Authentication Authorization and Accounting Configuration Guide, Cisco IOS Release 15E

CONTENTS

Device Sensor

The Device Sensor feature is used to gather raw endpoint data from network devices using protocols such as Cisco Discovery Protocol (CDP), Link Layer Discovery Protocol (LLDP), and DHCP. The endpoint data that is gathered is made available to registered clients in the context of an access session.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for Device Sensor

- Only Cisco Discovery Protocol, LLDP, DHCP, MDNS, SIP, and H323 protocols are supported.

- The session limit for profiling ports is 32.

- The length of one Type-Length-Value (TLV) must not be more than 1024 and the total length of TLVs (combined length of TLVs) of all protocols must not be more than 4096.

- The sensor profiles devices that are only one hop away.

• The Device Sensor feature is enabled by default, but cannot be disabled. Disabling device classifier using **no device classifier** command in global configuration mode does not disable device sensor. This is because device sensor is independent of IP device tracking and device classifier.

Note In Cisco IOS Release 15.2(1)E and later releases, you can exclude the protocols so that the Device Sensor feature does not analyze the data. To exclude the protocols, use the **device-sensor filter-spec** *protocol* **exclude all** command in global configuration mode.

Information About Device Sensor

Device Sensor

The device sensor is used to gather raw endpoint data from network devices. The endpoint information that is gathered helps in completing the profiling capability of devices. Profiling is the determination of the endpoint type based on information gleaned from various protocol packets from an endpoint during its connection to a network.

The profiling capability consists of two parts:

• Collector—Gathers endpoint data from network devices.

• Analyzer—Processes the data and determines the type of device.

The device sensor represents the embedded collector functionality. The illustration below shows the Cisco sensor in the context of the profiling system and also features other possible clients of the sensor.
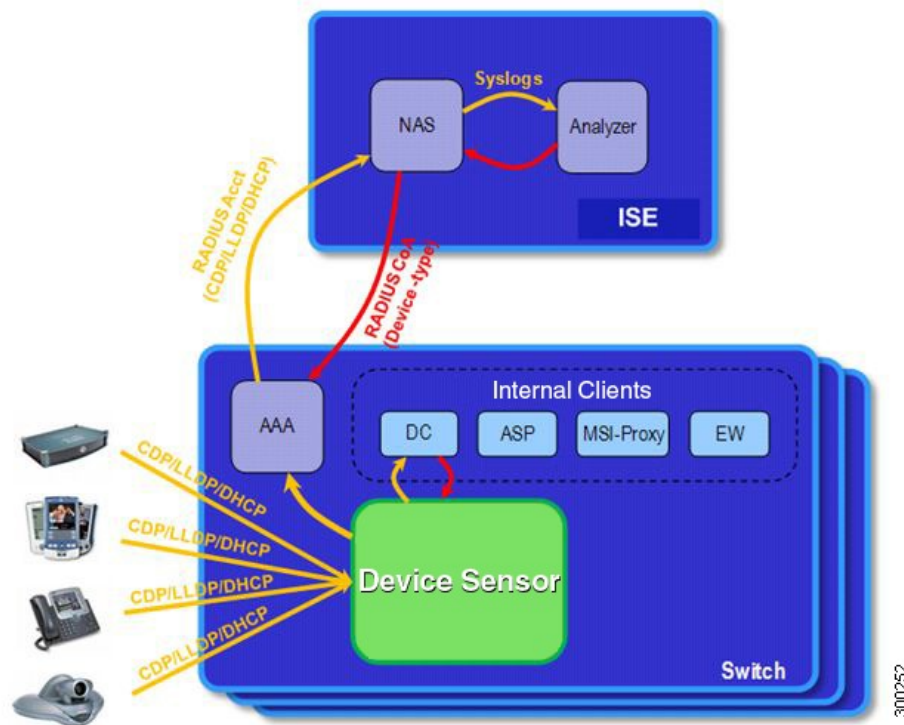
A device with sensor capability gathers endpoint information from network devices using protocols such as Cisco Discovery Protocol, LLDP, and DHCP, subject to statically configured filters, and makes this information available to its registered clients in the context of an access session. An access session represents an endpoint's connection to the network device.

The device sensor has internal and external clients. The internal clients include components such as the embedded Device Classifier (local analyzer), ATM switch processor (ASP), MSI-Proxy, and EnergyWise (EW). The external client, that is the Identity Services Engine (ISE) analyzer, will use RADIUS accounting to receive additional endpoint data.

Client notifications and accounting messages containing profiling data along with the session events and other session-related data, such as the MAC address and the ingress port, are generated and sent to the internal and external clients (ISE). By default, for each supported peer protocol, client notifications and accounting events are only generated where an incoming packet includes a TLV that has not previously been received in the context of a given session. You can enable client notifications and accounting events for all TLV changes, where either a new TLV has been received or a previously received TLV has been received with a different value using CLI commands.

The device sensor's port security protects the switch from consuming memory and crashing during deliberate or unintentional denial-of-service (DoS) type attacks. The sensor limits the maximum device monitoring sessions to 32 per port (access ports and trunk ports). In case of lack of activity from hosts, the age session time is 12 hours.

How to Configure Device Sensor

The device sensor is enabled by default.

Note In Cisco IOS Release 15.2(1)E and later releases, you can exclude the protocols so that the Device Sensor feature does not analyze the data. To exclude the protocols, use the **device-sensor filter-spec** *protocol* **exclude all** command in global configuration mode.

The following tasks are applicable only if you want to configure the sensor based on your specific requirements.

Note If you do not perform these configuration tasks, then the following TLVs are included by default:

- Cisco Discovery Protocol filter—secondport-status-type and powernet-event-type (type 28 and 29).

- LLDP filter—organizationally-specific (type 127).

- DHCP filter—message-type (type 53).

Enabling Accounting Augmentation

Perform this task to add device sensor protocol data to accounting records.

Before You Begin

For the sensor protocol data to be added to the accounting messages, you must enable session accounting by using the following standard authentication, authorization, and accounting (AAA), and RADIUS configuration commands:

```
Device(config)#aaa new-model
Device(config)#aaa accounting dot1x default start-stop group radius
Device(config)#radius-server host{hostname | ip-address}[auth-port port-number][acct-port
port-number][timeout seconds][retransmit retries][key string]
Device(config)#radius-server vsa send accounting
```

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **device-sensor accounting**
4. **end**

DETAILED STEPS

	Command or Action	**Purpose**
Step 1	**enable** **Example:** Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	**Purpose**
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**device-sensor accounting** **Example:** `Device(config)# device-sensor accounting`	Enables the addition of sensor protocol data to accounting records and also enables the generation of additional accounting events when new sensor data is detected.
Step 4	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Creating a Cisco Discovery Protocol Filter

Perform this task to create a Cisco Discovery Protocol filter containing a list of TLVs that can be included or excluded in the device sensor output.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **device-sensor filter-list cdp list** *tlv-list-name*
4. **tlv** {**name** *tlv-name* | **number** *tlv-number*}
5. **end**

DETAILED STEPS

	Command or Action	**Purpose**
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	**Purpose**
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

Step 3	**device-sensor filter-list cdp list** *tlv-list-name*
	
	Example:
	`Device(config)# device-sensor filter-list cdp`
	`list cdp-list`
		Creates a TLV list and enters CDP sensor configuration mode, where you can configure individual TLVs.

Step 4	**tlv** {**name** *tlv-name* | **number** *tlv-number*} **Example:** `Device(config-sensor-cdplist)# tlv number 10`	Adds individual Cisco Discovery Protocol TLVs to the TLV list. • You can delete the TLV list without individually removing TLVs from the list by using the **no device-sensor filter-list cdp list** *tlv-list-name* command.
Step 5	**end** **Example:** `Device(config-sensor-cdplist)# end`	Returns to privileged EXEC mode.

Creating an LLDP Filter

Perform this task to create an LLDP filter containing a list of TLVs that can be included or excluded in the device sensor output.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **device-sensor filter-list lldp list** *tlv-list-name*
4. **tlv** {**name** *tlv-name* \| **number** *tlv-number*}
5. **end**

DETAILED STEPS

	Command or Action	**Purpose**
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: Device> enable	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** Device# configure terminal	Enters global configuration mode.
Step 3	**device-sensor filter-list lldp list** *tlv-list-name* **Example:** Device(config)# device-sensor filter-list lldp list lldp-list	Creates a TLV list and enters LLDP sensor configuration mode, where you can configure individual TLVs.
Step 4	**tlv** {**name** *tlv-name* | **number** *tlv-number*} **Example:** Device(config-sensor-lldplist)# tlv number 15	Adds individual LLDP TLVs to the TLV list. • You can delete the TLV list without individually removing TLVs from the list by using the **no device-sensor filter-list lldp list** *tlv-list-name* command.
Step 5	**end** **Example:** Device(config-sensor-lldplist)# end	Returns to privileged EXEC mode.

Creating a DHCP Filter

Perform this task to create a DHCP filter containing a list of options that can be included or excluded in the device sensor output.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **device-sensor filter-list dhcp list** *option-list-name*
4. **option** {**name** *option-name* \| **number** *option-number*}
5. **end**

DETAILED STEPS

	Command or Action	**Purpose**
Step 1	**enable** **Example:** Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Device# configure terminal	Enters global configuration mode.
Step 3	**device-sensor filter-list dhcp list** *option-list-name* **Example:** Device(config)# device-sensor filter-list dhcp list dhcp-list	Creates an options list and enters DHCP sensor configuration mode, where you can configure individual options.
Step 4	**option** {**name** *option-name* | **number** *option-number*} **Example:** Device(config-sensor-dhcplist)# option number 10	Adds individual DHCP options to the option list. • You can delete the option list without individually removing options from the list by using the **no device-sensor filter-list dhcp list** *option-list-name* command.
Step 5	**end** **Example:** Device(config-sensor-dhcplist)# end	Returns to privileged EXEC mode.

Applying a Protocol Filter to the Sensor Output

Perform this task to apply a Cisco Discovery Protocol, LLDP, or DHCP filter to the sensor output. Session notifications are sent to internal sensor clients and accounting requests.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **device-sensor filter-spec** {**cdp** \| **dhcp** \| **lldp**} {**exclude** {**all** \| **list** *list-name*} \| **include list** *list-name*}
4. **end**

DETAILED STEPS

	Command or Action	**Purpose**
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

Step 3	**device-sensor filter-spec** {**cdp** | **dhcp** | **lldp**} {**exclude** {**all** | **list** *list-name*} | **include list** *list-name*}
	
	Example:
	`Device(config)# device-sensor`
	`filter-spec cdp include list list1`
		Applies a specific protocol filter containing a list of TLV fields to the device sensor output.
		
		• **cdp**—Applies a Cisco Discovery Protocol TLV filter list to the device sensor output.
		
		• **lldp**—Applies an LLDP TLV filter list to the device sensor output.
		
		• **dhcp**—Applies a DHCP TLV filter list to the device sensor output.
		
		• **exclude**—Specifies the TLVs that must be excluded from the device sensor output.
		
		• **include**—Specifies the TLVs that must be included from the device sensor output.
		
		• **all**—Disables all notifications for the associated protocol.
		
		• **list** *list-name*—Specifies the protocol TLV filter list name.

Step 4	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Tracking TLV Changes

Perform this task to enable client notifications and accounting events for all TLV changes. By default, for each supported peer protocol, client notifications and accounting events will only be generated where an incoming packet includes a TLV that has not previously been received in the context of a given session.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **device-sensor notify all-changes**
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**device-sensor notify all-changes** **Example:** `Device(config)# device-sensor notify all-changes`	Enables client notifications and accounting events for all TLV changes, that is, where either a new TLV is received or a previously received TLV is received with a new value in the context of a given session. **Note** Use the **default device-sensor notify** or the **device-sensor notify new-tlvs** command to return to the default TLV.
Step 4	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Verifying the Device Sensor Configuration

Perform this task to verify the sensor cache entries for all devices.

SUMMARY STEPS

1. **enable**
2. **show device-sensor cache mac** *mac-address*
3. **show device-sensor cache all**

DETAILED STEPS

Step 1   **enable**
Enables privileged EXEC mode.

Example:
```
Device> enable
```

Step 2   **show device-sensor cache mac** *mac-address*
Displays sensor cache entries (the list of protocol TLVs or options received from a device) for a specific device.

Example:
```
Device# show device-sensor cache mac 0024.14dc.df4d

Device: 0024.14dc.df4d on port GigabitEthernet1/0/24
--------------------------------------------------
Proto Type:Name                     Len Value
cdp     26:power-available-type      16 00 1A 00 10 00 00 00 01 00 00 00 00 FF FF FF FF
cdp     22:mgmt-address-type         17 00 16 00 11 00 00 00 01 01 01 CC 00 04 09 1B 65
                                        0E
cdp     11:duplex-type                5 00 0B 00 05 01
cdp      9:vtp-mgmt-domain-type       4 00 09 00 04
cdp      4:capabilities-type          8 00 04 00 08 00 00 00 28
cdp      1:device-name               14 00 01 00 0E 73 75 70 70 6C 69 63 61 6E 74
lldp     0:end-of-lldpdu              2 00 00
lldp     8:management-address        14 10 0C 05 01 09 1B 65 0E 03 00 00 00 01 00
lldp     7:system-capabilities        6 0E 04 00 14 00 04
lldp     4:port-description          23 08 15 47 69 67 61 62 69 74 45 74 68 65 72 6E 65
                                        74 31 2F 30 2F 32 34
lldp     5:system-name               12 0A 0A 73 75 70 70 6C 69 63 61 6E 74
dhcp    82:relay-agent-info          20 52 12 01 06 00 04 00 18 01 18 02 08 00 06 00 24
                                        14 DC DF 80
dhcp    12:host-name                 12 0C 0A 73 75 70 70 6C 69 63 61 6E 74
dhcp    61:client-identifier         32 3D 1E 00 63 69 73 63 6F 2D 30 30 32 34 2E 31 34
                                        64 63 2E 64 66 34 64 2D 47 69 31 2F 30 2F 32 34
dhcp    57:max-message-size           4 39 02 04 80
```

Step 3   **show device-sensor cache all**
Displays sensor cache entries for all devices.

Example:
```
Device# show device-sensor cache all

Device: 001c.0f74.8480 on port GigabitEthernet2/1
--------------------------------------------------
Proto Type:Name Len Value
dhcp 52:option-overload 3 34 01 03
dhcp 60:class-identifier 11 3C 09 64 6F 63 73 69 73 31 2E 30
dhcp 55:parameter-request-list 8 37 06 01 42 06 03 43 96
dhcp 61:client-identifier 27 3D 19 00 63 69 73 63 6F 2D 30 30 31 63 2E 30 66
37 34 2E 38 34 38 30 2D 56 6C 31
dhcp 57:max-message-size 4 39 02 04 80
Device: 000f.f7a7.234f on port GigabitEthernet2/1
--------------------------------------------------
Proto Type:Name Len Value
cdp 22:mgmt-address-type 8 00 16 00 08 00 00 00 00 00
cdp 19:cos-type 5 00 13 00 05 00
cdp 18:trust-type 5 00 12 00 05 00
cdp 11:duplex-type 5 00 0B 00 05 01
```

```
cdp 10:native-vlan-type 6 00 0A 00 06 00 01
cdp 9:vtp-mgmt-domain-type 9 00 09 00 09 63 69 73 63 6F
```

Troubleshooting Tips

After you have configured AAA Dead-Server Detection, you should verify your configuration using the **show running-config** command. This verification is especially important if you have used the **no** form of the **radius-server dead-criteria** command. The output of the **show running-config** command must show the same values in the "Dead Criteria Details" field that you configured using the **radius-server dead-criteria** command.

Configuration Examples for the Device Sensor Feature

Examples: Configuring the Device Sensor

The following example shows how to create a Cisco Discovery Protocol filter containing a list of TLVs:

```
Device> enable
Device# configure terminal
Device(config)# device-sensor filter-list cdp list cdp-list
Device(config-sensor-cdplist)# tlv name address-type
Device(config-sensor-cdplist)# tlv name device-name
Device(config-sensor-cdplist)# tlv number 34
Device(config-sensor-cdplist)# end
```

The following example shows how to create an LLDP filter containing a list of TLVs:

```
Device> enable
Device# configure terminal
Device(config)# device-sensor filter-list lldp list lldp-list
Device(config-sensor-lldplist)# tlv name chassis-id
Device(config-sensor-lldplist)# tlv name management-address
Device(config-sensor-lldplist)# tlv number 28
Device(config-sensor-lldplist)# end
```

The following example shows how to create a DHCP filter containing a list of options:

```
Device> enable
Device# configure terminal
Device(config)# device-sensor filter-list dhcp list dhcp-list
Device(config-sensor-lldplist)# option name address-type
Device(config-sensor-lldplist)# option name device-name
Device(config-sensor-lldplist)# option number 34
Device(config-sensor-lldplist)# end
```

The following example shows how to apply a Cisco Discovery Protocol TLV filter list to the device sensor output:

```
Device> enable
Device# configure terminal
Device(config)# device-sensor filter-spec cdp include cdp-list1
```

The following example shows how to enable client notifications and accounting events for all TLV changes:

```
Device> enable
Device# configure terminal
Device(config)# device-sensor notify all-changes
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Master Command List, All Releases
Security commands	• Security Command Reference: Commands A to C • Security Command Reference: Commands D to L • Security Command Reference: Commands M to R • Security Command Reference: Commands S to Z

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Device Sensor

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for Device Sensor

Feature Name	Releases	Feature Information
Device Sensor	Cisco IOS 15.2(1)E	The Device Sensor feature is used to gather raw endpoint data from network devices using protocols such as Cisco Discovery Protocol, Link Layer Discovery Protocol (LLDP), and DHCP. The endpoint data that is gathered is made available to registered clients in the context of an access session. The following commands were introduced or modified: **debug device-sensor**, **device-sensor accounting**, **device-sensor filter-list cdp**, **device-sensor filter-list dhcp**, **device-sensor filter-list lldp**, **device-sensor filter-spec**, **device-sensor notify**, and **show device-sensor cache**.

C H A P T E R **2**

AAA Double Authentication Secured by Absolute Timeout

The AAA Double Authentication Secured by Absolute Timeout feature allows you to secure the double authentication mechanism by protecting it with a per-user session timeout. This feature optimizes the connections to the network that are authorized by service providers and increases the security of the overall access to the network by ensuring that no unwanted sessions are connected.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for AAA Double Authentication Secured by Absolute Timeout

- You need access to a Cisco RADIUS or TACACS+ server and should be familiar with configuring RADIUS or TACACS+.

- You should be familiar with configuring authentication, authorization, and accounting (AAA) and enabling AAA automated double authentication.

Restrictions for AAA Double Authentication Secured by Absolute Timeout

- The AAA Double Authentication Secured by Absolute Timeout feature is for PPP connections only. Automated double authentication cannot be used with other protocols, such as X.25 or Serial Line Internet Protocol (SLIP).

- There may be a minimal impact on performance if a TACACS+ server is used. However, there is no performance impact if a RADIUS server is used.

Information About AAA Double Authentication Secured by Absolute Timeout

AAA Double Authentication

Use the AAA double authentication mechanism to pass the first authentication using a host username and password. The second authentication, after the Challenge Handshake Authentication Protocol (CHAP) or the Password Authentication Protocol (PAP) authentication, uses a login username and password. In the first authentication, a PPP session timeout is applied to the virtual access interface if it is configured locally or remotely.

The AAA Double Authentication Secured by Absolute Timeout feature allows you to secure the double authentication mechanism by protecting it with a per-user session timeout. The per-user session timeout, which can be customized, supersedes the generic absolute timeout value. This method works on the same principle as per-user access control lists (ACLs) in double authentication.

How to Apply AAA Double Authentication Secured by Absolute Timeout

Applying AAA Double Authentication Secured by Absolute Timeout

To apply the absolute timeout, you must configure session-timeout in the login user profile as a link control protocol (LCP) per-user attribute. Use the **access-profile** command to enable AAA double authentication. This command is used to apply your per-user authorization attributes to an interface during a PPP session. Before you use the **access-profile** command, you must first reauthorize LCP per-user attributes (for example, Session-Timeout) and then reauthorize Network Control Protocols (NCPs) to apply other necessary criteria, such as ACLs and routes. See the section "Examples for AAA Double Authentication Secured by Absolute Timeout."

Note   The Timeout configuration in a TACACS+ user profile is different from the configuration in a RADIUS user profile. In a RADIUS profile, only one session-timeout is configured, along with the autocommand **access-profile**. The timeout is applied to the EXEC session and to the PPP session respectively. In TACACS+, however, the timeout must be configured under the service types "exec" and "ppp" (LCP) to apply a timeout to the EXEC session and to the PPP session. If the timeout is configured only under the service type "ppp," the timeout value will not be available during an EXEC authorization, and the timeout will not be applied to the EXEC session.

Verifying AAA Double Authentication Secured by Absolute Timeout

To verify that AAA double authentication has been secured by absolute timeout and to see information about various attributes associated with the authentication, perform the following steps. These **show** and **debug** commands can be used in any order.

Note   If idle timeout is configured on a full virtual access interface and a subvirtual access interface, the **show users** command displays the idle time for both interfaces. However, if the idle timeout is not configured on both interfaces, the **show users** command will display the idle time for the full virtual access interface only.

SUMMARY STEPS

1. **enable**
2. **show users**
3. **show interfaces virtual-access** *number* [**configuration**]
4. **debug aaa authentication**
5. **debug aaa authorization**
6. **debug aaa per-user**
7. **debug ppp authentication**
8. Enter one of the following:

   - **debug radius**
     or

     debug tacacs

DETAILED STEPS

	Command or Action	**Purpose**
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show users** **Example:** `Device# show users`	Displays information about active lines on the device.
Step 3	**show interfaces virtual-access** *number* [**configuration**] **Example:** `Device# show interfaces virtual-access 2 configuration`	Displays status, traffic data, and configuration information about a specified virtual access interface.
Step 4	**debug aaa authentication** **Example:** `Device# debug aaa authentication`	Displays information about AAA TACACS+ authentication.
Step 5	**debug aaa authorization** **Example:** `Device# debug aaa authorization`	Displays information about AAA TACACS+ authorization.

	Command or Action	Purpose
Step 6	**debug aaa per-user** **Example:** `Device# debug aaa per-user`	Displays the attributes that are applied to each user as the user gets authenticated.
Step 7	**debug ppp authentication** **Example:** `Device# debug ppp authentication`	Displays whether a user is passing authentication.

Step 8	Enter one of the following:
	
	  • **debug radius**
	   or
	
	   debug tacacs
	
	Example:
	
	`Device# debug radius`
	
	Example:
	
	`Device# debug tacacs`
		Displays the debug information associated with the RADIUS server.
		
		or
		
		Displays the debug information associated with the TACACS+ server.

Examples

The following sample output is from the **show users** command:

```
Device# show users

    Line       User        Host(s       Idle        Location
 *  0 con 0    aaapbx2      idle         00:00:00    aaacon2 10
    8 vty 0    broker_def   idle         00:00:08    192.168.1.8
    Interface  User            Mode        Idle       Peer Address
    Vi2        broker_default  VDP         00:00:01   192.168.1.8 <=========
    Se0:22     aaapbx2         Sync PPP    00:00:23
```

The following sample output is from the **show interfaces virtual-access** command:

```
Device# show interfaces virtual-access 2 configuration

Virtual-Access2 is a Virtual Profile (sub)interface
Derived configuration: 150 bytes
!
interface Virtual-Access2
  ip unnumbered Serial0:23
  no ip route-cache
  timeout absolute 3 0
! The above line shows that the per-user session timeout has been applied.
  ppp authentication chap
```

```
        ppp timeout idle 180000
! The above line shows that the absolute timeout has been applied.
```

Configuration Examples for AAA Double Authentication Secured by Absolute Timeout

Example: RADIUS User Profile

The following sample output shows that a RADIUS user profile has been applied and that AAA double authentication has been secured by an absolute timeout:

```
aaapbx2 Password = "password1",
 Service-Type = Framed,
 Framed-Protocol = PPP,
 Session-Timeout = 180,
 Idle-Timeout = 180000,
 cisco-avpair = "ip:inacl#1=permit tcp any any eq telnet"
 cisco-avpair = "ip:inacl#2=permit icmp any any"
broker_default Password = "password1",
 Service-Type = Administrative,
 cisco-avpair = "shell:autocmd=access-profile",
 Session-Timeout = 360,
 cisco-avpair = "ip:inacl#1=permit tcp any any"
 cisco-avpair = "ip:inacl#2=permit icmp any any"
broker_merge Password = "password1",
 Service-Type = Administrative,
 cisco-avpair = "shell:autocmd=access-profile merge",
 Session-Timeout = 360,
 cisco-avpair = "ip:inacl#1=permit tcp any any"
 cisco-avpair = "ip:inacl#2=permit icmp any any"
 cisco-avpair = "ip:route#3=10.4.0.0 255.0.0.0"
 cisco-avpair = "ip:route#4=10.5.0.0 255.0.0.0"
 cisco-avpair = "ip:route#5=10.6.0.0 255.0.0.0"
broker_replace Password = "password1",
 Service-Type = Administrative,
 cisco-avpair = "shell:autocmd=access-profile replace",
 Session-Timeout = 360,
 cisco-avpair = "ip:inacl#1=permit tcp any any"
 cisco-avpair = "ip:inacl#2=permit icmp any any"
 cisco-avpair = "ip:route#3=10.4.0.0 255.0.0.0"
 cisco-avpair = "ip:route#4=10.5.0.0 255.0.0.0"
 cisco-avpair = "ip:route#5=10.6.0.0 255.0.0.0"
```

Example: TACACS User Profile

The following sample output shows that a TACACS+ user profile has been applied and that AAA double authentication has been secured by an absolute timeout.

Remote Host Authentication

The following example shows how to allow the remote host to be authenticated by the local host during the first-stage authentication and provides the remote host authorization profile.

```
user = aaapbx2
 chap = cleartext Cisco
 pap = cleartext cisco
 login = cleartext cisco
```

```
service = ppp protocol = lcp
 idletime = 3000
 timeout = 3
service = ppp protocol = ip
 inacl#1="permit tcp any any eq telnet"
service = ppp protocol = ipx
```

Using the access-profile Command Without Any Arguments

Using the **access-profile** command without any arguments causes the removal of any access lists that are found in the old configuration (both per-user and per-interface) and ensures that the new profile contains only access-list definitions.

```
user = broker_default
 login = cleartext Cisco
 chap = cleartext "cisco"
 service = exec
  autocmd = "access-profile"
! This is the autocommand that executes when broker_default logs in.
  timeout = 6
 service = ppp protocol = lcp
  timeout = 6
 service = ppp protocol = ip
! Put access lists, static routes, and other requirements that are
! needed here. Read the software specifications for details. If you leave
! this blank, the user will have no access lists (not even the ones that were
! installed prior to the creation of this user profile)!
  inacl#1="permit tcp any any"
  inacl#2="permit icmp host 10.0.0.0 any"
 service = ppp protocol = ipx
! Put access lists, static routes, and other requirements that are
! needed here. Read the software specifications for details. If you leave
! this blank, the user will have no access lists (not even the ones that were
! installed prior to the creation of this user profile)!
```

Using the access-profile Command with the merge Keyword

The **merge** keyword in the **access-profile** command is used to remove all old access lists, and any attribute-value (AV) pair is allowed to be uploaded and installed. The use of the **merge** keyword will allow for the uploading of any custom static routes, Service Advertisement Protocol (SAP) filters, and other requirements that users may need in their profiles. Configure the **merge** keyword with care because it leaves everything open in terms of conflicting configurations.

```
user = broker_merge
 login = cleartext Cisco
 chap = cleartext "cisco"
 service = exec
  autocmd = "access-profile merge"
! This is the autocommand that executes when broker_merge logs in.
  timeout = 6
 service = ppp protocol = lcp
 timeout = 6
 service = ppp protocol = ip
! Put access lists, static routes, and other requirements that are
! needed here. Read the software specifications for details. If you leave
! this blank, the user will have no access lists (not even the ones that were
! installed prior to the creation of this user profile)!
  route#1="10.4.0.0 255.0.0.0"
  route#2="10.5.0.0 255.0.0.0"
  route#3="10.6.0.0 255.0.0.0"
  inacl#5="permit tcp any any"
  inacl#6="permit icmp host 10.60.0.0 any"
 service = ppp protocol = ipx
! Put access lists, static routes, and other requirements that are
! needed here. Read the software specifications for details. If you leave
! this blank, the user will have no access lists (not even the ones that were
! installed prior to the creation of this user profile)!
```

Using the access-profile Command with the replace Keyword

If you use the **access-profile** command with the **replace** keyword, any old configurations are removed and a new configuration is installed.

> **Note** When the **access-profile** command is configured, the new configuration is checked for address pools and address-AV pairs. Because addresses cannot be renegotiated at this point, the command will fail to work when it encounters such an address-AV pair.

```
user = broker_replace
 login = cleartext Cisco
 chap = cleartext "cisco"
 service = exec
  autocmd = "access-profile replace"
! This is the autocommand that executes when broker_replace logs in.
  timeout = 6
 service = ppp protocol = lcp
  timeout = 6
 service = ppp protocol = ip
! Put access lists, static routes, and other requirements that are
! needed here. Read the software specifications for details. If you leave
! this blank, the user will have no access lists (not even the ones that were
! installed prior to the creation of this user profile)!
  route#1="10.7.0.0 255.0.0.0"
  route#2="10.8.0.0 255.0.0.0"
  route#3="10.9.0.0 255.0.0.0"
  inacl#4="permit tcp any any"
 service = ppp protocol = ipx
! Put access lists, static routes, and other requirements that are
! needed here. Read the software specifications for details. If you leave
! this blank, the user will have no access lists (not even the ones that were
! installed prior to the creation of this user profile)!
```

> **Note** The Timeout configuration in a TACACS+ user profile is different from the configuration in a RADIUS user profile. In a RADIUS profile, only one session-timeout is configured, along with the autocommand **access-profile**. The timeout will be applied to the EXEC session and to the PPP session. In the TACACS+ user profile, however, the timeout must be configured under the service types "exec" and "ppp" (LCP) to apply a timeout to the EXEC session and to the PPP session respectively. If the timeout is configured only under the service type "ppp," the timeout value will not be available during an EXEC authorization, and the timeout will not be applied to the EXEC session.

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Master Command List, All Releases

Related Topic	Document Title
Security commands	• Security Command Reference: Commands A to C • Security Command Reference: Commands D to L • Security Command Reference: Commands M to R • Security Command Reference: Commands S to Z

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for AAA Double Authentication Secured by Absolute Timeout

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 2: Feature Information for AAA Double Authentication Secured by Absolute Timeout

Feature Name	Releases	Feature Information
AAA Double Authentication Secured by Absolute Timeout	Cisco IOS 15.2(1)E	The AAA Double Authentication Secured by Absolute Timeout feature allows you to secure the double authentication mechanism by protecting it with a per-user session timeout. This feature optimizes the connection to the network by service providers to only connections that are authorized, and it increases the security of the overall access to the network by ensuring that no unwanted sessions are connected.

Login Password Retry Lockout

The Login Password Retry Lockout feature allows system administrators to lock out a local authentication, authorization, and accounting (AAA) user account after a configured number of unsuccessful attempts by the user to log in.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Login Password Retry Lockout

- You must be running a Cisco IOS image that contains the AAA component.

Restrictions for Login Password Retry Lockout

- Authorized users can lock themselves out because there is no distinction between an attacker who is guessing passwords and an authorized user who is entering the password incorrectly multiple times.

- A denial of service (DoS) attack is possible; that is, an authorized user could be locked out by an attacker if the username of the authorized user is known to the attacker.

Information About Login Password Retry Lockout

Lock Out of a Local AAA User Account

The Login Password Retry Lockout feature allows system administrators to lock out a local AAA user account after a configured number of unsuccessful attempts by the user to log in using the username that corresponds to the AAA user account. A locked-out user cannot successfully log in again until the user account is unlocked by the administrator.

A system message is generated when a user is either locked by the system or unlocked by the system administrator. The following is an example of such a system message:

```
%AAA-5-USER_LOCKED: User user1 locked out on authentication failure.
```
The system administrator cannot be locked out.

Note The system administrator is a special user who has been configured using the maximum privilege level (root privilege--level 15). A user who has been configured using a lesser privilege level can change the privilege level using the **enable** command. A user that can change to the root privilege (level 15) is able to act as a system administrator.

This feature is applicable to any login authentication method, such as ASCII, Challenge Handshake Authentication Protocol (CHAP), and Password Authentication Protocol (PAP).

Note No messages are displayed to users after authentication failures that are due to the locked status (that is, there is no distinction between a normal authentication failure and an authentication failure due to the locked status of the user).

How to Configure Login Password Retry Lockout

Configuring Login Password Retry Lockout

To configure the Login Password Retry Lockout feature, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **username** *name* [**privilege** *level*] **password** *encryption-type password*
4. **aaa new-model**
5. **aaa local authentication attempts max-fail** *number-of-unsuccessful-attempts*
6. **aaa authentication login default method**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**username** *name* [**privilege** *level*] **password** *encryption-type password* **Example:** `Router(config)# username user1 privilege 15 password 0 cisco`	Establishes a username-based authentication system.
Step 4	**aaa new-model** **Example:** `Router(config)# aaa new-model`	Enables the AAA access control model.
Step 5	**aaa local authentication attempts max-fail** *number-of-unsuccessful-attempts* **Example:** `Router(config)# aaa local authentication attempts max-fail 3`	Specifies the maximum number of unsuccessful attempts before a user is locked out.

	Command or Action	Purpose
Step 6	**aaa authentication login default method** **Example:** Router(config)# aaa authentication login default local	Sets the authentication, authorization, and accounting (AAA) authentication method at login. For example, **aaa authentication login default** *local* specifies the local AAA user database.

Unlocking a Login Locked-Out User

To unlock a login locked-out user, perform the following steps.

Note   This task can be performed only by users having the root privilege (level 15).

SUMMARY STEPS

1. **enable**
2. **clear aaa local user lockout** {**username** *username* | **all**}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**clear aaa local user lockout** {**username** *username*	**all**} **Example:** Router# clear aaa local user lockout username user1	Unlocks a locked-out user.

Clearing the Unsuccessful Login Attempts of a User

This task is useful for cases in which the user configuration was changed and the unsuccessful login attempts of a user that are already logged must be cleared.

To clear the unsuccessful login attempts of a user that have already been logged, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **clear aaa local user fail-attempts** {**username** *username* | **all**}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**clear aaa local user fail-attempts** {**username** *username*	**all**} **Example:** Router# clear aaa local user fail-attempts username user1	Clears the unsuccessful attempts of the user. • This command is useful for cases in which the user configuration was changed and the unsuccessful attempts that are already logged must be cleared.

Monitoring and Maintaining Login Password Retry Lockout Status

To monitor and maintain the status of the Login Password Retry Lockout configuration, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **show aaa local user lockout**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**show aaa local user lockout** **Example:** Router# show aaa local user lockout	Displays a list of the locked-out users for the current login password retry lockout configuration.

Example

The following output shows that user1 is locked out:

```
Router# show aaa local user lockout
          Local-user          Lock time
          user1               04:28:49 UTC Sat Jun 19 2004
```

Configuration Examples for Login Password Retry Lockout

Displaying the Login Password Retry Lockout Configuration Example

The following **show running-config** command output illustrates that the maximum number of failed user attempts has been set for 2 as the login password retry lockout configuration:

```
Router # show running-config
Building configuration...
Current configuration : 1214 bytes
!
version 12.3
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname LAC-2
!
boot-start-marker
boot-end-marker
!
!
username sysadmin
username sysad privilege 15 password 0 cisco
username user1 password 0 cisco
aaa new-model
aaa local authentication attempts max-fail 2
!
!
aaa authentication login default local
aaa dnis map enable
aaa session-id common
```

Additional References

The following sections provide references related to Login Password Retry Lockout.

Related Documents

Related Topic	Document Title
Cisco IOS security commands	*Cisco IOS Security Command Reference*

Standards

Standards	Title
None	--

MIBs

MIBs	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
None	--

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information for Login Password Retry Lockout

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 3: Feature Information for Login Password Retry Lockout

Feature Name	Releases	Feature Information
Login Password Retry Lockout	Cisco IOS 15.2(1)E	The Login Password Retry Lockout feature allows system administrators to lock out a local AAA user account after a configured number of unsuccessful attempts by the user to log in. This feature was introduced in Cisco IOS Release 12.3(14)T. This feature was integrated into Cisco IOS Release 12.2(33)SRE. The following commands were introduced or modified: **aaa local authentication attempts max-fail**, **clear aaa local user fail-attempts**, **clear aaa local user lockout**.

Glossary

- **local AAA method** --Method by which it is possible to configure a local user database on a router and to have AAA provision authentication or authorization of users from this database.

- **local AAA user** --User who is authenticated using the local AAA method.

Throttling of AAA RADIUS Records

The Throttling of AAA (RADIUS) Records feature supports throttling of access (authentication and authorization) and accounting records that are sent to the RADIUS server. This feature allows a user to configure the appropriate throttling rate to avoid network congestion and instability; such as when there is insufficient bandwidth to accommodate a sudden burst of records generated from the router to the RADIUS server.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About Throttling of AAA RADIUS Records

Benefits of the Throttling of AAA RADIUS Records Feature

A Network Access Server (NAS), acting as RADIUS client, can generate a burst of accounting or access requests, causing severe network congestion or causing the RADIUS server to become overloaded with a

burst of RADIUS traffic. This problem could be compounded when multiple NASs interact with the RADIUS servers.

The following conditions can trigger a sudden burst of RADIUS traffic:

- An interface flap, which in turn brings down all the subscriber sessions and generates accounting requests for each subscriber.

- The High Availability (HA) program generating a START record for every session that survived a switchover, such as the scenario described the preceding bullet.

A large number of generated requests can make the network unstable if there is insufficient bandwidth or if the RADIUS server is slow to respond. Neither the User Datagram Protocol (UDP) transport layer nor the RADIUS protocol has a flow control mechanism. The throttling mechanism provided by this feature provides a solution for these issues.

Throttling Access Requests and Accounting Records

The Throttling of AAA (RADIUS) Records feature introduces a mechanism to control packets (flow control) at the NAS level, which improves the RADIUS server performance.

Because of their specific uses, access requests and accounting records must be treated separately. Access request packets are time sensitive, while accounting record packets are not.

- If a response to an access request is not returned to the client in a timely manner, the protocol or the user will time out, impacting the device transmission rates.

- Accounting records packets are not real-time critical.

When configuring threshold values on the same server, it is important to prioritize threshold values for the handling of the time-sensitive access request packets and to place a lesser threshold value on the accounting records packets.

In some cases, when an Internet Service Provider (ISP) is using separate RADIUS servers for access requests and accounting records, only accounting records throttling may be required.

- The Throttling of AAA (RADIUS) Records is disabled, by default.

- Throttling functionality can be configured globally or at server group level.

How to Configure Throttling of AAA RADIUS Records

This section describes how to configure throttling of access (authentication and authorization) and accounting records that are sent to the RADIUS server for both, global and server groups.

Server-group configurations are used to enable or disable throttling for a particular server group and to specify the threshold value for that server group.

Note   Server-group configurations override any configured global configurations.

Throttling Accounting and Access Request Packets Globally

To globally configure the throttling of accounting and access request packets, perform the following task.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **radius-server throttle** { [**accounting** *threshold*] [**access** *threshold* [**access-timeout** *number-of-timeouts*]]}
4. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**radius-server throttle** { [**accounting** *threshold*] [**access** *threshold* [**access-timeout** *number-of-timeouts*]]} **Example:** `Router(config)# radius-server throttle accounting 100 access 200 access-timeout 2`	Configures global throttling for accounting and access request packets. For this example: • The accounting threshold value (the range is 0-65536) is set to 100, and the access threshold value is set to 200. **Note** The default threshold value is 0 (throttling disabled). • The number of timeouts per transaction value (the range is 1-10) is set to 2.
Step 4	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.

Throttling Accounting and Access Request Packets Per Server Group

The following server-group configuration can be used to enable or disable throttling for a specified server group and to specify the threshold value for that server group.

To configure throttling of server-group accounting and access request packets, perform the following task.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa group server radius** *server-group-name*
4. **throttle** {[**accounting** *threshold*] [**access** *threshold* [**access-timeout** *number-of-timeouts*]]}
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**aaa group server radius** *server-group-name* **Example:** `Router(config)# aaa group server radius myservergroup`	Enters server-group configuration mode.
Step 4	**throttle** {[**accounting** *threshold*] [**access** *threshold* [**access-timeout** *number-of-timeouts*]]} **Example:** `Router(config-sg-radius)# throttle accounting 100 access 200 access-timeout 2`	Configures the specified server-group throttling values for accounting and access request packets. For this example: • The accounting threshold value (the range is 0-65536) is set to 100, and the access threshold value is set to 200. **Note** The default threshold value is 0 (throttling disabled). • The number of time-outs per transaction value (the range is 1-10) is set to 2.

	Command or Action	Purpose
Step 5	**exit** **Example:** `Router(config-sg-radius)# exit`	Exits server-group configuration mode.

Configuration Examples for Throttling of AAA RADIUS Records

Throttling Accounting and Access Request Packets Globally Example

The following example shows how to limit the number of accounting requests sent to a server to 100:

```
enable
configure terminal
radius-server throttle accounting 100
```

The following example shows how to limit the number of access requests packets sent to a server to 200 and sets the number of time-outs allowed per transactions to 2:

```
enable
configure terminal
radius-server throttle access 200
radius-server throttle access 200 access-timeout 2
```

The following example shows how to throttle both accounting and access request packets:

```
enable
configure terminal
radius-server throttle accounting 100 access 200
```

Throttling Accounting and Access Request Packets Per Server Group Example

The following example shows how to limit the number of accounting requests sent to server-group-A to 100:

```
enable
configure terminal
aaa group server radius server-group-A
throttle accounting 100
```

The following example shows how to limit the number of access requests packets sent to server-group-A to 200 and sets the number of time-outs allowed per transactions to 2:

```
enable
configure terminal
aaa group server radius server-group-A
throttle access 200 access-timeout 2
```

The following example shows how to throttle both accounting and access request packets for server-group-A:

```
enable
configure terminal
```

```
aaa group server radius server-group-A
throttle accounting 100 access 200
```

Additional References

The following sections provide references related to the Throttling of AAA (RADIUS) Records feature.

Related Documents

Related Topic	Document Title
AAA and RADIUS	*Cisco IOS Security Configuration Guide: Securing User Services*, Release 15.0.

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	--

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information for Throttling of AAA RADIUS Records

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 4: Feature Information for Throttling of AAA (RADIUS) Records

Feature Name	Releases	Feature Information
Throttling of AAA (RADIUS) Records	Cisco IOS 15.2(1)E	The Throttling of AAA (RADIUS) Records feature supports throttling of access (authentication and authorization) and accounting records that are sent to the RADIUS server. This feature allows a user to configure the appropriate throttling rate to avoid network congestion and instability; such as when there is insufficient bandwidth to accommodate a sudden burst of records generated from the Cisco IOS router to the RADIUS server. The following commands were introduced or modified by this feature: **radius-server throttle, throttle**

CHAPTER **5**

MSCHAP Version 2

The MSCHAP Version 2 feature (introduced in Cisco IOS Release 12.2(2)XB5) allows Cisco routers to utilize Microsoft Challenge Handshake Authentication Protocol Version 2 (MSCHAP V2) authentication for PPP connections between a computer using a Microsoft Windows operating system and a network access server (NAS).

For Cisco IOS Release 12.4(6)T, MSCHAP V2 now supports a new feature: AAA Support for MSCHAPv2 Password Aging. Prior to Cisco IOS Release 12.4(6)T, when Password Authentication Protocol (PAP)-based clients sent username and password values to the authentication, authorization, and accounting (AAA) subsystem, AAA generated an authentication request to the RADIUS server. If the password expired, the RADIUS server replied with an authentication failure message. The reason for the authentication failure was not passed back to AAA subsystem; thus, users were denied access because of authentication failure but were not informed why they were denied access.

The Password Aging feature, available in Cisco IOS Release 12.4(6)T, notifies crypto-based clients that the password has expired and provides a generic way for the user to change the password. The Password Aging feature supports only crypto-based clients.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for MSCHAP Version 2

- Configure an interface type and enter interface configuration mode by using the **interface** command.

- Configure the interface for PPP encapsulation by using the **encapsulation** command.

- Be sure that the client operating system supports all MSCHAP V2 capabilities.

- For Cisco IOS Release 12.4(6)T, the Password Aging feature only supports RADIUS authentication for crypto-based clients.

- To ensure that the MSCHAP Version 2 features correctly interpret the authentication failure attributes sent by the RADIUS server, you must configure the **ppp max-bad-auth** command and set the number of authentication retries at two or more.

- In order for the MSCHAP Version 2 feature to support the ability to change a password, the authentication failure attribute, which is sent by the RADIUS server, must be correctly interpreted as described in Configuring MSCHAP V2 Authentication.

In addition, the **radius server vsa send authentication** command must be configured, allowing the RADIUS client to send a vendor-specific attribute to the RADIUS server. The Change Password feature is supported only for RADIUS authentication.

- The Microsoft Windows 2000, Microsoft Windows XP, and Microsoft Windows NT operating systems have a known caveat that prevents the Change Password feature from working. You must download a patch from Microsoft at the following URL:

http://support.microsoft.com/default.aspx?scid=kb;en-us;Q326770

For more information on completing these tasks, see the section "PPP Configuration " in the *Cisco IOS Dial Technologies Configuration Guide* , Release 12.4T. The RADIUS server must be configured for authentication. Refer to vendor-specific documentation for information on configuring RADIUS authentication on the RADIUS server.

Restrictions for MSCHAP Version 2

- MSCHAP V2 authentication is not compatible with MSCHAP V1 authentication.

- The change password option is supported only for RADIUS authentication and is not available for local authentication.

Information About MSCHAP Version 2

MSCHAP V2 authentication is the default authentication method used by the Microsoft Windows 2000 operating system. Cisco routers that support this authentication method enable Microsoft Windows 2000 operating system users to establish remote PPP sessions without configuring an authentication method on the client.

MSCHAP V2 authentication introduced an additional feature not available with MSCHAP V1 or standard CHAP authentication: the Change Password feature. This features allows the client to change the account password if the RADIUS server reports that the password has expired.

| Note | MSCHAP V2 authentication is an updated version of MSCHAP that is similar to but incompatible with MSCHAP Version 1 (V1). MSCHAP V2 introduces mutual authentication between peers and a Change Password feature. |

How to Configure MSCHAP Version 2

Configuring MSCHAP V2 Authentication

To configure the NAS to accept MSCHAP V2 authentication for local or RADIUS authentication and to allow proper interpretation of authentication failure attributes and vendor-specific RADIUS attributes for RADIUS authentication, use the following commands beginning in global configuration mode.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **radius-server vsa send authentication**
4. **interface** *type number*
5. **ppp max-bad-auth** *number*
6. **ppp authentication ms-chap-v2**
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose

Step 3	**radius-server vsa send authentication**
	
	Example:
	
	`Router(config)# radius-server vsa send`
	`authentication`
		Configures the NAS to recognize and use vendor-specific attributes.

Step 4	**interface** *type number* **Example:** `Router(config)# interface FastEthernet 0/1`	Configures an interface type and enters interface configuration mode.
Step 5	**ppp max-bad-auth** *number* **Example:** `Router(config-if)# ppp max-bad-auth 2`	Configures a point-to-point interface to reset immediately after an authentication failure or within a specified number of authentication retries. • The default value for the *number*argument is 0 seconds (immediately). • The range is between 0 and 255. **Note** The *number* argument must be set to a value of at least 2 for authentication failure attributes to be interpreted by the NAS.

Step 6	**ppp authentication ms-chap-v2**
	
	Example:
	
	`Router(config-if)# ppp authentication`
	`ms-chap-v2`
		Enables MSCHAP V2 authentication on a NAS.

Step 7	**end**
	
	Example:
	
	`Router(config-if)#`
	` end`
		Returns to privileged EXEC mode.

Verifying MSCHAP V2 Configuration

To verify that the MSCHAP Version 2 feature is configured properly, perform the following steps.

SUMMARY STEPS

1. **show running-config interface** *type number*
2. **debug ppp negotiation**
3. **debug ppp authentication**

DETAILED STEPS

	Command or Action	**Purpose**
Step 1	**show running-config interface** *type number* **Example:** `Router# show running-config interface Asynch65`	Verifies the configuration of MSCHAP V2 as the authentication method for the specified interface.
Step 2	**debug ppp negotiation** **Example:** `Router# debug ppp negotiation`	Verifies successful MSCHAP V2 negotiation.
Step 3	**debug ppp authentication** **Example:** `Router# debug ppp authentication`	Verifies successful MSCHAP V2 authentication.

Configuring Password Aging for Crypto-Based Clients

The AAA security services facilitate a variety of login authentication methods. Use the **aaa authentication login**command to enable AAA authentication no matter which of the supported login authentication methods you decide to use. With the **aaa authentication login**command, you create one or more lists of authentication methods that are tried at login. These lists are applied using the **login authentication** line configuration command.

After the RADIUS server requests a new password, AAA queries the crypto client, which in turn prompts the user to enter a new password.

To configure login authentication and password aging for crypto-based clients, use the following commands beginning in global configuration mode.

Note   The AAA Password Expiry infrastructure notifies the Easy VPN client that the password has expired and provides a generic way for the user to change the password. Please use RADIUS-server domain-stripping feature wisely in combination with AAA password expiry support.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication login** {**default** | *list-name*} **passwd-expiry** *method1* [*method2...*]
5. **crypto map** *map-name* **client authentication list** *list-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**aaa new-model** **Example:** Router(config)# aaa new-model	Enables AAA globally.
Step 4	**aaa authentication login** {**default**	*list-name*} **passwd-expiry** *method1* [*method2...*] **Example:** Router(config)# aaa authentication login userauthen passwd-expiry group radius	Enables password aging for crypto-based clients on a local authentication list.
Step 5	**crypto map** *map-name* **client authentication list** *list-name* **Example:** **Example:** Router(config)# crypto map clientmap client authentication list userauthen	Configures user authentication (a list of authentication methods) on an existing crypto map.

Configuration Examples

Configuring Local Authentication Example

The following example configures PPP on an asynchronous interface and enables MSCHAP V2 authentication locally:

```
interface Async65
  ip address 10.0.0.2 255.0.0.0
  encapsulation ppp
  async mode dedicated
  no peer default ip address
  ppp max-bad-auth 3
  ppp authentication ms-chap-v2
  username client password secret
```

Configuring RADIUS Authentication Example

The following example configures PPP on an asynchronous interface and enables MSCHAP V2 authentication via RADIUS:

```
interface Async65
  ip address 10.0.0.2 255.0.0.0
  encapsulation ppp
  async mode dedicated
  no peer default ip address
  ppp max-bad-auth 3
  ppp authentication ms-chap-v2
  exit
aaa authentication ppp default group radius
 radius-server host 10.0.0.2 255.0.0.0
 radius-server key secret
 radius-server vsa send authentication
```

Configuring Password Aging with Crypto Authentication Example

The following example configures password aging by using AAA with a crypto-based client:

```
aaa authentication login userauthen passwd-expiry group radius
!
aaa session-id common
!
crypto isakmp policy 3
 encr 3des
 authentication pre-share
 group 2
!
crypto isakmp client configuration group 3000client
 key cisco123
 dns 10.1.1.10
 wins 10.1.1.20
 domain cisco.com
 pool ippool
 acl 153
!
crypto ipsec transform-set myset esp-3des esp-sha-hmac
!
```

```
crypto dynamic-map dynmap 10
 set transform-set myset
!
crypto map clientmap client authentication list userauthen
!
radius-server host 10.140.15.203 auth-port 1645 acct-port 1646
radius-server domain-stripping prefix-delimiter $
radius-server key cisco123
radius-server vsa send authentication
radius-server vsa send authentication 3gpp2
!
end
```

Additional References

The following sections provide references related to the MSCHAP Version 2 feature.

Related Documents

Related Topic	Document Title
Configuring PPP interfaces	PPP Configuration in the *Cisco IOS Dial Technologies Configuration Guide* , Release 12.4T.
Descriptions of the tasks and commands necessary to configure and maintain Cisco networking devices	*Cisco IOS Dial Technologies Command Reference*
Lists of IOS Security Commands	*Cisco IOS Security Command Reference*
Configuring PPP authentication using AAA	Configuring PPP Authentication Using AAA in the Configuring Authentication module in the *Cisco IOS Security Configuration Guide: Securing User Services* , Release 12.4T.
Configuring RADIUS Authentication	Configuring RADIUS module in the *Cisco IOS Security Configuration Guide: Securing User Services*, Release 12.4T.

Standards

Standard	Title
No new or modified standards are supported by this feature.	--

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 1661	*Point-to-Point Protocol (PPP)*
RFC 2548	*Microsoft Vendor-specific RADIUS Attributes*
RFC 2759	*Microsoft PPP CHAP Extensions, Version 2*

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information for MSCHAP Version 2

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 5: Feature Information for MSCHAP Version 2

Feature Name	Releases	Feature Information
MSCHAP Version 2	Cisco IOS 15.2(1)E	The MSCHAP Version 2 feature (introduced in Cisco IOS Release 12.2(2)XB5) allows Cisco routers to utilize Microsoft Challenge Handshake Authentication Protocol Version 2 (MSCHAP V2) authentication for PPP connections between a computer using a Microsoft Windows operating system and a network access server (NAS). The following commands were introduced or modified: **aaa authentication login**, and **ppp authentication ms-chap-v2.**

MAC Authentication Bypass

The MAC Authentication Bypass feature is a MAC-address-based authentication mechanism that allows clients in a network to integrate with the Cisco Identity Based Networking Services (IBNS) and Network Admission Control (NAC) strategy using the client MAC address. The MAC Authentication Bypass feature is applicable to the following network environments:

- Network environments in which a supplicant code is not available for a given client platform.

- Network environments in which the end client configuration is not under administrative control, that is, the IEEE 802.1X requests are not supported on these networks.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Configuring MAC Authentication Bypass

IEEE 802.1x—Port-Based Network Access Control

You should understand the concepts of port-based network access control and have an understanding of how to configure port-based network access control on your Cisco platform. For more information, see the *Securing User Services Configuration Guide Library*.

RADIUS and ACLs

You should understand the concepts of the RADIUS protocol and have an understanding of how to create and apply access control lists (ACLs). For more information, see the documentation for your Cisco platform and the *Securing User Services Configuration Guide Library*.

The device must have a RADIUS configuration and be connected to the Cisco secure access control server (ACS). For more information, see the *User Guide for Secure ACS Appliance 3.2*.

Information About Configuring MAC Authentication Bypass

Overview of the Cisco IOS Auth Manager

The capabilities of devices connecting to a given network can be different, thus requiring that the network support different authentication methods and authorization policies. The Cisco IOS Auth Manager handles network authentication requests and enforces authorization policies regardless of authentication method. The Auth Manager maintains operational data for all port-based network connection attempts, authentications, authorizations, and disconnections and, as such, serves as a session manager.

The possible states for Auth Manager sessions are as follows:

- Idle—In the idle state, the authentication session has been initialized, but no methods have yet been run. This is an intermediate state.

- Running—A method is currently running. This is an intermediate state.

- Authc Success—The authentication method has run successfully. This is an intermediate state.

- Authc Failed—The authentication method has failed. This is an intermediate state.

- Authz Success—All features have been successfully applied for this session. This is a terminal state.

- Authz Failed—At least one feature has failed to be applied for this session. This is a terminal state.

- No methods—There were no results for this session. This is a terminal state.

How to Configure MAC Authentication Bypass

Enabling MAC Authentication Bypass

Perform this task to enable the MAC Authentication Bypass feature on an 802.1X port.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type slot* / *port*
4. **mab**
5. **end**
6. **show authentication sessions interface** *type slot* / *port* **details**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type slot* / *port* **Example:** `Device(config)# interface FastEthernet 2/1`	Enters interface configuration mode.
Step 4	**mab** **Example:** `Device(config-if)# mab`	Enables MAB.
Step 5	**end** **Example:** `Device(config-if)# end`	Returns to privileged EXEC mode.

	Command or Action	Purpose
Step 6	**show authentication sessions interface** *type slot* / *port* **details** **Example:** `Device# show authentication session interface FastEthernet 2/1 details`	Displays the interface configuration and the authenticator instances on the interface.

Enabling Reauthentication on a Port

By default, ports are not automatically reauthenticated. You can enable automatic reauthentication and specify how often reauthentication attempts are made.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type slot* / *port*
4. **switchport**
5. **switchport mode access**
6. **authentication port-control auto**
7. **mab** [**eap**]
8. **authentication periodic**
9. **authentication timer reauthenticate** {*seconds* | **server**}
10. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**interface** *type slot* / *port* **Example:** Device(config)# interface FastEthernet2/1	Enters interface configuration mode.
Step 4	**switchport** **Example:** Device(config-if)# switchport	Places interface in Layer 2 switched mode.
Step 5	**switchport mode access** **Example:** Device(config-if)# switchport mode access	Sets the interface type as a nontrunking, nontagged single VLAN Layer 2 interface.
Step 6	**authentication port-control auto** **Example:** Device(config-if)# authentication port-control auto	Configures the authorization state of the port.
Step 7	**mab** [**eap**] **Example:** Device(config-if)# mab	Enables MAB.
Step 8	**authentication periodic** **Example:** Device(config-if)# authentication periodic	Enables reauthentication.
Step 9	**authentication timer reauthenticate** {*seconds* | **server**} **Example:** Device(config-if)# authentication timer reauthenticate 900	Configures the time, in seconds, between reauthentication attempts.
Step 10	**end** **Example:** Device(config-if)# end	Exits interface configuration mode and returns to privileged EXEC mode.

Specifying the Security Violation Mode

When there is a security violation on a port, the port can be shut down or traffic can be restricted. By default, the port is shut down. You can configure the period of time for which the port is shut down.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type slot* / *port*
4. **switchport**
5. **switchport mode access**
6. **authentication port-control auto**
7. **mab** [**eap**]
8. **authentication violation** {**restrict** | **shutdown**}
9. **authentication timer restart** *seconds*
10. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type slot* / *port* **Example:** `Device(config)# interface FastEthernet2/1`	Enters interface configuration mode.
Step 4	**switchport** **Example:** `Device(config-if)# switchport`	Places interface in Layer 2 switched mode.

	Command or Action	**Purpose**
Step 5	**switchport mode access** **Example:** Device(config-if)# switchport mode access	Sets the interface type as a nontrunking, nontagged single VLAN Layer 2 interface.
Step 6	**authentication port-control auto** **Example:** Device(config-if)# authentication port-control auto	Configures the authorization state of the port.
Step 7	**mab** [**eap**] **Example:** Device(config-if)# mab	Enables MAB.
Step 8	**authentication violation** {**restrict**	**shutdown**} **Example:** Device(config-if)# authentication violation shutdown	Configures the action to be taken when a security violation occurs on the port.
Step 9	**authentication timer restart** *seconds* **Example:** Device(config-if)# authentication timer restart 30	Configures the period of time, in seconds, after which an attempt is made to authenticate an unauthorized port.
Step 10	**end** **Example:** Device(config-if)# end	Exits interface configuration mode and returns to privileged EXEC mode.

Configuration Examples for MAC Authentication Bypass

Example: MAC Authentication Bypass Configuration

In the following example, the **mab** command has been configured to enable the MAC Authorization Bypass (MAB) feature on the specified interface. The optional **show authentication sessions** command has been enabled to display the interface configuration and the authentication instances on the interface.

```
Device> enable
Device# configure terminal
Device(config)# interface GigabitEthernet2/1
Device(config-if)# mab
Device(config-if)# end
Device# show authentication sessions interface GigabitEthernet2/1 details
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Authentication commands	*Cisco IOS Security Command Reference*
IEEE 802.1x—Flexible Authentication	*Securing User Services Configuration Library*

MIBs

MIB	MIBs Link
• CISCO-AUTH-FRAMEWORK-MIB • CISCO-MAC-AUTH-BYPASS-MIB • CISCO-PAE-MIB • IEEE8021-PAE-MIB	To locate and download MIBs for selected platforms, Cisco IOS software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 3580	*IEEE 802.1x Remote Authentication Dial In User Service (RADIUS)*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for MAC Authentication Bypass

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 6: Feature Information for MAC Authentication Bypass

Feature Name	Releases	Feature Information
MAC Authentication Bypass (MAB)	Cisco IOS 15.2(1)E	The MAC Authentication Bypass feature is a MAC-address-based authentication mechanism that allows clients in a network to integrate with the Cisco IBNS and NAC strategy using the client MAC address. The following commands were introduced or modified: **dot1x mac-auth-bypass**, **show dot1x interface**.

Configurable MAB Username and Password

The Configurable MAB Username and Password feature enables you to configure a MAC Authentication Bypass (MAB) username format and password to allow interoperability between the Cisco IOS Authentication Manager and existing MAC databases and RADIUS servers.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About Configurable MAB Username and Password

Overview of the Configurable MAB Username and Password

A MAC Authentication Bypass (MAB) operation involves authentication using RADIUS Access-Request packets with both the username and password attributes. By default, the username and the password values are the same and contain the MAC address. The Configurable MAB Username and Password feature enables you to configure both the username and the password attributes in the following scenarios:

- To enable MAB for an existing large database that uses formatted username attributes, the username format in the client MAC needs to be configured. Use the **mab request format attribute 1** command to configure the username format.

- Some databases do not accept authentication if the username and password values are the same. In such instances, the password needs to be configured to ensure that the password is different from the username. Use the **mab request format attribute 2** command to configure the password.

The Configurable MAB Username and Password feature allows interoperability between the Cisco IOS Authentication Manager and the existing MAC databases and RADIUS servers. The password is a global password and hence is the same for all MAB authentications and interfaces. This password is also synchronized across all supervisor devices to achieve high availability.

If the password is not provided or configured, the password uses the same value as the username. The table below describes the formatting of the username and the password:

MAC Address	Username Format (Group Size, Separator)	Username	Password Configured	Password Created
08002b8619de	(1, :) (1, -) (1, .)	0:8:0:0:2:b:8:6:1:9:d:e 0-8-0-0-2-b-8-6-1-9-d-e 0.8.0.0.2.b.8.6.1.9.d.e	None	0:8:0:0:2:b:8:6:1:9:d:e 0-8-0-0-2-b-8-6-1-9-d-e 0.8.0.0.2.b.8.6.1.9.d.e
08002b8619de	(1, :) (1, -) (1, .)	0:8:0:0:2:b:8:6:1:9:d:e 0-8-0-0-2-b-8-6-1-9-d-e 0.8.0.0.2.b.8.6.1.9.d.e	Password	Password
08002b8619de	(2, :) (2, -) (2, .)	08:00:2b:86:19:de 08-00-2b-86-19-de 08.00.2b.86.19.de	None	08:00:2b:86:19:de 08-00-2b-86-19-de 08.00.2b.86.19.de
08002b8619de	(2, :) (2, -) (2, .)	08:00:2b:86:19:de 08-00-2b-86-19-de 08.00.2b.86.19.de	Password	Password
08002b8619de	(4, :) (4, -) (4, .)	0800:2b86:19de 0800-2b86-19de 0800.2b86.19de	None	0800:2b86:19de 0800-2b86-19de 0800.2b86.19de
08002b8619de	(4, :) (4, -) (4, .)	0800:2b86:19de 0800-2b86-19de 0800.2b86.19de	Password	Password
08002b8619de	(12, <not applicable>)	08002b8619de	None	08002b8619de

MAC Address	Username Format (Group Size, Separator)	Username	Password Configured	Password Created
08002b8619de	(12, <not applicable>)	08002b8619de	Password	Password

For more information on configuring MAB, see the "Configuring MAC Authentication Bypass" chapter in the *Authentication, Authorization, and Accounting Configuration Guide*.

How to Configure Configurable MAB Username and Password

Enabling Configurable MAB Username and Password

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mab request format attribute 1 groupsize {1 | 2 | 4 | 12} separator {- | : | .} [lowercase | uppercase]**
4. **mab request format attribute 2 [0 | 7]** *password*
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Device# configure terminal	Enters global configuration mode.
Step 3	**mab request format attribute 1 groupsize {1	2	4	12} separator {-	:	.} [lowercase	uppercase]** **Example:** Device(config)# mab request format attribute 1 groupsize 2 separator :	Configures the username format for MAB requests.

	Command or Action	Purpose

Step 4	**mab request format attribute 2** [**0** | **7**] *password*
	
	Example:
	`Device(config)# mab request format attribute 2`
	`password1`
		Configures a global password for all MAB requests.

Step 5	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Configuration Examples for Configurable MAB Username and Password

Example: Enabling Configurable MAB Username and Password

The following example shows how to configure the username format and password for MAC Authentication Bypass (MAB). In this example, the username format is configured as a group of 12 hexadecimal digits with no separator and the global password as **password1**.

```
Device> enable
Device# configure terminal
Device(config)# mab request format attribute 1 groupsize 2 separator :
Device(config)# mab request format attribute 2 password1
Device(config)# end
```

Additional References for Configurable MAB Username and Password

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases

Related Topic	Document Title
Security commands	• Cisco IOS Security Command Reference: Commands A to C • Cisco IOS Security Command Reference: Commands D to L • Cisco IOS Security Command Reference: Commands M to R • Cisco IOS Security Command Reference: Commands S to Z
Configuring MAC Authentication Bypass	*Authentication, Authorization, and Accounting Configuration Guide*

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature Information for Configurable MAB Username and Password

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 7: Feature Information for Configurable MAB Username and Password

Feature Name	Releases	Feature Information
Configurable MAB Username and Password	Cisco IOS 15.2(1)E	The Configurable MAB Username and Password feature enables you to configure MAC Authentication Bypass (MAB) username format and password to allow interoperability between the Cisco IOS Authentication Manager and existing MAC databases and RADIUS servers.
		The following commands were introduced or modified: **mab request format attribute 1**, **mab request format attribute 2**.

Configuring Accounting

The AAA Accounting feature allows the services that users are accessing and the amount of network resources that users are consuming to be tracked. When AAA Accounting is enabled, the network access server reports user activity to the TACACS+ or RADIUS security server (depending on which security method is implemented) in the form of accounting records. Each accounting record contains accounting attribute-value (AV) pairs and is stored on the security server. This data can then be analyzed for network management, client billing, and auditing.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Configuring Accounting

The following tasks must be performed before configuring accounting using named method lists:

- Enable AAA on the network access server by using the **aaa new-model**command in global configuration mode.

- Define the characteristics of the RADIUS or TACACS+ security server if RADIUS or TACACS+ authorization is issued. For more information about configuring the Cisco network access server to communicate with the RADIUS security server, see the Configuring RADIUS module. For more information about configuring the Cisco network access server to communicate with the TACACS+ security server, see the Configuring TACACS+ module.

Restrictions for Configuring Accounting

- Accounting information can be sent simultaneously to a maximum of only four AAA servers.

- For Service Selection Gateway (SSG) systems, the **aaa accounting network broadcast** command broadcasts only **start-stop** accounting records. If interim accounting records are configured using the **ssg accounting interval** command, the interim accounting records are sent only to the configured default RADIUS server.

Information About Configuring Accounting

Named Method Lists for Accounting

Similar to authentication and authorization method lists, method lists for accounting define the way accounting is performed and the sequence in which these methods are performed.

Named accounting method lists allow particular security protocol to be designated and used on specific lines or interfaces for accounting services. The only exception is the default method list (which is named "default"). The default method list is automatically applied to all interfaces except those that have a named method list explicitly defined. A defined method list overrides the default method list.

A method list is simply a named list describing the accounting methods to be queried (such as RADIUS or TACACS+), in sequence. Method lists allow one or more security protocols to be designated and used for accounting, thus ensuring a backup system for accounting in case the initial method fails. Cisco IOS software uses the first method listed to support accounting; if that method fails to respond, the Cisco IOS software selects the next accounting method listed in the method list. This process continues until there is successful communication with a listed accounting method, or all methods defined are exhausted.

Note The Cisco IOS software attempts accounting with the next listed accounting method only when there is no response from the previous method. If accounting fails at any point in this cycle--meaning that the security server responds by denying the user access--the accounting process stops and no other accounting methods are attempted.

Accounting method lists are specific to the type of accounting being requested. AAA supports seven different types of accounting:

- **Network** --Provides information for all PPP, SLIP, or ARAP sessions, including packet and byte counts.

- **EXEC** --Provides information about user EXEC terminal sessions of the network access server.

- **Commands** --Provides information about the EXEC mode commands that a user issues. Command accounting generates accounting records for all EXEC mode commands, including global configuration commands, associated with a specific privilege level.

- **Connection** --Provides information about all outbound connections made from the network access server, such as Telnet, local-area transport (LAT), TN3270, packet assembler/disassembler (PAD), and rlogin.

- **System** --Provides information about system-level events.

- **Resource** --Provides "start" and "stop" records for calls that have passed user authentication, and provides "stop" records for calls that fail to authenticate.

- **VRRS** --Provides information about Virtual Router Redundancy Service (VRRS).

Note System accounting does not use named accounting lists; only the default list for system accounting can be defined.

Once again, when a named method list is created, a particular list of accounting methods for the indicated accounting type are defined.

Accounting method lists must be applied to specific lines or interfaces before any of the defined methods are performed. The only exception is the default method list (which is named "default"). If the **aaa accounting** command for a particular accounting type is issued without specifying a named method list, the default method list is automatically applied to all interfaces or lines except those that have a named method list explicitly defined (A defined method list overrides the default method list). If no default method list is defined, then no accounting takes place.

This section includes the following subsections:

Method Lists and Server Groups

A server group is a way to group existing RADIUS or TACACS+ server hosts for use in method lists. The figure below shows a typical AAA network configuration that includes four security servers: R1 and R2 are RADIUS servers, and T1 and T2 are TACACS+ servers. R1 and R2 comprise the group of RADIUS servers. T1 and T2 comprise the group of TACACS+ servers.

Cisco IOS software, RADIUS and TACACS+ server configurations are global. A subset of the configured server hosts can be specified using server groups. These server groups can be used for a particular service. For example, server groups allow R1 and R2 to be defined as separate server groups (SG1 and SG2), and T1 and T2 as separate server groups (SG3 and SG4). This means either R1 and T1 (SG1 and SG3) or R2 and T2 (SG2 and SG4) can be specified in the method list, which provides more flexibility in the way that RADIUS and TACACS+ resources are assigned.

Server groups also can include multiple host entries for the same server, as long as each entry has a unique identifier. The combination of an IP address and a UDP port number creates a unique identifier, allowing different ports to be individually defined as RADIUS hosts providing a specific AAA service. In other words, this unique identifier enables RADIUS requests to be sent to different UDP ports on a server from the same IP address. If two different host entries on the same RADIUS server are configured for the same service--for example, accounting--the second host entry configured acts as failover backup to the first one. Using this example, if the first host entry fails to provide accounting services, the network access server tries the second

host entry configured on the same device for accounting services (The RADIUS host entries are tried in the order in which they are configured).

For more information about configuring server groups and about configuring server groups based on Dialed Number Identification Service (DNIS) numbers, see the "Configuring RADIUS" or "Configuring TACACS+" module in the Cisco IOS Security Configuration Guide: Securing User Services .

AAA Accounting Methods

The Cisco IOS software supports the following two methods for accounting:

- TACACS+--The network access server reports user activity to the TACACS+ security server in the form of accounting records. Each accounting record contains accounting AV pairs and is stored on the security server.

- RADIUS--The network access server reports user activity to the RADIUS security server in the form of accounting records. Each accounting record contains accounting AV pairs and is stored on the security server.

Note   With CSCuc32663, passwords and accounting logs are masked before being sent to the TACACS+ or RADIUS security servers. Use the **aaa accounting commands visible-keys** command to send unmasked information to the TACACS+ or RADIUS security servers.

Accounting Record Types

For minimal accounting, use the **stop-only** keyword, which instructs the specified method (**RADIUS** or **TACACS+**) to send a stop record accounting notice at the end of the requested user process. For more accounting information, use the **start-stop** keyword to send a start accounting notice at the beginning of the requested event and a stop accounting notice at the end of the event. To stop all accounting activities on this line or interface, use the **none** keyword.

Accounting Methods

The table below lists the supported accounting methods.

Table 8: AAA Accounting Methods

Keyword	Description
group radius	Uses the list of all RADIUS servers for accounting.
group tacacs+	Uses the list of all TACACS+ servers for accounting.
group *group-name*	Uses a subset of RADIUS or TACACS+ servers for accounting as defined by the server group *group-name*.

The method argument refers to the actual method the authentication algorithm tries. Additional methods of authentication are used only if the previous method returns an error, not if it fails. To specify that the authentication should succeed even if all other methods return an error, specify additional methods in the command. For example, to create a method list named acct_tac1 that specifies RADIUS as the backup method of authentication in the event that TACACS+ authentication returns an error, enter the following command:

```
aaa accounting network acct_tac1 stop-only group tacacs+ group radius
```
To create a default list that is used when a named list is not specified in the **aaa accounting**command, use the **default** keyword followed by the methods that are wanted to be used in default situations. The default method list is automatically applied to all interfaces.

For example, to specify RADIUS as the default method for user authentication during login, enter the following command:

```
aaa accounting network default stop-only group radius
```
AAA Accounting supports the following methods:

- **group tacacs** --To have the network access server send accounting information to a TACACS+ security server, use the **group tacacs+** *method* keyword.

- **group radius** --To have the network access server send accounting information to a RADIUS security server, use the **group radius** *method* keyword.

Note   Accounting method lists for SLIP follow whatever is configured for PPP on the relevant interface. If no lists are defined and applied to a particular interface (or no PPP settings are configured), the default setting for accounting applies.

- **group** *group-name* --To specify a subset of RADIUS or TACACS+ servers to use as the accounting method, use the **aaa accounting**command with the **group** *group-name* method. To specify and define the group name and the members of the group, use the **aaa group server** command. For example, use the **aaa group server** command to first define the members of **group loginrad**:

```
aaa group server radius loginrad
 server 172.16.2.3
 server 172.16.2 17
 server 172.16.2.32
```
This command specifies RADIUS servers 172.16.2.3, 172.16.2.17, and 172.16.2.32 as members of the **group loginrad**.

To specify **group loginrad** as the method of network accounting when no other method list has been defined, enter the following command:

```
aaa accounting network default start-stop group loginrad
```
Before a group name can be used as the accounting method, communication with the RADIUS or TACACS+ security server must be enabled.

AAA Accounting Types

Network Accounting

Network accounting provides information for all PPP, SLIP, or ARAP sessions, including packet and byte counts.

The following example shows the information contained in a RADIUS network accounting record for a PPP user who comes in through an EXEC session:

```
Wed Jun 27 04:44:45 2001
        NAS-IP-Address = "172.16.25.15"
        NAS-Port = 5
        User-Name = "username1"
        Client-Port-DNIS = "4327528"
        Caller-ID = "562"
        Acct-Status-Type = Start
        Acct-Authentic = RADIUS
        Service-Type = Exec-User
        Acct-Session-Id = "0000000D"
        Acct-Delay-Time = 0
        User-Id = "username1"
        NAS-Identifier = "172.16.25.15"

Wed Jun 27 04:45:00 2001
        NAS-IP-Address = "172.16.25.15"
        NAS-Port = 5
        User-Name = "username1"
        Client-Port-DNIS = "4327528"
        Caller-ID = "562"
        Acct-Status-Type = Start
        Acct-Authentic = RADIUS
        Service-Type = Framed
        Acct-Session-Id = "0000000E"
        Framed-IP-Address = "10.1.1.2"
        Framed-Protocol = PPP
        Acct-Delay-Time = 0
        User-Id = "username1"
        NAS-Identifier = "172.16.25.15"
Wed Jun 27 04:47:46 2001
        NAS-IP-Address = "172.16.25.15"
        NAS-Port = 5
        User-Name = "username1"
        Client-Port-DNIS = "4327528"
        Caller-ID = "562"
        Acct-Status-Type = Stop
        Acct-Authentic = RADIUS
        Service-Type = Framed
        Acct-Session-Id = "0000000E"
        Framed-IP-Address = "10.1.1.2"
        Framed-Protocol = PPP
        Acct-Input-Octets = 3075
        Acct-Output-Octets = 167
        Acct-Input-Packets = 39
        Acct-Output-Packets = 9
        Acct-Session-Time = 171
        Acct-Delay-Time = 0
        User-Id = "username1"
        NAS-Identifier = "172.16.25.15"
Wed Jun 27 04:48:45 2001
        NAS-IP-Address = "172.16.25.15"
        NAS-Port = 5
        User-Name = "username1"
```

```
               Client-Port-DNIS = "4327528"
               Caller-ID = "408"
               Acct-Status-Type = Stop
               Acct-Authentic = RADIUS
               Service-Type = Exec-User
               Acct-Session-Id = "0000000D"
               Acct-Delay-Time = 0
               User-Id = "username1"
               NAS-Identifier = "172.16.25.15"
```

The following example shows the information contained in a TACACS+ network accounting record for a PPP user who first started an EXEC session:

```
Wed Jun 27 04:00:35 2001 172.16.25.15    username1   tty4    562/4327528     starttask_id=28
      service=shell
Wed Jun 27 04:00:46 2001 172.16.25.15    username1   tty4 562/4327528        starttask_id=30
      addr=10.1.1.1    service=ppp
Wed Jun 27 04:00:49 2001 172.16.25.15    username1   tty4    408/4327528     update
task_id=30       addr=10.1.1.1   service=ppp     protocol=ip      addr=10.1.1.1
Wed Jun 27 04:01:31 2001 172.16.25.15    username1   tty4   562/4327528      stoptask_id=30
      addr=10.1.1.1    service=ppp     protocol=ip      addr=10.1.1.1    bytes_in=2844
  bytes_out=1682  paks_in=36       paks_out=24       elapsed_time=51
Wed Jun 27 04:01:32 2001 172.16.25.15    username1   tty4   562/4327528      stoptask_id=28
      service=shell   elapsed_time=57
```

Note   The precise format of accounting packets records may vary depending on the security server daemon.

The following example shows the information contained in a RADIUS network accounting record for a PPP user who comes in through autoselect:

```
Wed Jun 27 04:30:52 2001
        NAS-IP-Address = "172.16.25.15"
        NAS-Port = 3
        User-Name = "username1"
        Client-Port-DNIS = "4327528"
        Caller-ID = "562"
        Acct-Status-Type = Start
        Acct-Authentic = RADIUS
        Service-Type = Framed
        Acct-Session-Id = "0000000B"
        Framed-Protocol = PPP
        Acct-Delay-Time = 0
        User-Id = "username1"
        NAS-Identifier = "172.16.25.15"

Wed Jun 27 04:36:49 2001
        NAS-IP-Address = "172.16.25.15"
        NAS-Port = 3
        User-Name = "username1"
        Client-Port-DNIS = "4327528"
        Caller-ID = "562"
        Acct-Status-Type = Stop
        Acct-Authentic = RADIUS
        Service-Type = Framed
        Acct-Session-Id = "0000000B"
        Framed-Protocol = PPP
        Framed-IP-Address = "10.1.1.1"
        Acct-Input-Octets = 8630
        Acct-Output-Octets = 5722
        Acct-Input-Packets = 94
        Acct-Output-Packets = 64
        Acct-Session-Time = 357
        Acct-Delay-Time = 0
        User-Id = "username1"
        NAS-Identifier = "172.16.25.15"
```

The following example shows the information contained in a TACACS+ network accounting record for a PPP user who comes in through autoselect:

```
Wed Jun 27 04:02:19 2001 172.16.25.15   username1  Async5 562/4327528    starttask_id=35
      service=ppp
Wed Jun 27 04:02:25 2001 172.16.25.15   username1  Async5 562/4327528    update
task_id=35      service=ppp      protocol=ip      addr=10.1.1.2
Wed Jun 27 04:05:03 2001 172.16.25.15   username1  Async5 562/4327528    stoptask_id=35
      service=ppp      protocol=ip      addr=10.1.1.2  bytes_in=3366  bytes_out=2149
  paks_in=42      paks_out=28      elapsed_time=164
```

EXEC Accounting

EXEC accounting provides information about user EXEC terminal sessions (user shells) on the network access server, including username, date, start and stop times, the access server IP address, and (for dial-in users) the telephone number the call originated from.

The following example shows the information contained in a RADIUS EXEC accounting record for a dial-in user:

```
Wed Jun 27 04:26:23 2001
        NAS-IP-Address = "172.16.25.15"
        NAS-Port = 1
        User-Name = "username1"
        Client-Port-DNIS = "4327528"
        Caller-ID = "5622329483"
        Acct-Status-Type = Start
        Acct-Authentic = RADIUS
        Service-Type = Exec-User
        Acct-Session-Id = "00000006"
        Acct-Delay-Time = 0
        User-Id = "username1"
        NAS-Identifier = "172.16.25.15"
Wed Jun 27 04:27:25 2001
        NAS-IP-Address = "172.16.25.15"
        NAS-Port = 1
        User-Name = "username1"
        Client-Port-DNIS = "4327528"
        Caller-ID = "5622329483"
        Acct-Status-Type = Stop
        Acct-Authentic = RADIUS
        Service-Type = Exec-User
        Acct-Session-Id = "00000006"
        Acct-Session-Time = 62
        Acct-Delay-Time = 0
        User-Id = "username1"
        NAS-Identifier = "172.16.25.15"
```

The following example shows the information contained in a TACACS+ EXEC accounting record for a dial-in user:

```
Wed Jun 27 03:46:21 2001      172.16.25.15   username1  tty3   5622329430/4327528
start   task_id=2      service=shell
Wed Jun 27 04:08:55 2001      172.16.25.15   username1  tty3   5622329430/4327528
stop   task_id=2      service=shell  elapsed_time=1354
```

The following example shows the information contained in a RADIUS EXEC accounting record for a Telnet user:

```
Wed Jun 27 04:48:32 2001
        NAS-IP-Address = "172.16.25.15"
        NAS-Port = 26
        User-Name = "username1"
        Caller-ID = "10.68.202.158"
```

```
        Acct-Status-Type = Start
        Acct-Authentic = RADIUS
        Service-Type = Exec-User
        Acct-Session-Id = "00000010"
        Acct-Delay-Time = 0
        User-Id = "username1"
        NAS-Identifier = "172.16.25.15"

Wed Jun 27 04:48:46 2001
        NAS-IP-Address = "172.16.25.15"
        NAS-Port = 26
        User-Name = "username1"
        Caller-ID = "10.68.202.158"
        Acct-Status-Type = Stop
        Acct-Authentic = RADIUS
        Service-Type = Exec-User
        Acct-Session-Id = "00000010"
        Acct-Session-Time = 14
        Acct-Delay-Time = 0
        User-Id = "username1"
        NAS-Identifier = "172.16.25.15"
```

The following example shows the information contained in a TACACS+ EXEC accounting record for a Telnet user:

```
Wed Jun 27 04:06:53 2001        172.16.25.15    username1   tty26   10.68.202.158
starttask_id=41      service=shell
Wed Jun 27 04:07:02 2001        172.16.25.15    username1   tty26   10.68.202.158
stoptask_id=41       service=shell   elapsed_time=9
```

Command Accounting

Command accounting provides information about the EXEC shell commands for a specified privilege level that are being executed on a network access server. Each command accounting record includes a list of the commands executed for that privilege level, as well as the date and time each command was executed, and the user who executed it.

The following example shows the information contained in a TACACS+ command accounting record for privilege level 1:

```
Wed Jun 27 03:46:47 2001        172.16.25.15    username1   tty3   5622329430/4327528
stop    task_id=3       service=shell   priv-lvl=1      cmd=show version <cr>
Wed Jun 27 03:46:58 2001        172.16.25.15    username1   tty3   5622329430/4327528
stop    task_id=4       service=shell   priv-lvl=1      cmd=show interfaces Ethernet 0
<cr>
Wed Jun 27 03:47:03 2001        172.16.25.15    username1   tty3   5622329430/4327528
stop    task_id=5       service=shell   priv-lvl=1      cmd=show ip route <cr>
```

The following example shows the information contained in a TACACS+ command accounting record for privilege level 15:

```
Wed Jun 27 03:47:17 2001        172.16.25.15    username1   tty3   5622329430/4327528
stop    task_id=6       service=shell   priv-lvl=15     cmd=configure terminal <cr>
Wed Jun 27 03:47:21 2001        172.16.25.15    username1   tty3   5622329430/4327528
stop    task_id=7       service=shell   priv-lvl=15     cmd=interface Serial 0 <cr>
Wed Jun 27 03:47:29 2001        172.16.25.15    username1   tty3   5622329430/4327528
stop    task_id=8       service=shell   priv-lvl=15     cmd=ip address 10.1.1.1 255.255.255.0
 <cr>
```

Note   The Cisco implementation of RADIUS does not support command accounting.

Connection Accounting

Connection accounting provides information about all outbound connections made from the network access server such as Telnet, LAT, TN3270, PAD, and rlogin.

The following example shows the information contained in a RADIUS connection accounting record for an outbound Telnet connection:

```
Wed Jun 27 04:28:00 2001
        NAS-IP-Address = "172.16.25.15"
        NAS-Port = 2
        User-Name = "username1"
        Client-Port-DNIS = "4327528"
        Caller-ID = "5622329477"
        Acct-Status-Type = Start
        Acct-Authentic = RADIUS
        Service-Type = Login
        Acct-Session-Id = "00000008"
        Login-Service = Telnet
        Login-IP-Host = "10.68.202.158"
        Acct-Delay-Time = 0
        User-Id = "username1"
        NAS-Identifier = "172.16.25.15"

Wed Jun 27 04:28:39 2001
        NAS-IP-Address = "172.16.25.15"
        NAS-Port = 2
        User-Name = "username1"
        Client-Port-DNIS = "4327528"
        Caller-ID = "5622329477"
        Acct-Status-Type = Stop
        Acct-Authentic = RADIUS
        Service-Type = Login
        Acct-Session-Id = "00000008"
        Login-Service = Telnet
        Login-IP-Host = "10.68.202.158"
        Acct-Input-Octets = 10774
        Acct-Output-Octets = 112
        Acct-Input-Packets = 91
        Acct-Output-Packets = 99
        Acct-Session-Time = 39
        Acct-Delay-Time = 0
        User-Id = "username1"
        NAS-Identifier = "172.16.25.15"
```

The following example shows the information contained in a TACACS+ connection accounting record for an outbound Telnet connection:

```
Wed Jun 27 03:47:43 2001          172.16.25.15    username1    tty3    5622329430/4327528
start    task_id=10     service=connection     protocol=telnet addr=10.68.202.158 cmd=telnet
 username1-sun
Wed Jun 27 03:48:38 2001          172.16.25.15    username1    tty3    5622329430/4327528
stop    task_id=10     service=connection     protocol=telnet addr=10.68.202.158 cmd=telnet
 username1-sun    bytes_in=4467    bytes_out=96    paks_in=61     paks_out=72 elapsed_time=55
```

The following example shows the information contained in a RADIUS connection accounting record for an outbound rlogin connection:

```
Wed Jun 27 04:29:48 2001
        NAS-IP-Address = "172.16.25.15"
        NAS-Port = 2
        User-Name = "username1"
        Client-Port-DNIS = "4327528"
        Caller-ID = "5622329477"
        Acct-Status-Type = Start
```

```
            Acct-Authentic = RADIUS
            Service-Type = Login
            Acct-Session-Id = "0000000A"
            Login-Service = Rlogin
            Login-IP-Host = "10.68.202.158"
            Acct-Delay-Time = 0
            User-Id = "username1"
            NAS-Identifier = "172.16.25.15"

Wed Jun 27 04:30:09 2001
            NAS-IP-Address = "172.16.25.15"
            NAS-Port = 2
            User-Name = "username1"
            Client-Port-DNIS = "4327528"
            Caller-ID = "5622329477"
            Acct-Status-Type = Stop
            Acct-Authentic = RADIUS
            Service-Type = Login
            Acct-Session-Id = "0000000A"
            Login-Service = Rlogin
            Login-IP-Host = "10.68.202.158"
            Acct-Input-Octets = 18686
            Acct-Output-Octets = 86
            Acct-Input-Packets = 90
            Acct-Output-Packets = 68
            Acct-Session-Time = 22
            Acct-Delay-Time = 0
            User-Id = "username1"
            NAS-Identifier = "172.16.25.15"
```

The following example shows the information contained in a TACACS+ connection accounting record for an outbound rlogin connection:

```
Wed Jun 27 03:48:46 2001        172.16.25.15    username1  tty3   5622329430/4327528
start    task_id=12      service=connection    protocol=rlogin addr=10.68.202.158 cmd=rlogin
 username1-sun /user username1
Wed Jun 27 03:51:37 2001        172.16.25.15    username1  tty3   5622329430/4327528
stop    task_id=12      service=connection    protocol=rlogin addr=10.68.202.158 cmd=rlogin
 username1-sun /user username1 bytes_in=659926 bytes_out=138   paks_in=2378    paks_
out=1251        elapsed_time=171
```

The following example shows the information contained in a TACACS+ connection accounting record for an outbound LAT connection:

```
Wed Jun 27 03:53:06 2001        172.16.25.15    username1  tty3   5622329430/4327528
start    task_id=18      service=connection     protocol=lat     addr=VAX        cmd=lat
VAX
Wed Jun 27 03:54:15 2001        172.16.25.15    username1  tty3   5622329430/4327528
stop    task_id=18      service=connection     protocol=lat     addr=VAX        cmd=lat
VAX  bytes_in=0      bytes_out=0      paks_in=0      paks_out=0       elapsed_time=6
```

System Accounting

System accounting provides information about all system-level events (for example, when the system reboots or when accounting is turned on or off).

The following accounting record shows a typical TACACS+ system accounting record server indicating that AAA Accounting has been turned off:

```
Wed Jun 27 03:55:32 2001        172.16.25.15    unknown unknown unknown start    task_id=25
    service=system  event=sys_acct  reason=reconfigure
```

Note The precise format of accounting packets records may vary depending on the TACACS+ daemon.

The following accounting record shows a TACACS+ system accounting record indicating that AAA Accounting has been turned on:

```
Wed Jun 27 03:55:22 2001        172.16.25.15    unknown unknown unknown stop    task_id=23
    service=system  event=sys_acct  reason=reconfigure
```

Additional tasks for measuring system resources are covered in the Cisco IOS software configuration guides. For example, IP accounting tasks are described in the Configuring IP Services chapter in the *CiscoIOS Application Services Configuration Guide* .

Resource Accounting

The Cisco implementation of AAA accounting provides "start" and "stop" record support for calls that have passed user authentication. The additional feature of generating "stop" records for calls that fail to authenticate as part of user authentication is also supported. Such records are necessary for users employing accounting records to manage and monitor their networks.

This section includes the following subsections:

AAA Resource Failure Stop Accounting

Before AAA resource failure stop accounting, there was no method of providing accounting records for calls that failed to reach the user authentication stage of a call setup sequence. Such records are necessary for users employing accounting records to manage and monitor their networks and their wholesale customers.

This functionality generates a "stop" accounting record for any calls that do not reach user authentication; "stop" records are generated from the moment of call setup. All calls that pass user authentication behave as they did before; that is, no additional accounting records are seen.

The figure below illustrates a call setup sequence with normal call flow (no disconnect) and without AAA resource failure stop accounting enabled.

Figure 1: Modem Dial-In Call Setup Sequence With Normal Flow and Without Resource Failure Stop Accounting Enabled
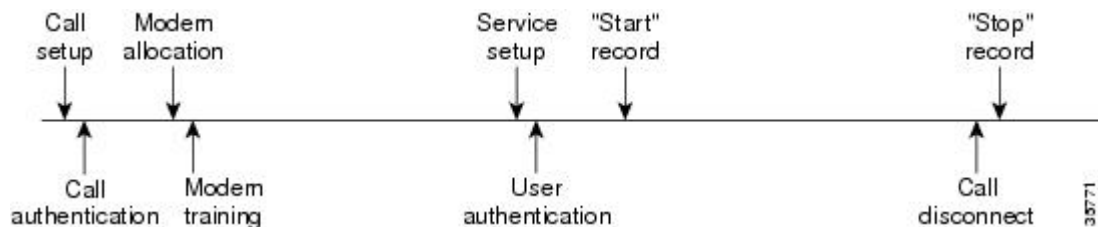
The figure below illustrates a call setup sequence with normal call flow (no disconnect) and with AAA resource failure stop accounting enabled.

Figure 2: Modem Dial-In Call Setup Sequence With Normal Flow and WIth Resource Failure Stop Accounting Enabled
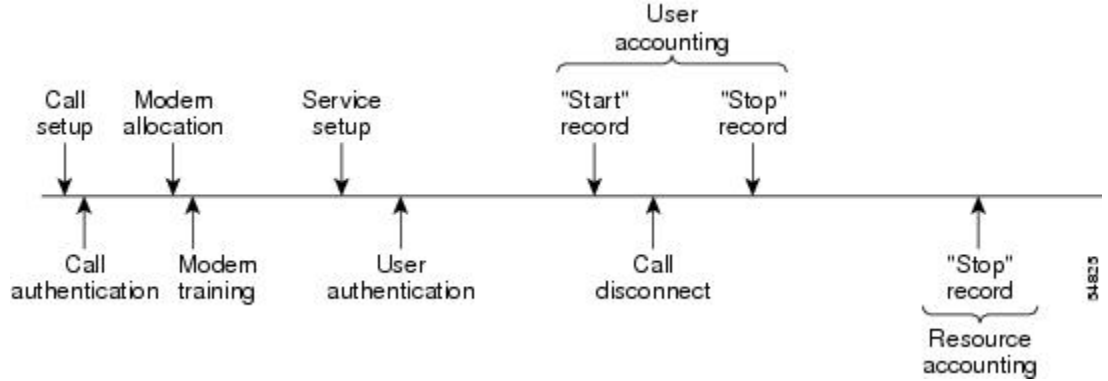
The figure below illustrates a call setup sequence with call disconnect occurring before user authentication and with AAA resource failure stop accounting enabled.

Figure 3: Modem Dial-In Call Setup Sequence With Call Disconnect Occurring Before User Authentication and With Resource Failure Stop Accounting Enabled

The figure below illustrates a call setup sequence with call disconnect occurring before user authentication and without AAA resource failure stop accounting enabled.

Figure 4: Modem Dial-In Call Setup Sequence With Call Disconnect Occurring Before User Authentication and Without Resource Failure Stop Accounting Enabled
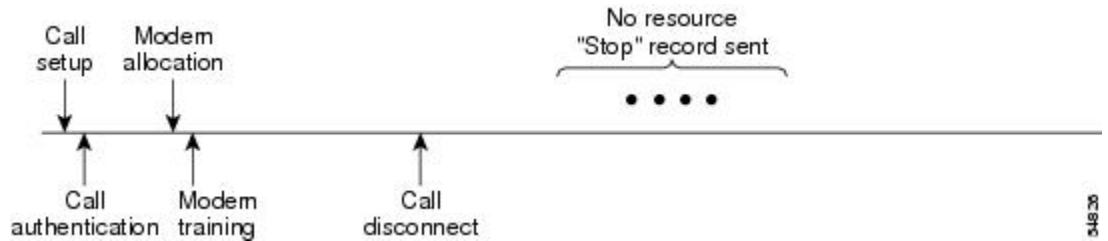
AAA Resource Accounting for Start-Stop Records

AAA resource accounting for start-stop records supports the ability to send a "start" record at each call setup, followed by a corresponding "stop" record at the call disconnect. This functionality can be used to manage and monitor wholesale customers from one source of data reporting, such as accounting records.

With this feature, a call setup and call disconnect "start-stop" accounting record tracks the progress of the resource connection to the device. A separate user authentication "start-stop" accounting record tracks the user management progress. These two sets of accounting records are interlinked by using a unique session ID for the call.

The figure below illustrates a call setup sequence with AAA resource start-stop accounting enabled.

Figure 5: Modem Dial-In Call Setup Sequence With Resource Start-Stop Accounting Enabled
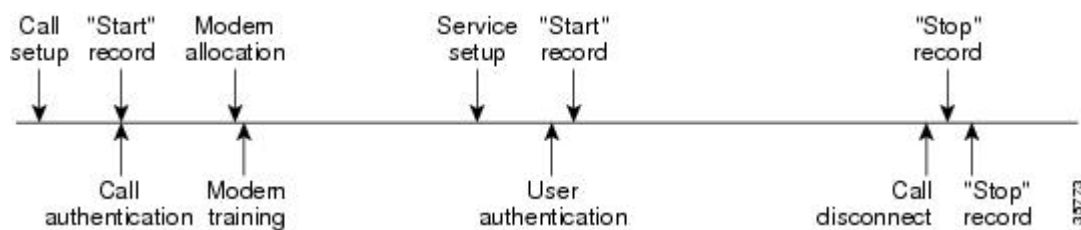
VRRS Accounting

Virtual Router Redundancy Service (VRRS) provides a multiclient information abstraction and management service between a First Hop Redundancy Protocol (FHRP) and a registered client. The VRRS multiclient service provides a consistent interface with FHRP protocols by abstracting over several FHRPs and providing an idealized view of their state. VRRS manages data updates, allowing interested clients to register in one place and receive updates for named FHRP groups or all registered FHRP groups.

Virtual Router Redundancy Protocol (VRRP) is an FHRP that acts as a server that pushes FHRP status information out to all registered VRRS clients. Clients obtain status on essential information provided by the FHRP, including current and previous redundancy states, active and inactive L3 and L2 addresses, and, in some cases, information about other redundant gateways in the network. Clients can use this information to provide stateless and stateful redundancy information to clients and protocols.

VRRS Accounting Plug-in

The VRRS Accounting plug-in provides a configurable AAA method list mechanism that provides updates to a RADIUS server when a VRRS group transitions its state. The VRRS accounting plug-in is an extension of existing AAA system accounting messages. The VRRS Accounting plug-in provides accounting-on and accounting-off messages and an additional Vendor-Specific Attribute (VSA) that sends the configured VRRS name in RADIUS accounting messages. The VRRS name is configured using the **vrrp name** command in interface configuration mode.

The VRRS Accounting plug-in provides a configurable AAA method list mechanism that provides updates to a RADIUS server when a VRRS group transitions its state.

The VRRS accounting plug-in is an extension of existing AAA system accounting messages. The VRRS Accounting plug-in provides accounting-on and accounting-off messages and an additional Vendor-Specific Attribute (VSA) that sends the configured VRRS name in RADIUS accounting messages. The VRRS name is configured using the **vrrp name** command in interface configuration mode. The VRRS Accounting plug-in

sends an accounting-on message to RADIUS when a VRRS group transitions to the master state, and it sends an accounting-off message when a VRRS group transitions from the master state.

The following RADIUS attributes are included in VRRS accounting messages by default:

- Attribute 4, NAS-IP-Address

- Attribute 26, Cisco VSA Type 1, VRRS Name

- Attribute 40, Acct-Status-Type

- Attribute 41, Acct-Delay-Time

- Attribute 44, Acct-Session-Id

Accounting messages for a VRRS transitioning out of master state are sent after all PPPoE accounting stop messages for sessions that are part of that VRRS.

AAA Accounting Enhancements

AAA Broadcast Accounting

AAA broadcast accounting allows accounting information to be sent to multiple AAA servers at the same time; that is, accounting information can be broadcast to one or more AAA servers simultaneously. This functionality allows service providers to send accounting information to their own private AAA servers and to the AAA servers of their end customers. It also provides redundant billing information for voice applications.

Broadcasting is allowed among groups of RADIUS or TACACS+ servers, and each server group can define its backup servers for failover independently of other groups.

Thus, service providers and their end customers can use different protocols (RADIUS or TACACS+) for the accounting server. Service providers and their end customers can also specify their backup servers independently. As for voice applications, redundant accounting information can be managed independently through a separate group with its own failover sequence.

AAA Session MIB

The AAA session MIB feature allows customers to monitor and terminate their authenticated client connections using Simple Network Management Protocol (SNMP). The data of the client is presented so that it correlates directly to the AAA Accounting information reported by either the RADIUS or the TACACS+ server. AAA session MIB provides the following information:

- Statistics for each AAA function (when used in conjunction with the **show radius statistics** command)

- Status of servers providing AAA functions

- Identities of external AAA servers

- Real-time information (such as idle times), providing additional criteria for use by SNMP networks for assessing whether or not to terminate an active call

Note This command is supported only on Cisco AS5300 and Cisco AS5800 universal access server platforms.

The table below shows the SNMP user-end data objects that can be used to monitor and terminate authenticated client connections with the AAA session MIB feature.

Table 9: SNMP End-User Data Objects

SessionId	The session identification used by the AAA Accounting protocol (same value as reported by RADIUS attribute 44 (Acct-Session-ID)).
UserId	The user login ID or zero-length string if a login is unavailable.
IpAddr	The IP address of the session or 0.0.0.0 if an IP address is not applicable or unavailable.
IdleTime	The elapsed time in seconds that the session has been idle.
Disconnect	The session termination object used to disconnect the given client.
CallId	The entry index corresponding to this accounting session that the Call Tracker record stored.

The table below describes the AAA summary information provided by the AAA session MIB feature using SNMP on a per-system basis.

Table 10: SNMP AAA Session Summary

ActiveTableEntries	Number of sessions currently active.
ActiveTableHighWaterMark	Maximum number of sessions present at once since last system reinstallation.
TotalSessions	Total number of sessions since last system reinstallation.
DisconnectedSessions	Total number of sessions that have been disconnected using since last system reinstallation.

Accounting Attribute-Value Pairs

The network access server monitors the accounting functions defined in either TACACS+ AV pairs or RADIUS attributes, depending on which security method is implemented.

How to Configure AAA Accounting

Configuring AAA Accounting Using Named Method Lists

To configure AAA Accounting using named method lists, perform the following steps:

Note System accounting does not use named method lists. For system accounting, define only the default method list.

SUMMARY STEPS

1. **enable**

2. **configure terminal**

3. Router(config)# **aaa accounting** {**system** | **network** | **exec** | **connection** | **commands** *level*} {**default** | *list-name*} {**start-stop** | **stop-only** | **none**} [*method1* [*method2...*]]

4. Do one of the following:

    • Router(config)# **line** [**aux** | **console** | **tty** | **vty**] *line-number* [*ending-line-number*]

    •

    •

    •

    • Router(config)# **interface** *interface-type interface-number*

5. Do one of the following:

    • Router(config-line)# **accounting** {**arap** | **commands** *level* | **connection** | **exec**} {**default** | *list-name*}

    •

    •

    •

    • Router(config-if)# **ppp accounting**{**default** | *list-name*}

6. Router(config-line)# **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	Router(config)# **aaa accounting** {**system** | **network** | **exec** | **connection** | **commands** *level*} {**default** | *list-name*} {**start-stop** | **stop-only** | **none**} [*method1* [*method2*...]] **Example:** Router(config)# aaa accounting system default start-stop	Creates an accounting method list and enables accounting. The argument *list-name* is a character string used to name the created list.
Step 4	Do one of the following: • Router(config)# **line** [**aux** | **console** | **tty** | **vty**] *line-number* [*ending-line-number*] • • • • Router(config)# **interface** *interface-type interface-number* **Example:** Router(config)# line aux line1	Enters the line configuration mode for the lines to which the accounting method list is applied. or Enters the interface configuration mode for the interfaces to which the accounting method list is applied.
Step 5	Do one of the following: • Router(config-line)# **accounting** {**arap** | **commands** *level* | **connection** | **exec**} {**default** | *list-name*} • • • • Router(config-if)# **ppp accounting** {**default** | *list-name*}	Applies the accounting method list to a line or set of lines. or Applies the accounting method list to an interface or set of interfaces.

	Command or Action	Purpose
	Example: Router(config-line)# accounting arap default	
Step 6	Router(config-line)# **end** **Example:** Router(config-line)# end	(Optional) Exits line configuration mode and returns to global configuration mode.

What to Do Next

This section includes the following subsection:

Configuring RADIUS System Accounting

Perform this task to configure RADIUS system accounting on the global RADIUS server:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **radius-server accounting system host-config**
5. **aaa group server radius** *server-name*
6. **server-private** {*host-name* | *ip-address*} **key** {[**0** *server-key* | **7** *server-key*] *server-key*
7. **accounting system host-config**
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.

	Command or Action	**Purpose**
Step 3	**aaa new-model** **Example:** Router(config)# aaa new-model	Enables AAA network security services.
Step 4	**radius-server accounting system host-config** **Example:** Router(config)# radius-server accounting system host-config	Enables the router to send a system accounting record for the addition and deletion of a RADIUS server.
Step 5	**aaa group server radius** *server-name* **Example:** Router(config)# aaa group server radius radgroup1	Adds the RADIUS server and enters server-group configuration mode. • The *server-name* argument specifies the RADIUS server group name.
Step 6	**server-private** {*host-name*	*ip-address*} **key** {[**0** *server-key*	**7** *server-key*] *server-key* **Example:** Router(config-sg-radius)# server-private 172.16.1.11 key cisco	Enters the hostname or IP address of the RADIUS server and hidden server key. • (Optional) **0** with the *server-key* argument specifies that an unencrypted (cleartext) hidden server key follows. • (Optional) **7** with the *server-key* argument specifies that an encrypted hidden server key follows. • The *server-key* argument specifies the hidden server key. If the *server-key* argument is configured without the **0** or **7** preceding it, it is unencrypted. **Note** Once the **server-private** command is configured, RADIUS system accounting is enabled.
Step 7	**accounting system host-config** **Example:** Router(config-sg-radius)# accounting system host-config	Enables the generation of system accounting records for private server hosts when they are added or deleted.
Step 8	**end** **Example:** Router(config-sg-radius)# end	Exits server-group (config-sg-radius) configuration mode and returns to global configuration mode.

Suppressing Generation of Accounting Records for Null Username Sessions

When AAA Accounting is activated, the Cisco IOS software issues accounting records for all users on the system, including users whose username string, because of protocol translation, is NULL. An example of this is users who come in on lines where the **aaa authentication login** *method-list* **none** command is applied. To prevent accounting records from being generated for sessions that do not have usernames associated with them, use the following command in global configuration mode:

Command	Purpose
`Router(config)#` **aaa accounting suppress null-username**	Prevents accounting records from being generated for users whose username string is NULL.

Generating Interim Accounting Records

To enable periodic interim accounting records to be sent to the accounting server, use the following command in global configuration mode:

Command	Purpose
`Router(config)#` **aaa accounting update** [**newinfo**] [**periodic**] *number*	Enables periodic interim accounting records to be sent to the accounting server.

When the **aaa accounting update** command is activated, the Cisco IOS software issues interim accounting records for all users on the system. If the keyword **newinfo** is used, interim accounting records are sent to the accounting server every time there is new accounting information to report. An example of this would be when IPCP completes IP address negotiation with the remote peer. The interim accounting record includes the negotiated IP address used by the remote peer.

When used with the keyword **periodic**, interim accounting records are sent periodically as defined by the *number* argument. The interim accounting record contains all of the accounting information recorded for that user up to the time the interim accounting record is sent.

⚠ **Caution**   Using the **aaa accounting update periodic** command can cause heavy congestion when many users are logged in to the network.

Generating Accounting Records for Failed Login or Session

When AAA Accounting is activated, the Cisco IOS software does not generate accounting records for system users who fail login authentication, or who succeed in login authentication but fail PPP negotiation for some reason.

To specify that accounting stop records be generated for users who fail to authenticate at login or during session negotiation, use the following command in global configuration mode:

Command	Purpose
Router(config)# **aaa accounting send stop-record authentication failure**	Generates "stop" records for users who fail to authenticate at login or during session negotiation using PPP.
Router(config)# **aaa accounting send stop-record always**	Sends authentication, authorization, and accounting (AAA) stop records regardless of whether a start record was sent earlier.

Specifying Accounting NETWORK-Stop Records Before EXEC-Stop Records

For PPP users who start EXEC terminal sessions, you can specify the NETWORK records to be generated before EXEC-stop records. In cases such as billing customers for specific services, it can be desirable to keep network start and stop records together, essentially "nesting" them within the framework of the EXEC start and stop messages. For example, a user dialing in using PPP can create the following records: EXEC-start, NETWORK-start, EXEC-stop, NETWORK-stop. By nesting the accounting records, NETWORK-stop records follow NETWORK-start messages: EXEC-start, NETWORK-start, NETWORK-stop, EXEC-stop.

To nest accounting records for user sessions, use the following command in global configuration mode:

Command	Purpose
Router(config)# **aaa accounting nested**	Nests network accounting records.

Configuring AAA Resource Failure Stop Accounting

To enable resource failure stop accounting, use the following command in global configuration mode:

Command	Purpose
`Router(config)#` **aaa accounting resource** *method-list* **stop-failure group** *server-group*	Generates a "stop" record for any calls that do not reach user authentication. **Note** Before configuring this feature, the tasks described in the Prerequisites for Configuring Accounting, on page 69 section must be performed, and SNMP must be enabled on the network access server. For more information about enabling SNMP on a Cisco router or access server, see the Configuring SNMP Support chapter in the Cisco IOS Network Management Configuration Guide.

Configuring AAA Resource Accounting for Start-Stop Records

To enable full resource accounting for start-stop records, use the following command in global configuration mode:

Command	Purpose
`Router(config)#` **aaa accounting resource** *method-list* **start-stop group** *server-group*	Supports the ability to send a "start" record at each call setup. followed with a corresponding "stop" record at the call disconnect. **Note** Before configuring this feature, the tasks described in the Prerequisites for Configuring Accounting, on page 69 section must be performed, and SNMP must be enabled on the network access server. For more information about enabling SNMP on a Cisco router or access server, see the Configuring SNMP Support chapter in the Cisco IOS Network Management Configuration Guide. **Note**

Configuring AAA Broadcast Accounting

To configure AAA broadcast accounting, use the aaa accounting command in global configuration mode:

Command	Purpose
`Router(config)#` **aaa accounting** {**system** | **network** | **exec** | **connection** | **commands** *level*} {**default** | *list-name*} {**start-stop** | **stop-only** | **none**} [**broadcast**] *method1* [*method2...*]	Enables sending accounting records to multiple AAA servers. Simultaneously sends accounting records to the first server in each group. If the first server is unavailable, failover occurs using the backup servers defined within that group.

Configuring Per-DNIS AAA Broadcast Accounting

To configure AAA broadcast accounting per DNIS, use the **aaa dnis map accounting network** command in global configuration mode:

Command	Purpose
`Router(config)#` **aaa dnis map** *dnis-number* **accounting network** [**start-stop** | **stop-only** | **none**] [**broadcast**] *method1* [*method2...*]	Allows per-DNIS accounting configuration. This command has precedence over the global **aaa accounting** command.
	Enables sending accounting records to multiple AAA servers. Simultaneously sends accounting records to the first server in each group. If the first server is unavailable, failover occurs using the backup servers defined within that group.

Configuring AAA Session MIB

The following tasks must be performed before configuring the AAA session MIB feature:

- Configure SNMP. For information on SNMP, see the chapter Configuring SNMP Support in the Cisco IOS Network Management Configuration Guide.

- Configure AAA.

- Define the RADIUS or TACACS+ server characteristics.

Note Overusing SNMP can affect the overall system performance; therefore, normal network management performance must be considered when this feature is used.

To configure AAA session MIB, use the following command in global configuration mode

SUMMARY STEPS

    1. Router(config)# **aaa session-mib disconnect**

DETAILED STEPS

	Command or Action	**Purpose**
Step 1	Router(config)# **aaa session-mib disconnect**	Monitors and terminates authenticated client connections using SNMP.
		To terminate the call, the **disconnect** keyword must be used.

Configuring VRRS Accounting

Perform the following task to configure Virtual Router Redundancy Service (VRRS) to send AAA Accounting messages to the AAA server:

SUMMARY STEPS

    1. **enable**

    2. **configure terminal**

    3. **aaa accounting vrrs** {**default** | *list-name*} **start-stop** *method1* [*method2...*]

    4. **aaa attribute list** *list-name*

    5. **attribute type** *name value* [**service** *service*] [**protocol** *protocol*][**mandatory**][**tag** *tag-value*]

    6. **exit**

    7. **vrrs** *vrrs-group-name*

    8. **accounting delay** *seconds*

    9. **accounting method** {**default** | *accounting-method-list*}

    10. **exit**

DETAILED STEPS

	Command or Action	**Purpose**
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**aaa accounting vrrs** {**default**	*list-name*} **start-stop** *method1* [*method2...*] **Example:** Router(config)# aaa accounting vrrs default start-stop	Enables AAA accounting for VRRS.
Step 4	**aaa attribute list** *list-name* **Example:** Router(config)# aaa attribute list list1	Defines a AAA attribute list locally on a router, and enters attribute list configuration mode.
Step 5	**attribute type** *name value* [**service** *service*] [**protocol** *protocol*][**mandatory**][**tag** *tag-value*] **Example:** Router(config-attr-list)# attribute type example 1	Defines an attribute type that is to be added to an attribute list locally on a router.
Step 6	**exit** **Example:** Router(config-attr-list)# exit	Exits attribute list configuration mode and returns to global configuration mode.
Step 7	**vrrs** *vrrs-group-name* **Example:** Router(config)# vrrs vrrs1	(Optional) Defines a VRRP group and configures parameters for the VRRS group, and enters VRRS configuration mode.
Step 8	**accounting delay** *seconds* **Example:** Router(config-vrrs)# accounting delay 10	(Optional) Specifies the delay time for sending accounting-off messages to the VRRS.
Step 9	**accounting method** {**default**	*accounting-method-list*} **Example:** Router(config-vrrs)# accounting method default	(Optional) Enables VRRS accounting for a VRRP group.
Step 10	**exit** **Example:** Router(config-vrrs)# exit	Exits VRRS configuration mode.

Establishing a Session with a Router if the AAA Server is Unreachable

To establish a console or telnet session with a router if the AAA server is unreachable, use the following command in global configuration mode:

Command	Purpose
`Router(config)#` **no aaa accounting system guarantee-first**	The **aaa accounting system guarantee-first** command guarantees system accounting as the first record, which is the default condition. In some situations, users may be prevented from starting a session on the console or terminal connection until after the system reloads, which can take more than three minutes. To resolve this problem, the **no aaa accounting system guarantee-first** command can be used.

Note   Entering the **no aaa accounting system guarantee-first** command is not the only condition by which the console or telnet session can be started. For example, if the privileged EXEC session is being authenticated by TACACS and the TACACS server is not reachable, then the session cannot start.

Monitoring Accounting

No specific **show** command exists for either RADIUS or TACACS+ accounting. To obtain accounting records displaying information about users currently logged in, use the following command in privileged EXEC mode:

Command	Purpose
`Router#` **show accounting**	Allows display of the active accountable events on the network and helps collect information in the event of a data loss on the accounting server.

Troubleshooting Accounting

To troubleshoot accounting information, use the following command in privileged EXEC mode:

Command	Purpose
`Router#` **debug aaa accounting**	Displays information on accountable events as they occur.

Configuration Examples for AAA Accounting

Example Configuring Named Method List

The following example shows how to configure a Cisco AS5200 (enabled for AAA and communication with a RADIUS security server) in order for AAA services to be provided by the RADIUS server. If the RADIUS server fails to respond, then the local database is queried for authentication and authorization information, and accounting services are handled by a TACACS+ server.

```
aaa new-model
aaa authentication login admins local
aaa authentication ppp dialins group radius local
aaa authorization network blue1 group radius local
aaa accounting network red1 start-stop group radius group tacacs+
username root password ALongPassword
tacacs-server host 172.31.255.0
tacacs-server key goaway
radius-server host 172.16.2.7
radius-server key myRaDiUSpassWoRd
interface group-async 1
 group-range 1 16
 encapsulation ppp
 ppp authentication chap dialins
 ppp authorization blue1
 ppp accounting red1
line 1 16
 autoselect ppp
 autoselect during-login
 login authentication admins
 modem dialin
```

The lines in this sample RADIUS AAA configuration are defined as follows:

- The **aaa new-model** command enables AAA network security services.

- The **aaa authentication login admins local** command defines a method list "admins", for login authentication.

- The **aaa authentication ppp dialins group radius local** command defines the authentication method list "dialins", which specifies that first RADIUS authentication and then (if the RADIUS server does not respond) local authentication is used on serial lines using PPP.

- The **aaa authorization network blue1 group radius local** command defines the network authorization method list named "blue1", which specifies that RADIUS authorization is used on serial lines using PPP. If the RADIUS server fails to respond, then local network authorization is performed.

- The **aaa accounting network red1 start-stop group radius group tacacs+**command defines the network accounting method list named red1, which specifies that RADIUS accounting services (in this case, start and stop records for specific events) are used on serial lines using PPP. If the RADIUS server fails to respond, accounting services are handled by a TACACS+ server.

- The **username** command defines the username and password to be used for the PPP Password Authentication Protocol (PAP) caller identification.

- The **tacacs-server host** command defines the name of the TACACS+ server host.

- The **tacacs-server key** command defines the shared secret text string between the network access server and the TACACS+ server host.

- The **radius-server host** command defines the name of the RADIUS server host.

- The **radius-server key** command defines the shared secret text string between the network access server and the RADIUS server host.

- The **interface group-async** command selects and defines an asynchronous interface group.

- The **group-range** command defines the member asynchronous interfaces in the interface group.

- The **encapsulation ppp** command sets PPP as the encapsulation method used on the specified interfaces.

- The **ppp authentication chap dialins**command selects Challenge Handshake Authentication Protocol (CHAP) as the method of PPP authentication and applies the "dialins" method list to the specified interfaces.

- The **ppp authorization blue1**command applies the blue1 network authorization method list to the specified interfaces.

- The **ppp accounting red1**command applies the red1 network accounting method list to the specified interfaces.

- The **line** command switches the configuration mode from global configuration to line configuration and identifies the specific lines being configured.

- The **autoselect ppp** command configures the Cisco IOS software to allow a PPP session to start up automatically on these selected lines.

- The **autoselect during-login** command is used to display the username and password prompt without pressing the Return key. After the user logs in, the autoselect function (in this case, PPP) begins.

- The **login authentication admins** command applies the admins method list for login authentication.

- The **modem dialin** command configures modems attached to the selected lines to only accept incoming calls.

The **show accounting**command yields the following output for the preceding configuration:

```
Active Accounted actions on tty1, User username2 Priv 1
 Task ID 5, Network Accounting record, 00:00:52 Elapsed
 task_id=5 service=ppp protocol=ip address=10.0.0.98
```
The table below describes the fields contained in the preceding output.

Table 11: show accounting Field Descriptions

Field	Description
Active Accounted actions on	Terminal line or interface name user with which the user logged in.
User	User's ID.
Priv	User's privilege level.
Task ID	Unique identifier for each accounting session.

Field	Description
Accounting record	Type of accounting session.
Elapsed	Length of time (hh:mm:ss) for this session type.
attribute=value	AV pairs associated with this accounting session.

Example Configuring AAA Resource Accounting

The following example shows how to configure the resource failure stop accounting and resource accounting for start-stop records functions:

```
!Enable AAA on your network access server.
aaa new-model
!Enable authentication at login and list the AOL string name to use for login authentication.
aaa authentication login AOL group radius local
!Enable authentication for ppp and list the default method to use for PPP authentication.
aaa authentication ppp default group radius local
!Enable authorization for all exec sessions and list the AOL string name to use for
authorization.
aaa authorization exec AOL group radius if-authenticated
!Enable authorization for all network-related service requests and list the default method
 to use for all network-related authorizations.
aaa authorization network default group radius if-authenticated
!Enable accounting for all exec sessions and list the default method to use for all start-stop
 accounting services.
aaa accounting exec default start-stop group radius
!Enable accounting for all network-related service requests and list the default method to
 use for all start-stop accounting services.
aaa accounting network default start-stop group radius
!Enable failure stop accounting.
aaa accounting resource default stop-failure group radius
!Enable resource accounting for start-stop records.
aaa accounting resource default start-stop group radius
```

Example Configuring AAA Broadcast Accounting

The following example shows how to turn on broadcast accounting using the global **aaa accounting** command:

```
aaa group server radius isp
 server 10.0.0.1
 server 10.0.0.2
aaa group server tacacs+ isp_customer
 server 172.0.0.1
aaa accounting network default start-stop broadcast group isp group isp_customer
radius-server host 10.0.0.1
radius-server host 10.0.0.2
radius-server key key1
tacacs-server host 172.0.0.1 key key2
```
The **broadcast** keyword causes "start" and "stop" accounting records for network connections to be sent simultaneously to server 10.0.0.1 in the group isp and to server 172.0.0.1 in the group isp_customer. If server 10.0.0.1 is unavailable, failover to server 10.0.0.2 occurs. If server 172.0.0.1 is unavailable, no failover occurs because backup servers are not configured for the group isp_customer.

Example Configuring Per-DNIS AAA Broadcast Accounting

The following example shows how to turn on per DNIS broadcast accounting using the global **aaa dnis map accounting network**command:

```
aaa group server radius isp
 server 10.0.0.1
 server 10.0.0.2
aaa group server tacacs+ isp_customer
 server 172.0.0.1
aaa dnis map enable
aaa dnis map 7777 accounting network start-stop broadcast group isp group isp_customer
radius-server host 10.0.0.1
radius-server host 10.0.0.2
radius-server key key_1
tacacs-server host 172.0.0.1 key key_2
```

The **broadcast** keyword causes "start" and "stop" accounting records for network connection calls having DNIS number 7777 to be sent simultaneously to server 10.0.0.1 in the group isp and to server 172.0.0.1 in the group isp_customer. If server 10.0.0.1 is unavailable, failover to server 10.0.0.2 occurs. If server 172.0.0.1 is unavailable, no failover occurs because backup servers are not configured for the group isp_customer.

Example AAA Session MIB

The following example shows how to set up the AAA session MIB feature to disconnect authenticated client connections for PPP users:

```
aaa new-model
aaa authentication ppp default group radius
aaa authorization network default group radius
aaa accounting network default start-stop group radius
aaa session-mib disconnect
```

Example Configuring VRRS Accounting

The following example shows how to configure VRRS to send AAA Accounting messages to the AAA server:

```
Router# configure terminal
Router(config)# aaa accounting vrrs vrrp-mlist-1 start-stop group radius
Router(config)# aaa attribute list vrrp-1-attr
Router(config-attr-list)# attribute type account-delay 10
Router(config-attr-list)# exit
Router(config)# vrrs vrrp-group-1
Router(config-vrrs)# accounting delay 10
Router(config-vrrs)# accounting method vrrp-mlist-1
Router(config-vrrs)# exit
```

Additional References

Related Documents

Related Topic	Document Title
Authorization	Configuring Authorization module

Related Topic	Document Title
Authentication	Configuring Authentication module
Accounting Commands	*Cisco IOS Security Command Reference*

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIB	MIBs Link
No new or modified MIBs are supported, and support for existing MIBs has not been modified.	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 2903	*Generic AAA Architecture*
RFC 2904	*AAA Authorization Framework*
RFC 2906	*AAA Authorization Requirements*
RFC 2989	*Criteria for Evaluating AAA Protocols for Network Access*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Configuring Accounting

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 12: Feature Information for Configuring Accounting

Feature Name	Releases	Feature Information
AAA Broadcast Accounting	Cisco IOS 15.2(1)E	AAA broadcast accounting allows accounting information to be sent to multiple AAA servers at the same time; that is, accounting information can be broadcast to one or more AAA servers simultaneously.
AAA Resource Accounting for Start-Stop Records	Cisco IOS 15.2(1)E	AAA resource accounting for start-stop records supports the ability to send a "start" record at each call setup, followed by a corresponding "stop" record at the call disconnect. This functionality can be used to manage and monitor wholesale customers from one source of data reporting, such as accounting records.

Feature Name	Releases	Feature Information
AAA Session MIB	Cisco IOS 15.2(1)E	The AAA session MIB feature allows customers to monitor and terminate their authenticated client connections using SNMP. The data of the client is presented so that it correlates directly to the AAA Accounting information reported by either the RADIUS or the TACACS+ server.
AAA: IPv6 Accounting Delay Enhancements	Cisco IOS 15.2(1)E	VRRS provides a multiclient information abstraction and management service between a First Hop Redundancy Protocol (FHRP) and a registered client.

C H A P T E R **9**

AAA-SERVER-MIB Set Operation

The AAA-SERVER-MIB Set Operation feature allows the authentication, authorization, and accounting (AAA) server configuration to be extended or expanded by using the CISCO-AAA-SERVER-MIB to create and add new AAA servers, modify the "KEY" under the CISCO-AAA-SERVER-MIB, and delete the AAA server configuration.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for AAA-SERVER-MIB Set Operation

AAA must have been enabled on the router, that is, the **aaa new-model** command must have been configured. If this configuration has not been accomplished, the set operation fails.

Restrictions for AAA-SERVER-MIB Set Operation

Currently, the CISCO SNMP set operation is supported only for the RADIUS protocol. Therefore, only RADIUS servers in global configuration mode can be added, modified, or deleted.

Information About AAA-SERVER-MIB Set Operation

CISCO-AAA-SERVER-MIB

The CISCO-AAA-SERVER-MIB provides that statistics reflect both the state of the AAA server operation with the server itself and of AAA communications with external servers. The CISCO-AAA-SERVER-MIB provides the following information:

- Statistics for each AAA operation

- Status of servers that are providing AAA functions

- Identities of external AAA servers

CISCO-AAA-SERVER-MIB Set Operation

Before Cisco IOS Release 12.4(4)T, the CISCO-AAA-SERVER-MIB supported only the "get" operation. Effective with this release, the CISCO-AAA-SERVER-MIB supports the set operation. With the set operation, you can do the following:

- Create or add a new AAA server.

- Modify the KEY under the CISCO-AAA-SERVER-MIB. This "secret key" is used for secure connectivity to the AAA server, which is present with the network access server (NAS) and the AAA server.

- Delete the AAA server configuration.

How to Configure AAA-SERVER-MIB Set Operation

Configuring AAA-SERVER-MIB Set Operations

No special configuration is required for this feature. The Simple Network Management Protocol (SNMP) framework can be used to manage MIBs. See the Additional References section for a reference to configuring SNMP.

Verifying SNMP Values

SNMP values can be verified by performing the following steps.

SUMMARY STEPS

1. enable

2. show running-config | include radius-server host

3. show aaa servers

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show running-config	include radius-server host** **Example:** `Router# show running-config	include` `radius-server host`	Displays all the RADIUS servers that are configured in the global configuration mode.
Step 3	**show aaa servers** **Example:** `Router# show aaa servers`	Displays information about the number of requests sent to and received from authentication, authorization, and accounting (AAA) servers.

Configuration Examples for AAA-SERVER-MIB Set Operation

RADIUS Server Configuration and Server Statistics Example

The following sample output shows the RADIUS server configuration and server statistics before and after the set operation.

Before the Set Operation

```
Router# show running-config | include radius-server host
! The following line is for server 1.
radius-server host 172.19.192.238 auth-port 2095 acct-port 2096 key cisco2
! The following line is for server 2.
radius-server host 172.19.192.238 auth-port 1645 acct-port 1646
```

Server Statistics

```
Router# show aaa servers
```

```
RADIUS: id 2, priority 1, host 172.19.192.238, auth-port 2095, acct-port 2096
State: current UP, duration 25s, previous duration 0s
     Dead: total time 0s, count 7
Authen: request 8, timeouts 8
     Response: unexpected 0, server error 0, incorrect 0, time 0ms
     Transaction: success 0, failure 2
Author: request 0, timeouts 0
     Response: unexpected 0, server error 0, incorrect 0, time 0ms
     Transaction: success 0, failure 0
Account: request 0, timeouts 0
     Response: unexpected 0, server error 0, incorrect 0, time 0ms
     Transaction: success 0, failure 0
Elapsed time since counters last cleared: 5m
RADIUS: id 3, priority 2, host 172.19.192.238, auth-port 1645, acct-port 1646
State: current UP, duration 5s, previous duration 0s
     Dead: total time 0s, count 2
Authen: request 8, timeouts 8
     Response: unexpected 0, server error 0, incorrect 0, time 0ms
     Transaction: success 0, failure 4
Author: request 0, timeouts 0
     Response: unexpected 0, server error 0, incorrect 0, time 0ms
     Transaction: success 0, failure 0
Account: request 0, timeouts 0
     Response: unexpected 0, server error 0, incorrect 0, time 0ms
     Transaction: success 0, failure 0
Elapsed time since counters last cleared: 3m
```

SNMP Get Operation to Check the Configuration and Statistics of the RADIUS Servers

```
aaa-server5:/users/smetri> getmany 10.0.1.42 casConfigTable
casAddress.2.2 = 172.19.192.238
casAddress.2.3 = 172.19.192.238
casAuthenPort.2.2 = 2095
casAuthenPort.2.3 = 1645
casAcctPort.2.2 = 2096
casAcctPort.2.3 = 1646
casKey.2.2 =
casKey.2.3 =
! The following line shows priority for server 1.
casPriority.2.2 = 1
! The following line shows priority for server 2.
casPriority.2.3 = 2
casConfigRowStatus.2.2 = active(1)
casConfigRowStatus.2.3 = active(1)
aaa-server5:/users/smetri>
```

SNMP Set Operation

The key of the existing RADIUS server is being changed. The index "1" is being used. That index acts as a wildcard for addition, deletion, or modification of any entries.

```
Change the key for server 1:=>
aaa-server5:/users/smetri>  setany -v2c 10.0.1.42 public casAddress.2.1 -a 172.19.192.238
casAuthenPort.2.1 -i 2095 casAcctPort.2.1 -i 2096 casKey.2.1 -o king
casAddress.2.1 = 172.19.192.238
casAuthenPort.2.1 = 2095
casAcctPort.2.1 = 2096
casKey.2.1 = king
aaa-server5:/users/smetri>
```

After the Set Operation

After the above SNMP set operation, the configurations on the router change. The following output shows the output after the set operation.

```
Router# show running-config | include radius-server host
radius-server host 172.19.192.238 auth-port 1645 acct-port 1646
```

```
! The following line shows a change in the key value to "king."
radius-server host 172.19.192.238 auth-port 2095 acct-port 2096 key king

Router# show aaa servers
RADIUS: id 3, priority 1, host 172.19.192.238, auth-port 1645, acct-port 1646
State: current UP, duration 189s, previous duration 0s
    Dead: total time 0s, count 2
Authen: request 8, timeouts 8
    Response: unexpected 0, server error 0, incorrect 0, time 0ms
    Transaction: success 0, failure 4
Author: request 0, timeouts 0
    Response: unexpected 0, server error 0, incorrect 0, time 0ms
    Transaction: success 0, failure 0
Account: request 0, timeouts 0
    Response: unexpected 0, server error 0, incorrect 0, time 0ms
    Transaction: success 0, failure 0
Elapsed time since counters last cleared: 6m

! The following line shows a new server with new statistics.
RADIUS: id 4, priority 2, host 172.19.192.238, auth-port 2095, acct-port 2096
State: current UP, duration 209s, previous duration 0s
    Dead: total time 0s, count 7
Authen: request 0, timeouts 0
    Response: unexpected 0, server error 0, incorrect 0, time 0ms
    Transaction: success 0, failure 0
Author: request 0, timeouts 0
    Response: unexpected 0, server error 0, incorrect 0, time 0ms
    Transaction: success 0, failure 0
Account: request 0, timeouts 0
    Response: unexpected 0, server error 0, incorrect 0, time 0ms
```

Additional References

The following sections provide references related to the AAA-SERVER-MIB Set Operation feature.

Related Documents

Related Topic	Document Title
Configuring SNMP	Configuring SNMP Support in the *Cisco IOS Network Management Configuration Guide*

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	--

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for AAA-SERVER-MIB Set Operation

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 13: Feature Information for AAA-SERVER-MIB Set Operation

Feature Name	Releases	Feature Information
AAA-SERVER-MIB Set Operation	Cisco IOS 15.2(1)E	The AAA-SERVER-MIB Set Operation feature allows the authentication, authorization, and accounting (AAA) server configuration to be extended or expanded by using the CISCO-AAA-SERVER-MIB to create and add new AAA servers, modify the "KEY" under the CISCO-AAA-SERVER-MIB, and delete the AAA server configuration. The following commands were introduced or modified: **show aaa servers, show running-config, show running-config vrf.**

Password Strength and Management for Common Criteria

The Password Strength and Management for Common Criteria feature is used to specify password policies and security mechanisms for storing, retrieving, and providing rules to specify user passwords.

For local users, the user profile and the password information with the key parameters are stored on the Cisco device, and this profile is used for local authentication of users. The user can be an administrator (terminal access) or a network user (for example, PPP users being authenticated for network access).

For remote users, where the user profile information is stored in a remote server, a third-party authentication, authorization, and accounting (AAA) server may be used for providing AAA services, both for administrative and network access.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for Password Strength and Management for Common Criteria

Only four concurrent users can log on to the system by using vty at any moment.

Information About Password Strength and Management for Common Criteria

Password Composition Policy

The password composition policy allows you to create passwords of any combination of upper and lowercase characters, numbers, and special characters that include "!", "@", "#", "$", "%","^", "&", "*", "(", and ")".

Password Length Policy

The administrator has the flexibility to set the password's minimum and maximum length. The recommended minimum password length is 8 characters. The administrator can specify both the minimum (1) and the maximum (64) length for the password.

Password Lifetime Policy

The security administrator can provide a configurable option for a password to have a maximum lifetime. If the lifetime parameter is not configured, the configured password will never expire. The maximum lifetime can be configured by providing the configurable value in years, months, days, hours, minutes, and seconds. The lifetime configuration will survive across reloads as it is a part of the configuration, but every time the system reboots, the password creation time will be updated to the new time. For example, if a password is configured with a lifetime of one month and on the 29th day, the system reboots, then the password will be valid for one month after the system reboots.

Password Expiry Policy

If the user attempts to log on and if the user's password credentials have expired, then the following happens:

1 The user is prompted to set the new password after successfully entering the expired password.

2 When the user enters the new password, the password is validated against the password security policy.

3 If the new password matches the password security policy, then the AAA database is updated, and the user is authenticated with the new password.

4 If the new password does not match the password security policy, then the user is prompted again for the password. From AAA perspective, there is no restriction on the number of retries. The number of retries

for password prompt in case of unsuccessful authentication is controlled by the respective terminal access interactive module. For example, for telnet, after three unsuccessful attempts, the session will be terminated.

If the password's lifetime is not configured for a user and the user has already logged on and if the security administrator configures the lifetime for that user, then the lifetime will be set in the database. When the same user is authenticated the next time, the system will check for password expiry. The password expiry is checked only during the authentication phase.

If the user has been already authenticated and logged on to the system and if the password expires, then no action will be taken. The user will be prompted to change the password only during the next authentication for the same user.

Password Change Policy

The new password must contain a minimum of 4 character changes from the previous password. A password change can be triggered by the following scenarios:

- The security administrator wants to change the password.

- The user is trying to get authenticated using a profile, and the password for that profile has expired.

When the security administrator changes the password security policy and the existing profile does not meet the password security policy rules, no action will be taken if the user has already logged on to the system. The user will be prompted to change the password only when the user tries to get authenticated using the profile that does not meet the password security restriction.

When the user changes the password, the lifetime parameters set by the security administrator for the old profile will be the lifetime parameters for the new password.

For noninteractive clients such as dot1x, when the password expires, appropriate error messages will be sent to the clients, and the clients must contact the security administrator to renew the password.

User Reauthentication Policy

Users are reauthenticated when they change their passwords.

When users change their passwords on expiry, they will be authenticated against the new password. In such cases, the actual authentication happens based on the previous credentials, and the new password is updated in the database.

Note Users can change their passwords only when they are logging on and after the expiry of the old password; however, a security administrator can change the user's password at any time.

Support for Framed (noninteractive) Session

When a client such as dot1x uses the local database for authentication, the Password Strength and Management for Common Criteria feature will be applicable; however, upon password expiry, clients will not be able to change the password. An appropriate failure message will be sent to such clients, and the user must request the security administrator to change the password.

How to Configure Password Strength and Management for Common Criteria

Configuring the Password Security Policy

Perform this task to create a password security policy and to apply the policy to a specific user profile.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa common-criteria policy** *policy-name*
5. **char-changes** *number*
6. **max-length** *number*
7. **min-length** *number*
8. **numeric-count** *number*
9. **special-case** *number*
10. **exit**
11. **username** *username* **common-criteria-policy** *policy-name* **password** *password*
12. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**aaa new-model** **Example:** `Device(config)# aaa new-model`	Enables AAA globally.

	Command or Action	**Purpose**
Step 4	**aaa common-criteria policy** *policy-name* **Example:** `Device(config)# aaa common-criteria policy policy1`	Creates the AAA security password policy and enters common criteria configuration policy mode.
Step 5	**char-changes** *number* **Example:** `Device(config-cc-policy)# char-changes 4`	(Optional) Specifies the number of changed characters between old and new passwords.
Step 6	**max-length** *number* **Example:** `Device(config-cc-policy)# max-length 25`	(Optional) Specifies the maximum length of the password.
Step 7	**min-length** *number* **Example:** `Device(config-cc-policy)# min-length 8`	(Optional) Specifies the minimum length of the password.
Step 8	**numeric-count** *number* **Example:** `Device(config-cc-policy)# numeric-count 4`	(Optional) Specifies the number of numeric characters in the password.
Step 9	**special-case** *number* **Example:** `Device(config-cc-policy)# special-case 3`	(Optional) Specifies the number of special characters in the password.
Step 10	**exit** **Example:** `Device(config-cc-policy)# exit`	(Optional) Exits common criteria configuration policy mode and returns to global configuration mode.

Step 11	**username** *username* **common-criteria-policy** *policy-name* **password** *password*
	
	Example:
	`Device(config)# username user1`
	`common-criteria-policy policy1 password password1`
		(Optional) Applies a specific policy and password to a user profile.

	Command or Action	Purpose
Step 12	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Verifying the Common Criteria Policy

Perform this task to verify all the common criteria security policies.

SUMMARY STEPS

1. **enable**
2. **show aaa common-criteria policy name** *policy-name*
3. **show aaa common-criteria policy all**

DETAILED STEPS

Step 1 **enable**

Enables privileged EXEC mode.

Example:
`Device> enable`

Step 2 **show aaa common-criteria policy name** *policy-name*

Displays the password security policy information for a specific policy.

Example:
```
Device# show aaa common-criteria policy name policy1

Policy name: policy1
Minimum length: 1
Maximum length: 64
Upper Count: 20
Lower Count: 20
Numeric Count: 5
Special Count: 2
Number of character changes 4
Valid forever. User tied to this policy will not expire.
```

Step 3 **show aaa common-criteria policy all**

Displays password security policy information for all the configured policies.

Example:
```
Device# show aaa common-criteria policy all
====================================================================
Policy name: policy1
Minimum length: 1
Maximum length: 64
Upper Count: 20
Lower Count: 20
Numeric Count: 5
Special Count: 2
Number of character changes 4
Valid forever. User tied to this policy will not expire.
====================================================================
Policy name: policy2
Minimum length: 1
Maximum length: 34
Upper Count: 10
Lower Count: 5
Numeric Count: 4
Special Count: 2
Number of character changes 2
Valid forever. User tied to this policy will not expire.
====================================================================
```

Troubleshooting Tips

Use the **debug aaa common-criteria** command to troubleshoot AAA common criteria.

Configuration Example for the Password Strength and Management for Common Criteria Feature

Example: Password Strength and Management for Common Criteria

The following example shows how to create a common criteria security policy and apply the specific policy to a user profile:

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa common-criteria policy policy1
Device(config-cc-policy)# char-changes 4
Device(config-cc-policy)# max-length 20
Device(config-cc-policy)# min-length 6
Device(config-cc-policy)# numeric-count 2
Device(config-cc-policy)# special-case 2
Device(config-cc-policy)# exit
Device(config)# username user1 common-criteria-policy policy1 password password1
Device(config)# end
```

Additional References

The following sections provide references related to the RADIUS Packet of Disconnect feature.

Related Documents

Related Topic	Document Title
AAA	Authentication, Authorization, and Accounting (AAA) section of the *Cisco IOS XE Security Configuration Guide, Securing User Services*, Release 2.
Security commands	*Cisco IOS Security Command Reference*
CLI Configuration	*Cisco IOS XE Configuration Fundamentals Configuration Guide*, Release 2

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS XE software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 2865	*Remote Authentication Dial-in User Service*
RFC 3576	*Dynamic Authorization Extensions to RADIUS*

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information for Password Strength and Management for Common Criteria

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 14: Feature Information for Password Strength and Management for Common Criteria

Feature Name	Releases	Feature Information
Password Strength and Management for Common Criteria	Cisco IOS 15.0(2)SE Cisco IOS 15.2(1)E	The Password Strength and Management for Common Criteria feature is used to specify password policies and security mechanisms for storing, retrieving, and providing rules to specify user passwords. The following commands were introduced or modified: **aaa common-criteria policy**, **debug aaa common-criteria**, and **show aaa common-criteria policy**.