF attributes that are currently unused by their names. These unused attributes are named in the following format: *attribute-nnn*, where *attribute* is the name of the attribute and *nnn* is the ID of the attribute.

In ACS 5.8.1, you have two new sub-attributes for the RADIUS IETF attribute “Service Type” and they are:

- **HP-Oper** and its ID is 252
- **HP-User** and its ID is 255

You can use these two sub-attributes in policy conditions. These two sub-attributes are specifically designed for the HP devices to understand permissions of the user.

RADIUS VSAs

ACS 5.8.1 supports RADIUS VSAs. The following set of predefined RADIUS VSAs are available after you install ACS 5.8.1:

- Cisco
- Cisco VPN 5000
- Microsoft
- US Robotics
- Ascend
- Nortel (Bay Networks)
- RedCreek
- Juniper

- Cisco VPN 3000
- Cisco Business Service Management (BSM)
- Cisco Aironet
- Cisco Airespace

You can modify these predefined RADIUS VSAs or define new RADIUS VSAs. You can create, edit, and duplicate RADIUS VSAs. For more information, see Creating, Duplicating, and Editing RADIUS Vendor-Specific Attributes, page 18-7.

ACS 5.8.1 as the AAA Server

A AAA server is a server program that handles user requests for access to computer resources, and for an enterprise, provides AAA services. The AAA server typically interacts with network access and gateway servers, and databases and directories that contain user information. The current standard by which devices or applications communicate with an AAA server is RADIUS.

ACS 5.8.1 functions as a AAA server for one or more network access devices (NADs). The NADs are clients of the ACS server. You must specify the IP address of ACS on each client NAD, to direct user access requests to ACS by using the RADIUS protocol.

RADIUS is universally used to secure the access of end-users to network resources. A RADIUS server can act as a proxy to other RADIUS servers or other kinds of authentication servers.

The NAD serves as the network gatekeeper and sends an Access-Request to ACS on behalf of the user. ACS verifies the username, password, and possibly other data by using either the internal identity store, or an externally configured LDAP or Windows Active Directory identity store.

ACS ultimately responds to the NAD with either an Access-Reject message or an Access-Accept message that contains a set of authorization attributes.

ACS 5.8.1 provides network transport over UDP and implements the RADIUS protocol, including RADIUS packet parsing and assembling, necessary data validation, and tracking of duplicate requests.

Some reasons for using UDP are:

- The processing time is only a few seconds.
- No special handling is required for rebooting or offline clients and servers.
- UDP is a connectionless protocol.
- UDP easily implements multithreaded servers to serve multiple client requests.

The UDP-assigned port number for RADIUS are:

- 1812 for access requests
- 1813 for accounting
- 1645 for access requests
- 1646 for accounting

ACS 5.8.1 is the entrance point to the authentication system. ACS listens on specific configurable UDP ports. When data arrives from the network:

Step 1 ACS tries to process the data as a RADIUS client request or proxy response packet.

Step 2 ACS verifies that the packet arrived from the NAD that is registered in the configuration, and then prevents duplicate packet processing.

Step 3 ACS parses the RADIUS packet and performs the necessary validations of its contents.

Step 4 ACS then passes the data for processing to the appropriate flow.

Step 5 When the system is ready to respond, ACS:

- Receives the result of the data processing.
  - Creates a corresponding response to the client.
  - Returns the response to the network.

RADIUS Attribute Support in ACS 5.8.1

ACS 5.8.1 supports the RADIUS protocol as RFC 2865 describes.

ACS 5.8.1 supports the following types of RADIUS attributes:

- IETF RADIUS attributes
- Generic and Cisco VSAs
- Other vendors' attributes

ACS 5.8.1 also supports attributes defined in the following extensions to RADIUS:

- Accounting-related attributes, as defined in RFC 2866.
- Support for Tunnel Protocol, as defined in RFCs 2867 and 2868.
- Support for EAP (via the EAP-Message attribute), as defined in RFCs 2869 and 3579.

Note When RADIUS parameters are referenced, the convention [*attribute-number*] [*attribute name*] is used. For example, [*1*]*User-Name*, where the number and name correspond to that assigned to the parameter in the specification.

RADIUS supports receiving, sending, and dictionary-based parsing and construction of any RADIUS attribute regardless of whether it is a regular attribute, VSA, or Cisco attribute-value (AV) pair. The RADIUS interface in ACS supports the attribute data types defined in RFC 2865, namely:

- *text* (UTF-8)
- *string* (binary)
- *address* (IP)
- *integer*
- *time*

Data types, integer, string, and text enumerated (ENUM) specifications of allowed values are supported. Attribute values are checked against these when packet parsing and construction occur.

ACS uses the RADIUS State attribute (24) to identify a specific conversation. Each conversation has a unique ID. Every conversation is processed under a specific configuration version—the latest available version at the moment the conversation was initiated.

Note The RADIUS State attribute (24) is not used for PAP authentication.

All transactions between the client and RADIUS server have their message integrity protected using the Request/Response Authenticator field inside each RADIUS packet, which makes use of a shared secret (that is, itself, not sent over the network directly).

In addition, some forms of RADIUS packets that include all of those that contain encapsulated EAP-Message attributes have the integrity of all of their RADIUS attributes additionally protected using a Message-Authenticator RADIUS attribute (that also makes use of the shared secret).

Furthermore, user passwords within the RADIUS packets sent between the client and RADIUS server are always encrypted to protect against the possibility that an unauthorized user on an insecure network could easily determine the password.

Authentication

ACS supports various authentication protocols transported over RADIUS. The supported protocols that do not include EAP are:

- PAP
- CHAP
- MSCHAPv1
- MSCHAPv2

In addition, various EAP-based protocols can be transported over RADIUS, encapsulated within the RADIUS EAP-Message attribute. These can be further categorized with respect to whether or not, and to what extent, they make use of certificates. These include:

- EAP methods that do not use certificates:
  - EAP-MD5
  - LEAP
- EAP methods in which the client uses the ACS server certificate to perform server authentication:
  - PEAP/EAP-MSCHAPv2
  - PEAP/EAP-GTC
  - EAP-FAST/EAP-MSCHAPv2
  - EAP-FAST/EAP-GTC
- EAP methods that use certificates for both server and client authentication:
  - EAP-TLS
  - PEAP/EAP-TLS

Authorization

Authorization is permitted according to the configured access policies.

Accounting

You can use the accounting functions of the RADIUS protocol independently of the RADIUS authentication or authorization functions. You can use some of the RADIUS accounting functions to send data at the start and end of sessions, and indicate the amount of resources (such as time, packets, bytes, and so on) that you used during the session.

An ISP might use RADIUS access control and accounting software to meet special security and billing needs.

RADIUS Access Requests

A user login contains a query (Access-Request) from the network access device to the RADIUS server and a corresponding response (Access-Accept or Access-Reject) from the server. The Access-Request packet contains the username, password, NAD IP address, and NAD port, and other relevant attributes.

When the RADIUS server receives the access-request from the NAD, it searches a database for the username. Depending on the result of the database query, an accept or reject is sent. A text message can accompany the access-reject message to indicate the reason for the refusal.

In RADIUS, authentication and authorization are coupled. If the RADIUS server finds the username and the password is correct, the RADIUS server returns an access-accept response, including a list of attribute-value pairs that describe the parameters to use for this session. This list of parameters sets the authorization rights for the user.

Typical parameters include:

- Service type
- Protocol type
- IP address to assign the user (static or dynamic)
- Access list to apply
- A static route to install in the NAD routing table

The configuration information in the RADIUS server defines which parameters to set on the NAD during installation.