



Configuring Network Elements

This chapter describes how to configure the BBSM-supported network device types: access points, switches, and CMTSs. To configure the network devices, you must first configure at least one site. Refer to [Chapter 11, “Configuring Routers.”](#)

These sections describe the network types and how to configure them:

- [Switch Clustering, page 12-2](#)
- [Configuring Access Points, page 12-2](#)
- [Adding and Configuring CMTSs, page 12-7](#)
- [Configuring Switches, page 12-13](#)



Caution

The SNMP password located in WEBconfig under Network Elements must match the SNMP read-write community string that is configured in the network device software. If the BBSM password does not match the community string (password), BBSM cannot communicate with or locate end users connected to the network device. To change the network device SNMP read-write community string, follow the manufacturer’s instructions.



Note

When BBSM is trying to locate the port to which a client is connected, BBSM sequentially queries each configured network device, looking for the client’s MAC address. When BBSM locates the client, it stops querying the network devices and displays the appropriate page set Connect page on the client’s browser.

If a configured network device does not respond to the BBSM query, BBSM times out on the query after a while and then retries the query and times out again. As a result, nonresponsive network devices greatly increase the time BBSM takes to locate clients on network devices that follow the nonresponsive network devices in the BBSM search order.

To prevent this unnecessary delay in client search logic, simply disable each nonresponsive network device using the Webconfig Network Elements web pages. When the nonresponsive network devices are connected and functioning correctly, enable them again on the Webconfig Network Elements pages.

Switch Clustering

Cisco switch clustering technology is supported as of BBSM 5.2. A switch cluster comprises up to 16 switches that are managed using just one IP address. The administrator can update the WEBconfig Switches page using only the master switch IP address and a unique SNMP read-write community string (password) for each switch in the cluster.

Some of the switches that support switch clustering are the Catalyst 1900, 2900 XL, 2950, 3500, and 3550 XL switches. The list changes frequently as Cisco releases new switches that are added to BBSM.



Note

Before running the Switch Discovery Wizard or configuring clustered switches in WEBconfig, you must enable the switch clustering capability for all cluster-capable switches. For detailed information, refer to your switch documentation.

Configuring Access Points

This section provides basic information about using access points, including authentication, and the procedure to configure them in WEBconfig.

Overview

Cisco Aironet access points are wireless LAN transceivers that serve as the center point of a stand-alone wireless network or as the connection point between wireless and wired networks. The port-hopping feature in BBSM enables a user to move among access points in a LAN if the user moves within the configurable period of the hop timer. In large installations, wireless users within radio range of an access point can roam throughout a facility while maintaining seamless, uninterrupted access to the network. The roaming functionality is based on signal quality, not proximity. When a client's signal quality drops, the client roams to another access point.

To make the access point work with BBSM, the access point must be online and able to receive a ping from the BBSM server. Then you configure the access point in WEBconfig. (For BBSM 5.0, choose **Generic without Link Status** for the access point. The access point appears as two ports—the uplink port and a client port. If the access point appears as 30 ports, you have the newer access point firmware.)

To handle several client connections in a wireless LAN, BBSM polls the bridge MIB on the access point to detect client MAC addresses just as it polls the MIB on a switch.

The following are common topics of interest about using access points:

- **EAP and LEAP**—Entering the IP addresses of the wireless access points and switches allows the full Extensible Authentication Protocol (EAP) and Light EAP (LEAP) authentication traffic to pass through the BBSM server. (Refer to the bulleted section below on wireless hotspots.)
- **Roaming**—If a client's signal to a distant access point remains strong, the client does not roam to a closer access point. If client devices checked continuously for closer access points, the extra radio traffic would slow throughput on the wireless LAN.
- **Segmenting users**—Wireless meeting room users can be segmented from public space users. These are the options:
 - **No wireless cell overlay**—Dedicate access points with meeting room page sets and public space access points with the RADIUS, credit card, or other page sets.

- **Wireless cell overlay**—Account for overlap and use the Mega page set. Meeting room clients use access codes while public space clients use RADIUS and credit cards, for example. This configuration allows for overlapping wireless cells to be used by both meeting room and public space clients. At the same time, bandwidth is being controlled.

Depending on the firmware version of the Cisco access point, the association of service set identifiers (SSIDs) and VLANs is supported. For example, different types of users can be assigned to different VLANs; the visitor VLAN can go to BBSM, and the enterprise user VLAN can bypass BBSM.

- **Wireless hotspots**—Use Cisco Aironet access points to deploy wireless hotspots. (These access points support open authentication through the use of an SSL certificate.)
- **Security with LEAP and Wired Equivalent Privacy (WEP)**—When access points at a hotspot have an open-air link to clients, eavesdroppers can tap into the traffic being transmitted very easily. Using IPSec 3DES VPN connections to the enterprise typically addresses these security concerns. However, mobile end user must first authenticate with BBSM through the unprotected link. For this reason, you can choose whether or not to use SSL-protected BBSM page sets to secure the connection between the end user and the server.
- **Disabling inter-client communication with PSPF**—Inter-client communication on Cisco switches is blocked by enabling the protected port feature on client ports and enabling Publicly Secure Port Forwarding (PSPF) on Cisco Aironet access points. For additional information, refer to the Cisco documentation for the applicable access point.
- **Disconnecting**—When the user ends a wireless session without disconnecting and multiple users are connected to a single access point, the access point has a table of MAC addresses for each connected client and a corresponding timer. When there is no activity, a timer counts down to zero from a preconfigured time period. The next time BBSM polls the access point, the server finds that the MAC has timed out and marks the client as disconnected. The user gets charged only for the actual connected time.

For additional information about Cisco wireless LAN products, refer to this website:

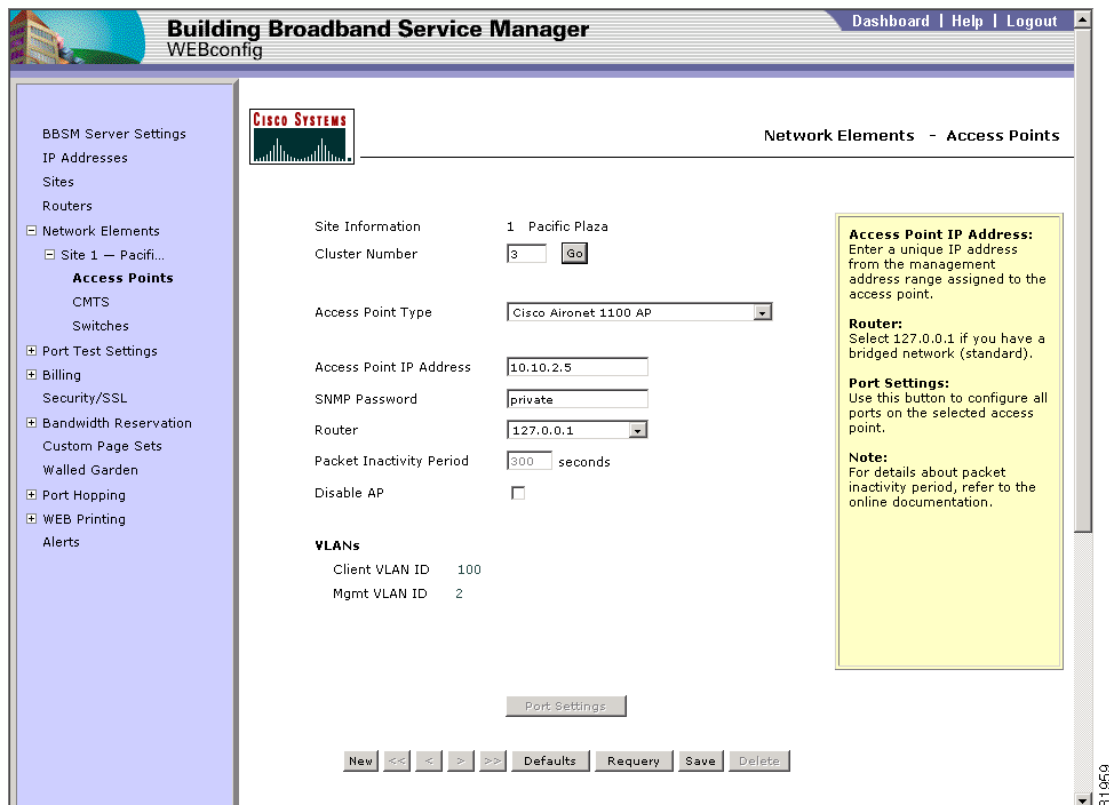
<http://www.cisco.com/en/US/products/hw/wireless/index.html>

Access Point Configuration Procedure

Follow this procedure to configure each access point in WEBconfig.

- Step 1** From the Dashboard, click **WEBconfig**. The BBSM Server Settings web page appears.
- Step 2** In the NavBar, navigate to the Access Points web page by choosing **Network Elements > Site x > Access Points**. The Access Points web page appears. (See [Figure 12-1](#).)

Figure 12-1 Access Points Web Page (Singlenet, Single VLAN)



- Step 3** Configure the access points based on the information shown in [Table 12-1](#) and click **Save**. The Network Element Port Settings window pops up. (See [Figure 12-2](#).)



Note If port configuration records already exist, the Network Element Port Settings window does not pop up automatically. Click **Port Settings**.

- Step 4** Enter the information in the Network Element Port Settings window based on the information in [Table 12-2](#) and click **Submit**. A dialog box appears, asking you to verify your changes. Click **OK** and you are returned to the Access Points web page.



Note If you add or remove a default VLAN for your access point, you must reconfigure the access point. To do this, click **Submit** in the Network Element Port Settings window. For more information on VLANs, refer to the [“VLANs” section on page 2-1](#).

Table 12-1 Access Points Web Page Options


Field	Description
Site Information	Displays the site number, site name associated with the access points to be configured.
Cluster Number Go	Displays the cluster number associated with the access point to be configured. Click Go to advance to any cluster number that has been configured in WEBconfig. This is a more convenient way to access records than using the < or > buttons to advance one record at a time.
Access Point Type	From the drop-down menu, choose an access point type.
Access Point IP Address	Enter a unique IP address in the management range assigned to the access point.
SNMP Password	Enter the SNMP read-write community string (password) that is used when communicating with the access point. The default is <i>private</i> .  Caution Cisco recommends that you change the default password on the access points because the default password is well known and could compromise network security.
Router	From the drop-down menu, choose the IP address of the router that this access point is connected to. If the site and cluster are directly connected to the BBSM server, use the default IP address for the BBSM server, which is <i>127.0.0.1</i> .
Packet Inactivity Period	Note This field is disabled unless your access point type supports packet inactivity. Enter the time, in seconds, that a user can be idle before being automatically signed off by BBSM. If needed, refer to the <i>Cisco BBSM Products Network Device Compatibility Guide</i> to verify the access points that monitor for packet inactivity.
Disable AP	Check this check box if you do not want BBSM to look for clients on the ports for the access point. Use when troubleshooting. Note Even if you disable an access point, its IP address remains reserved. If you need to reuse the IP address for a different network device, change the IP address of the disabled access point.
VLANs (These fields apply only when two VLANs are configured.)	
Clients VLAN ID	Displays the client VLAN ID.
Mgmt VLAN ID	Displays the management VLAN ID.
Buttons	
Port Settings	Configures the access point ports. The Network Element Port Settings window pops up. Enter the correct information, as described in Table 12-2 and click Submit .
New	Adds a new access point. The web page changes to reflect this new access point.
Defaults	Displays the default parameter settings.
Requery	Refreshes the web page (click before saving changes).
Save	Saves the changes made to the web page.
Delete	Deletes the access point.

Figure 12-2 Network Element Port Settings Pop-up Window

Table 12-2 Port Settings Window Options


Field	Description
Type	Displays the network device type.
Location Prefix	Enter a location prefix. The prefix can contain a maximum of 40 characters. (This field is optional.)
Page Set	From the drop-down menu, choose a page set. For descriptions of the default page sets that ship with BBSM, refer to Table 18-1 on page 18-3 . <div style="border: 1px solid black; padding: 5px;"> <p> Caution If you will be using SSL and have not yet installed your SSL certificate, you will not be able to select an SSL page set. Choose the <i>Clear</i> version of the page set until you install the certificate and then change your page set to the SSL page set. For example, select RADIUSClear until the certificate is installed, then after installing the certificate, change the page set to RADIUS. If you install the SSL page set before installing the certificate, the Start page will not display.</p> </div> <p>Note For CMTSs, the page set that you choose is the default page set that will be applied to the CMTS dynamic port-room configuration. Refer to the “Dynamic Port-Room Configuration for CMTSs” section on page 13-13.</p>
Start Page	BBSM automatically enters the Start page for the network device based on the page set. However, you can enter a different Start page.
Bandwidth	Enter a bandwidth throttling value in kbps for clients connected to this network device. The bandwidth is effective only if bandwidth management is turned on. (Refer to Chapter 9, “Changing the Internal Network IP Address Ranges.”) If the end user selects a bandwidth from the Connect page, that selection overrides this default bandwidth.

Table 12-2 Port Settings Window Options (continued)

Field	Description
Enable Port Hopping	Check this check box to enable port hopping.
Client IP Address Range (DHCP)	<i>This field appears only if you are using multinet.</i> If you are using multiple networks, click the default multinet number for clients connected to this network device: Multinet 1 or Multinet 2. Note The Connect page overrides this setting if the end user selects a public or private IP address.
Buttons	
Submit	Enters the changes you have made.
Reset	Before you have submitted the changes, resets the data to the stored information.
Cancel	Cancel any changes.

Adding and Configuring CMTSs

If you are using a CMTS, you must add a CMTS record in WEBconfig as a network device for a site. Follow this procedure to add and configure the CMTS record.

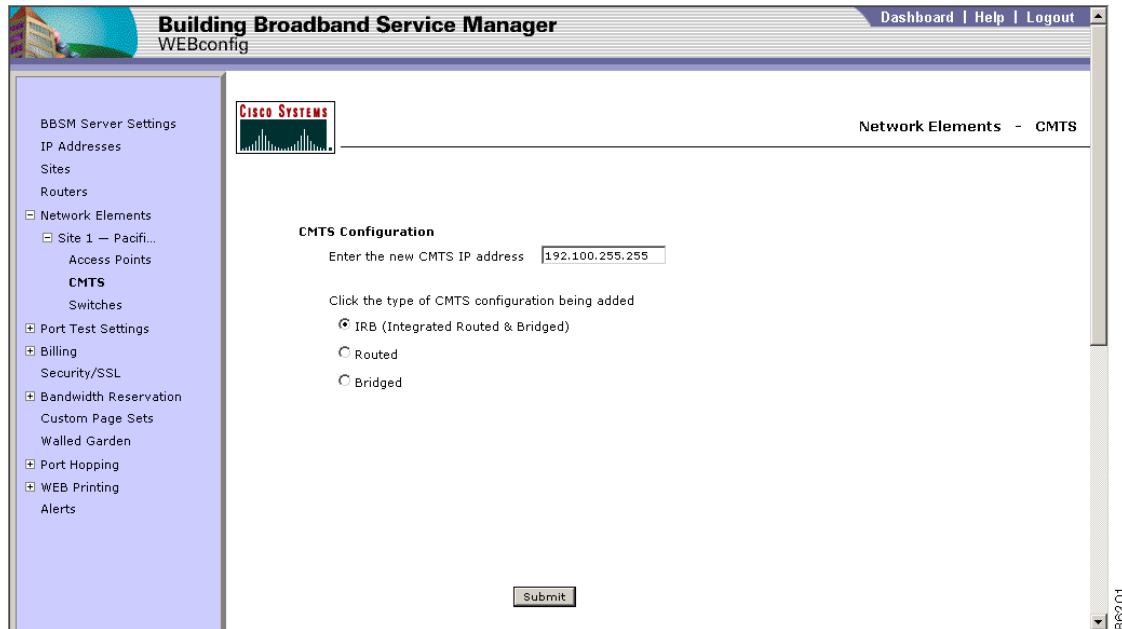


Note

If you are using an external provisioning server for your cable modem, such as TFTP, ToD, or a log server, you must create a walled garden entry for the cable modems to come online properly. The entry must consist of only an IP address and subnet mask for the cable modems to access these servers. The walled garden hostname, which is usually used for clients using a proxy server setting, can be just a description.

- Step 1** From the Dashboard, click **WEBconfig**. The BBSM Server Settings web page appears.
- Step 2** In the NavBar, navigate to the CMTS web page by choosing **Network Elements > Site 1** (or other applicable site) **> CMTS**. The initial CMTS configuration selection web page appears the first time you configure the CMTS. (See [Figure 12-3](#).)

Figure 12-3 CMTS Web Page



- Step 3** Enter the CMTS IP address and select a CMTS configuration (IRB, Routed, or Bridged) based on the information shown in [Table 12-3](#) and click **Submit**. The appropriate CMTS network configuration web page appears. (See [Figures 12-4](#) through [12-6](#).) (The IRB and Bridged CMTS configuration web pages are the same for singlenet or multinet. Only the Routed configuration web pages are different for singlenet and multinet.)

Table 12-3 Initial CMTS Web Page Options

Field	Description
Enter the new CMTS IP address	Enter the IP address of the CMTS being added. This is the CMTS client-side IP address: <ul style="list-style-type: none"> In a Bridged or IRB configuration, this IP address is on the same subnet as the DHCP and Management ranges. In a Routed configuration, this IP address is not on the BBSM internal network but on a subnet internal to the router.
IRB	Click if the CMTS is configured for an integrated routed and bridged configuration, which means that the CMTS acts as both a router for cable modems and a bridge for end users.
Routed	Click if the CMTS is configured as a router. In this case, BBSM cannot support static clients (plug and play).
Bridged	Click if the CMTS is configured in a bridged configuration.
Button	
Submit	Takes you to the CMTS configuration web page for the mode you selected.

- Step 4** Configure the CMTSs based on the information shown in [Table 12-4](#) and click **Save**. The Network Element Port Settings window pops up. (See [Figure 12-2](#) on [page 12-6](#).)



Note If port configuration records already exist, the Network Element Port Settings window does not pop up automatically. Click **Port Settings**.

- Step 5** Enter the applicable information based on the information in [Table 12-2 on page 12-6](#) and click **Submit**. A dialog box appears, asking you to verify your changes. Click **OK** and you are returned to the applicable CMTS web page.

Figure 12-4 IRB CMTS Web Page (Singlenet, Single VLAN)

Building Broadband Service Manager
WEBconfig

Dashboard | Help | Logout

Network Elements - CMTS

CISCO SYSTEMS

CMTS in IRB Mode

CMTS Type	Cisco uBR7x00		
Cluster Number	3	Disable CMTS	<input type="checkbox"/>
CMTS IP Address	192.100.255.255	Aging Period	300 seconds
Router	127.0.0.1	SNMP Password	private
Router Number	1	Gateway to Router	192.100.255.255

Configure Cable Modem DHCP Range and Options

Cable Modem DHCP Start	<input type="text"/>	(007)Log Server	<input type="text"/>
Cable Modem DHCP End	<input type="text"/>	(010)Impress Server	<input type="text"/>
Cable Modem Subnet Mask	<input type="text"/>	(011)Resource Location Server	<input type="text"/>
(002)Time Offset	0 seconds	(006)Boot Server	<input type="text"/>
(003)Router	<input type="text"/>	(067)Boot File Name	<input type="text"/>
(004)Time Server	<input type="text"/>		
(006)DNS Server	<input type="text"/>		

If port configuration records already exist, the Network Element Port Settings window does not pop up automatically when you click Save. Click **Port Settings**.

Even if you disable a CMTS, its IP address remains reserved. If you need to reuse the IP address for a different network element, change the IP address of the disabled CMTS temporarily; otherwise, you will not be able to update WEBconfig.

For Bridged configuration, the DHCP IP address range must be on the same subnet as your internal NIC. For IRB and Routed configurations, the DHCP IP range must not be on the same subnet as your internal internal NIC.

86203

Figure 12-5 Routed CMTS Web Page (Multinet, Dual VLAN)

The screenshot shows the 'Building Broadband Service Manager WEBconfig' interface. The left sidebar contains a navigation menu with options like 'BBSM Server Settings', 'IP Addresses', 'Sites', 'Routers', 'Network Elements', 'Site 1 - Pacific...', 'Access Points', 'CMTS', 'Switches', 'Port Test Settings', 'Billing', 'Security/SSL', 'Bandwidth Reservation', 'Custom Page Sets', 'Walled Garden', 'Port Hopping', 'WEB Printing', and 'Alerts'. The main content area is titled 'Network Elements - CMTS' and features the Cisco Systems logo. The configuration is for a 'CMTS in Routed Mode' with the following details:

- CMTS Type:** Cisco uBR7x00
- Cluster Number:** 3
- Disable CMTS:**
- CMTS IP Address:** 192.100.255.255
- Aging Period:** 300 seconds
- Router:** 192.100.255.255
- SNMP Password:** private@100
- Router Number:** 1
- Gateway to Router:** [Empty field]

Below these settings are two columns for 'Multinet 1' and 'Multinet 2' configuration:

	Multinet 1	Multinet 2
Router IP Address	192.100.255.255	[Empty]
Client Start	[Empty]	[Empty]
Client End	[Empty]	[Empty]
Client Subnet Mask	[Empty]	[Empty]
Temp DHCP Start	[Empty]	[Empty]
Temp DHCP End	[Empty]	[Empty]

The 'Configure Cable Modem DHCP Range and Options' section includes:

- Cable Modem DHCP Start: [Empty]
- Cable Modem DHCP End: [Empty]
- Cable Modem Subnet Mask: [Empty]
- (002)Time Offset: 0 seconds
- (003)Router: [Empty]
- (004)Time Server: [Empty]
- (006)DNS Server: [Empty]
- (067)Boot File Name: [Empty]
- (007)Log Server: [Empty]
- (010)Impress Server: [Empty]
- (011)Resource Location Server: [Empty]
- (066)Boot Server: [Empty]

The 'Multiple VLANs' section shows:

- Client VLAN ID: 100
- Mgmt VLAN ID: 2

At the bottom, there are navigation buttons: 'New', '<<', '<', '>', '>>', 'Query', 'Save', 'Delete', and 'Port Settings'. A yellow warning box on the right states: 'If port configuration records already exist, the Network Element Port Settings window does not pop up automatically when you click Save. Click Port Settings. Even if you disable a CMTS, its IP address remains reserved. If you need to reuse the IP address for a different network element, change the IP address of the disabled CMTS temporarily; otherwise, you will not be able to update WEBconfig. For Bridged configuration, the DHCP IP address range must be on the same subnet as your internal NIC. For IRB and Routed configurations, the DHCP IP range must not be on the same subnet as your internal internal NIC.'

Figure 12-6 Bridged CMTS Web Page (Dual VLAN)

Building Broadband Service Manager
WEBconfig

Dashboard | Help | Logout

Network Elements - CMTS

CMTS in Bridged Mode

CMTS Type: Cisco uBR7x00
 Cluster Number: 3
 CMTS IP Address: 192.100.255.255
 Router: 127.0.0.1

Disable CMTS:
 Aging Period: 300 seconds
 SNMP Password: private

Configure Cable Modem DHCP Range and Options

Cable Modem DHCP Start:
 Cable Modem DHCP End:

(002)Time Offset: 0 seconds (007)Log Server:
 (003)Router: (010)Impress Server:
 (004)Time Server: (011)Resource Location Server:
 (006)DNS Server: (066)Boot Server:
 (067)Boot File Name:

Buttons: New << < > >> Requery Save Delete Port Settings

Notes:

If port configuration records already exist, the Network Element Port Settings window does not pop up automatically when you click Save. Click **Port Settings**.

Even if you disable a CMTS, its IP address remains reserved. If you need to reuse the IP address for a different network element, change the IP address of the disabled CMTS temporarily; otherwise, you will not be able to update WEBconfig.

For Bridged configuration, the DHCP IP address range must be on the same subnet as your internal NIC. For IRB and Routed configurations, the DHCP IP range must not be on the same subnet as your internal internal NIC.

Table 12-4 IRB, Routed, and Bridged Configuration CMTS Web Page Options

Field	Description
CMTS Type Cluster Number CMTS IP Address Router	Based on the CMTS configuration and the CMTS IP address that you entered, the system automatically fills in the basic parameters and displays the CMTS type, cluster number, CMTS IP address, and router of the CMTS that you will be configuring.
Router Number	Displays the router that the CMTS is connected to.
Disable CMTS	Check if you do not want BBSM to look for CMTS clients on the ports for the cluster. Note Even if you disable a CMTS, its IP address remains reserved. If you need to reuse the IP address for a different network device, change the IP address of the disabled CMTS temporarily. If you do not change the IP address, you will not be able to update WEBconfig.
Aging Period (in seconds)	Enter the time period in seconds that the client can be idle before the end user is automatically signed off. The default is 300 (5 minutes).
SNMP Password	Enter the SNMP read-write community string (password) that is used when communicating with the CMTS. The default is <i>public</i> . (Cisco recommends that the default password on the switches and on BBSM be changed because the default password is well known and could compromise network security.)
Router Number (IRB or Routed configuration)	Displays the router number associated with the CMTS.

Table 12-4 IRB, Routed, and Bridged Configuration CMTS Web Page Options (continued)

Field	Description
Gateway to Router (IRB and Routed configurations)	Displays the IP address of the first hop from the BBSM server to the router.
Router IP Address (Routed configuration)	Displays the IP address of the router that you are connecting to. The router IP address is the same as the CMTS IP address when the CMTS is in the Routed configuration.
Client Start Client End Client Subnet Mask (Routed configuration)	Enter the starting and ending IP addresses and the subnet mask for the clients connecting to this CMTS. The BBSM server treats traffic from the Client Start through the Client End IP address range as coming from client computers.
Cable Modem DHCP Start Cable Modem DHCP End	Enter the starting and ending IP addresses to be assigned to the cable modems. <ul style="list-style-type: none"> For Bridged configuration, the IP address range must be on the same subnet as your internal NIC. For IRB and Routed configurations, the IP range must not be on the same subnet as your NIC.
Cable Modem Subnet Mask (IRB or Routed configuration)	Enter the cable modem subnet mask for the DHCP IP addresses. In a bridged configuration, the subnet mask is the same as your internal NIC subnet mask.
DHCP options	Because these options are standard DHCP options, they are not described here. An administrator configuring the CMTS will probably understand these options. Note Refer to the Internet Engineering Task Force (IETF) Request for Comments (RFC) 2132 for details about these DHCP options.

VLANs*(These fields apply only when two VLANs are configured.)*

Clients VLAN ID	Displays the client VLAN ID.
Mgmt VLAN ID	Displays the management VLAN ID.

Buttons

New	Configures a new CMTS. The initial CMTS web page appears.
Requery	Refreshes the web page (click before saving changes).
Save	Saves the changes made to the web page.
Delete	Deletes the CMTS.
Port Settings	Configures the CMTS ports. The CMTS Port Settings window pops up. Enter the correct information, as described in Table 12-2 on page 12-6 .

Configuring Switches

Follow this procedure to configure each switch. Most BBSM installations use two types of switches:

- Client switches—Connect to end-user computers called *clients*.
- Base switches—Connect to base switches, also known as *aggregation* switches.

Unused ports on the base switch can be used as client ports if the base switch is added to the Switches web page. When the base switch is also being used as a client switch, the ports connected to client switches must be marked as uplink ports. For instructions on how to configure a port as an uplink port, refer to the *Cisco BBSM 5.3 Operations Guide*.

As of BBSM 5.2, Cisco supports switch clustering. For additional information about the clustering architecture, refer to the “[Switch Clustering](#)” section on page 12-2.

- Step 1** From the Dashboard, click **WEBconfig**. The BBSM Server Settings web page appears.
- Step 2** In the NavBar, navigate to the Switches web page by choosing **Network Elements > Site x > Switches**. The Switches web page appears. (Figure 12-7 shows a dual-VLAN configuration.)

Figure 12-7 Switches Web Page (Dual VLAN)

The screenshot displays the 'Building Broadband Service Manager' WEBconfig interface. The main content area is titled 'Network Elements - Switches'. The configuration is for 'Site Information 1 Pacific Plaza'.

Site Information: 1 Pacific Plaza

Cluster Number: 1 (with a 'Go' button)

Cluster Member No.: 1

Switch Type: Cisco Catalyst 2950-24 (12.1.11)

Cluster/Switch IP Address: 192.168.255.3

Aging Period: 300 seconds

SNMP Password: private

Packet Inactivity Period: 300 seconds

Router: 127.0.0.1

No. of Client Ports: 24

Disable Switch:

VLANs:

- Client VLAN ID: 100
- Mgmt VLAN ID: 2

Port Settings: (button)

New Cluster/Switch: (button) **New Cluster Member:** (button)

Navigation buttons: << < > >> Defaults Requery Save Delete

Help Text (Yellow Box):

- No. of Client Ports:** Enter the number of ports on the switch that can be used by clients.
- Cluster/Switch IP Addr:** Enter the unique IP address from the management address range assigned to this switch.
- Aging Period:** Enter the number of seconds the switch waits before deactivating inactive clients.
- Port Settings:** Use this button to configure all ports on the selected switch.
- Note:** For details about packet inactivity period and switch clusters, refer to the online documentation.

86289

- Step 3** Configure the switches based on the information shown in [Table 12-5](#) and click **Save**. The Network Element Port Settings window pops up. (See [Figure 12-2 on page 12-6](#).)



Note If port configuration records already exist, the Network Element Port Settings window does not pop up automatically. Click **Port Settings**.

- Step 4** Enter the applicable information in the Network Element Port Settings window based on the information in [Table 12-2 on page 12-6](#) and click **Submit**. A dialog box appears, asking you to verify your changes. Click **OK** and you are returned to the Switches web page.

Table 12-5 Switches Web Page Options

Field	Description
Site Information	Displays the site number and name associated with the switch to be configured.
Cluster Number Cluster Member No. Go	Displays the cluster number and cluster member number associated with the switch to be configured. Click Go to advance to another previously configured switch. This is a convenient way to advance to another switch record without having to use the < or > buttons to advance one switch at a time.
Switch Type	From the drop-down menu, choose a switch type. Because the list of supported Cisco switch types continues to be updated, refer to the following document for the latest list of supported network devices: http://www.cisco.com/univercd/cc/td/doc/product/aggr/bbsm/devices.pdf
Cluster/Switch IP Address	Enter a unique IP address in the management range assigned to the cluster or switch. Check with the person installing your clusters and switches if you are unsure of this IP address.
SNMP Password	Enter the SNMP read-write community string (password) that is used when communicating with switches. (Non-Cisco stackable switches, which share the same stack, are installed with the same password.) The default is “public.” Note Cisco recommends that the default password on the switches and on BBSM be changed because the default password is well known and could compromise network security.
Router	From the drop-down menu, choose the router IP address of the router that this site and cluster are connected to. If the site and cluster are directly connected to the BBSM server, use the default IP address for the BBSM server, which is <i>127.0.0.1</i> .
Disable Switch	Check this check box if you do not want BBSM to look for clients on the cluster ports. Use when troubleshooting. (Even if you disable a switch, its IP address remains reserved. If you need to reuse the IP address for a different switch, change the IP address of the disabled switch temporarily. If you do not change the IP address, you will not be able to update WEBconfig.)
Aging Period (in seconds)	Enter a time period, in seconds, that the network device will wait before eliminating inactive clients from its internal tables, which causes BBSM to automatically sign off the client. The default time period is 300 (5 minutes).
Packet Inactivity Period (in seconds)	Note This field is disabled unless your switch type supports packet inactivity. Enter a time, in seconds, that a user can be idle before being automatically signed off by BBSM. If needed, refer to the <i>Cisco BBSM Products Network Device Compatibility Guide</i> to verify the switches that monitor for packet inactivity.
No. of Client Ports	Enter the number of ports that can be used as clients on switch 1 of the cluster. The default is 23.
VLANs (These fields apply for dual VLANs only.)	
Clients VLAN ID	Displays the client VLAN ID.
Mgmt VLAN ID	Displays the management VLAN ID.

Table 12-5 Switches Web Page Options (continued)

Field	Description
Buttons	
Port Settings	Click to configure the settings for all ports on this switch. The Network Element Port Settings window pops up. Enter the applicable information based on the parameters in Table 12-2 on page 12-6 and click Submit .
New Cluster/Switch	Adds a new cluster to the site. A new web page appears with blank fields so the new cluster and the associated switches can be configured. Use this option also to add a single, nonclustered switch.
New Cluster Member	Adds a new network device to an existing cluster. A new web page appears with blank fields so the associated parameters can be configured. (If a switch is not cluster capable or not configured as a cluster switch, BBSM considers the switch as a cluster of a single switch.)
Defaults	Displays the default parameter settings.
Requery	Refreshes the web page (click before saving changes).
Save	Saves the changes made to the web page.
Delete	Deletes the switch.

