



Configuring Settlement for Packet Telephony

This chapter shows you how to configure Settlement for Packet Telephony. The Cisco Settlement for Packet Telephony feature equips Cisco conferencing infrastructure products to use third-party settlement systems on multiple protocols. The Settlement for Packet Telephony feature allows Internet telephony service providers to do the following:

- 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 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 AAA feature to provide security and accounting services.

The Settlement for Packet Telephony feature complies with the ETSI Technical Specification (TS) 101 321.

This chapter contains the following sections:

- Settlement for Packet Telephony Overview
- Settlement for Packet Telephony Overview
- Settlement for Packet Telephony Overview
- Settlement for Packet Telephony Overview

For a complete description of the commands used in this chapter, refer to the *Cisco IOS Multiservice Applications Command Reference* publication. To locate documentation of other commands that appear in this chapter, use the command reference master index or search online.

Settlement for Packet Telephony 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 among 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 has become a more manageable, many-to-one system, with a set of public interfaces that service providers 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.

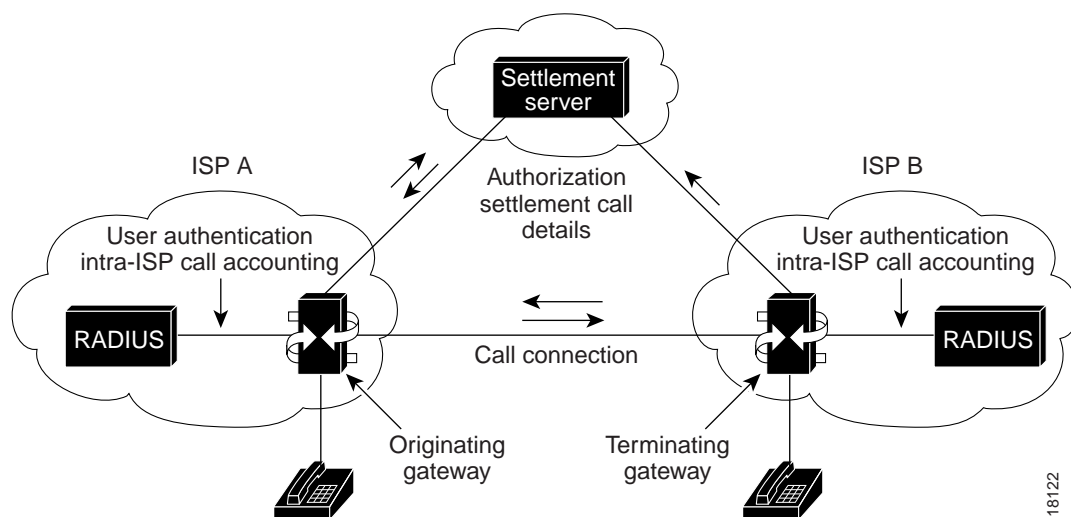
Figure 63 shows a typical gateway-based settlement setup. A voice or fax call is originated and routed through the gateway (Cisco AS5300 access server, or Cisco 2600 or 3600 series routers) to a database server (RADIUS or TACACS+) for user authentication and intra-ISP call accounting. Using TCL IVR scripts to gather and manipulate the caller 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 IVR feature, see the “Configuring Interactive Voice Response” chapter.

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 63 Gateway-Based Settlement



Settlement for Packet Telephony Prerequisite Tasks

Before you can configure your access server platform (Cisco AS5300, Cisco 3600, or other supported voice platform) with the Settlement for Packet Telephony feature, perform the following tasks:

- Make sure that your access platform has at least 16 MB Flash and 64 MB DRAM.
- Configure both the originating and terminating gateways to support IVR. In Cisco IOS Release 12.0(7)T and later, both the originating and terminating gateways must be using the IVR TCL 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. For information about configuring IVR, see the “Configuring Interactive Voice Response for Cisco Access Platforms” section earlier in this chapter.
- Confirm that the correct version of VCWare is downloaded to the Cisco AS5300 and Cisco Access Path platforms. For more information about downloading VCWare, refer to the “Managing Cisco AS5300 VFCs” section earlier in this chapter.
- Configure 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, refer to the Cisco IOS Release 12.0 documentation titled *Certification Authority Interoperability*.

Configuring Settlement for Packet Telephony

To configure settlement for packet telephony, perform the following tasks:

- Configuring the Public Key Infrastructure
- Configuring the Originating Gateway
- Configuring the Inbound POTS Dial Peer
- Configuring the Outbound VoIP Dial Peer
- Configuring the Terminating Gateway
- Configuring the Inbound VoIP Dial Peer
- Configuring the Outbound POTS Dial Peer

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 PKI, use the following commands beginning in privileged EXEC mode:

	Command	Purpose
Step 1	Router# <code>configure terminal</code>	Enters global configuration mode.
Step 2	Router(config)# <code>no crypto ca id name</code>	Clears the old certificate if one exists.

	Command	Purpose
Step 3	Router(config)# crypto key zeroize rsa	Clears the existing RSA key.
Step 4	Router(config)# hostname <i>router-name</i>	Configures the router hostname if this has not been done already.
Step 5	Router(config)# ip domain-name <i>domain-name</i>	Configures the router's IP domain name.
Step 6	Router(config)# crypto ca identity <i>name</i>	Enters CA-identity configuration mode and declares a Certification Authority (CA) name. For example, the CA name could be fieldlabs.cisco.com.
Step 7	Router(ca-identity)# enrollment url <i>url</i>	Uses a nonstandard cgi-bin script location URL.  Note This is for the TransNexus Public Key Infrastructure only.
Step 8	Router(ca-identity)# enrollment retry count <i>number</i>	(Optional) Specifies how many times the router will send unsuccessful certificate requests before giving up.
Step 9	Router(ca-identity)# enrollment retry period <i>minutes</i>	(Optional) Specifies the amount of time (in minutes) that the router waits to receive a certificate from the CA. If the router does not receive a certificate within a specified period of time (the retry period), the router will send another certificate request.
Step 10	Router(ca-identity)# exit	Exits CA-identity configuration mode.
Step 11	Router(ca-identity)# crypto ca authenticate <i>name</i>	Obtains the CA public key. Use the same <i>name</i> that you used when declaring the CA with the crypto ca identity command.
Step 12	Router(config)# crypto key generate rsa	Generates the RSA key pair.
Step 13	Router(config)# crypto ca enroll <i>name</i>	Obtains the router certificate for all your RSA key pairs.  Note This command requires that you create a challenge password that is not saved with the configuration. This password is required if your certificate is revoked.

**Note**

If your router reboots after you issue the **crypto ca enroll** command but before you receive the certificate, you must reissue the command.

Configuring the Originating Gateway

To configure the originating gateway to use the Settlement for Packet Telephony feature, use the following commands beginning in privileged EXEC mode:

	Command	Purpose
Step 1	Router# configure terminal	Enters global configuration mode.
Step 2	Router(config)# settlement <i>number</i>	Enters Settlement configuration mode and configures the Settlement provider number.
Step 3	Router(config-settlement)# type osp	Configures the Settlement provider type. In this release, OSP is the only type available.
Step 4	Router(config-settlement)# url <i>url</i>	Enters the Settlement provider URL for the ISP hosting the Settlement server.
Step 5	Router(config-settlement)# no shut	Displays the Settlement provider.



Note

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


Configuring the Inbound POTS Dial Peer

To configure the inbound POTS dial peer, use the following commands beginning in privileged EXEC mode:

	Command	Purpose
Step 1	Router# configure terminal	Enters global configuration mode.
Step 2	Router(config)# dial-peer voice <i>number</i> pots	Enters dial-peer configuration mode to configure a POTS dial peer.
		<p>Note The <i>number</i> value of the dial-peer voice pots command is a tag that uniquely identifies the dial peer.</p>
Step 3	Router(config-dial-peer)# application <i>application-name</i>	Associates the IVR TCL script application with the incoming POTS dial peer.
Step 4	Router(config-dial-peer)# destination-pattern <i>[+]string T</i>	Defines the telephone number associated with this dial peer.
Step 5	Router(config-dial-peer)# port <i>port-number</i>	Defines the voice port associated with this dial peer.

Configuring the Outbound VoIP Dial Peer

To configure the outbound VoIP dial peer, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# dial-peer voice <i>number</i> voip	Enters dial-peer configuration mode to configure the outbound VoIP dial peer.  Note The <i>number</i> value of the dial-peer voice voip command is a tag that uniquely identifies the dial peer.
Step 2	Router(config-dial-peer)# destination-pattern [+] <i>string</i> T	Defines the telephone number associated with this dial peer.
Step 3	Router(config-dial-peer)# session target settlement	Configures settlement as the target to resolve the terminating gateway address.



Note

The originating gateway 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 to use 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 beginning in global configuration mode:


	Command	Purpose
Step 1	Router(config)# settlement <i>number</i>	Enters Settlement configuration mode and configures the Settlement provider number.
Step 2	Router(config-settlement)# type osp	Configures the Settlement provider type. In this release, OSP is the only type available.
Step 3	Router(config-settlement)# url <i>url</i>	Enters the Settlement provider URL for the ISP hosting the Settlement server.
Step 4	Router(config-settlement)# no shut	Displays the Settlement provider.

**Note**

If you are configuring a TransNexus server, enter the **url** command, then enter the **customer-id** and **device-id** commands.

Configuring the Inbound VoIP Dial Peer

To configure the inbound VoIP dial peer, perform the following tasks beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# dial-peer voice <i>number</i> voip	Enters the dial-peer configuration mode to configure the inbound VoIP dial peer.  Note The <i>number</i> value of the dial-peer voice voip command is a tag that uniquely identifies the dial peer.
Step 2	Router(config-dial-peer)# application <i>application-name</i>	Associates the IVR TCL script application with the inbound VoIP dial peer.
Step 3	Router(config-dial-peer)# incoming called-number <i>string</i>	Defines the telephone number associated with the voice port for this dial peer.
Step 4	Router(config-dial-peer)# session target settlement	Enters the Settlement as the target to resolve the terminating gateway address.

Configuring the Outbound POTS Dial Peer

To configure the outbound POTS dial peer, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# dial-peer voice <i>number</i> pots	Enters dial-peer configuration mode to configure the outbound POTS dial peer. The <i>number</i> value of the dial-peer voice pots command is a tag that uniquely identifies the dial peer.
Step 2	Router(config-dial-peer)# destination-pattern <i>[+]string</i> T	Defines the telephone number associated with this dial peer. Use the called number for the <i>string</i> argument.
Step 3	Router(config-dial-peer)# port <i>port-number</i>	Associates the dial peer with a specific voice port.

**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

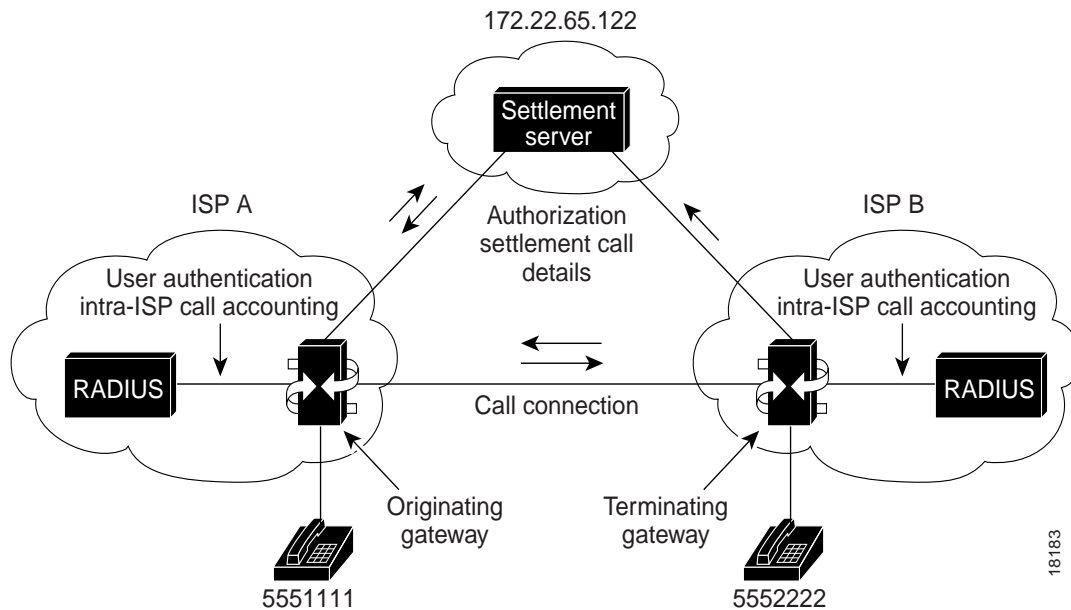
You can verify the Settlement for Packet Telephony feature configuration by performing the following tasks:

- To verify Settlement configuration parameters, use the **show running configuration** command.
- To verify that the operational status of the dial peer is up, use the **show dial-peer voice** command.

Settlement for Packet Telephony Configuration Examples

The following example shows settlement configurations for both the originating and terminating gateways. Figure 64 shows the topology for these configuration examples.

Figure 64 Example of Settlement Configurations for Originating and Terminating Gateways



Settlement on the Originating Gateway

The following output displays the configuration for the originating gateway; this output was created by using the **show running configuration** command:

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

```

Settlement on the Terminating Gateway

The following output displays the configuration for the terminating gateway; this output was created by using the **show running configuration** command:

```

!
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
```

