ALCATEL-LUCENT ENTERPRISE OPTIMIZING CLOUD INFRASTRUCTURE WITH Citrix CloudBridge

APPLICATION NOTE

TABLE OF CONTENTS

1. PREFACE

1.1 Overview

This document provides design guidance, configuration examples and Alcatel-Lucent recommended best practices for WAN optimization when interconnecting geographically dispersed data centers and when using Citrix® NetScaler® to implement Layer 2 (L2) connectivity across Layer 3 network infrastructure.

1.2 Executive Summary

The smart device era is driving adoption of mobility services at a rapid pace. Enterprises cannot continue to facilitate employee mobility and maximize productivity by simply growing the standalone data center. Instead, enterprises are assessing employee needs and applications with an eye to the cloud. Cloud enables a network that provides elastic compute power with pay-as-you-grow models. How to secure the cloud is the biggest question.

The enterprise network needs to address a number of L2 connectivity challenges to ensure high availability between geographically dispersed data centers. Exponential growth in data center resources, coupled with security requirements, is driving enterprises to connect multiple data centers, typically over longer distances. As a result, they are facing additional challenges such as maintaining the high availability of applications and dealing with complex multi-site interconnections.

This document describes how an Alcatel-Lucent Application Fluent Network that is integrated with Citrix WAN optimization and Citrix CloudBridge™ solutions provides a high-speed, low-latency network between data centers.

Extensive manual testing was conducted in a large-scale customer-representative network. The Alcatel-Lucent data center fabric and Citrix NetScaler cloud network platform were validated with a wide range of system test types, including system integration, fault and redundancy, to ensure successful enterprise deployments. End-to-end verification of web application traffic was an important part of the testing.

2. LEGACY DATA CENTER INTERCONNECT MODELS

This section provides an overview of legacy deployment models for interconnecting data centers and the challenges associated with extending L2 networks.

2.1 Legacy deployment models for data center interconnect

Several transport technologies are available for interconnecting data centers. Each technology provides various features and supports different distances, depending on factors such as the power of the optics, the lambda used for transmission, the type of fiber and other characteristics.

Consider the features of LAN and SAN switches that provide higher availability for interconnecting data centers before considering the available technologies. The convergence time required for the application is also important and should be evaluated. The following list describes common transport options:

- Dark fiber — Dark fiber is a viable method for extending virtual LANs (VLANs) over data center or campus distances. The maximum attainable distance is a function of the optical characteristics (transmit power and receive sensitivity) of the LED or laser that resides in a Small Form-Factor Pluggable (SFP) or Gigabit Interface Converter (GBIC) transponder, combined with the number of fiber joins and the attenuation of the fiber.
- Coarse Wavelength Division Multiplexing (CWDM) — CWDM offers a simple solution to carry up to eight channels (1 Gb/s or 2 Gb/s) on the same fiber. These channels can carry Ethernet or fiber channel. CWDM does not offer protected lambdas, but client protection allows rerouting of the traffic on the functioning links when a failure occurs. CWDM lambdas can be added and dropped, allowing the creation of hub-and-spoke, ring and meshed topologies. The maximum achievable distance is approximately 100 km with a point-to-point physical topology and approximately 40 km with a physical ring topology.
- Dense Wavelength Division Multiplexing (DWDM) — DWDM enables up to 32 channels (lambdas). Each of these channels can operate at up to 10 Gb/s. DWDM networks can be designed either as multiplexing networks that are similar to CWDM, or with a variety of protection schemes to guard against failures in the fiber plant. DWDM also offers more protection mechanisms — splitter protection and Y-cable protection, for example — than CWDM as well as the possibility to amplify the channels to reach greater distances.
- Metro Ethernet — Metro Ethernet service traditionally covers a small area, such as a MAN, providing a transparent Ethernet circuit between a pair of locations and emulating a direct Ethernet cable between devices on either end. The connection bridges all L2 protocols, such as the Spanning Tree Protocol (STP), as well as VLAN tags (including double-tagged frames).
- Multiprotocol Label Switching (MPLS) — MPLS IP VPN networks can extend across long distances. MPLS enables segmentation of a network to allow efficient and secure utilization of a shared network. MPLS helps to acquire and extend the resources required for services between data centers. MPLS also provides traffic engineering capabilities, enabling resiliency and more efficient link resource utilization, as well as quality of service (QoS) differentiation and bandwidth guarantees.

In nearly all of these deployment models, the costs associated with deploying and maintaining a dedicated network is the most significant concern. In addition, because there is no STP isolation, issues in one data center will affect other data centers. Another disadvantage is the lack of load balancing across redundant paths due to blocked links in the core network.

2.2 Challenges associated with extended Layer 2 networks

It is common practice to add redundancy to interconnect two data centers because it avoids split-subnet scenarios and interruption of communications between servers. A split-subnet architecture is one where a single LAN is split into multiple LANs and each LAN shares the same IP subnet. The split-subnet is not necessarily a problem if the routing metric prefers one site over the other. Also, if the servers at each site are part of a cluster and the communication is lost, mechanisms such as the quorum disk avoid a split-brain condition.

Adding redundancy to an extended Ethernet network typically means relying on STP to keep the topology free from loops. STP domains should be reduced as much as possible and limited within the data center. Alcatel-Lucent does not recommend deploying the legacy 802.1d standard because it underutilizes network capacity and limits scale. The solutions that this document describes provide L2 extension in a redundant configuration with STP isolation between data centers.

An extended L2 network presents a number of challenges:

- Unstable topologies. STP operates at L2. Its primary function is to prevent loops that redundant links create in bridge networks. STP timers with aggressive values can lead to an unstable topology. In these cases, loss of Bridge Protocol Data Units (BPDUs) can cause a loop to appear.
- Network scale. Even STP developments, such as Multiple Spanning Tree Protocol (MSTP), cannot scale when connecting hundreds of devices in a flat architecture. This results in slow convergence upon link or node failures.
- Disaster recovery and business continuity. These are the primary reasons for multi-site data centers. However, because data centers typically require L2 connectivity, failure in one data center can affect other data centers. This could lead to a black-out of all data centers at the same time.
- Broadcast storms. A broadcast storm propagates to every data center. If uncontrolled, this can result in a network-wide outage. Broadcast storms can be directly related to STP. A misconfigured link, such as a unidirectional link with auto-negotiation off or a loopback, at the access layer can generate a broadcast storm and disrupt remote data centers. Even with STP isolation between the data centers, broadcast storm issues can disrupt the entire L2 domain.
- Load balancing. Load balancing of traffic across redundant paths may not be possible due to blocked links in the core network.

3. Citrix CloudBridge OVERVIEW

A fundamental part of the Citrix cloud framework, Citrix CloudBridge is a tool used to build a cloud-extended data center. CloudBridge enables secure, optimized connections between the data center and the private or public clouds where enterprises host their cloud virtual storage, servers and other devices. Cloud-hosted applications function as if they were running on one contiguous enterprise network. With CloudBridge, enterprises can move their applications to the cloud while reducing costs and the risk of application failure.

3.1 How CloudBridge works

CloudBridge provides two main functions:

- Connectivity: The connection between data centers can be either L2 or Layer 3 (L3) and either mode (L2 or L3) can be secured using the Internet Protocol security (IPSec) protocol. In the L3 environment, a /30 address space between the NetScalers and a route configuration is needed to point to the other network through the directly connected Generic Routing Encapsulation (GRE) interface.
- Optimization: Every instance of CloudBridge includes an instance of Citrix Branch Repeater®, which ties into NetScaler, but runs as a separate virtual machine (VM). It offers various optimizations, including block-level data replication as well as Transmission Control Protocol (TCP) optimizations such as window scaling, Selective Acknowledgement (SACK) and aggressive retransmit for packet loss.

The connection is made through an IP tunnel that uses the GRE protocol. The GRE protocol provides a mechanism for encapsulating packets from a wide variety of network protocols for forwarding over another protocol. GRE is used to:

- Connect networks running non-IP, non-routable protocols, such as AppleTalk®, Novell® Internetwork Packet Exchange (IPX™) and Network Basic Input/Output System (NetBIOS).
- Bridge across a WAN.
- Create a transport tunnel for any type of traffic that needs to be sent unchanged across a different network.
- Encapsulate packets by adding GRE and a GRE IP header to the packets.

CloudBridge supports use of the IPSec)protocol suite to secure communications between peers in the CloudBridge. In a CloudBridge, the IPSec protocol ensures:

- Data integrity
- Data origin authentication
- Data confidentiality (encryption)
- Protection against replay attacks

The IPSec protocol uses the transport mode in which only the payload of the GRE-encapsulated packet is encrypted. The encryption uses the Encapsulating Security Payload (ESP) protocol, which ensures the integrity of the packet by using a hash method authentication code (HMAC) hash function and ensures confidentiality by using an encryption algorithm. After encrypting the payload and calculating the HMAC, the ESP protocol generates an ESP header and inserts it after the GRE IP header. The ESP protocol also generates an ESP trailer which it inserts at the end of the encrypted packets.

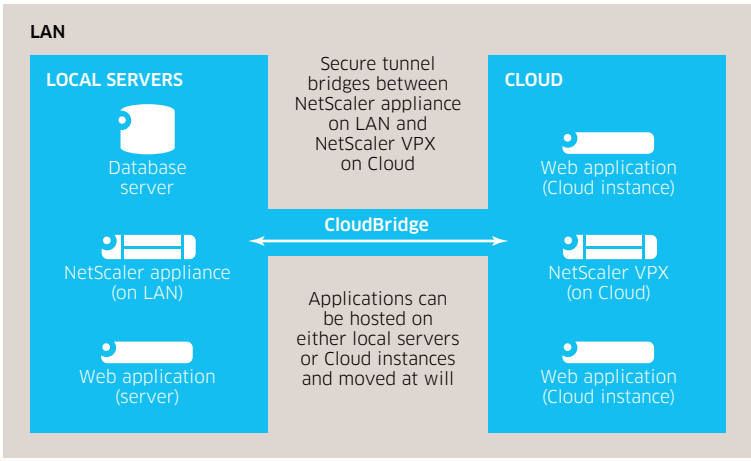
Before securing communications between the peers in the CloudBridge, using the Internet Key Exchange (IKE) protocol in IPSec:

1. The two peers authenticate with each other, using one of the following authentication methods:
   - Pre-shared key authentication. A text string called a pre-shared key, manually configured on each peer. The pre-shared keys of the peers are matched against each other for authentication. For the successful authentication, you must configure the same pre-shared key on each of the peers.
   - Digital certificates authentication. For digital certificate authentication, a peer (sender) initiator signs message interchange data by using its private key, and the other peer (receiver) uses the peer's (sender's) public key to verify the signature. Typically, the public key is exchanged in messages containing an X.509v3 certificate. This certificate provides a level of assurance that a peer's identity as represented in the certificate is associated with a particular public key.
2. The peers then negotiate to reach agreement on:
   - A security protocol to use, so that each one sends data in a format the other can understand.
   - An encryption algorithm.
   - Cryptographic keys for encrypting data in one peer and decrypting it in the other.

This agreement on the security protocol, encryption algorithm and cryptographic keys is called a Security Association (SA). SAs are one way (simplex). For example, when two NetScaler appliances, NS1 and NS2, are communicating through IPSec over a CloudBridge, NS1 has two SAs. One SA is used for processing outbound packets, and the other SA is used for processing inbound packets.

SAs expire after a specified interval of time, which is called the lifetime. The two peers then use the IKE protocol, which is part of the IPSec protocol suite, to negotiate new cryptographic keys and establish new SAs. The purpose of the limited lifetime is to prevent attackers from cracking a key. Figure 1 provides a conceptual illustration of a CloudBridge.

Figure 1. CloudBridge conceptual diagram



4. GLOBAL SERVER LOAD BALANCING OVERVIEW

Global Server Load Balancing (GSLB) describes a range of technologies to distribute resources around the Internet for various purposes. Depending on the user and nature of deployment, GSLB can have different goals. They include:

1. Disaster recovery. Providing an alternate location for accessing a resource in the event of a failure, or providing a means of shifting traffic easily to simplify maintenance (or both).
2. Load sharing. Distributing traffic between multiple locations to:
   - Minimize bandwidth costs
   - Limit the capacity used at a given location
   - Limit exposure to various issues, including outages and geographic disruption.
3. Performance. Positioning content closer to users to enhance their experience.
4. Legal obligations. Presenting users with different versions of resources based on their political geography.

Over time, various techniques have been developed to meet these requirements. Three techniques have withstood the test of time:

1. Domain Name System (DNS)-based redirection to different locations.
2. Content-level redirection to different locations using HTTP redirection.
3. Route Injection to advertise the same IP address to multiple locations.

4.1 How GSLB works

With standard DNS, when a client sends a DNS request, it receives a list of IP addresses for the domain or service. Generally, the client chooses the first IP address in the list and initiates a connection with that server. The DNS server uses a technique called DNS round robin to rotate through the IP addresses on the list, sending the first IP address to the end of the list and promoting the others after it responds to each DNS request. This technique ensures equal distribution of the load, but it does not support disaster recovery, load balancing based on load or proximity of servers or persistence.

When GSLB is configured on a NetScaler appliance and the Metric Exchange Protocol (MEP) is enabled, the appliance uses the DNS infrastructure to connect the client to the data center that best meets the set criteria. The criteria can specify any combination of the following:

- Least loaded data center
- Closest data center
- Data center that responds most quickly to requests from the client's location
- SNMP metrics

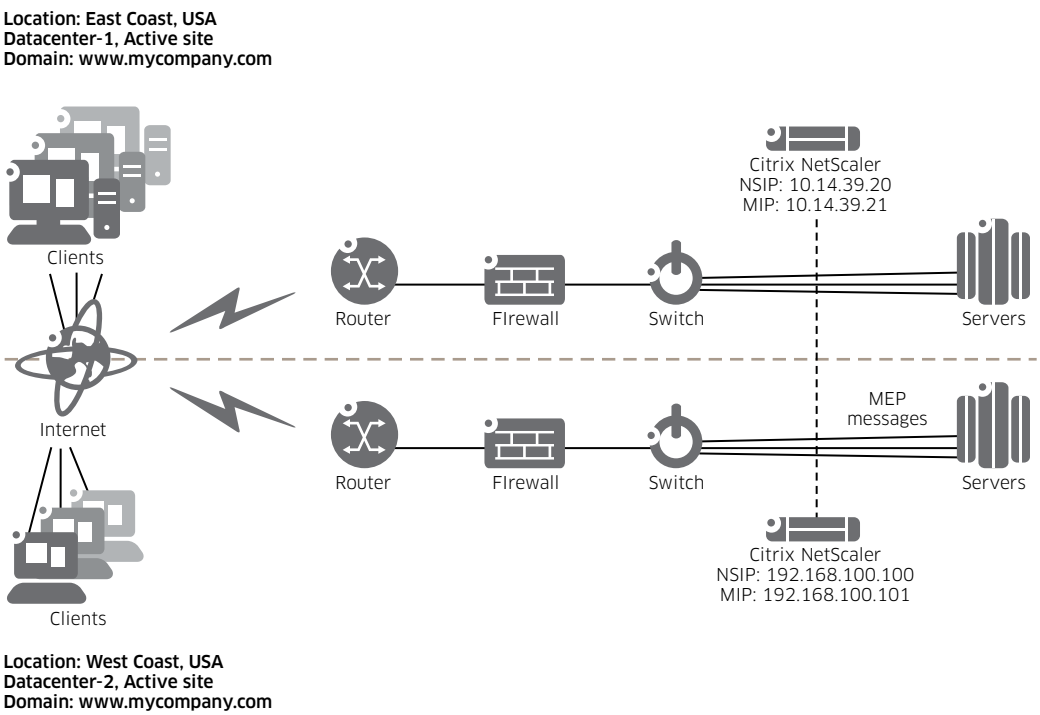
An appliance keeps track of the location, performance, load and availability of each data center and uses these factors to select the data center to which to send a client request.

A GSLB configuration consists of a group of GSLB entities on each appliance in the configuration. These entities include:

- GSLB sites
- GSLB services
- GSLB virtual servers
- Load balancing and content switching servers
- Authoritative DNS (ADNS) services

Global server load balancing is used to manage traffic flow to a web site that is hosted on two separate server farms that ideally are in different geographic locations. For example, consider a Web site, www.mycompany.com, which is hosted on two geographically separated server farms or data centers. Both server farms use NetScaler appliances. The NetScaler appliances in these server farms are set up in one-arm mode and function as authoritative DNS servers for the www.mycompany.com domain. Figure 2 illustrates this configuration.

Figure 2. Basic GSLB topology



To configure the GSLB setup shown in Figure 2

1. Configure a standard load balancing setup for each server farm or data center. This enables load balancing across the different servers in each server farm.
2. Configure both NetScaler appliances as ADNS servers.
3. Create a GSLB site for each server farm.
4. Configure GSLB virtual servers for each site.
5. Create GSLB services and bind them to the GSLB virtual servers.
6. Bind the domain to the GSLB virtual server.

4.2 GSLB sites

A typical GSLB setup consists of data centers, each of which has various network appliances that may or may not be NetScaler appliances. The data centers are called GSLB sites. Each GSLB site is managed by a NetScaler appliance that is local to that site. Each of these appliances treats its own site as the local site and all other sites, managed by other appliances, as remote sites.

If the appliance that manages a site is the only NetScaler appliance in that data center, the GSLB site hosted on that appliance acts as a bookkeeping placeholder for auditing purposes, because no metrics can be collected. Typically, this happens when the appliance is used only for GSLB while other products in the data center are used for load balancing or content switching.

4.3 GSLB services

A GSLB service is usually a representation of a load balancing or content switching virtual server, although it can represent any type of virtual server. The GSLB service identifies the virtual server's IP address, port number and service type. GSLB services are bound to GSLB virtual servers on the NetScaler appliances managing the GSLB sites:

- A GSLB service bound to a GSLB virtual server in the same data center is local to the GSLB virtual server.
- A GSLB service bound to a GSLB virtual server in a different data center is remote from that GSLB virtual server.

4.4 GSLB virtual servers

A GSLB virtual server has one or more GSLB services bound to it, and load balances traffic among those services. It evaluates the configured GSLB methods (algorithms) to select the appropriate service to which to send a client request. Because the GSLB services can represent either local or remote servers, selecting the optimal GSLB service for a request has the effect of selecting the data center that should serve the client request.

The domain for which GSLB is configured must be bound to the GSLB virtual server, because one or more services bound to the virtual server will serve requests made for that domain.

Unlike other virtual servers configured on a NetScaler appliance, a GSLB virtual server does not have its own virtual IP address (VIP).

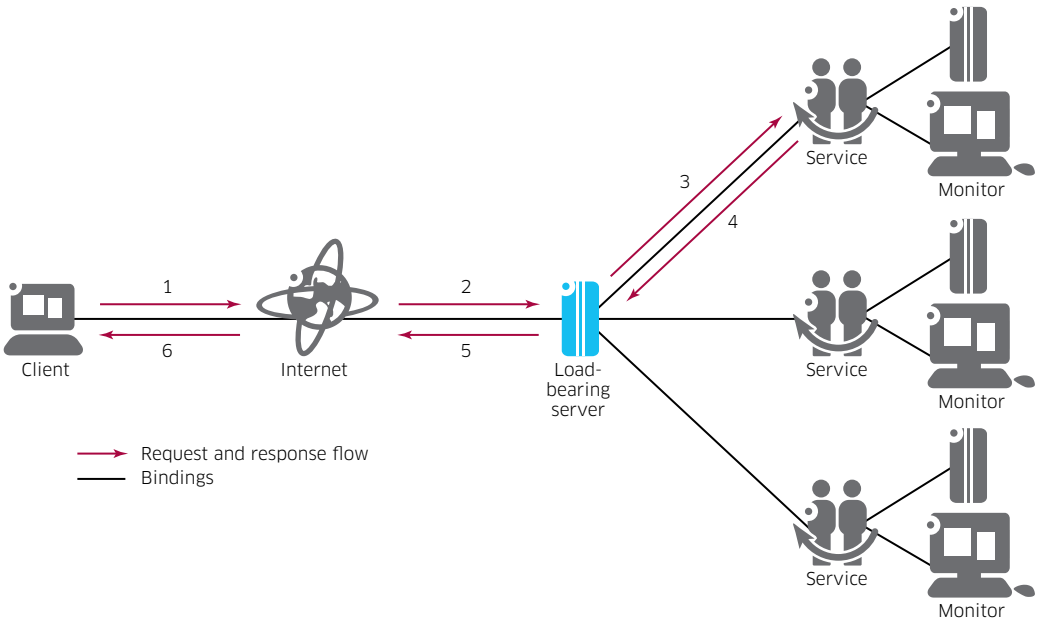
5. LOAD BALANCING OVERVIEW

In a basic load balancing setup, clients send their requests to the IP address of a virtual server configured on the NetScaler appliance. The virtual server distributes them to the load-balanced application servers according to a preset pattern, called the load balancing algorithm.

5.1 How load balancing works

A load balancing setup includes a load-balancing server and multiple load-balanced application servers. The virtual server receives incoming client requests, uses the load balancing algorithm to select an application server, and forwards the requests to the selected application server. Figure 3 illustrates a typical load balancing deployment. Another variation involves assigning a global HTTP port.

Figure 3. Typical load balancing architecture



The load balancing server can use any of a number of algorithms (or methods) to determine how to distribute load among the load-balanced servers that it manages. The default load balancing method is the “least connection method”, in which the NetScaler appliance forwards each incoming client connection to whichever load balanced application server currently has the fewest active user connections.
The following entities are configured in a typical NetScaler load balancing setup:

- Load balancing virtual server. The IP address, port and protocol combination to which a client sends connection requests for a particular load-balanced web site or application. If the application is accessible from the Internet, the VIP address VIP is a public IP address. If the application is accessible only from the LAN or WAN, the VIP is usually a private (ICANN non-routable) IP address.
- Service. The IP address, port and protocol combination used to route requests to a specific load-balanced application server. A service can be a logical representation of the application server itself, or of an application running on a server that hosts multiple applications. Each service is bound to a specific virtual server.
- Server object. An entity that identifies a physical server and provides the server’s IP address. The server’s IP address can be used as the name of the server object. Simply enter the server’s IP address when the service is created and the server object is automatically created. Alternatively, create the server object first, assign it a Fully Qualified Domain Name (FQDN) or other name, then specify that name instead of the IP address when the service is created.

- Monitor. An entity on the NetScaler appliance that tracks a service and ensures it is operating correctly. The monitor periodically probes (or performs a health check on) each service to which it is assigned. If the service does not respond within the time specified by the time-out, and a specified number of health checks fail, that service is marked as DOWN. The NetScaler appliance skips that service when performing load balancing until the issues that caused the service to quit responding are fixed.

6. CloudBridge AND GSLB TESTED TOPOLOGY

Figure 4 illustrates the physical CloudBridge and GSLB topology that was tested while Figure 5 illustrates the logical topology.

Figure 4. Physical topology tested

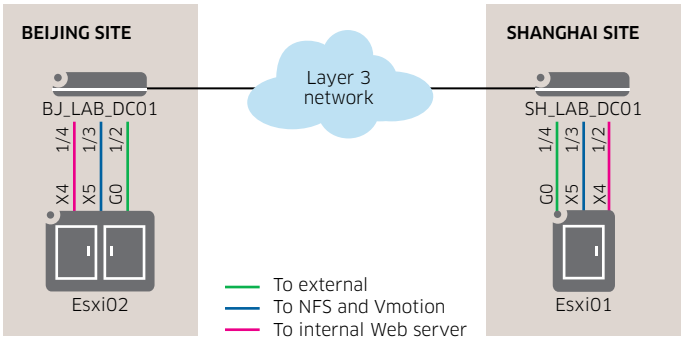
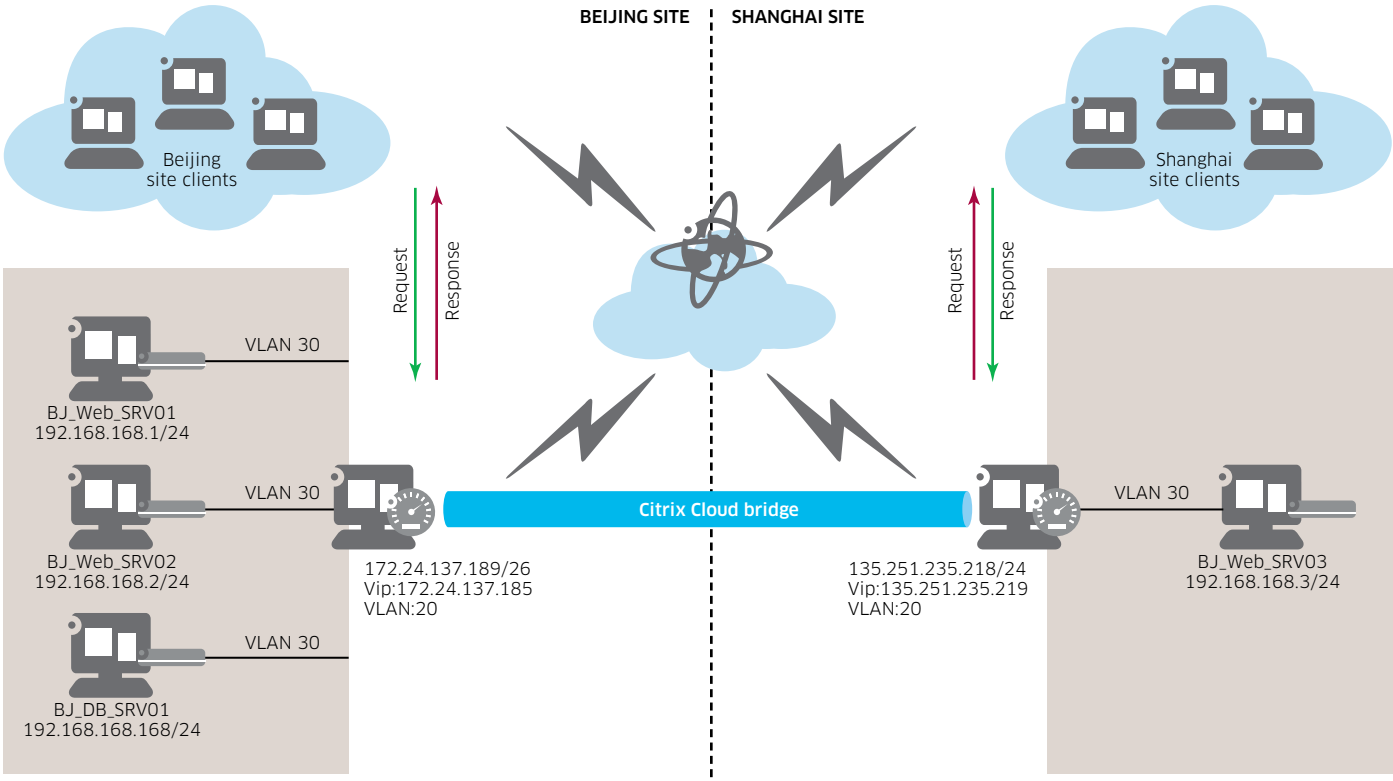


Figure 5. Logical topology tested



7. NETWORKING INFRASTRUCTURE CONFIGURATION

The following code describes the networking infrastructure configuration.

```
BJ_LAB_DC01-> show configuration snapshot
! Chassis:
system name BJ_LAB_DC01->
system location Lab_Rack
! Configuration:
! Capability Manager:
hash-control brief
! Multi-Chassis:
! Virtual Flow Control:
! Interface:
! Link Aggregate:
linkagg static agg 1 size 2 admin-state enable
linkagg static agg 1 name “os6900-2”
linkagg static port 1/20 agg 1
! VLAN:
vlan 1 admin-state disable
vlan 10 admin-state enable
vlan 10 name “NFS-ESXI-Vmotion”
vlan 20 admin-state enable
vlan 20 name “To-Office”
vlan 30 admin-state enable
vlan 30 name “Web-SRV”
vlan 40 admin-state enable
vlan 10 members port 1/3 untagged
vlan 10 members port 1/4 tagged
vlan 10 members linkagg 1 tagged
vlan 20 members port 1/1-2 untagged
vlan 20 members port 1/19 tagged
vlan 20 members linkagg 1 tagged
vlan 30 members port 1/4 tagged
vlan 30 members port 1/19 untagged
vlan 30 members linkagg 1 tagged
vlan 40 members linkagg 1 tagged
! Spanning Tree:
spantree vlan 1 admin-state enable
spantree vlan 10 admin-state enable
spantree vlan 20 admin-state enable
spantree vlan 30 admin-state enable
spantree vlan 40 admin-state enable
spantree vlan 133 admin-state enable
spantree vlan 200 admin-state enable

! Bridging:
! Port Mirroring:
! Port Mapping:
! IP:
ip service port 21 admin-state enable
```

```
ip service port 22 admin-state enable
ip service port 23 admin-state enable
ip service port 80 admin-state enable
ip service port 123 admin-state disable
ip service port 161 admin-state enable
ip service port 443 admin-state enable
ip interface “vlan10” address 10.100.100.100 mask 255.255.255.0 vlan 10 ifindex 1
ip interface “vlan30” address 192.168.168.100 mask 255.255.255.0 vlan 30 ifindex 2
ip interface “vlan40” address 192.168.10.1 mask 255.255.255.0 vlan 40 ifindex 3

! IPv6:
! IPSec:
! IPMS:
! AAA:
aaa authentication console “local”
aaa authentication telnet “local”
aaa authentication ftp “local”
aaa authentication snmp “local”
! NTP:
! QOS:
! Policy Manager:
! VLAN Stacking:
! ERP:
! MVRP:
! LLDP:
! UDLD:
! Server Load Balance:
! High Availability Vlan:
! Session Manager:
session cli timeout 3600
session prompt default “BJ_LAB_DC01->”

! Web:
! Trap Manager:
snmp station 10.100.100.190 162 “alcatel” v2 enable
! Health Monitor:
! System Service:
swlog appid capManSig subapp all level error
! SNMP:
snmp security no-security
snmp community-map mode enable
snmp community-map “alcatel” user “alcatel” enable
! BFD:
! IP Route Manager:
! VRRP:
! UDP Relay:
! RIP:
! OSPF:
! IP Multicast:
! DVMRP:
! IPMR:
! RIPng:
```

```
! OSPF3:
! BGP:
! Netsec:
! Module:
! RDP:
! DA-UNP:
unp dynamic-vlan-configuration enable
unp name Web_SRV vlan 30
unp name vlan40 vlan 40
unp classification vlan-tag 30 unp-name Web_SRV
unp port 1/5 enable
unp port 1/5 classification enable
unp port 1/6 enable
unp port 1/6 classification enable
! DHL:

SH_LAB_DC01-> show configuration snapshot
! Chassis:
system name SH_LAB_DC01->
! Configuration:
! Capability Manager:
hash-control brief
! Multi-Chassis:
! Virtual Flow Control:
! Interface:
! Link Aggregate:
! VLAN:
vlan 1 admin-state enable
vlan 10 admin-state enable
vlan 10 name “NFS-ESXI-Vmotion”
vlan 30 admin-state enable
vlan 30 name “Web_SRV”
vlan 10 members port 1/3 untagged
! Spanning Tree:
spantree vlan 1 admin-state enable
spantree vlan 10 admin-state enable
spantree vlan 30 admin-state enable
! Bridging:
! Port Mirroring:
! Port Mapping:
! IP:
ip service port 21 admin-state enable
ip service port 22 admin-state enable
ip service port 23 admin-state enable
ip service port 80 admin-state enable
ip service port 123 admin-state disable
ip service port 161 admin-state enable
ip service port 443 admin-state enable
ip interface “vlan10” address 10.100.100.222 mask 255.255.255.0 vlan 10 ifindex 1
ip interface “vlan30” address 192.168.168.222 mask 255.255.255.0 vlan 30 ifindex 2
! IPv6:
! IPSec:
```

```
! IPMS:
! AAA:
aaa authentication default “local”
aaa authentication console “local”
aaa authentication telnet “local”
aaa authentication snmp “local”
! NTP:
! QOS:
! Policy Manager:
! VLAN Stacking:
! ERP:
! MVRP:
! LLDP:
! UDLD:
! Server Load Balance:
! High Availability Vlan:
! Session Manager:
session cli timeout 3600
session prompt default “SH_LAB_DC01->”
session login-timeout 600

! Web:
! Trap Manager:
snmp station 10.100.100.190 162 “alcatel” v2 enable
! Health Monitor:
! System Service:
swlog appid capManSig subapp all level error
! SNMP:
snmp security no-security
snmp community-map mode enable
snmp community-map “alcatel” user “alcatel” enable
! BFD:
! IP Route Manager:
! VRRP:
! UDP Relay:
! RIP:
! OSPF:
! IP Multicast:
! DVMRP:
! IPMR:
! RIPng:
! OSPF3:
! BGP:
! Netsec:
! Module:
! RDP:
! DA-UNP:
unp name Web_SRV vlan 30
unp classification vlan-tag 30 unp-name Web_SRV
unp port 1/4 enable
unp port 1/4 classification enable
! DHL:
```

8. INSTALLING NetScaler VIRTUAL APPLIANCES ON VMWARE ESX

Before installing Citrix NetScaler virtual appliance release 9.3 on VMware ESX, make sure the VMware ESX server is installed on a machine with adequate system resources.

- To install virtual appliances on VMware ESX 4.0, use the VMware vSphere™ Client.
- To install virtual appliances on VMware ESX 3.5, use the VMware Open Virtualization Format (OVF) tool.

Note that the client or tool must be installed on a remote machine that can connect to VMware ESX through the network.

After the installation:

- Use vSphere Client 4.0 to manage virtual appliances on VMware ESX 4.0.
- Use VMware Infrastructure (VI) Client 2.5 to manage virtual appliances on VMware ESX 3.5.

Note: The VMware vSphere Client shows the guest operating system as "Sun Solaris 10" for NetScaler VPX. This is by design because VMware ESX 3.5 does not recognize FreeBSD.

8.1 Prerequisites for installing NetScaler VPX virtual appliances on VMware

Before installing a virtual appliance:

- Install VMware ESX 3.5 or later on hardware that meets the minimum requirements.
- Install VMware Client on a management workstation that meets the minimum system requirements.
- Install VMware Open Virtual Machine Format (OVF) Tool, which is required for VMware ESX 3.5, on a management workstation that meets the minimum system requirements.
- Download the NetScaler VPX™ setup files as described in section 8.2.
- Label the physical network ports of VMware ESX.
- Obtain NetScaler VPX license files. For more information about NetScaler VPX licenses, see the *NetScaler VPX Licensing Guide* at http://support.citrix.com/article/ctx122426

VMware ESX hardware requirements

Table 1 describes the minimum system requirements for VMware EXS servers running NetScaler nCore VPX.

Table 1. Minimum system requirements for VMware ESX servers running NetScaler nCore VPX

COMPONENT	REQUIREMENT
CPU	2 or more 64-bit x86 CPUs with virtualization assist (Intel-VT or AMD-V) enabled Note: To run NetScaler VPX, hardware support for virtualization must be enabled on the VMware ESX host. Make sure that the BIOS option for virtualization support is not disabled. For more information, see your BIOS
RAM	3 GB
Disk space	Locally attached storage (PATA, SATA, SCSI) with 40 GB of disk space available
Network	One 1 Gb/s Network Interface Card (NIC); Two 1 Gb/s NICs recommended. The network interfaces should be E1000.

For information about installing VMware ESX, see http://www.vmware.com/.

Table 2 lists the virtual computing resources that the VMware ESX server must provide for each NetScaler nCore VPX.

Table 2. Minimum virtual computing resources required to run NetScaler nCore VPX

COMPONENT	REQUIREMENT
Memory	2 GB
Virtual CPU (VCPU)	2
Virtual network interfaces	1 Note: If the virtual appliance is installed on VMware ESX 3.5 or VMware ESXi 3.5, a maximum of 4 virtual network interfaces can be installed. If the virtual appliance is installed on ESX 4.0, the maximum is 10.
Disk space	20 GB Note: This is in addition to any disk requirements for the hypervisor.

Note: For production use of NetScaler VPX, the full memory allocation must be reserved. CPU cycles (in MHz) equal to at least the speed of one CPU core of the ESX should also be reserved.

8.2 Downloading the NetScaler VPX setup files

The NetScaler VPX setup package for VMware ESX follows the Open Virtualization Format (OVF) standard. The files can be downloaded from MyCitrix.com. A My Citrix account is required to log on. To create a My Citrix account, go to http://www.mycitrix.com, click the New Users link and follow the instructions provided.

Once logged on:

1. Navigate the following path from the My Citrix home page:
   MyCitrix.com > Downloads > NetScaler > Virtual Appliances.
2. Copy the following files to a workstation on the same network as the ESX server. Copy all three files into the same folder.
   - NSVPX-ESX- < release number > - < build number > -disk1.vmdk
     For example: NSVPX-ESX-9.3-39.8-disk1.vmdk
   - NSVPX-ESX- < release number > - < build number > .ovf
     For example: NSVPX-ESX-9.3-39.8.ovf
   - NSVPX-ESX- < release number > - < build number > .mf
     For example: NSVPX-ESX-9.3-39.8.mf

Labeling the physical network ports of VMware ESX

Before installing a NetScaler VPX virtual appliance, label of all the interfaces that will be assigned to VPX virtual appliances in a unique format. Citrix recommends the following format: NS_NIC_1_1, NS_NIC_1_2, and so on.

In large deployments, labeling in a unique format helps quickly identify the interfaces that are allocated to the NetScaler VPX virtual appliance among interfaces used by other virtual machines, such as Microsoft® Windows® and Linux. Such labeling is especially important when different types of virtual machines share the same interfaces.

To label the physical network ports of VMware ESX server

1. Log on to the VMware ESX server using the vSphere Client.
2. On the vSphere Client, select the **Configuration** tab then click **Networking**.
3. At the top-right corner, click **Add Networking**.
4. In the **Add Network Wizard**, for **Connection Type**, select **Virtual Machine** then click **Next**.
5. Scroll through the list of vSwitch physical adapters and choose the physical port that will map to interface 1/1 on the virtual appliances.
6. Enter **NS_NIC_1_1** as the name of the vSwitch that will be associated with interface 1/1 of the virtual appliances.
7. Click **Next** to finish the vSwitch creation.

   Repeat the procedure, beginning with step 2, to add interfaces that will be used by the virtual appliances. Label the interfaces sequentially, in the correct format (for example, **NS_NIC_1_2**).

9. INSTALLING NetScaler VIRTUAL APPLIANCES ON VMWARE ESX 4.0 OR 5.0

After installing and configuring VMware ESX 4.0, use VMware vSphere Client to install virtual appliances on the VMware ESX. The number of virtual appliances installed depends on the amount of memory available on the hardware that is running VMware ESX.

To install NetScaler virtual appliances on VMware ESX 4.0 or 5.0 using VMware vSphere Client

1. Start the VMware vSphere Client on your workstation.
2. In the **IP address/Name** text box, type the IP address of the VMware ESX server that you want to connect to.
3. In the **User Name** and **Password** text boxes, type the administrator credentials then click **Login**.
   Note: The username and password are both “nsroot”.
4. From the **File** menu, select **Deploy OVF Template**.
5. In the **Deploy OVF Template** dialog box, in **Deploy from file**, browse to the location at which you saved the NetScaler VPX setup files, select the .ovf file then click **Next**.
6. Map the networks shown in the VPX OVF template to the networks configured on the ESX host. Click **Next** to start installing VPX on VMware ESX. When installation is complete, a pop-up window confirms the successful installation.
7. Start the NetScaler VPX. In the navigation pane, select the NetScaler VPX just installed and, from the right-click menu, select **Power On**. Click the **Console** tab to emulate a console port.
8. To install another virtual appliance, repeat steps 4 through 6.

10. CONFIGURING THE BASIC SYSTEM SETTINGS

After installing a Citrix NetScaler VPX virtual appliance, access it to configure the basic settings. Initially, the NetScaler command line is accessed through the management application for the virtualization host. This application is either Citrix XenCenter® for Citrix XenServer® or VMware vSphere Client for VMware ESX. A NetScaler IP (NSIP) address, subnet mask and default gateway must be specified. The NSIP is the management address from which the NetScaler command line or configuration utility can be accessed using a secure shell (SSH client). Either of these access methods, or the console, can be used to complete the basic configuration.

To access the configuration utility, type the NSIP into the address field of any browser (for example, http://<NSIP_address>). Java RunTime Environment (JRE) version 1.6 or later is required.

10.1 Setting up the initial configuration using the NetScaler VPX console

The first task after installing a NetScaler virtual appliance on a virtualization host is to use the NetScaler VPX console in the vSphere Client to configure the initial settings described below.

Note: If a virtual appliance was installed on XenServer using Command Center, these settings do not have to be configured. Command Center implicitly configures the settings during installation. For more information about provisioning VPX from Command Center, see the Command Center documentation.

NetScaler IP address (NSIP)
The IP address at which a NetScaler or a NetScaler virtual appliance is accessed for management. A physical NetScaler or virtual appliance can have only one NSIP. This IP address must be specified when the virtual appliance is configured for the first time. An NSIP address cannot be removed.

Netmask
The subnet mask associated with the NSIP address.

Default gateway
A default gateway must be added on the virtual appliance if it will be accessed through SSH or the configuration utility using an administrative workstation or laptop that is on a different network.

To configure the initial settings on the virtual appliance through the VPX Console using the management application

1. Connect to the VMware ESX server on which the virtual appliance is installed using vSphere Client.
2. In the **Details** pane, on the **Console** tab, log on to the virtual appliance using the administrator credentials.

Note: Both the username and password are “nsroot”.

3. At the prompts, enter the NSIP address, subnet mask and default gateway then save the configuration.

After the initial configuration is set up through the NetScaler VPX Console in the management application, either the NetScaler command-line interface or the configuration utility can be used to complete the configuration or change the initial settings.

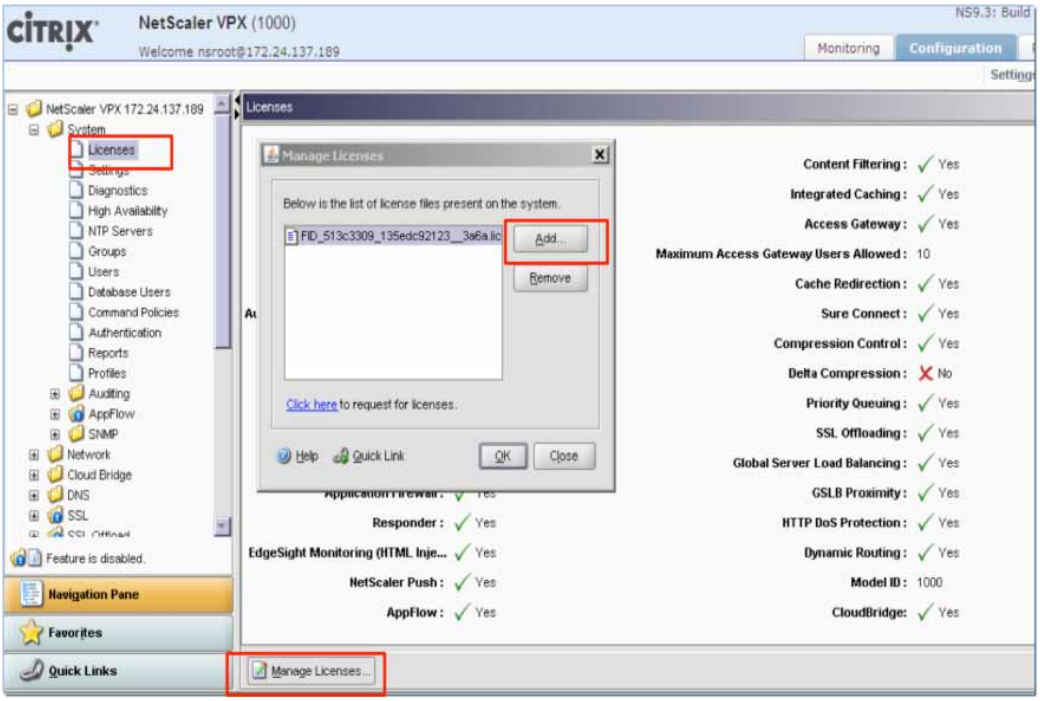
10.2 Installing the license

To install the license

1. Logon to NetScaler VPX using the graphical user interface (GUI) (http://172.24.137.189).
2. Click System > License > Manage license > Add.

The NetScaler VPX automatically reboots.

Figure 6. Interface for installing the license

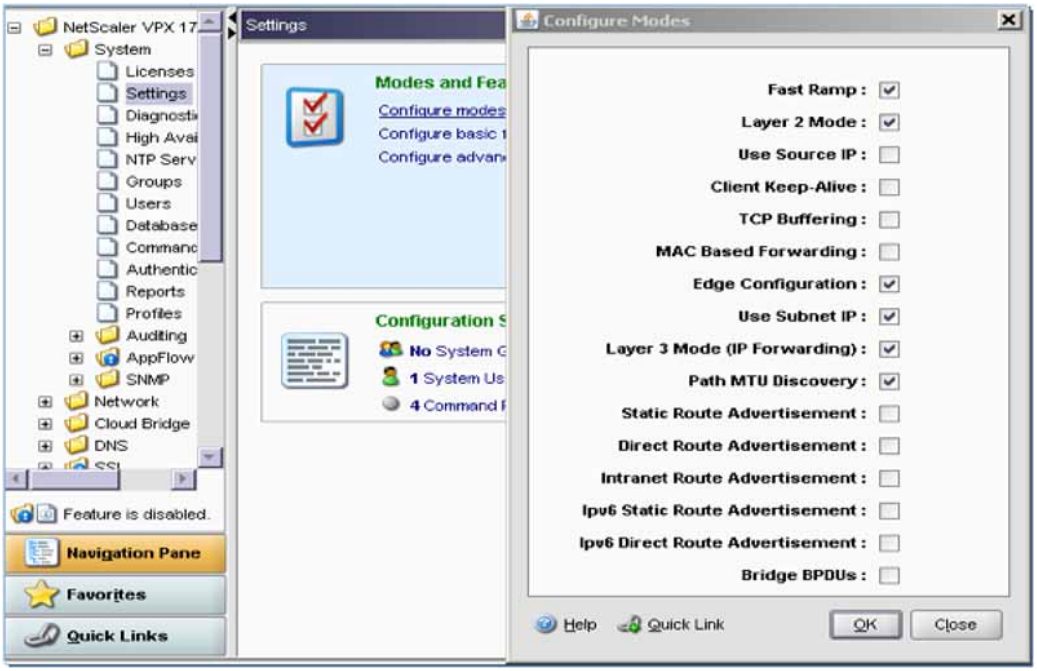


10.3 Enabling NetScaler modes and features

To enable NetScaler modes and features

1. Click System > Settings > Configure modes > Layer 2 Mode.

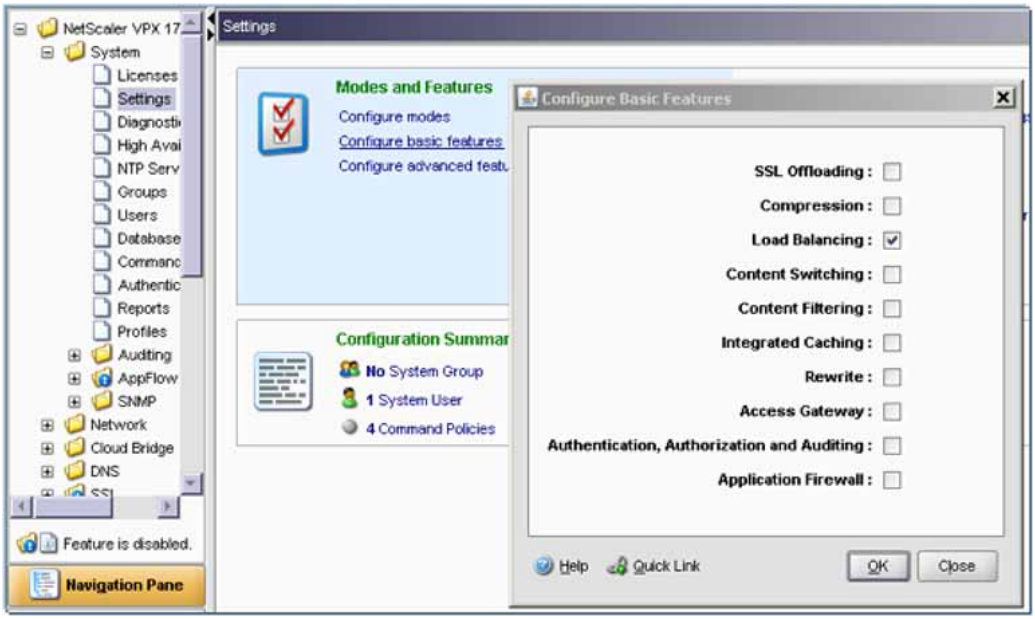
Figure 7. Interface for enabling modes and features



10.4 Enabling load balancing

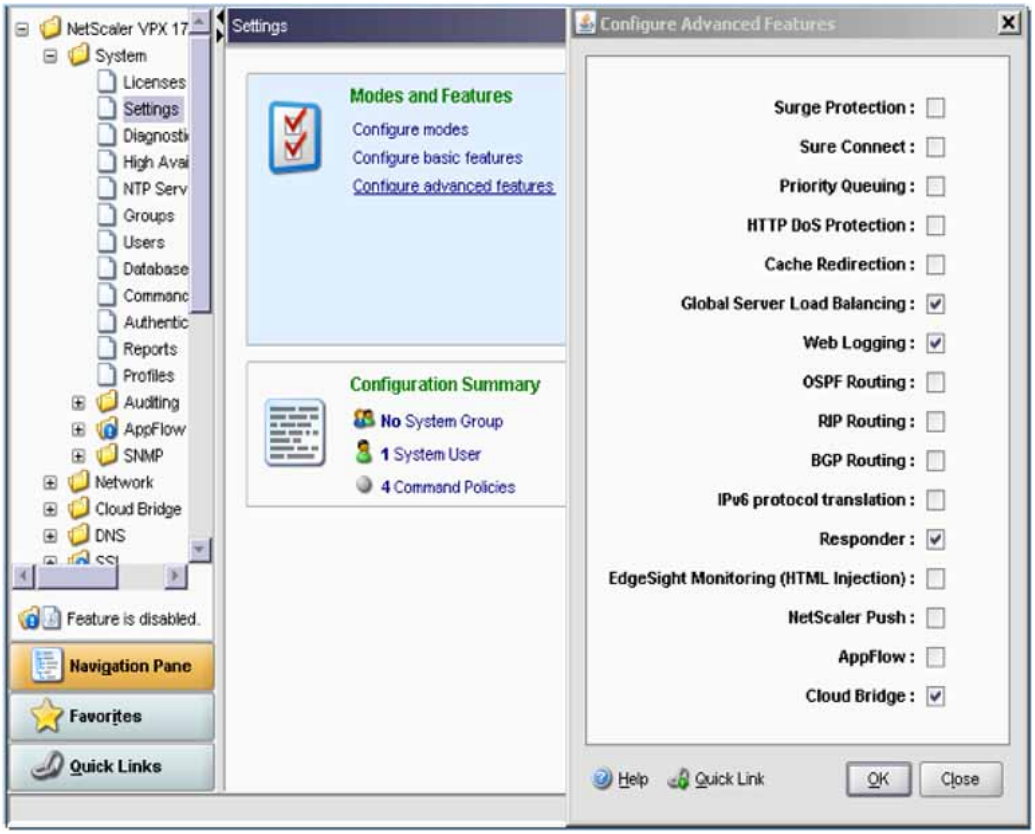
1. Click System > Settings > Configure basic features > Load Balancing.

Figure 8. Interface for enabling load balancing



2. Click System > Settings > Configure advanced features > Global Server Load Balancing.

Figure 9. Interface for enabling GSLB



10.5 Configuring the vSwitch and port group network

Before setting up CloudBridge, the vSwitch and port group network must be set up.

To configure the vSwitch and port group network

1. Logon to vCenter or the VMware ESXi server using the vSphere Client,
2. Click Configuration > Networking > edit vSwitch and port group Network properties > Promiscuous Mode.

Figures 10a and 10b illustrate the vSwitch properties before and after selecting Promiscuous Mode.

Figure 10a. Interface for configuring vSwitch properties

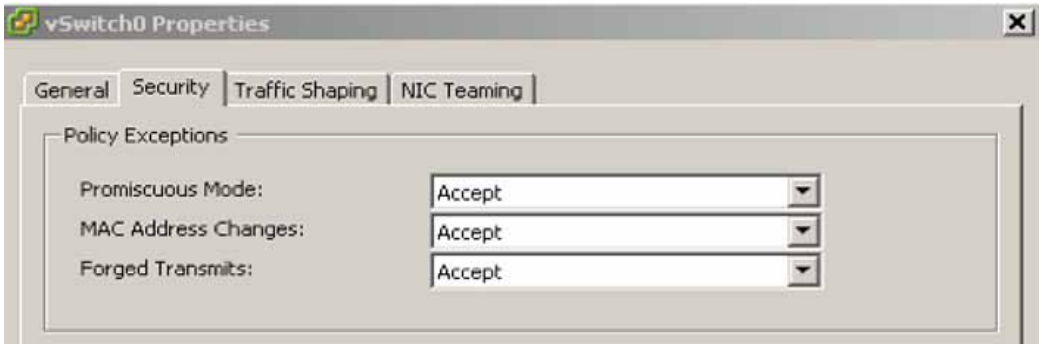
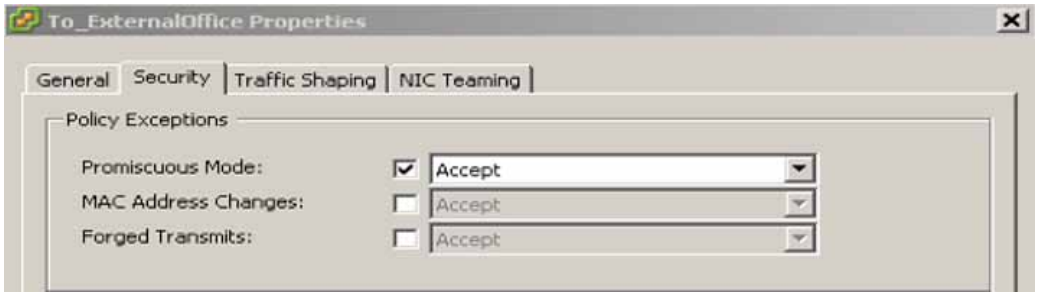


Figure 10b. vSwitch properties after selecting Promiscuous Mode



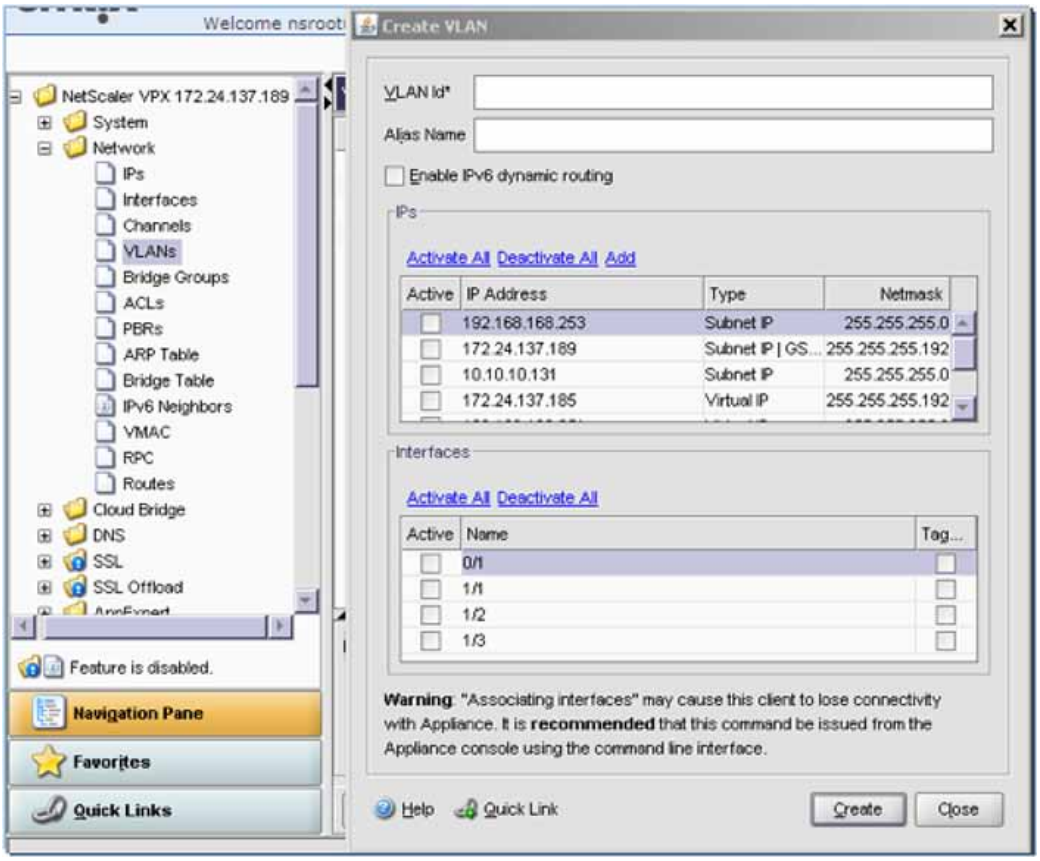
10.6 Configuring the bridge VLAN

The bridge VLAN must be configured before setting up CloudBridge.

To configure the bridge VLAN

1. Click Network > VLAN > Add.
2. Fill in the **VLAN Id** 30 and the port.

Figure 11. Interface for configuring VLAN bridges

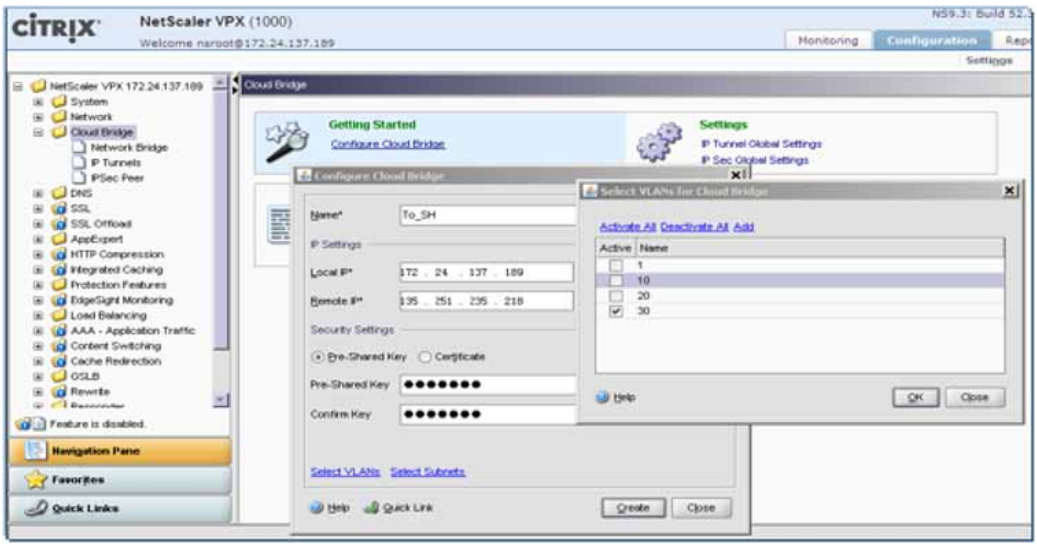


11. SETTING UP CloudBridge

To set up CloudBridge

1. Click CloudBridge > Configure Cloud Bridge.
2. Complete the **IP Settings** and **Pre-shared Key** fields.
3. Click **Select VLANS**.
4. Select bridge VLAN id (30).

Figure 12. Interface for setting up CloudBridge

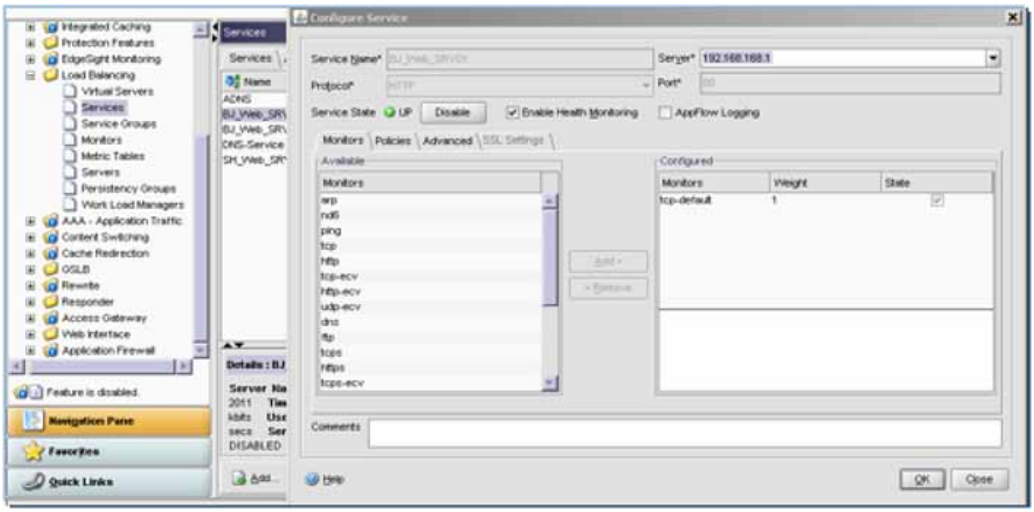


12. SETTING UP LOAD BALANCING

To set up load balancing

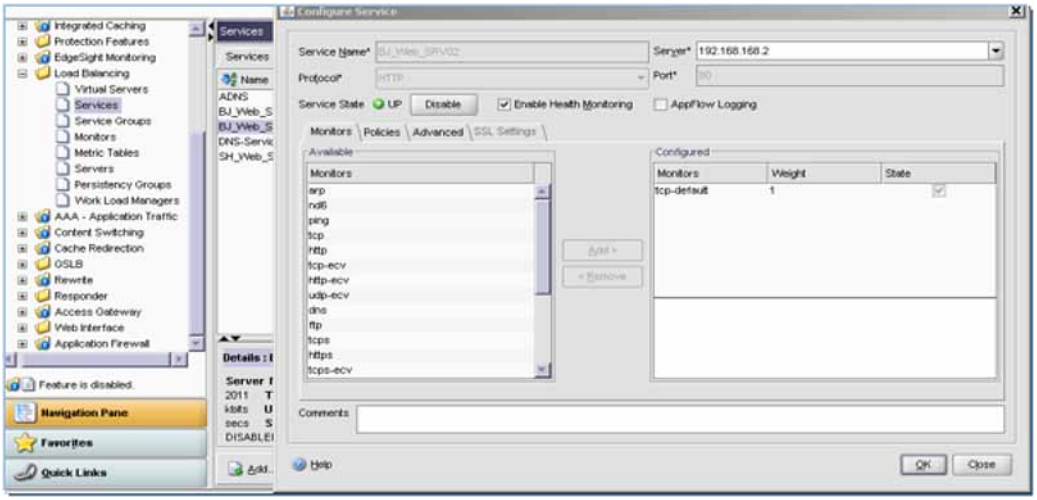
1. To add a service, click Load Balancing > Services > Add.
2. In the **Server** field, fill in the IP address of BJ_Web_SRV01.

Figure 13. Interface for configuring services



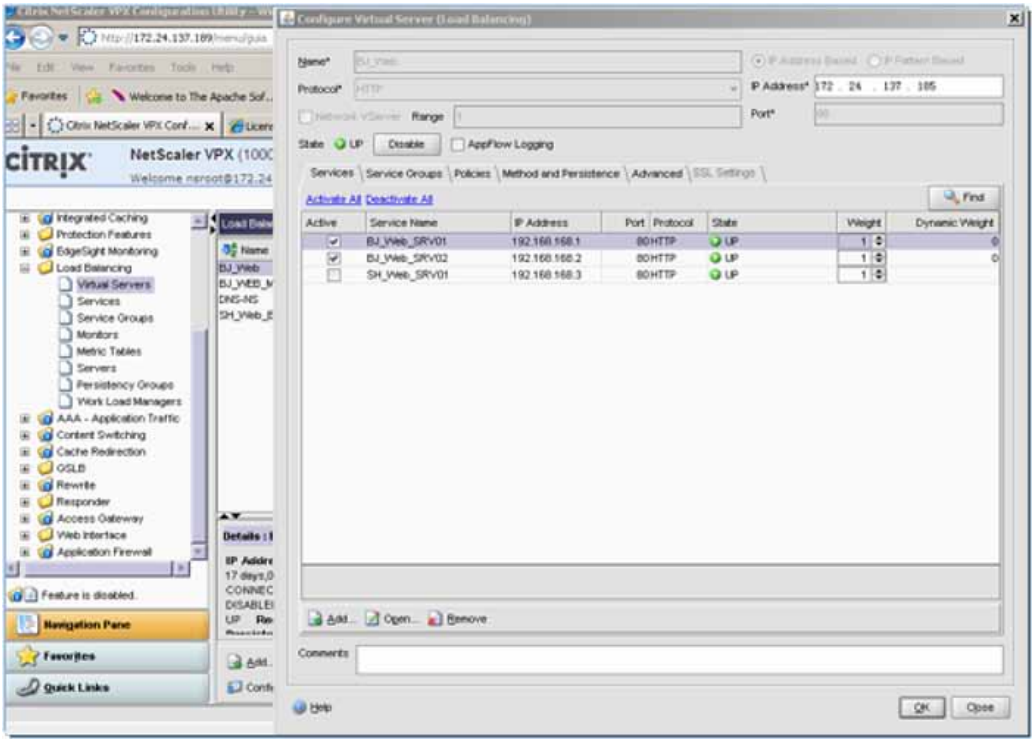
3. To add another service, click Load Balancing > Services > Add.
4. In the **Server** field, fill in the IP address of BJ_Web_SRV02.

Figure 14. Interface for configuring services



5. To add a server, click Load Balancing > Virtual Servers > Add.
6. In the **Server** field, fill in the IP address of the virtual server.
7. Select the web01 and web02 services.

Figure 15. Interface for configuring virtual servers

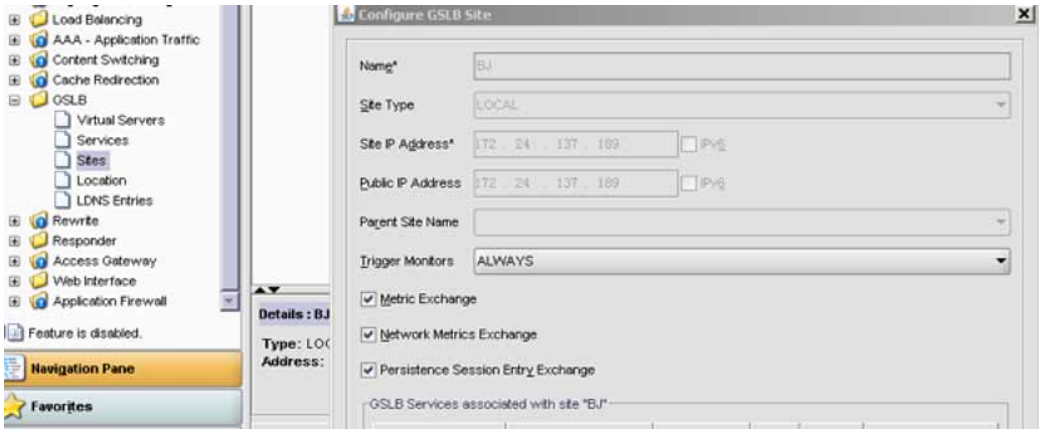


13. SETTING UP GSLB

To set up GSLB

1. To configure the local GLSB site BJ, click GSLB > Sites > Add.
2. Fill in the **Name**, **Site Type** (LOCAL) and **Site IP Address** (external VLAN IP address) fields.

Figure 16. Interface for configuring a local GSLB site



3. Click GSLB > Location > Add.
4. For the site BJ, complete the virtual server IP address and the site client IP address range, using the same location name server and client.

Figure 17a. Interface for creating a location

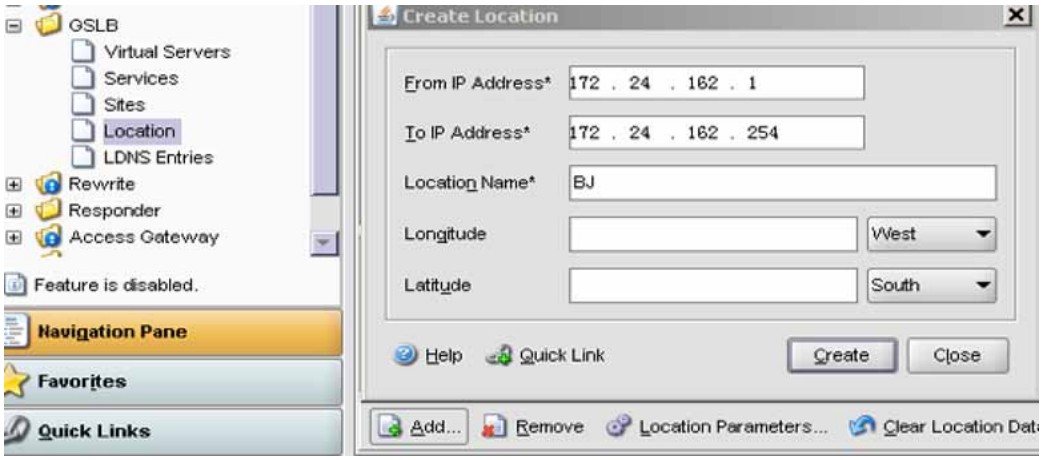
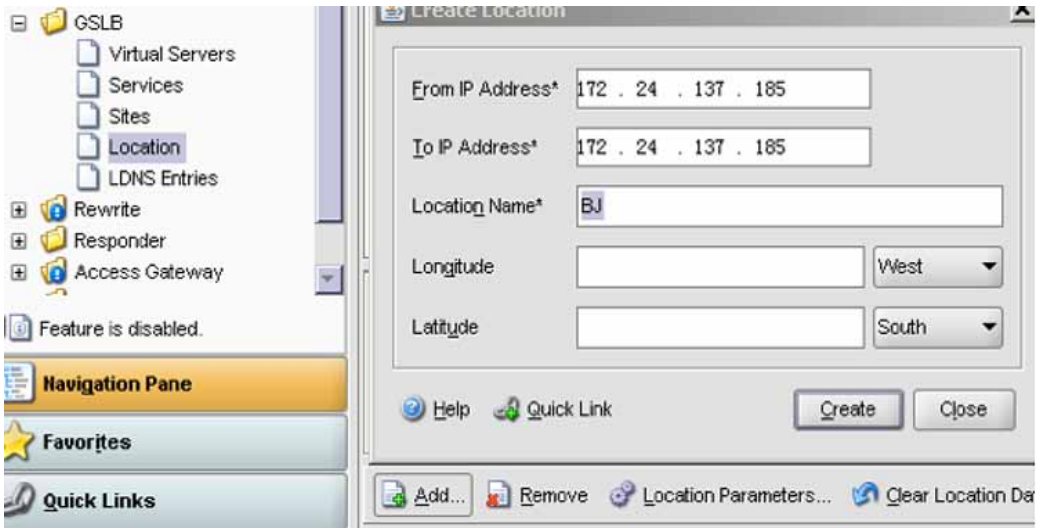


Figure 17b. Interface for creating a location



5. To configure GSLB location SH, click GSLB > Location > Add.
6. For the site SH, fill in the virtual server IP address and create the SH site client IP address range, using the same location name server and client.

Figure 18a. Interface for creating a location

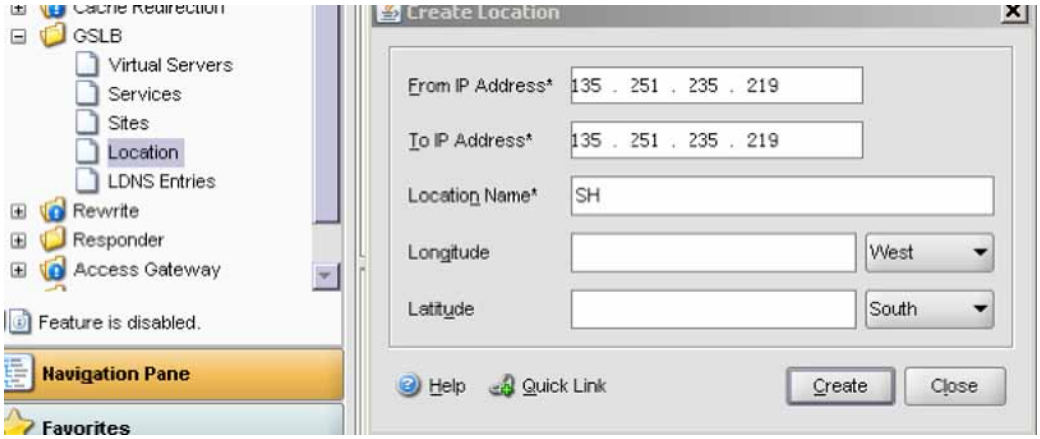
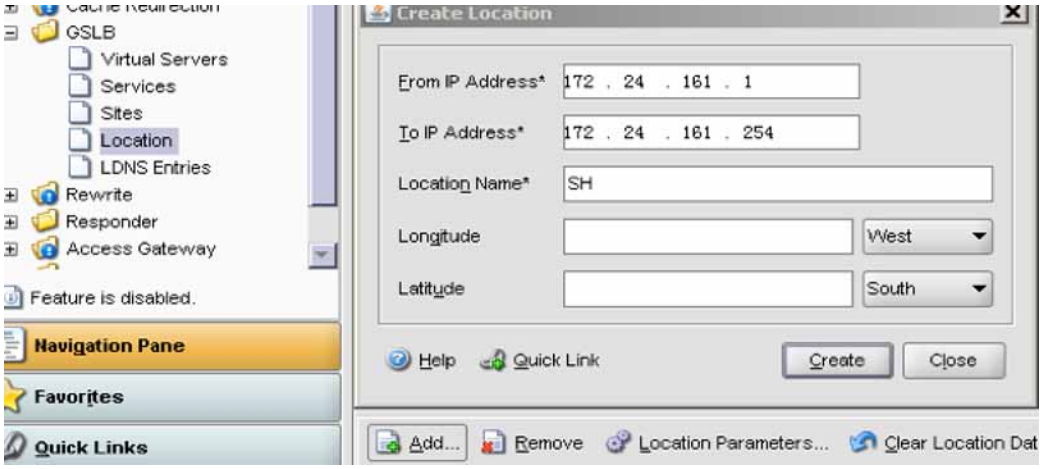


Figure 18b. Interface for creating a location

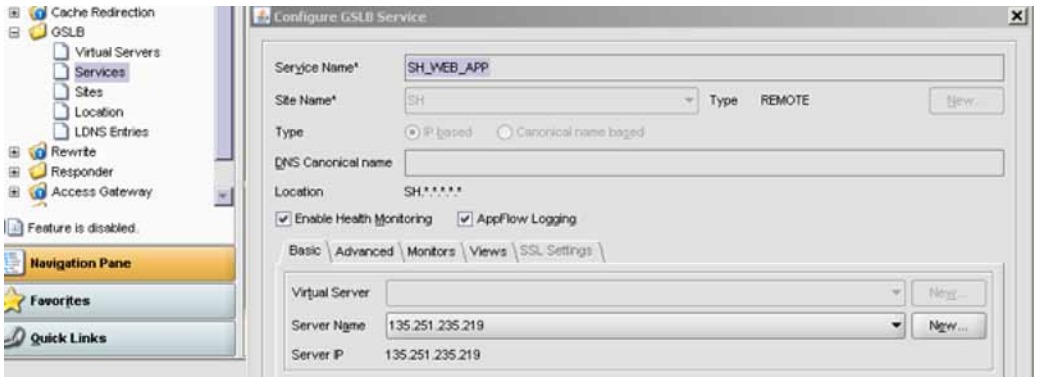


7. To configure GSLB service BJ, click GSLB > Services > Add.
8. Fill in the **Service Name**, **Site Name**, **Type**, **Server Name** and **Server IP** (the BJ site virtual server IP) fields.

Figure 19. Interface for configuring a GSLB service

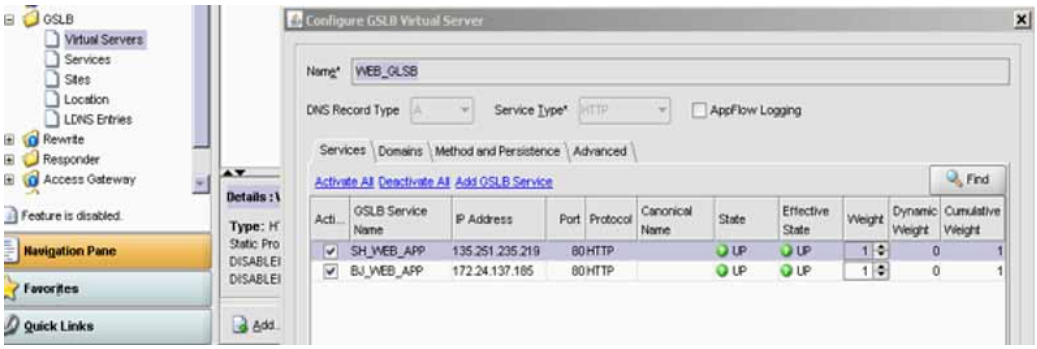
9. To configure the GSLB service SH, click GSLB > Services > Add.
10. Fill in the **Service Name**, **Site Name**, **Type**, **Server Name** and **Server IP** (SH site virtual server IP) fields.

Figure 20. Interface for configuring a GSLB service



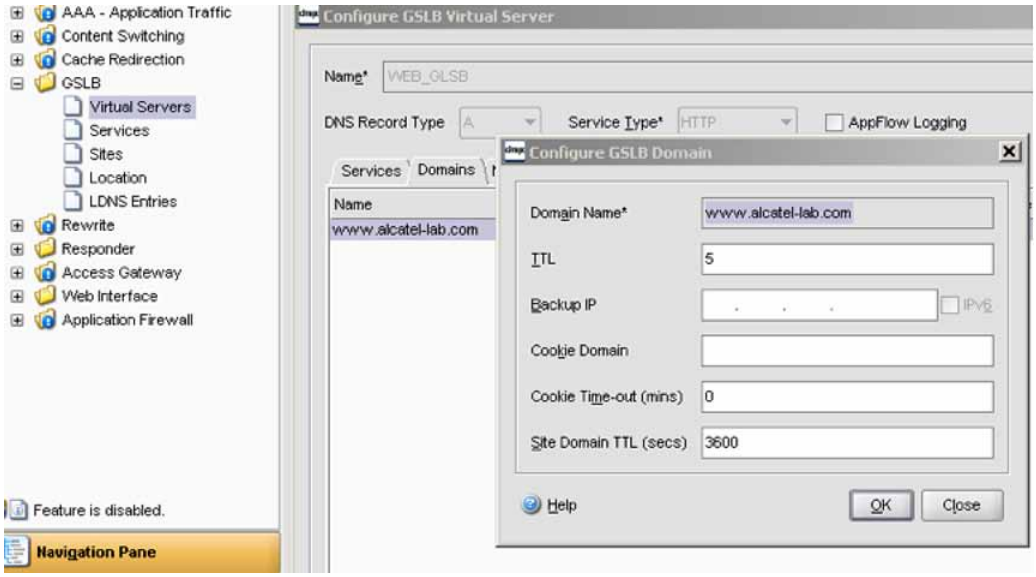
11. To configure the GSLB virtual server, click GSLB > Virtual Servers > Add.
12. Select the service names BJ and SH.

Figure 21. Interface for configuring GSLB virtual servers



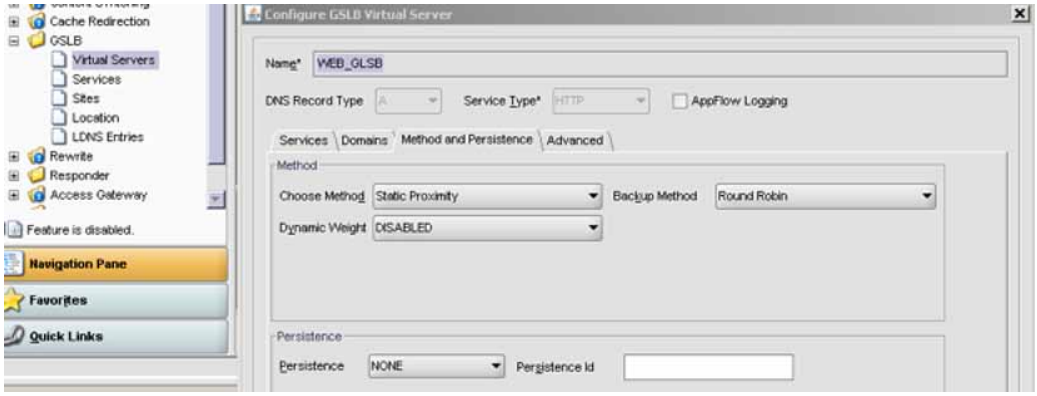
13. To configure GSLB server domains, click GSLB > Virtual Servers > open vServer.
14. Select Domains > Add a domain.
15. Fill in the **Domain Name** www.alcatel-lab.com.

Figure 22. Interface for configuring GSLB domains



16. To configure the GSLB method and persistence, click GSLB > Virtual Servers > open vServer.
17. In the **Choose Method** field, select Static Proximity.

Figure 23. Interface for configuring GSLB method and persistence



ABOUT CITRIX

Citrix Systems, Inc. (NASDAQ:CTXS) is the company transforming how people, businesses and IT work and collaborate in the cloud era. With market-leading cloud, collaboration, networking and virtualization technologies, Citrix powers mobile workstyles and cloud services, making complex enterprise IT simpler and more accessible for 260,000 enterprises. Citrix touches 75 percent of Internet users each day and partners with more than 10,000 companies in 100 countries. Annual revenue in 2011 was $2.21 billion. Learn more at www.citrix.com.

CITRIX®

Alcatel·Lucent
Enterprise