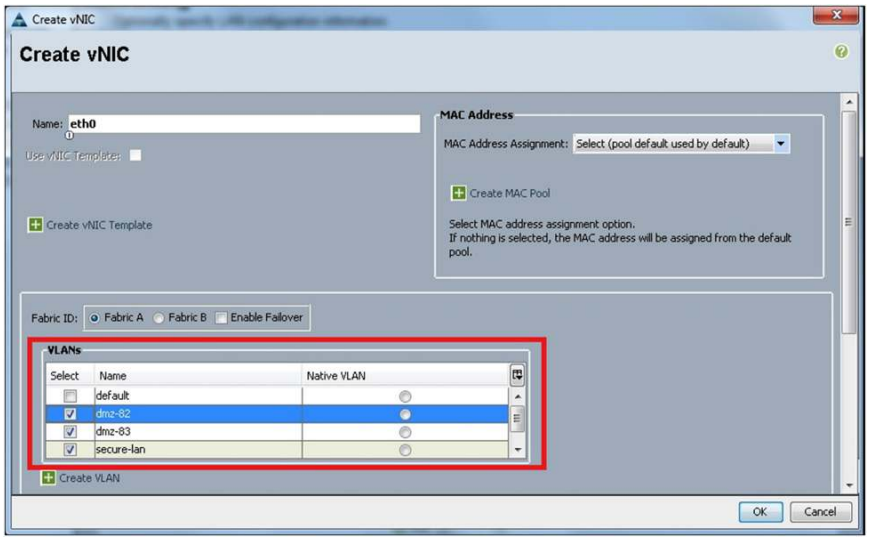
Configure Cisco UCS Organization-Aware VLANs to Restrict Network Access

What You Will Learn

Cisco UCS® Manager Release 2.0 allows users to configure service profiles to access any upstream VLAN, independent of the service profile's organization. This unrestricted access to networking resources increases the likelihood of user errors and the impact of erroneous or malicious configurations. Figure 1. shows the Cisco UCS 2.0 Create vNIC wizard with a complete list of the VLANs accessible to the target fabric. Using this wizard, a user could configure a service profile to access VLANs that are intended to be restricted, in violation of the company's network security policies. Because Cisco UCS Manager 2.0 does not have knowledge of the customer's network access policies, it is unable to prevent this configuration. Ideally, Cisco UCS Manager would provide a means for network administrators to restrict access to network resources based on their company's security policies. After they are configured, these access privileges would be used to simplify configuration and prevent access to restricted network resources. This function is provided by the Organization-Aware (Org-Aware) VLAN feature, the topic of this document.

Figure 1. The Cisco UCS Manager 2.0 Create vNIC Wizard Provides Unfiltered Access to VLANs



The Org-Aware[1] VLAN feature provides the capability to restrict access to VLANs based on user-configured VLAN access permissions and the organization that contains the service profile. This document discusses the Org-Aware VLAN feature and how customers can use it to meet their security requirements. It also discusses best practices for greenfield (new) and brownfield (existing) Cisco Unified Computing System™ (Cisco UCS) deployments. The Org-Aware VLAN feature is introduced as part of Cisco UCS Manager Release 2.1 and is supported by all versions of Cisco UCS hardware.

[1] An organization, or org, is a Cisco UCS administrative domain.

Background

This section provides an overview of Cisco UCS organizations and policy resolution, which are fundamental to understanding the Org-Aware VLAN feature.

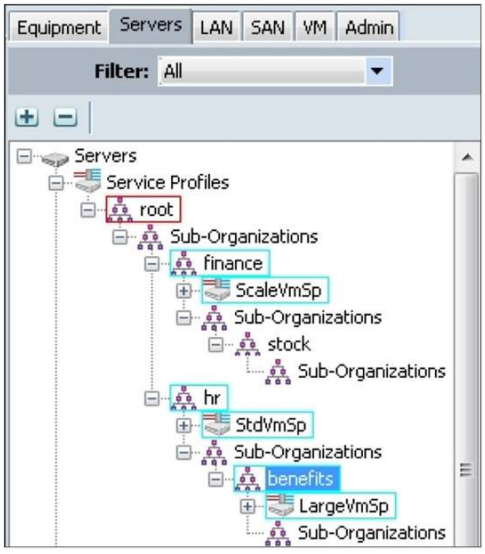
Organizations and Policy Resolution

Cisco UCS organizations are administrative domains to which privileged users can assign physical and logical resources. These resources include policies, pools, and physical infrastructure. Users create organizations and assign resources to them to provide a logical separation between the resources of different groups and to restrict access to these resources. For example, a Cisco UCS administrator can create organizations named **hr** and **finance** for the human resources and finance groups, respectively. In this way, each group can independently maintain and control its own policies without affecting the other group. To prevent other groups from configuring resources in an organization, Cisco UCS locales can be used. For example, an administrator can create a locale for the **hr** organization and assign it to the server, storage, and network administrators of the human resources group. Thus, only users assigned to the locale would be able to configure policies in this organization.

There are no privileges required to access policies because policy access cannot be configured[2]. Policy access is restricted only by the policy's containment hierarchy: that is, a policy is accessible only from its organization or descendent organizations. Thus, if a policy is created in the **hr** organization, it can be used only by service profiles in this organization or its suborganizations.

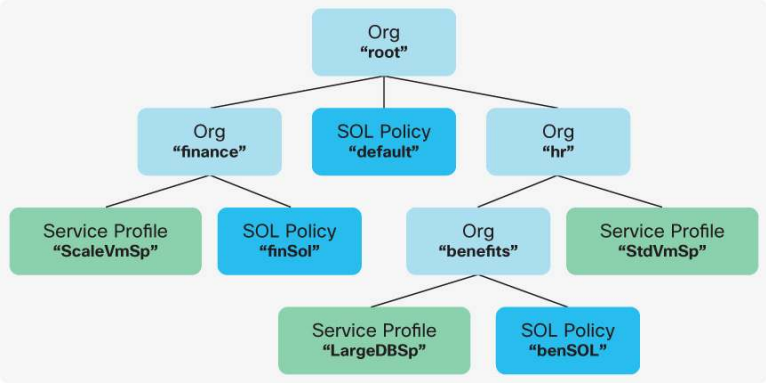
Figure 2. shows the Cisco UCS GUI view of an organization hierarchy. A simplified logical view of the same hierarchy is provided in Figure 3. This example illustrates policy access using service profiles that reference serial-over-LAN (SOL)[3] policies. The same policy access rules apply to all Cisco UCS policies.

Figure 2. Cisco UCS View of Organization Hierarchy



[2] Access here means the capability to refer to the policy from a service profile.
[3] SOL is a mechanism that enables input and output of a serial port to be redirected over IP. Cisco UCS SOL policies are used to configure SOL settings for servers.

Figure 3. Logical View of Cisco UCS Organizations with Contained Policies



According to Cisco UCS policy resolution rules, the following statements apply to policy access:

- All service profiles have access to SOL policy **default**.
- The SOL policy **benSOL** is accessible only to service profiles in the **benefits** organization.
- The SOL policy **finSOL** is accessible only to service profiles in the **finance** organization.

This example demonstrates the use of organization hierarchies to limit access to policies. The Org-Aware VLAN feature uses organizations to restrict access to VLANs.

Feature Overview

This section provides an overview of the Org-Aware VLAN feature followed by examples of Org-Aware VLAN configuration in brownfield and greenfield deployments.

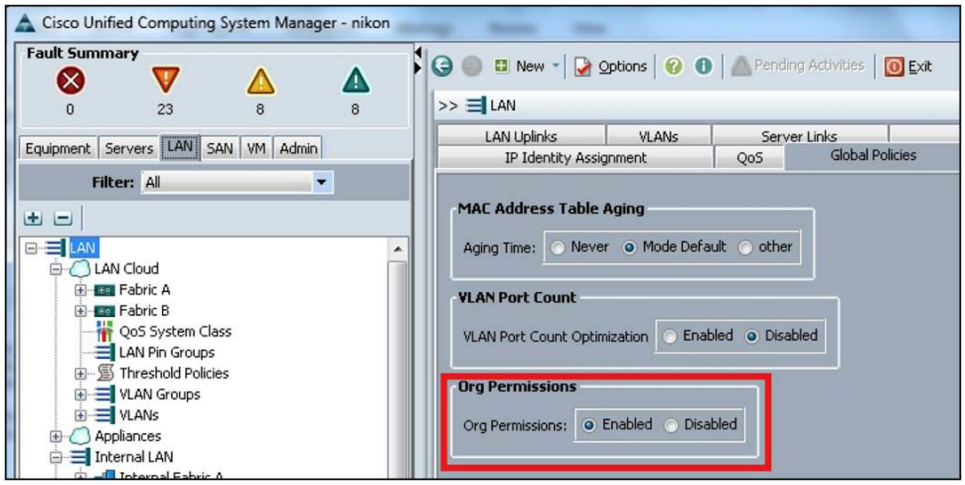
Enabling and Disabling Org-Aware VLANs

The Org-Aware VLAN feature is part of Cisco UCS Manager 2.1. To preserve backward compatibility and help ensure that server traffic is not interrupted during system upgrades, this feature is disabled by default. Thus, after you upgrade to Cisco UCS 2.1, service profiles have unrestricted access to all VLANs[4].

This feature can be enabled by navigating to the LAN tab, opening the Global Policies panel, and selecting the Org Permissions Enabled button, as shown in Figure 4.

[4] This behavior is the same as in Cisco UCS Manager 2.0.

Figure 4. The Org-Aware VLAN Feature Can Enabled or Disabled from the LAN Tab



After Org Permissions is enabled, VLAN permissions and VLAN group permissions determine VLAN access within an organization. For greenfield Cisco UCS deployments that require VLAN access restrictions, you should enable this feature prior to network configuration. For brownfield Cisco UCS deployments that require VLAN access restrictions, you should enable this feature after the network access configuration is complete. This way, there is no risk of server traffic interruption. These conventions are followed in the examples provided.

VLAN Permissions

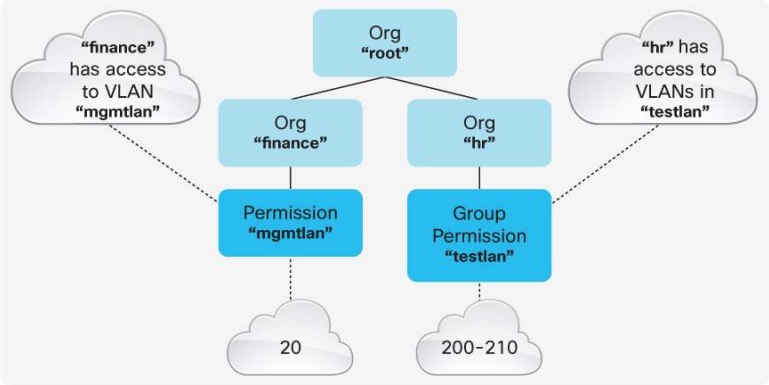
A VLAN permission is a user-configurable object that indicates that a named VLAN is accessible from the containing organization and its suborganizations. VLAN permissions can be created during VLAN creation and they can also be created or deleted for existing VLANs.

VLAN Group Permissions

A VLAN group permission is a user-configurable object that indicates that a VLAN group can be accessed by the containing organization and its suborganizations. VLAN group permissions can be created during VLAN group creation, and they can also be created or deleted for existing groups.

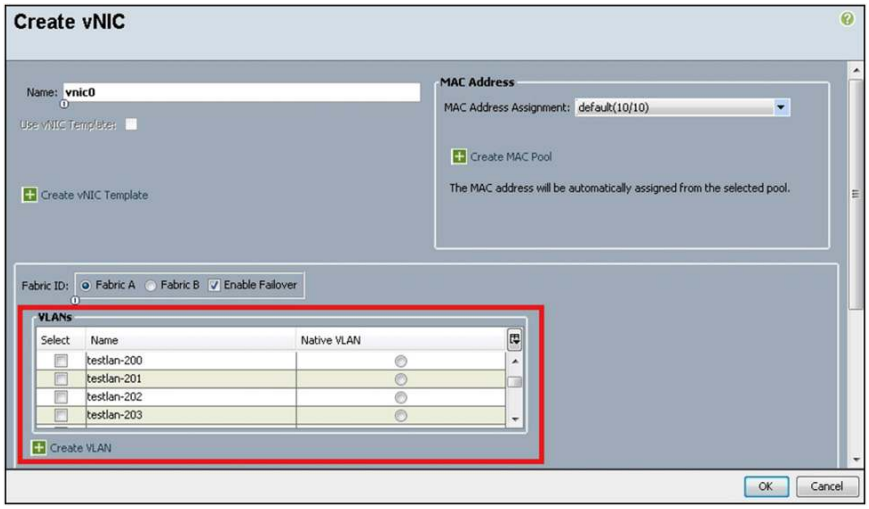
Figure 5 illustrates the logical use of VLAN permissions and VLAN group permissions. The organization **org-root/org-finance** has a VLAN permission named **mgmtlan**, providing access to all VLANs with the name **mgmtlan** (in this case, a VLAN with ID 20). The organization **org-root/org-hr** contains a VLAN group permission named **testlan**. Thus, it has access to all the VLANs in the group **testlan**. In this case, the VLAN group **testlan** contains VLANs with IDs 200 to 210.

Figure 5. Logical View of Organization Permissions and Group Provisions Providing Access to VLANs



Typically, the network administrator is responsible for configuring the VLANs, VLAN permissions, and VLAN group permissions consistent with the company's security practices. After they are configured, these permissions restrict the VLANs that service profiles can access. During service profile configuration, the server administrator's list of VLANs will be filtered to include only the VLANs that are accessible from the service profile's organization. For example, the virtual network interface card (vNIC) creation wizard shown in Figure 6 has transparently filtered the VLAN list to include only VLANs accessible from the hr organization. This filtering simplifies the configuration task and helps prevent erroneous or malicious configurations.

Figure 6. The Create vNIC Wizard Displays Only VLANs Accessible from the **hr** Organization



Configuration Warnings and Faults

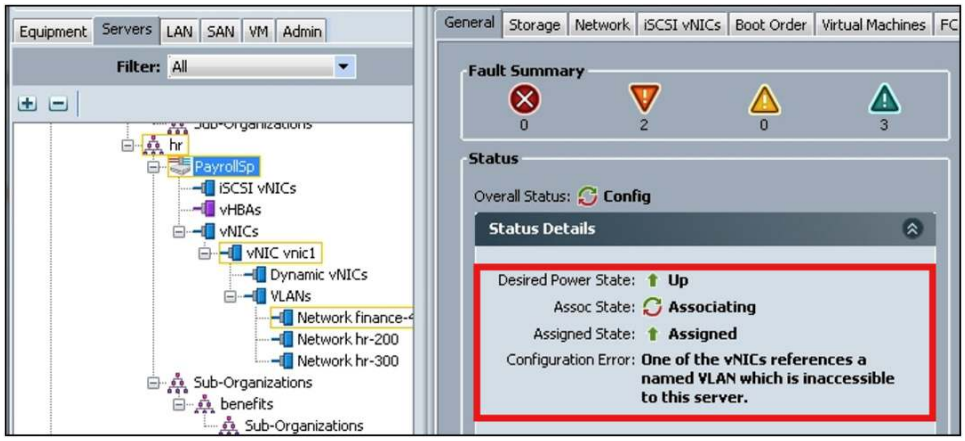
The Cisco UCS GUI will prevent a user from configuring a service profile's vNICs from using inaccessible VLANs. However, it is still possible to configure a service profile's vNICs to use inaccessible VLANs depending on the order and method of configuration[5]. In the scenario in which a vNIC is configured to access a VLAN without the required permissions, Cisco UCS does the following:

[5] For example, by using the command-line interface (CLI) because the CLI does not restrict VLAN selection. Also, this situation may occur if a VLAN permission is created or deleted after a vNIC has been configured to use it.

- Sets the vNIC's operational VLAN as the **default** VLAN
- Raises the critical fault **inaccessible-vlan-referenced** on the offending vNIC
- Raises a configuration warning for each inaccessible VLAN referenced

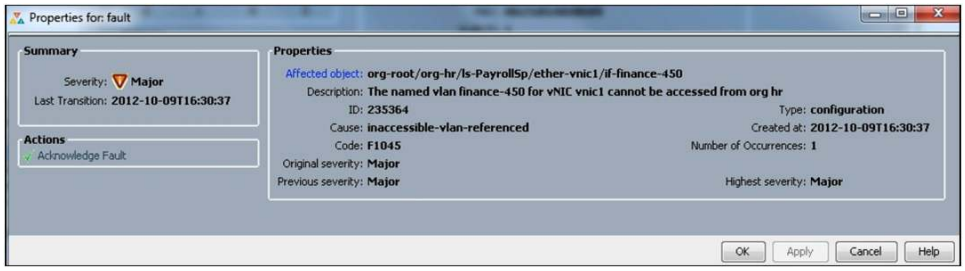
Although the server is configured to use an inaccessible VLAN, Cisco UCS prevents the server from using the VLAN by updating the operational VLAN to the **default** VLAN. In this case, the user is alerted with a configuration warning, as shown in Figure 7.

Figure 7. A Service Profile with a Configuration Error Because It References an Inaccessible VLAN



A critical fault is raised if a service profile is configured to use an inaccessible VLAN, as illustrated in Figure 8.

Figure 8. An **inaccessible-vlan-referenced** Fault Is Raised on vNICs Configured to Use Inaccessible VLANs



Greenfield Org-Aware VLAN Configuration

The following example shows how to configure Org-Aware VLANs in a greenfield Cisco UCS installation.

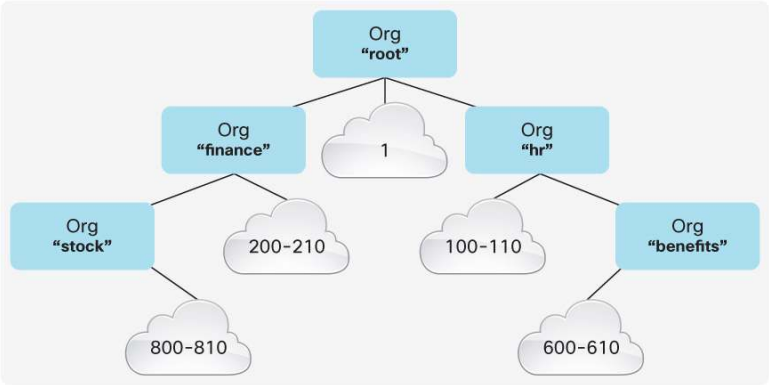
The configuration process includes the following steps:

1. Plan network access.
2. Enable the Org-Aware VLAN feature.
3. Create organizations.
4. Configure the **default** VLAN's permissions.
5. Configure VLANs and VLAN permissions.
6. Verify the configuration.
7. Configure the service profiles.

1. Plan Network Access

Typically, the network administrator is responsible for determining VLAN access based on network requirements and security policies. Figure 9. shows an example of an organization hierarchy with the VLANs required by each organization.

Figure 9. Desired VLAN Configuration



This example assumes that VLANs should be accessible only from the organization in which they are used and descendent organizations.

Table 1 shows the VLANs that are accessible from each organization.

Table 1. Accessible VLANs by Organization

Organization	Accessible VLANs
org-root	1
org-root/org-hr	1 and 100-110
org-root/org-hr/org-benefits	1, 100-110, and 600-610
org-root/org-finance	1, 200-210
org-root/org-finance/org-stock	1, 200-210 and 800-810

2. Enable the Org-Aware VLAN Feature

You can enable the Org-Aware VLAN feature at this point because this example assumes a greenfield deployment (that is, there is no server traffic to disrupt). The Org-Aware VLAN feature can be enabled from the LAN tab as previously described (see Figure 4).

3. Create Organizations

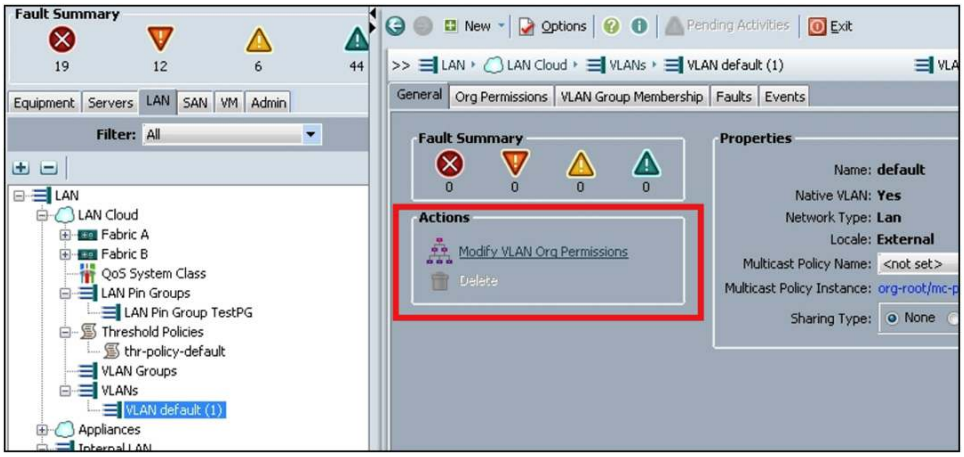
Create each organization that is part of your deployment plan. You create organizations from the Server tab by right-clicking the parent organization and choosing Create Organization.

4. Configure the Default VLAN Permission

A Cisco UCS best practice is to always create a VLAN permission in the **root** organization. This permission will restrict access for all organizations to the list of VLANs that have permissions or group permissions configured.[6] To create a permission for the **default** VLAN, navigate to the LAN tab, select the **default** VLAN, and click the Modify VLAN Org Permissions link, as illustrated in Figure 10.

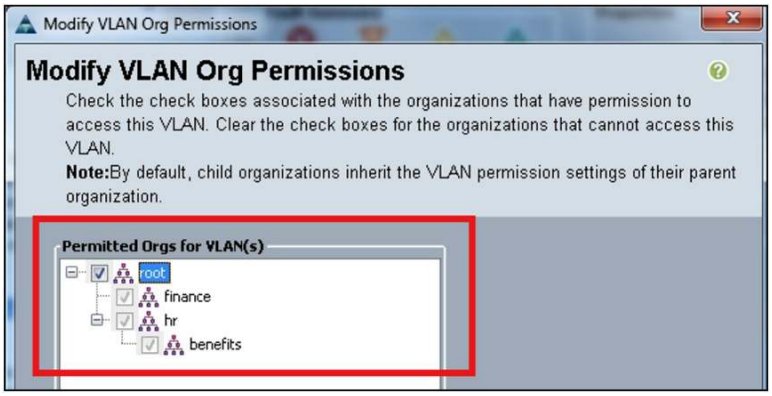
[6] The permission or group permission can be in the organization or in a parent organization.

Figure 10. Click the Modify VLAN Org Permissions Action to Configure the **Default** VLAN's permissions



When the "**Modify VLAN Org Permissions**" screen appears, select the "**root**" Org as shown in Figure 11.

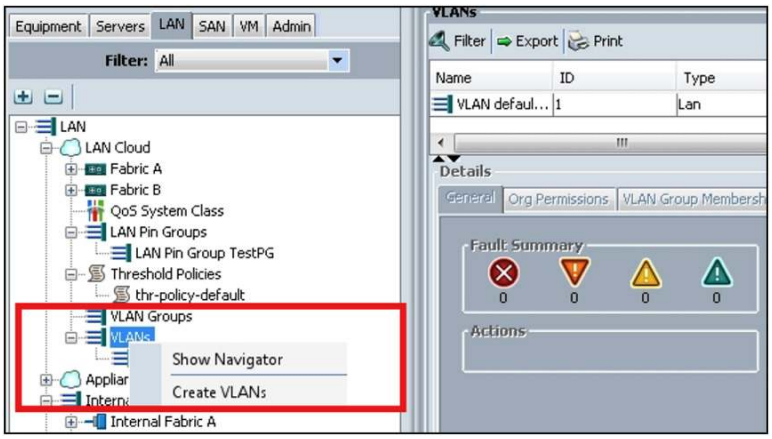
Figure 11. Modify the **Default** VLAN's Organization Permissions



5. Configure VLANs and VLAN Permissions

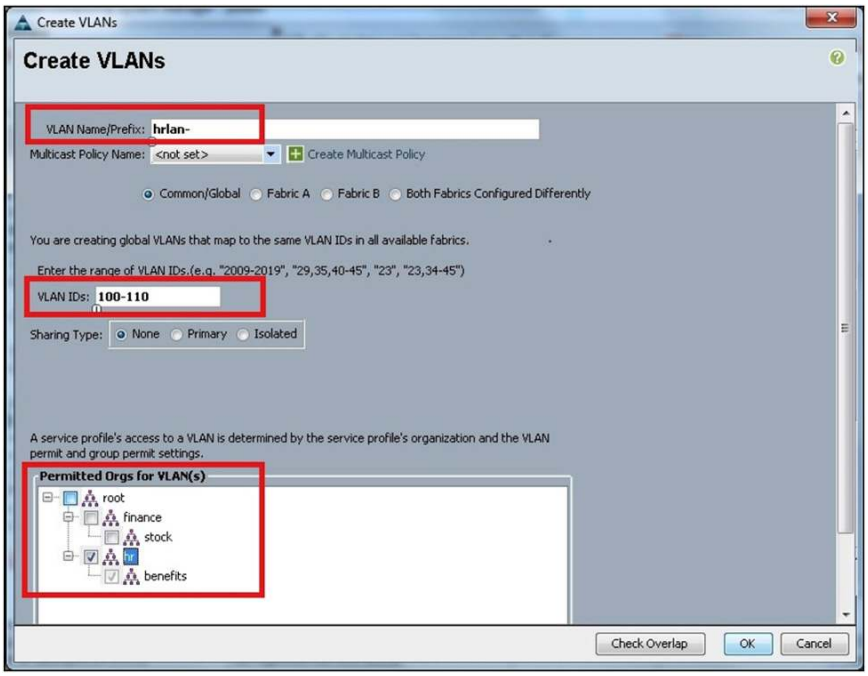
On the LAN tab, right-click the VLANs node and choose the Create VLANs option to launch the Create VLANs wizard, as shown in Figure 12.

Figure 12. Launch the Create VLANs Wizard



Configure a VLAN range from 100 to 110 and use the prefix **hrlan-**. Then select the **hr** organization as the permitted organization for the VLANs, as shown in Figure 13.

Figure 13. Use the Create VLANs Wizard to Create a Range of VLANs and Permissions



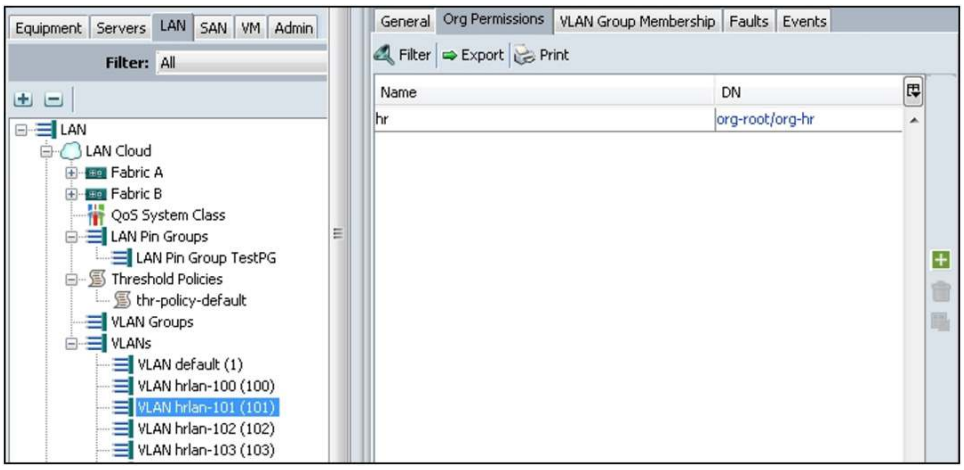
Configure the remaining VLANs in a similar manner, using the prefixes listed here:

- VLANs 600 to 610: Prefix **benlan-** and permitted organization **org-root/org-hr/org-benefits**
- VLANs 200 to 210: Prefix **finlan-** and permitted organization **org-root/org-finance**
- VLANs 800 to 810: Prefix **stocklan-** and permitted organization **org-root/org-finance/org-stock**

6. Verify the Configuration

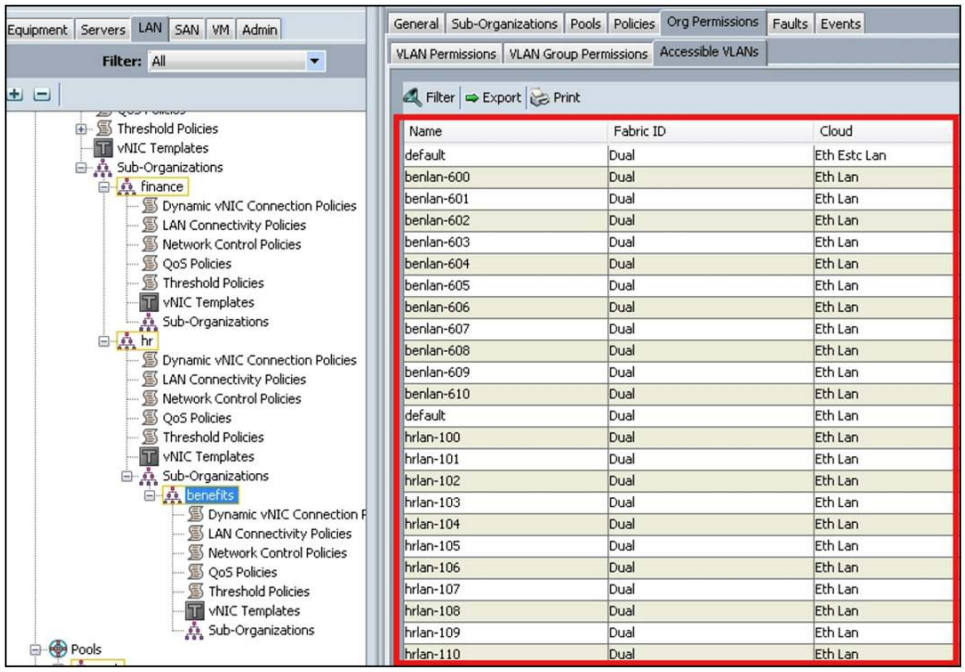
For each VLAN, you can view and modify VLAN permissions on the LAN tab, as shown in Figure 14.

Figure 14. VLANs and Their Permissions Can Be Viewed and Modified on the LAN Tab



The easiest way to verify the VLAN permission configuration is to check the accessible VLANs for each organization. You can do this from the LAN tab's organization nodes. In Figure 15, you can see that the **benefits** organization has access to VLANs **hrlan-100** to **hrlan-110** and **benlan-600** to **benlan-610**, as well as to the **default** VLAN. Other tabs allow you to view the VLAN permissions and VLAN group permissions that were created in this organization.

Figure 15. Viewing the VLANs Accessible from an Organization

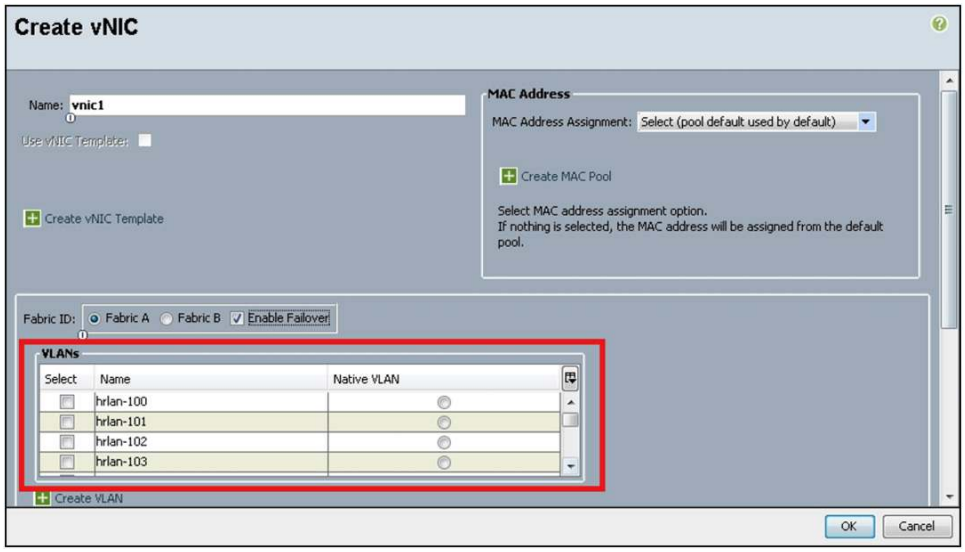


7. Configure the Service Profiles

At this point, the network configuration is complete, and all VLANs have been created and their accessibility configured. The server administrator can configure service profiles that consume these resources[7]. During service profile creation, the Cisco UCS GUI will allow the user to select only VLANs that are accessible from the service profile's organization. For example, if you create a service profile in the **benefits** organization, the Create vNIC wizard will let you select only VLANs **hrlan-100** to **hrlan-110** and **benlan-600** to **benlan-610** and the **default** VLAN, as shown in Figure 16.

[7] A comprehensive discussion of service profile configuration is beyond the scope of this document.

Figure 16. The Create vNIC Wizard Displays Only VLANs Accessible from the **Benefits** Organization



Brownfield Org-Aware VLAN Configuration

The following example shows how to configure Org-Aware VLANs in an existing Cisco UCS installation. This example assumes that the system has been upgraded to Cisco UCS Manager 2.1, that network traffic is running normally, and that the Org-Aware VLANs feature is disabled.

The configuration process includes the following steps:

1. Plan network access.
2. Configure the **default** VLAN's permissions.
3. Configure VLANs and VLAN permissions.
4. Verify the configuration.
5. Enable the Org-Aware VLAN feature.

You will keep the Org-Aware VLAN feature disabled until the network configuration has been validated. You do this to prevent disruption of server traffic. You will enable the feature after you are confident that the configuration is correct. When you enable the feature, the Cisco UCS GUI will warn you of any service profiles that reference inaccessible VLANs[8].

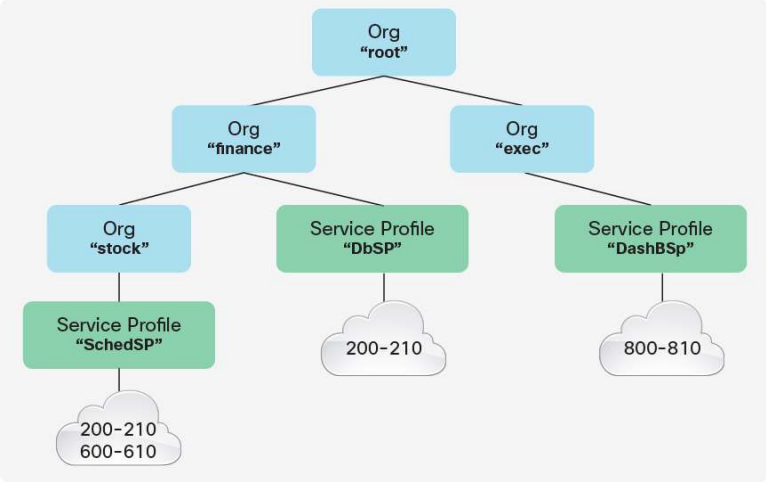
1. Plan Network Access

Typically, the network administrator is responsible for determining the network access required by the various organizations. To configure the desired VLAN access restrictions, it may be necessary to create new organizations or to move service profiles to other organizations. The actions required will depend on the existing and desired Cisco UCS configuration[9].

For this example, assume that the network administrator requires the VLAN setup illustrated in Figure 17.

[8] Recall that even though Cisco UCS will allow such a configuration, the server will have access only to VLANs accessible within its organization.
[9] Relocation of service profiles is a disruptive operation that requires a server reboot.

Figure 17. Logical View of Service Profile and Organization Hierarchy



On the basis of server requirements and organizational security restrictions, the network administrator can decide to restrict VLAN access as shown in Table 2.

Table 2. Accessible VLANs by Organization

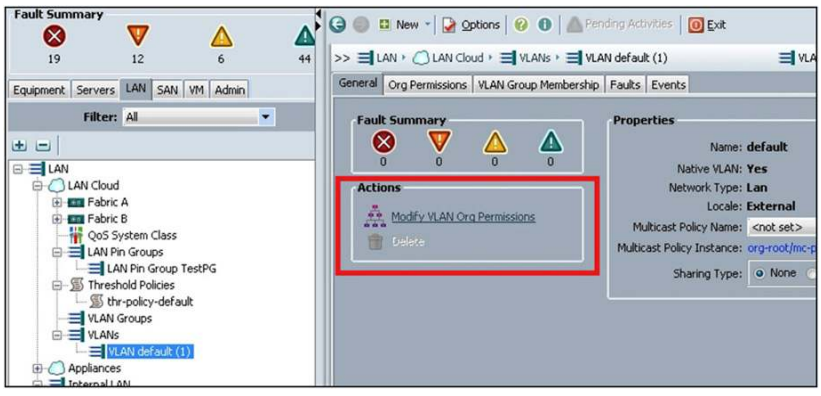
Organization	Accessible VLANs
org-root	1
org-root/org-exec	1 and 800-810
org-root/org-finance	1 and 200-210
org-root/org-finance/org-stock	1, 200-210, and 600-610

Note: Configuring access to VLANs 200 to 210 in **org-root/org-finance** will automatically provide access to them in **org-root/org-finance/org-stock**.

2. Configure the Default VLAN’s Permissions

A Cisco UCS best practice is to always create a VLAN permission in the **root** organization. This permission will restrict access for all organizations to the list of VLANs that have permissions or group permissions configured.[10] To create a permission for the **default** VLAN, navigate to the LAN tab, select the **default** VLAN, and the click Modify VLAN Org Permissions link, as illustrated in Figure 18.

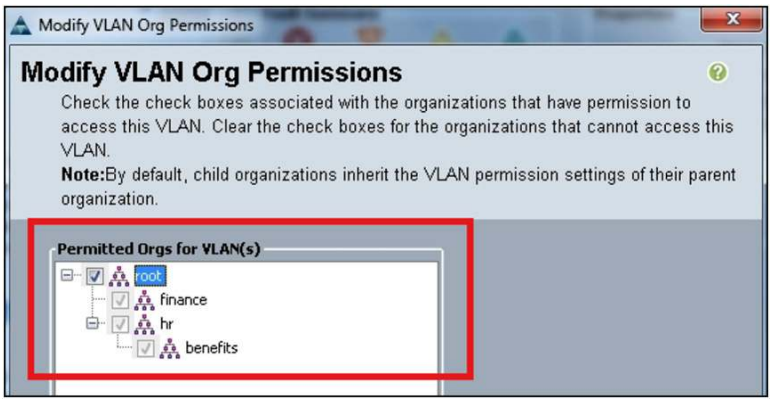
Figure 18. Click the Modify VLAN Org Permissions Action



[10] The permission or group permission can be in the organization or in a parent organization.

When the Modify VLAN Org Permissions screen appears, select the **root** organization, as shown in Figure 19.

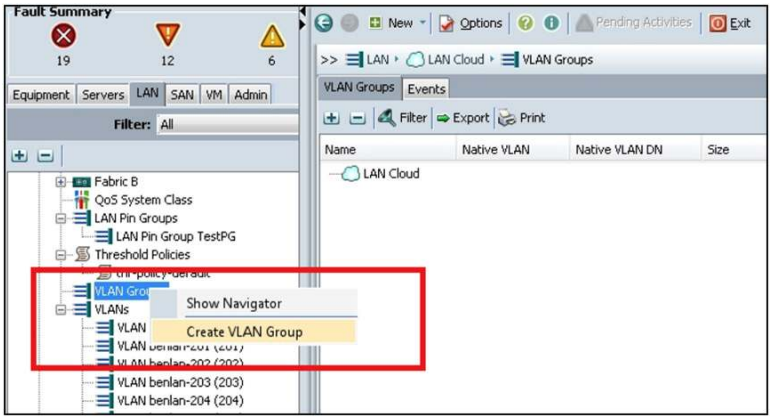
Figure 19. Modify the VLAN's Organization Permissions



3. Configure VLAN Permissions and VLAN Group Permissions

This example demonstrates a brownfield deployment, so it assumes that all necessary VLANs already exist. Thus, you proceed by creating VLAN groups and VLAN group permissions to assign access to the VLANs[11]. Navigate to the LAN tab and launch the Create VLAN Group wizard, as shown in Figure 20.

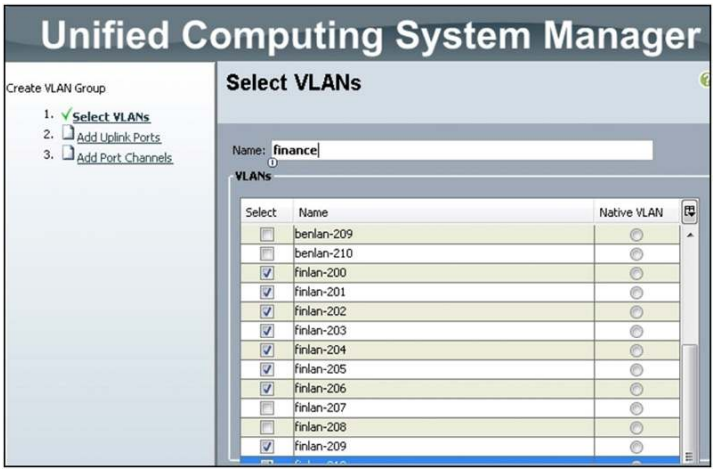
Figure 20. Launching the Create VLAN Group Wizard



In the Create VLAN Group wizard, create a group named **finance** and add VLANs **finlan-200** to **finlan-210**, as shown in Figure 21.

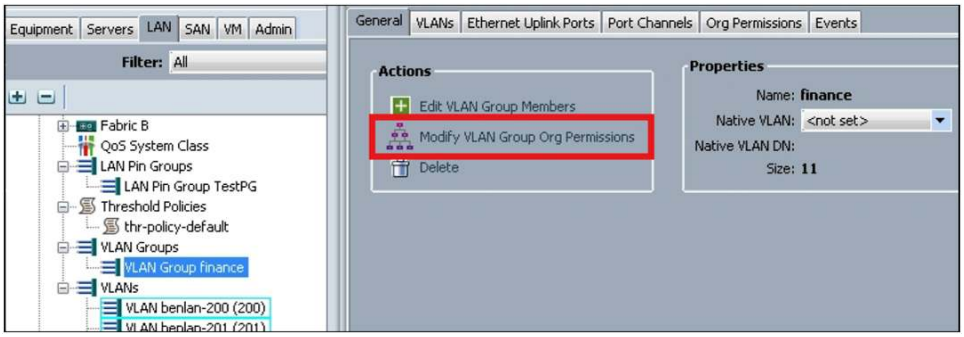
[11] An alternative approach would be to create VLAN permissions for each VLAN following the approach in the greenfield deployment example.

Figure 21. Add VLANs to the Group in the Create VLAN Group Wizard



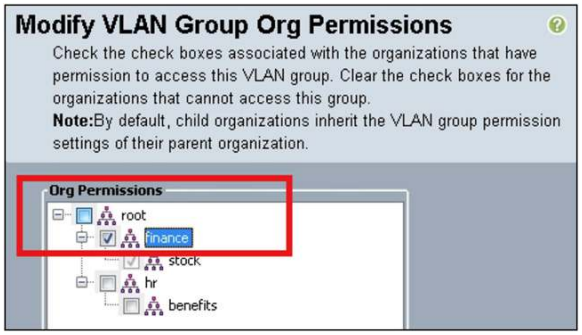
Now that the VLAN group is constructed, you can assign VLAN access to the group by creating VLAN group permissions. Navigate to the VLAN group on the LAN tab and click the Modify VLAN Group Org Permissions link[12], as shown in Figure 22.

Figure 22. Adding VLANs to a Group in the Create VLAN Group Wizard



In this example, choose the **finance** organization so that all the VLANs in this group will be accessible from this organization (and its suborganizations), as shown in Figure 23.

Figure 23. Modify VLAN Organization Permissions



[12] You have to configure the VLAN group permissions separately from the VLAN group creation process because the Org-VLAN Permit feature is disabled. After the feature is enabled, these two steps can be performed at the same time.

Repeat the preceding operation for each group of VLANs to create the VLAN groups listed in Table 3.

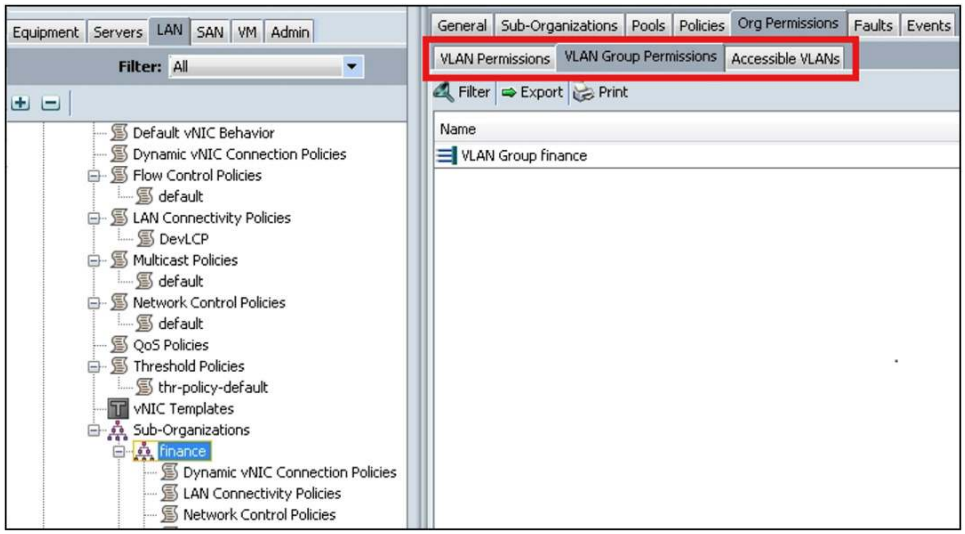
Table 3. VLAN Groups and Group Permissions

VLAN Group	Group Permission Organization	VLANs in Group
executive	**org-root/org-exec**	800-810
finance	**org-root/org-finance**	200-210
stock	**org-root/org-finance/org-stock**	600-610

4. Verify the Configuration

For each organization, you can view the VLAN permissions and the VLAN group permissions that will be used by UCS to determine the accessible VLANs, as shown in Figure 24. For each organization, verify that the correct VLAN permissions and VLAN group permissions are configured.

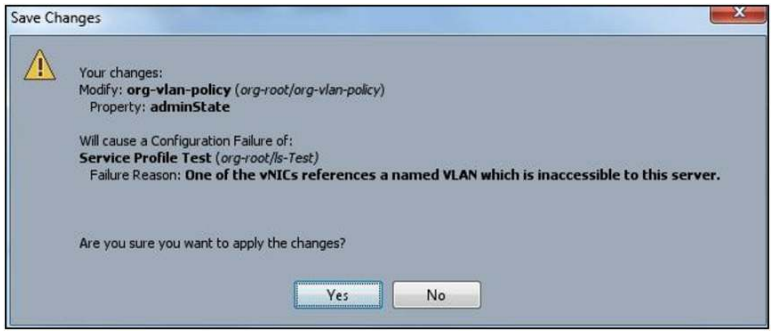
Figure 24. View Configured VLAN Permissions, VLAN Group Permissions, and Accessible VLANs



5. Enable the Org-Aware VLAN Feature

Enable the Org-Aware VLAN feature from the Global Policies tab as shown earlier in Figure 4. When you enable this feature, the Cisco UCS GUI will display a warning if any of the service profiles are using inaccessible VLANs. If this warning message appears, note the details, cancel the operation, and correct the configuration before enabling the feature (otherwise, you risk disrupting server traffic).

Figure 25. Dialog Box Warning That an Inaccessible VLAN Is Referenced



Deployment in a Secure Environment

Cisco UCS customers who require secure environments require organizations (and the servers they contain) to have access only to explicitly assigned VLANs. You can meet this requirement by creating a VLAN permission named **default** in the **root** organization[13]. This permission helps ensure that organizations have access only to explicitly assigned VLANs.

Conclusion

The Org-Aware VLAN feature provides the capability to restrict access to VLANs based on user-configured VLAN permissions and the organization that contains the service profile. The Org-Aware VLAN feature can be used by customers to meet their network security requirements in greenfield and brownfield Cisco Unified Computing System™ deployments.

For More Information

Contact your local Cisco representative or visit:

- Cisco Unified Computing System: http://www.cisco.com/go/unifiedcomputing
- Andersson, Gai, and Tommi Salai **Cisco Unified Computing System: A Complete Reference Guide to the Cisco Data Center**: Cisco Press, June 1st 2010. Cisco Developer Network: http://developer.cisco.com/web/unifiedcomputing/home
- Cisco UCS Manager product page on Cisco.com: http://www.cisco.com/en/US/products/ps10281/index.html
- Cisco UCS Platform Emulator (UCSPE) download: http://developer.cisco.com/web/unifiedcomputing/ucsemulatordownload
- Cisco UCS Manager Advantage video series: http://www.cisco.com/en/US/prod/ps10265/ucs_advantage_video_library.html
- Cisco IT solutions: http://www.cisco.com/web/about/ciscoitatwork/data_center/index.html

[13] Creation of a VLAN permission named **default** in the **root** organization is also a Cisco UCS best practice**.**

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

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

Printed in USA C11-718614-00 11/12