



## Clustering Switches

---

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

- [Understanding Switch Clusters, page 6-2](#)
- [Planning a Switch Cluster, page 6-5](#)
- [Creating a Switch Cluster, page 6-20](#)
- [Using the CLI to Manage Switch Clusters, page 6-26](#)
- [Using SNMP to Manage Switch Clusters, page 6-27](#)

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.

Refer to the release notes for the list of Catalyst switches eligible 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 2950 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 the *command switch* and up to 15 switches can be *member switches*. The total number of switches in a cluster cannot exceed 16 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 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 multilayer switch as a Layer 3 router between the Layer 2 switches in the cluster) network.

Cluster members are connected to the command switch according to the connectivity guidelines described in the [“Automatic Discovery of Cluster Candidates and Members”](#) section on page 6-5.

- Command-switch redundancy if a command switch fails. One or more switches can be designated as *standby command switches* to avoid loss of 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 1-6.

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

These sections describe:

- [Command Switch Characteristics](#), page 6-3
- [Standby Command Switch Characteristics](#), page 6-3
- [Candidate Switch and Member Switch Characteristics](#), page 6-4

## Command Switch Characteristics

A Catalyst 2950 command switch must meet these requirements:

- It is running Release 12.0(5.2)WC(1) 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.
- If the Catalyst 2950 command switch is running Release 12.1(9)EA1 or later, it is connected to the standby command switches through the management VLAN and to the member switches through a common VLAN.
- If the Catalyst 2950 command switch is running a release earlier than Release 12.1(9)EA1, it is connected to the standby command switches and member switches through its management VLAN.

**Note**

The CMP-NAT-ACL access list is created when a device is configured as the command switch. Configuring any other access list on the switch can restrict access to it and affect the discovery of member and candidate switches.

**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 3550 switch, that switch should be the command switch.
  - If your switch cluster has Catalyst 2900 XL, Catalyst 2950, and Catalyst 3500 XL switches, the Catalyst 2950 should be the command switch.
  - If your switch cluster has Catalyst 1900, Catalyst 2820, Catalyst 2900 XL, and Catalyst 3500 XL switches, either the Catalyst 2900 XL or Catalyst 3500 XL should be the command switch.

## Standby Command Switch Characteristics

A Catalyst 2950 standby command switch must meet these requirements:

- It is running Release 12.0(5.2)WC(1) or later.
- It has an IP address.
- It has CDP version 2 enabled.
- If the Catalyst 2950 standby command switch is running Release 12.1(9)EA1 or later, it is connected to other standby switches through its management VLAN and to all member switches through a common VLAN.
- If the Catalyst 2950 standby command switch is running a release earlier than Release 12.1(9)EA1, it is connected to the command switch and to other standby command switches and member switches through its management VLAN.

**Note**


---

Catalyst 2950 command switches running Release 12.1(9)EA1 or later can connect to standby command switches in the management VLAN.

---

- It is redundantly connected to the cluster so that connectivity to member switches is maintained.
- It is not a command or member switch of another cluster.

**Note**

- 
- Standby command switches must meet these requirements:
    - When the command switch is a Catalyst 3550 switch, all standby command switches must be Catalyst 3550 switches.
    - When the command switch is a Catalyst 2950 switch running Release 12.1(9)EA1 or later, all standby command switches must be Catalyst 2950 switches running Release 12.1(9)EA1 or later.
    - When the command switch is a Catalyst 2950 switch running Release 12.1(6)EA2 or later, all standby command switches must be Catalyst 2950 switches running Release 12.1(6)EA2 or later.
    - When the command switch is running Release 12.0(5)WC2 or earlier, the standby command switches can be these switches: Catalyst 2900 XL, Catalyst 2950, and Catalyst 3500 XL switches.
  - We strongly recommend that the command switch and standby command switches are of the same switch platform.
    - If you have a Catalyst 3550 command switch, the standby command switches should be Catalyst 3550 switches.
    - If you have a Catalyst 2950 command switch, the standby command switches should be Catalyst 2950 switches.
    - If you have a Catalyst 2900 XL or Catalyst 3500 XL command switch, the standby command switches should be Catalyst 2900 XL and Catalyst 3500 XL switches.
- 

## Candidate Switch and Member Switch 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. Although not required, a candidate or member switch can have its own IP address and password (for related considerations, see the [“IP Addresses”](#) section on page 6-16 and [“Passwords”](#) section on page 6-17).

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 member switch of another cluster.
- If the Catalyst 2950 member or candidate switch is running Release 12.1(9)EA1 or later, it is connected to the command switch through at least one common VLAN.
- If the Catalyst 2950 member or candidate switch is running a release earlier than Release 12.1(9)EA1, it is connected to the command switch through the command-switch management VLAN.

**Note**

Catalyst 2950 standby command switches running Release 12.1(9)EA1 or later can connect to candidate and member switches in VLANs different from their management VLANs.

## 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 Command Switches](#), page 6-13
- [IP Addresses](#), page 6-16
- [Host Names](#), page 6-17
- [Passwords](#), page 6-17
- [SNMP Community Strings](#), page 6-17
- [TACACS+ and RADIUS](#), page 6-18
- [Access Modes in CMS](#), page 6-18
- [Management VLAN](#), page 6-19
- [LRE Profiles](#), page 6-19
- [Availability of Switch-Specific Features in Switch Clusters](#), page 6-20

Refer to the release notes for the list of Catalyst switches eligible 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 in star or cascaded topologies.

**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. For more information about CDP, see [Chapter 19](#), “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 6-6
- [Discovery through Non-CDP-Capable and Noncluster-Capable Devices](#), page 6-8
- [Discovery through the Same Management VLAN](#), page 6-9
- [Discovery through Different Management VLANs](#), page 6-10
- [Discovery of Newly Installed Switches](#), page 6-11

## Discovery through CDP Hops

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 and to candidate switches. For example, member switches 9 and 10 in [Figure 6-1](#) 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.

In [Figure 6-1](#), the command switch is running a release earlier than Release 12.1(9)EA1 and has ports assigned to management VLAN 16. In [Figure 6-2](#), the command switch is running Release 12.1(9)EA1 or later and has ports assigned to VLANs 16 and 62. The CDP hop count is three. Each 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 (Command Switch Running a Release Earlier than Release 12.1(9)EA1)

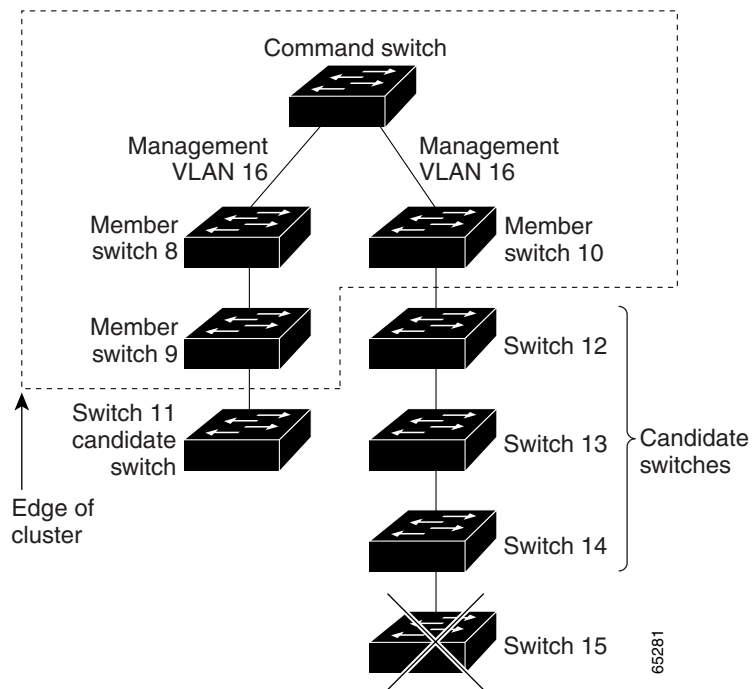
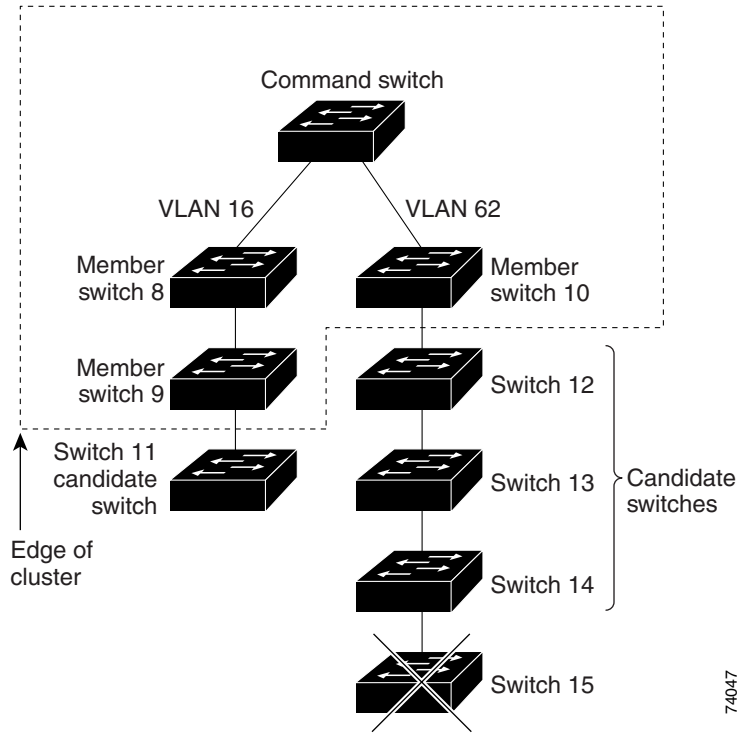


Figure 6-2 Discovery through CDP Hops (Command Switch Running Release 12.1(9)EA1 or Later)



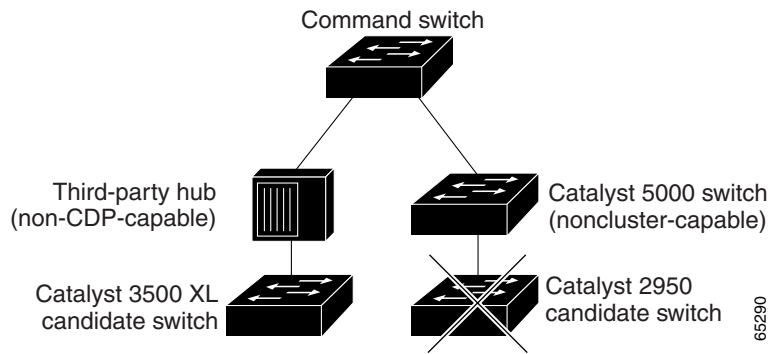
## Discovery through Non-CDP-Capable and Noncluster-Capable Devices

If a 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 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 6-3 shows that the command switch discovers the Catalyst 3500 XL switch, which is connected to a third-party hub. However, the command switch does not discover the Catalyst 2950 switch that is connected to a Catalyst 5000 switch.

Refer to the release notes for the Catalyst switches that can be part of a switch cluster.

**Figure 6-3** Discovery through Non-CDP-Capable and Noncluster-Capable Devices



## Discovery through the Same Management VLAN

A Catalyst 2900 XL command switch, a Catalyst 2950 command switch running a release earlier than Release 12.1(9)EA1, or a Catalyst 3500 XL command switch must connect to all cluster members through its management VLAN. The default management VLAN is VLAN 1. For more information about management VLANs, see the “[Management VLAN](#)” section on page 6-19.



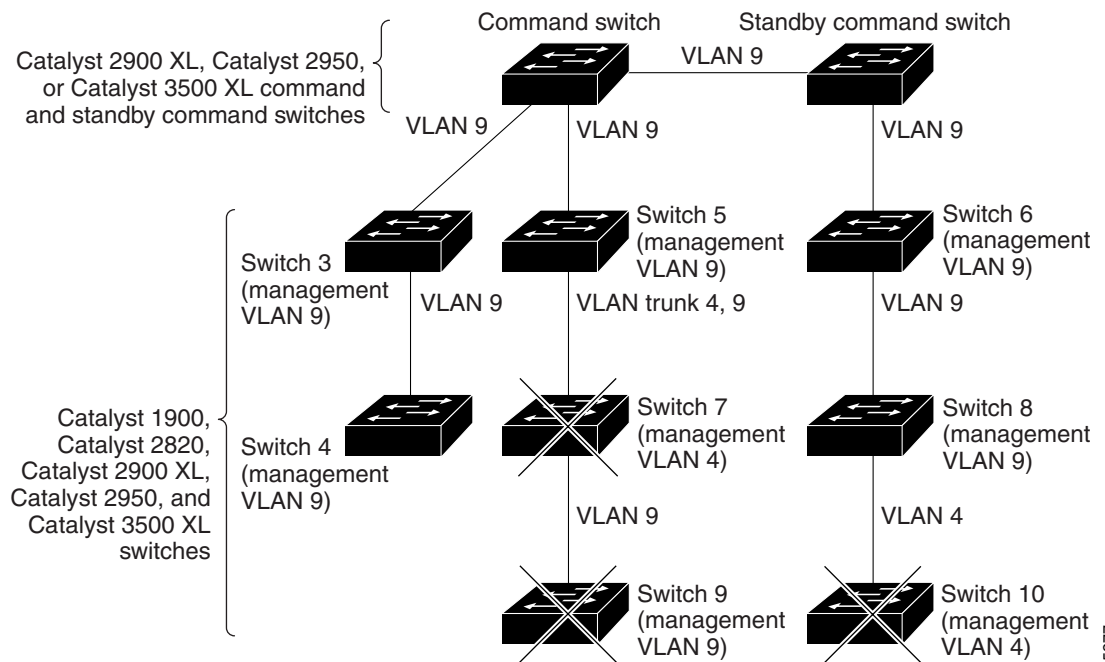
### Note

You can avoid this limitation by using, whenever possible, a Catalyst 3550 command switch or a Catalyst 2950 command switch running Release 12.1(9)EA1 or later. These command switches can manage cluster members even if they belong to different management VLANs. See the “[Discovery through Different Management VLANs](#)” section on page 6-10.

The command switch in [Figure 6-4](#) has ports assigned to management VLAN 9. It discovers all but these switches:

- Switches 7 and 10 because their management VLAN (VLAN 4) is different from the command-switch management VLAN (VLAN 9)
- Switch 9 because automatic discovery does not extend beyond a noncandidate device, which is switch 7

**Figure 6-4** Discovery through the Same Management VLAN



65277

## Discovery through Different Management VLANs

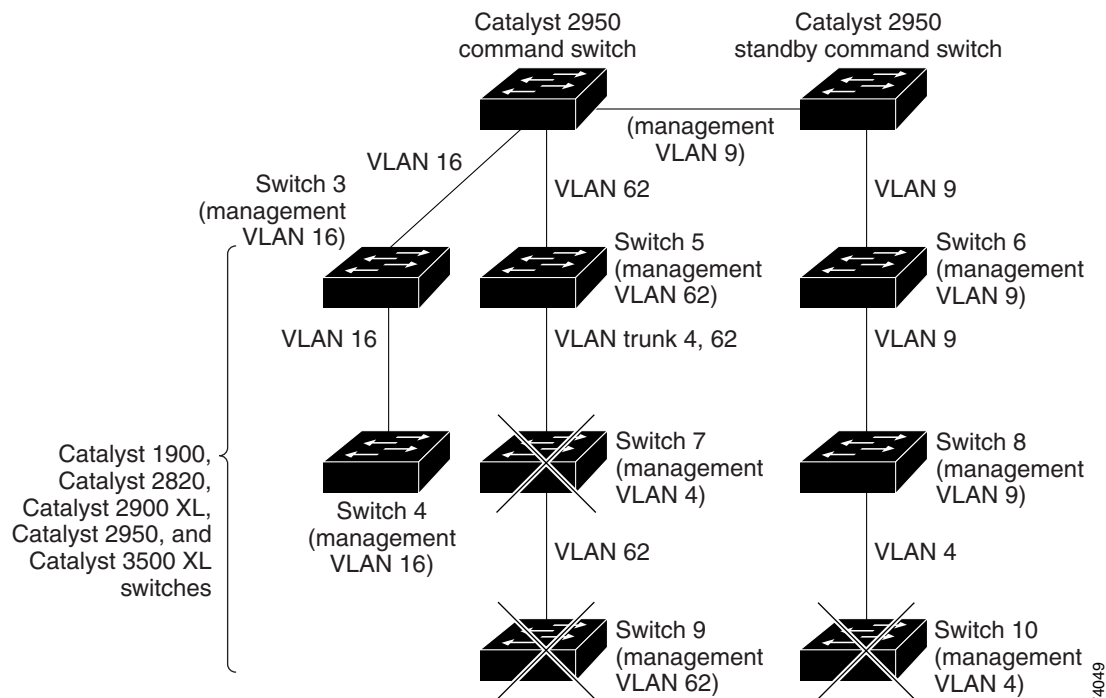
We recommend using a Catalyst 3550 command switch or a Catalyst 2950 command switch running Release 12.1(9)EA1 or later. These command switches can discover and manage member switches in different VLANs and different management VLANs. Catalyst 3550 member switches and Catalyst 2950 member switches running Release 12.1(9)EA1 or later must be connected through at least one VLAN in common with the command switch. All other member switches must be connected to the command switch through their management VLAN.

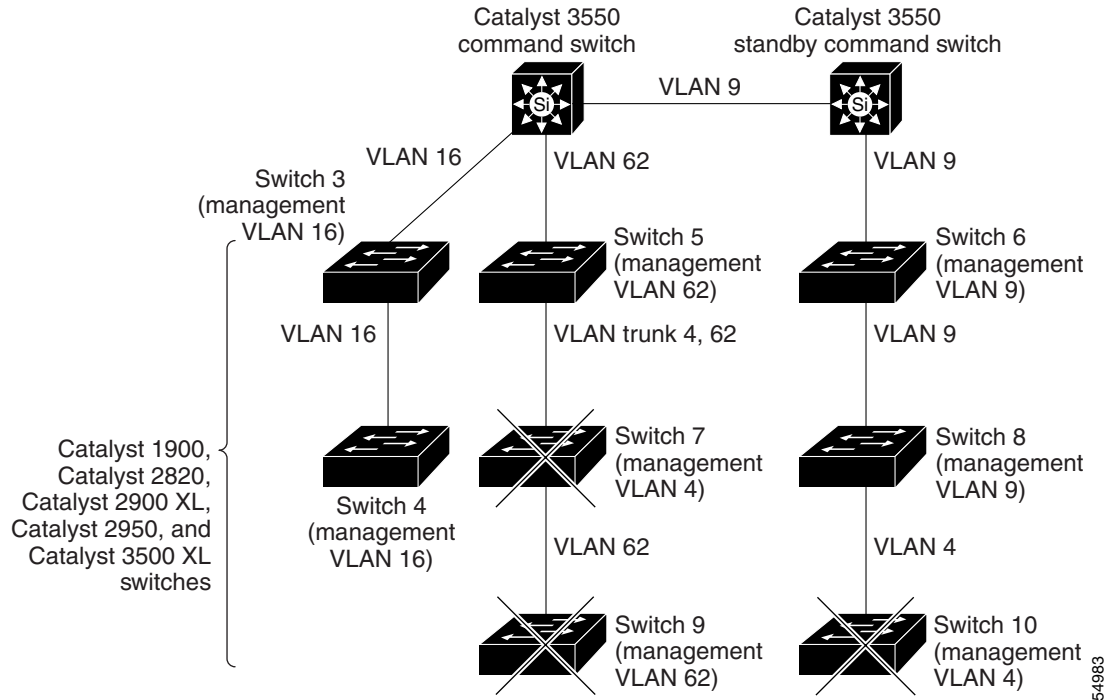
In contrast, a Catalyst 2900 XL command switch, a Catalyst 2950 command switch running a release earlier than Release 12.1(9)EA1, or a Catalyst 3500 XL command switch must connect to all cluster members through its management VLAN. The default management VLAN is VLAN 1. For information about discovery through the same management VLAN on these switches, see the [“Discovery through the Same Management VLAN”](#) section on page 6-9.

The Catalyst 2950 command switch (running Release 12.1(9)EA1 or later) in [Figure 6-5](#) and the Catalyst 3550 command switch in [Figure 6-6](#) have ports assigned to VLANs 9, 16, and 62. The management VLAN on the Catalyst 2950 command switch is VLAN 9. Each 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 command switch
- Switch 9 because automatic discovery does not extend beyond a noncandidate device, which is switch 7

**Figure 6-5** Discovery through Different Management VLANs with a Layer 2 Command Switch



**Figure 6-6** Discovery through Different Management VLANs with a Layer 3 Command Switch

## 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 the management VLAN. By default, the new switch and its access ports are assigned to management VLAN 1.

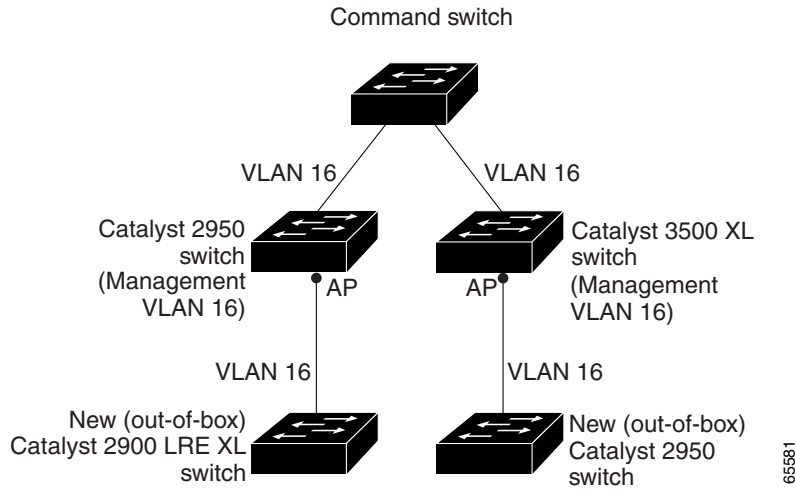
When the new switch joins a cluster, its default management VLAN changes to the VLAN of the immediately upstream neighbor. The new switch also configures its access port to belong to the VLAN of the immediately upstream neighbor.

The command switch (running a release earlier than Release 12.1(9)EA1) in [Figure 6-7](#) belongs to management VLAN 16. When the new Catalyst 2900 LRE XL and Catalyst 2950 switches join the cluster, their management VLAN and access ports change from VLAN 1 to VLAN 16.

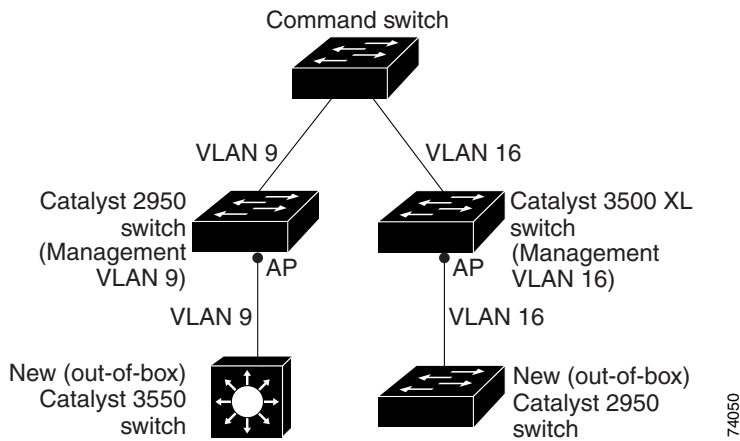
The command switch (running Release 12.1(9)EA1 or later) in [Figure 6-8](#) belongs to VLANs 9 and 16. When the new Catalyst 3550 and Catalyst 2950 switches join the cluster:

- The Catalyst 3550 switch and its access port are assigned to VLAN 9.
- The Catalyst 2950 switch and its access port are assigned to management VLAN 16.

**Figure 6-7** Discovery of Newly Installed Switches in the Same Management VLAN



**Figure 6-8** Discovery of Newly Installed Switches in Different Management VLANs



## 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 command switch to take over if the primary 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 6-3. Only one cluster standby group can be assigned per cluster.

**Note**

- When the command switch is a Catalyst 3550 switch, all standby command switches must be Catalyst 3550 switches.
- When the command switch is a Catalyst 2950 switch running Release 12.1(9)EA1 or later, all standby command switches must be Catalyst 2950 switches running Release 12.1(9)EA1 or later.
- When the command switch is a Catalyst 2950 switch running Release 12.1(6)EA2 or later, all standby command switches must be Catalyst 2950 switches running Release 12.1(6)EA2 or later.
- When the command switch is running Release 12.0(5)WC2 or earlier, the standby command switches can be these switches: Catalyst 2900 XL, Catalyst 2950, and Catalyst 3500 XL switches.

**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 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). 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. For the limitations to automatic discovery, see the “[Automatic Recovery of Cluster Configuration](#)” section on page 6-16. For information about changing HSRP priority values, refer to the **standby priority** interface configuration mode command in the IOS Release 12.1 documentation set. The HSRP 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 3 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 hello time intervals, refer to the Release 12.1 documentation set on Cisco.com.

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 command switches:

- [Virtual IP Addresses, page 6-14](#)
- [Other Considerations for Cluster Standby Groups, page 6-14](#)
- [Automatic Recovery of Cluster Configuration, page 6-16](#)

## 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 the management VLAN 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. This is in case the IP address of the active command switch is different from the virtual IP address of the cluster standby group.

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 current active command switch becomes the standby command switch again. For more information about IP address in switch clusters, see the [“IP Addresses” section on page 6-16](#).

## Other Considerations for Cluster Standby Groups

These requirements also apply:

- Standby command switches must meet these requirements:
  - When the command switch is a Catalyst 3550 switch, all standby command switches must be Catalyst 3550 switches.
  - When the command switch is a Catalyst 2950 switch running Release 12.1(9)EA1 or later, all standby command switches must be Catalyst 2950 switches running Release 12.1(9)EA1 or later.
  - When the command switch is a Catalyst 2950 switch running Release 12.1(6)EA2 or later, all standby command switches must be Catalyst 2950 switches running Release 12.1(6)EA2 or later.
  - When the command switch is running Release 12.0(5)WC2 or earlier, the standby command switches can be these switches: Catalyst 2900 XL, Catalyst 2950, and Catalyst 3500 XL switches.

We strongly recommend that the command switch and standby command switches are of the same switch platform.

- If you have a Catalyst 3550 command switch, the standby command switches should be Catalyst 3550 switches.
  - If you have a Catalyst 2950 command switch, the standby command switches should be Catalyst 2950 switches.
  - If you have a Catalyst 2900 XL or Catalyst 3500 XL command switch, the standby command switches should be Catalyst 2900 XL and Catalyst 3500 XL switches.
- Only one cluster standby group can be assigned to a cluster.

- 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 command switches. However, the total number of switches in the cluster—which would include the active command switch, standby-group members, and member switches—cannot be more than 16.

- Each standby-group member (Figure 6-9) must be connected to the command switch through its management VLAN. Each standby-group member must also be redundantly connected to each other through the management VLAN.

Catalyst 1900, Catalyst 2820, Catalyst 2900 XL, Catalyst 2950, and Catalyst 3500 XL member switches must be connected to the cluster standby group through their management VLANs.



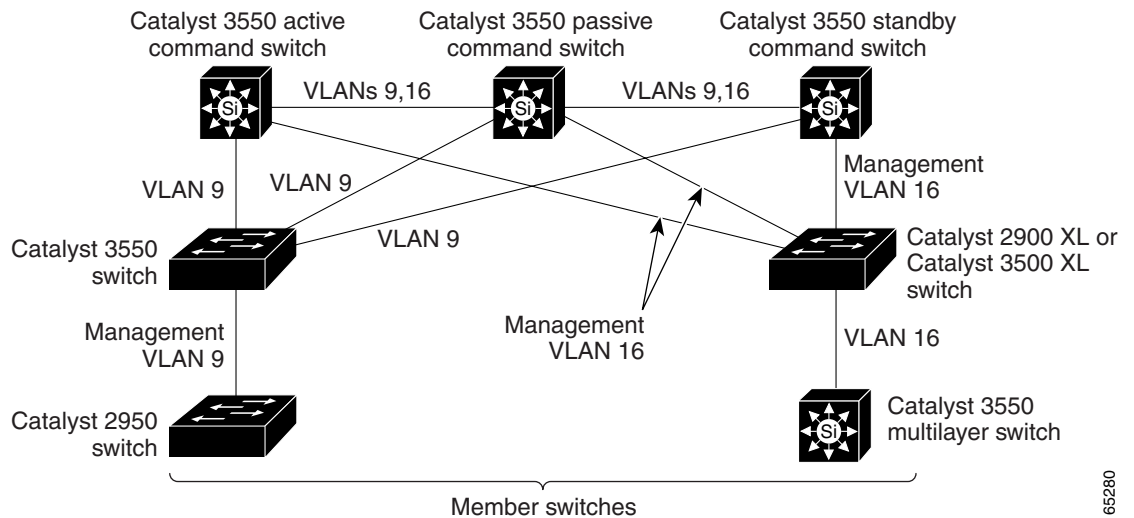
**Note**

Catalyst 2950 standby command switches running Release 12.1(9)EA1 or later can connect to candidate and member switches in VLANs different from their management VLANs.

For more information about VLANs in switch clusters, see these sections:

- “Discovery through the Same Management VLAN” section on page 6-9
- “Discovery through Different Management VLANs” section on page 6-10

**Figure 6-9 VLAN Connectivity between Standby-Group Members and Cluster Members**



65280

## Automatic Recovery of Cluster Configuration

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

Automatic discovery has these limitations:

- This limitation applies only to clusters that have Catalyst 2950 and Catalyst 3550 command and standby command switches: If the active command switch and standby command switch become disabled *at the same time*, the passive command switch with the highest priority becomes the active command switch. However, because it was a passive standby command switch, the previous command switch *did not* forward cluster-configuration information to it. The active command switch only forwards cluster-configuration information to the standby command switch. You must therefore rebuild the cluster.
- This limitation applies to all clusters: If the active command switch fails and there are more than two switches in the cluster standby group, the new command switch does not discover any Catalyst 1900, Catalyst 2820, and Catalyst 2916M XL member switches. You must re-add these member switches to the cluster.
- This limitation applies to all clusters: If the active command switch fails and becomes active again, it does not discover any Catalyst 1900, Catalyst 2820, and Catalyst 2916M XL member switches. You must again add these member switches to the cluster.

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

## IP Addresses

You must assign IP information to a command switch. You can access the cluster through the command-switch IP address. If you configure a cluster standby group, you must 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 or the IP address available on the new active command switch to access the cluster.

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 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 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 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 member switch inherits a null password. 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 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 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 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 SNMP and community strings, see [Chapter 23, “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.

## 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 7-9. For more information about RADIUS, see the [“Controlling Switch Access with RADIUS”](#) section on page 7-17.

## Access Modes in CMS

CMS provides two levels of access to the configuration options: read-write access and read-only access. Privilege levels 0 to 15 are supported.

- Privilege level 15 provides you with read-write access to CMS.
- Privilege levels 1 to 14 provide you with read-only access to CMS. Any options in the CMS windows, menu bar, toolbar, and popup menus that change the switch or cluster configuration are not shown in read-only mode.
- Privilege level 0 denies access to CMS.

For more information about CMS access modes, see the [“Access Modes in CMS”](#) section on page 3-29.



### Note

- If your cluster has these member switches running earlier software releases and if you have read-only access to these member switches, some configuration windows for those switches display incomplete information:
  - Catalyst 2900 XL or Catalyst 3500 XL member switches running Release 12.0(5)WC2 or earlier
  - Catalyst 2950 member switches running Release 12.0(5)WC2 or earlier
  - Catalyst 3550 member switches running Release 12.1(6)EA1 or earlier

For more information about this limitation, refer to the release notes.

- 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.

## Management VLAN

Communication with the switch management interfaces is through the command-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 command switch, member switches, and candidate switches must be connected through ports assigned to the command-switch management VLAN.

**Note**

- If the command switch is a Catalyst 2950 running Release 12.1(9)EA1 or later, candidate and member switches can belong to different management VLANs. However, they must connect to the command switch through their management VLAN.
- Catalyst 2950 standby command switches running Release 12.1(9)EA1 or later can connect to candidate and member switches in VLANs different from their management VLANs.

If you add a new, out-of-box switch to a 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 of the new switch to the one the cluster is using. This automatic VLAN change only occurs for new, out-of-box switches that do not have a `config.text` file and that have no changes to the running configuration. For more information, see the [“Discovery of Newly Installed Switches” section on page 6-11](#).

You can change the management VLAN of a member switch (not the command switch). However, the command switch will not be able to communicate with it. In this case, you will need to manage the switch as a standalone switch.

You can globally change the management VLAN for the cluster as long as each member switch has either a trunk connection or a connection to the new command-switch management VLAN. From the command switch, use the **cluster management vlan** global configuration command to change the cluster management VLAN to a different management VLAN.

**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.

For more information about changing the management VLAN, see the [“Management VLAN” section on page 6-19](#).

## LRE Profiles

A configuration conflict occurs if a switch cluster has Long-Reach Ethernet (LRE) switches that use 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 that use different private profiles.

## Availability of Switch-Specific Features in Switch Clusters

The menu bar on the command switch displays all options available from the switch cluster. Therefore, features specific to a 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 Command Switch, page 6-20](#)
- [Adding Member Switches, page 6-21](#)
- [Creating a Cluster Standby Group, page 6-23](#)
- [Verifying a Switch Cluster, page 6-25](#)

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 6-5.

**Note**

---

Refer to the release notes for the list of Catalyst switches eligible 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 as the command switch must meet the requirements described in the [“Command Switch Characteristics”](#) section on page 6-3, the [“Planning a Switch Cluster”](#) section on page 6-5, and the release notes.

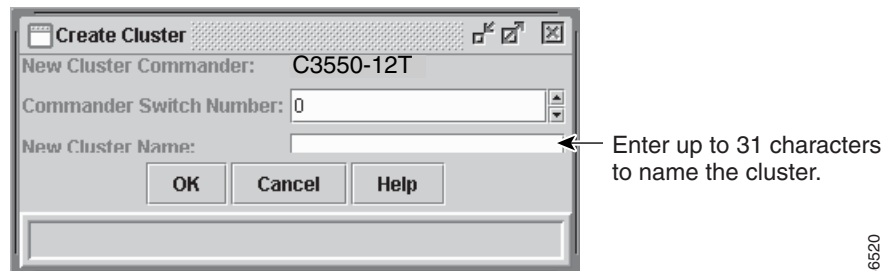
**Note**

- We strongly recommend that the highest-end, command-capable switch in the cluster be the command switch:
    - If your switch cluster has a Catalyst 3550 switch, that switch should be the command switch.
    - If your switch cluster has Catalyst 2900 XL, Catalyst 2950, and Catalyst 3500 XL switches, the Catalyst 2950 should be the command switch.
    - If your switch cluster has Catalyst 1900, Catalyst 2820, Catalyst 2900 XL, and Catalyst 3500 XL switches, either the Catalyst 2900 XL or Catalyst 3500 XL should be the command switch.
- 

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 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 6-10). Instead of using CMS to enable a command switch, you can use the **cluster enable** global configuration command.

Figure 6-10 Create Cluster Window



56520

## Adding Member Switches

As explained in the “Automatic Discovery of Cluster Candidates and Members” section on page 6-5, the command switch automatically discovers candidate switches. When you add new cluster-capable switches to the network, the command switch discovers them and adds them to a list of candidate switches. To display an updated cluster candidates list from the Add to Cluster window (Figure 6-11), 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 6-12). 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 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 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 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 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 to the cluster. If the candidate switch does not have a password, any entry is ignored.

If multiple candidate 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 6-17](#).

For additional authentication considerations in switch clusters, see the [“TACACS+ and RADIUS” section on page 6-18](#).

**Figure 6-11** Add to Cluster Window

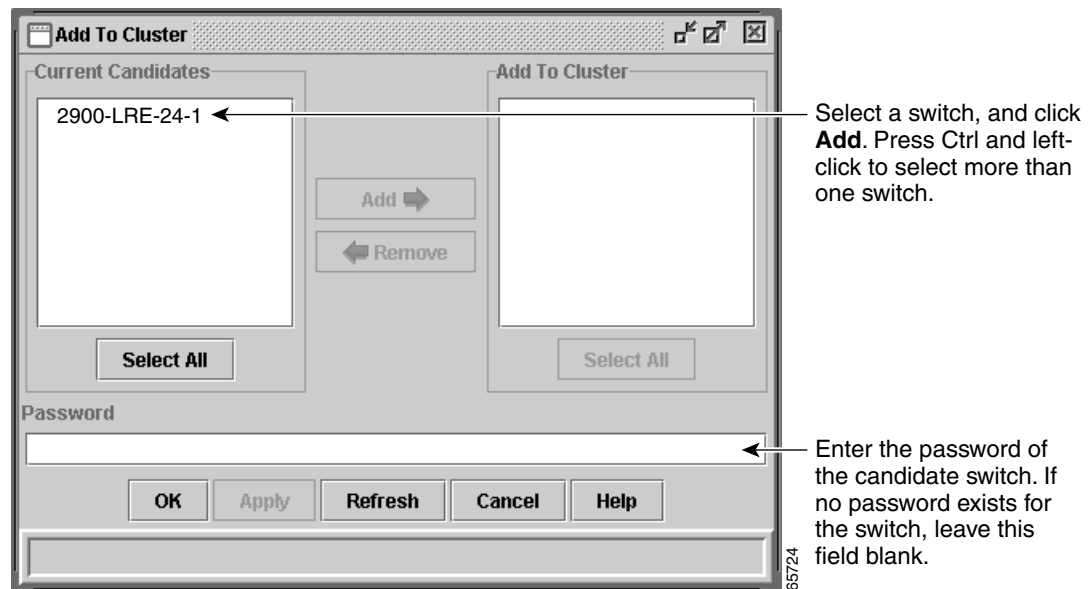
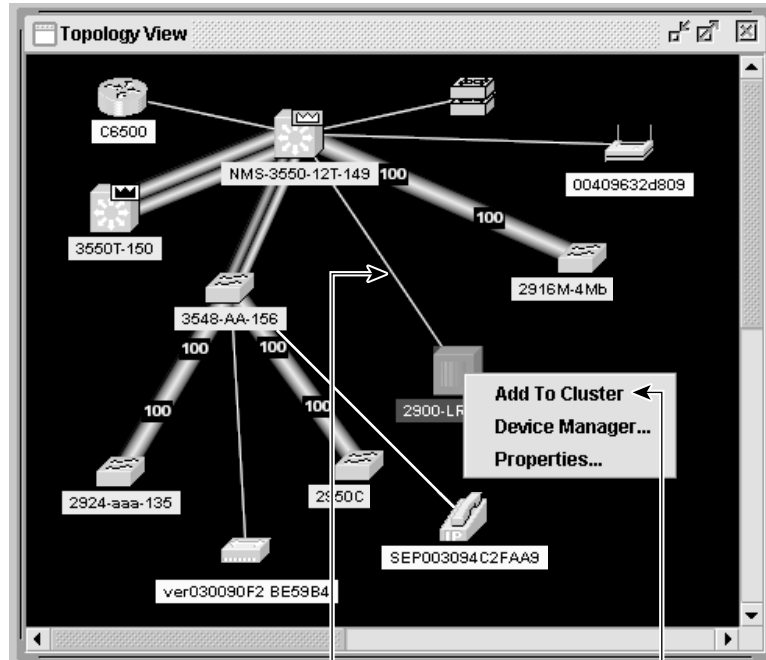


Figure 6-12 Using the Topology View to Add Member Switches



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.

65725

## Creating a Cluster Standby Group

The cluster standby group members must meet the requirements described in the “[Standby Command Switch Characteristics](#)” section on page 6-3 and “[HSRP and Standby Command Switches](#)” section on page 6-13. To create a cluster standby group, select **Cluster > Standby Command Switches** (Figure 6-13).

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

- When the command switch is a Catalyst 3550 switch, all standby command switches must be Catalyst 3550 switches.
- When the command switch is a Catalyst 2950 switch running Release 12.1(9)EA1 or later, all standby command switches must be Catalyst 2950 switches running Release 12.1(9)EA1 or later.
- When the command switch is a Catalyst 2950 switch running Release 12.1(6)EA2 or later, all standby command switches must be Catalyst 2950 switches running Release 12.1(6)EA2 or later.
- When the command switch is running Release 12.0(5)WC2 or earlier, the standby command switches can be these switches: Catalyst 2900 XL, Catalyst 2950, and Catalyst 3500 XL 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 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 31 characters.

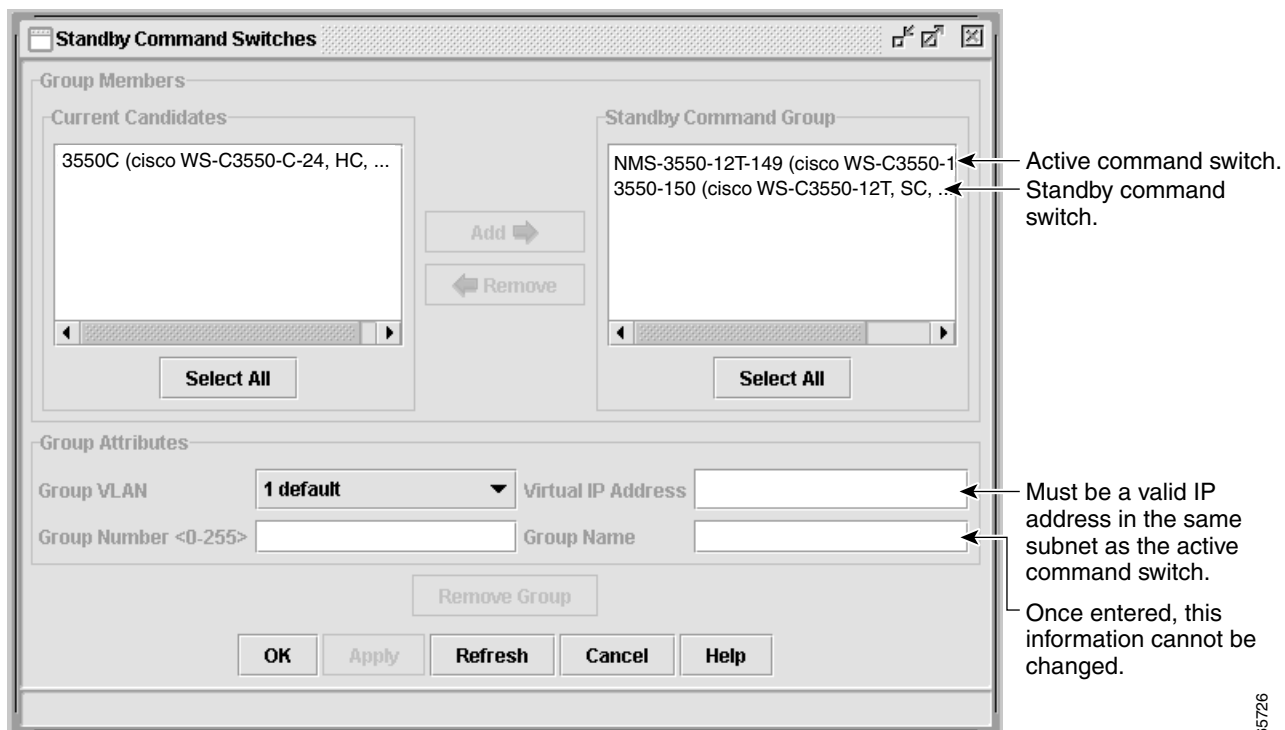
The Standby Command Configuration window uses the default values for the **preempt** and **name** commands that you have set by using the CLI. If you use this window to create the HSRP group, all switches in the group have the **preempt** command enabled. You must also provide a name for the group.



**Note**

The HSRP standby hold time interval should be greater than or equal to 3 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 hello time intervals, refer to the Cisco IOS Release 12.1 documentation set on Cisco.com.

**Figure 6-13 Standby Command Configuration Window**



65726

## Verifying a Switch Cluster

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

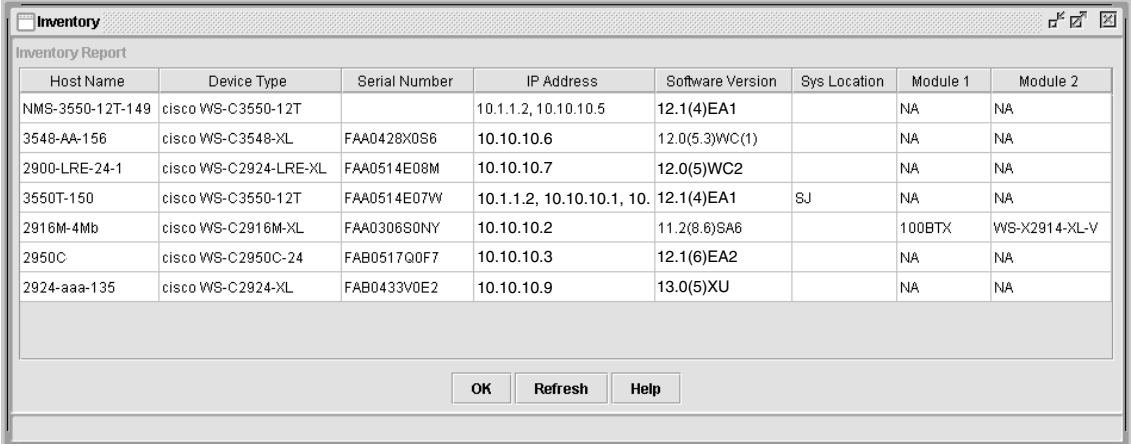
- Step 1** Enter the command switch IP address in the browser **Location** field (Netscape Communicator) or **Address** field (Microsoft Internet Explorer) to access all switches in the cluster.
- Step 2** Enter the command-switch password.
- Step 3** Select **View > Topology** to display the cluster 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 6-14).

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 command switch or use the **show cluster** user EXEC command from the command switch or from a member switch.

**Figure 6-14 Inventory Window**



Host Name	Device Type	Serial Number	IP Address	Software Version	Sys Location	Module 1	Module 2
NMS-3550-12T-149	cisco WS-C3550-12T		10.1.1.2, 10.10.10.5	12.1(4)EA1		NA	NA
3548-AA-156	cisco WS-C3548-XL	FAA0428X0S6	10.10.10.6	12.0(5.3)WC(1)		NA	NA
2900-LRE-24-1	cisco WS-C2924-LRE-XL	FAA0514E08M	10.10.10.7	12.0(5)WC2		NA	NA
3550T-150	cisco WS-C3550-12T	FAA0514E07W	10.1.1.2, 10.10.10.1, 10.	12.1(4)EA1	SJ	NA	NA
2916M-4Mb	cisco WS-C2916M-XL	FAA0306S0NY	10.10.10.2	11.2(8.6)SA6		100BTX	WS-X2914-XL-V
2950C	cisco WS-C2950C-24	FAB0517Q0F7	10.10.10.3	12.1(6)EA2		NA	NA
2924-aaa-135	cisco WS-C2924-XL	FAB0433V0E2	10.10.10.9	13.0(5)XU		NA	NA

If you lose connectivity with a member switch or if a command switch fails, see the “Using Recovery Procedures” section on page 27-1.

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 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. 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** privileged EXEC command on the 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 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 7-5](#).

## 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 command switch is at privilege level 15. If the 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 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 23-5. 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 software on the command switch appends the member switch number (*@esN*, where *N* is the switch number) to the first configured read-write and read-only 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 redirects traps from the member switch to the management station, as shown in [Figure 6-15](#). If a member switch has its own IP address and community strings, the member switch can send traps directly to the management station, without going through the command switch.

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 about SNMP and community strings, see [Chapter 23, “Configuring SNMP.”](#)

**Figure 6-15 SNMP Management for a Cluster**

