Cisco OverDrive 4.0 User Guide

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-24766-01

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco OverDrive 4.0 User Guide

CONTENTS

About This Guide

This preface briefly describes what this guide is about, who it is for, and how to read it.

- Is this guide for me?—It is for network operation and management staff of various levels of experience and responsibility who wish to create, revise, update, and manage physical and virtual cloud networks using OverDrive technology.
- What is this guide about?—It explains how to create and manage configured network equipment, and how to deploy virtual compute and storage resources to fulfill business needs. OverDrive tools for this include the Command Center, the Cloud Configurator, and the Cloud Orchestration Manager, as presented in this guide.
- How is this guide organized?—By OverDrive tool (command center, configurator, and manager). For the command center, topics proceed step-wise from fairly simple tasks and use cases to more powerful ones.
- What other documentation do I need?—To install OverDrive and bring up the command center, see Installing OverDrive; for an overview or introduction to OverDrive, see Introducing OverDrive; to write metamodels, see OverDrive Metamodels.

Is this guide for me?

This guide is designed for hands-on admins who will be managing and operating parts of generally large-scale networks, whether physical or virtual. You should be able to:

- Explain what you are doing, with reference as needed to the Introducing OverDrive guide, to other types of users.
- Modify the installation and configuration of your network, by using the OverDrive tools described here to configure the clouds, hardware, and software and their interactions with the operational environment, including LDAP, switches, routers, and so on.
- Deploy virtual resources in response your business needs, as you express them in the business policies that OverDrive will implement for you.
- Configure (and manage) clouds and subclouds, and VMs within them, that you or admins of your choosing make available to end users.

In general, this guide addresses two kinds of users:

- The OverDrive administrator who configures the network, policies, and so on, using the command center and the configurator.
- The vCOM user who creates VMs or subclouds

What is this guide about?

This guide explains how to use the OverDrive client applications to accomplish network management goals such as designing and implementing a network, creating and managing the configuration of network equipment, and deploying virtual resources in response to change and growth in your business needs.

It is task- and use-case-oriented, as opposed to the concept-oriented introductory guide listed in the "What other documentation do I need?" section.

How is this guide organized?

OverDrive can be used to manage a variety of installation types. Three broad types of deployment can be used either separately or in concert to manage user access within and between sites: site-to-site VPNs, network access control within a site, and cloud management.

This document is organized in general according to these three types of deployment that correspond to specific OverDrive user interfaces, as follows:

- The Command Center, which you use to model a network, including its business policies, network access policies and the like.
- Modeling simple, site-to-site, peer-to-peer networks involving only two computers: Chapter 1, "Creating a simple site-to-site network" and Chapter 2, "Setting up intra-site network access"
- Modeling hub-and-spoke networks involving client-server access and then bi-directional access such as for branch offices: Chapter 3, "Controlling intra-site network access"
- Modeling full-mesh networks in which resources can connect to all other resources: Chapter 4, "Controlling intra-site business access"
- Cloud Configurator, for configuring and managing a cloud of virtual computers: Chapter 5, "Configuring clouds"
- Cloud Orchestration Manager, which you and your assignees, other admins, and end-users, use to deploy virtual computers (VMs): Chapter 6, "Enabling VMs"

You can also access this information by installation or deployment type as follows:

- Site-to-site VPN deployment: Chapter 1, "Creating a simple site-to-site network" — sites, local resources, router, policies, applications (ports and protocols)
- Network access control with a site: Chapter 2, "Setting up intra-site network access" through Chapter 3, "Controlling intra-site network access" — network identities, VLANs, switches, RADIUS and Samba, policies, local resources, applications (ports and protocols)
- Cloud management: Chapter 5, "Configuring clouds" and Chapter 7, "Enabling VMs" — clouds, sites, VMs (most other objects come into play but are mostly automatically provisioned)

Note In general, each of Chapters 1 through 4 provides successive iterations through the Command Center UI. The best suggested reading path is through these chapters in sequence. Note also that the organization is by scenario or use case. The first appendix presents common tasks that are used by many or most of the scenarios in the body of this guide.

Appendices present:

- FAQs
- Troubleshooting suggestions
- Glossary of terms and abbreviations
- Index

What other documentation do I need?

The following documents may be useful to you:

- *Introducing Cisco OverDrive 4.0*, describing the OverDrive product, its concepts and architecture. This guide provides a common background that all users, installation experts, and network admins are expected to know or be able to reference.
- *Cisco OverDrive 4.0 Providing VMs Guide,* describes how users to create, power up or down, and remove VMs to be used by people in their group, department, or customer base.

Conventions

This document uses the following conventions:

Item	Convention
Commands and keywords	**boldface** font
Variables for which you supply values	*italic* font
Displayed session and system information	`screen` font
Information you enter	**`boldface screen`** `font`
Variables you enter	*`italic screen`* font
Menu items and button names	**boldface** font

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Warning **This symbol means danger. You are in a situation that could cause bodily injury.**

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

CHAPTER 1

Creating a simple site-to-site network

This chapter introduces you to using the OverDrive Command Center:

- Install type: site-to-site VPN basics
- Scenario 1a: Modeling a simple two-site network
- Scenario 1b: Moving servers from site to site
- Scenario 1c: Creating a business access policy

At this point, your OverDrive installation should have been completed, and the command center installed, as explained in *Cisco OverDrive 4.0 Installation Guide*. You should have read the chapter in *Introducing Cisco OverDrive 4.0* that describes concepts central to OverDrive, plus the main views and functions of the command center.

Install type: site-to-site VPN basics

Site-to-site VPNs are installations where each given site involves a router, a set of ports and protocols (formerly called applications), what OverDrive calls a business policy, and other local resources such as subnets, servers, and workstations that are assigned to the policy or policies.

In a nutshell, OverDrive allows you to define a policy that describes a business need, essentially that some resources need to communicate with some server, and then it builds all of the connections to support that. In the case of site-to-site connections, these include VPN, routing, and access control list configurations.

Scenario 1a: Modeling a simple two-site network

This section steps you through modeling a very simple network with two simple sites. This is mostly to introduce you to some common, general procedures, so you can become acquainted with the interface.

In summary, Scenario 1a exercises the following steps:

1. Create a couple of sites—"Creating sites" section on page 1-2
2. Create a resource at each site—"Setting up business policies" section on page 1-4
3. Create a business policy and add the resources into this—Step 2 of "Setting up business policies" section on page 1-4

Creating sites

To set up these basically one-time objects:

1. Click the Browse Layout icon on the right side of the icon toolbar. (You can use any of these layouts, but this guide generally uses the browse layout.)
2. Create a domain and enter a tooltip comment for it.
    a. Highlight the root domain, or a parent domain in which you want to create a domain, then click the domain icon in the toolbar.
    b. Enter a new domain name in the pre-filled text field, so that the Domain Name field reads Domain: North East.
    c. Enter a comment to be displayed when someone hovers over the new domain in the policy view.
    d. Click Submit.

    Why create a domain? Domains are used for delegating control, but also as a point to delineate network entities like a managed address space, or subdomains for VLANs.
3. Create two sites, named Site: Boston and Site: New York:
    a. Highlight the domain and choose New Site.
    b. Enter the site name.
    c. Click Submit.
    d. Repeat Steps a-c for the second site.

Note Ignore the alerts that say the site has no DSC. The next procedure addresses them.

Creating per-site devices and DSCs

For each site, define the DSC and devices in the Devices tab:

1. Highlight each site in turn and choose Edit.
2. Under each site’s Config tab:
    a. For the DSC, enter a name that is unique within the OverDrive managed network. A good practice is to use a prefix for your organization, followed by a unique ID that is helpful to you. For our example, enter DSC-HR-NewYork-01 and DSC-HR-Boston-01.

Note If you are an administrator of a subdomain, the name you choose must be unique among all the networks managed by OverDrive in the ROOT domain, no matter where they are in the tree.

    b. Enter a password and confirmation.
    c. Make a note of both the password and the DSC name as you will need them later when you configure the DSC appliance.
3. Under each site’s Device tab (for more details, see the“Specifying the site DSC and its devices” section on page A-3):

a. Choose the type of actual hardware role in the drop-down list labeled Add, at the bottom of the panel: switch (access, distribution, or aggregation), VM manager, NAT device, or router. (See the Glossary for definitions of these types of devices.)

b. Fill in the name, IP address, IPsec properties, and CLI and SNMP credentials, depending on the particular switch or router.

Note For now, just create a router for each site. Name it NewYork Router and Boston Router as appropriate, with username admin and password 123456, IP address of 10.0.0.1, tunnel IP addresses of 10.0.0.2, and tunnel interface of f0.

Name devices to help you and other administrators distinguish them. You can tell the difference between the agent and router/switches by recognizing the icons used for each, which are as follows:

Object	Icon	Object	Icon
Access switch	⇄	NAT device	✥
Aggregation switch	⁜	Router	●
Distribution switch	✳	VM manager	VM
DSC	▭		

c. Enter a useful comment, so you and other admins will know specifically which router or switch this is.

d. Click Submit.

Note You may get a warning that the tunnel interface must conform to the following patterns: g0, g0/0, g/0/0/0, where g can be letters e, f, and g; and 0 can be any digits 0-9).

Setting up business policies

Once you have defined the sites and its devices, you can begin to use policies to describe connections between resources at each site. Where you create sites, per-site devices, and DSCs basically once or seldom, your business policies may proliferate or change fairly often.

1. For each site, create local resources by specifying, in this example, the desktop and laptop:
    a. Right-click the site and choose New Local Resource.
    b. Specify the desktop icon (there is no icon for laptops) and name them Local Resource: SiteName Desktop and Local Resource: SiteName Laptop.
    c. Give each desktop and laptop an IP address of 10.0.0.3 and 10.0.0.4.

Note These need to be separate local resources, unless you specify a subnet that includes both IP addresses.

    d. Right-click each site in turn and select Edit. Note that in the Participating Resources tab, each site's desktop and laptop are listed in its Site Resources panel.
2. Specify communications ports and protocols to use between sites in the domain:
    a. Right-click the North East domain and choose New Ports & Protocols.
    b. Name this Ports & Protocols: Outposts Domain.
    c. Click Add and select ANY from the Predefined list.
    d. Click Submit and look for ANY under the Protocols column, and an asterisk (*) under the Ports column.
    e. Click Submit.
3. Create a business policy that uses the resources and protocol we have just set up:
    a. Right-click the North East domain and choose New Business Policy.
    b. Name it Business Policy: Let New York and Boston sites talk to each other.
    c. In the Ports & Policies tab, highlight what we created in Step 2 and click Add to move it into the Selected Ports & Protocols panel.
    d. In the Resources tab, highlight the four computers (local resources) listed in the Available Resources panel, and click Add to move them into the Participating Resources panel.
    e. Click Submit.

Now, the NSVE begins its work. It determines which sites are affected by the new policy. For each of these, it constructs a set of abstract directives to tell each site's DSC which network services and connections it needs to implement. (Network services are http, ftp, and so on. See the "Allowing ports and protocols for services" section on page A-6.)

Depending on which services are enabled at the sites, when the DSCs receive these instructions, they will begin to convert them into device-specific instructions and configure the devices accordingly.

Building business policies among multiple sites

You can permit users access to the network and have OverDrive write rules that permit them to access resources that have been defined for them. See the "Creating network identities" section on page 2-6.

In most cases it is sufficient to create business policies that enroll the users' assigned VLANs rather than their individual network IDs.

Note When when you enroll an LDAP group in a business policy, because OverDrive processes each user login as the user connects, the resulting rules will be written per-user host IP address and not per-VLAN. This in turn results in a large number of ACLs.

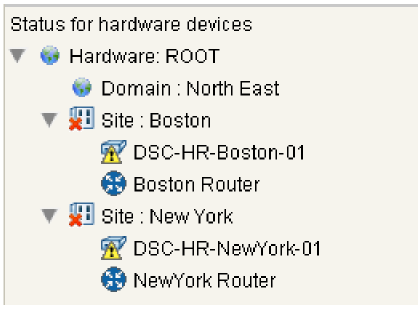
Troubleshooting this simple network

In the network status view, you should see the two DSCs and their network routers come up.

Note There are no network users in this network, and you would need network policies to create a connection between the two sites.

Figure 1-1 shows that both site routers seem to be working, but the DSCs have a warning flag (the exclamation mark in a yellow triangle). In this case, there is a particular problem with them, but the fact that the routers are up shows the DSCs are communicating with them and with the NSVE.

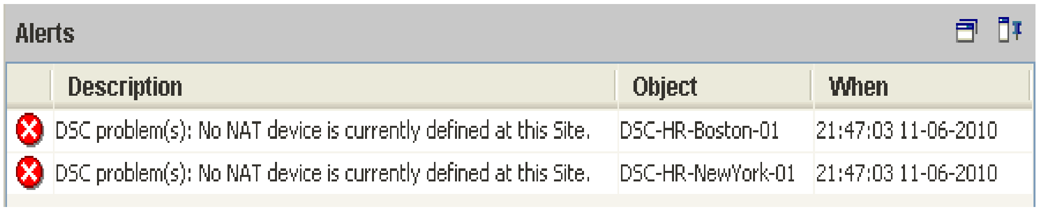
Figure 1-1 Unconnected routers, switches, or DSCs



Status for hardware devices

- ▼ Hardware: ROOT
  - Domain : North East
  - ▼ Site : Boston
    - DSC-HR-Boston-01
    - Boston Router
  - ▼ Site : New York
    - DSC-HR-NewYork-01
    - NewYork Router

Notice that the alert window reports the reason for this:



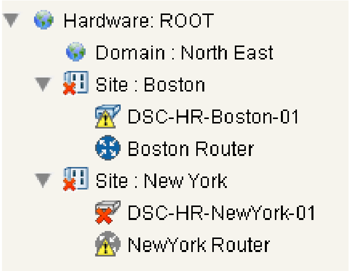
Alerts

	Description	Object	When
⊗	DSC problem(s): No NAT device is currently defined at this Site.	DSC-HR-Boston-01	21:47:03 11-06-2010
⊗	DSC problem(s): No NAT device is currently defined at this Site.	DSC-HR-NewYork-01	21:47:03 11-06-2010

To diagnose similar problems, follow these steps:

1. For routers and switches that have device down alerts, and if their DSCs are not accessible, as in the example below, confirm that the DSC processes are running on the DSC appliance:

Figure 1-2 Router with non-available DSC



Hardware: ROOT
Domain : North East
Site : Boston
DSC-HR-Boston-01
Boston Router
Site : New York
DSC-HR-NewYork-01
NewYork Router

2. For non-DSCs, try checking the IP address of the device, and then re-entering the CLI and SNMP credentials.
3. In the domain navigator, edit each site to make sure that your configuration specifies that the site's DSC has been assigned a device.
4. Check the device type, name, and so on.

Scenario 1b: Moving servers from site to site

This section explains what happens if you move a server from one site to another. Consider moving one from, say, San Francisco to Boston, and that you can move a rack mounted or even a VM-based server very quickly.

Without OverDrive, the networking infrastructure built to support users accessing the machine are not automatically going to be adjusted. Network engineers would have to change everyone's access.

With OverDrive, a high-level business policy drives the network. The policy, in this case, has already stated that all salesforce workstations need access to a CRM serve.

The policy already also specifies a network topology, in this case hub-and-spoke with the server at the hub.

With OverDrive, the change is simple: you don't need to edit the policy, just change the server's site and IP address.

The site drop-down list that lets you change the location of the server has a cheat-sheet at the bottom that tells which IP addresses to use for which site.

After you modify the site and address to match Boston's, and click Submit, the NSVE sends directives to the DSCs and devices to keep the business policy true. Within seconds, the connections change from a hub at San Francisco to a hub at Boston. In the following figure, the NSVE is already talking to each of the devices involved in Chicago and Nashville. The Boston-to-Nashville connection has been expanded to show the DSCs at those sites, and they each report traffic.

In a couple minutes, all the connections turn green. In the meantime, OverDrive displays any relevant status alerts, for example, whether the CRM server has confirmed transport connections.

Note Alerts and red flags do not mean something bad has happened. They indicate states without reported traffic. See Table 7-1 on page 7-3.

Once traffic starts flowing between the hub and each spoke, the connections all go green and the alerts go away. The logs will verify that all the sites have made the changes.

Scenario 1c: Creating a business access policy

This section leads you through modeling and verifying a business access policy that lets you provide access to a CRM server for a group of users in a sales department.

The following steps summarize the procedure:

1. Inspect the ports and protocols that are available to you in your domain (click the domain and check the summary view for ftp, http, and so on).
2. If there is not the protocol that you need to access the CRM server, create a new one and fill in TCP and the ports that are needed for access (see "Allowing ports and protocols for services" on page 86).
3. Click the create business policy icon.
4. Select the Sales VLAN and the CRM server.
5. Choose a hub and spoke configuration with the CRM server as the hub.
6. Choose the ports and protocols for accessing the CRM server.
7. Have a user connect to a managed switch and try to access the CRM server.

OverDrive will have created the Sales VLAN defined in the "Scenario 2a: creating VLANs for sites" section on page 2-7, because the user is in the group chosen in "Scenario 2b: creating a network ID and access policy" section on page 3-7, and associated with the user in the first section of Scenario 2b.

Overdrive will also have created access rules to permit access to the ports and protocols for the CRM server on the VLAN.

CHAPTER 2

Setting up intra-site network access

This chapter explains how to create and edit domains, sites, policies, and collections. It conveys the essentials of configuring an OverDrive network, in terms of its major components.

- Install type: intra-site network accesss—Network access control within a site
- Defining subnets and domain VLANs—Defining subnets and VLANs to new or existing domains; allocating sites to VLANs
- Using business and network access policies—Creating and refining business policies; making sure that network policies work (introductory material to be expanded in the next two chapters)
- Scenario 2a: creating VLANs for sites—Network access for machines, people, and groups: simple steps to re-create a specific example

The two chapters after this one look even more closely at controlling network access and managing business access policies, the heart of OverDrive network management.

Install type: intra-site network access

Of the following broad types of OverDrive deployments, site-to-site VPNs, network access control within a site, and cloud management, this chapter concentrates on network access control within a site.

Network access control within a site is concerned with how network identities (virtual machine interfaces or LDAP groups or individuals) work within VLANs created from virtual and physical switch devices, and how these identities interact with local resources and applications according to business policies, potentially using FreeRADIUS and Samba.

In a nutshell, first you create site-to-site VPNs as described in the previous chapter(“Creating a simple site-to-site network”), and then you set up more complex access to network resources by users and groups.

Providing network access for network identities

OverDrive offers a very powerful network identity-based management system. Network identities can be VM interfaces or LDAP identities pulled from an Active Directory server or some other LDAP store.

These network identities are granted access to the network by assignment to a network access policy that maps the VLAN connecting these network identities to switches, which might be, for example, in a data center or on branch office networks.

- VM interface-based network identities are primarily used in the creation of clouds and the allocation of VMs to the network, as discussed in later chapters (Chapter 5, "Configuring clouds" and Chapter 6, "Enabling VMs").
- LDAP-based network identities are used to identify users as they log into the network. Here, the standard features of 802.1x identity-based network access control provide the mechanisms that OverDrive employs for assigning users and group members to VLANs. In addition, once these users or group members are connected to the network, OverDrive applies business rules to provide fine-grained access to the destinations to which they are entitled (see Chapter 4, "Controlling intra-site business access").

Setting up access and routing mechanisms

In order to use LDAP-based network access control, you need to make sure that the site is configured with at least a distribution switch and an access switch. In addition to this, the inter-connect mode for the site needs to be set in the DSC's services.xml file, to either routed or end-to-end. Also, routed interconnects or trunks need to be configured between access and distribution switches.

For the interconnect modes:

- Routed—OverDrive builds VLANs at the access layer and provides routing to support traffic flow between each access switch and the distribution layer.
- End-to-end—OverDrive builds trunked VLANs from the access layer to the distribution layer to support traffic flow.

The access switches for network access control also need to be manually enabled for 802.1x support with FreeRADIUS, as described in *Cisco OverDrive 4.0 Installation Guide*, as well as in more detailed online instructions. (OverDrive Professional Services will help you to set this up on your network.)

Note An OverDrive authentication plug-in for FreeRADIUS provides the link from the RADIUS server to the OverDrive DSC and notifies OverDrive when a user is authenticated, and when unknown users try to access the network.

Defining subnets and domain VLANs

For intra-site access, you need to create VLANs in a domain. You may possibly need to create subnets as well.

Configuring subnets

When you create or edit a domain, you can specify subnets for it. They specify all of the addresses that are managed by OverDrive in that domain.

The managed address space for a domain is a set of subnets (collectively called the coherent region). These are usually one or more of the private addresses (10.x.x.x/8, 172.16.x.x./12 and 192.168.x.x/16), but could include public addresses for which OverDrive should be managing access.

You can use the coherent region to delineate subnet distribution over different domains, or to identify the block of addresses for OverDrive to control.

Domain subnets are inherited down the domain hierarchy to prevent admins from creating subnets outside of the defined list. You can further subdivide the coherent region to exert tighter control over the addresses in subdomains.

The Subnets tab in the domain creation/edit window lets you specify new subnets, edit existing ones, and delete existing ones in the list. As the comment under this tab states, “A list of all the subnets that are managed in this domain is called the coherent region. Setting this restricts the subnets that you can allocate to resources and VLANs in this domain, and sets the list of subnets for which OverDrive will manage ACLs.”

To add new subnets under the Subnets tab:

1. Click New.
2. Enter the IP address, for example, 172.16.0.0.
3. Enter an appropriate netmask, for example, 255.255.255.240.

Note If you prefer, you can use a subnet prefix or CIDR instead of typing out the full mask. The prefix for 255.255.255.240 is 27.

4. Click Accept.

Note You will not be able to edit your entry until you click Submit. However, this will submit all your changes to this new domain, and the domain will appear in the Summary tab of the selection view. To continue to edit your new domain if this happens, you will have to select it in the Summary tab and choose Edit.

Creating and configuring domain VLANs

A VLAN is a switched-based virtual LAN. It has the same attributes as a physical LAN, but it allows for devices or users to be grouped together even if they are not located on the same network switch.

When you first enable VLANs in a subdomain (by adding one to the domain), OverDrive recognizes the default VLAN that exists on all switch devices and creates a new VLAN called staging. This is where OverDrive places any user or virtual machine interface that is not a member of a network access policy.

There are domain VLANs and site VLANs. A site VLAN has the subnet assigned to it on the site. A domain VLAN is essentially a collection of all the sites' VLAN's subnets. For instance, for domain VLAN accounting is SiteA: accounting and SiteB: accounting VLANs.

Managed and unmanaged VLANs

Unmanaged VLANs are those that OverDrive does not manage, but are required on the switch devices for some infrastructural purpose (for example, a management VLAN to support services not managed by OverDrive).

Managed VLANs are managed by OverDrive network access policies.

You should create unmanaged VLANs if you need to preserve some that are already present on the switches that OverDrive will be managing. Otherwise, OverDrive sets the status on the device to be in error, and it reports the VLAN as out-of-policy. To correct this, you must define the VLAN as managed or unmanaged in OverDrive, or manually delete it from the switch.

Note In the services.xml file, you can set the treatment to report as described here, or to extinguish, which will remove any unmanaged VLANs not listed.

A managed VLAN is created for VLANs to which LDAP users or VM interfaces will be allocated when they have authenticated. When you define a managed VLAN you have to specify the name, number, site affiliation policy and ACL policy:

- Site affiliation determines whether the VLAN is automatically populated at all the sites in the current domain (and/or when a new site is created in that domain). You can choose to have the VLAN automatically appear at the site, or to require that it be manually allocated to sites.
- An ACL policy dictates how ACLs are applied to VLANs—you have the following choices, to:
- Apply no ACLs
- Restrict ACLs to lock everything except what is expressly permitted

Ports and Pools

The VLAN access-mode ports are expected to be either in a staging VLAN, in one of the designated managed VLANs, or in one of the designated unmanaged VLANs. Once the network identity (VM interface or LDAP person or group) is established, a network access policy determines how to assign it to the VLAN.

OverDrive defines VLAN groups at the domain level. When VLANs are instantiated at sites, they can be provisioned on switches. When a switch is enabled for management by OverDrive, any out-of-policy VLANs found on it are reported or extinguished, depending on the DSC’s configuration, if they are not defined in the site. OverDrive needs to know about VLANs, even if it does not manage them.

For more about when and how to use VLANs, see the “Reviewing available VLANs” section on page 3-2.

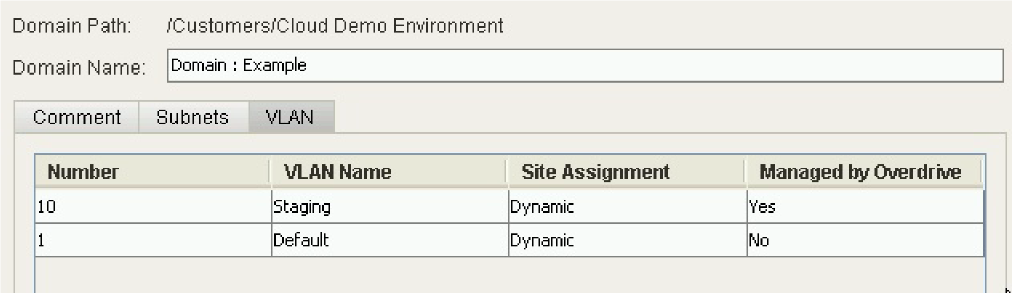
Creating a domain VLAN

To create a domain VLAN:

1. Click Add under the VLAN tab in the domain window for the domain being created or edited.
2. If this is the first VLAN that you are creating in this domain, you must enter a staging VLAN number before creating the VLAN: in the resulting staging and default VLANs popup, specify a number such as 10 for the staging VLAN, then click OK.

   (The default VLAN is pre-assigned to 1 and cannot be changed.)

   Now, the top part of the domain window should look like this:



Domain Path: /Customers/Cloud Demo Environment

Domain Name: Domain : Example

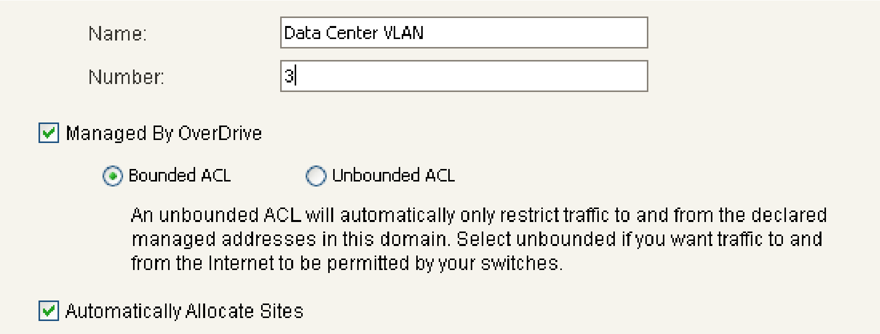
Number	VLAN Name	Site Assignment	Managed by Overdrive
10	Staging	Dynamic	Yes
1	Default	Dynamic	No

3. Now, click Add again to create a new VLAN:
   a. Specify a name and number: Data Center VLAN and 3.

      When you create the first VLAN in a domain, OverDrive prompts you for the number for the staging VLAN. The staging VLAN is like a quarantine VLAN into which all users who have no network access defined will be placed. Within OverDrive, users on this VLAN could be given access to an AD server and other services that are intended for guest access only.
   b. Generally, leave the following items checked except for the first:

   - Managed by OverDrive—Uncheck this if the VLAN that you are defining will not be managed by OverDrive.
   - Bounded or Unbounded ACL—A policy that determines how ACLs are enforced on the switches where VLANs are provisioned.
   - Automatically Allocate Sites—Leave this checked so OverDrive automatically allocates this VLAN to all sites currently in the domain and assigns it to any new sites created later. Uncheck it for static allocation, meaning to control site allocation manually.

   At this point, the top part of your new VLAN popup window should look like this:



Name: Data Center VLAN

Number: 3

☑ Managed By OverDrive

● Bounded ACL ○ Unbounded ACL

An unbounded ACL will automatically only restrict traffic to and from the declared managed addresses in this domain. Select unbounded if you want traffic to and from the Internet to be permitted by your switches.

☑ Automatically Allocate Sites

There are no site allocations yet, so the panes below this (not shown here) are empty.

   c. Click OK.

4. Repeat Step 3 as needed.
5. If you have configured all the tabs for your new or edited domain, click Submit.

Allocating VLANs to sites

Although VLANs are defined at the domain level, they have properties that are configured on a site-by-site basis. Where VLANs are intended to exist and not be managed by a DSC, they still need to be defined as unmanaged and allocated to the site so that the DSC does not interfere with the ports enrolled in that VLAN.

The site VLAN properties are its subnet and its DHCP helper.

1. Create or edit a VLAN or its information as directed in the "Creating and configuring domain VLANs" section on page 2-3.
2. If you do not want automatic allocation of the sites to VLANs, uncheck Automatically Allocate Sites, otherwise all the sites in the domain will be allocated.

Note When a VLAN is allocated to a site it is automatically included as permitted at each access switch at that site and will need to be manually removed on switches where it is not permitted.

3. Edit the site and open its VLAN tab.

   In the lower-right pane labeled VLANs Allocated, you will see the default and staging VLANs plus the new VLAN.

4. Highlight the new VLAN in the table just below the tabs, and click Edit.
5. Enter the subnet IP address and prefix, e.g., 10.10.8.0/24. ("Creating site subnets" section on page A-4.)

Note You can specify the subnet for an unmanaged VLAN. This will allow you to use this site VLAN in business policies. Although nothing will be provisioned on an unmanaged VLAN to enforce the policy, it will be enforced at all the other devices or VLANs that OverDrive is managing.

6. Enter the DHCP helper IP address. Each site has one or more of these helpers, to which DHCP requests are forwarded from VLANs.
7. Click Submit.

Creating network identities

Network identities map to LDAP distinguished names, therefore they can represent an individual or a group in Microsoft Active Directory. (They can also map to machine MAC addresses.)

You can create network identities by browsing to an LDAP store using the Command Center. You can also fill in the unique LDAP name if you know what it is for the user or group.

Create them within the domain in which they should be managed. Because the LDAP users could move from one site to another, they are not specifically allocated to a site. If the VLAN to which they are affiliated is assigned to a site and they log into an 802.1x-enabled switch at that site, OverDrive will build their VLAN and move the switch port into that VLAN to set up their network connectivity. LDAP users are therefore defined in the parent domain of the sites that the users will use.

Note Although you can assign network identities to business policies, we recommend that the VLAN to which they are assigned (in a network access policy) be used in business policies. Assigning LDAP identities to policies creates a unique set of rules for each user, whereas assigning rules to a VLAN group provides a uniform set of rules for all its users.

To create a network identity, such as a user:

1. Right-click a domain in the domain tree view, and choose New Network Identity.
2. Browse to a group or user in the Microsoft Active Directory.

Note A Microsoft administrator will have to have configured the LDAP credentials in OverDrive to make it possible to browse to an LDAP.

3. Click Add to add that user.

4. Click Submit.

Network identities are best understood as part of a scenario in which you allow a user to log onto the network and place that user into a group with the appropriate network access policy.

To see the creation of network identities in context, see "Creating a user for a network policy" section on page 3-4.

Using business and network access policies

Policies are the heart of OverDrive. They control, respectively, who can plug in and log into a switch, and, on the business end, who has access to which resources via the LAN or VPN WAN links that OverDrive manages.

Note Later chapters help you understand policy applications in an example network. This section tells you how to create and edit them.

Creating a network access policy

Network policy is a simple mechanism to let a user authenticate at the switch and then reach the VLAN and WAN/LAN environment.

To create a network access policy:

1. Right-click a domain and choose New Network Access Policy.
2. Enter the policy's name, and select a VLAN.

   For a new policy, only New VLAN and Staging are available.
3. Add or remove resources from the available and participating columns. OverDrive flags those that are already allocated elsewhere.
4. Click Submit.

To create users for a VLAN, see the"Creating a user for a network policy" section on page 3-4 To see how the policy affects user logins, see the "Watching a user log in" section on page 3-5.

For more about allocating VLANs to sites, see the"Reviewing available VLANs" section on page 3-2.

Scenario 2a: creating VLANs for sites

This section steps you through creating VLANs for a domain and assigning them to a site.

1. Create a domain if you don't have one already (see the "Creating a new domain" section on page A-1).
2. If you don't already have a site, create one in the domain that will represent the site where you will be managing network access control (see the "Creating a new site" section on page A-2).
3. Create a local resource for the CRM server at this site (see the "Creating a business policy for a CRM server" section on page 4-7).
4. Add a distribution switch and an access switch to the site (see the "Creating per-site devices and DSCs" section on page 1-2).

5. Edit the domain and go to the VLAN tab in the summary view.

6. Create VLANs for any infrastructure VLANs that need to exist on the switch but will not be managed by OverDrive, for example, a VLAN to be used for device management (see “Creating a domain VLAN” on page 25).

Note When you create the first VLAN you will be prompted to create a staging VLAN. Type in the VLAN number for it.

7. Create VLANs for each of the business groups that you want to manage in this network:

   a. Create a Sales VLAN (300) and an Accounting VLAN (301).

   b. Select Managed by Overdrive and the option to automatically assign to the site.

   c. Also select the option to have ACL enforcement on the VLAN.

Note The VLAN is applied to the site automatically as a site VLAN (for more about site VLANS, see the “Allocating VLANs to sites” section on page 2-5).

CHAPTER 3

Controlling intra-site network access

This chapter concentrates on using network access policies to control a user's access to the network.

- Install type: basic user access
- Reviewing available VLANs
- Showing VLAN switch assignments
- Creating a user for a network policy
- Watching a user log in
- Controlling access by active directory admins
- Scenario 2b: creating a network ID and access policy

We review how you give people access to the network. The chapter after this explains how to use collections to give groups of users access to resources on specific sites—see the"Controlling access by active directory admins" section on page 3-6.

Network access policies are about whether or not a user who plugs into the switch can be authenticated to the network via RADIUS and thus get access to the VLAN.

Install type: basic user access

You can further manage intra-site networks by concentrating on network access policies for individuals, groups, and services, as explained in this chapter.

Once you have created a network access policy and assigned network identities to it, you can choose which VLAN the policy will be affiliated with. Since a VLAN can only be assigned to one network access policy at a time, if you choose a VLAN that is already in use in another network access policy OverDrive warns that this will result in removing the VLAN from the other network access policy if you choose it.

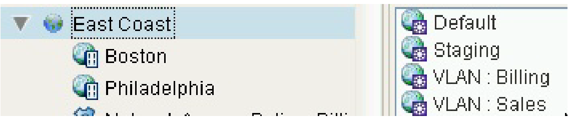
Network access polices only grant access to the network. When a user plugs a computer into an 802.1x enabled switch, the switch sends to RADIUS the authentication messages from the user's workstation. If the user is authenticated, the OverDrive plugin to RADIUS informs the DSC.

OverDrive looks this user up in its list of network access policies. If the user or the user's group is found to be associated with a VLAN, the DSC identifies the port to which the user is attached and begins to allocate the port to the VLAN. Once the user is assigned to the VLAN, OverDrive monitors the port until the user is allocated an IP address, at which time it begins to build policies to permit appropriate user access to destination resources.

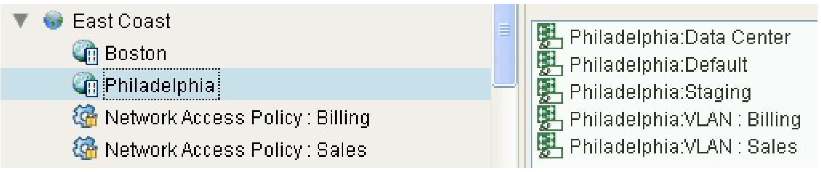
Reviewing available VLANs

In order for a person to be allowed on the network, there has to be a network access policy that associates him or her with a particular VLAN.

Let's look at a domain that already has some VLANs created in it. For example, select the domain and see the VLANs in the selection view:



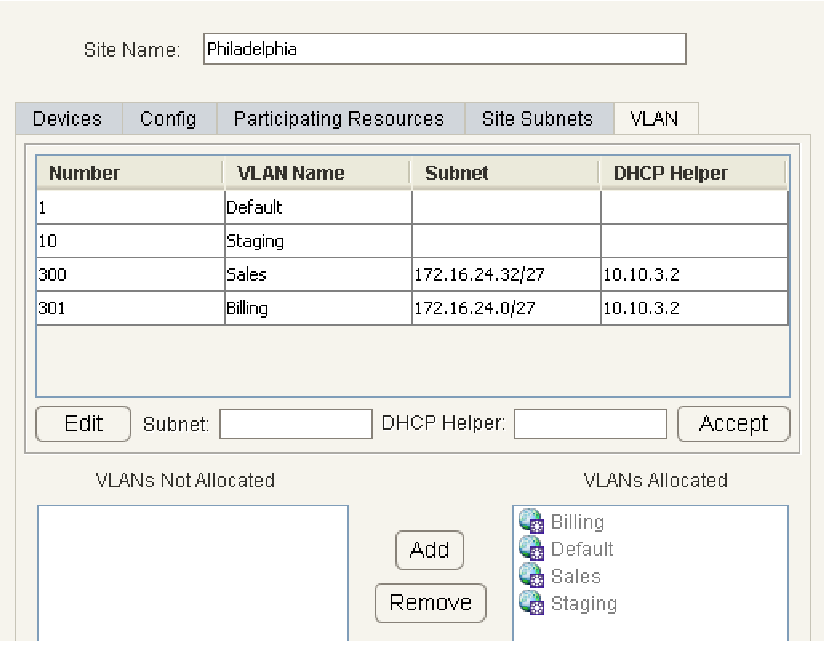
The two sites, Boston and Philadelphia, have their own versions of these: Boston: VLAN: Sales and Philadelphia: VLAN: Sales, as you can see by highlighting the Philadelphia site and looking at the VLANs tab in the selection view:


East Coast
Boston
Philadelphia
Network Access Policy : Billing
Network Access Policy : Sales
Philadelphia:Data Center
Philadelphia:Default
Philadelphia:Staging
Philadelphia:VLAN : Billing
Philadelphia:VLAN : Sales

The sites have these VLANs because they have inherited the VLANs that are defined for this domain. (As discussed in the "Creating and configuring domain VLANs" section on page 2-3, the staging and default VLANs always exist.)

If you select one of these, such as Philadelphia VLAN: Sales, you can see in the site's VLAN tab the various VLAN parameters as well as which have been allocated for use at the site. In the following section, we will add users from the sales department.

Figure 3-1 VLANs at the Philadelphia site in the East Coast domain



Site Name: Philadelphia

Number	VLAN Name	Subnet	DHCP Helper
1	Default		
10	Staging		
300	Sales	172.16.24.32/27	10.10.3.2
301	Billing	172.16.24.0/27	10.10.3.2

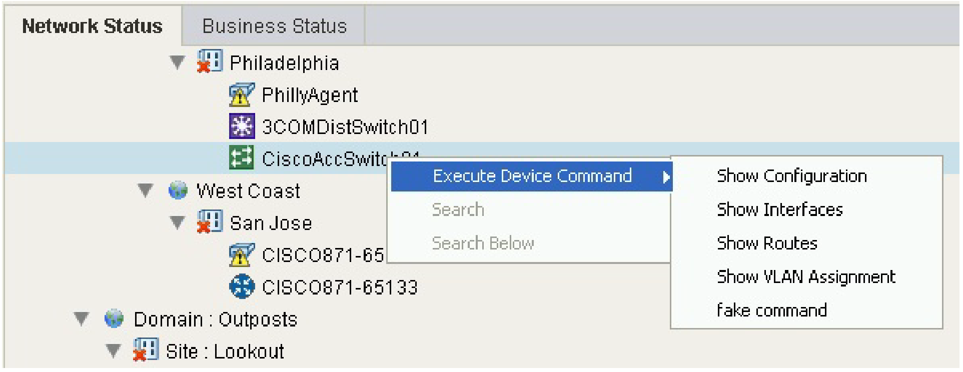
VLANs Allocated:
- Billing
- Default
- Sales
- Staging

(You can see the subnet and DHCP helper values in the preceding figure. See the "Allocating VLANs to sites" section on page 2-5 for a refresher on how these were assigned.)

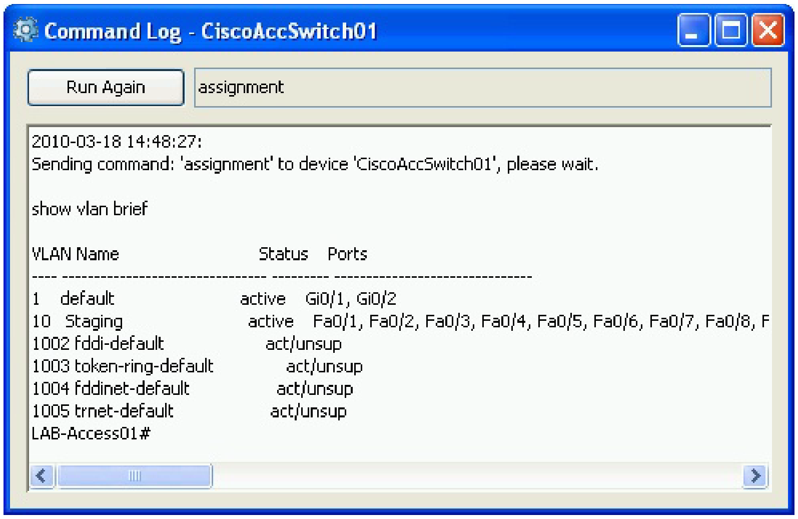
Showing VLAN switch assignments

In order to have network access, your site of course has to have switches: one for the distribution layer, which is where the routing happens, and one for the access layer, which is where people plug in. (Depending on the size of your site, you may also have an aggregation layer which aggregates a high port density or lower speed connections into faster trunks.)

You can run several commands on the switches to show configuration, interfaces, and routes, (as on the router), and you can also show VLAN assignments:



Typical output from the Show VLAN Assignment command to the switch is shown below:



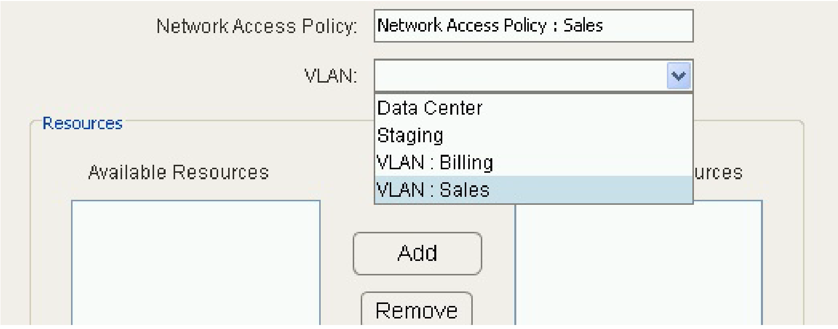
assignment

```
2010-03-18 14:48:27:
Sending command: 'assignment' to device 'CiscoAccSwitch01', please wait.

show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi0/1, Gi0/2
10   Staging                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4, Fa0/5, Fa0/6, Fa0/7, Fa0/8, F
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
LAB-Access01#
```

This figure shows the default and staging VLANs (numbered 1 and10), but no other VLANs, because the ones we want for sales and billing have not yet been populated with users, so they are not yet active.

Creating a user for a network policy

Let’s look at Philadelphia again so we can follow this example. In order to allow a person onto the net, as mentioned, you need a network access policy. Follow the instructions in the “Creating a network access policy” section on page 2-7, only now you can choose resources for one of the VLANs we have just created:


Network Access Policy: Network Access Policy : Sales

VLAN:

Starting with this network access policy that will associate a user with the Sales VLAN, here’s how to create a user and add him to the policy:

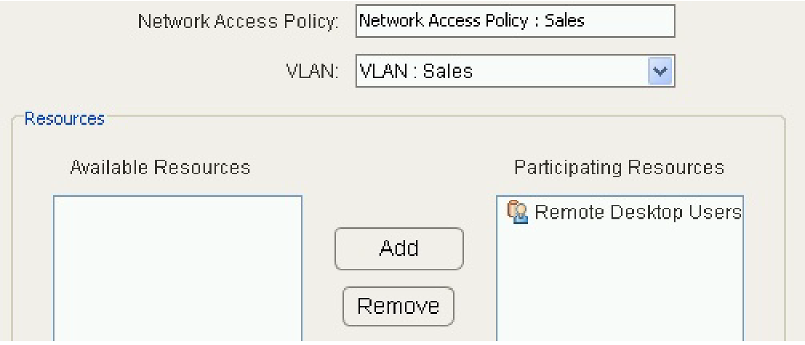
1. Right-click the East Coast domain (in our example) and choose New Network Identity
2. Click the Browse button to launch the LDAP browser. (See the *Cisco OverDrive 4.0 Installation Guide* for editing LDAP credentials in overdrive.xml on the server and in services.xml for the DSC.)
3. Browse to the Remote Sales group and click OK.

   We have created a new network identity named Remote Sales. It contains the users in the group. (See the “Creating network identities” section on page 2-6.)
4. Right-click Network Access Policy: Sales in the domain and choose Edit.

The network access policy for Sales opens up, with a VLAN: Sales. Remote Sales listed in the participating resources pane.

Note A site VLAN can only belong to a single network access policy. The network access policy shows domain VLANs as well as network identities. Because network identities can only be assigned to one network access policy at a time, OverDrive uses an asterisk (*) next to the name to indicate one that is already assigned elsewhere.

5. Choose the VLAN, highlight Remote Sales, and click Add to put it into the participating resources pane:



Network Access Policy: Network Access Policy : Sales

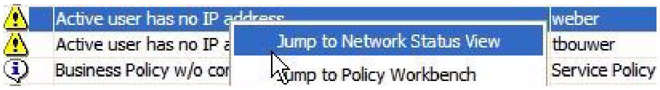
VLAN: VLAN : Sales

6. Click Submit.

What these steps have effected is a policy that says, if you see someone log into the network and he belongs to the group Remote Sales, put him into the Sales VLAN. That's why we talk about network access control.

Watching a user log in

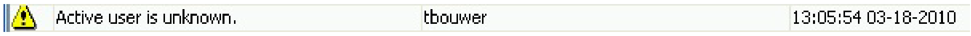
If the user you have added has not yet logged in, as soon as he does, he will show up in the Alerts window as an active user with no IP address:



Active user has no IP address weber
Active user has no IP a tbouwer
Business Policy w/o cor Service Policy

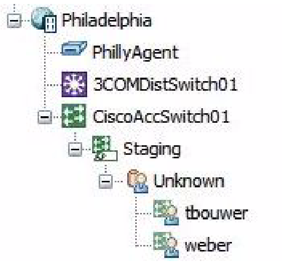
You can right-click that user and jump to the network status view to see who he is. If you're too slow, you'll see him in Remote Sales, instead, and you will not see him passing through the staging VLAN, as discussed below.

If, on the other hand, the user is for some reason not known to OverDrive (perhaps in a group that hasn't been configured in OverDrive), he will stay in the Alerts window as unknown:



Active user is unknown. tbouwer 13:05:54 03-18-2010

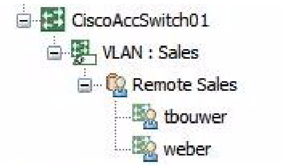
When you are looking at the network status view, and if you're fast enough, you'll see the newly logged in user showing up in Staging as an unknown user:



Note Defined VLANs don't exist on the screen all the time because they get created on demand. Also, note that we are adding two users, not one, because they are each members of the LDAP group Remote Sales.

At this point, the logged-in user has been authenticated but has not yet received an IP address. Even though OverDrive knows the username, it does not know where to place him.

Once the DHCP server has given him an IP address, for a brief moment, he will show up in the Alerts window as an active user with no IP address, and will then immediately be put into the VLAN to which he was assigned. In other words, when the network access policy recognizes this user as belonging to the Remote Sales group, it will put him into VLAN:Sales:



Controlling access by active directory admins

OverDrive permits controlled network administration by active directory administrators.

If you set up OverDrive to manage network access control, you can hand over a small part of the network control to a Microsoft administrator to decide who belongs on which VLAN. You can do this without actually handing over the keys to the switches, which is what you want, because you don't want that administrator to start configuring switches.

What's going to happen is that as soon as he adds users, with a login in Sales, OverDrive is going to begin recognizing them as being not only allowed on our system but allowed in Sales.

When you or the Microsoft administrator put a user into a VLAN, he won't have an IP address because he will be waiting for one from the DHCP server. Once he has an IP addresses, the system will figure out what he is allowed to access on the network, and will build policy to support that access.

(As mentioned earlier, we recommend that you use VLANs in policies rather than network identities unless you specifically want fine-grained control over an individual user's access.)

Scenario 2b: creating a network ID and access policy

This following steps outline how to create a network identity for a group individual in an LDAP directory.

Creating a network ID for a group is one of the steps in allowing a group of users access a resource such as a CRM server. For more information, see the "Creating network identities" section on page 2-6 and the "Creating a network access policy" section on page 2-7.

1. Click the create network ID icon.
2. Browse your LDAP and find a group that matches your Sales users.
3. Click OK.

At this point, you can create a network policy and assign the Sales group to it (for more information, see the "Creating a network access policy" section on page 2-7):

1. In the domain that you have selected for managing network access, click the create network access policy icon.
2. Type in a name for the network access policy (Sales).
3. Select the Sales VLAN using the dropdown.
4. Select the LDAP group that you created in the previous few steps, and add it to the Network Access Policy.

CHAPTER 4

Controlling intra-site business access

This chapter discusses what can happen once a user is allowed VLAN access by the network access policy. In OverDrive, this is controlled by business access policies.

- Install type: intra-site business policies
- Getting oriented
- Building a primary network policy
- Creating a business policy for a CRM server

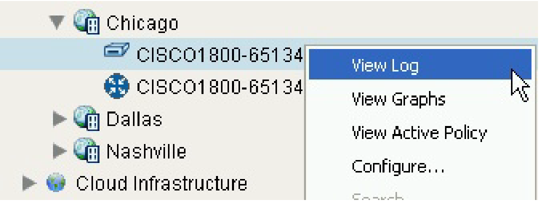
Install type: intra-site business policies

For intra-site access, an admin creates business policies that connect a VLAN to a local resource at the same site. You can further manage intra-site networks by concentrating on business policies as explained in this chapter.

Getting oriented

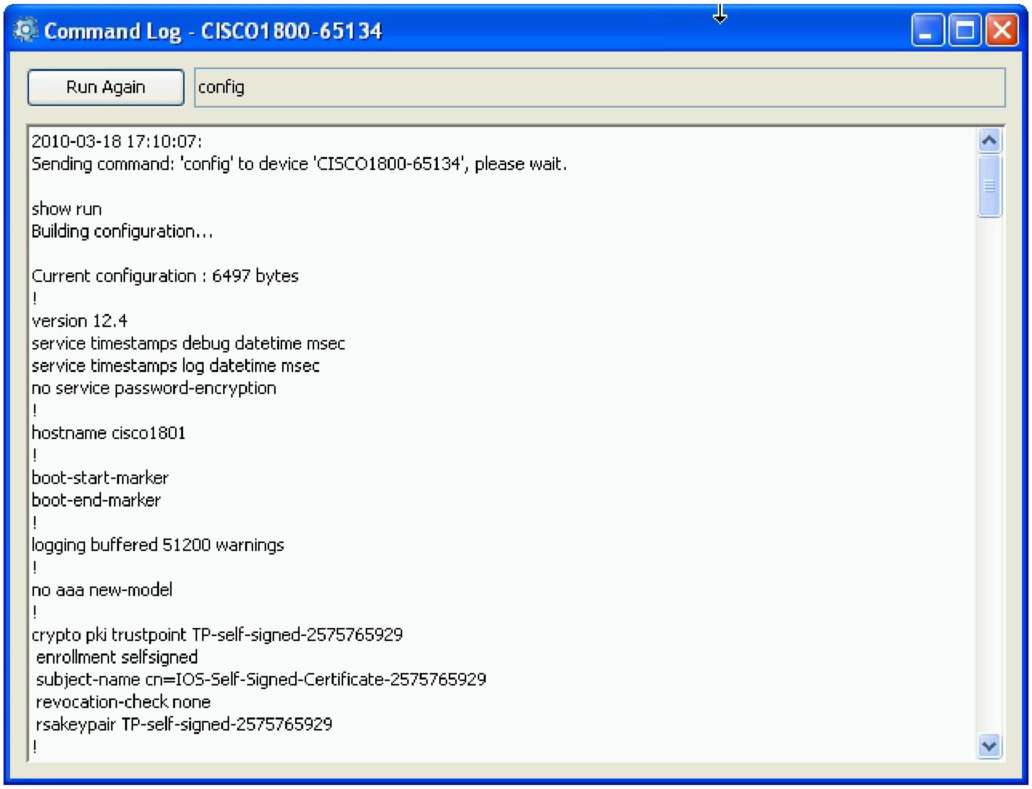
This chapter is based on a network pre-populated with a number of sites having devices such as Cisco switches, DSCs on OverDrive appliances, and various routers.

In the network status view, if we drill down to the Chicago site in the Central domain, and right-click the DSC, we can choose to see logs, graphs, or the active policy; or, we can choose to configure the DSC.



If you look at the DSC's log, you see tabs that let you choose a particular log: the DSC health, ntpd's success at synchronizing with the time server, and the results of the DSC's polling of the device (the DSC might be looking to see if there are any tunnels defined, for example).

If you go to the device itself (in this case, the router named CISCO1800-65134), you can execute device commands to show the device configuration, its interfaces, and its routes. For example, Show Configuration produces a device command log:



config

```
2010-03-18 17:10:07:
Sending command: 'config' to device 'CISCO1800-65134', please wait.

show run
Building configuration...

Current configuration : 6497 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname cisco1801
!
boot-start-marker
boot-end-marker
!
logging buffered 51200 warnings
!
no aaa new-model
!
crypto pki trustpoint TP-self-signed-2575765929
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-2575765929
 revocation-check none
 rsakeypair TP-self-signed-2575765929
!
```

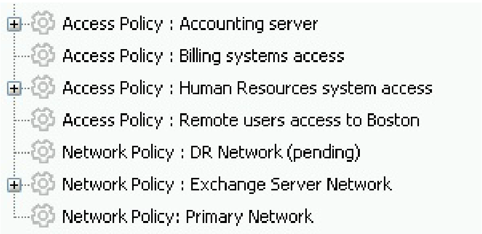
Since this is a Cisco device, the log reports a typical Cisco configuration coming up.

The device and DSC commands are configurable and can be added to and edited.

Building a primary network policy

This section walks you through building a primary network policy.

Notice in the following figure from the domain tree view that there are policies that are grayed out because they're not active yet.



Access Policy : Accounting server
Access Policy : Billing systems access
Access Policy : Human Resources system access
Access Policy : Remote users access to Boston
Network Policy : DR Network (pending)
Network Policy : Exchange Server Network
Network Policy: Primary Network

We refer to these as different types of policies, shown here as access and network policies, but under the covers, they are really the same—these all happen to be business access policies. That is, they build associations between resources at one site and resources at another site. Or between resources on network switches on one site and other resources at that site.

Note OverDrive supplies a suggested naming scheme for objects that you create. For network access policies such as discussed in the previous chapter, OverDrive provides a pre-filled name prefix, **Network Access Policy:** (for business policies, the prefix is **Business Policy:**).

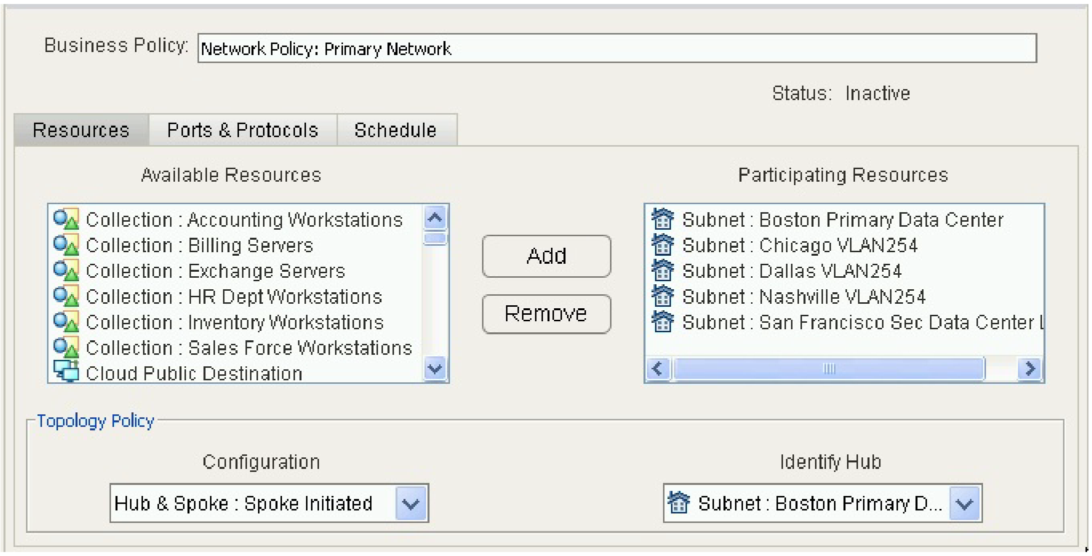
If you right-click a policy and choose Edit, you can see immediately whether it is a business or a network access policy. If you could do that for all the policies in the preceding figure, you would see that they are all business policies. Business policies determine what you are allowed to reach on the net, for instance, whether you can go to specific servers, and when. These policies provide the logic that allows you to do your business.

Editing and activating a primary networking policy

The primary networking policy described here constructs a connection between each of the subnets at different sites.

1. If you could, create a business policy named Network Policy: Primary Network, similar to the one shown in the following figure.
2. Place five site-specific subnets as participating resources in the pane on the right. One of them is the Boston primary data center. The other four (Chicago, Dallas, Nashville, and San Francisco) are to connect to Boston.

   This policy uses a hub and spoke configuration, with the Boston primary data center as the hub.



Business Policy: Network Policy: Primary Network

Status: Inactive

Resources | Ports & Protocols | Schedule

Available Resources
- Collection : Accounting Workstations
- Collection : Billing Servers
- Collection : Exchange Servers
- Collection : HR Dept Workstations
- Collection : Inventory Workstations
- Collection : Sales Force Workstations
- Cloud Public Destination

Participating Resources
- Subnet : Boston Primary Data Center
- Subnet : Chicago VLAN254
- Subnet : Dallas VLAN254
- Subnet : Nashville VLAN254
- Subnet : San Francisco Sec Data Center l

Topology Policy

Configuration: Hub & Spoke : Spoke Initiated

Identify Hub: Subnet : Boston Primary D...

3. Open the Ports & Protocols tab and choose ANY as the protocol so any traffic can go through.
4. Click Submit.

   The status will still be inactive (as you can see in the upper right), because the policy has not yet been activated.

5. Activate the policy by right-clicking it in the domain tree and choosing Activate.
6. Notice that the gear becomes blue:

Network Policy: Primary Network

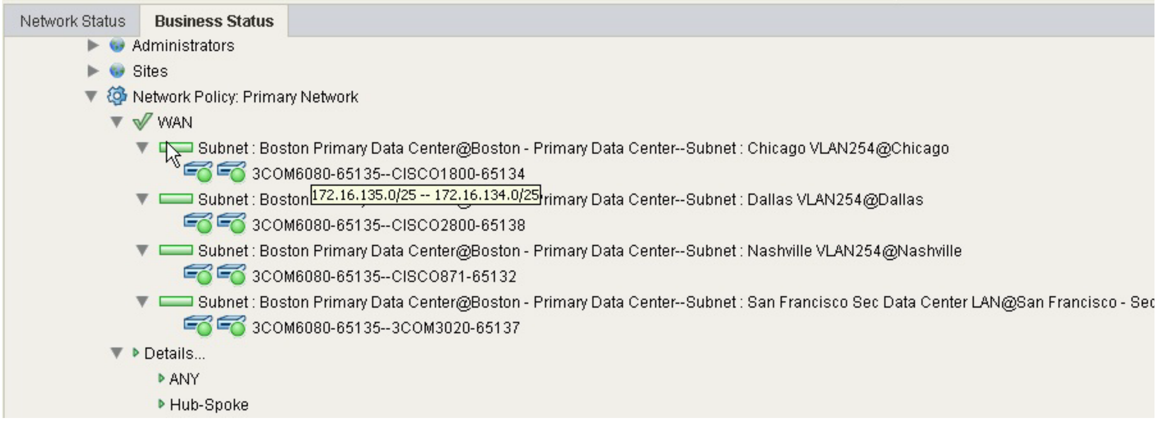
Verifying the policy

The NSVE now reconfigures the network. That is, it creates VPNs connecting, in this case, the four spoke sites to the central hub. This process is known as policy server provisioning, which means figuring out how to change all the sites that need to be changed to make the policy true.

The NSVE sends configuration directives to every site that has one of the participating resources, and builds connections back to the hub, using the DSCs at those sites.

In the business status view, these are the policies that have to be put into effect to make the policy true. Each of the devices responds to the DSC's poll asking the status of its connections. Once those connections are up, the devices report back to the DSCs, and the DSCs report back to the status view and say okay, the connections are up, the tunnels are in place, and communication is occurring over them.

Note The connections only show as green when there is traffic passing through them. Red doesn't indicate a connection is down, but rather that is shows no traffic.



```
▶ Administrators
▶ Sites
▼ Network Policy: Primary Network
  ▼ WAN
    ▼ Subnet : Boston Primary Data Center@Boston - Primary Data Center--Subnet : Chicago VLAN254@Chicago
        3COM6080-65135--CISCO1800-65134
    ▼ Subnet : Boston 172.16.135.0/25 -- 172.16.134.0/25 rimary Data Center--Subnet : Dallas VLAN254@Dallas
        3COM6080-65135--CISCO2800-65138
    ▼ Subnet : Boston Primary Data Center@Boston - Primary Data Center--Subnet : Nashville VLAN254@Nashville
        3COM6080-65135--CISCO871-65132
    ▼ Subnet : Boston Primary Data Center@Boston - Primary Data Center--Subnet : San Francisco Sec Data Center LAN@San Francisco - Sec
        3COM6080-65135--3COM3020-65137
  ▼ Details...
      ANY
      Hub-Spoke
```

If you mouse over, you get a tooltip that shows you the characteristics of the connection, for example, showing that the subnet at Boston is connected to the subnet at Chicago, and with which IP addresses, for instance.

Note In this example, there are only routers and no switches. These are just site interconnects.

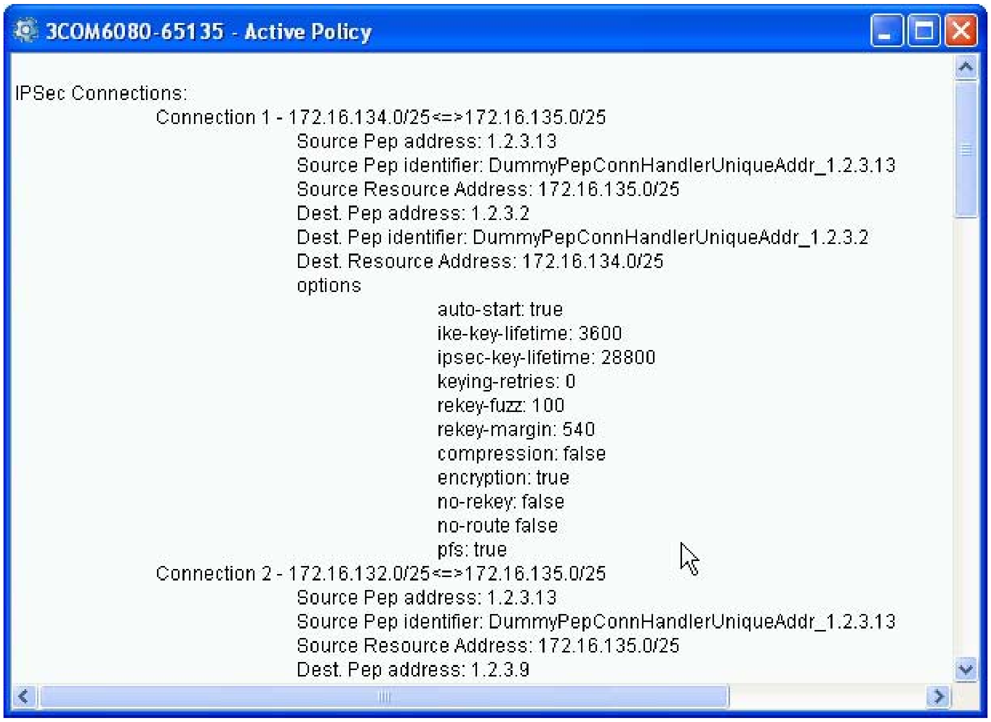
Viewing the active policy

When the connections are all up:

1. Go back to the network status view, and pick one of the sites.

   For this example, choose the Boston data center (the hub).

2. Right-click the DSC and choose View Active Policy.
3. Look for a report such as the following (shown in part):



```
IPSec Connections:
            Connection 1 - 172.16.134.0/25<=>172.16.135.0/25
                        Source Pep address: 1.2.3.13
                        Source Pep identifier: DummyPepConnHandlerUniqueAddr_1.2.3.13
                        Source Resource Address: 172.16.135.0/25
                        Dest. Pep address: 1.2.3.2
                        Dest. Pep identifier: DummyPepConnHandlerUniqueAddr_1.2.3.2
                        Dest. Resource Address: 172.16.134.0/25
                        options
                                    auto-start: true
                                    ike-key-lifetime: 3600
                                    ipsec-key-lifetime: 28800
                                    keying-retries: 0
                                    rekey-fuzz: 100
                                    rekey-margin: 540
                                    compression: false
                                    encryption: true
                                    no-rekey: false
                                    no-route false
                                    pfs: true
            Connection 2 - 172.16.132.0/25<=>172.16.135.0/25
                        Source Pep address: 1.2.3.13
                        Source Pep identifier: DummyPepConnHandlerUniqueAddr_1.2.3.13
                        Source Resource Address: 172.16.135.0/25
                        Dest. Pep address: 1.2.3.9
```

At the top are the four IPsec connections that were built to support the policy, including a description of the connections that had to be built. Below those are the subnet connections, followed by the firewall policy that reflects what is allowed across the connections, followed by VLAN connections (none, in this case).

Viewing device configurations

Now, view the device configuration:

1. In the network status view, right-click one of the Boston devices such as the distribution switch, and choose Execute Device Command > Show Configuration.
2. Look for the effects of the provisioning commands on the router, including static and dynamic routes, and ACLs.

And view the VLAN connections, including ID, name, IP address, subnet mask, inbound and outbound ACL settings, and ports.

Changing network topology

Suppose you need to allow the sites to communicate with each other.

You can change network topologies very easily. For example, you might prefer a full-mesh connection, instead of a hub-and-spoke. With a full-mesh connection, every site connects to all the others. With a hub-and-spoke, you have to go to each spoke site and build a connection from it to the hub.

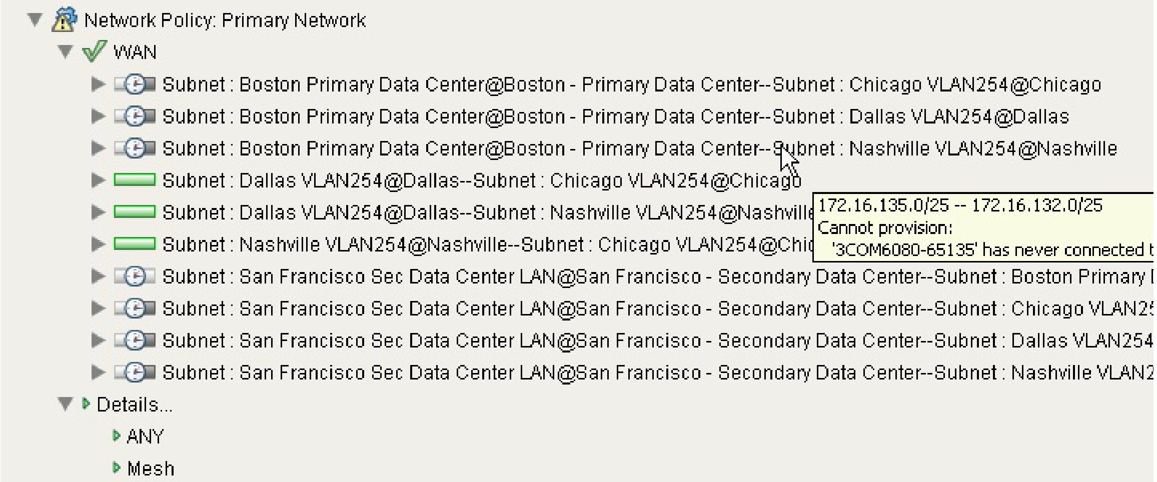
Without OverDrive, it takes a lot of preparation and work for a network engineer to make this change without error.

With OverDrive, it's easy:

1. Right-click the business policy, e.g., Network Policy: Primary Network and choose Edit.
2. Click the configuration drop-down and choose Full Mesh.
3. Click Submit.

   OverDrive figures out what needs to change, or not, and decides what has to be added to current or new connections to satisfy the policy.
4. Check the business status view to be sure traffic flows between all the sites.

   For example, the status view in the following figure has a tooltip showing a problem: cannot provision:



```
▼ Network Policy: Primary Network
  ▼ ✓ WAN
    ▶ Subnet : Boston Primary Data Center@Boston - Primary Data Center--Subnet : Chicago VLAN254@Chicago
    ▶ Subnet : Boston Primary Data Center@Boston - Primary Data Center--Subnet : Dallas VLAN254@Dallas
    ▶ Subnet : Boston Primary Data Center@Boston - Primary Data Center--Subnet : Nashville VLAN254@Nashville
    ▶ Subnet : Dallas VLAN254@Dallas--Subnet : Chicago VLAN254@Chicago
    ▶ Subnet : Dallas VLAN254@Dallas--Subnet : Nashville VLAN254@Nashville
    ▶ Subnet : Nashville VLAN254@Nashville--Subnet : Chicago VLAN254@Chic
    ▶ Subnet : San Francisco Sec Data Center LAN@San Francisco - Secondary Data Center--Subnet : Boston Primary I
    ▶ Subnet : San Francisco Sec Data Center LAN@San Francisco - Secondary Data Center--Subnet : Chicago VLAN25
    ▶ Subnet : San Francisco Sec Data Center LAN@San Francisco - Secondary Data Center--Subnet : Dallas VLAN254
    ▶ Subnet : San Francisco Sec Data Center LAN@San Francisco - Secondary Data Center--Subnet : Nashville VLAN2
  ▼ Details...
      ANY
      Mesh
```

```
172.16.135.0/25 -- 172.16.132.0/25
Cannot provision:
  '3COM6080-65135' has never connected t
```

   In this case, the router is not talking to the DSC. SeeTable 7-1 on page 7-3, which explains that the DSC on the left (for the Boston subnet) has not been deployed.
5. Finally, confirm that all connections are up and all green

Section summary

These steps have illustrated a basic inter-site connection policy connecting sites together. Anyone at any of the sites can access any of the resources on the other sites in this full-mesh network.

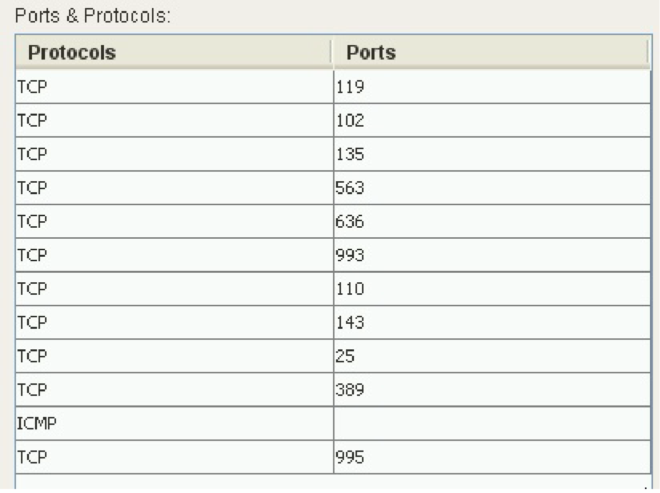
Creating a business policy for a CRM server

Consider a business policy that allows access to a CRM (customer relations management) server. Suppose you have sales people in a collection called Sales. These include all the people in an in-house sales force. When you build the policy, you don't care where the sales people are, or who they are individually. You need to give them all access to the CRM server.

To create the policy and activate it:

1. Create a new local resource named Server-VM: CRM in, for example, the San Francisco - Secondary Data Center.
2. Create a business policy called Business Policy: CRM Access, in a subdomain containing the San Francisco and Boston data centers.
   a. Assign a set of ports and protocols that are specific for the connection.

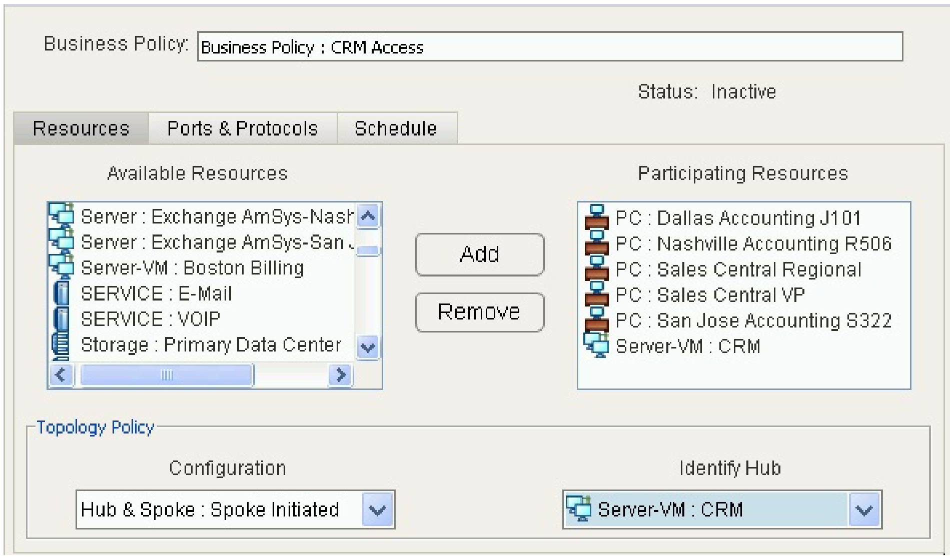
      The following figure shows an example of ports and protocols for an Exchange server, with certain TCP ports; you could possibly add certain UDP ports.



Ports & Protocols:

Protocols	Ports
TCP	119
TCP	102
TCP	135
TCP	563
TCP	636
TCP	993
TCP	110
TCP	143
TCP	25
TCP	389
ICMP	
TCP	995

   b. Assign it resources such as PC: Dallas Accounting J101 and other sales-related resources as shown in the following figure. Also, assign the CRM server:



Business Policy: Business Policy : CRM Access

Status: Inactive

Resources | Ports & Protocols | Schedule

Available Resources
- Server : Exchange AmSys-Nash
- Server : Exchange AmSys-San J
- Server-VM : Boston Billing
- SERVICE : E-Mail
- SERVICE : VOIP
- Storage : Primary Data Center

Add
Remove

Participating Resources
- PC : Dallas Accounting J101
- PC : Nashville Accounting R506
- PC : Sales Central Regional
- PC : Sales Central VP
- PC : San Jose Accounting S322
- Server-VM : CRM

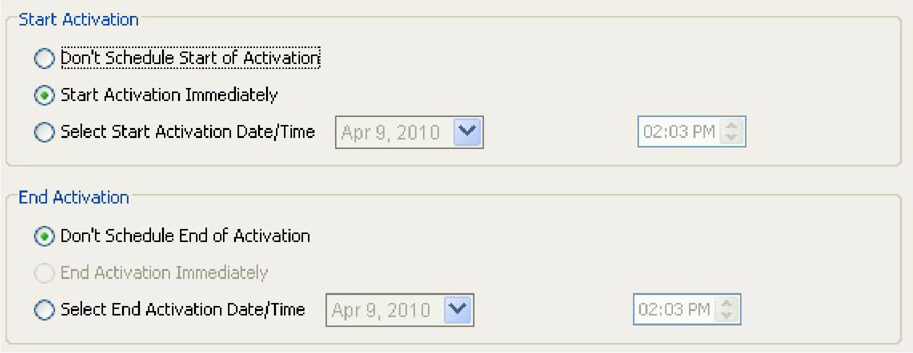
Topology Policy

Configuration: Hub & Spoke : Spoke Initiated

Identify Hub: Server-VM : CRM

c. Choose hub and spoke for the configuration, as shown above, and select the CRM server as the hub.

d. Accept the default scheduler to start immediately, with no end date, or change it as you wish:



Start Activation

○ Don't Schedule Start of Activation
● Start Activation Immediately
○ Select Start Activation Date/Time Apr 9, 2010 02:03 PM

End Activation

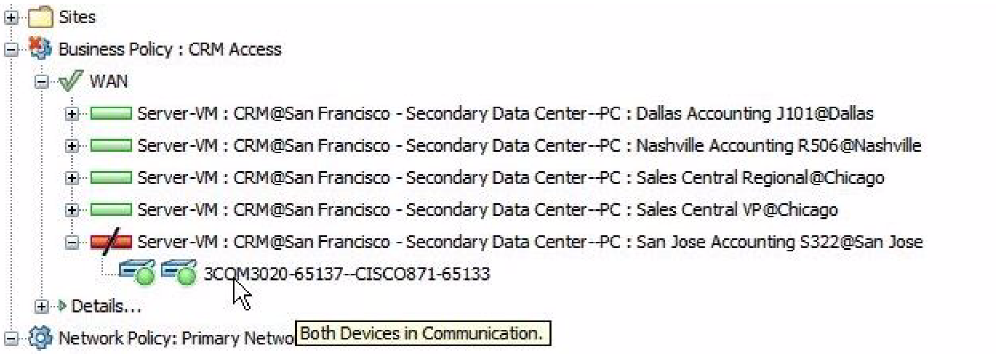
● Don't Schedule End of Activation
○ End Activation Immediately
○ Select End Activation Date/Time Apr 9, 2010 02:03 PM

3. Click Submit.

   OverDrive activates the policy and gives it all the connections needed to satisfy it. The connections should come up quickly.

4. Check the connections in the business status view.

You might see that neither side of a connection comes up, as in the figure below, where the green icons and tooltip signify that the DSCs are up, but haven't yet confirmed a connection between them to support this policy.



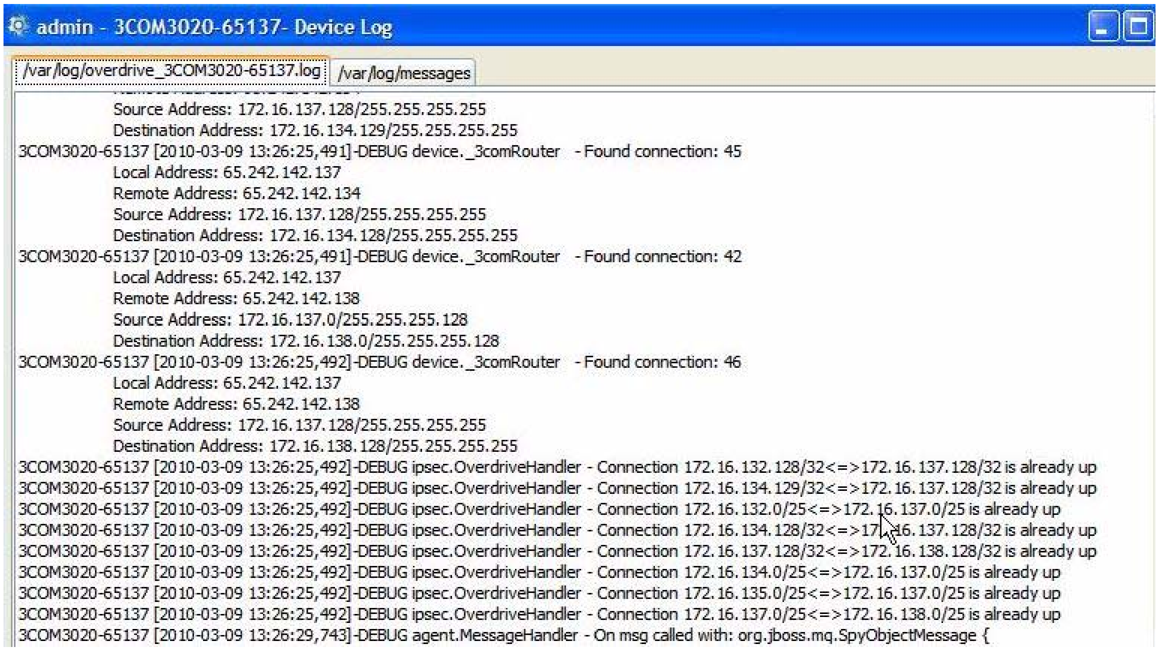
```
Sites
Business Policy : CRM Access
  WAN
    Server-VM : CRM@San Francisco - Secondary Data Center--PC : Dallas Accounting J101@Dallas
    Server-VM : CRM@San Francisco - Secondary Data Center--PC : Nashville Accounting R506@Nashville
    Server-VM : CRM@San Francisco - Secondary Data Center--PC : Sales Central Regional@Chicago
    Server-VM : CRM@San Francisco - Secondary Data Center--PC : Sales Central VP@Chicago
    Server-VM : CRM@San Francisco - Secondary Data Center--PC : San Jose Accounting S322@San Jose
      3COM3020-65137--CISCO871-65133
  Details...
Network Policy: Primary Netwo
```

Both Devices in Communication.

To troubleshoot the connections, you might:

1. Find the DSC in the network status view.
2. Right-click the DSC, and choose View Log.
3. See if the DSC thinks the connection is down for some reason.

You have to be quick, because the connection might come up while you’re looking at the log, as it has below:



admin - 3COM3020-65137- Device Log
/var/log/overdrive_3COM3020-65137.log
/var/log/messages

```
            Source Address: 172.16.137.128/255.255.255.255
            Destination Address: 172.16.134.129/255.255.255.255
3COM3020-65137 [2010-03-09 13:26:25,491]-DEBUG device._3comRouter   - Found connection: 45
            Local Address: 65.242.142.137
            Remote Address: 65.242.142.134
            Source Address: 172.16.137.128/255.255.255.255
            Destination Address: 172.16.134.128/255.255.255.255
3COM3020-65137 [2010-03-09 13:26:25,491]-DEBUG device._3comRouter   - Found connection: 42
            Local Address: 65.242.142.137
            Remote Address: 65.242.142.138
            Source Address: 172.16.137.0/255.255.255.128
            Destination Address: 172.16.138.0/255.255.255.128
3COM3020-65137 [2010-03-09 13:26:25,492]-DEBUG device._3comRouter   - Found connection: 46
            Local Address: 65.242.142.137
            Remote Address: 65.242.142.138
            Source Address: 172.16.137.128/255.255.255.255
            Destination Address: 172.16.138.128/255.255.255.255
3COM3020-65137 [2010-03-09 13:26:25,492]-DEBUG ipsec.OverdriveHandler - Connection 172.16.132.128/32<=>172.16.137.128/32 is already up
3COM3020-65137 [2010-03-09 13:26:25,492]-DEBUG ipsec.OverdriveHandler - Connection 172.16.134.129/32<=>172.16.137.128/32 is already up
3COM3020-65137 [2010-03-09 13:26:25,492]-DEBUG ipsec.OverdriveHandler - Connection 172.16.132.0/25<=>172.16.137.0/25 is already up
3COM3020-65137 [2010-03-09 13:26:25,492]-DEBUG ipsec.OverdriveHandler - Connection 172.16.134.128/32<=>172.16.137.128/32 is already up
3COM3020-65137 [2010-03-09 13:26:25,492]-DEBUG ipsec.OverdriveHandler - Connection 172.16.137.128/32<=>172.16.138.128/32 is already up
3COM3020-65137 [2010-03-09 13:26:25,492]-DEBUG ipsec.OverdriveHandler - Connection 172.16.134.0/25<=>172.16.137.0/25 is already up
3COM3020-65137 [2010-03-09 13:26:25,492]-DEBUG ipsec.OverdriveHandler - Connection 172.16.135.0/25<=>172.16.137.0/25 is already up
3COM3020-65137 [2010-03-09 13:26:25,492]-DEBUG ipsec.OverdriveHandler - Connection 172.16.137.0/25<=>172.16.138.0/25 is already up
3COM3020-65137 [2010-03-09 13:26:29,743]-DEBUG agent.MessageHandler - On msg called with: org.jboss.mq.SpyObjectMessage {
```

CHAPTER 5

Configuring clouds

This chapter tells you how to set up your OverDrive environment in order to be able to offer cloud services and VMs to clients and users.

- Install type: clouds
- Introducing clouds
- Introducing metamodels
- Creating clouds
- Supplying the right answers to the configurator
- Working with lists of clouds
- Working with clouds in domain models
- Scenario 3a: creating and configuring a cloud

Note Your network's structure, and its access and business policies, must be set up before you can successfully configure cloud services. Clouds are like subdomains in many respects.

See Chapter 6, "Enabling VMs" for creating VMs once you have created the appropriate clouds or subclouds.

Install type: clouds

Of the install types that OverDrive manages (site-to-site, intra-site, and cloud), cloud installations let you create and configure:

- Virtual private clouds (VPCs) that may contain other clouds and VMs
- Virtual data centers (VDCs), which may contain VMs

Introducing clouds

There are three distinct ways to use OverDrive, one of which is to provide cloud services, as described in this chapter. Cloud services combine VLAN management with business policies to automate provisioning of network resources and policies in response to requests for creating virtual machines (VMs).

Previous chapters have described using OverDrive for access control:

- For network access control, as described in Chapter 3, "Controlling intra-site network access," which explains how to use VLAN management and Active Directory to let users access the network.
- For business access control, as described in Chapter 4, "Controlling intra-site business access,"which describes how to use business policies to permit people to connect various resources at one site or another.

Clouds are segregated deployments of virtual computers. A cloud instance can be as complicated as an entire customer VPC with multiple complex configurations of VLANs and network services, or as simple as a single LAN segment with a collection of virtual machines.

The OverDrive NSV platform provides multiple cloud instances to satisfy both enterprise and service provider requirements for cloud services. OverDrive models the cloud as a set of resources and policies, therefore providing flexibility in how you define clouds and what you can do with cloud resources once they are created. For example:

- Service providers may define vCOMs (cloud operational models) to separate how cloud instances are distributed among network resources, e.g., offering a public cloud accessible from the internet and a private cloud accessible across the service provider's private MPLS network or via the Internet.
- Separate customers might purchase VPCs or cloud environments provided by cloud service providers who sell a cloud instance to each customer. These instances may be further subdivided into units that customers can allocate to their departments or divisions.
- Enterprises might construct VDCs that have one or more VLANs to support virtual machines, e.g., an enterprise might want to offer a virtual data center for their billing department and another for their sales department.

OverDrive enables a domain for cloud management by assigning a cloud metamodel to it. The OverDrive administrator will need to activate the cloud environment on the stack of network equipment by assigning it to the site and by setting the pools of resources (VLANs and subnet address scope).

A service provider may use the REST API that is provided by OverDrive to construct a portal to manage cloud operations.

OverDrive provides a Cloud Configurator which makes use of this REST API for this purpose to both enterprises and service providers. It may be used as a reference for the construction of a customer-facing portal of your own.

You define clouds using the OverDrive Cloud Configurator user interface, which provides the following features.

- Lists of clouds—visible to you and anyone you choose, including people to whom you provide the Cloud Orchestration Manager as described in *Providing VMs*
- Creation of new clouds based on metamodels—available to admins within your own or your client organizations
- Configuration of VLAN, DNS, DHCP, and NAT—for admins only
- Creation and deployment of cloud services based on clouds already created—suitable for self-service customers

- Creation and deployment of virtual machines within clouds—for self-service customers

Introducing metamodels

OverDrive provides and allows the construction of metamodels, which are represented by XML documents that describe the types of clouds and VMs that can be created with vCOM. These metamodels are accessible via the REST API and can be used to constrain and set attributes for a customized customer portal to present to end users.

Metamodels can therefore constrain the process of creating clouds with specific features. They contain parameters that may or must be specified when a cloud is created. OverDrive presents these in user-visible, usually editable, fields, often within a panel with related fields and choices. The same is true for VMs.

In other words, metamodels determine which parameters can actually be configured, as described by example in subsections in the "Supplying the right answers to the configurator" section on page 5-7.

Metamodels for a network may be set up during installation of OverDrive, or as written or adapted by OverDrive administrators. They generally are company-specific, as each company has its own way of representing its network.

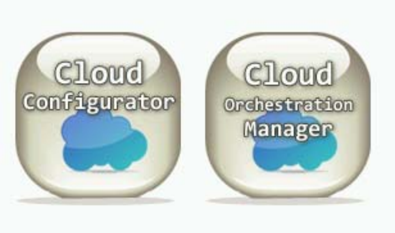
The main concept of metamodels is that they can be deployed like easily modified cookie cutters to speed up and simplify cloud deployments. Used in conjunction with the OverDrive REST API, the metamodels become tools that allow service providers to set attributes that will be made available to users from the OverDrive Configurator or a customized portal.

Creating clouds

The browser-based Cloud Configurator is a good example of the use of the REST API to create clouds.

To create clouds:

1. Access the configurator via the URL https://HostName:8443/vcom:

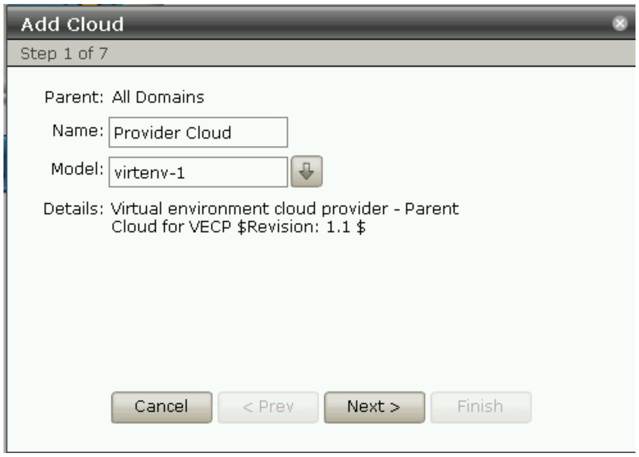


2. Click Cloud Configurator to access the login dialog.
3. Enter your user name and password, then click Login.

Note If there are already clouds defined, they are listed in the window that appears. Go to the "Working with lists of clouds" section on page 5-10.

4. Click the add cloud button in the upper right:

5. Enter the cloud name, choose a model from the drop-down list, as suggested in the following figure, and click Next.



Add Cloud
Step 1 of 7

Parent: All Domains
Name: Provider Cloud
Model: virtenv-1
Details: Virtual environment cloud provider - Parent Cloud for VECP $Revision: 1.1 $

The metamodel behind step 1

The XML metamodel, a behind-the-scenes document for the current user, looked something like this:

```
<metamodel name="virtenv-1" type="cloud">
<description>Virtual environment cloud provider - Parent Cloud for VECP $Revision: 1.1
$</description>
. . .
```

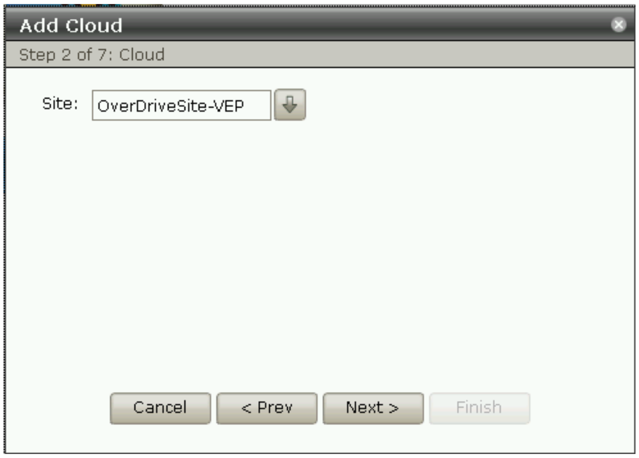
OverDrive searched through various metamodels that had been previously imported into its database, looking for every metamodel of type cloud, provided that it was not actually a subcloud. For each one it found, it populated the drop-down list for the Add Cloud window, and, when the user chooses a cloud in that list, presents that cloud’s description in the detail area.

How did OverDrive know if a metamodel were for a subcloud or not? It would have noticed if the <metamodel> element had been placed inside a <metamodels> element. For example:

```
<metamodel name="virtenv-1" type="cloud">
    <metamodels>
        <!-- subclouds are defined by a metamodel within metamodels -->
        <metamodel name="customer" type="cloud">
    </metamodels>
. . .
<metamodel>
```

Assigning a cloud to a site

When you add a cloud, the second step is to assign it to a site in the domain in which you are adding it. The Cloud Configurator automatically presents, for Step 2, a drop-down list of available sites, for example:



Site: OverDriveSite-VEP

Notice there is a tooltip saying, “Site to which the cloud is assigned.” For this and the remaining panels, each field or checkbox has a tooltip.

The cloud you create will be provisioned at that site.

How the metamodel determines the parameters per screen

OverDrive automatically decides which screens are shown in which order and with which parameters.

So far, we have created a VPC, that is, a cloud as might be suitable for a company that provides clouds to customers. The clouds it provides them are VCDs, or subclouds, perhaps one per customer, with perhaps levels of subclouds below them.

Clouds define network and business policies, resources, and so on, at the cloud or a lower level. This allows VMs to be created within them. It also allows the VMs to be managed by OverDrive’s network virtualization. The clouds might be configured to include DNS hosts for the cloud, VLAN pools, company-specific parameters, and perhaps DHCP service or NAT address translation ranges. Metamodels make it easy to set up these configurations, because they pre-supply parameters that can be tweaked by the user of the Cloud Configurator. They can be edited in the Command Center.

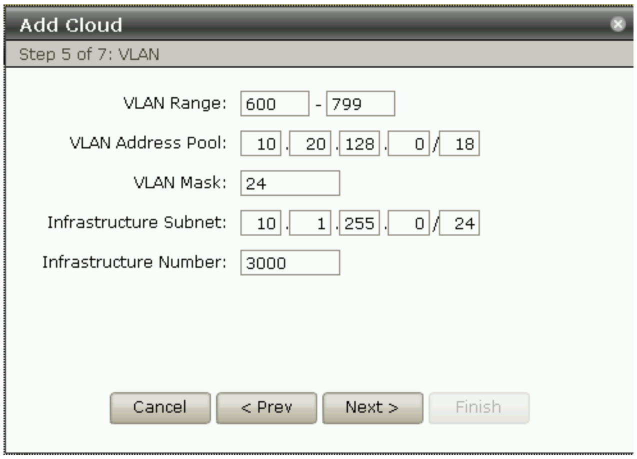
The Cloud Configurator marshals these configuration details into panels of related data fields, placing, for example, VLAN-related details on one panel, and NAT-related details on another. The number of panels (steps in the configuration) depends on the parameters specified in the metamodel for a cloud.

For example, consider the following parameters section of a metamodel. Any parameter whose name begins with tmpl or cloud is a candidate for being placed in a Cloud Configurator dialog box. If tmpl is followed by cloud, the parameter is a candidate for a dialog box when a cloud is being created; if followed by vm, then it is a candidate when a VM is being created, and so on.

The XML below produces two dialog boxes: one for VLAN parameters, and one for DNS. Because Step 1 is taken up by just choosing a metamodel and naming the resulting cloud, and Step 2 for assigning a cloud to a site, the following would specify Steps 3, and 4.

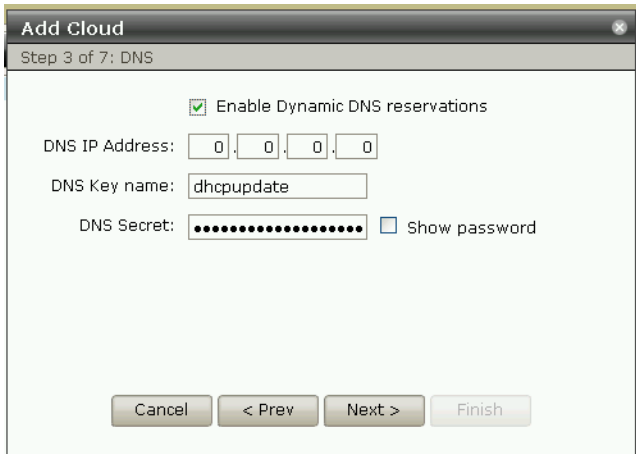
```
<metamodel name="virtenv-1" type="cloud">
    <description>Virtual environment cloud provider - Parent Cloud for VECP $Revision:
1.1 $</description>
. . .
    <parameters>
        <!-- Properties defined by the cloud metamodel type -->
        . . .
        <parameter name="tmpl.cloud.vlan.range" type="dt.range.vlanRange"/>
        <parameter name="tmpl.cloud.vlan.pool" type="dt.subnet"/>
        <parameter name="tmpl.cloud.vlan.mask"

type="dt.integer.subnetMask">27</parameter>
```

The dialog box that appears according to the tmpl.cloud.vlan.* parameters above is, for an example, as follows (the values here have been filled in by an actual metamodel):



VLAN Range: 600 - 799
VLAN Address Pool: 10 . 20 . 128 . 0 / 18
VLAN Mask: 24
Infrastructure Subnet: 10 . 1 . 255 . 0 / 24
Infrastructure Number: 3000

The following XML would result in a dialogue such as the following (again, where the values have been filled in by an actual metamodel):



☑ Enable Dynamic DNS reservations
DNS IP Address: 0 . 0 . 0 . 0
DNS Key name: dhcpupdate
DNS Secret: ●●●●●●●●●●●●●●●●●●● □ Show password

```
        <parameter name="tmpl.cloud.dns.enable"

type="dt.boolean">true</parameter>
        <parameter name="tmpl.cloud.dns.address" type="dt.ipaddress"/>
        <parameter name="tmpl.cloud.dns.credential" type="dt.password"/>
        <parameter name="tmpl.cloud.dns.key" type="dt.string"/>
        . . .
    </parameters>
. . .
</metamodel>
```

If the parameter is not known to OverDrive, the configurator will group it with any other unknown parameters and display them in a final panel, named Advanced.

Supplying the right answers to the configurator

To summarize so far: the Cloud Configurator lets you create clouds based on metamodels that specify parameters such as subnet address ranges, VLAN ranges, whether DNS is enabled and with which credentials and keys, the kinds of VMs that can be chosen, and so on. As mentioned above, this determines which panels open for you during the configuration, how many fields there are, and what type of information can be collected.

This section describes:

- The various subnets that you may need to understand if you are to supply addresses for the various address pools.
- The fields, lists, and checkboxes that you are likely to see presented for either your editing or information.

Note The particular fields that you see, their order and grouping, depend on the metamodels available to you, plus any customization, therefore we just present the more common details that you might supply.

Understanding address pools

OverDrive managed networks are assumed to have subnets and groups of IP address pools within which the networks exist. In OverDrive, these subnets and pools constitute what we call a coherent region. Every cloud and VLAN, for example, has to be encompassed within the subnets in the coherent region.

The coherent region is a group of subnets defined at generally high levels of the domain tree. They affect the tree all the way below the level at which they are defined. The coherent region doesn't have to be at the highest level. But, since it defines the subnets available to lower levels, it helps to place the coherent region higher. In practical terms, you might leave ROOT free from coherent region(s) and define them at customer levels below ROOT

Note that there might be subdomains which sub-administrators see as their top-level domain. They might not know there are higher domains. If you administer only subdomains, whoever assigned them to you should enter the subnets available in the comment field of the highest level domain to which you are assigned.

To check for subnets for a domain:

1. Right-click the domain and choose Edit.
2. Click the Subnets tab to see if they are specified there.
3. If not, click the Comment tab to see which ones you can use.

4. If there are no subnets in the Subnets or Comment tab, contact the administrator who assigned you to the domain.

For more on configuring subnets for domains, sites, and VLANs irrespective of clouds, see the following subsections:

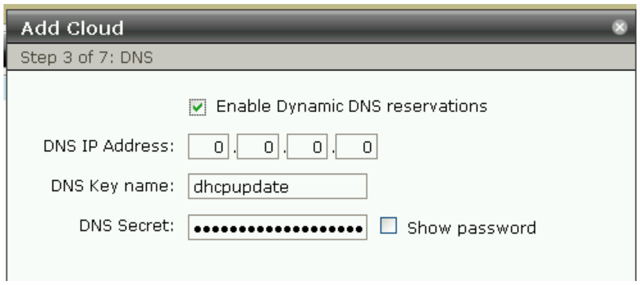
- Configuring subnets, page 2-2
- Creating site subnets, page A-4
- Allocating VLANs to sites, page 2-5

DNS parameters

When DNS is enabled, VMs created by OverDrive will have all interfaces dynamically registered with the DNS server prior to their being powered up.

Note The address of interface 0 will be registered in DNS.

A company using OverDrive may decide to rather have the DHCP server manage DNS reservations for their virtual machines, in which case OverDrive will not be requested to manage DNS reservations.


Add Cloud

Step 3 of 7: DNS

☑ Enable Dynamic DNS reservations

DNS IP Address: 0 . 0 . 0 . 0

DNS Key name: dhcpupdate

DNS Secret: ••••••••••••••••••• □ Show password

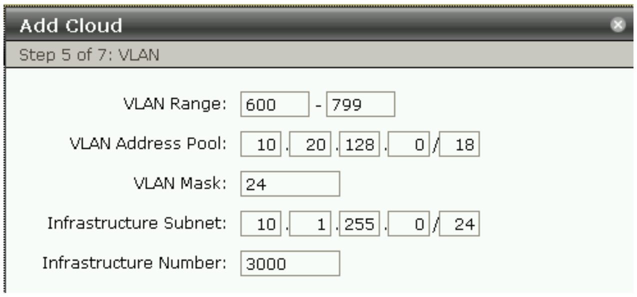
To specify DNS parameters:

1. Check Enable DNS lookups to enable the other fields in the panel.
2. Provide the IP address of the DNS server.
3. Provide credentials and a password (key).

   The credentials in this dialog are typically a username (account) but may also be a fully qualified domain name. The password is for the account that will run the DHCP server service.
4. Check Show password to see the actual characters you enter into the Key field, rather than the default asterisks that hide them.

VLAN parameters

The VLAN panel lets you define the pool of VLAN resources available in this cloud.



Add Cloud

Step 5 of 7: VLAN

VLAN Range: 600 - 799
VLAN Address Pool: 10 . 20 . 128 . 0 / 18
VLAN Mask: 24
Infrastructure Subnet: 10 . 1 . 255 . 0 / 24
Infrastructure Number: 3000

1. Enter the range of VLAN numbers for this cloud.

   The range specifies the entire set of VLANs for use by the cloud. This pool of VLANS will be used to draw from when assigning VLANs to clouds as they are needed.

2. Enter the starting IP address and VLAN mask for the VLAN address pool.

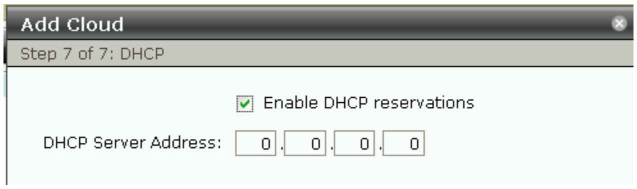
This is the pool of addresses that will be drawn from when VLANs are created. The mask defines the size of the pool and, consequently, the maximum number of VMs that can exist on that VLAN.

VLAN parameters (proprietary)

Any additional parameters you may see in the VLAN panel are company-specific, specifying perhaps a particular VLAN number and VLAN subnet for an infrastructure enclosure. Enter them as appropriate.

DHCP parameters

If you enable DHCP, OverDrive configures an IP Helper address for each VLAN that is created. This allows VMs to get an IP address from the DHCP server you specify.



Add Cloud

Step 7 of 7: DHCP

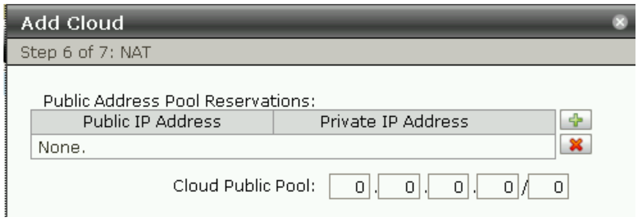
☑ Enable DHCP reservations

DHCP Server Address: 0 . 0 . 0 . 0

1. Check Enable DHCP reservations to enable the server address field.
2. Enter the IP address of the DHCP server.

NAT parameters

The NAT panel lets you provide a pool of public addresses that will be drawn from when creating public VMs. NAT rules are configurations that translate between the VM’s public address and its address on the public cloud VLAN.



Public Address Pool Reservations:

Public IP Address	Private IP Address
None.	

Cloud Public Pool: 0 . 0 . 0 . 0 / 0

1. In the Cloud Public Pool field, specify the pool of addresses to be made available to this cloud.

   This pool defines the entire public IP address pool for the cloud.
2. Click the add button to add any static NAT rules for public-to-private address mappings.
3. Enter the public and private IP address mappings.
4. Press Return to accept them.
5. Continue with Step 2 to add more, or click in a table row to edit the addresses within it.

   Click the delete button to delete a row.
6. Click Next or Create when finished.

Note If there are other tabs, such as Advanced, there will be more parameters. The models are company-specific.

Advanced parameters

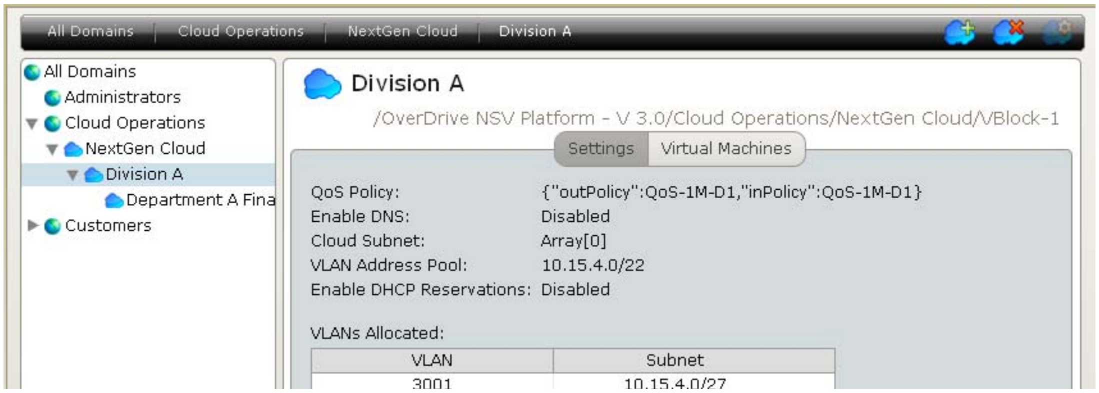
The Advanced tab appears when the metamodel configures parameters and settings that OverDrive has not been told to configure on other panels.

OverDrive uses the Advanced tab to display such parameter, their initial settings, and so forth

1. Enter information as appropriate.
2. Click Create to create the cloud.

Working with lists of clouds

When your cloud is created, you return to the initial dialog, with the cloud now listed in the domain tree on the left and pre-selected, for example:



Division A

/OverDrive NSV Platform - V 3.0/Cloud Operations/NextGen Cloud/VBlock-1

QoS Policy: {"outPolicy":QoS-1M-D1,"inPolicy":QoS-1M-D1}
Enable DNS: Disabled
Cloud Subnet: Array[0]
VLAN Address Pool: 10.15.4.0/22
Enable DHCP Reservations: Disabled

VLANs Allocated:

VLAN	Subnet
3001	10.15.4.0/27

1. If the cloud is not the one you expected, go to the domain with the cloud you want, and click the correct cloud.
2. Notice, under the Settings tab, various IP addresses, whether DHCP is enabled or not, the VLAN range, and allocated VLANs.
3. Click the Virtual Machines tab to open a table showing internal and/or external IP addresses for any VMs that might have already been defined for this cloud.

   If any VMs have already been defined, they will be listed, along with their current status. Notice the MAC addresses for the internal machines. For details on setting up the VMs, see Chapter 6, "Enabling VMs."
4. Use the cloud buttons in the top toolbar for the following functions:

Create a new cloud	+
Delete selected cloud	✗
Edit selected cloud	⚙

Working with clouds in domain models

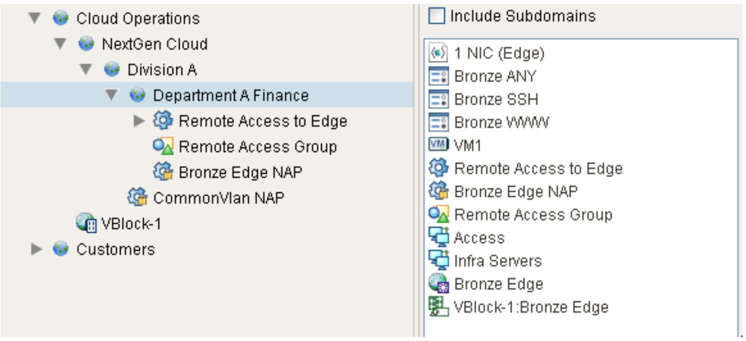
If you are an OverDrive administrator, you can use the Command Center to view detailed contents of the clouds.

If you are not an OverDrive administrator, but you have access to the Cloud Configurator, you may see some read-only information about various cloud aspects such as policies.

A subcloud context and summary contents

Clouds are very much like domains, except they contain additional information for managing dynamic cloud resources. They may, like domains, contain sites, business policies, and other domains or clouds.

Figure 5-1 An example cloud and subcloud



Cloud Operations
NextGen Cloud
Division A
Department A Finance
Remote Access to Edge
Remote Access Group
Bronze Edge NAP
CommonVlan NAP
VBlock-1
Customers

□ Include Subdomains

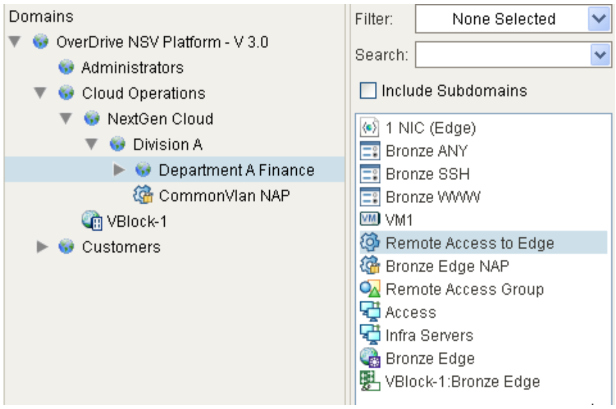
1 NIC (Edge)
Bronze ANY
Bronze SSH
Bronze WWW
VM1
Remote Access to Edge
Bronze Edge NAP
Remote Access Group
Access
Infra Servers
Bronze Edge
VBlock-1:Bronze Edge

For example, the domain Cloud Operations, above, contains a hierarchy of subclouds, including:

- A VPC named Division A, and within that, a VDC named Department A Finance.
- Department A Finance contains a metamodel named 1 NIC (Edge), plus access policies, collections, and so on.

Business policies within a cloud

If you clicked on the Remote Access to Edge business policy in the summary view:

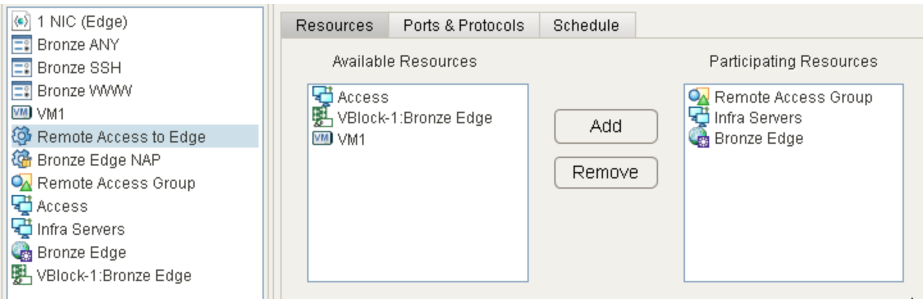


Domains
OverDrive NSV Platform - V 3.0
Administrators
Cloud Operations
NextGen Cloud
Division A
Department A Finance
CommonVlan NAP
VBlock-1
Customers

Filter: None Selected
Search:
□ Include Subdomains

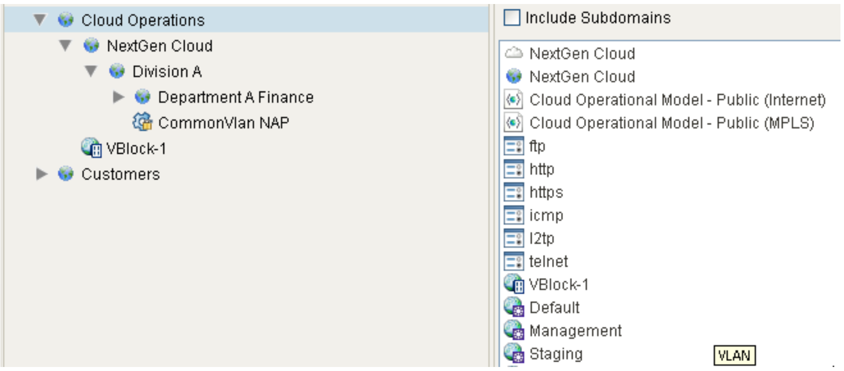
1 NIC (Edge)
Bronze ANY
Bronze SSH
Bronze WWW
VM1
Remote Access to Edge
Bronze Edge NAP
Remote Access Group
Access
Infra Servers
Bronze Edge
VBlock-1:Bronze Edge

To its right, in the Resources tab, you would see the participating resources, and the available resources, including VM1, as in the following figure:



A cloud’s summary view

Finally, if you clicked on domain containing clouds, you would see its summary view:



Here, the summary view lists a subcloud NextGen Cloud), ports and protocols (ftp, http, et al.), policies, collections, resources, switches, and so on.

A cloud’s metamodel

The summary view of a parent cloud shows the various cloud components.

1. Click the cloud.
2. Click a cloud component in the summary view.
3. Notice the metamodel used to create the component.

Scenario 3a: creating and configuring a cloud

Suppose you are an enterprise admin and you want to make it possible for several business units to create their own virtual data center (VDC).

Assume as a starting point that the metamodel has been created with a basic VDC defined in it that has one VLAN plus VMs that can attach to it.

1. Create a cloud according to a metamodel (Creating clouds, page 5-3).
2. Assign the cloud to a site (Assigning a cloud to a site, page 5-5).

3. Configure the cloud: parameters, address pools, DNS, VLAN, DHC, NAT (Supplying the right answers to the configurator, page 5-7).
4. Assume that the metamodel has created business policies, resources, et al.
5. Check the cloud’s summary and metamodel (A cloud’s metamodel, page 5-13).
6. Create a VM and log into it (“Enabling VMs in a cloud” section on page 6-1).
7. Create a second cloud for the second business unit.
8. Create a VM in the second cloud.
9. Optionally, try pinging one cloud from another.
10. Create a business policy that enrolls both the VLANs together.
11. Then, verify that you can ping from one VM to the other now that the business policy permits it.

CHAPTER 6

Enabling VMs

This chapter tells you how to use what you have set up so far. With your policies, sites, and network in place, you can offer VMs in an OverDrive-managed environment to your end users.

- Introducing VMs in OverDrivee
- Enabling VMs in a cloud
- Adding a virtual machine
- Powering on virtual machines
- Removing virtual machines
- Checking VMs in the command center
- Scenario 3b: VMs in clouds

Introducing VMs in OverDrive

At this point, you have automated provisioning of network resources and policies in response to requests for creating virtual machines (VMs). You have configured VLAN management. Your business policies allow people and resources to connect to resources across the networks. You have created the appropriate cloud or clouds to contain your VMs.

Enabling VMs in a cloud

Once you have defined a cloud with the various IP addresses, DHCP service, and VLAN range appropriate for your purpose, you can create, remove, or edit virtual machines.

Note To create VMs, OverDrive uses a VMware vCenter environment.

The general flow for creating a VM is as follows, assuming that the cloud already exists:

1. You select a cloud to contain the VM, provide a name, and choose a from some VM parameters offered by an appropriate metamodel.

Note The choice of available VM parameters is defined by the VM metamodel used in the cloud metamodel. This means, for instance, that you may be able to create a VM within a cloud, or you may have to create a subcloud and then create a VM within it.

2. The NSV engine (i.e., the policy server) uses the information in the VM metamodel to provision the VM. This information includes the VMware template VM name, which identifies one of the VMs registered in vCenter. This template serves as the seed image to be cloned into the VM.
3. The NSV engine provisions the VM by initiating a VM creation request to the DSC (agent), which provides the interface to vCenter.
4. The DSC prepares a request to clone the seed image into a VM and initiates that request to vCenter.

Note Someone must have first created a seed VM in vCenter with appropriate OS, networking, application suite, and data as appropriate to the purpose. The VM template is a complete machine, including the OS, waiting for the clone request. See the *Cisco OverDrive 4.0 Installation Guide* for more details.

5. Once the VM has been successfully cloned, the DSC initiates a request to customize the VM and its guest OS to match your chosen VM parameters. At this point in the VM life cycle, the VM is ready to be powered up. It is independent from the seed.

For clouds with DHCP support, OverDrive sets the IP helper address so that the VM can get DHCP addresses for all of its interfaces. This ensures that when the VM powers on and uses DHCP to discover its address, the address will already be assigned.

Note Alternatively, OverDrive uses a subnet range at cloud creation time to assign IP addresses to VMs.

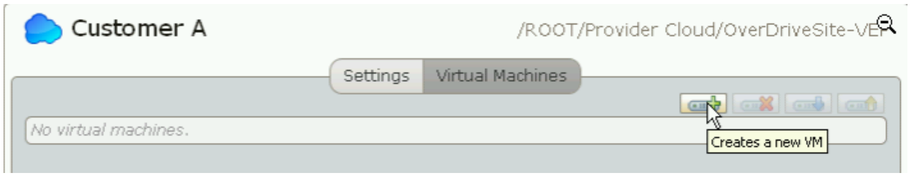
Adding a virtual machine

OverDrive provides two user interfaces for users to add VMs:

- In Cloud Configurator, the new VM toolbar button, as described below.
- In Cloud Orchestration Manager, the view cloud button. (The orchestration manager is designed for a privileged end user with some training.)

To add virtual machines:

1. Highlight the appropriate cloud in the domain tree and click its Virtual Machines tab, then its add VM button, for example:

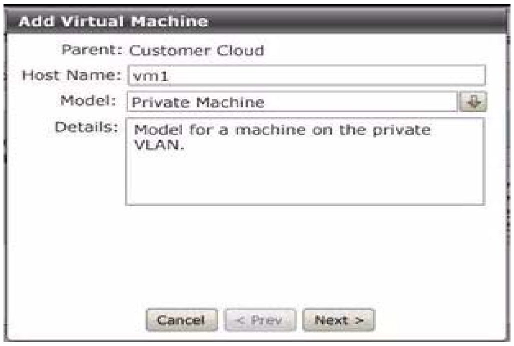


No virtual machines.

The Add Virtual Machine dialog displays.

Note If the new VM button does not light up, your cloud's metamodel does not contain a VM metamodel. Try creating a subcloud, and then the VM within it.

2. Specify the hostname, choose the model, and verify from the details that it is the right model, for example:


Add Virtual Machine

Parent: Customer Cloud

Host Name: vm1

Model: Private Machine

Details: Model for a machine on the private VLAN.

The metamodel may ask for or implicitly set access modes for the VM such as how many communication interfaces can be set; or which network interfaces are to be assigned to which VLANs.

Note As specified in this particular metamodel, a private VM has a single interface attached to the private VLAN; a public VM has two interfaces, one attached to the public VLAN and one attached to the private VLAN. A storage VM has one interface on the storage VLAN. This is all entirely metamodel-dependent.

3. Click Next or Create, depending on the metamodel that is driving the VM's creation parameterization.
4. If the metamodel specifies VM parameters to display and be edited or approved, you may see a panel asking how many MB of virtual memory to use, where 1024 MB is the equivalent of 1 GB.
5. Click Finish to create the VM.

Your VM should show up in a series of stages including creating, configuring interfaces, and powered off, resulting eventually in a display showing its IP address and hostname.

Powering on virtual machines

Use the deploy button to power on the VM that you have made. For example:

1. Highlight the VM and click the deploy button.
2. Observe that the VM's status changes to powered on.
3. At this point, you can provide directions for someone else to access the VM by IP address or hostname.

Removing virtual machines

To remove a VM:

1. Make sure it is not in use.
2. Highlight it and power it off using the undeploy button.

   This gracefully powers off the VM but does not delete it. For a VM that is only intermittently used, you need the undeploy functionality: if you just shutdown from within the VM itself (as a user might when finished with his task), OverDrive will power it right back on to make sure its deployed.
3. Use the delete button to remove it.

Note Any changes made by a user to the VM are entirely lost.

Checking VMs in the command center

For VMs, the Command Center lets you

- Display and edit VM property values on a per-VM basis
- Display and edit VM metamodels

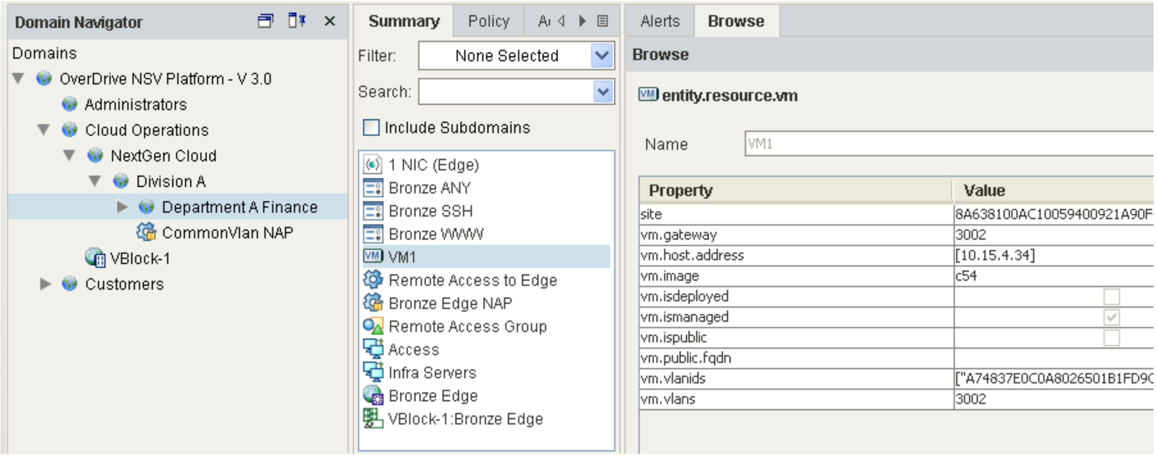
Viewing and editing VM entity resources

Entity resources are the property/value pairs comprising the VM's configuration information as known to the Command Center.

To view and edit these resources:

1. 1.In the domain tree, highlight the subcloud containing the VM.
2. 2.In the summary view, double-click the VM or right-click it and choose Edit. (If you have just created it, it will appear at the end of the summary view list.)

The VM's entity resource table appears, for example:



Filter: None Selected

Search:

□ Include Subdomains

Name VM1

Property	Value
site	8A638100AC10059400921A90F
vm.gateway	3002
vm.host.address	[10.15.4.34]
vm.image	c54
vm.isdeployed	□
vm.ismanaged	☑
vm.ispublic	□
vm.public.fqdn	
vm.vlanids	["A74837E0C0A8026501B1FD9C
vm.vlans	3002

The properties and their values are:

- site—The value is a UID representing the site to which the VM's cloud is attached, and consequently the VM itself.
- vm.host.address—The IP addresses of the VM's interfaces.
- vm.image—The name of the VM seed image in the vSphere collection of VMs.
- vm.isdeployed—Whether the VM is currently supposed to be powered on.
- vm.ismanaged—Managed VMs will be created or deleted by the DSC as needed. Unmanaged VMs will be recognized by the DSC as belonging to policy, but will not be actively managed (that is, they will not be created or destroyed).
- vm.ispublic—Whether the VM has a public address.
- vm.public.fqdn—If there is a public address, the fully qualified domain name.
- vm.vlans—The list of VLAN numbers associated with this VM.

3. Edit the values if necessary and click Submit.

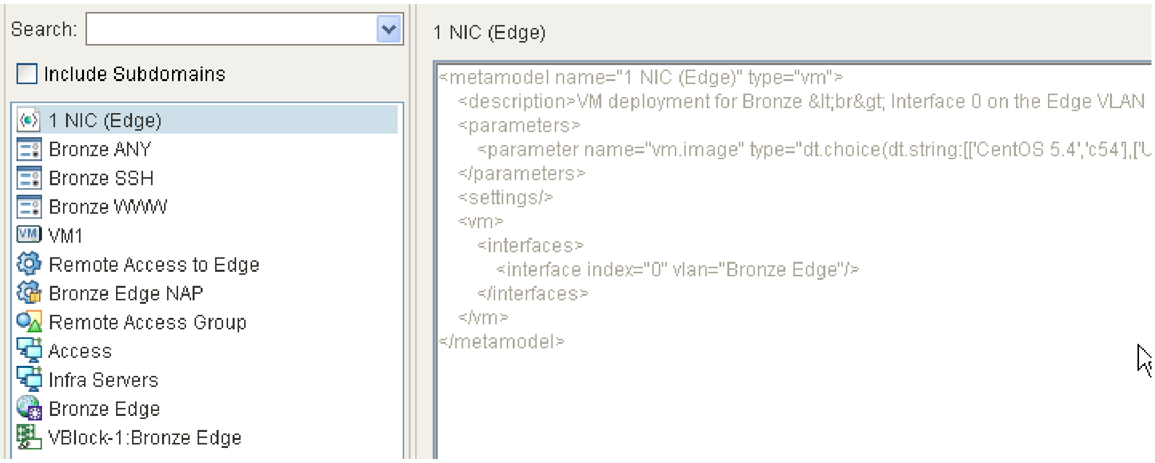
Note The only property here that can constructively change is vm.isdeployed. OverDrive does not, for example, change the VLAN connections on a created VM if you edit the vm.vlans property.

Viewing and editing VM metamodels

You can view and edit the metamodel used for creating a particular VM.

1. In the domain tree, highlight the subcloud containing the VM metamodels you want to see or edit.
2. In the summary view, double-click the VM metamodel or right-click it and choose Edit. (The interfaces are generally listed above the VM itself.)

   For example, the following screen opens if you clicked the metamodel named 1 NIC VM (Edge) in the preceding figure:



```
<metamodel name="1 NIC (Edge)" type="vm">
  <description>VM deployment for Bronze &lt;br&gt; Interface 0 on the Edge VLAN
  <parameters>
    <parameter name="vm.image" type="dt.choice(dt.string:[['CentOS 5.4','c54'],['U
  </parameters>
  <settings/>
  <vm>
    <interfaces>
      <interface index="0" vlan="Bronze Edge"/>
    </interfaces>
  </vm>
</metamodel>
```

3. Click Cancel to close without editing.
4. Click Submit if you have changed the metamodel.

Note Changing the metamodel does not change anything that already exists when you make the change—but only the next time a VM or other object is created.

Scenario 3b: VMs in clouds

To enable a VM:

1. Add it.
2. Power it on.
3. Confirm it in the command center.
4. Remove it.

CHAPTER 7

Monitoring network status

This chapter describes some of the techniques you can use in monitoring the status of the network you have created.

- Network and hardware status view
- Business status view

The structure of the status views includes information that can help you verify that the intent of configured policy matches what is actually being provisioned, including:

- Pairs of resources with communication between them enabled
- Resources disconnected because of missing or misconfigured policy.

Network and hardware status view

The network status view shows the status of sites and managed network devices. Sites are marked with a red [x] if the network device is not connected and working, or if there is a known issue, like unmanaged VLANs not listed for the domain.

You can mouse over a network device to see its status, as shown in the following figure.

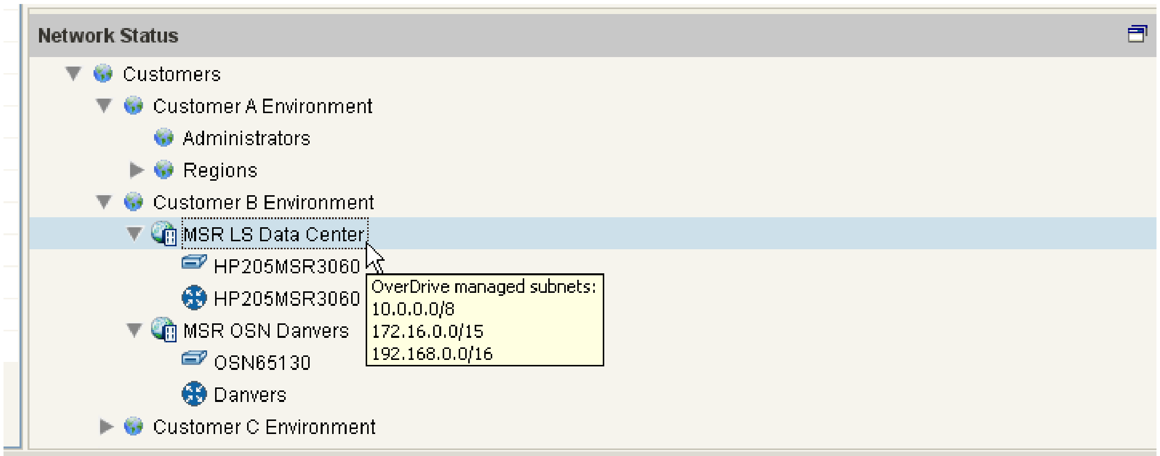
To display this view:

1. Click the Network Status tab in the lower-left of the status view.
2. Verify that you see a view comparable to the one in Figure 7-1 on page 7-2

Typical hover text reports business policy and device status such as:

- OverDrive managed subnets assigned to that site
- DSC IP address, connection up or down, heartbeat
- Router or switch IP address, functioning status

Figure 7-1 Network status view



OverDrive managed subnets:
10.0.0.0/8
172.16.0.0/15
192.168.0.0/16

You can quickly spot malfunctioning devices and respond to outages and potential performance problems.

For a DSC, you can right-click and examine the following information:

- Logs—There are two real-time logs, each selectable under their own tab: **/var/log/messages** and **/var/log/overdrive.log**. These are updated as logged events occur.
- Active policy—A static display of IPSec connections and their details; a list of which sites and IP addresses are connected; the firewall policy in effect for each device; and the VLAN connections.

For a router or switch, you can right-click, choose Execute Device Command, and see the following:

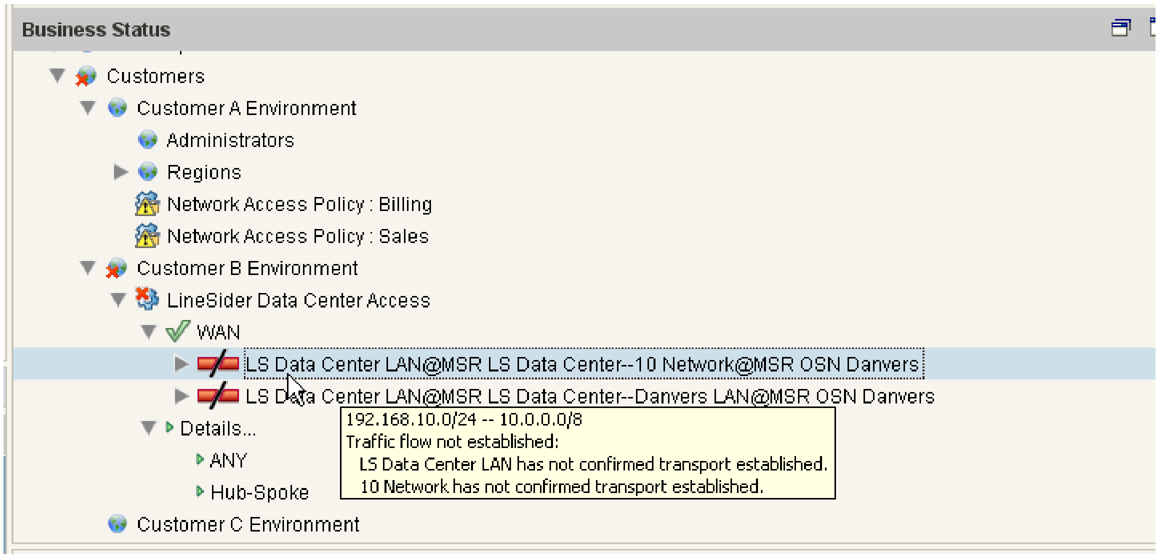
- Configuration details
- Interfaces
- Routes

The network hardware status view also lets you generate a site compliance report. See the "Creating site compliance reports" section on page 8-2.

Business status view

The business status view, as shown inFigure 7-2 on page 7-3, provides a top-down view of the deployed infrastructure and the policies that define and control its behavior.

Figure 7-2 ***Business status view***



Business Status

- Customers
  - Customer A Environment
    - Administrators
    - Regions
    - Network Access Policy : Billing
    - Network Access Policy : Sales
  - Customer B Environment
    - LineSider Data Center Access
      - WAN
        - LS Data Center LAN@MSR LS Data Center--10 Network@MSR OSN Danvers
        - LS Data Center LAN@MSR LS Data Center--Danvers LAN@MSR OSN Danvers
      - Details...
        - ANY
        - Hub-Spoke
  - Customer C Environment

192.168.10.0/24 -- 10.0.0.0/8
Traffic flow not established:
LS Data Center LAN has not confirmed transport established.
10 Network has not confirmed transport established.

Using this view, you can quickly identify non-functioning policies, for example, Billing and Sales, which have no resources assigned to them. You can drill down into a policy and see the IP address and traffic flow between the device's services, plus protocol and topology (here, ANY and hub-spoke). You can continue to drill down deeper into any specific service to see the status of the actual devices that support it.

The view is designed to help you see at a glance what is going on. DSCs, for example, use a round status icon that changes from red to green to tell you whether traffic is flowing through them or no.

For an explanation of device and tunnel connection icons, Table 7-1.

Table 7-1 ***Icons for device and tunnel connections***

Left device	Left connection	Right connection	Right device	Description	Icon
down	down	down	down	Configured; no traffic flowing	🟥/🟥
down	n/a	down	up	Left device down, tunnel reported down by right device: lost box altogether?	✗/🟥
down	n/a	n/a	down	Both DSCs down: lost both DSCs or devices?	✗/✗
down	n/a	up	up	Left device down, tunnel appears up: lost DSC?	✗/🟩
pending	pending	down	up	Left DSC not deployed	🕒

Table 7-1 Icons for device and tunnel connections (continued)

Left device	Left connection	Right connection	Right device	Description	Icon
pending	pending	pending	pending	Neither DSC deployed	🕒
up	down	n/a	down	Right DSC down, tunnel reported down by right DSC: lost box altogether?	🟥/✖
up	down	pending	pending	Right device undeployed	🕒
up	down	up	up	Left tunnel not reporting traffic	🟥/🟩
up	up	down	up	Right side not reporting traffic	🟩/🟥
up	up	n/a	down	Right DSC down, tunnel appears up: lost DSC?	🟩/✖
up	up	up	up	configured with traffic flowing	🟩
unmanaged	n/a	n/a	unmanaged	Unmanaged devices: no info available	⛔
*	*	*	*	All other combinations	❓

CHAPTER 8

Creating audits and reports

This chapter tells you how to create audits and reports.

- Rationale for reports
- Generating an audit log
- Generating HIPAA, PCI, and SOX reports
- Creating site compliance reports

OverDrive provides state-of-the art reporting for application access and network security.

Rationale for reports

Not only do you as an admin need reports and logs to manage a network to assure that it's working properly, that you can track down errors flagged against devices and business properties, and so on, but you must repair specific reports as required by federal regulations.

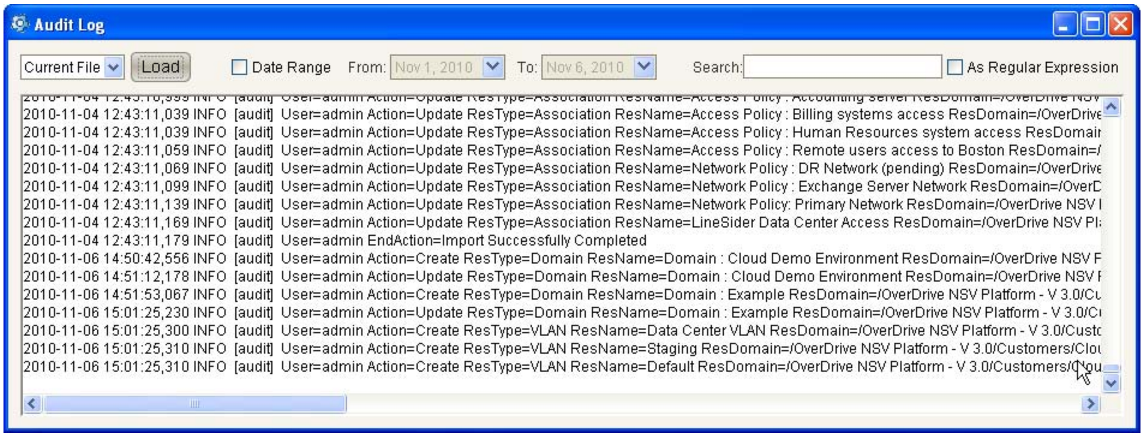
Generating an audit log

Audit logs record detailed information such as which:

- Admins have logged in, when, and in which roles
- Objects have been created, edited, renamed, or deleted
- Permissions have been granted, edited, or removed
- Resources have been resigned to which policies
- Policies that have been implemented, edited, or deleted

To generate an audit log:

1. Click the Launch Audit Log icon in the icon toolbar.
2. Choose one of the following:
   - Click Load to load the current file
   - Or specify a different file, and/or a date range, and/or a search string (check As Regular Expression if needed), as appropriate, and then click Load.



```
2010-11-04 12:43:10,999 INFO  [audit]  User=admin Action=Update ResType=Association ResName=Access Policy : Accounting server ResDomain=/OverDrive NSV
2010-11-04 12:43:11,039 INFO  [audit]  User=admin Action=Update ResType=Association ResName=Access Policy : Billing systems access ResDomain=/OverDrive
2010-11-04 12:43:11,039 INFO  [audit]  User=admin Action=Update ResType=Association ResName=Access Policy : Human Resources system access ResDomair
2010-11-04 12:43:11,059 INFO  [audit]  User=admin Action=Update ResType=Association ResName=Access Policy : Remote users access to Boston ResDomain=/
2010-11-04 12:43:11,069 INFO  [audit]  User=admin Action=Update ResType=Association ResName=Network Policy : DR Network (pending) ResDomain=/OverDrive
2010-11-04 12:43:11,099 INFO  [audit]  User=admin Action=Update ResType=Association ResName=Network Policy : Exchange Server Network ResDomain=/OverD
2010-11-04 12:43:11,139 INFO  [audit]  User=admin Action=Update ResType=Association ResName=Network Policy: Primary Network ResDomain=/OverDrive NSV I
2010-11-04 12:43:11,169 INFO  [audit]  User=admin Action=Update ResType=Association ResName=LineSider Data Center Access ResDomain=/OverDrive NSV Pl:
2010-11-04 12:43:11,179 INFO  [audit]  User=admin EndAction=Import Successfully Completed
2010-11-06 14:50:42,556 INFO  [audit]  User=admin Action=Create ResType=Domain ResName=Domain : Cloud Demo Environment ResDomain=/OverDrive NSV F
2010-11-06 14:51:12,178 INFO  [audit]  User=admin Action=Update ResType=Domain ResName=Domain : Cloud Demo Environment ResDomain=/OverDrive NSV F
2010-11-06 14:51:53,067 INFO  [audit]  User=admin Action=Create ResType=Domain ResName=Domain : Example ResDomain=/OverDrive NSV Platform - V 3.0/Cu
2010-11-06 15:01:25,230 INFO  [audit]  User=admin Action=Update ResType=Domain ResName=Domain : Example ResDomain=/OverDrive NSV Platform - V 3.0/Ci
2010-11-06 15:01:25,300 INFO  [audit]  User=admin Action=Create ResType=VLAN ResName=Data Center VLAN ResDomain=/OverDrive NSV Platform - V 3.0/Custc
2010-11-06 15:01:25,310 INFO  [audit]  User=admin Action=Create ResType=VLAN ResName=Staging ResDomain=/OverDrive NSV Platform - V 3.0/Customers/Clou
2010-11-06 15:01:25,310 INFO  [audit]  User=admin Action=Create ResType=VLAN ResName=Default ResDomain=/OverDrive NSV Platform - V 3.0/Customers/Clou
```

3. Search for the appropriate information, or copy the window contents to paste into a file for further analysis.

Generating HIPAA, PCI, and SOX reports

OverDrive delivers secure VPN access, network access policies, and access control rules for defined users or groups of users, ensuring that only business-policy specified users may access the applications defined by one or more business policies. This type of access security can be shown to comply with federal regulations.

OverDrive provides a mechanism for reporting back all of the rules and configurations that have been derived from business policies. This is an invaluable tool for building reports for HIPAA (Health Insurance Portability and Accountability Act) PCI (Payment Card Industry), and SOX (Sarbanes Oxley) regulations.

The reports show the defined policies, all users or groups of users associated with the policies, the applications and data sources associated with the policies, and the actual configuration statements in the devices that support the policies.

To generate such reports:

1. In the network status view, do one of the following:
   - Right-click on a site to generate a report of the connections in place at that site (see below).
   - Click on a domain to generate a report for all sites in that domain.

Creating site compliance reports

To generate a site compliance report from the network hardware status view:

1. Display the network status view.
2. Highlight a particular site or domain.
3. Generate the compliance report by choosing from the following:
   - For a site, choose Export Site Compliance Report.
   - For a domain, choose Export Combined Sites Compliance Report.

4. Browse to the directory you want, then click Export.

   The report is saved as a text file.

For examples, see the "Site and domain compliance reports" section on page B-1

APPENDIX A

Reference to common tasks

This section provides how-to information for common tasks that you need to know how to do before you can effectively work with the vCOM Command Center.

- Creating and editing domains
- Working with sites
- Creating administrators in domains
- Managing collections of resources
- Allowing ports and protocols for services
- Creating and refining business policies
- Adding groups and collections

Creating and editing domains

Creating a new domain

To create a new domain:

1. In your domain tree, choose one of these two options:

- Click on the ROOT domain or another one if more appropriate, then click the New Domain icon in the toolbar.
- Or, right-click the ROOT or other domain and choose New Domain in the resulting context menu.

  Notice that the browse view opens a maintenance panel with a pre-filled name for this new domain, the domain path for it, a text field to enter the domain name, and three tabs: Comment, Subnets, and VLAN.

2. Enter the domain name, for example, Customer Clouds.
3. In the comment pane, enter text to be seen when someone mouses-over this domain's name or icon in the tree view.

4. Click each appropriate tab and work through the settings and sub-tabs. For example:

- If subnets apply, click the Subnets tab. See the "Configuring subnets" section on page 2-2.
- If VLANs apply, click the VLANs tab. See the "Creating and configuring domain VLANs" section on page 2-34.

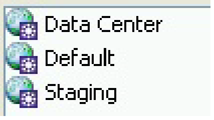
5. Click Submit.

Editing a domain

To edit an existing domain:

1. 1.Highlight it in the domain tree.
2. 2.Check that the selection view's Summary tab shows items contained within the domain that you have chosen.

   For our domain Example, if you have entered VLANs as suggested below, this list should be:



Data Center
Default
Staging

3. Choose Edit in the context menu.

You will return to the domain window in the browse view, with the Comment tab open on the mouse-over comment you have entered or edited previously.s

Working with sites

A site consists of a DSC and one or more DSC-managed devices; it has one or more resources affiliated with it, and it can be configured with VLANs.

A site is a logical location. It is possible to have several sites in one physical location or vice versa. The site is a point of control for OverDrive to manage a collection of devices.

An example of a site is a large distributed office complex with one point of ingress or egress at which policies are enforced. Another example of a site is a stack of network equipment in a data center built to provide virtual compute services. You may have several of these in one physical location.

Creating a new site

To create a new site:

1. Right-click a domain in the domain tree view and choose New Site.
2. Enter the site name, for example, Boston or Boston State Street Branch.
3. Click on each tab and follow these directions as appropriate:

   a. Participating Resources—These are resources available in the domain. Since this site is, for our example, in the Example domain, once we have created resources, future new sites will have them available. See Specifying site resources below.

Note Resources such as servers and subnets can only be assigned at one site at a time. Network IDs for LDAP users can be logged in at any of the sites in the domains in which they are visible.

b. Devices—Specify a name and password for the DSC controlling the device, and then specify the device itself, as described in Specifying site resources below.

c. Site Subnets—See the "Creating site subnets" section on page A-4.

d. VLAN—See site-specific information in the "Creating and configuring domain VLANs" section on page 2-3.

Specifying site resources

Site resources include users, notebooks, desktops, servers, and so on.

To specify a site resource:

1. Right-click the site in the domain tree and choose New Local Resource.
2. Give the resource a name, choose an icon, and specify its IP address.

Note The drop-down site list lets you reassign this resource to another site within the same domain.

3. Under the Business Policies tab, click the business policy that you want this resource to participate in (use Ctrl-click for more than one).
4. Click Add to move the policies to the joined panel.
5. Do the same under the Collections tab, as appropriate.
6. Click Submit.

The resource should appear in the Summary tab for the site.

Specifying the site DSC and its devices

When you bring up a device configuration window, it will tell you the site name, for example, Chicago.

On the Config tab for a new site:

1. Specify the DSC name.

   You might want to use an abbreviated name that reminds you of the site name, so, for example, you might use LIN-BOS-StateSt-01 for a DSC on a site named Linwood Boston State Street Branch.
2. Specify and confirm a password.
3. On the Device tab, specify needed information for devices.

Note For each device you want to add, choose the type from the Add drop-down list. Before adding switches, back up the switch configuration, and verify that all VLANs (managed and unmanaged) are known to OverDrive.

a. Specify configuration common to all devices:

- Name—A device name, as described above
- IP Address—Where they live on the net
- CLI Credentials—Access method (telnet/ssh), username, passwords
- SNMP Version—Most likely accept the default (3).
- V3 Credentials—Username, authorization passphrase, and private passphrase; SNMP credentials
- Comment—Tooltip text

b. For specific devices, provide the following information where applicable:

- Access switches have an Admin tab with the above information, plus a VLAN tab that shows permitted and non-permitted VLANs. This allows you to exclude a VLAN from designated switches. They also have uplink ports and access switch ports. Uplink ports may require an IP address that will be predefined on the switches. The DSC recognizes the uplink ports and reports them to the server to be used for validating that new VLANs do not overlap with the uplinks at the site; it does not configure the base static configuration of the switch (uplinks and downlinks): it configures dot1x, VLANs and ACLs.
- Aggregation switches may have several uplink and downlink trunk ports that permit traffic from the access layer to the distribution layer. You may specify certain managed ports on which OverDrive will dynamically create VLANs in addition to those it creates automatically such devices. This restricts traffic so that only managed or specified VLANs are permitted on the trunks.
- NAT devices need interface names for inside and outside.
- Routers need the IPsec interface IP address and the tunnel interface name.
- VM managers need property values that match those set in vCenter configuration: password, targetAddress, username, datacenter, targetFolder, templateFolder, vSwitch.

4. Click Submit.

Creating site subnets

Site subnets let you further constrain the address allocation within a domain by describing which addresses may be used at a site. The site subnet constrains the addresses that are available for resources at the site. The collection of site subnets is also used to aggregate routes and IPsec tunnel SA's.

Once you have created a site, you can create a subnet for it. A site subnet specifies the addresses in use at the sites and must be within the range of the domain subnets. It may not overlap with discovered uplink subnets or with VLANs at the site.

To do so:

1. If you are not already looking at the site window with the various tabs, right-click the site and choose Edit.
2. Click Site Subnets.
3. Click New, then enter an IP address and netmask.
4. Click Accept.

The site's resources will be required to adhere to this subnet.

Creating administrators in domains

When you create an administrator for a domain, you can choose that domain or one contained within it for him or her to manage. He or she will see only the domain you specify.

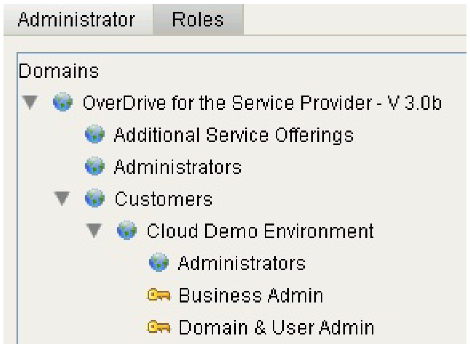
To create an administrator:

1. Right-click any domain and choose New Administrator.

   If you want to have all of your administrators in a particular location in the tree, create a new subdomain for them and call it Administrators.

Note You can create an admin anywhere. Depending on the privileges you assign determines where he logs in. We suggest creating an admin outside of his domain, so he can't edit himself.

2. In the new administrator screen, under the Administrator tab:
   a. Enter the username of the administrator you are specifying, plus a password and its confirmation.
   b. Enter a comment to appear on mouse-overs, for example:
   - Read Only: Automated daily reports
   - Global view
   - Read Only: NOC view
   - Domain administrator
3. Under the Roles tab, expand the domain tree.
4. Right-click one of the domains and choose the type of admin to create.
5. Double-click the domain to open it, then verify that the admin has been added, as you can see by the key icon and type of admin that you added, for example:



6. Now you're done. Click Submit and the new administrator will show up in the domain's Summary tab.

Managing collections of resources

A collection is a set of resources grouped together with some common purpose or function. A collection provides an efficient way to manage a number of resources. For example, it lets you give a group of users joint access to a resource even though they are distributed across multiple sites. A very common use for collections is where you want to apply a hub and spoke topology to more than one resource at the hub

Collections may include other collections as members.

To create a collection:

1. Right-click a domain and choose New Collection.
2. Enter the collection name and visit all three tabs: Resources, Business Policies, and Collections.
3. For each tab, highlight one more available items and click Add to assign them to participating resources, to joined business policies, or to joined collections.

   Once you have added them, you could highlight them and click Remove to return them to the available pool.
4. Enter something useful and appropriate in the comments field.
5. Click Submit.

Allowing ports and protocols for services

All network services use one or more ports and one or more protocols for communication. For the users on a given network to use a service, OverDrive must be configured to allow network traffic for it. (Some standard ports are predefined: http, telnet, ICMP, etc.)

Ports and protocols are an attribute of all business policies, which use them to permit certain traffic. See the "Creating a business policy for a CRM server" section on page 4-7 for an example.

To specify ports and protocols for a domain to use:

1. Right-click a domain and choose New Ports & Protocols.

Note If you don't specify at least one, the policy will be infeasible because no traffic will be considered valid for the policy.

2. Specify the name.
3. Click Add if the Ports & Protocols pane is empty. Otherwise, you may also highlight one set and click Edit or Remove.
4. In the Protocol section, leave Predefined selected, and choose ANY, ICMP, TCP, or UDP.
5. For TCP and UDP, enter the ports to use.
6. Click Submit to accept the new set of protocol and ports.
7. Click Submit to make it available to network services.

Creating and refining business policies

Business policies connect resources on the network. Two or more resources (local resources, VLANs, network identities) can be added to a business policy, and the system will configure all the devices required to enable the connection between them.

To create a business policy:

1. Right-click a domain and choose New Business Policy.
2. Specify a name.
3. Visit each tab in turn: Resources, Ports & Protocols, and Schedules.
    - or resources, choose from those available and click Add. Then choose the network configuration: full mesh, hub and spoke, or peer to peer.
    - For ports and protocols, choose and click Add.
    - For schedules, you can set when to start and end activation, not at all, or immediately, or at a certain time.
4. Definitely use the comment field because it is especially helpful when describing policies and expected access.
5. Click Submit.

For an in-context look at how this works, and how to see the connections come up, see the "Creating a business policy for a CRM server" section on page 4-7.

Adding groups and collections

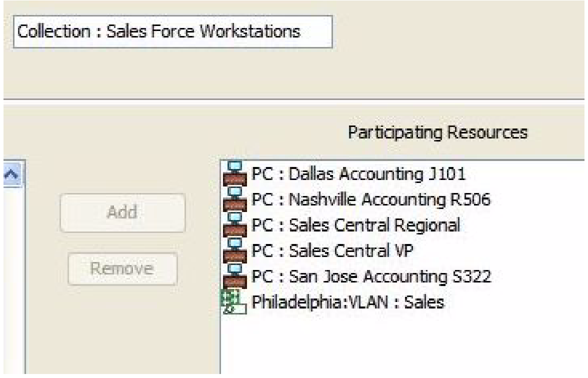
Earlier, we have shown you how to let users onto the network: see "Creating a user for a network policy" section on page 3-4.

Let's also assume that users Weber and Bouwer are in the same sales group in Philadelphia, and they need access to the CRM server, now in Boston. We have built a network access policy to associate their LDAP group with the sales VLAN (see "Creating a network access policy" section on page 2-7), and we have associated both sales and remote sales LDAP groups. Now, we only want those members who are in Philadelphia to be able to access the server.

In effect, we want the Philadelphia:VLAN: Sales to be part of the CRM access business policy. To do this, we're going to go and edit the collection (group) in Sales:

1. Right-click Business Policy: CRM Access, in the domain tree, and choose Edit.
2. In the participating resources panel, double-click Collection: Sales Force Workstations.

    This opens the edit window for the sales force workstation collection. See that the Resources tab opens.
3. In the available resources panel, highlight Philadelphia: VLAN: Sales, and click Add.



Collection : Sales Force Workstations

Participating Resources

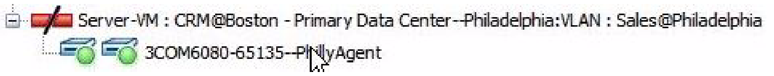
PC : Dallas Accounting J101
PC : Nashville Accounting R506
PC : Sales Central Regional
PC : Sales Central VP
PC : San Jose Accounting S322
Philadelphia:VLAN : Sales

4. Click Submit.

   You have defined an additional connection that specifies that the sales VLAN in Philadelphia needs access to the VM CRM server in Boston.

5. In the business status view, find the WAN node under Business Policy: CRM Access, and click it.

The sales VLAN now has access to the Boston primary data center, as specified by the CRM Access business policy.



Server-VM : CRM@Boston - Primary Data Center--Philadelphia:VLAN : Sales@Philadelphia
3COM6080-65135--PhillyAgent

As we have seen earlier, this connection will shortly turn all green.

APPENDIX B

Sample Reports

This appendix provides some sample reports that are referenced in one or more of the preceding chapters:

- Site and domain compliance reports

Site and domain compliance reports

You can generate individual site compliance reports or similar reports, called domain reports, or combined sites reports, depending on which item you highlight in the network sites view.

Sample single site report

The following listing shows a single site report. The combined sites (or domain) report contains all of the site reports within the domain you have chosen.

```
Site Compliance Report for: MSR Delaware
Connections and Policies by Peer Site:
MSR Delaware
 MSR Delaware - MSR OSN Danvers
    H3C205MSR3060--OSN65130
      192.168.10.0/24<-->1.1.1.0/24
        Delaware - Danvers
      192.168.10.0/24<-->192.168.128.0/23
        Delaware - Danvers
      192.168.10.0/24<-->10.0.0.0/8
        Delaware - Danvers
Connections for Device: H3C205MSR3060
IPSec Connections:
    Connection 1 - 1.1.1.0/24<=>192.168.10.0/24
        Source Pep address: 1.2.3.9
        Source Pep identifier: StubPepConnHandlerUniqueAddr_1.2.3.9
        Source Resource Address: 192.168.10.0/24
        Dest. Pep address: 1.2.3.10
        Dest. Pep identifier: DummyPepConnHandlerUniqueAddr_1.2.3.10
        Dest. Resource Address: 1.1.1.0/24
        options
            auto-start: true
            ike-key-lifetime: 3600
            ipsec-key-lifetime: 28800
            keying-retries: 0
            rekey-fuzz: 100
            rekey-margin: 540
```

```
                compression: false
                encryption: true
                no-rekey: false
                no-route false
                pfs: true
        Connection 2 - 192.168.10.0/24<=>192.168.128.0/23
            // Similar information to Connection 1
            . . .
        Connection 3 - 10.0.0.0/8<=>192.168.10.0/24
            // Similar information to Connection 1
            . . .
    Firewall Policy:
        Source: 1.1.1.0/24 Dest: 192.168.10.0/24
            rule Action: ALLOW
        Source: 192.168.10.0/24 Dest: 1.1.1.0/24
            rule Action: ALLOW
        Source: 192.168.128.0/23 Dest: 192.168.10.0/24
            rule Action: ALLOW
        Source: 192.168.10.0/24 Dest: 192.168.128.0/23
            rule Action: ALLOW
        Source: 10.0.0.0/8 Dest: 192.168.10.0/24
            rule Action: ALLOW
        Source: 192.168.10.0/24 Dest: 10.0.0.0/8
            rule Action: ALLOW
```

Sample domain (multi-site) compliance reports

The domain (multi-site) compliance reports simply report the domain involved (in the text below, Customers, and then provide a compliance report for each site within the domain.

```
Combined Compliance Report for Domain: Customers
Site Compliance Report for: Boston
Connections and Policies by Peer Site:
Boston
Connections for Device: BostonAgent

IPSec Connections:
    (none)
Firewall Policy:
    (none)
Site Compliance Report for: Boston - Primary Data Center
Connections and Policies by Peer Site:
Boston - Primary Data Center
Connections for Device: 3COM6080-65135

IPSec Connections:
    (none)
Firewall Policy:
    (none)
Site Compliance Report for: Chicago
Connections and Policies by Peer Site:
Chicago
Connections for Device: CISCO1800-65134

IPSec Connections:
    (none)
Firewall Policy:
    (none)
Site Compliance Report for: Dallas
Connections and Policies by Peer Site:
Dallas
Connections for Device: CISCO2800-65138
```

```
IPSec Connections:
    (none)
Firewall Policy:
    (none)

Site Compliance Report for: MSR Delaware (see Sample single site report)
...
Site Compliance Report for: MSR OSN Danvers (similar to above)
...
```

APPENDIX C

Cloud configurator fields

This appendix provides notes on the fields that may appear in the Cloud Configurator, depending on the metamodels used.

The property names (pnames) appear in the property tables in the Command Center. Metamodel names beginning with tmpl appear as parameters in metamodels.

Note Field names with asterisks (**) indicate non-generic, customer-specific fields.

Table C-1 Field names and related data

Field Name	Description	Panel	Metamodel Name Property Name	Notes
Cloud Name	Name of the cloud	Cloud	client.name	
Cloud Public Pool	Public address pool subnet	NAT	tmpl.cloud.public.pool	
Cloud Subnet	IP addresses available to the cloud	Cloud	tmpl.cloud.subnet cloud.subnet	
Customer VLAN Mask	Select Mask from choices available	Cloud	customer.vlan.mask	
DHCP Server Address	IP address of the DHCP helper	DHCP	tmpl.cloud.dhcp.address cloud.dhcp.address	
DNS IP Address	IP address of the DNS server	DNS	tmpl.cloud.dns.address cloud.dns.address	
DNS Key Name	Key name required for DNS changes	DNS	tmpl.cloud.dns.key cloud.dns.key	
DNS Secret	Credential required for DNS changes	DNS	tmpl.cloud.dns.credential cloud.dns.credential	
Enable DHCP Reservations	Enable DNS spoofing?	DHCP	tmpl.cloud.dhcp.enable cloud.dhcp.enable	
Enable DNS	Manage address reservations on a dynamic DNS server?	DNS	tmpl.cloud.dns.enable cloud.dns.enable	

Table C-1 Field names and related data (continued)

Field Name	Description	Panel	Metamodel Name Property Name	Notes
Public Address Pool Allocated**	The table of assigned public IP addresses	NAT	cloud.public.allocated	
QoS Policy**	Select a policy for quality of service	Cloud	tmpl.cloud.qospolicy cloud.qospolicy	
Site	Site to which the cloud is assigned	Cloud	client.siteID	
VLAN Address Pool	The subnet for VLAN addresses	VLAN	tmpl.cloud.vlan.pool cloud.vlan.pool	
VLAN Range	Range of VLAN numbers to use	VLAN	tmpl.cloud.vlan.range cloud.vlan.range	
VLANs Allocated**	The table of allocated VLANs	NAT	cloud.vlan.allocated	
VM Image	Select one of the VM images in vSphere	VM	vm.image	

APPENDIX D

FAQs

This appendix answers frequently asked questions, in the following sections:

- Status questions
- Procedural questions
- Questions about configuration

Status questions

This section concentrates on checking status of devices, DSC, communications, and so on.

Question: How can I talk to the switches if the DSC is down? In the network status view, everything is gray at my site: the DSC, the distribution switch, and the access switch?

Answer: That's a good question. You need to contact the DSC through its serial line interface:

a. Verify that it is powered on.

b. Verify that it is plugged into the network.

c. Try to ssh to it first.

d. Now try the serial cable.

Answer: You can also see what the last known IP address was in the tooltip and try to ping to SSH to that.

Question: The status change I'm looking for doesn't seem to be showing up?

Answer: Look for other changes related to this one and see if they took place. Look at the device logs. Be sure the DSC appliance and processes are both operational.

Procedural questions

These questions and answers concern how to do something.

Question: How do I save the model I've been working on?

Answer: You can export it using the toolbar's right-facing export-arrow icon. OverDrive automatically provides a pd2 extension to the filename.

Question: How do I import a model?

Answer: Go to the domain you want to replace, and use the toolbar down-arrow to open a file browser so you can specify a pd2 file.

Question: Can I import a model so it merges with the domain?

Answer: Sorry. Your import replaces the domain.

Question: Why do I get an "admin already exists" error when I import a pd2 file into the root domain in my model?

Answer: Admin is a special user when at the root. Your pd2 file is trying to replace that user with its own definition of a user named admin. None of the attributes of the root admin will be replaced or deleted.

Question: Where is the go-back button?

Answer: There isn't a go-back button. But, the full domain tree path, better known as bread crumbs, is shown above the domain tree navigator. This tells you where your currently highlighted object is in the domain tree. The domain path shown at the top of the browse/edit view is another locator of where you are. Even better, the Show List icon in the upper right of those views brings you to a list of all the open windows, kind of like TurboTax brings you to a list of all your tax forms.

Question: There seem to be old screens in the browse view.

Answer: If you open an information or edit window in the browse view and do not click Submit or Cancel, it stays in the view and gets overlaid with others that come later and don't get dismissed. You need to submit or cancel them before they go away.

Questions about configuration

These questions and answers relate to configuration.

Question: How many DSCs can be at one site?

Answer: One.

Question: How many devices can be assigned to one DSC?

Answer: Multiple.

Question: What are good suggestions for DSC names? What about sites? Devices?

Answer: We advocate naming sites something meaningful and quickly decipherable, for example, Boston or Boston State Street Branch, depending on the granularity of your networks' sites. The DSC and device names are typically shorter, so, for example, BOS001 might be a good name for a DSC at one branch, and BOS002 at another. For devices, typically you might want to use the model name followed by a string of numbers or characters to help distinguish it from others of the same type.

Question: What kinds of information are appropriate for comment fields for devices?

Answer: Generally, IP addresses; initially, perhaps, device type and/or manufacturer; record of VLAN and IP address pools (coherency region)

Question: What's the bare minimum of equipment and software? Just give me an idea.

Answer: To start actively managing the network, you need the following:

- A running LDAP server on the network, and the NSV engine must have its URL
- One or more DHCP servers available, and you need their IP addresses
- One or more DSC appliances (one per site)
- The name and password for each DSC
- For each switch:
  - Command Line Interface (CLI) access method (telnet or ssh); a CLI username and password
  - SNMP Version (1, 2c, or 3); for SNMPv3: the SNMP username, authorization password, and private passphrase; for SNMPv1 or v2: SNMP read community; SNMP write community
- For each router, the same needs as for a switch
- Installed certificate domain
- IPsec tunnel IP address and IP interface

APPENDIX E

Troubleshooting

This appendix provides hints and suggestions for troubleshooting.

- Common alerts
- Methodology hints

Note For network monitoring icons, refer to Table C-1 on page C-1.

Common alerts

The Alerts tab timestamps errors and classifies them into the following types:

- Serious errors flagged with a white x on a red circle
- Informative errors flagged with a blue i on a white circle

You can right-click these errors and jump to the network status to edit it in response, or to the policy in the policy view and edit that.

Serious errors

- DSC is down—Presumably it has connected to the NSVE before; wait a while.
- DSC problem(s): Device has never connected to server—Check that the appliance is up, processes are running, is pingable, and so on.
- DSC problem(s): Last known IP address. Device heartbeat timed out—Check powered on, reachable; right-click and jump to network status view, right-click DSC and view log and/or active policy.
- Device is down—Check if it is powered off; right-click and jump to network status view, then right-click and execute device commands as appropriate.
- DeviceName has not confirmed transport established—Device is reachable but does not report traffic; wait a while; right-click and jump to policy status view, then hover over connection pair for tooltip explanation.

  Note Transport not established is not necessarily a serious error: it could be that the tunnel is not in use at this time.

- No resources assigned to policy—Right-click, navigate to domain, check out, create, or edit policy as appropriate so resources appear in Participating Resources panel; right-click and edit network access policy to add resources to the panel.
- Policy has no connections—Right-click, jump to policy, investigate.
- Policy has no ports and protocols—Right-click, jump to policy, look in Ports & Protocols tab and fix Selected Ports & Protocols panel contents.

Informative errors

- Business policy w/o connections—Right-click, jump to policy, investigate.

Methodology hints

Every user finds his or her own methods for debugging, but if you're just starting out, the following subsections might give you some helpful ideas.

Tooltips

The tooltips can be your best friend when you can't figure out why something doesn't work. Hover over broken connections in the network or business status views. The tooltips can tell you, for example, that a connection is down because the business policy has not yet assigned ports and protocols.

Alerts

You can right-click on an alert and choose a navigation option, as follows:

- Jump to network status view—Bring up the hardware device tree, with the particular device highlighted. You can right-click that and choose to view its log, or view the active policy, which displays details about IPSec, VLAN, and other connections.
- Navigate to domain—Highlight the domain containing the object in the alert. You can look in its summary view or right-click it and choose Edit to see its subnets or VLAN table, if appropriate.
- Jump to policy status view—Bring up the business status view and highlight the connection or device. If possible, expand the item for more information, and look at its context.

GLOSSARY

A

ACL (access control list) Generally a list of permissions to objects, e.g., read, write, delete, for users or system processes.

Active Directory A hierarchical directory service built on DNS in which workgroup and individual names can be found, and associated together with privileges.

access switch Access hubs and switches working at the desktop layer connect workstations and servers to the network and provide MAC address filtering, bandwidth sharing, and bandwidth switching (moving data from one network to another).

administrator A role assigned to users allowing specific actions (create, read, update, and delete) in a specified domain. There are business, site, domain/user, technical, and audit admins. For example, an administrator with an audit role in a sub-domain can view the hierarchy, business policies, and resources, and can also generate site and domain compliance reports for its accessible domains.

agent DSC software, running on an OverDrive appliance, that manages network devices such as routers and switches. See DSC (device service controller).

aggregation switch A switch that provides aggregate or group networks.

B

business policy The controlling mechanism that provides network connectivity in terms of resources, ports, protocols, schedules, and connection topologies.

C

connection topology A network configuration that allows resources or collections to communicate in a specify arrangement: all together, individually to all others (full mesh, bidirectional); server-to-client (spoke-initiated hub and spoke, or peer to peer); hub and spoke but bi-directional, such as for remote desktop help; or just a single peer-to-peer pair, whether peer initiated or bi-directional).

command center The client UI interface to OverDrive, previously called an admin console, management portal, or policy workbench.

collection A group of resources with some common purpose or function, allowing multiple resources to be managed, as for example, a collection of users from multiple sites who need access to something regardless of where they are located. Formerly, group.

D

device Networking hardware such as a switch or router.

distribution switch A device working at the workgroup or distribution layer (as defined by Cisco to include LAN-based routers and layer 3 switches), to make sure that packets are routed between subnets and VLANs.

DSC (device service controller) Software running on Linux appliances. The DSC manages devices acting as edge routers, firewalls, distribution switches, and access switches. While these roles are logically singular, OverDrive can assign multiple devices to roles and can manage any resulting network redundancy by duplicating and rebuilding configurations where necessary. Formerly, agent.

DSC server An appliance with one or more DSCs on it.

domain The main organizational concept in the command center, domains exist in a hierarchy, much like directories in a file system. Since all objects in the system exist in a domain, the entire set of configuration items also has a hierarchical structure.

F

full mesh See connection topology.

H

hub and spoke See connection topologyy.

M

metamodel An XML document specifying configuration information for clouds, domains, VMs, and so on.

metapolicy A set of constraints and rules imposed on connections as they are being built to support the business policies, allowing them to be tuned. See Installing OverDrive.

MSP (managed service provider) Comparable to a reseller, an MSP provides services to a client, such as installing, configuring, and helping to mange OverDrive networks.

N

network access policy Defining access to a LAN resource for one or more network identities organized by the LDAP tree, as for example, by membership in a security group.

network identities Mappings to LDAP distinguished names, therefore able to represent an individual or a group in Microsoft Active Directory.

NSVE (network services virtualization engine) The NSV Platform engine that analyzes business and network access policies and produces requests for the DSCs to reconfigure the devices they control so that the VPNs specified by the NSVE will be provisioned appropriately. Formerly, policy server.

P

policies OverDrive uses two types of policies to manage resources. Network access policies define entitlements and access management on a network. Business policies give one set of resources access to another set of resources.

policy server See NSVE (network services virtualization engine).

ports and protocols The TCP/UDP port or IP protocol permitted in a policy. All network services use one or more ports and one or more protocols for communication. For the users on a given network to use a service, the OverDrive NSV platform must be configured to allow network traffic for the service. There are a number of standard ports that are predefined in the OverDrive environment, e.g., http, telnet, and ICMP. The predefined object ANY allows network communications on any port and protocol. Formerly, application.

R

resource An abstract definition of a a single host or a network subnet, instantiated as a LAN, a desktop machine, a mail server, laptop, or so on, with an IP address and subnet mask, and assigned to a single site. Resources may be moved from one site to another. They can include local resources, collections, VLANs, and network identities.

roles A logical grouping of devices, typically to specify which ones can be managed by a particular admin user.

S

site A logical collection of devices, normally thought of as in a geographical or virtual geographic location. A site consists of a DSC and one or more OverDrive-managed devices; it has one or more resources affiliated with it and can be configured with a set of subnets or VLANs. (With private tagged MPLS VLANs or frame relay networks, a single OverDrive site may be dispersed across multiple physical campuses but still have a single logical edge.)

subnet Networked computers and devices with a common IP routing prefix such as 192.168.

V

VLAN (virtual LAN) An abstraction of switch VLANs which could be managed as layer 2 802.1Q trunks (end-to-end VLANs) or in routed LAN environments (where the traffic on the LAN is routed among local switch VLANs at both the access and distribution layer). In OverDrive, VLANs are defined for an entire domain. Once one exists, it can be made available to some or all sites within that domain. OverDrive lets an administrator specify a list of VLANs permitted at a site or on specific devices.

VM (virtual machine) A computer environment such as those provided by VMware that allows one operating system to run on a host operating system as if it were stand-alone.

INDEX