

DNS Server Request Support in AAA

Feature Summary

Microsoft Point-to-Point Protocol (PPP) clients have the ability to request a primary and secondary domain naming system (DNS) server from the network access server (NAS) during IP Control Protocol (IPCP) negotiation. To support this functionality using authentication, authorization, and accounting (AAA) security services, two new TACACS+ attribute-value (AV) pairs and two new vendor-proprietary RADIUS attributes have been added.

Note The primary and secondary DNS servers designated by these attributes will only be applied when requested to do so by the client. At this time, only Microsoft PPP peers have the ability to request DNS servers.

Table 1 shows the new TACACS+ attribute-value (AV) pairs that have been added to provide DNS server request functionality.

Table 1 Supported TACACS+ AV Pairs

Attribute	Description
dns-servers	Identifies a DNS server (primary or secondary) that can be requested by Microsoft PPP clients from the network access server during IPCP negotiation. To be used with <code>service=ppp</code> and <code>protocol=ip</code> . The IP address identifying each DNS server is entered in dotted decimal format. If you have multiple IP addresses, the addresses are separated by a space. For example, <code>1.1.1.1 2.2.2.2</code>
wins-servers	Identifies a primary and secondary NetBIOS Name Service that can be requested by Microsoft PPP clients from the network access server during IPCP negotiation. To be used with <code>service=ppp</code> and <code>protocol=ip</code> . The IP address identifying each Windows NT server is entered in dotted decimal format. If you have multiple IP addresses, the addresses are separated by a space. For example, <code>1.1.1.1 2.2.2.2</code>

Table 2 shows the additional RADIUS vendor-proprietary attributes that have been added to provide DNS server request functionality.

Table 2 Vendor-Proprietary RADIUS Attributes

Number	Vendor-Proprietary Attribute	Description
135	Primary-DNS-Server	Identifies a primary DNS server that can be requested by Microsoft PPP clients from the network access server during IPCP negotiation.
136	Secondary-DNS-Server	Identifies a secondary DNS server that can be requested by Microsoft PPP clients from the network access server during IPCP negotiation.

Benefits

This feature provides additional AAA functionality by enabling Microsoft PPP users to request DNS servers during IPCP negotiation.

List of Terms

Attributes—Data items sent between a network access server and a daemon that are used to direct AAA activities.

Authentication, authorization, and accounting (AAA)—Suite of network security services that provide the primary framework through which access control can be set up on your Cisco router or access server.

Domain naming system (DNS)—Distributed database system used to translate host computer names into IP addresses.

Internet Engineering Task Force (IETF)—A task force, working under the auspices of the Internet Society (ISOC), consisting of more than 80 working groups. The IETF is responsible for developing Internet standards.

IP Control Protocol (IPCP)—Protocol for transporting IP traffic over a PPP connection.

Network access server (NAS)—A Cisco access server or any other Cisco device that is acting as a client to the RADIUS or TACACS+ server.

Platforms

The following platforms support DNS server request support in AAA:

- Cisco AS5200 series
- Cisco AS5300 series
- Cisco AS5800 series
- Cisco 7200 series

Prerequisites

For Microsoft PPP clients to be able to request either a primary or secondary DNS server during IPCP negotiation, you must perform the following prerequisite tasks:

- Install and configure Microsoft PPP on your NAS. The primary and secondary DNS servers designated by these attributes will not be applied automatically; they must be requested by the PPP clients. At this time, only Microsoft PPP peers have the ability to request DNS servers.
- Enable AAA security services on your NAS.
 - Use the **aaa new-model** global configuration command to enable AAA. TACACS+ and RADIUS are administered through AAA, so AAA must be enabled. For more information about AAA or using the **aaa new-model** command, refer to the “AAA Overview” chapter in the Cisco IOS Release 11.3 *Security Configuration Guide*.
 - Use the **aaa authentication** global configuration command to define method lists, selecting the applicable security protocol (TACACS+ or RADIUS) as the method for authentication. For more information about using the **aaa authentication** command, refer to the “Configuring Authentication” chapter in the Cisco IOS Release 11.3 *Security Configuration Guide*.
 - Use the **aaa authorization** global configuration command to define method lists, selecting the applicable security protocol (TACACS+ or RADIUS) as the method for authorization. For more information about using the **aaa authorization** command, refer to the Cisco IOS Release 11.3 (3)T feature, “Named Method Lists for AAA Authorization and Accounting.”
 - Use the **line** and **interface** commands to select specific lines and interfaces to which the defined authentication and authorization method lists will be applied. For more information about applying method lists to lines and interfaces, refer to the “Configuring Authentication” chapter in the Cisco IOS Release 11.3 *Security Configuration Guide* and the Cisco IOS Release 11.3 (3)T feature, “Named Method Lists for AAA Authorization and Accounting.”
- Configure your network access server to communicate with the applicable security server—in this case, either a TACACS+ or RADIUS daemon.
 - If you are using RADIUS, use the `radius-server host non-standard` command to enable your Cisco router, acting as a NAS, to recognize that the RADIUS security server is using a vendor-proprietary version of RADIUS. Use the `radius-server key` command to specify the shared secret text string used between your Cisco router and the RADIUS server. For more information, refer to the “Configuring RADIUS” chapter in the Cisco IOS Release 11.3 *Security Configuration Guide*.
 - If you are using TACACS+, use the `tacacs-server host` command to specify the IP address of one or more TACACS+ daemons. Use the `tacacs-server key` command to specify the shared secret text string used between your Cisco router and the TACACS+ daemon. For more information, refer to the “Configuring TACACS+” chapter in the Cisco IOS Release 11.3 *Security Configuration Guide*.

Supported MIBs and RFCs

No MIBs or RFCs are supported by this feature.

Configuration Tasks

After you have enabled AAA security services and configured your NAS to support the security protocol of your choice (either TACACS+, RADIUS, or a vendor-proprietary version of RADIUS), you need to define the applicable attribute or AV pair on your security server to configure DNS server requests for Microsoft PPP users. Refer to the documentation associated with your chosen security server for specific information about defining attributes or AV pairs.

Configuration Examples

There are essentially three different ways to configure DNS server requests for Microsoft PPP users: using TACACS+, using RADIUS, or using a vendor-proprietary version of RADIUS. This section provides the following examples:

- Configure DNS Server Requests Using TACACS+
- Configure DNS Server Request Using Vendor-Proprietary RADIUS
- Configure DNS Server Requests Using RADIUS

Configure DNS Server Requests Using TACACS+

The following is a general NAS configuration using TACACS+ with the AAA command set:

```
aaa new-model
aaa authentication login admins local
aaa authentication ppp dialins tacacs+ local
aaa authorization network tacacs+ local
aaa accounting network start-stop tacacs+

username root password ALongPassword

tacacs-server host 10.1.2.3
tacacs-server key goaway

interface group-async 1
  group-range 1 16
  encapsulation ppp
  ppp authentication pap dialins

line 1 16
  autoselect ppp
  autoselect during-login
  login authentication admins
  modem dialin
```

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

- The **aaa new-model** command enables AAA network security services.
- The **aaa authentication login admins local** command defines another method list, “admins,” for login authentication.
- The **aaa authentication ppp dialins tacacs+ local** command defines the authentication method list “dialins,” which specifies that TACACS+ authentication, then (if this server does not respond) local authentication will be used on serial lines using PPP.
- The **aaa authorization network tacacs+ local** command is used to assign an address and other network parameters to the TACACS+ user.

- The **aaa accounting network start-stop tacacs+** command tracks PPP usage.
- 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 IP address of the TACACS+ host.
- The **tacacs-server key** command defines the shared secret text string between the NAS and the TACACS+ 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 pap dialins** command applies the “dialins” 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 following example defines the TACACS+ AV pairs necessary to implement DNS server request functionality on the TACACS+ security server:

```
user = fred {
    service = ppp protocol = ip {
        dns-servers = "1.0.0.10 2.0.0.2"
        wins-servers = "3.3.3.3 4.0.2.1"
    }
}
```

Configure DNS Server Request Using Vendor-Proprietary RADIUS

The following sample is a general NAS configuration using vendor-proprietary RADIUS with the AAA command set:

```
aaa new-model
aaa authentication login admins local
aaa authentication ppp dialins radius local
aaa authorization network radius local
aaa accounting network start-stop radius

username root password ALongPassword

radius-server configure-nas
radius-server host alcatraz non-standard
radius-server key myRaDiUSpassWoRd
```

```
interface group-async 1
  group-range 1 16
  encapsulation ppp
  ppp authentication pap dialins

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 another method list, “admins,” for login authentication.
- The **aaa authentication ppp dialins radius local** command defines the authentication method list “dialins,” which specifies that RADIUS authentication, then (if the RADIUS server does not respond) local authentication will be used on serial lines using PPP.
- The **aaa authorization network radius local** command is used to assign an address and other network parameters to the RADIUS user.
- The **aaa accounting network start-stop radius** command tracks PPP usage.
- The **username** command defines the username and password to be used for the PPP Password Authentication Protocol (PAP) caller identification.
- The **radius-server configure-nas** command defines that the Cisco router or access server will query the RADIUS server for static routes and IP pool definitions when the device first starts up.
- The **radius-server host non-standard** command defines the name of the RADIUS server host and identifies that this RADIUS host uses a vendor-proprietary version of RADIUS.
- 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 pap dialins** command applies the “dialins” 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 following example defines the RADIUS attributes necessary to implement DNS server request functionality on the vendor-proprietary RADIUS security server:

```
Ascend-Primary-DNS = 1.0.0.2,  
Ascend-Secondary-DNS = 2.0.0.2
```

Configure DNS Server Requests Using RADIUS

If you are using IETF-compliant RADIUS, you can implement this feature by using RADIUS Attribute 26 (vendor-specific). The Cisco RADIUS implementation supports one vendor-specific option using the format recommended in the specification. Cisco's vendor-ID is 9, and the supported option has vendor-type 1, which is named "cisco-avpair."

The value is a string of the format:

```
protocol : attribute sep value
```

"Protocol" is a value of the Cisco "protocol" attribute for a particular type of authorization. "Attribute" and "value" are an appropriate AVpair defined in the Cisco TACACS+ specification, and "sep" is "=" for mandatory attributes and "*" for optional attributes.

The following example defines the RADIUS attributes necessary to implement DNS server request functionality on the RADIUS security server using Attribute 26:

```
cisco-avpair= "ip:dns-servers=1.0.0.2 2.0.0.2"  
cisco-avpair= "ip:wins-servers=3.0.0.2 4.0.0.2"
```

Command Reference

There are no new or modified commands introduced with this feature. All commands used with this feature are documented in the Cisco IOS Release 11.3 command references.

