CHAPTER 4

OverDrive Network Hypervisor Deployment Types

This chapter introduces the major types of OverDrive Network Hypervisor deployment:

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

You can use OverDrive Network Hypervisor 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 Network Hypervisor-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 Network Hypervisor 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 Network Hypervisor.

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

Network access control within a site

Within a single site, OverDrive Network Hypervisor 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 Network Hypervisor-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 Network Hypervisor 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.