CHAPTER 3

Configuring Virtualization

This chapter describes how to configure virtualization for the Cisco Application Control Engine (ACE) module.

This chapter contains the following sections:

Information About Virtualization

After reading this chapter, you should have a basic understanding of ACE virtualization and be able to partition your ACE into multiple virtual devices or virtual contexts (VCs) for more efficient operation.

Virtualization allows you to create a virtual environment in which a single ACE is partitioned into multiple virtual devices, each functioning as an independent ACE that is configured and managed independently.

You set up virtualization by performing the following configuration steps:

- Configure resource allocation for a virtual context
- Create a virtual context
- Configure access to the virtual context

An example virtual environment will be used throughout this guide, with the user context VC_WEB, for the web traffic through the network. This user context will be associated with the custom resource class RC_WEB.

In this chapter, you will create a virtual context. In subsequent chapters, you will create a virtual server within the virtual context. The virtual server is associated with a server farm and real servers. The example setup is shown in Table 3-1.

Table 3-1 Example Virtual Context

Virtual Context	Virtual Server	Server Farm	Real Servers
VC_WEB	VS_WEB	SF_WEB	RS_WEB1
			RS_WEB2
			RS_WEB3
			RS_WEB4

Before you begin configuring your ACE for virtualization, you should become familiar with a few concepts: virtual context, Admin and user contexts, and resource classes.

With ACE virtualization, you can create a virtual environment, called a virtual context, in which a single ACE appears as multiple virtual devices, each configured and managed independently. A virtual context allows you to closely and efficiently manage system resources, ACE users, and the services that you provide to your customers.

By default, the ACE initially provides you an Admin context, with the ability to define up to five user contexts. With additional licenses, you can define up to a maximum of 251 contexts: one Admin context and 250 user contexts.

As the system administrator, you have full system administrator access to configure and manage the Admin context and all user contexts. Each context can also have its own administrator and log-in mechanism that provides access only to the specific context. When you log in to the ACE using the console or Telnet, you are authenticated in the Admin context.

Although virtualization allows you to create multiple contexts, in the physical world, you still have a single ACE with finite resources, such as the number of concurrent connections. To address this limitation, the ACE provides resource classes that allow you to manage each virtual context's access to physical ACE resources. A resource class is a definition of what portion of an ACE's overall resources will be assigned, at a minimum or maximum, to any given context. One resource class may be associated with one or more contexts.

The ACE is preconfigured with a default resource class for the Admin context. This default resource class is applied to all virtual contexts that you create. It allows a maximum of 100 percent access to all resources by all virtual contexts. When a resource is being used to its maximum limit, the ACE will deny additional requests for that resource from any other virtual contexts. To avoid oversubscribing resources and to help guarantee that resource availability is shared among multiple virtual contexts, you create custom resource classes and associate them with the virtual contexts that you define.

Licensing Requirements for Virtual Contexts

By default, your ACE provides an Admin context and five user contexts that allow you to use multiple contexts if you choose to configure them. To increase the number of user contexts up to a maximum of 250, you must obtain a separate license from Cisco.

Table 3-2 shows the licensing requirements for increasing the number of virtual contexts in your ACE.

Table 3-2 ACE Virtualization Licensing Options

Feature	License Model	Description
Virtualization	ACE-VIRT-020	20 virtual contexts.
	ACE-VIRT-050	50 virtual contexts.
	ACE-VIRT-100	100 virtual contexts.
	ACE-VIRT-250	250 virtual contexts.
	ACE-VIRT-UP1	Upgrades 20 to 50 contexts.
	ACE-VIRT-UP2	Upgrades 50 to 100 contexts.
	ACE-VIRT-UP3	Upgrades 100 to 250 contexts.

For details about licensing, see the *Administration Guide, Cisco ACE Application Control Engine*.

Configuring a Virtual Context

This section describes how to configure a virtual context and it contains the following topics:

Task Flow for Configuring a Virtual Context

Follow these steps to configure a virtual context:

Step 1 Configure a resource class.

Step 2 Create a virtual context.

Step 3 Assign a management VLAN interface to the context.

Step 4 Configure remote management access to the user context.

Step 5 Configure the client-side VLAN interface.

Step 6 Configure the server-side VLAN interface.

Configuring a Resource Class

Note By default, the Admin context is a member of the default resource class. To ensure that the Admin context resources are not depleted by other virtual contexts and that the context will be guaranteed a minimum amount of resources, we recommend that you create a separate resource class, allocate the resources that you estimate will be required by the Admin context, and make the Admin context the only member.

Procedure

	Command	Purpose
Step 1	**telnet** *ip_address* **Example:** **Telnet 172.25.91.110** host1 login: admin Password: Cisco Application Control Software (ACSW) TAC support: http://www.cisco.com/tac Copyright (c) 2002-2009, Cisco Systems, Inc. All rights reserved. The copyrights to certain works contained herein are owned by other third parties and are used and distributed under license. Some parts of this software are covered under the GNU Public License. A copy of the license is available at http://www.gnu.org/licenses/gpl.html. switch/Admin#	Logs you in to the ACE as the system administrator from the console. At the prompt, enter **admin** and then the new password you entered in Step 3 in the "Sessioning and Logging in to the ACE from the Supervisor Engine" section in Chapter 2, Setting Up an ACE.
Step 2	**config** **Example:** host1/Admin# config host1/Admin(config)#	Enters configuration mode.
Step 3	**resource-class** *name* **Example:** host1/Admin(config)# resource-class RC_WEB host1/Admin(config-resource)#	Creates a resource class.
Step 4	**limit-resource all minimum** *number* **maximum unlimited | equal-to-min** **Example:** host1/Admin(config-resource)# limit-resource all minimum 10 maximum equal-to-min	Limits the resources of a context to 10 percent of the total resources available on the ACE.

	Command	Purpose
Step 5	**exit** **Example:** host1/Admin(config-resource)# exit host1/Admin(config)#	Exits resource configuration mode.
Step 6	**do copy running-config startup-config** **Example:** host1/Admin(config)# do copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

Creating a Virtual Context

Procedure

	Command	Purpose
Step 1	**context** *context_name* **Example:** host1/Admin(config)# context VC_WEB host1/Admin(config-context)#	Creates a new context.
Step 2	**allocate-interface vlan** *vlan_id* **Example:** host1/Admin(config-context)# allocate-interface vlan 60 host1/Admin(config-context)# allocate-interface vlan 400 host1/Admin(config-context)# allocate-interface vlan 500 host1/Admin(config-context)# allocate-interface vlan 1000	Associates existing VLAN 400 and VLAN 500 with the context so that the context can receive traffic classified for it. VLAN 60 and VLAN 1000 will be used later when you configure redundancy.
Step 3	**member** *class_name* **Example:** host1/Admin(config-context)# member RC_WEB	Associates the context with the resource class that you created in the "Configuring a Resource Class" section.
Step 4	**exit** **Example:** host1/Admin(config-context)# exit	Exits context configuration mode.
Step 5	**do show running-config context** **Example:** host1/Admin(config)# do show running-config context	Displays the virtual context configuration.

	Command	Purpose
Step 6	**do show running-config resource-class** **Example:** host1/Admin(config)# do show running-config resource-class	Displays the resource class configuration.
Step 7	**do copy running-config startup-config** **Example:** host1/Admin(config)# do copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

Configuring Remote Management Access to the User Contexts

Before remote network access can occur on the user context through Telnet or SSH, you must create a traffic policy that identifies the network management traffic that can be received by the ACE.

Procedure

	Command	Purpose
Step 1	**changeto** Example: host1/Admin# changeto VC_WEB host1/VC_WEB#	Changes to the VC_WEB user context.
Step 2	**config** **Example:** host1/VC_WEB# config host1/VC_WEB(config)#	Enters configuration mode.
Step 3	**class-map type management match-any** *name* **Example:** host1/VC_WEB(config)# class-map type management match-any REMOTE_ACCESS host1/VC_WEB(config-cmap-mgmt)#	Creates a management-type class map named REMOTE_ACCESS that matches any traffic.
Step 4	**description** *string* **Example:** host1/VC_WEB(config-cmap-mgmt)# description Remote access traffic match	(Optional) Provides a description for the class map.
Step 5	**match protocol** *protocol* **any** **Example:** host1/VC_WEB(config-cmap-mgmt)# match protocol ssh any host1/VC_WEB(config-cmap-mgmt)# match protocol telnet any host1/VC_WEB(config-cmap-mgmt)# match protocol icmp any	Configures the match protocol to permit traffic based on the SSH, Telnet, and ICMP protocols for any source address.

	Command	Purpose

Step 6	**exit**
	
	Example:
	`host1/VC_WEB(config-cmap-mgmt)# exit`
	`host1/VC_WEB(config)#`
		Exits class map management configuration mode.

Step 7	**policy-map type management first-match** *name*
	
	Example:
	`host1/VC_WEB(config)# policy-map type management first-match REMOTE_MGMT_ALLOW_POLICY`
	`host1/VC_WEB(config-pmap-mgmt)#`
		Creates a REMOTE_MGMT_ALLOW_POLICY policy map for traffic destined to an ACE interface.

Step 8	**class** *name*
	
	Example:
	`host1/VC_WEB(config-pmap-mgmt)# class REMOTE_ACCESS`
	`host1/VC_WEB(config-pmap-mgmt-c)#`
		Applies the REMOTE_ACCESS class map to this policy.

Step 9	**permit** **Example:** `host1/VC_WEB(config-pmap-mgmt-c)# permit`	Allows the ACE to receive the configured class map management protocols.

Step 10	**exit**
	
	Example:
	`host1/VC_WEB(config-pmap-mgmt-c)# exit`
	`host1/VC_WEB(config-pmap-mgmt)# exit`
	`host1/VC_WEB(config)#`
		Exits policy map management class configuration mode.

Step 11	**service-policy input** *policy_name* **Example:** `host1/VC_WEB(config)# service-policy input REMOTE_MGMT_ALLOW_POLICY`	In configuration mode, applies the REMOTE_MGMT_ALLOW_POLICY policy map globally to all interfaces in the user context. You can also apply a remote management policy to a VLAN. In this topology, you could apply the management policy to either VLAN 400 (client-side VLAN) or VLAN 500 (server-side VLAN).

Step 12	**exit**
	
	Example:
	`host1/VC_WEB(config-if)# exit`
	`host1/VC_WEB(config)#`
		Exits interface configuration mode.

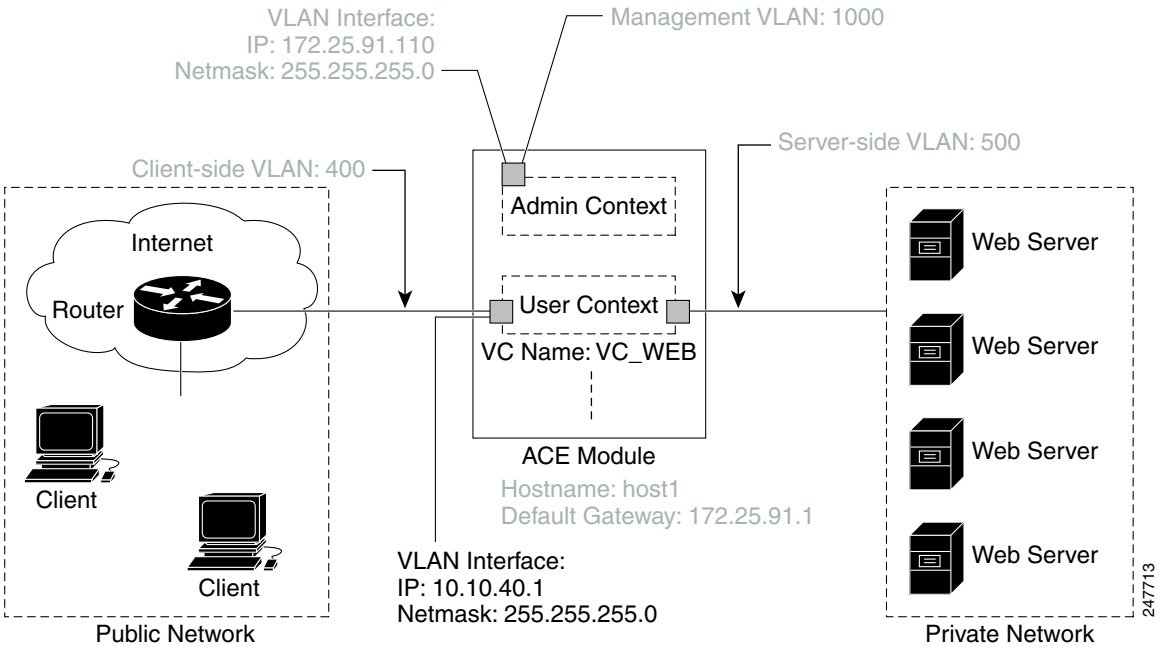
Step 13	**do show service-policy** *policy_name* **Example:** `host1/VC_WEB(config)# do show service-policy REMOTE_MGMT_ALLOW_POLICY`	Displays the REMOTE_MGMT_ALLOW_POLICY policy applied to all interfaces in the context.

	Command	Purpose
Step 14	**do show running-config** **Example:** host1/VC_WEB(config)# do show running-config	Displays the running configuration.
Step 15	**do copy running-config startup-config** **Example:** host1/VC_WEB(config)# do copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration in the VC_WEB context.

Configuring the Client-Side VLAN Interface

At this point, you can configure a client-side VLAN interface, the address to which the client traffic is sent, as shown in Figure 3-1.

Figure 3-1 Configuring the Client-Side VLAN Interface



Procedure

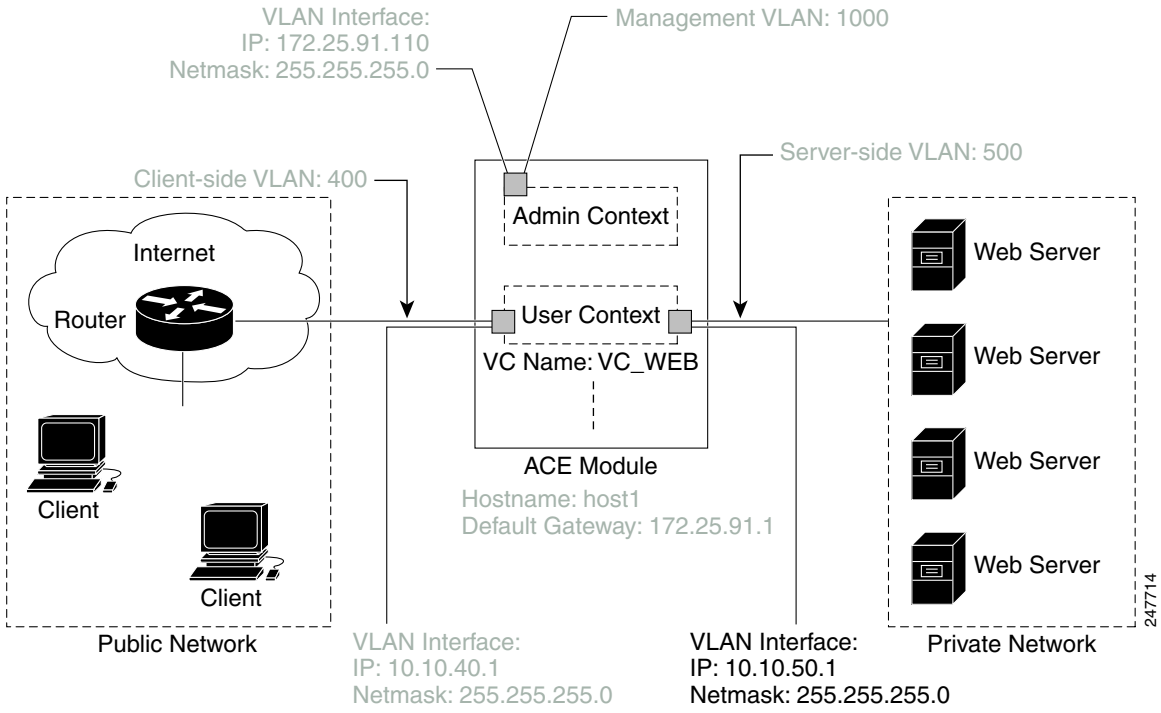
	Command	Purpose
Step 1	**interface vlan** *vlan_id* **Example:** host1/VC_WEB(config)# interface vlan 400 host1/VC_WEB(config -if)#	Accesses interface configuration mode in the VC_WEB context for client-side VLAN 400.
Step 2	**ip address** *ip_address netmask* **Example:** host1/VC_WEB(config-if)# ip address 10.10.40.1 255.255.255.0	Assigns an IP address of 10.10.40.1 and a subnet mask of 255.255.255.0 to the VLAN interface for management connectivity.
Step 3	**description** *string* **Example:** host1/VC_WEB(config-if)# description Client connectivity on VLAN 400	(Optional) Provide a description for the interface.
Step 4	**no shutdown** **Example:** host1/VC_WEB(config-if)# no shutdown	Enables the VLAN interface.
Step 5	**do show interface vlan** *vlan_id* **Example:** host1/VC_WEB(config-if)# do show interface vlan 400	Shows that VLAN 400 is active.
Step 6	**do show arp** **Example:** host1/VC_WEB(config-if)# do show arp	Displays the ARP table. **Note** The Address Resolution Protocol (ARP) allows the ACE to manage and learn the mapping of IP to Media Access Control (MAC) information to forward and transmit packets.
Step 7	**exit** **Example:** host1/VC_WEB(config-if)# exit host1/VC_WEB(config)#	Exits interface configuration mode.
Step 8	**do copy running-config startup-config** **Example:** host1/Admin(config)# do copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

Configuring the Server-Side VLAN Interface

Next, you can configure a server-side VLAN interface, the address to which the server traffic is sent, and a NAT pool as shown in Figure 3-2.

Note Network Address Translation (NAT) is designed to simplify and conserve IP addresses. It allows private IP networks that use unregistered IP addresses to connect to the Internet. You configure a NAT pool for the ACE so that the ACE exposes only one address for the entire network to the outside world. This pool, which hides the entire internal network behind that address, offers both security and address conservation.

Figure 3-2 Configuring the Server-Side VLAN Interface



Procedure

	Command	Purpose
Step 1	**interface vlan** *vlan_id* **Example:** host1/VC_WEB(config)# interface vlan 500 host1/VC_WEB(config -if)#	Accesses interface configuration mode in the VC_WEB context for server-side VLAN 500.
Step 2	**ip address** *ip_address netmask* **Example:** host1/VC_WEB(config-if)# ip address 10.10.50.1 255.255.255.0	Assigns an IP address of 10.10.50.1 and a subnet mask of 255.255.255.0 to the VLAN interface for management connectivity.

	Command	Purpose
Step 3	**description** *string* **Example:** host1/VC_WEB(config-if)# description Server connectivity on VLAN 500	(Optional) Provides a description for the interface.
Step 4	**no shutdown** **Example:** host1/VC_WEB(config-if)# no shutdown	Enables the VLAN interface.
Step 5	**do show interface vlan** *vlan_id* **Example:** host1/VC_WEB(config-if)# do show interface vlan 500	Shows that VLAN 500 is active.
Step 6	**do show arp** **Example:** host1/VC_WEB(config-if)# do show arp	Displays the ARP table. **Note** The Address Resolution Protocol (ARP) allows the ACE to manage and learn the mapping of IP to Media Access Control (MAC) information to forward and transmit packets.
Step 7	**exit** **Example:** host1/VC_WEB(config-if)# exit host1/VC_WEB(config)# exit host1/VC_WEB#	Exits interface configuration mode. Exits configuration mode.
Step 8	**copy running-config startup-config** **Example:** host1/Admin# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

Configuring a Default Route for the Virtual Context

Because the ACE does not share configurations across contexts, you must configure a default route for each virtual context that you create. For details about creating a default route, see the "Configuring a Default Route" section. The default route used for this virtual context is 172.25.91.1. See the configuration example at the end of this chapter.

Configuration Examples for Configuring a Virtual Context

The following examples show how to configure a virtual context. The two examples are for the Admin context and the VC_WEB virtual context, respectively. The commands that you have configured in this chapter are shown in bold text.

Admin Context Configuration Example

The following example shows the running configuration of the Admin context with the commands that you have configured in this chapter in bold text.

```
host1/Admin# show running-config

Generating configuration....

login timeout 0

resource-class RC_WEB
  limit-resource all minimum 10.00 maximum equal-to-min

class-map type management match-any REMOTE_ACCESS
  description Remote access traffic match
  2 match protocol telnet any
  3 match protocol ssh any
  4 match protocol icmp any

policy-map type management first-match REMOTE_MGMT_ALLOW_POLICY
  class REMOTE_ACCESS
    permit

interface vlan 1000
  description Management connectivity on VLAN 1000
  ip address 172.25.91.110 255.255.255.0
  service-policy input REMOTE_MGMT_ALLOW_POLICY
  no shutdown

ip route 0.0.0.0 0.0.0.0 172.25.91.1

context VC_WEB
  allocate-interface vlan 60
  allocate-interface vlan 400
  allocate-interface vlan 500
  allocate-interface vlan 1000
  member RC_WEB

username admin password 5 $1$JwBOOUEt$jihXQiAjF9igwDay1qAvK.  role Admin domain
default-domain
username www password 5 $1$xmYMkFnt$n1YUgNOo76hAhg.JqtymF/  role Admin domain
default-domain
```

VC_WEB Configuration Example

The following example shows the running configuration of the VC_WEB user context with the commands that you have configured in this chapter in bold text.

```
host1/Admin# changeto VC_WEB
VC_WEB/Admin# show running-config

Generating configuration....

class-map type management match-any REMOTE_ACCESS
  description Remote access traffic match
  2 match protocol ssh any
  3 match protocol telnet any
  4 match protocol icmp any

policy-map type management first-match REMOTE_MGMT_ALLOW_POLICY
  class REMOTE_ACCESS
    permit

service-policy input REMOTE_MGMT_ALLOW_POLICY

interface vlan 400
  description Client connectivity on VLAN 400
  ip address 10.10.40.1 255.255.255.0
  no shutdown
interface vlan 500
  description Server connectivity on VLAN 500
  ip address 10.10.50.1 255.255.255.0
  no shutdown

ip route 0.0.0.0 0.0.0.0 172.25.91.1
```

Where to Go Next

In this chapter, you have partitioned your ACE into an Admin context and a user context (VC_WEB). Each of the virtual contexts is now associated with a resource class that is appropriate to its intended use. You have also configured a management VLAN interface, as well as the client and server VLAN interfaces in the user context.

In the next chapter, you will configure an access control list (ACL) to secure your network and to permit traffic to enter the ACE.