



Clustering Switches

- [Understanding Switch Clusters, on page 1](#)
- [Planning a Switch Cluster, on page 3](#)
- [Using the CLI to Manage Switch Clusters, on page 12](#)
- [Using SNMP to Manage Switch Clusters, on page 13](#)

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 Switch 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 Switch can be *cluster member switches*. The total number of Switch in a cluster cannot exceed 16 Switch. The cluster command Switch is the single point of access used to configure, manage, and monitor the cluster member Switch. Cluster members can belong to only one cluster at a time.



Note A Switch cluster is different from a *switch stack*. A switch stack is a set of Catalyst 3750-X, Catalyst 3750-E, or Catalyst 3750 Switch connected through their stack ports.

The benefits of clustering Switch include:

- Management of Catalyst Switch regardless of their interconnection media and their physical locations. The Switch 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 3560, Catalyst 3750, Catalyst 3560-E, Catalyst 3750-E, Catalyst 3560-X, or Catalyst 3750-X Switch as a Layer 3 router between the Layer 2 Switch in the cluster) network.
- Command-switch redundancy if a cluster command Switch fails. One or more Switch 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 Switch.
- Management of a variety of Catalyst Switch 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.

The below table lists the 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.

Table 1: Switch Software and Cluster Capability

Switch	Cisco IOS Release	Cluster Capability
Catalyst 3750-X	12.2(53)SE2 or later	Member or command switch
Catalyst 3750-E	12.2(35)SE2 or later	Member or command switch
Catalyst 3750	12.1(11)AX or later	Member or command switch
Catalyst 3560-X	12.2(53)SE1 or later	Member or command switch
Catalyst 3560-E	12.2(35)SE2 or later	Member or command switch
Catalyst 3560	12.1(19)EA1b or later	Member or command switch
Catalyst 3550	12.1(4)EA1 or later	Member or command switch
Catalyst 2970	12.1(11)AX or later	Member or command switch
Catalyst 2960	12.2(25)FX or later	Member or command switch
Catalyst 2955	12.1(12c)EA1 or later	Member or command switch
Catalyst 2950	12.0(5.2)WC(1) or later	Member or command switch
Catalyst 2950 LRE	12.1(11)JY or later	Member or command switch
Catalyst 2940	12.1(13)AY or later	Member or command switch
Catalyst 3500 XL	12.0(5.1)XU or later	Member or command switch
Catalyst 2900 XL (8-MB switches)	12.0(5.1)XU or later	Member or command switch
Catalyst 2900 XL (4-MB switches)	11.2(8.5)SA6 (recommended)	Member switch only
Catalyst 1900 and 2820	9.00(-A or -EN) or later	Member switch only

Cluster Command Switch Characteristics

A cluster command Switch must meet these requirements:

- It is running a supported software release.
- 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 Switch through the management VLAN and to the cluster member Switch through a common VLAN.

Standby Cluster Command Switch Characteristics

A standby cluster command Switch must meet these requirements:

- It is running a supported software release.
- It has an IP address.

- It has CDP Version 2 enabled.
- It is connected to the command Switch and to other standby command Switch through its management VLAN.
- It is connected to all other cluster member Switch (except the cluster command and standby command Switch) through a common VLAN.
- It is redundantly connected to the cluster so that connectivity to cluster member Switch is maintained.
- It is not a command or member Switch of another cluster.



Note Standby cluster command Switch must be the same type of Switch as the cluster command Switch. For example, if the cluster command Switch is a Catalyst 3750-E Switch, the standby cluster command Switch must also be Catalyst 3750-E Switch. See the switch configuration guide of other cluster-capable Switch for their requirements on standby cluster command Switch.

Candidate Switch and Cluster Member Switch Characteristics

Candidate switches are cluster-capable Switch and Switch stacks that have not yet been added to a cluster. Cluster member Switch 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.

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.
- The **ip http** server global configuration command must be configured on the Switch.
- It is connected to the cluster command Switch through at least one common VLAN.



Note Catalyst 1900, Catalyst 2820, Catalyst 2900 XL, Catalyst 2940, Catalyst 2950, and Catalyst 3500 XL candidate and cluster member Switch must be connected through their management VLAN to the cluster command switch and standby cluster command switches. For complete information about these Switch in a switch-cluster environment, see the software configuration guide for that specific switch. This requirement does not apply if you have a Catalyst 2960, Catalyst 2970, Catalyst 3550, Catalyst 3560, Catalyst 3560-E, Catalyst 3750, Catalyst 3750-E, Catalyst 3650-X, or Catalyst 3750-X cluster command switch. Candidate and cluster member Switch 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.

See 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.



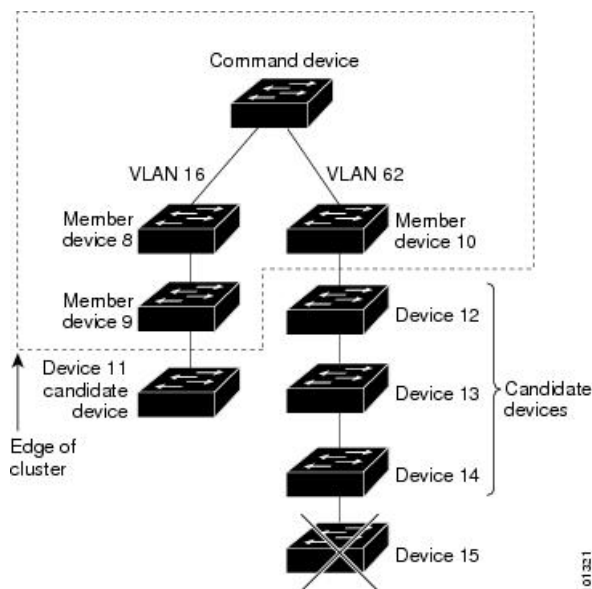
Note Do not disable CDP on the cluster command switch, on cluster members, or on any cluster-capable switches that you might want a cluster command switch to discover.

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 the Figure are at the edge of the cluster.

In the Figure below, 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 1: Discovery Through CDP Hops



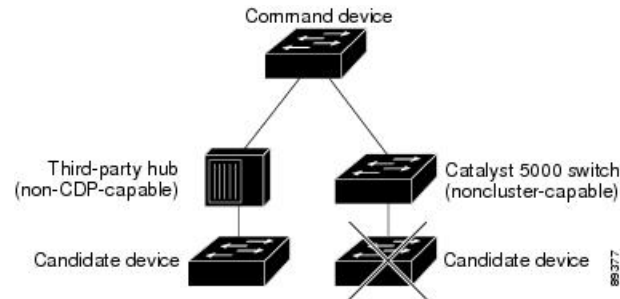
Discovery Through Non-CDP-Capable and Noncluster-Capable Devices

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.

Below figure 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 2: Discovery Through Non-CDP-Capable and Noncluster-Capable Devices



Discovery Through Different VLANs

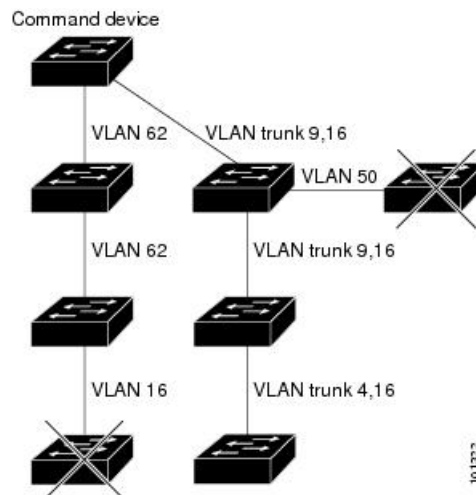
If the cluster command switch is a Catalyst 3560-E, Catalyst 3750-E, Catalyst 3560-X, or Catalyst 3750-X switch, the cluster can have cluster member switches in different VLANs. As cluster member switches, they must be connected through at least one VLAN in common with the cluster command switch. The cluster command switch in the figure as 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.



Note For additional considerations about VLANs in switch stacks, see the section “Switch Clusters and Switch Stacks”.

Figure 3: Discovery Through Different VLANs



Discovery Through Different Management VLANs

Catalyst 2960, Catalyst 2970, Catalyst 3550, Catalyst 3560, Catalyst 3560-E, Catalyst 3750, Catalyst 3750-E, Catalyst 3560-X, or Catalyst 3750-X 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.

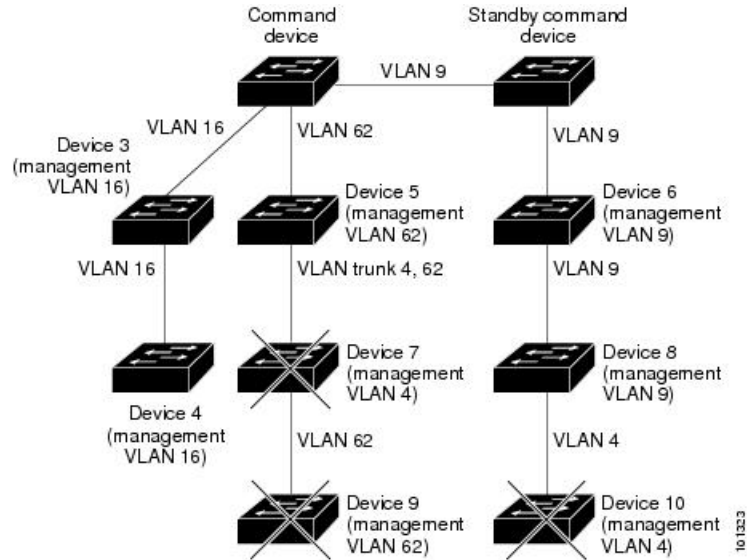


Note If the switch cluster has a Catalyst 3750-E or Catalyst 3750-X switch or switch stack, that switch or switch stack must be the cluster command switch.

The cluster command switch and standby command switch in the figure (assuming they are Catalyst 2960, Catalyst 2970, Catalyst 3550, Catalyst 3560, Catalyst 3560-E, Catalyst 3750, Catalyst 3750-E, Catalyst 3560-X, or Catalyst 3750-X cluster command switches) 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 4: Discovery Through Different Management VLANs with a Layer 3 Cluster Command Switch



Discovery of Newly Installed Switches

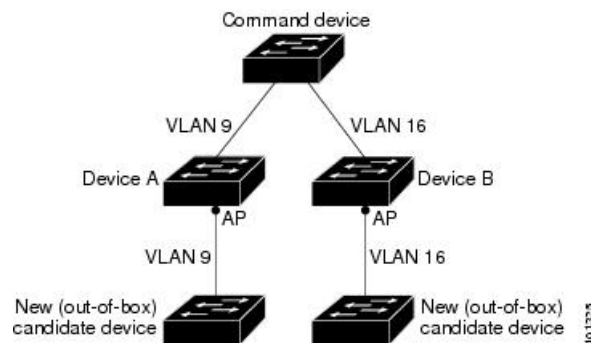
To join a cluster, the new, out-of-the-box switch must be connected to the cluster through one of its access ports. An access port (AP) carries the traffic of and belongs to only one VLAN. By default, the new switch and its access ports are assigned to VLAN 1.

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 the Figure 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 5: 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. Only one cluster standby group can be assigned per cluster.



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. 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.

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 decide 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.

Other Considerations for Cluster Standby Groups

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-E or Catalyst 3750-X switch, the standby cluster command switches must also be Catalyst 3750-E or Catalyst 3750-X switches. See the switch configuration guide of other cluster-capable switches for their requirements on standby cluster command switches.

If your switch cluster has a Catalyst 3750-X switch or a switch stack, it should be the cluster command switch. If not, when the cluster has a Catalyst 3750-E switch or switch stack, that switch 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 re-enable it by using the CLI.

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

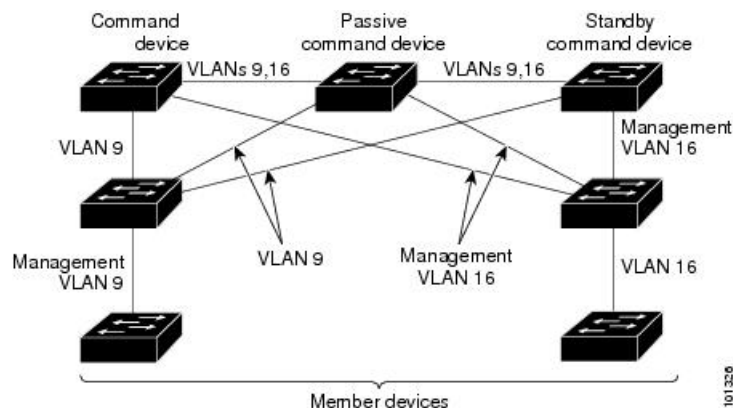


Note There is no limit to the number of switches that you can assign as standby cluster command switches. However, the total number of switches in the cluster—which would include the active cluster command switch, standby-group members, and cluster member switches—cannot be more than 16.

- Each standby-group member (Figure below) must be connected to the cluster command switch through the same VLAN. In this example, the cluster command switch and standby cluster command switches are Catalyst 3560-E, Catalyst 3750-E, Catalyst 3560-X, or Catalyst 3750-X cluster command switches. 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.

Figure 6: 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 2960, Catalyst 2970, Catalyst 3550, Catalyst 3560, Catalyst 3560-E, Catalyst 3560-X, Catalyst 3750, Catalyst 3750-E, and Catalyst 3750-X 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 must assign an IP address to manage it as a standalone switch.

Hostnames

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

If a switch joins a cluster and it does not have a hostname, the cluster command switch appends a unique member number to its own hostname 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 hostname, it retains that name when it joins a cluster and when it leaves the cluster.

If a switch received its hostname 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 switch overwrites the old hostname (such as *eng-cluster-5*) with the hostname 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 password considerations specific to the Catalyst 1900 and Catalyst 2820 switches, see 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 SNMP considerations specific to the Catalyst 1900 and Catalyst 2820 switches, see the installation and configuration guides specific to those switches.

TACACS+ and RADIUS

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 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.

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.

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 Cisco 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, see the switch command reference.

The Telnet session accesses the member-switch CLI at the same privilege level as on the cluster command switch. The Cisco IOS commands then operate as usual.



Note The CLI supports creating and maintaining switch clusters with up to 16 switch stacks.

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, see 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”. 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 the Figure. 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.

Figure 7: SNMP Management for a Cluster

