



Settlement for Packet Telephony on Cisco Access Platforms

The Cisco Settlement for Packet Telephony feature equips Cisco conferencing infrastructure products to use third-party Settlement systems on multiple protocols. This feature allows Internet telephony service providers to:

- Act as clearinghouses to validate and reconcile billing information from different sources and occurrences so that the service providers can produce separate billing statements for each call party.
- Provide functions, such as call routing, authentication, reconciliation, and the Settlement solution in multiple currencies. Cisco Systems provides a set of enabling technologies for Cisco IOS products to interface with these third-party Settlement systems.
- Enables Cisco access platforms to provide Open Settlement Protocol (OSP) for service providers.
- Works with the existing Authentication Authorization and Accounting (AAA) feature previously released with service provider features set.

Settlement for Packet Telephony on Cisco Access Platforms complies with the ETSI Technical Specification (TS) 101 321 and was introduced in Cisco IOS Release 12.0(4)XH1.

Note See “Glossary” for a description of terms.

This document includes the following sections:

- Feature Overview on page 2
- Supported Platforms on page 4
- Prerequisites on page 5
- Configuration Tasks on page 6
- Configuration Examples on page 12
- Command Reference on page 17
- Debug Commands on page 47
- Glossary on page 63

Feature Overview

When you make a telephone call, the cost charged can be divided between different carriers involved in the completion of the call. *Settlement* is the method used to divide the cost between carriers. Traditionally, Settlement agreements have been arranged between the carriers in a pairwise fashion. With the advance of voice and video conferencing over IP, pairwise Settlement agreements have become cumbersome. A number of companies have entered the market offering Settlement on a subscription basis. As a result, the Settlement process becomes a more manageable, many-to-one system, with a set of public interfaces that service providers must implement.

The Cisco gateway based Settlement protocol interacts between carriers to create a single authentication at initialization. The authentication is the basis for the establishment of a secure communication channel between the Settlement system and the infrastructure component. This channel then allows the following three types of transactions to be handled.

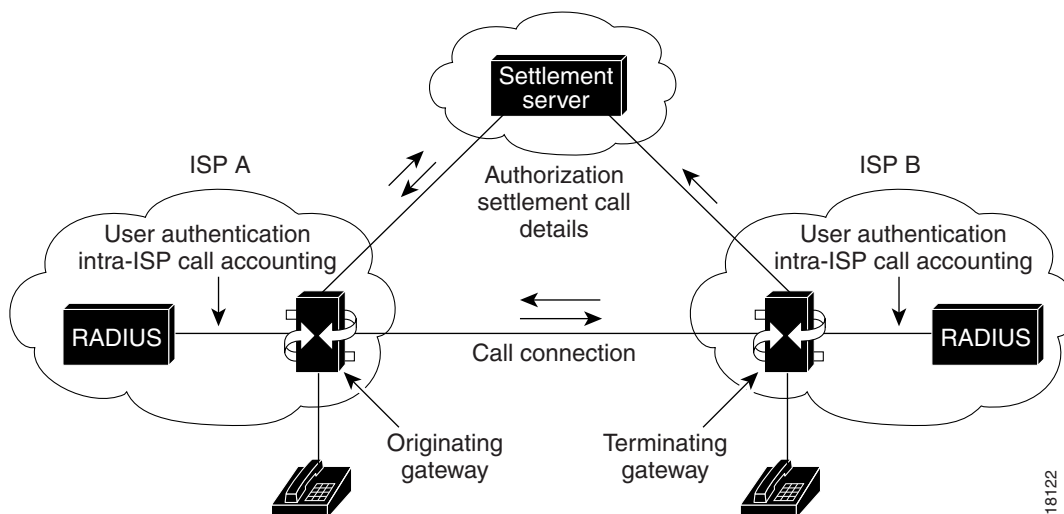
- Call routing—The Settlement system can either accept a gateway endpoint from the requestor or assign one for the requestor.
- Call authorization—Based on the terminating endpoint address, the Settlement system determines whether the requesting gateway is permitted to originate calls for the terminating gateway. If the call is authorized, the Settlement system generates a token that allows the terminating gateway to accept the call.
- Call detail reporting—Each endpoint in a call leg reports when the call stops, along with the usual call details. The Settlement system reconciles the different reports of the calling and called parties and generates billing information. Call details are reported on a call-by-call basis.

Figure 1 shows a typical gateway-based Settlement setup. A voice or fax call is originated and routed through the gateway (Cisco AS5300 access server, or Cisco 2600 or 3600 series routers) to a database server (RADIUS, TACACS+) for user authentication and intra-ISP call accounting. Using TCL IVR interactive voice response scripts to gather and manipulate the caller's data, the gateway forwards the call to the Settlement server, which authorizes the call and adds Settlement details in a token. The call, now carrying its unique Settlement token, passes through the originating gateway to the terminating gateway. The terminating gateway uses TCL IVR to validate the Settlement token and forwards the call to the receiving telephone or fax machine.

Note For a complete description of the Cisco Interactive Voice Response (IVR) software feature, refer to the online documentation located in Cisco Connection Online (CCO).

When the call is completed, both the terminating and originating gateways communicate the call details to the Settlement server. The Settlement server then reconciles the information it receives about the call from both gateways.

Figure 1 Gateway-Based Settlement



Benefits

- Enables Cisco Access platforms to provide Open Settlement Protocol (OSP) to internet service providers.
- Gives Internet service providers the ability to bid for the originating and terminating fee since the Settlement software complies with OSP.
- Offers a single authentication for the actual gateway or platform at initialization time.
- Provides a secure interface between the Settlement client and server.
- Offers a choice of languages, therefore the ISP can specify the currency with which to perform the transaction.

Restrictions

- The Cisco Settlement for Packet Telephony feature on Cisco requires Cisco IOS Release 12.0(7)T and the correct version of VCWare that is compatible with this version of the Cisco IOS software.
- The Settlement feature cannot be enabled on dial-peers that use RAS as the session target.
- The Settlement software is offered only in crypto images and therefore they are under export controls. All users must be “entitled” before they can receive 56 or 56i images. You (and your customers) can entitle yourselves by filling out the forms located at the following URL:

<http://www.cisco.com/kobayashi/library/12.0/>

— If you are not already entitled for crypto images, go to the link (at the above URL) that reads:

“Apply for Cisco IOS Cryptographic Software under export licensing controls”

— If you are entitled, go to the link (at the above URL) that reads:

"Download Cisco IOS cryptographic software under export licensing controls"

Once you are entitled, you will be able to see crypto images in the upgrade planner. Also, once you are entitled, you do not have to entitle yourself again, unless you are coming from a different host. You do not have to entitle yourself for every release because entitlement is good for all releases.

Related Features and Technologies

The Settlement for Packet Telephony feature is dependent upon the interoperability of the following feature:

- Interactive Voice Response

The IVR feature uses audio files that manage the voice prompting and digit collection to gather caller information for authenticating the user and identifying the destination.

Refer to the Cisco Connection Online for Cisco IOS Release 12.0(7)T Software features for the documentation.

- Certification Authority Interoperability

Ensure that this feature is functioning properly and configured as described in the task list. See “Configuration Tasks” on page 6. Additional configuration information is available in the Certification Authority Interoperability feature documentation on Cisco Connection Online (CCO) at:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113t/113t_3/interop.htm

Related Documents

- *Configuring the Cisco AS5300 for Voice Service Provider Features*
- *Voice over IP for the Cisco 2600/3600 Series*
- *Configuring H.323 VoIP Gateway for Cisco Access Platforms*
- *Configuring H.323 VoIP Gatekeeper for Cisco Access Platforms*
- *Configuring Interactive Voice Response for Cisco Access Platforms*
- *Token Card and Cisco Secure Authentication Support*
- *The SSL Protocol Version 3.0 as amended SSL 3.0 Errata of August 26, 1996*
- *Profiles for Interdomain Pricing, Authorization, and Usage Exchange for Basic Internet Telephony Service*
- *Certification Authority Interoperability*
- *Open Settlement Protocol ETSI/TIPHON documents*

Supported Platforms

- Cisco AS5300 access servers
- Cisco 2600 series routers
- Cisco 3600 series routers

Supported MIBs and RFCs

None

Prerequisites

- Ensure that your access platform has the following memory requirement:
16 MB Flash and 64 MB DRAM memory minimum.
- In Cisco IOS Release 12.0(7)T or later release, both the originating and terminating gateways must be using the Integrated Voice Response TCL IVR scripts to perform Settlement successfully. If a terminating gateway that is not configured with a TCL script receives Settlement calls, it will not recognize the tokens added by the Settlement server to those calls; therefore, those calls will pass through without being audited or charged.
- Ensure that the correct version of VCWare is downloaded to the Cisco AS5300 and Cisco Access Path platforms. See the VCWare version compatibility matrix in the VCWare Release Notes on CCO at:
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/index.htm>
- Before configuring the Settlement feature, you must have configured the Public Key Infrastructure (PKI) for secured communication between the access platform (or router) and the Settlement server. For detailed information about Certificates and secure devices see the Cisco IOS Release 12.0 documentation titled "*Certification Authority Interoperability*". The online version of this documentation is located at the following url:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/secur_c/scprt4/scinter.htm

Configuration Tasks

Before starting the Settlement server configuration tasks, ensure that the Cisco Enrollment Protocol (CEP) router has obtained a security certificate. For detailed information, see the Certification Authority Interoperability documentation in the Cisco IOS Release 12.0 documentation set, or go to the online version located at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/secur_c/scprt4/scinter.htm.

To configure the Cisco AS5300 access server, the Cisco 2600, or the Cisco 3600 series router, perform the following tasks:

- Configuring the Public Key Infrastructure on page 6
- Configuring the Originating Gateway on page 7
- Configuring the Inbound POTS Dial Peer on page 8
- Configuring the Outbound VoIP Dial Peer on page 9
- Configuring the Terminating Gateway on page 10
- Configuring the Inbound VoIP Dial Peer on page 10
- Configuring the Outbound POTS Dial Peer on page 11

Configuring the Public Key Infrastructure

Note Ensure that you have secure communication between the access platform or router and the Settlement server.

To configure the Public Key Infrastructure (PKI):

Step	Command	Purpose
1	Router # config terminal	Enter the global configuration mode.
2	Router (config)# no crypto ca id name	Clear the old certificate if it exists.
3	Router (config)# crypto key zeroize rsa	Clear the existing Registration Authority (RSA) key.
4	Router (config)# hostname router-name	Configure the router's hostname if this is not done already.
5	Router (config)# ip domain-name domain-name	Configure the router's IP domain name.
6	Router (config)# crypto ca identity name	Declare a Certification Authority (CA) name. For example, the tag-name could be <i>fieldlabs.cisco.com</i> . This command puts you into the <i>ca-identity</i> mode.
7	Router (ca-identity)# enrollment url url	Use a non-standard cgi-bin script location URL. Note This is for the transnexus Public Key Infrastructure only (http://ip-address/cgi-bin).

Step	Command	Purpose
8	Router (ca-identity)# enrollment retry count <i>number</i> Optional	Specify how many times the router will send unsuccessful certificate requests before giving up.
9	Router (ca-identity)# enrollment retry period <i>minutes</i> Optional	After specifying a certificate, the router waits to receive a certificate from the CA. If the router doesn't receive a certificate within a period of time (the retry period), the router will send another certificate request. You can change the retry period from the default of 1 minute.
10	Router (ca-identity)# exit	Exit ca-identify configuration mode.
11	Router (config)# crypto ca authenticate <i>name</i>	Obtain the CA's public key. Use the same <i>name</i> that you used when declaring the CA with the crypto ca identify command.
12	Router (config)# crypto key generate rsa	Generate the RSA key pair.
13	Router (config)# crypto ca enroll <i>name</i>	Obtain the router certificate for all your RSA key pairs. Note This command requires you to create a challenge password that is not saved with the configuration. This password is required if your certificate is revoked, so remember this password.

Note If your router reboots after you issued the **crypto ca enroll** command but before you received the certificate, you must reissue the command.

Configuring the Originating Gateway

To configure the originating gateway to use the Settlement feature, enter the following commands beginning in the global configuration mode:

Step	Command	Purpose
1	Router configure terminal	Enter the global configuration mode.
2	Router (config)# settlement <i>number</i>	Enter the Settlement mode and configure the Settlement provider number. The settlement command puts you in the <i>settlement</i> command mode.
3	Router (config-settlement)# type osp	Configure the Settlement provider type. In Cisco IOS Release 12.0(7)T, OSP is the only type available.
4	Router (config-settlement)# url <i>url</i>	Enter the Settlement provider URL for the ISP hosting the Settlement server.
5	Router (config-settlement)# no shut	Brings up the Settlement provider.

Note If you are configuring a TransNexus server, first enter the **url** *<url>*; then enter the **customer-id** and the **device-id** command.

Configuring the Inbound POTS Dial Peer

To configure the inbound POTS dial peer, enter the following commands:

Step	Command	Purpose
1	Router# config terminal	Enter the configuration mode.
2	Router (config-dial-peer)# dial-peer voice <i>number</i> pots	Enter the dial-peer configuration mode to configure a POTS dial peer. Note The <i>number</i> value of the dial-peer voice pots command is a tag that uniquely identifies the dial peer.
3	Router (config-dial-peer)# application <i>app name</i>	Enter the application command; then enter the desired TCL script <i>application name</i> .
4	Router (config-dial-peer)# destination-pattern [+] <i>string</i> [t]	Configure the dial peer's destination pattern. Enter the number or pattern of the outbound called number. The <i>string</i> is a series of digits that specify the E.164 or private dialing plan telephone number. Valid entries are the digits 0–9 and the letters A–D. The following special characters can be entered in the string: <ul style="list-style-type: none"> • The plus symbol (+) can be used to indicate an E.164 standard number. • The star character (*) and the pound sign (#) that appear on standard touch-tone dial pads can be used in any dial string. However, these characters cannot be used as leading characters in a string (for example, *650). • The period (.) can be used as a trailing character, and is used as a wildcard character. Multiple periods as trailing characters indicate multiple wildcard digits, such as for the 789... wildcard. • The comma (,) can be used only in prefixes, and is used to insert a one-second pause or a delay. The timer (T) character can be used to configure variable length dial plans.
5	Router (config-dial-peer)# port <i>port number</i>	Associate this voice-telephony dial peer with a specific voice port.

Configuring the Outbound VoIP Dial Peer

To configure the outbound VoIP dial peer, use the following commands:

Step	Command	Purpose
1	Router (config-dial-peer)# dial-peer voice <i>number</i> voip	Enter the dial-peer mode to configure the outbound VoIP dial peer.
2	Router (config-dial-peer)# destination-pattern [+] <i>string</i> [t]	<p>Configure the dial peer's destination pattern. Enter the number or pattern of the outbound called number.</p> <p>The <i>string</i> is a series of digits that specify the E.164 or private dialing plan telephone number. Valid entries are the digits 0–9 and the letters A–D. The following special characters can be entered in the string:</p> <ul style="list-style-type: none"> • The plus symbol (+) can be used to indicate an E.164 standard number. On the Cisco MC3810, the plus symbol (+) is not a valid character in the string. • The star character (*) and the pound sign (#) that appear on standard touch-tone dial pads can be used in any dial string. However, these characters cannot be used as leading characters in a string (for example, *650). • The period (.) can be used as a trailing character, and is used as a wildcard character. Multiple periods as trailing characters indicate multiple wildcard digits, such as for the 789... wildcard. • The comma (,) can be used only in prefixes, and is used to insert a one-second pause or a delay. <p>The timer (T) character can be used to configure variable length dial plans</p>
3	Router (config-dial-peer)# session target settlement	Enter the Settlement as the target to resolve the terminating gateway address.

Note The originating gateway's system clock must synchronize with the Settlement server clock. Use the **clock** or **ntp** command to set the router clock.

Configuring the Terminating Gateway



Caution If the terminating gateway is not configured by using TCL IVR application scripts, the Settlement tokens are bypassed, calls can get through, and Settlement calls will not be audited; therefore, you will not be notified that the calls are not going through the billing service.

To configure the terminating gateway, use the following commands:

Step	Command	Purpose
1	Router# <code>configure terminal</code>	Enter the global configuration mode.
2	Router (config)# <code>settlement number</code>	Enter the Settlement mode and configure the Settlement provider number.
3	Router (config-settlement)# <code>type osp</code>	Configure the Settlement provider type.
4	Router (config-settlement)# <code>url url</code>	Enter the Settlement provider URL for the ISP hosting the Settlement server.
5	Router (config-settlement)# <code>no shut</code>	Brings up the Settlement provider.

Note If you are configuring a transnexus server, enter the `url <url>` command; then enter the `customer-id` and `device-id` command.

Configuring the Inbound VoIP Dial Peer

To configure the inbound Voip dial peer, enter the following commands:

Step	Command	Purpose
1	Router (config-dial-peer)# <code>dial-peer voice number voip</code>	Enter the dial-peer mode to configure a VoIP dial peer.
2	Router (config-dial-peer) # <code>application app name</code>	Enter the application command; then enter the desired TCL application name.
3	Router (config-dial-peer) # <code>incoming called-number string</code>	Specify the telephone number of the voice-port associated with this dial-peer. Characters include wildcards to create the number or pattern.
4	Router (config-dial-peer) # <code>session target settlement</code>	Enter the Settlement as the target to resolve the terminating gateway address.

Configuring the Outbound POTS Dial Peer

To configure the outbound POTS dial peer, enter the following commands:

Step	Command	Purpose
1	Router (config-dial-peer) # dial-peer voice <i>number</i> pots	Enter the dial-peer mode to configure the outbound POTS dial peer.
2	Router (config-dial-peer) # destination-pattern [+] <i>string</i> [t]	<p>Configure the dial peer's destination pattern. Use the called number.</p> <p>The <i>string</i> is a series of digits that specify the E.164 or private dialing plan telephone number. Valid entries are the digits 0–9 and the letters A–D. The following special characters can be entered in the string:</p> <ul style="list-style-type: none"> • The plus symbol (+) can be used to indicate an E.164 standard number. • The star character (*) and the pound sign (#) that appear on standard touch-tone dial pads can be used in any dial string. However, these characters cannot be used as leading characters in a string (for example, *650). • The period (.) can be used as a trailing character, and is used as a wildcard character. Multiple periods as trailing characters indicate multiple wildcard digits, such as for the 789... wildcard. • The comma (,) can be used only in prefixes, and is used to insert a one-second pause or a delay. <p>The timer (T) character can be used to configure variable length dial plans.</p>
3	Router (config-dial-peer) # port <i>port number</i>	Associate the voice-telephony dial peer with a specific voice port. Activate the voice port associated with this dial peer.

Note The terminating gateway system clock must synchronize with the Settlement server clock. Use the **clock** or **ntp** command to set the router clock.

Verifying Settlement Configuration

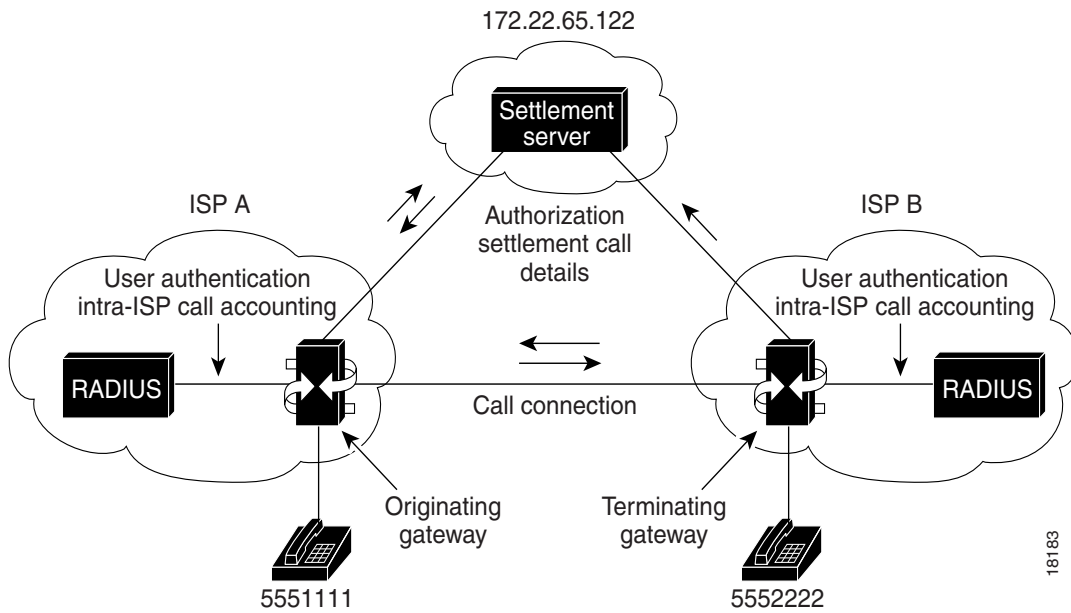
Use the **show running configuration** command to verify your configuration. See Figure 2.

Configuration Examples

Figure 2 shows example Settlement configurations for both the originating and terminating gateways.

Note All IP addresses and patterns are examples only.

Figure 2 Example of Settlement Configurations for Originating and Terminating Gateways



See samples of screen output displays for running configurations:

- Settlement on the Originating Gateway on page 13
- Settlement on the Terminating Gateway on page 15

Settlement on the Originating Gateway

See the following output by using the **show running configuration** command. Figure 2 is a graphic representation of the configuration.

```
!  
version 12.0  
service timestamps debug uptime  
service timestamps log uptime  
no service password-encryption  
service internal  
service udp-small-servers  
service tcp-small-servers  
!  
hostname c3620-px15  
!  
ip subnet-zero  
!  
settlement 0  
  type osp  
  url http://xxx.xxx.  
!  
voice-port 1/0/0  
  alerting audible  
!  
voice-port 1/0/1  
  alerting audible  
!  
dial-peer voice 1 pots  
  application session  
  destination-pattern 5551111  
  port 1/0/0  
!  
dial-peer voice 2 voip  
  destination-pattern 5552222  
  session target settlement:  
!  
interface Ethernet0/0  
  ip address 172.22.65.131 255.255.255.224  
  no ip directed-broadcast  
  ip route-cache same-interface  
  standby 1 priority 110  
!  
interface Serial0/0  
  no ip address  
  no ip directed-broadcast  
  shutdown  
!  
interface Ethernet0/1  
  no ip address  
  no ip directed-broadcast  
  shutdown  
!  
router eigrp 109  
  network 172.22.0.0  
!  
router rip  
  network 172.22.0.0  
!  
ip default-gateway 172.22.65.129  
no ip classless  
ip route 0.0.0.0 0.0.0.0 172.22.65.129  
!  
!  
line con 0
```

Settlement on the Originating Gateway

```
transport input none
line aux 0
line vty 0 4
password
login
!
end
```

Settlement on the Terminating Gateway

See the following output by using the **show running configuration** command. See Figure 2 for a graphic representation of the configuration.

```
!  
version 12.0  
service timestamps debug uptime  
service timestamps log uptime  
no service password-encryption  
service internal  
service udp-small-servers  
service tcp-small-servers  
!  
hostname 3620-px16  
!  
ip subnet-zero  
ip domain-name cisco.com  
ip name-server 198.92.30.32  
!  
settlement 0  
  type osp  
  url http://xxx.xxx.  
!  
voice-port 1/0/0  
  alerting audible  
!  
voice-port 1/0/1  
  alerting audible  
!  
dial-peer voice 1 pots  
  destination-pattern 5552222  
  port 1/0/0  
!  
dial-peer voice 2 voip  
  application session  
  incoming called-number 5552222  
  session target settlement:0  
!  
interface Ethernet0/0  
  ip address 172.22.65.143 255.255.255.224  
  no ip directed-broadcast  
  ip route-cache same-interface  
!  
interface Serial0/0  
  no ip address  
  no ip directed-broadcast  
  shutdown  
!  
interface Ethernet0/1  
  no ip address  
  no ip directed-broadcast  
  shutdown  
!  
router eigrp 109  
  network 172.22.0.0  
!  
router rip  
  network 172.22.0.0  
!  
ip default-gateway 172.22.65.129  
no ip classless  
ip route 0.0.0.0 0.0.0.0 172.22.65.129  
!  
snmp-server community public RO
```

```
!  
line con 0  
  exec-timeout 0 0  
  transport input none  
line aux 0  
line vty 0 4  
  password  
  login  
!  
end
```

Command Reference

This section documents only the new following commands. All other commands for this feature are documented in the Cisco IOS Release 12.0 command references.

- **connection-timeout**
- **customer-id**
- **device-id**
- **encryption**
- **max-connection**
- **response-timeout**
- **retry-delay**
- **retry-limit**
- **session-timeout**
- **settlement**
- **show settlement**
- **shutdown/no shutdown**
- **type**
- **url**

connection-timeout

To configure the time that a connection is maintained after completing a communication exchange, use the **connection-timeout** command in the Settlement configuration mode. The router maintains the connection for this period in anticipation of future communication exchanges to the same server. Use the **no** form of this command to reset to the default value of this command.

connection-timeout *num*

no connection-timeout *num*

Syntax Description

num Time (in seconds) that a connection is maintained after the communication exchange is completed. Values can range from zero (0) to 86400 seconds, zero (0) means forever.

Default

The default connection timeout is 3600 seconds (1 hour).

Command Mode

Settlement configuration

Command History

Release	Modification
12.0(4)XH1	This command was introduced.

Example

```
settlement 0
  connection timeout 3600
```

Related Commands

Command	Description
customer-id	Sets the customer identification.
device-id	Sets the device identification.
encryption	Specifies the encryption method.
max-connection	Sets the maximum simultaneous connections.
response-timeout	Sets the response timeout.
retry-delay	Sets the retry delay.
retry-limit	Sets the connection retry limit.
session-timeout	Sets the session timeout.
settlement	Enters the Settlement configuration mode.
show settlement	Displays the configuration for all Settlement server transactions.
noshutdown	Brings up the Settlement provider.
type	Specifies the provider type.
url	Specifies the Internet service provider address.

customer-id

To identify a carrier or ISP with a Settlement provider, use the **customer-id** command in the Settlement configuration mode. This is an optional attribute. Use the **no** form of this command to reset to the default value of this command.

customer-id *num*

no customer-id

Syntax Description

num Customer ID number as provided by the Settlement server

Default

The default customer ID is 0.

Command Mode

Settlement configuration

Command History

Release	Modification
12.0(4)XH1	This command was introduced.

Example

```
settlement 0
  customer id 1000
```

Related Commands

Command	Description
connection-timeout	Sets the connection timeout.
device-id	Sets the device identification.
encryption	Specifies the encryption method.
max-connection	Sets the maximum simultaneous connections.
response-timeout	Sets the response timeout.
retry-delay	Sets the retry delay.
retry-limit	Sets the connection retry limit.
session-timeout	Sets the session timeout.
settlement	Enters the Settlement configuration mode.
show settlement	Displays the configuration for all Settlement server transactions.
noshutdown	Brings up the Settlement provider.
type	Specifies the provider type.
url	Specifies the Internet service provider address.

device-id

To specify a gateway associated with a Settlement provider, use the **device-id** command in the Settlement configuration mode. This is an optional attribute. Use the **no** form of this command to reset to the default value of this command.

device-id *num*

no device-id

Syntax Description

num Device ID number as provided by the Settlement server

Default

The default device ID is 0.

Command Mode

Settlement configuration

Command History

Release	Modification
12.0(4)XH1	This command was introduced.

Example

```
settlement 0
  device-id 1000
```

Related Commands

Command	Description
connection-timeout	Sets the connection timeout.
customer-id	Sets the customer identification.
encryption	Specifies the encryption method.
max-connection	Sets the maximum simultaneous connections.
response-timeout	Sets the response timeout.
retry-delay	Sets the retry delay.
retry-limit	Sets the connection retry limit.
session-timeout	Sets the session timeout.
settlement	Enters the Settlement configuration mode.
show settlement	Displays the configuration for all Settlement server transactions.
noshutdown	Brings up the Settlement provider.
type	Specifies the provider type.
url	Specifies the Internet service provider address.

encryption

To set the encryption method to be negotiated with the provider, use the **encryption** command in the Settlement configuration mode. For Cisco IOS Release 12.0(7)T, only one encryption method is allowed for each provider. Use the **no** form of this command to reset to the default value of this command.

```

encryption {des-cbc-sha | des40-cbc-sha | dh-des-cbc-sha | dh-des40-cbc-sha | null-md5 |
              null-sha}
no encryption
    
```

Syntax Description

des-cbc-sha	Encryption type SSL_RSA_with_DES_CBC_SHA cipher suite
des40-cbc-sha	Encryption type SSL_RSA_EXPORT_with_DES40_CBC_SHA cipher suite
dh-des-cbc-sha	Encryption type SSL_DH_RSA_with_DES_CBC_SHA cipher suite
dh-des40-cbc-sha	Encryption type SSL_DH_RSA_EXPORT_with_DES40_CBC_SHA cipher suite
null-md5	Encryption type SSL_RSA_with_NULL_MD5 cipher suite
null-sha	Encryption type SSL_RSA_with_NULL_SHA cipher suite

Default

The default encryption method is **all**.

If none of the encryption methods are configured, then the system configures to use all of the encryption methods in the SSL session negotiation.

Command Mode

Settlement configuration

Command History

Release	Modification
12.0(4)XH1	This command was introduced.

Example

```

settlement 0
  encryption des-cbc-sha
    
```

Related Commands

Command	Description
connection-timeout	Sets the connection timeout.
customer-id	Sets the customer identification.
device-id	Sets the device idendification.
max-connection	Sets the maximum simultaneous connections.
response-timeout	Sets the response timeout.
retry-delay	Sets the retry delay.
retry-limit	Sets the connection retry limit.
session-timeout	Sets the session timeout.
settlement	Enters the Settlement configuration mode.
show settlement	Displays the configuration for all Settlement server transactions.
noshutdown	Brings up the Settlement provider.
type	Specifies the provider type.
url	Specifies the Internet service provider address.

max-connection

To set the maximum number of simultaneous connections to be used for communication with a Settlement provider, use the **max-connection** command in the Settlement configuration mode. Use the **no** form of this command to reset to the default value of this command.

max-connection *num*

no max-connection *num*

Syntax Description

num Maximum number of HTTP connections to a Settlement provider

Default

The default is 20 maximum connections.

Command Mode

Settlement configuration

Command History

Release	Modification
12.0(4)XH1	This command was introduced.

Example

```
settlement 0
  max-connections 10
```

Related Commands

Command	Description
connection-timeout	Sets the connection timeout.
customer-id	Sets the customer identification.
device-id	Sets the device idendification.
encryption	Specifies the encryption method.
response-timeout	Sets the response timeout.
retry-delay	Sets the retry delay.
retry-limit	Sets the connection retry limit.
session-timeout	Sets the session timeout.
settlement	Enters the Settlement configuration mode.
show settlement	Displays the configuration for all Settlement server transactions.
noshutdown	Brings up the Settlement provider.
type	Specifies the provider type.
url	Specifies the Internet service provider address.

response-timeout

To configure the maximum time to wait for a response from a server, use the **response-timeout** command in the Settlement configuration mode. If no response is received within this time limit, the current connection ends and the router attempts to contact the next service point. Use the **no** form of this command to reset to the default value of this command.

response-timeout *num*

no response-timeout

Syntax Description

num Response waiting time (seconds)

Default

The default response timeout is 1 second (one second).

Command Mode

Settlement configuration

Command History

Release	Modification
12.0(4)XH1	This command was introduced.

Example

```
settlement 0
  response-timeout 1
```

Related Commands

Command	Description
connection-timeout	Sets the connection timeout.
customer-id	Sets the customer identification.
device-id	Sets the device identification.
encryption	Specifies the encryption method.
max-connection	Sets the maximum simultaneous connections.
retry-delay	Sets the retry delay.
retry-limit	Sets the connection retry limit.
session-timeout	Sets the session timeout.
settlement	Enters the Settlement configuration mode.
show settlement	Displays the configuration for all Settlement server transactions.
noshutdown	Brings up the Settlement provider.
type	Specifies the provider type.
url	Specifies the Internet service provider address.

retry-delay

To set the time between attempts to connect with the Settlement provider, use the **retry-delay** command in the Settlement configuration mode. After exhausting all service points for the provider, the router is delayed for this length of time before resuming connection attempts. Use the **no** form of this command to reset to the default value of this command.

retry-delay *num*

no retry-delay

Syntax Description

num Length of time (in seconds) between attempts to connect with the Settlement provider. The valid range for retry-delay is 1-600 seconds.

Default

The default retry delay is 2 seconds.

Command Mode

Settlement configuration

Command History

Release	Modification
12.0(4)XH1	This command was introduced.

Example

```
settlement 0
  relay-delay 15
```

Related Commands

Command	Description
connection-timeout	Sets the connection timeout.
customer-id	Sets the customer identification.
device-id	Sets the device identification.
encryption	Specifies the encryption method.
max-connection	Sets the maximum simultaneous connections.
response-timeout	Sets the response timeout.
retry-limit	Sets the connection retry limit.
session-timeout	Sets the session timeout.
settlement	Enters the Settlement configuration mode.
show settlement	Displays the configuration for all Settlement server transactions.
noshutdown	Brings up the Settlement provider.
type	Specifies the provider type.
url	Specifies the Internet service provider address.

retry-limit

To set the maximum number of connection attempts to the provider, use the **retry-limit** command in the Settlement configuration mode. If no connection is established after the configured retries, the router ceases connection attempts. The retry limit number does not count the initial connection attempt. A retry limit of one (default) results in a total of two connection attempts to every service point. Use the **no** form of this command to reset to the default value of this command.

retry-limit *num*

Syntax Description

num Maximum number of connection attempts in addition to the first attempt

Default

The default retry limit is one (1) retry.

Command Mode

Settlement configuration

Command History

Release	Modification
12.0(4)XH1	This command was introduced.

Example

```
settlement 0
  relay-limit 1
```

Related Commands

Command	Description
connection-timeout	Sets the connection timeout.
customer-id	Sets the customer identification.
device-id	Sets the device identification.
encryption	Specifies the encryption method.
max-connection	Sets the maximum simultaneous connections.
response-timeout	Sets the response timeout.
retry-delay	Sets the retry delay.
session-timeout	Sets the session timeout.
settlement	Enters the Settlement configuration mode.
show settlement	Displays the configuration for all Settlement server transactions.
noshutdown	Brings up the Settlement provider.
type	Specifies the provider type.
url	Specifies the Internet service provider address.

session-timeout

To configure the lifetime of a single SSL session key, use the **session-timeout** command in the Settlement configuration mode. When this time limit is exceeded, the router negotiates a new session key. Communication exchanges in progress are not interrupted when this time limit expires. Use the **no** form of this command to reset to the default value of this command.

session-timeout *num*

no session-timeout *num*

Syntax Description

num Lifetime (in seconds) of a single SSL session key

Default

The default session timeout is 86,400 seconds (one day).

Command Mode

Settlement configuration

Command History

Release	Modification
12.0(4)XH1	This command was introduced.

Example

```
settlement 0
  session timeout 86400
```

Related Commands

Command	Description
connection-timeout	Sets the connection timeout.
customer-id	Sets the customer identification.
device-id	Sets the device identification.
encryption	Specifies the encryption method.
max-connection	Sets the maximum simultaneous connections.
response-timeout	Sets the response timeout.
retry-delay	Sets the retry delay.
retry-limit	Sets the connection retry limit.
settlement	Enters the Settlement configuration mode.
show settlement	Displays the configuration for all Settlement server transactions.
noshutdown	Brings up the Settlement provider.
type	Specifies the provider type.
url	Specifies the Internet service provider address.

settlement

To enter the Settlement mode and specify the attributes specific to a Settlement provider, use the **settlement** Global configuration command. The variable *provider-number* defines a particular Settlement provider. For Cisco IOS Release 12.0(7)T, only one clearinghouse per system is allowed, and the only valid value for *provider-number* is 0. Use the no form of this command to disable the settlement provider.

- settlement** *provider-number*
- no settlement** *provider-number*

Syntax Description

provider-number Digit defining a particular Settlement server. The only valid entry is 0.

Default

The default is 0.

Command Mode

Global configuration

Command History

Release	Modification
12.0(4)XH1	This command was introduced.

Example

```
settlement 0
```

Related Commands

Command	Description
connection-timeout	Sets the connection timeout.
customer-id	Sets the customer identification.
device-id	Sets the device identification.
encryption	Specifies the encryption method.
max-connection	Sets the maximum simultaneous connections.
response-timeout	Sets the response timeout.
retry-delay	Sets the retry delay.
retry-limit	Sets the connection retry limit.
session-timeout	Sets the session timeout.
show settlement	Displays the configuration for all Settlement server transactions.
no shutdown	Brings up the Settlement provider.
type	Specifies the provider type.
url	Specifies the Internet service provider address.

show settlement

To display the configuration for all Settlement servers and see the specific provider and transactions, use the **show settlement** privileged EXEC command.

show settlement [<provider-number> [transactions]]

no show settlement

Syntax Description

show settlement 0 transactions

<i>provider number</i>	Displays the attributes of a specific provider.
<i>transaction</i>	Displays the transaction status of a specific provider.

Default

None

Command Mode

Privileged EXEC

Command History

Release	Modification
12.0(4)XH1	This command was introduced.

Usage Guidelines

See Table 1 “Show Settlement Output” for a description of the fields that appear with the **show settlement** command.

The provider attributes not configured are not shown.

Table 1 Show Settlement Output

Field	Description
type	Settlement provider type
address url	URL address of the provider
encryption	SSL encryption method
max-connections	Maximum number of concurrent connections to provider
connection-timeout	Connection timeout with provider (in seconds)
response-timeout	Response timeout with provider (in seconds)
retry-delay	Delay time between retries (in seconds)
retry-limit	Number of retries
session-timeout	SSL session timeout (in seconds)
customer-id	Customer ID, assigned by provider
device-id	Device ID, assigned by provider
roaming	Roaming enabled
signed-token	Indicates if the Settlement token is signed by the server.

Example Output

```
router# show settlement
Settlement Provider 0
Type = osp
Address url = https://1.14.115.100:6556/
Encryption = all (default)
Max Concurrent Connections = 20 (default)
Connection Timeout = 3600 (s) (default)
Response Timeout = 1 (s) (default)
Retry Delay = 2 (s) (default)
Retry Limit = 1 (default)
Session Timeout = 86400 (s) (default)
Customer Id = 1000
Device Id = 1000
Roaming = Disabled (default)
Signed Token = on

Number of Connections = 0
Number of Transactions = 7
```

Example Output with Key Words

```
router# show settlement 0 transactions

Transaction ID=8796304133625270342
state=OSPC_GET_DEST_SUCCESS, index=0
callingNumber=5710868, calledNumber=15125551212
```

Related Commands

Command	Description
connection-timeout	Sets the connection timeout.
customer-id	Sets the customer identification.
device-id	Sets the device idendification.
encryption	Specifies the encryption method.
max-connection	Sets the maximum simultaneous connections.
response-timeout	Sets the response timeout.
retry-delay	Sets the retry delay.
retry-limit	Sets the connection retry limit.
session-timeout	Sets the session timeout.
settlement	Enters the Settlement configuration mode.
no shutdown	Brings up the Settlement provider.
type	Specifies the provider type.
url	Specifies the Internet service provider address.

shutdown/no shutdown

To activate a Settlement provider, use the **no shutdown** command in the Settlement configuration mode. Enter the **shutdown** command to deactivate the Settlement provider. Otherwise, transactions will not go through the provider to be audited and charged.

shutdown

no shutdown

Syntax Description

This command has no arguments or keywords.

Default

The default status of a Settlement provider is deactivated. The Settlement provider is down.

Command Mode

Settlement configuration

Command History

Release	Modification
12.0(4)XH1	This command was introduced.

Usage Guidelines

Enter the **no shutdown** command at the end of the configuration of a Settlement server to bring up the provider. This command activates the provider. Enter **shutdown** to deactivate the provider.

Example

```
settlement 0
shutdown
```

Related Commands

Command	Description
connection-timeout	Sets the connection timeout.
customer-id	Sets the customer identification.
device-id	Sets the device identification.
encryption	Specifies the encryption method.
max-connection	Sets the maximum simultaneous connections.
response-timeout	Sets the response timeout.
retry-delay	Sets the retry delay.
retry-limit	Sets the connection retry limit.
session-timeout	Sets the session timeout.
settlement	Enters the Settlement configuration mode.
show settlement	Displays the configuration for all Settlement server transactions.
type	Specifies the provider type.
url	Specifies the Internet service provider address.

type

To point to the specific Settlement server, use the **type** command in the Settlement configuration mode. This command line defines both the Settlement server that is doing the accounting and enables the server to do the accounting. In Cisco IOS Release 12.0(7)T, **osp** is the only Settlement server type supported.

type osp

Syntax Description

This command has no arguments or keywords.

Default

The default is **osp**.

Command Mode

Settlement configuration

Command History

Release	Modification
12.0(4)XH1	This command was introduced.

Example

```
settlement 0
  type osp
```

type

Related Commands

Command	Description
connection-timeout	Sets the connection timeout.
customer-id	Sets the customer identification.
device-id	Sets the device identification.
encryption	Specifies the encryption method.
max-connection	Sets the maximum simultaneous connections.
response-timeout	Sets the response timeout.
retry-delay	Sets the retry delay.
retry-limit	Sets the connection retry limit.
session-timeout	Sets the session timeout.
settlement	Enters the Settlement configuration mode.
show settlement	Displays the configuration for all Settlement server transactions.
no shutdown	Brings up the Settlement provider.
url	Specifies the Internet service provider address.

url

Enter the **url** command in the Settlement configuration mode to configure the Internet service provider (ISP) address. You can configure the address type multiple times. If you configure multiple URLs for the Settlement server, the gateway attempts to send the request to each URL in the order that you configured these addresses.

url *url-address*

Syntax Description

url-address

Valid URL address is in the format:
`http://fully qualified domain name[:port]/[URL]`

Default

None

Command Mode

Settlement configuration

Command History

Release	Modification
12.0(4)XH1	This command was introduced.

Example

```
settlement 0
url http://1.2.3.4/
url http://1.2.3.4:80/
url https://1.2.3.4:4444/
url https://yourcompany.com:443/
```

Related Commands

Command	Description
connection-timeout	Sets the connection timeout.
customer-id	Sets the customer identification.
device-id	Sets the device identification.
encryption	Specifies the encryption method.
max-connection	Sets the maximum simultaneous connections.
response-timeout	Sets the response timeout.
retry-delay	Sets the retry delay.
retry-limit	Sets the connection retry limit.
session-timeout	Sets the session timeout.
settlement	Enters the Settlement configuration mode.
show settlement	Displays the configuration for all Settlement server transactions.
no shutdown	Brings up the Settlement provider.
type	Specifies the provider type.

Debug Commands

This section documents new and modified **debug** commands associated with the Settlement feature. All other commands used with this feature are documented in the Cisco Release 12.0 command references. All **debug** commands are EXEC commands.

debug voip ivr settlement

The **debug voip ivr** command is used to debug the IVR application. IVR debug messages appear when a call is being actively handled by the IVR scripts. Error outputs only occurs if something is not working or an error condition has been raised. The output when the key word *states* is used, supplies information about the current status of the IVR script and the different events, that occur in that state. This document, for Cisco IOS Release 12.0(7)T shows the **debug voip ivr settlement** command using the output for the keyword **settlement** only.

Note To see the complete description of the **debug voip ivr** command refer to *Configuring Interactive Voice Response for Cisco Access Platforms*.

debug voip ivr [states | error | settlement | dynamic| all]

no debug voip ivr [states | error | settlement | dynamic| all]

Syntax Description

all	Displays both states and error messages.
dynamic	IVR dynamic prompt play debug.
error	Displays information only if an error occurs.
settlement	IVR settlement activities.
states	Displays verbose information about how IVR is handling each call.

Default

no debug voip ivr [states | error | settlement | dynamic | all]

Command History

Release	Modification
11.3(6)NA2	This command was introduced.
12.0(4)XH1	Settlement output logs were added.

Usage Guidelines

IVR debug messages appear when a call is handled by the IVR scripts. Error output should only occur if something is not working or an error condition has been raised. *States* output supplies information about the current status of the IVR script and the different events that occur in that state.

Settlement output logs activities related to settlement when a call is processed.

Example On the Originating Gateway

```
Router # debug voip ivr settlement
ivr settlement activities debugging is on
as5300-04#
00:00:52:settlement_validate_token:cid(1), target=, tokenp=0x0
00:00:54:pcSettlementAuthorize:cid(1) authorizing using calling=408,
called=15125551212
00:00:54:pcSettlementAuthorize:cid(1) sending authorize request type=1
00:00:57:pcSettlementSetup:cid(1) settlement_curr_dest=0, num_dest=3
00:00:57:pcSettlementGetDestination:trans=0 gets error=0,
credit_time=14400
00:00:57:pcSettlementSetup:cid(1) placing call through
ip(1.14.115.85), calling(408),called(15125551212), digits(15125551212)
00:00:57:pcSettlementSetup:set settlement acct for cid(2) on
ip=1.14.115.85
as5300-04#
```

Example On the Terminating Gateway

```
Router # debug voip ivr settlement
ivr settlement activities debugging is on
as5300-05#
00:10:02:settlement_validate_token:cid(1), target=settlement,
tokenp=0x618386B
4
00:10:02:settlement_validate_token:cid(1) return 1, credit_time=14400
00:10:02:Set settlement acct on cid(1) for trans=0, prov=0
as5300-05#
```

debug voip settlement all

To enable debugging in all Settlement areas, enter the **debug voip settlement all** EXEC command. Use the **no** form of this command to disable debugging output.

[no] debug voip settlement all

Command History

Release	Modification
12.0(4)XH1	This command was introduced.

Usage Guidelines

The **debug voip settlement all** EXEC command enables the following debug Settlement commands:

- **debug voip settlement enter**
- **debug voip settlement error**
- **debug voip settlement exit**
- **debug voip settlement misc**
- **debug voip settlement network**
- **debug voip settlement security**
- **debug voip settlement transaction**

debug voip settlement enter

To show all the Settlement function entrances, use the **debug voip settlement enter** command.

[no] debug voip settlement enter

Command History

Release	Modification
12.0(4)XH1	This command was introduced.

Usage Guidelines

The **debug voip settlement enter** command shows the Settlement function entrances.

Example

```
00:43:40:OSP:ENTER:OSPPMimeMessageCreate()
00:43:40:OSP:ENTER:OSPPMimeMessageInit()
00:43:40:OSP:ENTER:OSPPMimeMessageSetContentAndLength()
00:43:40:OSP:ENTER:OSPPMimeMessageBuild()
00:43:40:OSP:ENTER:OSPPMimeDataFree()
00:43:40:OSP:ENTER:OSPPMimePartFree()
00:43:40:OSP:ENTER:OSPPMimePartFree()
00:43:40:OSP:ENTER:OSPPMsgInfoAssignRequestMsg()
00:43:40:OSP:ENTER:ospHttpSelectConnection
00:43:40:OSP:ENTER:OSPPSockCheckServicePoint() ospvConnected = <1>
00:43:40:OSP:ENTER:OSPPSockWaitTillReady()
00:43:40:OSP:ENTER:ospHttpBuildMsg()
00:43:40:OSP:ENTER:OSPPSSLSessionWrite()
00:43:40:OSP:ENTER:OSPPSockWrite()
00:43:40:OSP:ENTER:OSPPSockWaitTillReady()
```

debug voip settlement error

To show all the Settlement errors, use the **debug voip settlement error** command.

[no] debug voip settlement error

Command History

Release	Modification
12.0(4)XH1	This command was introduced.

Example

```
00:45:50:OSP:OSPSPsockProcessRequest:http rcv init header failed
00:45:50:OSP:ospHttpSetupAndMonitor:attempt#0 on http=0x6141A514, limit=1 error=14310
```

Error Code Definitions

```
-1:OSP internal software error.
16:A bad service was chosen.
17:An invalid parameter was passed to OSP.
9010:Attempted to access an invalid pointer.
9020:A time related error occurred.

10010:OSP provider module failed initialization.
10020:OSP provider tried to access a NULL pointer.
10030:OSP provider could not find transaction collection.
10040:OSP provider failed to obtain provider space.
10050:OSP provider tried to access an invalid handle.
10060:OSP provider has reached the maximum number of providers.

11010:OSP transaction tried to delete a transaction which was not allowed.
11020:OSP transaction tried a transaction which does not exist.
11030:OSP transaction tried to start a transaction, but data had already been
delivered.

11040:OSP transaction could not identify the response given.
11050:OSP transaction failed to obtain transaction space.
11060:OSP transaction failed (possibly ran out) to allocate memory.
11070:OSP transaction tried to perform a transaction which is not allowed.
11080:OSP transaction found no more responses.
11090:OSP transaction could not find a specified value.
11100:OSP transaction did not have enough space to copy.
11110:OSP transaction - call id did not match destination.
11120:OSP transaction encountered an invalid entry.
11130:OSP transaction tried to use a token too soon.
11140:OSP transaction tried to use a token too late.
11150:OSP transaction - source is invalid.
11160:OSP transaction - destination is invalid.
11170:OSP transaction - calling number is invalid.
11180:OSP transaction - called number is invalid.
```

Error Codes Continued -

11190:OSP transaction - call id is invalid.
11200:OSP transaction - authentication id is invalid.
11210:OSP transaction - call id was not found
11220:OSP transaction - The IDS of the called number was invalid.
11230:OSP transaction - function not implemented.
11240:OSP transaction tried to access an invalid handle.
11250:OSP transaction returned an invalid return code.
11260:OSP transaction reported an invalid status code.
11270:OSP transaction encountered an invalid token.
11280:OSP transaction reported a status which could not be identified.
11290:OSP transaction in now valid after it was not found.
11300:OSP transaction could not find the specified destination.
11310:OSP transaction is valid until not found.
11320:OSP transaction - invalid signaling address.
11330:OSP transaction could not find the ID of the transmitter.
11340:OSP transaction could not find the source number.
11350:OSP transaction could not find the destination number.
11360:OSP transaction could not find the token.
11370:OSP transaction could not find the list.
11380:OSP transaction was not allowed to accumulate.
11390:OSP transaction - transaction usage was already reported.
11400:OSP transaction could not find statistics.
11410:OSP transaction failed to create new statistics.
11420:OSP transaction made an invalid calculation.
11430:OSP transaction was not allowed to get the destination.
11440:OSP transaction could not fine the authorization request.
11450:OSP transaction - invalid transmitter ID.
11460:OSP transaction could not find any data.
11470:OSP transaction found no new authorization requests.

12010:OSP security did not have enough space to copy.
12020:OSP security received and invalid argument.
12030:OSP security could not find the private key.
12040:OSP security encountered an un-implemented function.
12050:OSP security ran out of memory.
12060:OSP security received an invalid signal.
12065:OSP security could not initialize the SSL database.
12070:OSP security could not find space for the certificate.
12080:OSP security has no local certificate info defined.
12090:OSP security encountered a zero length certificate.
12100:OSP security encountered a certificate that is too big.
12110:OSP security encountered an invalid certificate.
12120:OSP security encountered a NULL certificate.
12130:OSP security has too many certificates.
12140:OSP security has no storage provided.
12150:OSP security has no private key.
12160:OSP security encountered an invalid context.
12170:OSP security was unable to allocate space.
12180:OSP security - CA certificates do not match.
12190:OSP security found no authority certificates
12200:OSP security - CA certificate index overflow.

13010:OSP error message - failed to allocate memory.

13110:OSP MIME error - buffer is too small.
13115:OSP MIME error - failed to allocate memory.
13120:OSP MIME error - could not find variable.
13125:OSP MIME error - no input was found.
13130:OSP MIME error - invalid argument.
13135:OSP MIME error - no more space.
13140:OSP MIME error - received an invalid type.
13145:OSP MIME error - received an invalid subtype.

Error Codes Continued -

13150:OSP MIME error - could not find the specified protocol.
13155:OSP MIME error - could not find MICALG.
13160:OSP MIME error - boundary was not found.
13165:OSP MIME error - content type was not found.
13170:OSP MIME error - message parts were not found.

13301:OSP XML error - received incomplete XML data.
13302:OSP XML error - bad encoding of XML data.
13303:OSP XML error - bad entity in XML data.
13304:OSP XML error - bad name in XML data.
13305:OSP XML error - bad tag in XML data.
13306:OSP XML error - bad attribute in XML data.
13307:OSP XML error - bad CID encoding in XML data.
13308:OSP XML error - bad element found in XML data.
13309:OSP XML error - no element found in XML data.
13310:OSP XML error - no attribute found in XML data.
13311:OSP XML error - OSP received invalid arguments.
13312:OSP XML error - failed to create a new buffer.
13313:OSP XML error - failed to get the size of a buffer.
13314:OSP XML error - failed to send the buffer.
13315:OSP XML error - failed to read a block from the buffer.
13316:OSP XML error - failed to allocate memory.
13317:OSP XML error - could not find the parent.
13318:OSP XML error - could not find the child.
13319:OSP XML error - data type not found in XML data.
13320:OSP XML error - failed to write a clock to the buffer.

13410:OSP data error - no call id preset.
13415:OSP data error - no token present.
13420:OSP data error - bad number presented.
13425:OSP data error - no destination found.
13430:OSP data error - no usage indicator present.
13435:OSP data error - no status present.
13440:OSP data error - no usage configured.
13445:OSP data error - no authentication indicator.
13450:OSP data error - no authentication request.
13455:OSP data error - no authentication response.
13460:OSP data error - no authentication configuration.
13465:OSP data error - no re-authentication request.
13470:OSP data error - no re-authentication response.
13475:OSP data error - invalid data type present.
13480:OSP data error - no usage information available.
13485:OSP data error - no token info present.
13490:OSP data error - invalid data present.
13500:OSP data error - no alternative info present.
13510:OSP data error - no statistics available.
13520:OSP data error - no delay present.

13610:OSP certificate error - memory allocation failed.

14010:OSP communications error - invalid communication size.
14020:OSP communications error - bad communication value.
14030:OSP communications error - parser error.
14040:OSP communications error - no more memory available.
14050:OSP communications error - communication channel currently in use.
14060:OSP communications error - invalid argument passed.
14070:OSP communications error - no service points present.
14080:OSP communications error - no service points available.
14085:OSP communications error - thread initialization failed.
14086:OSP communications error - communications is shutdown.

Error Codes Continued -

14110:OSP message queue error - no more memory available.
14120:OSP message queue error - failed to add a request.
14130:OSP message queue error - no event queue present.
14140:OSP message queue error - invalid arguments passed.

14210:OSP HTTP error - 100 - bad header.
14220:OSP HTTP error - 200 - bad header.
14221:OSP HTTP error - 400 - bad request.
14222:OSP HTTP error - bas service port present.
14223:OSP HTTP error - failed to add a request.
14230:OSP HTTP error - invalid queue present.
14240:OSP HTTP error - bad message received.
14250:OSP HTTP error - invalid argument passed.
14260:OSP HTTP error - memory allocation failed.
14270:OSP HTTP error - failed to create a new connection.
14280:OSP HTTP error - server error.
14290:OSP HTTP error - HTTP server is shutdown.
14292:OSP HTTP error - failed to create a new SSL connection.
14295:OSP HTTP error - failed to create a new SSL context.
14297:OSP HTTP error - service unavailable.

14300:OSP socket error - socket select failed.
14310:OSP socket error - socket receive failed.
14315:OSP socket error - socket send failed.
14320:OSP socket error - failed to allocate memory for the receive buffer.
14320:OSP socket error - socket reset.
14330:OSP socket error - failed to create the socket.
14340:OSP socket error - failed to close the socket.
14350:OSP socket error - failed to connect the socket.
14360:OSP socket error - failed to block I/O on the socket.
14370:OSP socket error - failed to disable nagle on the socket.

14400:OSP SSL error - failed to allocate memory.
14410:OSP SSL error - failed to initialize the context.
14420:OSP SSL error - failed to retrieve the version.
14430:OSP SSL error - failed to initialize the session.
14440:OSP SSL error - failed to attach the socket.
14450:OSP SSL error - handshake failed.
14460:OSP SSL error - failed to close SSL.
14470:OSP SSL error - failed to read from SSL.
14480:OSP SSL error - failed to write to SSL.
14490:OSP SSL error - could not get certificate.
14495:OSP SSL error - no root certificate found.
14496:OSP SSL error - failed to set the private key.
14497:OSP SSL error - failed to parse the private key.
14498:OSP SSL error - failed to add certificates.
14499:OSP SSL error - failed to add DN.

15410:OSP utility error - not enough space for copy.
15420:OSP utility error - no time stamp has been created.
15430:OSP utility error - value not found.
15440:OSP utility error - failed to allocate memory.
15450:OSP utility error - invalid argument passed.

15500:OSP buffer error - buffer is empty.
15510:OSP buffer error - buffer is incomplete.

15980:OSP POW error.

15990:OSP Operating system conditional variable timeout.

Error Codes Continued -

16010:OSP X509 error - serial number undefined.
16020:OSP X509 error - certificate undefined.
16030:OSP X509 error - invalid context.
16040:OSP X509 error - decoding error.
16050:OSP X509 error - unable to allocate space.
16060:OSP X509 error - invalid data present.
16070:OSP X509 error - certificate has expired.
16080:OSP X509 error - certificate not found.

17010:OSP PKCS1 error - tried to access invalid private key pointer
17020:OSP PKCS1 error - unable to allocate space.
17030:OSP PKCS1 error - invalid context found.
17040:OSP PKCS1 error - tried to access NULL pointer.
17050:OSP PKCS1 error - private key overflow.

18010:OSP PKCS7 error - signer missing.
18020:OSP PKCS7 error - invalid signature found.
18020:OSP PKCS7 error - unable to allocate space.
18030:OSP PKCS7 error - encoding error.
18040:OSP PKCS7 error - tried to access invalid pointer.
18050:OSP PKCS7 error - buffer overflow.

19010:OSP ASN1 error - tried to access NULL pointer.
19020:OSP ASN1 error - invalid element tag found.
19030:OSP ASN1 error - unexpected high tag found.
19040:OSP ASN1 error - invalid primitive tag found.
19050:OSP ASN1 error - unable to allocate space.
19060:OSP ASN1 error - invalid context found.
19070:OSP ASN1 error - invalid time found.
19080:OSP ASN1 error - parser error occurred.
19090:OSP ASN1 error - parsing complete.
19100:OSP ASN1 error - parsing defaulted.
19110:OSP ASN1 error - length overflow.
19120:OSP ASN1 error - unsupported tag found.
19130:OSP ASN1 error - object ID not found.
19140:OSP ASN1 error - object ID mismatch.
19150:OSP ASN1 error - unexpected int base.
19160:OSP ASN1 error - buffer overflow.
19170:OSP ASN1 error - invalid data reference ID found.
19180:OSP ASN1 error - no content value for element found.
19190:OSP ASN1 error - integer overflow.

20010:OSP Crypto error - invalid parameters found.
20020:OSP Crypto error - unable to allocate space.
20030:OSP Crypto error - could not verify signature.
20040:OSP Crypto error - implementation specific error.
20050:OSP Crypto error - tried to access invalid pointer.
20060:OSP Crypto error - not enough space to perform operation.

21010:OSP PKCS8 error - invalid private key pointer found.
21020:OSP PKCS8 error - unable to allocate space for operation.
21030:OSP PKCS8 error - invalid context found.
21040:OSP PKCS8 error - tried to access NULL pointer.
21050:OSP PKCS8 error - private key overflow.

22010:OSP Base 64 error - encode failed.
22020:OSP Base 64 error - decode failed.

22510:OSP audit error - failed to allocate memory.

156010:OSP RSN failure error - no data present.
156020:OSP RSN failure error - data is invalid.

debug voip settlement exit

To show all the Settlement function exits, use the **debug voip settlement exit** command.

[no] debug voip settlement exit

Command History

Release	Modification
12.0(4)XH1	This command was introduced.

Example

```
01:21:10:OSP:EXIT :OSPPMimeMessageInit()
01:21:10:OSP:EXIT :OSPPMimeMessageSetContentAndLength()
01:21:10:OSP:EXIT :OSPPMimeMessageBuild()
01:21:10:OSP:EXIT :OSPPMimePartFree()
01:21:10:OSP:EXIT :OSPPMimePartFree()
01:21:10:OSP:EXIT :OSPPMimeDataFree()
01:21:10:OSP:EXIT :OSPPMimeMessageCreate()
01:21:10:OSP:EXIT :OSPPMsgInfoAssignRequestMsg()
01:21:10:OSP:EXIT :ospHttpSelectConnection
01:21:10:OSP:EXIT :OSPPSockCheckServicePoint() isconnected(1)
01:21:10:OSP:EXIT :ospHttpBuildMsg()
01:21:10:OSP:EXIT :OSPPSockWrite() (0)
01:21:10:OSP:EXIT :OSPPSSLSessionWrite() (0)
01:21:10:OSP:EXIT :OSPPSSLSessionRead() (0)
01:21:10:OSP:EXIT :OSPPSSLSessionRead() (0)
01:21:10:OSP:EXIT :OSPPHttpParseHeader
01:21:10:OSP:EXIT :OSPPHttpParseHeader
01:21:10:OSP:EXIT :OSPPSSLSessionRead() (0)
01:21:10:OSP:EXIT :OSPPUtilMemCaseCmp()
```

debug voip settlement network

To show all the messages exchanged between a router and a Settlement provider, use the **debug voip settlement network** command.

[no] debug voip settlement network

Command History

Release	Modification
12.0(4)XH1	This command was introduced.

Usage Guidelines

Using the **debug voip settlement network** command shows the messages between the router and a Settlement provider. This debug output shows, in detail, the messages in HTTP and XML formats.

See the following screen output:

Example

```

00:47:25:OSP:HTTP connection:reused
00:47:25:OSP:OSPPSockWaitTillReady:HTTPCONN=0x6141A514, fd=0
00:47:25:OSP:OSPPSockWaitTillReady:read=0, timeout=0, select=1
00:47:25:OSP:osppHttpBuildAndSend():http=0x6141A514 sending:
POST /scripts/simulator.dll?handler HTTP/1.1
Host:1.14.115.12
content-type:text/plain
Content-Length:439
Connection:Keep-Alive

Content-Type:text/plain
Content-Length:370

<?xml version="1.0"?><Message messageId="1" random="8896">
<AuthorisationRequest componentId="1">
<Timestamp>
1993-03-01T00:47:25Z</Timestamp>
<CallId>
<![CDATA[12]]></CallId>
<SourceInfo type="e164">
5551111</SourceInfo>
<DestinationInfo type="e164">
5552222</DestinationInfo>
<Service/>
<MaximumDestinations>
3</MaximumDestinations>
</AuthorisationRequest>
</Message>

00:47:25:OSP:OSPPSockWaitTillReady:HTTPCONN=0x6141A514, fd=0
00:47:25:OSP:OSPPSockWaitTillReady:read=0, timeout=1, select=1
00:47:25:OSP:OSPM_SEND:bytes_sent = 577
00:47:25:OSP:OSPPSockProcessRequest:SOCKFD=0, Expecting 100, got
00:47:25:OSP:OSPPSockWaitTillReady:HTTPCONN=0x6141A514, fd=0
00:47:25:OSP:OSPPSockWaitTillReady:read=1, timeout=1, select=1
00:47:25:OSP:OSPPSSLSessionRead() recving 1 bytes:
HTTP/1.1 100 Continue
Server:Microsoft-IIS/4.0
Date:Wed, 20 Jan 1999 02:01:54 GMT
00:47:25:OSP:OSPPSockProcessRequest:SOCKFD=0, Expecting 200, got
00:47:25:OSP:OSPPSockWaitTillReady:HTTPCONN=0x6141A514, fd=0
00:47:25:OSP:OSPPSockWaitTillReady:read=1, timeout=1, select=1
00:47:25:OSP:OSPPSSLSessionRead() recving 1 bytes:
HTTP/1.1 200 OK
Server:Microsoft-IIS/4.0
Date:Wed, 20 Jan 1999 02:01:54 GMT
Connection:Keep-Alive
Content-Type:multipart/signed; protocol="application/pkcs7-signature"; micalg=sha1;
boundary=bar
Content-Length:1689

00:47:25:OSP:OSPPSockProcessRequest:SOCKFD=0, error=0, HTTP response

00:47:25:OSP:OSPPSockWaitTillReady:HTTPCONN=0x6141A514, fd=0
00:47:25:OSP:OSPPSockWaitTillReady:read=1, timeout=1, select=1
00:47:25:OSP:OSPPSSLSessionRead() recving 1689 bytes:

--bar
Content-Type:text/plain
Content-Length:1510

<?xml version="1.0"?><Message messageId="1" random="27285">
<AuthorisationResponse componentId="1">

```

```

<Timestamp>
1999-01-20T02:01:54Z</Timestamp>
<Status>
<Description>
success</Description>
<Code>
200</Code>
</Status>
<TransactionId>
101</TransactionId>
<Destination>
<AuthorityURL>
http://www.myauthority.com</AuthorityURL>
<CallId>
<![CDATA[12]]></CallId>
<DestinationInfo type="e164">
5552222</DestinationInfo>
<DestinationSignalAddress>
1.14.115.51</DestinationSignalAddress>
<Token encoding="base64">
PD94bWwgdGVyc2lvbj0xLjA/PjxNZXNzYWdlIG1lc3NhZ2VJZD0iMSIgcGFuZG9tPSIxODM0OSI+PFRva2VuSW5mbz48U291cmNlSW5mb30eXB1PSJlMTY0Ij41NTUxMTEzMDQ6MmF08L1ZhbG1kQWZ0ZXI+PFZhbG1kVW50aWw+MTk5OS0xMi0zMVQyMzo1OTo1OVo8L1ZhbG1kVW50aWw+PFRyYW5zYW50aWw+MTAxPC9UcmFuc2FjdGlvbk1kPjxVc2FnZURldGFpbD48QW1vdW50PjE0NDAwPC9BbW91bnQ+PEluY3JlbnVudD4xPC9JbnN1bnQ+PFNlcnZpY2UvPjxVbm10PnM8L1VuaXQ+PC9Vc2FnZURldGFpbD48L1Rva2VuSW5mbz48L01lc3NhZ2U+</Token>
<UsageDetail>
<Amount>
60</Amount>
<Increment>
1</Increment>
<Service/>
<Unit>
s</Unit>
</UsageDetail>
<ValidAfter>
1999-01-20T01:59:54Z</ValidAfter>
<ValidUntil>
1999-01-20T02:09:54Z</ValidUntil>
</Destination>
<transnexus.com:DelayLimit critical="False">
1000</transnexus.com:DelayLimit>
<transnexus.com:DelayPreference critical="False">
1</transnexus.com:DelayPreference>
</AuthorisationResponse>
</Message>

```

```

--bar
Content-Type:application/pkcs7-signature
Content-Length:31

```

This is your response signature

```
--bar--
```

debug voip settlement misc

To show the details on the code flow of each Settlement transaction, use the **debug voip settlement misc** command.

[no] debug voip settlement misc

Command History

Release	Modification
12.0(4)XH1	This command was introduced.

Usage Guidelines

Enter the **debug voip settlement misc** command to see detailed information on how each Settlement transaction is processed.

Example

```
00:52:03:OSP:osp_authorize:callp=0x6142770C
00:52:03:OSP:OSPPTTransactionRequestNew:ospvTrans=0x614278A8
00:52:03:OSP:osppCommMonitor:major:minor=(0x2:0x1)
00:52:03:OSP:HTTP connection:reused
00:52:03:OSP:osppHttpSetupAndMonitor:HTTP=0x6141A514, QUEUE_EVENT from
eventQ=0x6141A87C, comm=0x613F16C4, msginfo=0x6142792C
00:52:03:OSP:osppHttpSetupAndMonitor:connected = <TRUE>
00:52:03:OSP:osppHttpSetupAndMonitor:HTTP=0x6141A514, build msginfo=0x6142792C,
trans=0x2
00:52:04:OSP:osppHttpSetupAndMonitor:HTTP=0x6141A514, msg built and sent:error=0,
msginfo=0x6142792C
00:52:04:OSP:osppHttpSetupAndMonitor:monitor exit. errorcode=0
00:52:04:OSP:osppHttpSetupAndMonitor:msginfo=0x6142792C, error=0, shutdown=0
00:52:04:OSP:OSPMsgInfoProcessResponse:msginfo=0x6142792C, err=0, trans=0x614278A8,
handle=2
00:52:04:OSP:OSPMsgInfoChangeState:transp=0x614278A8, msgtype=12 current state=2
00:52:04:OSP:OSPMsgInfoChangeState:transp=0x614278A8, new state=4
00:52:04:OSP:OSPMsgInfoProcessResponse:msginfo=0x6142792C, context=0x6142770C, error=0
00:52:04:OSP:osp_get_destination:trans_handle=2, get_first=1, callinfop=0x614275E0
00:52:04:OSP:osp_get_destination:callinfop=0x614275E0 get dest=1.14.115.51,
validafter=1999-01-20T02:04:32Z, validuntil=1999-01-20T02:14:32Z
00:52:04:OSP:osp_parse_destination:dest=1.14.115.51
00:52:04:OSP:osp_get_destination:callinfop=0x614275E0, error=0, ip_addr=1.14.115.51,
credit=60
00:52:06:OSP:stop_settlement_ccapi_accounting:send report for callid=0x11,
transhandle=2
00:52:06:OSP:osp_report_usage:transaction=2, duration=0, lostpkts=0, lostfrs=0,
lostpktr=0, lostfrr=0
```

debug voip settlement security

To show all the tracing related to security, such as SSL or S/MIME, use the **debug voip settlement security** command.

[no] debug voip settlement security

Command History

Release	Modification
12.0(4)XH1	This command was introduced.

Usage Guidelines

The **debug voip settlement security** command shows the tracing at the SSL and S/MIME levels.

debug voip settlement transaction

To see all the attributes of the transactions on the settlement gateway, use the **debug voip settlement transaction** command.

[no] debug voip settlement transaction

Command History

Release	Modification
12.0(4)XH1	This command was introduced.

Example

Sample output from the originating gateway:

```
00:44:54:OSP:OSPPTTransactionNew:trans=0, err=0
00:44:54:OSP:osp_authorize:authorizing trans=0, err=0
as5300-04>
00:45:05:OSP:stop_settlement_ccapi_accounting:send report for
callid=7, trans
=0, calling=5710868, called=15125551212, curr_Dest=1
00:45:05:OSP:OSPPTTransactionDelete:deleting trans=0
```

Sample output from the terminating gateway:

```
00:44:40:OSP:OSPPTTransactionNew:trans=0, err=0
00:44:40:OSP:osp_validate:validated trans=0, error=0, authorised=1
```

Glossary

AAA—Authentication Authorization and Accounting. A Cisco IOS feature.

CDR—call detail record.

CEP—Cisco Enrollment Protocol.

ETSI—European Telecommunication Standards Institute.

ISP—Internet service provider.

IVR—Interactive Voice Response. A Cisco IOS software voice feature for internet telephony service providers.

MD 5—Message Digest 5. The algorithm used for message authentication in SNMP v.2; MDS verifies the integrity of the communication, authenticates the origin, and checks for timeliness.

PKI—Public key infrastructure.

OGW—originating gateway.

OSP—Open Settlement Protocol.

PKCS7—Public Key Cryptography Standard No.7.

RADIUS—Database for authenticating modem and ISDN connections and for tracking connections.

RAS—Registration, admission, and status. RAS is the protocol that is used between endpoints and the gatekeeper to perform management functions.

RSA—Rivest, Shamir, and Aldeman. Inventors of the public-key cryptographic system used for encryption and authentication.

SSL—Secure Socket Layer. Encryption technology for the Web used to provide secure transactions, such as the transmission of credit card numbers for e-commerce.

TACACS—Terminal access controller access control system.

TCL—Tool command language. TCL is an interpreted script language developed by Dr. John Ousterhout of the University of California, Berkeley, and is now developed and maintained by Sun Microsystems Laboratories.

TCP—Transmission Control Protocol.

TGW—terminating gateway.

VoIP—Voice over IP. The ability to carry normal telephone-style voice over an IP-based Internet with POTs-like functionality, reliability, and voice quality. VoIP is a blanket term, which generally refers to Cisco's standards based (for example H.323) approach to IP voice traffic.

