AAA DNIS Map for Authorization

The AAA DNIS Map for Authorization feature allows you to assign a Dialed Number Identification Service (DNIS) number to a particular authentication, authorization, and accounting (AAA) server group so that the server group can process authentication, authorization, and accounting requests for users dialing in to the network using that particular DNIS. Any phone line (a regular home phone or a commercial T1/PRI line) can be associated with several phone numbers. The DNIS number identifies the number that was called to reach you.

Prerequisites for AAA DNIS Map for Authorization

- Before configuring the device to select a particular AAA server group based on the DNIS of the server group, you must configure the list of RADIUS server hosts and AAA server groups.
- Before configuring AAA preauthentication, you must configure the **aaa new-model** command and make sure that the supporting preauthentication application is running on a RADIUS server in your network.

Information About AAA DNIS Map for Authorization

AAA Server Group Selection Based on DNIS

Cisco software allows you to assign a DNIS number to a particular AAA server group so that the server group can process authentication, authorization, and accounting requests for users dialing in to the network using that particular DNIS. Any phone line (a regular home phone or a commercial T1/PRI line) can be associated with several phone numbers. The DNIS number identifies the number that was called to reach you.

For example, suppose you want to share the same phone number with several customers, but you want to know which customer is calling before you pick up the phone. You can customize how you answer the phone because DNIS allows you to know which customer is calling when you answer.

Cisco devices with either ISDN or internal modems can receive the DNIS number. This functionality allows users to assign different RADIUS server groups for different customers (that is, different RADIUS servers for different DNIS numbers). Additionally, using server groups, you can specify the same server group for AAA services or a separate server group for each AAA service.

Cisco software provides the flexibility to implement authentication and accounting services in several ways:

- Globally—AAA services are defined using global configuration access list commands and applied in general to all interfaces on a specific network access server.
- Per interface—AAA services are defined using interface configuration commands and applied specifically to the interface being configured on a specific network access server.
- DNIS mapping—You can use DNIS to specify an AAA server to supply AAA services.

Because each of these AAA configuration methods can be configured simultaneously, Cisco has established an order of precedence to determine which server or groups of servers provide AAA services. The order of precedence is as follows:

- Per DNIS—If you configure the network access server to use DNIS to identify or determine which server group provides AAA services, this method takes precedence over any additional AAA selection method.
- Per interface—If you configure the network access server per interface to use access lists to determine how a server provides AAA services, this method takes precedence over any global configuration AAA access lists.
- Globally—If you configure the network access server by using global AAA access lists to determine how the security server provides AAA services, this method has the least precedence.

AAA Preauthentication

Configuring AAA preauthentication with ISDN PRI or channel-associated signaling (CAS) allows service providers to better manage ports using their existing RADIUS solutions and efficiently manage the use of shared resources to offer differing service-level agreements. With ISDN PRI or CAS, information about an incoming call is available to the network access server (NAS) before the call is connected. The available call information includes the following:

- The DNIS number, also referred to as the called number
- The Calling Line Identification (CLID) number, also referred to as the calling number
- The call type, also referred to as the bearer capability

The AAA preauthentication feature allows a Cisco NAS to decide--on the basis of the DNIS number, the CLID number, or the call type--whether to connect an incoming call. (With ISDN PRI, it enables user authentication and authorization before a call is answered. With CAS, the call must be answered; however, the call can be dropped if preauthentication fails.)

When an incoming call arrives from the public network switch, but before it is connected, AAA preauthentication enables the NAS to send the DNIS number, CLID number, and call type to a RADIUS server for authorization. If the server authorizes the call, the NAS accepts the call. If the server does not authorize the call, the NAS sends a disconnect message to the public network switch to reject the call.

In the event that the RADIUS server application becomes unavailable or is slow to respond, a guard timer can be set in the NAS. When the timer expires, the NAS uses a configurable parameter to accept or reject the incoming call that has no authorization.

The AAA preauthentication feature supports the use of attribute 44 by the RADIUS server application and the use of RADIUS attributes that are configured in the RADIUS preauthentication profiles to specify preauthentication behavior. They can also be used, for instance, to specify whether subsequent authentication should occur and, if so, what authentication method should be used.

The following restrictions apply to AAA preauthentication with ISDN PRI and CAS:

- Attribute 44 is available for CAS calls only when preauthentication or resource pooling is enabled.
- Multichassis Multilink PPP (MMP) is not available with ISDN PRI.
- AAA preauthentication is available only on some hardware platforms.
- ISDN PRI is supported only on some hardware platforms.

Guard Timer for Call Handling

Because response times for preauthentication and authentication requests can vary, the guard timer allows you to control the handling of calls. The guard timer starts when the DNIS is sent to the RADIUS server. If the NAS does not receive a response from AAA before the guard timer expires, it accepts or rejects the calls on the basis of the configuration of the timer.

How to Configure AAA DNIS Map for Authorization

Configuring AAA DNIS Preauthentication

DNIS preauthentication enables preauthentication at call setup based on the number dialed. The DNIS number is sent directly to the security server when a call is received. If the call authenticated by AAA, it is accepted.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa preauthorization**
4. **group** {**radius** | **tacacs+** | *server-group*}
5. **dnis** [**password** *string*]
6. **end**

DETAILED STEPS

Procedure

	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	**aaa preauthorization** **Example:** `Device(config)# aaa preauthorization`	Enters AAA preauthentication configuration mode.
Step 4	**group** {**radius** | **tacacs+** | *server-group*} **Example:** `Device(config-preauth)# group radius`	(Optional) Selects the security server to use for AAA preauthentication requests. • The default is RADIUS.
Step 5	**dnis** [**password** *string*] **Example:** `Device(config-preauth)# dnis password dnispass`	Enables preauthentication using DNIS and optionally specifies a password to use in Access-Request packets.
Step 6	**end** **Example:** `Device(config-preauth)# end`	Exits AAA preauthentication configuration mode and returns to privileged EXEC mode.

Configuring AAA Server Group Selection Based on DNIS

To configure the device to select a particular AAA server group based on the DNIS of the server group, configure DNIS mapping. To map a server group with a group name with a DNIS number, perform the following task.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa dnis map enable**
4. **aaa dnis map** *dnis-number* **authentication ppp group** *server-group-name*
5. **aaa dnis map** *dnis-number* **authorization network group** *server-group-name*
6. **aaa dnis map** *dnis-number* **accounting network** [**none** | **start-stop** | **stop-only**] **group** *server-group-name*
7. **exit**

DETAILED STEPS

Procedure

	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 dnis map enable** **Example:** `Device(config)# aaa dnis map enable`	Enables DNIS mapping.
Step 4	**aaa dnis map** *dnis-number* **authentication ppp group** *server-group-name* **Example:** `Device(config)# aaa dnis map 7777 authentication ppp group sg1`	Maps a DNIS number to a defined AAA server group; the servers in this server group are being used for authentication.
Step 5	**aaa dnis map** *dnis-number* **authorization network group** *server-group-name* **Example:** `Device(config)# aaa dnis map 7777 authorization network group sg1`	Maps a DNIS number to a defined AAA server group; the servers in this server group are being used for authorization.
Step 6	**aaa dnis map** *dnis-number* **accounting network** [**none** | **start-stop** | **stop-only**] **group** *server-group-name* **Example:** `Device(config)# aaa dnis map 8888 accounting network stop-only group sg2`	Maps a DNIS number to a defined AAA server group; the servers in this server group are being used for accounting.
Step 7	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.

Configuring AAA Preauthentication

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa preauthorization**
4. **group** *server-group*
5. **clid** [**if-avail** | **required**] [**accept-stop**] [**password** *string*]
6. **ctype** [**if-avail** | **required**] [**accept-stop**] [**password** *string*]
7. **dnis** [**if-avail** | **required**] [**accept-stop**] [**password** *string*]
8. **dnis bypass** *dnis-group-name*
9. **end**

DETAILED STEPS

Procedure

	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 preauthorization** **Example:** `Device(config)# aaa preauthorization`	Enters AAA preauthentication configuration mode.
Step 4	**group** *server-group* **Example:** `Device(config-preauth)# group sg2`	Specifies the AAA RADIUS server group to use for preauthentication.
Step 5	**clid** [**if-avail** | **required**] [**accept-stop**] [**password** *string*] **Example:** `Device(config-preauth)# clid required`	Preauthenticates calls on the basis of the CLID number.
Step 6	**ctype** [**if-avail** | **required**] [**accept-stop**] [**password** *string*] **Example:**	Preauthenticates calls on the basis of the call type.

	Command or Action	Purpose
	`Device(config-preauth)# ctype required`	
Step 7	**dnis** [**if-avail** | **required**] [**accept-stop**] [**password** *string*] **Example:** `Device(config-preauth)# dnis required`	Preauthenticates calls on the basis of the DNIS number.
Step 8	**dnis bypass** *dnis-group-name* **Example:** `Device(config-preauth)# dnis bypass group1`	Specifies a group of DNIS numbers that will be bypassed for preauthentication.
Step 9	**end** **Example:** `Device(config-preauth)# end`	Exits preauthentication configuration mode and returns to privileged EXEC mode.

Configuring a Guard Timer

To set a guard timer to accept or reject a call in the event that the RADIUS server fails to respond to an authentication or preauthentication request, perform the following task.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **isdn guard-timer** *milliseconds* [**on-expiry** {**accept** | **reject**}]
5. **call guard-timer** *milliseconds* [**on-expiry** {**accept** | **reject**}]
6. **end**

DETAILED STEPS

Procedure

	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 number* **Example:** `Device(config)# interface serial 1/0/0:23`	Enters interface configuration mode.
Step 4	**isdn guard-timer** *milliseconds* [**on-expiry** {**accept** | **reject**}] **Example:** `Device(config-if)# isdn guard-timer 8000 on-expiry reject`	Sets an ISDN guard timer to accept or reject a call in the event that the RADIUS server fails to respond to a preauthentication request.
Step 5	**call guard-timer** *milliseconds* [**on-expiry** {**accept** | **reject**}] **Example:** `Device(config-if)# call guard-timer 2000 on-expiry accept`	Sets a CAS guard timer to accept or reject a call in the event that the RADIUS server fails to respond to a preauthentication request.
Step 6	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Configuration Examples for AAA DNIS Map for Authorization

Example: AAA Server Group Selection Based on DNIS

The following example shows how to select RADIUS server groups based on DNIS to provide specific AAA services:

```
! This command enables AAA.
aaa new-model
!
! The following set of commands configures the RADIUS attributes for each server
! that will be associated with one of the defined server groups.
radius-server host 172.16.0.1 auth-port 1645 acct-port 1646 key cisco1
radius-server host 172.17.0.1 auth-port 1645 acct-port 1646 key cisco2
radius-server host 172.18.0.1 auth-port 1645 acct-port 1646 key cisco3
radius-server host 172.19.0.1 auth-port 1645 acct-port 1646 key cisco4
radius-server host 172.20.0.1 auth-port 1645 acct-port 1646 key cisco5
! The following commands define the sg1 RADIUS server group and associate servers
! with it.
aaa group server radius sg1
  server 172.16.0.1
  server 172.17.0.1
! The following commands define the sg2 RADIUS server group and associate a server
! with it.
aaa group server radius sg2
```

```
  server 172.18.0.1
! The following commands define the sg3 RADIUS server group and associate a server
! with it.
aaa group server radius sg3
  server 172.19.0.1
! The following commands define the default-group RADIUS server group and associate
! a server with it.
aaa group server radius default-group
  server 172.20.0.1
! The next set of commands configures default-group RADIUS server group parameters.
aaa authentication ppp default group default-group
aaa accounting network default start-stop group default-group
!
! The next set of commands enables DNIS mapping and maps DNIS numbers to the defined
! RADIUS server groups. In this configuration, all PPP connection requests using
! DNIS 7777 are sent to the sg1 server group. The accounting records for these
! connections (specifically, start-stop records) are handled by the sg2 server group.
! Calls with a DNIS of 8888 use server group sg3 for authentication and server group
! default-group for accounting. Calls with a DNIS of 9999 use server group
! default-group for authentication and server group sg3 for accounting records
! (stop records only). All other calls with DNIS other than the ones defined use the
! server group default-group for both authentication and stop-start accounting records.
aaa dnis map enable
aaa dnis map 7777 authentication ppp group sg1
aaa dnis map 7777 accounting network start-stop group sg2
aaa dnis map 8888 authentication ppp group sg3
aaa dnis map 9999 accounting network stop-only group sg3
```

Examples: AAA Preauthentication

The following is a simple configuration that specifies that the DNIS number be used for preauthentication:

```
aaa preauthentication
 group radius
 dnis required
```

The following example shows a configuration that specifies that both the DNIS number and the CLID number be used for preauthentication. DNIS preauthentication is performed first, followed by CLID preauthentication.

```
aaa preauthentication
 group radius
 dnis required
 clid required
```

The following example specifies that preauthentication be performed on all DNIS numbers except the two DNIS numbers specified in the DNIS group called “dnis-group1”:

```
aaa preauthentication
 group radius
 dnis required
 dnis bypass dnis-group1
dialer dnis group dnis-group1
 number 12345
 number 12346
```

The following is a sample AAA configuration with DNIS preauthentication:

```
aaa new-model
aaa authentication login CONSOLE none
aaa authentication login RADIUS_LIST group radius
```

```
aaa authentication login TAC_PLUS group tacacs+ enable
aaa authentication login V.120 none
aaa authentication enable default enable group tacacs+
aaa authentication ppp RADIUS_LIST if-needed group radius
aaa authorization exec RADIUS_LIST group radius if-authenticated
aaa authorization exec V.120 none
aaa authorization network default group radius if-authenticated
aaa authorization network RADIUS_LIST if-authenticated group radius
aaa authorization network V.120 group radius if-authenticated
aaa accounting suppress null-username
aaa accounting exec default start-stop group radius
aaa accounting commands 0 default start-stop group radius
aaa accounting network default start-stop group radius
aaa accounting connection default start-stop group radius
aaa accounting system default start-stop group radius
aaa preauthentication
 dnis password Cisco-DNIS
aaa nas port extended
!
radius-server configure-nas
radius-server host 10.0.0.0 auth-port 1645 acct-port 1646 non-standard
radius-server host 10.255.255.255 auth-port 1645 acct-port 1646 non-standard
radius-server retransmit 2
radius-server deadtime 1
radius-server attribute nas-port format c
radius-server unique-ident 18
radius-server key MyKey
```

Note To configure preauthentication, you must also set up preauthentication profiles on the RADIUS server.

Examples: Guard Timer for ISDN and CAS

The following example shows an ISDN guard timer that is set at 8000 milliseconds. A call is rejected if the RADIUS server does not respond to a preauthentication request when the timer expires.

```
interface serial 1/0/0:23
 isdn guard-timer 8000 on-expiry reject
aaa preauthentication
 group radius
 dnis required
```

The following example shows a CAS guard timer that is set at 20,000 milliseconds. A call is accepted if the RADIUS server does not respond to a preauthentication request when the timer expires.

```
controller T1 0
 framing esf
 clock source line primary
 linecode b8zs
 ds0-group 0 timeslots 1-24 type e&m-fgb dtmf dnis
 cas-custom 0
 call guard-timer 20000 on-expiry accept
aaa preauthentication
group radius
dnis required
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
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
AAA	*Authentication, Authorization, and Accounting Configuration Guide* (part of the Securing User Services Configuration Library)

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 DNIS Map for Authorization

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 AAA DNIS Map for Authorization

Feature Name	Releases	Feature Information
AAA DNIS Map for Authorization	12.1(1)T 12.2(2)T 12.2(27)SBA Cisco IOS XE Release 2.3	The AAA DNIS Map for Authorization feature allows you to assign a Dialed Number Identification Service (DNIS) number to a particular AAA server group so that the server group can process authentication, authorization, and accounting requests for users dialing in to the network using that particular DNIS. Any phone line (a regular home phone or a commercial T1/ PRI line) can be associated with several phone numbers. The DNIS number identifies the number that was called to reach you. The following commands were introduced or modified: **aaa dnis enable**, **aaa dnis map authentication group**, **aaa dnis map authorization network group**, and **aaa dnis map accounting network**.