C H A P T E R 6

Clustering Switches

This chapter provides the concepts and procedures to create and manage Catalyst 3750 switch clusters. Unless otherwise noted, the term *switch* refers to a standalone switch and to a switch stack.

> **Note** This chapter focuses on Catalyst 3750 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.

This chapter consists of these sections:

> **Note** 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 about using CMS to configure switch clusters, refer to the online help. For the CLI cluster commands, refer to the switch command reference.

Understanding Switch Clusters

A *switch cluster* is a set of up to 16 connected, cluster-capable Catalyst switches that are managed as a single entity. The switches in the cluster use the switch clustering technology so that you can configure and troubleshoot a group of different Catalyst desktop switch platforms through a single IP address.

In a switch cluster, 1 switch must be the *cluster command switch* and up to 15 other switches can be *cluster member switches*. The total number of switches in a cluster cannot exceed 16 switches. The cluster command switch is the single point of access used to configure, manage, and monitor the cluster 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 locations. The switches can be in the same location, or they can be distributed across a Layer 2 or Layer 3 (if your cluster is using a Catalyst 3550 or Catalyst 3750 switch as a Layer 3 router between the Layer 2 switches in the cluster) network.

    Cluster members are connected to the cluster command switch according to the connectivity guidelines described in the "Automatic Discovery of Cluster Candidates and Members" section on page 6-5. This section includes management VLAN considerations for the Catalyst 1900, Catalyst 2820, Catalyst 2900 XL, Catalyst 2950, and Catalyst 3500 XL switches. For complete information about these switches in a switch-cluster environment, refer to the software configuration guide for that specific switch.

- Command-switch redundancy if a cluster command switch fails. One or more switches can be designated as *standby cluster command switches* to avoid loss of contact with cluster members. A *cluster standby group* is a group of standby cluster 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 cluster command switch IP address.

Note A switch cluster is different from a *switch stack*. A switch stack is a set of Catalyst 3750 switches connected through their stack ports. For more information about how switch stacks differ from switch clusters, see the "Switch Clusters and Switch Stacks" section on page 6-15.

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

These sections describe:

- Cluster Command Switch Characteristics, page 6-3
- Standby Cluster Command Switch Characteristics, page 6-3
- Candidate Switch and Cluster Member Switch Characteristics, page 6-4

Cluster Command Switch Characteristics

A cluster command switch must meet these requirements:

- It is running Release 12.1(11)AX or later.
- It has an IP address.
- It has Cisco Discovery Protocol (CDP) version 2 enabled (the default).
- It is not a command or cluster member switch of another cluster.
- It is connected to the standby cluster command switches through the management VLAN and to the cluster member switches through a common VLAN.

Note We strongly recommend that the highest-end, command-capable switch in the cluster be the command switch. For example, if your switch cluster has a Catalyst 3750 switch or a Catalyst 3750 switch stack, it should be the cluster command switch.

Standby Cluster Command Switch Characteristics

A standby cluster command switch must meet these requirements:

- It is running Release 12.1(11)AX or later.
- It has an IP address.
- It has CDP version 2 enabled.
- It is connected to the command switch and to other standby command switches through its management VLAN.
- It is connected to all other cluster member switches (except the cluster command and standby command switches) through a common VLAN.
- It is redundantly connected to the cluster so that connectivity to cluster member switches is maintained.
- It is not a command or member switch of another cluster.

Note Standby cluster command switches must be the same type of switches as the cluster command switch. For example, if the cluster command switch is a Catalyst 3750 switch, the standby cluster command switches must also be Catalyst 3750 switches. Refer to the switch configuration guide of other cluster-capable switches for IOS release requirements on standby cluster command switches.

Candidate Switch and Cluster Member Switch Characteristics

Candidate switches are cluster-capable switches and switch stacks that have not yet been added to a cluster. Cluster member switches are switches and switch stacks that have actually been added to a switch cluster. Although not required, a candidate or cluster member switch can have its own IP address and password (for related considerations, see the "IP Addresses" section on page 6-14 and "Passwords" section on page 6-15).

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 not a command or cluster member switch of another cluster.
- If a cluster standby group exists, it is connected to every standby cluster command switch through at least one common VLAN. The VLAN to each standby cluster command switch can be different.
- It is connected to the cluster command switch through at least one common VLAN.

> **Note** Catalyst 1900, Catalyst 2820, Catalyst 2900 XL, Catalyst 2950, and Catalyst 3500 XL candidate and cluster member switches must be connected through their management VLAN to the cluster command switch and standby cluster command switches. For complete information about these switches in a switch-cluster environment, refer to the software configuration guide for that specific switch.
>
> This requirement does not apply if you have a Catalyst 3550 or Catalyst 3750 cluster command switch. Candidate and cluster member switches can connect through any VLAN in common with the cluster command switch.

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, page 6-5
- HSRP and Standby Cluster Command Switches, page 6-11
- IP Addresses, page 6-14
- Host Names, page 6-14
- Passwords, page 6-15
- SNMP Community Strings, page 6-15
- Switch Clusters and Switch Stacks, page 6-15
- TACACS+ and RADIUS, page 6-17
- Access Modes in CMS, page 6-17
- Availability of Switch-Specific Features in Switch Clusters, page 6-17

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

Automatic Discovery of Cluster Candidates and Members

The cluster command switch uses Cisco Discovery Protocol (CDP) to discover cluster member switches, candidate switches, neighboring switch clusters, and edge devices across multiple VLANs and in star or cascaded topologies.

Note Do not disable CDP on the cluster command switch, on cluster members, or on any cluster-capable switches that you might want a cluster command switch to discover. For more information about CDP, see Chapter 17, "Configuring CDP."

Following these connectivity guidelines ensures automatic discovery of the switch cluster, cluster candidates, connected switch clusters, and neighboring edge devices:

- Discovery Through CDP Hops, page 6-5
- Discovery Through Non-CDP-Capable and Noncluster-Capable Devices, page 6-6
- Discovery Through Different VLANs, page 6-7
- Discovery Through Different Management VLANs, page 6-8
- Discovery Through Routed Ports, page 6-9
- Discovery of Newly Installed Switches, page 6-10

Discovery Through CDP Hops

By using CDP, a cluster 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 cluster member switches are connected to the cluster and to candidate switches. For example, cluster member switches 9 and 10 in Figure 6-1 are at the edge of the cluster.

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

Note A switch stack in a cluster equates to a single cluster member switch. There is a restriction specific to adding cluster members through CMS. For more information, see the "Switch Clusters and Switch Stacks" section on page 6-15.

In Figure 6-1, the cluster command switch has ports assigned to VLANs 16 and 62. The CDP hop count is three. The cluster command switch discovers switches 11, 12, 13, and 14 because they are within three hops from the edge of the cluster. It does not discover switch 15 because it is four hops from the edge of the cluster.

*Figure 6-1   Discovery Through CDP Hops*
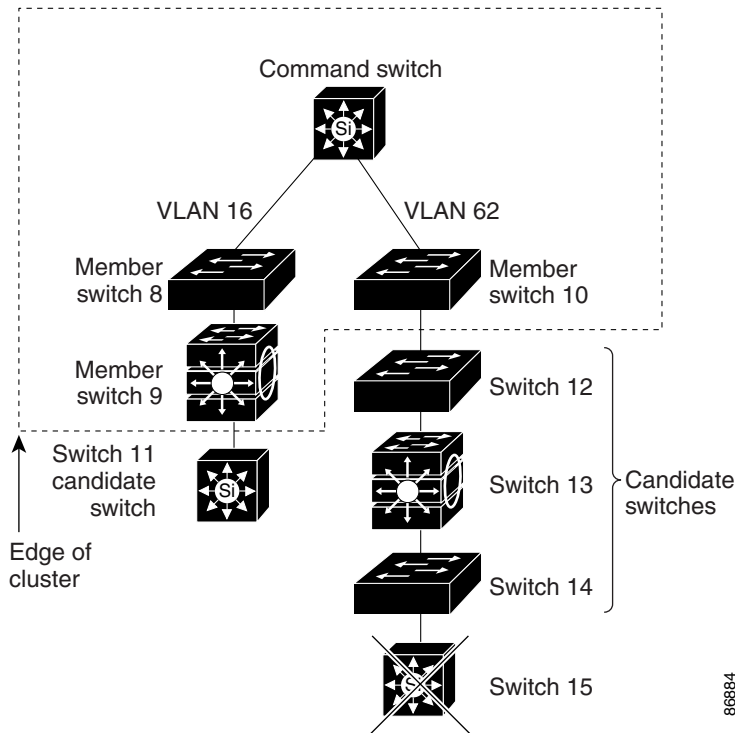
Discovery Through Non-CDP-Capable and Noncluster-Capable Devices

If a cluster command switch is connected to a *non-CDP-capable third-party hub* (such as a non-Cisco hub), it can discover cluster-enabled devices connected to that third-party hub. However, if the cluster command switch is connected to a *noncluster-capable Cisco device*, it cannot discover a cluster-enabled device connected beyond the noncluster-capable Cisco device.

Figure 6-2 shows that the cluster command switch discovers the switch that is connected to a third-party hub. However, the cluster command switch does not discover the switch that is connected to a Catalyst 5000 switch.

Figure 6-2   Discovery Through Non-CDP-Capable and Noncluster-Capable Devices
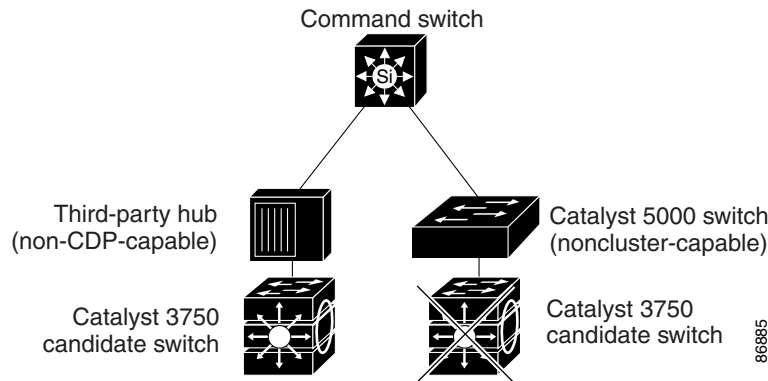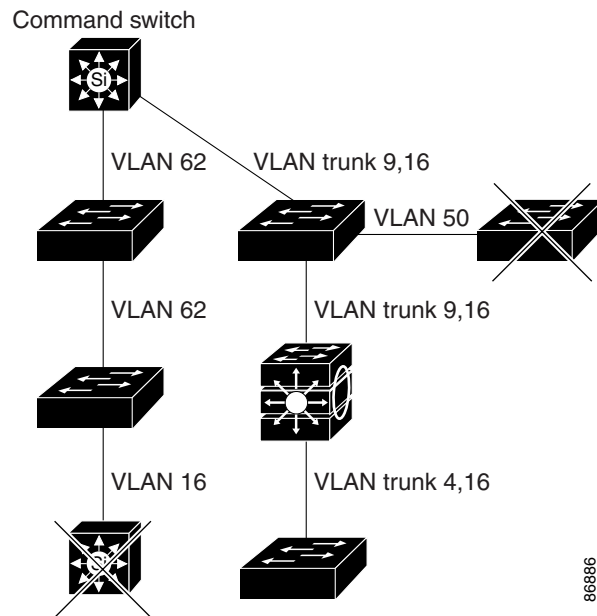
Discovery Through Different VLANs

If the cluster command switch is a Catalyst 3550 or Catalyst 3750 switch, the cluster can have cluster member switches in different VLANs. As cluster member switches, they must be connected through at least one VLAN in common with the cluster command switch. The cluster command switch in Figure 6-3 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 cluster command switch has no VLAN connectivity to it.

Catalyst 2900 XL, Catalyst 2950, and Catalyst 3500 XL cluster member switches must be connected to the cluster command switch through their management VLAN. For information about discovery through management VLANs, the "Discovery Through Different Management VLANs" section on page 6-8. For more information about VLANs, see Chapter 10, "Configuring VLANs."

Note   For additional considerations about VLANs in switch stacks, see the "Switch Clusters and Switch Stacks" section on page 6-15.

*Figure 6-3*   *Discovery Through Different VLANs*

Discovery Through Different Management VLANs

We recommend using Catalyst 3550 or Catalyst 3750 cluster command switches. These cluster command switches can discover and manage cluster member switches in different VLANs and different management VLANs. As cluster member switches, they must be connected through at least one VLAN in common with the cluster command switch. They do not need to be connected to the cluster command switch through their management VLAN. The default management VLAN is VLAN 1.

The cluster command switch and standby command switch in Figure 6-4 have ports assigned to VLANs 9, 16, and 62. The management VLAN on the cluster command switch is VLAN 9. Each cluster command switch discovers the switches in the different management VLANs except these:

- Switches 7 and 10 (switches in management VLAN 4) because they are not connected through a common VLAN (meaning VLANs 62 and 9) with the cluster command switch

- Switch 9 because automatic discovery does not extend beyond a noncandidate device, which is switch 7

Figure 6-4   Discovery Through Different Management VLANs with a Layer 3 Cluster Command Switch
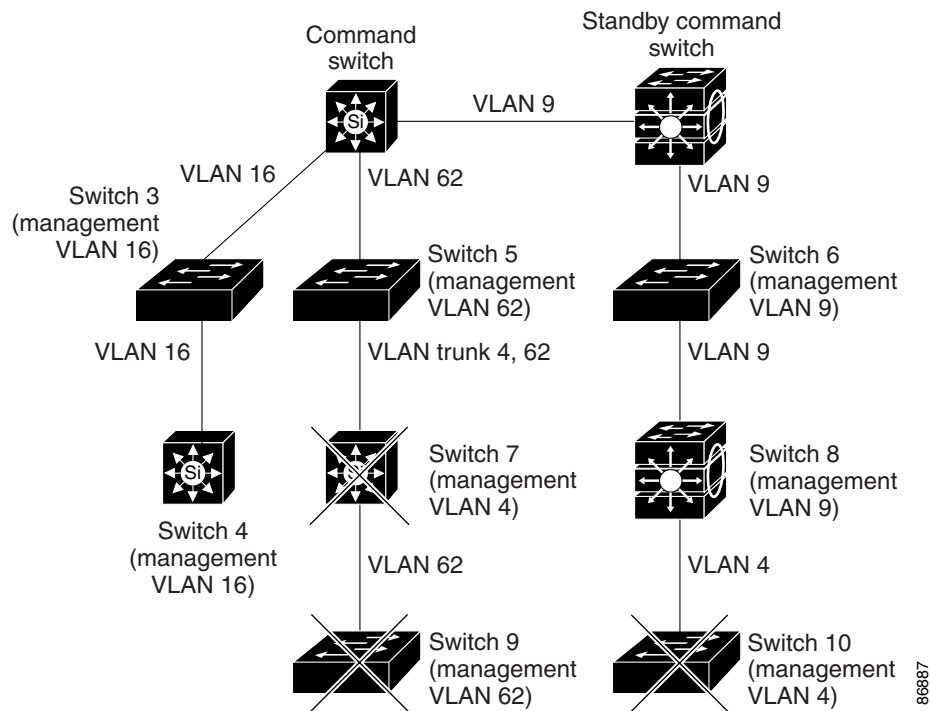
Discovery Through Routed Ports

If the cluster command switch has a routed port (RP) configured, it discovers only candidate and cluster member switches in the *same* VLAN as the routed port. For more information about routed ports, see the "Routed Ports" section on page 9-3.

The cluster command switch in Figure 6-5 can discover the switches in VLANs 9 and 62 but not the switch in VLAN 4. If the routed port path between the cluster command switch and cluster member switch 7 is lost, connectivity with cluster member switch 7 is maintained because of the redundant path through VLAN 9.

Figure 6-5   Discovery Through Routed Ports
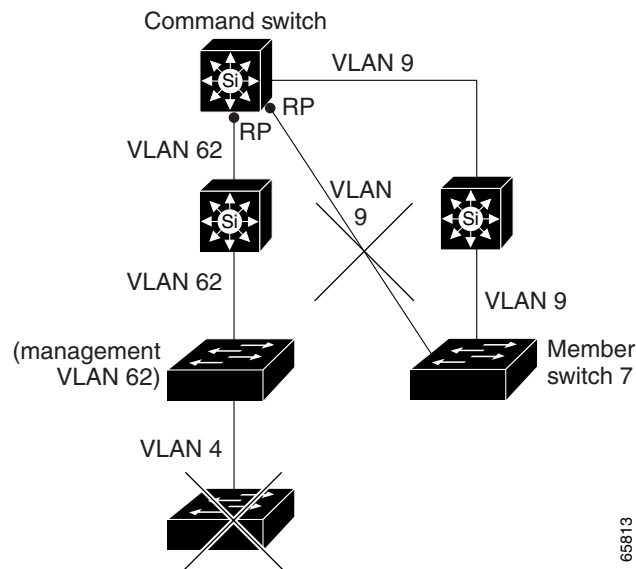
Discovery of Newly Installed Switches

To join a cluster, the new, out-of-the-box switch must be connected to the cluster through one of its access ports. An access port (AP) carries the traffic of and belongs to only one VLAN. By default, the new switch and its access ports are assigned to VLAN 1.

When the new switch joins a cluster, its default VLAN changes to the VLAN of the immediately upstream neighbor. The new switch also configures its access port to belong to the VLAN of the immediately upstream neighbor.

The cluster command switch in Figure 6-6 belongs to VLANs 9 and 16. When new cluster-capable switches join the cluster:

- One cluster-capable switch and its access port are assigned to VLAN 9.

- The other cluster-capable switch and its access port are assigned to management VLAN 16.

Figure 6-6   Discovery of Newly Installed Switches
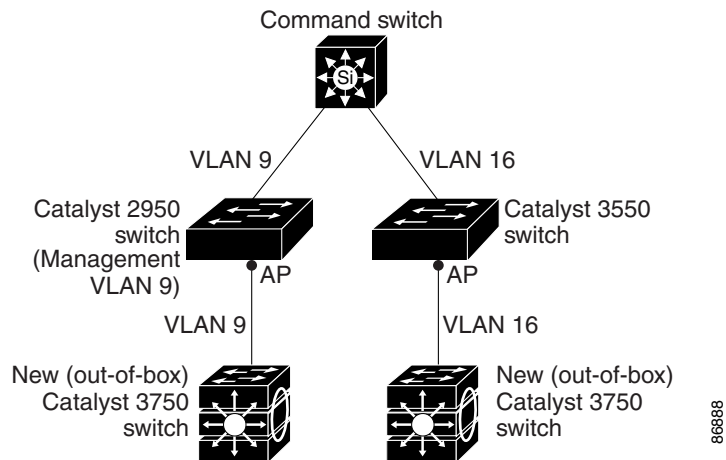
HSRP and Standby Cluster Command Switches

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

- For a cluster command switch stack, a standby cluster command switch is necessary if the entire switch stack fails. However, if only the stack master in the command switch stack fails, the switch stack elects a new stack master and resumes its role as the cluster command switch stack.

- For a cluster command switch that is a standalone switch, configure a standby cluster command switch to take over if the primary cluster command switch fails.

A *cluster standby group* is a group of command-capable switches that meet the requirements described in the "Standby Cluster Command Switch Characteristics" section on page 6-3. Only one cluster standby group can be assigned per cluster.

> **Note** We strongly recommend that the highest-end, command-capable switch in the cluster be the command switch. If your switch cluster has a Catalyst 3750 switch or a Catalyst 3750 switch stack, it should be the cluster command switch.

> **Note** The cluster standby group is an 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 cluster command switch* (AC). The switch with the next highest priority is the *standby cluster command switch* (SC). The other switches in the cluster standby group are the *passive cluster command switches* (PC). If the active cluster command switch and the standby cluster command switch become disabled *at the same time*, the passive cluster command switch with the highest priority becomes the active cluster command switch. For the limitations to automatic discovery, see the "Automatic Recovery of Cluster Configuration" section on page 6-13. For information about changing HSRP priority values, see the "Configuring HSRP Priority" section on page 27-6. The HSRP **standby priority** interface configuration commands are the same for changing the priority of cluster standby group members and router-redundancy group members.

> **Note** The HSRP standby hold time interval should be greater than or equal to three times the hello time interval. The default HSRP standby hold time interval is 10 seconds. The default HSRP standby hello time interval is 3 seconds. For more information about the standby hold time and standby hello time intervals, see the "Configuring HSRP Authentication and Timers" section on page 27-8.

These connectivity guidelines ensure automatic discovery of the switch cluster, cluster candidates, connected switch clusters, and neighboring edge devices. These topics also provide more detail about standby cluster command switches:

- Virtual IP Addresses, page 6-12
- Other Considerations for Cluster Standby Groups, page 6-12
- Automatic Recovery of Cluster Configuration, page 6-13

Virtual IP Addresses

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 cluster command switch. The active cluster command switch receives traffic destined for the virtual IP address. To manage the cluster, you must access the active cluster command switch through the virtual IP address, not through the command-switch IP address. This is in case the IP address of the active cluster command switch is different from the virtual IP address of the cluster standby group.

If the active cluster command switch fails, the standby cluster command switch assumes ownership of the virtual IP address and becomes the active cluster command switch. The passive switches in the cluster standby group compare their assigned priorities to determine the new standby cluster command switch. The passive standby switch with the highest priority then becomes the standby cluster command switch. When the previously active cluster command switch becomes active again, it resumes its role as the active cluster command switch, and the current active cluster command switch becomes the standby cluster command switch again. For more information about IP address in switch clusters, see the "IP Addresses" section on page 6-14.

Other Considerations for Cluster Standby Groups

Note For additional considerations about cluster standby groups in switch stacks, see the "Switch Clusters and Switch Stacks" section on page 6-15.

These requirements also apply:

- Standby cluster command switches must be the same type of switches as the cluster command switch. For example, if the cluster command switch is a Catalyst 3750 switch, the standby cluster command switches must also be Catalyst 3750 switches. Refer to the switch configuration guide of other cluster-capable switches for IOS release requirements on standby cluster command switches.

  We strongly recommend that the highest-end, command-capable switch in the cluster be the command switch. If your switch cluster has a Catalyst 3750 switch or a Catalyst 3750 switch stack, it should be the cluster command switch.

- Only one cluster standby group can be assigned to a cluster. You can have more than one router-redundancy standby group.

  An HSRP group can be both a cluster standby group and a router-redundancy group. However, if a router-redundancy group becomes a cluster standby group, router redundancy becomes disabled on that group. You can reenable it by using the CLI. For more information about HSRP and router redundancy, see Chapter 27, "Configuring HSRP."

- All standby-group members must be members of the cluster.

  Note There is no limit to the number of switches that you can assign as standby cluster command switches. However, the total number of switches in the cluster—which would include the active cluster command switch, standby-group members, and cluster member switches—cannot be more than 16.

- Each standby-group member (Figure 6-7) must be connected to the cluster command switch through the same VLAN. Each standby-group member must also be redundantly connected to each other through at least one VLAN in common with the switch cluster.

Catalyst 1900, Catalyst 2820, Catalyst 2900 XL, Catalyst 2950, and Catalyst 3500 XL cluster member switches must be connected to the cluster standby group through their management VLANs. For more information about VLANs in switch clusters, see these sections:

- "Discovery Through Different VLANs" section on page 6-7
- "Discovery Through Different Management VLANs" section on page 6-8

Figure 6-7   VLAN Connectivity between Standby-Group Members and Cluster Members
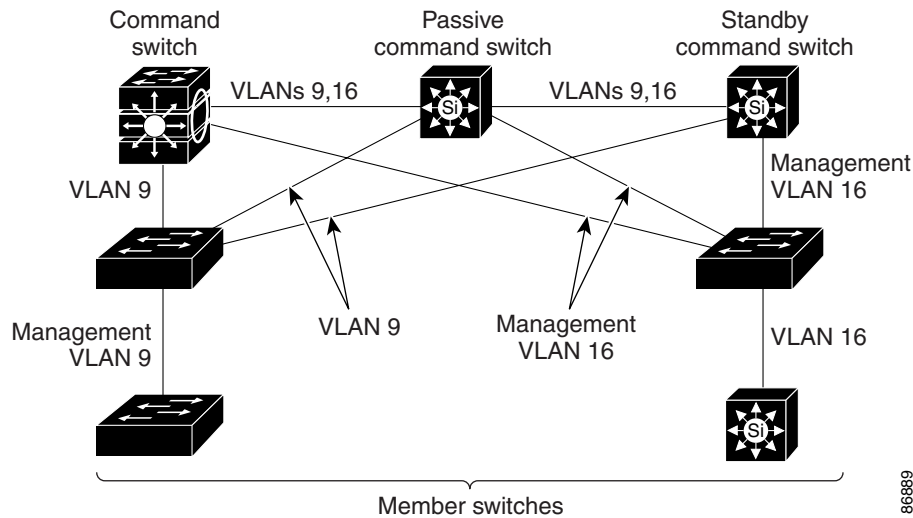
Automatic Recovery of Cluster Configuration

The active cluster command switch continually forwards cluster-configuration information (but not device-configuration information) to the standby cluster command switch. This ensures that the standby cluster command switch can take over the cluster immediately after the active cluster command switch fails.

Automatic discovery has these limitations:

- This limitation applies only to clusters that have Catalyst 2950, Catalyst 3550, and Catalyst 3750 command and standby cluster command switches: If the active cluster command switch and standby cluster command switch become disabled *at the same time*, the passive cluster command switch with the highest priority becomes the active cluster command switch. However, because it was a passive standby cluster command switch, the previous cluster command switch *did not* forward cluster-configuration information to it. The active cluster command switch only forwards cluster-configuration information to the standby cluster command switch. You must therefore rebuild the cluster.

- This limitation applies to all clusters: If the active cluster command switch fails and there are more than two switches in the cluster standby group, the new cluster command switch does not discover any Catalyst 1900, Catalyst 2820, and Catalyst 2916M XL cluster member switches. You must re-add these cluster member switches to the cluster.

- This limitation applies to all clusters: If the active cluster command switch fails and becomes active again, it does not discover any Catalyst 1900, Catalyst 2820, and Catalyst 2916M XL cluster member switches. You must again add these cluster member switches to the cluster.

When the previously active cluster command switch resumes its active role, it receives a copy of the latest cluster configuration from the active cluster command switch, including members that were added while it was down. The active cluster command switch sends a copy of the cluster configuration to the cluster standby group.

IP Addresses

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

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

You can assign an IP address to a cluster-capable switch, but it is not necessary. A cluster member switch is managed and communicates with other cluster member switches through the command-switch IP address. If the cluster 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 cluster 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 cluster command switch or an eligible cluster member. However, a host name assigned to the cluster command switch can help to 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 cluster 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 cluster 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 cluster command switch, was removed from a 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 cluster 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

You do not need 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 cluster member switch inherits a null password. Cluster member switches only inherit the command-switch password.

If you change the member-switch password to be different from the command-switch password and save the change, the switch is not manageable by the cluster command switch until you change the member-switch password to match the command-switch password. Rebooting the member switch does not revert the password back to the command-switch password. 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 7-1.

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

SNMP Community Strings

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

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

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

The switches support an unlimited number of community strings and string lengths. For more information about SNMP and community strings, see Chapter 22, "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.

Switch Clusters and Switch Stacks

A *switch cluster* can have one or more Catalyst 3750 switch stacks. Each switch stack can act as the cluster command switch or as a single cluster member. Table 6-1 describes the basic differences between switch stacks and switch clusters. For more information about switch stacks, see Chapter 5, "Managing Switch Stacks."

Table 6-1   Basic Comparison of Switch Stacks and Switch Clusters

Switch Stack	Switch Cluster
Made up of Catalyst 3750 switches only	Made up of cluster-capable switches, such as Catalyst 3750, Catalyst 3550, and Catalyst 2950 switches
Stack members are connected through StackWise ports	Cluster members are connected through LAN ports
Requires one *stack master* and supports up to eight other *stack members*	Requires 1 *cluster command switch* and supports up to 15 other *cluster member switches*
Can be a cluster command switch or a cluster member switch	Cannot be a stack master or stack member

Table 6-1   Basic Comparison of Switch Stacks and Switch Clusters (continued)

Switch Stack	Switch Cluster
Stack master is the single point of *complete* management for all stack members in a particular switch stack	Cluster command switch is the single point of *some* management for all cluster members in a particular switch cluster
Back-up stack master is automatically determined in case the stack master fails	Standby cluster command switch must be pre-assigned in case the cluster command switch fails
Switch stack supports up to eight simultaneous stack master failures	Switch cluster supports only one cluster command switch failure at a time
Stack members (as a switch stack) behave and is presented as a single, unified system in the network	Cluster members are various, independent switches that are not managed as and do not behave as a unified system
Integrated management of stack members through a single configuration file	Cluster members have separate, individual configuration files
Stack- and interface-level configurations are stored on each stack member	Cluster configuration are stored on the cluster command switch and the standby cluster command switch
New stack members are automatically added to the switch stack	New cluster members must be manually added to the switch cluster

Recall that stack members work together to behave as a unified system (as a single switch stack) in the network and are presented to the network as such by Layer 2 and Layer 3 protocols. Therefore, the switch cluster recognizes switch stacks, not individual stack members, as eligible cluster members. Individual stack members cannot join a switch cluster or participate as separate cluster members. Because a switch cluster must have 1 cluster command switch and can have up to 15 cluster members, a cluster can potentially have up to 16 switch stacks, totalling 144 devices.

Cluster configuration of switch stacks is through the stack master.

> **Note** From the CLI, you can configure a switch cluster to contain up to 16 switch stacks. However, from CMS, the maximum number of actual devices in a switch cluster is 16, irrespective of the number of devices in switch stack cluster members. For example, if a switch stack contains three stack members, they are counted as three separate devices.
>
> If you used the CLI to configure a switch cluster that contains more than 16 actual devices and then try to display the cluster from CMS, CMS requires you to remove cluster members until the CMS limit of 16 is reached.

These are considerations to keep in mind when you have switch stacks in switch clusters:

- If the cluster command switch is not a Catalyst 3750 switch or switch stack and a new stack master is elected in a cluster member switch stack, the switch stack loses its connectivity to the switch cluster if there are no redundant connections between the switch stack and the cluster command switch. You must add the switch stack to the switch cluster.

- If the cluster command switch is a switch stack and new stack masters are simultaneously elected in the cluster command switch stack and in cluster member switch stacks, connectivity between the switch stacks is lost if there are no redundant connections between the switch stack and the cluster command switch. You must add the switch stacks to the cluster, including the cluster command switch stack.

- All stack members should have redundant connectivity to all VLANs in the switch cluster. Otherwise, if a new stack master is elected, stack members connected to any VLANs not configured on the new stack master lose their connectivity to the switch cluster. You must change the VLAN configuration of the stack master or the stack members and add the stack members back to the switch cluster.

- If a cluster member switch stack reloads and a new stack master is elected, the switch stack loses connectivity with the cluster command switch. You must add the switch stack back to the switch cluster.

- If a cluster command switch stack reloads, and the original stack master is not re-elected, you must rebuild the entire switch cluster.

For more information about switch stacks, see Chapter 5, "Managing Switch Stacks,"

TACACS+ and RADIUS

Inconsistent authentication configurations in switch clusters cause CMS to continually prompt for a user name and password. If Terminal Access Controller Access Control System Plus (TACACS+) is configured on a cluster member, it must be configured on all cluster members. Similarly, if Remote Authentication Dial-In User Service (RADIUS) is configured on a cluster member, it must be configured on all cluster members. Further, the same switch cluster cannot have some members configured with TACACS+ and other members configured with RADIUS.

For more information about TACACS+, see the "Controlling Switch Access with TACACS+" section on page 7-10. For more information about RADIUS, see the "Controlling Switch Access with RADIUS" section on page 7-18.

Access Modes in CMS

If your cluster has these cluster member switches running earlier software releases and if you have read-only access to these cluster member switches, some configuration windows for those switches display incomplete information:

- Catalyst 2900 XL or Catalyst 3500 XL cluster member switches running Release 12.0(5)WC2 or earlier

- Catalyst 2950 cluster member switches running Release 12.0(5)WC2 or earlier

- Catalyst 3550 cluster member switches running Release 12.1(6)EA1 or earlier

These switches do not support read-only mode on CMS:

- Catalyst 1900 and Catalyst 2820

- Catalyst 2900 XL switches with 4-MB CPU DRAM

In read-only mode, these switches appear as unavailable devices and cannot be configured from CMS. For more information about CMS access modes, see the "Access Modes in CMS" section on page 3-29.

Availability of Switch-Specific Features in Switch Clusters

The menu bar on the cluster command switch displays all options available from the switch cluster. Therefore, features specific to a cluster member switch are available from the command-switch menu bar. For example, **Device > LRE Profile** appears in the command-switch 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 this information:

- Enabling a Cluster Command Switch, page 6-18
- Adding Cluster Member Switches, page 6-19
- Creating a Cluster Standby Group, page 6-21

This section assumes you have already connected the switches, as described in the switch hardware installation guide, and followed the guidelines described in the "Planning a Switch Cluster" section on page 6-4.

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

Enabling a Cluster Command Switch

The switch you designate as the cluster command switch must meet the requirements described in the "Cluster Command Switch Characteristics" section on page 6-3, the "Planning a Switch Cluster" section on page 6-4, and the release notes.

Note We strongly recommend that the highest-end, command-capable switch in the cluster be the command switch. If your switch cluster has a Catalyst 3750 switch or a Catalyst 3750 switch stack, it should be the cluster command switch.

You can enable a cluster command switch, name the cluster, and assign an IP address and a password to the cluster 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 cluster command switch during initial switch setup, launch Device 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 6-8). Instead of using CMS to enable a cluster command switch, you can use the **cluster enable** global configuration command.

Figure 6-8   Create Cluster Window

Enter up to 31 characters to name the cluster.
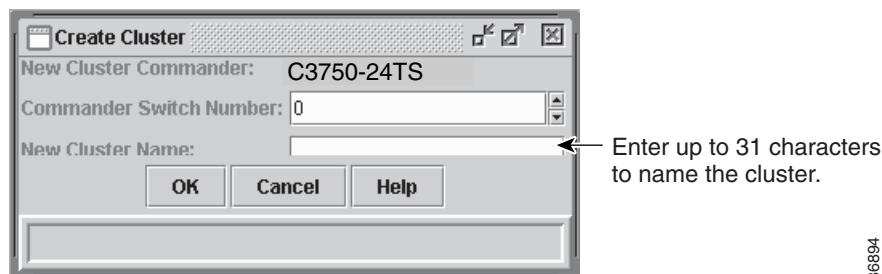
Adding Cluster Member Switches

Note   This task is available only on the stack master.

As explained in the "Automatic Discovery of Cluster Candidates and Members" section on page 6-5, the cluster command switch automatically discovers candidate switches. When you add new cluster-capable switches to the network, the cluster command switch discovers them and adds them to a list of candidate switches.

Note   A switch stack in a cluster equates to a single cluster member switch. There is a restriction specific to adding cluster members through CMS. From CMS, you can create a switch cluster with up to 15 cluster members. From the CLI, you can create a switch cluster with up to 144 devices. For more information, see the "Switch Clusters and Switch Stacks" section on page 6-15.

To display an updated cluster candidates list from the Add to Cluster window (Figure 6-9), 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.

From CMS, there are two ways to add switches to a cluster:

- Select **Cluster > Add to Cluster**, select a candidate switch from the list, click **Add**, and click **OK**. 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 6-10). In the Topology view, candidate switches are cyan, and cluster member switches are green. To add more than one candidate switch, press **Ctrl**, and left-click the candidates that you want to add.

Instead of using CMS to add members to the cluster, you can use the **cluster member** global configuration command from the cluster command switch. Use the **password** option in this command if the candidate switch has a password.

You can select 1 or more switches as long as the total number of switches in the cluster does not exceed 16 (this includes the cluster command switch). When a cluster has 16 members, the **Add to Cluster** option is not available for that cluster. In this case, you must remove a cluster member switch before adding a new one.

If a password has been configured on a candidate switch, you are prompted to enter it before it can be added it to the cluster. If the candidate switch does not have a password, any entry is ignored.

If multiple candidates switches have the same password, you can select them as a group, and add them at the same time.

If a candidate switch in the group has a password different from the group, only that specific candidate switch is not added to the cluster.

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 6-15.

For additional authentication considerations in switch clusters, see the "TACACS+ and RADIUS" section on page 6-17.
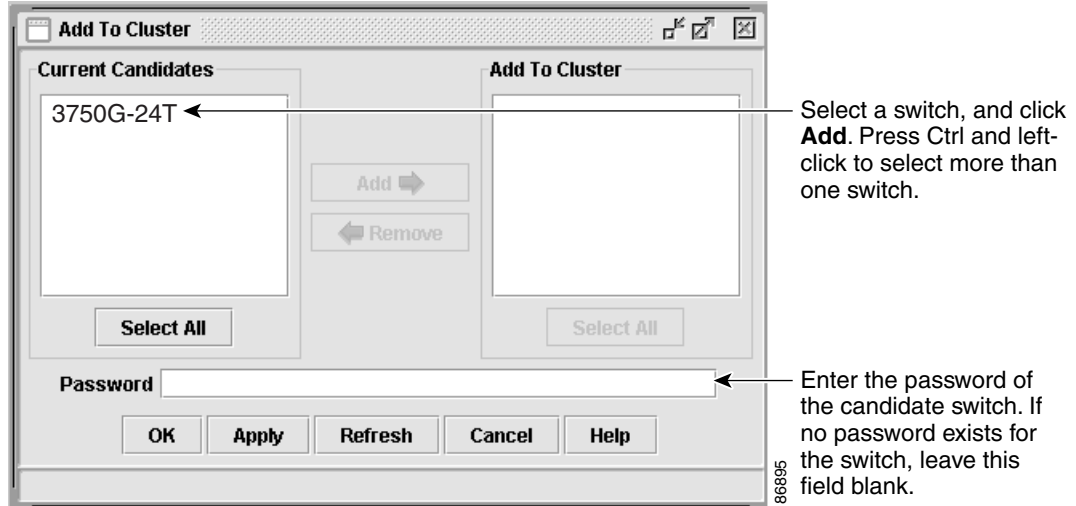
Figure 6-9   Add to Cluster Window

Select a switch, and click **Add**. Press Ctrl and left-click to select more than one switch.

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

Figure 6-10   Using the Topology View to Add Cluster Member Switches

Thin line means a connection to a candidate switch.

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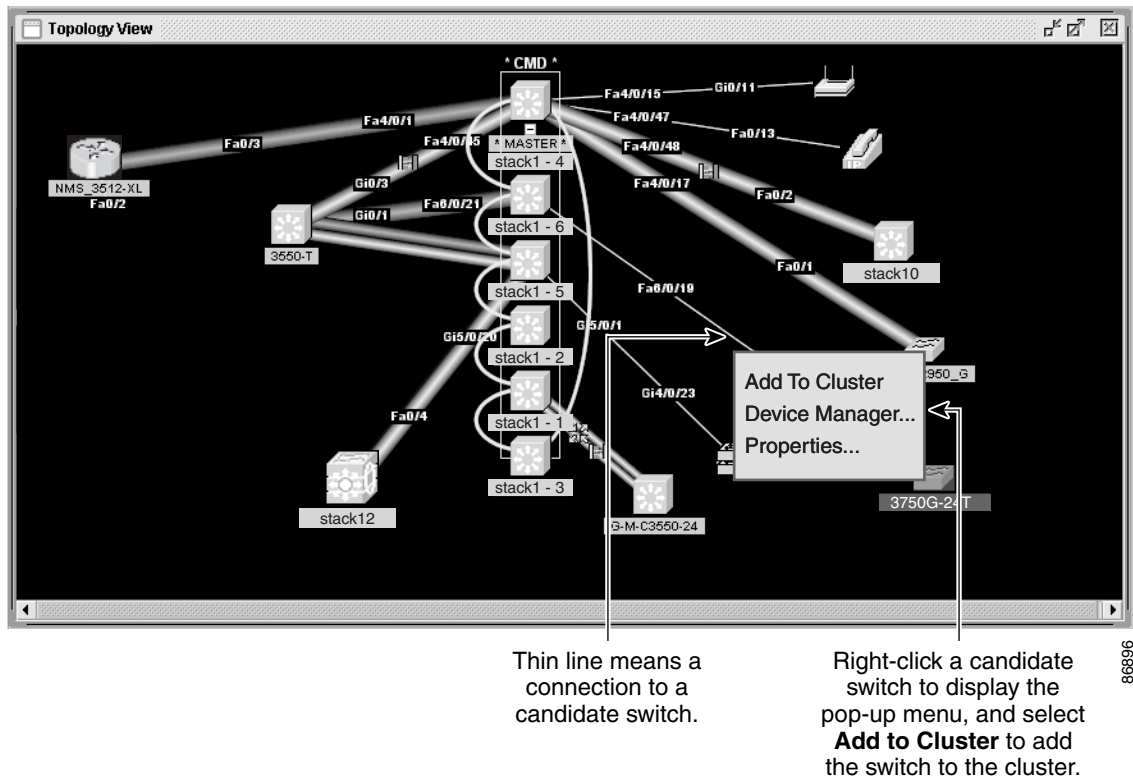
Creating a Cluster Standby Group

Note   This task is available only on the stack master.

The cluster standby group members must meet the requirements described in the "Standby Cluster Command Switch Characteristics" section on page 6-3 and "HSRP and Standby Cluster Command Switches" section on page 6-11. To create a cluster standby group, select **Cluster > Standby Command Switches** (Figure 6-11).

Instead of using CMS to add switches to a standby group and to bind the standby group to a cluster, you can use the **standby ip**, the **standby name**, and the **standby priority** interface configuration commands and the **cluster standby group** global configuration command.

Note   Standby cluster command switches must be the same type of switches as the cluster command switch. For example, if the cluster command switch is a Catalyst 3750 switch, the standby cluster command switches must also be Catalyst 3750 switches. Refer to the switch configuration guide of other cluster-capable switches for IOS release requirements on standby cluster command switches.

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

- AC—Active cluster command switch
- SC—Standby cluster command switch
- PC—Member of the cluster standby group but not the standby cluster command switch
- HC—Candidate switch that can be added to the cluster standby group
- CC—Cluster 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 31 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 standby group, all switches in the group have the **preempt** command enabled. You must also provide a name for the group.

Note   The HSRP standby hold time interval should be greater than or equal to three times the hello time interval. The default HSRP standby hold time interval is 10 seconds. The default HSRP standby hello time interval is 3 seconds. For more information about the standby hold time and standby hello time intervals, see the "Configuring HSRP Authentication and Timers" section on page 27-8.

Figure 6-11   Standby Command Configuration Window
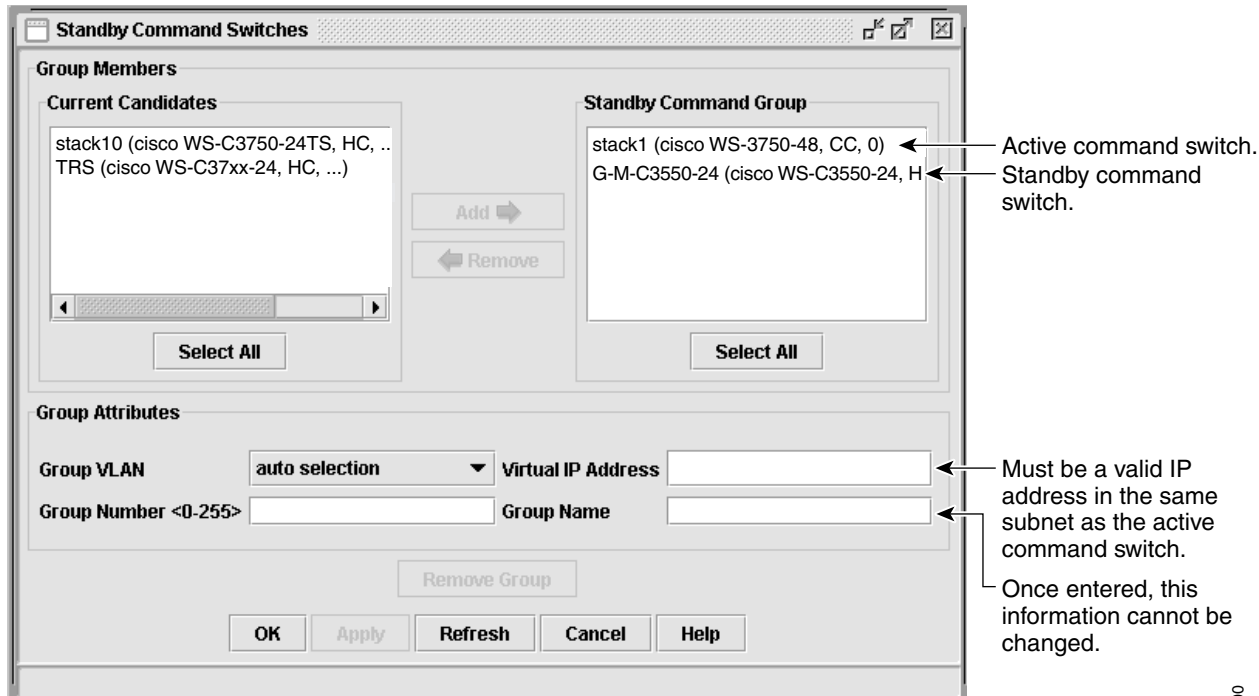
Verifying a Switch Cluster

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

Step 1   Enter the cluster 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 cluster topology and to view link information (Figure 3-6 on page 3-10). For complete information about the Topology view, including descriptions of the icons, links, and colors, 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 6-12).

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**.

Instead of using CMS to verify the cluster, you can use the **show cluster members** user EXEC command from the cluster command switch or use the **show cluster** user EXEC command from the cluster command switch or from a cluster member switch.

Figure 6-12 Inventory Window

Host Name	Device Type	Serial Nu...	Mac Addre...	IP Address	Software Ver...	Sys Locati...	System Uptime
stack1	cisco WS-C37...	Multiple	0003.fd63....	10.1.1.2, 10.1	12.1(0.0.133)...		1 day 42 minutes
stack12	cisco WS-C37...		0003.fd62....	10.10.10.9	12.1(11) AX		1 day 15 hours ...
stack10	cisco WS-C37...		0003.fd63....	10.10.10.6	12.1(11) AX		3 weeks 5 days ...
TRS	cisco WS-C37...		0003.fd63....	14.14.14.14, ...	12.1(11) AX		2 days 3 hours ...
3550-T	cisco WS-C35...	FAA0608T...	0005.313c...	10.10.10.7	12.1(0.0.606)...		3 weeks 5 days ...
G-M-C3550-...	cisco WS-C35...	CAB0545A...	0007.eb49...	10.10.10.2	12.1(0.0.610)...		1 week 4 days ...
NMS_2950_G	cisco WS-C29...	FHK0550Z...	0008.2126...	10.10.10.3	12.1(0.0.610)...		1 week 18 hour...

If you lose connectivity with a cluster member switch or if a cluster command switch fails, see the cluster-related recovery procedures in

For more information about creating and managing clusters, refer to the online help. For information about the cluster commands, refer to the switch command reference.

Using the CLI to Manage Switch Clusters

You can configure cluster member switches from the CLI by first logging into the cluster command switch. Enter the **rcommand** user EXEC command and the cluster member switch number to start a Telnet session (through a console or Telnet connection) and to access the cluster member switch CLI. The command mode changes, and the IOS commands operate as usual. Enter the **exit** privileged EXEC command on the cluster 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** privileged EXEC command on the cluster command switch. For more information about the **rcommand** command and all other cluster commands, refer to the switch command reference.

The Telnet session accesses the member-switch CLI at the same privilege level as on the cluster command switch. The IOS commands then operate as usual. For instructions on configuring the switch for a Telnet session, see the "Disabling Password Recovery" section on page 7-5.

> **Note**   The CLI supports creating and maintaining switch clusters with up to 16 switch stacks. For more information about switch stack and switch cluster, see the "Switch Clusters and Switch Stacks" section on page 6-15.

Catalyst 1900 and Catalyst 2820 CLI Considerations

If your switch cluster has Catalyst 1900 and Catalyst 2820 switches running standard edition software, the Telnet session accesses the management console (a menu-driven interface) if the cluster command switch is at privilege level 15. If the cluster command switch is at privilege level 1 to 14, you are prompted for the password to access the menu console.

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

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

- If the command-switch privilege level is 15, the cluster 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 22-5. On Catalyst 1900 and Catalyst 2820 switches, SNMP is enabled by default.

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

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

If the cluster member switch does not have an IP address, the cluster command switch redirects traps from the cluster member switch to the management station, as shown in Figure 6-13. If a cluster member switch has its own IP address and community strings, the cluster member switch can send traps directly to the management station, without going through the cluster command switch.

If a cluster member switch has its own IP address and community strings, they can be used in addition to the access provided by the cluster command switch. For more information about SNMP and community strings, see Chapter 22, "Configuring SNMP."

Figure 6-13   SNMP Management for a Cluster