

Configuring ISG Policies for Session Maintenance

Intelligent Services Gateway (ISG) is a Cisco IOS XE software feature set that provides a structured framework in which edge devices can deliver flexible and scalable services to subscribers. This module describes how to configure a session timer and connection timer through a service policy map. Additionally, the Internet Engineering Task Force (IETF) RADIUS attributes Session-Timeout (attribute 27) and Idle-Timeout (attribute 28) can be used in service profiles on an authentication, authorization, and accounting (AAA) server to configure the same session maintenance control.

IP subscriber session keepalive support is configured for monitoring session data traffic in the upstream direction for idleness. Address Resolution Protocol (ARP) is used for Layer 2 connected subscribers. For routed host (Layer 3 connected) subscribers, the protocol defaults to Internet Control Message Protocol (ICMP). ICMP is also used in configurations where the access interface does not support ARP.

- Prerequisites for ISG Policies for Session Maintenance, on page 1
- Information About ISG Policies for Session Maintenance, on page 1
- How to Configure ISG Policies for Session Maintenance, on page 3
- Configuration Examples for ISG Policies for Session Maintenance, on page 12
- Additional References, on page 15
- Feature Information for ISG Policies for Session Maintenance, on page 15

Prerequisites for ISG Policies for Session Maintenance

A traffic class is required only if an idle timer or session timer is being installed on a service that has a traffic class definition in it. If the timer is installed on a session or service that has no traffic class, a traffic class is not required. See the "Configuring ISG Subscriber Services" module for information about how to configure a traffic class.

Information About ISG Policies for Session Maintenance

Session Maintenance Timers

ISG provides two commands (each of which can be set independently) to maintain control over a session and its connection. The **timeout absolute** command controls how long a session can be connected before it is

terminated. The **timeout idle** command controls how long a connection can be idle before it is terminated. Both commands detect both PPP and IP sessions and can be applied in a non-traffic-class-based service, on a per-session basis, or in a flow (traffic-class-based service). All subscriber traffic will reset the timers; however, non-network traffic such as PPP control packets will not reset the timers.

The scope of the session timers and connection timers is determined by the type of service within which the timer is specified. If specified in a service profile for which no traffic class is defined, the timer action will be to terminate the session or connection. If a traffic class specifier resides in the service profile, the timer action will be to deactivate the service.

Benefits of Session Maintenance Timers

The PPP idle timeout functionality has been replaced by the ISG idle timeout feature. The idle timer is a generic feature that can be set to detect idle traffic in both PPP and IP sessions.

You set the idle timer in a service profile that is installed on a session to control how long that service stays installed before it is removed from the session because no traffic is flowing through that service. If the service has traffic class parameters associated with it, that traffic class is terminated when this timer expires, or when the session itself is terminated.

The same is true for the session timer, except that this timer determines how long the session or service stays up, regardless of traffic flowing through it.

Monitoring Sessions

The IP subscriber session's data traffic in the upstream direction can be monitored for idleness using a keepalive feature configured for the subscriber. If a session is idle for a configured period of time, keepalive requests are sent to the subscriber. This action verifies that the connection is still active. The protocol to use for the keepalive request and response can be configured based on the IP subscriber session type. If it is a directly connected host (Layer 2 connection), ARP is used. For routed host (Layer 3 connected) subscribers, ICMP is used. If the access interface does not support ARP, the keepalive protocol defaults to ICMP.

ARP for Keepalive Messages

When a session is established and the keepalive feature is configured to use ARP, the keepalive feature saves the ARP entry as a valid original entry for verifying future ARP responses.



Note In cases where the access interface does not support ARP, the protocol for keepalives defaults to ICMP.

When ARP is configured, the ARP unicast request is sent to the subscriber. After a configured interval of time, the ARP response (if received) is verified. If the response is correct and matches the original entry that was saved when the subscriber was initially established, the keepalive feature continues monitoring the data plane for the configured interval of time. If the response is not correct, the keepalive feature resends the ARP request until a correct response is received or the configured maximum number of attempts is exceeded.

ICMP for Keepalive Messages

If ICMP is configured, the ICMP “hello” request is sent to the subscriber and checked for a response, until the configured maximum number of attempts is exceeded.

For IP subnet sessions, the peer (destination) IP address to be used for ICMP “hello” requests will be all the IP addresses within the subnet. This means “hello” requests will be sent sequentially (not simultaneously) to all the possible hosts within that subnet. If there is no response from any host in that subnet, the session will be disconnected.

Another option is to configure ICMP directed broadcast for keepalive requests. If the subscriber hosts recognize the IP subnet broadcast address, the ISG can send the ICMP “hello” request to the subnet broadcast address. The subscribers need not be on the same subnet as the ISG for this configuration to work. A directed broadcast keepalive request can work multiple hops away as long as these conditions are satisfied:

- The group of subscribers identified by the subnet must have the same subnet mask provisioned locally as the subnet provisioned on the subnet subscriber session on the ISG. Otherwise, the subscriber hosts will not recognize the subnet broadcast address.
- The router directly connected to the hosts must enable directed-broadcast forwarding, so that the IP subnet broadcast gets translated into a Layer 2 broadcast.

When these two conditions are satisfied, you can optimize the ICMP keepalive configuration to minimize the number of ICMP packets.

Note Because enabling directed broadcasts increases the risk of denial of service attacks, the use of subnet directed broadcasts is not turned on by default.

HA Support for Session Maintenance Timers

The SSO and ISSU feature provides high availability (HA) support for ISG timers including the connection timer, session timer, and the session keepalive. The timers and keepalive are restarted on the new standby Route Processor (RP) after a stateful switchover (SSO) or In Service Software Upgrade (ISSU) event.

For information about configuring HA on the ISG router, see the High Availability Configuration Guide, Cisco IOS XE Release 3S .

How to Configure ISG Policies for Session Maintenance

Configuring the session maintenance timers requires two separate tasks, one to set the idle timer and one to set the session timer. Either one or both of these tasks can be performed in order to set session maintenance control. The following tasks show how to set these timers in a service policy map and in a RADIUS AAA server profile:

Configuring the Session Timer in a Service Policy Map

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type service** *policy-map-name*
4. [*priority*] **class type traffic***class-map-name*
5. **timeout absolute** *duration-in-seconds*
6. **end**

DETAILED STEPS

Procedure

	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 service** *policy-map-name* **Example:** `Router(config)# policy-map type service policy1`	Enters policy map configuration mode so you can begin configuring the service policy.
Step 4	[*priority*] **class type traffic***class-map-name* **Example:** `Router(config-control-policymap)# class type traffic class1`	Associates a previously configured traffic class with the policy map.
Step 5	**timeout absolute** *duration-in-seconds* **Example:** `Router(config-control-policymap-class-control)# timeout absolute 30`	Specifies the session lifetime, in seconds.
Step 6	**end** **Example:** `Router(conf-subscriber-profile)# end`	Returns to privileged EXEC mode.

What to Do Next

You may want to configure a method of activating the service policy map or service profile; for example, control policies can be used to activate services. For more information about methods of service activation, see the module "Configuring ISG Subscriber Services".

Configuring the Session Timer on a AAA Server

Perform this task to configure the session timer in a service profile on a AAA server.

SUMMARY STEPS

1. **Session-Timeout=***duration-in-seconds*

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**Session-Timeout=***duration-in-seconds*	Sets the IETF RADIUS session timer (attribute 27) in a user or service profile, in a range from 0 to 31104000 seconds.

Configuring the Connection Timer in a Service Policy Map

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type service** *policy-map-name*
4. [*priority*] **class type traffic** *class-map-name*
5. **timeout idle** *duration-in-seconds* [**both** | **inbound**]
6. **end**

DETAILED STEPS

Procedure

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

	Command or Action	Purpose
	`Router# configure terminal`	
Step 3	**policy-map type service** *policy-map-name* **Example:** `Router(config)# policy-map type service policy1`	Enters policy map configuration mode so you can begin configuring the service policy.
Step 4	[*priority*] **class type traffic** *class-map-name* **Example:** `Router(config-service-policymap)# class type traffic class1`	Associates a previously configured traffic class to the policy map.
Step 5	**timeout idle** *duration-in-seconds* [**both** | **inbound**] **Example:** `Router(config-control-policymap-class-traffic)# timeout idle 3000 inbound`	Specifies how long a connection can be idle before it is terminated and in which direction to apply the timer. The range is platform and release-specific. For more information, use the question mark (?) online help function.
Step 6	**end** **Example:** `Router(config-control-policymap-class-traffic)# end`	Returns to privileged EXEC mode.

What to Do Next

You may want to configure a method of activating the service policy map or service profile; for example, control policies can be used to activate services. For more information about methods of service activation, see the module "Configuring ISG Subscriber Services".

Configuring the Connection Timer on a AAA Server

Perform this task to set the connection timer (idle timeout) in a AAA service profile.

SUMMARY STEPS

1. **idle-timeout=** *duration-in-seconds*
2. **idle-timeout-direction=** *direction*

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**idle-timeout=** *duration-in-seconds*	Sets IETF RADIUS attribute 28 in a user or service profile, in a range from 1 to 15552000 seconds.
Step 2	**idle-timeout-direction=** *direction*	Sets the direction of subscriber traffic on which to apply the idle timeout. Values are **inbound** or **both**. If the timer is configured without specifying a direction, it is applied by default to the outbound direction.

Example

```
simulator radius subscriber 999
attribute 28 numeric 100
vsa cisco generic 1 string "subscriber:idle-timeout-direction=inbound"
attribute 44 string "00000008"
```

Verifying the Session and Connection Timer Settings

Perform this task to verify that the timers have been installed correctly.

SUMMARY STEPS

1. **enable**
2. **show subscriber session all**
3. **end**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show subscriber session all** **Example:** `Router# show subscriber session all`	Displays current subscriber information, including reports about the timers that are enabled.

	Command or Action	Purpose
Step 3	**end** **Example:** `Router# end`	Returns to privileged EXEC mode.

Troubleshooting the Session and Connection Timer Settings

The following sections describe the **debug** commands that can be used to troubleshoot the session maintenance timers:

Prerequisites for Troubleshooting the Session Maintenance Timers

Before performing the task in this section, it is recommended that you be familiar with the use of Cisco IOS **debug** commands described in the introductory chapters of the *Cisco IOS Debug Command Reference.* Also see the module "Troubleshooting ISG with Session Monitoring and Distributed Conditional Debugging."

Restrictions for Troubleshooting the Session Maintenance Timers



Caution Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use the Cisco IOS **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, we recommend that you use **debug** commands during periods of lower network traffic and fewer users, or on a debug chassis with a single active session. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Debug Commands Available for the Session Maintenance Timers

The table below lists the **debug** commands that can be used to diagnose problems with the session maintenance timers.

Table 1: Debug Commands for Troubleshooting Session Maintenance Timers

Command	Purpose
debug subscriber feature error	Displays general Feature Manager errors.
debug subscriber feature event	Displays general Feature Manager events.
debug subscriber feature name idle-timer error	Displays idle timer errors.
debug subscriber feature name idle-timer event	Displays idle timer events.
debug subscriber feature name session-timer error	Displays session timer errors.
debug subscriber feature name session-timer event	Displays session timer events.

Configuring a Session Keepalive on the Router

This task describes how to configure the keepalive feature on the router, using either ARP or ICMP.

Because the session keepalive feature is checking for the subscriber's health and presence, this feature is applied only to the session as a whole and not per-flow.

Note

- If a service profile includes an ISG traffic class configuration, the keepalive feature will be ignored.
- If this feature is applied to a non-IP session, for example, a PPP over Ethernet (PPPoE) or PPP over ATM (PPPoA) session, this feature application will fail and the following applies:
  - If the feature is applied at a session-start event, both the feature application and the session will fail.
  - If this feature is pushed onto a session after the session-start event, the push will fail.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type service** *policy-map-name*
4. **keepalive** [**idle** *idle-seconds*] [**attempts** *max-retries*] [**interval** *retry-seconds*] [**protocol** {**ARP** | **ICMP** [**broadcast**]}]
5. **exit**

DETAILED STEPS

Procedure

	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 service** *policy-map-name* **Example:** `Router(config)# policy-map type service policymap1`	Enters service policy map configuration mode.
Step 4	**keepalive** [**idle** *idle-seconds*] [**attempts** *max-retries*] [**interval** *retry-seconds*] [**protocol** {**ARP**	**ICMP** [**broadcast**]}]	Enables keepalive messages and sets the maximum idle period, number of requests, interval between requests, and protocol for keepalive messages.

	Command or Action	Purpose
	Example: `Router(config-service-policymap)# keepalive idle 7 attempts 3 interval 1 protocol arp`	• The ranges and default values for the **idle**, **attempts**, and **interval** keywords are platform and release-specific. For more information, use the question mark (**?**) online help function. • **protocol** —For Layer 2 connections, the default is ARP; for routed connections, the default is ICMP. • **broadcast** —This option is disabled by default. **Note** If this command is applied to a non-IP session, the command will fail. If the command is applied to a non-IP session at the session-start event, the session will also fail.
Step 5	**exit** **Example:** `Router(config-service-policymap)# exit`	Returns to global configuration mode.

Example

The following example configures the keepalive feature on a router using ARP:

```
policy-map type service accting_service
 class type traffic ALL
 !
 keepalive idle 7 attempts 3 interval 1 protocol arp
!
```

Configuring a Session Keepalive on a RADIUS Server

This task describes how to configure the session keepalive parameters on a RADIUS server.

SUMMARY STEPS

1. Service-Name password = “cisco”
2. Cisco-Avpair = “subscriber:keepalive = [idle *period1*] [attempts *Max-retries*] [interval *period2*] [protocol *ICMP* [broadcast] | *ARP*}”

DETAILED STEPS

Procedure

Step 1 Service-Name password = “cisco”

Step 2 Cisco-Avpair = "subscriber:keepalive = [idle *period1*] [attempts *Max-retries*] [interval *period2*] [protocol *ICMP* [broadcast] | *ARP*}"

Configures the allowable idle period, maximum number of attempts to connect, the interval between attempts, and the communication protocol to be used.

The ranges and defaults are as follows:

- Idle period: range is 5 to10 seconds; default is 10 seconds.
- Attempts: range is 3 to 10; default is 5.
- Interval: default is 1 to 10 seconds.
- Protocol: for Layer 2 connections, the default is ARP; for routed connections, the default is ICMP.
- Broadcast option: by default this option is disabled.

Note
If a service profile includes an ISG traffic class configuration, the keepalive feature will be ignored.

Configuring the ISG to Interact with the RADIUS Server

The ISG device interacts with the RADIUS server to listen for the Packet of Disconnect (POD) message from the RADIUS server. On receipt, the POD and associated attributes are handed to the appropriate client to disconnect the session. Perform this task to configure the ISG to interact with the RADIUS server to listen for the POD message.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa server radius dynamic-author**
5. **client** *ip-address*
6. **port** *port-number*
7. **server-key** *word*
8. **exit**

DETAILED STEPS

Procedure

	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	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**aaa new-model** **Example:** `Router(config)# aaa new-model`	Enables the authentication, authorization, and accounting (AAA) access control model.
Step 4	**aaa server radius dynamic-author** **Example:** `Router(config)# aaa server radius dynamic-author`	Configures a device as a AAA server to facilitate interaction with an external policy server and enters dynamic authorization local server configuration mode.
Step 5	**client** *ip-address* **Example:** `Router(config-locsvr-da-radius)# client 10.10.10.11`	Specifies a RADIUS client from which a device will accept Change of Authorization (CoA) and disconnect requests. • The example specifies 10.10.10.11 as the IP address of the RADIUS client.
Step 6	**port** *port-number* **Example:** `Router(config-locsvr-da-radius)# port 1650`	Specifies the port on which a device listens for RADIUS requests from configured RADIUS clients. • The example specifies port 1650.
Step 7	**server-key** *word* **Example:** `Router(config-locsvr-da-radius)# server-key abc`	Configures the RADIUS key to be shared between a device and RADIUS clients. • The example specifies “abc” as the encryption key shared with the RADIUS client.
Step 8	**exit** **Example:** `Router(config-locsvr-da-radius)# exit`	Returns to global configuration mode.

Configuration Examples for ISG Policies for Session Maintenance

Example: Session Timer Configuration in a Service Policy Map

The following example limits session time in a service policy map to 4800 seconds (80 minutes):

```
class-map type traffic match-any traffic-class
 match access-group input 101
 match access-group output 102
policy-map type service video-service
 class traffic-class
  police input 20000 30000 60000
  police output 21000 31500 63000
  timeout absolute 4800
 class type traffic default
 drop
```

Example: Connection Idle Timer Configuration in a Service Policy Map

The following example limits idle connection time in a service policy map to 30 seconds:

```
class-map type traffic match-any traffic-class
 match access-group input 101
 match access-group output 102
policy-map type service video-service
 class type traffic traffic-class
  police input 20000 30000 60000
  police output 21000 31500 63000
  timeout idle 30
 class type traffic default
 drop
```

Example: Session Timer Show Command Output

The following example shows the settings for the session timer displayed by the **show subscriber session all** privileged EXEC command:

```
Current Subscriber Information: Total sessions 1
------------------------------------------------
Unique Session ID: 3
Identifier: user01
SIP subscriber access type(s): PPPoE/PPP
Current SIP options: Req Fwding/Req Fwded
Session Up-time: 00:02:50, Last Changed: 00:02:53
AAA unique ID: 4
Interface: Virtual-Access2.1
Policy information:
  Context 02DE7380: Handle 1B000009
  Authentication status: authen
  User profile, excluding services:
    Framed-Protocol      1 [PPP]
    username             "user01"
    Framed-Protocol      1 [PPP]
    username             "user01"
  Prepaid context: not present
Non-datapath features:
 Feature: Session Timeout
  Timeout value is 180000 seconds
  Time remaining is 2d01h
Configuration sources associated with this session:
Interface: Virtual-Template1, Active Time = 00:02:52
```

Example: Connection Idle Timer Show Command Output

The following example shows the settings for the idle timer as displayed by the **show subscriber session all** privileged EXEC command:

```
Current Subscriber Information: Total sessions 1
------------------------------------------------
Unique Session ID: 4
Identifier: user01
SIP subscriber access type(s): PPPoE/PPP
Current SIP options: Req Fwding/Req Fwded
Session Up-time: 00:01:44, Last Changed: 00:01:46
AAA unique ID: 5
Interface: Virtual-Access2.1

Policy information:
  Context 02DE7380: Handle AD00000C
  Authentication status: authen
  User profile, excluding services:
    Framed-Protocol      1 [PPP]
    username             "user01"
    Framed-Protocol      1 [PPP]
    username             "user01"
  Prepaid context: not present
Session outbound features:
 Feature: PPP Idle Timeout
  Timeout value is 2000
  Idle time is 00:01:44

Configuration sources associated with this session:
Interface: Virtual-Template1, Active Time = 00:01:47
```

Example: Session Timer Debug Output

The following example shows output when the session timer debug commands (**debug subscriber feature error** , **debug subscriber feature event**, **debug subscriber feature name session-timer error** , and **debug subscriber feature name session-timer event**) are enabled:

```
*Jan 12 18:38:51.947: SSF[Vi2.1/Abs Timeout]: Vaccess interface config
update; not per-user, ignore
*Jan 12 18:38:53.195: SSF[Vt1/uid:3]: Install interface configured
features
*Jan 12 18:38:53.195: SSF[Vt1/uid:3]: Associate segment element handle
0x95000002 for session 1191182344, 1 entries
*Jan 12 18:38:53.195: SSF[Vt1/uid:3/Abs Timeout]: Group feature install
*Jan 12 18:38:53.195: SSF[uid:3/Abs Timeout]: Adding feature to none segment(s)
```

Example: Connection Idle Timer Debug Output

The following example shows output when the idle timer debug commands (**debug subscriber feature error**, **debug subscriber feature event**, **debug subscriber feature name idle-timer error**, and **debug subscriber feature name idle-timer event**) are enabled:

```
*Jan 12 18:43:15.167: SSF[Vt1/uid:4]: Install interface configured
features
*Jan 12 18:43:15.167: SSF[Vt1/uid:4]: Associate segment element handle
0xF4000003 for session 67108875, 1 entries
```

```
*Jan 12 18:43:15.167: SSF[Vt1/uid:4/Idle Timeout]: Group feature install
*Jan 12 18:43:15.167: SSF[uid:4/Idle Timeout]: Adding feature to outbound
segment(s)
*Jan 12 18:43:15.167: Idle Timeout[uid:4]: Idle timer start, duration 2000
seconds, direction: outbound
*Jan 12 18:43:16.327: SSM FH: [SSS:PPPoE:8198:Idle Timeout:4097] created
02DFFDD8
*Jan 12 18:43:16.327: SSM FH: [SSS:PPPoE:8198:Idle Timeout:4097] added
02DFFDD8 [outbound]
*Jan 12 18:43:16.327: SSM FH: [SSS:PPPoE:8198:Idle Timeout:4097]
installed: ok
*Jan 12 18:43:16.327: SSM FH: [SSS:PPPoE:8198:Idle Timeout:4097]
installed: ok
*Jan 12 18:43:19.147: SSM FH: [SSS:PPPoE:8198:Idle Timeout:4097] bound
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
ISG commands	Cisco IOS Intelligent Services Gateway Command Reference
ppp timeout idle and **timeout absolute** PPP timer commands	Cisco IOS Dial Technologies Command Reference
HA commands	Cisco IOS High Availability Command Reference
HA configuration	*Cisco IOS High Availability Configuration Guide*

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 ISG Policies for Session Maintenance

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 ISG Policies for Session Maintenance

Feature Name	Releases	Feature Information
ISG: Session: Lifecycle: Idle Timeout	Cisco IOS XE Release 2.2	The ISG idle timeout controls how long a connection can be idle before it is terminated.
ISG: Session Protection and Resiliency: Keepalive-ARP, ICMP	Cisco IOS XE Release 2.2	IP subscriber session keepalive support is configured for monitoring session data traffic in the upstream direction for idleness. Address Resolution Protocol (ARP) is used for Layer 2 connected subscribers. For routed hosts (Layer 3 connected) subscribers, the protocol defaults to Internet Control Message Protocol (ICMP). ICMP is also used in configurations where the access interface does not support ARP. The following command was introduced: **keepalive** (ISG).
ISG: Session: Lifecycle: Packet of Disconnect (POD)	Cisco IOS XE Release 2.2	An ISG can be configured to interact with external policy servers. A policy server can use RADIUS Packet of Disconnect (POD) to manage the life cycle of any ISG session. The primary role of the POD message is to terminate an ISG session.
Downstream Idle Timeout Support	Cisco IOS XE Release 3.4.1S	The connection timer (idle timeout) can be applied to subscriber traffic in a specific direction, through an ISG service policy map or a AAA service profile. The following command was modified: **timeout idle**.
Session Timeout Ext to 360 Days	Cisco IOS XE Release 3.5S	Maximum value of the session timer was increased to 31,104,000 seconds. Maximum value of the connection timer was increased to 15,552,000 seconds. The following commands were modified: **timeout absolute**, **timeout idle**.
ISG: Flow Control: SSO/ISSU	Cisco IOS XE Release 3.5S	HA support was added for the session maintenance timers and keepalive.