Configuring DHCP Option 60 and Option 82 with VPN-ID Support for Transparent Automatic Logon

Last Updated: December 19, 2012

Intelligent Services Gateway (ISG) is a Cisco IOS software feature set that provides a structured framework in which edge devices can deliver flexible and scalable services to subscribers. The DHCP Option 60 and Option 82 with VPN-ID Support for Transparent Automatic Logon feature enables service providers to provision triple-play services to households by supporting transparent automatic logon (TAL) through Dynamic Host Configuration Protocol (DHCP) option 60 and option 82, and wholesale IP sessions through the virtual private network (VPN) ID extension to option 82.

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.

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

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 DHCP Option 60 and Option 82 with VPN-ID Support for Transparent Automatic Logon

For vendor-class ID (option 60) to be used for authorization, the vendor-class ID must be inserted by the customer appliance (that is, the PC, phone, or set-top box) in the DHCP option 60 information.

For provisioning of wholesale IP sessions, the VPN-ID must be inserted in the DHCP option 82 information along with the circuit ID and the remote ID.

Restrictions for DHCP Option 60 and Option 82 with VPN-ID Support for Transparent Automatic Logon

RADIUS proxy users are not supported by this feature.

Information About DHCP Option 60 and Option 82 with VPN-ID Support for Transparent Automatic Logon

ISA Automatic Subscriber Logon

TAL enables a specified identifier to be used in place of the username in authorization requests. Enabling the Authentication, Authorization, and Accounting (AAA) server to authorize subscribers on the basis of a specified identifier allows subscriber profiles to be downloaded from the AAA server as soon as packets are received from subscribers.

Session start is the event that triggers TAL. For DHCP-initiated IP sessions, session start occurs when a DHCP DISCOVER request is received.

Authorization Based on Option 60 and Option 82

The circuit ID and remote ID fields (option 82) are part of the DHCP relay agent information option. A digital subscriber line access multiplexer (DSLAM) inserts the option 82 fields into DHCP messages; the customer appliance inserts the option 60 fields.

You can configure an ISG policy to use the circuit ID, remote ID, or vendor class ID, or a combination of the three, as the username in authorization requests. Alternatively, you can configure an ISG policy to use the NAS-Port-ID as the identifier for authorization. When you use the NAS-Port-ID as the identifier, you can configure it to include a combination of circuit ID, remote ID, and vendor-class ID.

By default, the ISG uses the circuit ID and remote ID that are provided by the Layer 2 edge-access device for authorization. The configuration of the **ip dhcp relay information option** command determines

whether the ISG uses the option 82 information received, generates its own, or (when the **encapsulate** keyword is specified) encapsulates a prior option 82 along with its own option 82. For more information, see the "Configuring the Cisco IOS DHCP Relay Agent" section of the *Cisco IOS IP Addressing Services Configuration Guide* .

If the NAS-Port-ID is not configured to include option 60 and option 82, the NAS-Port-ID is populated with the ISG interface that received the DHCP relay agent information packet; for example, Ethernet1/0.

DHCP Option 82 with VPN-ID Suboption

To support wholesale services for IP sessions, the VPN-ID, together with the circuit ID and remote ID, must be specified in authorization requests. The DHCP option 60 and option 82 with VPN-ID Support for Transparent Automatic Logon feature enables you to include two sets of option 82 information in a single message so that devices within a household can be differentiated:

- The first set of option 82 information carries household information and option 60 to associate the device within the household.
- The second set of option 82 information, if VPN-ID is configured, carries the VPN information for the household.

The DHCP server processes the option 82 information, forwarded by the relay, with the VPN-ID, remote ID, circuit ID, and option 60 information to allocate an address.

How to Configure DHCP Option 60 and Option 82 with VPN-ID Support for Transparent Automatic Logon

You can configure an ISG policy for TAL using either a username or the NAS-Port-ID for authorization.

- Configuring an ISG Control Policy Using Option 60 and Option 82, page 3
- Configuring an ISG Control Policy Using NAS-Port-ID, page 5
- Configuring NAS-Port-ID to Include Option 60 and Option 82, page 6

Configuring an ISG Control Policy Using Option 60 and Option 82

Perform this task to configure an ISG control policy that inserts a specified identifier into the username field of the authorization request.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type control** *policy-map-name*
4. **class type control** {*class-map-name* | **always**} **event session-start**
5. *action-number* **authorize** [**aaa** {*list-name* | **list** {*list-name* | **default**}} [**password** *password*]] [**upon network-service-found** {**continue** | **stop**}] [**use method** *authorization-type*] **identifier** *identifier-type* [**plus** *identifier-type*]
6. **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	**policy-map type control** *policy-map-name* **Example:** `Router(config)# policy-map type control TAL`	Enters control policy-map configuration mode to define a control policy.
Step 4	**class type control** {*class-map-name* | **always**} **event session-start** **Example:** `Router(config-control-policymap)# class type control TAL-subscribers event session-start`	Enters control policy-map class configuration mode to define the conditions that must be met in order for an associated set of actions to be executed. • Specify the control class-map that was configured in the section "Identifying Traffic for Automatic Logon in a Control Policy Class Map".
Step 5	*action-number* **authorize** [**aaa** {*list-name* | **list** {*list-name* | **default**}} [**password** *password*]] [**upon network-service-found** {**continue** | **stop**}] [**use method** *authorization-type*] **identifier** *identifier-type* [**plus** *identifier-type*] **Example:** `Router(config-control-policymap-class-control)# 1 authorize aaa list TAL_LIST password cisco identifier source-ip-address vendor-class-id plus circuit-id plus remote-id`	Inserts the specified identifier into the username field of authorization requests.
Step 6	**end** **Example:** `Router(config-control-policymap-class-control)# end`	Exits the current configuration mode and returns to privileged EXEC mode.

Configuring an ISG Control Policy Using NAS-Port-ID

Perform this task to configure an ISG control policy that uses NAS-Port-ID in the authorization request.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type control** *policy-map-name*
4. **class type control** {*class-map-name* | **always**} **event session-start**
5. *action-number* **authorize** [**aaa** {*list-name* | **list** {*list-name* | **default**}} [**password** *password*]] [**upon network-service-found** {**continue** | **stop**}] [**use method** *authorization-type*] **identifier nas-port**
6. **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	**policy-map type control** *policy-map-name* **Example:** `Router(config)# policy-map type control TAL`	Enters control policy-map configuration mode to define a control policy.
Step 4	**class type control** {*class-map-name*	**always**} **event session-start** **Example:** `Router(config-control-policymap)# class type control TAL-subscribers event session-start`	Enters control policy-map class configuration mode to define the conditions that must be met in order for an associated set of actions to be executed. • Specify the control class-map that was configured in the section "Identifying Traffic for Automatic Logon in a Control Policy Class Map".

	Command or Action	Purpose
Step 5	*action-number* **authorize** [**aaa** {*list-name* | **list** {*list-name* | **default**}} [**password** *password*]] [**upon network-service-found** {**continue** | **stop**}] [**use method** *authorization-type*] **identifier nas-port** **Example:** `Router(config-control-policymap-class-control)# 1 authorize aaa list TAL_LIST password cisco identifier nas-port`	Inserts the NAS port identifier into the username field of authorization requests.
Step 6	**end** **Example:** `Router(config-control-policymap-class-control)# end`	Exits the current configuration mode and returns to privileged EXEC mode.

Configuring NAS-Port-ID to Include Option 60 and Option 82

Perform this task to include option 60 and option 82 in the NAS-Port-ID.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **radius-server attribute nas-port-id include** {*identifier1* [**plus** *identifier2*] [**plus** *identifier3*]} [**separator** *separator*]

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 attribute nas-port-id include** {*identifier1* [**plus** *identifier2*] [**plus** *identifier3*]} [**separator** *separator*] **Example:** `Router(config)# radius-server attribute nas-port-id include circuit-id plus vendor-class-id`	Includes DHCP relay agent information option 60 and option 82 in the NAS-Port-ID.

Configuration Examples for DHCP Option 60 and Option 82 with VPN-ID Support for Transparent Automatic Logon

Example Option 60 and Option 82 in NAS-Port-ID

The following example uses the **radius-server attribute nas-port-id include** command to configure option 60 and option 82 authorization using circuit ID, remote ID, and vendor-class ID:

```
interface Ethernet0/0
 service-policy type control RULEA
!
interface Ethernet1/0
 service-policy type control RULEB
!
class-map type control match-all CONDA
 match source-ip-address 10.1.1.0 255.255.255.0
!
class-map type control match-all CONDB
 match vendor-class-id vendor1
!
policy-map type control RULEA
 class type control CONDA event session-start
  1 authorize aaa list TAL_LIST password cisco identifier vendor-class-id
!
policy-map type control RULEB
 class type control CONDB event session-start
  1 authorize aaa list TAL_LIST password cisco identifier nas-port
!
radius-server attribute nas-port-id include circuit-id plus remote-id plus vendor-class-
id separator #
```

Additional References

Related Documents

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

Related Topic	Document Title
ISG commands	*Cisco IOS Intelligent Services Gateway Command Reference*
Configuring ISG policies for automatic subscriber logon	"Configuring ISG Policies for Automatic Subscriber Logon" module in this guide
Configuring a DHCP relay agent	"Configuring the Cisco IOS DHCP Relay Agent" module in the *Cisco IOS XE IP Addressing Services Configuration Guide*

Standards

Standard	Title
None	-

MIBs

MIB	MIBs Link
•	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
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/cisco/web/support/index.html

Feature Information for DHCP Option 60 and Option 82 with VPN-ID Support for Transparent Automatic Logon

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 DHCP Option 60 and Option 82 Support and VPN-ID Support

Feature Name	Releases	Feature Information
ISG: Authentication: DHCP Option 60 and Option 82 with VPN-ID Support for Transparent Automatic Logon	12.2(33)SRD	Enables service providers to support TAL through DHCP option 60 and option 82 and wholesale IP sessions through the VPN-ID extension to option 82. This feature is platform independent and is supported on Cisco 7600 routers as well as on Cisco 7200 routers and Cisco 7301 routers. The following commands were introduced or modified: **radius-server attribute nas-port-id include** .