DCL V2.0 Performance Test Report

Abstract: OpenOSP is an open source server implementation of the Open Settlement Protocol (OSP). The code was implemented by Data Connection Limited (DCL). This document provides the test results for the V2 final release.

Table of Contents

A. INTRODUCTION 1

V2.0 Final Release 1

V2.0 Final Release Testing 2

B. TEST RESULTS 2

Performance 2

Stress 3

Capabilities Messages 3

Cisco Extension Audit Signal S/MIME Support 5

C. NOTES 5

D. DEFINITIONS 6

E. REFERENCES 7

Primary references 7

Secondary references 7

A. Introduction

OpenOSP is an open source implementation of an Open Settlement Protocol- (OSP-) based server. The current release, V2.0, completes the implementation of all messages and features stipulated in the final OSP V2.1.0 specification.

Note: V2.0 is the final release of the OpenOSP software. No bug fixes or support for OSP specifications beyond V2.1.0 has been planned at this point in time.

The goal of Data Connection Limited (DCL) testing is:

- To determine the performance of the OpenOSP stack in terms of maximum call rate
- To verify completeness of the features from a stand-alone open source OSP server and from a Certification Authority (CA)
- To verify the robustness of the DCL product while inter-operating with a Cisco AS5300 gateway

V2.0 Final Release

This document provides the test results for the V2.0 final release. Features advertised by DCL for this release include:

- All OSP messages (OSPv1 and OSPv2)
  AuthorizationConfirmation, AuthorizationIndication, AuthorizationRequest, AuthorizationResponse, CapabilitiesConfirmation, CapabilitiesIndication, PricingConfirmation, PricingIndication, ReauthorizationRequest, ReauthorizationResponse, SubscriberAuthenticationRequest, SubscriberAuthenticationResponse, UsageConfirmation, UsageIndication
- Token signing with all ciphers
- Secure Socket Layer/Transport Layer Security (SSL/TLS) security with all ciphers
- Secure Multipurpose Internet Mail Extensions (S/MIME) security with all the ciphers
- Full Simple Certificate Enrollment Protocol (SCEP) support
- Full multi-threaded operation including support for symmetric multi-processor systems
- Multiple Root
- Roaming
- Full Support for Cisco Extensions to allow the use of supported protocol types in Client CapabilitiesIndication messages and routing decisions
- Stack support for Cisco extensions for authorization of prepaid subscribers.

V2.0 Final Release Testing

Testing for V2 final release was focused on the following areas:

- Stress /Performance testing
  The testing was mainly executed with tools that DCL provided, with or without the crypto-accelerator integration.
- Features testing.
  OSPv2: Capabilities messages

Features not tested

- The following OSPv1 messages were not tested due to the lack of support in the OSP client:
  AuthorizationConfirmation, AuthorizationIndication, PricingConfirmation, PricingIndication, ReauthorizationRequest, ReauthorizationResponse.
- The following OSPv2 messages were not tested due to the lack of support in the OSP client:
  SubscriberAuthenticationRequest, SubscriberAuthenticationResponse.
- S/MIME testing was limited due to some inter-operability problems.

B. Test Results

Performance

Those performance numbers were obtained from scripts provided by DCL. When deployed, these scripts determined the maximum call rate by generating a high numbers of calls and calculating the time that OpenOSP takes to process all of the messages. Each call generated by the scripts included 3 messages, which are a combination of an AuthorizationRequest/AuthorizationResponse message plus 2 UsageIndication/UsageConfirmation messages.

Samplapp is the sample application provided by DCL, and includes all components, including access to a Lightweight Directory Access Protocol (LDAP) directory and verification of the signature.

Testapp is a modified version of samplapp without all time-consuming application processing, and is used to test the OpenOSP stack.

The crypto accelerator used for some test cases was a Crypto Swift EN/200, processing up to 200 calls per second (cps). The Ultra 60 used for the test has two 450MHz processors and a SPECint rating of 19.7. The Ultra 5 has one 360MHz processor and a SPECint rating of 12.1.

Note: SPECint is a processor-intensive benchmark that evaluates desktop performance using a representative mix of application instructions.

Hardware	OpenOSP application	SSL	Token Signing	Crypto accelerator	Maximum Call rate
Ultra 60	samplapp	Y	Y	N	53

Hardware	OpenOSP application	SSL	Token Signing	Crypto accelerator	Maximum Call rate
Ultra 60	samplapp, directory results cached	Y	Y	N	57
Ultra 60	samplapp	Y	Y	Y	198
Ultra 60	samplapp	Y	N	N	294
Ultra 5	samplapp	Y	N	N	19
Ultra 5	samplapp	Y	N	N	34
Ultra 60	testapp	Y	Y	N	800
Ultra 5	testapp	Y	Y	N	110

Stress

The stress testing was mostly completed with scripts provided by DCL.

Test	Result
Run the maximum number of calls using the DCL scripts: 80,000 calls at the same time, using 64 SSL connections with 1250 calls each, without the Crypto accelerator.	OK. It took about 35 minutes for OpenOSP to process these calls.
Run the maximum number of calls using the DCL scripts: 80,000 calls at the same time, using 64 SSL connections with 1250 calls each, with the Crypto accelerator.	OK. It took about 9 minutes for OpenOSP to process these calls.
Run the test with AS5300, instead of using the scripts, at 4 cps.	OK. The CPU utilization on the workstation was very low for this call rate, on both Ultra 5 and Ultra 60 (about 10% for Ultra 60, 20% for Ultra 5). The CSR was very higher than 99%

Capabilities Messages

Capabilities messaging is a new capability provided by OSP version 2. The Capabilities Indication message used by OSP clients indicates the highest OSP version it is willing to support, as well as the specific capabilities it is configured to use.

Test	Result
Configure a OSP v1-only gateway to work with the OpenOSP version 2 server. Make a basic call.	OK
Enable “Shutdown/no shutdown” settlement in the gateway, check	OK

Test	Result
CapabilitiesIndication and CapabilitiesConfirmation messages during the settlement initialization phase.	
Configure call threshold at the gateway, and then trigger the gateway. Send out a CapabilitiesIndication message when AlmostOutOfResource is true.	OK.
Verify the CapabilitiesConfirmation response messages from the OSP server that reply to the AlmostOutofResource CapabilitiesIndication messages.	OK
After the AlmostOutOfResource Capabilities message is received from one gateway, OpenOSP server should not route new calls to the gateway .	New incoming calls still be routed to the gateway. This behavior can be changed by modifying the OSP server code.
After the AlmostOutOfResource Capabilities message is received from one gateway, if other routes exist, the OSP server will select one of them as a "best choice" rather than the gateway that sent an AlmostOutOfResource message. Two gateways were configured at the OSP server to terminate same destination numbers. One has a higher price rate with available resources. The other has a lower price rate but has sent an AlmostOutOfResource message to the server.	OK The OSP server choose the higher priced gateway as the first route, and chose the AlmostOutOfResource gateway as the last route.
When gateway resource is available again, an AlmostOutOfResource = false message is sent to the OSP server.	OK
Verify the CapabilitiesConfirmation message for false AlmostOutOfResource messages.	OK
New calls can be routed to the gateway as they become available.	OK The OSP server choose the lower priced gateway as the first route.

Cisco Extension Audit Signal S/MIME Support

The Cisco extension, AuditSignal with S/MIME, is used to sign the actual Call Detail Records (CDRs) sent by the voice gateway to offer proof to the provider that the settlement service was rendered. The Cisco gateway sent signed UsageIndication messages only if the server embedded the audit start and stop signals in the Hyper-text Transfer Protocol (HTTP) status code.

Test	Result
Configure the OSP server to embed the audit start message in the HTTP response. There are no configuration options available for this feature. The feature support can only be activated by re-compiling the OSP server with altered source code. In the supplied sample application, osp_um_response() is called from sua_cb() in samplapp/suamain.c. The value of the audit_signal must be changed from 0 to OSP_UM_AUDIT_START.	OK.
The OSP server has the ability to embed the audit start/stop message for certain selected gateways.	This is not available at current OSP server sample application. As the AuditSignal element needs to be setup dynamically by the server, it is controlled programmatically by the audit_signal parameter on the osp_um_response() call. The sample OSP server can be modified to accomplish this test.
Verify that the Cisco extension element <cisco.com:AuditSignal> is embedded into the UsageConfirmation message sent by the OSP server.	OK
The OSP server sends back a confirmation message for incoming S/MIME signed UsageIndication messages.	Failed The OSP server reported a Bad Signature for incoming S/MIME messages.
Verify that the CDRs abstracted from S/MIME signed message are correct.	Failed No CDR was generated due to the failure of the previous test.

C. Notes

“Gateway” in this test document refers to a Cisco voice gateway with OSP support.

The reason for S/MIME test failures has been investigated on both the gateway and the OpenOSP server side. We believe that it is an inter-operability issue.

D. Definitions

BCG	Bulk Call Generator
Callgen	Cisco internal tool allowing to generate/receive calls
CA	Certification Authority
CDR	Call Detail Record
CRL	Certificate Revocation List
DCL	Data Connection Limited. British software company implementing OpenOSP
DN	Distinguished name
IPSEC	Framework of open standards developed by the IETF that provides security for transmission of sensitive information over unprotected networks such as the Internet. It acts at the network level and implements the following standards: IPSec, Internet Key Exchange (IKE), DES, MD5, SHA, Authentication Header (AH), Encapsulating Security Payload (ESP).
ISDN	Integrated Services Digital Network
IVR	Interactive Voice Response
LDAP	Lightweight Directory Access Protocol
MD5	Message Digest 5. MD5 is a secure hashing function that converts an arbitrarily long data stream into a digest of fixed size.
OpenOSP	Open source implementation of a OSP server
OSP	Open Settlement Protocol
OGW	Originating Gateway
PKCS #7	Public Key Cryptography Standard #7. Standard from RSA Data Security Inc., which is used to encrypt and sign certificate enrollment messages. RFC 2315.
PKCS #10	Public Key Cryptography Standard #10. Standard syntax from RSA Data Security Inc, for certificate requests. RFC 2314.
POTS	Plain Old Telephone Service
PRI	Primary Rate Interface: ISDN interface to 64kbps D channel plus 23 (T1) or 30 (E1)B channels for voice or data
PSTN	Public Switched Telephone Network
SCEP	Simple Certificate Enrollment Protocol
SHA	The Secure Hash Algorithm is defined in FIPS PUB 180-1. It produces a 20-byte output
S/MIME	Secure Multipurpose Internet Mail Extensions RFC 2311

SSL	Secure Socket Layer
TIPHON	Telecommunications and Internet Protocol Harmonization Over Networks
TGW	Terminating Gateway
UUT	Unit Under Test
VoIP	Voice Over IP

E. References

Primary references

OpenOSP Product Overview

OpenOSP Interface Specification

OpenOSP Release Notes

[OSPv1] ETSI TS 101 321 v1.4.2 / DTS/TIPHON-03004

[OSPv2] ETSI TS 101 321 v2.1.0 / DTS/TIPHON-03004-2

Secondary references

[PKCS7] Kaliski, B., "PKCS #7: Cryptographic Message Syntax Version 1.5", RFC 2315, March 1998.

[PKCS10] Kaliski, B., "PKCS #10: Certification Request Syntax Version 1.5", RFC 2314, March 1998.

[RFC2459] Housley, R., ec. al., "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", RFC 2459, January 1999.