CHAPTER 3

OverDrive Network Hypervisor Concepts

This chapter introduces many of the OverDrive Network Hypervisor-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 Network Hypervisor 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

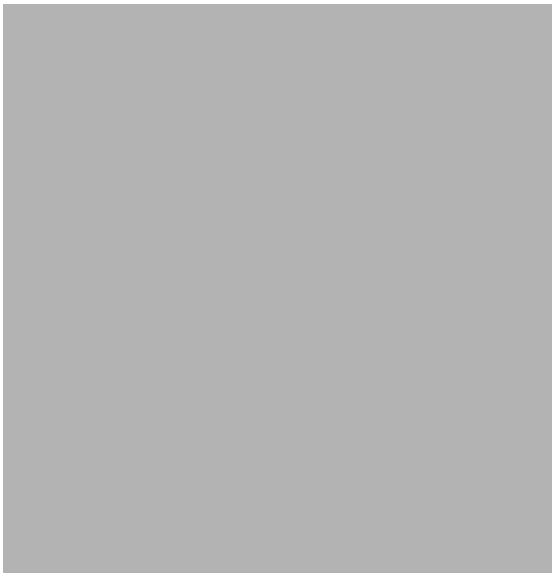
Domains are containers of sites, policies, and so on, that give you an abstract view of the network in a tree-like hierarchy.

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 Network Hypervisor objects that collectively allow a domain to support cloud creation and automation.

OverDrive Network Hypervisor 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 Network Hypervisor 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 Network Hypervisor 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 Network Hypervisor 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

Sites

A site corresponds to a single logical location. In many cases, an OverDrive Network Hypervisor site represents a discrete physical location. However, a single OverDrive Network Hypervisor 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 Network Hypervisor-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 Network Hypervisor 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 Network Hypervisor 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 Network Hypervisor 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 Network Hypervisor 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 Network Hypervisor 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 Network Hypervisor 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 Network Hypervisor 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