TESTING & INTEGRATION GROUP

TECHNICAL SOLUTION GUIDE

Radware AppDirector Load Balancing Microsoft LCS servers, LCS Director and LCS Access Proxy Servers.

TECHNICAL SOLUTION GUIDE
DATE: Tuesday, January 17, 2006
Version: 1.0

Author – Elad Kurzweil

Introduction

Communication within an organization is the dominant variable contributing to its effectiveness and success.

Modern communication involves E-mail, phone, messaging and video conferencing. Enterprises are looking for new technology that will allow them to reduce the communication equipment on the employee station, and will also allow a user to easily access the same communication channels while traveling. These communication solutions often require additional hardware (phone switch, for example) which comes at added costs, in consequence providing a more expensive solution. Moreover, these are not real time solutions and in many cases may cause delays and damage at instances in which critical information must be transferred immediately.

Microsoft's LCS (Live Communication Sever) 2005 enhances the communication within an organization and provides the ultimate solution for organizations looking to attain maximum efficiency from its employee's performance and from the organization as a whole.
Instant Messaging (IM) and other real time communication features such as peer-to-peer audio and video can now be utilized as the main channel of communication within an organization, resulting in a significant save in both time and money.
Employees can now connect with their colleagues, partners and suppliers in real time, share important and imperative information, while using built in security measures to safeguard the transferred information.
LCS 2005 can be easily utilized by any organization, as it does not require a sophisticated and expensive infrastructure. Un-complex and inexpensive hardware can be used to build a server farm so costs can stay at a minimum.

To achieve the utmost performance out of Microsoft's LCS 2005, an organization utilizing such solution, should be able to over come other difficulties, which are in many cases a side product of applications requiring server farms, such as scalability, over loading and crashes.
Radware's AppDirector ensures that the traffic created by the use of LCS 2005 is managed correctly and all servers are utilized efficiently therefore handling Load balancing, reducing failures at any end point and allowing for greater scalability.
AppDirector eliminates bottlenecks, failures and downtime from enterprise servers while constantly protecting data traffic from security violations as well. Therefore,
When using Radware's AppDirector, organizations promise to deliver not only an optimized solution but also a reliable and a secured one as well.

With Microsoft's LCS 2005 solution, organizations can now improve their internal and external means of communication and achieve greater effectiveness simply by having the ability to transfer data in real time while utilizing a low maintenance server farm to support the required applications.
Moreover, Radware’s AppDirector ensures the maximum utilization of the servers, economical operation and flawless scaling of the applications, consequently granting full availability and optimized accelerated performance.

Radware AppDirector

Radware AppDirector is an intelligent application delivery controller for the data center that provides scalability and application-level security for IT infrastructure optimization, fault tolerance and redundancy.

AppDirector combines the power of Radware's Multi-Gigabit Application Switching hardware with APSolute OS Application-Smart Networking to ensure local and global server availability, accelerated application performance and safeguard applications with integrated intrusion prevention and denial of service protection for fast, reliable, secure application delivery.

AppDirector uses advanced Layer 4-7 policies and granular application intelligence for end-to-end application-smart networking, aligning server infrastructure operations with application front end requirements to eliminate traffic surges, server bottlenecks, connectivity disconnects and downtime for assured application access, full application continuity and redundancy. AppDirector enables fine tuning of network behavior at all critical points, end-to-end, based on granular application-specific classification of packets to optimize traffic flows for a wide range of enterprise applications such as SAP, Oracle, BEA, Citrix, and other web-based applications including support for VoIP, streaming media, and secure LDAP applications.

With AppDirector's fully integrated intrusion prevention and Denial of Service protection data center applications and server resources are insulated against application level attacks. The ability to control multi-step SSL processing provides enhanced security of HTTP, FTP, SMTP and SIP over SSL.

AppDirector lets you get the most out of your IT investments by maximizing the utilization of server infrastructure resources and enabling seamless consolidation and high scalability. Make your network adaptive and more responsive to your dynamic application and business needs with AppDirector's fully integrated traffic classification and flow management, health monitoring and failure bypassing, traffic redirection, bandwidth management, intrusion prevention and DoS protection.

For more information, please visit: **http://www.radware.com**

Microsoft Live Communication server 2005 (LCS)

Microsoft® Office Live Communications Server 2005 (Live Communications Server 2005) provides a powerful, scalable, enterprise-grade IM (instant messaging) and integrated presence solution. IM is the ability to transfer text messages in real time over an Internet Protocol (IP) network such as the Internet or a corporate network. Presence awareness is the ability to detect another user's availability on one or more devices. Live Communications Server also supports peer-to-peer audio, video, application-sharing and data collaboration, instantly accelerating the workflow of today's information workers. Live Communications Server 2005 improves business efficiencies across organizational boundaries by extending IM and other real-time communication capabilities to trusted partners, customers and suppliers and, with the addition of Public IM Connectivity, also extending to users of the public IM service providers Microsoft Network (MSN®), America Online (AOL®) and Yahoo!®.

For more information, please visit: **http://www.microsoft.com/office/livecomm**

Solution Details

The document presents an organization that wants to have secure internal corporate communication between the company employees.
The setup is built with 2x LCS servers, 2x LCS Directors and 2x Access proxy servers. Radware AppDirector will load balance 3x clusters the LCS, Director and Proxy clusters. This will give the organization fail over solution and better traffic flow.

Important Notes:

- Port 5061 TCP/UDP should be allowed on the Firewall on both directions

- Instant messaging can flow in between internal network users and external network users. VoIP and Video conferencing between the Internal and External users **won't be available** because of SIP NAT problem.
- If there is a need to use VoIP and Video conferencing between the External and Internal clients the customer need to use 3rd party device that can bypass the SIP NAT problem like Ingate SIParators http://directory.partners.extranet.microsoft.com/redirecter.aspx?cat=0&sid=2942&pid=4540&fileid=4572&url=/collateral/2942/Release your full potential with Live Communications Server_en-F.pps.
- VoIP, Video conferencing and massaging between external clients will work fine. VoIP, Video conferencing and massaging between internal clients will work fine.

- When one of the LCS servers fails to operate, the internal client that was connected to the failed server will have to wait 2-3 minutes for automatic new client registration, or manually unregister and register again for immediate client connection. New clients can connect automatically to the available server through the AppDirector. When one of the Proxy or LCS servers fail, the external client that was connected to the failed server will have to wait 5-6 minutes for automatic new client registration, or to unregister and register again for immediate client connection. New clients can connect automatically to the available server through the AppDirector. There is a way to adjust that aging time on the Server side. Please refer to Microsoft technical support to get the technical configuration details.

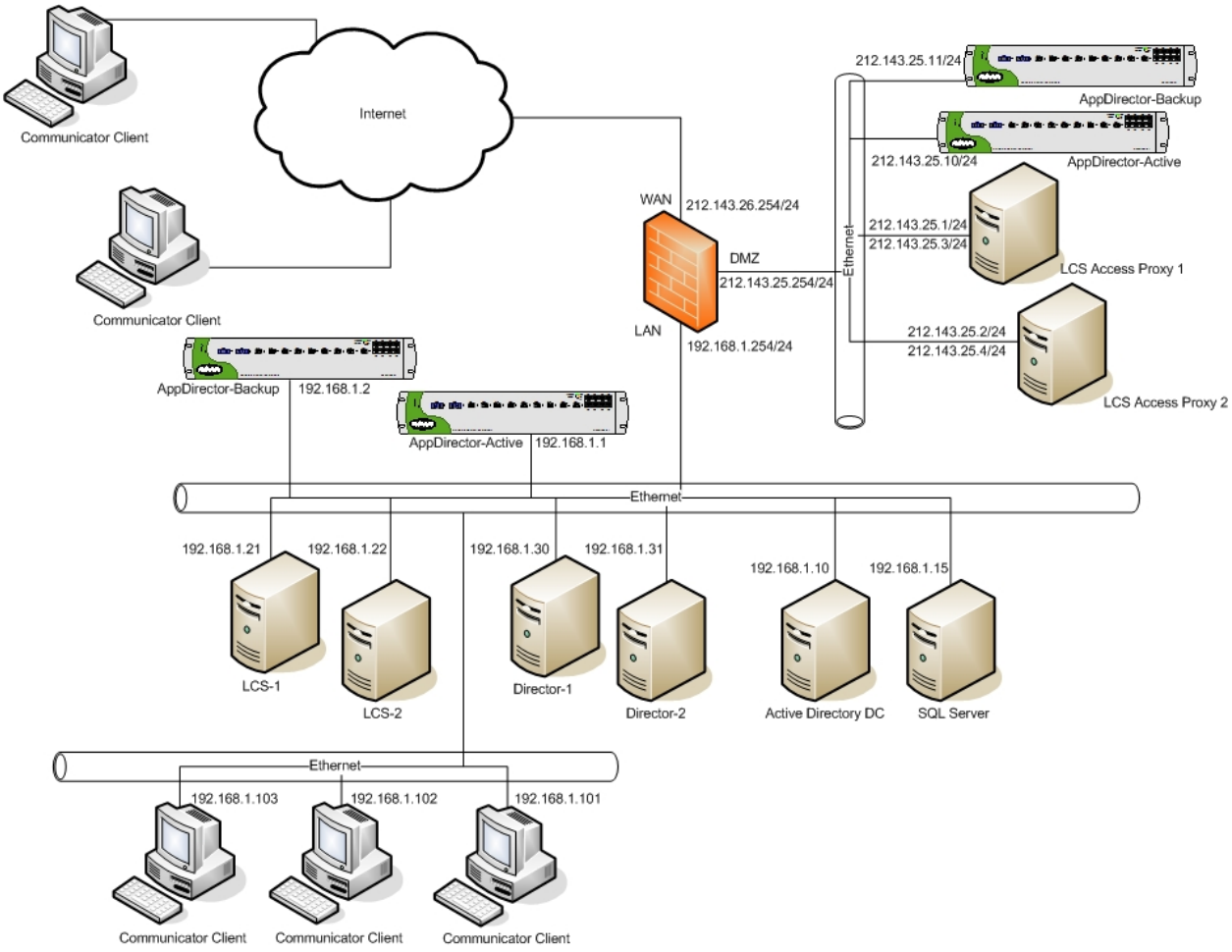
- This document assumes that the customer installed all Microsoft components to operate the LCS integration.

Software and Hardware

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

Microsoft LCS 2005 Enterprise Edition
Microsoft LCS 2005 Standard Edition (for Director)
Microsoft SQL Server 2000 with SP4
Microsoft Windows 2003 Enterprise Edition with AD
Microsoft Communicator
Radware's AppDirector v.1.00.01 Build Jan 23 2006, 12:00:25

Tested network overview



Network Diagram

Configuration

RADWARE APPDIRECTOR INTERNAL - ACTIVE

1. Create IP 192.168.1.1/24 on port 1

2. Create Default GW to 192.168.1.254

3. **Farm Configuration:**
   a. Create Farm called **LCS.FARM** in **AppDirector -> Farms ->Farm Table ->** with these parameters,
      i. IP Address – 192.168.1.200
      ii. Farm Name – **LCS.FARM**
      iii. Aging Time – 600 Sec.
      iv. Session mode - ServerPerSession
      v. Dispatch Method – Cyclic
      vi. Leave all other fields as default

   b. Create Farm called **Director.FARM** in **AppDirector -> Farms -> Farm Table ->** with these parameters,
      i. IP Address – 192.168.1.205
      ii. Farm Name – **Director.FARM**
      iii. Aging Time – 600 Sec.
      iv. Session mode - ServerPerSession
      v. Dispatch Method – Cyclic
      vi. Leave all other fields as default

4. **Farm Additional Parameters:**
   a. Enable the Client NAT to the FARM 192.168.1.200 in **AppDirector -> Farms –> Additional Parameters** with these parameters:
      i. Client NAT address – 192.168.1.210
      ii. Leave all other fields as default

   b. Enable the Client NAT to the FARM 192.168.1.205 in **AppDirector -> Farms –> Additional Parameters** with these parameters:
      i. Client NAT address – 192.168.1.210
      ii. Leave all other fields as default

5. **Server Configuration:**

   a. Add Server 192.168.1.21 (LCS Server) to Farm **192.168.1.200** (LCS.Farm) called **LCS.Server.1** in **AppDirector -> Servers -> Application Servers** with these parameters,
      i. Farm Address – 192.168.1.200
      ii. Server Address – 192.168.1.21
      iii. Server Name – **LCS.Server.1**
      iv. Client NAT - Enable
      v. Leave all other fields as default

b. Add Server 192.168.1.22 (LCS Server) to Farm **192.168.1.200** (LCS.Farm) called **LCS.Server.2** in **AppDirector -> Servers -> Application Servers** with these parameters,
   i. Farm Address – 192.168.1.200
   ii. Server Address – 192.168.1.22
   iii. Server Name – **LCS.Server.2**
   iv. Client NAT - Enable
   v. Leave all other fields as default

c. Add Server 192.168.1.30 (Director Server) to Farm **192.168.1.205** (Director.Farm) called **Director.Server.1** in **AppDirector -> Servers -> Application Servers** with these parameters,
   i. Farm Address – 192.168.1.205
   ii. Server Address – 192.168.1.30
   iii. Server Name – **Director.Server.1**
   iv. Client NAT - Enable
   v. Leave all other fields as default

d. Add Server 192.168.1.31 (Director Server) to Farm **192.168.1.205** (Director.Farm) called **Director.Server.2** in **AppDirector -> Servers -> Application Servers** with these parameters,
   i. Farm Address – 192.168.1.205
   ii. Server Address – 192.168.1.31
   iii. Server Name – **Director.Server.2**
   iv. Client NAT - Enable
   v. Leave all other fields as default

6. **Client NAT Configuration**

a. By default the NAT is disabled and the there is no memory allocation for the NAT addresses. To enable the Client NAT Addresses memory range please go to **Services -> Tuning -> Device** and change the Client NAT Addresses from 0 to 1 (this means that the AppDirector will use only 1 Client NAT Address) press apply and reboot the device.

b. Enable Client NAT in **AppDirector -> NAT -> Client NAT -> Global Parameters**

c. **Create Client NAT address configuration in AppDirector -> NAT -> Client NAT -> NAT Addresses with these parameters**
   i. From IP Address – 192.168.1.210
   ii. To IP Address – 192.168.1.210

d. **Create Client NAT intercept range in AppDirector -> NAT -> Client NAT -> Intercept addresses** with these parameters
   i. From Client IP – 0.0.0.0
   ii. To Client IP – 255.255.255.255

Health Monitoring

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

- Create a Check for SIP TLS port 5061 on server 192.168.1.21 in **Health Monitoring -> Check Table**
  - Check name – LCS1.SIP.Check
  - Method – TCP Port
  - Dest IP – 192.168.1.21
  - Dest Port – 5061
  - Leave all other fields as default

- Create a Check for SIP TLS port 5061 on server 192.168.1.22 in **Health Monitoring -> Check Table**
  - Check name – LCS2.SIP.Check
  - Method – TCP Port
  - Dest IP – 192.168.1.22
  - Dest Port – 5061
  - Leave all other fields as default

- Create a Check for SIP TLS port 5061 on server 192.168.1.30 in **Health Monitoring -> Check Table**
  - Check name – Director1.Check
  - Method – TCP Port
  - Dest IP – 192.168.1.30
  - Dest Port – 5061
  - Leave all other fields as default

- Create a Check for SIP TLS port 5061 on server 192.168.1.31 in **Health Monitoring -> Check Table**
  - Check name – Director2.Check
  - Method – TCP Port
  - Dest IP – 192.168.1.31
  - Dest Port – 5061
  - Leave all other fields as default

- Bind the SSL check LCS1.SIP.Check to Server 192.168.1.21 in **Health Monitoring -> Binding Table**
- Bind the SSL check LCS2.SIP.Check to Server 192.168.1.22 in **Health Monitoring -> Binding Table**
- Bind the SSL check Director1.Check to Server 192.168.1.30 in **Health Monitoring -> Binding Table**
- Bind the SSL check Director2.Check to Server 192.168.1.31 in **Health Monitoring -> Binding Table**

7. **VRRP Configuration**

    a. Enable VRRP in **AppDirector -> Redundancy -> Global Configuration**
        i. IP Redundancy Admin Status – VRRP
        ii. Interface Grouping – Enable
        iii. ARP with interface grouping – Send
        iv. VLAN Redundancy – Active
        v. Backup Fake ARP – Enable
        vi. Backup Interface Grouping – Enable

    b. Create Virtual Router interfaces in **AppDirector -> Redundancy -> VRRP -> VR Table**
        i. IF Index – 1
        ii. VR ID – 1
        iii. Priority – 255 (Highest number is Active device)
        iv. Primary IP – 192.168.1.1
        v. Leave all other options as default

    c. Create Associated IP Addresses in **AppDirector -> Redundancy -> VRRP -> Associated IP Addresses**
        i. IF Index – 1, VR ID – 1, Associated IP 192.168.1.1
        ii. IF Index – 1, VR ID – 1, Associated IP 192.168.1.200
        iii. IF Index – 1, VR ID – 1, Associated IP 192.168.1.205
        iv. IF Index – 1, VR ID – 1, Associated IP 192.168.1.210

8. **Client Table Mirroring**

    a. Enable Mirroring in **AppDirector -> Redundancy -> Mirroring -> Active Device Parameters**
        i. Client Table Mirroring – Enable
        ii. Client Mirror update time – 3
        iii. Leave all other options as default
        iv. Reboot the device

RADWARE APPDIRECTOR INTERNAL - BACKUP

1. Create IP 192.168.1.1/24 on port 1
2. Create Default GW to 192.168.1.254
3. Copy all configuration from the Active AppDirector device

4. **VRRP Configuration**

    b. Enable VRRP in **AppDirector -> Redundancy -> Global Configuration**
        i. IP Redundancy Admin Status – VRRP
        ii. Interface Grouping – Enable
        iii. ARP with interface grouping – Send
        iv. VLAN Redundancy – Active
        v. Backup Fake ARP – Enable
        vi. Backup Interface Grouping – Enable

    c. Create Virtual Router interfaces in **AppDirector -> Redundancy -> VRRP -> VR Table**
        i. IF Index – 1
        ii. VR ID – 1
        iii. Priority – 100 (Highest number is Active device)
        iv. Primary IP – 192.168.1.1
        v. Leave all other options as default

    d. Create Associated IP Addresses in **AppDirector -> Redundancy -> VRRP -> Associated IP Addresses**
        i. IF Index – 1, VR ID – 1, Associated IP 192.168.1.1
        ii. IF Index – 1, VR ID – 1, Associated IP 192.168.1.200
        iii. IF Index – 1, VR ID – 1, Associated IP 192.168.1.205
        iv. IF Index – 1, VR ID – 1, Associated IP 192.168.1.210
        v.

1. **Client Table Mirroring**

    e. Enable Mirroring in **AppDirector -> Redundancy -> Mirroring -> Backup Device Parameters**
        i. Mirroring Status – Enable
        ii. Active Device IP – 192.168.1.1
        iii. Reboot the device

RADWARE APPDIRECTOR EXTERNAL - ACTIVE

1. Create IP 212.143.25.10/24 on port 1

2. Create Default GW to 212.143.25.254

3. **Farm Configuration:**
   f. Create Farm called **Proxy.External.Farm** in **AppDirector -> Farms ->Farm Table ->** with these parameters,
      i. IP Address – 212.143.25.200
      ii. Farm Name – **Proxy.External.Farm**
      iii. Aging Time – 600 Sec.
      iv. Session mode - ServerPerSession
      v. Dispatch Method – Cyclic
      vi. Leave all other fields as default

   g. Create Farm called **Proxy.Internal.Farm** in **AppDirector -> Farms -> Farm Table ->** with these parameters,
      i. IP Address – 212.143.25.201
      ii. Farm Name – **Director.FARM**
      iii. Aging Time – 600 Sec.
      iv. Session mode - ServerPerSession
      v. Dispatch Method – Cyclic
      vi. Leave all other fields as default

4. **Server Configuration:**

   h. Add Server 212.143.25.2 (Proxy External leg Server) to Farm 212.143.25.200 (**Proxy.External.Farm**) called **Ext.Proxy.Server.1** in **AppDirector -> Servers -> Application Servers** with these parameters,
      i. Farm Address – 212.143.25.200
      ii. Server Address – 212.143.25.2
      iii. Server Name – **Ext.Proxy.Server.1**
      iv. Leave all other fields as default

   i. Add Server 212.143.25.4 (Proxy External leg Server) to Farm 212.143.25.200 (**Proxy.External.Farm**) called **Ext.Proxy.Server.2** in **AppDirector -> Servers -> Application Servers** with these parameters,
      i. Farm Address – 212.143.25.200
      ii. Server Address – 212.143.25.4
      iii. Server Name – **Ext.Proxy.Server.2**
      iv. Leave all other fields as default

j. Add Server 212.143.25.1 (Proxy Internal leg Server) to Farm 212.143.25.201 (**Proxy.Internal.Farm**) called **Int.Proxy.Server.1** in **AppDirector -> Servers -> Application Servers** with these parameters,
   i. Farm Address – 212.143.25.201
   ii. Server Address – 212.143.25.1
   iii. Server Name – **Int.Proxy.Server.1**
   iv. Leave all other fields as default

k. Add Server 212.143.25.3 (Proxy Internal leg Server) to Farm 212.143.25.201 (**Proxy.Internal.Farm**) called **Int.Proxy.Server.2** in **AppDirector -> Servers -> Application Servers** with these parameters,
   i. Farm Address – 212.143.25.201
   ii. Server Address – 212.143.25.3
   iii. Server Name – **Int.Proxy.Server.2**
   iv. Leave all other fields as default

Health Monitoring

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

- Create a Check for SIP TLS port 5061 on server 212.143.25.2 in **Health Monitoring -> Check Table**
  - Check name – **Ext.Proxy.Server.1.Check**
  - Method – TCP Port
  - Dest IP – 212.143.25.2
  - Dest Port – 5061
  - Leave all other fields as default

- Create a Check for SIP TLS port 5061 on server 212.143.25.4 in **Health Monitoring -> Check Table**
  - Check name – **Ext.Proxy.Server.2.Check**
  - Method – TCP Port
  - Dest IP – 1212.143.25.4
  - Dest Port – 5061
  - Leave all other fields as default

- Create a Check for SIP TLS port 5061 on server 212.143.25.1 in **Health Monitoring -> Check Table**
  - Check name – **Int.Proxy.Server.1.Check**
  - Method – TCP Port
  - Dest IP – 1212.143.25.1
  - Dest Port – 5061
  - Leave all other fields as default

- Create a Check for SIP TLS port 5061 on server 212.143.25.3 in **Health Monitoring -> Check Table**
  - Check name – **Int.Proxy.Server.2.Check**
  - Method – TCP Port
  - Dest IP – 1212.143.25.3
  - Dest Port – 5061
  - Leave all other fields as default

- Bind the SSL check **Ext.Proxy.Server.1.Check** to Server 212.143.25.2 in **Health Monitoring -> Binding Table**
- Bind the SSL check L **Ext.Proxy.Server.2.Check** to Server 212.143.25.4 in **Health Monitoring -> Binding Table**
- Bind the SSL check **Int.Proxy.Server.1.Check** to Server 212.143.25.1 in **Health Monitoring -> Binding Table**
- Bind the SSL check **Int.Proxy.Server.1.Check** to Server 212.143.25.3 in **Health Monitoring -> Binding Table**

5. **VRRP Configuration**

    l. Enable VRRP in **AppDirector -> Redundancy -> Global Configuration**
        i. IP Redundancy Admin Status – VRRP
        ii. Interface Grouping – Enable
        iii. ARP with interface grouping – Send
        iv. VLAN Redundancy – Active
        v. Backup Fake ARP – Enable
        vi. Backup Interface Grouping – Enable

    m. Create Virtual Router interfaces in **AppDirector -> Redundancy -> VRRP -> VR Table**
        i. IF Index – 1
        ii. VR ID – 1
        iii. Priority – 255 (Highest number is Active device)
        iv. Primary IP – 212.143.25.10
        v. Leave all other options as default

    n. Create Associated IP Addresses in **AppDirector -> Redundancy -> VRRP -> Associated IP Addresses**
        i. IF Index – 1, VR ID – 1, Associated IP 212.143.25.10
        ii. IF Index – 1, VR ID – 1, Associated IP 212.143.25.200
        iii. IF Index – 1, VR ID – 1, Associated IP 212.143.25.201

6. **Client Table Mirroring**

    a. Enable Mirroring in **AppDirector -> Redundancy -> Mirroring -> Active Device Parameters**
        i. Client Table Mirroring – Enable
        ii. Client Mirror update time – 3
        iii. Leave all other options as default
        iv. Reboot the device

RADWARE APPDIRECTOR EXTERNAL - BACKUP

1. Create IP 212.143.25.11/24 on port 1
2. Create Default GW to 212.143.25.254
3. Copy all configuration from the Active AppDirector device
4. **VRRP Configuration**

    b. Enable VRRP in **AppDirector -> Redundancy -> Global Configuration**
        i. IP Redundancy Admin Status – VRRP
        ii. Interface Grouping – Enable
        iii. ARP with interface grouping – Send
        iv. VLAN Redundancy – Active
        v. Backup Fake ARP – Enable
        vi. Backup Interface Grouping – Enable

    c. Create Virtual Router interfaces in **AppDirector -> Redundancy -> VRRP -> VR Table**
        i. IF Index – 1
        ii. VR ID – 1
        iii. Priority – 100 (Highest number is Active device)
        iv. Primary IP – 212.143.25.10
        v. Leave all other options as default

    d. Create Associated IP Addresses in **AppDirector -> Redundancy -> VRRP -> Associated IP Addresses**
        i. IF Index – 1, VR ID – 1, Associated IP 212.143.25.10
        ii. IF Index – 1, VR ID – 1, Associated IP 212.143.25.200
        iii. IF Index – 1, VR ID – 1, Associated IP 212.143.25.201

5. **Client Table Mirroring**

    e. Enable Mirroring in **AppDirector -> Redundancy -> Mirroring -> Backup Device Parameters**
        i. Mirroring Status – Enable
        ii. Active Device IP – 212.143.25.10
        iii. Reboot the device

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