Cisco Policy Suite 7.0 Troubleshooting Guide

First Published: September 26, 2014

Last Updated: January 02, 2023

Cisco Systems, Inc.
www.cisco.com

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco Policy Suite 7.0 Troubleshooting Guide
© 2015-2023 Cisco Systems, Inc. All rights reserved.

Preface vii

Readers vii

Additional Support vii

Terms and Definitions viii

CHAPTER 1 **Troubleshooting CPS** 1-1

Troubleshooting 1-1

General Troubleshooting 1-1

Trace Support Commands 1-2

trace.sh 1-3

trace_id.sh 1-3

Portal Troubleshooting 1-4

Domain Troubleshooting 1-6

RADIUS Troubleshooting 1-6

E2E Call Flow Troubleshooting 1-6

Troubleshooting Basics 1-6

Gathering Information 1-7

CPS Control Center Interface Guide 1-7

CPS Subscriber Services Admin User Interface Guide 1-8

Diameter Error Codes and Scenarios 1-8

Common Troubleshooting Scenarios 1-10

Scenario - No Response to Diameter Request 1-10

Using TCPDUMP 1-10

CPS Logs 1-10

TCPDUMP – User Id Filter 1-11

No Response – Using Policy Trace 1-12

Policy Trace – Match Response 1-12

Rare Troubleshooting Scenarios 1-13

Recovery using Remove/Add members Option 1-13

Remove Failed Members 1-14

Add Failed Members 1-15

Maintenance Window Procedures 1-17

Prior to Any Maintenance 1-17

Change Request Procedure 1-17

Software Upgrades 1-17
Application Restarts 1-18
VM Restarts 1-18
Hardware Restarts 1-18
Planned Outages 1-18
Non-maintenance Window Procedures 1-19
Common Troubleshooting Tasks 1-19
CPS Trace Monitoring 1-19
Kill All Cisco Processes From the Command Line as Root 1-19
Low or Out of Disk Space 1-21
df Command 1-21
du Command 1-21
Frequently Encountered Troubles 1-22
Subscriber not Mapped on SCE 1-23
CPS Server Will Not Start and Nothing is in the Log 1-24
Server returned HTTP Response Code: 401 for URL 1-24
com.broadhop.exception.BroadhopException: Unable to Find System Configuration for System 1-25
Log Files Display the Wrong Time but the Linux Time is Correct 1-25
JMX Management Beans are not Deployed 1-25
Unable to Access Binding Information 1-26
Error Processing Package, Reference Data Does Not Exist for NAS IP 1-26
REST Web Service Queries Returns an Empty XML Response for an Existing User 1-27
Error in Datastore: "err" : "E11000 Duplicate Key Error Index 1-27
Error Processing Request: Unknown Action 1-28
Memcached Server is in Error 1-28
Firewall Error: Log shows Host Not Reachable, or Connection Refused 1-29
Unknown Error in Logging: License Manager 1-29
Ecore File is Not Generated: 1-29
Logging Does Not Appear to be Working 1-30
Cannot Connect to Server Using JMX: No Such Object in Table 1-31
File System Check (FSCK) Errors 1-31
CPS: 27717 Mongo Stuck in STARTUP2 after sessionMgr01/2 Reboot 1-34
SR: 628099455 System Failure Errors in Control Center 1-36
Multi-user Policy Builder Errors 1-39
Not able to do any edits after login 1-39
Error in login due to conflict 1-39
No configuration visible in Policy Builder after login 1-40
Exception Occured During Login 1-41
Debug Details 1-41

Policy Reporting Configuration not getting updated post CPS Upgrade 1-41
CPS Memory Usage Increased 1-42
Detect and Reclaim Cached Memory 1-42
Errors while Installing HA Setup 1-43
Enable/disable Debit Compression 1-45
Diameter proxy error in diagnostics.sh output 1-46
Portal Landing page is slow (or) not getting redirected to Portal 1-47
Not able to Publish the Policy in Policy Builder 1-48
CPS not sending SNMP traps to External NMS server 1-49
Diameter Peer Connectivity is Down 1-50
SNMP Traps and Key Performance Indicators (KPIs) 1-50
Full (HA) Setup 1-50
All-in-one (AIO) Setup 1-52
Traps Generated by CPS 1-53
Component Notifications 1-53
Application Notifications 1-56
Components and KPI Values 1-61
Component Values 1-61
KPI Values 1-62
FAQs 1-64
Reference Document 1-66
Puppet based VM Installer Troubleshooting 1-66
Enable Custom Puppet to Configure Deployment 1-67
Deployed Node is not able to access Cluster Manager VM 1-69
Not Able to Deploy VM 1-69
VMs are not able to Communicate with each other 1-69
CSCuq83755 — Policy builder is losing repositories 1-69
CSCuq02899 — create_policy_builder_user.sh does not add read-only user 1-70
Not able to access IPv6 Gx port from PCEF/GGSN 1-70
CSCuq55352 — Mongo Session db reboots into STARTUP Mode 1-70

CHAPTER 2 **Check Subscriber Access** 2-1
Checking Access 2-1
Testing Subscriber Access with 00.testAccessRequest.sh 2-1
Testing Subscriber Access with soapUI 2-2
Testing for ISG Functionality and Connectivity with test aaa Scripts 2-6

CHAPTER 3 **TCP Dumps** 3-1
TCPDUMP Command 3-1

Options 3-1
To Specify Multiple Ports 3-1
Verbose Mode 3-2
Even more Verbose Mode 3-2
Restrict to a Specific Interface, such as eth0 3-2
Redirect Output of the Command to a File 3-2
More options 3-2
Specific Traffic Types 3-2
Capture RADIUS Traffic 3-2
Capture SNMP Traffic 3-2
Other Ports 3-3

APPENDIX A **Call Flows** A-1
One-click Call Flow A-2
User/Password Login Call Flow A-4
Data-limited Voucher Call Flow A-6
Time-limited Voucher Call Flow A-9
WISPr Call Flow A-11
EAP-TTLS Call Flow A-13
Service Selection Call Flow A-15
MAC TAL Call Flow A-17
Tiered Services Call Flow A-20
SP WiFi-4.0 Call Flows A-21
Authentication Sequence in WLC Network Device Manager A-22
Authentication Sequence for EAP Requests A-23
Authentication Sequence in iWAG Network Device Manager A-24
MAG Coupled Web Based Authentication A-25

APPENDIX B **Logs** B-1
Logs B-1
Basic Troubleshooting Using CPS Logs B-7
Logging Level and Effective Logging Level B-7

Preface

Welcome to Cisco Policy Suite 7.0 Troubleshooting Guide.

This document describes common methods and scenarios of correcting processing and production functions for the Cisco Policy Suite.

Read about these topics in these sections:

- Readers, page vii
- Additional Support, page vii
- Terms and Definitions, page viii

Readers

This guide is best used by the following readers.

- Deployment engineers
- System administrators
- Network administrators
- Network engineers
- Network operators
- Implementation engineers

This document assumes an intermediate level of understanding of network architecture, configuration, and operations. This document is most helpful if readers have completed Cisco training classes and have a firm introduction to the concepts and behavior of Cisco Policy Suite.

Additional Support

For further documentation and support:

- Contact your Cisco Systems, Inc. technical representative.
- Call the Cisco Systems, Inc. technical support number.
- Write to Cisco Systems, Inc. at support@cisco.com
- Refer to your other documents.

Terms and Definitions

This document uses certain terms and definitions specific to the CPS software application. Please refer to our common Glossary of Terms.

Troubleshooting CPS

Revised: July 10, 2015

This chapter covers the following sections:

- Troubleshooting, page 1-1
- Troubleshooting Basics, page 1-6
- Diameter Error Codes and Scenarios, page 1-8
- Common Troubleshooting Scenarios, page 1-10
- Rare Troubleshooting Scenarios, page 1-13
- Maintenance Window Procedures, page 1-17
- Common Troubleshooting Tasks, page 1-19
- Frequently Encountered Troubles, page 1-22
- SNMP Traps and Key Performance Indicators (KPIs), page 1-50
- Puppet based VM Installer Troubleshooting, page 1-66

Troubleshooting

- Find out if your problem is related to CPS or another part of your network.
- Gather materials that facilitate the support call.

General Troubleshooting

- Are their specific SNMP traps being reported that can help you isolate the issue?
- Run **/opt/broadhop/installer/diagnostic.sh**

```
[root@lab ~]# exec diagnostics.sh
?[H?[2JQNS Diagnostics
Validating hostnames...[?[32mPASS?[0m]
Checking basic ports (80, 11211, 7070, 8080, 27017,
9091, 9092)...[?[32mPASS?[0m]
Checking qns passwordless logins on all
boxes...[?[32mPASS?[0m]
Checking swap space...
Checking swap memory usage on
pcrfclient01...[?[33mWARN?[0m]
Swap usage is 977 MB. This may indicate that the system
```

```
needs more memory allocated. Please monitor closely for
swap usage increase.
If systems memory usage is no longer high, you can reset
swap with: /opt/broadhop/installer/diag/support/
swap2ram.sh
Checking disk usage...[?[32mPASS?[0m]
Checking QNS RADIUS (UDP) ports (1812, 1813)...
Could not connect to port 1812 on qns01 (Radius access
requests)...[?[1;31mFAIL?[0m]
Could not connect to port 1813 on qns01 (Radius
accounting requests)...[?[1;31mFAIL?[0m]
Retrieving QNS diagnostics from
qns01:9045...[?[33mWARN?[0m]
```

- Run **/opt/broadhop/control/statusall.sh**

```
[root@lab ~]# exec statusall.sh
Executing sudo /etc/init.d/qns status on all QNS Servers
lab
qns-1 (pid 21995) is running...
qns-2 (pid 22035) is running...
Connection to lab closed.
```

- From pcrfclient01, run **tail –f /var/log/broadhop/consolidated-qns.log**

  Go to the bottom of the log file and search backwards for 'ERROR'. For more details, see *Cisco Policy Suite 7.0 Alarming and SNMP Guide*.

- Look for stack traces.

```
2013-05-28 05:40:36 Error: [InternalErrorException]
Failed finding location.
#0 /var/www/portal/app/Controller/
SubscribersController.php(1420):
Subscriber->getLocation()
#1 /var/www/portal/app/Controller/
SubscribersController.php(45):
SubscribersController->_setLocationAndProfile()
#2 [internal function]:
SubscribersController->beforeFilter(Object(CakeEvent))
#3 /var/www/portal/lib/Cake/Event/
CakeEventManager.php(246): call_user_func(Array,
Object(CakeEvent))
#4 /var/www/portal/lib/Cake/Controller/
Controller.php(670):
CakeEventManager->dispatch(Object(CakeEvent))
#5 /var/www/portal/lib/Cake/Routing/
Dispatcher.php(100): Controller->startupProcess()
#6 /var/www/portal/lib/Cake/Routing/Dispatcher.php(85):
Dispatcher->_invoke(Object(SubscribersController),
Object(CakeRequest), Object(CakeResponse))
#7 /var/www/portal/app/webroot/index.php(153):
Dispatcher->dispatch(Object(CakeRequest),
Object(CakeResponse))
#8 {main}
```

Trace Support Commands

This section covers the following two commands:

- trace.sh

- trace_id.sh

trace.sh

trace.sh usage:

$0 -i <specific id> -d sessionmgr01:27719/policy_trace

$0 -x <specific id> -d sessionmgr01:27719/policy_trace

$0 -a -d sessionmgr01:27719/policy_trace

$0 -e -d sessionmgr01:27719/policy_trace

This script starts a selective trace and outputs it to standard out.

- Specific Audit Id Tracing

  $0 -i <specific id>

- Dump All Traces for Specific Audit Id

  $0 -x <specific id>

- Trace All.

  $0 -a

- Trace All Errors.

  $0 -e

trace_id.sh

trace_ids.sh usage:

$0 -i <specific id> -d sessionmgr01:27719/policy_trace

$0 -r <specific id> -d sessionmgr01:27719/policy_trace

$0 -x -d sessionmgr01:27719/policy_trace

$0 -l -d sessionmgr01:27719/policy_trace

This script starts a selective trace and outputs it to standard out.

- Add Specific Audit Id Tracing

  $0 -i <specific id>

- Remove Trace for Specific Audit Id

  $0 -r <specific id>

- Remove Trace for All Ids

  $0 -x

- List All Ids under Trace

  $0 -l

Portal Troubleshooting

- Is the right portal page displaying?
- If not, review the consolidated log output to see what network mapping is being applied and what the location query response is back to the portal.
- Fix any network mapping problems through your portal administration GUI. In a web browser go to <IP_address>users/login and log in as administrator.
- Enable API debugging in the portal by modifying the script **/var/www/portal/app/Config/broadhop.php**
- Run **tail -f /var/www/portal/app/tmp/logs/api_request.log**

```
2013-05-28 05:40:36 Api_request: REQUEST:
Array
(
[method] => POST
[body] => <soapenv:Envelope xmlns:soapenv="http://
schemas.xmlsoap.org/soap/envelope/" xmlns:typ="http://
broadhop.com/unifiedapi/soap/types">
<soapenv:Header/>
<soapenv:Body>
<typ:ExecuteActionRequest>
<typ:code>location-query</typ:code>
<typ:arg>
<typ:code>ip-address</typ:code>
<typ:value><![CDATA[127.0.0.1]]></typ:value>
</typ:arg>
<typ:arg>
<typ:code>port</typ:code>
<typ:value><![CDATA[60147]]></typ:value>
</typ:arg>
</typ:ExecuteActionRequest></soapenv:Body></
soapenv:Envelope>
[uri] => Array
(
[scheme] => http
[host] => 127.0.0.1
[port] => 8080
[path] => /ua/soap
)
[header] => Array
(
[Content-Type] => text/xml;charset="utf-8"
[Cache-Control] => no-cache
[Pragma] => no-cache
[SOAPAction] => ""
[Content-length] => 511
)
)
```

- For the older portal version run **tail -f /var/www/portal/app/tmp/logs/qns_calls.log**.
- For the newer portal version run **tail -f /var/www/portal/tmp/logs/api_response.log**.

```
2013-05-28 05:40:36 Api_response: RESPONSE:
object(HttpResponse)#67 (7) {
```

```
["body"]=>
string(1274) "<html>
<head>
<meta http-equiv="Content-Type" content="text/
html;charset=ISO-8859-1"/>
<title>Error 404 Not Found</title>
</head>
<body>
<h2>HTTP ERROR: 404</h2>
<p>Problem accessing /ua/soap. Reason:
<pre> Not Found</pre></p>
<hr /><i><small>Powered by Jetty://</small></i>
</body>
</html>
"
["headers"]=>
array(5) {
["Cache-Control"]=>
string(33) "must-revalidate,no-cache,no-store"
["Content-Type"]=>
string(28) "text/html;charset=ISO-8859-1"
["Content-Length"]=>
string(4) "1274"
["Connection"]=>
string(5) "close"
["Server"]=>
string(21) "Jetty(7.x.y-SNAPSHOT)"
}
["cookies"]=>
bool(false)
["httpVersion"]=>
string(8) "HTTP/1.1"
["code"]=>
string(3) "404"
["reasonPhrase"]=>
string(9) "Not Found"
["raw"]=>
string(1466) "HTTP/1.1 404 Not Found
Cache-Control: must-revalidate,no-cache,no-store
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 1274
Connection: close
Server: Jetty(7.x.y-SNAPSHOT)
<html>
<head>
<meta http-equiv="Content-Type" content="text/
html;charset=ISO-8859-1"/>
<title>Error 404 Not Found</title>
</head>
<body>
<h2>HTTP ERROR: 404</h2>
<p>Problem accessing /ua/soap. Reason:
<pre> Not Found</pre></p>
<hr /><i><small>Powered by Jetty://</small></i>
</body>
</html>
"
}
```

Domain Troubleshooting

- Run **tail –f consolidated-qns.log** from the bottom to determine what domain is being calculated for your call flow.
- The domain calculation comes after the location query response to the portal.
- If the domain calculation is wrong, either the wrong portal has been determined or the wrong domain is associated with your desired portalpage.
- You can fix your domain association through the portal administration page.
- If your domain is correct but the call flow is incorrect after that, access Cisco Policy Builder to review your domain configuration.

RADIUS Troubleshooting

- Test service definition requests from a PEP such as ISG to the CPS by running the following command:

  test aaa group radius L4REDIRECT_SERVICE password legacy

  - Repeat this command for PBHK_SERVICE and OPENGARDEN_SERVICE.
- Listen for RADIUS traffic from the PEP by logging into lb01 and lb02 and run the following command:

  tcpdump –i any port 1812 –s 0 -vvv

Test general subscriber access with the procedures in Check Subscriber Access, page 2-1.

E2E Call Flow Troubleshooting

- On an All-in-One deployment, run the following commands:

  tcpdump –i <any port 80 or 8080 or 1812 or 1700 or 1813 or 3868> –s 0 –vv

  - Append a **–w /tmp/callflow.pcap** to capture output to Wireshark file
- Open the file in WireShark and filter on HTTP or RADIUS to assist debugging the call flow.
- In a distributed model, you need to tcpdump on individual VMs:
  - Load balancers on port 1812, 1813, 1700, 8080 and 3868
  - Portallbs and Portals on ports 80

Correct call flows are shown in Appendix A, “Call Flows”

Troubleshooting Basics

Troubleshooting CPS consists of these types of basic tasks:

- Gathering Information
- Collecting logs

- Running traces

This section also presents CPS-specific tasks:

- Common Troubleshooting Scenarios
- System Maintenance and Recovery
- System Maintenance
- Replacing Hardware

Gathering Information

Determine the Impact of the Issue

- Is the issue affecting subscriber experience?
- Is the issue affecting billing?
- Is the issue affecting all subscribers?
- Is the issue affecting all subscribers on a specific service?
- Is there anything else common to the issue?
- Have there been any changes performed on the CPS system or any other systems?
- Has there been an increase in subscribers?
- Is the issue affecting all subscribers?
- Is the issue affecting all subscribers on a specific service?
- Is there anything else common to the issue?

Initially, categorize the issue to determine the level of support needed.

CPS Control Center Interface Guide

The CPS Control Center interface has screens that help you and your Cisco technical representative diagnose troubles.

1. Access the Control Center interface at **http://<ipserver>:8090** on your server. Here, ipserver is lbvip01.
2. Enter your username and password to log in.
3. Click the Monitoring tab and open the tree on the left to examine:
   - System health
   - Current statistics for your system
   - Trends

For Control Center documentation, locate the Cisco Policy Suite Control Center Interface Guide, document ID 178-266-001-x.x.

CPS Subscriber Services Admin User Interface Guide

The CPS Subscriber Service Portal interface has screens that help you and your Cisco technical representative diagnose troubles with the portal and its interaction with Cisco Policy Builder.

1. Access the Cisco Subscriber Service Portal interface at http://<ipserver>/users/login on your server. Here ipserver is sslvip01.
2. Log in as an admin user.
3. Click Settings and use any of these screens underneath:
   - Configuration Check
   - Location Settings
   - Query Map
   - CPS Logs

For Cisco Subscriber Service Portal documentation, refer to *Cisco Subscriber Services Portal Interface Guide for Administrators*.

Diameter Error Codes and Scenarios

The following table describes some common diameter error codes and scenarios:

Error Code	CPS Scenarios
DIAMETER_ERROR_BEARER_NOT_AUTHORIZED	Emergency service related - Used when the PCRF cannot authorize an IP-CAN bearer upon the reception of an IP-CAN bearer authorization request coming from the PCEF.
DIAMETER_ERROR_TRAFFIC_MAPPING_INFO_REJECTED	Emergency service related - Used when the PCRF does not accept one or more of the traffic mapping filters.
DIAMETER_USER_UNKNOWN	Subscriber not found in SPR.
DIAMETER_AUTHORIZATION_REJECTED	A request was received for which the user could not be authorized.No session created due to various reasons. For example, this error could occur if the service requested is not permitted to the user.
DIAMETER_UNABLE_TO_COMPLY	Message rejected as something else that went wrong and there's no specific reason.
DIAMETER_SUCCESS	Everything went well and Request processed successfully.

Error Code	CPS Scenarios
DIAMETER_TOO_BUSY	Message got discarded by the overload handling mechanism. **Note** CPS 7.0 adds the option to silently discard instead of sending DIAMETER_TOO_BUSY as discarding is often a better way to have other node back off instead of immediately resending the request in an overload scenario.
DIAMETER_UNABLE_TO_DELIVER	Message cannot be delivered, either because no host within the realm supporting the required application was available to process the request or because Destination-Host AVP was given without the associated Destination-Realm AVP.
DIAMETER_APPLICATION_UNSUPPORTED	A request was sent for an application that is not supported.
DIAMETER_UNKNOWN_PEER	A CER was received from an unknown peer.
DIAMETER_UNKNOWN_SESSION_ID	The request contained an unknown Session-Id.
DIAMETER_NO_COMMON_APPLICATION	When a CER message is received, and there are no common applications supported between the peers.
DIAMETER_ERROR_TRIGGER_EVENT	When the set of bearer/session information sent in a CCR originated due to a trigger event been met is incoherent with the previous set of bearer/session information for the same bearer/session.
DIAMETER_PCC_RULE_EVENT	When for some reason the PCC rules cannot be installed/activated. The reason is provided in the Event Trigger AVP value.
DIAMETER_PCC_BEARER_EVENT	When for some reason a PCC rule cannot be enforced or modified successfully in a network initiated procedure. The reason is provided in the Event Trigger AVP value.
DIAMETER_ERROR_UNKNOWN_POLICY_COUNTERS	Error used by the OCS to indicate to the PCRF that the OCS does not recognize one or more Policy Counters specified in the request, when the OCS is configured to reject the request provided with unknown policy counter identifier(s).
DIAMETER_ERROR_NO_AVAILABLE_POLICY_COUNTERS	Error used by the OCS to indicate to the PCRF that the OCS has no available policy counters for the subscriber.

Common Troubleshooting Scenarios

- Scenario - No Response to Diameter Request

Scenario - No Response to Diameter Request

Using TCPDUMP

- Collect tcpdump packet capture from the primary IOmanager:

  tcpdump –i any –port 3868 –s0 –w filename test.pcap

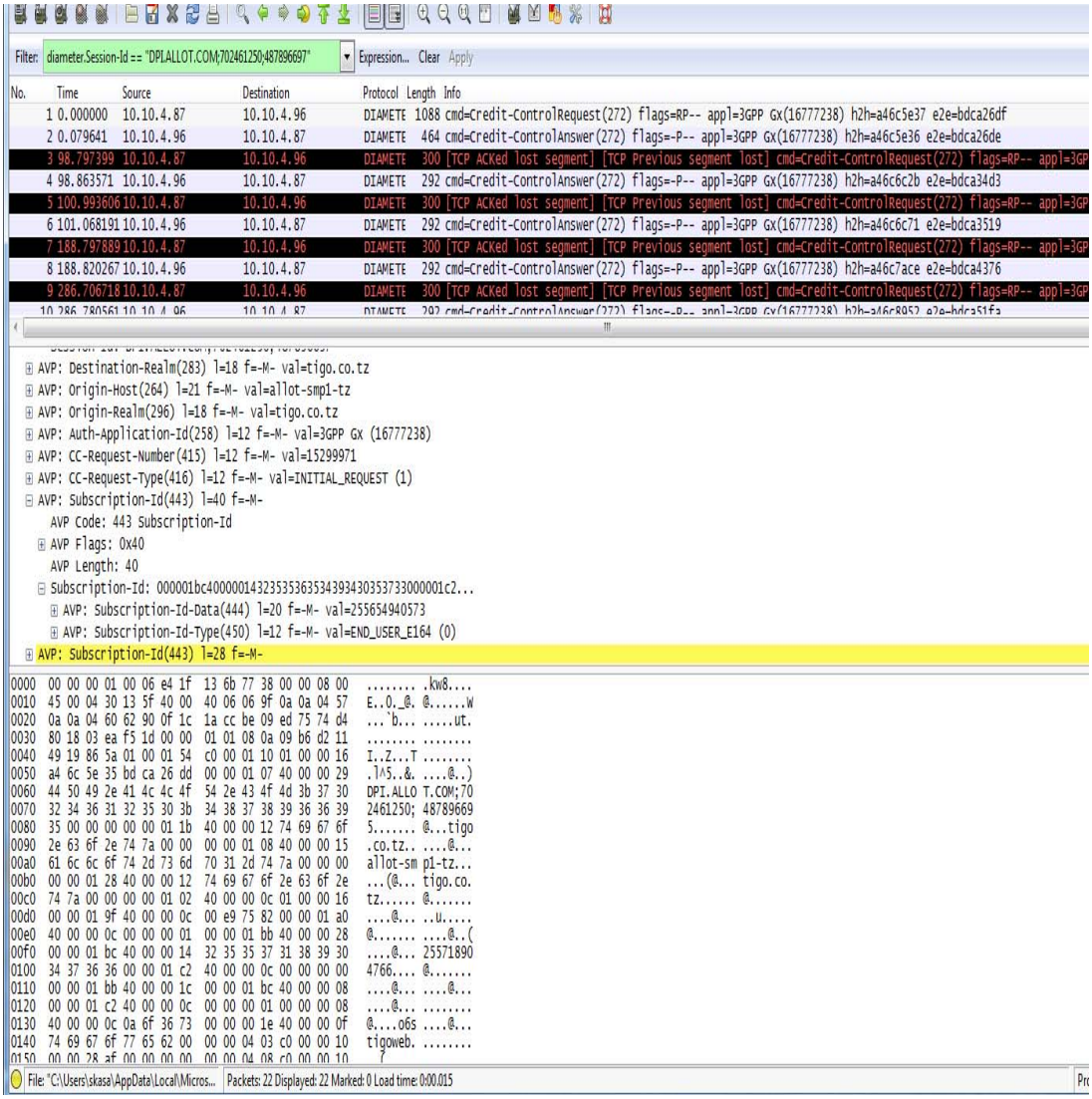
In the collected trace file,

- Verify that the response message is sent back to PCEF.
- Use Session-Id as filter if the Session-Id of the user's session is available.
- If Session-Id for the user is not available, use MSISDN as filter to retrieve the Session-Id. Then apply Session-Id filter to view all the messages for the session.
- Match the request to response for Credit Control Request, CC-Request-Type attribute (Initial/Update/Terminate).

CPS Logs

- Verify the consolidated-qns.log on PCRFCLIENT01 for any exceptions with policy executions, for example, Null Pointer Exception.
- Filter using Session-Id

TCPDUMP – User Id Filter



- Filter using Subscription-Id-Data (MSISDN) to retrieve the CCR initial request
- Start the policy trace for a subscriber using MSISDN as the search string. For example, in a deployment with qns01-04,

```
java -DsearchString=255654940574
-Dservers=qns01,qns02,qns03,qns04 -DtraceLogging=true
-jar traceMonitor.jar &> /var/tmp/policy-trace.log &
```

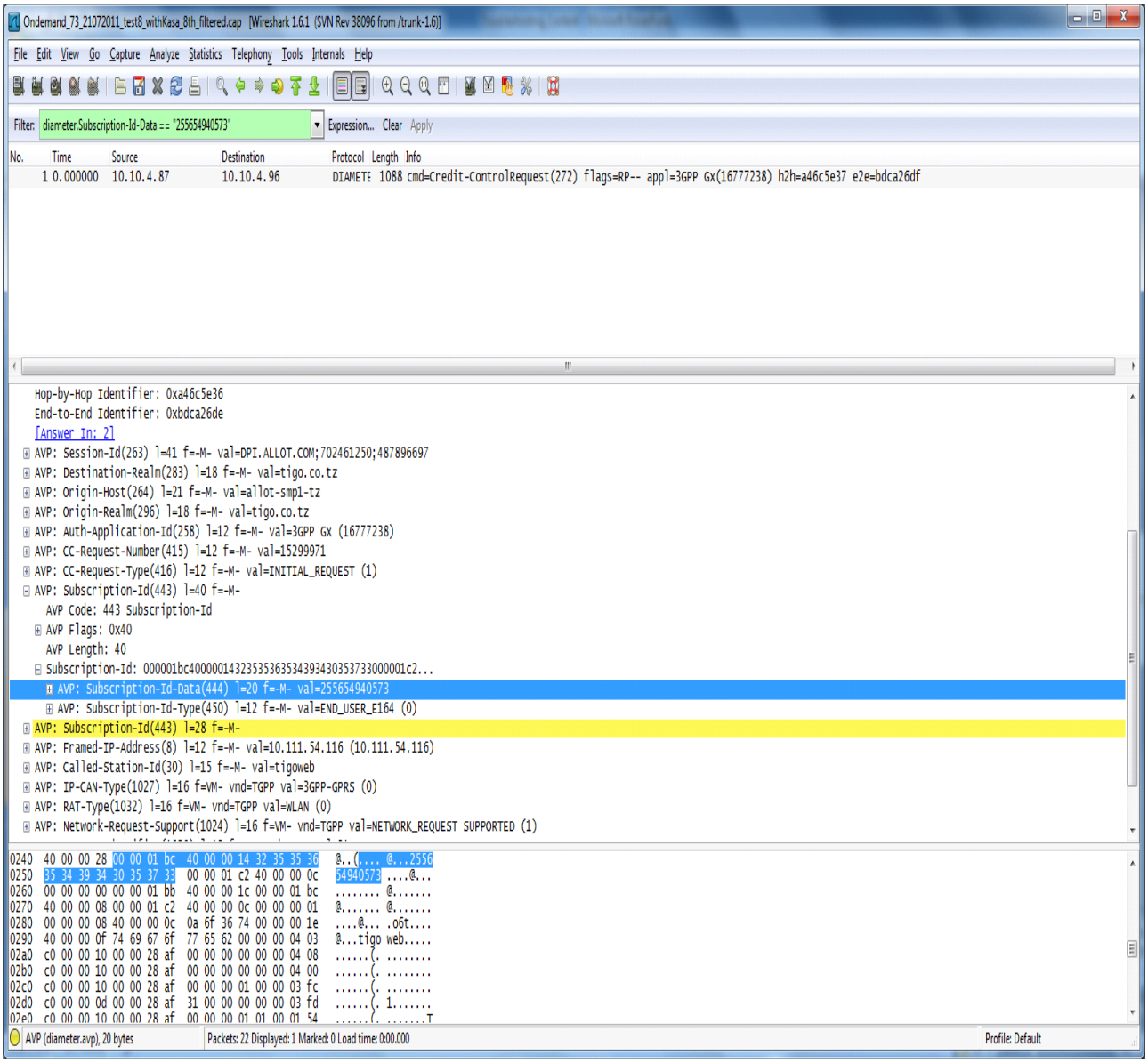
- When a deployment with qns01-06

```
java -DsearchString=255654940574
-Dservers=qns01,qns02,qns03,qns04,qns05,qns06
-DtraceLogging=true -jar traceMonitor.jar &> /var/tmp/policy-trace.log &
```

- The Policy trace logs all policies executed for each message handled for the user.
- Verify the log to match requests and responses using CC-Request-Type attribute in the request/response.

- Verify the log for any policy execution errors.

No Response – Using Policy Trace



Policy Trace – Match Response

Use the search string “Set Diameter Session Key” to identify incoming request

```
[255654940573] Policy executed "Set Diameter Session
Key"[255654940573]Triggering Conditions[255654940573]
Object ID : 21, Class:
com.broadhop.diameter.gx.allot.messages.DiameterCCRMess
age[255654940573]{subIdType=1, calledStationID=tigoweb,
```

```
requestId=bb487926-41c2-459f-aafd-d768cf5abe38#1026576,
msisdn=255654940573, originHost=allot-smp1-tz,
originRealm=tigo.co.tz, stackName=10.10.4.96:3868,
requestType=1, framedIpAddress=10.111.17.98,
bearerOperation=1, requestNumber=10660733,
usageVolume=-1,
sessionId=DPI.ALLOT.COM;702461250;485609944,
bearerIdentifier=1, eventTrigger=[],
chargingRuleReport=[], imsi=,
usageMonitoringControl=[]}
```

- Use the search string “Send Allot Gx Answer Message” to identify matching response

```
[255654940573]Object ID : 21, Class:
com.broadhop.diameter.gx.allot.messages.DiameterCCRMess
age[255654940573]{subIdType=1, calledStationID=tigoweb,
requestId=bb487926-41c2-459f-aafd-d768cf5abe38#1026576,
msisdn=255654940573, originHost=allot-smp1-tz,
originRealm=tigo.co.tz, stackName=10.10.4.96:3868,
requestType=1, framedIpAddress=10.111.17.98,
bearerOperation=1, requestNumber=10660733,
usageVolume=-1,
sessionId=DPI.ALLOT.COM;702461250;485609944,
bearerIdentifier=1, eventTrigger=[],
chargingRuleReport=[], imsi=,
usageMonitoringControl=[]}[255654940573]Policy object
changes: No changes[255654940573]Actions
executed[255654940573]
com.broadhop.diameter.actions.ISendDiameterAnswerSynch
```

Rare Troubleshooting Scenarios

Recovery using Remove/Add members Option

When Arbiter blade and a sessionmgr blade goes down, there wont be any primary sessionmgr node to cater requests coming from CPS VMs (Classic HA setup-1 arbiter, 2 sessionmgrs). As a result, system becomes unstable.

Safer way to recover from the issue is to bring UP down blades to working state. But if bringing blades back to working state is not possible then only way to keep setup working is removing failed members of replica-set from mongo-config. In doing so, UP and running sessionmgr node becomes primary. It is must to add failed members back to replica-set once they come online.

Following sections describe how to remove failed members from mongo-replica set and how to add them back in replica-set once they are online.

Note The steps mentioned in the following sections should be executed properly.

Note The following steps are done only when only one sessionmgr is UP but is in secondary mode and cannot become primary on its own, and bringing back down blades (holding arbiter and primary sessionmgr VMs) to operational mode is not possible.

Remove Failed Members

This option is usually used when member/s are not running and treated as failed member. The script removes all such failed members from replica-set.

Step 1 Login to pcrfclient01/02.

Step 2 Execute the diagnostics script to know which replica-set or respective component is failed and you want to remove.

```
#diagnostics.sh --get_replica_status
```

Step 3 Execute build_set.sh with below option to remove failed member/s from replica set, this operation removes the all failed members across the site.

```
#cd /opt/broadhop/installer/support/mongo/
```

For session db

```
#./build_set.sh --session --remove-failed-members
```

For spr db

```
#./build_set.sh --spr --remove-failed-members
```

For balance db

```
#./build_set.sh --balance --remove-failed-members
```

For report db

```
#./build_set.sh --report --remove-failed-members
```

For portal db

```
#./build_set.sh --portal --remove-failed-members
```

Step 4 Execute the diagnostics script again to verify if that particular member is removed.

```
#diagnostics.sh --get_replica_status
```

Note If status is not seen properly by above command, login to mongo port on sessionmgr and check replica status.

```
QNS Diagnostics
+-------------------------------------------------------------------------------------------------------------------------+
| Mongo:2.4.6                          MONGODB REPLICA-SETS STATUS INFORMATOIN                    Date : 2014-04-03 00:47:30 |
+-------------------------------------------------------------------------------------------------------------------------+
|    SET NAME    -      PORT : IP ADDRESS      -  REPLICA STATE  -        HOST NAME     -  HEALTH  -   LAG TIME    - PRIORITY |
+-------------------------------------------------------------------------------------------------------------------------+
| BALANCE:set02                                                                                                           |
|    Member-1    -     27718 : 192.168.94.123  -  UNKNOWN        -  pcrfclient01       - OFF-LINE -   --------     -   0    |
|    Member-2    -     27718 : 192.168.94.226  -  UNKNOWN        -  sessionmgr01       - OFF-LINE -  No Primary    -   1    |
|    Member-3    -     27718 : 192.168.94.227  -  SECONDARY      -  sessionmgr02       - ON-LINE  -  No Primary    -   1    |
+-------------------------------------------------------------------------------------------------------------------------+
| REPORTING:set03                                                                                                         |
|    Member-1    -     27719 : 192.168.94.123  -  UNKNOWN        -  pcrfclient01       - OFF-LINE -   --------     -   0    |
|    Member-2    -     27719 : 192.168.94.226  -  UNKNOWN        -  sessionmgr01       - OFF-LINE -  No Primary    -   1    |
|    Member-3    -     27719 : 192.168.94.227  -  SECONDARY      -  sessionmgr02       - ON-LINE  -  No Primary    -   1    |
+-------------------------------------------------------------------------------------------------------------------------+
|       NONE     -      NONE : NONE            -        NONE       -      NONE       -   NONE   -    NONE       -  NONE  |
|                      Current setup have problem while connecting to the server on port : 27717                          |
+-------------------------------------------------------------------------------------------------------------------------+
| SPR:set04                                                                                                               |
|    Member-1    -     27720 : 192.168.94.123  -  UNKNOWN        -  pcrfclient01       - OFF-LINE -   --------     -   0    |
|    Member-2    -     27720 : 192.168.94.226  -  UNKNOWN        -  sessionmgr01       - OFF-LINE -  No Primary    -   1    |
|    Member-3    -     27720 : 192.168.94.227  -  SECONDARY      -  sessionmgr02       - ON-LINE  -  No Primary    -   1    |
+-------------------------------------------------------------------------------------------------------------------------+
[root@pcrfclient02 mongo]# mongo sessionmgr02:27717
MongoDB shell version: 2.4.6
connecting to: sessionmgr02:27717/test
set01:PRIMARY> rs.status()
{
        "set" : "set01",
        "date" : ISODate("2014-04-03T06:48:15Z"),
        "myState" : 1,
        "members" : [
                {
                        "_id" : 2,
                        "name" : "sessionmgr02:27717",
                        "health" : 1,
                        "state" : 1,
                        "stateStr" : "PRIMARY",
                        "uptime" : 540,
                        "optime" : Timestamp(1396507695, 20),
                        "optimeDate" : ISODate("2014-04-03T06:48:15Z"),
                        "self" : true
                }
        ],
        "ok" : 1
}
set01:PRIMARY>
```

Add Failed Members

Step 1 Login to pcrfclient01/02.

Step 2 Once failed members are back online, they can be added back in replica-set.

Step 3 Execute the diagnostics script to know which replica-set member is not in configuration or failed member.

```
#diagnostics.sh --get_replica_status
```

Step 4 If status is not seen properly by above command, login to mongo port on sessionmgr and check replica status.

```
QNS Diagnostics
+-------------------------------------------------------------------------------------------------------------------------------+
| Mongo:2.4.6                          MONGODB REPLICA-SETS STATUS INFORMATOIN                          Date : 2014-04-03 00:47:30 |
+-------------------------------------------------------------------------------------------------------------------------------+
|    SET NAME    -      PORT : IP ADDRESS      -  REPLICA STATE  -        HOST NAME     -  HEALTH  -   LAG TIME     - PRIORITY |
+-------------------------------------------------------------------------------------------------------------------------------+
| BALANCE:set02                                                                                                                 |
|    Member-1    -     27718 : 192.168.94.123  -  UNKNOWN        -  pcrfclient01       - OFF-LINE -   --------     -    0    |
|    Member-2    -     27718 : 192.168.94.226  -  UNKNOWN        -  sessionmgr01       - OFF-LINE - No Primary     -    1    |
|    Member-3    -     27718 : 192.168.94.227  -  SECONDARY      -  sessionmgr02       - ON-LINE  - No Primary     -    1    |
+-------------------------------------------------------------------------------------------------------------------------------+
| REPORTING:set03                                                                                                               |
|    Member-1    -     27719 : 192.168.94.123  -  UNKNOWN        -  pcrfclient01       - OFF-LINE -   --------     -    0    |
|    Member-2    -     27719 : 192.168.94.226  -  UNKNOWN        -  sessionmgr01       - OFF-LINE - No Primary     -    1    |
|    Member-3    -     27719 : 192.168.94.227  -  SECONDARY      -  sessionmgr02       - ON-LINE  - No Primary     -    1    |
+-------------------------------------------------------------------------------------------------------------------------------+
|       NONE     -      NONE : NONE            -        NONE     -       NONE        -   NONE   -    NONE       -   NONE    |
|                        Current setup have problem while connecting to the server on port : 27717                              |
+-------------------------------------------------------------------------------------------------------------------------------+
| SPR:set04                                                                                                                     |
|    Member-1    -     27720 : 192.168.94.123  -  UNKNOWN        -  pcrfclient01       - OFF-LINE -   --------     -    0    |
|    Member-2    -     27720 : 192.168.94.226  -  UNKNOWN        -  sessionmgr01       - OFF-LINE - No Primary     -    1    |
|    Member-3    -     27720 : 192.168.94.227  -  SECONDARY      -  sessionmgr02       - ON-LINE  - No Primary     -    1    |
+-------------------------------------------------------------------------------------------------------------------------------+
[root@pcrfclient02 mongo]# mongo sessionmgr02:27717
MongoDB shell version: 2.4.6
connecting to: sessionmgr02:27717/test
set01:PRIMARY> rs.status()
{
        "set" : "set01",
        "date" : ISODate("2014-04-03T06:48:15Z"),
        "myState" : 1,
        "members" : [
                {
                        "_id" : 2,
                        "name" : "sessionmgr02:27717",
                        "health" : 1,
                        "state" : 1,
                        "stateStr" : "PRIMARY",
                        "uptime" : 540,
                        "optime" : Timestamp(1396507695, 20),
                        "optimeDate" : ISODate("2014-04-03T06:48:15Z"),
                        "self" : true
                }
        ],
        "ok" : 1
}
set01:PRIMARY>
```

#cd /opt/broadhop/installer/support/mongo

For session db

#./build_set.sh --session --add-members

For spr db

#./build_set.sh --spr --add-members

For balance db

#./build_set.sh --balance --add-members

For report db

#./build_set.sh --report --add-members

For portal db

#./build_set.sh --portal --add-members

Maintenance Window Procedures

The usual tasks for a maintenance window might include these:

- Prior to Any Maintenance
- Change Request Procedure
- Software Upgrades
- Application Restarts
- VM Restarts
- Hardware Restarts
- Planned Outages

Prior to Any Maintenance

Backup all relevant information to an offline resource. For more information on backup, see *Cisco Policy Suite 7.0 Backup and Restore Guide*.

- Data - Backup all database information. This includes Cisco MsBM, Cisco Unified SuM.

Note Sessions can be backed up as well.

- Configurations - Backup all configuration information. This includes SVN (from PCRFClient), the **/etc/broadhop** directory from all PCRFs
- Logs - Backup all logs for comparison to the upgrade. This is not required, but will be helpful if there are any issues

Change Request Procedure

- Have proper sign off for any change request. Cisco and all customer teams must sign off.
- Make sure the proposed procedures are well defined.
- Make sure the rollback procedures are correct and available.

Software Upgrades

- Determine if the software upgrade will cause an outage and requires a maintenance window to perform the upgrade.
- Typically software upgrades can be done on one node a time and so minimize or eliminate any outage.

- Most of the time, an upgrade requires a restart of the application. Most applications can be started in less than 1 minute.

Application Restarts

Application restarts are component independent. These are the components:

- PCRF/PCRFClient
- Load Balancer/IO Manager
- sessionMgr

IO Manager, PCRF, PCRFClient

- IO Managers and PCRF give up their resources and allow the fail overs to take over. They can be stopped directly with **service qns restart**
- PCRFClient is a GUI application and can be restarted at any point. If SVN is restarted, the PCRF applications continue to run, but throw errors saying that they cannot check for new configurations. This will not impact the environment.
- sessionMgr is deployed as active - standby and is used by the policy server to maintain the subscriber session state information.
- Load Balancers distribute the load for RADIUS, Web Services, MySQL, LDAP, and SVN. Two load balancers are deployed for each Cisco Policy Suite in active/passive mode.

VM Restarts

- LINUX must be shutdown normally for VM restarts.
- All VMs are Linux.
- The preferred methods are **Init 0 or shutdown –h**
- Failure to use the Linux OS shutdown can result in VM corruption and problems restarting the VM and applications.
- VM restart is typically done to increase resources to the VM (disk, memory, CPU).

Hardware Restarts

- Hardware restarts should be rare.
- When a hardware restart is needed, VMs must be shutdown first.
- When all VMs are stopped, shutdown the hardware with either the ESXi console or as a power off.

Planned Outages

- Planned outages are similar to hardware restarts.
- VMs need to be shutdown, hardware can then be stopped.
- When hardware is started, the typical hardware starting order is:
  - Start the servers with PCRFClient01, LB01, and SessionMgr01 first.

– Start all other servers in any order after that.

Non-maintenance Window Procedures

Tasks you can perform as non-maintenance, that is at any time, are these:

- Data archiving or warehousing
- Log removal

Common Troubleshooting Tasks

This section describes frequently used troubleshooting tasks you might use before calling support or as directed by support.

CPS Trace Monitoring

In this policy trace example: the search string searches the incoming message and the network session.

```
java -DsearchString=255654940574
-Dservers=qns01,qns02,qns03,qns04,qns05,qns06,qns07,qns08,
qns09 -DtraceLogging=true -jar traceMonitor.jar &> /var/
tmp/policy-trace.log &
```

Kill All Cisco Processes From the Command Line as Root

Depending on the Linux version, one or both of these ps commands are applicable. Remove the portion '| xargs kill -9' if you want to test out the command.

These commands do the following:

- print out all processes (ps), then
- search (grep) for all processes that do not contain the word grep or mysql, then
- use sed to remove all the remaining text except for the PID value, and then
- send that PID to kill -9.

PIDs must be 3 characters to 5 characters long.

```
[root@lab ~]# ps -A
PID TTY TIME CMD
1 ?              00:00:00 init
2 ?              00:00:01 migration/0
3 ?              00:00:00 ksoftirqd/0
4 ?              00:00:01 migration/1
5 ?              00:00:00 ksoftirqd/1
6 ?              00:18:49 events/0
7 ?              00:00:00 events/1
8 ?              00:00:00 khelper
49 ?             00:00:00 kthread
54 ?             00:00:00 kblockd/0
55 ?             00:00:00 kblockd/1
56 ?             00:00:00 kacpid
217 ?            00:00:00 cqueue/0
```

```
218 ?            00:00:00 cqueue/1
221 ?            00:00:00 khubd
223 ?            00:00:00 kseriod
299 ?            00:00:00 khungtaskd
300 ?            00:00:00 pdflush
301 ?            00:01:09 pdflush
302 ?            00:00:01 kswapd0
303 ?            00:00:00 aio/0
304 ?            00:00:00 aio/1
510 ?            00:00:00 kpsmoused
554 ?            00:00:00 mpt_poll_0
555 ?            00:00:00 mpt/0
556 ?            00:00:00 scsi_eh_0
560 ?            00:00:00 ata/0
561 ?            00:00:00 ata/1
562 ?            00:00:00 ata_aux
569 ?            00:00:00 kstriped
582 ?            00:00:00 ksnapd
597 ?            00:04:19 kjournald
623 ?            00:00:00 kauditd
656 ?            00:00:00 udevd
2168 ?           00:00:00 kmpathd/0
2169 ?           00:00:00 kmpathd/1
2171 ?           00:00:00 kmpath_handlerd
2194 ?           00:00:00 kjournald
2664 ?           00:00:00 vmmemctl
2795 ?           00:02:38 vmtoolsd
2877 ?           00:00:00 iscsi_eh
2920 ?           00:00:00 cnic_wq
2924 ?           00:00:00 bnx2i_thread/0
2925 ?           00:00:00 bnx2i_thread/1
2939 ?           00:00:00 ib_addr
2949 ?           00:00:00 ib_mcast
2950 ?           00:00:00 ib_inform
2951 ?           00:00:00 local_sa
2954 ?           00:00:00 iw_cm_wq
2958 ?           00:00:00 ib_cm/0
2959 ?           00:00:00 ib_cm/1
2963 ?           00:00:00 rdma_cm
2984 ?           00:00:00 iscsiuio
3784 ?           00:06:49 snmpd
3799 ?           00:00:00 snmptrapd
3814 ?           00:00:21 memcached
3836 ?           00:00:00 sshd
3857 ?           00:00:00 ntpd
3870 ?           00:00:00 mysqld_safe
3925 ?           00:00:19 mysqld
3977 ?           00:00:01 gpm
3992 ?           00:00:01 httpd
4006 ?           00:03:18 collectd
4058 ?           00:00:00 crond
4077 ?           00:00:42 pcrfclient_avai
4079 ?           00:00:34 qns_availabilit
4081 ?           00:00:17 database_availa
4082 ?           00:00:13 server_availabi
4098 ?           00:00:00 atd
4169 ?           00:00:03 avahi-daemon
4170 ?           00:00:00 avahi-daemon
4302 ?           2-15:01:05 java
4324 ?           00:21:27 java
4375 ?           00:20:32 mongod
4380 tty1        00:00:00 mingetty
4381 tty2        00:00:00 mingetty
4382 tty3        00:00:00 mingetty
```

```
4383 tty4        00:00:00 mingetty
4384 tty5        00:00:00 mingetty
4393 tty6        00:00:00 mingetty
4395 ?           00:00:00 gdm-binary
4433 ?           00:00:00 gdm-binary
4435 ?           00:00:02 gdm-rh-security
4436 tty7        00:05:28 Xorg
5022 ?           00:00:00 ntpd
14425 ?          00:00:00 sshd
14487 pts/0      00:00:00 bash
14823 ?          00:00:00 sleep
14837 ?          00:00:00 sleep
14854 ?          00:00:00 sleep
15014 ?          00:00:00 sleep
15019 pts/0      00:00:00 ps
25203 ?          00:00:00 gnome-vfs-daemo
25316 ?          00:00:00 pam_timestamp_c
28836 ?          00:00:06 httpd
28837 ?          00:00:06 httpd
28838 ?          00:00:06 httpd
28839 ?          00:00:06 httpd
28840 ?          00:00:06 httpd
28841 ?          00:00:06 httpd
28842 ?          00:00:06 httpd
28843 ?          00:00:06 httpd
[root@lab ~]#
```

Low or Out of Disk Space

To determine the disk space used, use these Linux disk usage and disk free commands:

- **du**
- **df**

df Command

Example is provided at

home# df -h

df

Response to this command is as follows:

```
Filesystem Size Used Avail Use% Mounted on
/dev/cciss/c0d0p5 56G 27G 26G 51% /
/dev/cciss/c0d0p1 99M 12M 83M 12% /boot
tmpfs 2.0G 0 2.0G 0% /dev/shm
none 2.0G 0 2.0G 0% /dev/shm
/dev/cciss/c0d0p2 5.8G 4.0G 1.6G 73% /home
```

As shown above, the **/home** directory is using the most of it's allocated space (73%).

du Command

The /home directory is typically for /home/admin but in some cases, there is also /home/qns or /home/remote. You can check both:

du

An example of this command is found at:

home# du -hs * Linux Disk Usage command

This command produces this output:

```
[root@lab home]# du -hs
160M .
[root@lab home]# du -hs *
1.3M   qns
158M   remote
36K    testuser
```

The **du** command shows where the space is being used. By default, the **du** command by itself gives a summary of quota usage for the directory specified and all subdirectories below it.

Note By deleting any directories, you remove the ability to roll back if for some reason an update is not working correctly. Only delete those updates to which you would probably never roll back, perhaps those 6 months old and older.

Frequently Encountered Troubles

This section lists the following trouble issues already diagnosed and solved.

- Subscriber not Mapped on SCE
- CPS Server Will Not Start and Nothing is in the Log
- Server returned HTTP Response Code: 401 for URL
- com.broadhop.exception.BroadhopException: Unable to Find System Configuration for System
- Log Files Display the Wrong Time but the Linux Time is Correct
- JMX Management Beans are not Deployed
- Unable to Access Binding Information
- Error Processing Package, Reference Data Does Not Exist for NAS IP
- REST Web Service Queries Returns an Empty XML Response for an Existing User
- Error in Datastore: "err" : "E11000 Duplicate Key Error Index
- Error Processing Request: Unknown Action
- Memcached Server is in Error
- Firewall Error: Log shows Host Not Reachable, or Connection Refused
- Unknown Error in Logging: License Manager
- Ecore File is Not Generated:
- Logging Does Not Appear to be Working
- Cannot Connect to Server Using JMX: No Such Object in Table
- File System Check (FSCK) Errors
- CPS: 27717 Mongo Stuck in STARTUP2 after sessionMgr01/2 Reboot

- SR: 628099455 System Failure Errors in Control Center
- Multi-user Policy Builder Errors
- Multi-user Policy Builder Errors
- Policy Reporting Configuration not getting updated post CPS Upgrade
- CPS Memory Usage Increased
- Errors while Installing HA Setup
- Enable/disable Debit Compression
- Diameter proxy error in diagnostics.sh output
- Portal Landing page is slow (or) not getting redirected to Portal
- Not able to Publish the Policy in Policy Builder
- CPS not sending SNMP traps to External NMS server
- Diameter Peer Connectivity is Down

Subscriber not Mapped on SCE

This issue was causing the subscriber to get no mapping on the SCE.

1. Write an awk script to perform the following grep to create a text file of over 1000 instances of this message:

   ```
   grep "No member in system" policy.log* >
   no_member_found.txt
   ```

   This grep resulted in a file with these lines:

   ```
   policy.log:2009-07-17 11:00:21,201 INFO
   wikiimport:com.broadhop.sme.business.network.accounting.Ne
   tworkAccountingUtil No member in system for d162818
   policy.log:2009-07-17 11:02:06,108 INFO
   wikiimport:com.broadhop.sme.business.network.accounting.Ne
   tworkAccountingUtil No member in system for D02625
   policy.log.1:2009-07-17 09:25:29,036 INFO
   wikiimport:com.broadhop.sme.business.network.accounting.Ne
   tworkAccountingUtil No member in system for D162346
   policy.log.1:2009-07-17 09:27:28,718 INFO
   wikiimport:com.broadhop.sme.business.network.accounting.Ne
   tworkAccountingUtil No member in system for d162365
   policy.log.1:2009-07-17 09:27:37,193 INFO
   wikiimport:com.broadhop.sme.business.network.accounting.Ne
   tworkAccountingUtil No member in system for d162365
   policy.log.1:2009-07-17 09:27:42,257 INFO
   wikiimport:com.broadhop.sme.business.network.accounting.Ne
   tworkAccountingUtil No member in system for d162365
   policy.log.1:2009-07-17 09:38:09,010 INFO
   wikiimport:com.broadhop.sme.business.network.accounting.Ne
   tworkAccountingUtil No member in system for d02116
   policy.log.1:2009-07-17 09:38:12,618 INFO
   wikiimport:com.broadhop.sme.business.network.accounting.Ne
   tworkAccountingUtil No member in system for D163647
   policy.log.1:2009-07-17 09:40:42,751 INFO
   wikiimport:com.broadhop.sme.business.network.accounting.Ne
   tworkAccountingUtil No member in system for d102096
   ```

2. Then use the following awk script to generate a new file that only has the user name. The script says print the 10th field:

```
awk '{print $10}' no_member_found.txt >
no_member_found_usernames_with_dupes.txt
```

3. Run the following command to remove duplicates:

```
sort no_member_found_usernames_with_dupes.txt | uniq >
uniq_sorted_no_member_found_usernames.txt
```

This resulted in a file with usernames only:

```
D00059
D00077
D001088
D00112
d001313
D00145
D001452
d00156
D00186
d00198
D00200
d00224
```

CPS Server Will Not Start and Nothing is in the Log

If the CPS server does not start (or starts and immediately crashes) and no errors appear in **/var/log/broadhop/qns.log** to give reasons it did not start, check the following list:

1. Check **/var/log/broadhop/service-qns-1.log**
2. Check **/etc/broadhop/servers**
   - There should be an entry in this file for the current host name (Type 'hostname' in the console window to find the local hostname)
   - There must be directory that corresponds to the hostname entry with config files. That is, if the servers file has svn01=controlcenter, there must be a /etc/broadhop/control center directory
3. Attempt to start the server directly from the command line and look for errors.
   - Type: **/opt/broadhop/qns/bin/qns.sh**
   - The server should start up successfully and the command line should not return. If the command prompt returns then the server did not start successfully.
   - Look for any errors displayed in the console output
4. Look for OSGi Errors
   - Look in /opt/broadhop/qns/configuration for a log file. If any exist examine the log file for error messages.

Server returned HTTP Response Code: 401 for URL

A 401 type error means you're not logging in to SVN with proper credentials.

The server won't start and the following appears in the log:

```
2010-12-10 01:05:26,668 \[SpringOsgiExtenderThread-8\]
ERROR c.b.runtime.impl.RuntimeLoader - There was an error
```

```
initializing reference data\!
java.io.IOException: Server returned HTTP response code:
401 for URL: http://lbvip01/repos/run/config.properties
sun.net.www.protocol.http.HttpURLConnection.getInputStream
(HttpURLConnection.java:1313) \~\[na:1.6.0_20\]
org.springframework.core.io.UrlResource.getInputStream(Url
Resource.java:124) \~\[org.springframework.core_3.0.0.REL
```

To fix this error:

- Edit **/etc/broadhop/qns.conf**
- Ensure that the configuration URL and repository credentials hostnames match.

```
\-Dcom.broadhop.config.url=http://lbvip01/repos/run/
\-Dcom.broadhop.repository.credentials=broadhop/
broadhop@lbvip01
```

com.broadhop.exception.BroadhopException: Unable to Find System Configuration for System

Symptoms: server won't stay started and the log displays this:

```
com.broadhop.exception.BroadhopException: Unable to find system configuration for
system:
The system that is set up in your Cisco Policy Builder (and cluster name) must match
the one specified in /etc/broadhop/qns.conf. Either add or change this via the Cisco
Policy Builder interface, and then publish or update the system/clustername in
/etc/broadhop/qns.conf
\-Dcom.broadhop.run.systemId=poc-system
\-Dcom.broadhop.run.clusterId=cluster-1
```

Log Files Display the Wrong Time but the Linux Time is Correct

If log files or other dates are showing in the incorrect time zone despite the Linux time being set to the proper time zone, most likely the time zone that the JVM reads is incorrect.

1. In **/etc/sysconfig**, run the command **cat clock** to see this output:

   ```
   ZONE="America/Denver"
   UTC=false
   ARC=false
   ```

2. Change the ZONE line to the time zone you desire, for instance you could change it to:

   ```
   ZONE="Asia/Singapore"
   UTC=false
   ARC=false
   ```
   to change the JVM time zone to Singapore time.

The value for ZONE is driven by the directories in **/usr/share/zoneinfo**

JMX Management Beans are not Deployed

1. Restart the CPS Server. The JMX Beans sometimes are not deployed when features are installed or updated.

2. Run **ps -ef | grep java** and look for: '**-javaagent:/opt/broadhop/qns/bin/jmxagent.jar**'. If this is absent, you have an old build and need to update.
3. If you have an old build, see the Operations guide for instructions on updating.

Unable to Access Binding Information

Make sure the binding has been compiled. This error is typically caused by a bad build.

Attempt to upgrade to a newer build.

If you're on a released build, try restarting, there's been a strange bug which causes web service problems after update.

```
2010-10-19 12:05:00,194 [pool-4-thread-1] ERROR
c.b.d.impl.DiagnosticController - Diagnostic failed. A
problem exists with the system --> Common Services: Feature
com.broadhop.ws.service is unabled to start. Error: Error
creating bean with name
'org.springframework.web.servlet.mvc.annotation.DefaultAnn
otationHandlerMapping#0' defined in URL [bundleentry://
27.fwk15830670/META-INF/spring/bundle-ws-context.xml]:
Initialization of bean failed; nested exception is
org.springframework.beans.factory.BeanCreationException:
Error creating bean with name 'subscriberEndpoint' defined
in URL [bundleentry://27.fwk15830670/META-INF/spring/
bundle-ws-context.xml]: Cannot resolve reference to bean
'jibxMarshaller' while setting bean property 'marshaller';
nested exception is
org.springframework.beans.factory.BeanCreationException:
Error creating bean with name 'jibxMarshaller' defined in
URL [bundleentry://27.fwk15830670/META-INF/spring/
bundle-ws-context.xml]: Invocation of init method failed;
nested exception is org.jibx.runtime.JiBXException: Unable
to access binding information for class
com.broadhop.ws.impl.messages.RemoveSubscriberProfileReque
st
```

Error Processing Package, Reference Data Does Not Exist for NAS IP

```
2010-10-19 13:25:53,481 [pool-11-thread-1] ERROR
c.b.u.t.udp.UdpMessageListener - Error processing packet {}
com.broadhop.exception.BroadhopException: Radius reference
data does not exist for NAS IP 192.168.180.74 or 10.0.0.52
at
com.broadhop.radius.impl.RadiusReferenceData.getRadiusDevi
ce(RadiusReferenceData.java:111)
~[com.broadhop.radius.service_1.0.0.release.jar:na]
at
com.broadhop.radius.impl.RadiusReferenceData.getSharedSecr
et(RadiusReferenceData.java:130)
~[com.broadhop.radius.service_1.0.0.release.jar:na]
at
com.broadhop.radius.impl.RadiusMessageListener.getSharedSe
cret(RadiusMessageListener.java:247)
~[com.broadhop.radius.service_1.0.0.release.jar:na]
at
com.broadhop.radius.impl.RadiusMessageListener.processPack
et(RadiusMessageListener.java:86)
~[com.broadhop.radius.service_1.0.0.release.jar:na]
```

```
at
com.broadhop.utilities.transports.udp.UdpMessageListener$1
.run(UdpMessageListener.java:192)
~[com.broadhop.utility_5.1.1.r019218.jar:na]
at
java.util.concurrent.Executors$RunnableAdapter.call(Unknow
n Source) [na:1.6.0_21]
at
java.util.concurrent.FutureTask$Sync.innerRun(Unknown
Source) [na:1.6.0_21]
at java.util.concurrent.FutureTask.run(Unknown
Source) [na:1.6.0_21]
at
java.util.concurrent.ThreadPoolExecutor$Worker.runTask(Unk
nown Source) [na:1.6.0_21]
at
java.util.concurrent.ThreadPoolExecutor$Worker.run(Unknown
Source) [na:1.6.0_21]
at java.lang.Thread.run(Unknown Source)
[na:1.6.0_21]
```

Ensure that this NAS IP has been set up in Cisco Policy Builder under Reference Data->Policy Enforcement Points. If you use an ISG, add to the ISG Pools folder. Otherwise, add to the RADIUS Device Pools folder. The IP's that matter are in the 'Devices' table on the ISG Pool object itself.

REST Web Service Queries Returns an Empty XML Response for an Existing User

For example:

<subscriberProfile><content/></subscriberProfile>

Because there are multiple ways needed to return web service data, the BroadHop Web Service Blueprint doesn't return any XML by default. To fix this issue, configure the 'Default Web Service Query Response' blueprint under the 'BroadHop Web Services' Blueprint.

Error in Datastore: "err" : "E11000 Duplicate Key Error Index

Note This removes ALL sessions

Typically, duplicate keys like this happen when initially configuring policies and switching primary keys. In a production scenario, you may not want to remove all sessions.

1. **ssh** into sessionmgr01
2. Open SessionMgr CLI

   /usr/bin/mongo --port 27717

   Using **/usr/bin/mongo** indicates whether the mongo replica set is primary or secondary.
3. Enter following commands on the MongoDB CLI

   use session_cache;

   db.session.remove();

4. If it gives you a 'not master' error, log into sessionmgr02 and do the same

Error Processing Request: Unknown Action

```
com.broadhop.policy.impl.RulesPolicyService - Error
processing policy request: Unknown action:
com.broadhop.pop3auth.actions.IPOP3AuthRequest and Remote
Actions are disabled.
```

If you see an error of the type above, it means that the implementation class it's looking for is not available on the server.

This can be caused by:

- The component needed is not installed on the server.
- Ensure that the pop3auth service is installed in your server.
- Look for exceptions in the logs when starting up.
- Try restarting the service bundle (pop3auth service in this case) using the OSGi console and looking at the logs.

Memcached Server is in Error

```
ERROR c.b.d.impl.DiagnosticController - Diagnostic failed.
A problem exists with the system --> Common Services:
2:Memcached server is in error
```

1. Log on to the server where qns is running
2. telnet to the memcache server's IP and port 11211 (ex: telnet lbvip01 11211).

   You can figure out which memcache server CPS is pointing to in Cisco Policy Builder. Look at: Reference Data > Systems > <System Name> > Cluster Name

   a. If you can't telnet to the port, do this

   Ensure memcache is running:

   – Log on to server where memcache is running

   run service memcached status

   [root@sessionmgr01 ~]# service memcached status

   memcached is stopped

   – If the service is stopped, start it:

   [root@sessionmgr01 ~]# service memcached start

   Starting a new distributed memory caching

   (memcached) process for 11211:

   b. Ensure firewall configuration is OK:

   To check if this is the problem, just stop the firewall.

/etc/init.d/iptables stop

If it is the problem, add an exception in **/etc/sysconfig/iptables**. Look at other entries in the file for an example.

After adding an exception, restart iptables **/etc/init.d/iptables restart**

Firewall Error: Log shows Host Not Reachable, or Connection Refused

In HA environment, if we see some connection refused errors, stop the firewall and execute

service iptables stop

to see if the problem is related to the iptables firewall issue.

Unknown Error in Logging: License Manager

```
2010-12-12 18:51:32,258 [pool-4-thread-1] ERROR
c.b.licensing.impl.LicenseManager - Unknown error in
logging
java.lang.NullPointerException: null
at
com.broadhop.licensing.impl.LicenseManager.checkFeatures(L
icenseManager.java:311) ~[na:na]
```

This issue may occur if no license has been assigned yet.

Option 1: If this is for development or Proof Of Concept deployments, you can turn on developer mode. This effectively gives you 100 users but is not for use in production.

1. Login to CPS.
2. Add the following to the **/etc/broadhop/qns.conf** file:

   -Dcom.broadhop.developer.mode=true
3. Restart CPS

Option 2: Generate a real license. Have your Cisco technical representative send you the Technical Article *Tool com.broadhop.licensing.service - Creating a CPS License*.

Option 3: If we have license error in the logs, check the MAC address of the VM and compare that with the MAC address in the license file in `/etc/broadhop/license/`.

Ecore File is Not Generated:

```
(Example shown is RADIUS feature)
2010-12-12 18:39:34,075 [SpringOsgiExtenderThread-8] ERROR
c.b.runtime.impl.RuntimeLoader - Unable to load class:
com.broadhop.refdata.radius.RadiusPackage. Ecore file is
not generated http://lbvip01/repos/run/
com.broadhop.radius.ecore
```

A feature (RADIUS) has been installed in Cisco Policy Builder, but is not installed on the server. Or, a features file being accessed is not where features have been placed.

1. Check if the feature is installed in your server by running **/opt/broadhop/qns-1/bin/list_installed_features.sh**.

2. If the feature IS installed, you probably are pointing to (or publishing to) the wrong repository. Check where you're publishing to in Policy Builder and check and what URL you are pulling from in **/etc/broadhop/qns.conf**
3. If the feature IS NOT installed, you may be pointing to a different features file than you expect. Do this:
   a. Login to CPS server and find the name of the qns server you are on
   b. Type: **hostname**
   c. Check **/etc/broadhop/servers** file

   Whatever is listed next to the hostname you are using should also have a directory in the **/etc/broadhop** directory. It is in THAT directory you should change the features file. This defaults qns01 to 'iomanager'. Change it to 'pcrf'.

Logging Does Not Appear to be Working

1. Run the JMX Command:

```
/opt/broadhop/qns/bin/jmxcmd.sh
ch.qos.logback.classic:Name=default,Type=ch.qos.logback
.classic.jmx.JMXConfigurator Statuses
```

or

2. Access that bean using JMX Term or JConsole to view the status of the Logback Appenders. To access JMX Term, follow these steps:
   - Execute below script: **/opt/broadhop/qns-1/bin/jmxterm.sh**
   - If user does not have permission to execute the command then change the permission using below command:

   chmod 777 opt/broadhop/qns-1/bin/jmxterm.sh

   - Again execute the script: **/opt/broadhop/qns-1/bin/jmxterm.sh**
   - Once command is executed, JMX terminal opens up.
   - Execute the below command to open connection:

   $>open qns01:9045

   - All beans can be seen using below command

   $>beans

```
#domain = JMImplementation:
JMImplementation:type=MBeanServerDelegate
#domain = ch.qos.logback.classic:
ch.qos.logback.classic:Name=default,Type=ch.qos.logba
ck.classic.jmx.JMXConfigurator
#domain = com.broadhop.action:
com.broadhop.action:name=AddSubscriberService,type=hi
stogram
com.broadhop.action:name=AddSubscriberService,type=se
rvice
com.broadhop.action:name=GetSessionAction,type=histog
ram
com.broadhop.action:name=GetSessionAction,type=servic
e
```

```
com.broadhop.action:name=GetSubscriberActionImpl,type
=histogram
com.broadhop.action:name=GetSubscriberActionImpl,type
=service
com.broadhop.action:name=LockSessionAction,type=histo
gram
com.broadhop.action:name=LockSessionAction,type=servi
ce
com.broadhop.action:name=LogMessage,type=histogram
com.broadhop.action:name=LogMessage,type=service
com.broadhop.action:name=OCSLoadBalanceState,type=his
togram
com.broadhop.action:name=OCSLoadBalanceState,type=ser
vice
java.nio:name=mapped,type=BufferPool
#domain = java.util.logging:
java.util.logging:type=Logging
```

Cannot Connect to Server Using JMX: No Such Object in Table

This is likely caused because the server's name is not set up in the hosts file with its proper IP address.

In /etc/hosts the hostname (e.g., qns01) SHOULD NOT be aliased to 127.0.0.1 or localhost.

If improperly aliased, JMX tells the server it's connecting to connect back with the IP of it's hostname. If it's aliased to localhost (127.0.0.1), the server attempts to open connections with itself, which is unfortunate.

Example Error:

```
ERROR com.broadhop.management.JmxClient -
Unable to connect to JmxClient: iomgr01:9045. Cause: no
such object in table Will attempt to reconnect.
```

File System Check (FSCK) Errors

During machine boot, **fsck** is run on file systems to check its consistency. This consistency check is done without user intervention and automatically fixes errors which it can. But sometimes, if there is a hard reset to CPS VM/machine, for example, because of abrupt power failure, then during **fsck**, all the problems are not automatically fixed and user intervention is must to fix the errors reported by fsck. The table below describes the common fsck errors along with their description and solution.

Table 1-1 FSCK Errors

SNo.	FSCK Error	Description/Solution
1	BAD SUPER BLOCK: MAGIC NUMBER WRONG USE ALTERNATE SUPER-BLOCK TO SUPPLY NEEDED INFORMATION	This error comes when file system is cleanly unmounted. Some superblock corruptions can be automatically repaired. But for some like BAD MAGIC number, fsck aborts and alternate superblock must be specified to fsck command to continue file system check. Reference link to fix the issue - http://www.cyberciti.biz/faq/recover-bad-superblock-from-corrupted-partition/
2	Block bitmap not in a group/inode bitmap not in a group	When this error occurs, data on the device need to be restored using dd or any other device specific command. Reference link to fix the issue - https://bbs.archlinux.org/viewtopic.php?id=128478 http://serverfault.com/questions/131536/ext3-fs-block-bitmap-for-group-1-not-in-group-block-0-is-fs-dead
3	Inode table not in a group	When this error occurs, data on the device need to be restored using dd or any other device specific command. Reference link to fix the issue - http://www.linuxquestions.org/questions/linux-hardware-18/missing-inode-table-646788/
4	Primary superblock is corrupt	Please refer to Error 1, apart from bad magic number if fsck detects corruption in any static parameters of primary superblock (file system size, inode list size etc) it requests operator to specify location of alternate superblock.
5	Journal superblock has an unknown read-only feature flag set	Please refer to Error 1 to 4 to fix this issue.
6	Resize inode is invalid	This error occurs after file system is resized. Reference link to fix this issue - https://bugzilla.redhat.com/show_bug.cgi?id=156954
7	Last mount time is in the future	This error occurs after reboot system clock is not synchronized with UTC. Reference link to fix this issue - http://forums.debian.net/viewtopic.php?t=45797

Table 1-1 FSCK Errors

SNo.	FSCK Error	Description/Solution
8	Root directory is not an inode	If primary superblock is corrupt this error occurs, alternate superblock needs to be specified to fsck in this case. Reference link to fix this issue - http://serverfault.com/questions/204617/causes-of-sudden-massive-filesystem-damage-root-inode-is-not-a-directory http://www.programmersheaven.com/user/mariapeter12/blog/4320-Resolving-Root-inode-is-not-a-directory-Clear-Linux-Error/
9	Duplicate '..' entry	An indirect block is a pointer to a list of every block claimed by an inode. fsck checks every block number against a list of allocated blocks: if two inodes claim the same block number, that block number is added to a list of duplicate block numbers. The administrator may be asked to choose which inode is correct, and usually time to verify files against backups. fsck additionally checks the integrity of the actual block numbers, which can also become corrupt - it should always lie in the interval between the first data block and the last data block. If a bad block number is detected, the inode is cleared. Similar to above example, this issue is with file system synchronization with actual disk. If machine is powered OFF before fs synchronization to hardware disk, on next reboot, fsck will ask corrective questions to the user to take the action accordingly. For which manual intervention is needed as corrective actions will defer case to case. For example, if one record is created by database operation and at the same time another record is deleted, and same block number (of deleted record) is used for the newly created record, duplicate block error might come.

Table 1-1 FSCK Errors

SNo.	FSCK Error	Description/Solution
10	Error reading block <block_no> (Attempt to read from filesystem resulted in short read) while doing inode scan.	This error stops the user from continuing with the fsck scan, and correcting the problem. Disks that have physical hardware errors often report - being unable to read inodes error. To resolve this issue replace the disk, rather than attempting any corrective action.
11	Journal superblock has an unknown incompatible feature flag set	Feature flag specifies what features a file system has. If this flag is corrupted, fsck asks whether you want to abort the operation. You need to specify "no" and after this fix the superblock corruption. Reference link to fix the issue - http://forums.debian.net/viewtopic.php?f=5&t=83716

- Following link gives list of all the errors which are automatically fixed by fsck as well as list of errors where user intervention is must - http://unix.stackexchange.com/questions/18526/what-does-fsck-p-preen-do-on-ext4
- Following link gives general idea about various phases in fsck - http://etutorials.org/Misc/solaris+exam+guide/Part+I+Solaris+9+Operating+Environment+Exam+I/Chapter+9+Introduction+to+File+Systems/Fixing+Problems+with+fsck/
- Following link describes all the errors in case of UFS file system - http://docs.oracle.com/cd/E19253-01/817-0403/tsfsck-26279/index.html

  This link can be used as a reference to fix the errors reported by fsck on CPS file system which is ext3.

CPS: 27717 Mongo Stuck in STARTUP2 after sessionMgr01/2 Reboot

There can be a situation where 27717 mongo process is stuck after sessionMgr01/02 is rebooted. In this situation follow the below mentioned steps to bring up 27717 all mongo process from STARTUP2 state to PRIMARY/SECONDARY state specific to session database only.

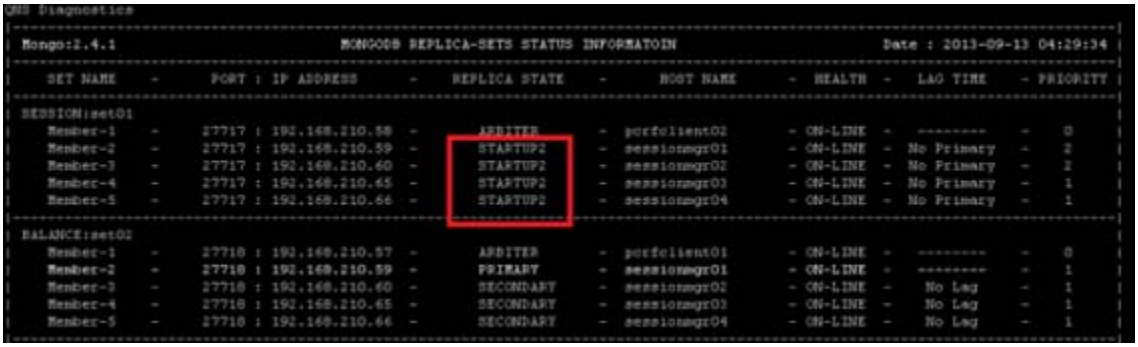
Step 1 Stop CPS process.

Step 2 Log onto pcrfclient01.

Step 3 Execute the diagnostic script to know which replica set (all members) have failed.

```
#diagnostics.sh --get_replica_status
```

The figure shows all replica set members of replica set set01 for session data are in bad shape.



Caution Currently, there is no support to create a specific replica set. For example, there is no support to create multiple session replica sets such as set01, set01a in configuration file.

Step 4 Take a backup of current configuration file and keep only the definition of replica set that needs to be rebuild.

#cd /etc/broadhop

#cp mongoConfig.cfg mongoConfig.cfg.bk

Step 5 Edit configuration file and keep only set01 definition (that is, failed replica set definition).

#vi mongoConfig.cfg

Step 6 Build session replica sets. Select 2 for session non-sharded sets.

```
#cd /opt/broadhop/installer/support/mongo/
./build_set.sh --session --create
```

Starting Replica-Set Creation

Please select your choice: replica sets sharded (1) or non-sharded (2):

2

Step 7 Ignore this step if the setup is HA environment, otherwise set priority 2 for primary site all replica set members. By default, 1 is used for secondary site members.

./set_priority.sh --p 2 --db session --sn pri

Step 8 Revert the backed-up configuration file.

#cd /etc/broadhop

#mv mongoConfig.cfg.bk mongoConfig.cfg

Step 9 Verify if priority is set correctly for newly created replica set.

#diagnostics.sh --get_replica_status

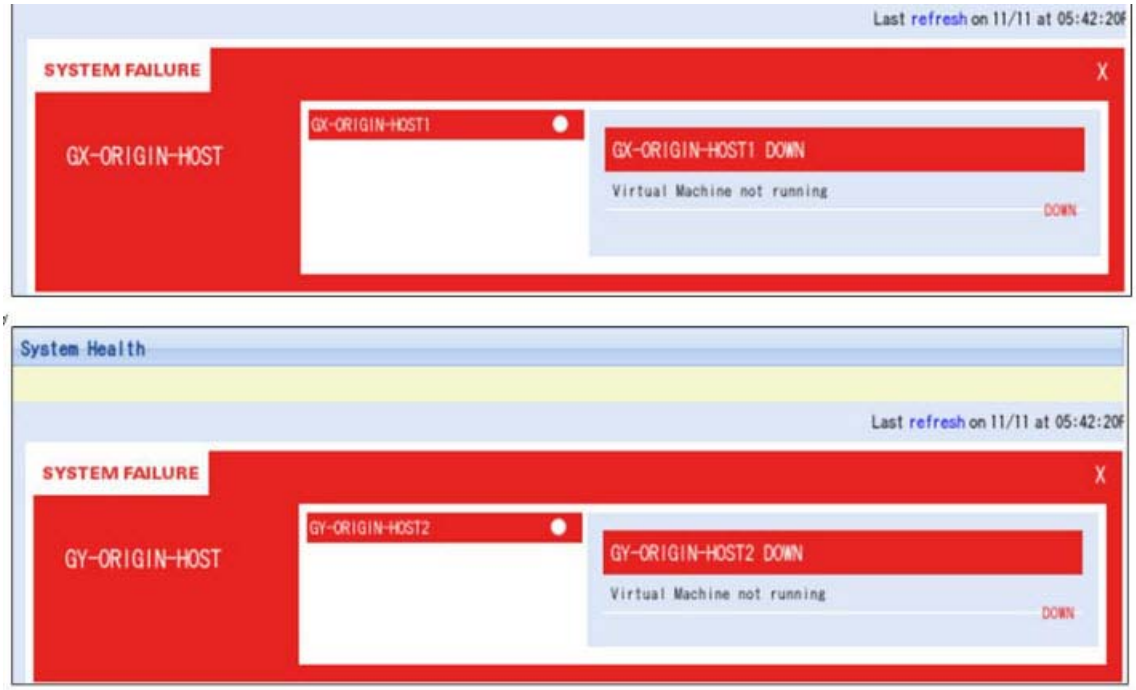
Step 10 To recover other failed set, follow the recovery steps from Step 1 to Step 9.

Step 11 Restart CPS.

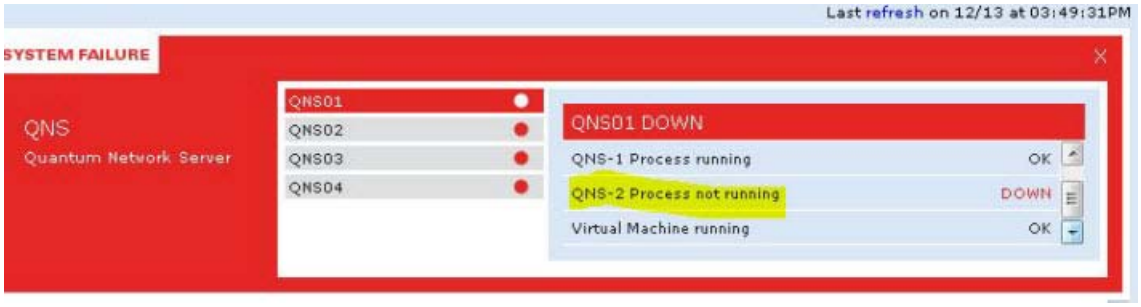
/opt/broadhop/control/restartall.sh

SR: 628099455 System Failure Errors in Control Center

Issue 1: The issue is that the Monitoring tab in control center is supposed to give system health status for the VM's that are hosted only within CPS. In this scenario, the Monitoring tab was reporting status for Gx-Origin and Gy-Origin host which are not the part of CPS setup but are added in `/etc/hosts` and we can't comment these Gx and Gy host name since this is used for diameter connectivity.



Issue 2: The customer is having only one QNS process running per CPS Virtual machine, but the control center reports that their second QNS process on all CPS VM is down. This second QNS process is not even configured in CPS virtual machine and the customer wants Control Center only to report for only one QNS process per CPS VM.



Step 1 Go to the path.

cd /etc/collectd.d

Step 2 List the files.

ls -lrth

Step 3 Take the backup of the below scripts before modifying them so that original data is preserved

cp server_ availability.sh old_serveravailablity.sh

cp database_availability.sh old_datbaseavailability.sh

cp types.db old_types.db

cp qns_availability.sh old_qnsavailability.sh

Step 4 Enter the file using vi mode.

vi server_availability.sh

Step 5 Change the line

```
#SERVERLIST=$(egrep -v "(localhost|vip|corporate_nms_ip)"
   /etc/hosts | awk '{print $2}'
```

to

```
SERVERLIST=$(egrep -v -i
   "(localhost|vip|corporate_nms_ip|#|GX|GY|ext)" /etc/hosts | awk
   '{print $2}'.
```

Step 6 Enter the file with vi mode.

vi database_availability.sh

Step 7 Change the lines

#PORTLIST="27717 27718 27719 27720 27730"

#NAMELIST="session session quota report usum

to

PORTLIST="27717 27718 27719 27720

NAMELIST="session quota report usum"

Step 8 Enter the file with vi mode.

vi qns_availability.sh

This step is to be performed only when we have one QNS process per CPS VM.

If you see `qns_availablity.sh` file, there are three ports 8080, 8081 and 9091. Identify the ports which are not catering any process,.

Steps to check a port that is not having QNS process: (from PCRF Client not in Vi Mode)

a. To list process:

netstat -an | grep 8080

netstat -an | grep 8081

netstat -an | grep 9091

b. Consider an example that 8081 is not carrying any QNS process. So to remove the same from `qns_availabilty.sh`, adjust the array size and also `qns -availblity.sh` should look exactly same as below.

PORTLIST[0]="8080"

#PORTLIST[1]="8081"

PORTLIST[1]="9091"

CMDLIST[0]='GET /service/Subscribers/wsdlDefinition.wsdl HTTP/1.0\r\n\r\n'

#CMDLIST[1]='GET /service/Subscribers/wsdlDefinition.wsdl HTTP/1.0\r\n\r\n'

CMDLIST[1]='ss com.broadhop.model.policy'

RESLIST[0]='200 OK'

#RESLIST[1]='200 OK'

RESLIST[1]='ACTIVE

Step 9 Enter the file with vi mode.

vi types.db

Step 10 Change the lines

#database_availability session_a_db:GAUGE:0:1 session_b_db:GAUGE:0:1 quota_db:GAUGE:0:1 report_db:GAUGE:0:1 usum_db:GAUGE:0:1

to

database_availability session_a_db:GAUGE:0:1 quota_db:GAUGE:0:1 report_db:GAUGE:0:1 usum_db:GAUGE:0:1

Step 11 This step should be performed only if you have one QNS process per CPS VM i.e., in CPS-B and CPS-C we have only one QNS process per Virtual machine.

Step 12 Change the line

#qns_availability qns_a:GAUGE:0:1 qns_b:GAUGE:0:1 qns_admin:GAUGE:0:1

to

qns_availability qns_a:GAUGE:0:1 qns_admin:GAUGE:0:1

Step 13 Enter the mongo DB and remove the qns availability records. This step should be performed only if you have one QNS process per CPS VM.

```
[root@pcrfclient01 collectd.d]# mongo --port 27017

MongoDB shell version: 2.4.6

connecting to: 127.0.0.1:27017/test

> use collectd

switched to db collectd

> db.exec.remove({"type" : "qns_availability"})

> exit
```

Step 14 Restart collectd process.

```
/etc/init.d/collectd restart
```

Step 15 Go to Control center and check for system health under Monitoring tab wait for 60 seconds (1 minute) and click Refresh.

The result of above steps is:

1. To monitor CPS that is having only one QNS process per CPS VM.
2. Make sure that Control center sends the health check only for the Virtual Machine hosted in CPS setup and not for all the hosts present under /etc/hosts.

Multi-user Policy Builder Errors

Not able to do any edits after login

Verify the newly created SVN user has write permission. User should be specified under admins in `/var/www/svn/users-access-file` file.

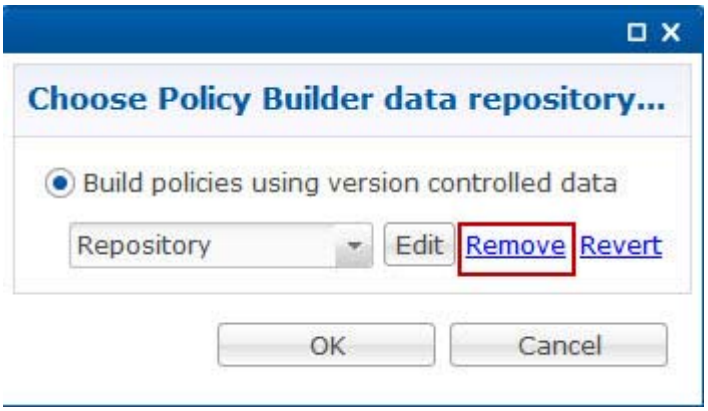
Error in login due to conflict

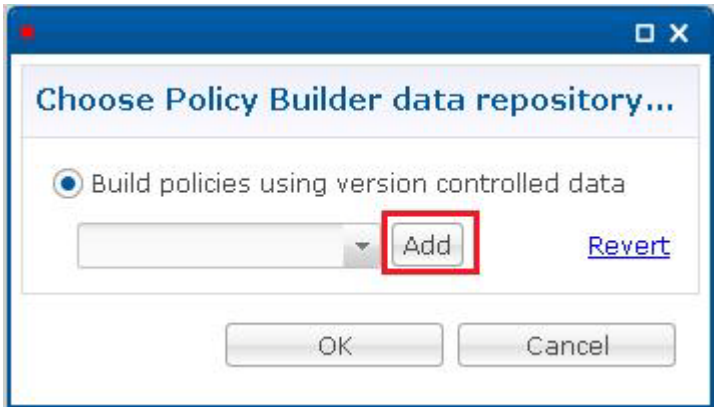
If error similar to below is seen during login, then revert the configuration and login again.

No configuration visible in Policy Builder after login

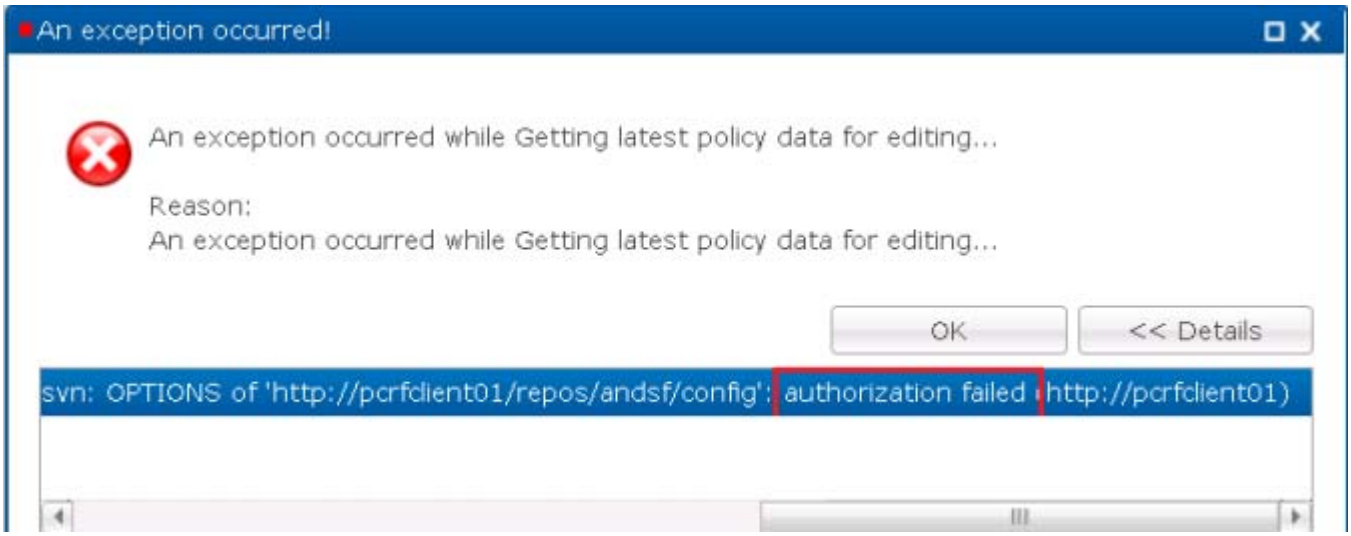
Step 1 Verify the directory `/var/broadhop/pb/workspace/<username>/checkout` is created and it contains `.xmi` files.

Step 2 If directory does not exist or does not have `.xmi` files then delete existing repository using Remove on login page and then add new repository using Add on login page.





Exception Occured During Login



This indicates user does not exist in SVN server.

Debug: Verify user exist in `/var/www/svn/.htpasswd` file.

Debug Details

Log Files: `/var/log/broadhop/qns-pb.log`

Policy Reporting Configuration not getting updated post CPS Upgrade

During CPS upgrade from 5.5.1 to 7.0, it is observed that Policy Reporting configuration does not get updated as per configuration done in CPS 5.5.1.

All the configuration saved in Cisco Policy Builder are converted into XMI files, which are added in the SVN repository. The XMI files based on the CPS 7.0 for Policy Reporting won't be fully compatible with the CPS 5.5 version.

To support backward compatibility, a utility script `migrateCdrXmi_5_5_to_7_0.sh` can be implemented, which upgrades the policy reporting configuration files (XMI files) to CPS 7.0.

Step 1 Obtain the installer archive from the update site corresponding to the build deployed on the system.

Step 2 Copy the archive into the **/tmp** directory of the CPS virtual machine pcrfclient01.

Step 3 Log in as root to the same CPS virtual machine and run these commands.

mkdir /opt/broadhop/installer/migrate/

tar -zxvf /tmp/<installer archive anme> -C /opt/broadhop/ installer/migrate/

chown -R qns:qns /opt/broadhop/installer/migrate

chmod +x /opt/broadhop/installer/migrate/*.sh

Step 4 Run these commands to execute the script:

cd /opt/broadhop/installer/migrate/

sh migrateCdrXmi_5_5_to_7_0.sh

The XMI files added or deleted from SVN configuration repository are displayed in the output.

Step 5 Open the Policy Builder page to verify the configuration changes and publish to runtime.

The utility upgrades the Policy reporting fields, the policy reporting records and the Policy CDR configuration in Policy Reporting section of the Cisco Policy builder.

If an older CPS configuration had any 'Reporting Server Configuration' (in Policy Reporting Plugin Configuration) that used any existing policy CDRs, you have to recreate those reporting configurations using the newly created policy CDRs.

CPS Memory Usage Increased

CPS memory consumption can be monitored using appropriate KPIs in Grafana graphs or other monitoring tools. If memory consumption increases beyond the default threshold of 90% on any CPS VM, CPS will generate a Low Memory alarm for that VM. This threshold is configurable in the CPS Deployment Template using the free_mem_per setting.

Detect and Reclaim Cached Memory

In some cases a Low Memory alarm may be a result of Linux memory management allocating objects in cache.

To evaluate how much memory a VM has cached, and to trigger Linux to free some of the cached memory:

Step 1 Compare the amount of memory cached on two or more CPS VMs by running the free -m command on each VM.

For example, on this qns01 VM, 1893 MB of memory is cached.

```
[root@qns01 ~]# free -m
             total       used       free     shared    buffers     cached
Mem:          7854       7719        135          0        311       1893
-/+ buffers/cache:       5514       2340
Swap:         4095         13       4082
```

However, on qns02, only **1273 MB** of memory is cached.

```
[root@qns02 ~]# free -m
             total       used       free     shared    buffers     cached
Mem:          7854       7175        678          0        321       1273
-/+ buffers/cache:       5580       2274
Swap:         4095         14       4081
[root@qns02 ~]#
```

From this example, qns01 is storing **620 MB** more memory in cache than qns02.

Step 2 To reclaim some of the inactive cached memory, execute the following command:

```
free && sync && echo 3 > /proc/sys/vm/drop_caches && echo "" && free
```

Note Running this command will discard cache objects which can cause a temporary increase in IO and CPU usage, **so it is recommend to run this command during off-peak hours/maintenance window**.

Note This is a non-destructive command and will only free memory that is not in use.

The **sync** command can also be used before running the above command to reduce the number of objects on the system. This can enable even more cached memory to can be freed.

For more information about Linux memory management, refer to http://www.linuxatemyram.com and http://linux-mm.org/Drop_Caches.

Errors while Installing HA Setup

Step 1 Modify file `/var/qps/config/deploy/csv/AdditionalHosts.csv` to correct `lbvip02` IP address and support `sslvip01`.

a. Correct lbvip02 IP address.

b. Add sslvip01 IP address.

c. Convert to json `/var/qps/install/current/scripts/import/import_deploy.sh`.

d. Synchronize host `/var/qps/install/7.0.0/scripts/bin/control/synchosts.sh`.

e. Restart all CPS process using:

/var/qps/install/7.0.0/scripts/bin/control/stopall.sh

/var/qps/install/7.0.0/scripts/bin/control/startall.sh

f. SSH to lbvip01 and update pcs resources.

g. Add below entries in `/etc/haproxy/haproxy-portal.cfg`.

```
listen  portal_proxy sslvip01:80
        mode    http
        balance source
        option forwardfor
        option forwardforport
        reqadd X-Forwarded-Proto:\ http
        server portal01 portal01:80 check
        server portal02 portal02:80 check
frontend https-portal
        bind sslvip01:443 ssl crt /etc/ssl/certs/quantum.pem
```

```
        default_backend portal_servers
        option forwardfor
backend portal_servers
        mode http
        balance source
        option forwardfor
        option forwardforport
        reqadd X-Forwarded-Proto:\ https
        server portal01 portal01:80 check
        server portal02 portal02:80 check
```

h. Restart `haproxy` portal.

/etc/init.d/haproxy-portal restart

i. Delete `lbvip02` resource.

/usr/sbin/pcs resource delete lbvip02

j. Create `lbvip02` and `sslvip01` resources.

/var/broadhop/init_pacemaker_res.sh

k. Restart httpd to use correct lbvip02 IP.

- SSH portal01 and restart httpd service.

/etc/init.d/httpd restart

- SSH portal02 and restart httpd service.

/etc/init.d/httpd restart

Step 2 27717 replica set members are in startup state, recreate replica set.

a. Go to pcrfclient01, sessionmgr01 and sessionmgr02, and execute the following command:

/etc/init.d/sessionmgr-27717 stop

b. Delete current data directory.

\rm -fr /var/data/sessions.1/*

c. Go to pcrfclient01, sessionmgr01 and sessionmgr02, and execute the following command:

/etc/init.d/sessionmgr-27717 start

/var/broadhop/initialize_replicaset.sh --port 27717 --hosts sessionmgr01,sessionmgr02 --arbiter pcrfclient01 --set set01

Step 3 Execute the following command to check errors:

/var/qps/install/7.0.0/scripts/bin/diag/diagnostics.sh (**shows some memory and basic port unreachable errors**)

a. Install bc and nc, using the following commands:

yum install bc

yum install nc

b. Open port 6514 on pcrfclient01 and pcrfclient02, add highlighted bold mark line in `/etc/sysconfig/iptables` and `restart iptables`.

```
-A INPUT -i eth0 -p udp -m multiport --ports 6514 -m comment --comment
"100 allow logstash syslog access" -j ACCEPT
-A INPUT -i eth0 -p tcp -m multiport --ports 6514 -m comment --comment
"100 allow logstash syslog access tcp" -j ACCEPT
```

/etc/init.d/iptables restart

Enable/disable Debit Compression

Debit compression can be used to identify what all the debits have happened for the subscriber. This data can also be used to cross check the debits with external entities.

- To disable compression: add/edit the following flag in `/etc/broadhop/qns.conf` file.

  -DcompressDebits=false

- To enable compression: add/edit the following flag in `/etc/broadhop/qns.conf` file.

  -DcompressDebits=true

We can also check directly in mongo how balance has been debited /credited for subscriber using the following queries:

Command to find subscriber:

- SPR db

  $use spr

  $db.subscriber.find({

  “credentials_key” : [

  {

  “network_id_key” : "111111201"

  }]});

  Or

- db.subscriber.find({“network_id_key” : “886906007135”})db.subscriber.find({“network_id_key” : “111111201”})

Output:


```
{
        "_id" : ObjectId("001000009576290454afdc77"),
        "_id_key" : "001000009576290454afdc77",
        "name_key" : {

        },
        "end_date_key" : null,
        "realm_key" : null,
        "parent_id_key" : null,
        "billing_info_key" : {
                "rate_plan_code_key" : null,
                "charging_id_key" : null
        },
        "status_key" : "ACTIVE",
        "version_key" : 0,
        "start_date_key" : null,
        "credentials_key" : [
                {
                        "network_id_key" : "111",
                        "description_key" : null,
                        "password_key" : null,
                        "type_key" : null,
                        "expiration_date_key" : null
                }
        ],
        "role_key" : "READ_ALL",
        "external_id_key" : null,
        "_transId" : "d2a3f602-69bb-4047-af6f-c979ec36732f-1"
}
```


Use "_id_key" output from the above command as subscriber id:

Balance_mgmt

$use balance_mgmt

$db.account.find({"subscriberId" : "001000009576290454afdc77"}).pretty();

Diameter proxy error in diagnostics.sh output

When you execute `diagnostics.sh` script on pcrfclient01 VM and it shows the following errors related to diameter proxy:

```
diameter_proxy-lb01_A DOWN L4CON

Sessions (current,max,limit): 0,0, Rate (sessions,max,limit): 0,0, Last Status
change (seconds): 2513094

diameter_proxy-lb01_B DOWN L4CON

Sessions (current,max,limit): 0,0, Rate (sessions,max,limit): 0,0, Last Status
change (seconds): 2513093

diameter_proxy-lb01_C DOWN L4CON

Sessions (current,max,limit): 0,0, Rate (sessions,max,limit): 0,0, Last Status
change (seconds): 2513092

diameter_proxy-BACKEND DOWN

Sessions (current,max,limit): 0,0,2000 Rate (sessions,max,limit): 0,0, Last
Status change (seconds): 2513092
```

The error L4CON message indicates that there is connection problem (e.g., “Connection refused” or “No route to host”) at layer 1-4. And the error message diameter_proxy-BACKEND DOWN signifies that all the service specified in diameter_proxy section in haproxy.cfg are down.

1. Check whether HAProxy is running on load balancer VM (i.e). Specifically for this error message, we should check in lb01.
2. Look into haproxy configuration:

   vi /etc/haproxy/haproxy.cfg

   It should show similar entries as shown below. Try to telnet to corresponding load balancer VM with corresponding ports:

   listen diameter_proxy lbvip01:3868

   mode tcp

   option tcpka

   balance leastconn

   server lb01_A lb01:3868 check inter 30s

   server lb01_B lb01:3869 check inter 30s

   server lb01_C lb01:3870 check inter 30s

   server lb02_A lb02:3868 check inter 30s

   server lb02_B lb02:3869 check inter 30s

   server lb02_C lb02:3870 check inter 30s

Portal Landing page is slow (or) not getting redirected to Portal

If you encounter slowness in landing page (or) if you are not getting redirect to portal page, check the following

- Check whether you have any firewall issues. check on port 80 or 8080.
- Check whether “Httpd” (apache) services running on both the portal0x VM.

- Check whether “stunnel (port: 443)” is running on Portal load balance Virtual machine.
- Check whether HA-proxy is running in active portal load balancer VM and while heartbeat should be running on both portal load balancer VM.
- On session manager VM, check whether mongo service is running on the port 27749 or 27717(port 27749 or 27717 is used for portal in most of CPS deployment).
- Check whether your portal and portal load balancer VM are synchronized with NTP like other VMs in your set-up.
- If the portal and portal load balancer VM are active and standby try switching to secondary and see if the situation is improving or not.
- Check MongoDb logs `/var/log/mongodb-27717.log` or `/var/log/mongodb-27749.log` and if you see the following error:

```
[initandlisten] connection refused because too many open connections: 819

[initandlisten] connection refused because too many open connections: 819
```

  - Check the number of open connections on session manager on the corresponding port where portal resides. E.g., `netstat -anp | grep 27717 | wc -l`
  - Try to increase the maximum number of open files in the file `/etc/init.d/sessionmgr-27717` and try to increase the value for open file to 2048 or 4096 with the attribute name. We can reach up-to 80% of this value `ulimit –n 2048` or `ulimit –n 4096`.
  - In order for the changes to come into effect please restart the session manager on respective port E.g., s`ervice sessionmgr-27717 restart`
- Check whether you are receiving proper ACK (acknowledgment) immediately for the SYN request sent to the stunnel on portallb VM. If you are not receiving try the following:
  - Check how many existing open connections you have for `stunnel netstat -ant | grep stunnel | wc -l` if the established connection is 80% of defined value, you have to increase the limit in file `/etc/init.d/stunnel` on Portal load balancer.
- Try to set the `sysctl reuse` parameter to 1 on portal load balancer and portal virtual machines. This allows reuse of sockets in TIME_WAIT state for new connections
  - Go to `/etc/sysctl.conf` file on portal and portal load balancer VM
  - Set the parameter `net.ipv4.tcp_tw_reuse = 1`
- If you are still facing issue then please collect below mentioned logs from portal virtual machine and debug further
  - /var/www/portal/app/tmp/logs/api_request.log
  - /var/www/portal/app/tmp/logs/api_response.log
  - /var/log/httpd/access_log
  - /var/log/httpd/error_log

Not able to Publish the Policy in Policy Builder

- Check whether you are getting any errors in diagnostics.sh and try to fix the error.
- Make sure that you have the correct URL for the run time environment. E.g., http://pcrfclient01/repos/run

- Make sure that you have following configuration on `/etc/broadhop/pb/pb.conf` configuration file. If not then do the changes as shown below and run the `synconfig.sh` and `restartall.sh` for the changes to come into effect:

  AIO Sample Configuration:

  ```
  SESSION_TIMEOUT="-Dsession.timeout=9000"
  QNS_SESSION_DATABASE="-Dsession.db.primary=sessionmgr01
  -Dsession.db.secondary=sessionmgr02 -Dsession.db.port=27717
  -Dua.client.submit.audit=false"
  ```

  HA System Sample Configuration:

  ```
  SESSION_TIMEOUT="-Dsession.timeout=9000"
  QNS_SESSION_DATABASE="-Dsession.db.primary=sessionmgr01
  -Dsession.db.secondary=sessionmgr02 -Dsession.db.port=27717
  -Dua.client.submit.audit=true
  -Dua.client.server.url=http://:8080
  ```

Note The IP-address is usually LBVIP01 where the SOAP requests are sent to Unified API for our configuration.

- If you still face issue, collect and analyze the following logs:
  - `/var/log/broadhop/qns-engine-pb.log`
  - `/var/log/broadhop/service-qns-pb.log`.

CPS not sending SNMP traps to External NMS server

- Check whether the “snmpd” process is running in respective VM with the command `service snmpd status`. If it is stopped, start the snmpd process with the command `service snmpd start`.
- Check whether all the IP tables have been turned off and check the status of UDP port 162, provided we are using the same UDP port 162 at the NMS as well.
- Check the external NMS IP is defined in load balancer VM under `/etc/hosts` and also in the `/etc/snmp/scripts/ component_trap_convert` in place of “corporate_nms_ip”.
- Check the file `cat /etc/snmp/snmpd.conf` has the line “rocommunity Broadhop” because all the internal traps from various QNS VM to active Load balancer VM is been sent over this default community name “Broadhop” as mentioned above.
- Check the trap community name is same both in Load balancer and as well as in external NMS system E.g., cat /etc/snmp/scripts/snmp_communities trap_community=cisco (customer external NMS system should also have this same “cisco” community name.
- Check whether the traps from respective QNS VM is properly reaching active load balancer VM, this can be checked under `/var/log/snmp/trap`.
- Check for `/var/log/messages` on active load balancer for further analysis.

Diameter Peer Connectivity is Down

If your Diameter Peer connectivity is down, check the following:

1. Check the TCP connection on the diameter port (i.e) “netstat -pant | grep 3868". It should be in established state.
2. If the TCP connection is not getting established, disable the firewall `service iptables stop` and check the port status `/opt/broadhop/installer/support/add_open_port.sh pcrf 3868`
3. Open the Internet browser and go to http:///repos/run and check the published policies in runtime environment. You should notice the following configuration. If the following configuration is not there, then most probably its a bad publish.

   DiameterConfiguration-_4davIF2KEeOXe-MDH-2FEQ.xmi

   DiameterStack-default-_A5cgQF2LEeOXe-MDH-2FEQ.xmi
4. If the problem is not in CPS and something is mis-configured in PCEF then you may notice the following messages in CPS `tail -f /var/log/broadhop/service-qns-1.log`

```
Sending Alert Notification for host: pcef realm: lab.realm is down
Sending Alert Notification for host: pcef realm: lab.realm is back up
Sending Alert Notification for host: pcef realm: lab.realm is down
Sending Alert Notification for host: pcef realm: lab.realm is back up
```

SNMP Traps and Key Performance Indicators (KPIs)

This section covers the following topics:

- Full (HA) Setup
- All-in-one (AIO) Setup
- Traps Generated by CPS
- Components and KPI Values
- FAQs
- Reference Document

Full (HA) Setup

Step 1 Check whether `snmpd` service is running on all VMs. If the service is not running then start it by executing the command:

service snmpd start

Step 2 Check whether `snmptrapd` is running on LB VMs. If the service is not running then start it by executing the command:

service snmptrapd start

Step 3 On pcrfclient01:

a. Verify whether `/etc/broadhop/<server_name>/snmp/manager.xml` file has below content. If the content is not present, add the following content to the file:

Note server_name details can be found from `/etc/broadhop/server` file.

```
<manager-list>
 <manager>
  <address>localhost</address>
  <port>162</port>
  <version>1</version>
 </manager>
</manager-list>
```

b. Execute the command `syncconfig.sh` so that the change done in Step a gets synchronized to all VMs.

c. Execute the command `restartall.sh` to restart all qns processes.

Perform the following steps on all pcrfclient VMs:

d. Verify whether `service monit` is running or not. If the service is not running then start it by executing the command:

service monit start

Note If monit in not installed on pcrfclient VMs then you need to get the monit rpm and install it in on all pcrfclient VMs.

e. Verify whether `monit.conf` file has entries of check_program executing different traps generating script. If the entries are not present, then get the latest `monit.conf` file for pcrfclient VMs and update it on all pcrfclient VMs setup.

f. Restart monit service.

service monit start

Step 4 On LB VMs:

a. Verify whether `/etc/hosts` file has the entry as `corporate_nms_ip <ip_address>` .

Note <ip_address> is the NMS address.

b. Verify whether `service monit` is running or not, If the service is not running then start it by executing the command:

service monit start

Note If monit in not installed on LB VMs then you need to get the monit rpm and install it on all LB VMs.

c. Verify whether `monit.conf` file has entries of check_program executing different traps generating script. If the entries are not present then get the latest `monit.conf` file for LB VMs and update it on all LB VMs,

d. Restart monit service.

service monit start

All-in-one (AIO) Setup

Step 1 Verify whether snmpd and snmptrapd services are running. If the services are not running, then start them by executing the following commands:

service snmpd start

service snmptrapd start

Step 2 Verify whether `/etc/broadhop/<server_name>/snmp/manager.xml` file has below content. If the content is not present, add the following content to the file:

Note server_name details can be found from `/etc/broadhop/server` file.

```
<manager-list>
<manager>
<address>localhost</address>
<port>162</port>
<version>1</version>
</manager>
</manager-list>
```

Step 3 Execute `restartall.sh` command to restart all qns processes.

Step 4 Verify whether /etc/hosts has entry as corporate_nms_ip <ip_address>.

Note <ip_address> is the NMS address.

Step 5 Verify whether service monit is running or not. If the service is not running then start it by executing the command:

service monit start

Note If monit in not installed on LB VMs then you need to get the monit rpm and install it on all LB VMs.

Step 6 Verify whether `monit.conf` file has entries of check_program executing different traps generating script. If the entries are not present then get the latest monit.conf file for AIO VM and update it on all AIO VM.

Step 7 Restart monit service.

service monit start

Traps Generated by CPS

The following tables describes the various traps generated by CPS and different procedures associated with individual traps to test the traps. For example, when a trap is generated, it is thrown to LBVIP02 (can be on port 162. On LB, process snmptrapd is listening on port 162. When snmptrap sees trap on 162, it logs it in the file `/var/log/snmpd/trap` and re-throws it on corporate_nms_ip on port 162.

This section covers the following topics:

- Component Notifications
- Application Notifications

Component Notifications

Alarm Name	Procedure to Test
Disk Full: This alarm gets generated for following file system: 1. / 2. /var 3. /home 4. /boot 5. /opt	**Step 1** In /etc/snmp/snmpd.conf, set "disk / 90%". (So when disk remaining is 90% ie. Disk occupied is 10%, alarm is generated.) **Step 2** service snmpd restart **Step 3** Verify the generated alarm on NMS server and /var/log/snmp/trap of active lb. **Step 4** trap have messages like :dskErrorMsg.1 = STRING: /: less than 90% free (= 100%)
Disk Full Clear: This alarm gets generated for following file system: 1. / 2. /var 3. /home 4. /boot 5. /opt	**Step 1** In /etc/snmp/snmpd.conf, set "disk / X%". (X should just less than actual remaining space. For example, if drive / is 25% full, put 74% as value of X). **Step 2** service snmpd restart **Step 3** Now dump a big file which consumes at least 2-3 % space on drive /. This generates diskful alarm first. **Step 4** Then delete this file. This generates clear alarm. **Step 5** Verify the generated alarm on NMS server and /var/log/snmp/trap of active lb.

Alarm Name	Procedure to Test	
Load Average of local system: The alarm gets generated for 1 minute 5 minute 15 minute Average	**Step 1**	In /etc/snmp/snmpd.conf, set "load 1 1 1". (first digit corresponds to average 1 min load. Second digit is for 5 minutes average load. Third is for 15 mins. When it crosses 1 %, alarm is generated.)
	Step 2	service snmpd restart
	Step 3	Verify the generated alarm on NMS server and /var/log/snmp/trap of active lb.
	Step 4	trap have message like 1 min Load Average too high (= 1.41)
Load Average Clear of local system	**Step 1**	In /etc/snmp/snmpd.conf, set "load 1 1 1". (first digit corresponds to average 1 min load. Second digit is for 5 minutes average load. Third is for 15 mins. When it crosses 1 %, alarm is generated.)
	Step 2	service snmpd restart
	Step 3	Verify the generated alarm on NMS server and /var/log/snmp/trap of active lb.
	Step 4	trap have message like 1 min Load Average too high (= 1.41)
	Step 5	Now wait till load comes below 1 % OR write a script which runs in infinite loop and create some load on CPU. Killing this script reduces the load and generates clear trap.
Low Swap memory alarm	**Step 1**	swapoff -a /* - This command makes the swap off. You can see swap as 0 in top command output. The trap should get generated if swap is 0 in output of top*/.
	Step 2	Verify the generated alarm on NMS server and /var/log/snmp/trap of active lb.
	Step 3	trap have message mentioning swap.
Low Swap memory clear	**Step 1**	swapon -a /* - This will make swap to on. The top command output will show the swap memory size. The clear trap gets generated if swap alarms gets generated earlier*/.
	Step 2	Verify the generated alarm on NMS server and /var/log/snmp/trap of active lb.
	Step 3	trap have message mentioning swap.

Alarm Name	Procedure to Test
Link Down Alarm: This alarm gets generated for all physical interface attached to the system.	**Step 1** ifconfig <interface_name> down (For example, ifconfig eth2 down) **Step 2** within 1 minute interval interface down trap gets generated **Step 3** Verify the generated alarm on NMS server and /var/log/snmp/trap of active lb.
Link Up Alarm: This alarm gets generated for all physical interface attached to the system.	**Step 1** ifconfig <interface_name> up (For example, ifconfig eth2 up) **Step 2** within 1 minute interval interface up trap gets generated **Step 3** Verify the generated alarm on NMS server and /var/log/snmp/trap of active lb.
Low Memory Alert Alarm	**Step 1** In output of top command find out the current free RAM memory value. **Step 2** Update snmpd.conf file monitor entry for Low Memory Alert to have value just less than the current free RAM memory value. **Step 3** service snmpd restart **Step 4** Do some activity on VM such as running some command or starting some process so that free RAM value goes below the configured value. **Step 5** The low memory alert alarm gets generated within a minute interval. **Step 6** Verify the generated alarm on NMS server and /var/log/snmp/trap of active lb.
Low Memory Clear Alarm	**Step 1** In output of top command find out the current free RAM memory value. **Step 2** Update snmpd.conf file monitor entry for Low Memory Clear to have value just more than the current free RAM memory value. **Step 3** service snmpd restart **Step 4** Kill some processes on VM so that free RAM memory value is more than the configured value. **Step 5** The low memory clear alarm gets generated within a minute interval. **Step 6** Verify the generated alarm on NMS server and /var/log/snmp/trap of active lb.

Application Notifications

Alarm Name	Procedure to Test	
License Usage Threshold Exceeded	**Step 1**	Create the license having small no. of Usage Threshold limit.
	Step 2	Install the above created license on setup.
	Step 3	restart all qns processes
	Step 4	Send multiple request so that it crosses the threshold limit.
	Step 5	The License Usage Threshold Exceeded alarm gets generated.
	Step 6	Verify the generated alarm on NMS server and /var/log/snmp/trap of active lb.
Memcached ConnectError	**Step 1**	Kill the memcached process running on active LB.
	Step 2	Within 5 minutes of interval Memcached Connect Error trap gets generated from QNS VMs.
	Step 3	Verify the generated alarm on NMS server and /var/log/snmp/trap of active lb.
ApplicationStartError	**Step 1**	Rename any of the dependent jar files from /opt/broadhop/qns-1/plugins dir e.g. rename com.broadhop.spr.dao jar file.
	Step 2	restart qns process
	Step 3	Within 5 minute of interval ApplicationStartError Trap getsgets generated.
	Step 4	Verify the generated alarm on NMS server and /var/log/snmp/trap of active lb.
LicensedSessionCreation	**Step 1**	Create the license having small no. of Session Usage Threshold limit.
	Step 2	Install the above created license on setup.
	Step 3	restart all qns processes
	Step 4	Send multiple request so that it crosses session threshold limit.
	Step 5	For the next request after the limit over LicenseSessionCreation alarm gets generated.
	Step 6	Verify the generated alarm on NMS server and /var/log/snmp/trap of active lb.

Alarm Name	Procedure to Test	
InvalidLicense	**Step 1**	Copy the license of pcrfclient02 on pcrfclient01 or create a license for pcrfclient02 and install it on pcrfclient01.
	Step 2	restart lmgrd service
	Step 3	restart qns process
	Step 4	Within 5 minutes of interval the License invalid trap gets generated.
	Step 5	Verify the generated alarm on NMS server and /var/log/snmp/trap of active lb.
PolicyConfiguration	**Step 1**	Configure some wrong policy in PB Policies tab.
	Step 2	Publish the configuration.
	Step 3	restartall.sh
	Step 4	Last policy configuration failed with the following message:xxx trap gets generated.
	Step 5	Verify the generated alarm on NMS server and /var/log/snmp/trap of active lb.
SessionManagerUnavailable	**Step 1**	Make any sessionmgr down using command such as etc/init.d/sessionmgr-27017.
	Step 2	Within 5 minute of interval the SessionManagerUnAvailable trap gets generated.
	Step 3	Verify the generated alarm on NMS server and /var/log/snmp/trap of active lb.
PoliciesNotConfigured	**Step 1**	Create the invalid blueprint (java code having syntax error) in PB under Policies tab.
	Step 2	Assign the created blueprint to some policies.
	Step 3	Publish the configuration.
	Step 4	restart all qns process
	Step 5	PoliciesNotConfigured trap gets generated.
	Step 6	Verify the generated alarm on NMS server and /var/log/snmp/trap of active lb.
DiameterPeerDown	**Step 1**	Make a seagull diameter call.
	Step 2	After seagull script terminate it generates the diameter peer down trap.
	Step 3	Verify the generated alarm on NMS server and /var/log/snmp/trap of active lb.

Alarm Name	Procedure to Test
HA_Failover	**Step 1** Cat /etc/broadhop/mongoConfig.cfg. **Step 2** If there are two or more sessionmgr ports configured as replica set then find out the one acting as a primary member using rs.isMaster().primary. **Step 3** Shutdown the primary instance of sessionmgr. **Step 4** Within 1 minute of interval HA Failover trap gets generated. **Step 5** Verify the generated alarm on NMS server and /var/log/snmp/trap of active lb.
Geo_Failover	**Step 1** Cat /etc/broadhop/mongoConfig.cfg. **Step 2** There should be primary and secondary member set for each replica set. Found the current active sessionmgr instance of a replica set using rs.isMaster().primary. **Step 3** Shutdown all sessionmgr instances of active sessionmgr instance set. **Step 4** Within 1 minute of interval Geo Failover trap gets generated. **Step 5** Verify the generated alarm on NMS server and /var/log/snmp/trap of active lb.
All_replica_of_DB_down	**Step 1** Get all members of replica set from /etc/broadhop/mongoconfig.cfg. **Step 2** Go to each sessionMgr of a replica set and stop the sessionmgr service or shutdown the sessionmgr VM. **Step 3** Within 5 minutes of interval All replicas of DB Down trap gets generated. **Step 4** Verify the generated alarm on NMS server and /var/log/snmp/trap of active lb.
No_Primary_member_found	**Step 1** run diagnostics.sg -get_replica_status. **Step 2** Choose any set which has arbiter and primary and secondary db member. **Step 3** Shutdown Arbiter VM. **Step 4** Shutdown Primary Sessionmgr VM. **Step 5** Within 5 minute of interval No primary Member found trap gets generated. **Step 6** Verify the generated alarm on NMS server and /var/log/snmp/trap of active lb.

Alarm Name	Procedure to Test
Secondary DB Down	**Step 1** Cat /etc/broadhop/mongoConfig.cfg. **Step 2** Shutdown any of the sessionmgr VM listed in the configuration as db member of replica set. **Step 3** Within 5 minute of interval Secondary DB down trap gets generated. **Step 4** Verify the generated alarm on NMS server and /var/log/snmp/trap of active lb.
Arbiter Down	**Step 1** Cat /etc/broadhop/mongoConfig.cfg. **Step 2** Shutdown any of the arbiter VM listed in the configuration. **Step 3** Within 5 minute of interval Arbiter down trap gets generated. **Step 4** Verify the generated alarm on NMS server and /var/log/snmp/trap of active lb.
Config Server is Down	**Step 1** Cat /etc/broadhop/mongoConfig.cfg. **Step 2** Shutdown any of the config server VM listed in the configuration. **Step 3** Within 5 minute of interval config server down trap gets generated. **Step 4** Verify the generated alarm on NMS server and /var/log/snmp/trap of active lb.
Site Down	Assumption: Configured the same NMS address on both sites. **Step 1** Make lbvip01 and lbsvip01 down of one site using command ifconfig eth1:0 down on active lb and ifconfig eth1:0 down on standby lb of same site. **Step 2** Within 5 minutes of interval Site Down trap gets generated from other site. **Step 3** On configured NMS server the trap gets received and tail -f /var/log/snmp/trap on active LB of other site will log the site down generated trap.
VM Down	**Step 1** cat /etc/hosts file on lb VM. **Step 2** Make any one of the VM down listed under /etc/hosts. **Step 3** Within 5 minutes of interval VM down trap getsgets generated. **Step 4** Verify the generated alarm on NMS server and /var/log/snmp/trap of active lb.

Alarm Name	Procedure to Test
QPS Process Down	**Step 1** Make qns process down using command service qns stop. **Step 2** Within 5 minutes of interval CPS process down trap gets generated. **Step 3** Verify the generated alarm on NMS server and /var/log/snmp/trap of active lb.
Admin Logged In	**Step 1** Create a new telnet session for any VM and login with root user on it. **Step 2** Within 1 minute interval Admin User logged in trap gets generated. **Step 3** Verify the generated alarm on NMS server and /var/log/snmp/trap of active lb.
VirtualInterfaceError	**Step 1** Login to active lb VM. **Step 2** Run command ifconfig eth1:0 down **Step 3** VirtualInterfaceError trap with the interface name gets generated. **Step 4** You can see this trap on NMS server.
Developer Mode License traps	**Step 1** Use developer mode in qns.conf file. **Step 2** restart qns process **Step 3** Within 5 minutes interval the Developer Mode License gets generated. **Step 4** Verify the generated alarm on NMS server and /var/log/snmp/trap of active lb.
Can't create sessions due to errors.	**Step 1** Install invalid license on the setup. **Step 2** Send session creation request such as diameter/radius call request. **Step 3** Session creation not allowed, trap gets generated. **Step 4** Verify the generated alarm on NMS server and /var/log/snmp/trap of active lb.

Alarm Name	Procedure to Test
ZeroMQConnectionError	**Step 1** Start QNS. **Step 2** Start Messaging Load (CCR-I,CCR-U,CCR-T) scenario at high TPS. **Step 3** The trap will be seen if message sending over socket between LB and QNS fails (Due to socket send errors). For subsequent failures there is no further trap raised. **Step 4** Verify the generated alarm on NMS server and /var/log/snmp/trap of active lb.
ZeroMQConnectionError(clear)	**Step 1** This trap will be sent when message send on socket succeeds after the prior failure. **Step 2** Verify the generated alarm on NMS server and /var/log/snmp/trap of active lb.

Components and KPI Values

The following table describes component and KPI values and procedures to get them.

This sections covers the following topics:

- Component Values
- KPI Values

Component Values

Component Values	
LB01	snmpwalk -v 2c -c broadhop -m +BROADHOP-MIB:BROADHOP-QNS-MIB <lbvip01> BROADHOP-QNS-MIB::broadhopProductsQNSComponents53LB01 List all(14)component scalar parameter values of LB01
LB02	snmpwalk -v 2c -c broadhop -m +BROADHOP-MIB:BROADHOP-QNS-MIB <lbvip01> BROADHOP-QNS-MIB::broadhopProductsQNSComponents53LB02 List all(14)component scalar parameter values of LB02

KPI Values

KPI Values	
LB01/LB02	snmpwalk -v 2c -c broadhop -m +BROADHOP-MIB:BROADHOP-QNS-MIB <lbvip01> BROADHOP-QNS-MIB::broadhopProductsQNSKPI53LB(01/02) List all KPIs value of LB, if all values are 0 then ExternalCurrentSession **Step 1** Open another terminal. **Step 2** telent lbvip01 8080 **Step 3** On previous terminal run the above snmpwalk command again. **Step 4** This time it will display the externalCurrentSession KPIs value to be 1. **Step 5** Repeat the process with more telnet session open on lbvip01 8080 port InternalCurrentSession **Step 1** Open another terminal. **Step 2** telent lbvip02 8080 **Step 3** On previous terminal run the above snmpwalk command again. **Step 4** This time it will display the internalCurrentSession KPIs value to be 1. **Step 5** Repeat the process with more telnet session open on lbvip01 8080 port.

KPI Values	
PortalLB01/PortalLB02	snmpwalk -v 2c -c broadhop -m +BROADHOP-MIB:BROADHOP-QNS-MIB <lbvip01> BROADHOP-QNS-MIB::broadhopProductsQNSKPI53PortalLB(01/02) List all KPIs value of PortalLB, if all values are 0 then ExternalCurrentSession **Step 1** Open another terminal. **Step 2** telent sslvip01 80 **Step 3** On previous terminal run the above snmpwalk command again. **Step 4** This time it will display the externalCurrentSession KPIs value to be 1. **Step 5** Repeat the process with more telnet session open on sslvip01 80 port.
QNS01/QNS02/QNS03 /QNS04	snmpwalk -v 2c -c broadhop -m +BROADHOP-MIB:BROADHOP-QNS-MIB <lbvip01> BROADHOP-QNS-MIB::broadhopProductsQNSKPI53QNS(01/02/03/04) List all KPIs value of QNS VM For example, the output will be displayed as below: BROADHOP-QNS-MIB::kpi53QNS04PolicyCount = STRING: 1 BROADHOP-QNS-MIB::kpi53QNS04PolicyCount.0 = STRING: 1 BROADHOP-QNS-MIB::kpi53QNS04QueueSize = STRING: 0 BROADHOP-QNS-MIB::kpi53QNS04QueueSize.0 = STRING: 0 BROADHOP-QNS-MIB::kpi53QNS04FailedEnqueueCount = STRING: 0 BROADHOP-QNS-MIB::kpi53QNS04FailedEnqueueCount.0 = STRING: 0 BROADHOP-QNS-MIB::kpi53QNS04ErrorCount = STRING: 0 BROADHOP-QNS-MIB::kpi53QNS04ErrorCount.0 = STRING: 0 BROADHOP-QNS-MIB::kpi53QNS04SessionCount = STRING: 0 BROADHOP-QNS-MIB::kpi53QNS04SessionCount.0 = STRING: 0 BROADHOP-QNS-MIB::kpi53QNS04FreeMemory = STRING: 3943912704 BROADHOP-QNS-MIB::kpi53QNS04FreeMemory.0 = STRING: 3943912704

FAQs

Q. Where to check if traps are getting generated or not?

A. On active LB VMs tail the below log file `/var/log/snmp/trap` to get the generated trap.

Q. Traps are getting generated from different VMs such as pcrfclient or QNS VMs but not getting logged to /var/log/snmp/trap and not appear on NMS receiver?

A. Check on Active LB VM if /etc/snmp/scripts/application_trapv1_convert and component_trap_convert files are present or not. If the files are present but traps are not getting generated then try to execute the following commands and test it again

dos2unix /etc/snmp/scripts/application_trapv1_convert

dos2unix /etc/snmp/scripts/component_trap_convert

Q. The traps are getting logged in `/var/log/snmp/trap` but not receive on NMS?

A.

1. Check the setup configuration is correct or not as per the instruction given above.
2. Perform the steps given in Question.
3. Check if NMS IP is accessible from LB VMs. Using command such as ping <nms_ip>

Q. DB related traps not getting generated?

A.

1. Check the setup is configured and running as per instruction given above.
2. On pcrfclient/lb vms all the scripts generating the traps are logging the details inside `/var/log/broadhop/script/<script_name><date>.log` file. Open log file to check if there is any error in the script or is it generating the traps successfully or not. If not generated by script then contact system administrator team to resolve the issue.

Q. How can I enable debug logging level in CPS?

A.

1. Login into pcrfclient01 VM.
2. Go to directory cd /etc/broadhop.

   vi logback.xml

   Perform the following changes:

   a. logger name=“com.broadhop.policy.trace” “level=info” this to be changed to “debug (i,e) logger name=“com.broadhop.policy.trace” level=”debug””

   b. root level= “info” change this to “debug (i.e) root level=”debug”"
3. Save and exit.
4. Run the command “synconfig.sh”.

Note It is advisable to run the production setup with “Info” or “Warn” state rather than “debug” level.

Q. What is the difference between pcrfclient01 and pcrfclient02 virtual machines?

A.

pcrfclient01 --Master / Standby

pcrfclient02 ---Slave / Standby

pcrfclient02 support high availability of policy related services but it may not replicate all the services which were present in pcrfclient01.

Q. How many java virtual instances does my qns virtual machine have?

A. If you have CPS 5.5 and above, we have only one java instance running per qns virtual machine. If you have CPS 5.5 and lower then we have two instances running per qns virtual machines

Q. What is the ideal threshold limit for processor load in particular VM?

A. Ideally the threshold limit should be equal to number of vCPU that are present in the VM.

You can check the vCPU on a particular VM using the following command:

grep ^processor /proc/cpuinfo | wc -l

So if we have 12 vCPU, then threshold limit for processor load is 12.

Q. Does CPS support Gx_V9?

A. No, Gx_v9 is deprecated. We should use GX_TGPP instead in Diameter stack configuration. CPS support usage_monitoring with GX_TGPP.

Q. What is the different between mongos and mongod instance?

A. mongos instances runs on storage server while mongod instances runs on configuration server.

mongos instances are used for sharding i.e. horizontal scaling and logical replication of databases. For the mongos instances to be running in storage server it is mandatory/prerequisite that we need to have “mongod” instances running on configuration server.

Q. How can I rotate my mongodB logs?

A. On the session manager virtual machine open the mongodb file by executing the following command:

cat/etc/logrotate.d/mongodb,

You will have output as similar to the one shown below:

A. /var/log/mongodb-27717.log /var/log/mongodb-27718.log /var/log/mongodb-27719.log /var/log/mongodb-27720.log

```
{
daily
rotate 5
copytruncate
create 640 root root
sharedscripts
postrotate
endscript
}
```

In the above script the mongodb logs are rotated daily and it ensures that it keeps the latest 5 backups of these log files.

Q. I have multiple release trains (software releases) in my repository file (cat/etc/broadhop/repositories). Which one will take high precedence?

A. The highest version number is always selected and it is all merged. The versions are classified as follows and each type of versions will have version number and highest version takes high precedence:

1. major
2. Minor
3. Patch
4. Build

Q. What are the timers in diameter stack?

A. There are multiple timers associated with diameter stack they are,

- CEA Time-out: Determines how long it takes for CER/CEA (Capability Exchange Request and Answer) exchanges to time-out if there is no response. The delays are in milliseconds.
- LAC time-out: Determines how long the stack waits to retry the communication with a peer that has stopped answering DWR (Device watch dog request) messages. The delay is in milliseconds.
- DWA time-out: Determines how long it takes for a DWR/DWA (watch dog request/answer) exchange to time-out if there is no response. The delay is in milliseconds.
- DPA Time-out: Determines how long it takes for a DPR/DPA (disconnect peer request/answer) exchange to time-out if there is no response. The delay is in milliseconds.
- REC Time-out: Determines how long it takes for the reconnection procedure to time-out. The delay is in milliseconds.
- Stale Session Timer: Once the session is created in CPS and if the CPS doesn't receive any response from PCEF within this timer then CPS will remove the session. Default stale session timer is 180 Minutes.
- In Response time-out: The CPS will wait for this timer to receive the response/Answer from PCEF. Upon expiration of this timer the message will be discarded. But the session will not be removed until the stale session timer expires.

Reference Document

For more information on SNMP traps and KPIs, refer to *CPS 7.0 Alarming and SNMP Guide*.

Puppet based VM Installer Troubleshooting

This section covers the following troubleshooting scenarios:

- Enable Custom Puppet to Configure Deployment
- Deployed Node is not able to access Cluster Manager VM
- Not Able to Deploy VM
- VMs are not able to Communicate with each other
- CSCuq83755 — Policy builder is losing repositories
- CSCuq02899 — create_policy_builder_user.sh does not add read-only user

- Not able to access IPv6 Gx port from PCEF/GGSN
- CSCuq55352 — Mongo Session db reboots into STARTUP Mode

Enable Custom Puppet to Configure Deployment

Some customers may need to customize the configuration for their deployment. As we are using puppet to configure the system, we need to use the following steps to make the changes in the installer.

Note If system configurations are manually changed in the VM itself, they might get lost after VMs are re-puppetized.

First you need to determine what node types you need to override. This is heavily dependent on the requirements of the change.

To explain the process, let us consider that we modify all VMs built from an installer, so we use the `qns` node definition.

For the above mentioned example, add custom routes via the examples42-network Puppet module. (For more information on the module, refer to https://forge.puppetlabs.com/example42/network).

Step 1 Make sure that the proper paths are available:

```
$ mkdir -p /etc/puppet/env_config/nodes
```

Step 2 Install the necessary Puppet module:

```
$ puppet module install \

--modulepath=/etc/puppet/env_config/modules:/etc/puppet/modules \

example42-network

Notice: Preparing to install into /etc/puppet/env_config/modules ...

Notice: Downloading from https://forge.puppetlabs.com ...

Notice: Installing -- do not interrupt ...

/etc/puppet/env_config/modules

example42-network (v3.1.13)
```

For more information on installing and updating Puppet modules, refer to https://docs.puppetlabs.com/puppet/latest/reference/modules_installing.html

Step 3 Copy the existing node definition into the `env_config` nodes:

```
$ cp /etc/puppet/modules/qps/nodes/qps.yaml \

/etc/puppet/env_config/nodes
```

Step 4 Add a reference to your custom Puppet manifest:

```
$ echo '  custom::static_routes:' >> \
```

/etc/puppet/env_config/nodes/qps.yaml

Step 5 Create your new manifest for static routes:

```
$ cat

 >/etc/puppet/env_config/modules/custom/manifests/static_routes.pp <<EOF class
     custom::static_routes {

   network::route {'eth0':

    ipaddress => ['192.168.1.0',],

    netmask   => ['255.255.255.0',],

    gateway   => ['10.105.94.1',],

   }

}

EOF
```

Step 6 Validate the syntax of your newly created puppet script(s):

```
$ puppet parser validate

/etc/puppet/env_config/modules/custom/manifests/static_routes.pp
```

Step 7 Rebuild your Environment Config:

```
$ /var/qps/install/current/scripts/build/build_env_config.sh
```

Step 8 Reinitialize your environment:

```
$ /var/qps/install/current/scripts/updater/reinit.sh
```

At this point your new manifest is applied across the deployment. For more details, refer to the installer image in the `/etc/puppet/env_config/README`.

It is recommended that version control is used to track changes to these Puppet customizations.
For example, to use 'git', perform the following steps:

Step 1 Initialize the directory as a repository:

```
# git init

Initialized empty Git repository in /var/qps/env_config/.git/
```

Step 2 Add everything:

```
# git add .
```

Step 3 Commit your initial check-in:

```
# git commit -m 'initial commit of env_config'
```

Step 4 If you are making more changes and customizations, make sure you create new revisions for those:

git add .

git commit -m 'updated static routes'

Deployed Node is not able to access Cluster Manager VM

- Make sure the `/etc/hosts` in the VM node contains the installer entry.
- Make sure the IP address of the VM node is in the Internal subnet as specified in the VLAN excel sheet.

Not Able to Deploy VM

- Make sure the entries in the Definitions sheet, Datastores column of the excel file does not contain any space in the string.
- Make sure the *hv_password_0* and *hv_user_0* (which is the ESX servers user name and password) are correct.
- Make sure the target esx server has enough memory for the VM.

VMs are not able to Communicate with each other

- Make sure they are on the same Internal subnet.
- Make sure the `/etc/hosts` file in the VM contains all the hosts specified in the excel sheet.

CSCuq83755 — Policy builder is losing repositories

Root Cause Analysis (RCA)

We have hapoxy load balancer which forwards request to Policy Builder server on pcrfclient01. If it is not available, then it forwards the request to backup server on pcrfclient02.

Consider pcrfclient01 is up and we added new repository from PB GUI. This repository gets saved on pcrfclient01 (on file at `/etc/broadhop/pb/policyRepositories.xml`, `/etc/broadhop/pb/publishRepositories.xml`).

After sometime if because of some reason pcrfclient01 is not accessible, haproxy sends request to pcrfclient02 where it does not find the above mentioned two files (`publishRepositories.xml`, `policyRepositories.xml`) and does not display any repository on PB GUI.

Fix

Currently, we are not supporting automatic synchronization of the two repository files (`/etc/broadhop/pb/policyRepositories.xml`, `/etc/broadhop/pb/publishRepositories.xml`).

So manually copy the two files from pcrfclient01 to pcrfclient02 or vice versa.

CSCuq02899 — create_policy_builder_user.sh does not add read-only user

In 7.0 puppet based installation we are not supporting `create_policy_builder_user.sh` script. Also user authentication is happening by linux pam.

To create a new user, perform the following steps:

Step 1 Create linux user by executing the following command:

- useradd -M admina

Step 2 Change password for newly created user:

- passwd admina

Step 3 To provide access to the user, edit the file `/var/www/svn/users-access-file` and enter username against admins for read/write access or enter against nonadmins to provide read only access.

Sample file:

```
[groups]
admins = broadhop, admina
nonadmins = read-only, test,
[/]
@admins = rw
@nonadmins = r
```

Not able to access IPv6 Gx port from PCEF/GGSN

Make sure the IPv6 firewall is disabled on lb01and lb02. If the firewall is not disabled, then you can disable it by executing the command:

service ip6tables stop

CSCuq55352 — Mongo Session db reboots into STARTUP Mode

Root Cause Analysis (RCA)

After restarting all sessionmgr* VMs at a time it appears that the sessionmgrs does not have data on them and configuration information is removed from the members. This is due to the setup session data db path “/data/sessions.1” directory mounted to the “tmpfs”.

The tmpfs is a special file system that does not reside on a physical disk but rather in a portion of your memory. This has the side effect that if you lose power (or reboot) all contents on tmpfs are lost.

Here all members are went down when power was lost and when the power was back, no data was found in replica-set members and only arbiter had the configuration information. The reason is that the members are configured as replica-set members but not a single member did not find the PRIMARY/SECONDARY in replica-set. This is the reason all members remain in STARTUP2 state.

Fix

We can execute `monitor_replica.sh` script from installer or pcrfclient01 VM to recover session db from STARTUP2 state.

```
cd /var/qps/bin/support/mongo

sh monitor_replica.sh
```

OR

We can add `monitor_replica.sh` script to the `crontab` so that every hour script will trigger automatically to check whether the session db is in STARTUP2 state or not. If script finds session db in STARTUP2 state, then it re-creates session db automatically.

Example:

```
crontab -e
```

Update the below line (It means every hour script will trigger):

```
0 * * * * /var/qps/bin/support/mongo/monitor_replica.sh -o /var/log/monitor_replica_$(date
    +%m%d%y)
```

Save the file.

Check Subscriber Access

Revised: July 10, 2015

This chapter covers the following sections:

- Checking Access, page 2-1

Checking Access

When you are confident that the installation and configuration tasks are complete and processing properly, try running a small amount of test traffic, following it through the system. Here are three ways to ascertain correct process of access from a subscriber perspective.

Testing Subscriber Access with 00.testAccessRequest.sh

00.testAccessRequest.sh is a test script used to test subscriber access to the ISG and CPS system.

You can find the **00.testAccessRequest.sh in /opt/broadhop/installer/isg/troubleshooting** directory on the CPS server.

To configure the subscriber used, edit **/opt/broadhop/installer/isg/troubleshooting/config.ini**

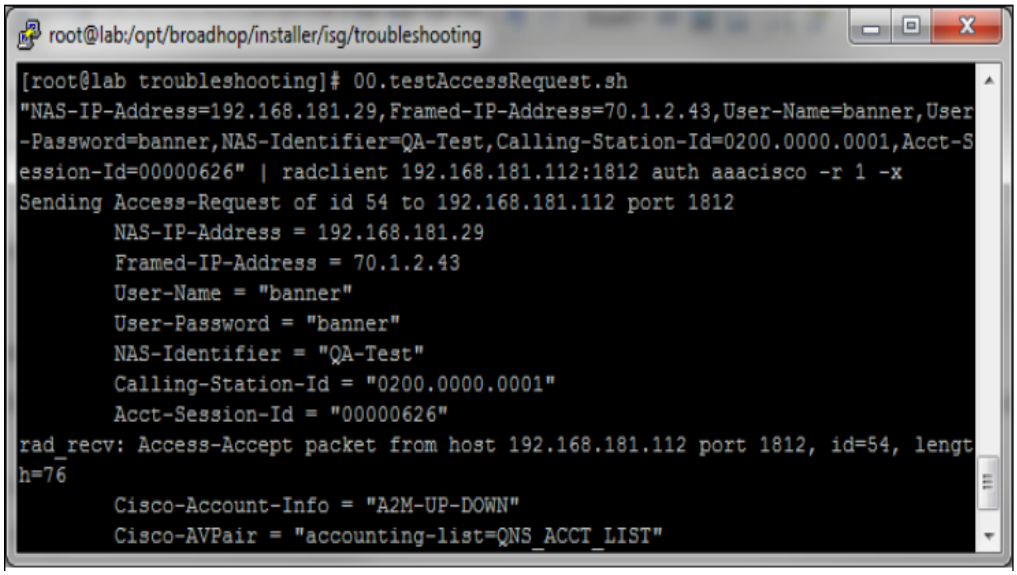
Step 1 In the config.ini file, change the User-Name and Password fields.

Note You may need to change some of the other parameters in order to match your configuration. The other main attributes to change will be the NAS-IP-Address and Framed-IP-Address.

Step 2 Run the script from a command line. No arguments are necessary:

00.testAccessRequest.sh

Upon success, this output displays:



Testing Subscriber Access with soapUI

This procedure tests end subscriber access to your system.

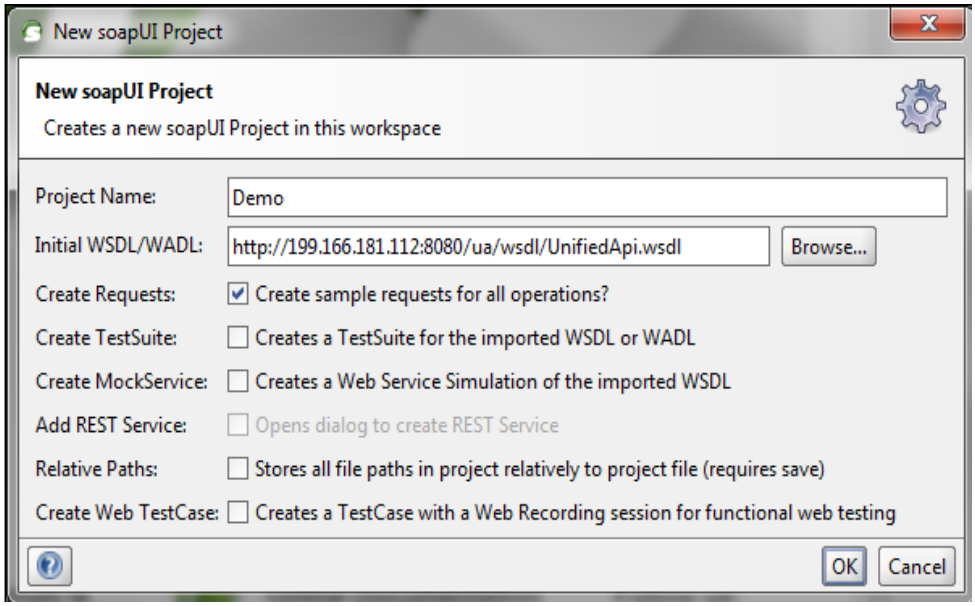
Step 1 Download soapUI from here: http://www.soapui.org/

You only need the freeware version (not soapUI Pro).

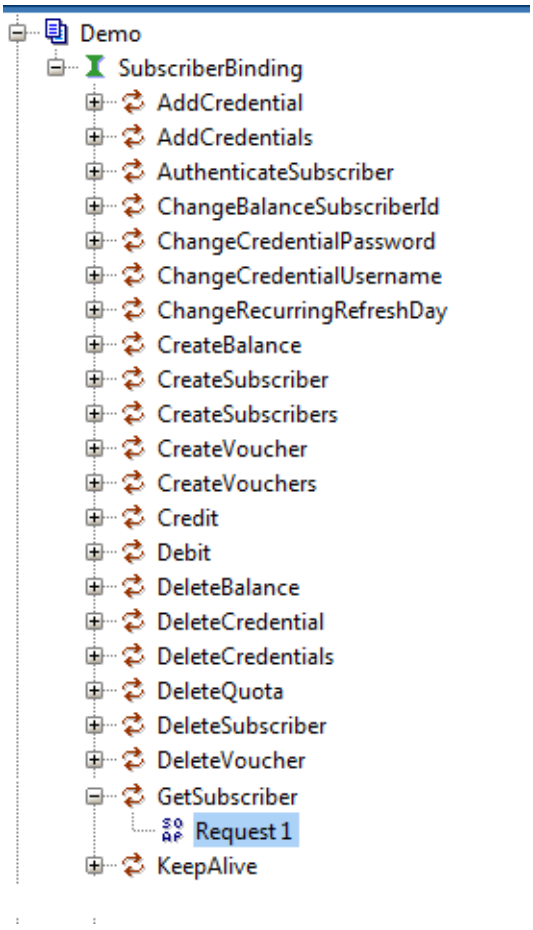
Step 2 Launch soapUI.

Step 3 Right click on projects, select New soapUIProject from the drop-down menu.

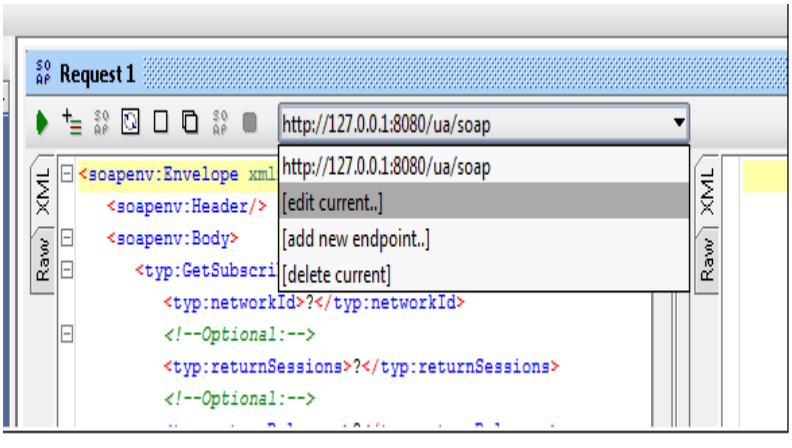
Step 4 Name your project and enter into Initial WSDL/WADL the appropriate WSDL URL (you may have to replace the IP in display with your own IP) and select OK:



Step 5 In the tree click Demo > SubscriberBinding > GetSubscriber > Request 1, as shown in the figure on the right.



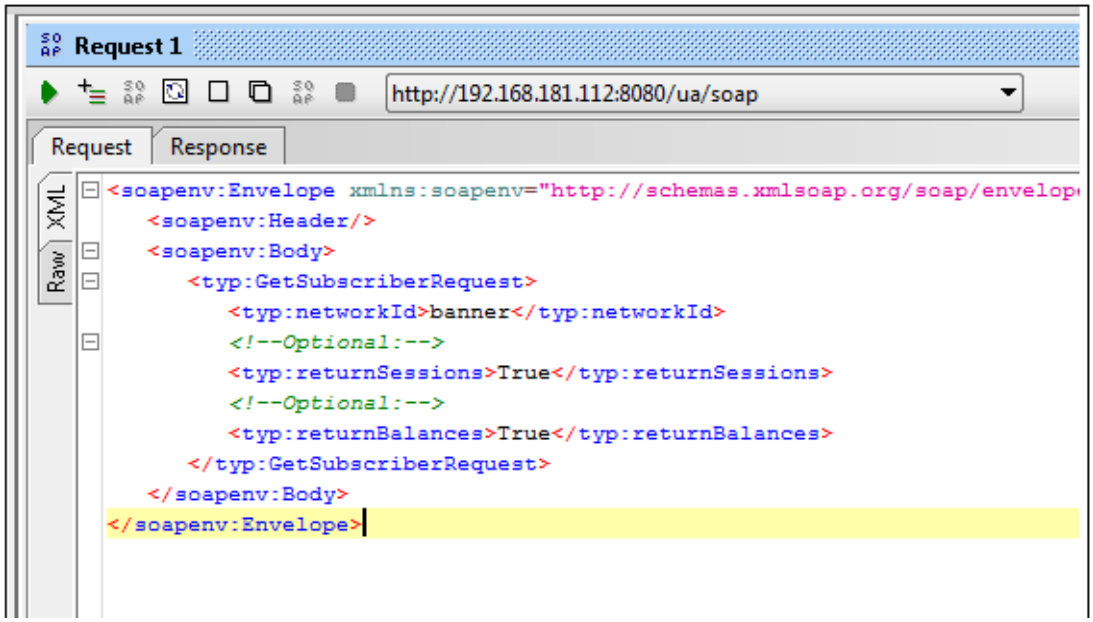
Step 6 Edit the End Point by selecting from the drop down: [edit current...]. Enter the appropriate IP.



Step 7 In the XML file:

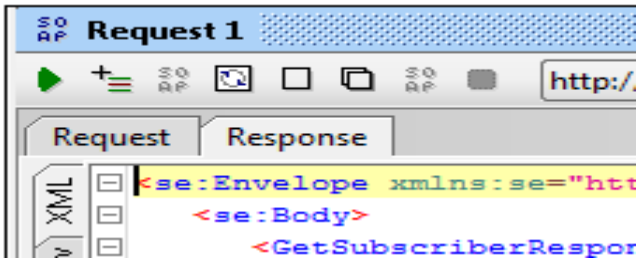
- Replace the ? in <typ:networkId>?</typ:networkId> with the appropriate credential or network Id.
- Replace the ? in <typ:returnSessions>?</typ:returnSessions> with "True".
- Replace the ? in <typ:returnBalance>?</typ:returnBalance> with "True"

.



Step 8 Click on the green arrow (underneath "Request 1")

.



Step 9 Check the resulting XML output. Pay special attention to the relevant subscriber information:

```
<se:Envelope xmlns:se="http://schemas.xmlsoap.org/soap/envelope/">
   <se:Body>
      <GetSubscriberResponse xmlns="http://broadhop.com/unifiedapi/soap/types">
         <errorCode>0</errorCode>
         <errorMessage>Request completed successfully</errorMessage>
         <subscriber>
            <id>4fb54d03e4b01e8478d309c2</id>
            <name>
               <fullName>Bruce Banner</fullName>
            </name>
            <credential>
               <networkId>banner</networkId>
               <password>banner</password>
            </credential>
            <credential>
               <networkId>0200.0000.0001</networkId>
               <expirationDate>2012-05-17T13:17:07.020-06:00</expirationDate>
            </credential>
            <service>
               <code>SERVICE_A</code>
               <enabled>true</enabled>
            </service>
            <session>
               <sessionKey>
                  <code>UserIdKey</code>
                  <primary>false</primary>
                  <keyField>
                     <code>userId</code>
                     <value>banner</value>
                  </keyField>
               </sessionKey>
               <sessionObject>
                  <entry>
                     <string>tags</string>
                     <list>
```

Testing for ISG Functionality and Connectivity with *test aaa* Scripts

The four scripts described here test ISG functionality and connectivity.

Step 1 Connect to the ISG with username and password.

Step 2 Type the 'en' command.

Step 3 Enter 'cisco' as the password to the en command.

From here use the four "test aaa" scripts to verify correct ISG functionality and connectivity. No IP addresses or any other arguments are needed.

```
test aaa group QNS_AAA PBHK_SERVICE servicecisco legacy
test aaa group QNS_AAA L4REDIRECT_SERVICE servicecisco legacy
test aaa group QNS_AAA OPENGARDEN_SERVICE servicecisco legacy
test aaa group QNS_AAA BroadHop BroadHop legacy
```

If functioning correctly, each script returns this message:

```
Attempting authentication test to server-group QNS_AAA using
radius
User was successfully authenticated.
```

TCP Dumps

Revised: July 10, 2015

CPS administrators can use the tcpdump Linux command in the command line to intercept and display TCP/IP packets, as well as others, as they are being transmitted or received.

With the tcpdump command, you can analyze network behavior, performance, and applications that generate or receive network traffic.

While not specific to CPS, the following examples of tcpdump are frequently helpful for troubleshooting CPS network packets.

This chapter covers the following sections:

- TCPDUMP Command, page 3-1
- Specific Traffic Types, page 3-2

TCPDUMP Command

tcpdump -i any -s 0 port XXXX

where XXXX is the port number you are interested in, RADIUS ports are used for Default examples unless otherwise specified.

Options

To Specify Multiple Ports

To capture more than one port,

tcpdump -i any -s 0 port 1812 or 1813

To capture a port range,

tcpdump -i any -s 0 portrange 1812-1817

Combining both techniques:

tcpdump -i any -s 0 portrange 1812-1817 or port 1700

Verbose Mode

tcpdump -i any -s 0 -v port XXXX

Even more Verbose Mode

tcpdump -i any -s 0 -vv port XXXX

Restrict to a Specific Interface, such as eth0

tcpdump -i eth0 -s 0 port XXXX

Redirect Output of the Command to a File

tcpdump -i any -s 0 port 1812 -w output.pcap

The resulting output.pcap file can be opened and utilized using such tools as WireShark

More options

From a UNIX/Linux prompt, type **man tcpdump**

Specific Traffic Types

Note These examples assume that the default ports have not been changed or have been specified in Cisco Policy Builder. One must modify these examples to use the appropriate ports that have been specified in Cisco Policy Builder if the default/typical values have been changed.

Capture RADIUS Traffic

tcpdump -i any -s 0 port 1812 or 1813

Port 1812 is the default for Authorization traffic.

Port 1813 is the default for Accounting traffic.

Capture SNMP Traffic

tcpdump -i any -s 0 port 1161 or 1162 or 161 or 162

Note This command works for both the sending and receiving machine; the port just needs to match the source or destination port.

Other Ports

The following information is the information format:

Host/VM name Port "Service/traffic type"

where XX is the numeric value of the given host, i.e. pcrfclient01.

pcrfclientXX 80 "Subversion"

pcrfclientXX 7070 "Policy Builder"

sessionmgrXX 27717 "Session Database"

sessionmgrXX 27718 "Quota/Balance Database"

sessionmgrXX 27719 "Reporting Database"

sessionmgrXX 27720 "USuM Database"

lbvipXX 80 "Portal vip management"

lbvipXX 80 "Subversion vip external"

lbvipXX 8080 "QNS/Unified API VIP"

lbvipXX 11211 "Memcache vip internal"

lbvipXX 7070 "Policy Builder VIP"

lbvipXX 8082 "Portal Admin VIP"

qnsXX 9091 "QNS admin port"

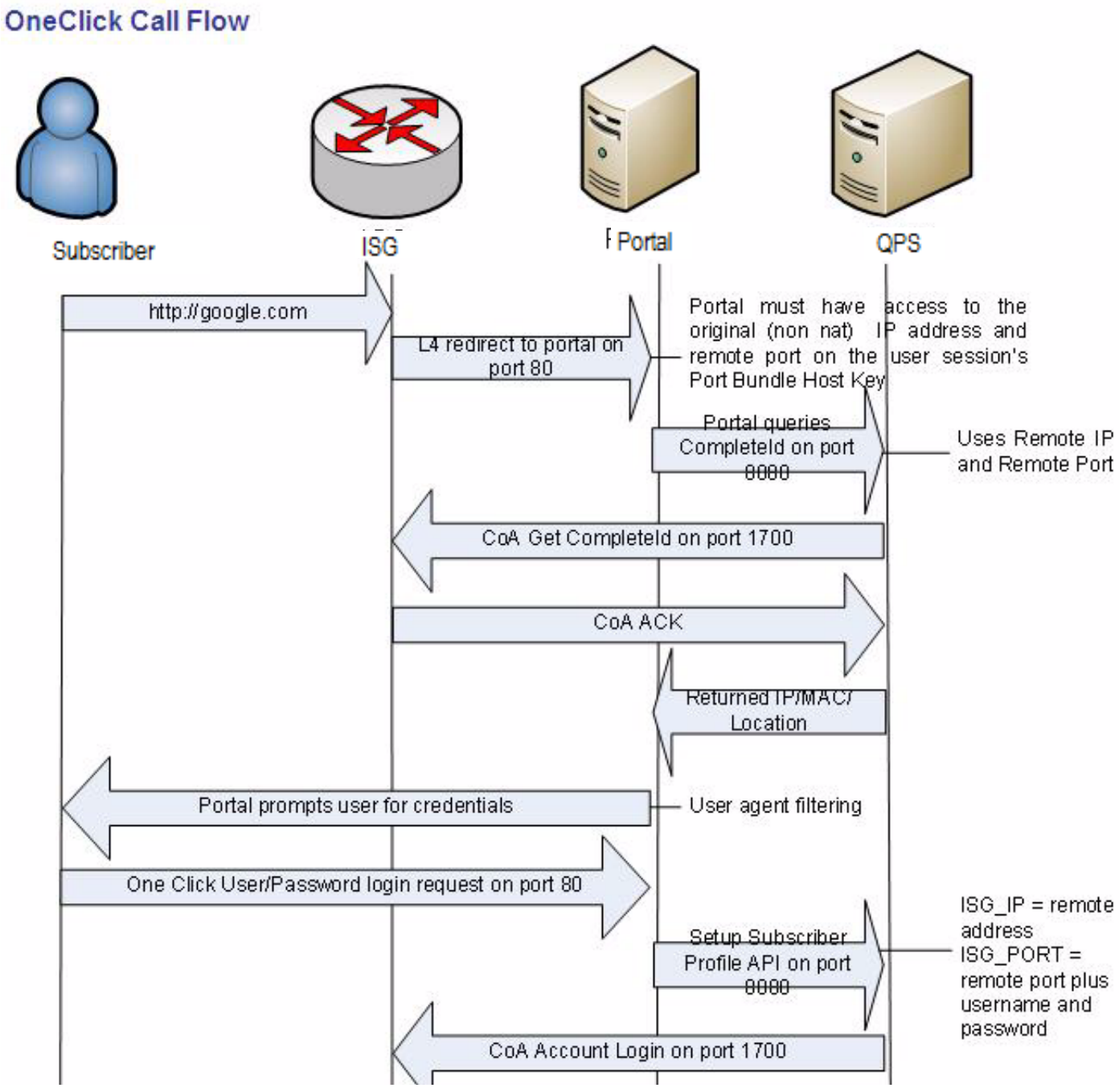
Call Flows

Revised: July 10, 2015

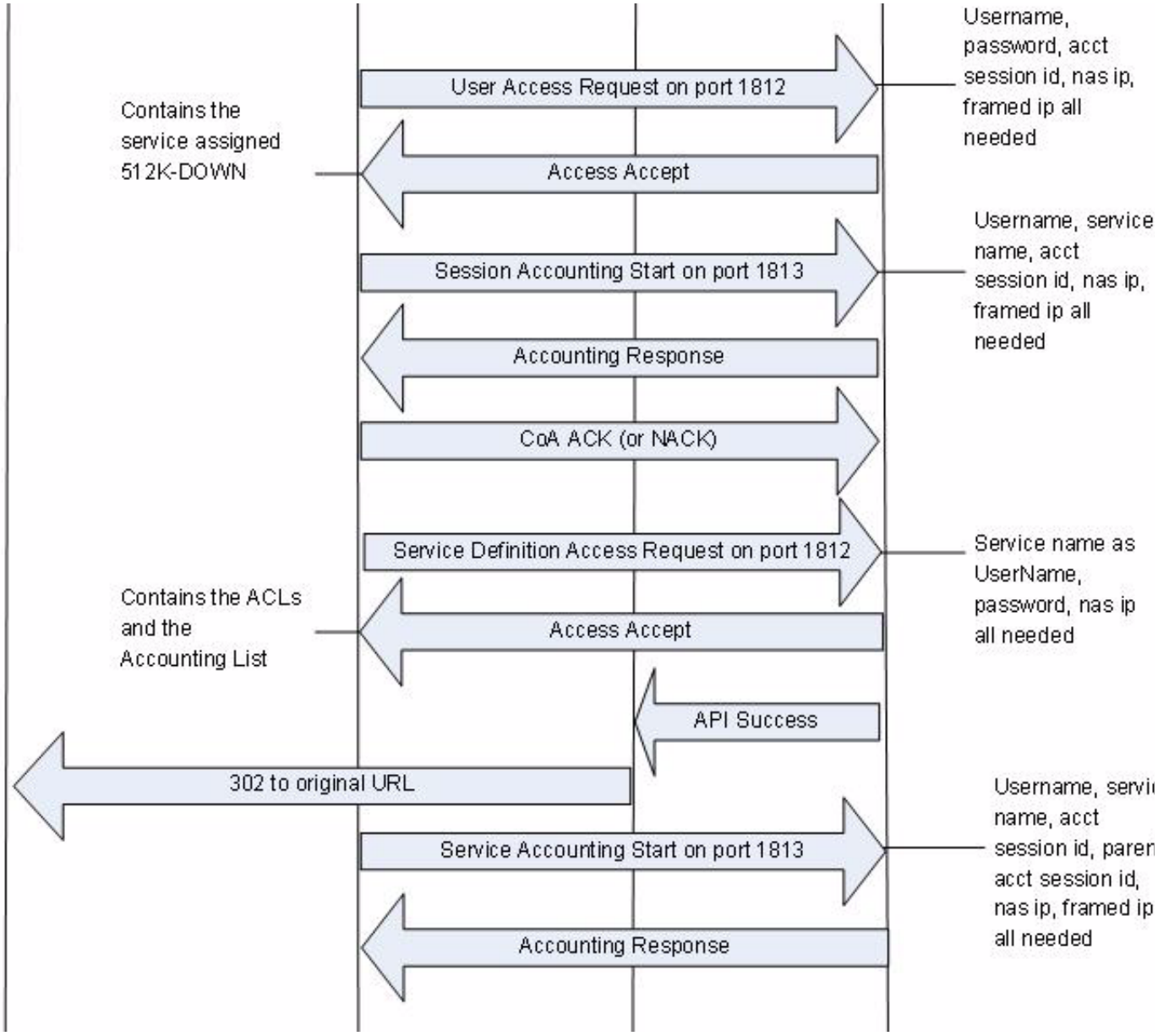
The following call flow diagrams are given to help you troubleshoot and understand CPS deployment.

- One-click Call Flow
- User/Password Login Call Flow
- Data-limited Voucher Call Flow
- Time-limited Voucher Call Flow
- WISPr Call Flow
- EAP-TTLS Call Flow
- Service Selection Call Flow
- MAC TAL Call Flow
- Tiered Services Call Flow
- SP WiFi-4.0 Call Flows

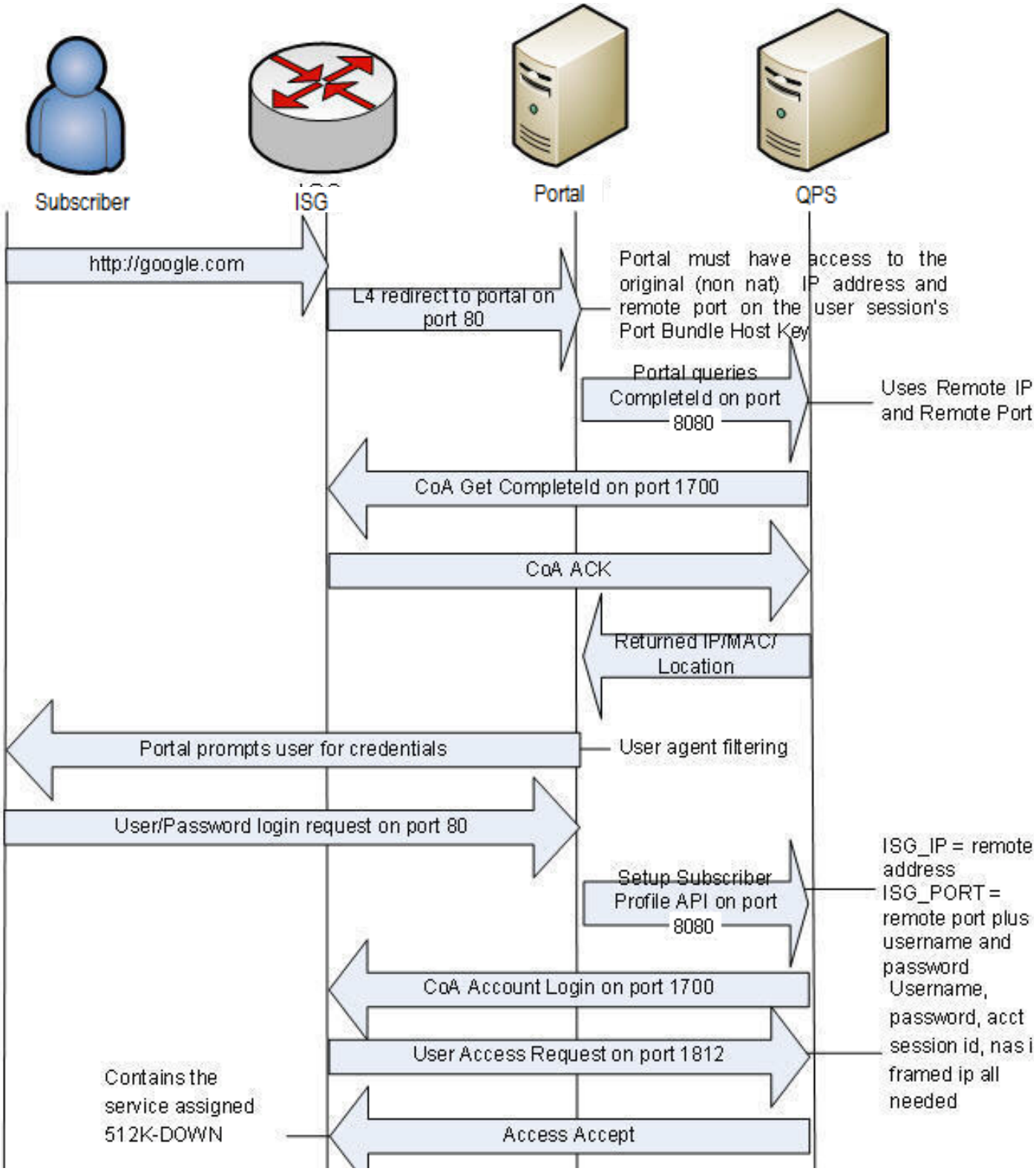
One-click Call Flow



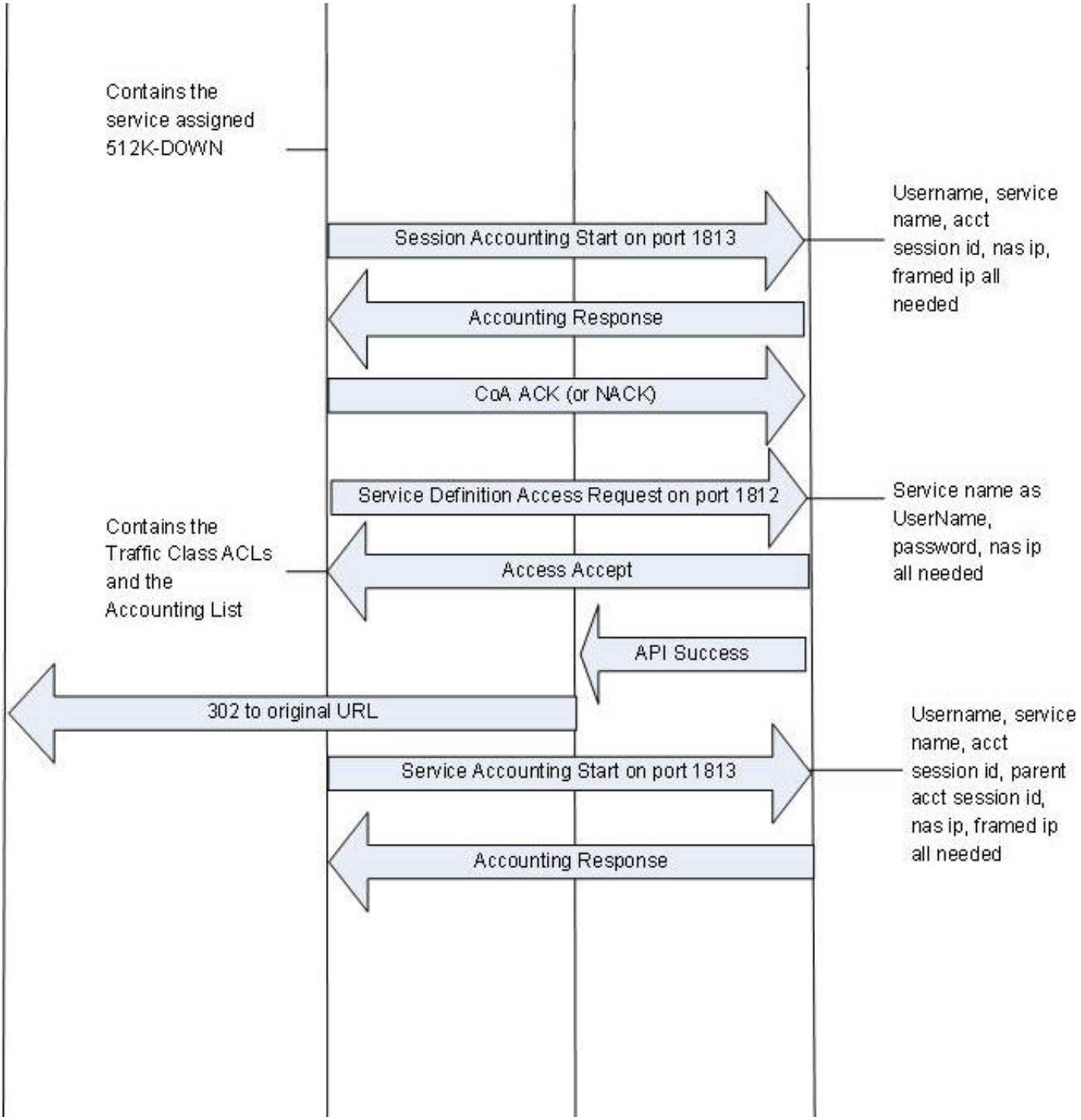
(continued)


Username, password, acct session id, nas ip, framed ip all needed
User Access Request on port 1812
Contains the service assigned 512K-DOWN
Access Accept
Username, service name, acct session id, nas ip, framed ip all needed
Session Accounting Start on port 1813
Accounting Response
CoA ACK (or NACK)
Service Definition Access Request on port 1812
Service name as UserName, password, nas ip all needed
Contains the ACLs and the Accounting List
Access Accept
API Success
302 to original URL
Username, servi name, acct session id, paren acct session id, nas ip, framed ip all needed
Service Accounting Start on port 1813
Accounting Response

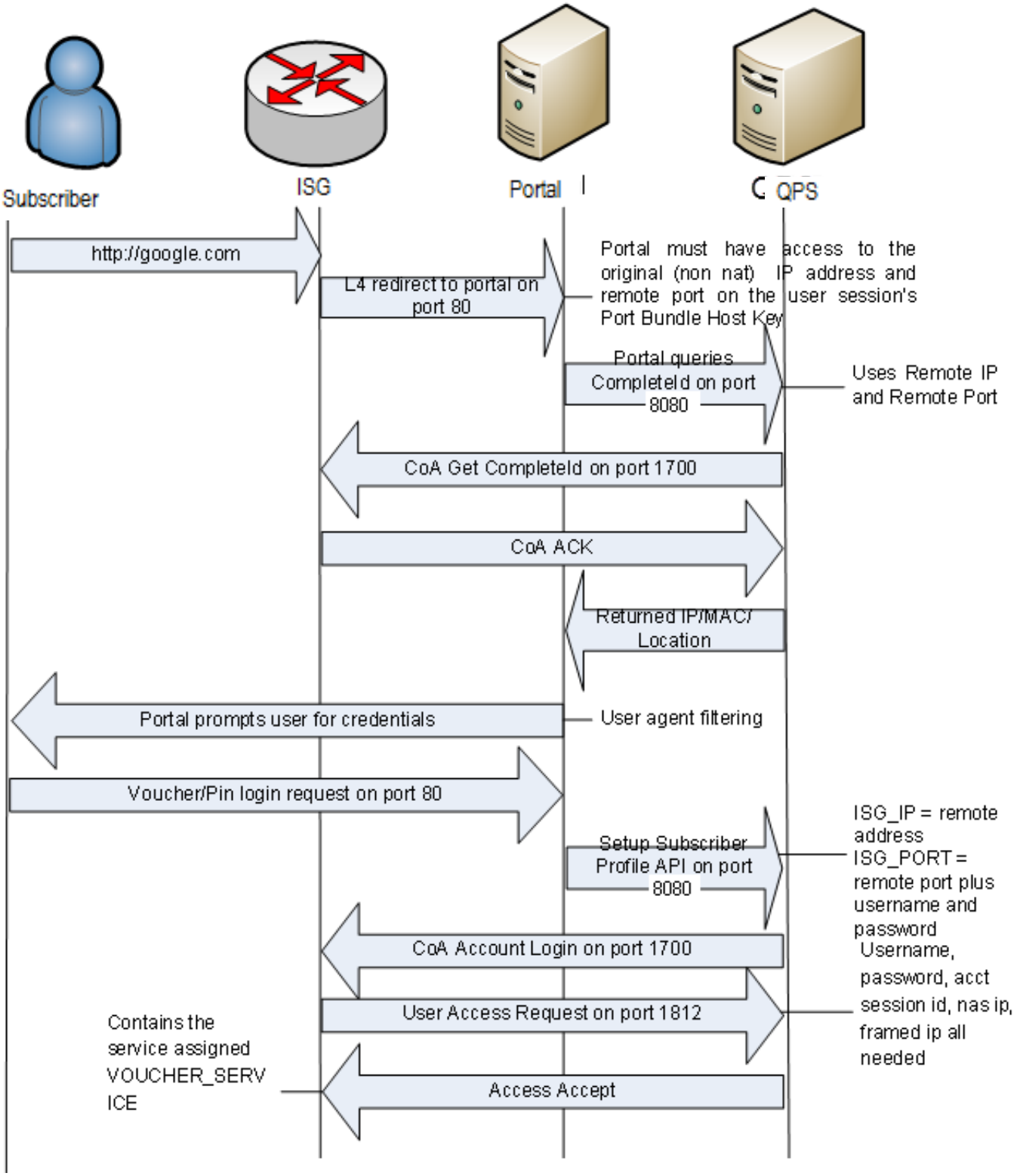
User/Password Login Call Flow



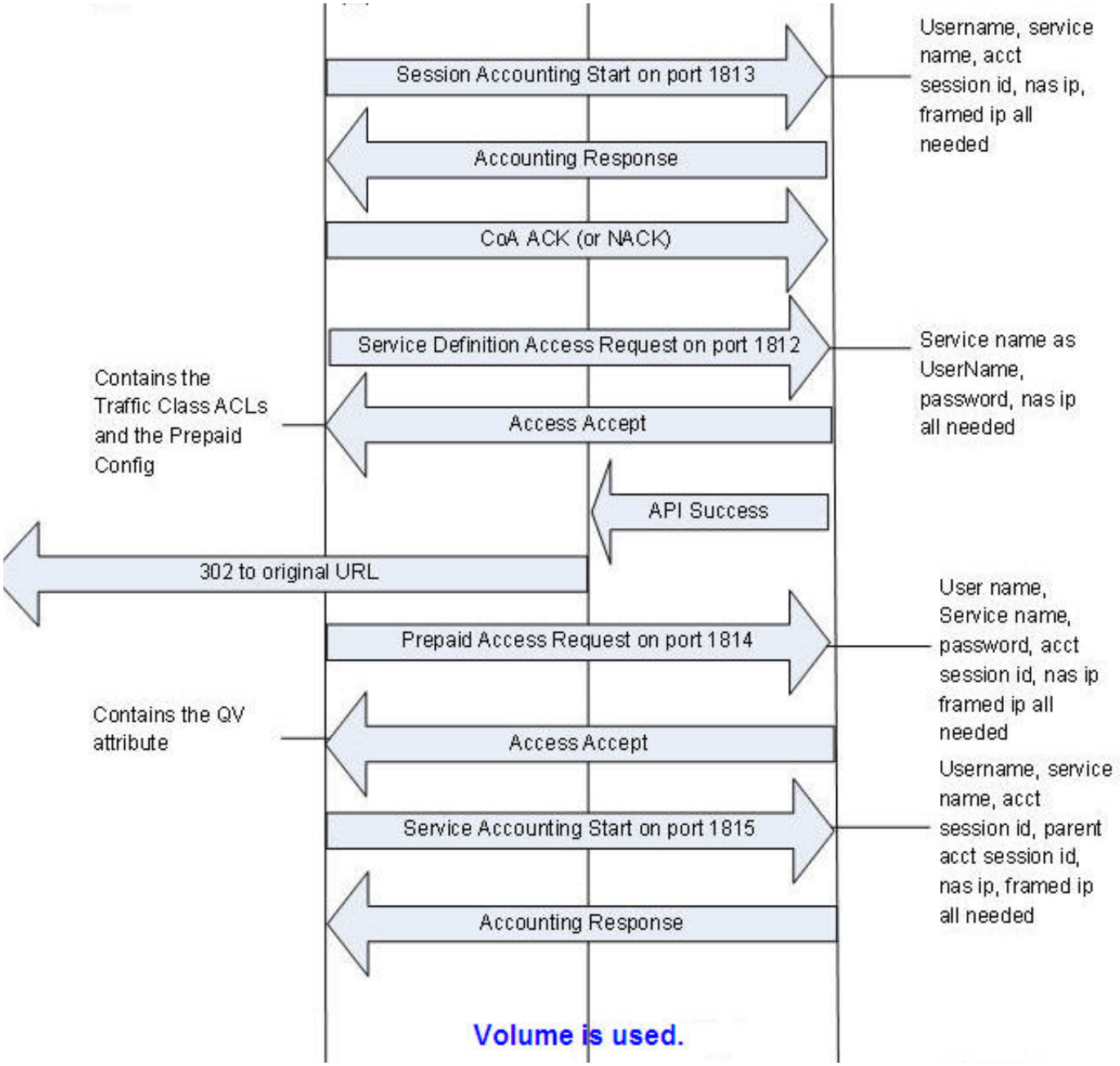
(continued)


Contains the service assigned 512K-DOWN
Session Accounting Start on port 1813
Username, service name, acct session id, nas ip, framed ip all needed
Accounting Response
CoA ACK (or NACK)
Service Definition Access Request on port 1812
Service name as UserName, password, nas ip all needed
Contains the Traffic Class ACLs and the Accounting List
Access Accept
API Success
302 to original URL
Service Accounting Start on port 1813
Username, service name, acct session id, parent acct session id, nas ip, framed ip all needed
Accounting Response

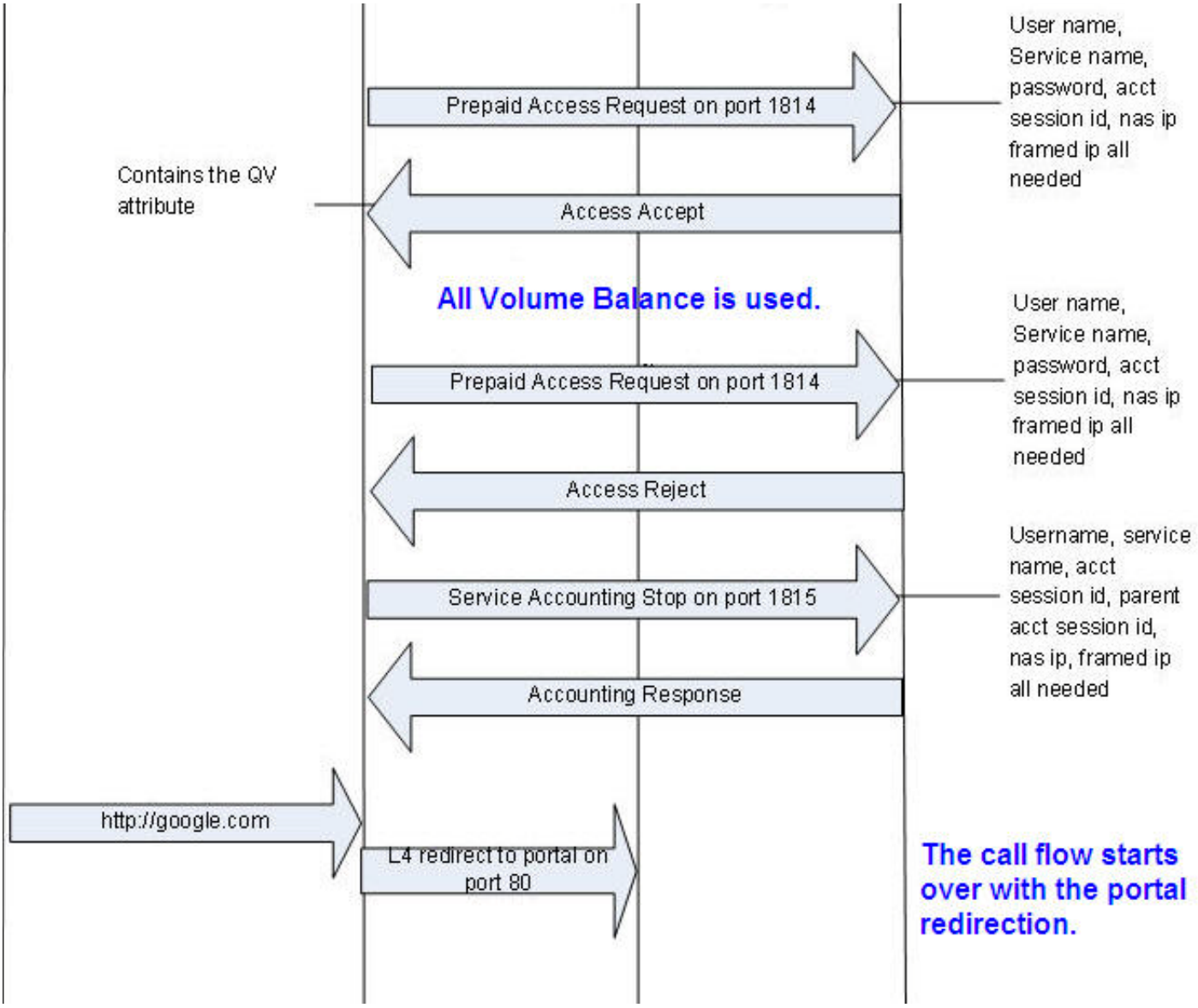
Data-limited Voucher Call Flow



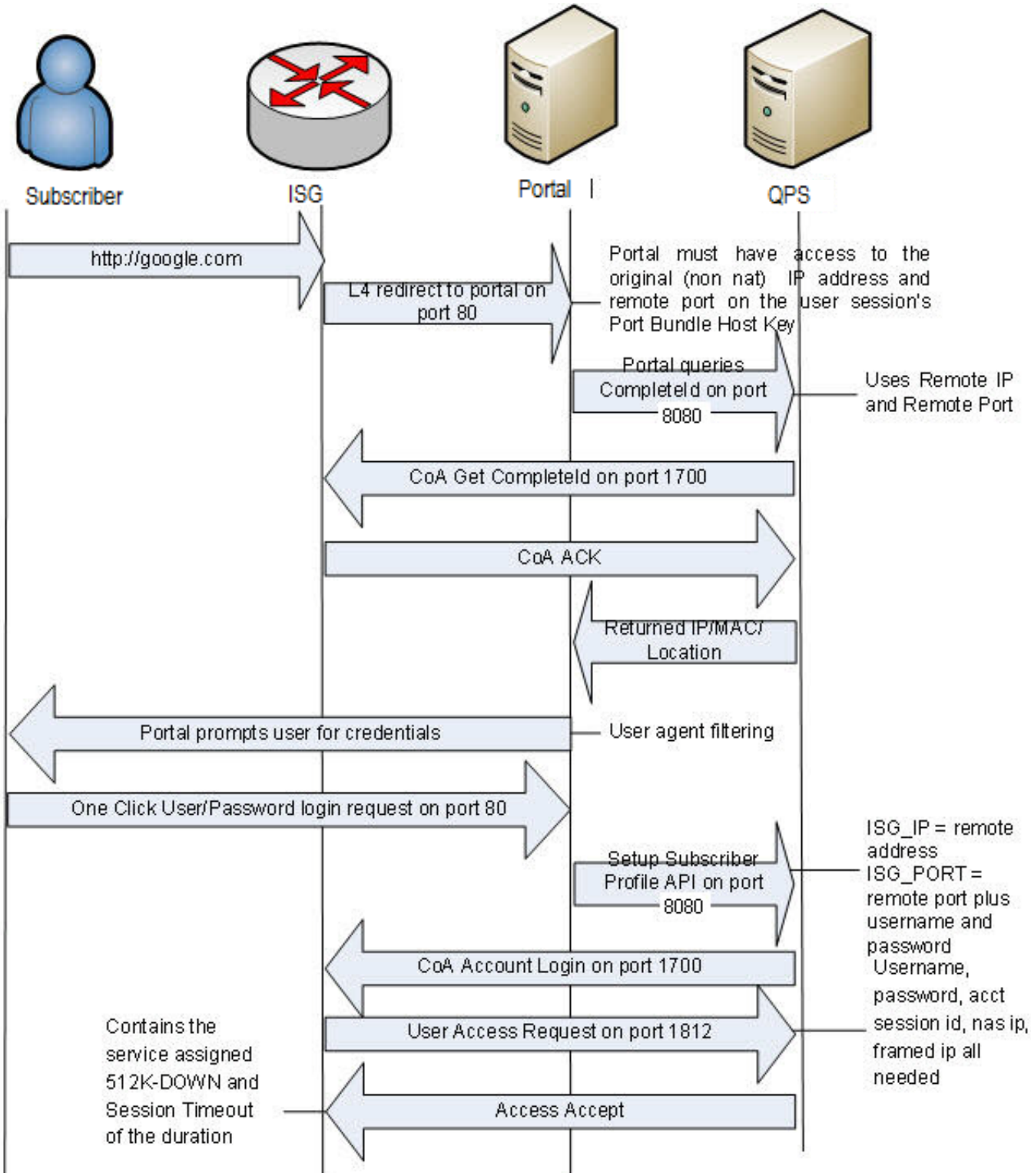
(continued)


Session Accounting Start on port 1813
Username, service name, acct session id, nas ip, framed ip all needed
Accounting Response
CoA ACK (or NACK)
Service Definition Access Request on port 1812
Service name as UserName, password, nas ip all needed
Contains the Traffic Class ACLs and the Prepaid Config
Access Accept
API Success
302 to original URL
Prepaid Access Request on port 1814
User name, Service name, password, acct session id, nas ip framed ip all needed
Contains the QV attribute
Access Accept
Service Accounting Start on port 1815
Username, service name, acct session id, parent acct session id, nas ip, framed ip all needed
Accounting Response
Volume is used.

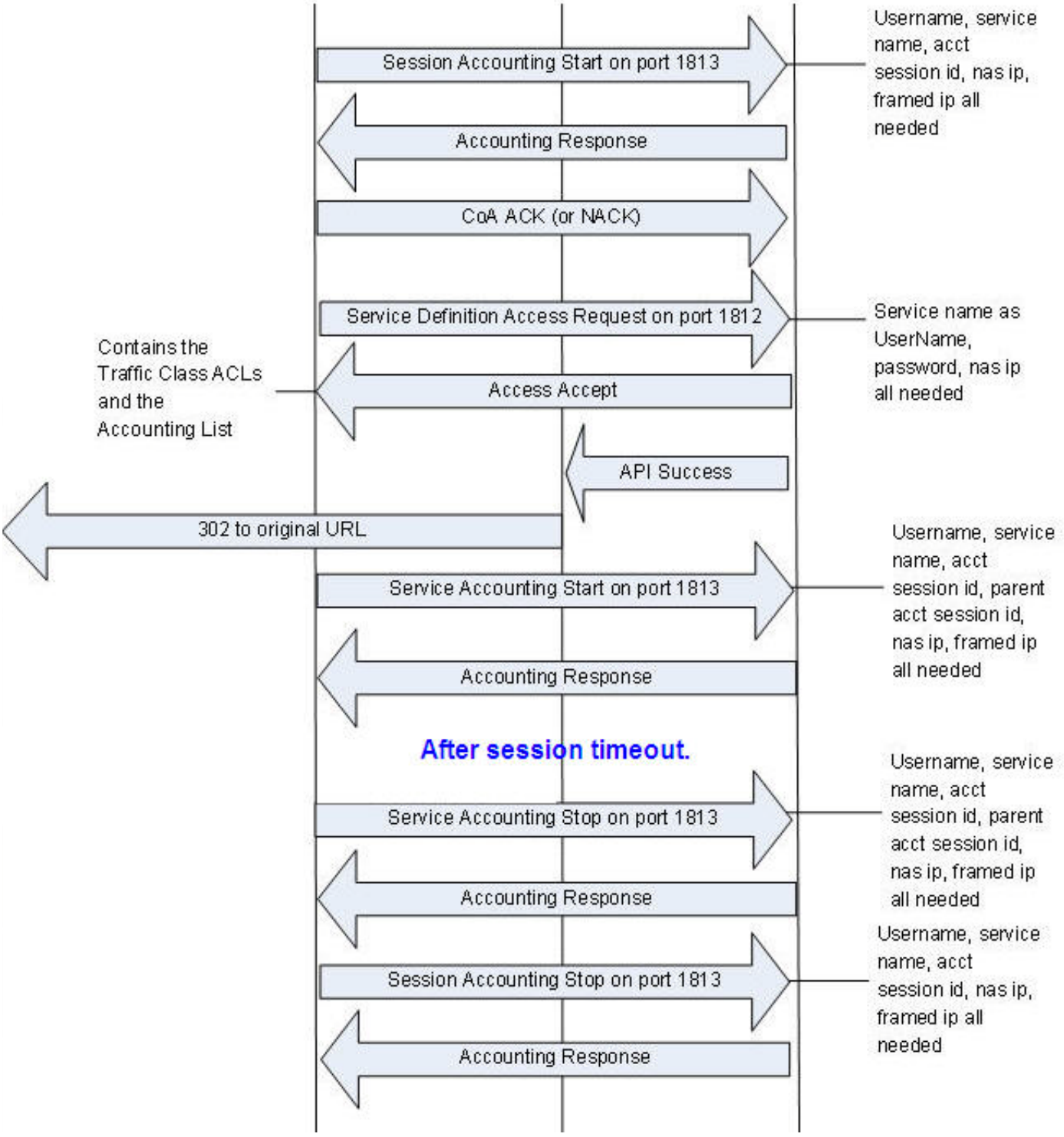
(continued)


User name, Service name, password, acct session id, nas ip framed ip all needed
Prepaid Access Request on port 1814
Contains the QV attribute
Access Accept
All Volume Balance is used.
User name, Service name, password, acct session id, nas ip framed ip all needed
Prepaid Access Request on port 1814
Access Reject
Username, service name, acct session id, parent acct session id, nas ip, framed ip all needed
Service Accounting Stop on port 1815
Accounting Response
http://google.com
L4 redirect to portal on port 80
The call flow starts over with the portal redirection.

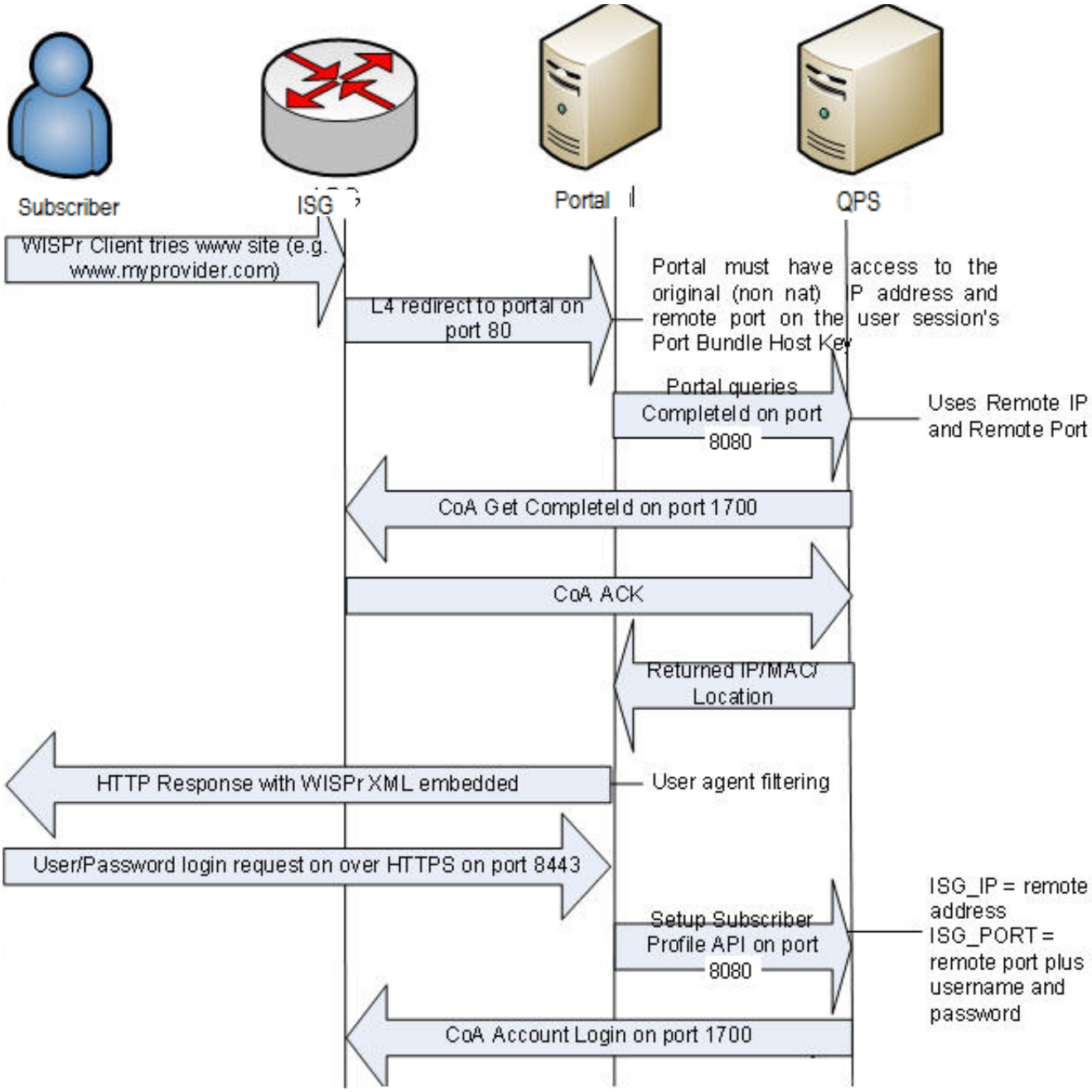
Time-limited Voucher Call Flow



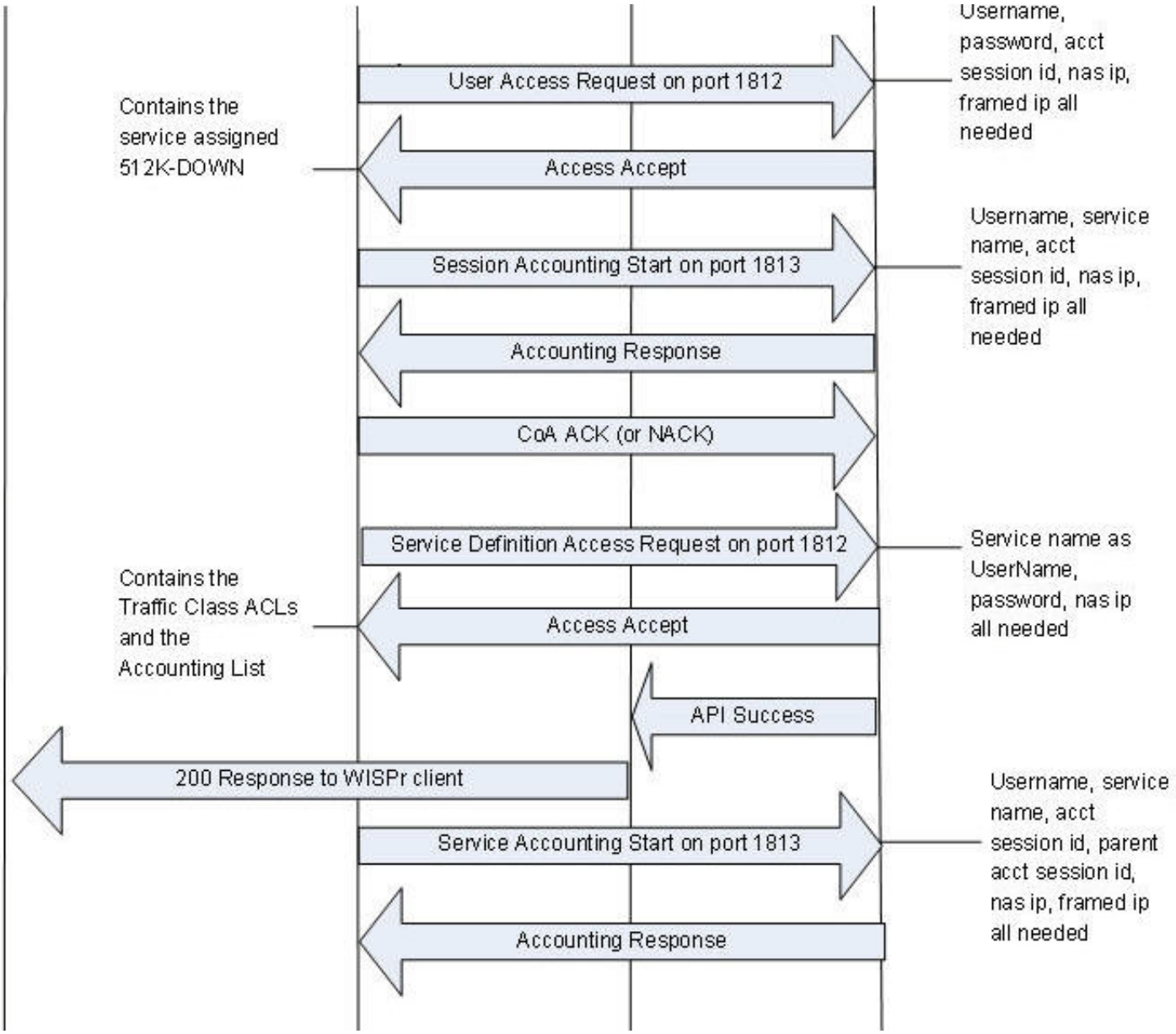
(continued)


Session Accounting Start on port 1813
Username, service name, acct session id, nas ip, framed ip all needed
Accounting Response
CoA ACK (or NACK)
Service Definition Access Request on port 1812
Service name as UserName, password, nas ip all needed
Contains the Traffic Class ACLs and the Accounting List
Access Accept
API Success
302 to original URL
Service Accounting Start on port 1813
Username, service name, acct session id, parent acct session id, nas ip, framed ip all needed
Accounting Response
After session timeout.
Service Accounting Stop on port 1813
Username, service name, acct session id, parent acct session id, nas ip, framed ip all needed
Accounting Response
Session Accounting Stop on port 1813
Username, service name, acct session id, nas ip, framed ip all needed
Accounting Response

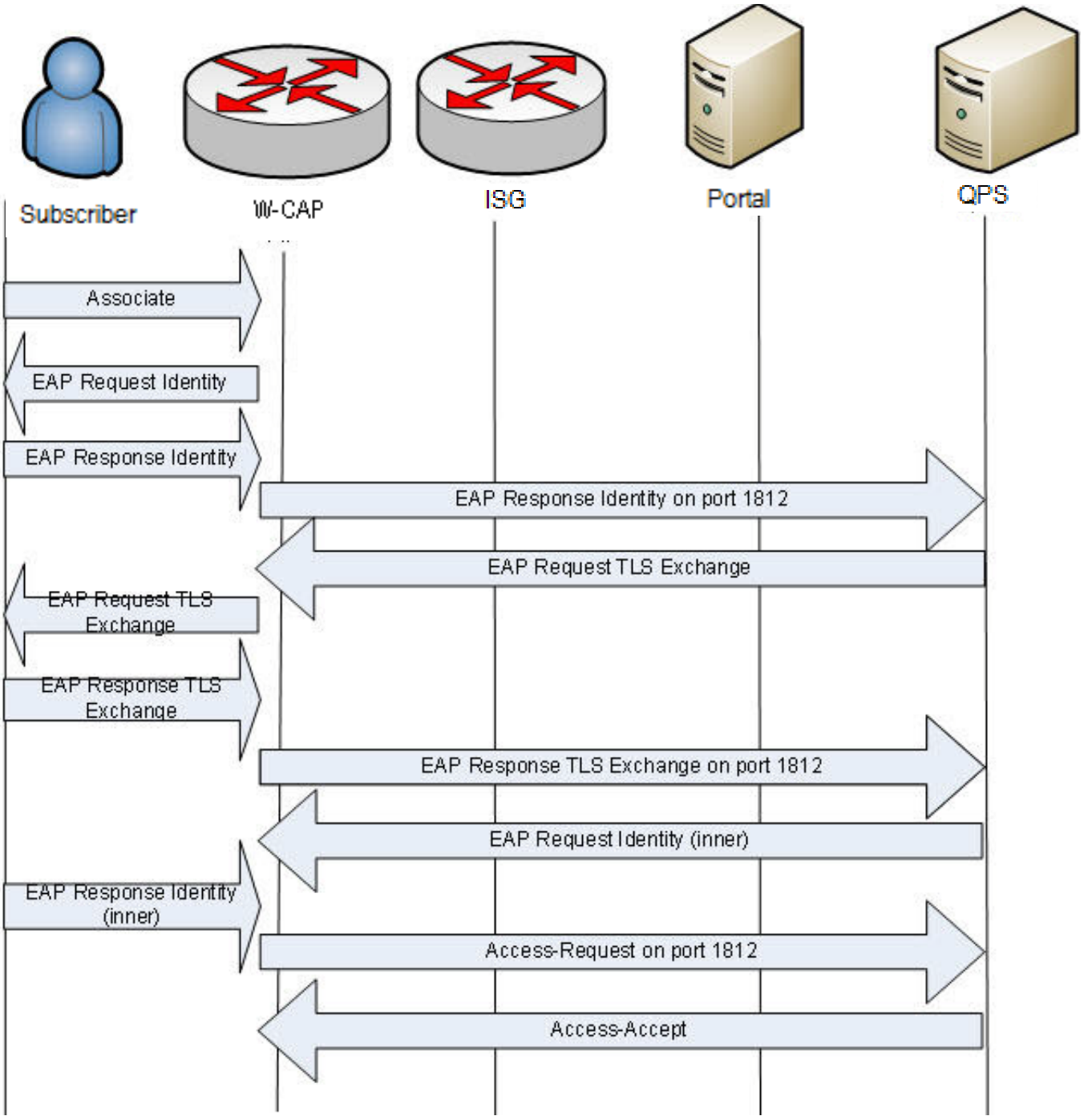
WISPr Call Flow



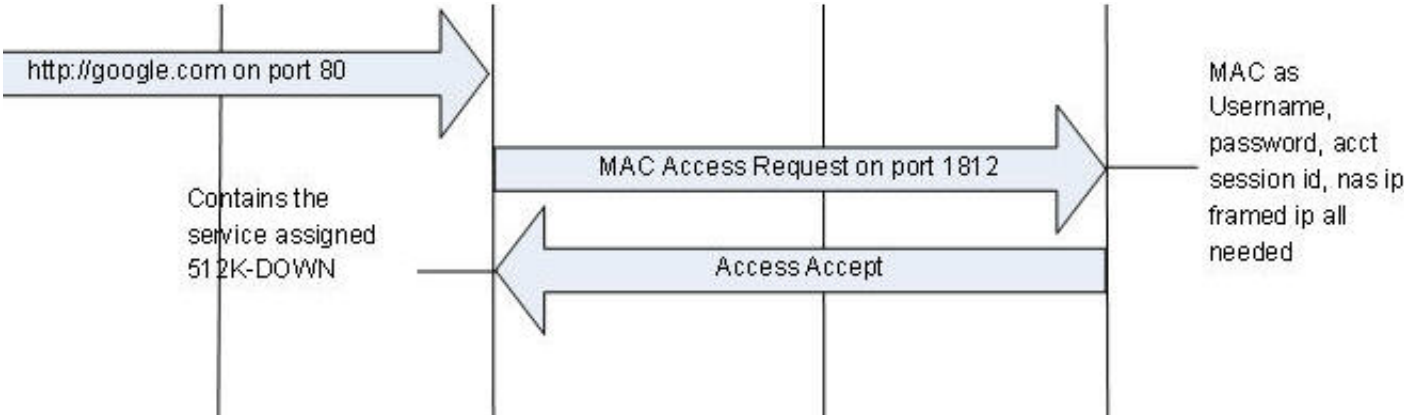
(continued)


Username, password, acct session id, nas ip, framed ip all needed
User Access Request on port 1812
Contains the service assigned 512K-DOWN
Access Accept
Username, service name, acct session id, nas ip, framed ip all needed
Session Accounting Start on port 1813
Accounting Response
CoA ACK (or NACK)
Service Definition Access Request on port 1812
Service name as UserName, password, nas ip all needed
Contains the Traffic Class ACLs and the Accounting List
Access Accept
API Success
200 Response to WISPr client
Username, service name, acct session id, parent acct session id, nas ip, framed ip all needed
Service Accounting Start on port 1813
Accounting Response

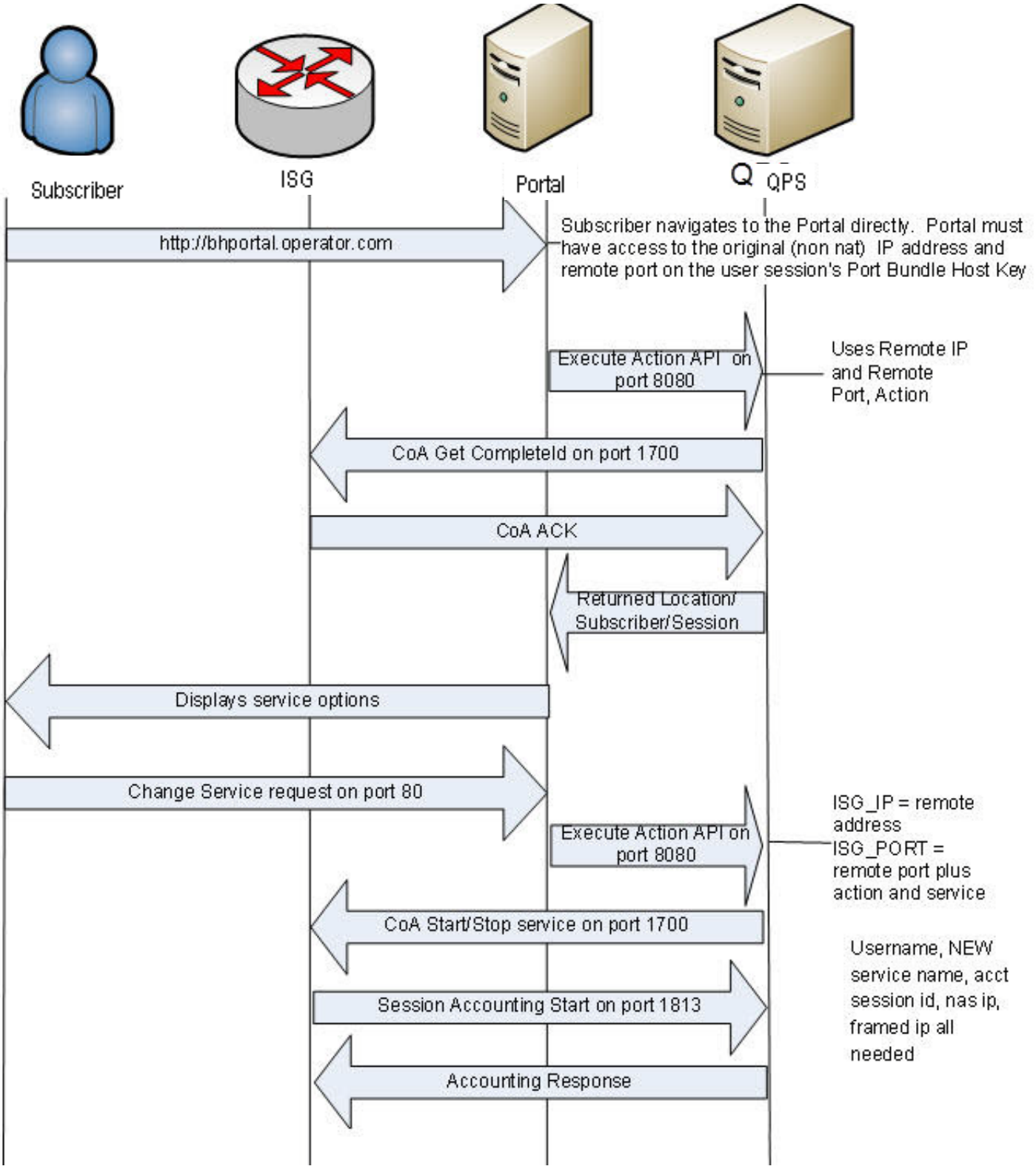
EAP-TTLS Call Flow



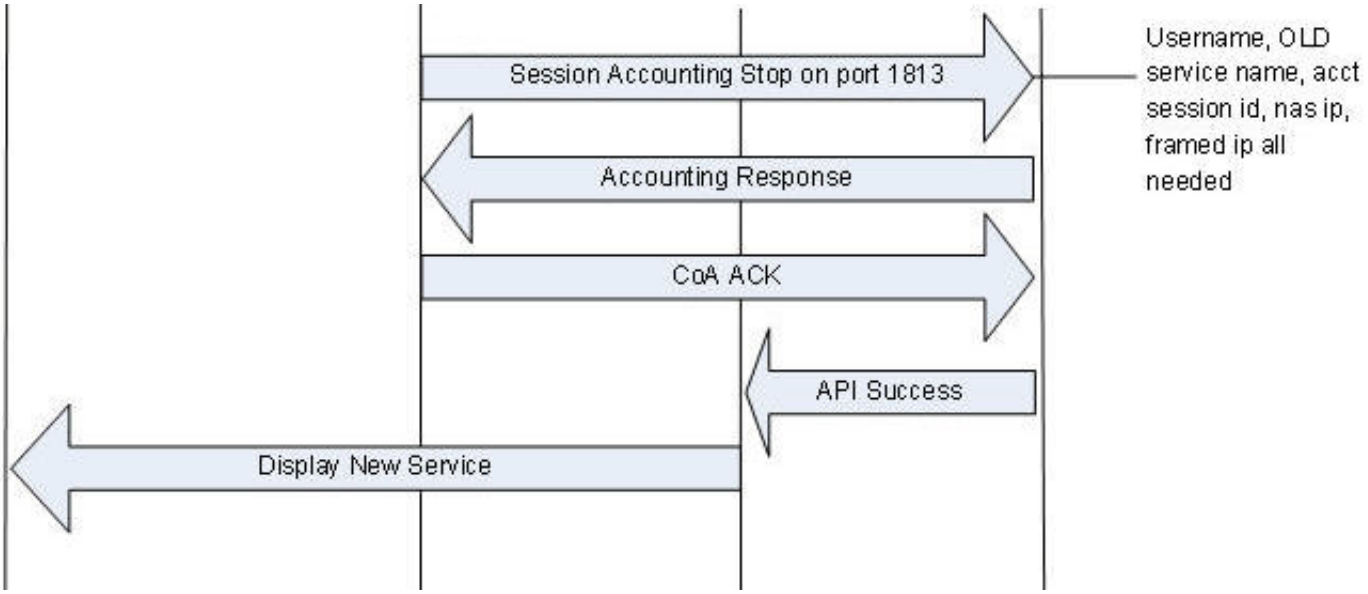
(continued)


http://google.com on port 80
MAC Access Request on port 1812
MAC as Username, password, acct session id, nas ip framed ip all needed
Contains the service assigned 512K-DOWN
Access Accept

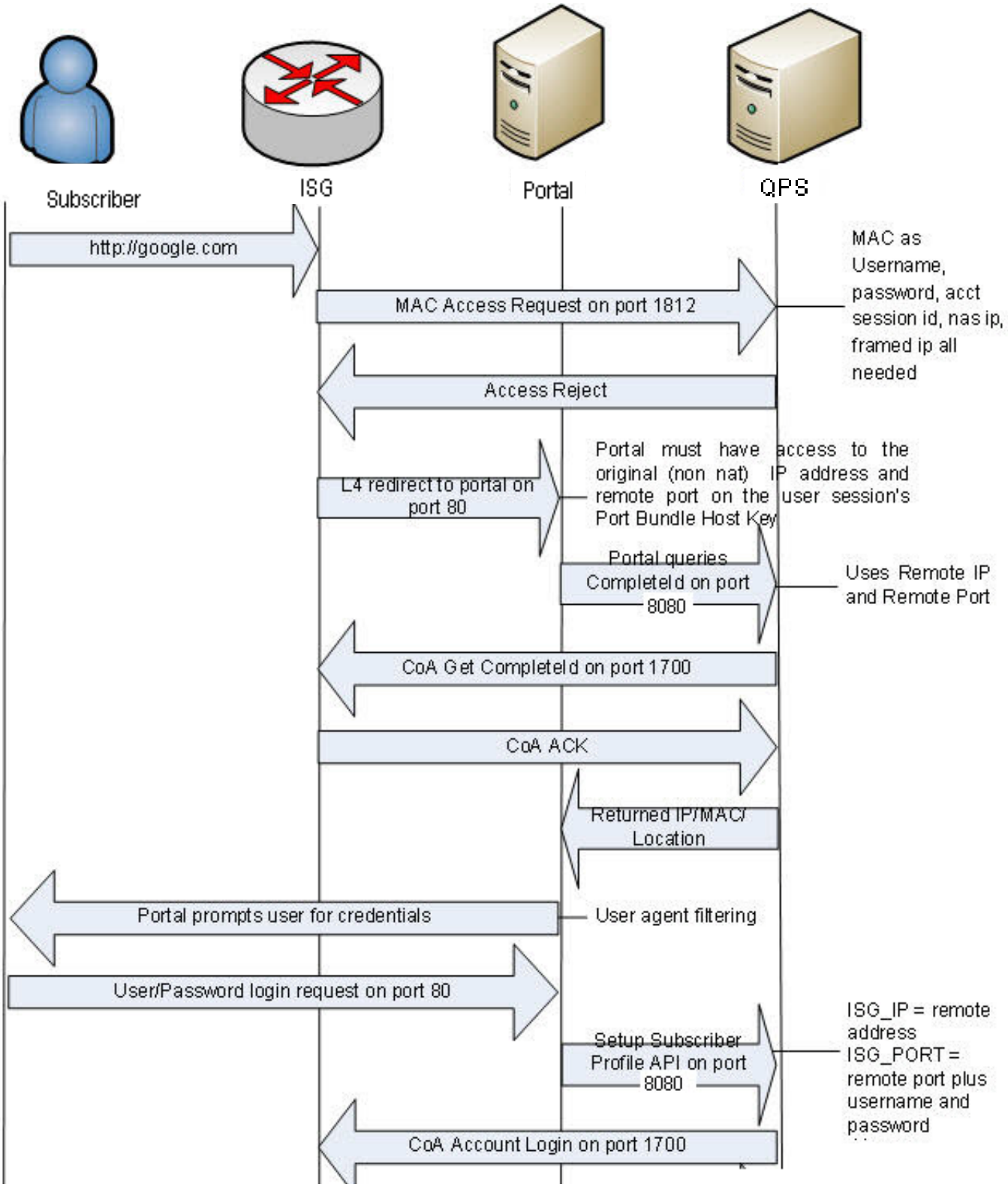
Service Selection Call Flow



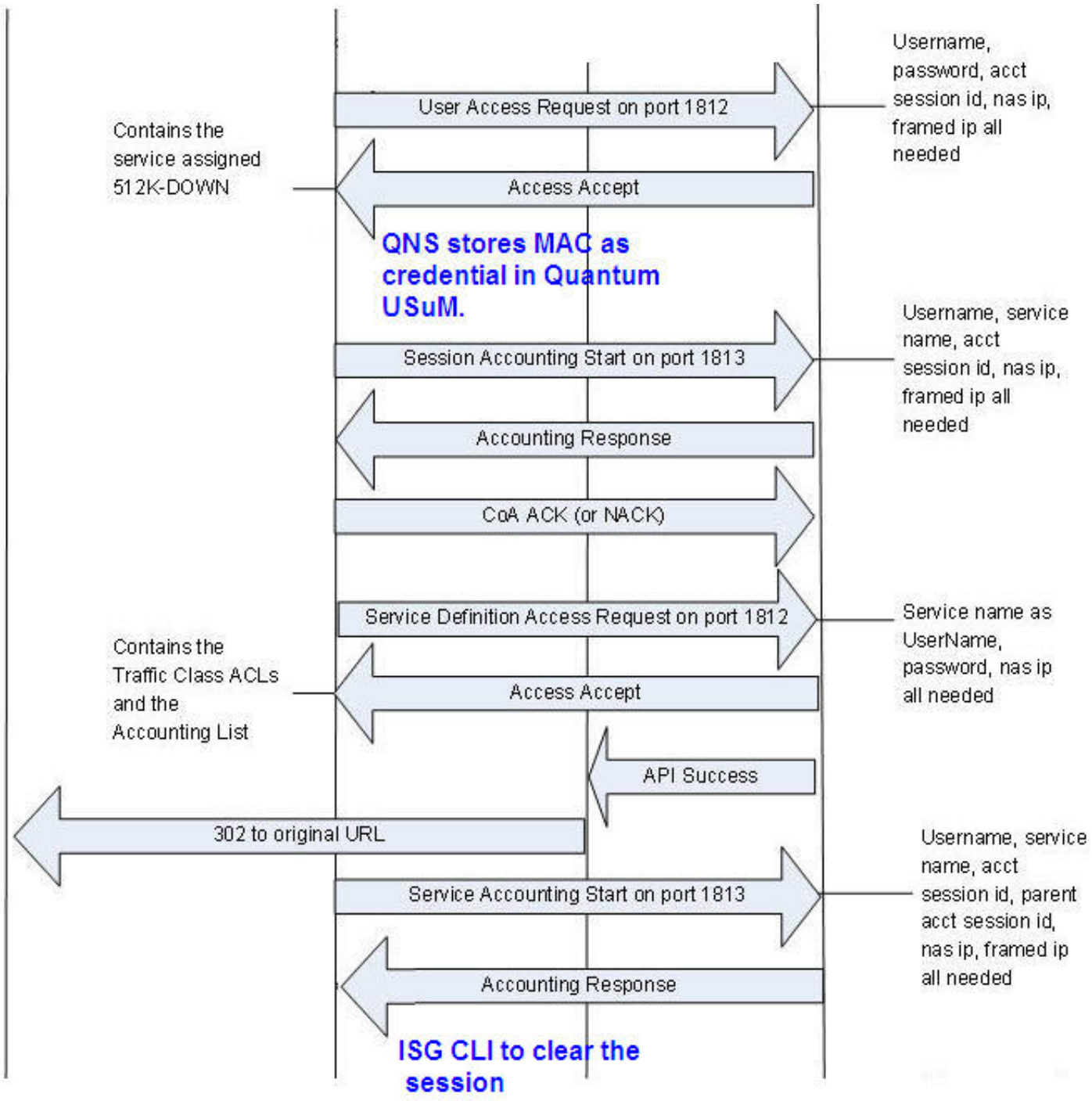
(continued)


Session Accounting Stop on port 1813
Username, OLD service name, acct session id, nas ip, framed ip all needed
Accounting Response
CoA ACK
API Success
Display New Service

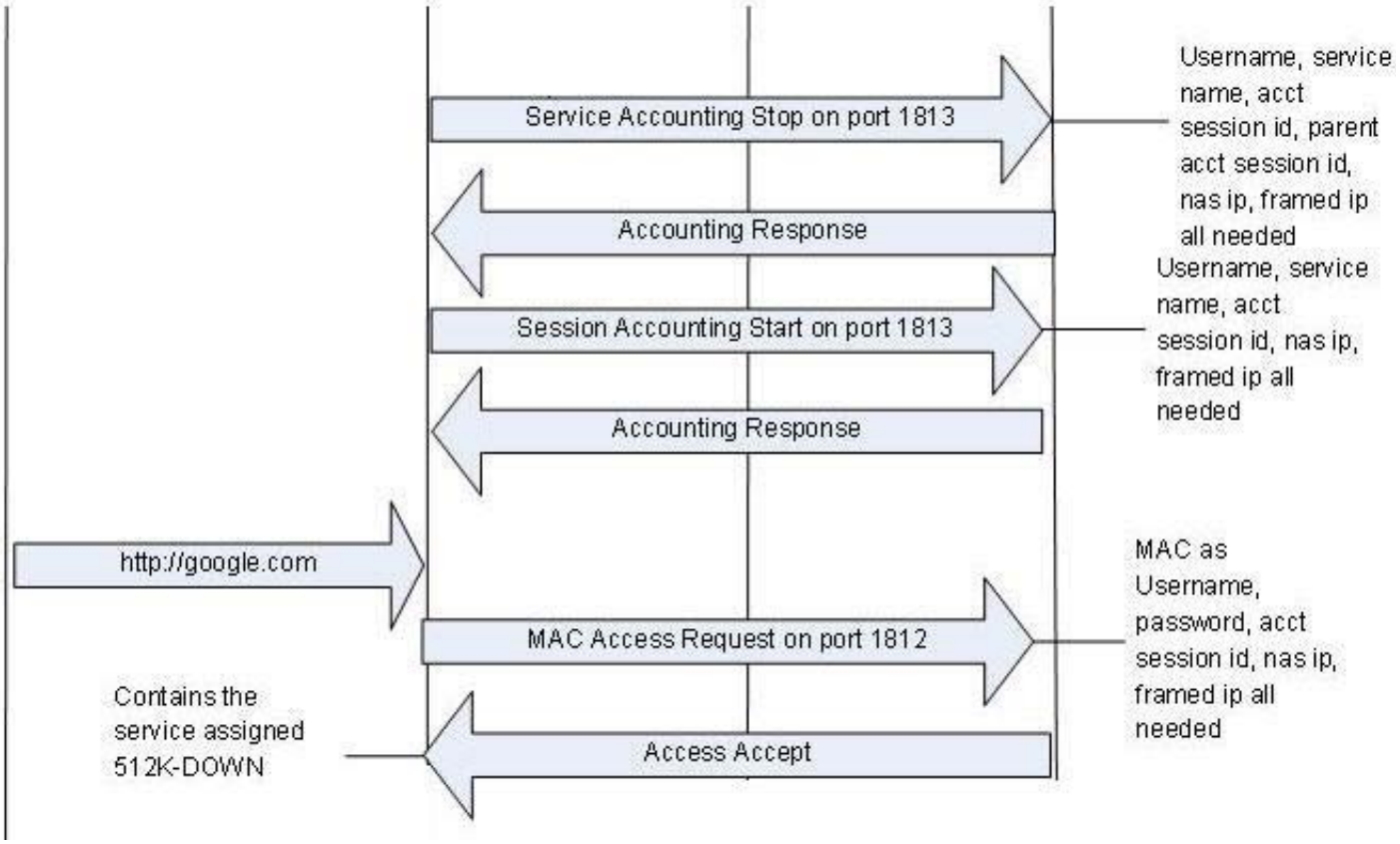
MAC TAL Call Flow



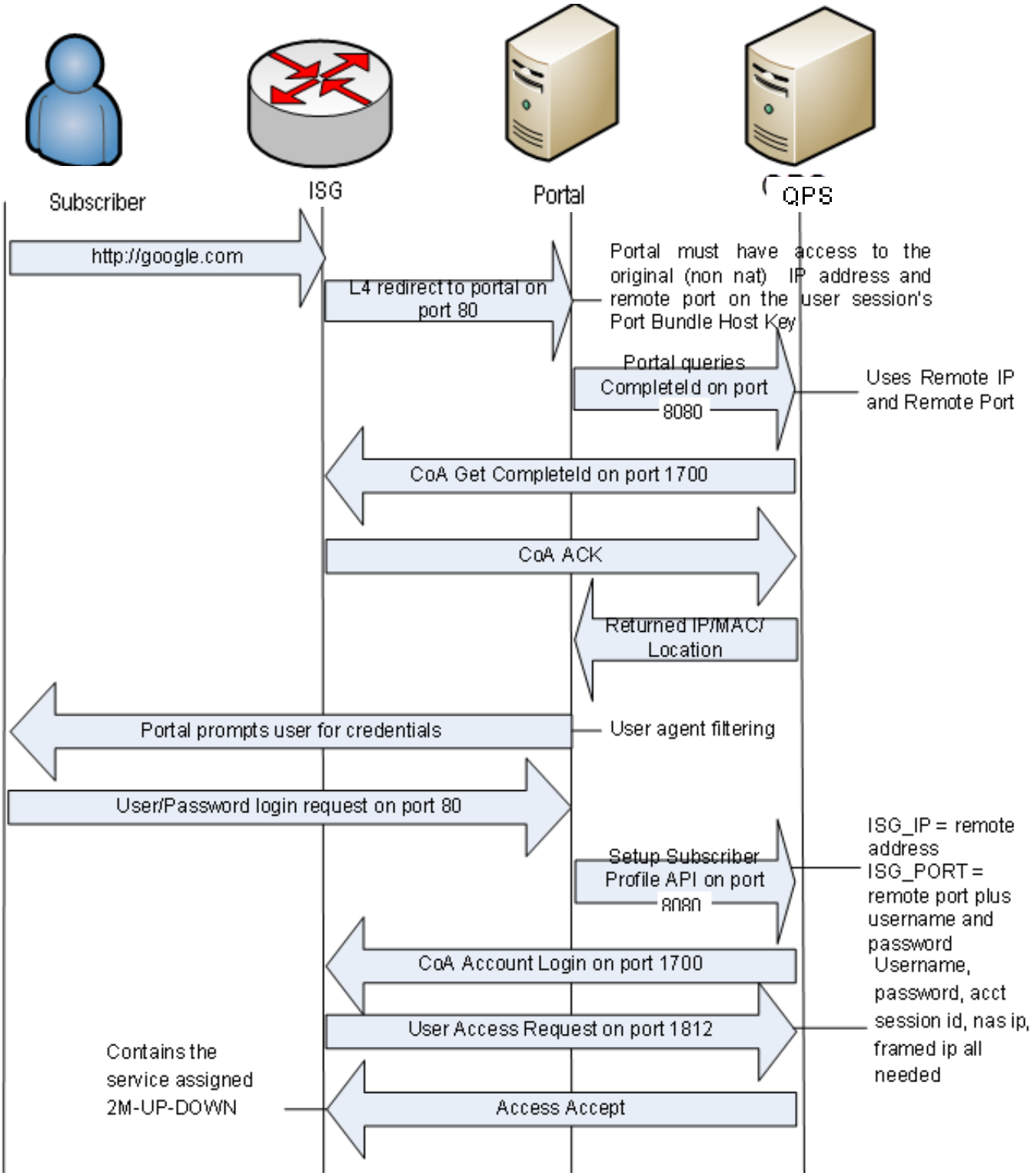
(continued)


Username, password, acct session id, nas ip, framed ip all needed
User Access Request on port 1812
Contains the service assigned 512K-DOWN
Access Accept
QNS stores MAC as credential in Quantum USuM.
Username, service name, acct session id, nas ip, framed ip all needed
Session Accounting Start on port 1813
Accounting Response
CoA ACK (or NACK)
Service Definition Access Request on port 1812
Service name as UserName, password, nas ip all needed
Contains the Traffic Class ACLs and the Accounting List
Access Accept
API Success
302 to original URL
Username, service name, acct session id, parent acct session id, nas ip, framed ip all needed
Service Accounting Start on port 1813
Accounting Response
ISG CLI to clear the session

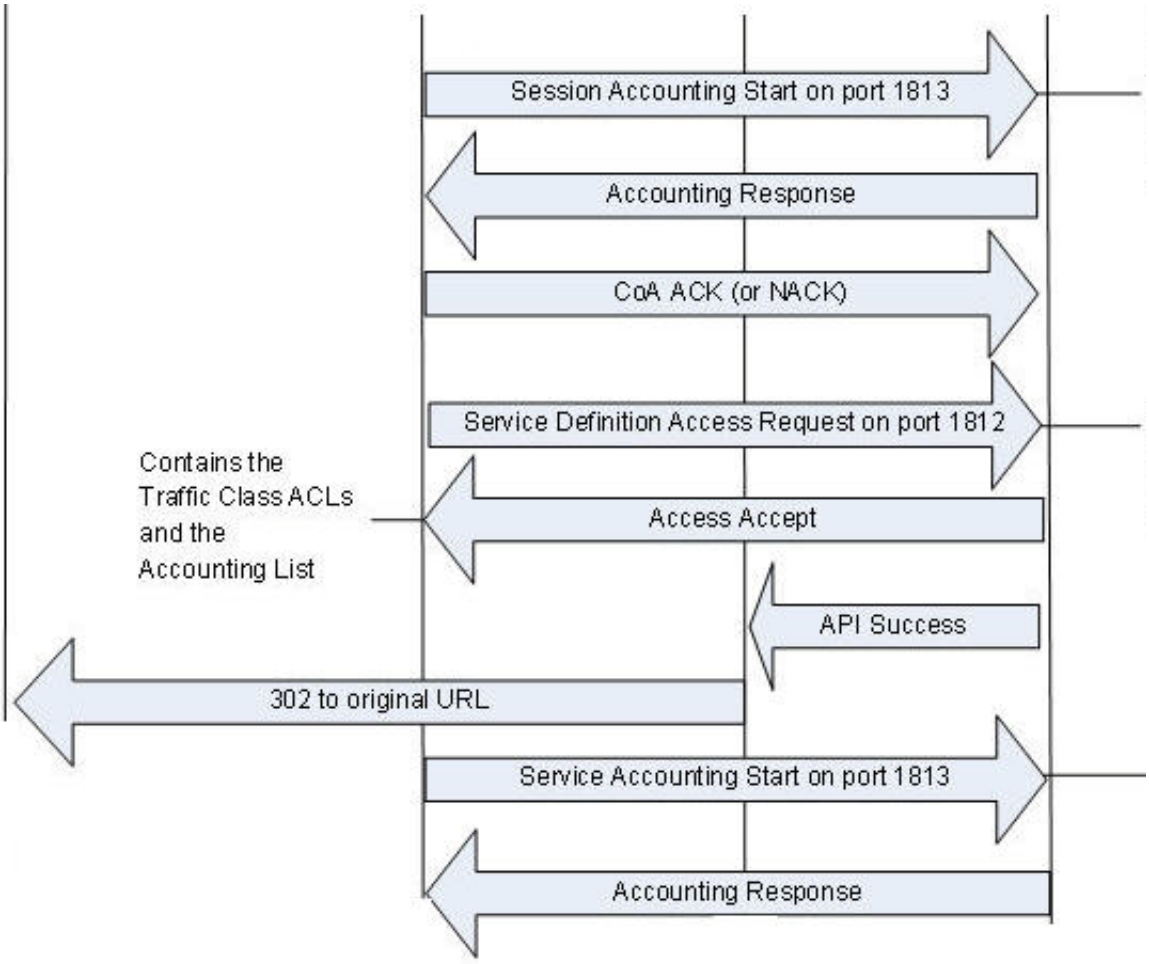
(continued)


Service Accounting Stop on port 1813
Username, service name, acct session id, parent acct session id, nas ip, framed ip all needed
Accounting Response
Session Accounting Start on port 1813
Username, service name, acct session id, nas ip, framed ip all needed
Accounting Response
http://google.com
MAC Access Request on port 1812
MAC as Username, password, acct session id, nas ip, framed ip all needed
Contains the service assigned 512K-DOWN
Access Accept

Tiered Services Call Flow



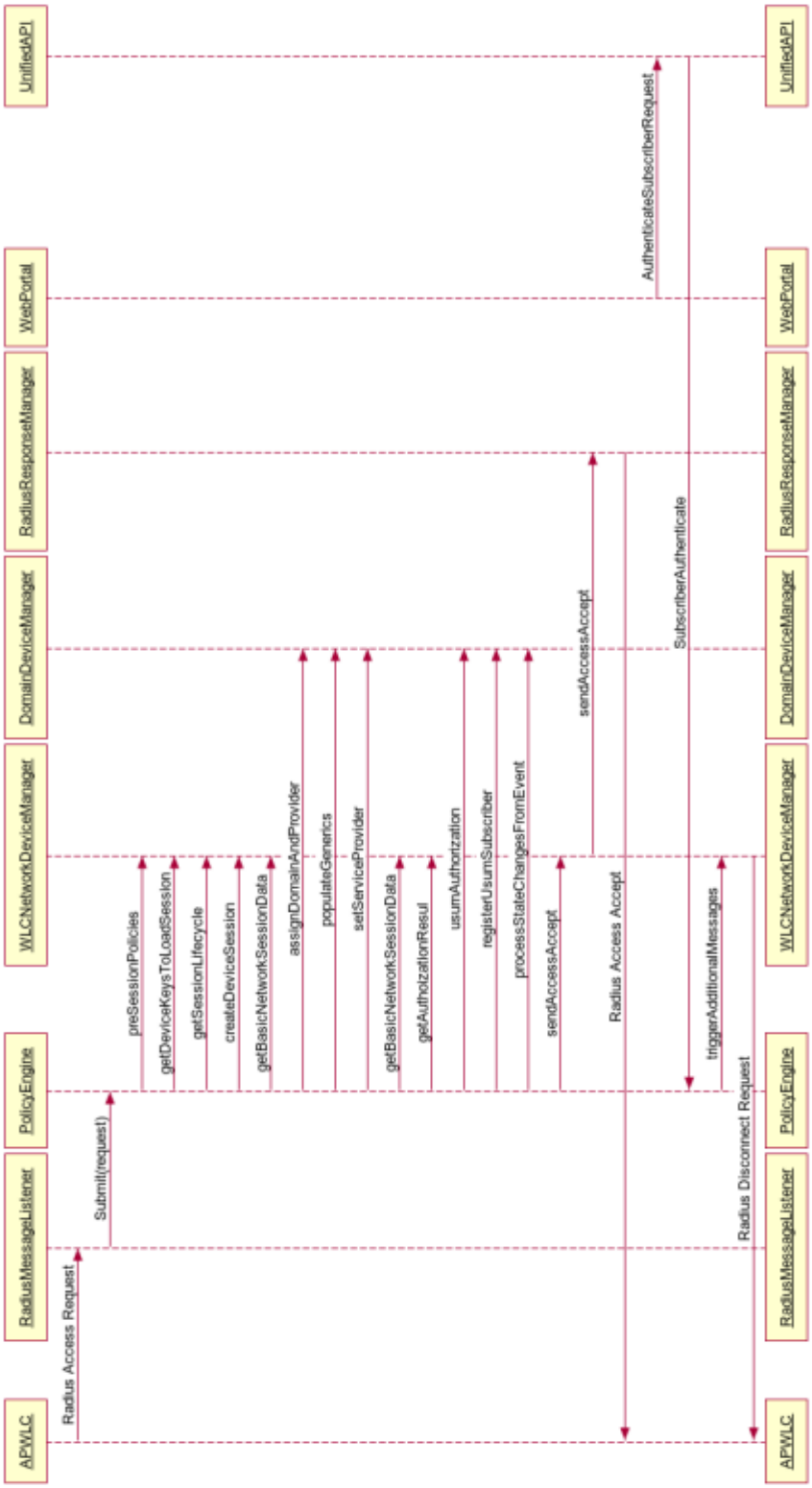
(continued)



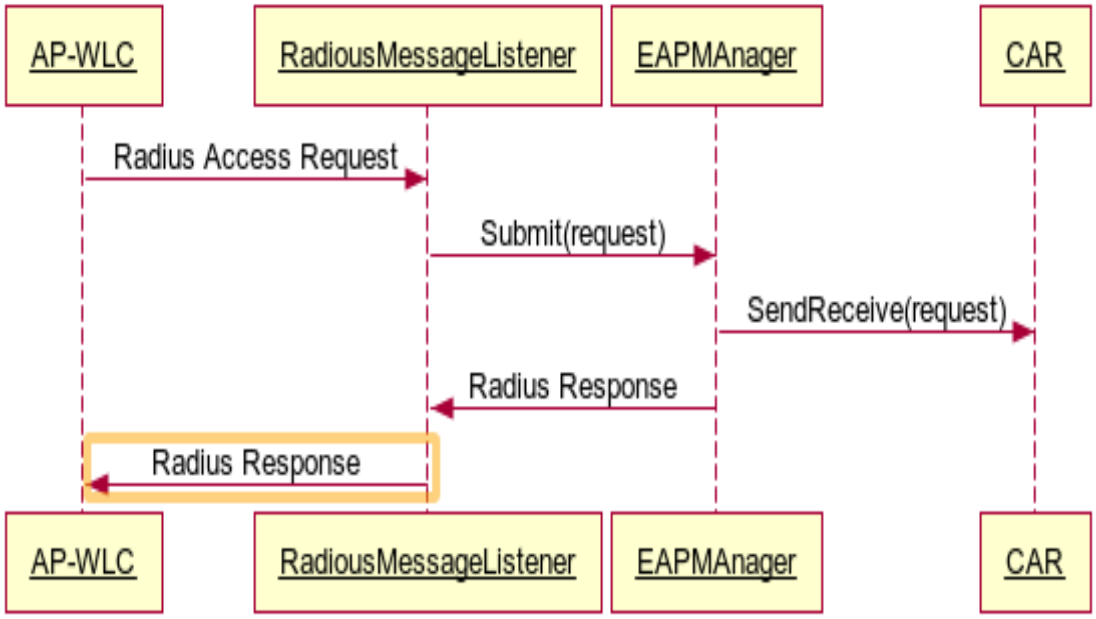
SP WiFi-4.0 Call Flows

Following are the call flows within the CPS system based on the requests received from the network device and the presence of the subscriber information in SPR profile.

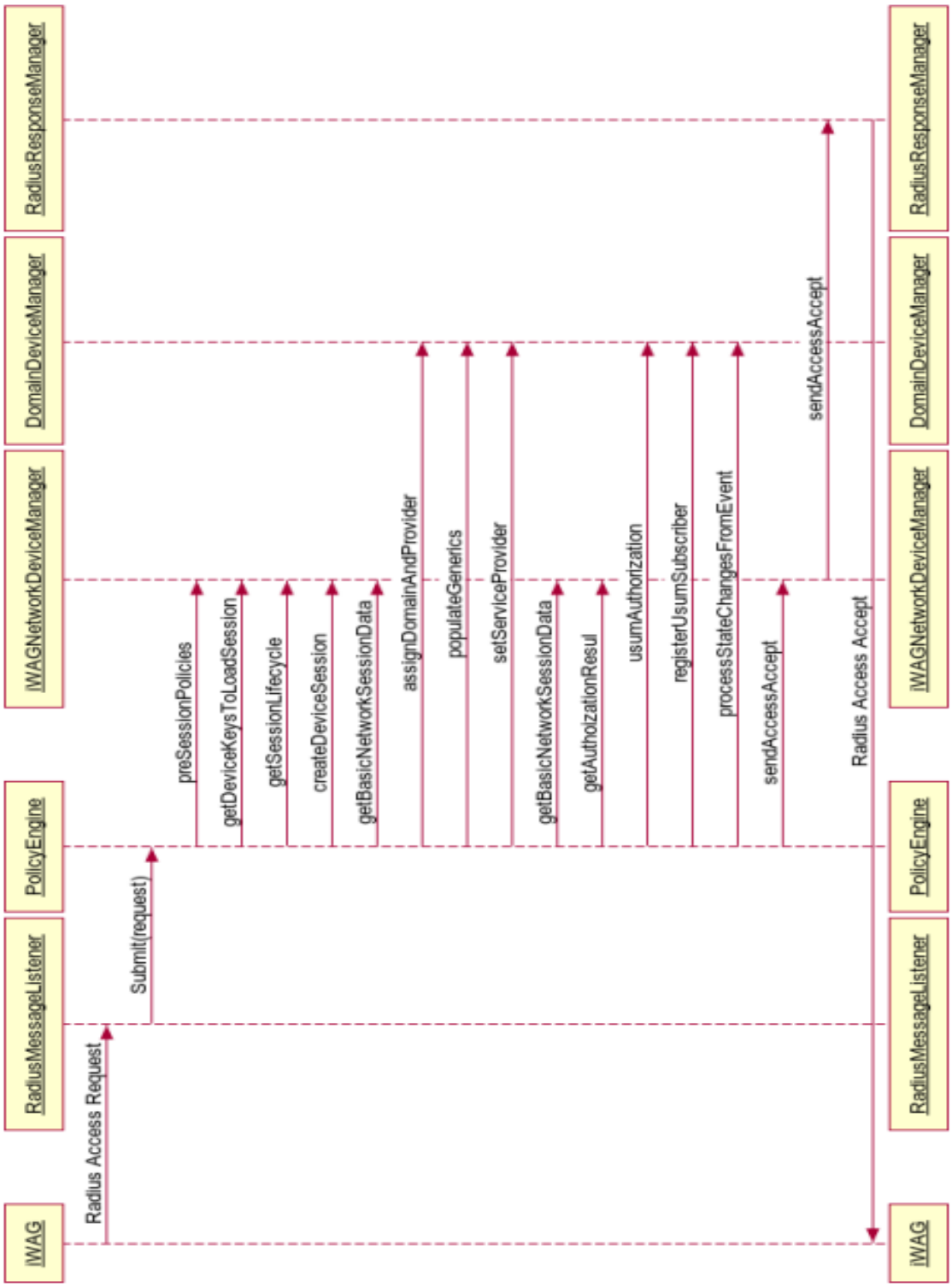
Authentication Sequence in WLC Network Device Manager



Authentication Sequence for EAP Requests

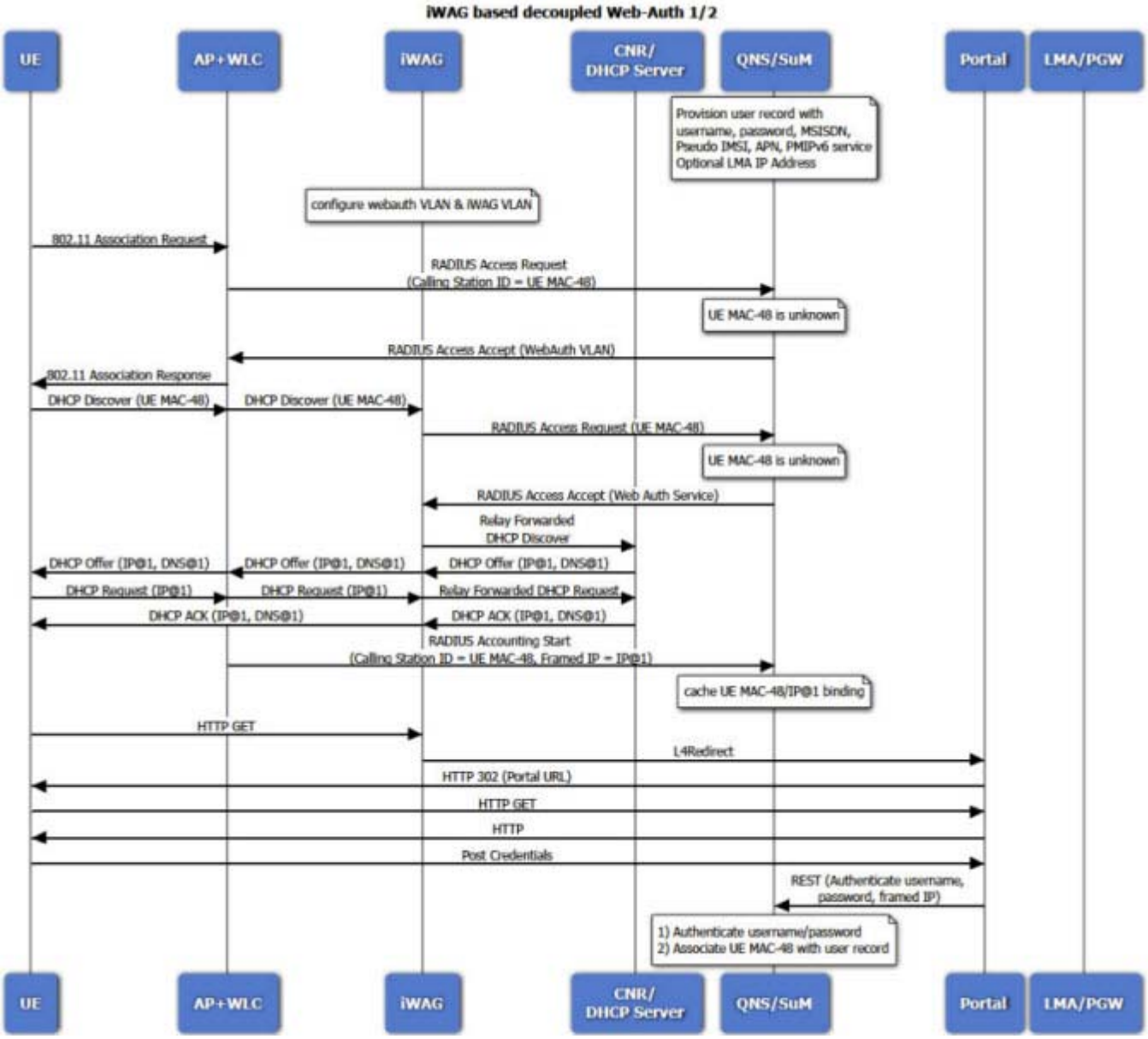


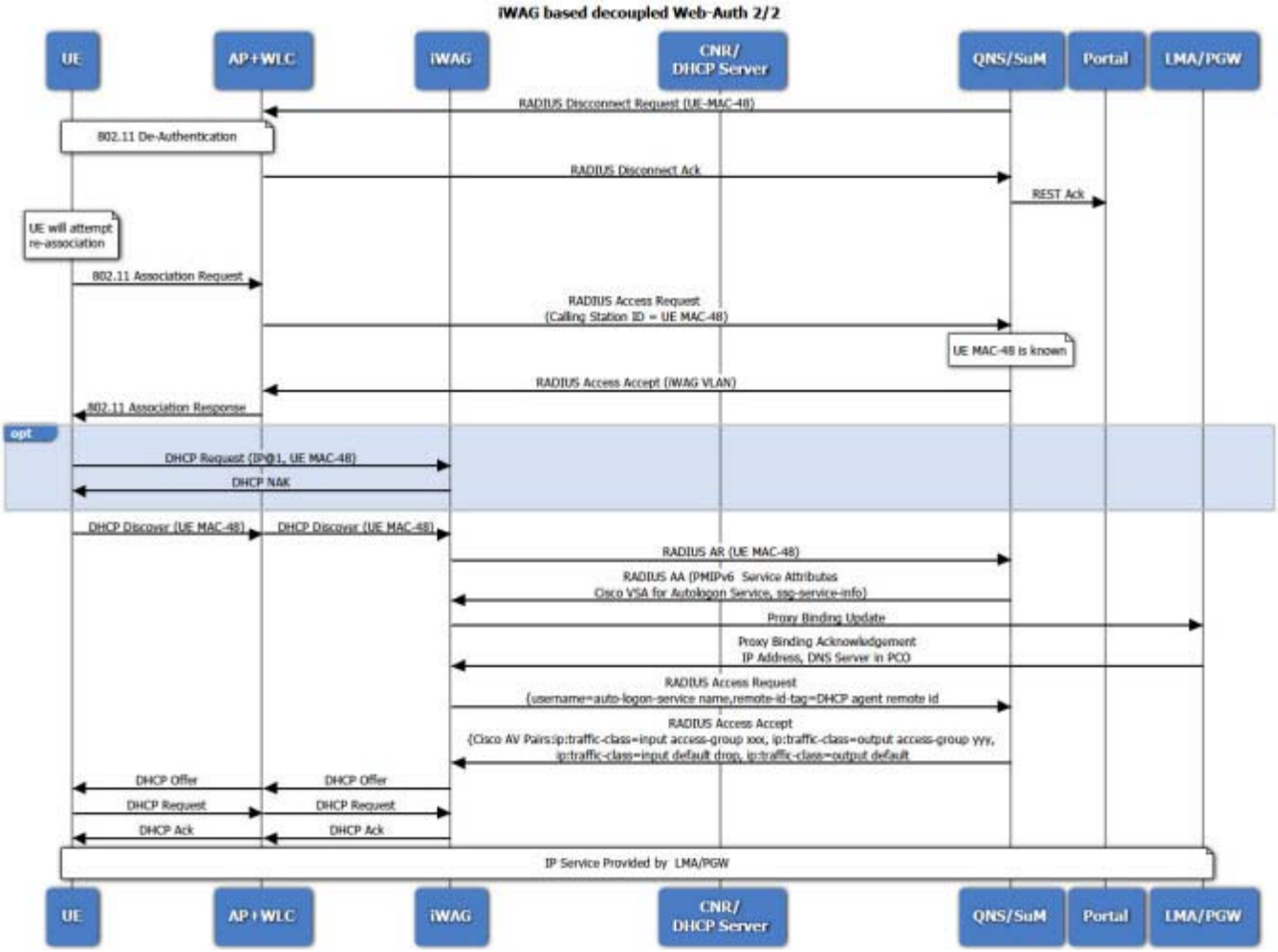
Authentication Sequence in iWAG Network Device Manager



MAG Coupled Web Based Authentication

MAG coupled Web based authentication entails that the unauthenticated client will be assigned a temporary IP address. This temporary IP address is used as the source address by the UE while accessing the web portal. After successful authentication, the client is forced to re-associate and that will cause the client to go through the IP address assignment phase again. At this stage since the client is already authenticated, the LMA will assign the IP address for the client.




iWAG based decoupled Web-Auth 2/2
UE
AP+WLC
iWAG
CNR/ DHCP Server
QNS/SuM
Portal
LMA/PGW
RADIUS Disconnect Request (UE-MAC-48)
802.11 De-Authentication
RADIUS Disconnect Ack
REST Ack
UE will attempt re-association
802.11 Association Request
RADIUS Access Request (Calling Station ID = UE MAC-48)
UE MAC-48 is known
RADIUS Access Accept (iWAG VLAN)
802.11 Association Response
opt
DHCP Request (IP@1, UE MAC-48)
DHCP NAK
DHCP Discover (UE MAC-48)
DHCP Discover (UE MAC-48)
RADIUS AR (UE MAC-48)
RADIUS AA (PMIPv6 Service Attributes Cisco VSA for Autologon Service, ssg-service-info)
Proxy Binding Update
Proxy Binding Acknowledgement IP Address, DNS Server in PCO
RADIUS Access Request (username=auto-logon-service name,remote-id-tag=DHCP agent remote id
RADIUS Access Accept (Cisco AV Pairs:ip:traffic-class=input access-group xxx, ip:traffic-class=output access-group yyy, ip:traffic-class=input default drop, ip:traffic-class=output default
DHCP Offer
DHCP Offer
DHCP Request
DHCP Request
DHCP Ack
DHCP Ack
IP Service Provided by LMA/PGW

Logs

Revised: July 10, 2015,

Logs

Most of the CPS logs are located locally in `/var/log/broadhop/` on virtual machines IOMGRxx, QNSxx, and PCRFclientXX. PCRFclient01 contains the consolidated logs from all of the IOMGR, QNS and PCRFCLIENT virtual machines.

The CPS logs can be divided based on Application/Script which produces the logs:

- Application/Script Produces Logs: Upgrade Script, Upgrade Binary, page B-1
- Application/Script Produces Logs: qns, page B-2
- Application/Script Produces Logs: qns pb, page B-3
- Application/Script Produces Logs: mongo, page B-3
- Application/Script Produces Logs: httpd, page B-4
- Application/Script Produces Logs: portal, page B-4
- Application/Script Produces Logs: license manager, page B-5
- Application/Script Produces Logs: svn, page B-5
- Application/Script Produces Logs: auditd, page B-5
- Application/Script Produces Logs: graphite, page B-6
- Application/Script Produces Logs: kernel, page B-7

Application/Script Produces Logs: Upgrade Script, Upgrade Binary

- **Log:** upgrade log
- **Description:** Log messages generated during upgrade of CPS.
- **Log file name, format, path:**

  AIO: /var/log/broadhop/upgrade<date>_<time>.log

  HA/GR: pcrfclient01:/var/log/broadhop/upgrade<date>_<time>.log
- **Log config File:** NA
- **Log Rollover:** No

Application/Script Produces Logs: qns

- **Log:** qns log
  - **Description:** Main and most detailed logging. Contains initialization errors and application level errors.
  - **Log file name, format, path:**

    AIO: /var/log/broadhop/qns-<instance no>.log

    HA/GR: pcrfclient01:/var/log/broadhop/qns-<instance no>.log
  - **Log config File:** /etc/broadhop/logback.xml
  - **Log Rollover:** No
- **Log:** qns engine logs
  - **Description:** Higher level event based logging including what services a subscriber has, the state of the session, and other useful information.
  - **Log file name, format, path:**

    AIO: /var/log/broadhop/qns-engine-<instance no>.log

    HA/GR: /var/log/broadhop/qns-engine-<instance no>.log
  - **Log config File:** NA
  - **Log Rollover:** No
- **Log:** qns service logs
  - **Description:** Contains start up logs. Also if the logback.xml is incorrectly formatted all logging statements go into this log.
  - **Log file name, format, path:**

    AIO: /var/log/broadhop/service-qns-<instance no>.log

    HA/GR: qns0*: /var/log/broadhop/service-qns-<instance no>.log
  - **Log config File:** NA
  - **Log Rollover:** No
- **Log:** consolidated qns logs
  - **Description:** Contains the consolidation of all qns logs with the IP of the instance as part of the log event.
  - **Log file name, format, path:**

    AIO: NA

    HA/GR: pcrfclient01: /var/broadhop/log/consolidated-qns.log
  - **Log config File:** /etc/broadhop/controlcenter/logback.xml
  - **Log Rollover:** No
- **Log:** consolidated engine logs
  - **Description:** Contains the consolidation of all qns engine logs with the IP of the instance as part of the log event.
  - **Log file name, format, path:**

    AIO: NA

    HA/GR: /etc/broadhop/controlcenter/logback.xml

  - **Log config File:** /etc/broadhop/controlcenter/logback.xml
  - **Log Rollover:** No
- **Log:** consolidated diagnostics logs
  - **Description:** Contains logs about errors occurred during diagnostics of CPS.
  - **Log file name, format, path:**

    AIO: NA

    HA/GR: /pcrfclient01: /var/log/broadhop/ consolidated-diag.log
  - **Log config File:** NA
  - **Log Rollover:** No

Application/Script Produces Logs: qns pb

- **Log:** qns pb logs
  - **Description:** Policy builder startup, initialization logs get logged into this log file.
  - **Log file name, format, path:**

    AIO: /var/log/broadhop/ qns-pb.log

    HA/GR: pcrfclient01: /var/log/broadhop/qns-pb.log
  - **Log config File:** NA
  - **Log Rollover:** No
- **Log:** service qns pb logs
  - **Description:** Policy builder service logs.
  - **Log file name, format, path:**

    AIO: /var/log/broadhop/ service-qns-pb.log

    HA/GR: pcrfclient01: /var/log/broadhop/service-qns-pb.log
  - **Log config File:** NA
  - **Log Rollover:** No
- **Log:** qns engine pb logs
  - **Description:** Policy builder engine logs.
  - **Log file name, format, path:**

    AIO: /var/log/broadhop/ qns-engine-pb.log

    HA/GR: pcrfclient01: /var/log/broadhop/qns-engine-pb.log
  - **Log config File:** NA
  - **Log Rollover:** No

Application/Script Produces Logs: mongo

- **Log:** mongo db logs
- **Description:** Contains useful information about the mongo db operations including queries, errors, warnings, and users behavior.
- **Log file name, format, path:**

AIO: /var/log/mongodb-<port>.log

HA/GR: sessionmgr01: /var/log/mongodb-<port>.log

- **Log config File:** /etc/mongod.conf
- **Log Rollover:** No

Application/Script Produces Logs: httpd

- **Log:** httpd access logs
  - **Description:** Apache server records all incoming requests and all requests processed to a log file.
  - **Log file name, format, path:**

    AIO: /var/log/httpd/access_log

    HA/GR: pcrfclient01: /var/log/httpd/access_log
  - **Log config File:** /etc/httpd/conf/httpd.conf
  - **Log Rollover:** Yes
- **Log:** httpd error logs
  - **Description:** All apache errors/diagnostic information about other errors found during serving requests are logged to this file. This apache log file often contain details of what went wrong and how to fix it.
  - **Log file name, format, path:**

    AIO: /var/log/httpd/error_log

    HA/GR: pcrfclient01: /var/log/httpd/error_log
  - **Log config File:** /etc/httpd/conf/httpd.conf
  - **Log Rollover:** Yes

Application/Script Produces Logs: portal

- **Log:** portal request logs
  - **Description:** Contains the API requests that are sent from the portal to the QNS system.
  - **Log file name, format, path:**

    AIO: /var/www/portal/app/tmp/logs/api_request.log

    HA/GR: portal01: /var/www/portal/app/tmp/logs/api_requests.log
  - **Log config File:** NA
  - **Log Rollover:** No
- **Log:** portal response logs
  - **Description:** Contains the API response that are sent from the qns to portal.
  - **Log file name, format, path:**

    AIO: /var/www/portal/app/tmp/logs/api_response.log

    HA/GR: portal01: /var/www/portal/app/tmp/logs/api_response.log
  - **Log config File:** NA
  - **Log Rollover:** No

- **Log:** portal error logs
  - **Description:** Contains error level logs of the application. Generally not useful to anyone except the portal developers. It generally reveals permission issues on installations.
  - **Log file name, format, path:**

    AIO: /var/www/portal/app/tmp/logs/error.log

    HA/GR: portal01: /var/www/portal/app/tmp/logs/error.log
  - **Log config File:** NA
  - **Log Rollover:** No
- **Log:** portal debug logs
  - **Description:** Contains debug level logs of the application.Generally not useful to anyone except the portal developers. It generally reveals permission issues on installations.
  - **Log file name, format, path:**

    AIO: /var/www/portal/app/tmp/logs/debug.log

    HA/GR: /var/www/portal/app/tmp/logs/debug.log
  - **Log config File:** NA
  - **Log Rollover:** No

Application/Script Produces Logs: license manager

- **Log:** lmgrd logs
- **Description:** Contains license file related errors.
- **Log file name, format, path:**

  AIO: /var/log/broadhop/lmgrd.log

  HA/GR: pcrfclient01: /var/log/broadhop/lmgrd.log
- **Log config File:** NA
- **Log Rollover:** No

Application/Script Produces Logs: svn

- **Log:** SVN log
- **Description:** svn log command displays commit log messages. For more information refer: `/usr/bin/svn log -help`. For example,./usr/bin/svn log http://lbvip02/repos/run
- **Log file name, format, path:**

  AIO: NA

  HA/GR: NA
- **Log config File:** NA
- **Log Rollover:** No

Application/Script Produces Logs: auditd

- **Log:** audit logs
- **Description:** Contains log of all sessions established with CPS VM. SSH session logs, cron job logs.

- **Log file name, format, path:**

  AIO: /var/log/audit/audit.log

  HA/GR: pcrfclient01: /var/log/audit/audit.log
- **Log config File:** NA
- **Log Rollover:** Yes

Application/Script Produces Logs: graphite

- **Log:** carbon client logs
  - **Description:** Contains client connection logs.
  - **Log file name, format, path:**

    AIO: /var/log/carbon/client.log

    HA/GR: pcrfclient01: /var/log/carbon/client.log
  - **Log config File:** /root/monitoring/graphite/conf/carbon.conf
  - **Log Rollover:** No
- **Log:** carbon console logs
  - **Description:** Contains process startup and initialization logs.
  - **Log file name, format, path:**

    AIO: /var/log/carbon/ console.log

    HA/GR: pcrfclient01: /var/log/carbon/console.log
  - **Log config File:** /root/monitoring/graphite/conf/carbon.conf
  - **Log Rollover:** No
- **Log:** carbon query logs
  - **Description:** Contains log queries which are performed on the application.
  - **Log file name, format, path:**

    AIO: /var/log/carbon/query.log

    HA/GR: pcrfclient01: /var/log/carbon/query.log
  - **Log config File:** /root/monitoring/graphite/conf/carbon.conf
  - **Log Rollover:** No
- **Log:** carbon creates logs
  - **Description:** This log tells you what .wsp (whisper) db files are being created.
  - **Log file name, format, path:**

    AIO: /var/log/carbon/creates.log

    HA/GR: pcrfclient01: /var/log/carbon/creates.log
  - **Log config File:** /root/monitoring/graphite/conf/carbon.conf
  - **Log Rollover:** Yes
- **Log:** carbon listener logs
  - **Description:** Contains connection related logs.
  - **Log file name, format, path:**

AIO: /var/log/carbon/listener.log

HA/GR: pcrfclient01: /var/log/carbon/listener.log

- **Log config File:** /root/monitoring/graphite/conf/carbon.conf
- **Log Rollover:** Yes

Application/Script Produces Logs: kernel

- **Log:** haproxy
- **Description:** Contains information like if VIP handoff.
- **Log file name, format, path:**

  AIO: /var/log/messages

  HA/GR: pcrfclient01: /var/log/messages
- **Log config File:** NA
- **Log Rollover:** Yes

Basic Troubleshooting Using CPS Logs

- Start the engine logs on pcrfclient01.
- This displays issues or problems in the subscriber or services. If the event is not found in the engine logs, check the qns logs to look for anomalies.
- It is good to understand when the call was supposed to occur in order to narrow down the issue.
- If there are no ERRORs or no exceptions, etc, then we can increase the logging levels. Policy tracing and logs at DEBUG levels can usually indicate the problem.
- But just like a router, too much debugging can affect the performance of the system.
- Use grep usernames, mac addresses, IP addresses, etc in logs to find required information.

Logging Level and Effective Logging Level

Logging level and the actual effective logging level can be two different levels because of the following logback logging rules:

1. When a logging level is set, if the logging level of the parent process is higher than the logging level of the child process, then the effective logging level of the child process is that of the parent process. That is, even though the logging level of the child process is set, it cannot be below the logging level of the parent process and is automatically overridden to the higher logging level of the parent process.
2. There is a global “root” logging level that each process can inherit as an effective default logging level. If you do not want to have a default effective logging level, then set the root level to OFF.
3. Each logging level prints the output of the lower logging levels.

This following table displays the logging level and the message types printed due to 3. above.

Level	Message Types Printed
All	Equivalent to Trace and some more messages.
Trace	Trace, Debug, Info, Warn, & Error
Debug	Debug, Info, Warn, & Error
Info	Info, Warn, & Error
Warn	Warn & Error
Error	Error
Off	-

The following table describes the different logging levels and what they should be used for:

Logging Level	Description	Valid Use Case	Invalid Use Case
Error	Error conditions that breaks a system feature. Errors logging level should not be used for call flow errors.	Database is not available.	Subscriber not found.
Warn	Helps to understand the early signs that will prevent the system from functioning in the near future OR are triggered by unexpected preconditions in a method.	Retrieved more then one Gx QoS profile.	Warnings should not be used for individual call flows. No service found for session.
Info	Helps to understand the life cycle of components and subsystems, such as plug-ins, databases.	NA	Info should not be used for individual call flows.
Debug	Helps to understand the flow of the code execution at Class/Method level. i.e. in _createIsgDeviceSession({log...)	NA	NA
Trace	Helps to understand the values of the statement and branch of logics within the method for troubleshooting.	NA	NA

You can configure target and log rotation for consolidated logs in log configuration file `/etc/broadhop/controlcenter/logback.xml`.

The following parameters can be configured for target VM and port.

```
<appender name="SOCKET-BASE"
class="ch.qos.logback.classic.net.SocketAppender>"
    <RemoteHost>${logging.controlcenter.host:-lbvip02}</RemoteHost>
    <Port>${logging.controlcenter.port:-5644}</Port>
    <ReconnectionDelay>10000</ReconnectionDelay>
    <IncludeCallerData>false</IncludeCallerData>
```

```
</appender>
```

The above configuration is used to redirect consolidated logs to lbvip02 VM on port 5644 with reconnection delay.

Log rotation is configured using following configuration in `/etc/broadhop/controlcenter/logback.xml`.

```
<rollingPolicy
      class="ch.qos.logback.core.rolling.FixedWindowRollingPolicy">
      <fileNamePattern>
${com.broadhop.log.dir:-/var/log/broadhop}/consolidated-diag.%i.log.g
z
      </fileNamePattern>
      <minIndex>1</minIndex>
      <maxIndex>5</maxIndex>
    </rollingPolicy>
<triggeringPolicy
      class="ch.qos.logback.core.rolling.SizeBasedTriggeringPolicy">
      <maxFileSize>100MB</maxFileSize>
    </triggeringPolicy>
```

Using the above configuration 100 MB log files are generated and after that log files rotate from index 1 to 5.

When the 100 MB log file trigger condition is met, the order in which CPS system performs the file operations is:

- log.5.gz > deleted
- log.4.gz > log.5.gz
- log.2.gz > log.3.gz
- log.1.gz > log.2.gz
- Current > log.1.gz

Similar configurations can be applied for qns logs in `/etc/broadhop/logback.xml`.