Planning and Creating Clusters

This chapter provides the concepts and procedures to plan and create clusters with Network Assistant. For information on using Network Assistant to configure clusters, refer to its online help.

Note You can also create clusters through the command-line interface (CLI), but less easily. For the CLI cluster commands, refer to the command reference for the command device.

Planning a Cluster

This section describes the guidelines, requirements, and caveats that you should understand before you create a cluster:

Command Device Characteristics

A command device must meet these requirements:

- It has an IP address.
- Clustering and the HTTP server are enabled (the default except on Catalyst 4500 series switches).
- Cisco Discovery Protocol (CDP) version 2 is enabled (the default).
- It is not a command device or a member in another cluster.
- It is connected to standby command devices through the management VLAN and to cluster members through a common VLAN.

Note Standby command devices are not required in a cluster, and they are not supported by Catalyst 4500 series switches.

Standby Command Device Characteristics

A standby command device must meet these requirements:

- It has an IP address.
- It has CDP version 2 enabled.

- It is connected to the command device and to other standby command devices through its management VLAN.
- It is connected to all other cluster members through a common VLAN.
- It is redundantly connected to the cluster so that connectivity to members is maintained.
- It is not a command device or a member in another cluster.

Standby command devices must be the same type of device as the command device. For example, if the command device is a Catalyst 3750 switch, the standby command devices must also be Catalyst 3750 switches. If you want to maintain the same level of feature support when a standby command device takes over, it should run the same release of Cisco IOS that the command device runs.

Candidate and Member Characteristics

Candidates are cluster-capable devices that have not yet been added to a cluster. Members are devices that have actually been added to a cluster. Although not required, a candidate or member can have its own IP address and password.

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

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

Note Catalyst 2900 XL, Catalyst 2950, and Catalyst 3500 XL candidates and members must be connected through their management VLAN to the command device and the standby command devices.

This requirement does not apply if you have a Catalyst 2970, Catalyst 3550, Catalyst 3560, Catalyst 3750, or Catalyst 4500 command device. Candidates and members can connect through any VLAN in common with the command device.

A Catalyst 4500 switch can be a cluster member only if another Catalyst 4500 switch is the command device.

Automatic Discovery of Candidates and Members

The command device uses CDP to discover members, candidates, neighboring clusters, and edge devices across multiple VLANs and in star or cascaded topologies.

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

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

- Discovery through CDP Hops, page 4-3
- Discovery through Non-CDP-Capable and Noncluster-Capable Devices, page 4-4
- Discovery through Different VLANs, page 4-5
- Discovery through Different Management VLANs, page 4-5
- Discovery through Routed Ports, page 4-6
- Discovery of Newly Installed Devices, page 4-7

Discovery through CDP Hops

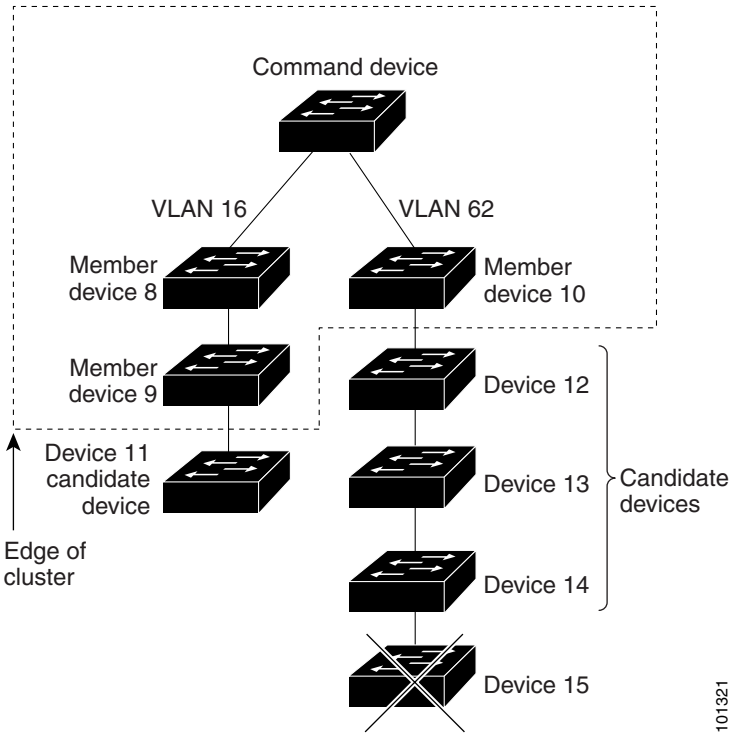
By using CDP, a command device can discover devices up to seven CDP hops away (the default is three hops) from the edge of the cluster. The edge of the cluster is where the last members are connected to the cluster and to candidate devices. For example, members 9 and 10 in Figure 4-1 are at the edge of the cluster.

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

Note A stack in a cluster functions as a single member device. See the "Clusters and Stacks" section on page 4-11 if you plan to use a stack in a cluster.

In Figure 4-1, the command device has ports assigned to VLANs 16 and 62. The CDP hop count is three. The command device discovers devices 11, 12, 13, and 14 because they are within three hops from the edge of the cluster. It does not discover device 15 because it is four hops from the edge of the cluster.

Figure 4-1 Discovery through CDP Hops

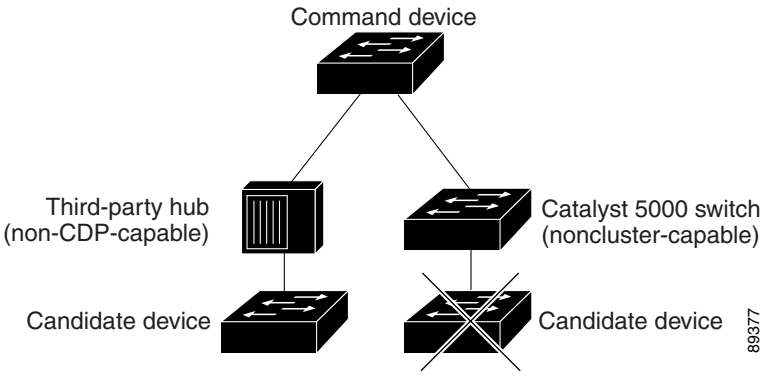


Discovery through Non-CDP-Capable and Noncluster-Capable Devices

If a command device 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 hub. However, if the command device is connected to a *noncluster-capable Cisco device*, it cannot discover a cluster-enabled device connected beyond the noncluster-capable Cisco device.

Figure 4-2 shows that the command device discovers the device that is connected to a third-party hub. However, the command device does not discover the device that is connected to a Catalyst 5000 switch.

Figure 4-2 Discovery through Non-CDP-Capable and Noncluster-Capable Devices



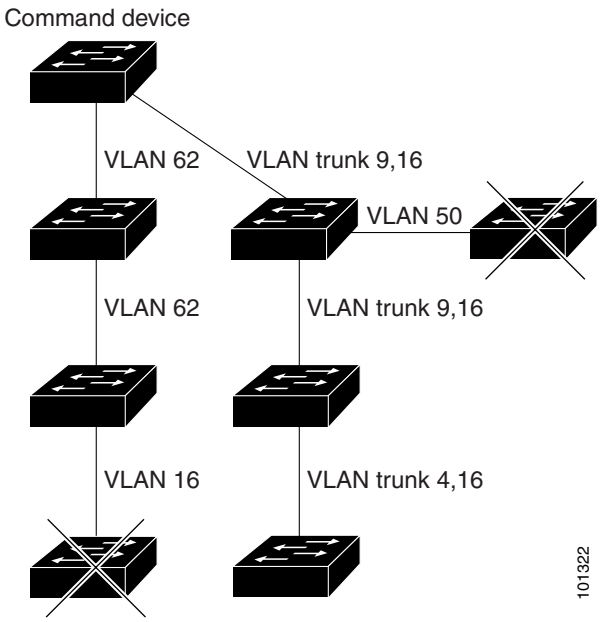
Discovery through Different VLANs

If the command device is a Catalyst 2970, Catalyst 3550, Catalyst 3560, Catalyst 3750, or Catalyst 4500 switch, the cluster can have members in different VLANs. As members, they must be connected through at least one VLAN in common with the command device. The command device in Figure 4-3 has ports assigned to VLANs 9, 16, and 62 and therefore discovers the devices in those VLANs. It does not discover the device in VLAN 50. It also does not discover the device in VLAN 16 in the first column because the command device has no VLAN connectivity to it.

Catalyst 2900 XL, Catalyst 2950, and Catalyst 3500 XL members must be connected to the command device through their management VLAN. For information about discovery through management VLANs, see the "Discovery through Different Management VLANs" section on page 4-5.

Note For additional considerations about VLANs in stacks, see the "Clusters and Stacks" section on page 4-11.

Figure 4-3 Discovery through Different VLANs



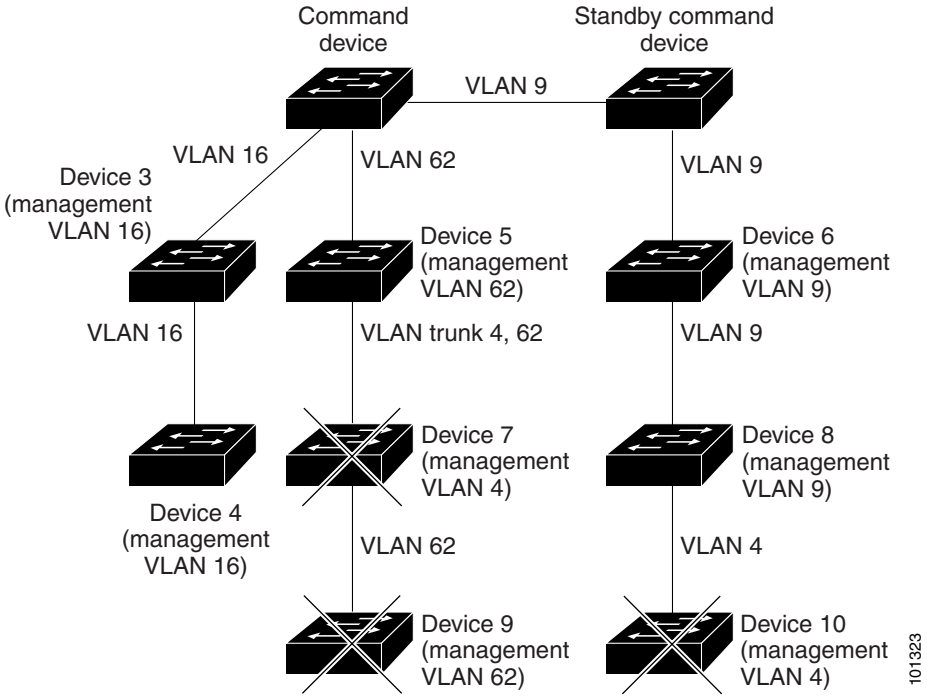
Discovery through Different Management VLANs

As command devices, Catalyst 2970, Catalyst 3550, Catalyst 3560, Catalyst 3750, and Catalyst 4500 switches can discover and manage members in different VLANs and different management VLANs. As members, they must be connected through at least one VLAN in common with the command device. They do not need to be connected to the command device through their management VLAN. The default management VLAN is VLAN 1.

The command device and standby command device in Figure 4-4 (assuming they are Catalyst 2970, Catalyst 3550, Catalyst 3560, Catalyst 3750, or Catalyst 4500 switches) have ports assigned to VLANs 9, 16, and 62. The management VLAN on the command device is VLAN 9. Each command device discovers the devices in the different management VLANs except these:

- Devices 7 and 10 (devices in management VLAN 4) because they are not connected through a common VLAN (meaning VLANs 62 and 9) with the command device
- Device 9 because automatic discovery does not extend beyond a noncandidate, which is device 7

Figure 4-4 Discovery through Different Management VLANs

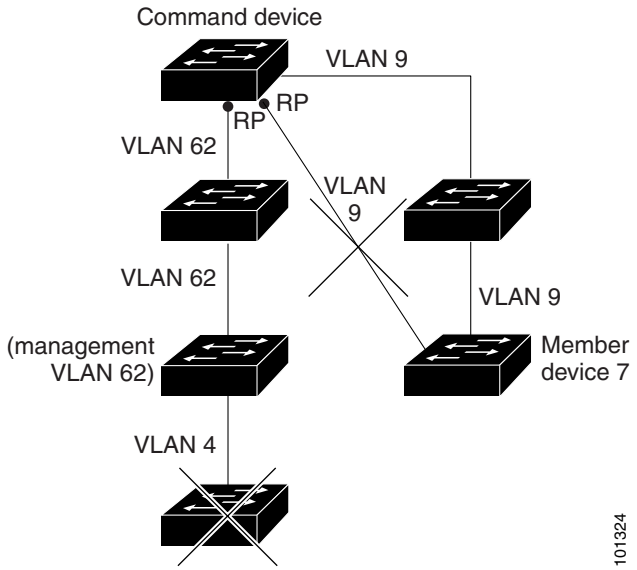


Discovery through Routed Ports

If the command device has a routed port (RP) configured, it discovers only candidates and members in the *same* VLAN as the routed port.

The Layer 3 command device in Figure 4-5 can discover the devices in VLANs 9 and 62 but not the device in VLAN 4. If the routed port path between the command device and member 7 is lost, the redundant path through VLAN 9 maintains connectivity with member 7.

Figure 4-5 Discovery through Routed Ports



Discovery of Newly Installed Devices

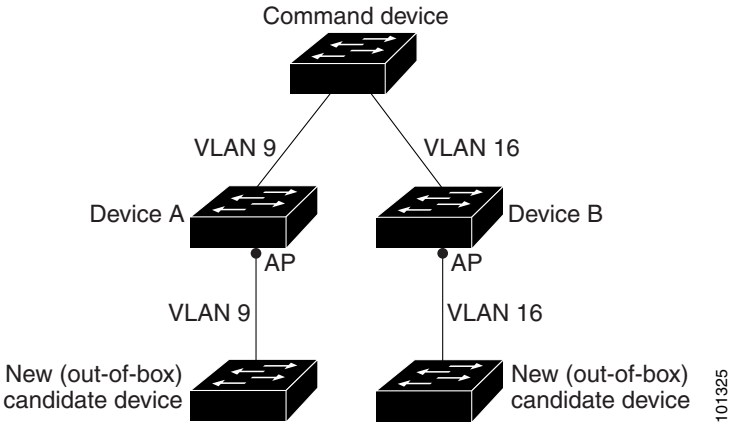
To join a cluster, a new, out-of-the-box device must be connected to the cluster through one of its access ports. An access port (AP) carries the traffic of and belongs to only one VLAN. By default, the new device and its access ports are assigned to VLAN 1.

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

The command device in Figure 4-6 belongs to VLANs 9 and 16. When new cluster-capable devices join the cluster:

- One cluster-capable device and its access port are assigned to VLAN 9.
- The other cluster-capable device and its access port are assigned to management VLAN 16.

Figure 4-6 Discovery of Newly Installed Devices



HSRP and Standby Command Devices

You can configure a group of standby command devices on devices that support Hot Standby Router Protocol (HSRP). Because a command device manages the forwarding of all communication and configuration information to all the members, we strongly recommend the following:

- If the command device is a stack, configure a standby command device to take over in case the entire stack fails. (If only the stack master fails, the stack elects a new stack master, and the stack resumes its role as the command device.)
- If a command device is a standalone device, configure a standby command device to take over if the command device fails.

Devices in the standby group are ranked according to HSRP priorities. The device with the highest priority in the group is the *active command device*. The device with the next highest priority is the *standby command device*. The other devices in the standby group are the *passive command devices*. If the active command device and the standby command device fail *at the same time*, the passive command device with the highest priority becomes the active command device.

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.

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

- Virtual IP Addresses, page 4-8
- Other Considerations for Standby Groups, page 4-9
- Automatic Recovery of Cluster Configuration, page 4-10

Virtual IP Addresses

You must assign a unique virtual IP address and group number and name to the standby group. Configure this information on a specific VLAN or a routed port on the active command device. The active command device receives traffic destined for the virtual IP address. To manage the cluster, you must access the active command device through the virtual IP address, not through the command-device IP address. This is in case the IP address of the active command device is different from the virtual IP address of the standby group.

If the active command device fails, the standby command device assumes ownership of the virtual IP address and becomes the active command device. The passive devices in the standby group compare their assigned priorities to decide the new standby command device. The passive standby device with the highest priority then becomes the standby command device. If the previously active command device becomes active again, it resumes its role as the active command device, and the current active command device again becomes the standby command device. For more information about IP addresses in device clusters, see the "IP Addresses" section on page 4-10.

Other Considerations for Standby Groups

These requirements also apply:

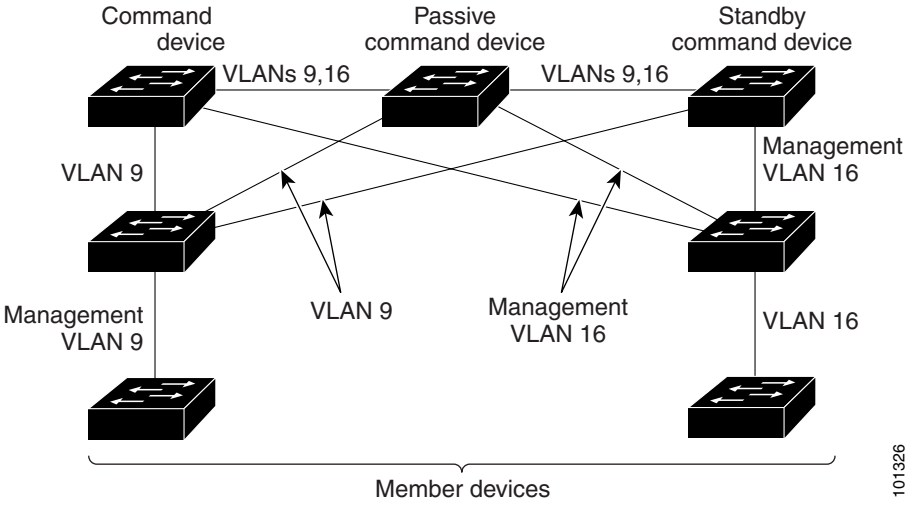
- Standby command devices must be the same type of device as the command device. For example, if the command device is a Catalyst 3750 switch, the standby command devices must also be Catalyst 3750 switches.
- Only one standby group can be assigned to a cluster. You can have more than one router-redundancy standby group.

  An HSRP group can be both a standby group and a router-redundancy group. However, if a router-redundancy group becomes a standby group, router redundancy becomes disabled on that group.
- All standby-group members must be members of the cluster.

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

- Each standby-group member (Figure 4-7) must be connected to the command device through the same VLAN. In this example, the command device and standby command devices are Catalyst 2970, Catalyst 3550, Catalyst 3560, or Catalyst 3750 command switches. Each standby-group member must also be redundantly connected to each other through at least one VLAN in common with the cluster.

Figure 4-7 VLAN Connectivity between Standby-Group Members and Other Members



Note For additional considerations about standby groups in stacks, see the "Clusters and Stacks" section on page 4-11.

Automatic Recovery of Cluster Configuration

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

Automatic discovery has these limitations:

- (This limitation applies only to clusters that have Catalyst 2950, Catalyst 3550, Catalyst 3560, and Catalyst 3750 command and standby devices command devices.) If the active command device and the standby command device fail *at the same time*, the passive command device with the highest priority becomes the active command device. However, because it was a passive standby command device, the previous command device *did not* forward cluster-configuration information to it. The active command device only forwards cluster-configuration information to the standby command device. You must therefore rebuild the cluster.
- If the active command device fails and there are more than two devices in the cluster standby group, the new command device does not discover Catalyst 2916M XL members. You must re-add these members to the cluster.
- If the active command device fails and becomes active again, it does not discover Catalyst 2916M XL members. You must re-add these members to the cluster.

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

IP Addresses

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

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

You can assign an IP address to a cluster-capable device, but it is not necessary. A member is managed and communicates with other members through the command-device IP address. If a member 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 device.

Note Changing the IP address of the command device ends your Network Assistant session on the device.

Host Names

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

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

If a device 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 device received its host name from the command device, was removed from the cluster, and was added to a new cluster with 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 device in the new cluster (such as *mkg-cluster-5*). If the member number changes in the new cluster (such as *3*), the device retains the previous name (*eng-cluster-5*).

Passwords

You do not need to assign passwords to a device if it will be a cluster member. When a device joins a cluster, it inherits the command-device password and retains it when it leaves the cluster. If no command-device password is configured, the member inherits a null password. Members only inherit the command-device password.

If you change the member password to be different from the command-device password and save the change, the member cannot be managed by the command device until you change the member password to match the command-device password. Rebooting the member does not change the password back to the command-device password. We recommend that you do not change the member password after it joins a cluster.

SNMP Community Strings

A member inherits the first read-only (RO) and read-write (RW) community strings of the command device, with *@esN* appended to the community strings. *N* is the member number.

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

Clusters and Stacks

A cluster can have one or more Catalyst 3750 stacks. Each stack can act as the command device or as a single member. Table 4-1 compares stacks and clusters.

Table 4-1 Comparison of Stacks and Clusters

Stack	Cluster
Made up of only Catalyst 3750 switches.	Made up of cluster-capable devices, such as Catalyst 2950, Catalyst 3550, Catalyst 3750, and Catalyst 4500 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 command device and supports up to 15 other members.
Can be a command device or a member.	Cannot be a stack master or stack member.

Table 4-1 Comparison of Stacks and Clusters (continued)

Stack	Cluster
Stack master is the single point of *complete* management for all stack members.	Command device is the single point of *some* management for all members of a cluster.
Back-up stack master is automatically determined in case the stack master fails.	Standby command device must be pre-assigned in case the command device fails. **Note** This does not apply if a Catalyst 4500 switch is the command device.
Supports up to eight simultaneous stack master failures.	Supports only one command device failure at a time.
Stack members behave and are presented as a single, unified system in the network.	Cluster members are independent devices that are neither managed as nor behave as a unified system.
Integrated management of stack members is through a single configuration file.	Each member has its own configuration file.
Stack- and interface-level configurations are stored on each stack member.	Cluster configuration is stored on the command device and the standby command device.
New stack members are automatically added to the stack.	New members are manually added to the cluster.

Stack members work together to behave as a unified system in the network and are presented to the network as such by Layer 2 and Layer 3 protocols. Therefore, a cluster recognizes an entire stack as an eligible cluster member. Individual stack members cannot join a cluster or participate as separate members. Because a cluster must have 1 command device and can have up to 15 members, a cluster can potentially have up to 16 stacks, totalling 144 devices.

Stacks are configured through the stack master.

Note From the CLI, you can configure a cluster to contain up to 16 stacks. However, from Network Assistant, the maximum number of devices in a cluster is 16, counting the individual devices in a stack. For example, Network Assistant counts a stack with three stack members as three separate devices.

If you use the CLI to configure a cluster of more than 16 actual devices and then try to display the cluster from Network Assistant, you will have to remove members until the Network Assistant limit of 16 separate devices is reached.

Keep these considerations in mind if you have stacks in clusters:

- If the command device is not a Catalyst 3750 switch or a stack and a new stack master is elected, the stack loses its connectivity to the cluster if there are no redundant connections between the stack and the command device. You must add the stack to the cluster.
- If the command device is a stack and new stack masters are simultaneously elected in that stack and in member stacks, connectivity between the stacks is lost if there are no redundant connections between them. You must add the stacks to the cluster, including the stack that is the command device.
- All stack members should have redundant connectivity to all the VLANs in the 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 cluster. You must change the VLAN configuration of the stack master or the stack members and add the stack members back to the cluster.

- If a stack in the role of a member reloads and a new stack master is elected, the stack loses connectivity with the command device. You must add the stack back to the cluster.
- If a stack that is acting as the command device reloads and the original stack master is not re-elected, you must rebuild the entire cluster.

TACACS+ and RADIUS

Inconsistent authentication configurations in clusters cause Network Assistant to continually prompt for a username and password. If TACACS+ is configured on a member, it must be configured on all members. Similarly, if RADIUS is configured on a member, it must be configured on all members. Further, the same cluster cannot have some members configured with TACACS+ and other members configured with RADIUS.

Access Modes in Network Assistant

Some configuration windows display incomplete information if you have read-only access to a cluster with these devices and Cisco IOS releases:

- Catalyst 2900 XL or Catalyst 3500 XL members running Cisco IOS Release 12.0(5)WC2 or earlier

Note Catalyst 2900 XL switches with 4-MB CPU DRAM do not support read-only mode.

- Catalyst 2950 members running Cisco IOS Release 12.0(5)WC2 or earlier
- Catalyst 3550 members running Cisco IOS Release 12.1(6)EA1 or earlier

In read-only mode, these devices appear as unavailable and cannot be configured from Network Assistant.

LRE Profiles

A configuration conflict occurs if a 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.

Creating a Cluster

To create a cluster, you enable a command device and add cluster members. To ensure that you have a backup command device in case the primary one fails, you should also create a standby group. Finally, you should verify that the cluster contains the devices that you think it contains. This section tells you how to perform these tasks.

Note Refer to the release notes for the list of devices eligible for clustering, including which ones can be command devices and which ones can only be members.

Enabling a Command Device

Follow these steps to enable a command device:

1. During the setup of the device, assign an IP address and a password to the device. For information about using the setup program, refer to the release notes.
2. Launch Network Assistant, and enter the assigned IP address in the Connect window.
3. Choose **Cluster > Create Cluster** on the feature bar.
4. Use the Create Cluster window to enter a cluster number (the default is 0) and a cluster name.

Adding Cluster Devices

There are two ways to add members to a cluster. The first uses the Add to Cluster window:

1. On the feature bar, choose **Cluster > Add to Cluster** to open the Add to Cluster window.
2. Select a candidate device from the list, click **Add**, and click **OK**.

   To add more than one candidate, press **Ctrl** and make your choices, or press **Shift** and choose the first and last switch in a range.

The second way uses the Topology view:

1. If the Topology view is not displayed, choose **View > Topology** from the feature bar.
2. Right-click a candidate icon, and select **Add to Cluster**.

   Candidates are cyan; members are green. To add more than one candidate, press **Ctrl** and left-click the candidates that you want to add.

You can select 1 or more devices so long as the total number of devices in the cluster does not exceed 16 (including the command device). 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 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 have the same password, you can select them as a group and add them at the same time. If a candidate in the group has a different password from the others, it is not added to the cluster with the others.

When a candidate joins a cluster, it inherits the command-device password.

Creating a Standby Group

Standby group members must meet the requirements described in the "Standby Command Device Characteristics" section on page 4-1 and the "HSRP and Standby Command Devices" section on page 4-8.

Note The Catalyst 4500 series switch does not support standby groups.

Follow these steps to create a standby group:

1. From the feature bar, choose **Cluster > Standby Command Devices**, and use the Standby Command Devices window.
2. Enter a virtual IP address for the standby group. It must be in the same subnet as the IP addresses of the device.
3. Enter a group number that is unique within the IP subnet.
4. Enter a group name of up to 31 characters.

Verifying a Cluster

Follow these steps to verify the cluster:

1. Choose **View > Topology** to display the Topology view.
2. Choose **Reports > Inventory** to display an inventory of the devices in the cluster.

   This summary includes device model numbers, serial numbers, software versions, IP information, and location.
3. Display port and device statistics from **Reports > Port Statistics** and **Port > Port Settings > Runtime Status**.