CHAPTER 2

Setting up intra-site network access

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

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

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

Install type: intra-site network access

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

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

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

Providing network access for network identities

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

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

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

Setting up access and routing mechanisms

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

For the interconnect modes:

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

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

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

Defining subnets and domain VLANs

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

Configuring subnets

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

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

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

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

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

To add new subnets under the Subnets tab:

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

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

4. Click Accept.

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

Creating and configuring domain VLANs

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

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

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

Managed and unmanaged VLANs

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

Managed VLANs are managed by OverDrive network access policies.

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

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

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

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

Ports and Pools

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

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

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

Creating a domain VLAN

To create a domain VLAN:

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

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

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

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

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

   b. Generally, leave the following items checked except for the first:

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

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

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

   c. Click OK.

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

Allocating VLANs to sites

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

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

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

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

3. Edit the site and open its VLAN tab.

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

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

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

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

Creating network identities

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

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

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

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

To create a network identity, such as a user:

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

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

3. Click Add to add that user.

4. Click Submit.

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

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

Using business and network access policies

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

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

Creating a network access policy

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

To create a network access policy:

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

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

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

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

Scenario 2a: creating VLANs for sites

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

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

5. Edit the domain and go to the VLAN tab in the summary view.
6. Create VLANs for any infrastructure VLANs that need to exist on the switch but will not be managed by OverDrive, for example, a VLAN to be used for device management (see "Creating a domain VLAN" on page 25).

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

7. Create VLANs for each of the business groups that you want to manage in this network:
   a. Create a Sales VLAN (300) and an Accounting VLAN (301).
   b. Select Managed by Overdrive and the option to automatically assign to the site.
   c. Also select the option to have ACL enforcement on the VLAN.

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