Open Settlements Protocol Feature Questions and Answers

Open Settlements Protocol and Cisco

Q. What is the Open Settlement Protocol (OSP)?
A. OSP is a client-server protocol defined by the ETSI TIPHON to establish authenticated connections between gateways, and allow gateways and servers to transfer accounting and routing information securely. OSP allows service providers to roll out VoIP services without establishing direct peering agreements with other ITSPs.

The protocol specifies a method for an originating gateway at a subscriber carrier to request a termination point from the OSP server at the clearinghouse organization. The OSP server provides a secure token-based signature to certify to a terminating gateway that the call has been authorized and will be settled. The OSP server provides a secure link between the gateways and server to transfer accounting and routing information. The OSP protocol does not specify the method by which routes are selected by the route server, a function of the OSP server. OSP-based clearinghouses provide least cost and best route selection algorithms based on a variety of parameters their subscriber carriers provide, including cost, quality, and specific carrier preferences.

Q. Why has Cisco implemented OSP?
A. OSP is the only standards-based way to provide inter-carrier settlements for VoIP calls. It is being implemented by all leading gateway and settlement vendors.

Q. What new options do VoIP service providers have using OSP?
A. Access to clearinghouse services who use OSP for route selection. call authorization and call accounting. This widens the options for VoIP service providers wishing to interconnect with other service providers at the IP level.

Voice over IP service providers can also use the technology provided by OSP server companies to establish a clearinghouse function within their own networks for partner interconnection.

Q. What is settlements?
A. Settlements is the process by which two parties agree on what each owes the other. Settlements can be facilitated by a third party, or can be accomplished through a bilateral agreement.

Q. How does OSP facilitate settlements?

A. OSP facilitates settlements by providing a mechanism through which parties who may not trust each other can be guaranteed that calls accepted will be paid for. With OSP, each service provider to trust the settlement provider only, and the service provider guarantees payment. This is an important function, particularly when interconnecting with new service providers with limited credit history, or service providers in other countries where there may be significant risk of currency fluctuation.

Q. How are ITSPs billed in a settled environment?

A. All inter-carrier billing is done through the settlement provider and the settlement provider guarantees payment to the creditor.

Q. If I have my own billing system, how does this interact with the settlement provider?

A. The bill from the settlements provider can be audited by comparing calls reported to your internal billing system via RADIUS CDRs to the bill using the Call ID which is common to both CDRs.

Q. Is the OSP Protocol an open standard?

A. Yes. This release implements the ETSI TIPHON Technical Specification 101321 version 1.4.2 of the OSP specification. This specification was approved by ETSI on December 1998. For more information check the ETSI web site at

http://www.etsi.org

Q. Is OSP likely to be widely adopted?

A. Yes. In addition to Cisco, Ascend and 3Com have announced plans to implement OSP. GRIC Communications and TransNexus LLP have announced Clearinghouse services products using OSP.

Q. Is OSP Development continuing?

A. Yes. ETSI TIPHON recently reconvened in Bangkok in May 1999 to discuss version 2.0 of the specification. Version 2.0 is expected to be approved by the committee by December 1999.

Q. What new features have been added to CISCO IOS™?

A. Cisco has implemented an Open Settlements Protocol (OSP) client application into the AS5300, C2600 and C3600 series voice over IP gateways. Cisco worked closely with OSP Server partners GRIC Communications and TransNexus LLC in this development. This has been field-tested and proven compatible both the GRIC Communications and TransNexus OSP Server applications.

Clearinghouse Services

Q. What are the functions of a clearinghouse?

A. Call routing, call authorization, settlement and billing.

- Call routing: selecting a route from among the possible routes available at interconnecting carriers using least cost routing and/or parameters indicated by the member service provider and communicating that termination address back to the originating gateway.
- Call authorization: pre-authorizing an incoming call attempt and communicating to the terminating party that the call is authorized and will be paid for.
- Settlement and billing: accounting for the net of each interconnecting service provider's credits and debits, collecting any net liability from each service provider, and distributing any net credit owed.

Q. What are the key benefits to the service provider of using a clearinghouse service?

A. Clearinghouse services provide both a business and technical bridge to extend the reach of the service beyond the boundaries of the service providers' own network. The service providers signs on with a clearinghouse service, and immediately has access to the entire clearinghouse network of affiliated carriers for interconnection.

The benefits include:

- Enables VoIP end to end
- Increase service marketability by providing cost effective coverage to a wider calling area
- Reduced receivables risk: the clearinghouse authorized calls are guaranteed to be settled
- Incremental revenue from terminating calls from other service providers
- Single negotiation with the settlement provider instead of dozens or hundreds of bilateral agreements
- Outsources the task of maintaining the complex rating and routing tables for interconnection to the clearinghouse
- Flexibility in selecting appropriate termination points, considering cost, equipment, and service quality metrics, allowing increased flexiblity in meeting service provider service definition goals
- Immediate access to new and profitable international calling

Q. What are the benefits using OSP for clearinghouse communications?

A.

- OSP uses proven standard technologies for message privacy and signatures.
- OSP is not protocol specific, so the same mechanism and applications can be used to settle calls using different signaling protocols, including H.323 or SIP.
- Because OSP is a well-defined specification based on two widely implemented security technologies (XML and SSL), interoperable implementations are relatively easy to accomplish.
- With OSP, both the originating and terminating gateways submit CDRs to the settlement server, resulting in accurate billing even in failure scenarios.

Q. What is the process of subscribing to and interconnecting with an OSP clearinghouse?

A. In order to subscribe to a clearinghouse service:

- The ITSP system administrator installs OSP software on the gateways, and configures and enables the Cisco Enrollment Protocol on each gateway.
- ITSP activates the account with the clearinghouse, specifying desired route selection policy, and asking price for termination service to the gateway.
- If the ITSP intends to accept incoming traffic from the clearinghouse, the system administrator enters information into the OSP server system indicating the service providers route ratings for termination services (asking prices) for each terminating gateway (each IP address).
- The clearinghouse administrator will tell you if you need to contact a third party certificate authority and obtain a certificate for your gateways, or if the clearinghouse will do that for you.
- (If using Transnexus, the ITSP system administrator must also configure in a unique gateway ID supplied by Transnexus.)
- Then, the Cisco Enrollment Protocol on the gateways automatically registers them to the OSP server.

Q. What questions should a service provider ask when evaluating clearinghouse services?

A. Key questions to ask and factors to evaluate when looking at a clearinghouse service include:

- Does the clearinghouse support Cisco VoIP gateways?
- Does the clearinghouse identify and authorize your use of termination points on other service providers networks, in addition to settling the accounts, or do you have to establish those agreements yourself?
- Geographic coverage the clearinghouse can provide.
- Volume of traffic the clearinghouse can handle from your network, particularly on the routes you expect high volume on: location and number of VoIP gateway ports available for terminating calls.
- Volume of traffic flowing through the clearinghouse is a consideration if the service provider is expecting to get minutes for termination on its own network.

- Quality of the clearinghouse subscribers. Are there other member networks whose networks you would want your traffic to terminate on? Does the clearinghouse have quality standards or ratings for members?
- How sophisticated is the clearinghouse in selecting routes for you?
- Will the clearinghouse agree to accept and terminate all the traffic you need to send, or will some termination requests be refused either because of the limited footprint of the clearinghouse or resource unavailability?
- What tools and reports are available for you to monitor your account status with the clearinghouse?
- How comfortable are you with the clearinghouse plans for maintaining service reliability?
- What is the clearinghouse business model? How much will the clearinghouse charge you for its services?
- What migration plan is available for you should you choose to migrate towards a corresponding-partnership model from the clearinghouse subscriber model?

Q. How does the gatekeeper-based clearinghouse model compare to OSP?

A. H.323 RAS is designed for route selection within a domain, and it performs that function well. H.323 RAS interdomain often does not work well because gatekeeper to gatekeeper communications has not been adequately specified in H.323. OSP is designed for inter-domain route selection.

There are a number of proprietary gatekeeper-based clearinghouse implementations in the market today. The clearinghouse function is not part of the H.323 protocol suite. However, a clearinghouse application can be implemented on top of H.323. Existing H.323-based clearinghouse applications either extend H.323 messages or make use of some fields in a proprietary fashions: as such this represents a vertical closed application suite which uses H.323 as transport between applications.

In a gatekeeper-based clearinghouse model, the demarcation between the originating service provider and the clearinghouse is between two gatekeepers. This has the advantage that only the gatekeepers need to be configured with the other network's information, and this architecture can support H.323 terminals as well as gateways. This design is of course limited to H.323 implementations, whereas OSP is not. The a key disadvantage of the H.323 gatekeeper solution today is that, because H.323 does not clearly specify gatekeeper to gatekeeper communications, the available implementations are necessarily proprietary and non-interoperable. Security methods used for gatekeeper-authorized interconnections vary widely, and are non-standard.

OSP Settlements Solution Detailed Features

Q. Can an OSP server use multiple certificate authorities?

A. Not at this time. One of the enhancements being considered for the next release of the Cisco OSP support is support for multiple root certificates. This allows the OSP server to use one certificate for the SSL connection and a stronger certificate to sign the tokens.

Q. Can a service provider work with multiple OSP-based clearinghouses?

A. No, multiple clearinghouses are not supported yet. This feature is being considered for a future release. In theory, the 1.4.2 version of the OSP protocol could support this.

Q. What certificate authorities are supported?

A. The Cisco Enrollment Protocol has been tested and validated with the Verisign and Entrust certificate authorities, and testing is underway with the Netscape certificate authority. GRIC is using the Netscape certificate authority and TransNexus is using the Verisign certificate authority.

Q. Can OSP be used for intra-net route authorization and route selection?

A. Yes, an OSP server could be used in place of a gatekeeper for internal service provider route selection. This may be particularly appropriate where there is concern about the security of the internal network, and the signature and tokens provided by the OSP messages are required. The chief limitation of this approach is that the OSP protocol does not provide for resource availability messages from the VoIP gateways, and therefore would not know which gateways were busiest. H.323 v2 does include a message called the RAI or Resource Availability Indicator, which Cisco is supporting in Cisco IOS 12.0(5)T.

Q. Can you combine OSP for intra-carrier route selection and H.323 RAS for inter-carrier route selection?
A. Yes. It is possible to configure a Cisco VoIP gateway to first check the originating provider's own network for a termination point, by querying the local gatekeeper, and only then to proceed to query the clearinghouse. OSP and H.323 RAS must be configured on different dial peers, which can be ordered so that the gateway tries to find a match with the first one on the list before proceeding to the second.

Q. Can service providers use OSP to build least cost routing policies in a VoIP network?
A. Definitely, though the actual assignment of costs and route selection is out of the scope of the protocol.

With OSP, service provider queries a clearinghouse database receive multiple routes which match the service providers criteria. The actual route costing and route selection is determined by a higher layer application: OSP is used for transporting such information, not determining it.

Q. Can you use OSP settlements and H.323 RAS on the same gateway at the same time?
A. Yes. The gateway can use H.323 RAS to communicate with gatekeepers and OSP to communicate with OSP servers.

Q. How does the route selection, call authorization and call set-up work in a mixed H.323 gatekeeper and OSP scenario?
A. The following describes a scenario in which a service provider tries to identify a termination point within its own network first, using H.323 RAS, and when it determines that this call should terminate outside this network, then contacts a clearinghouse to identify a termination point with another carrier.

1. Call arrives at the originating VoIP gateway.
2. The gateway searches the dial peer configuration.
3. If the first dial peer is configured as RAS session target, it will route the request to the gatekeeper in an ARQ message.
4. The gatekeeper may reject the request if the destination address does not fall within the gatekeeper system.
5. The gateway searches for a second dial peer, finding one with an OSP session target. If it doesn't have one already, the gateway establishes an SSL connection with the OSP clearinghouse.
6. The gateway sends an AuthorizationRequest (timestamp, callid, sourceinfo, destinationInfo, Maximumdestinations) to the OSP server.
7. The OSP server uses its algorithms to select up to three destination addresses.
8. The clearinghouse creates an authorization token by signing the destination addresses using the clearinghouse certificate and the clearinghouse private key.
9. The OSP server responds with an AuthorizationResponse (Timestamp, Status, TransactionId, Destination) specifying up to three destination addresses as requested by the gateway in the MaximumDestinations parameter.
10. The originating gateway will use the first IP address to intiate a call the destination gateway including the token from the clearinghouse in the H.323 set up message.
11. If the first terminating gateway does not have the resources to provide the service, the originating gateway will try the second IP address received from the OSP server.
12. Once the terminating gateway accepts the call, it will validate the token to ensure the caller is authorized by the clearinghouse. No communication with the clearinghouse is needed to do the validation: the terminating gateway can validate the clearinghouse' signature using the clearinghouse's public key.
13. Once the token is validated, the gateways establish the voice path.
14. At the end of the call, both originating and terminating gateways send the following CDR information to the OSP server: UsageIndication (Timestamp, Role, TransactionID, CallID, SourceInfom DestinationInfom, UsageDetail).
15. The OSP will response to both the gateways with UsageConfimation (TimeStamp, Status).

Q. How does OSP simplify dial plan administration across multiple service providers?

A. Without a clearinghouse to select termination points, the originating service provider would have to pre-configure their corresponding partners' termination addresses into their network. With OSP, the originating service provider merely configures the address of the OSP server at the clearinghouse into each participating gateway, and the OSP server will provide the address of the terminating gateway.

Q. Can you support pre-paid calling services with OSP?

A. OSP could support pre-paid calling card services with a re-authorization transaction, which allows you to refresh an authorization, but H.323 has no such refresh mechanism.

Q. Can you support roaming users with an OSP clearinghouse?

A. The OSP specification supports roaming, but the initial release of the Cisco implementation does not.

Q. What elements of this solution are secure or encrypted and why?

A. The connection between the gateway and the OSP server is secure and encrypted. This prevents spoofing and provides non-repudiation, and protects sensitive account information from sniffing.

The H.323 signaling between the gateways is secure in that the token that is propagated between them certifies that the OSP clearinghouse has authorized the call, but the H.225 and H.245 signaling is not encrypted.

The voice path is neither secure nor encrypted.

Availability and Ordering

Q. What releases and images will include OSP?

A. First release will be in 12.0(4)XL scheduled for First Customer Ship in July 1999 on the AS5300, 26x0 and 36x0 series gateways.

Platform	Images	Memory Requirements	Releases
Cisco 26x0	c2600-js56i-mz		12.0(6)T
Cisco 36x0	c3620-js56I-mz c3640-js56i-mz		12.0(6)T
Cisco AS5300	c5300-js56I-mz	64MB DRAM, 16MB FLASH	12.0(4)XL, 12.0(6)T

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems Europe s.a.r.l.
Parc Evolic, Batiment L1/L2
16 Avenue du Quebec
Villebon, BP 706
91961 Courtaboeuf Cedex
France
http://www-europe.cisco.com
Tel: 33 1 69 18 61 00
Fax: 33 1 69 28 83 26

Americas
Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Headquarters
Nihon Cisco Systems K.K.
Fuji Building, 9th Floor
3-2-3 Marunouchi
Chiyoda-ku, Tokyo 100
Japan
http://www.cisco.com
Tel: 81 3 5219 6250
Fax: 81 3 5219 6001

Cisco Systems has more than 200 offices in the following countries. Addresses, phone numbers, and fax numbers are listed on the **Cisco Connection Online Web site at http://www.cisco.com/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Canada • Chile • China • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE Finland • France • Germany • Greece • Hong Kong • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Singapore Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela

5/99 LW