TESTING & INTEGRATION GROUP

SOLUTION GUIDE

Oracle Communication Service Load Balancing with Radware SIP Director.

Contents

TECHNICAL SOLUTION GUIDE

AUTHOR: Elad Kurzweil

DATE: Monday, Tuesday, March 02, 2010
Version: 1.0

Introduction

More and more Voice applications are moving from the legacy voice infrastructure to the IP network. The IP allows more flexibility in serving large amounts of calls, and the SIP communication protocol that runs over the IP network allows faster development of advanced VoIP services. This is achieved through the use of Application server platforms – rich infrastructure to develop an application logic reducing Time-to-Market for new services.

Moving to IP brings opportunities and challenges with it. The opportunity to change the static delivery and resource allocation of legacy systems to a much more efficient IP service delivery brings a few challenges with it, like guaranteeing the availability and scalability of IP services with 99.999% of call completion and the highest quality of service. To avoid such challenges, smart delivery solutions are used on the IP network to guarantee the delivery of VoIP applications over IP networks.

This document describes a highly available and scalable solution for building a SIP application server platform. The solution is based on Oracle's Communication Server technology clustered behind Radware's SIP Director, a SIP application delivery product.

Radware SIP Director Overview

Radware's SIP Director guarantees SIP service delivery. SIP Director is a comprehensive SIP Application Delivery Controller (ADC) for SIP value-added application vendors, Telecom Equipment Manufacturers (TEMs) and System Integrators (SIs). SIP Director is designed to work with a wide range of applications including application/feature servers such as IVRs, conference applications and 911 services. SIP Director provides carrier grade performance across all IMS network layers from the Service Plane through the Control and Signaling Plane to the Transport Plane. SIP Director is also optimized for pre-IMS networks and entities including softswitches and SBCs.

Radware's VoIP/SIP ADC solution delivers the intelligence needed to address the VoIP/SIP service delivery requirements of carriers and operators deploying today's VoIP services. Radware's solution for VoIP/SIP service continuity and optimization provides:

High availability through local and global clustering, health monitoring and optimal call completion

Scalability through unlimited call handling capacity, load balancing, traffic acceleration and performance optimization

Enhanced interoperability through support of SIP/SIPS over UDP, TCP and TLS, including protocol conversion

Unmatched flexibility through an easy to use configuration with no scripting or coding required

Integration & operation simplicity by functioning as a SIP Proxy

Security providing user and network protection and privacy enablement

Reduced time-to-market through out-of-the-box carrier grade compliance enablement

By using SIP Director carriers, operators, vendors, SIs and TEMs benefit from service continuity, enhanced user experience, reduced OPEX/CAPEX as well as shorter development and deployment cycles reducing time-to-market.

For further information about how Radware products ensure the safe delivery of critical applications across a variety of networks, explore our full suite of application delivery products.

Oracle Communication Service

Oracle Communications Service Delivery is a family of open, standards-based telecom service delivery platform (SDP) middleware and application products, designed to enable network operators, service providers, enterprises, and third party developers to harness and monetize the power of the Web, telecommunications, social networking, and IT assets. This product family is designed to meet the needs of customers implementing a wide variety of SDP solutions, including converged IP services, open third party service exposure platforms, next-generation Intelligent Network (IN) communication services, and mobile marketing and advertising campaigns.

The Oracle Communications Service Delivery product family consists of products that deliver converged Web and telecom service creation, execution, exposure, and management capabilities. This includes the industry-leading converged Java EE-SIP-IMS application server, Oracle Communications Converged Application Server (formerly BEA WebLogic SIP Server), and the industry's most widely deployed network service exposure and SDP policy and partner management platform, Oracle Communications Services Gatekeeper (formerly BEA WebLogic Network Gatekeeper).

The Oracle Communications Service Delivery product family consists of the following products:

- Oracle Communications Converged Application Server: Converged Web-telecom application server, to enable the rapid, low-cost and profitable development and deployment of converged IP services based on open, industry standards such as SIP Servlets, Java EE, IMS and SOA/Web Services. Leading customer use cases include Voice over IP (VoIP), conferencing, IP Centrex, IP Multimedia Subsystem (IMS) and Next-Generation IN (NGIN) services.
- Oracle Communications Services Gatekeeper: Open, third-party service exposure platform, designed to enable operators to better monetize their network assets by leveraging content and applications from third party developers and partners. It is based on leading industry standards including Java EE, SIP/IMS, Parlay X, Web 2.0 (REST), SOA, and Web Services. Leading customer use cases include third party service exposure, content delivery, policy enforcement, and active mediation.
- Oracle Communications Marketing and Advertising: Centralized marketing and advertising campaign management and execution platform, to enable operators to offer partners and advertisers with highly targeted, and personalized marketing and ad campaigns. Based on open, industry standards including Java, SOA, and Web Services. Customer use cases include targeted bulk messaging campaigns over SMS, MMS and WAP Push.

Network operators, service providers and enterprises worldwide have implemented and launched commercially successful services using Oracle Communications Service Delivery products, such as Telecom Italia, O2 UK, SingTel, 3 Australia, mobilkom austria, Telstra, VimpelCom, Aircel, ETRI, InterCall, Italtel, Korea Telecom, and Vodafone Netherlands, among others.

For more information, please visit:
http://www.oracle.com/industries/communications/oracle-communications-services-delivery.html

Solution Details

The suggested solution uses 2 Oracle Communication Service servers for SIP. The 2 SIP Directors are installed in the front of the Oracle Communication Service servers in order to provide SIP load balancing, availability, acceleration and protection:

- SIP Director continuously monitors the operational availability of the Oracle Communication Service servers
- SIP Director intelligently distributes the VOIP calls transactions between the Oracle Communication Service servers, making sure that all transactions that belong to the same VOIP session will reach the same Oracle Communication Service servers. Session stickiness between servers is maintained by using call ID persistency.
- SIP Director seamlessly enables TCP support for the cluster, transforming SIP/TCP requests to SIP UDP. To enable TLS, a similar paradigm would be followed.
- The dual SIP Director are providing a highly available solution with no single point of failure
- The SIP Director is using the Configuration Synchronization mechanism to provide automatic configuration synchronization.

Traffic flow from client can come in UDP or TCP and will be translated to UDP in the backend server side; the servers are working in B2BUA mode, when the server opens a call to another client will act as a client (new session ID), all traffic outgoing from the servers are directed to the SIP Director VIP (outbound proxy). All server side traffic is done in SIP UDP and Client side is done in TCP or UDP.

Important Notes:

- **SIP traffic – policy settings**

The SIP Director works as a proxy and deals both with the calls coming from the network to the application server cluster and calls going out from the application server cluster (B2BUA) to the network. For that, the SIP Director manages different L4 policies. The first one is for traffic coming from the network, that goes through the load balancing logic to select an application server. The second one is for handling communication coming from the servers towards the network, that goes through simple SIP routing logic.

- **Pre-requisites for Configuration Synchronization**

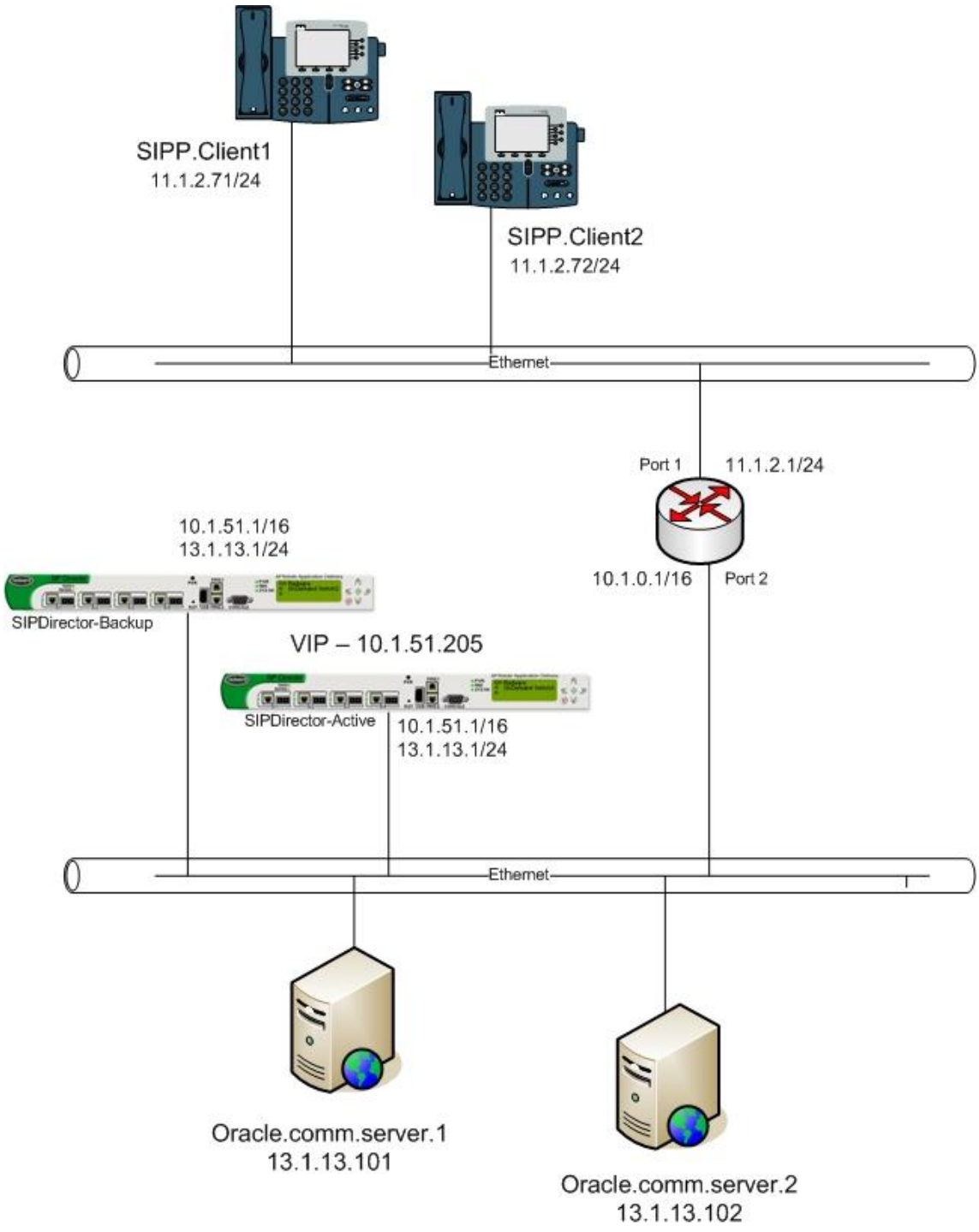
In order for the auto-configuration synchronization to work, master and slave devices must match the following criteria:
1. Hardware platform type - The Master device and the Slave device must use the same hardware platform.
2. Memory size.
3. License - (license upgrading will have to be done manually on both devices, since each license is bound to a specific machine).
4. Software version - Any software upgrade will be performed manually on each device. During this time, the configuration synchronization must be disabled.
5. Network topology (parallel ports connected to the same subnets and the same IP addresses matching crosswise).
6. Before the configuration is synchronized for the first time, there must be at least one matching IP interface (same subnet, same interface) on the two devices.

Software and Hardware

The following is a list of hardware and Multimedia software tested to verify the interoperabilty of the presented solution:

Radware's SIP Director v.2.20
SIP Servers : Oracle Communication Service Servers v.4.0
SIP Client: SIPP v3.0

Tested network overview



Network Diagram

Configuration

Radware Devices

SIP DIRECTOR ACTIVE CONFIGURATION

Network Configuration

- Create IP 10.1.51.1/16 on port 1 in **Router -> IP Router -> Interface Parameters** with these parameters,
  - IP Address – 10.1.51.1
  - Network Mask – 255.255.0.0
  - If Number – 1
  - Peer Address – 10.1.51.2 (This IP represent the backup device for Configuration Synchronization)

- Create IP 13.1.13.1/24 on port 1 in **Router -> IP Router -> Interface Parameters** with these parameters,
  - IP Address – 13.1.13.1
  - Network Mask – 255.255.255.0
  - If Number – 1
  - Peer Address – 13.1.13.2 (This IP represent the backup device for Configuration Synchronization)

- Create IP 10.210.6.22/16 (management) on port 1 in **Router -> IP Router -> Interface Parameters** with these parameters,
  - IP Address – 10.210.6.22
  - Network Mask – 255.255.0.0
  - If Number – MNG1
  - Peer Address – 10.210.6.23 (This IP represent the backup device for Configuration Synchronization)

- Create Default Gateway to 10.1.0.1 (management) on port 1 in **Router -> IP Router -> Routing Table** with these parameters,
  - Destination Address – 0.0.0.0
  - Network Mask – 0.0.0.0
  - Next Hop – 10.1.0.1
  - Interface Index – 1

SIP Farm Configuration

- Create Farm named "oracle.communication.farm" in **SIP Director-> SIP -> Farms -> Farm Table** with these parameters
  - Farm Name – oracle.communication.farm
  - Leave all other fields as default

SIP Servers Configuration

- Create Server named "oracle.com.server.1" and attach it to Farm "oracle.communication.farm" in **SIP Director -> SIP -> Servers -> Server Table** with these parameters
  - Server Name - oracle.com.server.1
  - Farm Name – oracle.communication.farm
  - Server Address – 13.1.13.101
  - Leave all other fields as default

- Create Server named "oracle.com.server.2" and attach it to Farm "oracle.communication.farm" in **SIP Director -> SIP -> Servers -> Server Table** with these parameters
    - Server Name - oracle.com.server.2
    - Farm Name – oracle.communication.farm
    - Server Address – 13.1.13.102
    - Leave all other fields as default

SIP Layer 4 Configuration

- Create L4 Policy for SIP Traffic named "oracle.comm.flow" in **SIP Director -> SIP -> Layer 4 Target Selection -> Layer 4 Policy Table** with these parameters
    - Virtual IP – 10.1.51.205
    - L4 Protocol – UDP
    - L4 Port – 5060
    - L4 Policy Name – oracle.comm.flow
    - Application – SIP
    - Action Type – Farm
    - Action – oracle.communication.farm
    - Leave all other fields as default

- Create L4 Policy for SIP Traffic named "outbound.from.servers" in **SIP Director -> SIP -> Layer 4 Target Selection -> Layer 4 Policy Table** with these parameters
    - Virtual IP – 10.1.51.205
    - L4 Protocol – UDP
    - L4 Port – 5060
    - L4 Policy Name – outbound.from.servers
    - Source IP From – 13.1.13.101
    - Source IP To – 13.1.13.102
    - Application – SIP
    - Action Type – Routing
    - Leave all other fields as default

Classification Criteria Configuration

- Create network call for oracle.server.2 named "oracle.server.2" in **SIP Director -> SIP -> Classification Criteria -> IP Networks** with these parameters
    - IP Network Name – oracle.server.2
    - IP Network Index – 1
    - From IP – 13.1.13.102
    - To IP – 13.1.13.102
    - Leave all other fields as default

- Create network call for oracle.server.1 named "oracle.server.1" in **SIP Director -> SIP -> Classification Criteria -> IP Networks** with these parameters
    - IP Network Name – oracle.server.1
    - IP Network Index – 1
    - From IP – 13.1.13.101
    - To IP – 13.1.13.101
    - Leave all other fields as default

SIP Forwarding Policies Configuration

Note1 *- Because oracle.server.2 is configured to listen to port 5070 we need to multiplex destination port 5060 that comes from the client side to port 5070 UDP that the oracle.server.2 is listening.*

SIP Forwarding Policy Table Classification

- Create Forwarding Policy for port 5070 multiplexing Traffic named "oracle.server.2.to.udp.5070" in **SIP Director -> SIP -> Proxy Control -> SIP Forwarding Policies** with these parameters
    - Priority – 1
    - Name – oracle.server.2.to.udp.5070
    - Virtual IP – 10.1.51.205
    - Destination Port – 5060
    - Transport – UDP
    - Scheme – SIP
    - Target Network – oracle.server.2
    - Expression - ANY
    - Leave all other fields as default

SIP Forwarding Policy Table Action

- Change the Forwarding Policy Action for port 5070 multiplexing Traffic named "oracle.server.2.to.udp.5070" in **SIP Director -> SIP -> Proxy Control -> SIP Forwarding Policies** with these parameters
    - UDP Destination Port - 5070
    - Leave all other fields as default

Note2 *– Clients that are using SIP TCP 5060 we need to translate client SIP TCP to SIP UDP (oracle.server.1 is listening for SIP 5060 UDP traffic).*

SIP Forwarding Policy Table Classification

- Create Forwarding Policy for port 5060 Traffic named "oracle.server.1.from.tcp.5060.to.udp.5060" in **SIP Director -> SIP -> Proxy Control -> SIP Forwarding Policies** with these parameters
    - Priority – 2
    - Name – oracle.server.1.from.tcp.5060.to.udp.5060
    - Virtual IP – 10.1.51.205
    - Destination Port – 5060
    - Transport – TCP
    - Scheme – SIP
    - Target Network – oracle.server.1
    - Expression - ANY
    - Leave all other fields as default

SIP Forwarding Policy Table Action

- Change the Forwarding Policy Action for port 5060 Traffic named "oracle.server.1.from.tcp.5060.to.udp.5060" in **SIP Director -> SIP -> Proxy Control -> SIP Forwarding Policies** with these parameters
    - Transport - UDP
    - Leave all other fields as default

Note3 *– Clients that are using SIP TCP 5060 needs to translate client SIP TCP to SIP UDP (oracle.server.2 is listening for SIP 5070 UDP traffic).*

SIP Forwarding Policy Table Classification

- Create Forwarding Policy for port 5070 Traffic named "oracle.server.1.from.tcp.5060.to.udp.5070" in **SIP Director -> SIP -> Proxy Control -> SIP Forwarding Policies** with these parameters
    - Priority – 2
    - Name – oracle.server.1.from.tcp.5060.to.udp.5070
    - Virtual IP – 10.1.51.205
    - Destination Port – 5060
    - Transport – TCP
    - Scheme – SIP
    - Target Network – oracle.server.2
    - Expression - ANY
    - Leave all other fields as default

SIP Forwarding Policy Table Action

- Change the Forwarding Policy Action for port 5060 Traffic named "oracle.server.1.from.tcp.5060.to.udp.5060" in **SIP Director -> SIP -> Proxy Control -> SIP Forwarding Policies** with these parameters
    - Transport – UDP
    - UDP Destination Port - 5070
    - Leave all other fields as default

Configuration Synchronization

This feature enables automatic configuration synchronization between redundant devices.
Main and slave devices require consistent configuration. Configuration synchronization brings the following benefits:

- No need to ensure that the configurations are kept in synchronization, which means tedious error-prone manual process whenever a configuration is changed.
- No need to manually export the slave configuration produced on the main device and import it into the slave device.

This feature provides a mechanism by which the configuration is updated automatically and synchronously on a slave device. This way, the device configurations are guaranteed to be always synchronized, without requiring manual intervention.

This capability operates in a Master/Slave mode where the Master device is the only one that can be configured by the administrator and the Slave device is configured by the Master device only. Automatic configuration synchronization is achieved by providing an online update of the Slave device for all configuration operations performed on the Master device.

- Enable as Master the Configuration Synchronization at **Redundancy -> Configuration Synchronization -> Device Role**
    - Device Role – Master
    - Leave all other fields as default

SIP Director Health Monitoring

- Enable Health Monitoring in **Health Monitoring -> Global Parameters**

- Create a Check for UDP port on server 13.1.13.101 in **Health Monitoring -> Check Table**
    - Check name – Oracle.com.server.1
    - Method – UDP
    - Dest IP – 13.1.13.101
    - Dest Port – 5060

- Create a Check for UDP port on server 13.1.13.102 in **Health Monitoring -> Check Table**
    - Check name – Oracle.com.server.2
    - Method – UDP
    - Dest IP – 13.1.13.102
    - Dest Port – 5070 (Oracle.com.server.2 is listening for SIP on port 5070)

- Bind the UDP 5060 check Oracle.com.server.1 to oracle.communication.farm - 13.1.13.101 - 0 in **Health Monitoring -> Binding Table**

- Bind the UDP 5070 check Oracle.com.server.2 to oracle.communication.farm - 13.1.13.102 - 0 in **Health Monitoring -> Binding Table**

VRRP Configuration

- Enable VRRP in **SIP Director -> Redundancy -> Global Configuration**
    - IP Redundancy Admin Status – VRRP
    - ARP with interface grouping – Send
    - Backup Interface Grouping – Enable
    - Leave all other options as default

- Create Virtual Router interfaces in **SIP Director -> Redundancy -> VRRP -> VR Table**
    - IF Index – 1
    - VR ID – 1
    - Priority – 255 (Highest number is Active device)
    - Primary IP – 10.1.51.1
    - Leave all other options as default

- Create Virtual Router interfaces in **SIP Director -> Redundancy -> VRRP -> VR Table**
    - IF Index – 1
    - VR ID – 2
    - Priority – 255 (Highest number is Active device)
    - Primary IP – 13.1.13.1
    - Leave all other options as default

Create Associated IP Addresses in **SIP Director -> Redundancy -> VRRP -> Associated IP Addresses**

- IF Index – 1, VR ID – 1, Associated IP 10.1.51.1
- IF Index – 1, VR ID – 1, Associated IP 10.1.51.205
- IF Index – 1, VR ID – 1, Associated IP 13.1.13.1

SIP DIRECTOR BACKUP CONFIGURATION

Network Configuration

- Create IP 10.1.51.2/16 on port 1 in **Router -> IP Router -> Interface Parameters** with these parameters,
    - IP Address – 10.1.51.2
    - Network Mask – 255.255.0.0
    - If Number – 1
    - Peer Address – 10.1.51.1 (This IP represent the backup device for Configuration Synchronization)

- Create IP 13.1.13.2/24 on port 1 in **Router -> IP Router -> Interface Parameters** with these parameters,
    - IP Address – 13.1.13.2
    - Network Mask – 255.255.255.0
    - If Number – 1
    - Peer Address – 13.1.13.1 (This IP represent the backup device for Configuration Synchronization)

- Create IP 10.210.6.23/16 (management) on port 1 in **Router -> IP Router -> Interface Parameters** with these parameters,
    - IP Address – 10.210.6.23
    - Network Mask – 255.255.0.0
    - If Number – MNG1
    - Peer Address – 10.210.6.22 (This IP represent the backup device for Configuration Synchronization)

- Create Default Gateway to 10.1.0.1 (management) on port 1 in **Router -> IP Router -> Routing Table** with these parameters,
    - Destination Address – 0.0.0.0
    - Network Mask – 0.0.0.0
    - Next Hop – 10.1.0.1
    - Interface Index – 1

Configuration Synchronization
This feature enables automatic configuration synchronization between redundant devices.
Main and slave devices require consistent configuration. Configuration synchronization brings the following benefits:

- No need to ensure that the configurations are kept in synchronization, which means tedious error-prone manual process whenever a configuration is changed.
- No need to manually export the slave configuration produced on the main device and import it into the slave device.

This feature provides a mechanism by which the configuration is updated automatically and synchronously on a slave device. This way, the device configurations are guaranteed to be always synchronized, without requiring manual intervention.

This capability operates in a Master/Slave mode where the Master device is the only one that can be configured by the administrator and the Slave device is configured by the Master device only. Automatic configuration synchronization is achieved by providing an online update of the Slave device for all configuration operations performed on the Master device.

- Enable as Backup the Configuration Synchronization at **Redundancy -> Configuration Synchronization -> Device Role**
    - Device Role – Backup
    - Leave all other fields as default

ORACLE COMMUNICATION SERVICE SERVER-1

- Create IP 13.1.13.101/24 on network interface
- Create Default GW to 13.1.13.1/24
- Configure the server with outbound proxy of the VIP (10.1.51.205) please refer to this page for more information http://download.oracle.com/docs/cd/E13209_01/wlcp/wlss31/configref/enginetier_dd.html

ORACLE COMMUNICATION SERVICE SERVER -2

- Create IP 13.1.13.102/24 on network interface
- Create Default GW to 13.1.13.1/24
- Configure the server with outbound proxy of the VIP (10.1.51.205) please refer to this page for more information http://download.oracle.com/docs/cd/E13209_01/wlcp/wlss31/configref/enginetier_dd.html

Technical Support

Radware offers technical support for all of its products through the Radware Certainty Support Program. Please refer to your Certainty Support contract, or the Radware Certainty Support Guide available at:
http://www.radware.com/content/support/supportprogram/default.asp

For more information, please contact your Radware Sales representative or:
U.S. and Americas: (866) 234-5763
International: +972(3) 766-8666