CHAPTER 2

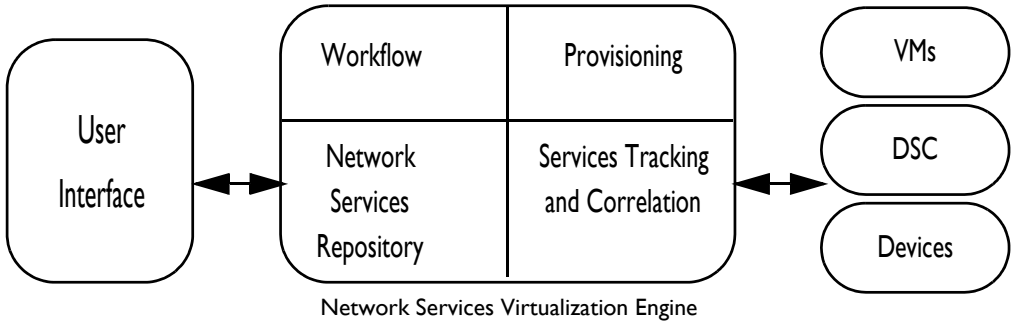
Introducing OverDrive Network Hypervisor Architecture

This chapter introduces the OverDrive Network Hypervisor architecture:

- Overview
- The NSVE policy server
- Device service controllers
- The OverDrive Network Hypervisor user interface

Overview

Figure 2-1 Overview of Architecture



OverDrive Network Hypervisor 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 Network Hypervisor 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 Network Hypervisor-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 Network Hypervisor 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 Network Hypervisor NSV platform supports the firewall role on the edge routers.
- Many 3Com and Cisco branch office switches are supported. OverDrive Network Hypervisor 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 Network Hypervisor 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 Network Hypervisor 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 Network Hypervisor user interface

OverDrive Network Hypervisor 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.