CHAPTER 3

Controlling intra-site network access

This chapter concentrates on using network access policies to control a user's access to the network.

- Install type: basic user access
- Reviewing available VLANs
- Showing VLAN switch assignments
- Creating a user for a network policy
- Watching a user log in
- Controlling access by active directory admins
- Scenario 2b: creating a network ID and access policy

We review how you give people access to the network. The chapter after this explains how to use collections to give groups of users access to resources on specific sites—see the"Controlling access by active directory admins" section on page 3-6.

Network access policies are about whether or not a user who plugs into the switch can be authenticated to the network via RADIUS and thus get access to the VLAN.

Install type: basic user access

You can further manage intra-site networks by concentrating on network access policies for individuals, groups, and services, as explained in this chapter.

Once you have created a network access policy and assigned network identities to it, you can choose which VLAN the policy will be affiliated with. Since a VLAN can only be assigned to one network access policy at a time, if you choose a VLAN that is already in use in another network access policy OverDrive warns that this will result in removing the VLAN from the other network access policy if you choose it.

Network access polices only grant access to the network. When a user plugs a computer into an 802.1x enabled switch, the switch sends to RADIUS the authentication messages from the user's workstation. If the user is authenticated, the OverDrive plugin to RADIUS informs the DSC.

OverDrive looks this user up in its list of network access policies. If the user or the user's group is found to be associated with a VLAN, the DSC identifies the port to which the user is attached and begins to allocate the port to the VLAN. Once the user is assigned to the VLAN, OverDrive monitors the port until the user is allocated an IP address, at which time it begins to build policies to permit appropriate user access to destination resources.

Reviewing available VLANs

In order for a person to be allowed on the network, there has to be a network access policy that associates him or her with a particular VLAN.

Let's look at a domain that already has some VLANs created in it. For example, select the domain and see the VLANs in the selection view:

The two sites, Boston and Philadelphia, have their own versions of these: Boston: VLAN: Sales and Philadelphia: VLAN: Sales, as you can see by highlighting the Philadelphia site and looking at the VLANs tab in the selection view:

The sites have these VLANs because they have inherited the VLANs that are defined for this domain. (As discussed in the "Creating and configuring domain VLANs" section on page 2-3, the staging and default VLANs always exist.)

If you select one of these, such as Philadelphia VLAN: Sales, you can see in the site's VLAN tab the various VLAN parameters as well as which have been allocated for use at the site. In the following section, we will add users from the sales department.

Figure 3-1 VLANs at the Philadelphia site in the East Coast domain

(You can see the subnet and DHCP helper values in the preceding figure. See the "Allocating VLANs to sites" section on page 2-5 for a refresher on how these were assigned.)

Showing VLAN switch assignments

In order to have network access, your site of course has to have switches: one for the distribution layer, which is where the routing happens, and one for the access layer, which is where people plug in. (Depending on the size of your site, you may also have an aggregation layer which aggregates a high port density or lower speed connections into faster trunks.)

You can run several commands on the switches to show configuration, interfaces, and routes, (as on the router), and you can also show VLAN assignments:

Typical output from the Show VLAN Assignment command to the switch is shown below:

This figure shows the default and staging VLANs (numbered 1 and10), but no other VLANs, because the ones we want for sales and billing have not yet been populated with users, so they are not yet active.

Creating a user for a network policy

Let's look at Philadelphia again so we can follow this example. In order to allow a person onto the net, as mentioned, you need a network access policy. Follow the instructions in the "Creating a network access policy" section on page 2-7, only now you can choose resources for one of the VLANs we have just created:

Starting with this network access policy that will associate a user with the Sales VLAN, here's how to create a user and add him to the policy:

1. Right-click the East Coast domain (in our example) and choose New Network Identity
2. Click the Browse button to launch the LDAP browser. (See the *Cisco OverDrive 4.0 Installation Guide* for editing LDAP credentials in overdrive.xml on the server and in services.xml for the DSC.)
3. Browse to the Remote Sales group and click OK.

   We have created a new network identity named Remote Sales. It contains the users in the group. (See the "Creating network identities" section on page 2-6.)
4. Right-click Network Access Policy: Sales in the domain and choose Edit.

The network access policy for Sales opens up, with a VLAN: Sales. Remote Sales listed in the participating resources pane.

Note A site VLAN can only belong to a single network access policy. The network access policy shows domain VLANs as well as network identities. Because network identities can only be assigned to one network access policy at a time, OverDrive uses an asterisk (*) next to the name to indicate one that is already assigned elsewhere.

5. Choose the VLAN, highlight Remote Sales, and click Add to put it into the participating resources pane:

6. Click Submit.

What these steps have effected is a policy that says, if you see someone log into the network and he belongs to the group Remote Sales, put him into the Sales VLAN. That's why we talk about network access control.

Watching a user log in

If the user you have added has not yet logged in, as soon as he does, he will show up in the Alerts window as an active user with no IP address:

You can right-click that user and jump to the network status view to see who he is. If you're too slow, you'll see him in Remote Sales, instead, and you will not see him passing through the staging VLAN, as discussed below.

If, on the other hand, the user is for some reason not known to OverDrive (perhaps in a group that hasn't been configured in OverDrive), he will stay in the Alerts window as unknown:

When you are looking at the network status view, and if you're fast enough, you'll see the newly logged in user showing up in Staging as an unknown user:

Note Defined VLANs don't exist on the screen all the time because they get created on demand. Also, note that we are adding two users, not one, because they are each members of the LDAP group Remote Sales.

At this point, the logged-in user has been authenticated but has not yet received an IP address. Even though OverDrive knows the username, it does not know where to place him.

Once the DHCP server has given him an IP address, for a brief moment, he will show up in the Alerts window as an active user with no IP address, and will then immediately be put into the VLAN to which he was assigned. In other words, when the network access policy recognizes this user as belonging to the Remote Sales group, it will put him into VLAN:Sales:

Controlling access by active directory admins

OverDrive permits controlled network administration by active directory administrators.

If you set up OverDrive to manage network access control, you can hand over a small part of the network control to a Microsoft administrator to decide who belongs on which VLAN. You can do this without actually handing over the keys to the switches, which is what you want, because you don't want that administrator to start configuring switches.

What's going to happen is that as soon as he adds users, with a login in Sales, OverDrive is going to begin recognizing them as being not only allowed on our system but allowed in Sales.

When you or the Microsoft administrator put a user into a VLAN, he won't have an IP address because he will be waiting for one from the DHCP server. Once he has an IP addresses, the system will figure out what he is allowed to access on the network, and will build policy to support that access.

(As mentioned earlier, we recommend that you use VLANs in policies rather than network identities unless you specifically want fine-grained control over an individual user's access.)

Scenario 2b: creating a network ID and access policy

This following steps outline how to create a network identity for a group individual in an LDAP directory.

Creating a network ID for a group is one of the steps in allowing a group of users access a resource such as a CRM server. For more information, see the "Creating network identities" section on page 2-6 and the "Creating a network access policy" section on page 2-7.

1. Click the create network ID icon.
2. Browse your LDAP and find a group that matches your Sales users.
3. Click OK.

At this point, you can create a network policy and assign the Sales group to it (for more information, see the "Creating a network access policy" section on page 2-7):

1. In the domain that you have selected for managing network access, click the create network access policy icon.
2. Type in a name for the network access policy (Sales).
3. Select the Sales VLAN using the dropdown.
4. Select the LDAP group that you created in the previous few steps, and add it to the Network Access Policy.