

CA Spectrum®

Standards-Based Protocol Reference Guide

Release 9.3



This Documentation, which includes embedded help systems and electronically distributed materials, (hereinafter referred to as the "Documentation") is for your informational purposes only and is subject to change or withdrawal by CA at any time.

This Documentation may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA. This Documentation is confidential and proprietary information of CA and may not be disclosed by you or used for any purpose other than as may be permitted in (i) a separate agreement between you and CA governing your use of the CA software to which the Documentation relates; or (ii) a separate confidentiality agreement between you and CA.

Notwithstanding the foregoing, if you are a licensed user of the software product(s) addressed in the Documentation, you may print or otherwise make available a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all CA copyright notices and legends are affixed to each reproduced copy.

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to CA that all copies and partial copies of the Documentation have been returned to CA or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENTATION "AS IS" WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL CA BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF CA IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice.

The manufacturer of this Documentation is CA.

Provided with "Restricted Rights." Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

Copyright © 2013 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

CA Technologies Product References

This guide references CA Spectrum® Infrastructure Manager (CA Spectrum).

Contact CA Technologies

Contact CA Support

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

- 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

Providing Feedback About Product Documentation

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

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at <http://ca.com/docs>.

Contents

Chapter 1: Standard Protocols Supported by CA Spectrum	7
About Standard Protocols Supported by CA Spectrum	7
Bridging	7
PPP Bridging	8
QBridge	8
Source Routing	9
Spanning Tree Bridges	9
Static Bridging	9
Transparent Bridges	10
Broadband	10
ADSL	10
DOCSIS	11
Device and System Identity	11
Entity	11
Host Resources	12
System Application	12
IP Protocols and Services	12
DHCP	12
ICMP	13
IGMP	13
IP	13
IPM	14
IP Tunnel	14
MPLS	14
MSDP	15
PIM	15
SNMP	15
TCP	16
UDP	16
LAN	17
Character Stream	17
Ethernet	17
FDDI	17
Link Aggregation	18
Power Over Ethernet	18
RS-232	18
Token Ring	19

Wireless LAN	19
Performance.....	19
RMON.....	19
Traceroute/Lookup	20
Routing.....	20
BGP4.....	21
IP Routing.....	21
IS-IS Routing	21
OSPF	21
Repeater.....	22
RIP2	22
VRRP.....	22
SAN.....	22
Fibre Channel	23
Security.....	23
Port-Based Network Access Control	23
RADIUS	24
User-Based Security Model	24
WAN	24
ATM.....	24
DS1	25
Frame Relay.....	25
PNNI	26
PPP	26
SONET.....	26
Chapter 2: Accessing Standard Protocol Information in OneClick	27
Access Standards-Based Information Using the Information Tab.....	27
Locater Search.....	27
Search for Application Models	27
Appendix A: RFC Reference	29
Index	35

Chapter 1: Standard Protocols Supported by CA Spectrum

This section contains the following topics:

[About Standard Protocols Supported by CA Spectrum](#) (see page 7)

[Bridging](#) (see page 7)

[Broadband](#) (see page 10)

[Device and System Identity](#) (see page 11)

[IP Protocols and Services](#) (see page 12)

[LAN](#) (see page 17)

[Performance](#) (see page 19)

[Routing](#) (see page 20)

[SAN](#) (see page 22)

[Security](#) (see page 23)

[WAN](#) (see page 24)

About Standard Protocols Supported by CA Spectrum

This chapter describes the standard protocols that CA Spectrum supports. When a device is modeled in OneClick, CA Spectrum automatically creates child application models for the standards supported by that device. Information about the standards is available in various OneClick subviews. From OneClick, you can view standard MIB information through model attributes, create attribute watches, and edit attribute values.

The standards that are described in this chapter are organized according to their functionality.

Bridging

This section describes the bridging standards applications that CA Spectrum supports. Bridging applications include models such as Spanning Tree and PPP Bridging.

Bridges are generally more flexible and intelligent than repeaters because they interconnect separate LAN or WAN data links and they learn the addresses of nodes that can be reached over each data link. Traffic can then be relayed selectively across each bridge. The bridging function operates in the MAC (Media Access Control) sublayer and is transparent to layers above the MAC sublayer.

Bridges can interconnect networks using different transmission techniques or MAC methods. A bridge can connect a LAN data link to a WAN telecommunications operation. Multiple bridges can be used to interconnect a series of networks. A pair of bridges with a telecommunications entity located between them can interconnect two different LAN locations.

Individual LAN data links that are interconnected by a bridge are considered to be a single subnetwork. Subnetwork station addresses must be unique and must use the same station address format. An Extended LAN is actually a LAN subnetwork constructed of bridges and is different from a single physical LAN. Operating layers above the MAC sublayer view, the Extended LAN acts as if it were a single LAN data link.

A bridge can implement a frame-filtering mechanism, or filtering bridge, to receive all frames that are transmitted over each attached data link. Based on each frame's destination address, the bridge determines if each frame can be transmitted across the bridge to any other attached data links. A bridge can therefore isolate network traffic generated on a LAN data link from other LAN data links in the Extended LAN. Broadcast traffic generated on one LAN is transmitted across a bridge to other data links to which it is attached; traffic generated by any station is received by all stations on the Extended LAN.

PPP Bridging

PPP (Point-to-Point Protocol) is used for managing the bridge network control protocol on subnetwork interfaces using the family of Point-to-Point protocols.

- RFC 1474
 - **Name:** PPP Bridge
 - **Model Type Name:** PPP_Bridge_App
 - **Name:** PPP_Bridge
 - **Model Type Name:** PPP_BdgApp1474

QBridge

QBridge, or IEEE 802.1Q, defines VLAN tagging, used to allow multiple bridged networks to transparently share the same physical network link without leakage of information between networks.

- RFC 2674
 - **Name:** Q Bridge
 - **Model Type Name:** qbridge_app_05

Source Routing

The Source Routing application contains utilization statistics derived from source routing. This information may be present in bridging token ring packets, and may affect a specific token ring interface. The Source Routing data is collected from the source routing information potentially present in any token ring packet. This information can be present in a transparent bridging or a mixed bridging environment, and can only be valid in a pure source route bridging environment.

- RFC 1525
 - **Name:** Source Routing
 - **Model Type Name:** rfc1525App

Spanning Tree Bridges

A spanning tree bridge learns appropriate routes from frames and verifies that all bridges are using the same network topology. Spanning tree bridges are used to form tree structures in which any two stations on an extended LAN are connected by one active path. A spanning tree bridge is transparent to ordinary stations on the interconnected LANs. To create and maintain the spanning tree, each bridge periodically multicasts Hello packets to all other bridges on the extended LAN. These packets are used to calculate the spanning tree and to verify that all bridges are using the same topology. Redundant links are not used. If a bridge or link failure occurs, the Hello packet transmissions allow the bridges to quickly calculate a new spanning tree.

- RFC 1493
 - **Name:** Spanning Tree
 - **Model Type Name:** Span_Tree_App

Static Bridging

Static bridging deals with destination-address filtering, letting you create an entry that stays in the static routing table without aging out or being removed if a device is powered off.

The Static Group, one of the five groups within the Bridge MIB, contains objects that describe the entity's state with respect to destination address filtering. If destination address filtering is not supported, this group is not implemented. This group is applicable to any type of bridge that performs destination address filtering.

- RFC 1493
 - **Name:** Static
 - **Model Type Name:** Static_App

Transparent Bridges

Transparent bridges operate in a manner that is transparent to network hosts. A transparent bridge learns the network's topology by analyzing the source address of incoming frames from all attached networks. From this process, it builds a table, which it then uses as a basis for traffic forwarding. When a frame is received on one of the bridge's interfaces, the bridge looks up the frame's destination address in its internal table. If the table contains an association between the destination address and any of the bridge's ports, aside from the one on which the frame was received, the frame is forwarded out to the indicated port. If no association is found, the frame is sent to all ports except the inbound port. Broadcasts and multicasts are also flooded in this way.

- RFC 1493
 - **Name:** Transparent
 - **Model Type Name:** Transparnt_App

Broadband

This section describes the broadband standards applications that CA Spectrum supports.

ADSL

ADSL (Asymmetric Digital Subscriber Line) is a continuously available connection over an existing phone line.

- RFC 2662
 - **Name:** ADSLLineApp
 - **Model Type Name:** ADSLLineApp

DOCSIS

DOCSIS (Data Over Cable Service Interface Specifications) is an international standard that defines the communications and operation support interface requirements for a data over cable system. It permits the addition of high-speed data transfer to an existing Cable TV system.

- Draft DOCS-BPI-MIB
 - **Name:** DOCSISBPIApp
 - **Model Type Name:** DOCSISBPIApp
- Draft DOCS-BPI2-MIB
 - **Name:** DOCSISBPI2App
 - **Model Type Name:** DOCSISBPI2App
- RFC 2669
 - **Name:** DOCSISCbIDvApp
 - **Model Type Name:** DOCSISCbIDvApp
- RFC 2670
 - **Name:** DOCSISIFApp
 - **Model Type Name:** DOCSISIFApp
- Draft DOCS-QOS-MIB
 - **Name:** DOCSISQOSApp
 - **Model Type Name:** DOCSISQOSApp

Device and System Identity

This section describes the device and system identity standards applications that CA Spectrum supports.

Entity

RFC 2737, Entity MIB, provides insight into logical and physical entities managed by an SNMP agent.

- RFC 2737
 - **Name:** EntityMIBApp
 - **Model Type Name:** RFC2737App

Host Resources

CA Spectrum supports the following Host Resources standards applications:

- RFC 2790
 - **Name:** Host Resources
 - **Model Type Name:** rfc2790App
- RFC 1514
 - **Name:** Host Resources
 - **Model Type Name:** rfc1514App

System Application

The system application RFC provides objects for fault, configuration, and performance management of applications from a systems perspective.

- RFC 2287
 - **Name:** SystemLvIApp
 - **Model Type Name:** RFC2287App

IP Protocols and Services

This section describes the standards CA Spectrum supports for application models associated with IP protocols and services.

DHCP

DHCP (Dynamic Host Configuration Protocol) is a computer networking protocol used by devices (DHCP clients) to obtain configuration information for operation in an Internet Protocol network.

- RFC 2131
 - **Name:** dhcpApp
 - **Model Type Name:** dhcpApp

ICMP

ICMP (Internet Control Message Protocol) uses IP datagrams and is typically generated in response to errors in IP datagrams or for diagnostic or routing purposes.

- RFC 792
 - **Name:** ICMP
 - **Model Type Name:** ICMP_App

Note: If the firmware on your device supports both the draft and the RFC version of the 2933 MIB, only the RFC2933App is modeled.

IGMP

IGMP (Internet Group Management Protocol) provides support for managing the membership of IP multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships.

- Draft RFC 2933
 - **Name:** IGMP Draft
 - **Model Type Name:** Draft2933App
- RFC 2933
 - **Name:** IGMP
 - **Model Type Name:** RFC2933App

IP

IP (Internet Protocol) is commonly used as a delivery service. IP is a connectionless service responsible for moving datagrams from one device to another. As a delivery agent, IP watches to verify that the datagrams are within shipping regulations. To deliver datagrams, IP deals with two issues: addressing and fragmentation.

- RFC 1354
 - **Name:** IP
 - **Model Type Name:** IP1_App

IPM

The IP Multicast Routing (IPM) standard is used for managing IP Multicast Routing for IPv4, independent of the specific multicast routing protocol in use.

- RFC 2932
 - **Name:** IPMRouteStd
 - **Model Type Name:** RFC2932App

IP Tunnel

IP Tunnel MIB describes managed objects used for managing tunnels of any type over IPv4 networks.

- RFC 2667
 - **Name:** IPTunnel
 - **Model Type Name:** RFC2667App

MPLS

MPLS (Multi-Protocol Label Switching) is a standards-approved technology for speeding up network traffic flow and making it easier to manage.

- MplsVpn Draft 3
 - **Name:** MplsVpnApp
 - **Model Type Name:** MplsVpnApp
- MplsVpn Draft 4
 - **Name:** MplsVpnD4App
 - **Model Type Name:** MplsVpnD4App

MSDP

MSDP (Multicast Source Discovery Protocol) is a standard that describes a mechanism to connect multiple IPv4 protocol independent multicast sparse-mode (PIM) domains together.

- IETF Draft 3
 - **Name:** Msdp_D3_App
 - **Model Type Name:** Msdp_D3_App
- IETF Draft 7
 - **Name:** Msdp_D7_App
 - **Model Type Name:** Msdp_D7_App

PIM

PIM (Protocol Independent Multicast) describes objects used for managing the PIM protocol for IPv4, which is applicable to IPv4 routers that implement PIM.

- RFC 2934
 - **Name:** PIM-MIB
 - **Model Type Name:** rfc2934App

SNMP

SNMP is the standard protocol used to monitor IP gateways and the networks to which they attach.

- RFC 1213
 - **Name:** MIB-I
 - **Model Type Name:** SNMP1_Agent
- RFC 1213
 - **Name:** MIB-II
 - **Model Type Name:** SNMP2_Agent
- RFC 4293
 - **Name:** SNMP2_v6_Agent
 - **Model Type Name:** SNMP2_v6_Agent

- RFC 2271, RFC 3411
 - **Name:** SNMP Management Frameworks
 - **Model Type Name:** RFC2271App
- RFC 3413
 - **Name:** SNMP Applications
 - **Model Type Name:** RFC3413App
- RFC 3584
 - **Name:** SNMP Coexistence
 - **Model Type Name:** RFC3584App
- RFC 3415
 - **Name:** View-based Access Control Model
 - **Model Type Name:** RFC3415App
- RFC 1213
 - **Name:** System
 - **Model Type Name:** System1_App

TCP

TCP (Transmission Control Protocol) refers to the connection-oriented transport (communications) protocol used in the Internet suite.

- RFC 2012
 - **Name:** TCP
 - **Model Type Name:** TCP1_App

UDP

UDP (User Datagram Protocol) is part of the transport layer of the OSI model and uses the services of IP to deliver data.

- RFC 2013
 - **Name:** UDP
 - **Model Type Name:** UDP1_App

LAN

This section describes the LAN standards applications that CA Spectrum supports.

Character Stream

The Character Stream application standard provides objects for the management of character stream devices, specifically to interface ports that carry a character stream, whether physical or virtual, serial or parallel, synchronous or asynchronous.

- RFC 1316
 - **Name:** Character Stream
 - **Model Type Name:** RFC1316App

Ethernet

The Ethernet standard provides objects for managing ethernet, such as media.

- RFC 1284
 - **Name:** Ethernet IF App
 - **Model Type Name:** EthernetIfApp

FDDI

FDDI (Fiber Distributed Data Interface) provides speed and reliability to a LAN and is often used as a backbone technology as well as a means of connecting high-speed computers in a local area. CA Spectrum supports the following FDDI applications:

- RFC 1512
 - **Name:** FDDI
 - **Model Type Name:** rfc1512App
 - **Name:** SMT_1
 - **Model Type Name:** GenFDDISmt_II
 - **Name:** MAC_1.1
 - **Model Type Name:** GenFDDIMac_I
 - **Model Type Name:** GenFDDIMac_II

Link Aggregation

Link aggregation is supported via the IEEE8023-LAG-MIB, developed by IEEE for managing 802.3ad.

- 802.3ad
 - **Name:** LinkAggregation
 - **Model Type Name:** 802dot3adApp

Power Over Ethernet

Power over Ethernet (POE) provides objects that allow management of power ethernet power sourcing equipment.

- RFC 3621
 - **Name:** Power Ethernet
 - **Model Type Name:** RFC3621App

For devices that support POE, their corresponding device model's POE interfaces can be identified through the POE column in the Interfaces table. You can disable the POE interface identification by changing the value of the 'EnablePOEMapping' attribute on the selected device model.

Note: For more information about setting attribute values, see the *Modeling and Managing Your IT Infrastructure Administrator Guide*.

RS-232

RS-232 is one of several common data terminal equipment (DTE) or data circuit-terminating equipment (DCE) interface standards. There are three RS-232 applications:

- RFC 1317
 - **Name:** RS-232
 - **Model Type Name:** RFC1317App
 - **Name:** RS-232 sync
 - **Model Type Name:** RFC1317sync
 - **Name:** RS-232 async
 - **Model Type Name:** RFC1317async

Token Ring

The standard for the Token Ring protocol is IEEE 802.5. FDDI also uses a Token Ring protocol.

- RFC 1231
 - **Name:** Token Rng IF App
 - **Model Type Name:** TokenRingIfApp

Wireless LAN

802.11 is a family of IEEE standards for wireless local area networks (WLANs).

- 802.11
 - **Name:** WirelessLAN
 - **Model Type Name:** 802dot11App

Performance

This section describes the standards CA Spectrum supports for performance-related application models.

RMON

The RMON (Remote Network Monitoring) MIB is based on RFC1757 (Ethernet) and RFC1513 (Token Ring). It is divided into the following groups:

- Statistics
- History
- Alarm
- Host
- HostTopN
- Matrix
- Filter
- Packet Capture

- Event
- Token Ring

Each group defines a set of objects to be monitored. In addition, each group stores data and statistics collected by the agent on the device, which may have multiple network interfaces.

The RMONApp model accesses and presents RMON data from all network interfaces supported by a device. CA Spectrum supports the following RMON application models:

- RFC 1757, RFC 1513
 - **Name:** RMON
 - **Model Type Name:** RMONApp
- RFC 1757
 - **Name:** E Probe
 - **Model Type Name:** RMONEthProbe
- RFC 1513
 - **Name:** T R Probe
 - **Model Type Name:** RMONTRProbe

Traceroute/Lookup

The Traceroute/Lookup standard defines objects for performing remote ping, traceroute, and lookup operations at a remote host.

- RFC 2925
 - **Name:** RFC2925App
 - **Model Type Name:** RFC2925App

Routing

This section describes the routing standards applications that CA Spectrum supports.

BGP4

BGP (Border Gateway Protocol) is the core routing protocol of the Internet.

- RFC 1269
 - **Name:** BGP4
 - **Model Type Name:** BGP4_App

IP Routing

The IP routing applications contain information used by CA Spectrum to resolve the interconnections of devices through the network at the IP level (Layer 3).

- RFC 1213, RFC 2096, RFC 1354
 - **Name:** IP Routing
 - **Model Type Name:** IPRtrApp
 - **Name:** IP Routing
 - **Model Type Name:** IP2RtrApp

IS-IS Routing

The Intermediate System to Intermediate System (IS-IS) routing protocol is used to build routing tables for IP networks.

- RFC 4444
 - **Name:** IS-IS Routing
 - **Model Type Name:** RFC4444App

OSPF

The OSPF (Open Shortest Path First) protocol is a hierarchical interior gateway protocol (IGP) for routing.

- RFC 1253
 - **Name:** OSPF
 - **Model Type Name:** OSPF2RtrApp

Repeater

The Repeater standard provides support for objects used to manage IEEE 802.3 repeaters, sometimes referred to as hubs.

- RFC 1516
 - **Name:** SNMP-Repeater
 - **Model Type Name:** rfc1516App

RIP2

RIP2 (Routing Information Protocol 2) is a distance-vector routing protocol.

- RFC 1724
 - **Name:** RIP2
 - **Model Type Name:** RFC1724App

VRRP

The VRRP (Virtual Router Redundancy Protocol) application allows several routers on a multi-access link to use the same virtual IP address. One router is elected as the master with the other routers acting as backups. This allows host systems to be configured (manually or using DHCP) with a single default gateway rather than running an active routing protocol. This protocol also supports the ability to load-share traffic when both routers are up.

- RFC 2338
 - **Name:** VRRP
 - **Model Type Name:** VRRPApp

SAN

This section describes the SAN (Storage Area Network) standards applications that CA Spectrum supports.

Fibre Channel

Fibre Channel is a gigabit-speed network technology. It is the standard connection type for SAN in enterprise storage.

- Draft FC MGMT-MIB
 - **Name:** FcMgmt
 - **Model Type Name:** DraftFcMgmtApp
- Draft RFC 2837
 - **Name:** FcFabricElement
 - **Model Type Name:** Draft2837App
- RFC 2837
 - **Name:** FcFabricElement
 - **Model Type Name:** RFC2837App

The CA Spectrum DraftFcMgmtApp application model type supports versions 3.0 and 4.0 of the Fibre Channel Management Framework Integration MIB, which was developed by the Fibre Alliance in order to provide an integrated management environment for an enterprise class storage network. If a device that supports this MIB is modeled with CA Spectrum, a DraftFcMgmtApp model is created for that device.

Security

This section describes the security-related standards CA Spectrum supports.

Port-Based Network Access Control

The IEEE 802.1x standard is designed to enhance the security of wireless local area networks (WLANs). It provides an authentication framework for wireless LANs, allowing a user to be authenticated by a central authority.

- 802.1x
 - **Name:** PortNetAccControl
 - **Model Type Name:** 802dot1xApp

RADIUS

CA Spectrum supports the following RADIUS (Remote Authentication Dial-In User Service) standards applications:

- RFC 2618
 - **Name:** RADIUS Authentication Client
 - **Model Type Name:** RFC2618App
- RFC 2620
 - **Name:** RADIUS Accounting Client
 - **Model Type Name:** RFC2620App

User-Based Security Model

This standard provides a description of the User-based Security Model (USM) for SNMP. It defines the elements of procedure for providing SNMP message-level security and provides objects for remotely monitoring and managing the configuration parameters for this security model.

- RFC 3414
 - **Name:** User-based Security Model
 - **Model Type Name:** RFC3414App

WAN

Wide Area Network (WAN) data link technology is used to implement point-to-point connections between devices. This section describes the WAN standards applications that CA Spectrum supports.

ATM

The ATM (Asynchronous Transfer Mode) Client application allows you to monitor virtual channel links and change channel statistics.

- RFC 1695
 - **Name:** ATM_Client
 - **Model Type Name:** ATMClientApp
 - **Name:** ATM_Switch
 - **Model Type Name:** ATMSwitchApp

DS1

DS1 is a high-speed baseband transmission link.

- RFC 1406
 - **Name:** DS1
 - **Model Type Name:** DS1App1406
 - **Model Type Name:** DS1_1406App
- RFC 1232
 - **Name:** DS1
 - **Model Type Name:** RFC1232App

Frame Relay

Frame relay is a packet-based interface standard that has been optimized for the transport of protocol-oriented data. The frame relay interface specification provides a signaling and data transfer mechanism. Frame relay's ability to statistically multiplex means that paths or virtual circuits are defined throughout the network, but no bandwidth is allocated to the paths until data needs to be transmitted. Frame relay provides multiple logical connections within a single physical connection.

RFC 1315 is the MIB for Frame Relay DTEs (Data Terminal Equipment).

- RFC 1315
 - **Name:** Frame Relay
 - **Model Type Name:** FR_1315App
 - **Name:** Frame Relay
 - **Model Type Name:** rfc1315App

Note: The FR_1315App replaces the rfc1315App when Frame Relay Manager is installed.

RFC 2115 is the MIB for Frame Relay DTEs using SMIv2.

- RFC 2115
 - **Name:** FrameRelayApp
 - **Model Type Name:** rfc2115App

PNNI

PNNI (Private Network-to-Network Interface) is a suite of network protocols that can be used to discover an ATM network topology, create a database of topology information, and route calls over the discovered topology.

- PNNI-MIB
 - **Name:** PNNI_App
 - **Model Type Name:** PNNI_App

PPP

The PPP (Point-to-Point Protocol) application provides a method for transmitting datagrams over serial point-to-point links.

- Draft IETF-PPP-MIB
 - **Name:** PPP
 - **Model Type Name:** PPPLinkApp

SONET

SONET (Synchronous Optical Network) applications let you manage SONET/SDH (Synchronous Digital Hierarchy) interfaces. The following SONET standards are supported by CA Spectrum:

- RFC 1595
 - **Name:** SONET
 - **Model Type Name:** rfc1595App
- RFC 2558
 - **Name:** SONET
 - **Model Type Name:** rfc2558App

Chapter 2: Accessing Standard Protocol Information in OneClick

This section describes how to access standards-based application information in OneClick. You can access application models and the information related to them from the device's Information tab or by using the search functionality in the Locator tab.

This section contains the following topics:

[Access Standards-Based Information Using the Information Tab](#) (see page 27)

[Locator Search](#) (see page 27)

Access Standards-Based Information Using the Information Tab

Depending on the device you have modeled, you may have various OneClick subviews available to you from the Information tab in the Component Detail panel. From these subviews you can view application model information.

To access standards-based information from a specific device model

1. Select the device from which you want to view RFC information.
2. In the Component Details panel, in the Information tab, expand the subview containing the information you want to review.

Various subviews will be available depending on what MIB standards the device supported when it was modeled.

Locator Search

You can use the search functionality in the Locator tab to find application models and to subsequently view application model information. Search results appear in the Results tab of the Contents panel. Detailed information for application models selected in the results list appears in the Component Detail panel.

Search for Application Models

If you are not sure which device to access for the application models you want to view, you can use the Locator tab's search functionality to list every application model that was created and to which you have access rights.

Note: If you are operating a Distributed SpectroSERVER (DSS) environment, some searches require you to select which landscapes to include in your search from the 'Select Landscapes to Search' dialog.

To access application models using Locater search

1. Click the Locater tab in the Navigation panel.
2. In the Locater tab, in the Name column, click 'Application Models' to expand it, and then do one of the following:
 - Double-click 'All Application Models.'
 - Click 'All Application Models,' and then click the 'Create a new search' button.
3. Enter any additional information if prompted, depending on the type of search you are running, and click OK.

If additional input is not required, the search runs immediately and the search results appear in the Results tab of the Contents panel.

4. To narrow your search, enter further criteria in the Filter box at the top of the results list in the Results tab.

For example, if you were looking for the Repeater application, you could enter **1516** in the Filter box, which would find the Repeater model by its Model Type Name, 'rfc1516App.' Alternatively, you could enter **repeater** in the Filter box, which would find the Repeater model by its Name, '<device_name>_SNMP-Repeater.'

The Results tab refreshes to show only those models that match the criteria in the Filter box.

5. In the Results tab list, select the application model you want more information about.

The Component Detail view displays details about the selected application model.

6. Click any of the available tabs in the Component Detail view to review information specific to the selected application model.

Note: For more information about using Locater search functionality, see the *Operator Guide*.

Appendix A: RFC Reference

The following is a list of all RFCs that are supported by CA Spectrum. RFC support is typically provided in the form of application models, which allows it to be dynamically applied to any device model in CA Spectrum that is identified as supporting the particular RFC, including GnsnmpDev.

RFC Number	RFC Name	RFC Description
RFC1286	RFC1286-MIB	Definitions of Managed Objects for Bridges.
RFC1493	BRIDGE-MIB	
RFC1474	PPP-BRIDGE-NCP-MIB	
RFC2674	Q-BRIDGE-MIB	Management Information Base for Network Management of TCP/IP-based Internets: MIB-II.
RFC1525	SOURCE-ROUTING-MIB	Definitions of Managed Objects for Source Routing Bridges.
RFC1289	RFC1289-phivMIB	DECnet Phase IV MIB Extensions.
RFC1559	DECNET-PHIV-MIB	
RFC2662	ADSL-LINE-MIB	Definitions of Managed Objects for the ADSL Lines.
RFC2669	DOCS-CABLE-DEVICE-MIB	DOCSIS Cable Device MIB Cable Device Management Information Base for DOCSIS Compliant Cable Modems and Cable Modem Termination Systems.
RFC2670	DOCS-IF-MIB	Radio Frequency (RF) Interface Management Information Base for MCNS/DOCSIS Compliant RF Interfaces.
RFC2737	ENTITY-MIB	The MIB module for representing multiple logical entities supported by a single SNMP agent.
RFC1514	HOST-RESOURCES-MIB	Host Resources MIB.
RFC2790		
RFC1565	APPLICATION-MIB	Network Services Monitoring MIB.
RFC2248	NETWORK-SERVICES-MIB	
RFC2788		

RFC Number	RFC Name	RFC Description	
RFC1566	MTA-MIB	Mail Monitoring MIB.	
RFC2249			
RFC2789			
RFC1567	DSA-MIB	X.500 Directory Monitoring MIB.	
RFC2605			
RFC1628	UPS-MIB	UPS Management Information Base.	
RFC2287	SYSAPPL-MIB	Definitions of System-Level Managed Objects for Applications. The MIB module defines management objects that model applications as collections of executables and files installed and executing on a host system. The MIB presents a system-level view of applications; objects in this MIB are limited to those attributes that can typically be obtained from the system itself without adding special instrumentation to the applications.	
RFC792		Internet Control Message Protocol (ICMP).	
RFC2933	IGMP-STD-MIB	The MIB module for IGMP Management.	
RFC1158	RFC1158-MIB	Management Information Base for Network Management of TCP/IP-based internets: MIB-II.	
RFC1213	RFC1213-MIB		
RFC1354	RFC1354-MIB		
RFC2011	IP-MIB		
RFC2012	TCP-MIB		
RFC2013	UDP-MIB		
RFC2096	IP-FORWARD-MIB		
RFC4293	IP-MIB		
RFC2465	IPV6-TC		
RFC2452	IPV6-TCP-MIB		
RFC1573	IANAifType-MIB		The MIB module which defines the IANAifType textual convention, and thus the enumerated values of the ifType object defined in MIB-II's ifTable.
RFC1907	SNMPv2-MIB		The MIB module for SNMPv2 entities.

RFC Number	RFC Name	RFC Description
RFC2233	IF-MIB	The MIB module to describe generic objects for network interface sub-layers. This MIB is an updated version of the MIB-II ifTable, and incorporates the extensions defined in RFC1229.
RFC2863		
RFC2213	INTEGRATED-SERVICES-MIB	The MIB module to describe the Integrated Services Protocol.
RFC2932	IPMROUTE-STD-MIB	The MIB module for management of IP Multicast routing, but independent of the specific multicast routing protocol in use.
RFC2667	TUNNEL-MIB	The MIB module for management of IP Tunnels, independent of the specific encapsulation scheme in use.
RFC2934	PIM-MIB	The MIB module for management of PIM routers.
RFC2271	SNMP-FRAMEWORK-MIB	An Architecture for Describing SNMP Management Frameworks.
RFC3411		
RFC3413	SNMP-TARGET-MIB	Defines five types of SNMP applications that make use of an SNMP engine as described in STD 62, RFC3411.
RFC3584	SNMP-COMMUNITY-MIB	Describes the coexistence between Version 1, Version 2, and Version 3 of the Internet-Standard Network Management Framework.
RFC3415	SNMP-VIEW-VASED-ACM-MIB	View-Based Access Control Model (VACM) for the Simple Network Management Protocol.
RFC1316	RFC1316-MIB	Definitions of Managed Objects for Character Stream Devices using SMIV2.
RFC1658	CHARACTER-MIB	
RFC1284	RFC1284-MIB	Definitions of Managed Objects for the Ethernet-like Interface Types.
RFC1398	RFC1398-MIB	
RFC1623	EtherLike-MIB	
RFC1643		
RFC2665		
RFC1285	RFC1285-MIB	FDDI Management Information Base.

RFC Number	RFC Name	RFC Description
RFC1512	FDDI-SMT73-MIB	
RFC3621	POWER-ETHERNET-MIB	An extension to the Ethernet-like Interfaces MIB with a set of objects for managing Power Sourcing Equipment (PSE).
RFC1317	RFC1317-MIB	Definitions of Managed Objects for RS-232-like Hardware Devices using SMIv2.
RFC1659	RS-232-MIB	
RFC1318	RFC1318-MIB	Definitions of Managed Objects for Parallel-printer-like Hardware Devices using SMIv2.
RFC1660	PARALLEL-MIB	
RFC1231	RFC1231-MIB	IEEE 802.5 MIB using SMIv2.
RFC1743	TOKENRING-MIB	
RFC1748		
RFC1271	RFC1271-MIB	Remote Network Monitoring Management Information Base Version 2 using SMIv2.
RFC1757	RMON-MIB	
RFC2021	RMON2-MIB	
RFC2925	DISMAN-PING-MIB	Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations.
RFC4560		
RFC1269	RFC1269-MIB	Definitions of Managed Objects for the Fourth Version of the Border Gateway Protocol (BGP-4) using SMIv2.
RFC1657	BGP4-MIB	
RFC1243	RFC1243-MIB	AppleTalk Management Information Base II.
RFC1742	APPLETALK-MIB	
RFC1248	RFC1248-MIB	OSPF Version 2 Management Information Base.
RFC1252	RFC1252-MIB	
RFC1253	RFC1253-MIB	
RFC1850	OSPF-MIB	
RFC1368	SNMP-REPEATER-MIB	Definitions of Managed Objects for IEEE 802.3 Repeater Devices.
RFC1516		
RFC2108		

RFC Number	RFC Name	RFC Description
RFC3289	DIFFSERV-DSCP-TC	The Textual Conventions defined in this module should be used whenever a Differentiated Services Code Point is used in a MIB.
RFC1724	RIPv2-MIB	The MIB module to describe the RIP2 Version 2 Protocol.
RFC2837	FIBRE-CHANNEL-FE-MIB	The MIB module for Fibre Channel Fabric Element.
RFC2618	RADIUS-AUTH-CLIENT-MIB	The OID assigned to Remote Access Dialin User Service (RADIUS) MIB work by the IANA.
RFC2620	RADIUS-ACC-CLIENT-MIB	The MIB module for entities implementing the client side of the RADIUS accounting protocol.
RFC2574	SNMP-USER-BASED-SM-MIB	The management information definitions for the SNMP User-Based Security Model.
RFC3414		
RFC1696	Modem-MIB	Modem Management Information Base (MIB) using SMIv2.
RFC2787	VRRP-MIB	Definitions of Managed Objects for the Virtual Router Redundancy Protocol (VRRP).
RFC1695	ATM-MIB	Definitions of Managed Objects for ATM Management.
RFC2514	ATM-TC-MIB	
RFC2515	ATM-MIB	
RFC1232	RFC1232-MIB	Definitions of Managed Objects for the DS1, E1, DS2, and E2 Interface Type.
RFC1406	RFC1406-MIB	
RFC2495	DS1-MIB	
RFC1233	RFC1233-MIB	Definitions of Managed Objects for the DS3/E3 Interface Type.
RFC1407	RFC1407-MIB	
RFC2496	DS3-MIB	
RFC1315	RFC1315-MIB	Management Information Base for Frame Relay DTEs Using SMIv2.
RFC2115	FRAME-RELAY-DTE-MIB	

RFC Number	RFC Name	RFC Description
RFC1595	SONET-MIB	Definitions of Managed Objects for the SONET/SDH Interface Type.
RFC2558		

Index

A

- accessing standards-based information
 - from device model • 27
 - from Locator • 27
- ADSL • 10
- ATM • 24

B

- BGP4 • 21
- bridging applications • 7
- broadband applications • 10

C

- Character Stream • 17

D

- device and system identity applications • 11
- DHCP • 12
- DOCSIS • 11
- DS1 • 25

E

- Entity • 11
- ethernet • 17

F

- FDDI • 17
- frame relay • 25

H

- host resources • 12

I

- ICMP • 13
- IGMP • 13
- IP • 13
- IP protocols and services applications • 12
- IP routing • 21
- IP tunnel • 14
- IPM • 14

L

- LAN applications • 17
- link aggregation • 18
- Locator tab, search • 27

M

- MPLS • 14
- MSDP • 15

O

- OSPF • 21

P

- performance applications • 19
- PIM • 15
- PNNI • 26
- POE • 18
- port-based network access control • 23
- PPP • 8, 26

Q

- QBridge • 8

R

- RADIUS • 24
- Repeater • 22
- RFC 1158 • 29
- RFC 1213 • 15, 21, 29
- RFC 1231 • 19
- RFC 1232 • 25
- RFC 1253 • 21
- RFC 1269 • 21
- RFC 1284 • 17
- RFC 1315 • 25
- RFC 1316 • 17
- RFC 1354 • 13, 21, 29
- RFC 1406 • 25
- RFC 1474 • 8, 29
- RFC 1493 • 9, 10
- RFC 1512 • 17
- RFC 1513 • 19
- RFC 1514 • 12, 29
- RFC 1516 • 22

RFC 1525 • 9
RFC 1566 • 29
RFC 1567 • 29
RFC 1573 • 29
RFC 1595 • 26
RFC 1628 • 29
RFC 1695 • 24
RFC 1724 • 22
RFC 1757 • 19
RFC 1907 • 29
RFC 2011 • 29
RFC 2012 • 16, 29
RFC 2013 • 16, 29
RFC 2096 • 21, 29
RFC 2115 • 25
RFC 2131 • 12
RFC 2233 • 29
RFC 2248 • 29
RFC 2249 • 29
RFC 2271 • 15
RFC 2287 • 12, 29
RFC 2338 • 22
RFC 2452 • 29
RFC 2465 • 29
RFC 2558 • 26
RFC 2605 • 29
RFC 2618 • 24
RFC 2620 • 24
RFC 2662 • 10, 29
RFC 2667 • 14
RFC 2669 • 11, 29
RFC 2670 • 11, 29
RFC 2674 • 8, 29
RFC 2737 • 11, 29
RFC 2789 • 29
RFC 2790 • 12, 29
RFC 2837 • 23
RFC 2863 • 29
RFC 2925 • 20
RFC 2932 • 14
RFC 2933 • 13, 29
RFC 2934 • 15
RFC 3411 • 15
RFC 3413 • 15
RFC 3414 • 24
RFC 3415 • 15
RFC 3584 • 15
RFC 3621 • 18
RFC 4293 • 15, 29

RFC 792 • 13, 29
RFC descriptions • 29
RFC1286 • 29
RFC1493 • 29
RFC1559 • 29
RFC1565 • 29
RFC2 789 • 29
RFC792 • 29
RIP2 • 22
RMON • 19
routing applications • 20
RS-232 • 18

S

SAN • 22
SAN applications • 22
security applications • 23
SNMP • 15
SONET • 26
source routing • 9
standard protocols • 7
static bridging • 9
system application • 12

T

token ring • 19
traceroute/lookup • 20
transparent bridges • 10

U

UDP • 16
user-based security model • 24

V

VRRP • 22

W

WAN • 24
WAN applications • 24
WLANs • 19