CA Spectrum® Infrastructure Manager

Cable Broadband Infrastructure Administration Guide

r9.2

CA Product References

This guide references CA Spectrum®.

Contact CA

Contact Technical Support

For your convenience, CA provides one site where you can access the information you need for your Home Office, Small Business, and Enterprise CA products. At http://ca.com/support, you can access the following:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Provide Feedback

If you have comments or questions about CA product documentation, you can send a message to techpubs@ca.com.

If you would like to provide feedback about CA product documentation, complete our short customer survey, which is also available on the CA Support website, found at http://ca.com/docs.

Contents

Chapter 1: Getting Started with Cable Broadband Solution

This section contains the following topics:

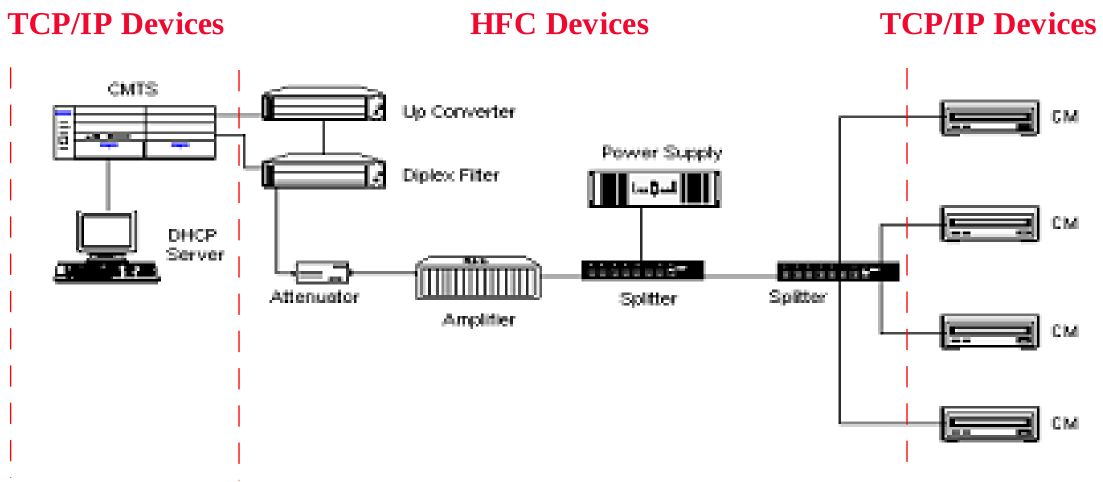
Network Management Factors

This section describes the elements of a broadband network and the Cable Broadband models in the CA Spectrum Cable Broadband Solution.

For a cable broadband management system to be effective, it must meet the challenge of acquiring an array of information available from a variety of devices diversely deployed to meet the demands of many different business requirements. To be useful to managers, the acquired information must be displayed in a meaningful manner.

The following image provides an example of a simple cable broadband network deployment.

Basic Components of a Cable Broadband Network



The cable broadband network includes Hybrid Fiber Coax (HFC) devices and TCP/IP devices. The HFC devices consist of Up Converters, Diplex Filters, Attenuators, Amplifiers, Splitters, and Power Supplies. The TCP/IP devices consist of DHCP servers, Cable Modem Termination Systems (CMTS), and Cable Modems (CM). The HFC components gather HFC information through proprietary communication methods. The TCP/IP devices gather network information through the Simple Network Management Protocol (SNMP).

In addition to the challenges imposed by the diversity of devices and deployments, an added complexity for network managers is the need to control SNMP traffic. Using SNMP, CMs communicate information to CMTSs over the HFC network using shared channel frequencies. The downstream frequency channel aggregates information from the CMTSs to the CMs and the upstream frequency channels aggregate information from the CMs to the CMTSs. Managers must have visibility into the amount of SNMP traffic that is generated on this shared media in order to maximize network efficiencies, plan for network growth, and have visibility into the operational status of devices for purposes of fault isolation and root cause analysis.

CA Spectrum's cable broadband network management solution meets the challenges summarized previously by:

- Supporting devices and MIBs produced by a variety of vendors.
- Limiting ICMP and SNMP traffic by introducing modeling techniques designed for cable broadband networks.
- Providing a mechanism for logically grouping device models.
- Providing a means for aggregating alarms from selected devices and setting aggregate threshold values based on mission criticality.
- Providing fault isolation and root cause analysis down to the port level.

More information:

Vendor MIB Support (see page 8)

Vendor MIB Support

Depending on the management module, vendor-specific information can be found either off the device model or in the Component Detail panel view in the form of an application. The following table lists the device-specific CA Spectrum management modules related to cable broadband devices. For example, the AM Communications device type supports the SM-AMC1000 management module.

AM Communications

SM-AMC1000

Arris Cadant C4 CMTS

SM-ARS1000

Broadband Service Containers

SM-BSC1000

Cheetah Gateway Integration

SM-SFA1000

Cisco uBR72xxCMTS

SM-CIS1008

DOCSIS Applications

SM-DCSCMN

DOCSIS Devices

SM-DCS1000

LANCity Cable TV Modem

SM-LCH1000

Motorola CDLP Cable Router

SM-MOT1001

RiverDelta BSR 1000/64000

SM-RVD1000

Riverstone SmartSwitch Router

SM-RST1000

Scientific Atlanta Explorer HCT

SM-SFA1000

Telecom CUDA 12000

SM-ADC1000

Terayon BroadbandEdge2000/TeraLink 1000

SM-TRN1000

Terayon BW3500 CMTS

SM-TRN1001

CA Spectrum Device Support

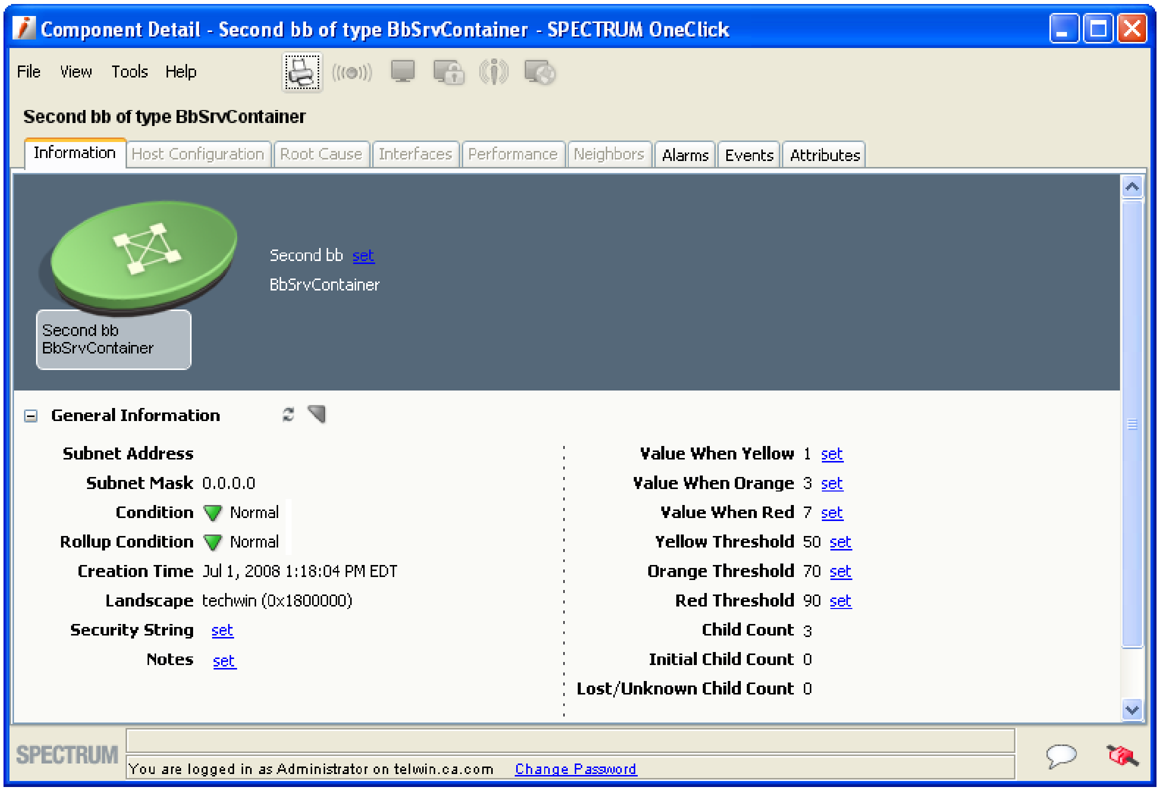
This section describes the cable broadband models and their functionality in CA Spectrum.

CA Spectrum provides efficient information gathering by limiting ICMP and SNMP traffic across the cable broadband network. This is accomplished by providing four model paradigms as follows:

- CMTS models provide the full information gathering aspects of a GnSNMPDev model type.
- Lightweight models provide focused information gathering for CMs and set-top boxes.
- Broadband Service Container models provide a method of logically grouping Lightweight models.
- HFC Device Event Modeling

Each of these models is designed to focus information gathering to meet management's need for useful information, to eliminate distracting information, and to reduce the impact of polling on an efficiently operating cable broadband network.

The following image provides an example of how CA Spectrum displays cable broadband component details:



CMTS Models

The following section describes CA Spectrum's support of CMTS devices and DOCSIS-compliant devices.

CMTS Model Device Support

CA Spectrum supports a variety of CMTS devices from vendors including Cisco, Terayon, Motorola, Nortel LANCity, River Delta (acquired by Motorola), ADC, and Riverstone. The CMTS device models have standard device support including model creation for applications and interfaces, Topology and Device Interface views, interface connectivity/port resolution, Discovery, and fault isolation capabilities. These device models are based on the standard support provided by the GnSNMPDev model type.

CMTS Model DOCSIS Support

CA Spectrum also supports CMTS devices that comply with DOCSIS.

CMTS Fault Isolation, Polling, and Logging

For information about fault isolation, polling, and logging, see the *Modeling and Managing Your IT Infrastructure Administrator Guide*.

Lightweight Models

Lightweight models include CMs and set-top boxes. The lightweight model paradigm supports devices that do not require the full functionality that GnSNMPDev models provide.

Lightweight Model Device Support

CA Spectrum supports the Motorola cable modem, a DOCSIS-compliant cable modem, and the Scientific Atlanta set-top box. A cable broadband network can include thousands of these devices; therefore, the models of these devices are designed as lightweight models. The lightweight series of models provide a way to represent and collect meaningful SNMP data from all cable modems and set-top boxes while limiting the effects of polling on the network.

The implementation of the new lightweight model paradigm has many significant differences over conventional GnSNMPDev models. The lightweight models have increased model capacity on a SpectroSERVER, reduced SNMP traffic, and reduced memory and CPU usage. However, the lightweight models do not create interface models for port resolution, and do not participate in fault isolation. They only communicate SNMP to their real world counterpart, whereas a GnSNMPDev model will also try to use ICMP ping to contact the device.

Lightweight Model DOCSIS Support

Support also includes a generic DOCSIS-compliant CM device model for those vendor devices that CA Spectrum does not support but which are DOCSIS-compliant.

Lightweight Model Fault Isolation

Because the Lightweight Model Architecture does not participate in fault isolation, there is no value from a fault isolation standpoint of connecting these models by pipes. Also, by default lightweight models do not alarm. If contact with the device via SNMP has been lost, the model will turn gray and go into a suppressed state. This is done to keep the alarm manager from being flooded with red alarms from cable or set-top models losing contact. This functionality is configurable and can be set to alarm or not to alarm.

Lightweight Model Polling and Logging

Lightweight models do not log or poll any attributes. For this reason, they keep in contact with the device at three times the polling interval. This is why lightweight models do not turn active over a polling interval. Lightweight models can only be modeled by model type; you cannot model them using Discovery or by using Model by IP.

Note: Modeling cable modems over the HFC network is not advised. Because most cable modems change IP addresses on a regular basis, there would be too much SNMP traffic generated to update cable modem models.

In the future, CA Spectrum will contain auto-population features that will create and update cable modem models from the CMTS MIB tables.

Broadband Service Container Models

The broadband service container model (BbSrvContainer) provides a mechanism for the logical grouping of lightweight models. To see how the broadband service container differs from other standard containers, first consider the process used by a standard container to monitor the condition of models it collects.

Standard Container Characteristics

With standard containers, such as a Network or LAN, the container is responsible for summing the condition value of every device (or container) it collects. This sum is written to an attribute called composite condition. The composite condition is then compared to the rollup threshold values of yellow, orange, and red. The rollup thresholds are defined for minor, major, and critical severities. For every severity state, there is a significance level that can be defined. If the composite condition exceeds a rollup threshold then the rollup condition assumes that threshold condition and color. This process for standard containers is described in detail in the *Modeling and Managing Your IT Infrastructure Administrator Guide*.

Broadband Service Container Characteristics

In contrast to standard containers, the broadband service container monitors the percentage of models it has collected that have lost contact compared with the total sum of models, excluding any model still in the initial state. The percentage thresholds are defined for minor, major, and critical severities. For every severity state, there is a significance level that can be defined. However, when a threshold has been violated, the broadband service container assumes the condition associated with the threshold. The broadband service container assumes a condition to reflect the condition of the network represented by the devices grouped in the container. This is done because the alarms on the individual cable or set-top models are suppressed.

The container model's General Information subview contains the following two attributes which determine the condition shown on the container in the Topology view: Condition Value and Lost/Unknown Child Count.

The Lost/Unknown Child Count displays the percentage of the devices collected by this container that have lost contact. The value of Lost/Unknown Child Count is compared with the rollup thresholds. If the value of Lost/Unknown Child Count exceeds a threshold, the container will set the Condition Value attribute to that criticality. The table below shows possible condition values.

Once the Condition Value of the Broadband Service Container assumes a criticality of yellow, orange, or red, the significance levels are taken into consideration by CA Spectrum. That is, the current Condition Value of the BbSrvContainer is compared with the significance level values and the significance value of the BbSrvContainer is then set, based on this comparison.

Models of cable modems and set-top boxes should never be directly connected in CA Spectrum to models of CMTS devices. To help ensure proper fault isolation for CMs and set-top boxes, the broadband service container model must be used to group models of these lightweight devices.

HFC Device Event Modeling

CA Spectrum does not model HFC devices. Most HFC devices communicate with a Headend Communications Controller (HEC). The communication protocol between the HEC and HFC devices is usually proprietary. For example, Acterna (Cheetah) and AM Communications developed a software application to communicate with their respective HECs. These software applications are capable of sending SNMP traps. CA Spectrum collects and processes these traps (sent from either software application) using the Southbound Gateway.

When an SNMP trap is sent from the software application, the Southbound Gateway analyzes the data and creates a new event model, if one has not already been created. From that point forward, traps sent from the application are mapped to that event model. The traps will be further processed and events and alarms created on the event model.

DOCSIS MIB Support

Support also includes a generic DOCSIS-compliant CMTS device for those vendor devices that CA Spectrum does not support but are DOCSIS-compliant. In the case of these devices, the CMTS models will have the DOCSIS information available in the application view as applications. There is an application for each of the DOCSIS MIBs shown in the following table that will discover automatically if the device supports the MIB.

DOCSIS MIB Listing	1.0 Standard	1.1 Standard	2.0 Standard	Supported by CA Spectrum
RFC 2669: Cable Device MIB	Yes	Yes	Yes	Yes
RFC 2670: Radio Frequency Interface	Yes	Yes	Yes	Yes
RFC 3083: Baseline Privacy Interface	Yes	Yes	Yes	Yes
Quality of Service	No	Yes	Yes	Yes
Baseline Privacy Interface Plus	No	Yes	Yes	Yes

Chapter 2: Broadband Service Container Model

This section describes how to model broadband network devices and access MIB attribute information from the BbSrvContainer model's General Information subview.

This section contains the following topics:

Create a Broadband Service Container Model

The following procedure describes how to create a Broadband Service Container model.

Note: For more information about creating models and container models, see *Modeling and Managing Your IT Infrastructure Administrator Guide*.

To create a Broadband Service Container model

1. In the Explorer tab of the OneClick Navigation panel, select the Universe topology view where you want to add the new container.

   The selected topology view appears in the Topology tab of the Contents panel.

2. In the Topology tab of the Contents panel, click  (Creates a new model by type) in the Topology tab toolbar.

   The Select Model Type dialog opens.

3. Click 'BbSrvContainer' in the Containers tab and click OK to add the container to the Topology tab.

   The 'Create Model of Type BbSrvContainer' dialog appears.

4. Type a Name and Security String for the container and click OK.

   The container is added to the Topology view and you can view details in the Component Detail panel.

Note: You can create more than one container model to separately monitor different parts of a network. A container model can be created inside other container models, and it can be copied and pasted into the topology on an appropriate interface to provide port resolution for the broadband devices. Where and how you model containers and devices depends on your network configuration and how you want to view it in CA Spectrum.

Model Devices

Once the Broadband container model has been created, you can model devices in its Topology view as needed. The following procedure describes how to do so manually. For more detailed information about creating models and container models, see *Modeling and Managing Your IT Infrastructure Administrator Guide*.

To manually add device models to the Broadband Service Container

1. In the Explorer tab of the OneClick Navigation panel, select the broadband service container to which you want to add new device models.

   The selected topology view appears in the Topology tab of the Contents panel.

2. Click  (Creates a new model by type) in the Topology tab toolbar.

   The Select Model Type dialog appears.

3. Select the desired model type and click OK.

   The 'Create Model of Type' dialog appears.

4. Complete the fields as needed and click OK.

   The device model is added to the Topology view and you can view details in the Component Detail panel.

General Information Subview

From the Broadband container model's General Information subview you can access information about the status of the model and its children, its rollup thresholds, and its significance levels. It contains the settings listed here and in the following sections.

Condition

Reflects the current contact or alarm status of the model itself.

Rollup Condition

Applies to container models; reflects the composite status of all the other models in the container, which are sometimes referred to as its children. The percentage of devices in the container that are down, excluding those devices whose models were never active.

The following table shows possible Rollup Condition values:

Condition Value	Alarm Status	Label Color
0	Normal	Green
1	Minor	Yellow
2	Major	Orange
3	Critical	Red

Child Count

Specifies the total number of devices in the container, which includes active, Initial Child, and Lost Child models.

Initial Child Count

Specifies the number of devices in the container whose models are in the Initial state.

Lost/Unknown Child Count

Specifies the number of devices in the container that were active but have lost contact with the network.

Significance Levels

Significance levels for the BbSrvContainer model weigh the importance of the model for each possible alarm severity the model may reach.

In the case of the BbSrvContainer model, the significance levels represent the importance of the cable modems and set-top models. When a BbSrvContainer model is collected by a parent container and the BbSrvContainer model reaches a particular alarm severity, the significance value will be used to calculate the parent container's alarm severity.

Value When Yellow

Specifies the point value of a Yellow alarm condition existing in a child towards the rollup alarm threshold value for the parent container.

Default: 1

Value When Orange

Specifies the point weight of an Orange alarm condition existing in a child towards the rollup alarm threshold value for the parent container.

Default: 3

Value When Red

The point weight of a Red alarm condition existing in a child towards the rollup alarm threshold value for the parent container.

Default: 7

Rollup Thresholds

The rollup thresholds are three read-write values that control when the BbSrvContainer model's rollup condition icon changes color and also controls when alarms are triggered. Each of the threshold values represents the percentage of active devices in the BbSrvContainer that have gone down. When the actual percentage of devices that are down equals or exceeds a threshold value, the BbSrvContainer model's rollup condition icon changes to the color associated with that threshold and a commensurate alarm is triggered.

Expressed mathematically, the rollup threshold value is:

```
Lost Child Count divided by (Child Count - Initial Child Count) x 100
```

In other words, models that have never been active are excluded from the percentage value.

You can set the thresholds to suit your requirements or use the default values. Recommendations for each threshold value are as follows:

Yellow Threshold

Minor alarm threshold. Specifies the minimum points needed to trigger a Yellow rollup alarm for a container. You might use this threshold to indicate a network condition that is less than optimum but does not threaten service.

Default: 50

Orange Threshold

Major alarm threshold. Specifies the minimum points needed to trigger an Orange rollup alarm for a container. You might use this threshold to indicate a network condition that should be examined before it threatens service.

Default: 70

Red Threshold

Critical alarm threshold. Specifies the minimum points needed to trigger a Red rollup alarm for a container. You might use this threshold to indicate a network condition that has a serious impact on service.

Default: 90

Note: Change threshold levels carefully; you may see an increase in generated alarms if threshold levels are set lower, or a decrease in generated alarms if levels are set higher.

Index