



Configuring Settlement Applications

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.
- Enable Cisco access platforms to provide Open Settlement Protocol (OSP) for service providers
- Work with the existing AAA feature to provide security and accounting services
- Specify a list of patterns that can be matched with a user account to see if that user is roaming
- Limit calls to authorized users and prevents unauthorized usage of limited telephony resources
- Allow users to initiate a Voice over Internet Protocol (VoIP) telephone connection from a web server page

Cisco provides a set of enabling technologies for Cisco IOS products to interface with third-party settlement systems.

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

This chapter contains the following sections:

- [Settlement for Packet Telephony Overview, page 500](#)
 - [Settlement \(OSP\) Enhancements, page 501](#)
 - [Roaming, page 501](#)
 - [Public Key Infrastructure Multiple Roots, page 503](#)
 - [User-Network Interface OSP, page 504](#)
 - [Click-to-Talk Functionality, page 505](#)
- [Settlement for Packet Telephony Prerequisite Tasks, page 506](#)
- [Settlement for Packet Telephony Configuration Task List, page 506](#)
- [Settlement for Packet Telephony Configuration Examples, page 520](#)

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

To identify the hardware platform or software image information mentioned in this chapter, use the [Feature Navigator](#) on Cisco.com to search for information about the feature or refer to the software release notes for a specific release. For more information, see the “Identifying Supported Platforms” section in the “Using Cisco IOS Software” chapter.

Settlement for Packet Telephony Overview

When you make a telephone call, the cost charged can be divided among various carriers involved in the completion of the call. *Settlement* is the method used to divide the cost among the carriers. Traditionally, settlement agreements have been arranged between pairs of carriers. 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 implemented by service providers.

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 various reports of the calling and called parties and generates billing information. Call details are reported on a call-by-call basis.

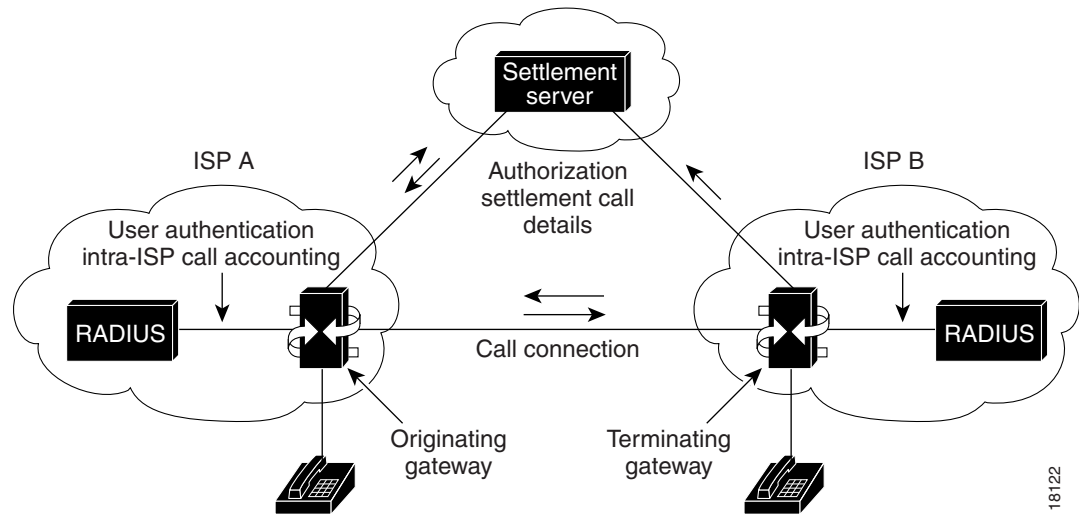
[Figure 99](#) shows a typical gateway-based settlement network topology. A voice or fax call is originated and routed through the gateway (a Cisco AS5300 Universal Access Server or a Cisco 2600 or Cisco 3600 series router) to a database server (RADIUS or TACACS+) for user authentication and intra-internet service provider (ISP) call accounting. Using tool command language (TCL) interactive voice response (IVR) 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 IVR feature, see the chapter “Configuring TCL IVR Applications.”

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 99 Gateway-Based Settlement



Settlement (OSP) Enhancements

Since the introduction of Settlements for Packet Voice, the Settlements for Packet Voice protocol has also undergone several feature enhancements. These enhancements are documented in the following sections:

- [Roaming, page 501](#)
- [Public Key Infrastructure Multiple Roots, page 503](#)
- [User-Network Interface OSP, page 504](#)

Roaming

Support for the settlement functions required for roaming callers has been added. A caller is roaming when dialing into a gateway that is not the home gateway. A home gateway belongs to the user's service provider. Usually, the subscriber is billed with additional charges for roaming calls. The settlement server and the service provider need to know when a caller is roaming in order to create accurate billing statements.

A roaming caller must be authenticated before a call can go through a gateway. Both authentication, authorization, and accounting (AAA) and the settlement server can authenticate a roaming user. If AAA fails to authenticate a roaming caller, the roaming call must be routed to a settlement server. If the settlement server cannot authenticate the caller, the call is terminated.

You can use the following methods to configure the roaming feature on the gateway:

- Setting the roaming patterns to determine if a caller (by user identification) is roaming
- Setting the roaming capability in the settlement provider
- Setting the roaming capability in the dial peer
- Forcing a call to be routed via a settlement server in a dial peer

User Identification

The gateway can specify a list of patterns to be matched with a user account number (user identification) to see if that user is roaming. The user enters an account number and personal identification number (PIN) as part of the interaction with the TCL IVR prompts.

The roaming patterns are configured by using the **settlement roam-pattern** command in global configuration mode.

For additional information about the IVR or AAA, refer to the following Cisco IOS documents:

- *Cisco Interactive Voice Response*
- *Service Provider Features for Voice over IP*

Settlement Provider

Some settlement providers want to know if a user is roaming so they can apply the appropriate charge to a user account. Other settlement providers do not distinguish between local and roaming users.

A settlement provider can use the **roam** command in the settlement configuration mode to track roaming users. If a user is roaming and the settlement provider is tracking roaming, the gateway sends the user account number and PIN to the settlement server so that the user can be properly authenticated.

Dial Peer

A gateway can dictate if a particular outbound dial peer can terminate roaming calls and only permit local calls with the **no roam** command. The default of the dial peer is no roaming support. The gateway allows a roaming call to go through only if both the dial peer associated with that call and the settlement provider support roaming. In other words, a call fails if the dial peer has roaming enabled but the settlement provider does not, and vice versa. Therefore, the roaming feature must be explicitly enabled in the dial peer.

Dial Peer Settlement Option

The **settle-call** keyword forces the call to go through a settlement server regardless of the session target type. If the session target type is ipv4, dns, or RAS, the gateway resolves the terminating gateway address and asks the settlement server to authorize that terminating gateway.

The restrictions and behaviors associated with use of the **settle-call** keyword with outbound dial peers are described in the “Restrictions” section later in this chapter.

Public Key Infrastructure Multiple Roots

The public key infrastructure (PKI) multiple roots allows a settlement server to use one certificate for a Secure Socket Layer (SSL) handshake and a different certificate for token signing. Cisco devices can share public keys using digital certificates.

Digital certificates are normally issued by trusted third parties, which are called certificate authorities (CAs). Every router that uses digital certificates should enroll its public key with the CA server. Typically during enrollment, the certificate administrator (a person) will manually verify that the requesting router is authentic and grant the certificate; some CA servers can authenticate the routers automatically.

A certificate has many fields, including a serial number, a fingerprint, and an expiry date. A certificate can be revoked before its expiry date because of key compromise or other security reasons. The CA server maintains a list of revoked certificates, which is called a certificate revocation list (CRL). Routers can be configured not to accept a peer certificate that has been revoked. A router downloads a CRL from the CA server for this purpose.

Cisco routers use a proprietary Certificate Enrollment Protocol (CEP) to communicate with the CA server. The CA server should understand CEP.

The PKI Multiple Roots feature is based on the Cisco security and PKI technology. For in-depth information about security, refer to the *Cisco IOS Security Configuration Guide*.

Different commands are used for the following purposes (as follows):

- For SSL handshake with the settlement server, the gateway uses the certificate obtained through the **crypto ca authenticate** command.
- For token verification, the gateway can use one of the root certificates configured with the **crypto ca trusted-root identity** command.

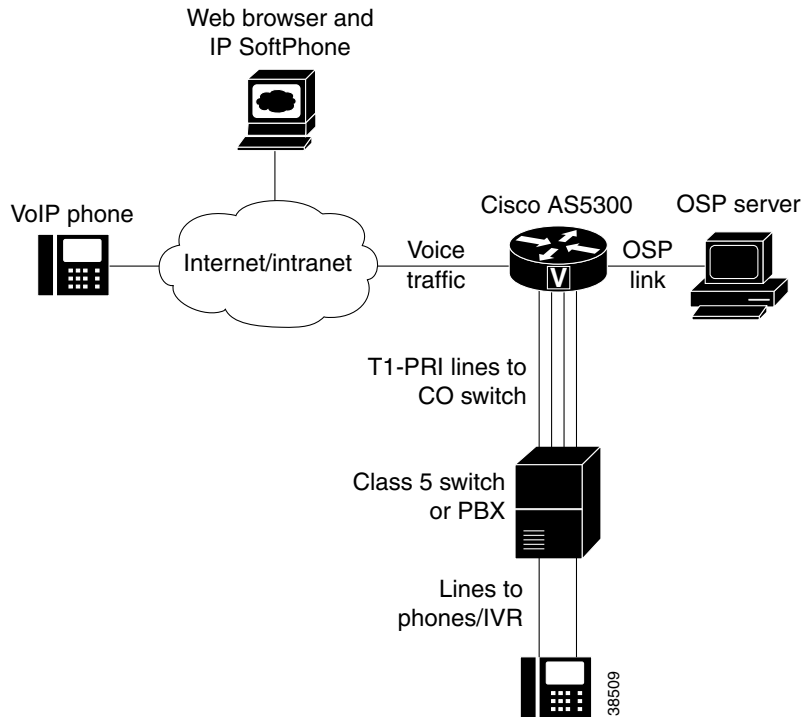
**Note**

To specify which root certificate is used for token validation, use the command **token-root-name** in the settlement configuration mode.

User-Network Interface OSP

The User-Network Interface (UNI)-OSP feature, illustrated in [Figure 100](#), allows a single Cisco AS5300 gateway to use OSP to authenticate VoIP calls to the PSTN.

Figure 100 Authenticating VoIP Calls with the Cisco AS5300 Gateway



To implement VoIP authentication, the gateway must be connected to the Internet or intranet and to an OSP server. The OSP server, which can be any properly configured Windows NT or UNIX server, communicates over a Computer Telephony Interface (CTI) link to a Class 5 switch or PBX. Use the settlement command **type** and include the *uni-osp* argument to configure the UNI-OSP feature.

When a VoIP device sends an H.323 setup message to the gateway, the destination number (DNIS) of the call is matched to a POTS dial peer configured on the voice gateway. The voice gateway then sends an OSP authorization request, containing the call ID (a unique 16-bit number), and a calling and called number (E.164 ANI/DNIS).

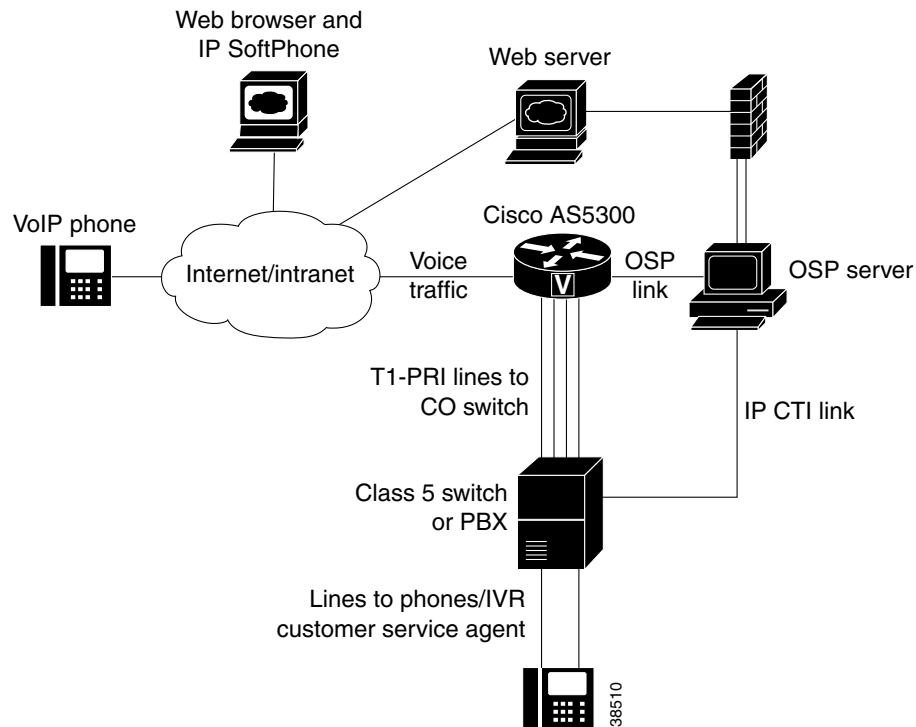
The OSP server sends an authorization response back to the voice gateway, which then initiates a call to a PBX or Class 5 switch over one of its T1-PRI spans. When the voice gateway detects that a call has ended, it transmits usage information to the OSP server, informing it that the call has terminated.

Note that the “src-info” field of the OSP authorization request contains the IP address of the caller’s PC, with all “dot” characters removed and each three-digit segment right justified. For example, the automatic number identification (ANI) field for a call originating from IP address 172.16.1.20 would appear as “172069221002.”

Click-to-Talk Functionality

As illustrated in [Figure 101](#), the UNI-OSP feature can be used when implementing a “click-to-talk” function on web server pages.

Figure 101 Implementing Click-to-Talk with the Cisco 5300 Gateway



When using the click-to-talk function, a customer selects a link on a web page indicating that a request to talk to a customer service or technical support representative. The web server then launches a preinstalled SoftPhone on the web browser machine through a browser plug-in. The web server supplies the PC SoftPhone application with the telephone destination number (DNIS) of the appropriate agent, and the route point, queue, and IP address of the voice gateway.

When the SoftPhone sends an H.323 setup message to the voice gateway, the destination number (DNIS) is matched to a POTS dial peer configured on the voice gateway. An authorization request is then sent over the OSP link to the OSP server, containing the call ID (a unique 16 bit number) and a calling and called number (E.164 ANI/DNIS). Because the originating device is a PC SoftPhone, the ANI field contains the IP address of the PC.

The OSP server compares the IP address received in the ANI field with those customers who have pressed the click-to-talk link. The OSP server sends an authorization response to the voice gateway, containing the E.164 number of the appropriate agent, based on the web page from which click-to-talk was initiated.

When the voice gateway initiates a call to a PBX or Class 5 switch, the arriving call causes a setup indication to appear on the switch or PBX. The CTI link between the PBX or switch and the OSP server informs the OSP server of the incoming call and includes information such as the DNIS, ANI (IP address of the caller's PC), and the incoming trunk line. The OSP server then has sufficient information to route the call to the appropriate customer service or technical support agent queue.

Settlement for Packet Telephony Prerequisite Tasks

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

- Ensure that your access platform has a minimum of 16 MB Flash memory and 64 MB DRAM.
- In Cisco IOS Release 12.0(4)XH or later releases, both the originating and terminating gateways must be using the 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 to those calls by the settlement server; therefore, those calls will pass through without being audited or charged.
- Ensure that the correct version of VCWare is downloaded.
- Before configuring the settlement feature, you must have configured the 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 document titled *Certification Authority Interoperability*.

Restrictions

- The Settlements for Packet Voice, Phase 2, feature requires Cisco IOS Release 12.1(1)T and a compatible version of VCWare.



Note The Cisco AS5800 universal access server uses portware, not VCWare, with its modems.

- The Settlements for Packet Voice, Phase 2, feature set cannot be enabled on dial peers that use remote access server (RAS) as the session target.
- The software that includes the Settlements for Packet Voice, Phase 2, feature set is offered only in crypto images and therefore is under export controls.

Settlement for Packet Telephony Configuration Task List

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

- [Configuring the Public Key Infrastructure, page 507](#)
- [Configuring the Originating Gateway, page 508](#)
- [Configuring the Terminating Gateway, page 511](#)
- [Configuring Settlement with Roaming, page 514](#)
- [Configuring Settlement with PKI Multiple Roots, page 515](#)
- [Configuring Settlement with Suggested Route, page 516](#)

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 global configuration mode:

	Command	Purposes
Step 1	Router(config)# no crypto ca identity <i>name</i>	Clears the old CA identity if a previous one exists.
Step 2	Router(config)# crypto key zeroize rsa	Clears the existing RSA key.
Step 3	Router(config)# hostname <i>router-name</i>	Configures the host name of the router if this has not been done already.
Step 4	Router(config)# ip domain-name <i>domain-name</i>	Configures the IP domain name of the router.
Step 5	Router(config)# ip host <i>CA-hostname</i> <i>CA-ipaddress</i>	Enters the CA host name and IP address.
Step 6	Router(config)# crypto ca identity <i>name</i>	Declares a CA name and enters CA-identity configuration mode. For example, the <i>name</i> argument could be fieldlabs.cisco.com.
Step 7	Router(ca-identity)# enrollment url <i>url</i>	The /cgi-bin/pkclient.exe file is the default Common Gateway Interface (CGI) script that Cisco IOS software assumes. The script path should be given in the URL if it is different from the default. Note The URL should have the format http://CA-hostname where CA-hostname is previously configured in Step 5 .
Step 8	Router(ca-identity)# enrollment retry count <i>number</i>	(Optional) Specifies how many times the router will poll the CA server for the certificate status when the certificate requests are pending. Note The router sends the certificate request only once. Then it periodically polls the CA server until the certificate is granted or denied, or until the retry count exceeds the retry count configured.
Step 9	Router(ca-identity)# enrollment retry period <i>minutes</i>	(Optional) Specifies the interval between subsequent polls. Default = 1 minute. Note The retry period contains two subsequent polls for certificate status. The router does not send another certificate request. It merely polls for the status as long as the CA server returns the certificate status as pending, or until the retry count is reached. Note After specifying a certificate, the router waits to receive a certificate from the CA. If the router does not receive a certificate within a period of time (the retry period), the router sends another certificate request.
Step 10	Router(ca-identity)# exit	Exits CA-identity configuration mode.

	Command	Purposes
Step 11	Router(config)# crypto ca authenticate <i>name</i>	Obtains the CA's 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 you to create a challenge password that is not saved with the configuration. This password is required in order to obtain a new certificate if your certificate is revoked, so remember this password. 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, perform the following tasks:

- [Configuring the Settlement Provider, page 508](#)
- [Configuring the Inbound POTS Dial Peer, page 509](#)
- [Configuring the Outbound VoIP Dial Peer, page 510](#)

Configuring the Settlement Provider

To configure the settlement provider to authorize calls, use the following commands beginning in global configuration mode:

	Command	Purposes
Step 1	Router(config)# settlement <i>provider</i>	Enters settlement configuration mode and configures the settlement provider number.
Step 2	Router(config-settlement)# type osp	Configures the settlement provider type.
Step 3	Router(config-settlement)# shutdown	Shuts down the settlement provider.
Step 4	Router(config-settlement)# url <i>url-address</i>	Enters the settlement provider URL for the ISP that is hosting the settlement server. Note This step can be repeated if the settlement provider has more than one service point.
Step 5	Router(config-settlement)# response-timeout <i>number</i>	Configures the maximum time, in seconds, to wait for a response from a server. The default response timeout is 1 second.
Step 6	Router(config-settlement)# no shutdown	Activates the settlement provider.

**Note**

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

Configuring the Inbound POTS Dial Peer

**Note**

In [Step 2](#) of the following procedures, do not use the default session application. The default session application does not support settlement. Calls handled by the default session application are not routed to a settlement server. Settlement tokens are not validated in the default session application.

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

	Command	Purposes
Step 1	Router(config)# dial-peer voice <i>number</i> pots	Enters dial-peer configuration mode to configure a POTS dial peer. The <i>number</i> argument uniquely identifies the dial peer.
Step 2	Router(config-dial-peer)# application <i>application-name</i>	Configures the application attribute and identifies the desired TCL script using the <i>application-name</i> argument. Note The <i>application-name</i> must be the name of the TCL IVR script. If the application attribute is not configured, or if the POTS dial peer is not created, the default session application will process the call.
Step 3	Router(config-dial-peer)# destination-pattern [+] <i>string</i> [T]	Configures the destination pattern of the dial peer. Enter the number or pattern of the outbound called number. The <i>string</i> argument is a series of digits that specify an 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"> • Plus sign (+)—(Optional) Indicates an E.164 standard number. The plus sign (+) is not supported on the Cisco MC3810 multiservice concentrator. • <i>string</i>—Specifies the E.164 or private dialing plan telephone number. Valid entries are the digits 0 through 9, the letters A through D, and the following special characters: <ul style="list-style-type: none"> – Asterisk (*) and pound sign (#) that appear on standard touch-tone dial pads. – Comma (,) inserts a pause between digits. – Period (.) matches any entered digit (this character is used as a wildcard). • T—(Optional) Indicates that the destination-pattern value is a variable length dial-string.
Step 4	Router(config-dial-peer)# port <i>port-number</i>	Associates 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 beginning in global configuration mode:

	Command	Purposes
Step 1	Router(config)# dial-peer voice <i>number</i> voip	Enters dial-peer configuration mode to configure the outbound VoIP dial peer. The <i>number</i> argument uniquely identifies the dial peer.
Step 2	Router(config-dial-peer)# destination-pattern [+] <i>string</i> [T]	<p>Configures the destination pattern of the dial peer. Enter the number or pattern of the outbound called number.</p> <p>The <i>string</i> is a series of digits that specify an 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"> • Plus sign (+)—(Optional) Indicates an E.164 standard number. The plus sign (+) is not supported on the Cisco MC3810 multiservice concentrator. • <i>string</i>—Specifies the E.164 or private dialing plan telephone number. Valid entries are the digits 0 through 9, the letters A through D, and the following special characters: <ul style="list-style-type: none"> – Asterisk (*) and pound sign (#) that appear on standard touch-tone dial pads. – Comma (,) inserts a pause between digits. – Period (.) matches any entered digit (this character is used as a wildcard). • T—(Optional) Indicates that the destination-pattern value is a variable length dial-string.
Step 3	Router(config-dial-peer)# session target settlement	<p>Configures settlement as the target to resolve the terminating gateway address.</p> <p>Note The <i>provider-number</i> argument should match one of the number values previously configured in Step 1.</p>



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, perform the following tasks:

- [Configuring the Settlement Provider, page 511](#)
- [Configuring the Inbound VoIP Dial Peer, page 512](#)
- [Configuring the Outbound POTS Dial Peer, page 513](#)

Configuring the Settlement Provider

To configure the settlement provider, use the following commands beginning in global configuration mode:

	Command	Purposes
Step 1	Router(config)# settlement <i>provider-number</i>	Enters settlement configuration mode and configures the settlement provider number.
Step 2	Router(config-settlement)# type osp	Configures the settlement provider type.
Step 3	Router(config-settlement)# url <i>url-address</i>	Enters the settlement provider URL for the ISP hosting the settlement server. Note This step can be repeated if the settlement provider has more than one service point.
Step 4	Router(config-settlement)# response-timeout <i>number</i>	Configures the maximum time, in seconds, to wait for a response from a server. The default response timeout is 1 second.
Step 5	Router(config-settlement)# no shutdown	Activates the settlement provider.



Note

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

Configuring the Inbound VoIP Dial Peer


Note

The default session application does not support settlement. Calls handled by the default session application are not routed to a settlement server. Settlement tokens are not validated in the default session application.

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

	Command	Purposes
Step 1	Router(config)# dial-peer voice <i>number</i> voip	Enters the dial-peer configuration mode to configure the inbound VoIP dial peer. The <i>number</i> argument uniquely identifies the dial peer.
Step 2	Router(config-dial-peer)# application <i>application-name</i>	Configures the application attribute and identifies the desired TCL script using the <i>application-name</i> argument.
Step 3	Router(config-dial-peer)# incoming called-number <i>string</i>	Specifies the telephone number of the voice port associated with this dial peer. String characters include wildcards to create the number or pattern.
Step 4	Router(config-dial-peer)# session target settlement <i>provider-number</i>	Identifies settlement as the session target to resolve the terminating gateway address. Note The <i>provider-number</i> value should match one of the number values previously configured in Step 1 of the section “Configuring the Settlement Provider” .

Configuring the Outbound POTS Dial Peer

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

	Command	Purposes
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> argument uniquely identifies the dial peer.
Step 2	Router(config-dial-peer)# destination-pattern [+] <i>string</i> [T]	Configures the destination pattern of the dial peer pattern. Use the called number. The <i>string</i> is a series of digits that specify an 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"> • Plus sign (+)—(Optional) Indicates an E.164 standard number. The plus sign (+) is not supported on the Cisco MC3810 multiservice concentrator. • <i>string</i>—Specifies the E.164 or private dialing plan telephone number. Valid entries are the digits 0 through 9, the letters A through D, and the following special characters: <ul style="list-style-type: none"> – Asterisk (*) and pound sign (#) that appear on standard touch-tone dial pads. – Comma (,) inserts a pause between digits. – Period (.) matches any entered digit (this character is used as a wildcard). • T—(Optional) Indicates that the destination-pattern value is a variable length dial-string.
Step 3	Router(config-dial-peer)# port <i>port-number</i>	Associates the voice-telephony dial peer with a specific voice port. Activates 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-config** command to verify your configuration.

Configuring Settlement with Roaming

To configure settlement with the roaming capability, perform the configuration tasks described in the following sections:

- [Configuring the Roaming Patterns on the Originating Gateway, page 514](#)
- [Enabling the Roaming Feature for the Settlement Provider, page 514](#)
- [Enabling the Roaming Feature in the Outbound Dial Peer, page 514](#)

Configuring the Roaming Patterns on the Originating Gateway

To configure the roaming patterns on the originating gateway, use the following commands beginning in global configuration mode:

Command	Purposes
Router(config)# settlement roam-pattern <i>pattern</i>	Defines the pattern for roaming account numbers. Enter multiple instances of this command to specify multiple patterns.

Enabling the Roaming Feature for the Settlement Provider

To enable the roaming feature for the settlement provider, use the following commands beginning in global configuration mode:

	Command	Purposes
Step 1	Router(config)# settlement <i>provider-number</i>	Enters settlement configuration mode and configures the settlement provider number.
Step 2	Router(config-settlement)# roaming	Enables the roaming capability on this provider.

Enabling the Roaming Feature in the Outbound Dial Peer

To enable the roaming feature in the outbound dial peer, use the following commands beginning in global configuration mode:

	Command	Purposes
Step 1	Router(config)# dial-peer voice <i>number</i> voip	Enters dial-peer configuration mode to configure a VoIP dial peer.
Step 2	Router(config-dial-peer)# roaming	Enables roaming on this dial peer.

Configuring Settlement with PKI Multiple Roots

To configure the PKI multiple roots capability, perform the configuration tasks described in the following sections:

- [Configuring Settlement with PKI Multiple Roots, page 515](#)
- [Configuring the Root Certificate for Token Validation on the Terminating Gateway, page 515](#)
- [Defining the Token Validation on the Terminating Gateway, page 515](#)

Configuring a Settlement Server with PKI Multiple Roots on the Originating Gateway

To configure a settlement server with PKI Multiple Roots on the Originating Gateway, use the following commands beginning in global configuration mode:

	Command	Purposes
Step 1	Router(config)# settlement <i>provider-number</i>	Enters settlement configuration mode for a specific provider.
Step 2	Router(config-settlement)# url <i>url-address</i>	Enters the URL to the service point that uses two different certificates for SSL and token.

Configuring the Root Certificate for Token Validation on the Terminating Gateway

To configure the root certificate for token validation on the Terminating Gateway, use the following commands beginning in global configuration mode:

	Command	Purposes
Step 1	Router(config)# crypto ca trusted-root <i>identity</i>	Configures the root certificate that the server uses to sign the settlement tokens.
Step 2	Router(ca-root)# root tftp <i>tftp-ipaddress</i> <i>root-ca-file</i>	Specifies where to obtain the root certificate file.
Step 3	Router(ca-root)# crypto ca authenticate <i>identify-name</i>	Starts downloading the root certificate file from the server.

Defining the Token Validation on the Terminating Gateway

To define the token validation on the Terminating Gateway, use the following commands beginning in global configuration mode:

	Command	Purposes
Step 1	Router(config)# settlement <i>provider-number</i>	Enters settlement configuration mode for a specific provider.
Step 2	Router(config-settlement)# token-root-name <i>name</i>	Specifies which root certificate the gateway uses to validate the token. The name must match the name of the certificate configured using either the crypto ca identity <i>name</i> or the crypto ca trusted-root <i>identity</i> commands.

Configuring Settlement with Suggested Route

The **session target** command in the dial peer dictates how the gateway resolves the terminating address to complete the call. Besides settlement, the gateway could use the **ipv4** or **dns** options if it knows the exact address of the Terminating Gateway, or it could use the **ras** option to consult a gatekeeper.

To force a call to be authorized by a settlement server, use the following commands beginning in global configuration mode:

	Command	Purposes
Step 1	Router(config)# dial-peer voice <i>number</i> <i>voip</i>	Enters dial-peer configuration mode to configure a VoIP dial peer.
Step 2	Router(config-dial-peer)# settle-call [<i>provider-number</i>]	Forces a call to be authorized with a settlement server that uses the address resolution method specified in the session target type command.

Table 39 shows how settlement is enabled on a dial peer based on various combinations of the **session target** and **settle-call** commands.

Table 39 The **settle-call** and **session target** Commands

Command	session target IP DNS	session target settlement	session target RAS
settle-call	Settlement processing will occur; see Table 40.	Settlement processing will occur; see Table 40.	Illegal (legal once cc_ResolveAddress function is implemented).
no settle-call	Settlement processing will <i>not</i> occur; see Table 40.	Settlement processing will occur; see Table 40.	Settlement processing will <i>not</i> occur; see Table 40.



Note

If the **session target settlement** and **settle-call** keywords are used, the keywords must be the same or an error is generated. If one Cisco IOS command specifies *one keyword* and the other does not, the specified *keyword* becomes the only clearinghouse used. If neither specifies a *keyword*, all clearinghouses can be searched.

Table 40 shows the results of using the **session target settlement** command.

Table 40 Results of the session target settlement Command

User Status	The settle Command	The no settle Command
User is authenticated and local.	<ul style="list-style-type: none"> • Authorizes call • Routes call • Generates settlement CDR¹ 	<ul style="list-style-type: none"> • Authorizes call • Routes call • Generates settlement CDR
User is authenticated and roaming.	<ul style="list-style-type: none"> • Authenticates roaming user • Authorizes call • Routes call • Generates settlement CDR 	<ul style="list-style-type: none"> • Authenticates roaming user • Authorizes call • Routes call • Generates settlement CDR
User is roaming but not yet authenticated.	<ul style="list-style-type: none"> • Authenticates roaming user • Authorizes call • Routes call • Generates settlement CDR 	<ul style="list-style-type: none"> • Authenticates roaming user • Authorizes call • Routes call • Generates settlement CDR

1. CDR = call detail record.

Table 41 shows the results of using the **session target ipv4** or **session target dns** command.

Table 41 Results of the session target IPV4 and session target DNS Commands

User Status	The settle Command	The no settle Command
User is authenticated and local.	<ul style="list-style-type: none"> • Authorizes call • Provides IP address in a “DestinationAlternate” field and fails call if settlement returns something different • Generates settlement CDR 	Performs no settlement operations.
User is authenticated and roaming.	<ul style="list-style-type: none"> • Authorizes call • Provides IP address in a “DestinationAlternate” field and fails call if settlement returns something different • Generates settlement CDR 	Performs no settlement operations. This dial peer is configured so that the administration can use roaming-enabled AAA but not settlement.
User is roaming but not yet authenticated.	<ul style="list-style-type: none"> • Authenticates call <p>Note Authentication failure is possible and implies that the “place call” TCL verb must return a code that allows the script to loop back to recollect account information.</p> <ul style="list-style-type: none"> • Authorizes call • Provides IP address in a “DestinationAlternate” field and fails call if settlement returns something different • Generates settlement CDR 	Fails the call (the user is not authenticated and there is no facility to do so using settlement).

Table 42 shows the result of using the **session target ras** command with no token.



Note

Settlement and RAS session targets are *illegal* in Cisco IOS Release 12.0(4)XH. Table 42 applies to releases that allow RAS automatic repeat request (ARQ)/ Advanced Communications Function (ACF) to be performed prior to calling settlement.

The gateway needs a way to decide whether the gatekeeper has done settlement authorization. The gateway checks to see if the returned ACF contains a settlement token. Table 42 applies to the case where no token is returned.

Table 42 Results of the session target RAS Command with No Token

User Status	The settle Command	The no settle Command
User is authenticated and local.	<ul style="list-style-type: none"> • Authorizes call • Provides RAS signal address in “DestinationAlternate” field and fails call if settlement returns something different • Generates settlement CDR 	Performs no settlement operations.
User is authenticated and roaming.	<ul style="list-style-type: none"> • Authenticates user • Authorizes call • Specifies “destinationSignalAddr” in “OSP DestinationAlternate” field and fails call if CH returns something different • Generates settlement CDR 	Performs no settlement operations.
User is roaming but not yet authenticated.	<ul style="list-style-type: none"> • Authenticates user • Authorizes call • Specifies “destinationSignalAddr” in “OSP DestinationAlternate” field and fails call if CH returns something different • Generates settlement CDR 	Fails the call (there is no way to authenticate the user).

Table 43 shows the result of using the **session target ras** command with token. In Table 43, the ACF returns a valid token, indicating that the call has already been authorized and routed by settlement.

**Note**

The roaming scenarios require that the “ARQ sourceAlternative” field be formatted with the user credentials.

Table 43 Results of the session target RAS Command with Token

User Status	The settle Command	The no settle Command
User is authenticated and local.	<ul style="list-style-type: none"> • Generates settlement CDR only 	Fails the call (implies that the dial peer was not configured to work with a settlement-enabled gatekeeper).
User is authenticated and roaming.	<ul style="list-style-type: none"> • Generates settlement CDR only 	Fails the call (implies that the dial peer was not configured to work with a settlement-enabled gatekeeper).
User is roaming but not yet authenticated.	<ul style="list-style-type: none"> • Generates settlement CDR only 	Fails the call (implies that the dial peer was not configured to work with a settlement-enabled gatekeeper).

Table 44 shows what happens when an incoming VoIP call is detected, depending on whether the setup message contains a token.

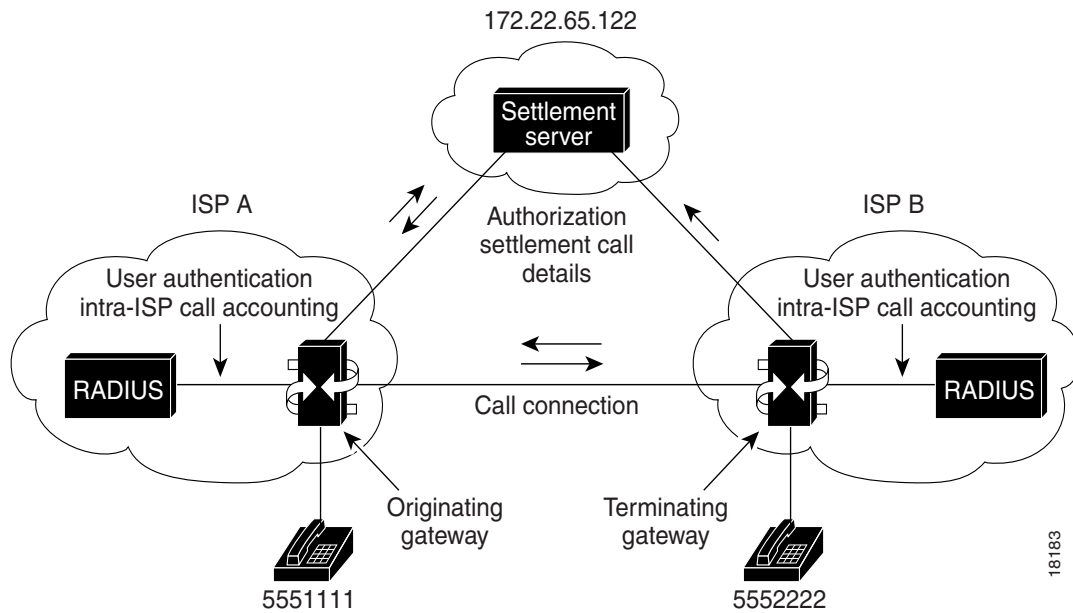
Table 44 Results of Receiving Inbound Calls

Token Status	The settle Command	The no settle Command
Settlement token is received in setup message.	<ul style="list-style-type: none"> Validates token Generates settlement CDR 	Rejects the call (because the dial peer is not configured to do settlement, originated calls will not be settled).
No settlement token is received.	<ul style="list-style-type: none"> Fails calls (to avoid fraudulent calls) 	Accepts the call.

Settlement for Packet Telephony Configuration Examples

The examples that follow show settlement configurations for both the originating and terminating gateways. Figure 102 shows the topology for these configuration examples.

Figure 102 Example of Settlement Configurations for Originating and Terminating Gateways



18183

Settlement on the Originating Gateway Example

The following example displays the configuration for the originating gateway by using the **show running-config** command:

```
!  
version 12.2  
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 Example

The following example displays the configuration for the terminating gateway resulting from the use of the **show running-config** command:

```

!
version 12.2
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

```

Settlement with Roaming Example

The following output is the result of the settlement with roaming configuration:

```

!
version 12.2
service timestamps debug datetime
service timestamps log datetime
no service password-encryption
service internal
!
hostname as5300-05
!
enable secret 5 $1$1FSH$khsM3jB11ldHfXNlxqmaN1
enable password lab1
!
!resource-pool disable
!
!ip subnet-zero
ip host pkiserver 1.14.115.100
ip domain-name fieldlabs.cisco.com
ip name-server 172.16.1.4
!
isdn switch-type primary-5ess
isdn voice-call-failure 0
cns event-service server
mta receive maximum-recipients 1024
!
crypto cisco algorithm des
crypto cisco algorithm 40-bit-des
!
crypto ca identity transnexus
 enrollment retry count 100
 enrollment retry period 2
 enrollment url http://pkiserver:80
crypto ca certificate chain transnexus
 certificate ca 0171
 3082024C 308201B5 02020171 300D0609 2A864886 F70D0101 04050030 6E310B30

```

Settlement for Packet Telephony Configuration Examples

```

09060355 04061302 55533110 300E0603 55040813 0747656F 72676961 31183016
06035504 0A130F54 72616E73 4E657875 732C204C 4C433114 30120603 55040B13
0B446576 656C6F70 6D656E74 311D301B 06035504 03131454 52414E53 4E455855
53204245 54412043 41203130 1E170D39 39303332 32313334 3630395A 170D3030
30333231 31333436 30395A30 6E310B30 09060355 04061302 55533110 300E0603
55040813 0747656F 72676961 31183016 06035504 0A130F54 72616E73 4E657875
732C204C 4C433114 30120603 55040B13 0B446576 656C6F70 6D656E74 311D301B
06035504 03131454 52414E53 4E455855 53204245 54412043 41203130 819F300D
06092A86 4886F70D 01010105 0003818D 00308189 02818100 B1B8ACFC D78F0C95
0258D164 5B6BD8A4 6F5668BD 50E7524B 2339B670 DC306537 3E1E9381 DE2619B4
4698CD82 739CB251 91AF90A5 52736137 658DF200 FAFEFE6B 7FC7161D 89617E5E
4584D67F F018EDAB 2858DDF9 5272F108 AB791A70 580F994B 4CA54F08 38C32DF5
B44077E8 79830F95 96F1DA69 4CAE16F2 2879E07B 164F5F6D 02030100 01300D06
092A8648 86F70D01 01040500 03818100 2FDCB580 C29E557C 52201151 A8DB5F47
C06962D5 8FDA524E A69DE3EE C3FE166A D05C8B93 2844CD66 824A8859 974F22E0
46F69F7E 8027064F C19D28BC CA750E4E FF2DD68E 1AA9CA41 8BB89C68 7A61E9BF
49CBE41E E3A42B16 AAEDAEC7 D3B4F676 4F1A817B A5B89ED8 F03A15B0 39A6EBB9
0AFA6968 17A9D381 FD62BBB7 A7D379E5
quit
certificate 8697B659C0E190E1A8D48961EBED0DB1
30820247 308201B0 A0030201 02021100 8697B659 C0E190E1 A8D48961 EBED0DB1
300D0609 2A864886 F70D0101 04050030 6E310B30 09060355 04061302 55533110
300E0603 55040813 0747656F 72676961 31183016 06035504 0A130F54 72616E73
4E657875 732C204C 4C433114 30120603 55040B13 0B446576 656C6F70 6D656E74
311D301B 06035504 03131454 52414E53 4E455855 53204245 54412043 41203130
1E170D39 39303430 36313833 3430315A 170D3030 30343036 31383334 30315A30
81873181 84300F06 03550405 13083131 38313833 37393018 06092A86 4886F70D
01090813 0B312E31 342E3131 352E3835 302A0609 2A864886 F70D0109 02161D61
73353330 302D3035 2E666965 6C646C61 62732E63 6973636F 2E636F6D 302B0603
55040314 245B7472 616E736E 65787573 2E636F6D 20475749 443D3230 30302043
5349443D 31303030 5D305C30 0D06092A 864886F7 0D010101 0500034B 00304802
4100AF40 5CC8E37D 7211E3C4 2D036E52 70B5DA88 96600C12 8654B85E 7CEFE204
27A9B9DD B0F6B85C 1EB561BB 0F3481A2 D4661087 2B0B403A 5A65B7E0 ED9A0165
EBC10203 010001A3 0F300D30 0B060355 1D0F0404 030205A0 300D0609 2A864886
F70D0101 04050003 8181005C 1E379447 C0FCBC3F 0ABC75FA ADF79A26 770419A4
02BEC849 ECB7BDB1 58EA815B 48844DB3 4E8934E8 397F4762 F04EB716 8413C418
4289AA64 6E2EAFE1 9C9F1F31 3A5BE996 AF749623 18FBFD36 569732BF 8335C522
4ACA0BCA CFCC27C6 294AD416 15472F07 C1609E93 E1FEDA66 B69DA603 1A99699E
86937EC5 609A3D52 72A45B
quit
!
xgcp snmp sgcp
!
controller T1 0
 framing esf
 clock source line primary
 linecode b8zs
 pri-group timeslots 1-24
!
controller T1 1
 clock source line secondary 1
!
controller T1 2
!
controller T1 3
!
voice-port 0:D
!
dial-peer voice 1 pots
 application session
 destination-pattern 5710877
 port 0:D
!
dial-peer voice 5 voip

```

```
application session
incoming called-number +1404.....
session target settlement:0
!
dial-peer voice 2 pots
destination-pattern +255....
port 0:D
prefix 255
!
! Enable roaming for this dialpeer
!
dial-peer voice 6 voip
roaming
destination-pattern 1512.....
session target settlement
!
dial-peer voice 7 pots
destination-pattern +1650.....
port 0:D
prefix 1650
!
dial-peer voice 8 voip
application session
incoming called-number +1650.....
session target settlement:0
!
dial-peer voice 3 voip
application session
incoming called-number +1408.....
session target settlement:0
!
dial-peer voice 12 pots
destination-pattern 1404.....
port 0:D
prefix 1404
!
dial-peer voice 13 pots
destination-pattern 1512.....
port 0:D
prefix 1512
!
!User with account number matching 875.... is a roaming caller
!
settlement roam-pattern 875.... roam
!
!Enable roaming for this settlement provider using the "roaming" attribute
!
settlement 0
type osp
url https://1.14.115.100:8443/
device-id 2000
customer-id 1000
roaming
no shutdown
!
!
interface Ethernet0
ip address 1.14.115.85 255.255.0.0
no ip directed-broadcast
no ip mroute-cache
no cdp enable
!
interface Serial0:23
no ip address
```

```

no ip directed-broadcast
dialer-group 1
isdn switch-type primary-5ess
isdn protocol-emulate user
isdn incoming-voice modem
fair-queue 64 256 0
no cdp enable
!
interface FastEthernet0
no ip address
no ip directed-broadcast
no ip mroute-cache
shutdown
duplex auto
speed auto
no cdp enable
!
router igrp 200
network 1.0.0.0
!
ip default-gateway 1.14.0.1
ip classless
ip route 172.16.0.0 255.255.0.0 1.14.115.65
no ip http server
!
no cdp run
!
line con 0
logging synchronous
transport input none
line aux 0
line vty 0 4
password lab
login
!
scheduler interval 1000
end

```

Settlement with PKI Multiple Roots Example

The following example shows configuration of settlement with PKI Multiple Roots on the settlement server. As shown in the example, the router has been enrolled under VeriSign TestDerive CA. It has confided Netscape CMS as a trusted root. The Netscape CMS is installed on the server Cisco ca-ultra.

```

version 12.2
service timestamps debug datetime
service timestamps log datetime
no service password-encryption
service internal
!
hostname as5300-04
!
enable secret 5 $1$Ld7z$CapnZCfz2kMSh8sMHh2hy0
enable password lab1
!
resource-pool disable
!
ip subnet-zero
ip domain-name fieldlabs.cisco.com
ip name-server 172.16.2.132
!

```

```

isdn switch-type primary-5ess
isdn voice-call-failure 0
cns event-service server
mta receive maximum-recipients 1024
!
crypto cisco algorithm des
crypto cisco algorithm des cfb-8
crypto cisco algorithm 40-bit-des
!
!Configure the second root to be downloaded from tftp server
!
crypto ca trusted-root transnexus2
root tftp 1.14.115.100 onsite_ca.der
!
crypto ca identity transnexus
enrollment retry count 100
enrollment retry period 2
enrollment url http://hostname
crypto ca certificate chain transnexus
certificate ca 0171
3082024C 308201B5 02020171 300D0609 2A864886 F70D0101 04050030 6E310B30
09060355 04061302 55533110 300E0603 55040813 0747656F 72676961 31183016
06035504 0A130F54 72616E73 4E657875 732C204C 4C433114 30120603 55040B13
0B446576 656C6F70 6D656E74 311D301B 06035504 03131454 52414E53 4E455855
53204245 54412043 41203130 1E170D39 39303332 32313334 3630395A 170D3030
30333231 31333436 30395A30 6E310B30 09060355 04061302 55533110 300E0603
55040813 0747656F 72676961 31183016 06035504 0A130F54 72616E73 4E657875
732C204C 4C433114 30120603 55040B13 0B446576 656C6F70 6D656E74 311D301B
06035504 03131454 52414E53 4E455855 53204245 54412043 41203130 819F300D
06092A86 4886F70D 01010105 0003818D 00308189 02818100 B1B8ACFC D78F0C95
0258D164 5B6BD8A4 6F5668BD 50E7524B 2339B670 DC306537 3E1E9381 DE2619B4
4698CD82 739CB251 91AF90A5 52736137 658DF200 FAFEF66B 7FC7161D 89617E5E
4584D67F F018EDAB 2858DDF9 5272F108 AB791A70 580F994B 4CA54F08 38C32DF5
B44077E8 79830F95 96F1DA69 4CAE16F2 2879E07B 164F5F6D 02030100 01300D06
092A8648 86F70D01 01040500 03818100 2FDCB580 C29E557C 52201151 A8DB5F47
C06962D5 8FDA524E A69DE3EE C3FE166A D05C8B93 2844CD66 824A8859 974F22E0
46F69F7E 8027064F C19D28BC CA750E4E FF2DD68E 1AA9CA41 8BB89C68 7A61E9BF
49CBE41E E3A42B16 AAEDEAEC7 D3B4F676 4F1A817B A5B89ED8 F03A15B0 39A6EBB9
0AFA6968 17A9D381 FD62BBB7 A7D379E5
quit
certificate B7DD210B9BFE007E41EEB177AF39F78C
30820247 308201B0 A0030201 02021100 B7DD210B 9BFE007E 41EEB177 AF39F78C
300D0609 2A864886 F70D0101 04050030 6E310B30 09060355 04061302 55533110
300E0603 55040813 0747656F 72676961 31183016 06035504 0A130F54 72616E73
4E657875 732C204C 4C433114 30120603 55040B13 0B446576 656C6F70 6D656E74
311D301B 06035504 03131454 52414E53 4E455855 53204245 54412043 41203130
1E170D39 39303430 36313833 3635325A 170D3030 30343036 31383336 35325A30
81873181 84300F06 03550405 13083131 37363837 37353018 06092A86 4886F70D
01090813 0B312E31 342E3131 352E3834 302A0609 2A864886 F70D0109 02161D61
73353330 302D3034 2E666965 6C646C61 62732E63 6973636F 2E636F6D 302B0603
55040314 245B7472 616E736E 65787573 2E636F6D 20475749 443D3130 30302043
5349443D 31303030 5D305C30 0D06092A 864886F7 0D010101 0500034B 00304802
4100C82B 8E4CBD44 06C763FB 1DC1A78F 8D71F1DA 110EDAC3 C9AA6256 6E1BF15B
79E48BEF 741D26CF DEBEACCC FA09D420 F54B76A1 F6CDCE33 02C8D9F7 5873E012
AFC90203 010001A3 0F300D30 0B060355 1D0F0404 030205A0 300D0609 2A864886
F70D0101 04050003 81810056 C05E1151 BE2D5515 624010AE 22F03D58 8BD9F2D3
E037EBC8 376E321A 5C53D4C6 770CE32F CF1CB0F4 2FD44C0D CA8EE22C 2372EE64
349FF062 137A6780 DC554F6A 3BA9F17C 85A7F390 D5B99E35 D7FBF927 75910E9E
992C7052 54AE0887 ED1DEEA0 C6BCA9C4 49F3D98E 4835A5E2 0FD470B6 F6D727A8
8AA0F923 5D60985B F8DD19
quit
crypto ca certificate root transnexus2 DB3882D37891B597970BF0F18B008F13
308201F4 3082015D A0030201 02021100 DB3882D3 7891B597 970BF0F1 8B008F13
300D0609 2A864886 F70D0101 04050030 15311330 11060355 040A130A 5472616E

```

```

734E6578 7573301E 170D3939 30333138 30303030 30305A17 0D303930 33313832
33353935 395A3015 31133011 06035504 0A130A54 72616E73 4E657875 7330819F
300D0609 2A864886 F70D0101 01050003 818D0030 81890281 8100AB91 E2123C3F
E83DE86A 3B8A18DF 750FB756 3034D692 2A363692 721F9E59 6CDB046F AAF9A212
6B4B1033 9DDE94DB B132E768 085376EC 9EC7E2FD 0BB92B43 8FEC1243 35A33F89
41390517 AF2D6D46 2FAAC116 8AE55865 C326C77A 3381C944 5BE107B1 E66CA111
B3560313 A29A0081 201D84C5 FE24E452 6338C52C EFDE6B95 4A570203 010001A3
44304230 22060355 1D11041B 3019A417 30153113 30110603 55040313 0A4F6E73
69746532 2D363230 0F060355 1D130408 30060101 FF020100 300B0603 551D0F04
04030201 06300D06 092A8648 86F70D01 01040500 03818100 481E4F13 79EB3B5F
D9BCEED9 9C756BF7 B42167B1 4DE11B8C 240D3446 5A14E2E1 A79D2454 1EA84109
17EF6E8E 8AFD06C7 8209753B F760761C EC13A2D6 95348D69 4F73F0D5 9211DD95
0FE00D23 4583002A 242C769E 695FAFD4 EE12D014 580C5DFC F377F3FF F20F25D6
831E4F2B 253DFA9C 8B3E00A8 002F03D7 BC0C19D8 7EA134A6
quit
!
xgcp snmp sgcp
!
controller T1 0
 framing esf
 clock source line primary
 linecode b8zs
 pri-group timeslots 1-24
!
controller T1 1
 clock source line secondary 1
!
controller T1 2
!
controller T1 3
!
voice-port 0:D
!
dial-peer voice 1 pots
 application session
 destination-pattern 5710876
 port 0:D
!
dial-peer voice 7 voip
 destination-pattern +255....
 session target settlement:0
!
dial-peer voice 13 pots
 destination-pattern 1770.....
 port 0:D
 prefix 1770
!
dial-peer voice 1770 voip
 incoming called-number 1770.....
 ip precedence 7
 session target settlement:0
!
dial-peer voice 1650 voip
 destination-pattern +1650.....
 session target settlement:0
!
dial-peer voice 10 voip
 destination-pattern 1408.....
 session target settlement
!
dial-peer voice 1404 voip
 destination-pattern 1404.....
 session target settlement
!

```

```
dial-peer voice 1512 voip
 destination-pattern 1512.....
 session target settlement
!
!Specify which root to use to validate the settlement token
!via token-root-name attribute
!
settlement 0
 type osp
 url https://1.14.115.100:8443/
 retry-delay 2
 device-id 1000
 customer-id 1000
 token-root-ca transnexus2
 no shutdown
!
interface Ethernet0
 ip address 1.14.115.84 255.255.0.0
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
 no cdp enable
!
interface Serial0:23
 no ip address
 no ip directed-broadcast
 dialer-group 1
 isdn switch-type primary-5ess
 isdn protocol-emulate user
 isdn incoming-voice modem
 fair-queue 64 256 0
 no cdp enable
!
interface FastEthernet0
 no ip address
 no ip directed-broadcast
 shutdown
 duplex auto
 speed auto
 no cdp enable
!
router igrp 200
 network 1.0.0.0
!
ip default-gateway 1.14.0.1
ip classless
no ip http server
!
no cdp run
!
line con 0
 logging synchronous
 transport input none
line aux 0
line vty 0 4
 password lab
 login
!
ntp clock-period 17180879
ntp update-calendar
ntp server 1.14.42.23
scheduler interval 1000
end
```

Settlement with UNI-OSP Example

The following configuration example shows UNI-OSP settlement:

```
Router# settlement 0  
Router# type uni-osp  
Router# url 172.16.100.1
```