APPLICATION DELIVERY

Solution Guide: Load Balancing with the Brocade ServerIron Platform

Brocade ServerIron switches, when deployed in front of the Microsoft Office Communications Server 2007, increase application uptime, maximize server farm utilization, and shield the servers and applications from malicious attacks.

BROCADE

CONTENTS

Unified Communications Application Delivery 3
Deployment Architecture 5
General Requirements 7
Further Design Considerations for OCS solution 8
High Availability 8
Security 8
ServerIron Configuration 9
Appendix A: High Availability and Redundancy 12
To Set Up Hot-Standby Redundancy 12
Optionally, Set Up Active-Standby Redundancy 13
Optionally, Set Up Active-Active Redundancy 13
Appendix B: Running Configuration 14
Appendix C: Microsoft Office Communication Server 2007 17
Appendix D: Brocade ServerIron 18
Application Performance 18
Application Availability 18
Application and Server Farm Security 19
Application and Server Farm Scalability 19
Higher Return on Investment (ROI) 19

UNIFIED COMMUNICATIONS APPLICATION DELIVERY

Microsoft unified communications technologies use the power of software to deliver complete communications-, including messaging, voice, and video, across the applications and devices that people use every day. Integrating the experiences associated with the telephone---phone calls, voice-mail, and conferencing---into the work done on a computer---documents, spreadsheets, instant messaging, e-mail, and calendars---has the power to fundamentally change the way the world works.

Microsoft® Office Communications Server 2007 is the first Microsoft product to combine enterprise-ready Instant Messaging (IM), presence, conferencing, and Voice over IP (VoIP) telephony in a fully integrated unified communications solution. Office Communications Server 2007 provides richer presence capabilities, enhanced support for group IM, and improved deployment and management than its predecessor, Microsoft Office Live Communications Server 2005 SP1. To existing features, such as federation and public IM connectivity, Office Communications Server 2007 includes real-time conferencing hosted on servers inside the organization's firewall and a full-featured, software-powered VoIP solution, which can stand on its own or integrate easily with an existing private bank exchange (PBX) infrastructure.

Office Communications Server 2007 extends the architecture of Live Communications Server 2005 to include components that support VoIP and conferencing. The key architectural features include:

- Pool configurations
- Front-end servers
- Conferencing components
- VoIP components
- Perimeter network configuration and components
- Conference protocols
- Conference call flow

For more details on the Microsoft Office Communication Server 2007, see Appendix C.
For technical overview and deployment and implementation details, visit:
http://www.microsoft.com/uc/products/ocs2007.mspx

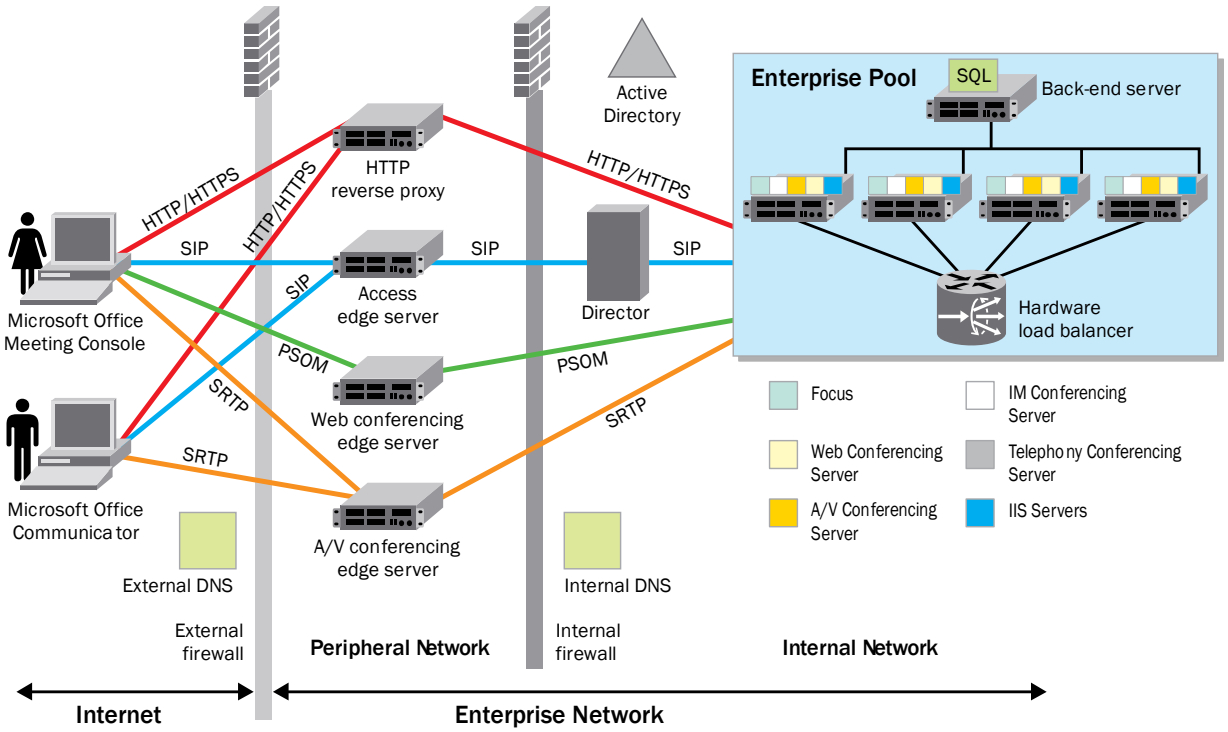

Figure 1. Reference architecture

Brocade ServerIron switches, when deployed in front of the Microsoft Office Communications Server 2007, increase application uptime, maximize server farm utilization, and shield the servers and applications from malicious attacks. The switches receive all client requests and distribute them efficiently to the "best" server among the available pool. ServerIron switches consider server availability, load, response time, and other user-configured performance metrics when selecting a server for incoming client connections. By performing sophisticated and customizable "health checks" to the servers and the Microsoft Office Communications Server 2007, the ServerIron switches quickly identify resource outages in real time and redirect client connections to other available servers. Server capacity can be increased or decreased on demand without impacting the applications and client connections. When demand grows, IT engineers can simply "slide" in new server resources and configure the ServerIron switch to use the new servers for client connections

ServerIron switches are application aware and can inspect many types of application-level content to perform intelligent switching of client requests to appropriate servers. Application switching eliminates the need to replicate content and application functions on all servers and optimizes overall resource utilization, application performance, and availability.

ServerIron switches support switching based on broad content types including URL, HTTP headers, HTTP cookies, SSL session IDs, and XML tags. For implementations in which session persistence across multiple TCP ports on the same server is a key requirement, the ServerIron switches offer support for the industry's most advanced and easily customizable load balancing interface.

In addition, the power of performance delivered by ServerIron switches ensures that the applications provide the best end-user response time and immense scalability even when enabled for Layer 4 through 7 switching. Using sticky sessions and track-group switching, a group of transactions from a given client are sent to the server originally selected and has the session created when the client first connected. A crucial benefit of using Brocade ServerIron is its ability to ensure the client stays with one real server so that all real-time information is preserved as the client continues to communicate across several application ports.

Another benefit of using the Brocade ServerIron to load balance is its ability to protect server farms and applications from malicious attacks. The ServerIron switches are proven to defeat wire-speed Gigabit-rate Denial of Service (DoS) attacks while maintaining peak application performance. Brocade switches also provide high-performance content inspection and filtering for malicious content, including viruses and worms, which are spread through application-level messages to cripple the servers and take down applications.

Brocade ServerIron solutions provide immediate Return on Investment (ROI), and also improves the ROI of Microsoft Office Communications Server 2007. They support significantly higher application traffic and number of users on existing server resources by maximizing utilization. On-demand and unlimited virtual server farm scalability eliminates the need for forklift upgrades and dramatically improves the ROI on the server infrastructure. Downtime associated with security breaches and scheduled maintenance is eliminated, resulting in improved availability, which in turn results in savings of tens of thousands to millions of dollars a year.

Load balancing technology has become a technology of choice to improve the scalability, availability and security of IP applications. Brocade ServerIron switches, with their networking and application intelligence, provide rich features and high performance required for building massively scalable and highly secure application infrastructure.

Deployment Architecture

An Office Communications Server 2007 pool consists of one or more front-end servers that provide IM, presence, and conferencing services and are connected to a SQL Server database for storing user and conference information. Depending on the pool configuration, the database might reside on the same server. In addition, certain conferencing components might be deployed on the same physical computer, depending on the chosen pool configuration. Office Communications Server 2007 offers three pool configurations: one Standard Edition configuration and the consolidated and expanded Enterprise Edition configurations. Both Enterprise Edition configurations consist of identical front-end servers that are connected to a separate dedicated Microsoft SQL Server 2005 back-end database. (In an Enterprise pool, the back-end database must be on a dedicated computer, separate from all Enterprise Edition servers.)

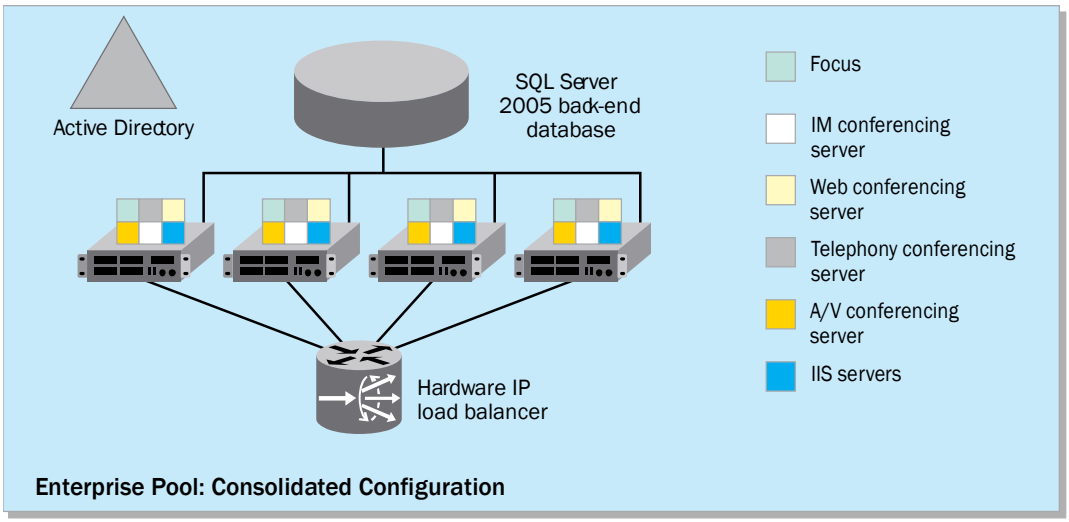

Figure 2. Consolidated configuration

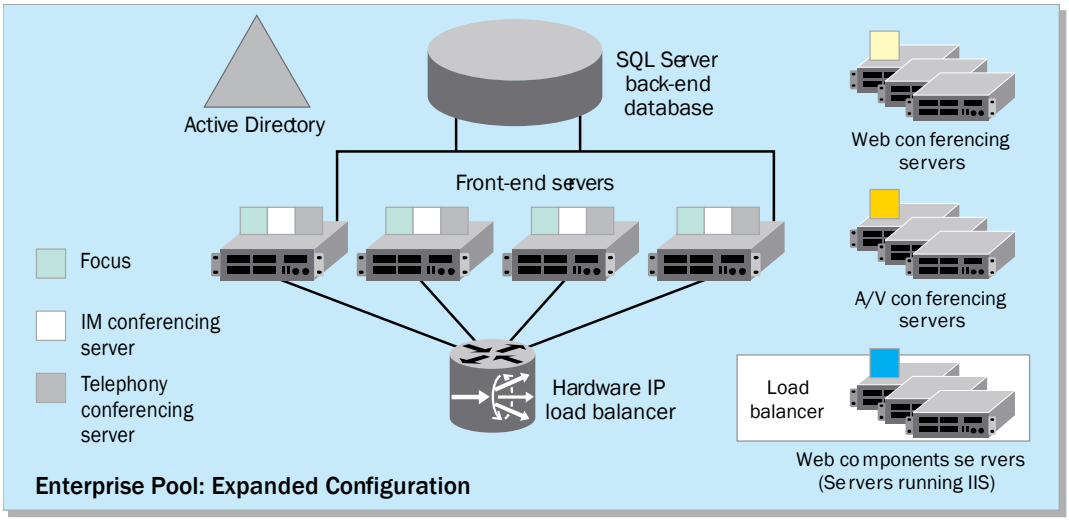

Figure 3. Expanded configuration

Also the access edge servers, HTTP reverse proxy and A/V edge server can be load balanced in the perimeter network. In addition, the Communicator Web Access and Director can be deployed on multiple servers which are load balanced. The scenario is shown in Figure 4.

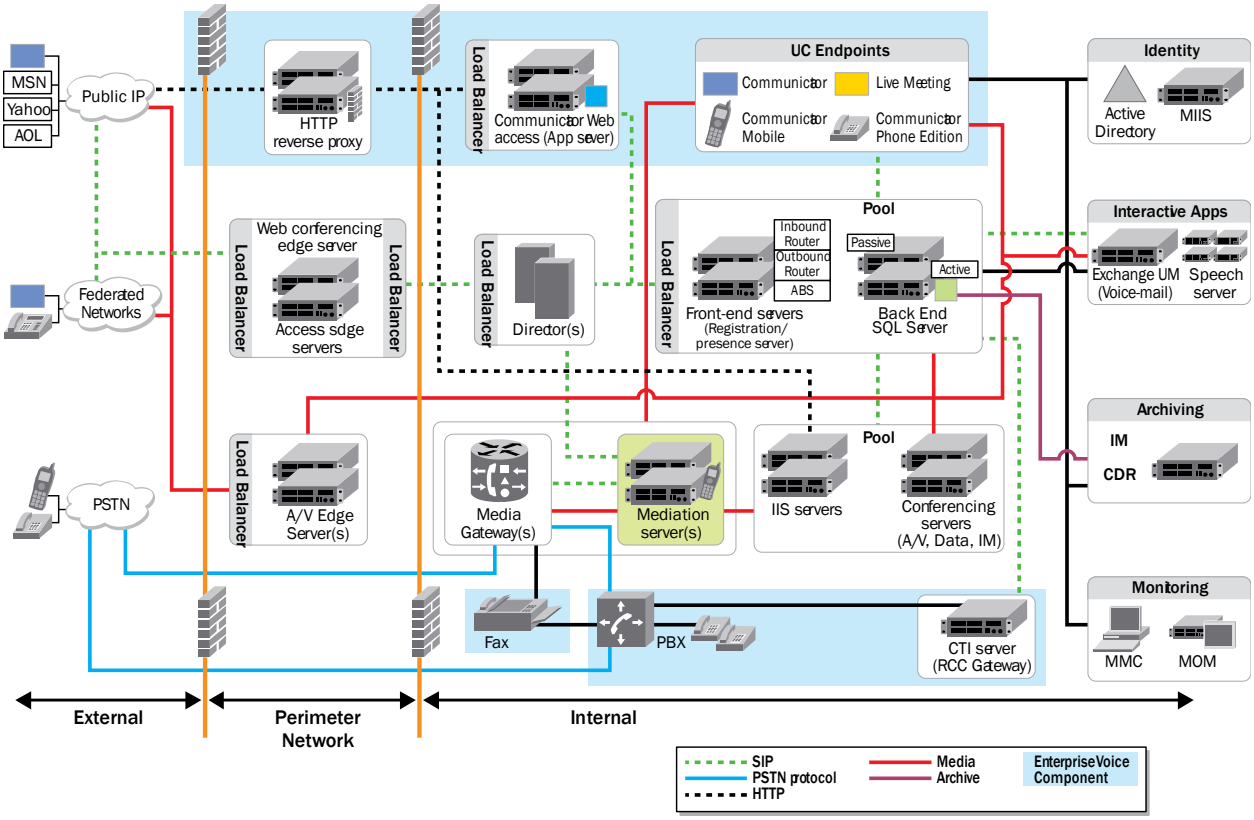

Figure 4. Load balancing on multiple servers

General Requirements

A front-end server requires a hardware load balancer. If you are deploying a Standard Edition Server or a single Enterprise Edition Front End Server, a load balancer is not required. A hardware load balancer is also required for arrays of Office Communications Server 2007 Edge Servers or an array of Standard Edition Servers configured as a Director. These requirements are summarized in the Table 1.

Table 1. Microsoft recommended hardware load balancer requirements for OCS 2007

Deployment	Load Balancer Requirement
A single Standard Edition Server	Load balancer not required
Enterprise pool with multiple front-end servers	Hardware load balancer required
Array of directors	Hardware load balancer required
Array of edge servers	Hardware load balancer required

Table 2. Hardware load balancer ports required for office Communications Server 2007

Port Required	Virtual IP	Port Use
5060	Load balancer VIP used by front-end servers	Client-to-server SIP communication over TCP
5061	Load balancer VIP used by front-end servers	Client-to-front-end server SIP communication over TLS SIP communication between the front-end servers over MTLS
135	Load balancer VIP used by front-end servers	To move users and perform other pool-level WMI operations over DCOM
444	Load balancer VIP used by front-end servers	Communication between the internal components that manage conferencing and the conferencing servers
443	Load balancer VIP used by the Web components server	HTTPS traffic to the pool URLs

The configurations provided in this document are configured for use to load balance groups of servers whether they are EE pools, access groups, or Director Servers. The provided configuration is provided for a one-arm configuration where the servers are not directly connected to the ServerIron (which requires source-nat to ensure return communication returns through the ServerIron).

FURTHER DESIGN CONSIDERATIONS FOR OCS SOLUTION

High Availability

Attached in the Appendix is a section on Redundancy and how to enable this on the ServerIrons to ensure if one ServerIron goes down another ServerIron takes over while the other has failed and is transparent to the users. Both ServerIron switches share a common MAC address known to the clients. Therefore, if a failover occurs, the clients still know the ServerIron by the same MAC address. The active sessions running on the clients continue and the clients and routers do not need to re-ARP for the ServerIron MAC address.

Security

The built-in DoS Protection (when enabled with the "ip tcp syn-proxy command) identifies and blocks Denial of Service attacks, protecting the network from service failures and downtime. As a TCP SYN request comes in a TCP SYN/ACK is returned with a special SEQ number. If a TCP ACK is not returned or if it is incorrect the session is never even add to the session table thereby never wasting any resources unless a ServerIron IPv6 Network, Management, and Application Switching Support proper response is returned. If the proper TCP ACK is returned with a proper SEQ number a connection is establish and the entry is written to the session table,

This method of SYN protection all Brocade to allow the highest level of DOS protection in the industry by mitigating attacks of over 2.5 million SYNs per second, which is the equivalent of thwarting a real time 1GB line attack in real time while completely unaffecting legitimate traffic flows and user connections. Appendix D provides more details about the Brocade ServerIron.

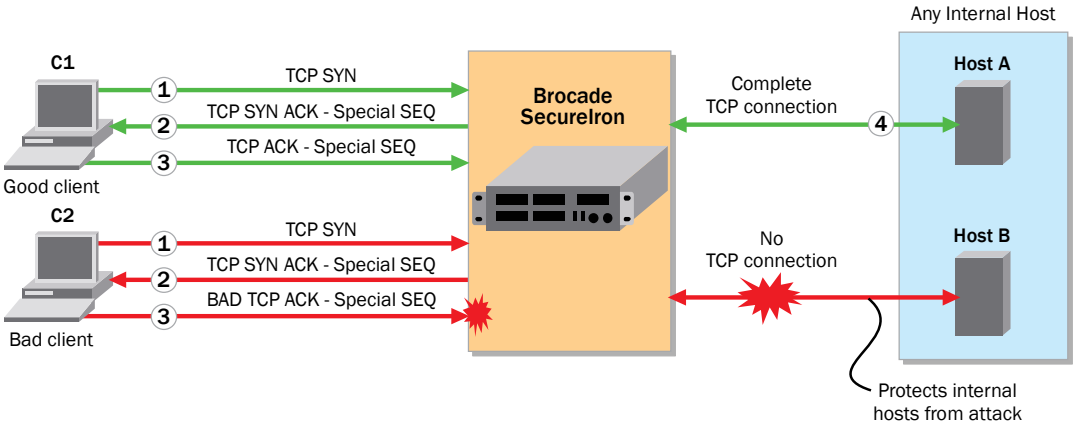

Figure 5. Brocade security solution

SERVERIRON CONFIGURATION

This configuration is a basic switch configuration for the ServerIron that will work with Enterprise Pool, Access Groups, and Director Pools by utilizing the standard ports used by these servers for the OCS 2007 applications. The version of ServerIron software tested is SI v10.0.0a

Additionally customization must be review against the Microsoft OCS Preplanning Guide.

Prior to configuring, determine the Server names, IP addresses, and ports required

Table 3. Server names, IP addresses, and ports required

Server Name	IP Address	Ports Used
cabletvd12	32.254.0.12	80, 135, 443, 444, 5060, 5061
cabletvd13	32.254.0.13	80, 135, 443, 444, 5060, 5061
cabletvd14	32.254.0.14	80, 135, 443, 444, 5060, 5061
cabletvd15	32.254.0.15	80, 135, 443, 444, 5060, 5061

To manage the ServerIron via the Command-Line Interface (ICL)I:

- At the opening CLI prompt, enter **enable**.
  `ServerIron> enable`
- Access the configuration level of the CLI by entering the following command:
  `ServerIron (config)#`
- To assign an IP address , enter the following command:
  `ServerIron (config)# ip add 32.254.0.253 255.255.255.0`
- To assign a default gateway , enter the following command:
  `ServerIron (config)# ip default-gateway 32.254.0.230`
- To assign a DNS address and domain, enter the following commands:
  `ServerIron (config)# ip dns domain-name microsoft.com`
  `ServerIron (config)# ip dns server-address 32.254.0.2`
- Other optional commands:
  `ServerIron (config)# hostname rtcfoundry1`
  `ServerIron (config)# enable super-user-password foundry |`
  `ServerIron (config)# no enable aaa console`
  `ServerIron (config)# telnet server`
  `ServerIron (config)# username ocsadmin nopassword`
- To exit from the configuration level of the CLI, enter the following command:
  `Rtcfoundry1 (config)# exit`
- To save the configuration to NVRAM, enter the following command:
  `Rtcfoundry1# write memory`

Initial configuration:

```
Rtcfoundry1 (config)# vlan 220 Rtcfoundry1 (config-vlan-1)# untag e2
Rtcfoundry1(config-vlan-1)# no spanning-tree
```

Set up the default server ports used for SIP:

```
Rtcfoundry1 (config)# server port 5060
Rtcfoundry1(config)# tcp
Rtcfoundry1(config)# server port 5061
Rtcfoundry1(config)# tcp
Rtcfoundry1(config)# server port 135
Rtcfoundry1(config)# tcp
Rtcfoundry1(config)# server port 80
Rtcfoundry1(config)# tcp
Rtcfoundry1(config)# server port 443
Rtcfoundry1(config)# tcp
Rtcfoundry1(config)# server port 444
Rtcfoundry1(config)# tcp
```

Define the real servers:

```
Rtcfoundry1(config)# server real cabletvd12 32.254.0.12
Rtcfoundry1(config)# port 444
Rtcfoundry1(config)# port ssl
Rtcfoundry1(config)# port http
Rtcfoundry1(config)# port http url "HEAD /"
Rtcfoundry1(config)# port 135
Rtcfoundry1(config)# port 5061
Rtcfoundry1(config)# port 5060
Rtcfoundry1(config)# server real cabletvd13 32.254.0.13
Rtcfoundry1(config)# port 444
Rtcfoundry1(config)# port ssl
Rtcfoundry1(config)# port http
Rtcfoundry1(config)# port http url "HEAD /"
Rtcfoundry1(config)# port 135
Rtcfoundry1(config)# port 5061
Rtcfoundry1(config)# port 5060
Rtcfoundry1(config)# server real cabletvd14 32.254.0.14
Rtcfoundry1(config)# port 444
Rtcfoundry1(config)# port ssl
Rtcfoundry1(config)# port http
Rtcfoundry1(config)# port http url "HEAD /"
Rtcfoundry1(config)# port 135
Rtcfoundry1(config)# port 5061
Rtcfoundry1(config)# port 5060
Rtcfoundry1(config)# server real cabletvd15 32.254.0.15
Rtcfoundry1(config)# port 444
Rtcfoundry1(config)# port ssl
Rtcfoundry1(config)# port http
Rtcfoundry1(config)# port http url "HEAD /"
Rtcfoundry1(config)# port 135
Rtcfoundry1(config)# port 5061
Rtcfoundry1(config)# port 5060
```

Virtual server setup:

```
Rtcfoundry1(config)# server virtual cabletvpool 32.254.0.240
Rtcfoundry1(config)# port 444
Rtcfoundry1(config)# port ssl
Rtcfoundry1(config)# no port ssl sticky
Rtcfoundry1(config)# port http
Rtcfoundry1(config)# port 135
Rtcfoundry1(config)# port 5061
Rtcfoundry1(config)# port 5060
Rtcfoundry1(config)# track-group 5061 135
Rtcfoundry1(config)# bind 444 cabletvd12 444 cabletvd13 444 cabletvd14 444 cabletvd15
444
Rtcfoundry1(config)# bind ssl cabletvd12 ssl cabletvd13 ssl cabletvd14 ssl cabletvd15
ssl
Rtcfoundry1(config)# bind http cabletvd12 http cabletvd13 http cabletvd14 http
cabletvd15 http
Rtcfoundry1(config)# bind 135 cabletvd12 135 cabletvd13 135 cabletvd14 135 cabletvd15
135
Rtcfoundry1(config)# bind 5061 cabletvd12 5061 cabletvd13 5061 cabletvd14 5061
cabletvd15 5061
Rtcfoundry1(config)# bind 5060 cabletvd12 5060 cabletvd13 5060 cabletvd14 5060
cabletvd15 5060
```

APPENDIX A: HIGH AVAILABILITY AND REDUNDANCY

No failover is easiest to configure and to manage. The downside is the loss of all access to the servers. Failover allows another ServerIron to continue to provide access to the servers in case of a failure. The sample configuration is an example of Hot-Standby.

- **Hot Standby:** One active ServerIron, another ServerIron in standby.
- **Active-Standby** : Both ServerIrons are active but for different VIPs. Each has its own VIP, if one ServerIron fails; the other becomes "owner" of the failed ServerIron's VIP.
- **Active-Active:** Both ServerIrons are active, the ServerIron that receives the request services that request. In case of a ServerIron failure, the remaining ServerIron handles all requests.

To Set Up Hot-Standby Redundancy

In a typical hot standby configuration, one ServerIron is the active device and performs all the Layer 2 switching as well as the Layer 4 SLB switching while the other ServerIron monitors the switching activities and remains in a hot standby role.

If the active ServerIron becomes unavailable, the standby ServerIron immediately assumes the unavailable ServerIron's responsibilities. The failover from the unavailable ServerIron to the standby ServerIron happens transparently to users. Both ServerIron switches share a common MAC address known to the clients. Therefore, if a failover occurs, the clients still know the ServerIron by the same MAC address. The active sessions running on the clients continue and the clients and routers do not need to re-ARP for the ServerIron MAC address.

Note: All real servers are connected directly to the ServerIrons with Active Standby NIC configuration where the Active Nic is connected to the active ServerIron.

- Configure port 1 on each ServerIron, enter the following command:
  `ServerIron (config)# server backup Ethernet 1 00e0.1234.1234`

  (The same primary MAC address is used on both ServerIrons.)
- To turn off spanning tree, enter the following command:
  `ServerIron (config)# no spanning-tree`
- To set the number of minutes on the primary ServerIron that it waits before retaking the primary role back over after an outage, enter the following command (only on the primary ServerIron): (5 minutes is minimum value)
  `ServerIron# server backup-preference 5`
- To save the configuration to NVRAM, enter the following command:
  `ServerIron# write memory`

Optionally, Set Up Active-Standby Redundancy

On boot, the ServerIron checks for a private link:

- If a private link (sync-link) is not present, the ServerIron becomes the active partner in the pair.
- If a private link is present, a random number listening-time is initiated. The ServerIron listens for the presence of a primary ServerIron through the backup monitoring port.
- If the ServerIron detects a primary (active ServerIron) through its backup monitoring port, the ServerIron is placed in standby mode.
- If the ServerIron does not detect a primary within one second and the link status is good, then the ServerIron becomes the primary ServerIron when the listening-time expires.

See the server software configuration guide for further details.

Optionally, Set Up Active-Active Redundancy

Active-active SLB uses session information to ensure that the same ServerIron load balances all requests for a given VIP. The first ServerIron that receives a request for the VIP load balances the request, creates a session table entry for the VIP, and sends the session information to the other ServerIron. Both ServerIrons in the configuration use the session information to use the same ServerIron for subsequent requests for the VIP.

In this example, ServerIron A and ServerIron B each have been configured to provide active-active SSLB (Symmetrical Server Load Balancing) for the HTTP port on VIP1 and VIP2. The first ServerIron to receive a request for port HTTP on one of these VIPs load balances the request, creates session entries for the VIP, and sends the session information to the other ServerIron. Both ServerIrons use the session information for the VIP to ensure that the same ServerIron load balances subsequent requests for the same application port and VIP.

Either ServerIron can use session information to forward the server reply back to the client. For example, if ServerIron A is the load balancer for a client request and the server reply comes back through ServerIron B, ServerIron B can use the session information received from ServerIron A through session synchronization to perform the required address translations and send the reply to the client. ServerIron B does not need to forward the reply to ServerIron A for address translation and forwarding.

See the server software configuration guide for further details.

APPENDIX B: RUNNING CONFIGURATION

```
SLB-rtcfoundry1#sh run
!Building configuration...
!Current configuration : 2707 bytes
!
ver 10.0.00aTI2
!
!
no global-stp
server backup-preference 5
!
!
server port 5060
tcp
server port 5061
tcp
server port 135
tcp
server port 80
tcp
server port 443
tcp
server port 444
tcp
server source-nat
server source-nat-ip 32.254.0.231 255.255.255.0 32.254.0.230 port-range 2
!
server real cabletvd14 32.254.0.14
port 444
port ssl
port http
port http url "HEAD /"
port http l4-check-only
port 135
port sips
port sip
!
server real cabletvd15 32.254.0.15
port 444
port ssl
port h port http url "HEAD /"
port http l4-check-only
port 135
port sips
port sip
!
server real cabletvd12 32.254.0.12
port 444
port ssl
port http
port http url "HEAD /"
port 135
port sips
port sip
```

```
!
server real cabletvd13 32.254.0.13
port 444
port ssl
port http
port http url "HEAD /"
port http l4-check-only
port 135
port sips
port sip
!
!
server virtual cabletvpool 32.254.0.240
port 444
port ssl
no port ssl sticky
port http
port 135
port sips
port sip
track-group sips 135
bind 444 cabletvd12 444 cabletvd13 444 cabletvd14 444 cabletvd15 444
bind ssl cabletvd12 ssl cabletvd13 ssl cabletvd14 ssl cabletvd15 ssl
bind http cabletvd12 http cabletvd13 http cabletvd14 http cabletvd15 http
bind 135 cabletvd12 135 cabletvd13 135 cabletvd14 135 cabletvd15 135
bind sips cabletvd12 sips cabletvd13 sips cabletvd14 sips cabletvd15 sips
bind sip cabletvd12 sip cabletvd13 sip cabletvd14 sip cabletvd15 sip
!
!
vlan 1 name DEFAULT-VLAN by port
no spanning-tree ttp
!
vlan 220 by port
untagged ether 2
no spanning-tree
!
!
enable super-user-password foundry
no enable aaa console
hostname rtcfoundry2
ip address 32.254.0.253 255.255.255.0
ip default-gateway 32.254.0.230
ip dns domain-name microsoft.com
ip dns server-address 32.254.0.2
telnet server
username ocsadmin nopassword
snmp-server
snmp-server community pub ro
snmp-server community public rw
web-management
web-management enable ether 3
!
!
End
```

NOTE: (If there is a backup ServerIron, the configuration will be similar to the primary. In the following case, two commands are different:

- No command “server backup-preference 5” entered on the secondary.
- The command for server source Nat should reflect ” server source-nat-ip 32.254.0.231 255.255.255.0 32.254.0.230 port-range 1”

APPENDIX C: MICROSOFT OFFICE COMMUNICATION SERVER 2007

Brocade ServerIron load balancing switches have been certified in Microsoft's load balancing OCS 2007 interoperability labs: http://office.microsoft.com/en-us/communicationsserver

Office Communications Server 2007 is the next version of Microsoft Live Communications Server 2005. Office Communications Server 2007 builds on the foundation of Presence and Instant Messaging, Federated Communications and Remote Call Control delivered by Live Communications Server 2005 and Microsoft Office Communicator 2005.

Key new features include a number of improvements to Instant Messaging and Presence capability such as integration with Microsoft Exchange Server distribution lists as well as the addition of software-powered VoIP, allowing users to make, receive and manage voice (phone) calls using Office Communicator 2007 running on their computer and multi-party on-premise audio/video and Web conferencing. Office Communications Server 2007 also supports the ICE framework of protocols, allowing users to take advantage of these communications capabilities from wherever they are without needing to establish a VPN connection.

Microsoft designed Office Communication Server 2007 to interoperate with Live Communication Server 2005. The migration process involves deploying some Office Communication 2007 infrastructure in parallel to a Live Communication Server 2005 deployment and then easily migrating users across the new infrastructure. For migration details, read the Microsoft Office 2007 product documentation found in Microsoft technical library at the OCS link referenced above.

Load balancing technology has become a technology of choice to improve the scalability, availability and security of IP applications. Brocade ServerIron switches, with their networking and application intelligence, provide rich features and high performance required for building massively scalable and highly secure application infrastructure.

See the Microsoft OCS planning guide: http://technet.microsoft.com/en-us/library/bb676082.aspx

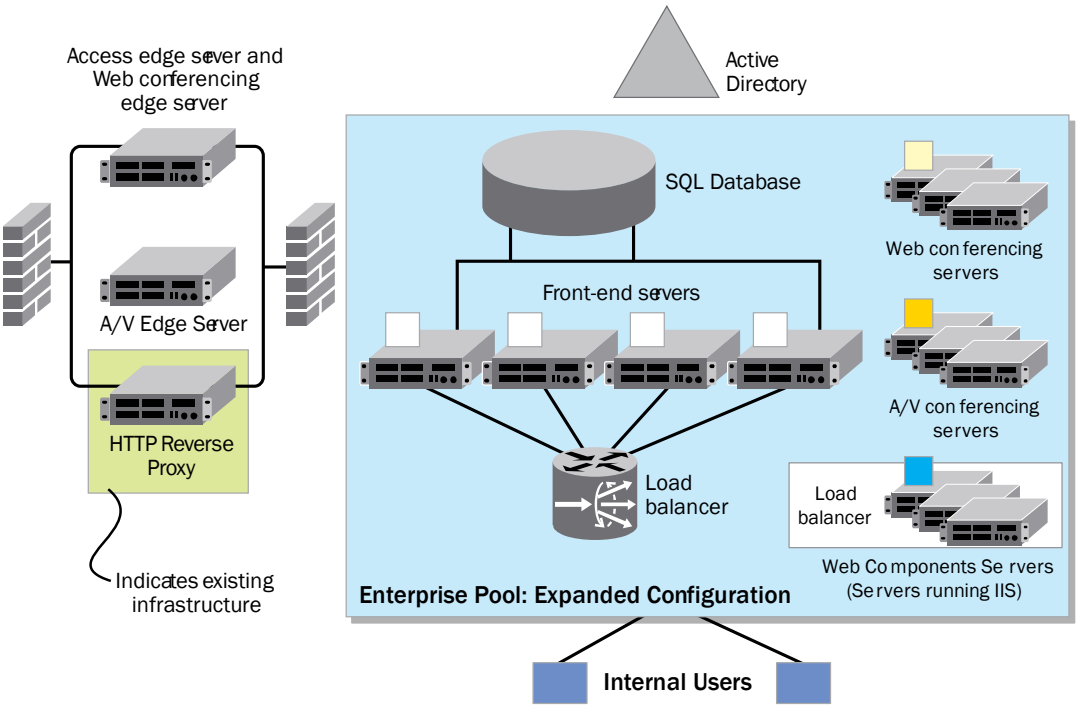

Figure 6. High-scale, high-availability deployment supporting IM and conferencing for internal and external users

APPENDIX D: BROCADE SERVERIRON

The Brocade ServerIron switches receive all client requests, and distribute them efficiently to the "best" server among the available pool. ServerIron switches consider server availability, load, response time, and other user-configured performance metrics when selecting a server for incoming client connections.

The ServerIron performs sophisticated and customizable "health checks" to the Office Communication servers, quickly identifying resource outages in real time and re-direct client connections to other available servers. The ServerIron provides a highly scalable solution that allows server capacity to be increased or decreased on demand without impacting the applications and client connections. When demand grows, IT engineers can simply "slide" in new server resources and configure the ServerIron switch to use the new servers for client connections.

ServerIron switches are application aware and can inspect many types of application level content to perform intelligent switching of client requests to appropriate servers. Application switching eliminates the need to replicate content and application functions on all servers, and optimizes overall resource utilization, application performance and availability. ServerIron switches support switching based on broad content types including URL, HTTP headers, HTTP cookies, SSL session IDs, and XML tags.

For implementations where session persistence across multiple TCP ports on the same server is a key requirement, the ServerIron switches offer support for the industry's most advanced and easily customizable load balancing interface. In addition, the power of performance delivered by the ServerIron switches ensures that the applications provide the best end-user response time and immense scalability even when enabled for Layer 4 through 7 switching. Using sticky sessions and track-group switching, a group of transactions from a given client are sent to the server originally selected and has the session created when the client first connected.

Application Performance

ServerIron switches, with their intelligent application-aware load balancing and content switching, significantly improve overall performance by optimally utilizing server resources. Using customizable load balancing methods and metrics, application performance can be tuned to achieve best response time and maximum throughput. By taking advantage of HTTP1.1 protocol mechanisms, the ServerIron switches support Server Connection Offload feature, which eliminates connection overhead from the servers and provides robust security. Server resources are truly dedicated to maximize application performance and user response time.

Application Availability

High-performance load balancing using ServerIron switches ensures always-on applications by intelligently distributing application traffic among all available servers, and dynamically monitoring the ability of serves and applications running on them to deliver optimal performance. Using customizable health checks at various levels of granularity like host, port, application and transaction,

ServerIron switches instantaneously and transparently react to increases and decreases in server resources by re-directing client traffic as needed. To protect applications from catastrophic failures, the switches can be deployed in multiple high-availability modes with stateful session failover. Applications are completely transparent to switch failures, and continue to function uninterrupted.

Application and Server Farm Security

Security is a critical challenge for businesses, especially for the mission-critical applications where the stakes are very high. As reliance on the network to deliver the mission-critical applications increases, so does the threat posed by network-based attacks. ServerIron switches have many intelligent features and superior performance to reliably protect against many forms of DoS, Virus and worm attacks. They protect application infrastructure and server farms against wire-speed Gigabit rate DoS attacks, which translates to 1.5 million attack messages in a second. ServerIron product family features industry's most advanced security intelligence to provide high-performance IronShield security that meets the needs of even the most demanding networks and applications serving millions of clients.

Application and Server Farm Scalability

Scaling applications and server farms is one of the most fundamental requirements for continued business growth, and is easily and permanently met by the ServerIron load balancers. ServerIron switches provide unlimited scalability to any IP-based application, and allow businesses to leverage commodity servers to build highly sophisticated and secure application infrastructure. Massive scalability is achieved with complete transparency to existing clients and servers without downtime.

Higher Return on Investment (ROI)

Brocade ServerIron load balancers provide immediate ROI, and also improve the ROI of application and server infrastructure. By implementing the new Server Connection Offload feature in existing server farm and application deployments, customers can immediately improve the overall capacity by an average of 20 to 40%. The ServerIron switches support significantly higher application traffic and clients with existing resources by efficient utilization. Downtime associated with security breaches, and server and application maintenance is eliminated, resulting in improved availability. Load balancers also simplify application and server farm management, which improves productivity and helps conserve valuable capital to address other critical problems in the network.

© 2009 Brocade Communications Systems, Inc. All Rights Reserved. 07/09 GA-SG-196-00

Brocade, the B-wing symbol, BigIron, DCX, Fabric OS, FastIron, IronPoint, IronShield, IronView, IronWare, JetCore, NetIron, SecureIron, ServerIron, StorageX, and TurboIron are registered trademarks, and DCFM and SAN Health are trademarks of Brocade Communications Systems, Inc., in the United States and/or in other countries. All other brands, products, or service names are or may be trademarks or service marks of, and are used to identify, products or services of their respective owners.

Notice: This document is for informational purposes only and does not set forth any warranty, expressed or implied, concerning any equipment, equipment feature, or service offered or to be offered by Brocade. Brocade reserves the right to make changes to this document at any time, without notice, and assumes no responsibility for its use. This informational document describes features that may not be currently available. Contact a Brocade sales office for information on feature and product availability. Export of technical data contained in this document may require an export license from the United States government.