



Clustering Switches

This chapter provides these topics to help you get started with switch clustering:

- [Understanding Switch Clusters, page 5-2](#)
- [Planning a Switch Cluster, page 5-4](#)
- [Creating a Switch Cluster, page 5-15](#)
- [Using the CLI to Manage Switch Clusters, page 5-20](#)
- [Using SNMP to Manage Switch Clusters, page 5-21](#)

Configuring switch clusters is more easily done from the Cluster Management Suite (CMS) web-based interface than through the command-line interface (CLI). Therefore, information in this chapter focuses on using CMS to create a cluster. See [Chapter 3, “Getting Started with CMS,”](#) for additional information about switch clusters and the clustering options. For complete procedures on using CMS to configure switch clusters, refer to the online help.

For the cluster commands, refer to the *Catalyst 3550 Multilayer Switch Command Reference*.



Note

Refer to the release notes for the list of Catalyst switches enabled for switch clustering, including which ones can be command switches and which ones can only be member switches, and for the required software versions and browser and Java plug-in configurations.



Note

This chapter focuses on Catalyst 3550 switch clusters. It also includes guidelines and limitations for clusters mixed with other cluster-capable Catalyst switches, but it does not provide complete descriptions of the cluster features for these other switches. For complete cluster information for a specific Catalyst platform, refer to the software configuration guide for that switch.

Understanding Switch Clusters

A switch cluster is a group of connected Catalyst switches that are managed as a single entity. In a switch cluster, 1 switch must be designated as the *command switch* and up to 15 switches can be *member switches*. The command switch is the single point of access used to configure, manage, and monitor the member switches. Cluster members can belong to only one cluster at a time.

The benefits of clustering switches include:

- Management of Catalyst switches regardless of their interconnection media and their physical location. The switches can be in the same location, or they can be distributed across a Layer 2 or Layer 3 (if you are using Catalyst 3550 multilayer switches) network. Cluster members are connected through at least one VLAN in common with the command switch, according to the connectivity guidelines described in the [“Automatic Discovery of Cluster Candidates and Members” section on page 5-4](#).
- Command-switch redundancy if a command switch fails. One or more switches can be designated as *standby command switches* to avoid losing contact with cluster members. A *cluster standby group* is a group of standby command switches.
- Management of a variety of Catalyst switches through a single IP address. This conserves on IP addresses, especially if you have a limited number of them. All communication with the switch cluster is through the command switch IP address.

For other clustering benefits, see the [“Advantages of Using CMS and Clustering Switches” section on page 1-7](#).

Refer to the release notes for the list of Catalyst desktop switches enabled for switch clustering, including which ones can be command switches and which ones can only be member switches, and the required software versions.

Command Switch Characteristics

A Catalyst 3550 command switch must meet these requirements:

- It is running Cisco IOS Release 12.1(4)EA1.
- It has an IP address.
- It has Cisco Discovery Protocol (CDP) version 2 enabled (the default).
- It is not a command or member switch of another cluster.

**Note**

When a cluster has a mix of Catalyst switches, we strongly recommend using only a Catalyst 3550 switch as the command switch.

Standby Command Switch Characteristics

A Catalyst 3550 standby command switch must meet these requirements:

- It is running Cisco IOS Release 12.1(4)EA1.
- It has an IP address.
- It has CDP version 2 enabled.
- It is connected to the command switch and all other standby command switches through the same VLAN.
- It is redundantly connected to the cluster so that connectivity to member switches is maintained.
- It is a member of the cluster.



Note When the command switch is a Catalyst 3550, all standby command switches must also be Catalyst 3550 switches.

Candidate and Member Switches Characteristics

Candidate switches are cluster-capable switches that have not yet been added to a cluster. Member switches are switches that have actually been added to a switch cluster. A candidate or member switch can have its own IP address, but it is not required. It can also have its own password.

To join a cluster, a candidate switch must meet these requirements:

- It is running cluster-capable software.
- It has CDP version 2 enabled.
- It is connected to the command switch through at least one common VLAN.
- It is connected to every standby command switch through at least one common VLAN. The VLAN to each standby command switch can be different.
- It is not a command or member switch of another cluster.



Note Catalyst 2950, Catalyst 3500 XL, Catalyst 2900 XL, Catalyst 1900, and Catalyst 2820 member switches must be connected through their management VLAN to the command switch and standby command switches.

Planning a Switch Cluster

Anticipating conflicts and compatibility issues is a high priority when you manage several switches through a cluster. This section describes these guidelines, requirements, and caveats that you should understand before you create the cluster:

- “Automatic Discovery of Cluster Candidates and Members” section on page 5-4
- “HSRP and Standby Command Switches” section on page 5-11
- “IP Addresses” section on page 5-13
- “Host Names” section on page 5-13
- “Passwords” section on page 5-14
- “SNMP Community Strings” section on page 5-14
- “Availability of Switch-Specific Features in Switch Clusters” section on page 5-14

**Note**

Refer to the release notes for the list of Catalyst switches enabled for switch clustering, including which ones can be command switches and which ones can only be member switches, and for the required software versions and browser and Java plug-in configurations.

Automatic Discovery of Cluster Candidates and Members

The command switch uses Cisco Discovery Protocol (CDP) to discover member switches, candidate switches, neighboring switch clusters, and edge devices across multiple VLANs and in star or cascaded topologies. By using CDP, a command switch can discover switches up to seven CDP hops away (the default is three hops) from the edge of the cluster. The edge of the cluster is where the last member switches are connected to the cluster (for example, the command switch and member switches 8, 9, and 10 in [Figure 5-1](#) are at the edge of the cluster).

You can set the number of hops the command switch searches for candidate and member switches by selecting **Cluster > Hop Count**. When new candidate switches are added to the network, the command switch discovers them and adds them to the list of candidate switches.

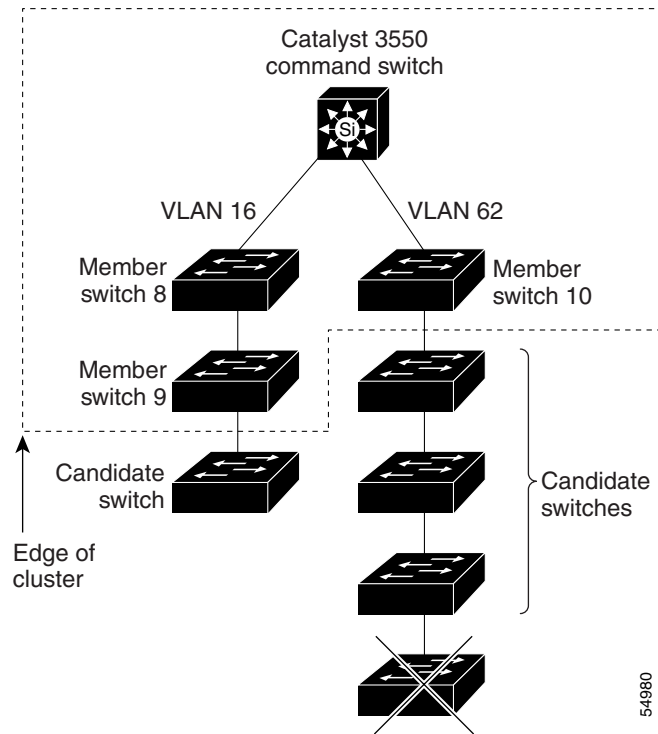
For more information about CDP, see [Chapter 12, “Configuring CDP.”](#)

**Note**

Do not disable CDP on the command switch, on cluster members, or on any cluster-capable switches that you might want a command switch to discover.

Figure 5-1 shows a switch cluster with candidate switches. The command switch has ports assigned to VLANs 16 and 62. The CDP hop count is three. The command switch discovers the candidate switch in VLAN 16 and the first three candidate switches in VLAN 62. Because the hop count is three, the command switch does not discover the fourth switch from the edge of the cluster.

Figure 5-1 Discovery through CDP Hops



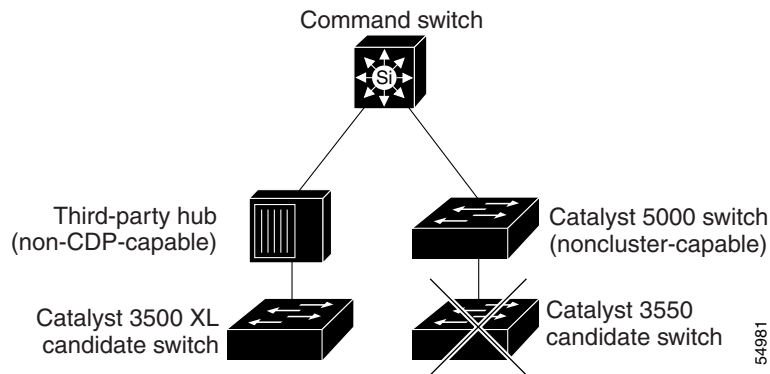
Connectivity Considerations for Automatic Discovery

Follow these connectivity guidelines to ensure automatic discovery of the switch cluster, cluster candidates, connected switch clusters, and neighboring edge devices:

- When an edge device that does not support CDP (such as a non-Cisco switch) is connected to the command switch, the command switch can discover the candidate and member switches that are attached to the edge device. However, if a Cisco switch that is not cluster-capable is connected to the command switch, the command switch is unable to discover cluster-enabled switches attached to the non-cluster-enabled switch.

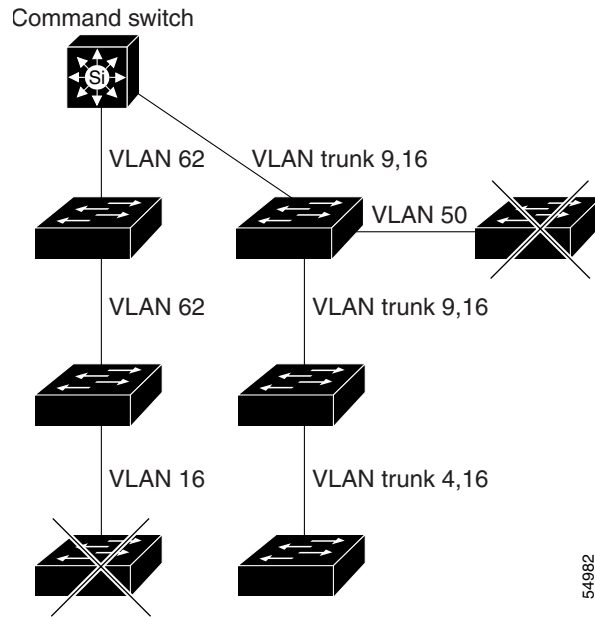
Figure 5-2 shows that the command switch discovers the Catalyst 3500 XL switch, which is connected to a third-party device. However, the command switch does not discover the Catalyst 3550 switch, which is connected to a Catalyst 5000 switch.

Figure 5-2 Discovery through Non-CDP-Capable and Non-Cluster-Capable Devices



- A cluster can have Catalyst 3550 member switches configured with different VLANs. However, each member switch must be connected through at least one VLAN in common with the command switch. The command switch in [Figure 5-3](#) has ports assigned to VLANs 9, 16, and 62 and therefore discovers the switches in those VLANs. It does not discover the switch in VLAN 50. It also does not discover the switch in VLAN 16 in the first column because the command switch has no VLAN connectivity to it. For more information about VLANs, see [Chapter 8, “Creating and Maintaining VLANs.”](#)

Figure 5-3 Discovery through Different VLANs



- We strongly recommend that a Catalyst 3550 switch be the command switch in a cluster that has Catalyst 2950, Catalyst 3500 XL, Catalyst 2900 XL, Catalyst 1900, and Catalyst 2820 member switches. These member switches must connect to the command switch through their management VLAN, which is VLAN 1 by default. The management VLANs of these member switches can be different. For information about management VLANs and switch clusters, refer to the software configuration guide of the specific switch.

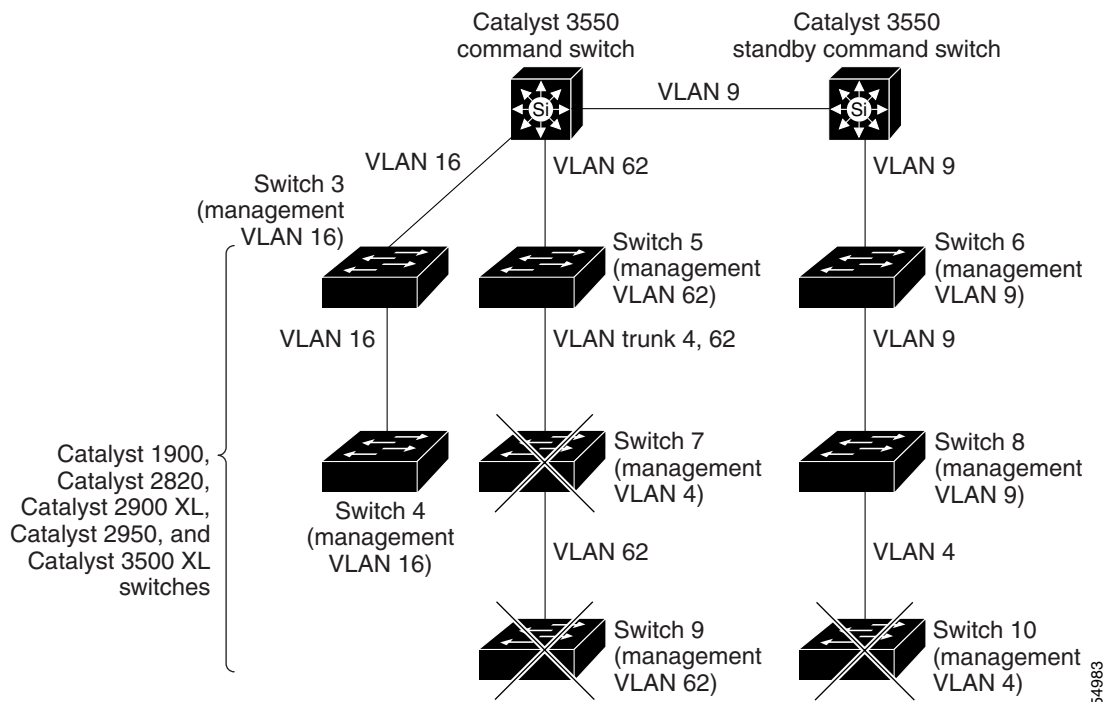
The command switch in [Figure 5-4](#) has ports assigned to VLANs 9, 16, and 62. It discovers all of the switches except for these switches:

- The switches in management VLAN 4
- The switch in VLAN 62 (switch 9) because automatic discovery does not extend beyond a non-candidate device (such as switch 7)

You can have a cluster that has a Catalyst 2950, Catalyst 3500 XL, or Catalyst 2900 XL command switch with Catalyst 3550 member switches. This type of cluster has these limitations:

- Catalyst 3550 member switches must be connected to the command-switch management VLAN.
- Catalyst 3550 member switches appear as unknown devices in the Topology view on CMS.

Figure 5-4 Discovery through Different Management VLANs



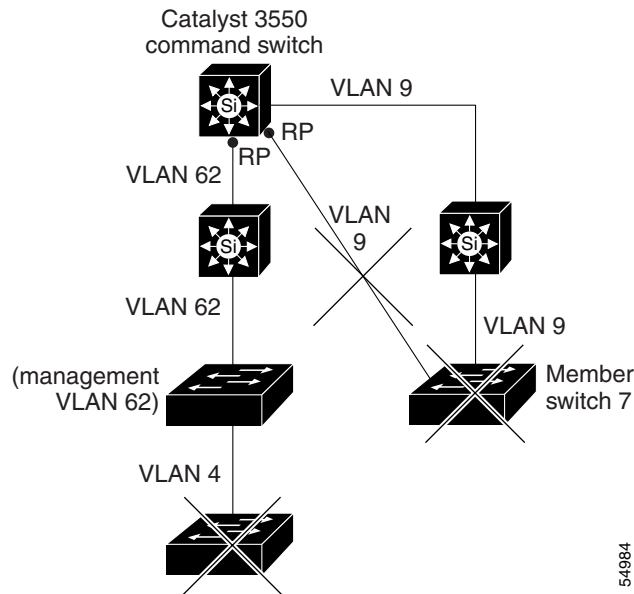
- If the command switch has a routed port (RP) configured, it discovers only candidate and member switches in the *same* VLAN as the routed port. For more information about routed ports, see the “Routed Ports” section on page 7-4.

**Note**

If there is a redundant path to a member switch, and one of the paths goes through a routed port, the command switch *always* uses the routed port path. Therefore, if the routed port path is lost, the command switch does not use the other redundant path and thus loses connectivity with the member switch. You can avoid this problem by not using a routed port in a redundant path to a cluster member.

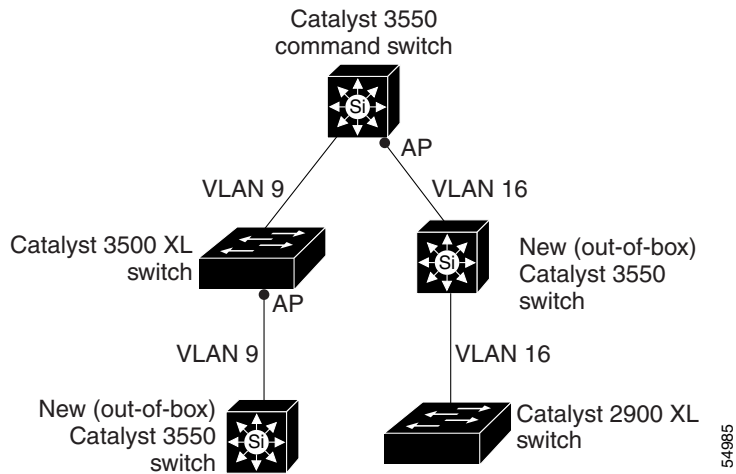
The command switch in [Figure 5-5](#) can discover the switches in VLANs 9 and 62 but not the switch in VLAN 4. If the routed port path between the command switch and member switch 7 is lost, connectivity with member switch 7 is lost, even if there is a redundant path to it through VLAN 9.

Figure 5-5 Discovery with Routed Ports



- When you add a brand new Catalyst 3550 switch to the cluster, it must be connected to the cluster through an access port (AP). The new switch automatically configures the access port to belong to the immediately upstream VLAN (see [Figure 5-6](#)). For more information about access ports, see the “Access Ports” section on page 7-2.

Figure 5-6 Discovery of Newly Installed Catalyst 3550 Switches



HSRP and Standby Command Switches

The switch supports Hot Standby Router Protocol (HSRP) so that you can configure a group of standby command switches. Because a command switch manages the forwarding of all communication and configuration information to all the member switches, we strongly recommend that you configure a cluster standby group to take over if the command switch fails.

A *cluster standby group* is a group of command-capable switches that meet the requirements described in the “[Standby Command Switch Characteristics](#)” section on page 5-3. Only one cluster standby group can be assigned per cluster.

**Note**

The cluster standby group is a HSRP group. Disabling HSRP disables the cluster standby group.

The switches in the cluster standby group are ranked according to HSRP priorities. The switch with the highest priority in the group is the *active command switch* (AC). The switch with the next highest priority is the *standby command switch* (SC). The other switches in the cluster standby group are the *passive command switches* (PC). For information about changing HSRP priority values, see the “[Configuring HSRP Priority](#)” section on page 21-6. The commands are the same for changing the priority of cluster standby group members and router-redundancy group members.

You need to assign a unique virtual IP address and group number and name to the cluster standby group. This information must be configured on a specific VLAN or routed port on the active command switch. The active command switch receives traffic destined for the virtual IP address. To manage the cluster, you must access the active command switch through the virtual IP address, not through the command-switch IP address.

If the active command switch fails, the standby command switch assumes ownership of the virtual IP address and becomes the active command switch. The passive switches in the cluster standby group compare their assigned priorities to determine the new standby command switch. The passive standby switch with the highest priority then becomes the standby command switch. When the previously active command switch becomes active again, it resumes its role as the active command switch, and the active command switch becomes the standby command switch.

Automatic Recovery of Cluster Configuration

To ensure that the standby command switch can take over the cluster immediately after the active command switch fails, the active command switch continually forwards cluster configuration information to the standby command switch.

**Note**

The active command switch forwards cluster configuration information to the standby switch but not device-configuration information.

When the previously active command switch resumes its active role again, it learns the latest cluster configuration from the active command switch, including members that were added while it was down.

**Note**

If the active command switch and the standby command switch become disabled *at the same time*, the passive command switch with the highest priority becomes the active command switch. However, cluster configuration is not forwarded, and you must rebuild the cluster.

Considerations for Cluster Standby Groups

In addition to providing a virtual IP address to the cluster standby group, these guidelines and requirements apply:

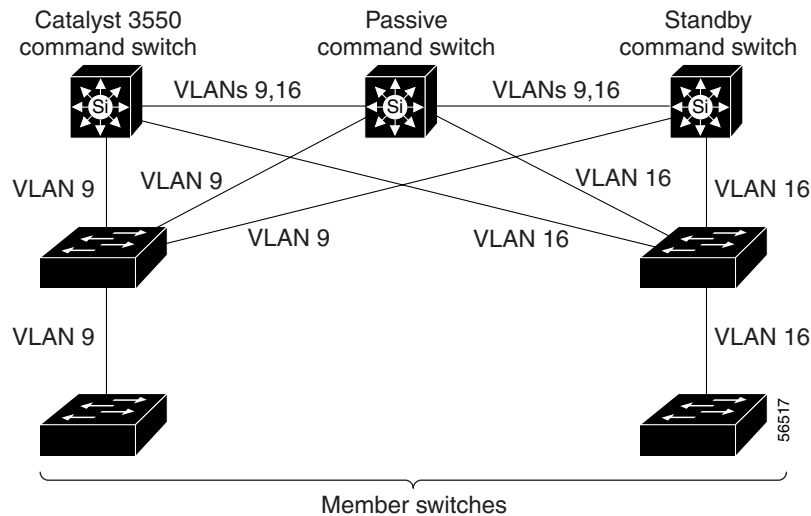
- In a cluster where the active command switch is a Catalyst 3550 switch, all standby-group members must also be Catalyst 3550 switches.
- All standby-group members must be members of the cluster.



Note There is no limit to the number of switches you can assign as standby command switches, but the total number of cluster members and standby-group members cannot be more than 16, including the active command switch.

- The active command switch must be connected to each standby-group member through the same VLAN. Each standby-group member must also be redundantly connected through at least one VLAN in common with the switch cluster. See [Figure 5-7](#).

Figure 5-7 VLAN Connectivity between Standby-Group Members and Cluster Members



- Catalyst 2950, Catalyst 3500 XL, Catalyst 2900 XL, Catalyst 1900, and Catalyst 2820 member switches must be connected to the cluster standby group through their management VLANs.
- Only one cluster standby group can be assigned to a cluster. You can have more than one router-redundancy standby group.

A HSRP group is both a cluster standby group and a router-redundancy group. For more information about HSRP and router redundancy, see [Chapter 21, “Configuring HSRP.”](#)

IP Addresses

You must assign IP information to a command switch. You can assign more than one IP address to the command switch, and you can access the cluster through any of the command-switch IP addresses. If you configure a cluster standby group, we recommend that you use the standby-group virtual IP address to manage the cluster from the active command switch. Using the virtual IP address ensures that you retain connectivity to the cluster if the active command switch fails and that a standby command switch becomes the active command switch.

If the active command switch fails and the standby command switch takes over, you must either use the standby-group virtual IP address to access the cluster or any of the IP addresses available on the new active command switch.

You can assign an IP address to a cluster-capable switch, but it is not necessary. A member switch is managed and communicates with other member switches through the command switch IP address. If the member switch leaves the cluster and it does not have its own IP address, you then must assign IP information to it to manage it as a standalone switch.

**Note**

Changing the command switch IP address ends your CMS session on the switch. Restart your CMS session by entering the new IP address in the browser **Location** field (Netscape Communicator) or **Address** field (Internet Explorer), as described in the release notes.

For more information about IP addresses, see [Chapter 4, “Assigning the Switch IP Address and Default Gateway.”](#)

Host Names

You do not need to assign a host name to either a command switch or an eligible cluster member. However, a host name assigned to the command switch can help to more easily identify the switch cluster. The default host name for the switch is *Switch*.

If a switch joins a cluster and it does not have a host name, the command switch appends a unique member number to its own host name and assigns it sequentially as each switch joins the cluster. The number means the order in which the switch was added to the cluster. For example, a command switch named *eng-cluster* could name the fifth cluster member *eng-cluster-5*.

If a switch has a host name, it retains that name when it joins a cluster. It retains that host name even after it leaves the cluster.

If a switch received its host name from the command switch, was removed from cluster, was then added to a new cluster, and kept the same member number (such as 5), the old host name (such as *eng-cluster-5*) is overwritten with the host name of the command switch in the new cluster (such as *mkg-cluster-5*). If the switch member number changes in the new cluster (such as 3), the switch retains the previous name (*eng-cluster-5*).

Passwords

It is not necessary to assign passwords to an individual switch if it will be a cluster member. When a switch joins a cluster, it inherits the command-switch password and retains it when it leaves the cluster. If no command-switch password is configured, the member switch inherits a null password. Member switches only inherit the command-switch password. If you change the member switch password and save the change, the switch is not manageable by the command switch until you change the member switch password to match the command switch password or until you reboot the member switch. We recommend that you do not change the member-switch password after it joins a cluster.

For more information about passwords, see the [“Preventing Unauthorized Access to Your Switch” section on page 6-1](#).

For password considerations specific to the Catalyst 1900 and Catalyst 2820 switches, refer to the installation and configuration guides specific to those switches.

SNMP Community Strings

A member switch inherits the command-switch first read-only (RO) and read-write (RW) community strings with *@esN* appended to the community strings:

- *commander-readonly-community-string@esN*, where *N* is the member-switch number.
- *commander-readwrite-community-string@esN*, where *N* is the member-switch number.

If the command switch has multiple read-only or read-write community strings, only the first read-only and read-write strings are propagated to the member switch.

The switches support an unlimited number of community strings and string lengths. For more information about configuring community strings, see the [“SNMP Community Strings” section on page 16-3](#). For complete information about SNMP, see [Chapter 16, “Configuring SNMP”](#).

For SNMP considerations specific to the Catalyst 1900 and Catalyst 2820 switches, refer to the installation and configuration guides specific to those switches.

Availability of Switch-Specific Features in Switch Clusters

When a switch has features specific to it and the switch is part of a switch cluster, the CMS menu bars display the configuration options of those features. For example, **Device > LRE Profile** appears in the menu bar when at least one Catalyst 2900 LRE XL switch is in the cluster.

Creating a Switch Cluster

Using CMS to create a cluster is easier than using the CLI commands. This section provides information about enabling a command switch, adding member switches and cluster standby group members, and verifying the cluster. This section assumes you have already cabled the switches, as described in the switch hardware installation guide, and followed the guidelines described in the “[Planning a Switch Cluster](#)” section on page 5-4.



Note

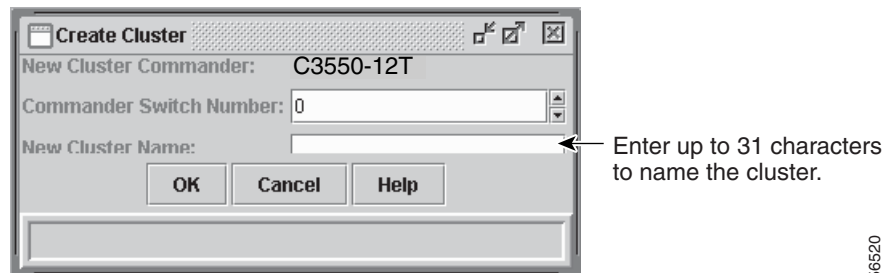
Refer to the release notes for the list of Catalyst switches enabled for switch clustering, including which ones can be command switches and which ones can only be member switches, and for the required software versions and browser and Java plug-in configurations.

Enabling a Command Switch

The switch you designate to be the command switch must meet the requirements described in the “[Command Switch Characteristics](#)” section on page 5-2, “[Planning a Switch Cluster](#)” section on page 5-4, and the release notes. You can enable a command switch, name the cluster, and assign an IP address and a password to the command switch when you run the setup program during initial switch setup. For information about using the setup program, refer to the release notes.

If you did not enable a command switch during initial switch setup, launch Device Manager (also referred to as Switch Manager) from a command-capable switch, and select **Cluster > Create Cluster**. Enter a cluster number (the default is 0), and use up to 31 characters to name the cluster ([Figure 5-8](#)).

Figure 5-8 Create Cluster Window



56520

Adding Members Switches

As explained in the [“Automatic Discovery of Cluster Candidates and Members”](#) section on page 5-4, the command switch automatically discovers candidate switches. When you add new cluster-capable switches to the network, the command switch discovers and adds them to a list of candidate switches. To display an updated cluster candidates list from the Add to Cluster window ([Figure 5-9](#)), either relaunch CMS and redisplay this window, or follow these steps:

1. Close the Add to Cluster window.
2. Select **View > Refresh**.
3. Select **Cluster > Add to Cluster** to redisplay the Add to Cluster window.

There are two ways to add switches to a cluster:

- Select **Cluster > Add to Cluster**, and select a candidate switch from the list. To add more than one candidate switch, press **Ctrl**, and make your choices, or press **Shift**, and choose the first and last switch in a range.
- Display the Topology view, right-click a candidate-switch icon, and select **Add to Cluster** ([Figure 5-10](#)). In the Topology view, candidate switches are cyan, and member switches are green. To add more than one candidate switch, press **Ctrl**, and left-click the candidates you want to add.

You can select one or more switches as long as the total number of switches in the cluster does not exceed 16 (this includes the command switch). When a cluster reaches the maximum of 16 members, the **Add to Cluster** option is not available for that cluster. In this case, you must remove a member switch before adding a new one.

If a password has been configured on the candidate switch, you are prompted to enter it and your username. If multiple candidate switches have the same password, you can add them at the same time. If you incorrectly enter a password or if you enter a password when one was not configured on the candidate switch, the candidate switch is not added. If any candidate switch cannot be added to the cluster, CMS displays a message stating which candidates were not added and why.

When a candidate switch joins a cluster, it inherits the command-switch password. For more information about setting passwords, see the [“Passwords”](#) section on page 5-14.

Figure 5-9 Add to Cluster Window

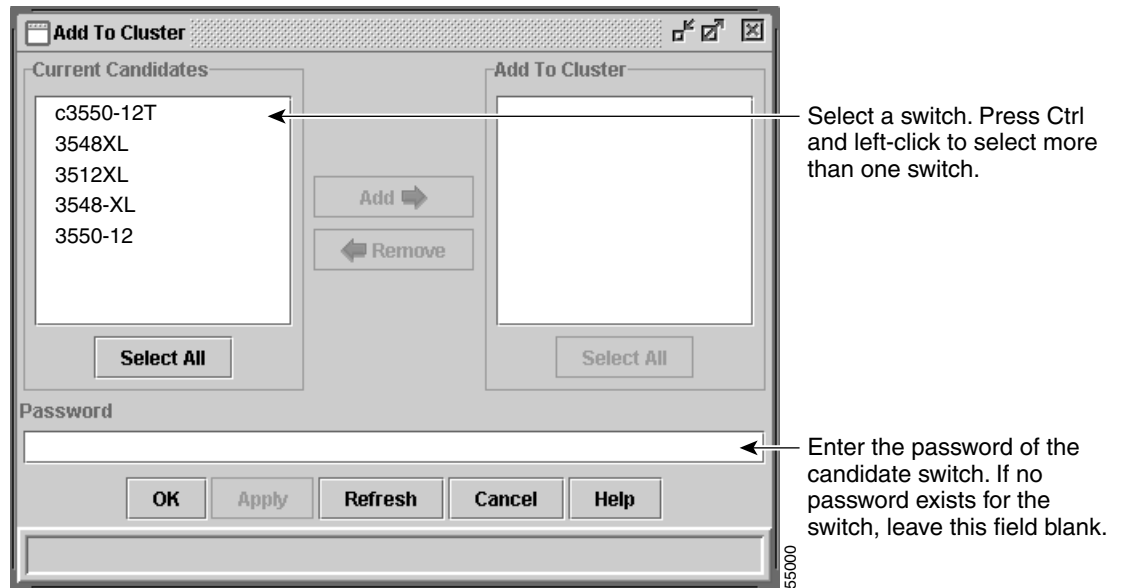
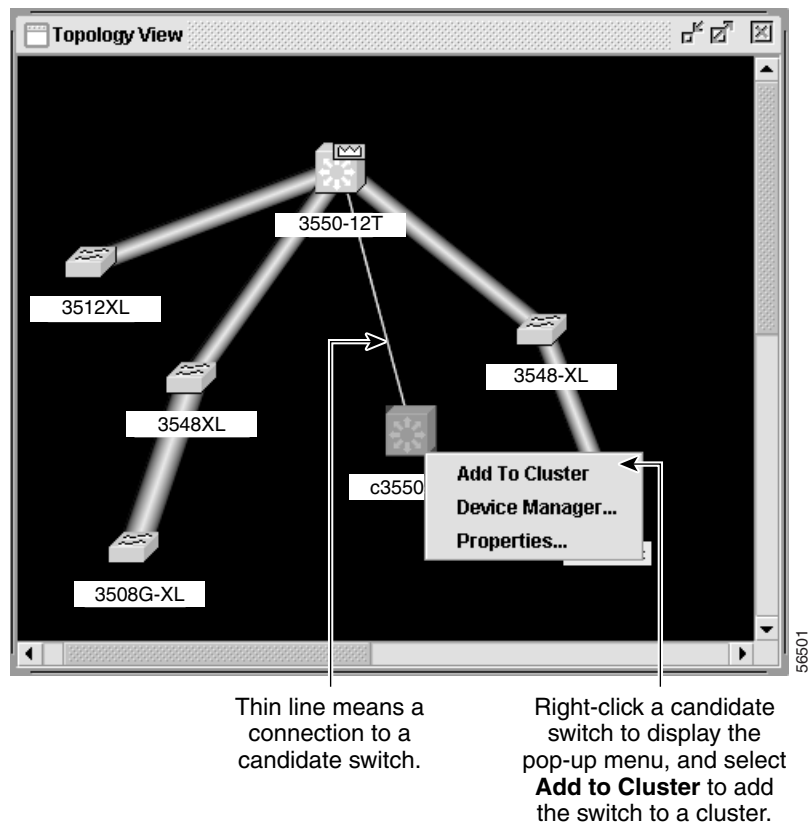


Figure 5-10 Using the Topology View to Add Member Switches



Creating a Cluster Standby Group

The cluster standby group members must meet the requirements described in the “[Standby Command Switch Characteristics](#)” section on page 5-3 and the “[HSRP and Standby Command Switches](#)” section on page 5-11. To create a cluster standby group, select **Cluster > Standby Commanders** (Figure 5-11).

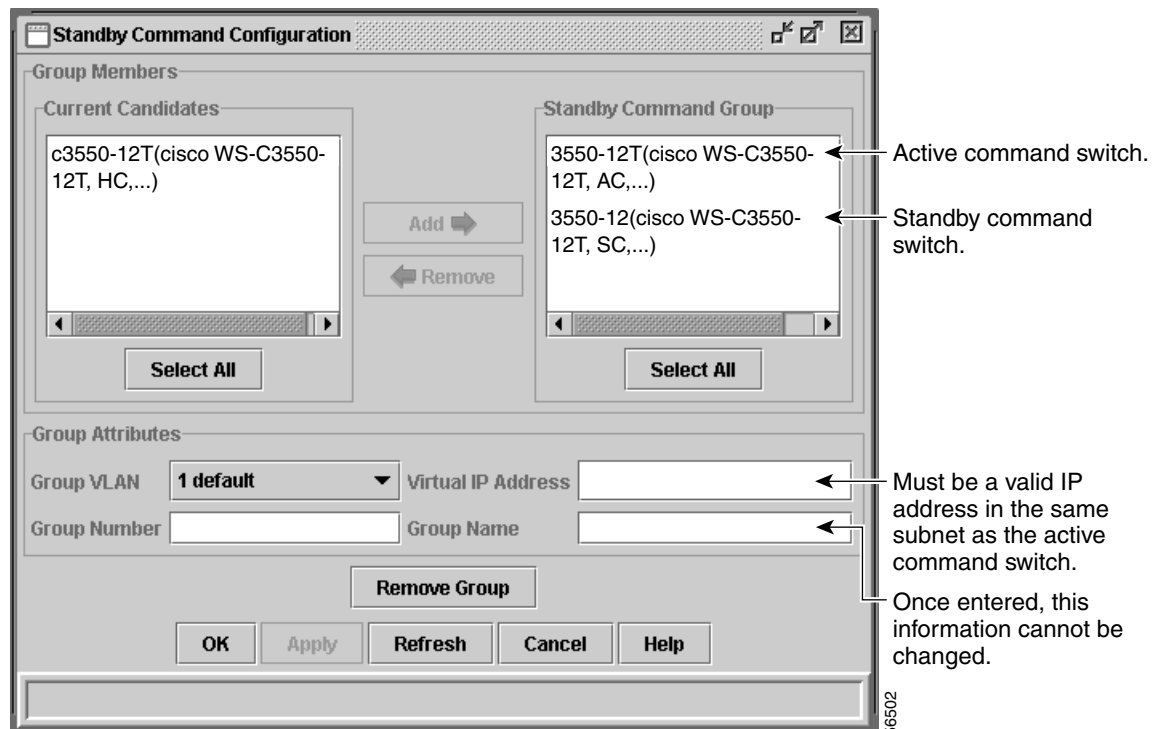
These abbreviations are appended to the switch host names in the Standby Command Group list to show their status in the cluster standby group:

- AC—Active command switch
- SC—Standby command switch
- PC—Member of the cluster standby group but not the standby command switch
- HC—Candidate switch that can be added to the cluster standby group
- CC—Command switch when HSRP is disabled

You must enter a virtual IP address for the cluster standby group. This address must be in the same subnet as the IP addresses of the switch. The group number must be unique within the IP subnet. It can be from 0 to 255, and the default is 0. The group name can have up to 32 characters.

The Standby Command Configuration window uses the default values for the **preempt** and **name** commands that you have set by using the CLI. If you use this window to create the HSRP group, all switches in the group have the **preempt** command enabled. You must also provide a name for the group.

Figure 5-11 Standby Command Configuration Window



Verifying a Switch Cluster

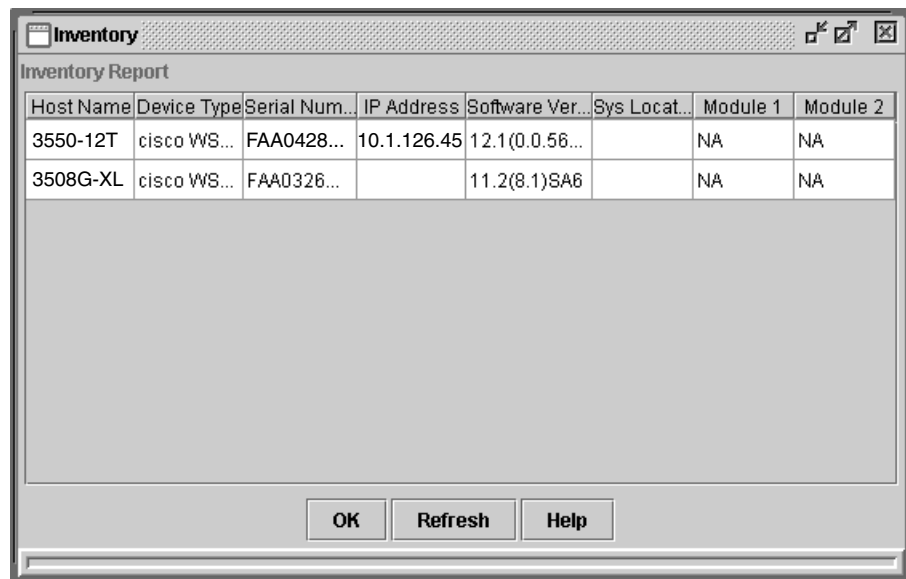
When you finish adding cluster members, follow these steps to verify the cluster:

- Step 1** Enter the command switch IP address in the browser **Location** field (Netscape Communicator) or **Address** field (Microsoft Internet Explorer) to access all switches in the cluster.
- Step 2** Enter the command-switch password.
- Step 3** Select **View > Topology** to display the topology of the switch cluster and view link information (Figure 3-7 on page 3-10). For complete information about the Topology view, including descriptions of the icons, links, and colors used in the Topology view, see the “Topology View” section on page 3-9.
- Step 4** Select **Reports > Inventory** to display an inventory of the switches in the cluster (Figure 5-12).

The summary includes information such as switch model numbers, serial numbers, software versions, IP information, and location.

You can also display port and switch statistics from **Reports > Port Statistics** and **Port > Port Settings > Runtime Status**.

Figure 5-12 Inventory Window



Host Name	Device Type	Serial Num...	IP Address	Software Ver...	Sys Locat...	Module 1	Module 2
3550-12T	cisco WS...	FAA0428...	10.1.126.45	12.1(0.0.56...		NA	NA
3508G-XL	cisco WS...	FAA0326...		11.2(8.1)SA6		NA	NA

If you lose connectivity with a member switch or if a command switch fails, see the “[Recovery Procedures](#)” section on page 25-1.

For more information about creating and managing clusters, refer to the online help. For information about the cluster commands, refer to the *Catalyst 3550 Multilayer Switch Command Reference*.

Using the CLI to Manage Switch Clusters

You can configure member switches from the CLI by first logging into the command switch. Enter the **rcommand** user EXEC command and the member switch number to start a Telnet session (through a console or Telnet connection) and to access the member switch CLI. After this, the command mode changes and the IOS commands operate as usual. Enter the **exit** privileged EXEC command on the member switch to return to the command-switch CLI.

This example shows how to log into member-switch 3 from the command-switch CLI:

```
switch# rcommand 3
```

If you do not know the member-switch number, enter the **show cluster members** user EXEC command on the command switch. For more information about the **rcommand** command and all other cluster commands, refer to the *Catalyst 3550 Multilayer Switch Command Reference*.

The Telnet session accesses the member-switch CLI at the same privilege level as on the command switch. The IOS commands then operate as usual. For instructions on configuring the switch for a Telnet session, see the [“Setting a Telnet Password for a Terminal Line” section on page 6-5](#).

Catalyst 1900 and Catalyst 2820 CLI Considerations

For Catalyst 1900 and Catalyst 2820 switches running standard edition software, the Telnet session accesses the management console (a menu-driven interface) if the command switch is at privilege level 15. If the command switch is at privilege level 14, you are prompted for the password before being able to access the menu console.

Command-switch privilege levels map to the Catalyst 1900 and Catalyst 2820 member switches running standard and Enterprise Edition Software as follows:

- If the command-switch privilege level is 1 to 14, the member switch is accessed at privilege level 1.
- If the command-switch privilege level is 15, the member switch is accessed at privilege level 15.

**Note**

The Catalyst 1900 and Catalyst 2820 CLI is available only on switches running Enterprise Edition Software.

For more information about the Catalyst 1900 and Catalyst 2820 switches, refer to the installation and configuration guides for those switches.

Using SNMP to Manage Switch Clusters

When you first power on the switch, SNMP is enabled if you enter the IP information by using the setup program and accept its proposed configuration. If you did not use the setup program to enter the IP information and SNMP was not enabled, you can enable it as described in the “[Configuring SNMP](#)” section on page 16-4. On Catalyst 1900 and Catalyst 2820 switches, SNMP is enabled by default.

When you create a cluster, the command switch manages the exchange of messages between member switches and an SNMP application. The Cluster Management software appends the member switch number ($@esN$, where N is the switch number) to the first configured RW and RO community strings on the command switch and propagates them to the member switch. The command switch uses this community string to control the forwarding of gets, sets, and get-next messages between the SNMP management station and the member switches.



Note

When a cluster standby group is configured, the command switch can change without your knowledge. Use the first read-write and read-only community strings to communicate with the command switch if there is a cluster standby group configured for the cluster.

If the member switch does not have an IP address, the command switch passes traps from the member switch to the management station, as shown in [Figure 5-13](#). If a member switch has its own IP address and community strings, they can be used in addition to the access provided by the command switch. For more information, see the “[SNMP Community Strings](#)” section on page 5-14 and [Chapter 16](#), “[Configuring SNMP](#).”

Figure 5-13 SNMP Management for a Cluster

