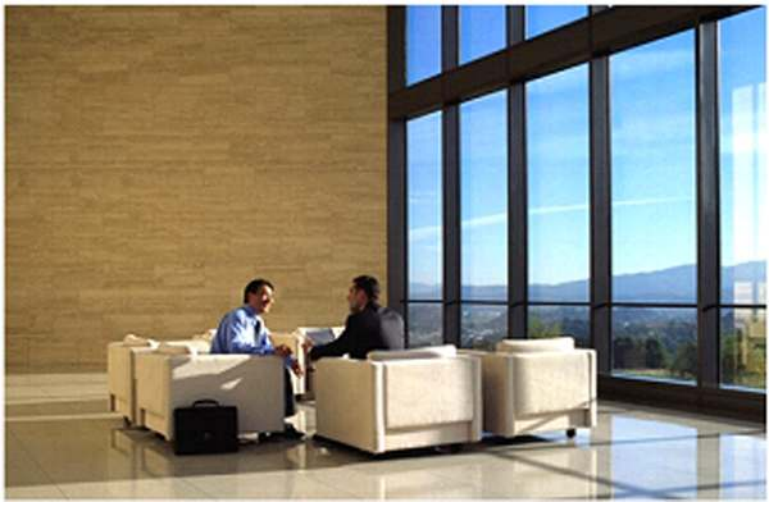
Design Guide

Oracle E-Business Suite 11i with Cisco ACE Series Application Control Engine Deployment Guide, Version 1.0

This design guide describes how to deploy the Cisco® Application Control Engine (Cisco ACE) by Cisco Systems® with the Oracle E-Business Suite 11i (Oracle 11i). This guide was created through the collaborative efforts of Cisco and Oracle as a part of a larger effort to provide Cisco and Oracle solutions to the market. Additional design guides for other product combinations, and other related documents are available from Cisco and Oracle.



Oracle E-Business Suite 11i (Oracle 11i) is a fully integrated, comprehensive suite of business applications for the enterprise that provides better business information for effective decision-making, facilitates the adaptivity needed for optimal responsiveness, and offers the best practices and industry-specific capabilities needed to respond to change and compete more effectively. Oracle 11i dramatically lowers IT and business costs by improving business processes, reducing customizations, decreasing integration costs, and consolidating instances.

The Cisco ACE performs high-performance server load balancing (SLB) among groups of servers, server farms, firewalls, and other network devices, based on Layer 3 as well as Layer 4 through Layer 7 packet information. The ACE can also terminate and initiate SSL-encrypted traffic, which enables it to perform intelligent load balancing while ensuring secure end-to-end encryption. The module is capable of internetworking speeds of 4 Gigabits per second (Gbps) by default, and can achieve speeds of 8 Gbps with the purchase of an upgrade license. a high-performance and feature-rich product that provides application-aware functions on the network, including Layer 4-7 load balancing, TCP optimization, Secure Sockets Layer (SSL) offloading, etc.

Oracle 11i, when deployed with Cisco ACE, provides a solution for enterprises that offers security, scalability, and availability.

This document is a guide for deploying Oracle 11i with Cisco ACE for a multi-tiered architecture.

The network architecture presented in this document meets the functional requirements for Oracle 11i. Additional application optimization technologies such as HTTP compression and dynamic caching are not discussed in this document but can be easily integrated using features of Cisco ACE and other products.

SUMMARY

This document discusses the following features of the application and network architecture:

- The network architecture meets all the functional requirements of the Oracle 11i deployment architecture.
- For this deployment, Oracle 11i (Oracle9i Application Server, Concurrent Manager, and Oracle Forms Server) runs on multiple application front-end servers.
- The data center network architecture (a Cisco ACE module installed in a Cisco Catalyst® 6509-E Multilayer Switch Feature Card [MSFC] router chassis) discussed in this document does not require source Network Address Translation (NAT) for any load-balanced traffic, facilitating implementation and management.
- Bridge mode (transparent mode) implementation of Cisco ACE facilitates application deployment and management.
- Application health-checking, persistence, and adjustable connection timeout capabilities of Cisco ACE facilitate high availability and optimized use of application resources.
- For simplicity, this document shows a single-device deployment only. In real-world settings, redundant designs are deployed to provide high availability.

TERMS AND DEFINITIONS

This section defines of some of the Oracle 11i and Cisco ACE terms relevant to this document.

Oracle E-Business Suite 11i

Following are Oracle E-Business Suite 11i terms relevant to this document:

APPHost	Server that Oracle 11i (Oracle9i Application Server, Concurrent Manager, Oracle Forms Server, and Oracle HTTP Server [OHS]) runs on; provides front-end connectivity functions
DBHost	Servers with the 2-node Oracle Database 10g Enterprise Edition with Oracle Real Application Clusters (RAC) for application data
OHS	Oracle HTTP Server
Service	Group of processes running on a single machine that provides a particular function—for instance, HTTP service
Tier	Grouping of services, potentially across physical machines; a tier represents a logical grouping and can be represented by multiple network segments (subnets), with a particular application (running on multiple physical machines) deployed in each subnet, or multiple applications can be merged into a single network segment

Cisco ACE

Following are Cisco ACE Series Application Control Engine terms relevant to this document:

Probe	Application health checks sent by the load balancer
Rserver	Real server; in a Cisco ACE configuration, it is the physical server
Server farm	Group of rservers running the same applications and providing the same content
Sticky	Mechanism that binds a client to the same server for the duration of a session; also called session persistence
Virtual address	Virtual IP address on the front end of load-balanced applications

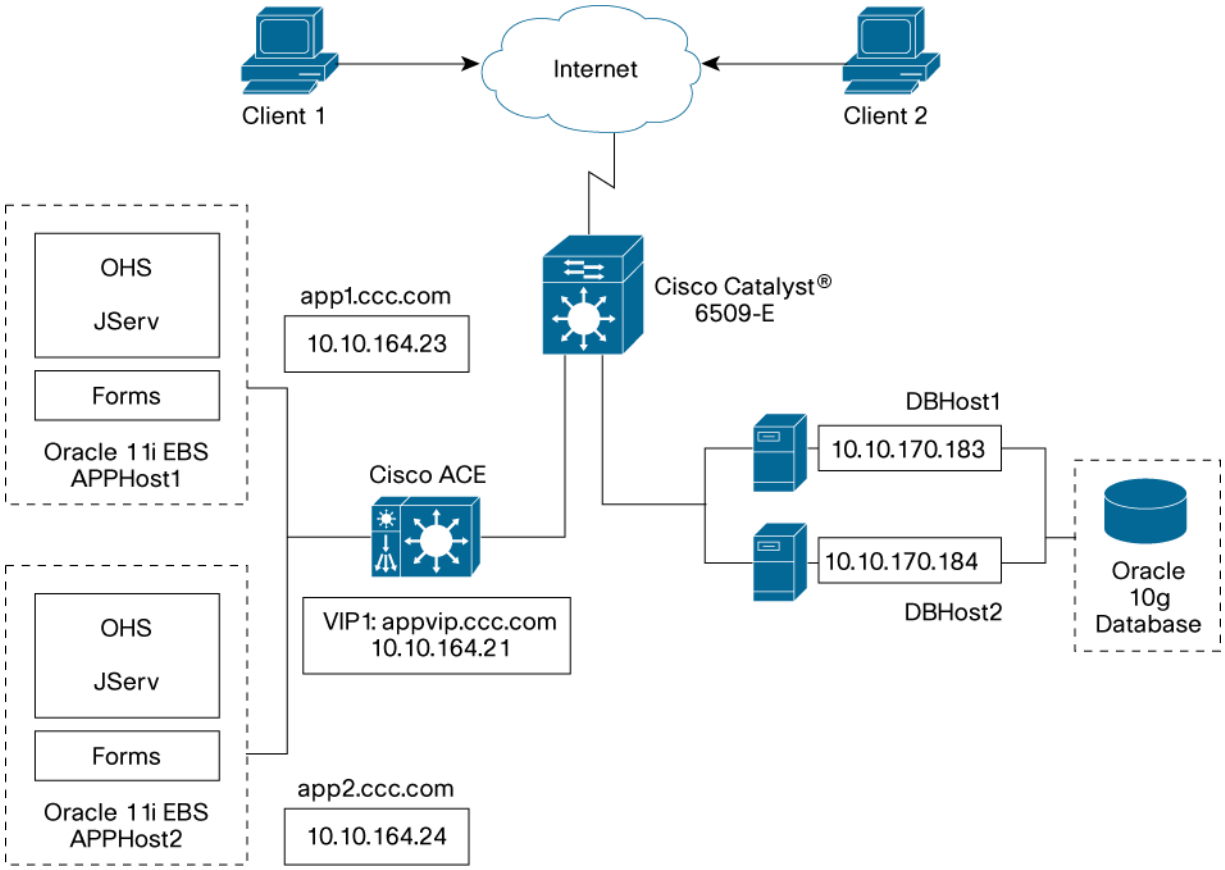
APPLICATION AND NETWORK ARCHITECTURE

Architecture Overview

From the application perspective, the architecture is divided into three tiers: the desktop tier, application tier, and database tier.

- Desktop tier—This tier represents the clients on the Internet or intranet accessing the portal site. The client interface is provided through a Java-enabled Web browser. The desktop client downloads Java applets as needed. In Figure 1, Client 1 and Client 2 represent the desktop tier in this architecture.

Figure 1. Overall Application and Network Architecture



- Application tier—This tier represents the front-end (Web) environment that is directly accessed by external (Internet) clients and internal clients (corporate clients or other Oracle application products). The primary method used to access this tier is plaintext HTTP or SHTTP. In this architecture, the application tier is represented by a single network segment.
  - In Figure 1, Oracle 11i APPHost1 and Oracle 11i APPHost2 provide front-end connectivity functions. The traffic to these two APPHost servers is load balanced by Cisco ACE using VIP1. OHS, JServ, and Forms servers are running on the APPHost servers. APPHost servers also communicate with database servers.
  - The flows to the APPHost servers are discussed in more detail later in this document.

- Database tier—This tier contains database servers, which store all the data maintained by Oracle E-Business Suite 11i. In general, the desktop tier does *not* communicate with database servers directly; however, servers in the application tier communicate with database servers to process certain client requests. Traffic to database servers does not get load balanced in this deployment; therefore, Figure 1 does not show database servers deployed behind Cisco ACE. Hosts included in this tier are DBHost1 and DBHost2. High availability and load balancing of database servers is provided by Oracle RAC.

Application Flows

This section describes the flows for the Oracle 11i APPHost application server suite.

Client to Oracle E-Business Suite 11i

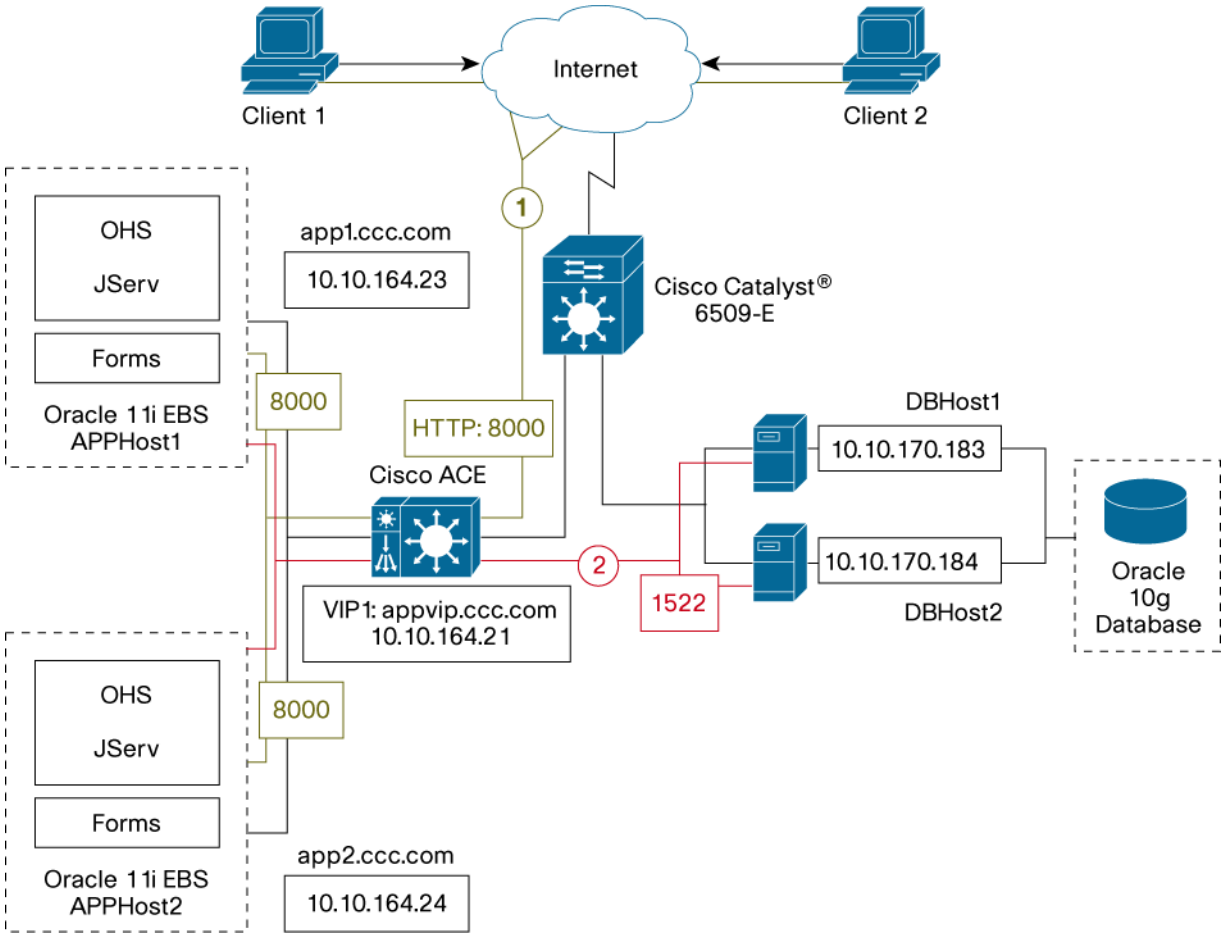
The clients on the Intranet accesses http://appvip.ccc.com:8000, which is configured as VIP1: 10.10.164.21 as on the Cisco ACE. This deployment can be easily configured for HTTPS port 443 if needed.

Cisco ACE load balances the request to one of the available Web (OHS) servers running on Oracle 11i APPHost1 or APPHost2.

Session persistence based on the client source IP address or HTTP cookies should be configured on Cisco ACE for this flow.

This flow is marked as 1 in green in Figure 2.

Figure 2. APPHost (Portal) Flows



Oracle E-Business Suite 11i APPHost to Oracle Database 10g Server

Oracle 11i APPHost1 and APPHost2 make database queries to the database server DBHost1 and DBHost2. The default TCP port is 1521, but for this topology this connection is established on the destination TCP port 1522 (SQL*NET or NET8 as referred to by Oracle) running on the database servers.

This request traverses the network and is routed by Cisco ACE and the router on the network.

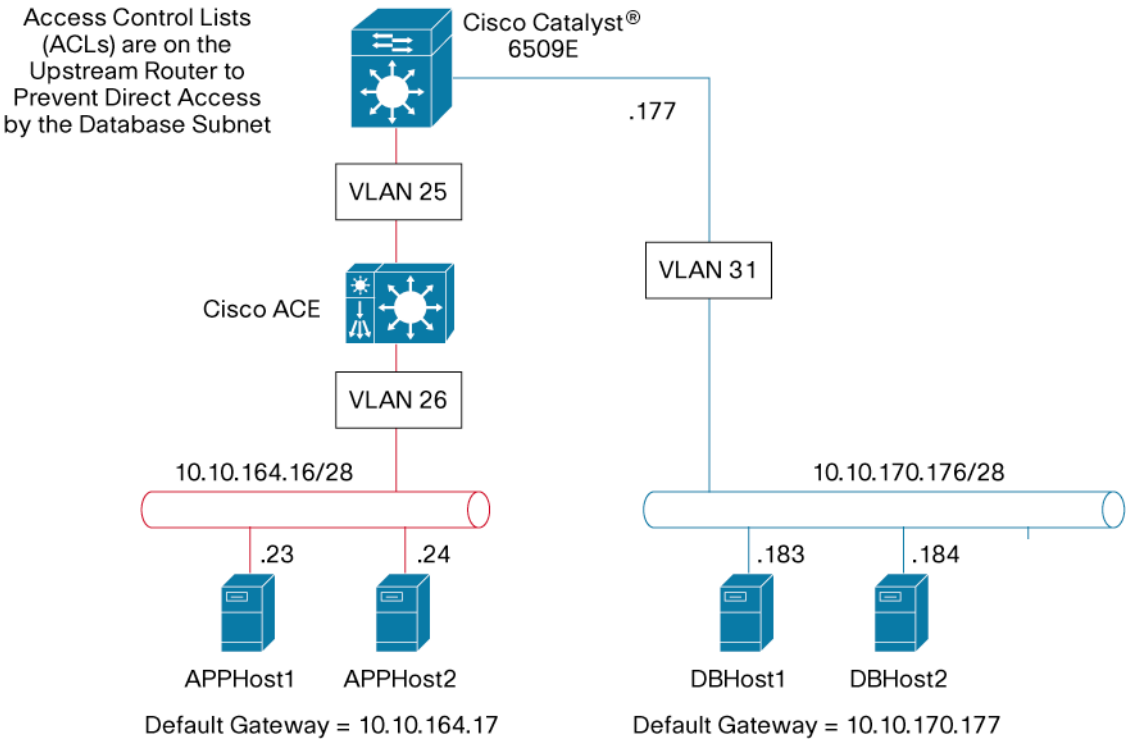
This flow is marked as 2 in red in Figure 2.

NETWORK DESIGN AND CONFIGURATION

Network Topology and Design Features

The logical network topology diagram in Figure 3 shows how Cisco ACE is deployed. Cisco ACE is configured in bridge mode, simply bridging traffic from one VLAN to another (VLAN 25 to 26). Routing between VLANs is managed by the upstream router.

Figure 3. Detailed Network Topology



The following sections describe some of the primary network design features.

1. Bridge Mode

- In this network design, the Cisco ACE module is deployed in bridge mode, which is a simple deployment model.
- In this mode, Cisco ACE acts as a bridge between two VLANs and performs load balancing for traffic destined for the VIP address.
- Each VLAN pair is configured on the switch, but only the client-side VLAN has an IP address on the upstream router.
- The default gateway for the server is configured to point to the upstream router (Hot Standby Router Protocol [HSRP]) IP address for each client-side VLAN.
- Direct server access is possible if security policy allows it.

2. Server Segmentation Using Multiple Subnets

- Each functional group of servers is deployed on its own IP subnet.
- This segmentation provides logical grouping for similar functions and facilitates future expansion.

3. Security Handling by the Upstream Router and Cisco ACE

- ACLs on the upstream router permit wanted traffic to reach Cisco ACE and servers directly.
- ACLs are configured on the upstream router to prevent direct access to database servers.
- Cisco ACE ACLs are configured to allow access to the VIP on application ports.

4. (Optional) SSL Termination on Cisco ACE

- Although not shown in this document, SSL termination on Cisco ACE is easy to configure.
- In this scenario, SSL traffic (port 443) is terminated on the Cisco ACE. Cisco ACE sends plaintext traffic to application servers on the Webcache services port (port 8000).
- The client's source IP address is preserved in this transaction.
- By default, Cisco ACE supports up to 1000 SSL transactions per second (TPS). For higher performance requirements, licenses need to be installed on Cisco ACE.

Server Configuration

Table 1 provides an overview of the servers deployed in this architecture.

Table 1. Server Information

Server Name	IP Address	Subnet Mask	Function	External Listening Ports
Oracle E-Business Suite 11i APPHost1 (app1.ccc.com)	10.10.164.23	255.255.255.240	OHS, JServ, and Forms Server 1	8000
Oracle E-Business Suite 11i APPHost2 (app2.ccc.com)	10.10.164.24	255.255.255.240	OHS, JServ, and Forms Server 1	8000
DBHost1	10.10.170.183	255.255.255.240	Database server 1 for application metadata repository	1522
DBHost1	10.10.170.184	255.255.255.240	Database server 2 for application metadata repository	1522

Note: Table 1 lists the external listening ports for only the flows included in this document. In addition, each application server may have other ports used for administrative access. Those ports also need to be allowed in the ACL configuration. Please refer to Oracle documentation for further details.

Oracle E-Business Suite 11i Configuration

This section describes the Oracle 11i configuration changes needed to allow deployment with Cisco ACE.

At a high level, perform these steps:

Step 1. Install the Oracle E-Business Suite 11i application with a virtual name, or clone the existing application with a virtual name (alias). The virtual name used for this deployment is appvip.ccc.com.

Step 2. After installation or cloning, remove the virtual name and configure Cisco ACE with the same name as the virtual name used for the installation. In this deployment, on Cisco ACE, appvip.ccc.com resolves to VIP1: 10.10.164.21.

Next, make changes on each Oracle E-Business Suite 11i APPHost server to allow the application to use Cisco ACE. In this deployment, two Oracle E-Business Suite 11i APPHost servers are used: Oracle E-Business Suite 11i APPHost1 and Oracle E-Business Suite 11i APPHost2.

- The DNS (host) name for Oracle E-Business Suite 11i APPHost 1 is app1.ccc.com.
- The DNS (host) name for Oracle E-Business Suite 11i APPHost 2 is app2.ccc.com.

Changes need to be made to use the actual host name instead of the virtual host name.

Step 3. Modify $TNS_ADMIN/listener.ora:

```
(ADDRESS= (PROTOCOL= TCP)(Host= app1)(Port= 1621))
```

Step 4. Modify $IAS_ORACLE_HOME/Apache/modplsql/plsql.conf:

```
ProxyPass /pls/http://app1.ccc.com:8000/pls/
```

Step 5. Modify $IAS_ORACLE_HOME/Apache/Apache/conf/oprocmgr.conf:

```
<IfModule mod_oprocmgr.c>
...
   ProcNode app1.ccc.com <oprocmgr_port>
```

oprocmgr_port used here has no relation to the port configured on Cisco ACE (port 8000)

```
...
     <Location />
    Order Deny,Allow
    Deny from all
    Allow from localhost
    Allow from app1
    Allow from app1.ccc.com
   </Location>
```

Step 6. Modify $IAS_ORACLE_HOME/Apache/Apache/conf/httpd_pls.conf:

```
...
 <VirtualHost _default_:*>
   <Location />
...
    Allow from app1
    Allow from app1.ccc.com
  </Location>
</VirtualHost>
...
```

Step 7. Configure a loopback address for the virtual name on the server. A loopback address for the server needs to be added so that any traffic generated by Oracle 11i and intended for itself is looped back properly. Add the loopback entry 127.0.0.1 in /etc/host file for appvip.ccc.com:

```
127.0.0.1       appvip.ccc.com appvip
```


Step 8. Perform steps 3 through 7 to configure app2.ccc.com (instead of app1, use app2, etc.).

Step 9. When configuration is complete, start the application and test the services. The concurrent manager should start on only one node unless Oracle Parallel Concurrent Manager (PCP) is implemented.

Router Configuration

Cisco ACE is installed in a distribution layer Cisco Catalyst 6509-E switch chassis. The MSFC module in the chassis also serves as the upstream router for Cisco ACE.

Follow these steps to configure the upstream router in this deployment:

Step 1. Add Cisco ACE VLANs and the database server VLAN.

For this topology, two Cisco ACE VLANS and one database server VLAN need to be added to the MSFC as follows:

```
vlan 25
 name ACE-APP-CLIENT:10.10.70.164.16/28
!
vlan 26
 name ACE-APP-SERVER
!
vlan 31
 name ACE-DB-SERVERIDM:10.10.165.176/28
```

Note: Name definition is for description purposes only and can be configured based on an organization's naming conventions.

Step 2. Permit VLAN traffic to Cisco ACE

The Cisco ACE will not accept VLAN traffic unless Cisco Catalyst 6509E switch is specifically configured to allow VLANs to access the ACE module. By not allowing all VLANs to access ACE, broadcast storms on non-ACE VLANs have no effect to the ACE. For this deployment, the Cisco ACE is installed in slot 4 in the Cisco Catalyst 6509E chassis. The following configuration needs to be added to allow Cisco ACE-specific VLAN traffic to be directed toward the Cisco ACE:

```
svclc multiple-vlan-interfaces
svclc module 4 vlan-group 11
svclc vlan-group 11  25,26
```

Step 3. Add the switched virtual interface (SVI) configuration.

The SVI configuration defines the Layer 3 instance on the router (the MSFC). For this deployment, two SVIs need to be configured: one on the Cisco ACE client-side VLAN, and one on the database server-side VLAN.

Configure the Cisco ACE client-side VLAN SVI as follows:

```
interface Vlan25
 description ACE-APPSRV-Client-Side
 ip address 10.10.164.17 255.255.255.240
 no ip redirects
 no ip proxy-arp
```


Note: This IP address serves as the default gateway for APPHost servers and Cisco ACE. In a redundant design, this IP address is configured as an HSRP address. Please see the Cisco HSRP Configuration Guide for an example: http://www.cisco.com/en/US/tech/tk648/tk362/technologies_tech_note09186a0080094afd.shtml

Configure the database server-side VLAN SVI as follows:

```
interface Vlan31
 description ACE-APPSRV-Client-Side
 ip address 10.10.170.177 255.255.255.240
 no ip redirects
 no ip proxy-arp
```

Note: This IP address serves as the default gateway for database servers. In a redundant design, this IP address is configured as an HSRP address. Please see the Cisco HSRP Configuration Guide for an example: http://www.cisco.com/en/US/tech/tk648/tk362/technologies_tech_note09186a0080094afd.shtml

Cisco ACE Configuration

Table 2 summarizes configuration information for the Cisco ACE deployment in this architecture.

Table 2. Cisco ACE Configuration Information

Host	Virtual IP Address and Port	Associated Servers	Server Ports	Health Check Mechanism	TCP Optimization Applicable?
appvip.ccc.com:8000	10.10.164.21:8000	10.10.164.23 10.10.164.24	8000 8000	HTTP	Yes

When configuring the Cisco ACE, please refer to Figure 3 earlier in this guide to correlate the configuration steps with the topology.

Step 1: Management Access Configuration

To access the Cisco ACE module remotely using Telnet, Secure Shell (SSH) Protocol, Simple Network Management Protocol (SNMP), HTTP, or HTTPS or to allow Internet Control Message Protocol (ICMP) access to the Cisco ACE module, define a policy and apply it to the interfaces where the access will be performed.

1. Configure class-map of type management:

```
class-map type management match-any remote-access
  10 match protocol ssh any
  20 match protocol telnet any
  30 match protocol icmp any
  40 match protocol http any     (needed if XML interface access)
50 match protocol https any      (needed through HTTP(S))
```

2. Configure policy-map of type management:

```
policy-map type management first-match everyone
  class remote-access
    permit
```


3. Apply policy-map to the VLAN interfaces:

```
interface vlan 25
  service-policy input everyone

interface vlan 26
service-policy input everyone
```

Step 2: Probe Configuration

Cisco ACE uses probe as one of the keepalive methods for verifying the availability of a real server. Several types of probes can be configured on Cisco ACE, but for this deployment, probes of type HTTP are used.

Configure the following probe for this deployment:

```
probe http ACECFG-http
  port 8000
  interval 30
passdetect interval 10
request method head url /index.html      This can be another URI based on the server configuration.
  expect status 200 202
```

Step 3: Real Server Configuration

Rservers are the servers that the load balancer selects, on the basis of various criteria, to send the intended traffic. When configuring an rserver, be aware that the rserver name is case-sensitive. The minimum parameters needed for an rserver configuration are the IP address and the inservice specification.

Configure the following rservers for this deployment:

```
rserver host app1
  ip address 10.10.164.23
  inservice
rserver host app2
  ip address 10.10.164.24
  inservice
```

Step 4: Server Farm Configuration

A server farm is a logical collection of rservers that the load balancer selects on the basis of various criteria. As with rservers, the server farm name is case-sensitive. The minimum parameters needed for server farm configuration are the rserver and probe specifications.

Configure the following server farm for this deployment:

```
serverfarm host aceCFG
  probe ACECFG-http
  rserver app1
    inservice
  rserver app2
    inservice
```


Step 5: Session Persistence (sticky) Configuration

Session persistence, or stickiness, allows multiple connections from the same client to be sent to the same real server by Cisco ACE. Stickiness can be configured based on the source IP address, HTTP cookies, SSL session ID (for SSL traffic only), etc. For this deployment, stickiness is configured based on the source IP address.

To configure stickiness, specify the type (source IP address, cookies, etc.), sticky group name, timeout value, and server farm associated with the sticky group.

Configure the following sticky settings for this deployment (ACECFG-sticky is the sticky group name used for this deployment):

```
sticky ip-netmask 255.255.255.0 address both ACECFG-sticky timeout 720
  serverfarm aceCFG
```

Step 6: Server Load-Balancing Configuration

Cisco ACE uses class-map, policy-map, and service-policy to classify, enforce, and take action on incoming traffic. Traffic trying to reach a VIP address on a specific a port can be classified as Layer 4.

Configure load balancing as follows:

1. Configure the VIP address using class-map of type match-all:

```
class-map match-all VIP-aceCFG
2 match virtual-address 10.10.164.21 tcp eq 8000
```

2. Configure policy-map of type loadbalance to associate sticky-serverfarm:

```
policy-map type loadbalance first-match vip-lb-ACECFG
  class class-default
    sticky-serverfarm ACECFG-sticky
```

3. Configure policy-map of type multi-match to associate class-map configured in step 1:

```
policy-map multi-match lb-vip
  class VIP-aceCFG
    loadbalance vip inservice
  loadbalance vip-lb-ACECFG
```

4. Apply policy-map to the interface VLAN:

```
interface vlan 25
  service-policy input lb-vip

interface vlan 26
service-policy input lb-vip
```


Step 7: Bridge Mode Configuration

The Cisco ACE module doesn't include any external physical interfaces. Instead, it uses internal VLAN interfaces. An interface on the Cisco ACE can be configured as either routed or bridged. Bridge mode configuration allows simplified deployment of the Cisco ACE. In this deployment VLAN 25 faces toward the client side and VLAN 26 faces toward the real server side.

The following configuration steps are needed to implement bridge mode configuration on the Cisco ACE:

1. Access List Configuration

An access control list (ACL) must be configured on every interface in order to permit connections. Otherwise, the Cisco ACE denies all traffic on the interface. For this deployment, two access lists named PERMIT_ALL are configured to permit IP and ICMP traffic on interface VLANs. The access list named PERMIT_ALL is assigned for security policies on interface VLAN 25 to allow direct access to real servers; the same access list is also assigned for security policies on interface VLAN 26 in order to permit traffic between real servers and also to access other networks from the real servers. The following configuration permits all IP and ICMP traffic on desired interface VLANs, but Cisco ACE can be easily configured to filter incoming/outgoing traffic on the interface VLANs based on criteria such as source address, destination address, protocol, protocol specific parameters, and so on if required by the Customers.

```
access-list PERMIT_ALL line 5 extended permit ip any any
access-list PERMIT_ALL line 6 extended permit icmp any any
```

2. VLAN Interfaces Configuration

For bridge mode configuration, both client-side and server-side VLANs need to be configured. The interface VLANs share a common bridge group. ACLs and load-balancing service policy are also associated with the interface VLANs.

Configure the interface VLANs for this deployment as follows:

```
interface vlan 25
  bridge-group 1
  access-group input PERMIT_ALL
  service-policy input everyone
  service-policy input lb-vip
  no shutdown
interface vlan 26
  bridge-group 1
  service-policy input everyone
  service-policy input lb-vip
  no shutdown
```

3. Bridge group Virtual Interface (BVI) Configuration

The BVI configuration defines the Layer 3 instance of the bridge group. The BVI configuration allows the bridging of traffic between the two VLANs. The interface number is the same as for bridge-group defined in step 2.

Configure the BVI for this deployment as follows:

```
interface bvi 1
  ip address 10.10.164.20 255.255.255.240
no shutdown
```


Step 8: Default Gateway Configuration

To access remote machines and respond to client requests on other networks, a default route needs to be configured for each Layer 3 interface VLAN that needs to be load balanced. The default gateway for Cisco ACE points to the IP address of the Layer 3 interface on the upstream router. In redundant designs, it points to the HSRP address instead of the interface address.

The following is the default gateway configuration for Cisco ACE for interface VLAN 25:

```
ip route 0.0.0.0 0.0.0.0 10.10.164.17
```

Configure a separate gateway for every additional interface that needs to be load balanced. For example, configure a separate gateway for interface VLAN 32 in a pair with VLAN 32 and 33.

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the Cisco.com Website at www.cisco.com/go/offices.

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus • Czech Republic Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Printed in USA C07-362648-00 09/06