CHAPTER 5

Clustering Switches

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

- Switch cluster overview
- Planning a switch cluster
- Creating a switch cluster
- Verifying a switch cluster
- Using the command-line interface (CLI) to manage switch clusters
- Using Simple Network Management Protocol (SNMP) to manage switch clusters

Configuring switch clusters is more easily done from the Cluster Management Suite (CMS) web-based interface than through the CLI. Therefore, information in this chapter focuses on using CMS. See Chapter 2, "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 2900 Series XL and Catalyst 3500 Series XL 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 the required software versions and browser and Java plug-in configurations.

Understanding Switch Clusters

A switch cluster is a group of connected Catalyst desktop switches that are managed as a single entity. The switches can be in the same location, or they can be distributed across a contiguous Layer 2 network. All communication with cluster switches is through one IP address.

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. It identifies and controls all member switches in a cluster, regardless of where they are located and how they are connected. You can designate one or more switches as *standby command switches* to avoid losing contact with cluster members if the command switch fails.

The following sections list the requirements for the following cluster members:

- Command switch
- Standby command switches
- Candidate and member switches

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 the required software versions.

Command Switch Characteristics

The command switch must meet the following requirements:

- It is running Cisco IOS Release 12.0(5)XP or later.
- 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.
- It belongs to the same management VLAN as the cluster member switches.
- No access lists have been defined for the switch because access lists can restrict access to a switch. Access lists are not usually used in configuring the Catalyst 2900 XL and Catalyst 3500 XL switches, except for the access class 199 that is created when a device is configured as the command switch.

Standby Command Switch Characteristics

You can assign one or more switches to a standby group of command switches. There is no limit to the number of switches you assign to a standby group. To be eligible for a standby group, a switch must meet the following requirements:

- It is running Cisco IOS Release 12.0(5)XP or later.
- It has its own IP address.
- It has CDP version 2 enabled.
- It is not a command or member switch of another cluster.
- It is in the same management VLAN as the active command switch.
- It is a member of the cluster.

For redundancy, we also recommend that each standby command switch is cabled so that connectivity to cluster members is maintained.

Candidate and Cluster Member 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 enable or enable secret password.

Note Before adding a candidate switch to the cluster, you must know its enable or enable secret password.

To join a cluster, a switch must meet the following requirements:

- It is running cluster-capable software.
- It has CDP version 2 enabled.
- It is connected to a command switch through ports that belong to the same management VLAN (see the "Management VLAN" section on page 5-11).
- It is not an active member or the command switch of another cluster.

Planning a Switch Cluster

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

Refer to the release notes for software compatibility considerations and requirements on cluster-capable switches.

Automatic Discovery of Cluster Candidates

The switch uses Cisco Discovery Protocol (CDP) to discover and display candidate switches that can be added to a cluster. By using CDP, a switch can automatically discover switches in star or cascaded topologies that are up to three cluster-enabled devices away from the edge of the cluster. You can configure the command switch to discover switches up to seven cluster-enabled devices away. The default is three hops. To set the number of hops the command switch searches for candidate and member switches, or to disable the automatic display of suggested candidates, select **Cluster > User Settings**.

Note Do not disable CDP. CDP must be enabled for the switch to discover and display the switch cluster and connected switch clusters, cluster candidates, and neighboring edge devices.

When an edge device that does not support CDP is connected to the command switch, CDP can still discover the candidate switches that are attached to it. When a switch that does support CDP but does not support clustering is connected to the command switch, the cluster is unable to discover candidates that are attached to that switch. For example, Cluster Builder cannot create a cluster that includes candidates that are connected to a Catalyst 5000 series or Catalyst 6000 switch connected to the command switch. For more information about CDP, see the "Configuring CDP" section on page 6-22.

Standby Command Switches

Because a command switch manages the forwarding of all communication and configuration information to all the cluster members, we strongly recommend that you configure a standby command switch to take over if the command switch fails. We also recommend redundant cabling from the standby command switch to the switch cluster.

IOS Release 12.0(5)XU and higher supports a version of the Hot Standby Router Protocol (HSRP) so that you can configure a *standby group* of command switches. A standby group is a group of switches that meet the requirements described in the "Standby Command Switch Characteristics" section on page 5-3.

Note Catalyst 2900 XL and Catalyst 3500 XL switches running releases earlier than IOS Release 12.0(5)XU can belong to clusters supported by standby command switches, but they cannot belong to a standby group.

The standby group of command switches are ranked according to a set of user-defined priorities. Switches are ranked first by the number of links they have and second by the switch speed. If switches have the same number of links and speed, they are listed alphabetically. The member switch with the highest priority in the group is the *standby command switch*. The standby group is *bound* to the switch cluster so that the standby command switch becomes active if the primary command switch fails.

You assign a unique virtual IP address to the standby group. The primary command switch receives member traffic destined for the virtual IP address. To manage the standby group, you must access the primary command switch through the virtual IP address, not through the command-switch IP address. If HSRP is enabled and you use the command-switch IP address, you will be prompted a second time for a password when you move between Cluster Builder and VSM.

Figure 5-1 shows a group of switches with a standby command switch.

Figure 5-1 A Cluster with a Standby Command Switch

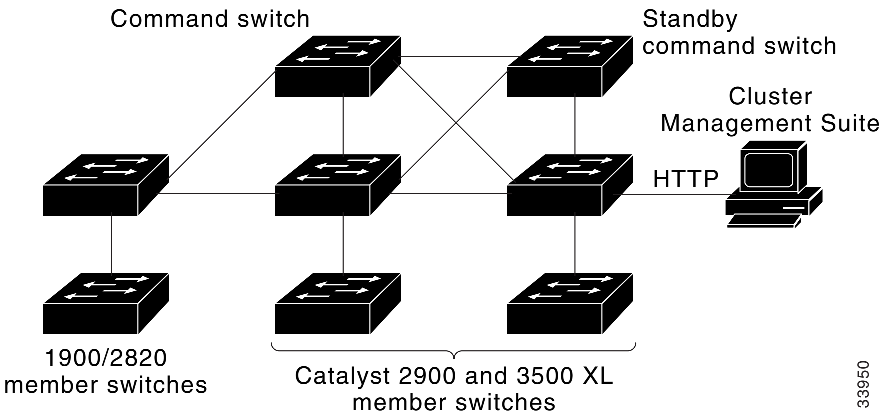
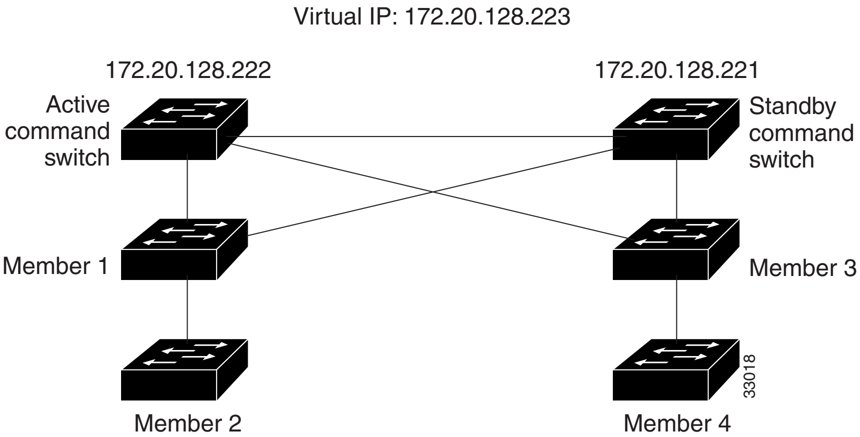


Figure 5-2 shows a network cabled to allow the standby switch to maintain management contact with the member switches if the cluster command switch fails. Spanning Tree Protocol (STP) prevents the loops in such a configuration from reducing performance.

Figure 5-2 Redundant Cabling to Support HSRP



To ensure that the standby command switch can take over the cluster if the primary command switch fails, the primary command switch continually forwards cluster configuration information to the standby command switch.

Note The command switch forwards cluster configuration information to the standby switch but not device-configuration information. The standby command switch is informed of new cluster members but not the configuration of any given switch.

If the primary command switch fails, the standby command switch assumes ownership of the virtual IP address and MAC address and begins acting as the command switch. The remaining switches in the standby group compare their assigned priorities to determine the new standby command switch.

When the primary command switch becomes active again, the command switch resumes its role as the active command switch. An automatic recovery procedure adds cluster members that were added to the cluster while the primary command switch was down.

To configure an HSRP standby command group, see the "Designating and Enabling Standby Command Switches" section on page 5-17.

IP Addresses

Clustering switches conserves IP addresses if you have a limited number of them. If you plan to create switch clusters, you must assign IP information to a command switch. Through the command-switch IP address, you can manage and monitor up to 16 switches.

When a switch joins a cluster, it is managed and communicates with other member switches through the command-switch IP address. You can assign an IP address to the candidate or member switch, but it is not necessary. When a member switch has its own IP address, it remains manageable if it leaves the cluster and becomes a standalone switch.

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

You can assign IP information by using the setup program (refer to the release notes) or by manually assigning it (see the "Changing IP Information" section on page 6-2).

Passwords

If you plan to create switch clusters, you should assign an enable secret password to the command switch. You can assign a privilege level (1 to 15) to the password, where level 15, the default, provides the highest level of security. An enable secret password with privilege level 15 is required to access to the switch or switch cluster through CMS and TACACS+ authentication. You can assign this password by using the setup program (refer to the release notes) or by manually assigning it (see the "Changing the Password" section on page 6-15).

It is not necessary to assign passwords to an individual switch if it will be a cluster member. If a candidate switch has a password, you must enter that password to add the switch to the cluster. When the switch joins the 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.

If you change the member-switch password, it 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.

Note Copies of the CMS pages you display are saved in your browser memory cache until you exit the browser session. A password is not required to redisplay these pages, including the Cisco Systems Access page. You can access the CLI by clicking **Web Console - HTML access to the command line interface** from a cached copy of the Cisco Systems Access page. To prevent unauthorized access to CMS and the CLI, exit your browser to end the browser session.

If a Catalyst 1900 or Catalyst 2820 switch joins the cluster, its passwords and privilege levels are altered. Keep in mind the following caveats if your cluster has Catalyst 1900 and Catalyst 2820 member switches:

- Password length
  - If the command-switch enable password is longer than eight characters, the member-switch enable password is truncated to eight characters.
  - If the command-switch enable password is between one and eight characters inclusive, the member-switch enable password is the same as the command switch password. (Though the password length for Catalyst 1900 and Catalyst 2820 switches is from four to eight characters, the length is only checked when the password is configured from the menu console or with the CLI.)
  - Both the command switch and member switch support up to 25 characters (52 characters encrypted) in the enable secret password.
- Privilege level

  The command switch supports up to 15 privilege levels. Catalyst 1900 and Catalyst 2820 member switches support only levels 1 and 15.
  - Command-switch privilege levels 1 to 14 map to level 1 on the member switch.
  - Command-switch privilege level 15 maps to level 15 on the member switch.

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 any Catalyst 2900 XL and Catalyst 3500 XL 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 indicates the member number of the switch. For example, a command switch named *eng-cluster* could name cluster member number 5, *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 the cluster, and was then was added to a new cluster, its old host name (such as *eng-cluster-5*) is overwritten with the host name of the command switch in the new cluster.

SNMP Community Strings

The Cluster Management software appends the member switch number (*@esN*, where *N* is the switch number) to the first configured RO and RW community strings on the command switch and propagates them to the member switch:

- *commander-readonly-community-string@esN*
- *commander-readwrite-community-string@esN*

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 Catalyst 2900 XL and Catalyst 3500 XL switches support an unlimited number of community strings and string lengths.

The Catalyst 1900 and Catalyst 2820 switches support up to four read-only and four read-write community strings; each string contains up to 32 characters. When these switches join the cluster, the first read-only and read-write community string on the command switch is propagated and overwrites the fourth read-only and read-write community string on the member switches. To support the

32-character string-length limitation on the Catalyst 1900 and Catalyst 2820 switches, the command-switch community strings are truncated to 27 characters when propagating them to these switches, and the @*esN* (where *N* refers to the member switch number and can be up to two digits) is appended to them.

For more information about configuring community strings through Cluster Manager, see the "Configuring SNMP" section on page 6-18. For more information about using SNMP to manage clusters, see the "Using SNMP to Manage Switch Clusters" section on page 5-22.

Management VLAN

Communication with the switch management interfaces is through the switch IP address. The IP address is associated with the management VLAN, which by default is VLAN 1. To manage switches in a cluster, the port connections among the command, member, and candidate switches must be connected through ports that belong to the management VLAN.

Any VLAN can serve as the management VLAN as long as there are links between the command switch and the member switches for both the old and the new management VLAN. When you change the management VLAN on an existing cluster, the command switch synchronizes activities with member switches to ensure that no loss of management connectivity occurs.

Note Activity synchronization is only valid for IOS Release 12.0(5)XU and higher. Previous releases of the software require that switches be upgraded one at a time.

If your cluster includes members that are running a software release earlier than Cisco IOS Release 12.0(5)XP, you cannot change the management VLAN of the cluster. If your cluster includes member switches that are running Cisco IOS Release 12.0(5)XP, those members need to have the VLAN changed before using the Management VLAN window.

⚠

Caution You can change the management VLAN through a console connection without interrupting the console connection. However, changing the management VLAN ends your CMS session. Restart your CMS session by entering the new IP address in the browser **Location** field (Netscape Communicator) or **Address** field (Microsoft Internet Explorer), as described in the release notes.

To change the management VLAN on an existing cluster, see the "Changing the Management VLAN for a New Switch" section on page 8-5.

If you add a new switch to an existing cluster and the cluster is using a management VLAN other than the default VLAN 1, the command switch automatically senses that the new switch has a different management VLAN and has not been configured. The command switch issues commands to change the management VLAN on the new switch to match the one in use by the cluster. This automatic change of the VLAN only occurs for new, out-of-box switches that do not have a config.text file and for which there have been no changes to the running configuration.

Network Port

A network port cannot link cluster members. For more information about the network port, see the "Enabling a Network Port" section on page 7-7.

NAT Commands

When a cluster is created, Network Address Translation (NAT) commands are added to the configuration file of the command switch. Do not remove these commands.

LRE Profiles

A configuration conflict occurs if a switch cluster has LRE switches using both private and public profiles. If one LRE switch in a cluster is assigned a public profile, all LRE switches in that cluster must have that same public profile. Before you add an LRE switch to a cluster, make sure that you assign it the same public profile used by other LRE switches in the cluster.

A cluster can have a mix of LRE switches using different private profiles.

For more information about LRE port profiles, see the "Configuring the LRE Ports" section on page 7-22.

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 Cluster Manager menu bar when at least one Catalyst 2900 LRE XL switch is in the cluster. However, these options are only available when the appropriate switch is selected from the Host Name drop-down list.

Creating a Switch Cluster

You create a cluster by performing these tasks:

1. Cabling together switches running clustering software
2. Assigning basic information to one switch (the command switch)
3. Starting VSM to designate and enable a command switch
4. Starting Cluster Builder to add candidate and standby command switches to the cluster

After the cluster is formed, you can access all switches in the cluster by entering the IP address of the command switch into the browser **Location** field (Netscape Communicator) or **Address** field (Microsoft Internet Explorer).

This section provides procedures for enabling a command switch and building a cluster. For procedures on connecting switches together, refer to the switch hardware installation guide. For procedures on assigning basic information to the command switch, refer to the release notes.

Designating and Enabling a Command Switch

Before you enable a switch as a command switch, refer to the release notes for command-switch requirements. To enable a command switch, display VSM, select **Cluster > Cluster Command Configuration**, and in the Command Switch Status field, select **Enable**. You can use up to 31 characters to name your cluster.

After enabling a command switch, select **Cluster > Cluster Builder** to begin building your cluster.

Adding and Removing Cluster Members

Each time you launch CMS, it displays the Suggested Candidates window (Figure 5-3) and prompts you to create a cluster by adding qualified candidates. This window lists the cluster candidates discovered by the switch. The Suggested Candidate window lists each candidate switch with its device type, MAC address, and the switch through which it is connected to the cluster. By default, the suggested candidates are highlighted in the Suggested Candidates window, but you can select 1 or more switches as long as the number of switches selected does not exceed 16. This window does not appear after the number of switches in the cluster reaches the maximum of 16. Only candidates that you accept are added to the cluster.

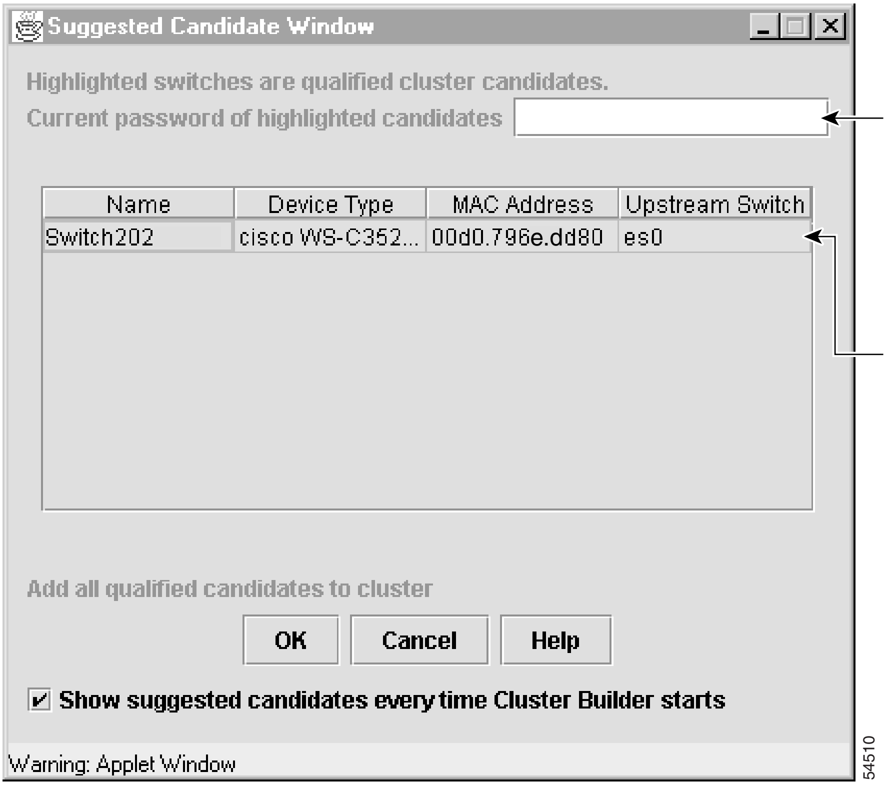
When you add new cluster-eligible switches to the network, CMS discovers those new switches and the next time you launch Cluster Builder, it prompts you with an updated Suggested Candidates window.

Note The Suggested Candidates window displays prequalified candidates whether or not they are in the same management VLAN as the command switch. If you enter the password for a candidate in a different management VLAN than the cluster and click **OK**, this switch is not added to the cluster. It appears as a candidate switch in Cluster Builder. For information about how to change the management VLAN, see the "Management VLAN" section on page 5-11.

From the Cluster Builder topology, you can also add a candidate switch to a cluster. Display Cluster Builder, right-click the candidate icon, and from the pop-up menu, select **Add to Cluster** (Figure 5-4). Cluster members have green labels, and candidates have blue labels. You can add a switch to a cluster if the cluster has no more than 16 members; otherwise, you must remove a member before adding a new one. The Add to Cluster option is disabled when the number of cluster members reaches 16.

To add several switches to a cluster, press **Ctrl**, and left-click the candidates you want to add. If any of the candidates cannot be added, Cluster Builder displays a message that states which candidates were not added and why.

Figure 5-3 Suggested Candidate Window



Suggested Candidate Window

Highlighted switches are qualified cluster candidates.

Current password of highlighted candidates

Name	Device Type	MAC Address	Upstream Switch
Switch202	cisco WS-C352...	00d0.796e.dd80	es0

Add all qualified candidates to cluster

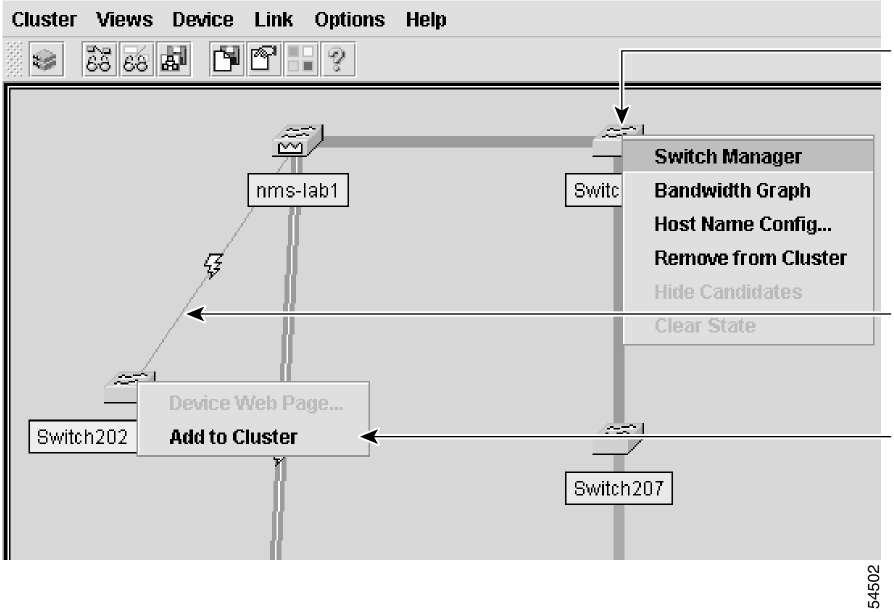
☑ Show suggested candidates every time Cluster Builder starts

Warning: Applet Window

Enter the password of the candidate switch. If no password exists for the switch, leave this field blank for the switch to join the cluster.

Candidate switch information.

Figure 5-4 Cluster Builder



Right-click a member switch to display the device pop-up menu, and select an option to display the Switch Manager, display switch information, or remove the switch from the cluster.

Thin line indicates a connection to a candidate switch.

Right-click a candidate switch to display the device pop-up menu, and select **Add to Cluster** to add the switch to a cluster.

If a password has been configured on the candidate switch, you are prompted to enter it and your username. You can add multiple candidates at the same time if they have the same password. If you enter a password that does not match the password defined for the candidate or if you enter a password for a candidate that does not have a password, the candidate is not added to the cluster. In all cases, once a candidate switch joins a cluster, it inherits the command-switch password.

To remove a member switch, right-click it, and from the pop-up menu, select **Remove from Cluster**. The switch retains its configured password when it leaves the cluster. For more information about setting passwords, see the "Passwords" section on page 5-8.

If the candidate is in a different management VLAN than the command switch, a message states that this candidate is unreachable, and you will not be able to add it to the cluster. For more information about management VLAN considerations, see the "Management VLAN" section on page 5-11.

For information about how to remove Catalyst 1900 or Catalyst 2820 member switches, refer to the *Catalyst 1900 Series Installation and Configuration Guide* or the *Catalyst 2820 Series Installation and Configuration Guide*.

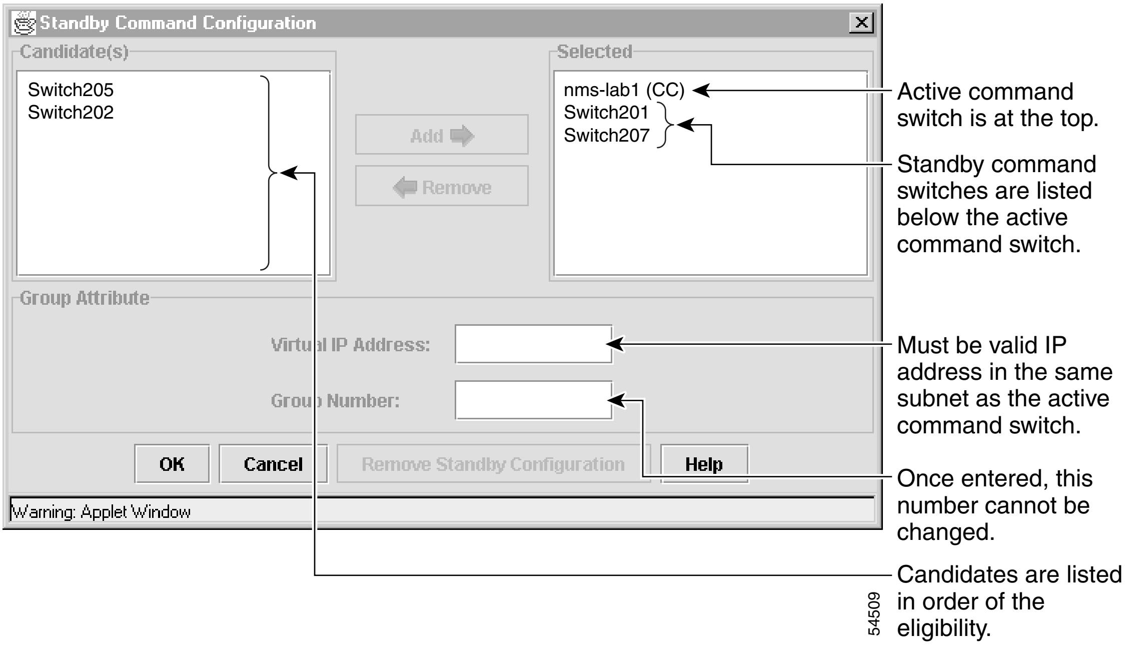
Designating and Enabling Standby Command Switches

To create a standby group, display Cluster Manager, and select **Cluster > Standby Command Configuration** to display the Standby Command Configuration window (Figure 5-5).

Eligible switches are listed in the Candidates list according to an eligibility ranking. Candidate switches are ranked first by the number of links they have and second by the switch speed. If the switches have the same number of links and speed, they are listed alphabetically.

In the Selected list, the active command switch has the highest priority and is always at the top of the list. The standby switch with the next highest priority becomes the standby command switch. The standby command switch is listed after the active command switch, followed by the other standby switches according to their priority. The last switch has the lowest priority. If the primary command switch fails, the standby command switch becomes the primary command switch. The standby switch with the next highest priority then becomes the standby command switch.

Figure 5-5 Standby Command Configuration



Active command switch is at the top.

Standby command switches are listed below the active command switch.

Must be valid IP address in the same subnet as the active command switch.

Once entered, this number cannot be changed.

Candidates are listed in order of the eligibility.

The following abbreviations are appended to the switch host names in the Selected list to show their status in the standby group:

- AC—Active command switch
- SC—Standby command switch
- PC—Member of the standby group but not the standby command switch
- CC—Command switch when HSRP is disabled

The virtual IP address must be in the same subnet as the IP addresses of the switches, and the group number must be unique within the IP subnet. It can be from 0 to 255, and the default is 0.

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, and the name for the group is *clustername_standby.*

Verifying a Switch Cluster

You can display the switch cluster you have built by

- Displaying an inventory of the switches in the cluster.
- Displaying the topology of the switch cluster and viewing link information.

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

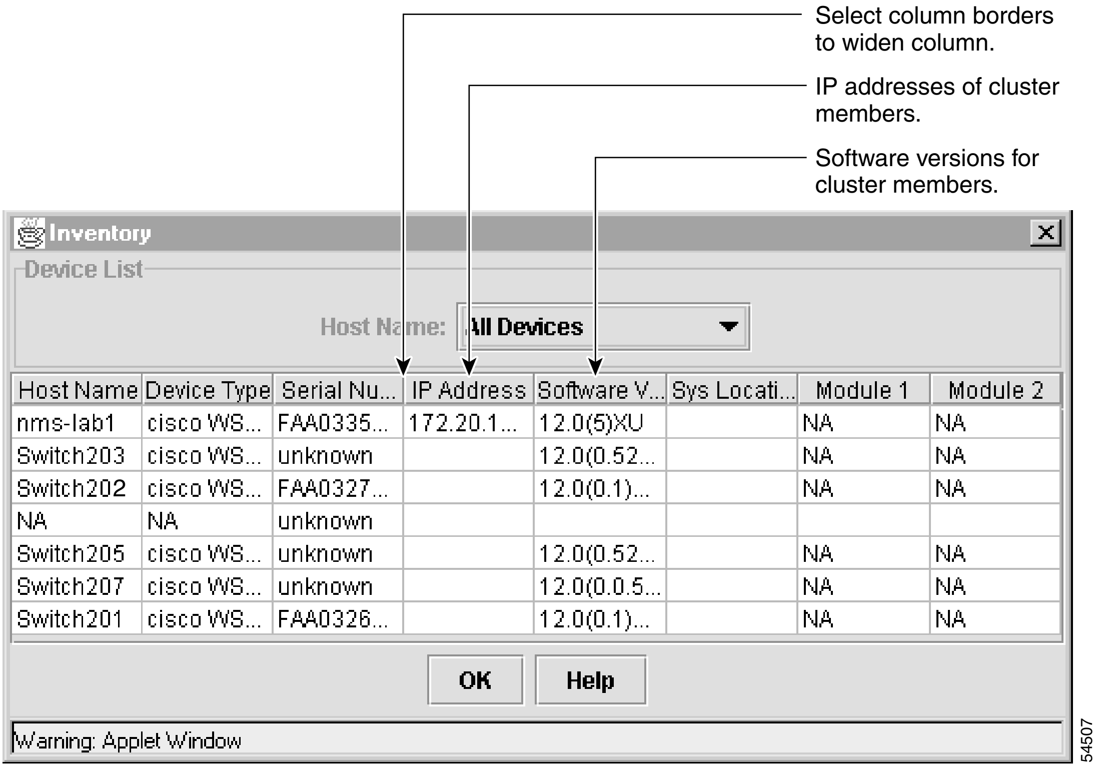
For information about troubleshooting switch clusters, see Chapter 9, "Troubleshooting."

Displaying an Inventory of the Clustered Switches

To display an inventory of the switch cluster, display VSM or Cluster Manager, and select **System > Inventory** to display the Inventory window (Figure 5-6). To display this information for a single switch, select the switch image, right-click it, and select **System > Inventory**.

The inventory summary of the cluster members includes information such as switch model numbers, serial numbers, software versions, IP information, location, and any installed modules.

Figure 5-6 Inventory



Select column borders to widen column.

IP addresses of cluster members.

Software versions for cluster members.

Host Name	Device Type	Serial Nu...	IP Address	Software V...	Sys Locati...	Module 1	Module 2
nms-lab1	cisco WS...	FAA0335...	172.20.1...	12.0(5)XU		NA	NA
Switch203	cisco WS...	unknown		12.0(0.52...		NA	NA
Switch202	cisco WS...	FAA0327...		12.0(0.1)...		NA	NA
NA	NA	unknown					
Switch205	cisco WS...	unknown		12.0(0.52...		NA	NA
Switch207	cisco WS...	unknown		12.0(0.0.5...		NA	NA
Switch201	cisco WS...	FAA0326...		12.0(0.1)...		NA	NA

Warning: Applet Window

Displaying Link Information

You can see how the cluster members are interconnected from Cluster Builder. It shows how the switches are connected and the type of connection between each device. To display a legend describing the icons, links, and colors used in Cluster Builder, select **Help > Legend**. To display port-connection information such as port numbers for each end of the link, select **Views > Toggle Labels**.

Using the CLI to Manage Switch Clusters

You can configure member switches from the CLI by first logging in to 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 IOS commands operate as usual. Enter the **exit** privileged EXEC command on the member switch to return to the command-switch CLI. For more information about the rcommand command, refer to the *Catalyst 2900 Series XL and Catalyst 3500 Series XL Command Reference*.

The following 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 Catalyst 2900 XL and Catalyst 3500 XL switches, 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 Catalyst 2900 XL or Catalyst 3500 XL switch for a Telnet session, see the "Accessing the CLI" section on page 3-8.

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.

Using SNMP to Manage Switch Clusters

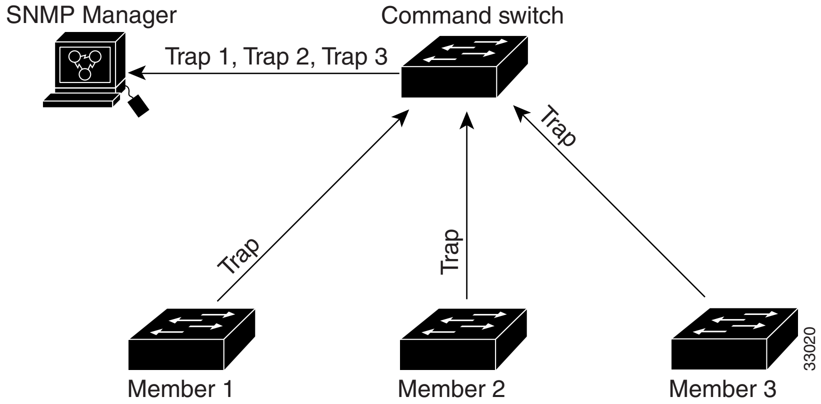
You must enable SNMP for the Cluster Management reporting and graphing features to function properly. When you first power on the switch, SNMP is enabled if you enter the IP information by using the setup program and accept its proposed configuration. If you did not use the setup program to enter the IP information and SNMP was not enabled, you can enable it on the SNMP Configuration page described in the "Configuring SNMP" section on page 6-18. 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 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 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 5-7. 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 5-10 and the "Configuring SNMP" section on page 6-18.

Figure 5-7 SNMP Management for a Cluster


SNMP Manager
Command switch
Trap 1, Trap 2, Trap 3
Trap
Trap
Trap
Member 1
Member 2
Member 3
33020