



## **Introducing Cisco OverDrive 4.0**

### **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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

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.

*Introducing Cisco OverDrive 4.0*

© 2011 Cisco Systems, Inc. All rights reserved.



# CONTENTS

## About This Guide vii

- Is this guide for me? vii
- What is it about? vii
- How is it organized? vii
- What other documentation do I need? viii
- Conventions viii
- Obtaining Documentation and Submitting a Service Request viii

---

## CHAPTER 1

### What is OverDrive? 1-1

- Network services 1-1
- Virtualization of network services 1-1
- The OverDrive NSV platform 1-2

---

## CHAPTER 2

### Introducing OverDrive Architecture 2-1

- Overview 2-1
- The NSVE policy server 2-2
- Device service controllers 2-2
  - Overview of what a DSC does 2-2
  - DSCs and enterprise security 2-2
  - DSC details 2-3
- The OverDrive user interface 2-3
  - Command center 2-3
  - Cloud configurator 2-4
  - Cloud orchestration manager 2-4

---

## CHAPTER 3

### OverDrive Concepts 3-1

- Domains 3-1
- Clouds 3-2
- Resources 3-3
  - Local resources 3-3
  - VLANs 3-4
  - Domain subnets 3-4
  - Network Identities 3-4

Sites	3-4
Collections	3-5
Ports and protocols	3-6
Policies	3-6
Network access policies	3-6
Business policies	3-7
Metapolicies	3-8
Administrator roles	3-8

**CHAPTER 4****OverDrive Deployment Types 4-1**

Site-to-site VPNs	4-1
Network access control within a site	4-2
Cloud installations	4-2

**CHAPTER 5****OverDrive modeling tools 5-1**

Command center	5-1
Overview of command center views	5-2
Domain navigator view	5-3
Selection view	5-3
Browse/alerts view	5-3
Status views	5-3
Creating objects in the command center	5-5
General recommendations	5-5
Creating objects from the toolbar	5-6
Cloud configurator	5-7
Creating and configuring clouds	5-7
Populating clouds with VMs	5-8
Cloud orchestration manager	5-8
Metamodels	5-8
The REST API	5-9

**CHAPTER 6****Network management scenarios 6-1**

Putting another admin in charge of a subdomain	6-1
Monitoring network and device status	6-2
Workflow for a sample business policy	6-2
Adjusting the network after moving a server	6-2
Creating reports	6-3

APPENDIX A	FAQs	A-1
GLOSSARY		
INDEX		





## 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 designed for most people who are interested in an overview of the OverDrive product, including:

- Network planners, configurators, and users of all types
- Network admins

It is for anyone who wants to know basically what OverDrive is, architecturally and component-wise. It provides a common background that all users, installation experts, network admins, cloud creators, and VM providers are expected to know or be able to reference.

### What is it about?

It describes the OverDrive product, its concepts architecture, terminology, and where to find the guides for how to install and use its various components. It is not task oriented.

### How is it organized?

It proceeds from a high-level overview of architecture and concepts, to an introduction to the OverDrive Command Center views and terminology, and from there to a quick look at some example network management scenarios. It describes logical components, domains, local resources, VLANs, network identities, sites, collections, protocols, policies, and network topologies.

It then introduces the Cloud Configurator and Cloud Orchestration Manager (a subset of the configurator) as used to create clouds using metamodels, and then to create VMs using metamodels.

Appendices present equipment availability (adding new devices, etc.), and a glossary of terms and abbreviations

## What other documentation do I need?

To install Cisco OverDrive and bring up the command center, see the *Cisco OverDrive 4.0 Installation Guide*; for task-oriented help in managing an OverDrive network, see *Cisco OverDrive 4.0 User Guide*. For end users to create, power up or down, and remove VMs to be used by people in their group, department, or customer base, see Providing VMs.

## Conventions

This document uses the following conventions:

Item	Convention
Commands and keywords	<b>boldface</b> font
Variables for which you supply values	<i>italic</i> font
Displayed session and system information	screen font
Information you enter	<b>boldface screen</b> font
Variables you enter	<i>italic screen</i> font
Menu items and button names	<b>boldface</b> 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

## What is OverDrive?

---

In conceptual terms, OverDrive combines a network services virtualization engine, as sketched in this chapter, with clients in an architecture that enables creation and management of site-to-site VPNs, network access control within a site, and cloud services to be used by VMs, as described in later chapters.

(Sites in OverDrive are logical entities, either single physical locations or multiple physical locations that retain a single, logical edge.)

The OverDrive engine reacts to high-level creation and modification of network models by using easily specified business and network policies to configure or reconfigure user access (by people or machines) to resources (services) available on-site, intra-net, or in-cloud.

This chapter briefly describes:

- [Network services](#)—shared resources
- [Virtualization of network services](#)—automatic and dynamic data center environments
- [The OverDrive NSV platform](#)— real-time, policy-based, automation and control

## Network services

Network services provide capabilities to shared resources and users. Examples of such capabilities are DHCP, DNS, routing and VPNs, switching and VLANs, firewalls (ACLs), security (ACLs and 802.1x), and identity-based network access control.

## Virtualization of network services

The term virtualization in an OverDrive context applies to a wide range of computer- or server-related hardware, software, memory, storage, data, desktops, and networking.

OverDrive virtualizes network services by creating or abstracting a logical network in concordance with the physical network that it also manages. It controls the physical network by virtualizing hardware switches and routers to create subnets of network addressing space, typically VPNs, that also enable and orchestrate clouds and VMs.

The logical network is driven by policies that control network access for individuals to resources. The policies specify high-level resource sharing. They can be created externally or using the OverDrive Command Center, as documents that can be imported, exported, and edited within the center. At the XML level, they comprise elements that model all the specifications (and more) that can be expressed

in the command center, using a grammar of variable and parameter substitutions that let admins and network configurators easily specify individual and multiple models that OverDrive can express. For this reason, they are called metamodel files.

Thus, OverDrive invents and defines network services virtualization as a model-based definition of a network addressing space, the physical and virtual (VM) resources in that space, and the managed services, capabilities, and relationships between those network resources. That is, the deployed network and service infrastructure.

In abstracting a logical from a physical network, the model enables dynamic responses to physical network changes. These responses ensure the on-going operational intent of the logical network services model.

By virtualizing clouds and physical centers, OverDrive provides an infrastructure that is entirely dynamic, controlled by the OverDrive NSVE (network services virtualization engine).

The NSVE controls the virtualized data center hardware, VM, and cloud environments, so that end users are connected to the network resources they need for their particular business responsibilities, without requiring someone to reconfigure and re-provision as computing resources change.

The result happens quickly, consistently, and predictably.

## The OverDrive NSV platform

In virtualizing network services, OverDrive orchestrates real-time automation and control, based on business policies that define relationships between users, computing resources, and network services (including clouds, VMs, and storage).

This orchestration is based on business semantics. It is a top-down approach to managing a network, instead of a bottom-up approach that concentrates on routers, switches, and other network hardware.

To support this business policy emphasis, OverDrive automates device level configurations, thereby automating network service delivery and network management. The NSVE interprets the policy, identifies devices and services that need to be modified to satisfy it, and dynamically pushes configuration updates to the selected devices. In brief, it:

- Creates all configuration updates for appropriate devices
- Negotiates required services among selected devices
- Initiates multiple services in parallel and in concert
- Provides real-time feedback as services are initiated across the network

In other words, OverDrive provides the services and configurations that each business policy needs.

A key component of the NSVE is a process called the provisioner or provisioning engine. This determines which sites are affected by the new policy. For each one, it constructs a set of abstract directives to tell the site's DSC (device service controller) which policies it needs to implement. Depending on which services are enabled at the sites, when the service controller receives the directives, it converts them into device-specific instructions and configures the devices accordingly.



## CHAPTER 2

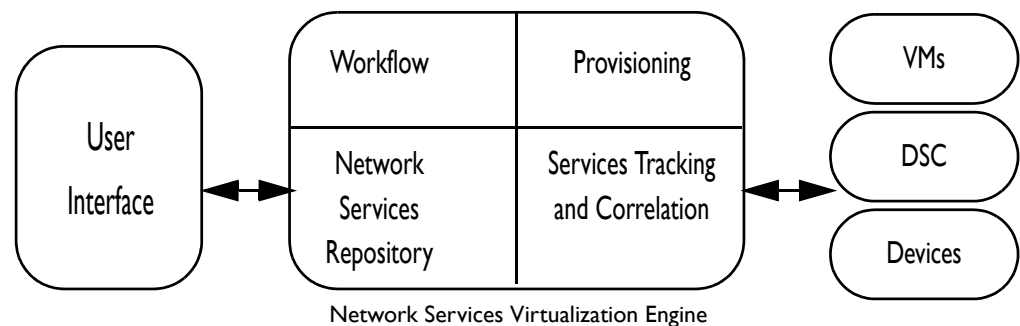
# Introducing OverDrive Architecture

This chapter introduces the OverDrive architecture:

- [Overview](#)
- [The NSVE policy server](#)
- [Device service controllers](#)
- [The OverDrive user interface](#)

## Overview

**Figure 2-1** Overview of Architecture



OverDrive achieves its automation and control of the logical and physical networks through three primary technology components, as shown in [Figure 2-1](#):

- The NSVE manages network policy and provisions the managed devices.
- The DSC at each site sits between the NSVE and the site's VMs and devices such as switches and routers, using SNMP and SSH (or Telnet) for command line interface to the devices where necessary.
- The user interface provides access to tools to configure, administer, and monitor business policies and the objects that support them.

## The NSVE policy server

The NSVE is the heart of the OverDrive NSV platform, maintaining a persistent, real-time model of the deployed network and service infrastructure. It:

- Accepts policy requests from the command center
- Translates them into device-level configuration directives
- Sends them to the appropriate DSCs that manage the devices

The NSVE can translate one policy request into many device-level directives that simultaneously go out to devices across a network. In large networks, a single policy request can generate hundreds of separate device-level configuration updates to establish appropriate routing, VPN, and/or VLAN connectivity, firewall access rules, and so on.

Policy requests that generate configuration updates and changes persist in the NSVE repository, permanently linked to the deployed configuration updates that they implemented. The persistence maintained by the NSVE ensures that the deployed network environment remains in compliance with appropriate regulation requirements, and provides for easy generation of audit and compliance reports.

## Device service controllers

The DSCs provide the services described below.

### Overview of what a DSC does

The NSVE uses DSCs to implement its directives and to provide feedback on whether they are successful. Each DSC understands the underlying devices that it manages. It reports status to the NSVE, which alerts network administrators using the command center, and shows them via alerts and status views onto network hardware and business policies, if policies or actions cannot be deployed.

### DSCs and enterprise security

OverDrive-enabled devices can be installed directly at the wide-area network edge, or behind enterprise firewalls where a site's DSC has access to the devices under its management. The devices may provide IP-based services such as VoIP, or higher-level application services in the enterprise LAN environment.

The DSC initiates a secure connection outbound to the NSVE, to support and manage large enterprise networks with services that run behind multiple layers of firewall security.

To ensure full end-to-end security, all information flows through the OverDrive communications plane between components—including the deployed software agents—use X.509 digital certificates and 128-bit SSL encryption.

This encrypted, bi-directional communication plane allows the NSVE to deconstruct a single business-language policy request into specific configuration directives and send those to the deployed devices via the DSC.

Meanwhile, the deployed DSCs that manage the devices are continuously relaying real-time performance and service feedback for immediate use by administrators.

## DSC details

The DSC manages six types of roles: access, distribution, and aggregation switches; NAT devices, and routers.

- The edge router role can be fulfilled by either one of the 3Com MSR series router with the DSC installed on one of the device's blades, or by any of the Cisco ISR series routers.
- In V3.0, the OverDrive NSV platform supports the firewall role on the edge routers.
- Many 3Com and Cisco branch office switches are supported. OverDrive configures them as either a routed switch environment or an 802.1Q trunked environment.

Roles are not tightly coupled to devices, which can be assigned more than one role, just as a role can be assigned to multiple devices. For example, a switch in a network could fulfill the role of an access switch and a distribution switch at the same time.

OverDrive does not do a bare-metal configuration. Rather, the DSC enrolls a device and begins to configure only those network services that are required by the services that OverDrive manages. However, the DSC extinguishes configuration elements in these areas that do not conform to policy or do not appear in the configured list as allowed exceptions.

(Examples of the network services owned by the DSC are: IPsec VPN configuration, VPN ACLs, router static routes, router WAN interface ACLs, managed VLANs, managed VLAN interface ACLs, and specified OSPF and EIGRP areas.)

## The OverDrive user interface

OverDrive provides three user views, depending on where the user is in the spectrum from network designer, configurator, or administrator; to cloud or VM configurator; to VM manager providing VMs to end users.

## Command center

The command center presents a UI that lets you easily define, control, monitor, and otherwise manage all IP services across your entire network. You can grant rights to admin users based on their roles and profiles, so that at a very granular level you can control and define who can change specific devices, sites, and/or services.

You can specify business-level policy requests to define and control the infrastructure to start and manage network services. The requests are sent to the NSVE, which translates them into service directives that it sends to the deployed DSCs in the network to tell them to start or modify infrastructure services dynamically.

You also receive critical, near real-time feedback on deployed services, configurations, and devices. This feedback appears in two views: one showing how the deployed network environment is actually operating (based on which policies are currently in force), and one displaying a list of alerts detailing status events, warnings, and other problem conditions regarding the policies, components, and devices under management.

## Cloud configurator

The cloud configurator lets administrators define clouds and populate them with VMs.

## Cloud orchestration manager

The cloud orchestration manager provides a subset of the functionality of the cloud configurator, so that IT- and admin-oriented users can add, run, stop, and remove VMs from a cloud, as needed by end uses of the VMs.



## CHAPTER 3

# OverDrive Concepts

---

This chapter introduces many of the OverDrive-specific terms and concepts:

- **Domains**—an abstract view of the network, sites, policies, and so on: a hierarchy of resources and policies
- **Clouds**—metamodels and other OverDrive objects that support the creation of clouds containing VMs in various configurations
- **Resources**—local resources, VLANs, and network/LDAP identities
- **Collections**—groups of resources for a particular purpose
- **Ports and protocols**—particular protocols (TCP, UDP) with the ports (such as http, ftp, telnet) they need for particular network services
- **Policies**—entitlements and network access; resources access to another set of resources
- **Administrator roles**—user-to-domain mappings for who can view or change the system

The concepts are central to network management. They are not restricted to the command center, but note that this section uses screenshots from the command center as that is where they are commonly found.

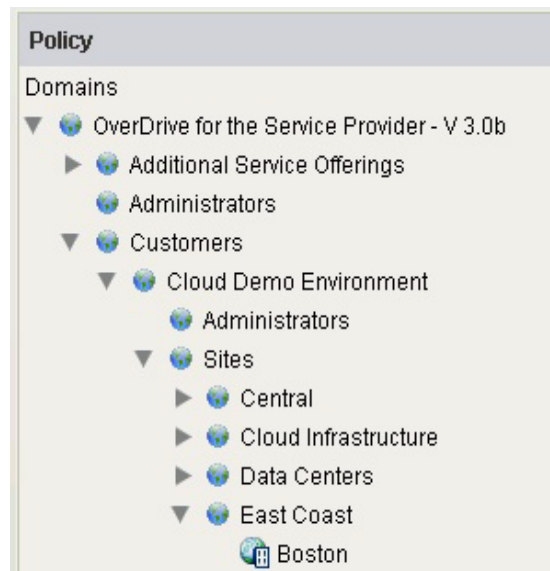
## Domains

Domains are containers of sites, policies, and so on, that give you an abstract view of the network in a tree-like hierarchy.

As you set up the domain tree, you can separate or link systems and networks, and delegate administrative responsibilities based on geography, business needs, or other requirements.

The root domain contains all other network elements, including subdomains.

Subdomains delegate network management responsibilities to defined areas within the root] domain. Typically, an enterprise would use subdomains to separate geographic regions, or to assign administrative responsibility to regional or branch managers.

**Figure 3-1 Domains and subdomains**

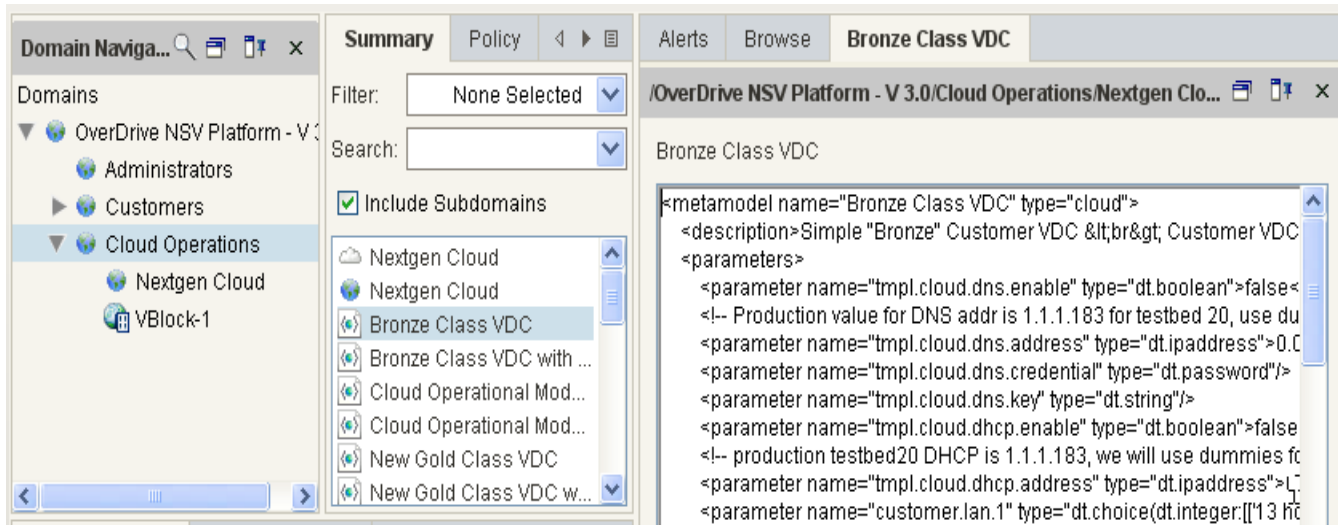
Since every object in the system exists within a domain, the entire set of configuration items also has a hierarchical structure.

## Clouds

Clouds are segregated deployments of virtual computers (VMs). They contain metamodels and other OverDrive objects that collectively allow a domain to support cloud creation and automation.

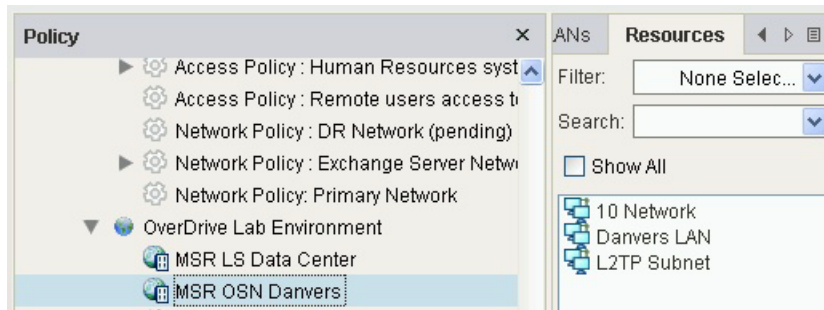
OverDrive enables a domain for cloud management by assigning a cloud metamodel to it. [Figure 3-2](#) shows a domain, Cloud Operations, containing a cloud, Nextgen Cloud, with a tiered metamodel, Bronze Class VDC, which is an XML document partially displayed at the right of the figure.



**Figure 3-2** Clouds and metamodels

## Resources

OverDrive identifies all the elements that may be enrolled into policies as resources. The resources are classed as local resources, VLANs, or network identities.

**Figure 3-3** Local resources in example 3Com lab

## Local resources

A local resource is an abstract definition of a network subnet or single host on a network. A local resource is defined using a name, IP address, and subnet mask, and may incorporate icons to distinguish resource types such as LAN, desktop machine, mail server, etc. A local resource is assigned to a site (see the “Sites” section on page 3-4) but can be moved between sites.

## VLANs

A VLAN is an abstraction of a switch LAN. It may be managed end-to-end as 802.1Q trunks, or, in a routed LAN environment where the LAN traffic is routed among local switch VLANs, at both the access and distribution layers.

OverDrive allows you to define your VLANs at the level of a domain so that you can maintain a consistent naming and numbering scheme for one or more site in the domain. Once defined, you can make one available to some or all of those sites. You can specify the list of VLANs permitted at the site or on specific devices.

**Note**

All VLANs must be known to the NSVE, even if they are not managed by it. VLANs not known to the NSVE are reported as alerts until removed from the switch or incorporated into the policy model. In other words, OverDrive raises alerts about unknown VLANs on the switches it manages. A configuration setting in the DSC specifies whether to report or extinguish unknown VLANs.

## Domain subnets

Domain subnets delimit addressing scope and establish validation constraints within a domain. All the computers and devices within a domain subnet share a common IP routing prefix.

## Network Identities

A network identity is a mapping to a server's MAC address or to an LDAP distinguished name. A network identity could therefore represent an individual or a group in Active Directory. [Figure 3-4](#) shows an example of a browsed-for network identity in the active directory at a specific LDAP server.

**Figure 3-4**      *Assigning a network identity*

The screenshot shows a configuration form with the following fields and values:

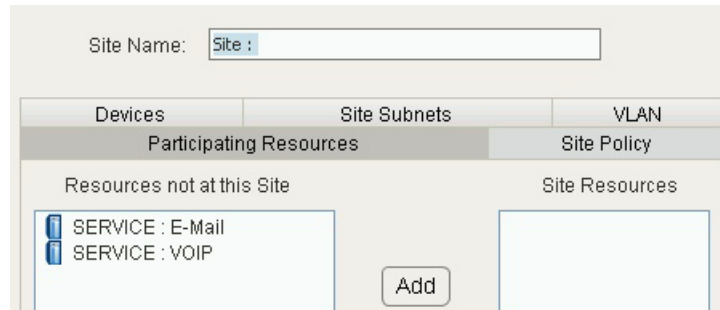
Network Identity Name:	<input type="text" value="Network Identity :"/>
LDAP Server:	ldap://1.1.1.180:389
LDAP BaseDN:	DC=SECOND,DC=LINESIDER,DC=NET
LDAP User:	Administrator
Location:	<input type="text"/>
<input type="button" value="Browse"/>	

## Sites

A site corresponds to a single logical location. In many cases, an OverDrive site represents a discrete physical location. However, a single OverDrive site may be dispersed across multiple physical campuses while retaining a single, logical edge by using private-tagged MPLS VLANs or frame relay networks. Similarly, as with cloud automation, you could have more than one site in a single VDC (virtual data center), with each site offering different cloud services.

Each site is managed by a DSC and one or more OverDrive-managed devices, one or more resources, including subnets or VLANs. Address space for a site is managed as a function of specified subnet definitions and/or explicit VLANs assigned to the site.

**Figure 3-5** *Creating a site and assigning resources*

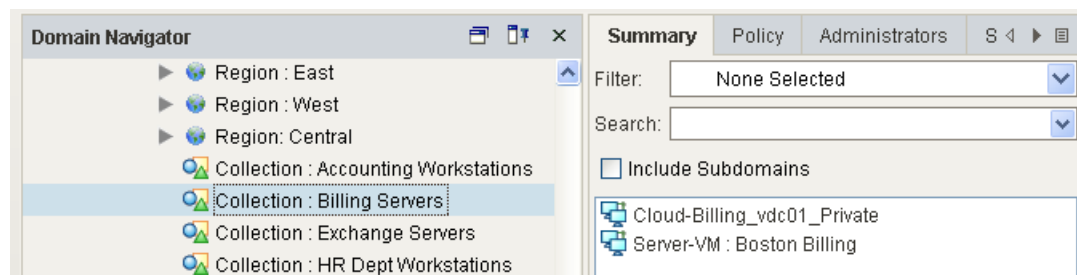


To use a site, you must specify the DSC by name and password, setting up the credentials for the DSC to use in communicating with the NSVE. These are used, along with a digital certificate, to authenticate a DSC.

## Collections

A collection is a set of resources grouped together for some common purpose or function. Collections may include other collections as members.

**Figure 3-6** *A collection of billing servers in an accounting department*



A collection provides an efficient way to manage a number of resources. For example, a collection could contain users that are distributed across multiple sites, so they can gain joint access to a particular destination regardless of their location.

# Ports and protocols

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 the service. (Some standard services are predefined: http, Telnet, ICMP, etc.)

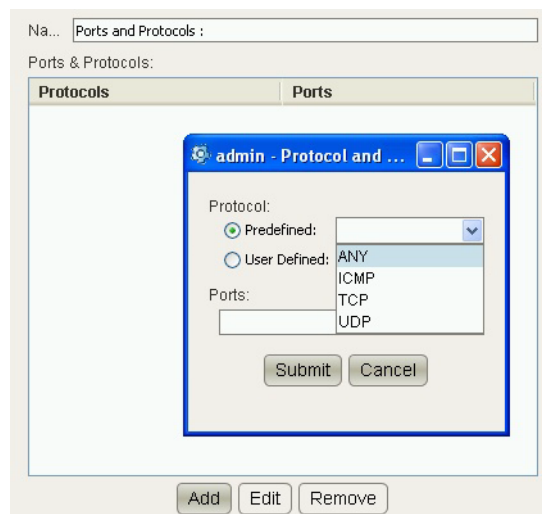
Port and protocol objects can be created if a network service is not defined. You may use the predefined object named ANY to allow network communication on any port and any protocol.



## Note

Ports and protocols were formerly called applications in the GUI. However, the OverDrive code base and metamodel schema continue to use the term applications.

**Figure 3-7** *Assigning TCP protocol to a port*



When you add a port and protocol, you can specify a predefined or user-defined protocol, and a particular port number to use it.

## 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.

## Network access policies

The network access policy is the primary vehicle for defining a network identity's access to a LAN. Network access can also be defined for servers and virtual machines using their MAC addresses as network identities.

This policy manages LAN access for groups of users, based on their membership in security groups or other organizational units in an LDAP tree. Adding a user to an LDAP group gives him or her rights to participate in a switched network; removing the user removes those rights.

OverDrive administrators can set up a model where user assignment to VLANs on switched network can be managed. For example, in a Microsoft active directory, the administrator can map specific active directory groups to VLANs.

## Business policies

The business policy is the primary vehicle for controlling network connectivity.

A business policy is defined in terms of its resources, its ports and protocols, its schedule, and its connection topology. Business policies can be activated or deactivated.

**Resources** (including local resources, collections, and VLANs) can be added or removed from business policies, controlling which systems or subnets can communicate with each other.

**Ports and protocols** must be associated with a business policy for it to be meaningful. A business policy without ports and protocols allows no traffic and appears as invalid in the business status view in the command center.

The **schedule** lets you set starting and ending dates and times for business policies, allowing temporary network access, restricting it after a given date, etc. If you don't set a schedule, the policy will come into effect immediately.

The **connection topology** defines how particular resources can communicate, based on five commonly used models. A business policy may use one of these connection topologies:

- Full mesh—Each resource may connect, bidirectionally, to all other resources in the business policy.
- Hub and spoke, aka spoke initiated—Designates one resource or collection as the hub and all other resources as spokes. Each spoke resource can connect to the hub resource but not to the other resources in the business policy. Only the resources at the spokes can initiate connections.

Typically, this topology is used to enable server-to-client access.

- Hub and spoke, bi-directional—Designates one resource or collection as the hub and all other resources as spokes. Each spoke resource can connect to the hub resource, but not to the other resources in the business policy. Connections can be initiated by resources at the spokes or by the hub.

Typically, this topology is used for head office to branch office access, remote desktop help, and VoIP.

- Peer-to-peer, peer initiated—Designates two resources that can connect to each other. A connection can only be initiated by the designated peer.

Typically, this topology is used to enable a client-server relationship between two peer machines.

- Peer-to-peer, bi-directional—Designates two resources that can connect to each other but not to the other resources in the business policy. Either resource may initiate the connection.

Typically, this topology is used to connect two exchange servers where either side initiates connections and the relationship is only between the peer machines, as, for example, in a connection between the head office and the data center.

The OverDrive provisioning engine can derive from the business policy which sites' network devices must change configurations to support the policy. DSCs automatically reconfigure their devices as policies change, as for example, if a resource is moved to another site or from one switch to another.



### Note

This is key to what OverDrive does: it uses a top-down approach to managing your network to keep the policy true in response to changes.

## Metapolicies

In addition to the network access and business policies, the NSVE uses a metapolicy model to establish some of the constraints and rules to apply when building connections to support the business policies.

The metapolicy allows advanced system administrators to configure the system's default behavior. It is typically configured at initial product installation. The encryption policy (VPN pre-shared versus certificate-based), LDAP credentials, and VLAN architecture and implementation defaults are examples of this.

Metamodels provide similar configuration, principally at initial product installation. See “Metamodels” on page 38.

## Administrator roles

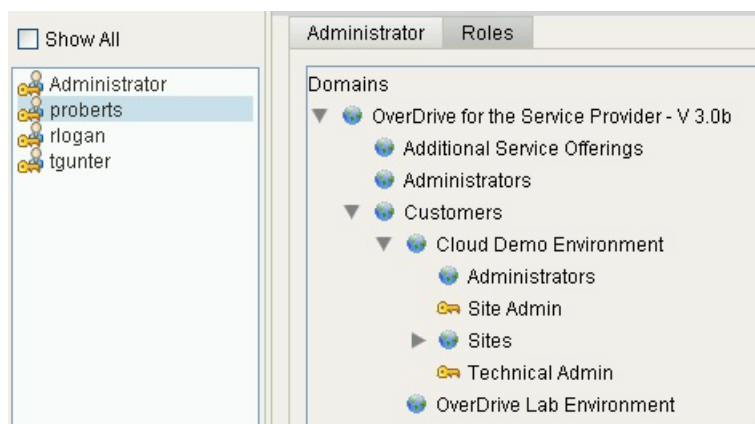
An administrator is a user who can log into the command center to view or change the system. A new OverDrive installation has a default super-user login ID admin with the default password admin.

The command center provides for five administrative roles that may be granted to a user in any combination: business admin, site admin, domain and user admin, technical admin, and audit admin.

The administrative roles determine the actions (such as create, read, update, delete, etc.) that an administrator can perform for certain classes of objects in a given domain and all its subdomains. For example, a user with the audit admin role in a subdomain can view the subdomain's hierarchy, business policies, and resources. Such a user can also generate site and domain compliance reports for its accessible domains.

Domains and subdomains are assigned to admins. For example, the figure below shows that proberts has two admin roles, site and technical, for the Cloud Demo Environment domain and all its subdomains.

**Figure 3-8** Admin proberts, site and technical manager





## CHAPTER 4

# OverDrive Deployment Types

---

This chapter introduces the major types of OverDrive deployment:

- [Site-to-site VPNs](#)
- [Network access control within a site](#)
- [Cloud installations](#)

You can use OverDrive to model and manage a variety of installation or deployment types, which may be used separately or in concert to manage user access to resources within and between sites. For example, you could have a multi-site network with multiple branch offices be connected together.

Domains and sites are common to all the types of installations.

- Domains provide an abstract view of the network, sites, policies, and so on, in a tree-like hierarchy of resources and policies (see the [“Domains” section on page 3-1](#)).
- Sites, as components of domains, contain local resources, network hardware such as routers and switches, and one DSC that manages the hardware as orchestrated by the NSV engine in concert with the command center (see the [“Sites” section on page 3-4](#)).

## Site-to-site VPNs

Site-to-site VPNs include:

- Sites
- Local resources, for example, LAN, desktop machine, mail server, and so on (see the [“Local resources” section on page 3-3](#))
- OverDrive-managed routers such as those by Cisco or 3Com
- Policies for network and business access (see the [“Network access policies” section on page 3-6](#), and the [“Business policies” section on page 3-7](#))
- Port and protocol assignments, which allow users on a given network to access a service (see the [“Ports and protocols” section on page 3-6](#))

OverDrive manages the routers as specified by the command center. It creates VPNs between two or more sites to satisfy the policies defined in the command center, which in turn identify local resources to be made available.

Site-to-site VPNs may be hub-and-spoke (bi-directional or not), or full mesh, as easily specified in OverDrive.

Site-to-site VPNs are managed from the command center.

## Network access control within a site

Within a single site, OverDrive uses network access control features to allow machines or users to share VLAN access to switch ports. The components of this network access control include:

- Network IDs for the devices, in the form of MAC addresses), or for users (in the form of LDAP identities: see the [“Network Identities” section on page 3-4](#))
- OverDrive-managed switches such as those by Cisco, EMC or 3Com
- VLANs as automatically configured on switches (see the [“VLANs” section on page 3-4](#))
- Optionally: RADIUS and Samba as needed, respectively, for authentication (for identity-based network access control) or file and print services, plus policies, local resources, and ports and protocols, as described under [Site-to-site VPNs, page 4-1](#), above.

## Cloud installations

Cloud installations comprise:

- Sites, with local resources and network hardware
- Clouds, essentially virtual data centers containing VMs, combining VLAN management with business policies to automate provisioning of network resources and policies in response to requests for creating VMs
- VMs, which are loaded from seed images created in vSphere and managed by vCenter via the DSC
- Other OverDrive objects as automatically provisioned

Clouds are created and managed by the Cloud Configurator.

VMs are made available as described in the [“Cloud configurator” section on page 5-7](#), and [“Cloud orchestration manager” section on page 5-8](#).





## CHAPTER 5

# OverDrive modeling tools

---

This chapter provides an overview of modeling OverDrive-managed networks in terms of the user interface, the REST API, and XML metamodels for streamlining their creation:

- [Command center](#)—the main OverDrive interface to site-to-site VPNs and network access within a site
- [Cloud configurator](#)—the cloud-oriented user interface to defining and populating clouds with VMs that can be created and managed
- [Cloud orchestration manager](#)—the VM-oriented interface to allow provisioning of VMs to end users
- [Metamodels](#)—for creating clouds and VMs programmatically in concert with the orchestration manager
- [The REST API](#)—for administering and displaying network status without the OverDrive user interface

## Command center

The OverDrive vCOM Command Center is the administrator's main user interface for working with policies, status, alerts, the domain tree, and so on, including many aspects of cloud configuration and management.

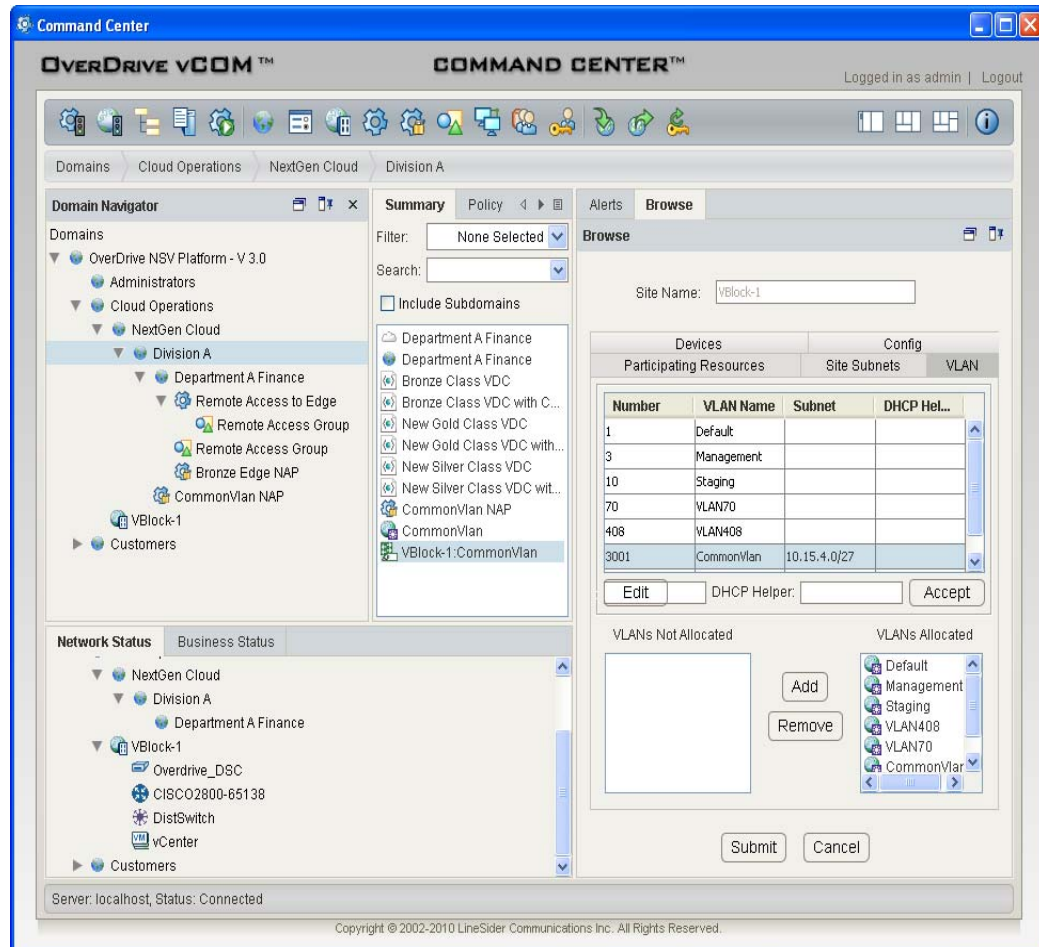
This section provides an overview of the command center's views, and introduces the major components: domains, resources, collections, ports and protocols, policies, and administrative roles:

- [Overview of command center views](#)—the policy view, summary view, status views, browse/edit and alert views
- [Creating objects in the command center](#)—general introduction to how to name objects and how to select them from the toolbar.

## Overview of command center views

The command center contains several views or window panes that you use, along with the toolbar, to control or examine the network components. For example, this is the browse layout view:

**Figure 5-1** Views in the command center's browse layout



The layout selection toolbar in the upper right corner lets you choose from three basic arrangements or perspectives for the views.



These options include, from left to right:

- Hide status layout, the default, which suppresses the status views in favor of displaying a docked domain navigator plus selection (summary) and alert/browse views.

The docked navigator layout is good for an environment where you infrequently need to browse through the tree to find things in different domains. With this layout, you can right-click on domains to navigate into them, and you can use the domain bread crumb trail (below the icon toolbar) to navigate up the domain tree.

- Browse layout, as shown in [Figure 5-1](#). In this view you can click either status tab (network or business), and the alerts or browse tab, to see their particular views.

This layout is appropriate for working in the domain tree, moving through the network, checking network and business status, reacting to alerts, and editing object properties.

- Status layout, in which the business and network status views are both displayed at the same time, and, by default, the alerts view.

The status layout gives you a very quick overview of the status of the entire network. The domain navigator and summary view are by default practically bookmarks and take up little room on the screen.

## Domain navigator view

The command center formats the policy or domain view as a tree of hierarchical container items, which have other objects as members, such as: domains, clouds, collections, sites, network access and business policies, etc.

Non-container items (local resources, administrators, network identities, ports and protocols, as well as network devices) do not appear in this view, but only appear in the selection view.

To see the contents of a particular item, left-click it, and a list of the contents will be displayed in the selection view. To edit an item, right-click it and select Edit. You can also create a new item by right-clicking and then selecting the type of item to create.

## Selection view

The selection view displays the contents of an item selected in the domain view. The view's menu bar lets you view only a particular type, such as policy, metamodels, administrators, sites, devices, VLANs, or resources. Or, you can select Summary to see them all.

This view provides a filter to restrict items to display, or to search for a particular one.

## Browse/alerts view

The browse view via the browse tab displays information about the currently selected object, or it displays the object creation dialogue for a new item. The displayed information depends on the type of object.

The alerts view via the Alerts tab presents warnings and other alerts. This is not a static display, as the entries appear as the alerts happen and disappear when resolved.

## Status views

The status views show the effects of the provisioning process. There are two views: network status and business status. Both views are hierarchic in nature. Each node represents a summary or organizing container for information below it.

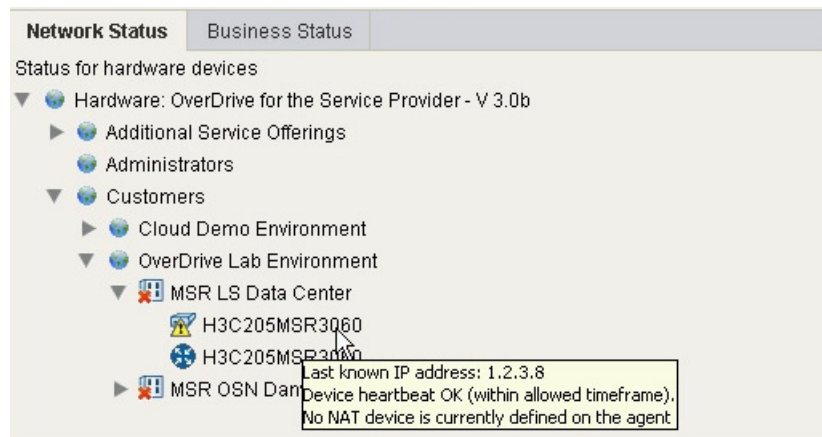
The structure of the views includes information that helps to verify that the intent of configured policies matches what is actually being provisioned. Concretely, this includes what is enabled to allow pairs of resources to communicate with each other as a result of provisioning and also which resources are not being connected due to missing or misconfigured policy.

The items in the views have associated context (right-click) menus for showing more information about them, whether logs and the active policy for network devices, or compliance reports, and so on, in addition to tooltips that report on subnets and devices waiting for their first connection.

## Network status view

The network status view shows the status of sites and managed network devices. It is organized hierarchically. Sites are marked with a red [x] if the network device is not connected and working. You can mouse over (that is, hover over) a network device to see its status.

**Figure 5-2** Network status view



Color coding shows device status, with real-time performance information appearing in a variety of graphical formats. (Real-time device log files are also available.)

Using the site view, admins can quickly spot malfunctioning devices and respond to outages and potential performance problems.

## Business status view

The business policy status view is about the resource pairs being provisioned, where two defined resources are permitted to exchange IP packets.

The business policy status view is particularly useful in debugging configuration problems, because implicit and invalid resource pairs are listed along with well-formed resource pairs.

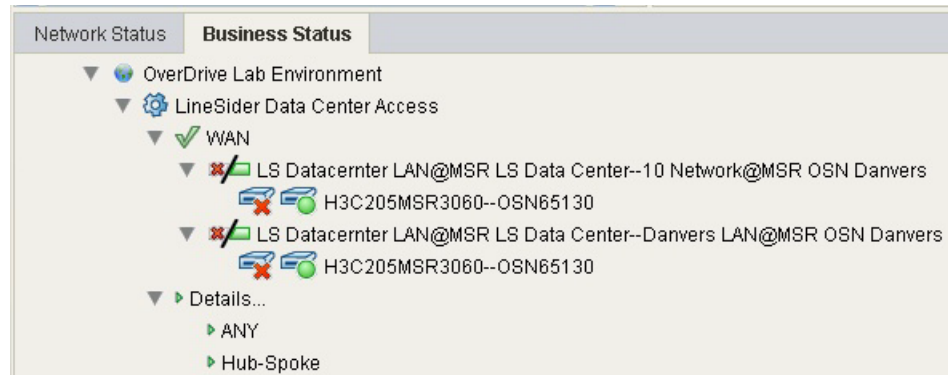
Implicit pairs are those that cannot be provisioned due to some type of user-configuration error, such as a resource with missing or insufficient information, for example, a resource with an undefined IP address, or a resource not yet assigned to a site.

Invalid pairs are those resource-to-resource connections that are possible due to underlying network connectivity that is beyond the control of OverDrive, for example, two resources in the same subnet on the same physical LAN segment.

If configuration is incorrect, pairs that should be provisioned but for some reason are not will appear in the invalid or implicit categories. (You can hover your mouse over the pair to see the reason.)

The business policy view, as shown in [Figure 5-3](#) provides a unique, top-down picture of the deployed infrastructure and the policies that define and control its behavior.

**Figure 5-3 Business status view**



Using this view, you can quickly identify non-functioning policies. You can drill down into an individual policy and see its individual services and their status. You can continue to drill down deeper into any specific service to see the status of the actual devices that support it.

## Creating objects in the command center

You can use right-click context menus as well as toolbars, to create objects, as briefly described below. When you do so, follow the general recommendations here.

## General recommendations

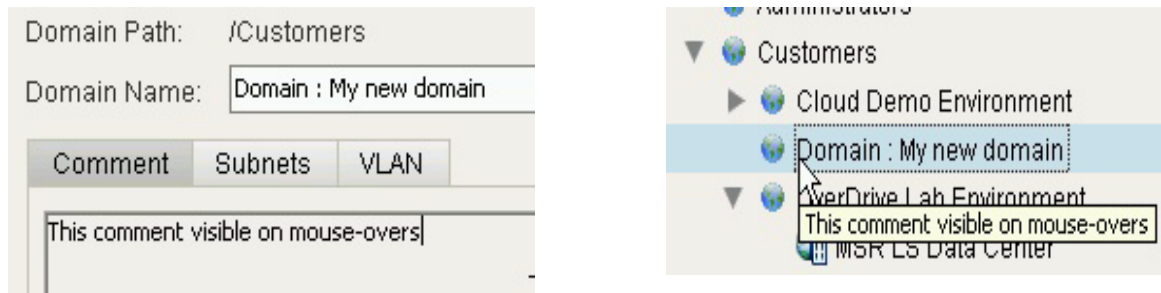
All items you create have two features in common, as shown in [Figure 5-4](#):

- A name, pre-filled with the type of object, such as, for example, Domain: Keep this pre-filled type string until you build up a good understanding of what types of items you see where in the command center.



**Note** Routers and switches may not have spaces in their names.

- A comment or description displayed as a tooltip when you hover the mouse over the object. These comments help you capture additional information that can be displayed about the object, for example, contact information for a site, or the purpose of a resource.

**Figure 5-4** Object type and mouse-over comments.







- Name routers and switches uniquely and identifiably, generally, by including the model and a unique ID, typically a number.  
We recommend that you use a combination of the name and the comment field to help you properly identify a device.
- When you configure an object, enter as much information as possible on all tabs.
- If you enroll an object like a local resource or VLAN into a policy, the NSVE alerts you if some of the critical information needed to build the services is missing. For example, if you create a local resource, name it, and assign it to a site without filling in the IP address, and then try to use it in a policy, an alert in the business policy status view tells you that the IP address is missing.




## Creating objects from the toolbar

The toolbar icons light up or gray out, depending on which item you have highlighted in the policy view. They stay the same if you next highlight an item in the selection view. In the selection view, you can create an object of the same kind that you have highlighted in the domain tree.

If you have selected an object that can contain other objects, they will be included in the container object. For example if you select a site and create a local resource, it will automatically be included in the site.

**Table 5-1** Objects you can create from the toolbar

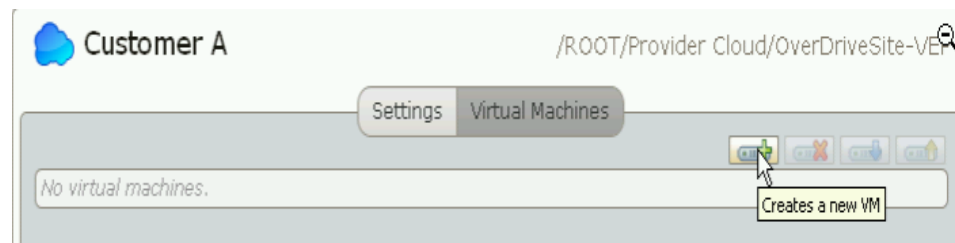
Object	Icon	Object	Icon
Administrator		Network access policy	
Business policy		Network identity	
Collection		Ports & protocols	

Object	Icon	Object	Icon
Domain		Site	
Local resource			

## Cloud configurator

The Cloud Configurator user interface allows administrators to define clouds and populate them with VMs. For example, here is a representative view, with the Settings tab in focus:

**Figure 5-5** Cloud settings screen example



Clouds are very similar to domains and may have the same components, but they also combine VLAN management with business policies to automate provisioning of network resources and policies in response to requests for creating VMs. They may, like domains, contain sites, business policies, and other domains or clouds.

## Creating and configuring clouds

Clouds are created based on customizable models called metamodels that specify parameters such as subnet address ranges, VLAN ranges, whether DNS is enabled and with which credentials and keys, which types of customers can access the cloud, and what kinds of VMs they can use.

The metamodels determine which panels of prompts are presented to collect configuration specifications, how many fields there are within a panel, and what type of data can be collected. For example, the following figure illustrates parameters that have been specified for collection in a VLAN-specific panel:

**Figure 5-6 Customizable cloud parameters (VLAN)**

**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

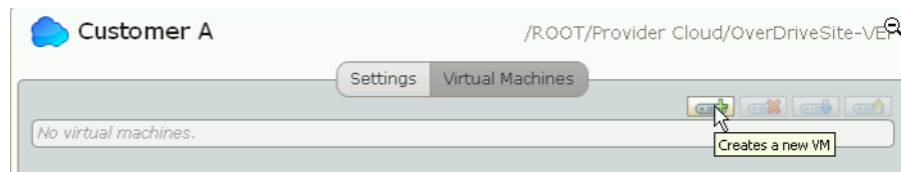
Infrastructure Number: 3000

Cancel < Prev Next > Finish

Once clouds are created, the configurator provides a Settings tab with appropriate information, as in [Figure 5-5 on page 5-7](#).

## Populating clouds with VMs

Adding virtual machines to a cloud is simple: click the cloud's Virtual Machines tab, then the add VM button. Provide a hostname, and a model from a drop-down list, specify a few parameters (which may be optional).



Run, stop, power down, and remove VMs very simply.

## Cloud orchestration manager

The Cloud Orchestration Manager provides a subset of the functionality of the Cloud Configurator, namely, the ability to add, run, stop, and remove VMs from a previously created cloud.

This interface is designed for use by near-end users who will create and power on VMs for generally temporary use by real end users.

## Metamodels

Metamodels let OverDrive administrators support network configurations to automate cloud creation such as for virtual data centers with virtual machines.



These XML documents provide preconfigured settings to:

- Create parts of OverDrive-managed networks
- Present certain cloud and VM settings for the Cloud Configurator or Orchestration Manager user to enter or modify
- Specify domains, business policies, network access policies, resources, VLANs, and so on

## The REST API

OverDrive uses a RESTful web service API to support the OverDrive command center and to allow administration and display of the status of a network, without requiring a specific user interface. It allows for the development of in-company-specific interfaces

The API operates on the following primary resource types, which have been described earlier: domains, sites, DSCs, resources, network elements (IDs), policies, groups, and admins.





## CHAPTER 6

# Network management scenarios

---

This chapter sketches some network management scenarios:

- [Putting another admin in charge of a subdomain](#)
- [Monitoring network and device status](#)
- [Workflow for a sample business policy](#)
- [Adjusting the network after moving a server](#)
- [Creating reports](#)

This chapter does not tell you much about how to do something, but what can be done. It provides some overall perspective on what OverDrive can do, and how easy it is. If you want to see how to do these actions in detail, refer to the *Cisco OverDrive 4.0 User Guide*.

## Putting another admin in charge of a subdomain

Domains support delegation; technically they are administrative domains. The scope of an administrative role is defined by the domain in which it is granted to the administrator. This role applies to that domain, and all its subdomains. OverDrive lets you assign any or all of the five roles to an administrator.

Do the following:

- 
- Step 1** Right click any domain and choose New Administrator.
  - Step 2** Under the Administrator tab, enter the username and password, and a comment to show as a tooltip.
  - Step 3** Under the Roles tab:
    - a. Expand the domain tree.
    - b. Right-click the highest-level domain to which the administrator will be allowed access for the role you are assigning.
    - c. Choose the administrator's role (his function and permissions).
  - Step 4** Double-click the domain to open it, and verify that the admin has been added correctly, as with the business admin in the following example figure:
  - Step 5** Click Submit.

For details, especially the types of roles, see the *Cisco OverDrive 4.0 User Guide*.

---

## Monitoring network and device status

Monitoring the network is very easy, thanks to the graphic presentation of device and communication status in the network status view.

When some error condition highlights a disadvantaged status by displaying an error flag, you can drill down into the devices and associated logs to see what is happening.

For example, OverDrive might report a network (hardware) problem, as in the following window:

To find the problem do the following:

- 
- |               |   |
|---------------|---|
| <b>Step 1</b> | Click the Network Status tab.                 |
| <b>Step 2</b> | Find the DSC (here H3C205MSR3060).            |
| <b>Step 3</b> | Right-click it and choose View Configuration. |
- 

See the *Cisco OverDrive 4.0 User Guide* for more information about monitoring network and device status, as well as using the alerts window:

- Recognizing a library of connection icons.
- Using the alerts window.

## Workflow for a sample business policy

With OverDrive, you can create a new business policy in a just a few steps and then implement it network-wide.

The entire process can be completed within seconds, as suggested in this example.

1. Suppose the admin wants to allow users to communicate, whether they are in Danvers, on the LS Datacenter LANS, or on the 10 Network.
2. The admin creates a new business policy, specifying the participating resources by adding them from the Available Resources column to the Participating Resources column.
3. He then choose a hub-spoke network, allowing the ANY communications protocol.
4. The NSVE contacts the DSCs involved. They contact the switches and routers to link the two sites, and the status view shows the communications in effect:

## Adjusting the network after moving a server

Consider moving a server from San Francisco to Boston. Without OverDrive, network engineers would have to change everyone's access, but with OverDrive, high-level business policies drive the network, and their components are very easy to update.

Making the change from San Francisco to Boston is really simple:

- 
- |               |  |
|---------------|--|
| <b>Step 1</b> | Right-click on the server to be changed, in the Resources tab for the appropriate domain, and choose Edit. |
| <b>Step 2</b> | Change the Site drop-down from San Francisco to Boston.  |

**Step 3** Change the IP address to the Boston server's IP address.

**Step 4** Click Submit.

That's it. In a minute or two, OverDrive creates new VPN tunnels as needed for the configuration change. For details, see *Cisco OverDrive 4.0 User Guide*.

---

## Creating reports

OverDrive lets you generate reports easily, for example, to:

- Satisfy federal regulations such as for HIPAA (Health Insurance Portability and Accountability Act), PCI (Payment Card Industry), and SOX (Sarbanes Oxley)
- Provide site and domain compliance reports using the Launch Audit Log toolbar button.





# APPENDIX **A**

## FAQs

---

This appendix answers frequently asked questions.

**1. How many NSV engines do I need?**

You only need one. That should be enough for hundreds of DSCs. However, for fail-safe and redundancy issues, you might want at least two

**2. How many DSCs do I need?**

You need one DSC for every site. DSCs come in models that handle 25, 50, or 100 devices. Some sites will have only a router. Others will have both a distribution and access switch, while others may have combinations of those and/or aggregation switches, managed devices, or NAT device. See the [“DSC details” section on page 2-3](#).

**3. What are NSVE and DSC hardware and operating system requirements?**

This is covered in Installing OverDrive, but basically each NSVE and each DSC is a Linux box running CentOS.

**4. What options are available for redundancy?**

The PostgreSQL database uses a warm standby method with write-ahead logs containing changes to apply to the database. When PostgreSQL runs in archive mode, these files are copied to another location, so they can be used to recover in the event of a failure. The standby is then run in recovery mode, with the archive files copied to it, and then applied to the database. In the event of a failure of the primary, the standby is taken out of recovery mode (by creating a trigger file), and then the standby can take over as the new primary. (A script performs the steps to create the warm standby server.).







## GLOSSARY

---

### A

<b>ACL (access control list)</b>	Generally a list of permissions to objects, e.g., read, write, delete, for users or system processes.
<b>Active Directory</b>	A hierarchical directory service built on DNS in which workgroup and individual names can be found, and associated together with privileges.
<b>access switch</b>	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).
<b>administrator</b>	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.
<b>agent</b>	DSC software, running on an OverDrive appliance, that manages network devices such as routers and switches. See DSC (device service controller).
<b>aggregation switch</b>	A switch that provides aggregate or group networks.

---

### B

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

---

### C

<b>connection topology</b>	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).
<b>command center</b>	The client UI interface to OverDrive, previously called an admin console, management portal, or policy workbench.
<b>collection</b>	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

<b>device</b>	Networking hardware such as a switch or router.
<b>distribution switch</b>	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.
<b>DSC (device service controller)</b>	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.
<b>DSC server</b>	An appliance with one or more DSCs on it.
<b>domain</b>	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

<b>full mesh</b>	See <a href="#">connection topology</a> .
------------------	---

---

## H

<b>hub and spoke</b>	See <a href="#">connection topology</a> .
----------------------	---

---

## M

<b>metamodel</b>	An XML document specifying configuration information for clouds, domains, VMs, and so on.
<b>metapolicy</b>	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.
<b>MSP (managed service provider)</b>	Comparable to a reseller, an MSP provides services to a client, such as installing, configuring, and helping to manage OverDrive networks.

---

## N

<b>network access policy</b>	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.
------------------------------	---

<b>network identities</b>	Mappings to LDAP distinguished names, therefore able to represent an individual or a group in Microsoft Active Directory.
<b>NSVE (network services virtualization engine)</b>	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

<b>policies</b>	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.
<b>policy server</b>	See <a href="#">NSVE (network services virtualization engine)</a> .
<b>ports and protocols</b>	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

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

---

## S

<b>site</b>	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.)
<b>subnet</b>	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

---

### Numerics

3Com MSR series router [2-3](#)  
802.1Q [2-3, 3-4](#)

---

### A

access control  
    intra-site [4-2](#)  
Active Directory [3-7](#)  
administrative  
    roles [3-8](#)  
administrator [3-8](#)  
ANY [3-6](#)  
applications [3-6](#)  
architecture [2-1](#)

---

### B

browse layout [5-3](#)  
business policies [3-7](#)  
business policy view [5-5](#)  
business status view [5-3, 5-4](#)

---

### C

cautions  
    significance of [2-viii](#)  
Cisco ISR series router [2-3](#)  
cloud  
    configurator [2-4, 5-7](#)  
    installations [4-2](#)  
    orchestration manager [2-4, 5-8](#)

clouds [3-2](#)  
collections [3-5](#)  
command center [2-3, 5-1](#)  
connection topologies [3-7](#)  
conventions [2-viii](#)

---

### D

deployment types [4-1](#)  
device conditions [6-2](#)  
distinguished names [3-4](#)  
domains  
    root [3-1](#)  
    subdomains [3-1](#)  
    tree [3-1](#)  
Domain subnets [3-4](#)  
DSC [2-1](#)  
    high-level details [2-3](#)  
    overview [2-2](#)

---

### E

edge routers [2-3](#)  
EIGRP [2-3](#)  
encryption policy [3-8](#)  
extinguishing VLANs [3-4](#)

---

### F

firewalls [2-2](#)  
full mesh topology [3-7](#)

---

**G**

groups

Active Directory [3-7](#)

---

**H**

hide status layout [5-2](#)

HIPAA (Health Insurance Portability and Accountability Act) [6-3](#)

http [3-6](#)

hub and spoke [3-7](#)

---

**I**

ICMP [3-6](#)

identities

network [3-4](#)

intra-site access control [4-2](#)

invalid resource pairs [5-4](#)

IPsec VPN configuration [2-3](#)

---

**L**

LAN traffic [3-4](#)

layout

browse [5-3](#)

hide status [5-2](#)

status [5-3](#)

LDAP

distinguished names [3-4](#)

groups [3-6](#)

servers [3-4](#)

local resources [3-3](#)

local switch VLANs [3-4](#)

logical network [1-1](#)

---

**M**

MAC addresses [4-2](#)

managed VLANs [2-3, 3-4](#)

metamodels [1-2](#)

metapolicies [3-8](#)

monitoring

devices [6-2](#)

network [6-2](#)

MPLS VLANs [3-4](#)

---

**N**

network

access policies [3-6](#)

conditions [6-2](#)

identities [3-4](#)

logical [1-1](#)

management scenarios [6-1](#)

services virtualization [1-2](#)

status view [5-3](#)

network identities [3-3](#)

network status view [5-4](#)

NSVE policy server [2-2](#)

---

**O**

OSPF [2-3](#)

OverDrive user interfaces [2-3](#)

---

**P**

PCI (Payment Card Industry) [6-3](#)

peer-to-peer [3-7](#)

policies

business [3-7](#)

metapolicies [3-8](#)

network access [3-6](#)

- types [3-6](#)
- policy requests [2-2, 2-3](#)
- ports and protocols [3-6](#)
- PostgreSQL [A-1](#)
- provisioning engine [1-2](#)

## R

- RADIUS [4-2](#)
- reports [6-3](#)
- resource pairs [5-4](#)
  - invalid [5-4](#)
  - well-formed [5-4](#)
- resources [3-3, 3-7](#)
  - collections of [3-5](#)
  - local [3-3](#)
- RESTful API [5-9](#)
- roles
  - administrative [3-8](#)
- root domains [3-1](#)
- routed switch environments [2-3](#)
- routers
  - 3Com MSR [2-3](#)
  - Cisco ISR [2-3](#)
  - edge [2-3](#)
- router static routes [2-3](#)
- router WAN interface ACLs [2-3](#)

## S

- Samba [4-2](#)
- scenarios
  - network management [6-1](#)
- selection view [5-3](#)
- sites [3-4](#)
- site-to-site VPNs [4-1](#)
- SNMP [2-1](#)
- SOX (Sarbanes Oxley) [6-3](#)

- SSH [2-1](#)
- SSL encryption [2-2](#)
- static routes [2-3](#)
- status layout [5-3](#)
- status view [5-3](#)
- subdomains [3-1, 3-2](#)
- submitting a service request [2-viii](#)
- subnets [3-3, 3-5, 3-7](#)

## T

- Telnet [2-1, 3-6](#)
- tunnels
  - VPN [6-3](#)

## V

- vCenter [4-2](#)
- vCOM command center [5-1](#)
- VDCs [3-4](#)
- views
  - business policy [5-5](#)
  - business status [5-3, 5-4](#)
  - network status [5-3, 5-4](#)
  - selection [5-3](#)
  - status [5-3](#)
- VLANs [3-3, 3-4](#)
  - extinguishing [3-4](#)
  - managed [2-3, 3-4](#)
  - MPLS [3-4](#)
- VMs
  - populating in clouds [5-8](#)
- VoIP [2-2, 3-7](#)
- VPNs
  - ACLs [2-3](#)
  - site-to-site [4-1](#)
  - tunnels [6-3](#)
- vSphere [4-2](#)

---

## W

warnings, significance of [2-viii](#)

well-formed resource pairs [5-4](#)

---

## X

X.509 digital certificates [2-2](#)