

# Entuity<sup>®</sup> 16.5 Entuity User Reference Manual

Entuity empowers service providers, systems integrators and enterprises with network control and predictability foundational to meeting any of today's complex IT infrastructure challenges. Entuity provides a succinct suite of the most important functionality for network management – inventory, fault and performance management – but presented in an easy to use, quick to deploy format.

#### North America Headquarters 4 Mount Royal Avenue Suite 340 Marlborough, MA 01752 Tel: +1 508 357 6344 Fax: +1 508 357 6358

#### EMEA Headquarters

9a Devonshire Square London, EC2M 4YN Tel: +44 (0)20 7444 4800 Fax: +44 (0)20 7444 4808

#### Entuity

The Entuity product and its related documentation are protected by copyright and distributed under licenses restricting use, copying, distribution and decompilation. Unless you have negotiated with Entuity specific terms and conditions for using its product and associated documentation, such use shall be governed by Entuity's standard licence terms, a copy of which is distributed with the product.

Entuity may make improvements and/or changes to the product(s) and/or program(s) described in this publication at any time. These changes will be incorporated into new editions of the relevant publication.

Entuity®, SurePath®, Eye of the Storm®, InSight Center®, Green IT Perspective™, Network Delivery Perspective™ and Service Delivery Perspective™ are registered trademarks of Entuity. All other trademarks are the property of their respective owners.

License terms and conditions of use for Entuity and included third party software can be found on the Entuity server at *entuity\_home/licenseTerms/*. A listing of these third party trademarks, references and software included with Entuity is available through its web UI.

## Contents

1	Entuity	/ User	Reference	<b>Materials</b>

2	Device and Device Components
	Device General Attributes
	Device Stream Attributes
	Device Topology Node10
	Device Associations
3	Port and Port Components
	Port General Attributes15
	Port Stream Attributes
	Weighted Rollups for Fault and Discard24
	Port MAC Addresses25
	Hot Standby Router Protocol (HSRP) Details26
	HSRP Port State27
	Load Balancer Ports27
	Load Balancer Ports Traffic28
	Load Balancer Ports Utilization
	Matrix Switch Port Inventory29
	Port Topology Node
	Port Associations
	Plada O anterna
4	BladeCenters
	BladeCenter Management
	BladeCenter Attributes
	BladeCenter Stream Attributes
	Media Tray
	Chassis Voltages
	Chassis Temperature
	BladeCenter Blades
	Blades Inventory
	Blade State
	Blade Temperature
	Blade Voltages

#### 5 VM Platforms

	Virtual Platforms General	
	Virtual Platform Hypervisor General	
	Virtual Platform VM Guest O/S40	
	VMware Switches	
	vSwitch Details40	
	Virtual Port Group Details41	
	Virtual Port Group Connection Details43	
	Amazon Web Services44	
	Hypervisors and Zones44	
	Virtual Machine44	
	Virtual Machine/Instance45	
	Block Device Mapping46	
	Volume	
	VNIC	
	Security Group48	
	Virtual Private Cloud48	
	Placement Group48	
	Region49	
	Subnet49	
	VPNConnection49	
	Static Route50	
	Route Table50	
	Route50	
	Customer Gateway51	
	Elastic IP51	
6	Applications and Application Sonvers	
0	Application Servers	
	Application Details	
	Application Server Details	
7	CUCMs	
	CUCM as a Managed Host Application	
	CUCM Details	
	CUCM General Attributes	
	CUCM General Stream Attributes57	
	CUCM Associations58	
	CUCM CTI Devices	
	CTI Device Attributes	
	CTI Device Stream Attributes60	
	CUCM Device Pools60	

	CUCM Groups	.60
	Device Pool Attributes	.61
	CUCM Phone Extension	.62
	Phone Extension Attributes	.62
	Phone Extension Stream Attributes	.62
	Failed Phone Attributes	.62
	Gatekeeper Devices	.63
	Gatekeeper Attributes	.63
	Gatekeeper Stream Attributes	.63
	Gateway Devices	.63
	Gateway General Attributes	.63
	Gateway Stream Attributes	.64
	CUCM H.323 Devices	.65
	H.323 General Attributes	.65
	H.323 Stream Attributes	.66
	Inter-Region Bandwidths	.66
	General Attributes	.67
	Media Devices	.67
	General Attributes	.67
	Media Device Stream Attributes	.68
	Phones	.69
	General Attributes	.69
	Phone Stream Attributes	.69
	Phone Extensions Attributes	.70
	CUCM Processes	.70
	Process General Attributes	.71
	Process Stream Attributes	.71
	Voicemail Devices	.71
	Voicemail General Attributes	.71
	Voicemail Stream Attributes	.72
	Remote CUCMs	.72
	Remote CUCM General Attributes	.73
0	Cines Unified Computing System (UCS)	
8	Cisco Unified Computing System (UCS)	75
		.15
	Cisco LICS Liconsing	.15
	Supple and Incidents	.11
	Compute Plade	.10
		.10

	Association	79
	Fans	79
	Local Disk	80
	Management Interface	81
	Power Supplies	82
	Association	83
	Rack Unit	83
	Service Profiles	83
	Association	84
	Slot	84
	Storage Controller	84
	Association	85
	Switch Card	85
	Association	86
	Temperature Sensor	86
	VNIC Ethernet	87
9	Entuity Firewall	
	Firewall General Attributes	
	Representing Firewall Connectivity	90
	Nokia/Checkpoint Firewall	90
	Firewall Packages	90
	Firewall High Availability Stream Attributes	91
	High Availability Module Inventory	93
	NetContinuum Firewall	93
	NetContinuum Monitored Server Attributes	94
	NetContinuum Monitored Server Stream Attributes	94
	NetContinuum Application Status Attributes	94
	NetContinuum Application Status Stream Attributes	94
10	) Load Balancers	
	Load Balancer Summary	97
	Load Balancer Resources	98
	Load Balancer Advanced	100
	Load Balancer Stream Attributes	101
	Local Pools	
	Real Servers	
	Virtual Services	
	Virtual Servers	

-		
-n	tu	
	u	uy.

11 Multiprotocol Label Switching (MPLS)	
Label Distribution Protocol (LDP)	108
LDP Overview	109
MPLS LDP Entity General Attributes	110
MPLS LDP Entity Stream Attributes	111
MPLS LDP Peers	112
MPLS LDP Peers General Attributes	113
MPLS LDP Label Ranges	114
MPLS LDP Peer Status	114
MPLS LDP Label Ranges	115
MPLS LDP Label Range MPLS LDP Peers	115
Label Switch Routers	115
MPLS LSR	115
MPLS VPN	117
MPLS VRF General	118
MPLS Route Targets	118
MPLS VRFs Status	119
MPLS Interface VRF Instances General	120
MPLS Interface VRF BGP Neighbors	120
VRF on an Interface Instance	121
12 Power over Ethernet	
PoE Midspan Injectors	122
Overview of Microsemi PoE Midspan Injectors	122
Entuity PoE Implementation	122
Entuity PoE Injector Devices	123
PoE Injector Attributes	123
PoE Injector Stream Attributes	123
PoE Injector Port Attributes	124
PoE Injector Port Stream Attributes	124

### 13 Entuity QoS

QoS Overview	126
Collecting QoS Data	126
Simple QoS Example	126
Traffic Identification through Access Groups	127
Access Group General Details	128
Access Group Status	128
Traffic Management through Class Maps	128
Class Map General Details	129

Access Groups associated with Class Maps	129
Class Map Status	129
Policy Maps	130
Policy Map General Details	130
Classes associated with Policy Maps	130
QoS Traffic Policing	
Traffic Policing General Details	131
Traffic Policer Status	131
Managing Congestion through Queues	
Queue General Details	
Queue Status	133
Congestion Avoidance	
Random Early Detection General Details	
Random Early Detection Status	135
QoS Packet Marking	
Set General Details	
QoS Traffic Shaping	
Traffic Shaping General Details	
Traffic Shaping Status	139
14 Routing Protocols	
BGP Bouting Protocol	140
Device Advanced Info	140
BGP Device Attributes	141
BGP Peer Stream Attributes	
EIGBP Bouting Protocol	142
EIGRP Peer Attributes	
EIGRP Local Interface	142
EIGRP Peer Stream Attributes	142
OSPE Bouting Protocol	143
OSPE General Attributes	143
OSPF Peer Stream Attributes	144
IS-IS Bouting Protocol	144
IS-IS Support	145
IPv6 Peering	······································
	146
	146
15 Entuity Cisco SSL Services	146

### 16 VPN Gateways

VPN Attributes	·	149
----------------	---	-----

Entuity			
	-		5 A
	E	DTU	11/
		nua	IL Y

VPN Gateway Resources	155
17 Wireless Controllers and WAPs	
Wireless Controllers	156
Wireless Controllers Stream Attributes	156
Trapeze WAPs	160
Trapeze WAPs General Attributes	160
Trapeze WAPs Stream Attributes	160
Cisco WAPs	161
Cisco WAPs General Attributes	161
Cisco WAPs Stream Attributes	161
AWAPs and their Wireless Ports	162
AWAPs	162

#### **18 WAAS**

WAAS General Attributes	164
WAAS Stream Attributes	164
WAAS Device Connection Details	165
WAAS Device Connection Statistics	166
WAAS Device Connection Status	166
Glossary	167
Index	195

# **Figures**

Figure 1	Port Advanced Details	14
Figure 2	Virtual Switch Advanced Details	41
Figure 3	Virtual Port Group	42
Figure 4	Port Group Connections Advanced	44
Figure 5	Applications on a Device	54
Figure 6	Entuity UCS Data Model Tree	74
Figure 7	UCS Device Summary	76
Figure 8	Mapping Firewalls	90
Figure 9	Load Balancer Data Types and Associations	96
Figure 10	Load Balancer Summary	97
Figure 11	Current Sessions Chart	98
Figure 12	Load Balancer Resources	99
Figure 13	Load Balancer Processor with High CPU Utilization	100
Figure 14	Load Balancer Data	101
Figure 15	Pool Data	104
Figure 16	Real Servers	105
Figure 17	Virtual Services	106
Figure 18	Virtual Servers	107
Figure 19	MPLS LDP Label Range MPLS LDP Peers	115
Figure 20	A Simple MPLS VPN Configuration	118
Figure 21	IS-IS Port Peer	145
Figure 22	IS-IS Routing Map	146
Figure 23	SSL Proxy Device	147
Figure 24	Trapeze Wireless Controller Details	159
Figure 25	Autonomous WAP Details	163

# **Tables**

Table 1	Device General Tab3
Table 2	Device Stream Attributes
Table 3	Port Topology Node 10
Table 4	Port Topology Node 11
Table 5	Device Associations 11
Table 6	Port Attributes
Table 7	Port Stream Attributes 17
Table 8	Port MAC Addresses
Table 9	HSRP Details
Table 10	HSRP Port State
Table 11	Load Balancer Ports 27
Table 12	Load Balancer
Table 13	Load Balancer Ports Traffic
Table 14	Load Balancer Ports Utilization
Table 15	Load Balancer Statistics
Table 16	Port Topology Node
Table 17	BladeCenter Associations
Table 18	BladeCenter Attributes
Table 19	BladeCenter Stream Attributes
Table 20	Hypervisor General Details
Table 21	Virtual Platform VM Guest O/S 40
Table 22	vSwitch Advanced Details 40
Table 23	Virtual Port Group Connection 41
Table 24	Virtual Port Group Connection 43
Table 25	Hypervisors and Zones Attributes 44
Table 26	Virtual Machine Attributes
Table 27	Instance Attributes
Table 28	Block Device Mapping Attributes 46
Table 29	Volume Attribute
Table 30	VNIC Attributes
Table 31	Security Group Attributes
Table 32	Virtual Private Cloud Attributes
Table 33	Placement Group Attributes
Table 34	Region Attributes
Table 35	Subnet Attributes
Table 36	VPNConnection Attributes
Table 37	Static Route Attributes
Table 38	Route Table Attributes 50
Table 39	Route Attributes 51
Table 40	Customer Gateway Attributes 51
Table 41	Elastic IP Attributes

Table 42	Application Summary Page5	53
Table 43	Application Details 5	54
Table 44	Application Server Details 5	55
Table 45	CUCM General Attributes 5	57
Table 46	CUCM General Stream Attributes 5	57
Table 47	CTI Device Attributes 5	59
Table 48	CTI Device Stream Attributes 6	0
Table 49	Device Pool Attributes 6	61
Table 50	CUCM Phone Extension Attributes 6	62
Table 51	CUCM Phone Extension Stream Attributes 6	62
Table 52	CUCM Failed Faulty Phone Attributes 6	62
Table 53	Gatekeeper Device Attributes	63
Table 54	CUCM Gatekeeper Stream Attributes 6	63
Table 55	CUCM Gateways Attributes 6	64
Table 56	Gateways Stream Attributes 6	64
Table 57	CUCM H.323 Devices Attributes 6	65
Table 58	CUCM H.323 Devices Stream Attributes 6	6
Table 59	CUCM Inter Region Bandwidths Attributes 6	67
Table 60	Media Devices Attributes 6	67
Table 61	Media Device Stream Attributes 6	8
Table 62	Phones Attributes	6
Table 63	Phones Stream Attributes	6
Table 64	Phone Extensions Attributes7	0
Table 65	CUCM Processes Attributes	'1
Table 66	CUCM Process Stream Attributes7	′1
Table 67	CUCM Voicemail Attributes 7	′1
Table 68	CUCM Voicemail Stream Attributes7	2
Table 69	Remote CUCM Attributes 7	<b>'</b> 3
Table 70	UCS Licensing	7
Table 71	Compute Blade Attributes 7	8'
Table 72	Compute Blade Associations7	8'
Table 73	Fans General Attributes7	<b>'</b> 9
Table 74	Fans Stream Attributes 8	80
Table 75	Local Disk Attributes	80
Table 76	Local Disk Stream Attributes 8	81
Table 77	Management Interface Attributes 8	81
Table 78	Management Interface Stream Attributes 8	32
Table 79	Power Supply Attributes 8	32
Table 80	Power Supply Stream Attributes 8	32
Table 81	Rack Unit Attributes 8	33
Table 82	Service Profiles Attributes	34
Table 83	Slot Attributes	34
Table 84	Storage Controller Attributes	85
Table 85	Switch Card Attributes 8	85

Table 86	Switch Card Stream Attributes	86
Table 87	Temperature Sensor Attributes	87
Table 88	Temperature Sensor Stream Attributes	87
Table 89	VNIC Ethernet Attributes	87
Table 90	Firewall General Attributes	89
Table 91	Firewall Packages	91
Table 92	Firewall High Availability Stream Attributes	91
Table 93	High Availability Inventory	93
Table 94	Monitored Server Attributes	94
Table 95	Monitored Server Stream Attributes	94
Table 96	Monitored Application Status Attributes	94
Table 97	NetContinuum Monitored Application Stream Attributes	94
Table 98	Load Balancers Stream Attributes	101
Table 99	MPLS LDP Entity Attributes	110
Table 100	MPLS LDP Entity Status	111
Table 101	Remote Peer Attributes	113
Table 102	MPLS LDP Peers General Attributes	113
Table 103	MPLS LDP Label Ranges	114
Table 104	MPLS LDP Peer Status	114
Table 105	MPLS LSR	116
Table 106	MPLS VRF General	118
Table 107	MPLS Route Targets	119
Table 108	MPLS VRFs Status	119
Table 109	MPLS Interface VRF Instances	120
Table 110	MPLS Interface VRF BGP Neighbors	120
Table 111	VRF on an Interface Instance	121
Table 112	Entuity PoE Attributes	123
Table 113	PoE Injector Stream Attributes	124
Table 114	PoE Injector Port Attributes	124
Table 115	PoE Injector Port Stream Attributes	124
Table 116	Access Group General Details	128
Table 117	Access Group Status	128
Table 118	Class Map General Details	129
Table 119	Class Map Status	129
Table 120	Policy Map General Details	130
Table 121	Classes associated with Policy Maps	130
Table 122	Traffic Policing General Details	131
Table 123	Traffic Policer Status	131
Table 124	Queue General Details	132
Table 125	Queue Status	133
Table 126	Random Early Detection General Details	134
Table 127	Random Early Detection Status	135
Table 128	Set General Details	136
Table 129	Traffic Shaping General Details	138

Table 130	Traffic Shaping Status 139
Table 131	Device BGP General Attributes 140
Table 132	BGP Device Attributes 141
Table 133	BGP Peer Stream Attributes 141
Table 134	EIGRP General Attributes 142
Table 135	EIGRP Local Interface 142
Table 136	EIGRP Peer Stream Attributes
Table 137	OSPF General Attributes
Table 138	OSPF Peer Stream Attributes 144
Table 139	SSL Proxy Stream Attributes 148
Table 140	VPN Stream Attributes
Table 141	Wireless Controllers Stream Attributes 156
Table 142	Trapeze WAPs General Attributes 160
Table 143	Trapeze WAP Stream Attributes
Table 144	Cisco WAP General Attributes
Table 145	Cisco WAP Stream Attributes
Table 146	Autonomous WAP Details 162
Table 147	WAAS General Attributes 164
Table 148	WAAS Stream Attributes
Table 149	WAAS Device Connection Details 165
Table 150	WAAS Device Connection Statistics 166
Table 151	WAAS Device Connection Status

# **1** Entuity User Reference Materials

This reference manual details attribute information, useful when understanding the relevance of attribute values. Information is grouped according to their parent type:

- Chapter 2 Device and Device Components
- Chapter 3 Port and Port Components
- Chapter 4 BladeCenters
- Chapter 5 VM Platforms
- Chapter 6 Applications and Application Servers
- Chapter 7 CUCMs
- Chapter 9 Entuity Firewall
- Chapter 10 Load Balancers
- Chapter 11 Multiprotocol Label Switching (MPLS)
- Chapter 12 Power over Ethernet
- Chapter 13 Entuity QoS
- Chapter 14 Routing Protocols
- Chapter 15 Entuity Cisco SSL Services
- Chapter 16 VPN Gateways
- Chapter 17 Wireless Controllers and WAPs
- Chapter 18 WAAS.

For details on Entuity system processes and configuration files and parameters refer to the *Entuity System Administrator Reference Manual*, which provides access to information useful to system administrators wanting to understand or adjust Entuity configuration. Specifically it details:

- Descriptions of Entuity system processes, utilities and third party tools.
- System files, including configuration options.
- Generic trap definitions, detailing the OIDs and trap formats of generic standard and standard enterprise traps. Entuity identifies the OID substring and then the trap number, from which it can generate an appropriate event in Event Viewer.

Internal Entuity identifiers. Entuity uses a series of codes to identify the types of objects it manages. These internal codes are sometimes useful when troubleshooting or integrating with Entuity.

# 2 Device and Device Components

### **Device General Attributes**

Attribute	Description	Device Type
BGP Identifier	Each router running BGP must have a BGP identifier. This identifier is included in the BGP identifier field of open messages, which are sent between two BGP peers when establishing a BGP session.	All
BGP Local AS	Local AS of the device.	All
Certified	Entuity certifies the device model used to manage this device type.	All
Configuration Transfer Server	The IP address of the server to receive files is set in entuity.cfg (tftpServerIp) and shared by all transfer methods. Through this attribute administrators can override this IP address on a per device basis, for example when the Entuity server has multiple IP addresses.	
Configuration Retrieval Number of Archives	Number of archived configurations retained by Entuity. By default this is four, i.e. four startup and four running configurations, although it is configurable. These configurations are retrieved by Configuration Monitor.	All
Description	Manufacturers device description.	All
Device Type	Entuity manages devices through the Device Type, e.g. Router, Switch. Devices managed through the VM Platform device type require specific connection details.	All
Location	Text description of the physical location of the device that is contained on the device, e.g. Development Cabinet.	All

Table 1 Device General Tab

Attribute	Description	Device Type
Management Level	<ul> <li>Full - Entuity fully manages the device and all of its interfaces.</li> <li>Full (Mgmt Port Only) - Entuity fully manages the device but only manages the management interface.</li> <li>Full Management (No Ports) - Entuity fully manages the device but does not maintain any port level information.</li> <li>Basic - Entuity collects only basic system information and the full IP address table via SNMP. This management level is used when Entuity does not have the appropriate vendor file, cannot generate an appropriate file or you only want the device placed under basic management.</li> <li>Ping Only - Entuity does not collect SNMP data for these devices, it only reports whether these devices respond to ICMP ping.</li> </ul>	All
Management MAC Address	MAC address of this device.	All
Manufacturer	Manufacturer name and is derived by matching the manufacturer number against the first 2500 Private Enterprise Codes compiled by the Internet Assigned Numbers Authority (http://www.iana.org/assignments/enterprise- numbers). Where the manufacturer code is not matched then the first part of the device name is taken, usually this is the manufacturer's name.	All
Model	Device model.	All
Name	Name of the device	All
OSPF Admin Status (AS)	The status of an OSPF interface defines whether routes and/or OSPF protocol packets are propagated over the interface. Status may be active, passive, or off.	All
OSPF Area Border Router	Identifies the router as one with interfaces in different areas but within the same autonomous system. By collecting mapping information from these area this router can calculate the shortest distances between points.	All
OSPF Autonomous System Border Router	Identifies the router as an Autonomous System Border Router, which acts as a gateway between OSPF and external routes. It is these routers that propagate routes to external networks.	All
OSPF Router ID	The unique identifier for the router as defined by the OSPF router-id command or the address of the loopback 0 interface.	All
OSPF TOS Support	Indicates whether the router supports TOS.	All
Poll Status	Status of Entuity SNMP polling of the device, i.e. Polling, Non-Polling.	All

Table 1 Device General Tab

Attribute	Description	Device Type
Polled Device Name	Name Entuity uses to poll the device.	All
Polled IP Address	IP address Entuity uses to poll the device.	All
Power Consumption	Power consumption in watts of the device.	All
Serial Number	Device serial number.	All
StormWorks ID	Internal identifier of the object.	All
System Capabilities	Indicates the device capabilities, i.e. <b>None</b> , <b>Unknown</b> , <b>Routing</b> , <b>Routing</b> and <b>Switching</b> .	Routers, Switches, PoE
System Description	Textual description of the chassis hardware. This value should include the full name and version identification of the system's hardware and copyright information.	All
System Name	Administratively-assigned name for the chassis. By convention, this is the node's fully-qualified domain name.	All
System Object ID	Manufacturer's authoritative identification of the chassis object identifier.	All
System Services	Set of services that the chassis primarily offers.	
Version	Device version number.	All
Watts	Status of the module, i.e. OK, Standby, Unknown, Other, Minor Alarm, Major Alarm and Down.	All
XML Data Collection	When set to <b>True</b> XML Data Collection is enabled on the device. Entuity XML API currently retrieves the MAC addresses and interface names from the Nexus range of Cisco devices. Credential sets must also be defined for successful XML data collection.	All

Table 1 Device General Tab

### **Device Stream Attributes**

Stream Attribute	Description	Device Type
Active Sessions	Number of active sessions.	Managed Host

Stream Attribute	Description	Device Type
Authenticated Response Time		Managed Host
Average CPU Utilization%	Average CPU utilization across all of the device's CPUs.	All
Average Memory Used%	Percentage of average memory used.	All
Average SNMP Response Time	The average time over the reporting period between the SNMP request being sent by the Entuity server to a device and it receiving a response.	All
Buffer Allocation Failure Rate	Number of buffer allocation failures over the last hour.	Router, Port
Buffer No Memory Failure Rate	Number of buffer No Memory failures caused over the last hour.	Router, Port
Chassis Description	Chassis type, e.g. c2503.	All
Chassis Fan Status	Chassis fan status.	Router, Switch, Load Balancer
Chassis Model Number	Chassis model number.	All
Chassis Serial Number	Chassis serial number.	All
Chassis Status	Chassis Status	Router, Switch, Load Balancer
Chassis Temperature	Chassis temperature status.	Router, Switch, Load Balancer
Current Cache Volume	Current cache volume.	WAAS
Device Reachable Status	Device Reachable Status without Root Cause Analysis	All
Device Reachable Time	Device Reachable Time without Root Cause Analysis	All
Device Reachable Time Unknown	Device Reachable Time without Root Cause Analysis	All
Device Status	Device status.	All
Device SysUpTime Counter Wraps		All
Device UpTime Known	Length of the time the device has been up. You can also run Inventory reports on Device Uptime.	All

Stream Attribute	Description	Device Type
Device UpTime Known%	Time the device was up as a percentage of the reporting period.	All
Device UpTime Unknown		All
Device UpTime Unknown%		All
Event Description	Events	All
Events Summary	Daily Event Rollup	All
External URL Response Time		Managed Host
Firmware Version	ROM system software version.	All
Hardware Version	Chassis hardware revision level.	All
ICMP Redirect Rate	Rate of packets redirected by this device.	Router
ICMP Redirects%	Number of packets redirected in percentages.	Router
ICPM Reachable Known%	Device Reachable Time without Root Cause Analysis	All
ICPM Reachable Unknown%	Device Reachable Time without Root Cause Analysis	All
IP Discard Rate (no route)	Rate of IP packets discarded by the device.	Router
IP Discards (no route)%	Rate of IP packets discarded by the device in percentages.	Router
IP Packet Forward Rate	Rate of IP packets forwarded by the device.	Router
IP Packet Forwards%	Rate of IP packets forwarded by the device in percentages.	Router
IP Packet Received Rate	Rate of IP packets received by the device.	Router
Label Retention Mode	<ul> <li>When set to:</li> <li>Conservative, the advertised label mappings are retained only if they will be used to forward packets, i.e. if label came from a valid next hop.</li> <li>Liberal, all advertised label mappings are retained whether they are from a valid next hop or not.</li> </ul>	Router
Last Reboot Time	The time of the last device reboot.	All

Stream Attribute	Description	Device Type
Last SNMP Restart Time	The last time the SNMP agent restarted. This also indicates when SNMP counters were reset, which is useful when identifying the reasons behind data spikes.	Managed Host
LDP Session Traps Enabled	<ul> <li>When set to:</li> <li>Enabled, the mplsLdpSessionUp and mplsLdpSessionDown can be generated.</li> <li>Disabled, the mplsLdpSessionUp and mplsLdpSessionDown can not be generated. The default is Disabled.</li> </ul>	Router
Loop Detection Capability	<ul> <li>Indicates the LSR loop detection capability, and not necessarily its current state. Loop detection is determined during session initialization, individual sessions may not run with loop detection. Loop detection can be:</li> <li>None, loop detection is not supported on this LSR.</li> <li>Other, loop detection is supported but by a method other than those explicitly defined in the MIB.</li> <li>Hop Count, loop detection is supported only through hop count.</li> <li>Path Vector, loop detection is supported only through path vector.</li> <li>Hop Count And Path Vector, loop detection is supported by both hop count and path vector.</li> </ul>	Router
LSR Cross Connect Traps Enabled	Traps indicating changes to the cross-connect table, e.g. the association between incoming and outgoing segments (labels).	Router
LSR ID	The Label Switching Router (LSR) identifier is the first 4 bytes of the Label Distribution Protocol (LDP) identifier.	Router
LSR In Segment Traps Enabled	Traps indicating incoming MPLS segments (labels). If administrative and operational status objects are down, the LSR does not forward packets. If these status objects are up, the LSR forwards packets.	Router
LSR Out Segment Traps Enabled	Traps indicating outgoing MPLS segments (labels).	Router
Max Label Stack Depth	Maximum stack depth supported by this LSR.	Router
Messages Received	Status messages received in the last five minutes.	Managed Host
Name Resolution State	SNMP Responding State	All

Stream Attribute	Description	Device Type
Newly Disappeared Modules	Module Change History	All
Newly Discovered Modules	Module Change History	All
Number of Active VRFs	Number of configured VRFs currently in use.	Router
Number of Configured VRFs	Number of VRFs configured on the router.	Router
Number of Interfaces Connected to VRFs	Number of interfaces connected to all of the router's VRFs.	Router
Number of LSR Ports	Number of ports.	Router
OSPF Peer Remote IP Addresses	The remote IP address of this entry's OSPF peer.	Router
Processes	Number of processes.	Managed Host
Running Configuration Files	Archived Running Configuration Files	All
SNMP Failure Rate	The rate of failed SNMP requests to the device over the reporting period.	All
SNMP Percent Waiting	The average time Entuity spent waiting for a response to its SNMP requests to a device expressed as a percentage of the total report period. A higher percentage may indicate a higher load on the device.	All
SNMP Response State	SNMP Responding State	All
SNMP Success Rate	The rate of successful SNMP requests to the device over the reporting period.	All
Software Version	Chassis software revision level.	All
Startup Configuration Files	Archived Startup Configuration Files	All
System Contact	Textual identification of the contact person for this managed node, together with information on how to contact this person.	All
System Description	Textual description of the chassis hardware. This value should include the full name and version identification of the system's hardware and copyright information.	All
System Location	Physical location of this chassis, e.g. room 3, 2nd floor.	All

Stream Attribute	Description	Device Type
System Name	Administratively-assigned name for the chassis. By convention, this is the node's fully-qualified domain name.	All
User	Number of users.	Managed Host
VPN Global Route Limit	Number of routes allowed on the router, which is only limited by the amount available for the router.	Router
VPN Notifications Enabled	Must be set to <b>Enable</b> for the router to send MPLS VPN SNMP notifications.	Router

## Device Topology Node

Attribute	Description
Node Key	
Node State	
Root Cause Node	
StormWorks ID	Entuity internal object identifier.
StormWorks Type	StormWorks object type, DeviceTopoNode.

Table 3Port Topology Node

## **Device Associations**

Attribute	Description
Node Key	
Node State	
Root Cause Node	
StormWorks ID	Entuity internal object identifier.
StormWorks Type	StormWorks object type, PortTopoNode.

Table 4Port Topology Node

Association	Device Type
Blades	BladeCenter
Blowers	BladeCenter
Fans	Router
Hypervisors	VM Platform
IP Addresses	All
Local Pools	Load Balancer
Management Modules	BladeCenter
Memory	All
Modules	Router
Monitored Device	All
OSPF Peers	Router
PoE Injector Ports	PoE Injector
Ports	All
Power Supplies	BladeCenter, Router
Processors	All
Real Servers	Load Balancer

Table 5Device Associations

Association	Device Туре
Router Buffers	Router, WAAS
Services	Router, Load Balancer
SSL Certificates	SSL Proxy
SSL Proxy Services	SSL Proxy
Switch Bays	BladeCenter
Virtual Servers	Load Balancer
VLANs	Switch
Volumes	Firewall, Managed Host, WAAS
vSwitches	VM Platform
WAAS Connection	WAAS
Wireless Ports	Autonomous WAP

Table 5 Device Associations

# **3** Port and Port Components

Port and port component details are accessible through Explorer. The Port Advanced page provides a full listing of attributes collected against ports. The depth of information is suitable for advanced users, providing access to detailed information on the port.



The content of the Port Advanced Details page varies according to the port type and the enabled modules. This section indicates the type of available information.

£ entuity	User: admin@century <u>[logou</u> <u>Page Updated</u> : 21:48:25, BST
Dashboards InSight Center Explorer Events Maps Ch	arts Flows Reports Tools Administration Preferences Help
Port: [ Et0/0 ] to c3560 fa0/17 My Network (century.entury.local) Summary + Flows III Threshold A Advanced	(on <u>10.44, 1.36</u> ) d
Attribute	Value
Administrative Status	up
Alias	to c3560 fa0/17
Classification	Physical
Description (Mib2)	Ethernet0/0
Descriptive Alias	
Device Name	10.44.1.36
Duplex Status	Unknown
Inbound Speed	10.0M bps
Interface Description	[ Et0/0 ] to c3560 fa0/17
Operational Status	up
Outbound Speed	10.0M bps
Port MAC	00:03:e3:58:38:00
Short Description	[Et0/0]
Spare Status	No
StormWorks ID	1087
Type (IANA)	Ethernet
VIP Status	Router
Steasm Attribute	Value
	Value
Administrative Status	up
CDP Local Port Name (Mib2)	Ethernet0/0
CDP Local Port Name (ifXMib)	Et0/0
CDP Remote Device IP Address	10.44.1.39
CDP Remote Port Name	FastEthernet0/17
Event Description	Port Inbound Fault High Cleared (No Packet Corruption), source: 10.44.1.36 [Et0/0] to c3560 fa0/17, impacting: UPLINK, details: inFault=0.20% dtresh=1% (no component breakdown) inFault=122/60.12k packets in 300 sec
Events Summary	3 x Port Inbound Fault High Cleared (No Packet Corruption) on Fri May 11 2012
IP Addresses	10.44.1.36/255.255.0.0
Inbound Discards%	0%
Inbound Fault%	0%
Inbound Non-Unicast Packet Rate	34.5 pkts/s
Inbound Peak Traffic	103.978k bos

Figure 1 Port Advanced Details

## **Port General Attributes**

Attribute	Description
Administrative Status	Current port status as set by the system administrator.
Alias	The port's alias.
Alternative Interface Index	
BGP Identifier	Each router running BGP must have a BGP identifier. This identifier is included in the BGP identifier field of open messages, which are sent between two BGP peers when establishing a BGP session.
BGP Local AS	Local AS of the device.
Classification	Indicates whether the port is a physical or virtual port.
Description	Manufacturers device description.
Description (Mib2)	Port description taken from SNMP-MIB2.
Descriptive Alias	Allows entry of a brief description, e.g. Link from Washington to Peterlee. The CIO Perspective's Component Availability report can use this description to add context to a port.
Device	The port's device address.
Device Name	The port's device address.
Duplex Status	The port's duplex status.
Enterprise Interface Index	
Hosts	Lists the hosts using the port.
Inbound Speed	Inbound speed of a port. For use in Entuity your System Administrator can amend the port inbound speed through the Edit dialog from the Advanced tab of the device.
Interface Description	
Interface Index	Unique identifier of the interface.
Location	Text description of the physical location of the device that is contained on the device, e.g. Development Cabinet.
Operational Status	Current operational status, e.g. up, down.

Table 6 Port Attributes

Attribute	Description
Outbound Speed	Outbound speed of a port. For use in Entuity your System Administrator can amend the port outbound speed through the Edit dialog from the Advanced tab of the device.
Peer Distinguished Name	
Peer Port ID	
Peer Slot ID	
Port ID	
Port MAC	
Poll Status	Status of Entuity SNMP polling of the device, i.e. Polling, Non-Polling.
Port Index	The port index number.
Port Interface Type	Indicates the interface type, e.g. ethernet6.
Port MAC Address	Port MAC Address.
QoS Enabled	This attribute is used by the Entuity QoS module to control whether QoS data is collected for the port. By default collection of QoS data is restricted to infrastructure ports, ports with a <i>VIP Status</i> of <b>Router</b> , <b>Trunk</b> , <b>Uplink</b> or <b>Server Link</b> , so only for those ports is <i>QoS Enabled</i> set to <b>Yes</b> . You can override the default value from the Advanced tab of the device.
Role	
Short Description	Brief description of the port. It is also available through Entuity maps.
Slot ID	
Spare Status	Indicates whether Entuity considers the port in use or spare.
StormWorks ID	Entuity internal object identifier.
System Description	Textual description of the chassis hardware. This value should include the full name and version identification of the system's hardware and copyright information.
System Name	Administratively-assigned name for the chassis. By convention, this is the node's fully-qualified domain name.
System Object Identifier	Manufacturer's authoritative identification of the chassis object identifier.
Swtich ID	
Transport	

Table 6 Port Attributes

Attribute	Description
Туре	The managed object type, e.g. port.
Type (IANA)	Indicates the interface type, e.g. ethernet6.
VIP Status	The port type, e.g. Router, Trunk, Uplink, Server Link.
VLANs	The list of VLANs the port is associated to.
Watts	Status of the module, i.e. OK, Standby, Unknown, Other, Minor Alarm, Major Alarm and Down.

Table 6 Port Attributes

## **Port Stream Attributes**

Stream Attribute	Description
Active Oper Status%	
Administrative Status	History of port status as set by the system administrator.
Average CPU Utilization%	Average CPU utilization across all of the device's CPUs.
Average Memory Used%	Percentage of average memory used.
Average SNMP Response Time	Chain of SNMP Response Time
BGP Peer Remote IP Addresses	BGP Peering Changes
Buffer Allocation Failure Rate	Number of buffer allocation failures over the last hour.
Buffer No Memory Failure Rate	Number of buffer No Memory failures caused over the last hour.
CDP Local Port Name (ifxMib)	Port used in the CDP neighbor discovery. The name of the port as read from MIB2.
CDP Local Port Name (Mib2)	Port used in the CDP neighbor discovery. The name of the port as read from MIB2.

Stream Attribute	Description
CDP Remote Device IP Address	Device containing the port which is connected to the local port. The connection is identified through CDP neighborhood discovery.
CDP Remote Port Name	Remote port connected to the local port as identified through CDP neighbor discovery.
Chassis Description	Chassis type, e.g. c2503.
Chassis Fan Status	Chassis fan status.
Chassis Model Number	Chassis model number.
Chassis Serial Number	Chassis serial number.
Chassis Status	
Chassis Temperature	Chassis temperature status.
Device Reachable Status	Device Reachable Status without Root Cause Analysis
Device Reachable Time	Device Reachable Time without Root Cause Analysis
Device Reachable Time Unknown	Device Reachable Time without Root Cause Analysis
Device Status	Device Status
Device SysUpTime Counter Wraps	Reboots
Device UpTime Known	Device UpTime (secs)
Device UpTime Known%	Device UpTime (%)
Device UpTime Unknown	Device UpTime (secs)
Device UpTime Unknown%	Device UpTime (%)
EIGRP Peer Remote IP Addresses	EIGRP Peering Changes
Error free discards (RX)	LSR Performance
Error free discards (TX)	LSR Performance
Event Description	Description of the last event raised against the port, including event type, source and impacted details.
Event Summary	

Stream Attribute	Description
Events Summary	Daily summary of events. Entuity summarizes the number of events of each event type raised against the port.
Firmware Version	ROM system software version.
Hardware Version	Chassis hardware revision level.
ICMP Reachable Known%	Device Reachable Time without Root Cause Analysis
ICMP Reachable Unknown%	Device Reachable Time without Root Cause Analysis
ICMP Redirect Rate	Routing Data
ICMP Redirects%	Routing Data
ICMP TTL Exceeded Rate	Routing Data
ICMP TTL Exceeded%	Routing Data
Inbound Aborts Proportion%	
Inbound Alignment Errors Proportion%	
Inbound CRC Errors proportion%	
Inbound Discarded Packet %	The number of inbound packets discarded, for which no errors were detected, as a percentage of the total number of packets received during the sample period.
Inbound Discarded Packet Rate	The inbound discard rate of packets for which no errors were detected. Packets may be discarded to free up buffer space.
Inbound Discards %	The number of inbound packets discarded, for which no errors were detected, as a percentage of the total number of packets received during the sample period.
Inbound Errored Packet %	The number of inbound packets with errors discarded as a percentage of the total number of packets received during the sample period.
Inbound Errored Packet Rate	The inbound discard rate of packets with errors.
Inbound Fault%	The number of inbound packets with errors discarded as a percentage of the total number of packets received during the sample period.

Stream Attribute	Description
Inbound Interface Speed	Inbound speed of the port. For use in Entuity, system administrator's can amend the port inbound speed through the Edit dialog from the Advanced tab of the device.
Inbound Non-Unicast Packet Rate	The transmission rate of non-unicast (i.e., subnetwork-broadcast or subnetwork-multicast) packets.
Inbound Non-Unicast Packet%	The number of inbound non-unicast (i.e. subnetwork-broadcast or subnetwork-multicast) packets expressed as a percentage of the total number of packets received during the sample period.
Inbound Octet Rate	The number of octets set for transmission during the sample period, this includes packets that were discarded or not sent but excludes packets addressed to a multicast or broadcast address at this sub-layer.
Inbound Packet Rate	The number of packets received during the sample period, this includes errors, discards, good unicast and non-unicast packets and excludes packets addressed to a multicast or broadcast address at this sub-layer.
Inbound Peak Rate	Peak received rate during the sample period expressed as packets per second.
Inbound Traffic	Total inbound traffic during the sample period expressed as bits per second.
Inbound Utilization (WAN) %,	Utilization expressed as a percentage of actual traffic volume received against the maximum volume that can be handled by the port during the polling period.
Interface Type	Interface type, e.g. Ethernet.
IP Addresses	IP addresses assigned to the port.
IP Discard Rate (no route)	Routing Data
IP Discards (no route)%	Routing Data
IP Packet Forward Rate	Routing Data
IP Packet Forwards%	Routing Data
IP Packet Received Rate	Routing Data
Label Retention Mode	When set to:
	Conservative, the advertised label mappings are retained only if they will be used to forward packets, i.e. if label came from a valid next hop.
	Liberal, all advertised label mappings are retained whether they are from a valid next hop or not.
Label Space	LSR Config

Stream Attribute	Description
Labels In Use (RX)	LSR Performance
Labels In Use (TX)	LSR Performance
Last Reboot Time	The time of the last device reboot.
Latest mac address count	Count of MAC addresses identified during the last poll of the device.
LDP Session Traps	When set to:
Enabled	Enabled, the mplsLdpSessionUp and mplsLdpSessionDown can be generated.
	Disabled, the mplsLdpSessionUp and mplsLdpSessionDown can not be generated. The default is Disabled.
Lookup failure discards	LSR Performance
Loop Detection Capability	Indicates the LSR loop detection capability, and not necessarily its current state. Loop detection is determined during session initialization, individual sessions may not run with loop detection. Loop detection can be:
	<b>None</b> , loop detection is not supported on this LSR.
	• Other, loop detection is supported but by a method other than those explicitly defined in the MIB.
	Hop Count, loop detection is supported only through hop count.
	Path Vector, loop detection is supported only through path vector.
	Hop Count And Path Vector, loop detection is supported by both hop count and path vector.
LSR Cross Connect Traps Enabled	Traps indicating changes to the cross-connect table, e.g. the association between incoming and outgoing segments (labels).
LSR ID	The Label Switching Router (LSR) identifier is the first 4 bytes of the Label Distribution Protocol (LDP) identifier.
LSR In Segment Traps Enabled	Traps indicating incoming MPLS segments (labels). If administrative and operational status objects are down, the LSR does not forward packets. If these status objects are up, the LSR forwards packets.
LSR Out Segment Traps Enabled	Traps indicating outgoing MPLS segments (labels).
MAC Address	List of MAC addresses associated with the device.
Mac address history	All of the MAC addresses discovered on the port. This is a change history of the MAC addresses on the port, each time the MACs on a port change Entuity retains a record of all of the MACs on the port at that time (by default Entuity retains fifty samples, although this is configurable through entuity.cfg).

Stream Attribute	Description
Max label (RX)	LSR Config
Max label (TX)	LSR Config
Max Label Stack Depth	Maximum stack depth supported by this LSR.
Max Packet Size	Maximum packet size before fragmentation.
Min label (RX)	LSR Config
Min label (TX)	LSR Config
Most recent mac address(es)	Most recent MAC addresses discovered on the port. Entuity retains MAC addresses for two days after they were last polled on the device (this is a configurable setting through entuity.cfg).
Name Resolution State	SNMP Responding State
Newly Disappeared Modules	Module Change History
Newly Discovered Modules	Module Change History
Nominal interface speed	Interface speed polled from the port.
Number of Active VRFs	Number of configured VRFs currently in use.
Number Of Configured VRFs	Number of VRFs configured on the router.
Number Of Interfaces Connected To VRFs	Number of interfaces connected to all of the router's VRFs.
Number of LSR Ports	Number of ports.
Operational Status	Operational status of the port.
OSPF Peer Remote IP Addresses	OSPF Peering Changes
Outbound Aborts Proportion%	
Outbound Carrier Loss Proportion%	
Stream Attribute	Description
-------------------------------------	--
Outbound Discarded Packet %	The number of outbound packets discarded, for which no errors were detected, as a percentage of the total number of packets transmitted during the polling period.
Outbound Discarded Packet Rate	The outbound discard rate of packets for which no errors were detected. Packets may be discarded to free up buffer space.
Outbound Discards %	The number of outbound packets discarded, for which no errors were detected, as a percentage of the total number of packets transmitted during the polling period.
Outbound Errored Packet %	The number of outbound packets with errors discarded as a percentage of the total number of packets transmitted during the polling period.
Outbound Errored Packet Rate	The outbound discard rate of packets with errors.
Outbound Fault%	The number of outbound packets with errors discarded as a percentage of the total number of packets transmitted during the polling period.
Outbound Interface Speed	Outbound speed of the port. For use in Entuity, system administrator's can amend the port outbound speed through the Edit dialog from the Advanced tab of the device.
Outbound Non-Unicast Packet Rate	The transmission rate of non-unicast (i.e., subnetwork-broadcast or subnetwork-multicast) packets.
Outbound Non-Unicast Packet%	The number of outbound non-unicast (i.e. subnetwork-broadcast or subnetwork-multicast) packets expressed as a percentage of the total number of packets transmitted during the polling period.
Outbound Octet Rate	The number of octets set for transmission during the sample period, this includes packets that were discarded or not sent but excludes packets addressed to a multicast or broadcast address at this sub-layer.
Outbound Packet Rate	The number of packets set for transmission during the sample period, this includes packets that were discarded or not sent but excludes packets addressed to a multicast or broadcast address at this sub- layer.
Outbound Peak Rate	Peak transmission rate during the sample period expressed as packets per second.
Outbound SQE Errors Proportion%	
Outbound Traffic	Total outbound traffic during the sample period expressed as bits per second.

Table 7 Port Stream Attributes

Stream Attribute	Description
Outbound Utilization %	Utilization expressed as a percentage of actual traffic volume transmitted against the maximum volume that can be handled by the port during the polling period.
Packets fragmented	LSR Performance.
Port State	Current state of the port, e.g. Up, Down.
Running Configuration Files	Archived Running Configuration Files.
SNMP Failure Rate	Chain of SNMP Response Time.
SNMP Percent Waiting	Chain of SNMP Response Time.
SNMP Response State	SNMP Responding State.
SNMP Success Rate	Chain of SNMP Response Time.
Software Version	Chassis software revision level.
Startup Configuration Files	Archived Startup Configuration Files.
System Contact	Textual identification of the contact person for this managed node, together with information on how to contact this person.
System Description	Textual description of the chassis hardware. This value should include the full name and version identification of the system's hardware and copyright information.
System Location	Physical location of this chassis, e.g. room 3, 2nd floor.
System Name	Administratively-assigned name for the chassis. By convention, this is the node's fully-qualified domain name.
Time in Current State	Length of time since the last change in Port State.
Time of Last State Change	Date and time of the last change in Port State.
VPN Global Route Limit	Number of routes allowed on the router, which is only limited by the amount available for the router.
VPN Notifications Enabled	Must be set to Enable for the router to send MPLS VPN SNMP notifications.

Table 7Port Stream Attributes

#### Weighted Rollups for Fault and Discard

The hourly and daily rolled up fault and discard data is weighted, taking into account the underlying packet rate at the time of the data sample. For example: A five minute sample which reported 1 inbound packet and a 100% fault (i.e. the 1 packet was

a fault) does not have the same influence on the hourly rollup as a sample with 1000 packets and 100 faults - a fault rate of 10%:

- Sample 1: 1 packet, 1 fault = 100% fault
- Sample 2: 1000 packets, 100 faults, = 10% fault.

Entuity calculates:

```
Weighted Rollup = (1+100) 101 faults / (1 +1000) 1001 packets * 100 = 10.09%
```

 $\odot$ 

This is a simplified example, Entuity would expect 12 5-minute samples in an hourly rollup and not just the 2 used here.

Entuity fault and discard data retention for:

- 5 minute polled data is 8 days.
- 1 hourly rolled up data is 210 days.
- Daily rolled up data is 210 days.

Entuity compresses the main fault and discard values (inFault, outFault, inDiscards, outDiscards) accurate to 3 significant figures. The component values (alignment errors, CRC errors, in-aborts, giants, SQE errors, late collisions, excessive collisions, out-aborts, carrier-loss) are accurate to 2 significant figures.

#### **Port MAC Addresses**

Entuity discovers MAC details associated with ports. MAC addresses are unique identifiers attached to most forms of networking equipment, but they can be changed.

Attribute	Description
Most Recent MAC Address(es)	Most recent MAC addresses discovered on the port. Entuity retains MAC addresses for two days after they were last polled on the device (this is a configurable setting through entuity.cfg).
MAC Address History	All of the MAC addresses discovered on the port. This is a change history of the MAC addresses on the port, each time the MACs on a port change Entuity retains a record of all of the MACs on the port at that time (by default Entuity retains fifty samples, although this is configurable through entuity.cfg).

Table 8 Port MAC Addresses

## Hot Standby Router Protocol (HSRP) Details

Hot Standby Router Protocol (HSRP) establishes a framework between network routers to allow default gateway failover if the primary gateway becomes unavailable. Entuity provides for HSRP:

- Inventory details.
- An inventory Flex Report available through the web interface.
- Two events reporting on changes in active router state.

Attribute	Description
Group Number	Identifies the HSRP standby group. For Token Ring, values between 0 and 2 inclusive are valid. For other media values between 0 and 255 inclusive are valid.
Priority	The priority level of the router. When comparing priorities of two different routers, the router with the numerically higher priority wins, becoming the active router. When both routers have the same priority level the router with the higher IP address wins.
Virtual IP Address	The virtual IP address of the group. When a router's virtual IP address is not configured, it can be derived through an authenticated HSRP hello message.
Active Router	The IP address of the current active router for this HSRP standby group.
Standby Router	The IP address of the current standby router for this HSRP standby group.
Use Configured Virtual IP Address	<ul> <li>When set to:</li> <li>1, indicates Virtual IP Address is a configured IP address.</li> <li>0, indicates Virtual IP Address is derived through an authenticated HSRP hello message.</li> </ul>
Virtual MAC Address	For Ethernet and FDDI, the automatically generated MAC address when HSRP is configured. The standard virtual MAC address used is: 0000.0C07.ACxy, where xy is the group number in hexadecimal. The functional address is used for Token Ring.
Preempt	<ul> <li>When set to:</li> <li>true, a router automatically assumes the active role whenever its priority is higher than the current active router's priority.</li> <li>false, preempt is not enabled. Changes in the active and standby router designation only occur when one or the other goes down, or an election takes place. For example, by default if the active router does not respond to three hello messages, the standby router becomes the active router and a new standby router is identified.</li> </ul>

Table 9 HSRP Details

Attribute	Description
Preempt Delay	The delay between a router coming up and preempting the current active router (only applicable when <i>Preempt</i> is true.) By default this is set to 0 seconds, allowing immediate preemption. You can set a preemption delay, for example to allow the router to populate its routing table before becoming the active router.

Table 9 HSRP Details

## HSRP Port State

Attribute	Description
Standby State	Indicates the current standby state of the router, i.e. Initial, Learn, Listen, Speak, Standby.

Table 10 HSRP Port State

## Load Balancer Ports

Attribute	Description
Learn Mode	The mode of the port, e.g. Learn Forward, No Learn Forward, No Learn Drop.
Enabled	Set to <b>true</b> for enabled, <b>false</b> for disabled.
Duplex Status	The port's duplex status.

Table 11 Load Balancer Ports

Entuity currently manages F5 Labs Big IP 6400 Load Balancer. Entuity delivers additional polling of the device ports using F5 lab's propriety MIB, returning.

Attribute	Description
Port Identification	Load balancer specific details.
Port Status	Standard Entuity port status details.

Table 12 Load Balancer

Attribute	Description
Port Utilization	Standard Entuity port utilization measures displayed through the Load Balancer Port Utilization tab. Administrators can also set port utilization event thresholds, and therefore have events raised, against load balancer utilization.
Port Traffic	Standard Entuity port traffic measures displayed through the Traffic (Load Balancer Port) tab. Administrators can also set port traffic event thresholds, and therefore have events raised, against load balancer traffic.

Table 12 Load Balancer

## Load Balancer Ports Traffic

Attribute	Description
Inbound octets per sec	Inbound octets per second.
Outbound octets per sec	Outbound octets per second.
Inbound packets per sec	Inbound packets per second.
Outbound packets per sec	Outbound packets per second.
Inbound errors per sec	Inbound errors per second.
Outbound errors per sec	Outbound errors per second.
Inbound drops per sec	Inbound drops per second.
Outbound drops per sec	Outbound drops per second.
Collisions per sec	Number of collisions on the port per second.

Table 13 Load Balancer Ports Traffic

## Load Balancer Ports Utilization

Attribute	Description
Inbound Utilization%	Inbound utilization of the load balancer port as a percentage of the port capacity.
Outbound Utilization%	Outbound utilization of the load balancer port as a percentage of the port capacity.

Table 14 Load Balancer Ports Utilization

## Matrix Switch Port Inventory

Attribute	Description
Matrix Connected Blade	Blade Number containing the port this port is connected to.
Matrix Connected Blade	Port Number with the blade that this port is connected to.

Table 15 Load Balancer Statistics

# Port Topology Node

Attribute	Description
Node Key	
Node State	
Root Cause Node	
StormWorks ID	Entuity internal object identifier.
StormWorks Type	StormWorks object type, PortTopoNode.

Table 16 Port Topology Node

## **Port Associations**

The Entuity data structure expands collection of port information and relationships through associated components. From Ports Advanced page the Associations section provides details and hyperlinks from the port to its associations, for example:

- Access Point
- Autonomous WAP Device
- Device, the port's device
- EIGRP Peer
- HSRP Port Groups

#### Entuity

- Host MAC Addresses
- IP Addresses
- IPv6 Interface
- Layer 3 Port Peers
- MPLS Interface VRF Instances
- MPLS LDP Ranges
- Module
- Parent MPLS LDP Label Range
- Policy Maps
- Vlans
- Xedia Traffic Classes.

# **4 BladeCenters**

# **BladeCenter Management**

The Entuity BladeCenter module allows Entuity to manage IBM BladeCenters in a similar manner to other devices, e.g. switches, routers and hubs.

Entuity groups BladeCenter components into managed associated objects.

Association	Description
Blades	A blade encloses the server hardware.
Blowers	BladeCenters usually have two blowers (fans), empty blow bays are not displayed.
Management Modules	BladeCenter has two management modules, one acts as a backup to the other, inheriting its configuration. By default this data is polled every twenty-four hours and retained for six months.
Power Supplies	BladeCenter holds up to four power modules. For consistency within Entuity modules are referred to as Power Supply Units and named from one to four, i.e. PSU1, PSU2, PSU3 and PSU4. By default this data is polled every twenty-four hours and retained for six months. Empty power module bays are not displayed.
Switch Bays	Entuity monitors ethernet switch modules using an enhanced form of its standard ethernet switch support facilities. For example, the Nortel switch module uses the Nortel proprietary MIB as the source of the port names and these can be defined in the switch configuration. Ports are listed in Entuity using names that reflect their purpose such as connections to specific bays/blades/slots or the main connection to the external network. By default this data is polled every twenty-four hours and retained for six months.

 Table 17
 BladeCenter Associations

# **BladeCenter Attributes**

Attributes	Description
BIA	Burned-in MAC (BIA) address.
BladeCenter Name	Name of the BladeCenter.
Data Rate	Data transfer rate to be used over the Ethernet interface.

Table 18 BladeCenter Attributes

Attributes	Description
DHCP Enabled	Indicates whether DHCP is enabled on this interface.
Duplex Setting	Duplex setting for the data transfer over the Ethernet interface.
Gateway IP Address	IP address of the default gateway for the blade server (typically configured on a Layer 3 device). The IP address of the gateway/router for the Ethernet interface.
Host Name	DNS host name for this interface.
IP Address	IP address for the Ethernet interface.
LAA	Locally administered MAC address
MTU	Maximum Transmission Unit for the Ethernet interface.
Name	Name.
Serial Number	Chassis VPD serial number.
Subnet Mask	Subnet mask for the Ethernet interface.
Туре	Chassis type.
Blades	
Blade Name	Blade slot identifier.
Blade Bay	Name of the blade taken from the OID.
Switch Bays	
Bay Name	Switch bay name of this switch in the BladeCenter.
Bay Number	Number of this switch bay.

Table 18 BladeCenter Attributes

# **BladeCenter Stream Attributes**

Stream Attributes	Description
Chassis FRU Number	Chassis Field Replacement Unit number.
Chassis Hardware Revision	Chassis hardware revision.
Chassis Manufacturing ID	Chassis hardware manufacturer identifier, e.g. IBM.

Stream Attributes	Description
Chassis UUID	Chassis Universally Unique Identifier.
Chassis +2.5V Rail Minimum	Minimum power supply voltage reading of the +2.5V rail expressed in millivolts.
Chassis +3.3V Rail Average	Average power supply voltage reading of the +3.3V rail expressed in millivolts.
Chassis +3.3V Rail Maximum	Maximum power supply voltage reading of the +3.3V rail expressed in millivolts.
Chassis +3.3V Rail Minimum	Minimum power supply voltage reading of the +3.3V rail expressed in millivolts.
Chassis +5V Rail Average	Average power supply voltage reading of the +5V rail expressed in millivolts.
Chassis +5V Rail Maximum	Maximum power supply voltage reading of the +5V rail expressed in millivolts.
Chassis +5V Rail Minimum	Minimum power supply voltage reading of the +5V rail expressed in millivolts.
Front Panel Average Temperature	Front panel average temperature in degrees centigrade.
Front Panel Maximum Temperature	Front panel maximum temperature in degrees centigrade.
Front Panel Minimum Temperature	Front panel minimum temperature in degrees centigrade.
Management Module Average Temperature	Management module average temperature in degrees centigrade.
Management Module Maximum Temperature	Management module maximum temperature in degrees centigrade.
Management Module Minimum Temperature	Management module minimum temperature in degrees centigrade.
Model	Chassis model.
Media Tray FRU Number	Field Replacement Unit number of the media tray.
Media Tray Hardware Revision	Media tray VPD hardware revision number.
Media Tray Manufacturing ID	Identifies the media tray manufacturer.
Chassis -5V Rail Average	Average power supply voltage reading of the -5V rail expressed in millivolts.
Chassis -5V Rail Maximum	Maximum power supply voltage reading of the -5V rail expressed in millivolts.

Stream Attributes	Description
Chassis -5V Rail Minimum	Minimum power supply voltage reading of the -5V rail expressed in millivolts.
Chassis +1.8V Rail Average	Average power supply voltage reading of the +1.8V rail expressed in millivolts.
Chassis +1.8V Rail Maximum	Maximum power supply voltage reading of the +1.8V rail expressed in millivolts.
Chassis +1.8V Rail Minimum	Minimum power supply voltage reading of the +1.8V rail expressed in millivolts.
Chassis +12V Rail Average	Average power supply voltage reading of the +12V rail expressed in millivolts.
Chassis +12V Rail Maximum	Maximum power supply voltage reading of the +12V rail expressed in millivolts.
Chassis +12V Rail Minimum	Minimum power supply voltage reading of the +12V rail expressed in millivolts.
Chassis +2.5V Rail Average	Average power supply voltage reading of the +2.5V rail expressed in millivolts.
Chassis +2.5V Rail Maximum	Maximum power supply voltage reading of the +2.5V rail expressed in millivolts.
Media Tray UUID	Media tray Universally Unique Identifier.
Revision	Hardware revision.
FRU Number	Field Replacement Unit number.
UUID	Unique Unit Identifier.
Blades	
Blade +1.25V Rail Average	Average power supply voltage reading of the +1.25V rail expressed in millivolts.
Blade +1.25V Rail Maximum	Maximum power supply voltage reading of the +1.25V rail expressed in millivolts.
Blade +1.25V Rail Minimum	Minimum power supply voltage reading of the +1.25V rail expressed in millivolts.
Blade +1.5V Rail Average	Average power supply voltage reading of the +1.5V rail expressed in millivolts.
Blade +1.5V Rail Maximum	Maximum power supply voltage reading of the +1.5V rail expressed in millivolts.
Blade +1.5V Rail Minimum	Minimum power supply voltage reading of the +1.5V rail expressed in millivolts.
Blade +12V Rail Average	Average power supply voltage reading of the +12V rail expressed in millivolts.
Blade +12V Rail Maximum	Maximum power supply voltage reading of the +12V rail expressed in millivolts.
Blade +12V Rail Minimum	Minimum power supply voltage reading of the +12V rail expressed in millivolts.
Blade +2.5V Rail Average	Average power supply voltage reading of the +2.5V rail expressed in millivolts.

Stream Attributes	Description
Blade +2.5V Rail Maximum	Maximum power supply voltage reading of the +2.5V rail expressed in millivolts.
Blade +2.5V Rail Minimum	Minimum power supply voltage reading of the +2.5V rail expressed in millivolts.
Blade +3.3V Rail Average	Average power supply voltage reading of the +1.8V rail expressed in millivolts.
Blade +3.3V Rail Maximum	Maximum power supply voltage reading of the +1.8V rail expressed in millivolts.
Blade +3.3V Rail Minimum	Minimum power supply voltage reading of the +1.8V rail expressed in millivolts.
Blade +5V Rail Average	Average power supply voltage reading of the +5V rail expressed in millivolts.
Blade +5V Rail Maximum	Maximum power supply voltage reading of the +5V rail expressed in millivolts.
Blade +5V Rail Minimum	Minimum power supply voltage reading of the +5V rail expressed in millivolts.
Connection Type	Blade State.
Connection Type	Indicates the blade server connection type is none, ethernet, or fiber.
CPU1 Temperature	Temperature of the blade's first CPU, measured in degrees centigrade.
CPU2 Temperature	Temperature of the blade's second CPU, measured in degrees centigrade.
DASD Temperature	Temperature of the blade's DASD, measured in degrees centigrade.
Daughter Card Type	Type of daughter card held by the blade.
Daughter FRU Number	Field Replacement Unit number of the blade daughter card.
Daughter Manufacturing ID	Daughter card hardware manufacturer identifier, e.g. IBM.
Daughter Revision	Blade daughter card's hardware revision.
Daughter UUID	Blade daughter hardware Universally Unique Identifier.
Health State	System health state for the blade server, Unknown, Good, Warning and Bad.
Health State Severity	Indicates the state of health of the blade server, i.e. unknown, good, warning and bad.
Health Summary Description	Description of the state of health of the blade server.
Machine Type	Blade hardware VPD machine type.
Manufacturing ID	Manufacturing ID.
Owns KVM	Indicates whether the KVM is owned by the blade, i.e. either false or true.
Owns Media Tray	Indicates whether the remote media tray is owned by the blade, i.e. either false or true.
Power State	Indicates whether the server blade specified is powered <b>on</b> or <b>off</b> .

Stream Attributes	Description
Remote KVM Enable	Indicates whether the state of the remote keyboard/video/monitor for the blade server is either <b>disabled</b> or <b>enabled</b> .
Remote Media Enable	Indicates whether the state of the remote media tray for the blade server is <b>disabled</b> or <b>enabled</b> .
Remote Power Enable	Indicates whether the state of the remote power for the blade server is <b>disabled</b> or <b>enabled</b> .
Remote Wake On LAN Enable	Indicates whether the state of the remote wake on the LAN for the blade server is either <b>disabled</b> or <b>enabled</b> .
Serial Number	Blade Serial Number.
Blowers	
Blower Speed	Speed of the blower as a percentage of its maximum rate.By default Entuity polls for blower speed every fifteen minutes, rolled up as statistical data and retained for six months.
Switch Bays	
Firmware Build Date	Switch module firmware build date.
Firmware Build ID	Switch module firmware build identifier.
Firmware Revision Number	Switch module firmware revision number.
Type of Switch Module	The type of switch module installed.

#### Media Tray

BladeCenter Media Tray displays information on the BladeCenter media tray. By default this data is polled twenty-four hourly and retained for six months.

#### **Chassis Voltages**

BladeCenter Chassis Voltages displays information on the BladeCenter chassis power supply voltage. By default this data is polled every fifteen minutes, rolled up as statistical data and retained for six months.



Voltage rails are instrumented in the MIB as strings with the measurement shown to two decimal places. In Entuity, the voltage attributes are stored as signed integers representing the voltage in millivolts, e.g. +5.07 volts is represented as 5070 millivolts. This allows the voltages to be plotted graphically.

#### **Chassis Temperature**

BladeCenter Temperature displays information on the BladeCenter temperature. By default this data is polled every fifteen minutes, rolled up as statistical data and retained for six months.

Temperatures are instrumented as strings with the measurement shown to two decimal places. Entuity rounds the measurement, allowing easier plotting. The precision of the temperature measurement within a degree is of little relevance the values will be stored in signed integers. This allows the temperatures to be plotted graphically.

# **BladeCenter Blades**

There are fourteen bays in a chassis and each bay can accept one blade. A blade encloses the server hardware. BladeCenter Blades tab displays information on the BladeCenter blade server. By default this data is polled every twenty-four hours and retained for six months.



The terms blade and bay are used interchangeably in this document.

#### **Blades Inventory**

Blades Inventory tab details the blade and any blade daughter cards. By default this data is polled every twenty-four hours and retained for six months.

#### **Blade State**

The Blade State indicates the state of each blade. By default blade state data is polled every fifteen minutes and retained for one week

#### **Blade Temperature**

The Blade Temperature tab indicates the temperature of each blade. By default blade state data is polled every fifteen minutes.

 $\odot$ 

Although temperatures are instrumented as strings with the measurement shown to two decimal places, Entuity displays temperature values as signed integers. The loss of precision is marginal but does allow temperatures to be plotted graphically.

## **Blade Voltages**

BladeCenter Blade Voltages displays information on the blade server power supply voltage. By default this data is polled every fifteen minutes, rolled up as statistical data and retained for six months.

Voltage rails are instrumented in the MIB as strings with the measurement shown to two decimal places. In Entuity the voltage attributes are stored as signed integers representing the voltage in millivolts, e.g. +5.07 volts is represented as 5070 millivolts. This allows the voltages to be plotted graphically.

# **5 VM Platforms**

Through the VM Platform device type Entuity manages these VM platforms:

- Amazon Web Services
- VMware ESXi
- Microsoft Hyper-V
- Oracle VM.

Entuity integrates management of virtual machines, e.g. their virtual CDROMs, virtual controllers using the same mechanisms as for managing real machines' CDROMs and controllers. In addition Entuity manages the VM platform, its hypervisors and virtual machines.

#### **Virtual Platforms General**

A VM Platform is an Entuity device type, and as one Entuity can collect standard device details, e.g. Type, location, IP Address.

#### **Virtual Platform Hypervisor General**

Attribute	Description
Hypervisor Product Name	Product name, version and build of the VM platform. When VMs on an Oracle platform are not running, they are not associated to a hypervisor. Entuity associates these VMs to its own logical construct, an unassigned hypervisor.
Hypervisor Name	User-specified guest physical memory size.
Hypervisor Product Build	Build number of the hypervisor.
Hypervisor Total Memory	Total physical memory on the hypervisor.
Hypervisor Product Version	Version number of the hypervisor.

Table 20 Hypervisor General Details

## Virtual Platform VM Guest O/S

Attribute	Description
Guest OS	Operating system implemented on the VM.
Memory (MB)	User defined guest physical memory size.
Name	Name of the VM.
Configuration File	Location and name of the VM configuration file.
VMUUID	Universal Unique Identifier for the Virtual Machine. Keeping the same identifier when moving/copying a VM maintains its properties, e.g. keeps the same MAC address.

Table 21 Virtual Platform VM Guest O/S

# **VMware Switches**

There are three types of VMware vSwitch:

- VMware standard vSwitch, usually deployed for standalone VMware hypervisors.
- VMware distributed vSwitch, a distributed vSwitch provided by VMware which allows multiple hypervisors to connect to a shared distributed switch and supports vMotion, DRS, etc.
- Cisco Nexus 1000v, provides the same functionality as the VMware distributed vSwitch, but with enhanced configuration options and performance operations.

#### vSwitch Details

Attribute	Description
Current Ports	Total number of ports currently active on the vSwitch.
Кеу	User defined guest physical memory size.
Max Ports	Name of the VM.
Name	Location and name of the VM configuration file.
StormWorks ID	Universal Unique Identifier for the Virtual Machine. Keeping the same identifier when moving/copying a VM maintains its properties, e.g. keeps the same MAC address.

Table 22 vSwitch Advanced Details

Attribute	Description
Туре	vSwitch type, e.g. Distributed Switch, Standard vSwitch.
VM Platform Device ID	Unique VM platform identifier.
Association	
Services	Services associated with the vSwitch.
SNMP Polled vSwitch	You may also manage a vSwitch as an SNMP polled device. This provides a link to the polled data.
Port Groups	Port groups provide VLAN type tagging isolation between VMs within the confines of a virtual switch. Each port group is identified by a network label, which is unique to the current host.

Table 22 vSwitch Advanced Details

VSwitch: vSwitch0 (on blade) Regional (century)	
<u>ກໍ່</u> Summary 🛄 Threshold ກຼໍ່ <b>ປີ Advanced</b>	
Attribute	Value
Current Ports	43
Кеу	13165,blade.entuity.local,key-vim.host.VirtualSwitch-vSwitch0
Max Ports	64
Name	vSwitch0
StormWorks ID	13208
Туре	Standard vSwitch
VM Platform Device ID	13165
Association	Objects
Services	
SNMP Polled vSwitch	
Port Groups	Management Network, Physical Adapters, VM Network

#### Figure 2 Virtual Switch Advanced Details

## Virtual Port Group Details

Attribute	Description
Current Ports	Total number of ports currently active on the vSwitch.
Кеу	User defined guest physical memory size.

Table 23 Virtual Port Group Connection

Attribute	Description
Max Ports	Maximum number of ports in the VM group.
Name	Location and name of the VM configuration file.
StormWorks ID	Universal Unique Identifier for the Virtual Machine. Keeping the same identifier when moving/copying a VM maintains its properties, e.g. keeps the same MAC address.
Туре	Virtual Port Group type, e.g. Distributed Port Group, Standard Port Group.
VLAN	A port group label may have an appended VLAN identifier.
Association	
Services	Services associated with the vSwitch.
vSwitch	vSwitch associated with the virtual port group.
vSwitch Uplinks	Uplinks associated with the virtual port group.
Connections	Port group connection to the VM.

Table 23 Virtual Port Group Connection

#### Virtual Port Group: Management Network (on <u>vSwitch0</u>) Regional (century)

,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	
ភ្នំ Summary 🔟 Threshold រ្បំ🕁 Advanced	
Attribute	Value
Compound Key	13165,blade.entuity.local,key-vim.host.VirtualSwitch-vSwitch0,key- vim.host.PortGroup-Management Network
Key	key-vim.host.PortGroup-Management Network
Name	Management Network
StormWorks ID	13217
Туре	Standard Port Group
VLAN	No VLAN
Association	Objects
Services	
vSwitch	vSwitch0
vSwitch Uplinks	
Connections	MAC: b8:ac:6f:82:5e:c9

Figure 3 Virtual Port Group

# Virtual Port Group Connection Details

Attribute	Description
Entity	Total number of ports currently active on the vSwitch.
Key	User defined guest physical memory size.
MAC	Name of the VM.
Name	Location and name of the VM configuration file.
StormWorks ID	Universal Unique Identifier for the Virtual Machine. Keeping the same identifier when moving/copying a VM maintains its properties, e.g. keeps the same MAC address.
VLAN	A port group label may have an appended VLAN identifier.
VNIC Key	Virtual NIC key.
Association	
Services	Services associated with the vSwitch.
Port	vSwitch associated with the virtual port group.
Virtual Machine	Uplinks associated with the virtual port group.
Port Group	Port group connection to the VM.
Virtual NIC	Virtual NIC.

Table 24 Virtual Port Group Connection

Port Group Connection	MAC: 00:0c:29:02:1b:4e	(NFAEE-Lin)
-----------------------	------------------------	-------------

Regional (century)

ភ្នំ Summary 🛄 Threshold ភ្នំជ្ Adv	ranced 🔠
Attribute	Value
Entity	
Кеу	key-vim.host.PortGroup.Port-16777229
MAC	00:0c:29:02:1b:4e
Name	MAC: 00:0c:29:02:1b:4e (NFAEE-Lin)
StormWorks ID	13273
VLAN	
VNIC Key	
Association	Objects
Port	
Virtual Machine	NFAEE-Lin
Services	
Port Group	VM Network
Virtual NIC	Network adapter 1

Figure 4 Port Group Connections Advanced

# **Amazon Web Services**

#### Hypervisors and Zones

These are the common attributes with the existing Hypervisor type and the other existing Hypervisor attributes are not relevant.

Attributes	Description
Hypervisor Name	User-specified guest physical memory size.
Virtualization Platform Type	Virtualization platform type.

Table 25 Hypervisors and Zones Attributes

#### **Virtual Machine**

Existing attributes that are also relevant and populated when possible:

Attribute	Description
VMUUID	Universal Unique Identifier for the Virtual Machine. Keeping the same identifier when moving/copying a VM maintains its properties, e.g. keeps the same MAC address.
VMMemoryMB	User defined guest physical memory size.
VMName	Name of the Virtual Platform.
VMGuestOS	Operating system implemented on the VM.

Table 26 Virtual Machine Attributes

## Virtual Machine/Instance

Attribute	Description
AMI ID	AMI identifier.
Access KeyName	Used in authentication and authorization to identify who is making a call and whether to allow the requested access. In Amazon Web Services (AWS), these are typically the access key ID and the secret access key.
Architecture	Operating system architecture.
Availability Zone	Distinct location within a region that is insulated from failures in other Availability Zones. Provides inexpensive, low-latency network connectivity to other Availability Zones in the same region.
Device Name	Device name.
GuestOS	Operating system installed.
HypervisorType	Hypervisor type.
Image Id	Image ID, e.g. ami-04003319.
Instance Type	Defines the memory, CPU, storage capacity, and hourly cost for an instance. Some instance types are designed for standard applications, whereas others are designed for CPU-intensive, memory-intensive applications.
Kernel	CPU kernel.
Launch Time	Time and date of launch.

Table 27 Instance Attributes

Attribute	Description
Life Cycle	The lifecycle state of the instance contained in an AutoScalingGroup. Instances progress through several states over their lifespane.g. Pending, InService, Terminating and Terminated.
Memory (MB)	Memory size.
Name	Name of the instance.
Platform	Platform used to run the instance.
Private Address	Private IP address assigned to the instance at launch.
Private DNS	Private Domain Name System.
Public Address	Public IP address assigned to the instance at launch.
Public DNS	Public Domain Name System.
Ram Disk Id	RAM Disk identifier.
Reservation	A collection of instances started as part of the same launch request.
Virtualization Type	Guest VMs can run on one or more levels above the host hardware, depending on the type of virtualization, e.g. Paravirtual virtualization, Hardware Virtual Machine virtualization.

Table 27 Instance Attributes

#### Block Device Mapping

Mapping from volumes to device name such as /dev/xvda.

Attribute	Description
Attached Time	Time and date attached.
Block Device Name	Device name.
Delete on Termination	e.g. <i>yes</i> or <i>no</i> .
Volume Id	Volume identifier.

Table 28 Block Device Mapping Attributes

#### Volume

Storage area, either on instance or remote.

Attribute	Description
Create Time	Time and date created.
Size (GiB)	Size.
Snapshot	A user-initiated point backup of a instance, e.g. snap-98878e1d.
Volume Id	Volume identifier, e.g. vol-585c3441.

Table 29 Volume Attribute

## VNIC

An Elastic Network Interface that can be attached/detached and therefore moved between Instances in a VPC.

Attribute	Description
Description	Description of the VNIC, e.g. Primary network interface.
Elastic IP Address	A fixed (static) IP address allocated in Amazon EC2 or Amazon VPC and then attached to an instance. Elastic IP addresses are associated with an account, not a specific instance.
Key	Identifies an AWS account or user to AWS.
MAC	Message authentication code.
Ownerld	Owner ID.
Private DNS Name	Private Domain Name System.
Private IP Address	Private IP address assigned to the VNIC.
Requester	The person (or application) that sends a request to AWS to perform a specific action.
Subnet Id	Subnet identifier.
VPC Id	VPC identifier.
Zone	Zone name.

Table 30 VNIC Attributes

## **Security Group**

A named set of allowed inbound and outbound network connections created for a VPC and associated with an instance. Each security group consists of a list of protocols, ports, and IP address ranges. A security group can apply to multiple instances, and multiple groups can regulate a single instance.

Attribute	Description
Description	Consists of group name and time/date created, e.g. launch-wizard-3 created 2015-04- 08T11:55:34.613+01:00
GroupId	Group identifier.
Group Name	Group name, e.g. launch-wizard-3.
Group Owner	Group owner.

Table 31 Security Group Attributes

## **Virtual Private Cloud**

A VPN is an elastic network populated by infrastructure, platform, and application services that share common security and interconnection.

Attribute	Description
CIDR Block	IP address and its associated routing prefix, e.g.172.31.0.0/16.
Region	Identifies the named set of AWS resources in the same geographical area. A region comprises of at least two Availability Zones.
VPC Id	VPC identifier.
VPC Tenancy	Can be either dedicated or default.

Table 32 Virtual Private Cloud Attributes

## **Placement Group**

Logical grouping of instances for low latency 10Gbps high network throughput. Contained in a zone (hypervisor).

Attribute	Description
Placement Group Name	Placement group name.
InstanceID	Instance ID.

Table 33 Placement Group Attributes

## Region

A named set of AWS resources in the same geographical area. A region comprises of at least two Availability Zones.

Attribute	Description
Region Endpoint	URL that identifies a host and port as the entry point for a web service.
Region Name	Region name.

Table 34 Region Attributes

## Subnet

A subnet can be public or private. Public subnets will contain instances with public IP addresses/elastic IPs. Private subnets will have instances with only private IPs.

Attribute	Description
Address Count	Number of IP addresses contained in the subnet.
CIDR Block	IP address and its associated routing prefix, e.g.172.31.0.0/16.
Route Table Id	Route table identifier.
Subnet Id	Subnet identifier.
VPC Id	VPC identifier.

Table 35 Subnet Attributes

## VPNConnection

Specifically means the IPsec connection between a VPC and some other network, such as a corporate data center, home network, or co-location facility.

Attribute	Description
VPNConnection	VPNConnection.
Customer Gateway	Customer Gateway.
Virtual Private Gateway	Virtual Private Gateway.
Туре	VPN Connection type.
VPC	Virtual Private Cloud.

Table 36 VPNConnection Attributes

#### **Static Route**

Static routes are non-propogated routes, which are statically defined for VPNs.

Attribute	Description
CIDR	IP address and its associated routing prefix, e.g.172.31.0.0/16.
Source	Static route source.

 Table 37
 Static Route Attributes

## **Route Table**

Each subnet must be associated with a route table but not vice-versa. In the absence of an explicit route table, the subnet is associated with the Main route table (the Main route table can itself be explicitly defined). Route tables have route entries for the local subnet and any gateway (internet gateway or virtual private gateway and propagated VPN routes).

Attribute	Description
Route Table Id	Route table identifier, e.g. rtb-8ad921e3.
VPC Id	VPC identifier, e.g. vpc-090bf560.

 Table 38
 Route Table Attributes

## Route

A route is a CIDR block or IP Address and a Gateway (target). It can point to the publicly visible designated NAT instance.

Attribute	Description
Destination CIDR	The CIDR address block used for the destination match., e.g. 172.31.0.0/16.
Gateway	The ID of an Internet gateway or virtual private gateway attached to your VPC.
NAT VM	The ID of a NAT instance in your VPC.
NAT VM Owner	Name of the NAT VM owner.
NIC	ID of the NIC.
Originator	Originator of the route, e.g. CreateRouteTable.
Route Table Id	Route table identifier.
VPC Conn Id	VPC connection ID.

Table 39 Route Attributes

## **Customer Gateway**

A customer gateway is a physical device or software on the customer side of a VPN.

Attribute	Description
Customer Gateway	Customer gateway.
IP Address	IP address.
Туре	Gateway type.

Table 40 Customer Gateway Attributes

## **Elastic IP**

A fixed (static) IP address that you have allocated in Amazon EC2 or Amazon VPC and then attached to an instance. Elastic IP addresses are associated with your account, not a specific instance. They are elastic because you can easily allocate, attach, detach, and free them as your needs change. Elastic IP addresses allow an instance to be accessed from outside the VPC Subnet.

Attribute	Description
Instance Id	Instance identifier.
Network Interface Id	Network interface ID.
Owner	Owner of the elastic IP.
Private IP	Private IP address.
Public IP	Public IP address.

Table 41 Elastic IP Attributes

# 6 Applications and Application Servers

Availability Monitor identifies the true cause of unavailability whether at the network, device/server or application level.

# **Application Details**

From the device Applications page you can view:

- Attached Applications, applications running on attached servers/devices.
- Hosted Applications, applications running on the devices itself.

Users with administrator access rights can also configure which applications to monitor on a device.

Attribute	Description				
Icons	Link to other pages that display details on this device, e.g. Port Advanced Details page. (See <i>Navigate through Explorer</i> .)				
Port Name	Identifies the port, e.g. Port: [00028] Vlan1. The color of the icon indicates the port status:				
	red indicates the port is administratively up but operationally down				
	green indicates the port is administratively and operationally up				
	grey indicates the port is administratively and operationally down.				
View(Server)	Name of the Entuity view and server, e.g. All Objects (COMPRESSOR).				
Hosted Applications see which you can sort by c	ction, displays the defined Entuity application types on the device in a table licking on the column headings.				
Attached Applications s devices.	ection uses the same table type for showing applications on attached				
Туре	Identifies the application type and is also a hyperlink to the Application Summary page.				
TCP Port	Application port Entuity connects to when establishing the application's availability.				

Table 42 Application Summary Page

Attribute	Description
IP	IP address of the application device.
Latency Threshold	Availability Monitor measures Entuity server to application latency through Application Monitor, measuring time to TCP connect. When this value is above the set threshold Entuity raises an AvailMonitor High Latency Reaching Application.
Added	Date the application was defined in Entuity.
Last Status Change	Date and time Entuity reported a change in the availability status of the application.

 Table 42
 Application Summary Page

R	}e∩	tuity								User: adr Page Upd	min@entlonppvm01 lated: 16:30:05, GN	<mark>[Loqout]</mark> IT
Das	shboards	InSight Center	Explorer	Events	Maps Cha	arts Flows	Reports	Administration	Help			P
	Man All Obje	aged Ho	<b>ost: esp</b> 1001)	-serve	r							
ů	Summary	+₩ Flows	별 Ports	Resi	ources	Applications	Con	figuration 抗	Threshold ឮ	Advance	d	
	Name			Тур	e TCP Por	rt IP		Latency Thresho	ld Added		Last Status Chan	je
0	http			Host	ed 80	10.44.4.40		3000 ms	5 Nov 201	5, GMT	16:10:43, 5 Nov 20	15, GMT
0	mysql			Host	ed 3306	10.44.4.40		<u>3000 ms</u>	5 Nov 201	5, GMT	16:10:43, 5 Nov 20	15, GMT
											Add Re	move

#### Figure 5 Applications on a Device

You can display application details through the web UI, by highlighting a device in the Explorer tree and selecting the Application tab.

Attribute	Description
Filter	Entuity view and server machine.
Application	Application name and its server (device).
Poll Method	Connection type and port Entuity uses to connect to the application.

Table 43 Application Details

Attribute	Description
ApplicationType	Name of the monitored application type, e.g. pop3, http.
IP Address	Location of the application.
High Latency Threshold	Latency threshold level in seconds, above which Entuity raises a high latency event.
Name	Application name and server on which it is managed.
Date Added	Date and time the application was added to Entuity.

Table 43 Application Details

# **Application Server Details**

You can display application server details by highlighting an application server in the Tree pane and viewing its details in the Details pane, or by double clicking on the application server to open the application server object dialog.

Attribute	Description
Filter	Filter applied to the application.
Server	Server name.
Туре	Managed object type, i.e. Application Server.
IP Address	Server's IP address.
MAC Address	Server's MAC address.
Network Port	Address of the application port.
Applications	A table listing the applications on the server, specifically: Application is the application name.
	<ul> <li>First Discovered is the first date and time Entuity discovered the application.</li> <li>Last Discovered is the last date and time Entuity discovered the application. An application continues to exist on Entuity for fourteen days after it was last discovered.</li> </ul>

Table 44 Application Server Details

# 7 CUCMs

Entuity CUCM improves CUCM performance through management of both the application itself, the CUCM's managed host, and the network over which it is managing calls. For example, Entuity reports on switch failures, memory utilization, CPU utilization and power supply status, all of which could impact service delivery.

# **CUCM** as a Managed Host Application

Entuity considers CUCMs as applications of managed hosts. Information on these managed host devices can be viewed in Entuity. (For details see the *Entuity User and System Administrator Guide*.)

Entuity CUCM module allows Entuity to manage CUCM, particularly:

- Cisco Unified Communications Manager Groups
- Date/Time Groups
- Regions
- Device Pools
- Device Defaults
- Enterprise Parameters
- Call Admission Control
- Automated Alternate Routing
- Survivable Remote Site Telephony References.

## **CUCM** Details

Entuity CUCM details are displayed under Managed Hosts and Applications. Each CUCM managed by Entuity has an entry in the CUCM folder.

#### Entuity

# **CUCM General Attributes**

Attribute	Description
Host Device	Host Device
StormWorks ID	Internal identifier of the object.

Table 45 CUCM General Attributes

# **CUCM General Stream Attributes**

Stream Attribute	Description
Active Gateways	Number of active gateways.
Active Phones	Number of active phones.
Alarms Enabled	Alarms enabled.
ID	Installation ID.
Inactive Gateways	Number of inactive gateways.
Inactive Phones	Number of inactive phones.
Max Processes	Maximum number of running processes.
Phone Alarm Interval	Phone failure alarm interval.
Phone Status Alarm Interval	Phone status alarm interval.
Processes	Number of running processes.
Registered CTI	Number of registered CTI devices.
Registered Gateways	Number of registered gateways.
Registered Media	Number of registered media devices.
Registered Phones	Number of registered phones.
Registered VM	Number of registered voice mail devices.
Rejected CTI	Number of rejected CTI devices.
Rejected Gateways	Number of rejected gateways.

Table 46 CUCM General Stream Attributes

Stream Attribute	Description
Rejected Media	Number of rejected media devices.
Rejected Phones	Number of rejected phones.
Rejected VM	Number of rejected voice mail devices.
Restart Time	Time of last restart.
Sessions	Number of user sessions.
Total CPU%	Non-idle processor load (%).
Total Memory	Total system memory (KB).
Unregistered CTI	Number of unregistered CTI devices.
Unregistered Gateways	Number of unregistered gateways.
Unregistered Media	Number of unregistered media devices.
Unregistered Phones	Number of unregistered phones.
Unregistered VM	Number of unregistered voice mail devices.
Version	System version number.

Table 46 CUCM General Stream Attributes

#### **CUCM** Associations

Entuity groups CUCM components into easily managed units. Against these associations more information is held:

- CTI Device
- Device Pools
- Extensions
- Failed Phones
- Gatekeeper Devices
- Gateway Devices
- H.323 Devices
- Inter-Region Bandwidths
- Media Devices
- Phones
#### Entuity

Processes

- Voicemail Devices
- Remote CUCMs.

Entuity CUCM, by default, polls every fifteen minutes and retains data for twenty-eight days.

# **CUCM CTI Devices**

Computer Telephony Integration (CTI) allows leveraging of information systems while making, receiving and managing telephone calls. For example, CTI applications allow:

- retrieval of information from databases derived from caller ID,
- routing of calls to the appropriate customer service representative using information gained through an interactive voice response (IVR) system.

#### **CTI Device Attributes**

CTI Device tab displays details of the Computer Telephony Integration devices on the CUCM.

Attribute	Description
Application Name or Type	Name of the CTI application type, e.g. screen population.
Description	Description of the CTI device.
IP Address	IP address of the CTI device.
Index	CTI device identifier.
Name	CTI device name.
Туре	CTI control device type, i.e. CTI Port, CTI Route Point, Cisco IP Phones.

Table 47 CTI Device Attributes

#### CTI Device Stream Attributes

Stream Attributes	Description
Status	Device status, <b>unknown</b> , <b>registered</b> , <b>unregistered</b> and <b>rejected</b> . When the device registers with the local CUCM, status changes from <b>unknown</b> to <b>registered</b> .
Last Registered	Time the device last registered with the CUCM.
Change Cause	Reason for the change in device status: noError unknown noEntryInDatabase databaseConfigurationError deviceNameUnresolveable maxDevRegReached connectivityError initializationError deviceInitiatedReset callManagerReset
Last Update	Time the device status last changed.

Table 48 CTI Device Stream Attributes

### **CUCM Device Pools**

Cisco CUCM groups are associated to devices through device pools. Each device belongs to a device pool, and each device pool specifies the Cisco Unified Communications Manager group for all of its devices.

The Device Pools folder lists the device pools on the current CUCM. For each CUCM device pool there is a:

- General tab that outlines the pool's attributes, including associated CUCM Group and Region.
- Device tabs, one for each type of device, i.e. media devices, CTIs, gatekeepers, gateways, phones. These tabs detail all of the devices of that type within the pool. When a particular device type is not in a pool then its tab is not displayed.

#### **CUCM Groups**

A CUCM group comprises a prioritized list of up to three CUCMs. The first CUCM in the list serves as the primary CUCM for that group, and the other members of the group serve as secondary (backup) CUCM.

For most systems, you will assign a single CUCM to multiple groups to achieve better load distribution and redundancy.

### **Device Pool Attributes**

Attributes	Description
Group	Name of the CallManager group. A group comprises of three CUCMs, one the primary CUCM the others available as backup in case of CUCM failure. Groups and device pools are an important part of CUCMs redundancy capability.
Group Index	CUCM Group identifier.
Index	Device pool identifier.
Name	Name of the device pool.
Region	Name of the CUCM region. <i>Region</i> specifies the voice codecs used within and between regions, these are only required when using different types of voice codecs within the network.
Region Index	Region identifier.
TFTP	Identifies whether this is the default CUCM Trivial File Transfer Protocol (TFTP) server group ( <b>True</b> ) or not ( <b>False</b> ). The TFTP server enables the downloading of configuration files, device loads (operating code), and ring types.
TZ Hrs	Offset, in hours, of the group's time zone from GMT.
TZ Index	Time zone identifier.
TZ Mins	Offset in minutes of the group's time zone from GMT.
TZ Name	CUCM Date/Time Group associated to the device pool. The group sets the server date and time, usually synchronised to the local time zone.

Table 49 Device Pool Attributes

# **CUCM Phone Extension**

#### **Phone Extension Attributes**

Attribute	Description
Extension	Extension number.
Extension Index	Extension identifier.
IP Address	IP address of the extension.
Multilines	Number of multiline appearances for the extension.
Phone Index	Phone identifier.

Table 50 CUCM Phone Extension Attributes

### Phone Extension Stream Attributes

Stream Attribute	Description
Status	Device status, <b>unknown</b> , <b>registered</b> , <b>unregistered</b> and <b>rejected</b> . When the device registers with the local CUCM, status changes from <b>unknown</b> to <b>registered</b> .

Table 51 CUCM Phone Extension Stream Attributes

# **Failed Phone Attributes**

Attribute	Description
Cause	Reason for phone failure, e.g. device name unresolvable.
Index	Failed phone identifier.
IP Address	Last known IP address of the phone experiencing a communication failure. A value of all zeros indicates that the IP Address of a device is unavailable.
MAC Address	MAC address of the failed phone.
Name	Type of phone failure.

Table 52 CUCM Failed Faulty Phone Attributes

### -

Entuity

# **Gatekeeper Devices**

Gatekeeper devices provide address translation, admission control and zone management.

GateKeepers Advanced tab displays details of the gatekeepers that provide call admission control in a distributed system with a separate CUCM or CUCM cluster at each site.

#### **Gatekeeper Attributes**

Attribute	Description
Index	Gatekeeper identifier.
Name	Name of the gatekeeper device.
IP Address	Last known IP Address of the gatekeeper. A value of all zeros indicates that the IP Address is not available.
Description	Description of gatekeeper device, available when the gatekeeper is configured in the CCM.
Туре	Type of gatekeeper device, i.e. Unknown, Other, Terminal and Gateway.

Table 53 Gatekeeper Device Attributes

#### **Gatekeeper Stream Attributes**

Stream Attribute	Description
Status	Device status, <b>unknown</b> , <b>registered</b> , <b>unregistered</b> and <b>rejected</b> . When the device registers with the local CUCM, status changes from <b>unknown</b> to <b>registered</b> .

Table 54 CUCM Gatekeeper Stream Attributes

# **Gateway Devices**

CUCM communicate with non-IP telecommunications devices through a Cisco IP telephony gateway. Entuity CUCM monitors gateway devices, identifying their type and IP address, device pool and current status.

#### **Gateway General Attributes**

The gateway receives packetized voice transmissions from users and then routes them to others, using a carrier system interface and sending them over the public switched telephone network.

Attribute	Description
Description	Description of the gateway, e.g. its particular function.
IP Address	Last known IP Address of the gateway. A value of all zeros indicates that the IP Address is not available.
Index	Gateway identifier.
Name	Name of the gateway assigned through CUCM.
Product ID	Product identifier of the gateway device.
Туре	Type of gateway device, e.g. Standalone, ICS77XX, Cisco Catalyst 4000 and 6000 Voice Gateway modules.

Table 55 CUCM Gateways Attributes

#### **Gateway Stream Attributes**

Attribute	Description
Status	Device status, <b>unknown</b> , <b>registered</b> , <b>unregistered</b> and <b>rejected</b> . When the device registers with the local CUCM, status changes from <b>unknown</b> to <b>registered</b> .
Last Registered	Time the device last registered with the CUCM.
Change Cause	Reason for the change in device status: noError unknown noEntryInDatabase databaseConfigurationError deviceNameUnresolveable maxDevRegReached connectivityError initializationError deviceInitiatedReset callManagerReset
Last Update	Time the device status last changed.
D-Channel Status	Status of the D-channel, either Active or Inactive.
D-Channel Number	Channel on which the signalling data is passed to the CUCM.

Table 56 Gateways Stream Attributes

#### Entuity

# CUCM H.323 Devices

In large systems, more than one CUCM cluster may be required to handle the call processing load. Communication between the clusters is through intercluster trunks using H.323 protocol.

#### H.323 General Attributes

Attribute	Description
Name	Name assigned to the H.323 device when added to the CUCM.
Description	Description of the device.
IP Address	Last known IP Address of the H.323 device. A value of all zeros indicates that the IP Address is not available.
Index	H.323 identifier.
Product ID	Device product identifier.
Dev Cfg GK IP	Configured gatekeeper DNS name or IP address for the H.323 device. This is applicable only for H.323 devices with gatekeepers configured. When there is no gatekeeper configured, this will be NULL.
Act. GK IP	Active gatekeeper IP address.
Alt. 1.GK IP	First alternate gatekeeper DNS name or IP address for the H.323 device. This is applicable only for H.323 devices with gatekeepers configured. When there is no first alternate gatekeeper, this will be NULL.
Alt. 2.GK IP	Second alternate gatekeeper DNS name or IP address for the H.323 device. This is applicable only for H.323 devices with gatekeepers configured. When there is no first alternate gatekeeper, this will be NULL.
Alt. 3.GK IP	Third alternate gatekeeper DNS name or IP address for the H.323 device. This is applicable only for H.323 devices with gatekeepers configured. When there is no first alternate gatekeeper, this will be NULL.
Alt. 4.GK IP	Fourth alternate gatekeeper DNS name or IP address for the H.323 device. This is applicable only for H.323 devices with gatekeepers configured. When there is no first alternate gatekeeper, this will be NULL.
Alt. 5.GK IP	Fifth alternate gatekeeper DNS name or IP address for the H.323 device. This is applicable only for H.323 devices with gatekeepers configured. When there is no first alternate gatekeeper, this will be NULL.
CUCM 1 IP	First remote CUCM DNS name or IP address configured for the H.323 device. When a primary remote CUCM is not configured, a null value is returned.
CUCM 2 IP	Second remote CUCM DNS name or IP address configured for the H.323 device. When a secondary remote CUCM is not configured, a null value is returned.

Table 57 CUCM H.323 Devices Attributes

Attribute	Description
CUCM 3 IP	Third remote CUCM DNS name or IP address configured for the H.323 device. When a tertiary remote CUCM is not configured, a null value is returned.

Table 57 CUCM H.323 Devices Attributes

#### H.323 Stream Attributes

Attribute	Description
Status	Device status, <b>unknown</b> , <b>registered</b> , <b>unregistered</b> and <b>rejected</b> . When the device registers with the local CUCM, status changes from <b>unknown</b> to <b>registered</b> .
Last Registered	Time the device last registered with the CUCM.
Change Cause	Reason for the change in device status: noError unknown noEntryInDatabase databaseConfigurationError deviceNameUnresolveable maxDevRegReached connectivityError initializationError deviceInitiatedReset callManagerReset
Last Update	Time the device status last changed.

Table 58 CUCM H.323 Devices Stream Attributes

## **Inter-Region Bandwidths**

Regions should only be implemented when there is a requirement to set different bandwidth thresholds for different areas of the network. For example, for CUCM multisite deployments you may require a lower bandwidth limit for individual calls that are sent across a WAN link, than that set for internal calls.

The default voice codec for all calls through CUCM specifies G.711. When only the default codec is implemented, Regions are not necessary.

### **General Attributes**

Inter-Region Bandwidth lists the voice codecs used for calls both between and within CUCM regions.

Attributes	Description
Name	Inter-region name comprising of both regions,
Bandwidth	Identifies bandwidth through the implemented codec. The voice codec type specifies the technology that is used to compress and decompress voice signals. The choice of voice codec determines the compression type and amount of bandwidth that is used per call.
Dest Index	Destination index.
Index	Inter-region identifier, made up of the source and the destination index.
Src Index	Source index.

Table 59 CUCM Inter Region Bandwidths Attributes

## **Media Devices**

CUCM media devices allow deployment annunciator, media termination point, transcoding, conferencing and music on hold services. These resources are distributed throughout the cluster through device pools.

#### **General Attributes**

Attribute	Description
Name	Name assigned to the device, assigned when a new device of that type is added to the CUCM.
Description	Media device description derived from when the device is configured.
IP Address	Last known IP address of the media device. A value of all zeros indicates that the IP address is not available.
Index	Media device identifier.

Table 60 Media Devices Attributes

Attribute	Description
Туре	<ul> <li>Media device type: unknown Media Termination Points (MTPs), e.g. ciscoMediaTerminPointWSX6608, media termination point (media streaming application server) on a WS-X6608 Blade, ciscoSwMediaTerminationPoint, software media termination point Conference Bridges, e.g. ciscoConfBridgeWSX6608, audio conference bridge configured on a WS- X6608 Blade, ciscoSwConfBridge. Music On Hold (MOH) server, e.g. ciscoMusicOnHold. Annunciator (ANN), the annunciator device provides multiple one-way, RTP stream connections to devices, such as Cisco IP Phones and gateways.</li> </ul>

Table 60 Media Devices Attributes

### Media Device Stream Attributes

Attribute	Description
Status	Device status, <b>unknown</b> , <b>registered</b> , <b>unregistered</b> and <b>rejected</b> . When the device registers with the local CUCM, status changes from <b>unknown</b> to <b>registered</b> .
Last Registered	Time the device last registered with the CUCM.
Change Cause	Reason for the change in device status: noError unknown noEntryInDatabase databaseConfigurationError deviceNameUnresolveable maxDevRegReached connectivityError initializationError deviceInitiatedReset callManagerReset
Last Update	Time the device status last changed.

Table 61 Media Device Stream Attributes

# **Phones**

Entuity CUCM monitors IP phones, for example detailing phone type, IP address, extensions, device pools and phone status.

#### **General Attributes**

Attribute	Description
Description	Name of the device.
Emergency Location	Emergency, or 911, location.
Index	Phone identifier.
IP Address	Last known IP address of the phone.
Last User	Name of the user of the phone. When the phone is not in use, the name refers to the last known user of the phone.
MAC Address	Physical (MAC) address of the phone.
Name	Name of the phone.
Phone Load ID	Load ID of the phone.
Protocol	Phone's network terminal control protocol, e.g. SCCP, SIP.
Туре	Type of phone device. e.g. ciscoTeleCasterBid.

Table 62 Phones Attributes

### Phone Stream Attributes

Attribute	Description
Status	Device status, <b>unknown</b> , <b>registered</b> , <b>unregistered</b> and <b>rejected</b> . When the device registers with the local CUCM, status changes from <b>unknown</b> to <b>registered</b> .
Last Registered	Time the device last registered with the CUCM.

Table 63 Phones Stream Attributes

Attribute	Description
Change Cause	Reason for the change in device status: noError unknown noEntryInDatabase databaseConfigurationError deviceNameUnresolveable maxDevRegReached connectivityError initializationError deviceInitiatedReset callManagerReset
Last Update	Time the device status last changed.

Table 63 Phones Stream Attributes

### **Phone Extensions Attributes**

Attribute	Description
Extension	Extension number.
Extension Index	Extension identifier.
IP Address	IP address of the extension.
Multilines	Number of Multilines appearances for the extension.
Phone Index	Phone identifier.

Table 64 Phone Extensions Attributes

### **CUCM Processes**

Entuity CUCM monitors each process on the CUCM managed host, raising events when any process uses more resources than the set threshold. Also, as CUCM is an application on a managed host, Entuity has visibility into that device's resources and performance, for example monitoring device disk space, CPU utilization, memory utilization, fans and power supplies.

#### **Process General Attributes**

Processes General Information tab details the attributes of each process on the CUCM's managed host.

Attribute	Description
PID	Unique process identifier,
Name	Name of the process.

Table 65 CUCM Processes Attributes

#### **Process Stream Attributes**

For each process on the CUCM managed host Entuity monitors CPU and memory usage. Thresholds may be set against these metrics, which when crossed Entuity raises events. Entuity CUCM monitors both CUCM and non-CUCM processes, as it is possible that a problem with CUCM may be caused by another application on the managed host.

For troubleshooting this information can be tracked through the Attribute Grapher. For example, spikes in excess of 80 percent may indicate CUCM cannot manage more functions or is dropping calls. Entuity CUCM allows running of Flex Reports against these metrics, for example maximum and average statistics can provide valuable trending information.

Attribute	Description
CPU (%)	Process' usage of CPU as a percentage.
Memory	Process' usage of memory.

Table 66 CUCM Process Stream Attributes

# **Voicemail Devices**

Entuity CUCM identifies both the type of voicemail devices installed and their current status.

#### **Voicemail General Attributes**

Attribute	Description
Description	Description of voicemail device.

Table 67 CUCM Voicemail Attributes

Attribute	Description
Index	Voicemail identifier.
IP Address	IP address of phone.
Name	Name of voicemail device.
Product ID	Product identifier of voicemail.

Table 67 CUCM Voicemail Attributes

### **Voicemail Stream Attributes**

Attribute	Description
Status	Device status, <b>unknown</b> , <b>registered</b> , <b>unregistered</b> and <b>rejected</b> . When the device registers with the local CUCM, status changes from <b>unknown</b> to <b>registered</b> .
Last Registered	Time the device last registered with the CUCM.
Change Cause	Reason for the change in device status: noError unknown noEntryInDatabase databaseConfigurationError deviceNameUnresolveable maxDevRegReached connectivityError initializationError deviceInitiatedReset callManagerReset
Last Update	Time the device status last changed.

Table 68 CUCM Voicemail Stream Attributes

# **Remote CUCMs**

Entuity CUCM monitors remote CUCMs held in separate clusters by detailing the CUCM's IP address, status and cluster name.

### **Remote CUCM General Attributes**

Remote CUCMs tab details remote CUCMs connected to the local CUCM.

Attribute	Description
Cluster ID	Identifies a cluster to which the remote CUCM belongs.
Description	Remote CUCM description.
IP Address	IP address of the remote CUCM.
Index	Remote CUCM identifier.
Name	Name of the remote CUCM.
Status	Current status of the CUCM: <b>Up</b> , remote CUCM is running and able to communicate with the local CUCM. <b>Unknown</b> , current status of the CUCM is unknown <b>Down</b> , CUCM is down or is unable to communicate with the local CUCM.
Version	Version of the CUCM software.

Table 69 Remote CUCM Attributes

Entuity

# 8 Cisco Unified Computing System (UCS)

Cisco UCS is a data center server platform that unifies computing, networking, storage access, and virtualization resources into one system. Entuity management of UCS concentrates on the physical components underlying that system, e.g. chassis, servers, fabric interconnects, fabric extenders.



Figure 6 Entuity UCS Data Model Tree

Entuity

The Cisco UCS Manager is an application embedded on a Fabric Interconnect (switch). The UCS Manager places into one management domain all network objects connected to the fabric interconnects. Entuity manages UCS through the UCS Manager by polling the UCS MIBs.

The wealth of information available through the UCS MIBs makes it unfeasible to simply poll them. Instead through the Entuity discovery process Entuity builds its own object tree using each object's unique Distinguished Name. Entuity then polls the objects in that tree. Entuity provides a high level inventory and monitors UCS fault and states.

#### **Device Support**

Entuity manages the Cisco Unified Computing System (UCS) and:

- Supports UCS Manager 1.4 onwards running on the 6100/6200 series Fabric Interconnects.
- Supports UCS B-series and C-series.
- Discovers and monitors the entire UCS rack through one point of entry.
- Discovers chassis, fabric extenders, rack units, switches, service profiles.
- Allows drill-downs within components, for example from chassis you can drill down to its fan modules, blades, PSUs.

#### User Interface

Entuity represents UCS in a similar way to how it represents VM Platforms and the virtualization environment (although the network objects here are physical rather than virtual). There is a top level summary (UCS Manager) from which you can drill down to related objects and from each of these related objects you may also be able to further drill down. For example you can drill down from UCS Manager to Fan Modules to Fans.

2 entuitu					User: admin@entlonppvm	n01
	Mars Charts Flour	Denote Tech	A desirable states the se	11ala	Page Updated: 10:43:09,	, BST
nboards insight Center Explorer Events	s maps charts mows	Reports Tools	Administration	neip		
UCS Device: Cisco-UCS	5120					
ucs (ENTLONPPVM01)						
Summary + Flows E Ports	Resources III Application	Configuration	111 Thresh	old ភ្លំដ្រ Ac	lvanced	
vents						
O course () for the literate ) for the literate literate	h \					
Severe (view open incluencs, view Event his	(014)					
ev Metrics						
		/ >				
Average CPU% Average Memory%	Latency (ms) Avg SNI	IP Response (ms)				
	S					
709/ 679/		0.0				
/0% 0/%	0.9	0.9				
Average CPU Utilization%	Average Memory Used%	ICMP Later	ncy (ms)	Average	SNMP Response Time (ms)	
100%		40		10		
50% 50% 50%		20		5		
07:00 08:00 09:00 10:00	07:00 08:00 09:00 10:00	07:00 08:00	09:00 10:00	07:00	08:00 09:00 10:00	
orts	⊎©©©©©©©	00000000	000000	00000	®®®®®®®®®®®®®®®®®®®®®®®®®®®®®®®®®®®®®	00
rorts <b>2000000000000000000</b> towing al 52 ports chassis	₽@@@@ <b>@@@</b> @@	00000000	200000	00000	<b>₽</b> @@@@ <b>@@@</b> @@	00
orts	90000 <b>00000</b>	Model	)@@@@@@	0000	969999 <b>9</b> 9999	•
orts Owing all 52 pors Distinguished Name	90000 <b>0000</b>	Model N20-C6508	2000000	0000	90000 <b>0000</b> 0	
orts 00 00 00 00 00 00 00 00 00 00 00 00 00	<b>9000000000</b>	Model N20-C6508	200000	0000	90000 <b>0000</b>	
orts Owing all 52 ports hassis Distinguished Name Vs/chassis-1 witches	900000000	Model N20-C6508	200000	0000	D&&&&	•
orts Overs O	Node	Model N20-C6588		@@@@@	0000000000	
orts  Owing all S2 ports  bissinguished Name vsr/chasse-1  witches  bistinguished Name vsr/chasse-2  bistinguished Name vsr/chasse-	Model	Model N20-C6588	20000000	er of ports	90000 <b>000000</b>	
orts Overage All States Overage All All States Overage All All All All States Overage All All All All States Overage All All All All All All All All All Al	Model           Nuc-Ssillo           Nuc-Ssillo           Nuc-Ssillo	Model N20-C6508	2000 Numb	er of ports	DOUGO <b>OOO</b> O	
orts  Owing all 52 ports  hassis  Distinguished Name  stichassis:1  witches  Distinguished Name  stismtch-Aslat-1  solwatch-Aslat-2  solwa	Model           Model           Mi0-55100           Mi0-55100           Mi0-55000	100del 120-C558	20000000	er of ports	0000000000	
orts	Nodel           Ni0-55100           Ni0-55100           Ni0-55100           Ni0-55000           Ni0-55000	Podel 120-C6508	20 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	@@@@@(	0000000000	
	Model           Model           M0-55100           M0-65000           M0-55000           M0-55000           M0-55000	Model N20-65508	20000000000000000000000000000000000000	@@@@@(	0000000000	
orts  Owning all 52 ports  Distinguished Name	Hodel           N0-55100	Model N20-C6508	Numb           20           6           20           5	er of ports	DOUGU <b>???</b>	
	Hodel           NI0-55100           NI0-55100           NI0-55100           NI0-55100           NI0-5060           NI0-50060	Podel N20-C6598	20000000 20000000 20 5 20 5	er of ports	DOUGO <b>OOO</b>	
Ports	Model           Model           Nile-E0060           Nile-E0060           Nile-E0060           Nile-E0060	Model N20-C6508	Numb 2000000 20 6 20 6	er of ports	00000 <b>000000</b>	
Ports Provide Control	Model         Model           Model <td>Model N20-0558</td> <td>Number         20         0<!--</td--><td>er of ports</td><td>00000</td><td></td></td>	Model N20-0558	Number         20         0 </td <td>er of ports</td> <td>00000</td> <td></td>	er of ports	00000	
Ports	Model         Model           Model         Mi0-S5100           Mi0-E0060         Mi0-S500           Mi0-E0060         Mi0-S5100           Mi0-S5100         Mi0-S5100	Model N20-C5508	Numb           20         0 <td>er of ports</td> <td>0000000000</td> <td></td>	er of ports	0000000000	
Ports	Model         Model           Model         Mile-Solide           Mile-E0060         Mile-Solide           Mile-E0060         Mile-Solide           Mile-E0060         Mile-Solide           Mile-E0060         Mile-Solide	Manufacture ) Serial Number 1920 - Costas	Pomo (1997) Pomo	er of ports	00000 <b>000000</b>	

Figure 7 UCS Device Summary

It is the UCS Manager that is taken under Entuity management:

UCS Manager is managed through the Ethernet Switch device type although Entuity identifies it as a UCS Device.

- UCS Managers are available from the Explorer tree in the same way as other devices. All of the standard device level:
  - Metrics are available, for example CPU, memory, RTT dials + graphs), events count, port icons, general info (model, polled IP, version, reboot time).
  - Tabs are available, i.e. Summary, Flows, Ports, Resources, Applications, Configuration, Threshold and Advanced.

Entuity functionality available on ports polled using the UCS MIBs differs from that available on other ports, e.g. different port level traps may be available, flow support is unavailable.

- From the UCS Manager Summary tab are tables showing related network objects, for example:
  - Chassis
  - Fabric Extenders
  - Rack Units
  - Switches
  - Service Profiles.

If you drill down on one of these objects, there are three tabs available, Summary, Threshold and Advanced. When available Entuity displays tables for related objects on which you can further drill down, for example from Chassis you can drill down to its Fan Modules, Blades, PSUs.

#### **Cisco UCS Licensing**

In the device licensing model each chassis associated with a UCS Manager costs one license object, the UCS Manager is not charged. In the object licensing model each managed port costs one object license.

Component	Object Licensing	Device Licensing
Fabric Interconnect running UCS Manager	1 license credit for the device and 1 for each port (which includes both local and chassis ports).	1 license credit.
UCS Chassis	1 license credit for the device.	1 license credit.
UCS Switch Ports	0 cost (ports are already licensed through the UCS Manager).	0 cost.

Table 70 UCS Licensing

#### Entuity

### **Events and Incidents**

UCS Manager includes 8 UCS incidents and 40 UCS events. (See the Entuity Event Reference Manual.)

# **Compute Blade**

Attribute	Description
Assignment	e.g. sys/chassis-1/blade-1.
CPUs	
Cores	
Distinguished Name	Unique name identifying the blade and its location, e.g. sys/rack-unit-1/fan- module-1-1/fan-1.
Ethernet Host Interfaces	
Manufacturer	Manufacturer name.
Model	Device model.
Serial Number	Device serial number.
StormWorks ID	Internal identifier of the object.
StormWorks Type	StormWorks object type, ComputeBlade
UCS Blade Index	Unique identifier of the blade.

Table 71 Compute Blade Attributes

Association	Objects
Availability	sys/chassis-1/blade-1
Memory	Cisco-UCS6120
Operational	org-root/ls-ESXi-1/ether-FI-B-VMkernel

Table 72 Compute Blade Associations

Association	Objects
Power	
Presence	

Table 72 Compute Blade Associations

#### Association

Adaptor Units

Chassis

Device

Memory Arrays

Processors

Service Profiles

Storage Controllers

### Fans

Attribute	Description
Distinguished Name	Unique name identifying the fan and its location, e.g. sys/rack-unit-1/fan- module-1-1/fan-1.
Index	Unique identifier of the fan.
Manufacturer	Manufacturer name.
Model	Device model, e.g. FAN1_TACH1.
Name	Name of the fan, e.g. sys/rack-unit-1/fan-module-1-1/fan-1.
Serial Number	Device serial number.
StormWorks ID	Internal identifier of the object.

Table 73 Fans General Attributes

Attribute	Description
StormWorks Type	StormWorks object type, FanEx.
Tray	Identifies media tray.

Table 73 Fans General Attributes

Stream Attribute	Description
Fan Status	Status, e.g. Up.
Operational	Additional Status, e.g. operable
Performance	Additional Status, e.g. unknown
Power	Additional Status, e.g. unknown
Thermal	Additional Status, e.g. unknown
Voltage	Additional Status, e.g. unknown

Table 74 Fans Stream Attributes

# Local Disk

Attribute	Description
Block Size	
Configuration policy	
Distinguished Name	Unique name identifying the local disk and its location.
Manufacturer	Manufacturer name.
Model	Device model.
Number of Blocks	
Serial Number	Device serial number.
Size	Size of the local disk.
StormWorks ID	Entuity internal object identifier.

Table 75 Local Disk Attributes

Attribute	Description
StormWorks Type	StormWorks object type, ManagementInterface.
UCS Local Disk Index	Unique identifying number associated with the local disk, name of the local disk.

Table 75 Local Disk Attributes

Stream Attribute	Description
Presence	e.g. equipped.
Status	Management interface status, e.g. operable.

Table 76 Local Disk Stream Attributes

# Management Interface

Attribute	Description
Access	
Distinguished Name	Unique name identifying the blade and its location.
IP	IP address of this device.
Interface Type	Indicates the interface type.
MAC	MAC address of this device.
StormWorks ID	Entuity internal object identifier.
StormWorks Type	StormWorks object type, ManagementInterface.
Subject	
UCS Management Interface Index	Unique identifying number associated with the interface, name of the interface.

Table 77 Management Interface Attributes

Attribute	Description
Administrative Status	Current interface status as set by the system administrator.

Table 78 Management Interface Stream Attributes

# **Power Supplies**

Attribute	Description
Distinguished Name	Unique name identifying the power supply and its location, e.g. sys/ switch-A/psu-1.
Manufacturer	Manufacturer name.
Model	Device model.
Name	Name of the power supply, e.g. sys/switch-A/psu-1.
Revision	Power supply revision level.
Serial Number	Device serial number.
StormWorks ID	Internal identifier of the object.
StormWorks Type	StormWorks object type, PowerSupplyEx.
Туре	Power supply typw, e.g. Cisco Systems, Inc. N10-PAC1-550W (0).

Table 79 Power Supply Attributes

Stream Attribute	Description
Operational	Additional Status, e.g. operable
Performance	Additional Status, e.g. unknown
Power	Additional Status, e.g. on
Status	Power Supply Status, e.g. Ok
Thermal	Additional Status, e.g. ok

Table 80 Power Supply Stream Attributes

Stream Attribute	Description
Voltage	Additional Status, e.g. unknown

Table 80 Power Supply Stream Attributes

#### Association

Device

Switch Card

# **Rack Unit**

Attribute	Description
Total Memory	Total physical memory on the rack unit.
UCS Rack Unit Distinguished Name	Unique name identifying the UCS rack unit and its location.
UCS Rack Unit Instance	
StormWorks ID	Internal identifier of the object.
StormWorks Type	StormWorks object type, RackUnit.

Table 81 Rack Unit Attributes

Device

Power Supplies

Processors

Storage Controllers

# **Service Profiles**

Attribute	Description
Assignment	sys/chassis-1/blade-1
Distinguished Name	Unique name identifying the service profile and its location, e.g. sys/rack-unit- 1/fan-module-1-1/fan-1.
StormWorks ID	Internal identifier of the object.
StormWorks Type	StormWorks object type, ServiceProfile.
UCS Service Profile Index	UCS service profile identifier.

Table 82 Service Profiles Attributes

### Association

Device

**VNIC Ethernets** 

# Slot

Attribute	Description
Distinguished Name	Unique name identifying the slot and its location, e.g. sys/rack-unit-1/fan- module-1-1/fan-1.
StormWorks ID	Internal identifier of the object.
StormWorks Type	StormWorks object type, Slot.

Table 83 Slot Attributes

# Storage Controller

Attribute	Description
Device RAID Support	Indicates RAID support, e.g. yes or no.
Distinguished Name	Unique name identifying the storage controller and its location, e.g. sys/ chassis-1/blade-1/board/storage-SAS-1.
Manufacturer	Manufacturer name, LSI Logic Symbios Logic.
Model	Device model, e.g. SAS1064E PCI-Express Fusion-MPT SAS.
RAID Support	RAID support, e.g. RAID0, RAID1
Revision	Storage controller revision level.
StormWorks ID	Internal identifier of the object.
StormWorks Type	StormWorks object type, StorageController
Туре	Storage controller type, e.g. SAS.
UCS Storage Controller Index	Unique identifier for storage controller.

Table 84 Storage Controller Attributes

### Association

Device

Local Disks

# **Switch Card**

Attribute	Description
Description	Administrator-defined name of the switch card, e.g. 20x10GE/ Supervisor

Table 85 Switch Card Attributes

Attribute	Description
Distinguished Name	Unique name identifying the switch blade and its location, e.g. sys/switch-A/slot-1
Manufacturer	Manufacturer name, Cisco Systems, Inc.
Model	Device model.
Number Of Ports	Number of ports
Serial Number	Device serial number.
Slot	Slot identifier.
StormWorks ID	Internal identifier of the object.
Version	Device version number.

Table 85 Switch Card Attributes

Stream Attribute	Description
Card State	Status e.g. online.
Operational State	Status, e.g. operable.

Table 86 Switch Card Stream Attributes

#### Association

Device

Fan Modules

Management Interfaces

**Power Supplies** 

Slots

## **Temperature Sensor**

You can set high and low temperature thresholds for the selected object. These are associated with the Device Sensor Warning Value and Device Sensor Warning Value Cleared events and the Device Sensor Warning Value incident.

Attribute	Description
Data Scale	Units.
Data Type	Data type, e.g. Celsius
Index	Unique identifier.
Measured Entity	Name of devise measured.
Name	Name of the sensor, e.g. Module-1, Outlet-1
StormWorks ID	Internal identifier of the object.
StormWorks Type	StormWorks object type, TemperatureSensor

Table 87 Temperature Sensor Attributes

Stream Attribute	Description
Formatted Value	Sensor Value, e.g. 37.0 C
Status	Sensor Value, e.g.Ok
Temperature Value	Temperature Sensor Value, e.g.37°C
Value	Sensor Value, e.g. 37.0 C

Table 88 Temperature Sensor Stream Attributes

# **VNIC Ethernet**

Attribute	Description
Adaptor Profile	VMWare
Distinguished Name	Unique name identifying the VNIC ethernet and its location, e.g. org-root/ls- ESXi/ether-FI-B-VMkernel.
Ethernet Address	Ethernet address.
Identifier Pool	FI-B-C1

Table 89 VNIC Ethernet Attributes

Attribute	Description
MTU	Maximum Transmission Unit for the Ethernet interface.
Network Control Policy	CDP_ON
Network Template	FI-B-C1-VMkernel
StormWorks ID	Internal identifier.
StormWorks Type	StormWorks object type, VNICEthernet
UCS VNIC Ethernet Index	Unique VNIC identifier.

Table 89 VNIC Ethernet Attributes

# 9 Entuity Firewall

Entuity Firewall includes an extensive breakdown of the firewall inventory.

Entuity Firewall considers firewalls as devices, and as such they are placed as a subfolder of devices. Many of the firewall tabs are standard tabs applicable to other device types. This section outlines tabs of particular interest or specific to firewall management.

## **Firewall General Attributes**

Attributes	Description
Firewall SNMP Read-Only Community	Community string required for the checkpoint agent. It defaults to the same as used for firewall discovery, but it is an editable field.
Total Memory	Total memory on the firewall server.
Firewall SNMP UDP Port	Port used by the IPSO agent, by default port 161.
User Set Oper State	<ul> <li>Expected state of the module. By default, High Availability Module status monitoring in Entuity is unconfigured, but once configured Entuity polls the status every five minutes. When the state on the device does not match the expected state as set in Entuity, Entuity raises a Firewall High Avail User Set Oper State Non Compliant event. The High Availability status can be:</li> <li>Unconfigured, state internal to Entuity.</li> <li>Active, High Availability module is installed and active.</li> <li>Standby, High Availability module is ready to replace an active module.</li> <li>Active Attention, High Availability module is active even though all the members of the cluster have some problem. The gateway with the least problems, e.g. fewer failed critical processes, and the next highest priority level is active and working as a backup until the highest priority level gateway can be restored.</li> <li>Down, the module is down.</li> </ul>
	<ul> <li>Initializing, the module is initializing.</li> </ul>

Table 90 Firewall General Attributes

# **Representing Firewall Connectivity**

Firewalls are represented as devices in Entuity maps.





# Nokia/Checkpoint Firewall

Entuity Firewall includes an extensive breakdown of the firewall inventory. For those firewalls that support the managed hosts MIB, for example Nokia/Checkpoint firewall, Entuity Firewall collects performance and resource data.

#### **Firewall Packages**

Entuity Firewall details the packages installed to Nokia/Checkpoint firewalls, including version number details useful to maintaining the security of the network. The number of packages discovered is configurable through Threshold Settings. A limit is useful when a large number of packages are installed.

Attributes	Description
Name	Package name, including version number.
Installed	Date the package was installed to the firewall.
Туре	Type of package, e.g. Application, Operating System.

Table 91 Firewall Packages

### Firewall High Availability Stream Attributes

Stream Attribute	Description
Accepted Packet Rate	Rate of packets accepted per second.
Accepted Packet Rate Daily Mean	Rate of packets accepted per second, expressed as a mean average over the previous twenty-four hour day.
Accepted Packet Rate Hourly Mean	Rate of packets accepted per second expressed as a mean average over the previous hour.
Active Sessions	Number of active sessions.
Authenticated Response Time	
Connection Rate	
Connections Daily Mean	Mean average number of connections over the previous twenty-four hour day.
Connections Hourly Mean	Mean average number of connections over the previous hour.
Current Connections	Number of connections when polled.
Dropped Pkt Hourly Mean	Hourly mean of packets dropped.
Dropped Pkt Rate	Rate of packets dropped.
Dropped Pkt Rate Daily Mean	Daily mean of packets dropped.
External URL Response Time	

Table 92 Firewall High Availability Stream Attributes

Stream Attribute	Description
Last SNMP Restart Time	The last time the SNMP agent restarted. This also indicates when SNMP counters were reset, which is useful when identifying the reasons behind data spikes.
Maximum Connections	Maximum number of connections over a five minute period.
Maximum Number of Connections - Daily	Maximum number of connections over a five minute period, recorded over the previous twenty-four hour day.
Maximum Number of Connections - Hourly	Maximum number of connections over a five minute period, recorded over the previous hour.
Messages Received	Status messages received in the last five minutes.
New Connection Rate Daily Mean	Daily mean of new connection rate.
New Connection Rate Hourly Mean	Hourly mean of new connection rate.
Processes	Number of processes.
Rejected Packet Rate	
Rejected Packet Rate Daily Mean	
Rejected Packet Rate Hourly Mean	
TCP Connection Rate	The Transmission Control Protocol (TCP) Connection operation discovers the time it takes to connect to the target device.
TCP Connection Setup Rate Daily Mean	Daily mean of the device's TCP connection rate.
TCP Connection Setup Rate Hourly Mean	Hourly mean of the device's TCP connection rate.
UDP Connection Rate	User Datagram Protocol connection rate.
UDP Connection Setup Rate Daily Mean	Daily mean of the User Datagram Protocol connection setup rate.
UDP Connection Setup Rate Hourly Mean	Hourly mean of the User Datagram Protocol connection setup rate.

Table 92 Firewall High Availability Stream Attributes

Stream Attribute	Description
User	Number of users.

Table 92 Firewall High Availability Stream Attributes

#### High Availability Module Inventory

By default, polling of a High Availability module inventory data is unconfigured, but once *User Set Oper State* is changed from **unconfigured** Entuity Firewall polls for inventory data daily.

Attributes	Description
State	Operational state of the module. It is this setting that is polled every five minutes and compared with <i>User Set Oper State</i> , and where there are changes in compliance events are raised.
Product Name	Name of the module, i.e. High Availability.
Installed	1 indicates the product is installed.
Version	Version of the module.
Started?	Indicates whether the module has started, i.e. <b>Yes</b> , the module is active, <b>No</b> , the module is inactive.
Block State	Indicates whether the state is ok.
Work Mode	Synchronization method for changes in <i>State</i> across devices in the same cluster.

Table 93High Availability Inventory

# NetContinuum Firewall

Entuity Firewall includes an extensive breakdown of the firewall inventory accessible through Entuity and reports.

NetContinuum firewalls are grouped with other firewalls, placed within Entuity as a subfolder of devices. Many of the firewall tabs are standard tabs applicable to other device and firewall types. This section outlines tabs specific to NetContinuum firewall management.

### NetContinuum Monitored Server Attributes

Attributes	Description
NetContinuum Monitored Server	Name and path of the monitored web server.

Table 94 Monitored Server Attributes

#### NetContinuum Monitored Server Stream Attributes

Attributes	Description
IP Address,	IP address of the monitored web server.
Operational Status	Operational status of the web server, e.g. IN-SERVICE.

Table 95 Monitored Server Stream Attributes

#### **NetContinuum Application Status Attributes**

Attributes	Description
NetContinuum Application Description	Name and path of the monitored web application.

Table 96 Monitored Application Status Attributes

#### NetContinuum Application Status Stream Attributes

The Application Status Advanced tab provides a breakdown of access control activity for the web server application. These values are for the previous poll period, by default five minutes.

Stream Attributes	Description
Denied HTTP Requests,	Number of times during the last polling period NetContinuum denied HTTP requests for this application.
Blocked DAP,	Number of times during the last polling period NetContinuum used Dynamic Application Profiling (DAP) to block access to this application.

 Table 97
 NetContinuum Monitored Application Stream Attributes
Stream Attributes	Description
Blocked Entry Control	Number of times during the last polling period NetContinuum blocked entry control requests for this application.
Blacklisted	Number of times during the last polling period NetContinuum blacklisted users attempting to access this application.
Blocked Methods	Number of times during the last polling period NetContinuum blocked access to this application.
Robots Denied	Number of times during the last polling period NetContinuum denied robot access to this application.
Robots Allowed,	Number of times during the last polling period NetContinuum permitted robots to access this application.
URL Encoding Errors	URL Encoding Errors
Slash Dot URLs Blocked	Operational status of the web server, e.g. IN-SERVICE.
Tilder URLs Blocked	Blocking of access to URLs containing tildas (~).
Character Set Encoding Errors	Character Set Encoding Errors
Bad Certificates	Number of times bad security certificates were identified.
Meta Character Intrusions	Name and path of the monitored web server.
Keyword Intrusions	Keyword Intrusions
Query Length Intrusions	Query Length Intrusions
Cookie Overflow Intrusions	Cookie Overflow Intrusions
Header Count Intrusions	Header Count Intrusions
Header Overflow Intrusions	Header Overflow Intrusions
Content Overflow Intrusions	Content Overflow Intrusions
Parameter Length Overflows	Parameter Length Overflows
Empty Valued	Empty Valued

Table 97 NetContinuum Monitored Application Stream Attributes

# **10 Load Balancers**

Entuity Load Balancer includes an extensive breakdown of the load balancer inventory, accessible through web UI and reports.

Entuity Load Balancer considers load balancers as devices. From the web UI you can view data associated directly with the load balancer and data collected against its associated objects, for example virtual servers, virtual services.



Figure 9 Load Balancer Data Types and Associations

Entuity Load balancer polls every 5 minutes for data for which it retains a history, for example the current number of sessions. Entuity uses the standard data device model to manage different load balancer models, the extent of data collected against each attribute is dependent upon the MIB of each load balancer.

### Entuity

# Load Balancer Summary

The Summary tab is available for all devices. For load balancers Entuity generates a current sessions gauge.

	Center Explo								User: admin@cen	tury <u>(Logo</u>
ashboards InSight	Center Explo	en Europe							Page Updated: 11	: 19:50, BST
Load Ba		rer Events	Maps Charts	Flows Reports	Tools Ad	ministration I	Preferences	Help		P
My Network (cer	ancer De	evice: 10	.66.18.1							
🖞 Summary 🛛 📲	Flows 🛱 P	orts La Res	ources 🏨 Ap	plications	Configuration	111 Thresh	old <u>ૌ</u> ⊕ /	Advanced		
Events	nor (View Open	Incidents, View E	vent History)							
Key Metrics										
Average CPU%	Average Mer	nory% La	tency (ms)	Current Sessions						
78.7%	0%		1.4	Trapeze WAPs O	eneral Attribut	es				
Average CPU	Utilization%	Aver 100% 50% 0%	age Memory Used%		ICMP Latency (r	ns)	200M 100M 0	rrent Sessions	00 11:00	
Ports Ports Ports Showing all 36 ports General Info Management Leve Model: Polled IP Address:	E Full Big IP Optimus 10.66.18.1	Certified: Version: Last Reboot T	Certified 9.1.2, 69.0 F ime: May 15, 2013	Inal Fri Sep 8 09:58	N 14 PDT 2006 S ₩	SSS lanufacturer: erial Number: lanaged Since	F5 Labs Inc n/a s Apr 24, 201	, 3 1:50:50 PM		

Figure 10 Load Balancer Summary

The Current Sessions gauge indicates the current sessions on the load balancer at the time it was last polled. Entuity polls for current session data every five minutes. You can click on the gauge to run a graph.



Figure 11 Current Sessions Chart

## Load Balancer Resources

Load balancer Resources displays the performance of processors, memory and power supplies of the load balancer.

Firefox 🔻	- C - X-
€ entuity	User: admin@century [Logout] Page Updated: 11:44:00_BST
Dashboards InSight Center Explorer Events Maps Charts Flows Reports Tools Administration Preferences Help	20
Load Balancer Device: 10.66.18.1  My Network (century-enuity-local)	
ភ្នំ Summary 배 Flows 🛱 Ports 🗮 Resources 🏨 Applications 👖 Configuration 🏛 Threshold ភ្នំក្ Advanced	
Processors	
Description CPU Utilization (%)	
Processor 1 100	
Processor 2 Processor 2 (2) 100	
TMM Processor TMM Processor Utilization High	
0	
Memory	
Size Used Memory (bytes) Free Memory (bytes) Used Memory (%)	
Chassis Non-Volatile Memory 0 Chassis Volatile Memory 0	
System RAM 72000000403681105 5G 10G 10G	
0 J	
	1
Power Supplies	
Туре	
<u>Power Supply 101</u> F5 Power Supply     F5 Power Supply	
	8 10 204 0 0
century/webot/viewevents.doi:serventa=cbobses/~c4es-4552-65earoo44402410c5dt/lew=My Networkdtobjectid=10594&compiD=-214/48304	0.102241010

Figure 12 Load Balancer Resources

Entuity updates the state of the managed objects indicating where there are issues with the event diamond severity icon. You can click through to view more details.



Figure 13 Load Balancer Processor with High CPU Utilization

## Load Balancer Advanced

The Advanced page for load balancers includes details and links to further information on:

- Load balancer details including:
  - Session statistics with current sessions, total sessions, max sessions, total errors and total sessions rate. Through the context menu you can access charts, change history and export to CSV functionality.
  - Device type, name, model.

Firefox 🔻				
€ entuity		User: admin@century [Logout] Page Updated: 12:01:24, BST		
Dashboards InSight Center	Explorer Events Maps Charts Flows Reports Tools Administration Preferences I	Help P		
Browse Prop Box	Load Balancer Device: 10.66.18.1			
century.entuity.local	Applications     Applications	uration <u>iti</u> Threshold <u>i</u> t Advanced		
<ul> <li>➡ ♥ 10.44.12.13</li> <li>➡ ♥ 10.44.44.44</li> </ul>	Average CPU Utilization% Unified Device CPU Utilization 915- Average Memory Lised% Linified Device Memory 0%	40542%		
10.44.63.2	Chassis Description Chassis #2.5	SMP Tue Apr 25 15:38:38 PDT 2006		
+ 10.66.18.1	Chassis Fan Status Chassisman data Ok Chassis Model Number Chassis Big I	Ok Big IP Optimus		
+ 10.66.51.3	Chassis Serial Number Chassis n/a	n/a		
+ 😢 10.66.60.1	Chassis Status Chassisman data Unkr Chassis Temperature Chassisman data Ok	nown		
10.66.60.4	Connection Limited Exceeded Rate Connection Error Statistics 1.34	4k /s		
10.66.60.5	Current Sessions Session Statistics Show on chart	A-40230		
10.66.70.5	Analysis Add to current chart	•		
+ 10 200.5.1	Device Reachable Time Device Reachable Time with Change history Analysis Export to CSV			
10.200.5.6	Device Reachable Time Unknown Device Reachable Time without Root Cause 0 se Analysis	:cs		
HPCOL1	Device Status Device Status			
	Device SystinTime Counter Wrans Reboots 0			
century/webUI/objectDetails.d	prserver=cbub9e5/-c4e9-4352-89ea-0b444b241dc36kview=My Network&ld=958# 24.0	0 hrs		

Figure 14 Load Balancer Data

- Associated load balancer objects:
  - Local Pools
  - Real Servers
  - Virtual Services
  - Virtual Servers.

## Load Balancer Stream Attributes

Stream Attribute	Description
Chassis Fan Status	Chassis fan status.
Chassis Status	Chassis Status
Chassis Temperature	Chassis temperature status.
Current sessions	Current number of sessions or client side connections.

Table 98 Load Balancers Stream Attributes

Stream Attribute	Description
Connection Limited Exceeded Rate	
Dropped Pkt Rate	Rate of packets dropped.
Failed Connection Memory Err Rate	
In Err Rate	The inbound discard rate of packets with errors.
License Deny Dropped Pkt Rate	
Maximum Sessions	Maximum number of sessions or client side connections
No Handler Deny Pkt Rate	
No Syn Denied Pkt Rate	
Out Err Rate	The outbound discard rate of packets with errors.
Session Rate	Rate of sessions per second
Total Error Rate	Total discard rate of packets with errors, both inbound and outbound.
Local Pool Member Service Statistics	
Member Services Qty	Number of member services in the local pool.
Member Services Available Qty	Number of available member services in the local pool.
Member Services Unavailable Qty	Number of unavailable member services in the local pool.
Local Pool Member Statistics	
Member Servers Qty	Number of member servers in the local pool.
Member Services Available Qty	Number of available member services in the local pool.
Member Services Unavailable Qty	Number of unavailable member services in the local pool.

Table 98 Load Balancers Stream Attributes

Stream Attribute	Description
Member Servers Unknown Qty	Number of unknown member servers in the local pool.
Member Disabled Qty	Number of disabled member servers in the local pool.
Real Servers	
Sessions Rate	Rate of sessions per second.
State	The current state of the virtual server.
Current sessions	Current number of sessions or client side connections.
Virtual Services	
Sessions rate	Rate of sessions per second.
Failed Sessions Rate	Rate of failed sessions per second.
State	The current state of the virtual server.
Current sessions	Current number of sessions or client side connections.
Virtual Servers	
Sessions Rate	Rate of sessions per second.
Packets In Rate	Inbound packet rate.
Traffic Rate	Inbound traffic.
State	The current state of the virtual server.
Current sessions	Current number of sessions or client side connections.
Max sessions	Maximum number of sessions or client side connections.

Table 98 Load Balancers Stream Attributes

# **Local Pools**

A load balancing pool is a set of devices, servers, that are grouped together to receive and process network traffic. For each pool there is an algorithm which determines the applied load balancing method.

For each local pool, Entuity polls for the local pool *Pool Name* and *Algorithm*. Entuity also identifies members of the pool, the load balancer device, real servers, virtual servers and virtual services.

Firefox *														
£ entuity												User: admin@o Page Updated:	entury 11:57:47, I	[Loqout] BST
Dashboards InSight Center	Explor	er Events	Maps	Charts	Flows	Reports	Tools	Admini	stration	Preferences	Help			ρŢ
🕆 Browse 🗳 Drop Box	#		I Ser	ver P	ool	tcookr		(op. 10.6	c 10 1)					
Consolidate servers: off	<b>•</b>	My Netu	insk (centr	urv enhilti	(local)	cookp	0011	(011 10.0	0.10.1)					
entury.entuity.local	~	ny neur	ork (cerra	a y critary	nocary									
My Network		<u>្ប័</u> Summary	<u>10</u> 1	hreshold	Ĩ\$	Advanced								
10.44.12.13		Attribute							Value					
+ 🕢 10.44.44.44		Algorithm												
10.44.63.2		Pool Name							tcookpo	ol 1				
+ 10.66.18.1	E	StormWorks II	)						10414					
10.66.50.1														
10 66 51 3	•	Stream Attr	ibute			Stre	am				Value			
		Member Disabl	ed Qty			Local	Local Pool Member Statistics 0							
10.66.60.1		Member Serve	rs Availab	le Qty		Local	Pool Mem	per Stati	stics		0			
10.66.60.4		Member Serve	rs Unavai	able Qty		Local	Pool Mem	per Stati	SUCS		0			
10.66.60.5		Member Serve	rs Unknov	vn Qty		Local	Pool Mem	per Stati	sucs		0			
+ 🗸 10.66.70.5		Member Servic	es Avaliat	Je Qty Jahle Ohu		Local	Pool Mem	Jer Servi	ce Statist	JCS ice	0			
+ 10.200.5.1		Member Servic	es onava	lable Qty		LUCAI	POOL Mem	Jer Servi	CE STRUST	105	U			
10.200.5.4												Sho	w Empty As	ssociations
+ 🕢 10.200.5.6		Association							Object	s				
+		Load Balancer	Device						10.66.1	8.1				
⊕ Ssw1	-													

Figure 15 Pool Data

## **Real Servers**

For each real server Entuity polls for the *IP Address* and *Real Server Name*. Entuity also identifies the associated load balancer device, virtual services and assigned local pools.

For each real server Entuity collects for the sample period, and retains, data on:

Firefox 🔻											- • ×
€ er	ntuity									User: admin@cen Page Updated: 11	tury [Logout] :53:35, BST
Dashboards	InSight Center	Expl	orer Events	Maps Cha	ts Flows	Reports Tools	Admi	inistration F	Preferences Help		PŢ
Browse Consolidate ser	Drop Box     Drop Box	-	Load	Balanc	er Devi tuity.local)	ce: <b>10.66</b> .	18.1				
i Mv	Network		<u>n</u> Summary	+₩ Flows	這 Ports	Resources		Applications	Configuration	till Threshold	jீ⊕ Advanced
	10.44, 12.13 10.44, 14.44 10.44, 63.2 10.66, 18.1 10.66, 50.1 10.66, 51.3 10.66, 60.1 10.66, 60.1 10.66, 60.4 10.66, 60.5	m 🖌	Association Processors Real Servers					Objects Processor 1 Processor 2 TMM Process 10.160.80.1 10.160.80.1 10.166.80.0 10.168.100. 10.168.100	01 14 15 15 15 15 15 15 15 15 15 15 15 15 15		
	10.200.5.1	-						10.168.100. 10.168.102. 10.168.102.	59 10 11		-

Figure 16 Real Servers

# **Virtual Services**

For each virtual service Entuity polls for the *IP Address*, *Service Port* and *Virtual Service Name*. Entuity also identifies the associated load balancer device, real server and assigned local pool.

For each virtual service Entuity collects for the sample period, and retains, data on:

Firefox 💌													• <b>X</b>
8 er	ituity			Evalua	tion: 22	Days re	emaining					User: admin@crux Page Updated: 22: 17:4	[Logout] <del>1</del> 9, BST
Dashboards	InSight Center	Explorer Eve	ents	Maps	Chart	Flows	Reports	Tools	Administration	Preferences	Help		PŢ
Browse	🚔 Drop Box		-	$\mathbf{O}$	Virt	ual S	ervice	: mo	ni-ivazwe	b 10.20	0.24	101 8808 (m 10	1 66 33 15)
Consolidate ser	vers: off		- 🗳		My Neh	work (cru	x)						100100110
erux			~				~						
📄 💼 My	Network			<u> 1</u> Su	ummary	in	Threshold	j⊕ A	dvanced				
•	10.44.1.55		=	Attr	ibute					Value			
	10.66.13.22			IP A	ldress					10.200.24.10	1		
+0	10.66.13.25			Serv	ice Name					moni-jyqzweb	_10.200.2	24.101_8808	
	10.66, 13, 27			Serv	ice port					8808			
	10 66 33 2			Storr	nWorks I	D				10947			
	10.66.23.E		•	-									
	10.00.33.3			Stre	am Att	ribute		1	Stream		Va	alue	
<b>₩</b>	10.66.33.7			Curr	ent Sessi	ons		1	/irtual Service Stat	istics	16	6	
÷ 🗸	10.66.33.10			Sess	ions Rate			١	/irtual Service Stat	istics			
+	10.66.33.15			State	2			1	/irtual Service Stat	istics	up	p	
••	10.66.33.49											Show Empt	y Associations
•••	10.66.65.102			Ass	ociation					Objects			
•••	10.66.65.103			Load	Balancer	Device				10.66.33.15			
•••	10.66.65.108			Real	Server					10.200.24.10	1		
	10.66.65.110			Load	Balancer	Local Po	lool			moni-jygzweb			
	10 66 65 110		-										
•			•										

Figure 17 Virtual Services

# **Virtual Servers**

For each virtual server Entuity polls for the *IP Address* and *Virtual Server Name*. Entuity also identifies the associated load balancer device and assigned local pool.

For each virtual server Entuity collects for the sample period, and retains, data on:

F1 (												
Firefox *												
8 en	tuity										User: admin@cent Page Updated: 12:	ury [Logout] 01:24, BST
Dashboards	InSight Center	Explorer	Events	Maps C	harts Flows	Reports	Tools	Administrat	on Preferences	Help		<u>₽</u>
Browse	🖀 Drop Box	-	Load	Balan	cor Dovi	co: 10	66.1	8 1				
Consolidate ser	vers: off		Mulliotu	Dalan		ce. 10	.00.1	0.1				
entury.en	tuity.local		my neum	nk (century.	enuny.iocai)							
m My I	Network	<u>i</u>	Summary	+₩ Flow	s 🛱 Ports	Re:	sources	Applic	ations 🕌 Con	figuration	111 Threshold	ាំ្មា Advanced
	10.44.12.13	M	lemory					Chas	sis Non-Volatile Mem	ory		A
	10.44.44.44							Syste	m RAM			
	10 44 63 2							TMM	RAM			
	10.66.19.1	= Vi	irtual Servers					vs 10 vs 10	0 168 78 32 0 168 78 36			
	10.00.10.1							<u>vs 1</u>	168 86 51			
	10.66.50.1	•						<u>vs 1</u> vs 1	0 168 80 119 0 168 80 126			
± 🗸	10.66.51.3							<u>vs 2</u>	13 86 58 195			
<b>⊨</b> ⊗	10.66.60.1							vs 10	1.168.87.97 80			
<b>₽</b>	10.66.60.4							<u>vs 1</u>	168 66 68 80			
<b>⊞ 😣</b>	10.66.60.5							<u>vs 10</u>	168 66 91 80			
<b>H</b>	10.66.70.5							VS 10	168 66 92 80			
÷ 🔿	10.200.5.1							<u>vs 1</u>	168 76 24 80			
•	10.200.5.4							vs 10 vs 10	0 168 76 41 80 0 168 76 56 80			
+0	10.200.5.6							<u>vs 1</u>	168 76 71 80			
+0	HPCOL1							<u>vs 1</u> vs 1	) 168 76 77 80			
	bsw1							<u>vs 10</u>	168 76 77 96			
		Ŧ						<u>VS 1</u>	100 70 07 00			Ψ.

Figure 18 Virtual Servers

# 11 Multiprotocol Label Switching (MPLS)

Entuity MPLS functionality comprises of:

- Label Distribution Protocol (LDP)
- Label Switch Routers
- MPLS VPN.

## Label Distribution Protocol (LDP)

The Label Distribution Protocol (LDP) establishes MPLS LSPs using the existing IP routing network. Entuity provides a detailed inventory of LDP distribution within its managed network. You can view a series of tabs including a breakdown of LDP configuration and current performance:

- MPLS LDP Entity
- MPLS LDP Entity Status
- MPLS LDP Peers
- MPLS LDP Peer Status
- MPLS LDP Label Ranges
- MPLS LDP Label Range MPLS LDP Peers
- MPLS LDP Label Range Ports.

Entuity MPLS includes a set of events which monitor this polled data, providing clear insight into changes and possible problems with your LDP distribution. Events are raised against these measures, event thresholds are configurable:

- MPLS LDP Entity Errors
- MPLS LDP Entity Operational Status
- MPLS LDP Entity Rejected Sessions
- MPLS LDP Entity Shutdown Notifications Received
- MPLS LDP Entity Shutdown Notifications Sent
- MPLS LDP Peer Disappeared
- MPLS LDP Peer Newly Discovered

- MPLS LDP Peer Operational Status
- MPLS LDP Peer TLV Errors
- MPLS LDP Peer Unknown Message Types

Entuity MPLS includes a series of key reports:

- LDP Inventory Detail Report
- LDP Inventory Summary Report
- LDP Label Range Report
- LDP Peer Performance Report

You can also create new reports.

### **LDP Overview**

LDP is a set of procedures by which one LSR informs another of the meaning of labels used to forward traffic between and through them. It is through LDP that LSRs establish Label Switched Paths (LSPs). LSPs are also known as MPLS tunnels.

To maintain the Label Switched Router (LSR) database MPLS labels must be distributed.

LDP associates a Forwarding Equivalence Class (FEC) with each LSP it creates. The FEC associated with an LSP specifies which packets are handled by that LSP.

An LSP starts at the Label Edge Router (LER), which assigns the first label to the packet determined by the FEC. The LER then forwards the packet to the next router in the path, which swaps the packet's outer label for another label, and forwards it to the next router. The last router in the path removes the label from the packet and forwards the packet based on the header of its next layer, for example IPv4.

LDP Peers are two LSRs which use LDP to exchange label/FEC mapping information. This exchange takes place during an LDP session.

## MPLS LDP Entity General Attributes

Attribute	Description
Label Retention Mode	<ul> <li>When configured to</li> <li>Conservative, the advertised label mappings are retained only if they will be used to forward packets, i.e. if label came from a valid next hop.</li> <li>Liberal, then all advertised label mappings are retained whether they are from a valid next hop or not.</li> </ul>
Threshold for Session Initiation Attempts	<ul> <li>When set to:</li> <li>0 indicates that the threshold is infinity, and so effectively the SNMP notification is disabled.</li> <li>1 or greater, the LDP entity sends an mplsLdpFailedInitSessionThresholdExceeded when the number of session initialization messages sent exceeds this threshold.</li> </ul>
Label Distribution Method	<ul> <li>When the LSR is using:</li> <li>Downstream Unsolicited distribution it advertises FEC-label bindings to its peers when it is ready to forward packets in the FEC by means of MPLS.</li> <li>Downstream on Demand distribution provides FEC-label bindings to a peer in response to specific requests from the peer for a label for the FEC.</li> </ul>
LDP Protocol Version	Version number of the protocol. When set to 0, this indicates that the version of the protocol is unknown.
Hop Count Limit	Maximum allowable number of hops permitted, applicable when <i>Loop Detection Capability</i> must be set to either <b>Hop Count And Path Vector</b> or <b>Hop Count</b> .
LDP TCP Discovery Port	LDP TCP port 646 used for establishing transport connection.
PVL Mismatch Traps Enabled	The mplsLdpPathVectorLimitMismatch notification is generated when there is a mismatch in the Path Vector Limits between the Entity and Peer during session initialization. The session uses the value which is configured as the Entity's Path Vector Limit. However, a notification should be generated to indicate that a mismatch occurred.
Hello Hold Time	Value which is the proposed Hello hold time for this LDP Entity. A value of 0 means use the default, which is 15 seconds for Link Hellos and 45 seconds for Targeted Hellos. A value of 65535 means infinite.
Is Targeted Peer	When set to:         Image: true, the LDP entity uses targeted peers         Image: false the LDP entity does not uses targeted peers.
Targeted Peer Address	Address used for the Extended Discovery.

Table 99 MPLS LDP Entity Attributes

Attribute	Description
Maximum PDU Length	Maximum PDU Length that is sent in the Common Session Parameters of an Initialization Message. A value of 255 or less specifies the default maximum length of 4096 octets.
Keep Alive Hold Time	Value which is the proposed keep alive hold timer for this LDP Entity.
LDP UDP Discovery Port	UDP port, by default 646, used with the discovery message.
Path Vector Limit	When set to: <ul> <li>0, loop detection for path vectors is disabled.</li> </ul>
	<ul> <li>a value greater than zero, loop detection for path vectors is enabled, and the Path Vector Limit is this value.</li> <li>For the <i>Path Vector Limit</i> to have effect the device's <i>Loop Detection Capability</i> must be set to either Hop Count And Path Vector or Path Vector.</li> </ul>

Table 99 MPLS LDP Entity Attributes

## MPLS LDP Entity Stream Attributes

Attribute	Description
Admin Status	Administrative status of this LDP Entity. When set to:
	<b>Enable</b> , the entity can create new sessions with its peer.
	Disable, any existing peer connections are lost. When set to disable the administrator can amend entity values
Oper Status	Operational status of the LDP entity, which can be:
	<b>Unknown</b> , this should only be a transitional state.
	Enabled
	Disabled
Attempted Sessions	Total number of attempted sessions for this LDP Entity.
Rejects (No Hello)	Count of the Session Rejected/No Hello Error Notification Messages sent or received by the LDP entity.
Rejects (Bad Ad.)	A count of the Session Rejected/Parameters Advertisement Mode Error Notification Messages sent or received by this LDP Entity.
Rejects (PDU Length)	A count of the Session Rejected/Parameters Max Pdu Length Error Notification Messages sent or received by this LDP Entity.

Table 100 MPLS LDP Entity Status

Attribute	Description
Rejects (LR)	A count of the Session Rejected/Parameters Label Range Notification. Notification Messages sent or received by this LDP Entity.
Bad Identifier	Number of Bad LDP Identifier Fatal Errors detected by the session(s) (past and present) associated with this LDP Entity.
Bad PDU Length,	Number of Bad PDU Length Fatal Errors detected by the session(s) (past and present) associated with this LDP Entity.
Length Errors	Number of Bad Message Length Fatal Errors detected by the session(s) (past and present) associated with this LDP Entity.
TLV Length Errors	Number of Bad TLV Length Fatal Errors detected by the session(s) (past and present) associated with this LDP Entity.
Bad TLV Values	Number of Malformed TLV Value Fatal Errors detected by the session(s) (past and present) associated with this LDP Entity.
Keep Alive Timeouts	Number of Session Keep Alive Timer Expired Errors detected by the session(s) (past and present) associated with this LDP Entity.
Shutdowns Received	Number of Shutdown Notifications received related to session(s) (past and present) associated with this LDP Entity.
Shutdowns Sent	Number of Shutdown Notifications sent related to session(s) (past and present) associated with this LDP Entity.
Rejected Sessions Delta	Change in the number of rejected sessions between the two most recent pollings.
Error Delta	Change in the number of errors between the two most recent pollings.
Shutdowns Received Delta	Change in the number of shutdowns received between the two most recent pollings.
Shutdowns Sent Delta,	Change in the number of shutdowns sent between the two most recent pollings.

Table 100 MPLS LDP Entity Status

### **MPLS LDP Peers**

The connection from the local LDP entity to an LDP peer is through to the remote LDP entity. Details of the remote peered LDP are as viewed from the local entity.

Attribute	Description
General	Discovery details, for example advertised IP address
MPLD LDP Label Ranges	Supported label ranges
MPLS LDP Entity	Details of the remote entity
Peer Status	Key status metrics.

Table 101 Remote Peer Attributes

## MPLS LDP Peers General Attributes

Attribute	Description
Path Vector Loop Detection	Indicates whether loop detection based on path vectors is disabled or enabled for this LDP peer.
Advertised IP	IP address advertised to its LDP peers.
Path Vector Hop Limit	<ul> <li>When set to:</li> <li>0, loop detection for path vectors is disabled.</li> <li>a value greater than zero, loop detection for path vectors is enabled, and the Path Vector Limit is this value.</li> </ul>
	For the <i>Path Vector Hop Limit</i> to have effect the device's <i>Loop Detection Capability</i> must be set to either <b>Hop Count And Path Vector</b> or <b>Path Vector</b> .
Label Distribution Method	<ul> <li>When the LSR is using:</li> <li>Downstream Unsolicited distribution it advertises FEC-label bindings to its peers when it is ready to forward packets in the FEC by means of MPLS.</li> </ul>
	<b>Downstream on Demand</b> distribution provides FEC-label bindings to a peer in response to specific requests from the peer for a label for the FEC.

Table 102 MPLS LDP Peers General Attributes

## MPLS LDP Label Ranges

Attribute	Description
Name	Name of the label range.
IF Index	Interface index of the outgoing label of this LSP.
Maximum Label	Upper boundary of the label range.
Minimum Label	Lower boundary of the label range.

Table 103 MPLS LDP Label Ranges

### **MPLS LDP Peer Status**

### An LDP peer is a remote LDP entity.

Attribute	Description
Status	Polled state of the session, i.e. Non existent, Initialized, Open receive, Open sent and Operational.
LDP Version	Version number of the protocol. When set to 0, this indicates that the version of the protocol is unknown.
Peer Max PDU Length	Maximum PDU Length that is sent in the Common Session Parameters of an Initialization Message. A value of 255 or less specifies the default maximum length of 4096 octets.
Unknown Message Type Errors	Number of Unknown Message Type Errors detected during this session. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of mplsLdpSeeionDiscontinuityTime.
Unknown TLV Errors	Number of Unknown TLV Errors detected during this session. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of mplsLdpSeeionDiscontinuityTime.
Unknown Message Type Error Delta	Difference in the number of Unknown Message Type Errors detected between the last two pollings.
Unknown TLV Error Delta	Difference in the number of Unknown TLV Errors detected between the last two pollings.

Table 104 MPLS LDP Peer Status

### MPLS LDP Label Ranges

### MPLS LDP Label Range MPLS LDP Peers

Attribute	Description
Name	Name of the MPLS LDP peer.
Path Vector Loop Detection	Indicates whether loop detection based on path vectors is disabled or enabled for this LDP peer.
Advertised IP	IP address advertised to its LDP peers.
Path Vector Hop Limit	<ul> <li>When set to:</li> <li>0 - loop detection for path vectors is disabled.</li> <li>a value greater than zero - loop detection for path vectors is enabled, and the Path Vector Limit is this value.</li> <li>For the Path Vector Hop Limit to have effect the device's Loop Detection Capability must be set to either Hop Count And Path Vector or Path Vector.</li> </ul>
Label Distribution Method	<ul> <li>When the LSR is using:</li> <li>Downstream Unsolicited distribution it advertises FEC-label bindings to its peers when it is ready to forward packets in the FEC by means of MPLS.</li> <li>Downstream on Demand distribution provides FEC-label bindings to a peer in response to specific requests from the peer for a label for the FEC.</li> </ul>

Figure 19 MPLS LDP Label Range MPLS LDP Peers

## **Label Switch Routers**

Label Switch Routers (LSRs) support MPLS. LSRs originate the Label Switch Path (LSP). The ingress LSR computes the path for a given LSP. The egress router is the point of output from the LSR.

### **MPLS LSR**

The label space can be set at the platform or interface space. You can also view the LSR configuration at both the device and interface level.

Attribute	Description
Min label (RX)	Minimum value of an MPLS label that this LSR is willing to receive on this interface.
Max label (RX)	Maximum value of an MPLS label that this LSR is willing to receive on this interface.
Min label (TX)	Minimum value of an MPLS label that this LSR is willing to send on this interface.
Max label (TX)	Maximum value of an MPLS label that this LSR is willing to send on this interface.
Usable Bandwidth	Total amount of usable bandwidth on this interface and is specified in kilobits per second (Kbps). This variable is not applicable when applied to the interface with index 0.
Available Bandwidth	Total amount of available bandwidth available on this interface - specified in kilobits per second (Kbps). This value is calculated as the difference between the amount of bandwidth currently in use and that specified in mplsInterfaceTotalBandwidth. This variable is not applicable when applied to the interface with index 0.
Allocated Space	Total amount of buffer space allocated for this interface. This variable is not applicable when applied to the interface with index 0.
Available Space	Total amount of buffer space available for this interface. This variable is not applicable when applied to the interface with index 0.
Label Space	<ul> <li>Either set to per Platform(0) or per Interface(1). When the value is:</li> <li>perInterface(1) bit is set then the value of <i>Min label (RX), Max label (RX), Min label (TX),</i> and <i>Max label (TX)</i> for this entry reflect the label ranges for this interface.</li> <li>perPlatform(0) bit is set, then the value of value of <i>Min label (RX), Max label (RX), Min label (TX),</i> and <i>Max label (TX)</i> for this entry must be identical to the instance of these objects with index 0.</li> </ul>
Labels In Use (RX)	Number of inbound labels used.
Packets (RX)	Number of labeled packets that have been received on this interface.
Error Free Discards (e.g. insufficient buffer)	Number of outbound labeled packets, which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a labeled packet could be to free up buffer space.
Lookup Failure Discards	Number of labeled packets that have been received on this interface and were discarded because there were no matching entries found for them in mplsInSegmentTable.
Labels In Use (Tx)	Number of top-most labels in the outgoing label stacks that were in use on this interface.
Packets (TX)	Number of labeled packets that have been transmitted on this interface.

Table 105 MPLS LSR

Attribute	Description
Error Free Discards (Tx)	Number of outbound labeled packets, which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a labeled packet could be to free up buffer space.
Packets Fragmented	Number of outgoing MPLS packets that required fragmentation before transmission on this interface.
Rx Discard No Error Pkt Rate	Difference between two contiguous inbound <i>Error Free Discards</i> sampled values, as a per second average.
Tx Discard No Error Pkt Rate	Difference between two contiguous outbound <i>Error Free Discards</i> sampled values, as a per second average.
Rx Discard Lookup Failure Pkt Rate	Difference between two contiguous inbound <i>Packets (Rx)</i> sampled values, as a per second average.
TX Pkt Fragmentation Rate	Difference between two contiguous outbound <i>Packets Fragmented</i> sampled values, as a per second average.

Table 105 MPLS LSR

## **MPLS VPN**

A network with an MPLS backbone provides the flexibility to deliver high value VPN services. The Provider Edge (PE) router provides a different, private view of the network to each VPN. This allows for different customers to use the same network resources, using different addressing to gain secure, customer specific routing. This separation is realized through separate VRF instances on a PE behaving as separate router emulations.

These Virtual Routing and Forwarding Tables (VRF) are dedicated routing tables for Layer 3 VPNs containing IP prefixes. Entuity can monitor the performance of VRF instances through monitoring the success or failure of its route target distribution.



Figure 20 A Simple MPLS VPN Configuration

### MPLS VRF General

Entuity gathers MPLS configuration data from every MPLS enabled port.

Attribute	Description
VRF Name	VRF name.
VRF Description	Description of the VRF, for example its purpose.
VRF High-Water Route Threshold	Denotes high-level water marker for the number of routes which this VRF may hold.
VRF Mid-Water Route Threshold	Denotes mid-level water marker for the number of routes which this VRF may hold.
VRF Route Distinguisher	Route Distinguisher that makes the VRF unique, distinguishing between overlapping addresses in the VRF.
VRF Maximum Routes	Maximum number of routes on the VRF. It must be less than or equal to the maximum possible number of routes unless it is set to 0.

Table 106 MPLS VRF General

### **MPLS Route Targets**

Route targets are used as targets for routing updates. The VRF RTs tab shows all of the routing targets associated with all instances of the VRF.

Attribute	Description
Name	Name of the route target distribution policy.
Route Target	Route target identifier.
Description	Description of the route target
Туре	Import/export distribution policy for the route target, i.e. <b>import, export</b> and <b>import and export</b> . The configuration of the VPN topology is determined through the <i>Type</i> setting of VRFs.

Table 107 MPLS Route Targets

### **MPLS VRFs Status**

The VRFs Status tab shows the status of the VRF and a summary of key statistics for the VRF instances.

Attribute	Description
Oper status	Operational status of the VRF. When it is set to:
	<b>Up</b> , one or more interfaces associated with the VRF is up
	<b>Down</b> , the are no interfaces associated with the VRF, or all of the interfaces associated to the VRF are down.
Active Interface	Number of interfaces associated with the VRF that are up.
Associated Interface	Number of interfaces associated with the VRF, including both active and inactive interfaces.
Routes Added	Number of routes added over the lifetime of the VRF.
Routes Deleted	Number of routes deleted over the lifetime of the VRF.
Routes	Number of routes currently used by this VRF.
Illegal labels	Number of illegal label violations on the interface. These may indicate MPLS misconfiguration or an attempt to breach network security.
Illegal labels Threshold	Illegal label violation threshold.
Illegal label Violation Rate	Number of illegal label violations per second.

Table 108 MPLS VRFs Status

## MPLS Interface VRF Instances General

With MPLS you configure virtual routers, and within them divide a physical interface into multiple logical interfaces. For each logical interface you can assign a different VRF which can be for a different customer with a distinct FEC. You can configure routing send traffic to the appropriate virtual interface.

Attribute	Description
Name	Identifies the VRF and its interface.
MPLS VRF Interface	VRF interface.
VRF Name	VRF name.
Classification	The VPN classification which denotes the context of the link, e.g. carrier-of-carrier's, enterprise, inter- provider.
Edge Type	Either the provider edge (PE) or customer edge (CE) router.
RDP	VRF Interface Route Distribution Protocol across the PE-CE link, which can be: dummy none BGP OSPF RIP ISIS other

Table 109 MPLS Interface VRF Instances

### MPLS Interface VRF BGP Neighbors

This tab details the BGP neighbors of the VRF instance on the interface.

Attribute	Description
Name	Resolved name, or IP address of the device.
Role	Role played by this EBGP neighbor with respect to this VRF, e.g. CE.

Table 110 MPLS Interface VRF BGP Neighbors

Attribute	Description
Address	IP address of the EBGP neighbor.

Table 110 MPLS Interface VRF BGP Neighbors

### VRF on an Interface Instance

This tab details the MPLS VRF associated with the virtual interface.

Attribute	Description
Name	VRF name.
VRF Description	Description of this VRF, e.g its purpose.
VRF High-Water Routes Threshold	High-level water marker for the number of routes which this VRF may hold.
VRF Mid-Water Routes Threshold	Mid-level water marker for the number of routes which this VRF may hold.
VRF Route Distinguisher	Route distinguisher for this VRF.
VRF Maximum Routes	Maximum number of routes, summed across all VRFs, which the device allows. When set to 0, this indicates that the device is unable to determine the absolute maximum, and you could potentially set a configured maximum greater than that allowed by the device.
VRF Name	Name of the VRF.

Table 111 VRF on an Interface Instance

# **12 Power over Ethernet**

Entuity Power over Ethernet (PoE) supports PoE Midspan Injectors.

## **PoE Midspan Injectors**

Entuity PoE allows the management of Microsemi PoE midspan injector devices, with SNMP polling of port configuration and power supply status.

### **Overview of Microsemi PoE Midspan Injectors**

Microsemi (formerly PowerDsine) manufacture a range of Power over Ethernet (PoE) midspan injector devices with various port densities. These devices allow power to be injected into Ethernet circuits close to the end-device that actually consumes the power.

Each unit has a network connection that is used to communicate with the SNMP agent and webserver. The power is injected via separate ports that are not instrumented for traffic monitoring.

The use of these midspan power injectors avoids the need for installing PoE hardware modules into the access layer Ethernet switches.

### **Entuity PoE Implementation**

Midspan injector devices are IP addressable and have an SNMP agent that allows management access. Entuity discovers and adds PoE midspan injectors to its database in a similar manner to that used for routers and Ethernet switches. PoE midspan injector devices are automatically classified as midspan injector devices and placed into their own Devices folder.

Entuity PoE monitors the status of the power supply and the individual port configuration, status and power drain through the injector devices.

Each device includes an in-built webserver, which allows browser access to status and configuration settings. Entuity PoE includes a user action for the context launching of a web browser.



Unlike modular Ethernet switches Entuity PoE assumes that each PoE midspan injector device is implemented as a single module.

### Entuity

### **Entuity PoE Injector Devices**

Entuity PoE considers midspan injectors as devices, and as such they are placed within a subfolder of devices. Many of the midspan injector attributes are standard attributes applicable to other device types, e.g. Ports, Chassis Data and KPI tabs. This section outlines attributes of particular interest or specific to PoE management:

### **PoE Injector Attributes**

Attribute	Description
Manufacturer	Manufacturer name and is derived by matching the manufacturer number against the first 2500 Private Enterprise Codes compiled by the Internet Assigned Numbers Authority (http://www.iana.org/assignments/ enterprise-numbers). Where the manufacturer code is not matched then the first part of the device name is taken, usually this is the manufacturer's name. This would be Microsemi or, as it was formerly called, PowerDsine.
Model	Device model.
Version	Device version number.
Serial Number	Device serial number.
Polled IP Address	IP address Entuity uses to poll the device.
Location	Device location.
System Object Identifier	Value of the system object identifier MIB variable for the device.
System Description	Manufacturer's device description which may include the application and boot version identifiers.
Power Budget	Percentage of maximum available power when operating from a UPS.
Maximum Power	Maximum power available to the device, measured in watts.
System Capabilities	Traffic management capabilities of the device. It is not applicable to this device type.
Nominal Power	Theoretical level of power available to the device, measured in watts.
Poll Status	Indicates whether the device is currently available to poll.

Table 112 Entuity PoE Attributes

### **PoE Injector Stream Attributes**

PoE midspan injectors supply power to network devices through their injector ports. You can monitor power supply at both the injector device and injector port level. Entuity PoE can detail PoE injector device power configuration.

Attribute	Description
Operational Status	Operational status of the device, i.e. <b>On</b> , <b>Off</b> .
Total Power Supplied	Sum of all power supplied to the device's ports.
Voltage	Mains power supply received by the PoE midspan injector.

Table 113 PoE Injector Stream Attributes

## **PoE Injector Port Attributes**

PoE injector ports inject power into the end device and so are not instrumented for traffic monitoring.

Attribute	Description
Name	Port name.
Maximum Power	Maximum power the port can handle, measured in watts.
Device Classification	Power class of the powered device (PD).
Power Priority	Priority of the port used to decide which ports continue to supply full power to their end device when power to the midspan injector is insufficient to meet all requirements. Three states are available <b>Critical</b> , <b>High</b> and <b>Low</b> (default).
Port Description	Description which can be used to identify the end device, or its purpose, that this port is supplying with power.

Table 114 PoE Injector Port Attributes

### **PoE Injector Port Stream Attributes**

PoE injector ports inject power into the end device and so are not instrumented for traffic monitoring. Entuity PoE can detail the status of their power delivery, updating these values using a one hour polling cycle. This information is available for graphing through the Attribute Grapher, for reporting on through Flex Reports.

Attribute	Description
Power Supplied	'Power the port is currently delivering, measured in watts.
Administrative Status	Port can be administratively <b>Enabled</b> or <b>Disabled</b> .

Table 115 PoE Injector Port Stream Attributes

Attribute	Description
Detection Status	Status of the port power detection, i.e. <b>Disabled</b> , <b>Searching</b> , <b>Delivering Power</b> , <b>Fault</b> , <b>Test</b> , <b>Other Fault</b> , <b>Unknown</b> .

Table 115 PoE Injector Port Stream Attributes

# **13 Entuity QoS**

## **QoS Overview**

Entuity® QoS module supports Cisco® QoS Modular CLI (QMC). It provides support for discovery of QMC configuration and its performance at a port level from policy maps through class map definitions down to individual traffic matching rules. This information is appropriate for effective QoS management including typical rate limiting configuration, traffic profiling, traffic shaping and cascading diffServ.

QoS comprises of four components:

- Traffic identification, enabled through match statements (access-lists).
- Class maps, collections of access-lists.
- Policy maps, collections of paired class-maps and action.
- Service policy, application of policy maps to interfaces. One policy map for the ingress and egress of each interface.

### **Collecting QoS Data**

All data is gathered from Cisco-Class-Based-QOS-MIB. Entuity QoS presents a highly granular view of QoS objects, including detailed performance statistics. SNMPv1 and v2c support (64 bit support in v1 via. split 32bit counters).

 $\odot$ 

Entuity advise using named access lists, both as best practice and as Entuity QoS does not present the lowest level match statements.

### Simple QoS Example

This QoS example identifies three types of traffic through match statements - telnet, SNMP and ICMP. These named access lists are placed in class maps, in this simple example one access list to each class map. These class maps are built into the traffic profile policy map. This policy map can then be applied to the ethernet interface.

```
!match traffic flows
access-list TELNET permit tcp any eq telnet any
```

#### Entuity

```
access-list SNMP permit udp any any eq snmp
access-list ICMP permit icmp any any
!Use access-lists to build class maps
class-map match-all icmp-only
match access-group ICMP
class-map match-all snmp-only
match access-group SNMP
class-map match-all telnet-only
match access-group TELNET
```

```
!use class maps to build policy map
policy-map traffic-profile
  class telnet-only
  class snmp-only
  class icmp-only
```

```
!apply policy map to interface
interface Ethernet0/0
ip address 192.168.3.34 255.255.255.0
service-policy input traffic-profile
```

## Traffic Identification through Access Groups

Through access lists devices can classify packets by physical port, source or destination IP address, application port, IP Protocol type, MAC address and so on. Entuity displays access lists:

- ordering them in the same sequence as they are configured, and therefore the same order as they are applied.
- pre- and post- policy traffic performance statistics.



Entuity QoS identifies access lists through their access groups, so it is important these groups are given meaningful, descriptive names.

## **Access Group General Details**

Entuity displays access groups through their association to class maps. These attributes are associated with the defined access group.

Attribute	Description
Name	Name of the access group.
Information	Description of the access group.

Table 116 Access Group General Details

### **Access Group Status**

These attributes detail the pre-policy performance of the interface.

Attribute	Description
Pre Policy Packets	Number of packets that match the access list handled by the device before applying the traffic policy.
Pre Policy Bytes	Number of bytes that match the access list handled by the device before applying the traffic policy.
Pre Policy Bit Rate	Bit rate managed by the router before applying the traffic policy.

Table 117 Access Group Status

# Traffic Management through Class Maps

Classification and admission control are always performed at the network edge, ensuring traffic conforms to the internal network policy. Packets can be marked with special flags (colors), which are used inside the network for QoS management. For each class, Entuity displays traffic management configuration and pre- and post-policy performance statistics.

### **Class Map General Details**

Attribute	Description
Name	Name of the class map.
Description	Short description of the class map, e.g. related to the type of traffic it manages.
Information	Information on the class map, e.g. the type of match evaluation statement employed.

Table 118 Class Map General Details

### Access Groups associated with Class Maps

A class map may have one or more associated access groups.

### **Class Map Status**

These attributes identify the current performance of the class map.

Attribute	Description
Pre Policy Packets	Number of packets to be handled that match the class, before the policy is applied.
Pre Policy Bytes	Number of bytes to be handled that match the class, before the policy is applied.
Pre Policy Bit Rate	Bit rate of the class, before the policy is applied.
Post Policy Bytes	Number of packets handled that match the applied class.
Post Policy Bit Rate	Bit rate of the class after the policy is applied
Dropped Packets	Class's number of dropped packets.
Dropped Bytes	Class's number of dropped bytes.
Packets Dropped (No Bursts)	Class's number of packets dropped
Drop Bit Rate	Per class drop bit rate.

Table 119 Class Map Status

#### Entuity

# **Policy Maps**

Policy maps are applied to the interface as service policies. Each interface has a maximum of two service policies, one for inbound traffic, one for outbound. Entuity details the classes associated with the policy map.

### Policy Map General Details

Attribute	Description
Name	Name of the policy map.
Direction	Direction of the traffic to which the policy is applied, i.e. inbound or outbound.

Table 120 Policy Map General Details

### **Classes associated with Policy Maps**

A policy map may have one or more associated classes. This attribute identifies the class associated with the policy map:

Attribute	Description
Name	Name of the class map.

Table 121 Classes associated with Policy Maps

# **QoS Traffic Policing**

Traffic policing allows you to control the maximum rate of traffic sent or received on an interface, and to partition a network into multiple priority levels or classes of service (CoS).

Using Entuity's Business Views you can monitor the traffic policing configuration on interfaces at the edge of your network. Typically, conforming traffic is transmitted and traffic that exceeds is sent with a decreased priority or dropped.

Through Entuity providing detailed QoS configuration information and extensive statistics on port performance, you can amend the configuration to meet changing network requirements.
## **Traffic Policing General Details**

Attribute	Description
Exceed Set Value	IP precedence value the router sets packets to that exceed the conform threshold but are within the exceed parameters.
Conform Set Value	Sets the IP precedence for conforming packets.
Violate Action	Action taken when traffic exceeds the conform and exceed token buckets.
Violate Set Value	IP precedence value the router sets packets to that violate the exceed threshold. 0 is the default value.
Burst Size	Amount of traffic, in bytes, in excess of the committed policing rate that is permitted by the policing configuration.
Extended Burst Size	Must be a value greater than the normal burst value. Setting the extended burst value equal to the normal burst value excludes the extended burst capability. When extended burst is configured, the flow is allowed to borrow the needed tokens to allow the packet to be sent. This capability exists so as to avoid tail-drop behavior, and, instead, engage behavior like that of Random Early Detection (RED).
Conform Action	Action the router performs on packets that conform to the policy, e.g. using <i>Conform Set Value</i> to set packet IP precedence.
Exceed Action	Action the router performs on packets that exceed, but do not violate the traffic policy, e.g. using <i>Exceed</i> Set Value to set packet IP precedence.
Rate	Committed policing rate. This is the sustained rate permitted by the policing configuration. All traffic below the rate is considered in profile.

Table 122 Traffic Policing General Details

## **Traffic Policer Status**

These attributes detail the policer performance.

Attribute	Description
Conform Bit Rate	Bit rate of traffic handled as conforming to the policy.
Conform Bytes	Number of bytes handled as conforming to the policy.
Conform Packets	Number of packets handled as conforming to the policy.

Table 123 Traffic Policer Status

Attribute	Description
Exceed Bit Rate	Bit rate of traffic handled as exceeding, but not violating, the policy.
Exceed Bytes	Number of bytes handled as exceeding, but not violating, the policy.
Exceed Packets	Number of packets handled as exceeding, but not violating, the policy.
Violated Bit Rate	Bit rate of traffic handled as violating the policy.
Violated Bytes	Number of bytes handled as violating the policy.
Violated Packets	Number of packets handled as violating the policy.

Table 123 Traffic Policer Status

## Managing Congestion through Queues

Queue management is an important congestion tool, for example for avoiding tail drops, where the possibility exists of high priority packets being dropped because they cannot be added to the router's queue and therefore identified. Queues are associated with classes, one queue per class. A low priority class can be assigned smaller queue depth, high priority classes greater resources reducing the probability of losing high priority packets.

Entuity details both queue configuration and current performance, for example current queue depth and number of discarded packets. You can check queues associated with high priority classes are assigned greater resources, reducing the probability of losing high priority packets, than those associated with lower priority classes.

Attribute	Description
Bandwidth	Amount of bandwidth assigned to the traffic class. In the case of a bandwidth policy, this value represents a minimum bandwidth guarantee for the traffic class. In the case of a priority policy, this value represents the maximum rate at which priority service is guaranteed.
Queuing Units	Unit of measurement used for Bandwidth.
Queue Limit Units	Unit of measurement used for Priority Burst Size.
Individual Queue Size	Number of packets in the queue.

#### **Queue General Details**

Table 124 Queue General Details

Attribute	Description
Aggregate Queue Size	Maximum number of packets that can be held in all the individual queues associated with this class before packets are dropped.
Aggregate Queue Limit	Maximum allowed queue size for all of the individual queues associated with this class. When the queue size exceeds this value, the packets are dropped.
Dynamic Queue Number	Number of dynamic queues supported when flow-based fair-queue is enabled.
Flow Enabled	When set to:
	<b>false</b> , flow-based fair-queue is not enabled for the class,
	<b>true</b> , flow-based fair-queue is enabled for the class.
Priority Enabled	Signifies whether low latency queuing (LLQ) is enabled for this class, by default it is disabled. Precedence 5 is used for the most critical or highest priority traffic, such as interactive audio and video.
Priority Burst Size	Permitted maximum single burst size for priority queue, only used when Priority Enabled is true.

Table 124 Queue General Details

#### **Queue Status**

These attributes detail the queuing action related statistical information status.

Attribute	Description
Current Depth	Current depth of the class queue.
Discard Bytes	Number of bytes dropped by the class when traffic exceeds Max Queue Depth.
Discard Packets	Number of packets dropped by the router when traffic exceeds Max Queue Depth.
Max Queue Depth	Maximum depth of the class queue after which packets will be dropped.

Table 125 Queue Status

# **Congestion Avoidance**

Congestion avoidance can be achieved through packet dropping. Cisco IOS QoS allows Class-Based Weighted Fair Queuing Configuration (CBWFQ) with Weighted Random Early Detection (WRED). Entuity allows you to appropriately modify congestion management through displaying class configuration and its performance. For example:

whether explicit congestion notification is enabled for the class, precedence thresholds for the service profiles

erformance statistics such as number of transmitted packets, tail dropped packets, random packets.

## Random Early Detection General Details

These attributes identify the congestion management configuration.

Attribute	Description
Discard Exponential Weight	Weight factor used in Weighted Random Early Detection (WRED) calculations. The decay factor is equal to raising 2 to the power of N, where N could be up to 16. The smaller the number, the faster it decays.
Mean Queue Size	Average queue size is based on the previous average and the current size of the queue. The formula is: average = (old_average * (1-2 -n)) + (current_queue_size * 2 -n) where n is <i>Discard Exponential Weight</i> .
DSCP Precedence	Indicator of which random early detection mechanism is used: 1, IP Precedence 2, DSCP 3, Discard Class 4, layer 2 cost of service 5, ATM CLP.
ECN Enabled	<ul> <li>Indicates whether explicit congestion notification is enabled for the class:</li> <li>1, enabled</li> <li>2, disabled.</li> </ul>
Precedence n Min Threshold	Minimum size of the queue threshold for the <i>n</i> service profile (packets with a specific IP precedence), when it exceeds <i>Mean Queue Size</i> the router starts dropping packets, according to WRED specified in <i>DSCP Precedence.</i>
Precedence n Max Threshold	Maximum size of the queue threshold for the <i>n</i> service profile (packets with a specific IP precedence), when it exceeds <i>Mean Queue Size</i> the router starts dropping packets, according to WRED specified in <i>DSCP Precedence.</i>
Precedence n Drop Probability	Fraction of packets dropped when the average queue size is at the maximum threshold for the <i>n</i> service profile. When <i>Mean Queue Size</i> is greater than <i>Precedence n Max Threshold</i> all packets are dropped.

Table 126 Random Early Detection General Details

## Random Early Detection Status

These attributes identify the congestion management status.

Attribute	Description
ECN Marked Bytes	Count of Explicit Congestion Notification (ECN) marked bytes when the number of packets in the associated queue was greater than the minimum threshold and less than the maximum threshold.
ECN Marked Packets	Count of packets ECN marked when the number of packets in the associated queue was greater than the minimum threshold and less than the maximum threshold.
Transmitted Packets	Number of transmitted bytes.
Mean Queue Size	Average queue size computed and used by the WRED algorithm
Units	Mean queue size units.
Transmitted Bytes	The 64 bits count of octets transmitted
Random Dropped Bytes	Count of bytes dropped when the number of packets in the associated queue was greater than the minimum threshold and less than the maximum threshold.
Random Dropped Packets	Count of packets dropped when the number of packets in the associated queue was greater than the minimum threshold and less than the maximum threshold.
Tail Dropped Packets	Number of packets dropped when the number of packets in the associated queue was greater than the maximum threshold, using the tail drop congestion method (the default method when WRED is not implemented).
Tail Dropped Bytes	Number of bytes dropped when the number of packets in the associated queue was greater than the maximum threshold, using the tail drop congestion method (the default method when WRED is not implemented).

Table 127 Random Early Detection Status

# **QoS Packet Marking**

Packet marking allows you to partition your network into multiple priority levels or classes of service (CoS). QoS Packet Marking can be implemented through:

- Marking packets by setting the IP precedence bits or the IP differentiated services code point (DSCP) in the Type of Service (ToS) byte.
- Associate a QoS group value with a packet.

Entuity

After setting the IP precedence bits or the IP DSCP, packets are classified by their IP precedence bit or IP DSCP value. These classifications are then used to apply user-defined differentiated QoS services to the packet.

Associating a packet with a QoS group allows users to associate a group ID with a packet. The group ID can be used to classify packets into QoS groups based on prefix, autonomous system, and community string.

A user can assign up to eight IP precedence values, 64 IP DSCP markings, and 100 QoS groups.

Entuity QoS identifies the packet marking method applied on the parent class map and displays its configuration details.

### **Set General Details**

Set tab displays the set values of the packet marking feature applied on the parent class map.

Attribute	Description
Discard Class Value	The match criteria chosen using the Select Discard Class Allows you to use specified discard class values in a class map to match packets. This feature is used to set the match criteria for examining discard classes marked on the packet. Up to eight discard class values can be matched in one match statement. For example, match discard class 0 1 2 3 4 5 6 7 returns matches for discard class variables 0, 1, 2, 3, 4, 5, 6, and 7. Only one of the discard class values must be a successful match criterion, not all of the specified discard class values. The discard class value is used as a matching criterion only. The value has no mathematical significance. For instance, the discard class value 2 is not greater than 1. The value simply indicates that a packet marked with the discard class of 2 should be treated differently than a packet marked with a discard class value of 1.
QoS Group Value	An identifier that can be used to classify packets based on prefix, autonomous system, or community string. This QoS group marking can only be used to classify traffic within a router, and cannot be used to mark packets leaving the router. A user can set up to 100 different QoS group markings, from 0 to 99.

Table 128 Set General Details

Attribute	Description
Feature	Bit-wise representation of a packet marking feature, identifying which appropriate fields are marked for applicable packets, syntax bits represent: <ul> <li>0, IP DSCP</li> </ul>
	1, IP Precedence
	2, QoS Group
	3, Frame Relay DE
	4, ATM CLP
	5, Layer 2 Cost of Service
	6, MPLS Experimental
	7, Discard Class.
DSCP Value	Measure of the Quality of Service (QoS) level of the packet (within a class, value from 0 to 63). The policing function determines if the traffic level is within the specified profile (contract), and allows either dropping out-of-profile traffic or marking it down to a different Differential Services Code Point (DSCP) value to enforce a contracted service level. DSCP is a measure of the Quality of Service (QoS) level of the packet. Along with DSCP, IP precedence and Class of Service (CoS) are also used to convey the QoS level of the packet. By default DSCP is set to 0.
MPLS Experimental Value	Value of the Multiprotocol Label Switching (MPLS) experimental field used as a match criterion against which packets are checked to determine if they belong to the class. It may be set instead of overwriting <i>IP Precedence Value</i> .
L2 CoS Value	Associating a packet with a local CoS value allows users to associate a Layer 2 CoS value with a packet. The value can then be used to classify packets based on user-defined requirements. Layer 2 to Layer 3 mapping can also be configured by matching on the CoS value, because switches already have the capability to match and set CoS values. If a packet that needs to be marked to differentiate user-defined QoS services is leaving a router and entering a switch, the router should set the CoS value of the packet, because the switch can process the Layer 2 CoS header marking. A user can set up to 8 different CoS markings, from 0 to 7.

Table 128 Set General Details

Attribute	Description
IP Precedence Value	Allows you to specify the class of service of a packet using the three precedence bits in the ToS field of the IP version 4 (IPv4) header. The bits provide a priority of 0-7, although 6 and 7 are reserved. Other features configured throughout the network can then use these bits to determine how to treat the packet in regard to the type of service to grant it. For example, although IP Precedence is not a queuing method, other queuing methods such as WFQ can use the IP Precedence setting of the packet to prioritize traffic.

Table 128 Set General Details

## **QoS Traffic Shaping**

Traffic shaping attempts to control the volume of traffic sent into a network and the rate at which the traffic is sent. Therefore, traffic shaping is implemented at the network edges, and may involve separating traffic into traffic flows and individually shaping each of these flows, smoothing the peaks and troughs of data transmission.

Entuity QoS can show the separated traffic flows and the individual shaping of each, indicating where the current configuration can be improved to better manage the current traffic.

#### **Traffic Shaping General Details**

Traffic Shaping tab displays the set values of the packet marking feature applied on the parent class map.

Attribute	Description
Limit Type	Indicates if traffic-shaping is limiting traffic based on peak rate or average rate.
Burst Size	Specifies in bits (or bytes) per burst how much traffic can be sent within a given unit of time to not create scheduling concerns. (For a shaper, such as GTS, it specifies bits per burst; for a policer, such as CAR, it specifies bytes per burst.). Also called the Committed Burst (Bc) size.
Rate	Also called the committed information rate (CIR), it specifies how much data can be sent or forwarded per unit time on average.

Table 129 Traffic Shaping General Details

Attribute	Description
Extended Burst Size	Corresponds to the number of non-committed bits, those outside the CIR, that are accepted by the device but marked as discard eligible (DE). When <i>Extended Burst Size</i> is set to:
	0, the interface sends no more than the burst size every interval, achieving an average rate no higher than the mean rate.
	greater than 0, the interface can send as many bits in a burst as the sum of <i>Burst Size</i> plus <i>Extended Burst Size</i> , if in a previous time period the maximum amount was not sent.
Adaptive Rate	Current bit rate to which traffic is shaped when backward explicit congestion notifications (BECNs) are received on the interface.
Adaptive Enabled	Enables traffic shaping for outbound traffic on the interface.

Table 129 Traffic Shaping General Details

#### **Traffic Shaping Status**

Traffic Shaping Status tab displays the current performance of the traffic shaping scheme.

Attribute	Description
Delayed Bytes	Number of bytes delayed to avoid traffic congestion, but eventually transmitted.
Delayed Packets	Number of packets delayed to avoid traffic congestion, but eventually transmitted.
Dropped Bytes	Number of bytes dropped to conform to the traffic shaping scheme.
Dropped Packets	Number of packets dropped to conform to the traffic shaping scheme.
Active	Indicates whether the traffic shaping scheme is active (true) or inactive (false).
Queue Size	Current queue size.

Table 130 Traffic Shaping Status

# **14 Routing Protocols**

These protocols are included with the Routing Protocols module:

- BGP Routing Protocol
- EIGRP Routing Protocol
- OSPF Routing Protocol
- IS-IS Routing Protocol.

## **BGP Routing Protocol**

The Border Gateway Protocol (BGP) is the core protocol of the internet. BGP maintains a table of IP networks or 'prefixes' which designate network reachability among autonomous systems (AS). It is the purpose of BGP to pass information between AS.

To achieve scalability, BGP uses many route parameters, called attributes, to define routing policies and maintain a stable routing environment. BGP neighbors exchange full routing information when the TCP connection between neighbors is first established.

When changes to the routing table are detected, the BGP routers send to their neighbors only those routes that have changed. BGP routers do not send periodic routing updates, and BGP routing updates advertise only the optimal path to a destination network.

BGP peering details can be viewed against devices that support BGP. In Entuity you can follow BGP peering by viewing the local device, opening its BGP peers, and track the associations within the network.

#### **Device Advanced Info**

Routing Protocols Extension adds additional attributes to the device Advanced tab.

Attribute	Description
BGP Local AS	Local AS of the device.

Table 131 Device BGP General Attributes

Attribute	Description
BGP Identifier	Each router running BGP must have a BGP identifier. This identifier is included in the BGP identifier field of open messages, which are sent between two BGP peers when establishing a BGP session.

Table 131 Device BGP General Attributes

#### **BGP Device Attributes**

Attribute	Description
Local IP Address	Local IP address of the device.
Remote AS	Describes routing domain; e.g. each building may have its own number.
Peer Type	When set to:
	<ul> <li>Internal, peering is between routers in the same AS.</li> </ul>

Table 132 BGP Device Attributes

#### **BGP Peer Stream Attributes**

Entuity polls for router BGP state information every five minutes, and uses these values for event generation.

Attribute	Description
BGP Peer State	When set to:
	Established, allows passing of information.
	Idle, Connect, Active, Open Sent and Open Confirm the peer is not established.
BGP Admin Status	Administrator set value when set to:
	Start should be operating,
	Stop should be down.
Established Transitions	Number of changes in peer status during the polling period. A high value may indicate flapping and require
Count	further investigation.
Established Time	Only transitions into and out of the Established state cause this timer to be reset.

Table 133 BGP Peer Stream Attributes

#### Entuity

# **EIGRP Routing Protocol**

Enhanced Interior Gateway Routing Protocol (EIGRP) is a Cisco proprietary routing protocol. EIGRP is an advanced distance-vector routing protocol, with optimizations to minimize both the routing instability incurred after topology changes, as well as the use of bandwidth and processing power in the router.

#### **EIGRP Peer Attributes**

Attribute	Description
Local IP Address	Local IP address of the device.
Remote IP Address	Source IP address used by the peer to establish EIGRP adjacency with this router.

Table 134 EIGRP General Attributes

#### **EIGRP Local Interface**

Attribute	Description
Name	Interface identification.
Device Name	IP address or resolved device name.
Type (IANA)	Device type.

Table 135 EIGRP Local Interface

#### **EIGRP Peer Stream Attributes**

Entuity polls for router EIGRP state information every five minutes, and uses these values for event generation.

Attribute	Description
EIGRP Peer State	<ul> <li>When set to:</li> <li>Established, allows passing of information.</li> <li>Stale, the device is up but the EIGRP peer is no longer reported to exist.</li> </ul>

Table 136 EIGRP Peer Stream Attributes

Attribute	Description
Established Time	Time the peer has been in its current state. On first establishing of the peer, the format of the time and date values in the MIB changes frequently. On the first day new values are written to the database every five minutes. After the first day, Entuity only updates established information daily.

Table 136 EIGRP Peer Stream Attributes

## **OSPF Routing Protocol**

The Open Shortest Path First (OSPF) protocol is a hierarchical interior gateway protocol (IGP) for routing in Internet Protocol, using a link-state in the individual areas that make up the hierarchy. Routing Protocols Extension supports OSPF version 2, which supports IPv4.

A link state database (LSDB) is constructed as a tree-image of the network topology, and identical copies of the LSDB are periodically updated on all routers in each OSPF-aware area. By convention, area 0 represents the core region of an OSPF-enabled network, and other OSPF area numbers may be designated to serve other regions of an enterprise (large, business) network - however every additional OSPF area must have a direct or virtual connection to the backbone OSPF area. The backbone area has the identifier 0.0.0.0. Inter-area routing goes via the backbone.

Routers in the same broadcast domain or at each end of a point-to-point telecommunications link form adjacencies when they have detected each other. This detection occurs when a router identifies itself in a hello packet. This identifies a two way state. The router selects a designated router (DR) and a backup designated router (BDR) which act as a hub to reduce traffic between routers. OSPF uses both unicast and multicast to send hello packets and link state updates.

#### **OSPF General Attributes**

Attribute	Description
Router ID	Unique identifier for the router as defined by the <b>ospf router-id</b> command or the address of the loopback 0 interface.
Options	Summarized description of the device, e.g. stub area, TOS capability.

Table 137 OSPF General Attributes

Attribute	Description
Priority	<ul> <li>Helps determine the designated router for this network. When two routers attached to a network both attempt to become the designated router, the one with the higher router priority takes precedence. If there is a tie, the router with the higher Router ID takes precedence.</li> <li>When priority is set to: <ul> <li>0, it is ineligible to become the designated router or backup designated router.</li> <li>1, is the lowest priority and also the default. The highest value is 255.</li> </ul> </li> </ul>
Remote Peer IP Address	IP address of remote OSPF peer interface.
Local Peer IP Address	IP address of local OSPF peer interface.
Hello Suppressed	<ul> <li>When set to:</li> <li>True, suppression of the hello message may indicate point-to-point interfaces, where only one end of the circuit sends hello messages. Periodic hello messages are suppressed and periodic refreshes of link-state advertisements (LSAs) do not flood the demand circuit.</li> <li>False, indicates the device sends periodic hello messages.</li> </ul>
Permanence	Type of peering permanence, e.g. Dynamic.

Table 137 OSPF General Attributes

#### **OSPF Peer Stream Attributes**

Entuity polls for router OSPF state information every five minutes and uses these values for event generation.

Attribute	Description
State	Current state of the router. <b>Full</b> is the normal state. If a router remains in another state, it is an indication that there are problems in forming peerings.
State Changes	Number of state changes during the polling interval.
Retry Queue	Current retries queue length.

Table 138 OSPF Peer Stream Attributes

# **IS-IS Routing Protocol**

The Intermediate System to Intermediate System (IS-IS) is an interior gateway protocol, intended to work in administrative domains and networks. It is a link-state routing protocol, that uses the DECnet Phase V routing method, in which routers

exchange data about routing using a single metric to determine the network topology. Each IS-IS router independently builds a database of the network's topology, aggregating the flooded network information.

As with the OSPF protocol, IS-IS uses Dijkstra's algorithm for computing the best path through the network. Packets are then forwarded using the computed ideal path through the network to the destination.

#### **IS-IS Support**

Entuity implementation of IS-IS routing protocol support represents:

- IS-IS peers at the device level.
- IS-IS circuits at the device level.
- IS-IS Port Peers at the port level.
- Peering from one device's IS-IS peered port to the other device's IS-IS peered port.

Firefox 🔻													
entuity											User: admin@ea Page Updated: 1	arth 14:39:14, E	[Loqout] BST
Dashboards I	InSight Center	Explorer	Events	Maps C	Charts Flow	s Reports	Tools	Administration	Preferences	Help			PŢ
JIS-IS	S PortPe	er: Por	t: [ Fa	<b>0/1</b> ]	FastEt	ernet0	/1, 19	6-IS Peer	to IP: 1	0.73.	30.1, MAC	: ca-1	1 <b>3-09-</b> 1
ຼ ກຼິ Summary	111 Thresho	old ាំ្្ំ⊕ A	Advanced										22
Events No open incide	ents ( <u>View Event</u>	t History)											_
General In	fo												
IS-IS Peer R MAC:	temote IP, 1 1	0.73.30.1:ca 3-09-19-00-0	- 18:4.1	IS-1 Nan	IS Port Peer ne:	Port: [Faŭ Peer to	)/1]FastE	thernet0/1, IS-IS	S Display Name:	Port: Peer	[Fa0/1] FastEthen to	net0/1, IS-	-IS

Figure 21 IS-IS Port Peer

IS-IS routing protocol support includes its representation on the map. Entuity map allows the:

- Display of IS-IS Port Peer connectivity, identifying each end of the port peers.
- Drill-down of the port peers.
- Color of the link between peers to show the state of each peer.

Firefox 🔻														0	<b>X</b>
entuity													User: admin@eart <u>Page Updated</u> : 14:	h :35:46, BS	[Loqout] ST
Dashboards	InSight Center	Explorer	Events	Maps	Charts	Flows	Reports	Tools	Administ	ration	Preferences	Help			PŢ
*	🎝 🕞 🖓	- + J	• R	€ 9	ā	<u></u>	s 🔅 🗸	🗽 🗙	8	• 🌒	is-is				
Links: IS-IS	Show: Status	Highlight: N	one												
					~										
				1	10.73.11	1.1			10.7	73.21.1					
•								State	Incident None	Port: [F	10.73.21.1 Fa0/1 ] FastEt	<u>hern</u> <-	<b>10.73.31.</b> -> <u>Port: [Fa0/0] Fasti</u>	L Ethern	X (IS-IS)
					-										
					10.73.1	1.2			10.	73.31.1	1				



IS-IS allows includes events and their associated incidents for identifying when:

- IS-IS Peer Disappeared
- IS-IS Peer Established
- IS-IS Peer Newly Discovered
- IS-IS Peer Not Established.

#### **IPv6 Peering**

Entuity has a number of methods for obtaining IP addresses for port peers it only stores IPv4 addresses and uses those for port peering. IS-IS may appear to identify links between IPv6 devices, however the peering is not through the IPv6 addressing but through the device's MAC addresses.

# **15 Entuity Cisco SSL Services**

Entuity manages SSL proxy servers as logical devices, using their IP address to generate device type information. You can view proxy device inventory details using the web UI and Entuity reports.



Figure 23 SSL Proxy Device

Stream Attribute	Description
Notification Interval	The SSL Certificate Notification Interval displayed as hours. Entuity raises an expiry event for any SSL certificates on this device that will expire within the notification period. Within Entuity you can amend this value.
SSL Certificates	
Certificate Name	Name of the certificate.
Start Date	First date of the certification period.
Time until Expiry	Time until the certificate expires. Entuity polls the expiry date every twenty-four hours.
Serial Number	Certificate serial number.
Web Site	Site associated with the certificate.
Certificate Authority	Name of the authorizing authority.
SSL Proxy Servers	SSL Proxy Servers will be displayed as managed objects within their own folders underneath each Cisco SSL Service Device.
Virtual Server TCP Port	The virtual server transport protocol (TCP), and port number for which the SSL Services Module is the proxy.
Real Server TCP Port	Real TCP port used by the proxy server.
Operation Status	Current operational status.
Virtual Server IP Address	The virtual server IP address for which the SSL Services Module is the proxy.
Administrative Status	Current administrative status.
Operational Down Reason	Reason for the current Operation Status.
Real Server IP Address	Real IP address used by the proxy server.
Туре	Network management object type.

Table 139 SSL Proxy Stream Attributes

# **16 VPN Gateways**

Entuity includes an extensive breakdown of the VPN Gateway inventory, resource and performance data. Entuity manages VPN Gateways through the VPN device type. Many of the VPN tabs are standard tabs applicable to other device types. This section outlines tabs of particular interest or specific to VPN Gateway management.

## **VPN Attributes**

Stream Attribute	Description
Uptime	The length of the time the device has been up. You can also run Inventory reports on Device Uptime.
Maximum Allowed Tunnels	Maximum number of allowed simultaneous VPN tunnels.
VPN Resources	
Free Memory	Total free memory on the device.
Load Average	Average number of processes in the runqueue since the previous poll (default five minutes). A load average of one is good, lower than one signifies a light load. A VPN Gateway can operate with a load average of 10.
Active Tunnel Count	Number of active tunnels when the device was polled.
Active Tunnel Usage%	Number of active tunnels when the device was polled expressed as a percentage of the maximum number of tunnels allowed.
VPN Traffic Inbound Rate	Total inbound VPN traffic rate.
VPN Traffic Outbound Rate	Total outbound VPN traffic rate.
Bad Auth Error Rate	Number of times tunnel authentication failed due to errors other than an invalid signature, an invalid certificate or no profile.
Tunnels Landed Rate	Number of remote user tunnels formed since the VPN Gateway was last configured.
Failed Connections Rate	Number of failed connections since the last poll.
Successful Connections Rate	Number of successful connections since the last poll

Stream Attribute	Description
Packet Loss Clear Rate	Counter that indicates the number of packets dropped from the NIC driver.
Packet Loss Tunnel Rate	Counter that indicates the number of packets dropped from the encryption/decryption queue.
VPN Hourly Resources	
Free Memory Hourly Mean	Total free memory on the device expressed as a mean average over the previous hour.
Load Average Hourly Mean	Average number of processes in the runqueue since the previous poll (default five minutes).
Load Average Hourly Max	Maximum number of processes in the runqueue over the previous hour.
Active Tunnel Count Hourly Max	Maximum number of active tunnels over the previous hour.
Active Tunnel Count Hourly Mean	Number of active tunnels expressed as a mean average over the previous hour.
VPN Traffic Inbound Rate Hourly Max	Maximum value polled over the previous hour of the total inbound VPN traffic rate.
VPN Traffic Inbound Rate Hourly Mean	Total inbound VPN traffic rate expressed as a mean average over the previous hour.
VPN Traffic Outbound Rate Hourly Max	Maximum value polled over the previous hour of the total outbound VPN traffic rate.
VPN Traffic Outbound Rate Hourly Mean	Total outbound VPN traffic rate expressed as a mean average over the previous hour.
Bad Auth Error Rate Hourly Mean	Number of times tunnel authentication failed due to errors other than an invalid signature, an invalid certificate or no profile, expressed as a mean average over the previous hour.
Tunnels Landed Rate Hourly Mean	Number of remote user tunnels formed since the VPN Gateway was last configured, expressed as a mean average over the previous hour.
Failed Connection Rate Hourly Mean	Number of failed connections expressed as a mean average over the previous hour.
Successful Connections Rate Hourly Mean	Number of successful connections expressed as a mean average over the previous hour.
Packet Loss Clear Rate Hourly Mean	Rate of packet loss per second, of traffic passing through the device in clear, non-tunnel mode, expressed as a mean average over the previous hour.

Stream Attribute	Description				
Packet Loss Tunnel Rate Hourly Mean	Rate of packet loss per second, of traffic passing through the device in tunnel mode, expressed as a mean average over the previous hour.				
VPN Daily Resources					
Free Memory Daily Mean	Total free memory on the device expressed as a mean average over the previous day.				
Load Average Daily Mean	Average number of processes in the runqueue over the previous day.				
Load Average Daily Mean of Hourly Max	<i>lean</i> Mean average of the previous day's hourly maximum load average hourly values.				
Load Average Daily Max	Maxim number of processes in the runqueue over the previous day.				
Active Tunnel Count Daily Max	Maximum number of active tunnels over the previous day.				
Active Tunnel Count Daily Mean	Number of active tunnels expressed as a mean average over the previous day.				
Active Tunnel Count Daily Mean of Hourly Max	Mean average of the previous day's hourly maximum active tunnel count average hourly values.				
VPN Traffic Inbound Rate Daily Max	Maximum value polled over the previous day of the total inbound VPN traffic rate.				
VPN Traffic Inbound Rate Daily Mean	Total inbound VPN traffic rate expressed as a mean average over the previous day.				
VPN Traffic Inbound Rate Daily Mean of Hourly Max	Mean average of the previous day's inbound VPN traffic rate average hourly values.				
VPN Traffic Outbound Rate Daily Max	Maximum value polled over the previous day of the total outbound VPN traffic rate.				
VPN Traffic Outbound Rate Daily Mean	Total outbound VPN traffic rate expressed as a mean average over the previous day.				
VPN Traffic Outbound Rate Daily Mean of Hourly Max	Mean average of the previous day's outbound VPN traffic rate average hourly values.				
Bad Auth Error Rate Daily Mean	Number of times tunnel authentication failed due to errors other than an invalid signature, an invalid certificate, or no profile, expressed as a mean average over the previous day.				

Stream Attribute	Description
Tunnels Landed Rate Daily Mean	Number of remote user tunnels formed since the VPN Gateway was last configured, expressed as a mean average over the previous hour.
Failed Connection Rate Daily Mean	Number of failed connections expressed as a mean average over the previous day.
Successful Connections Rate Daily Mean	Number of successful connections expressed as a mean average over the previous day.
Packet Loss Clear Rate Daily Mean	Rate of packet loss per second, of traffic passing through the device in clear, non-tunnel mode, expressed as a mean average over the previous day.
Packet Loss Tunnel Rate Daily Mean	Rate of packet loss per second, of traffic passing through the device in tunnel mode, expressed as a mean average over the previous day.
VPN Network Ports	
Name	Port index number.
Speed	The port's interface speed. For use in Entuity your System Administrator can amend the port interface speed.
IP Addresses	A list of the port's IP addresses.
Description	A description of the port.
VPN Port Performance	
Inbound Util	Inbound utilization of the port expressed as a percentage of the port's capacity.
Outbound Util	Outbound utilization of the port expressed as a percentage of the port's capacity.
Inbound Byte Rate	Inbound byte rate at the time of polling.
Outbound Byte Rate	Outbound byte rate at the time of polling.
Inbound Packet Rate	Inbound packet rate at the time of polling.
Outbound Packet Rate	Outbound packet rate at the time of polling.
Inbound Error Rate	Inbound error rate at the time of polling.
Outbound Error Rate	Outbound error rate at the time of polling.
Inbound Discard Rate	Inbound discard rate at the time of polling.
Outbound Discard Rate	Outbound discard rate at the time of polling.

Stream Attribute	Description
Hourly VPN Port Performance	
Inbound Util Hourly Mean	Inbound utilization of the port over the previous hour expressed as a percentage of the port's capacity.
Outbound Util Hourly Mean	Outbound utilization of the port over the previous hour expressed as a percentage of the port's capacity.
Inbound Util Hourly Max	Maximum inbound utilization of the port polled over the previous hour expressed as a percentage of the port's capacity.
Outbound Util Hourly Max	Maximum outbound utilization of the port polled over the previous hour expressed as a percentage of the port's capacity.
Inbound Byte Rate Hourly Mean	Inbound byte rate, expressed as a mean average over the previous hour.
Outbound Byte Rate Hourly Mean	Outbound byte rate, expressed as a mean average over the previous hour.
Inbound Byte Rate Hourly Max	Inbound byte rate, expressed as a mean average over the previous hour.
Outbound Byte Rate Hourly Max	Outbound byte rate, expressed as a mean average over the previous hour.
Inbound Packet Rate Hourly Mean	Inbound packet rate, expressed as a mean average over the previous hour.
Outbound Packet Rate Hourly Mean	Outbound packet rate, expressed as a mean average over the previous hour.
Inbound Error Rate Hourly Mean	Inbound error rate, expressed as a mean average over the previous hour.
Outbound Error Rate Hourly Mean	Outbound error rate, expressed as a mean average over the previous hour.
Inbound Discard Rate Hourly Mean	Inbound discard rate, expressed as a mean average over the previous hour.
Outbound Discard Rate Hourly Mean	Outbound discard rate, expressed as a mean average over the previous hour.

Stream Attribute	Description
Daily VPN Port Performance	
Inbound Util Daily Mean	Inbound utilization of the port over the previous day expressed as a percentage of the port's capacity.
Outbound Util Daily Mean	Outbound utilization of the port over the previous day expressed as a percentage of the port's capacity.
Inbound Util Daily Max	Maximum inbound utilization of the port polled over the previous day expressed as a percentage of the port's capacity.
Outbound Util Daily Max	Maximum outbound utilization of the port polled over the previous day expressed as a percentage of the port's capacity.
Inbound Util Daily Mean of Hourly Max	Mean average of the previous day's port inbound utilization average hourly values.
Outbound Util Daily Mean of Hourly Max	Mean average of the previous day's port outbound utilization average hourly values.
Inbound Byte Rate Daily Mean	Inbound byte rate, expressed as a mean average over the previous day.
Outbound Byte Rate Daily Mean	Outbound byte rate, expressed as a mean average over the previous day.
Inbound Byte Rate Daily Max	Inbound byte rate, expressed as a mean average over the previous day.
Outbound Byte Rate Daily Max	Outbound byte rate, expressed as a mean average over the previous day.
Inbound Byte Rate Daily Mean of Hourly Max	Mean average of the previous day's port inbound byte rate average hourly values.
Outbound Byte Rate Daily Mean of Hourly Max	Mean average of the previous day's port outbound byte rate average hourly values.
Inbound Packet Rate Daily Mean	Inbound packet rate, expressed as a mean average over the previous day.
Outbound Packet Rate Daily Mean	Outbound packet rate, expressed as a mean average over the previous day.
Inbound Error Rate Daily Mean	Inbound error rate, expressed as a mean average over the previous day.

	nti	1111
	ни	אזונא
_		

Stream Attribute	Description
Outbound Error Rate Daily Mean	Outbound error rate, expressed as a mean average over the previous day.
Inbound Discard Rate Daily Mean	Inbound discard rate, expressed as a mean average over the previous day.
Outbound Discard Rate Daily Mean	Outbound discard rate, expressed as a mean average over the previous day.

# **VPN Gateway Resources**

For VPN Gateway resource values are useful in monitoring VPN Gateway inventory, through tools, events and the extensive history available to reporting. The Resources tab is available against all devices.

# **17 Wireless Controllers and WAPs**

Entuity Wireless module supports these wireless controllers and access points:

- Wireless Controllers
- Trapeze WAPs
- Cisco WAPs
- AWAPs and their Wireless Ports
- AWAPs.

## **Wireless Controllers**

Entuity Wireless directly manages Wireless Controllers which are assigned a unique device type (GMF) number of 1102 by the corresponding vendor files. All other aspects of the wireless network configuration are discovered by further SNMP interrogation of the Wireless Controllers.

Each Wireless Controller has a collection of Wireless Access Points (WAPs) associated to it. Each WAP has zero or more Antennas available (WAPs that are listed as 'down' do not list any antennas). Each Wireless Controller also has one or more Wireless LANs (WLANs) each of which has an associated SSID string.

Entuity manages Wireless Controllers as a sub-type of device, and can therefore present generic device information. This information is available through standard tabs in Entuity.

#### Wireless Controllers Stream Attributes

Stream Attribute	Description
Foreign AP Supported	Foreign AP supported.
Max Number of APs Supported	Max number of APs supported.
IP Address	The switch's network IP address.
Web Access Mode	The switch's web access mode.

Table 141 Wireless Controllers Stream Attributes

Stream Attribute	Description
Mgmt via Wireless	Management via wireless is allowed or not.
Host Count	Attached host count.
Number of APs currently connected	Number of APs currently connected.
Cisco Only	
Machine type	Machine type.
Maintenance Level	Maintenance level.
Operating System	Operating system.
GigE Card Present	GigE card present.
Crypto Card Present	Crypto card present.
LWAPP Transport Mode	LWAPP transport mode.
Device Name	Name of the device this controller is residing on.
Slot Number	Slot number in the chassis that this controller is residing in.
Port Number	Port number on the chassis that this controller is residing in.
Peer Port Number	Port number of this controller's peer on the same slot on chassis that this controller is residing in.
Peer IP Address	IP address of this controller's peer on the same slot on chassis that this controller is residing in.
Default Gateway	The switch's network default gateway.
Config Protocol	The switch's network config protocol.
Distribution Port	The switch's distribution port number.
Idle Timeout	The switch's idle timeout in seconds.
ARP Timeout	The switch's ARP entry timeout in seconds.
Mgmt VLAN ID	VLAN ID of the network management interface.
GVRP Status	GVRP support status.
Burned-In MAC Address	The switch's Burned-In MAC address.
Subnet Mask	The switch's network subnet mask.
Multicast Support	Switch's ethernet multicast support.

Table 141 Wireless Controllers Stream Attributes

Stream Attribute	Description
Broadcast SSID Mode	When enabled, this mode allows WLAN SSIDs to be broadcasted.

Table 141 Wireless Controllers Stream Attributes

 $\odot$ 

Wireless controllers from different vendors, e.g. Cisco, Trapeze, Aruba, use different MIBs that do not contain exactly the same information. Entuity Wireless either does not display attributes which do not apply to a device, or displays the attribute with a null value.

Entuity Wireless Controllers can monitor wireless networks through their Wireless Controller architecture. In large wireless network deployments, individual Wireless Access Points (WAPs) are logically associated with a Wireless Controller. Some larger networks use multiple Wireless Controllers and have separate groups of Access Points associated with each Controller.

All SNMP management communication is performed with Wireless Controllers rather than with the Access Points. The Wireless Controllers act as a management proxy into the wireless network and can provide details of the configuration and behavior of each Access Point, Antenna/Radio and wireless attached host.

Entuity Wireless discovers and monitors the Wireless Controllers and their associated Access Points and Antennas/Radios. Entuity Wireless gathers inventory, configuration, performance and fault statistics, from which reports and events can be generated.



Figure 24 Trapeze Wireless Controller Details

Entuity

# Trapeze WAPs

## **Trapeze WAPs General Attributes**

Attribute	Description
Associated Wireless Controller	Name of the wireless controller associated with this WAP.
Connection Type	Connection Type, e.g. LWAPP, SLAPP or CAPWAP.
Dot3 MAC Address	Dot3 MAC address of the WAP.

Table 142 Trapeze WAPs General Attributes

### Trapeze WAPs Stream Attributes

Stream Attribute	Description
Admin Status	AP administrative status.
Boot Version	Major minor boot version of AP.
CPU Speed	Reported speed of the AP CPU.
Group VLAN Name	The AP Group to which this AP has been associated with.
Host Count	Attached host count.
Memory available	Reported memory of the AP.
Model	AP model number.
Oper Status	AP operational status.
Serial Number	AP serial number.

Table 143 Trapeze WAP Stream Attributes

#### Entuity

# Cisco WAPs

## **Cisco WAPs General Attributes**

Attribute	Description
Associated Wireless Controller	Name of the wireless controller associated with this WAP.
Is Static IP	When <b>disabled</b> , the WAP will use DCHP to get the IP address. When <b>enabled</b> , the user should enter the IP address, Netmask and Gateway.
Static IP Address	Static IP address configuration for the WAP. This can only be changed when the LWAPP mode is in Layer-3.
IP Address	IP address. This will not be available when the switch is operating in the Layer-2 mode.
Location	User specified location of the WAP.
Netmask	The Netmask of the IP address of the WAP.
Gateway	Gateway for the WAP.
Ethernet MAC Address	Access point MAC address.
Dot3 MAC Address	Dot3 MAC address of the WAP.

Table 144 Cisco WAP General Attributes

#### **Cisco WAPs Stream Attributes**

Stream Attributes	Description
Oper Status	AP operational status.
Admin Status	AP administrative status.
Host Count	Attached host count.
Boot Version	Major minor boot version of AP.
Model	AP model number.
Serial Number	AP serial number.
Group VLAN Name	The AP Group to which this AP has been associated with.

Table 145 Cisco WAP Stream Attributes

Stream Attributes	Description
Primary Controller Name	SysName of the primary wireless controller with which AP should associate.
Secondary Controller Name	SysName of the secondary wireless controller with which AP should associate.
Tertiary Controller Name	SysName of the tertiary wireless controller with which AP should associate.
IOS Version	AP IOS version.

Table 145 Cisco WAP Stream Attributes

## AWAPs and their Wireless Ports

Entuity Wireless monitors Autonomous WAPs (AWAPs) as an extension of devices, providing both standard device information as well as wireless specific information. Similarly, Entuity Wireless monitors wireless ports as an extension of ports, providing information on both standard and wireless specific port attributes.

## **AWAPs**

Entuity manages AWAPs as a sub-type of device, and as a device Entuity presents standard information on AWAPs. Through its standard functionality Entuity also details for each AWAP:

- General identifying information
- Routing and Router Buffer Summary details
- Memory Pools, Processors, Resources
- Chassis Data
- Applications.

Attribute	Description
Host Count	Attached host count.
Wireless Ports	

Table 146 Autonomous WAP Details



Figure 25 Autonomous WAP Details

# 18 WAAS

# **WAAS General Attributes**

Attribute	Description
WAAS Cluster ID	Identifier of the cluster to which the WAAS device belongs.
WAAS Cluster Name	Name of the cluster to which the WAAS device belongs.
WAAS Device Type	Type of WAAS device, i.e. core, edge.

Table 147 WAAS General Attributes

# WAAS Stream Attributes

Stream Attribute	Description
Active Sessions	Number of active sessions.
Authenticated Response Time	
External URL Response Time	
Last Evicted Time	Cache statistics.
Max Cache Volume	Maximum cache volume.
Messages Received	Status messages received in the last five minutes.
Processes	Number of processes.
Resource Evicted Number	Number of resources evicted per second.
User	Number of users.
Volume High Watermark	Volume high watermark.
Volume Low Watermark	Volume low watermark

Table 148 WAAS Stream Attributes

Stream Attribute	Description
Volume Percentage High Watermark	Volume percentage high watermark.
Volume Percentage Low Watermark	Volume percentage low watermark.
WAAS CIFS Connected Session Count	WAAS CIFS connected session count.
WAAS CIFS Local Request Count	WAAS CIFS local request count.
WAAS CIFS Open Files	Number of open files.
WAAS CIFS Remote Request Count	WAAS CIFS remote request count.
WAAS CIFS Total Local Time	WAAS CIFS total local time.
WAAS CIFS Total Octets Read	CIFS total octets read.
WAAS CIFS Total Octets Written	WAAS CIFS total octets written.
WAAS CIFS Total Remote Time	WAAS CIFS total remote time.

Table 148 WAAS Stream Attributes

## WAAS Device Connection Details

Attribute	Description	Description
WAAS Connection Name	Entuity derived connection name.	nnection name.

Table 149 WAAS Device Connection Details

## WAAS Device Connection Statistics

Attribute	Description
Inbound Compression Ratio (%)	Inbound compression ratio (%) of the traffic for the connection.
Outbound Compression Ratio (%)	Outbound compression ratio (%) of the traffic for the connection.
Inbound Traffic Octets per sec	Inbound traffic octets per second.
Outbound Traffic Octets per sec	Outbound traffic octets per second.
Inbound Messages per sec	Inbound messages per second.
Outbound Messages per sec	Outbound messages per second.

Table 150 WAAS Device Connection Statistics

### WAAS Device Connection Status

Attribute	Description
Connection Status	Indicates the current status of the connection, Yes connected, No disconnected.

Table 151 WAAS Device Connection Status
# Glossary

## 802.1p

An IEEE standard for providing quality of service (QoS) in 802-based networks. 802.1p uses three bits (defined in 802.1q) to allow switches to reorder packets based on priority level. It also defines the Generic Attributes Registration Protocol (GARP) and the GARP VLAN Registration Protocol (GVRP). GARP lets client stations request membership in a multicast domain, and GVRP lets them register into a VLAN.

## AAL (ATM Adaptation Layer)

AAL enhances the service provided by the ATM layer to a level required by the next higher layer. It performs the functions for the user, control and management planes and supports the mapping between the ATM layer and the next higher layer.

## **Advanced Actions**

Advanced Actions, also known as user menus and user actions, are defined through configuration files. Actions may be automatically triggered through Entuity raising an appropriate event, or interactively through advanced action menus, available both from the menu bar and context menus.

## Agent

Intelligent management software embedded in a network device. In network management systems, agents reside in all managed devices and report the values of specified variables to management stations.

## Antenna / Radio

Each Wireless Access Point has one or more Antennas. Each Antenna is attached to an 802.11 radio within the Access Point. Wireless Hosts communicate with the network via a wireless association with an Antenna/Radio. Each Antenna/Radio can have multiple hosts simultaneously attached. Each Antenna/Radio operates in a chosen 802.11 compatibility mode such as 802.11a, 802.11b or 802.11g. Additionally, each Antenna/Radio has a single SSID assigned. Each Antenna/Radio operates on a chosen radio channel and with a specified transmit power setting, which is measured in mW. Many controller based installations use dynamic optimization algorithms to pick a suitable channel and power setting. Frequent auto-adjustment of these setting indicates that there are problems being encountered with the quality of the wireless communications.

## AP (Access Point) / WAP (Wireless Access Point)

A device that has one or more 802.11 radios and Wireless Antennas. For example, laptops, PDAs, connect to a wired LAN through an AP, which is a hardware device or software that acts as a communication hub.

It bridges traffic from wireless attached hosts to/from an Ethernet interface that connects to an access layer switch port. APs provide heightened wireless security and extend the physical range of a wireless LAN. The access layer switch will see the MAC addresses of the individual wireless attached hosts (the MAC address of the wireless NICs) plus the MAC of the Access Point Ethernet interface.

## **AR System**

BMC Remedy Action Request System (AR System) is a framework within which applications are built by AR System administrators. Applications consist of a set of AR System forms that are linked using workflow rules designed for the application. These forms contain fields which Entuity can be configured to populate.

## ARs

Entuity integrates with AR System to generate Action Requests (ARs). The sample integration with the Remedy Help Desk includes ARs of the type incident.

## ARP

ARP (Address Resolution Protocol) is the layer 2 standard for TCP/IP. It is used to obtain a node's physical address when only its logical IP address is known.

## ATM

ATM (Asynchronous Transfer Mode) is a packet-switching technology, that delivers high-speed performance together with a scalable architecture. Its use of small packets (fixed length cells of 53 bytes), provide for low latency so sound and vision arrive together. It can also handle bursty, non time-sensitive data, translating variable length packets to fixed size packets.

## Attribute

In Entuity an attribute is a property of an object that is defined through Entuity Configurable Framework. Attribute data can be charted using the Attribute Grapher and is available to Report Builder.

## Autonomous Wireless Access Point (AWAP)

A Wireless Access Point (WAP) that embodies all of its necessary control functionality in a self-contained manner. AWAPs are usually connected to switched access layer ports and

can coexist with ordinary wired connections to end user hosts and servers on the same switch. AWAPs do not require wireless controllers and do not interact with them if they exist.

#### Backbone

The part of a network that acts as the primary path for traffic that is most often sourced from, and destined for, other networks.

#### BECN (Backward Explicit Congestion Notification)

BECN is a bit in the header of a frame-relay frame that is set when frames are sent on the data path backwards from destination to source. It indicates congestion to the source node.

WAN News combines BECN and FECN values to determine congestion on a data path.

#### Bandwidth

The upper limit of the rate at which data can be transferred.

#### **BMC Atrium CMDB**

The BMC Atrium Configuration Management Database (BMC Atrium CMDB) is a data repository that provides a working model of your enterprise IT infrastructure.

#### BMC Cell

BMC Impact Manager instance. A cell receives events from Entuity and displays them in the BMC IX.

#### **BMC II Web Services Server**

BMC Impact Integration Web Services Server. You can connect to the BMC II Web Services at the end point as defined by the URL format, http://webServerHostName: webServerPortNumber/webServiceName, e.g. http://decade:6080/impactManager.

#### BMC IX

BMC IX (BMC Impact Explorer) displays events received from Entuity.

#### BMC ProactiveNet Performance Management

BMC ProactiveNet Performance Management which receives events from Entuity.

#### Blackout

Blackout is complete loss of the network, as opposed to a brownout, which is degradation in the performance of the network.

## BPDU

Bridge Data Protocol Units are special frames that contain spanning tree information. There are two types of BPDU, Topology Change Notification (TCN) BPDU contains topology change information, Configuration BDU contain configuration information.

## Bridge

A device that interconnects local or remote networks. Bridges form a single logical network, centralizing network administration. They operate at the physical and link layers of the OSI Reference Model.

## Brownout

Brownouts, also known as soft faults, are typically caused by cabling faults, faulty transceivers, faulty NIC cards and configuration errors such as duplex/half-duplex mismatches. These problems cause a percentage of the packets traversing that particular area of the network to be corrupted. The total number of packets discarded as a percentage of packets is directly related to the severity of the brownout.

## Burst

Burst is the access rate of the physical connection to the Frame Relay carrier network.

## **Central Server**

A central server is an Entuity server trusted by remote Entuity server(s). A user logged into the central Entuity server is able to view information collected by the remote Entuity server(s), according to their user account access rights. A remote Entuity server responds to requests from a trusted central Entuity server, and freely shares information with it.

An Entuity server can be configured to perform both roles, be both a remote and central Entuity Server. This allows administrators to create both hub-n-spoke and fully meshed deployments.

A central Entuity server can also act as a central license server. From it you can allocate, and de-allocate, license credits to its remote servers.

Configuration of central and remote servers is through the Multi-Server Administration area of the Entuity web UI.

# CDP (Cisco Discovery Protocol)

CDP is primarily used to obtain protocol addresses of neighboring devices and discover the platform of those devices. CDP can also be used to show information about the interfaces your router uses. CDP is media- and protocol-independent, and runs on all Cisco-manufactured equipment including routers, bridges, access servers, and switches.

Entuity uses CDP as a method when maintaining links on maps and identifying trunk ports.

# CI

Within BMC Atrium CMDB a Configuration Item (CI) is a collection of objects related to the specific functionality of a larger system.

## CIR

Committed Information Rate is the rate (in bps) that the network agrees to transfer information over a permanent virtual circuit (PVC) in Frame Relay. The CIR applies to the rate of data entering the network.

## **Cisco IOS IP SLA Operations**

Cisco IOS IP SLA Operations are created on devices by Entuity (via SNMP). Entuity currently fully supports DHCP, DNS, HTTP, HTTP Raw, ICMP Echo, ICMP Path Echo, TCP, UDP Echo, UDP Jitter and UDP Jitter VoIP operations. Entuity can also monitor operations other than these ten, for example FTP. The completeness of the returned data depends upon how close the operation's data structure corresponds to Entuity's default representation of the IP SLA operation data structure.

These are the ten fully supported operations:

- DHCP, Verify availability of dynamic IP addresses.
- DNS, DNS server functionality check.
- HTTP, Web page availability.
- HTTP Raw, Web page availability.
- ICMP Echo, Simple connectivity tests.
- ICMP Path Echo, Simple connectivity tests.
- TCP, Connect Application availability.
- UDP Echo, Simple connectivity tests.
- UDP Jitter, Detailed latency measurements (requires IP SLA on both devices).
- UDP Jitter VoIP, Detailed latency measurements (requires IP SLA on both devices).

#### Client

A computer that requests a service from another. In Entuity the Java client is Component Viewer which requests, for example, information from the Entuity server on the devices on your network.

## Collisions

Collisions occur when two transmitters attempt to send data at the same time. The greater the number of collisions the poorer network performance appears.

## **Component Viewer**

Component Viewer is the Entuity Java client, available through the web UI Tools menu. Through it you can quickly scan the network for both current and historical performance data. It creates an intuitive hierarchy which lets you easily view configuration settings, check status information and launch fault, utilization and traffic volume history graphs.

#### **Context Menus**

Context menus are available from the Entuity web UI and Component Viewer. The contents of the menu are dependent on the position of the mouse when you clicked the right button.

#### **Core Ports**

Entuity considers core ports, as WAN ports, administratively up ports which have a configured IP addresses (i.e. layer 3 ports) on devices which are routers or have router capability, or trunks and uplinks that are administratively up.

By default the port status event, Port Operationally Down, is only enabled for core ports.

#### **Current Configuration**

The device configuration (either startup- or running) currently being processed.

## **DLCI (Data Link Connection Identifier)**

A unique logical identifier assigned to a PVC end point in a frame relay network. It identifies a particular PVC endpoint within a user's access channel therefore allowing multiple connections to many destinations over a single, physical channel.

## Data Management Kernel (DMK)

The DMK supports Entuity's intelligent discovery function. It includes out of the box data models for a wide range of managed devices including hundreds of Ethernet switches and routers. These customizable data models define the attributes of each managed element, its possible dependencies in relation to other elements of the network, and the specific details to retrieve for each element. The DMK manages these data models and automatically applies updates and changes to the Entuity database schema.

#### Data Path

A data direction on each PVC is a data path. For example, a PVC that connects points A and B has two data paths, from A to B and from B to A. WAN News analyzes the data paths separately.

## Data Rollup

Data Rollup is a method of taking polled data and bundling it into larger more manageable units, e.g. rolling 24 hourly datapoints into one daily sample. If Entuity generated monthly reports from live polled data then this would cause a significant increase on the processing overhead, i.e. instead of one datapoint for each day there would be hundreds.

## **DE (Discard Eligibility)**

DE is a bit in the header of a frame-relay frame that indicate the frame may be discarded in preference to other frames if congestion occurs. It is usually set by a network node if the user is offering data (frames) at a higher rate than has been negotiated. This maintains the committed quality of service within the network. Frames with the DE bit set are considered to be excess data.

## **Derived Events**

IA derived event is an event derived from an existing event definition. It retains the event identifier of the original definition, unlike a custom event which has its own unique identifier. Derived events are defined as part of an action. They useful for adding additional information to an incoming event, and can also be called from an incident.

#### Devices

In Entuity devices refers to network devices, for example switches and routers.

## **Device Support Datasets**

Device support datasets define the attributes of each managed element, its device type, its possible dependencies in relation to other elements of the network, and the specific details to retrieve for each element. This comprehensive library streamlines modeling and ultimately shows exactly what you own, where it is deployed and how it is connected.

Datasets are available through these types of vendor files, all have a .vendor extension. These vendor files are, listed in ascending order of priority:

newbin.vendor, which is created in *entuity\_home*\etc when Entuity discovers devices with sysoids for which there is not a device support dataset. These generic device support datasets should be considered temporary definitions, and only used until Entuity supply an appropriate vendor file.

Device support datasets in newbin.vendor have the lowest priority when Entuity is determining which vendor device definition to use to manage a device type.

- bin.vendor has the second lowest priority when Entuity is determining the source of device information.Device support datasets in bin.vendor have the second lowest priority when Entuity is determining which of those available to use to manage a device type.
- exotica vendor files are installed to *entuity\_home*\etc\exotica. Exotica files are only used by Entuity when they are copied to *entuity\_home*\etc, either manually or during Entuity configuration, e.g. when selecting a module.

Device support datasets in exotica vendor files have the highest priority when Entuity is determining which vendor device definition to use to manage a device type. These files use a simple naming convention, using the vanilla filename, with a plus sign in the filename and identifying name, e.g. SOLSERV+managed Host.vendor.

During Entuity upgrades configure identifies and removes exotica files from the installation that are now part of the updated bin.vendor.

vendinfo identifies the vendor device support datasets available to Entuity and the decisions made when more than one vendor file is available for a particular sysoid; which device support dataset Entuity uses to manage that device type (as identified through its sysoid).

## **Device Types**

In Entuity every device has a type, which you can view through the web interface and Component Viewer. The device type is derived from its vendor file information, and helps to determine how Entuity manages a device. Device types include hubs, switches and routers. There are also two Unclassified device types, Basic Management and Ping Only, and also Full Management.

Unclassified device types have two distinct roles:

- Basic Management and Ping-only, is used for those devices Entuity has taken under management at the Basic Management and Ping-only level.
- Full Management, is used for those devices Entuity has taken under management at the Full level but for which there is no vendor file information but Entuity can generate a suitable generic device type. These are uncertified devices.

#### Domains

Domains and domain filters are terms used within Component Viewer, in fact supplied domains are now only used within Component Viewer to group objects in its Explorer tree, e.g. the routers domain. In the web UI, where you manage views In Entuity, domain filters are referred to by the more apt term view content filters as they determine the type of object that can potentially appear in a view.

## **DHCP** Operation

The IP SLA DHCP operation measures the round trip time (RTT) taken to discover a DHCP Server and obtaining a lease from it. After obtaining an IP Address, Cisco IOS IP SLA releases the IP address that was leased by the server.

The Dynamic Host Configuration Protocol (DHCP) is an Internet protocol for automating the configuration of computers that use TCP/IP. DHCP can be used to automatically assign IP addresses, to deliver TCP/IP stack configuration parameters such as the subnet mask and default router.

## **Drop Box**

Drop box acts as a temporary repository for objects, for example gauges, charts, links, device metrics, that you want to include to new reports, dashboards.

#### **Duplex**

A full-duplex link with one telegrapher at each end, transmitting alternately in each direction.

## **Dynamic Thresholds**

Dynamic thresholds enable Entuity to alert the user to deviations from what Entuity's previous polling has established as normal behavior for that hour on that day. Entuity establishes normal behavior for a given attribute on a given port by maintaining the last four weeks worth of polled data, and applying an averaging algorithm.

## EIR

The Excess Information Rate (EIR) is the sustainable rate of information in excess of CIR, that the network will deliver if there is available bandwidth. The total information rate is CIR + EIR.

Frame Relay allows data rates in excess of the CIR to be successfully used on occasions. It is also possible that the amount of data that can be transferred per measurement interval (Tc) may be limited to less than the burst (or access rate) of the physical connection to the carrier network.

EIR defines how many bits per second beyond the CIR the data rate may be exceeded. This is may be policed by the carrier ingress switch per Tc on a pro-rata basis. This means that although data can be transmitted for periods of time at the burst rate of the physical port it would not be possible to continue transferring data at this rate successfully on a continuous basis if the CIR+EIR were to be less than the burst rate.

## Entuity

Entuity is both the name of the network management software and the company producing it. Entuity software is designed for networks of any size and complexity, from the smallest, simplest corporate infrastructure to the largest multinational. Every customer can access the full functionality of our cornerstone solution, incorporating fault, performance and inventory management.

#### entuity\_home

*entuity\_home* is used within the Entuity documentation to indicate the Entuity server's root folder. The root folder is set by Entuity install, in Windows environments the default is C:\Entuity. You can view its current setting through *destination* in *entuity\_home*\etc\entuity.cfg. Within Entuity configuration files it is represented by the variable *ENTUITY\_HOME*.

## Ethernet

IEEE standard network protocol that specifies how data is placed on and retrieved from a common transmission medium. Forms the underlying transport vehicle used by several upper-level protocols, including TCP/IP and XNS.

## Events

Events are alerts and alarms that are generated through Entuity monitoring the network. Event Viewer displays events and they can also be reported on.

## Expect

Expect is a Unix automation and testing tool, written by Don Libes as an extension to the Tcl scripting language, for interactive applications such as telnet, ftp, passwd, fsck, rlogin, tip, ssh, and others. It uses Unix pseudo terminals to wrap up subprocesses transparently, allowing the automation of arbitrary applications that are accessed over a terminal. With Tk, interactive applications can be wrapped in X11 GUIs.

## Eye of the Storm® (EYE)

Until Entuity 12.5 the software was known as Eye of the Storm (EYE).

## Entuity Remedy AR System Integration

The Entuity Remedy AR System integration allows forwarding of event and managed object information from Entuity to one or more AR System servers.

Entuity allows two types of forwarding:

- automatic generation of Action Requests (ARs), derived from Entuity events, to particular application forms on target AR System servers
- interactive generation of Action Requests (ARs), initiated from Entuity. The specified application forms on target AR System servers are opened for editing, with default data populated from the current Entuity managed object(s) or event(s).

Entuity can also pass to AR System a URL identifying the managed object that is the source of the AR. From AR System you can open Entuity's Component Viewer with the focus on the managed object.

## **Factory Default**

The shipped values of event thresholds are the factory defaults. You can amend a factory default, which if done at the root level effectively changes the default value for all objects against which that threshold can be set. For example, if you amend a threshold setting for a device event at the Entuity (system) level, all devices on that server will have a new default value.

## FEC

Forwarding Equivalence Class (FEC) is central concept to MPLS. An FEC is a set of packets that a single router forwards to the same next hop, using the same interface and with the same handling (e.g. queuing). The FEC is determined only once, at the ingress to an LSP, rather than at every router hop along the path.

## FECN (Forward Explicit Congestion Notification)

FECN is a bit in the header of a frame relay frame that is set to indicate to the destination node that congestion is occurring on the network. WAN News combines BECN and FECN values to determine congestion on a data path.

#### Filters

Filters in Entuity act by filtering in those objects specified in the filter. There are three types of filters, view, event and Flex Report.

Entuity uses these types of filter:

- View content filters are applied to the views, restricting the components available from a view to those that meet the criteria.
- Event Filters restrict the events available through a view.
- Flex Report filters restrict the data included to the report.

#### **Flow Collector**

The Flow Collector is the set of processes within an Entuity Integrated Flow Analyzer responsible for the receiving, processing and storage of flow records.

Administrators can enable/disable an Entuity server's Flow Collector through configure, a decision which should be made according to the role the administrator wants the server to perform in the management of the network.

## Frame Relay

A fast packet protocol that relies on physical component and higher level software reliability. The network discards any frame with bit errors. Frame relay services include PVCs (Permanent Virtual Circuit) and SVCs (Switched Virtual Circuit).

## **Full Duplex**

A full-duplex link with one telegrapher at each end, transmitting alternately in each direction.

## **Generic Device Type**

Entuity uses the concept of an underlying generic object against which are mapped the characteristics of different device types, e.g. routers, switch, firewalls, BladeCenters. This allows complete management of devices that have characteristics of one or more of the traditional types of devices, e.g. a router with switching capabilities.

## Half-Duplex

A type of communication channel using a single circuit which can carry data in either direction but not both directions at once.

#### Host Identifier

Your Entuity representative requires the host identifier of the Entuity server machine before they can generate your license. The host identifier associates the Entuity license with the physical footprint of the machine. Entuity install and configure programs both display the host identifier, alternatively you can run the command line program hostIdent (which is included with the software but is also available from the Support website).

#### Hot Standby Router Protocol (HSRP)

Hot Standby Router Protocol (HSRP) establishes a framework between network routers to achieve default gateway failover if the primary gateway becomes unavailable in close association with a rapid-converging routing protocol like EIGRP or OSPF. By multicasting packets, HSRP sends its hello messages to the multicast address 224.0.0.2 (all routers) using UDP port 1985, to other HSRP-enabled routers, defining priority between the routers. The primary router with the highest configured priority will act as a virtual router with its own IP and MAC address, which the hosts on the local segment will be configured to use as a gateway to the destination in question. If the primary router should fail, or the link to the destination drop, the router with the next-highest priority would take over communications through alternative routes within seconds, without major interruption to network connectivity.

HSRP and VRRP on some routers have the ability to trigger a failover if one or more interfaces on the router go down. This can be useful for dual branch routers each with a single serial link back to the head end. If the serial link of the primary router goes down, you would want the backup router to take over the primary functionality and thus retain connectivity to the head end.

#### Hypervisor

A hypervisor, also called virtual machine monitor (VMM), allows multiple operating systems to run concurrently on a host computer. The hypervisor presents to the guest operating systems a virtual operating platform and monitors the execution of the guest operating systems. Multiple instances of a variety of operating systems may share the virtualized hardware resources. Hypervisors are installed on server hardware whose only task is to run guest operating systems.

#### **Infrastructure Ports**

Entuity considers infrastructure ports, as:

Entuity considers infrastructure ports, as router ports, as uplinks which are ports connecting routers with switches and as trunk ports which are ports connecting switches together.

- Router ports.
- Uplinks, ports connecting routers with switches.
- Trunk ports, ports connecting switches together.

#### Interface

This is the entity on a node which is polled, such as a physical port. Nodes are likely to have more than one interface.

## IP

In TCP/IP, the standard for sending the basic unit of data, an IP datagram, through the Internet.

## **IP** Link

IP links may be autoDiscovered or created manually. They represents a link of some form at layer 3 or above e.g. a pair of IP addresses, an IP address and a URL.

#### **IP Peering**

IP Peering provides visibility into your WAN links, i.e. leased line, Frame Relay DLCIs, ATM VCCs, using subnet masking. It also reflects any manual IP pairings you may have made in Entuity.

#### ISO

International body that is responsible for establishing standards for communications and information exchange; developed the OSI reference model. ISO is not an acronym, but the Greek word for "equal."

#### Java Web Start

A technology for simplifying deployment of Java applications. It allows you to download and launch the Entuity client from your Web browser or shortcuts placed on your PC.

## **Key Metrics Gauge**

From Entuity's Explorer you can access the Device and Port Summary pages, both of which display Key Metric graphs. Key metrics vary according to the managed object, e.g. Device CPU utilization, Port Inbound Utilization%.

These graphs are of two forms a:

- green only gauge is used with metrics that do not have thresholds.
- green and red gauge is used with metrics that have thresholds. When the indicator is pointing to the red area then the threshold has been crossed. The relative size of the red and green areas of the gauge is fixed, i.e. the red area does not take a larger or smaller proportion of the total area of the gauge on changes to the threshold level.

You can view the current threshold value by passing the cursor over the data value below the graph.

You can click on each key metric gauge to view a larger graph.

#### LAP (Lightweight Wireless Access Point)

A low cost Wireless Access Point (WAP) that delegates much of the control functionality usually embodied within an Autonomous WAP to a WC. LAPs are usually connected to switched access layer ports and can coexist with ordinary wired connections to end user

hosts and servers on the same switch. The associations between the LAPs and WCs are negotiated dynamically and can change under fault conditions.

A LAP is an AP that is designed to be connected to a wireless LAN (WLAN) controller (WLC). The LAP provides dual band support for IEEE 802.11a, 802.11b, and 802.11g and simultaneous air monitoring for dynamic, real-time radio frequency (RF) management. In addition, Cisco Aironet 1000 Series LAPs handle time-sensitive functions, such as Layer 2 encryption, that enable Cisco WLANs to securely support voice, video, and data applications.

Entuity Wireless currently supports Cisco LAP, part of the Cisco Unified Wireless Network architecture.

#### Leased Line

A leased line is a dedicated point-to-point connection over a WAN via a router at the subscriber's premises to the telecommunications provider.

Entuity identifies a leased line, by default, when both of these conditions are true:

- The interface type is either IANAifType 22 (propPointToPointSerial) or 23 (PPP).
- The WAN port is not:
- A Frame Relay port.
- An ATM port.
- An ISDN port. These are identified as having an associated lower layer protocol port (found from the ifStack table) of ifType 81 (ds0). This indicates the port is a layer on top of either basic rate or primary rate ISDN.

#### Link Layer Discovery Protocol (LLDP)

The IEEE 802.1AB Link Layer Discovery Protocol (LLDP), provides a solution for the configuration issues caused by expanding LANs. It runs over the data link layer and specifically defines a standard method for Ethernet network devices to advertise information about themselves to other nodes on the network and store the information they discover. LLDP is available as a technology link type on the Entuity maps.

#### Load Balancers

Load balancers are devices that control and optimize traffic flow over your network. For example directing traffic away from over utilized servers to those less utilized, improving mission critical service delivery, providing fall over protection.

Entuity delivers a similar level of fault, performance and inventory management for load balancers as provided for other standard Entuity device types, e.g. routers, switches, hubs. For example device reports include load balancers, you can build your own reports using Flex Reports, device and port events apply and full load balancer details are viewable through Component Viewer.

Entuity currently manages F5 Labs Big IP 6400 Load Balancer. Entuity delivers additional polling of the device ports using F5 lab's propriety MIB, returning additional port identification, port status, port traffic and port utilization data. The full integration of this

additional data within Entuity allows administrators to set up utilization and traffic events against this data.

## Log Files

Entuity process messages are written to their individual log files, in *entuity\_home*/log. For example, applicationMonitor writes to applicationMonitor.log. When the log file becomes full, it automatically wraps to another file with up to four versions, e.g. applicationMonitor.log.1, applicationMonitor.log.2, applicationMonitor.log.3.

## **Management Level**

Every device under Entuity management is managed according to its management level, which is set when the device is added to Entuity but can be subsequently amended. Each managed device costs one license object.

These are the management levels:

- Full Management (all interfaces), Entuity manages all interfaces on the device.
- Full Management (management interfaces only), Entuity only manages the management interface.
- Full Management (no interfaces)
- Basic Management Entuity collects only basic system information and the full IP address table via SNMP. This management level is used when Entuity does not have the appropriate device support dataset (vendor file), cannot generate an appropriate dataset or you only want the device placed under basic management. Entuity does not manage any ports or modules on the device.
- Ping Only, devices only under ping management, SNMP data is not collected for these devices.

#### Managing Agent

Handles requests for information or action from the management station on a node. A protocol links the management station and the Managing Agent; for Entuity users this must be SNMP.

#### MIB (Management Information Base)

Entuity supports SNMP MIBs only. MIBs are present within nodes on a network, and comprise a logical collection of managed objects arranged in a tree structure. Managing agents on an element use MIBs to store information regarding the element, e.g. the speed at which packets of information are transferred.

All managed objects within a MIB share a common root.

## **Mobility Controller**

An SNMP manageable hardware device, manufactured by Aruba, that controls and coordinates the operation of a group of Aruba Wireless Access Points. In an Aruba wireless network deployment all wireless equipment discovery and real-time monitoring is performed via the Mobility Controllers rather than via SNMP/ping monitoring of the individual Access Points.

#### Multicast

Network communication between a single sender and multiple receivers.

#### My Network

Supplied view that contains the entire set of managed object's the user is permitted to view. Different users may have different devices in their My Network view, reflecting their different access permissions.

#### Node

An SNMP managed device attached to a network, from which data can be retrieved. For example, node devices such as hubs, routers, bridges, or network printers.

## OID

An Object Identifier is a sequence of integers that represent the position of an object in the hierarchical structure of objects in a MIB.

## OMF (Open Modeling Framework)

Flexible Entuity framework that allows the fast integration and management of new types of managed objects, e.g. new device types. For example, the BladeCenter device type is implemented through the OMF.

## **OSI Model**

A model for networks developed by International Standards Organization (ISO). The network is divided into seven layers, each layer building on the services provided below it.

## Packet

Any logical block of data sent over a network; it contains a header consisting of control information such as sender, receiver, and error-control data, as well as the message itself. May be fixed or variable length.

## PCR (Peak Cell Rate)

PCR is the maximum short term data throughput supported by an ATM port; the limit to which traffic can burst.

#### **Percentile Utilization**

Percentile Utilization indicates that for a defined percent of the time, e.g. 95, port utilization is below this value. It is useful for monitoring the sustained utilization of the port.

The 95th percentile is derived by ordering the utilization data by value, from highest to lowest. Application of a least square fit method removes spikes that would distort the analysis. The top 5% values are discarded, leaving the 95th percentile. This value is calculated for both inbound and outbound utilization.

## **Policy Group**

Entuity licensing is enabled by grouping related types of managed objects into groups. These Policy Groups are then assigned a license credit quota. Before Entuity manages an object it first checks whether the license allows its management and then whether a credit is required. When a license credit is required, Entuity checks that the policy group to which the object's type is associated has available credits. For example, before Entuity manages a device it checks the device licensing policy group for available credits.

#### Polling

Devices on the network are accessed by the system at regular, pre-defined, intervals in order to retrieve required data. This is referred to as polling the devices.

## **Polling Engine**

The Polling Engine (or Core Management Engine) is the set of processes within an Entuity server responsible for all general network management tasks excluding flow collection (e.g. network discovery, inventory, monitoring, event management).

Administrators can enable/disable an Entuity server's Polling Engine through configure, a decision which should be made according to the role the administrator wants the server to perform in the management of the network.

## Port

Entuity considers ports as interfaces on network devices, e.g. routers, and as endpoints in communications systems. In IP an upper-layer process that receives information from lower layers. Ports are numbered, and each numbered port is associated with a specific process. For example, SMTP is associated with port 25.

TCP and UDP transport layer protocols used on Ethernet use port numbers to distinguish between (demultiplex) different logical channels on the same network interface on the same computer.

#### Protocol

A set of formal rules detailing how to transmit data across a network. Example protocols include TCP, UDP and IP.

## **PVC (Permanent Virtual Circuit)**

PVC is a Frame Relay virtual connection providing the user with the equivalent of a physical connection to a destination address, using shared facilities. Virtual circuits can be permanent (PVC) or switched (SVC).

## Reachability

Availability Monitor sends an ICMP ping to the management IP address of managed devices, by default every two minutes. Devices that respond are considered reachable, those that do not respond, after the set number of retries, are considered unreachable. When Availability Monitor (applicationMonitor) is not running, then the reachability of the device is Unknown for that period, although Entuity maintains the last known state of the device.

#### Reboot

Entuity uses the device sysuptime to calculate when the device was last rebooted, or more accurately when the device last came up after being rebooted.

## **Reconciliation Rules**

Within BMC Atrium reconciliation rules are applied by the reconciliation engine to improve accuracy and efficiency of maintaining IT environment data in the CMDB. Reconciliation is used to identify and merge CI information and relationship form imported dataset with production dataset.

## Remedy Help Desk / Service Desk

Entuity Remedy AR System Integration for Remedy AR System 7.0 includes a sample configuration which integrates with the Remedy Service Desk application.

## **Remote Server**

A remote server is an Entuity server configured to trust another central Entuity server. A user logged into the central Entuity server is able to view information collected by the remote Entuity server(s), according to their user account access rights. A remote Entuity server responds to requests from a trusted central Entuity server, and freely shares information with it.

An Entuity server can be configured to perform both roles, be both a remote and central Entuity Server, allowing administrators to create both hub-n-spoke and fully meshed deployments.

Configuration of central and remote servers is through the Multi-Server Administration area of the Entuity web UI.

#### Router

A device that routes data between networks. Routers connect multiple LAN segments to each other or to a WAN.

Routers may be equipped to provide frame relay support to the LAN devices they serve. These routers can:

- encapsulate LAN frames in frame relay frames and send those frames to a frame relay switch for transmission across the WAN.
- receive frame relay frames from the WAN, strip the frame relay frame off each frame producing the original LAN frame, and forward it to the end device.

#### **Running-config**

The configuration controlling the current operation of a piece of Cisco hardware. This may be different to the start-up config if changes have been made since start-up and the changes have not been saved. The running-config can be saved as the startup-config replacing any previous start-up config. The running config is held in DRAM. If the machine is restarted without the running-config being saved, all changes are lost.

#### Sample Interval

In Entuity the period between two data samples. This may be between two pollings of a port, or between two rolled up data samples.

## SCR (Sustainable Cell Rate)

SCR is the long term data throughput of an ATM port. Traffic can burst above this limit up to the PCR.

#### Server

Any computer whose function in a network is to provide user access to files, printing, communications, and other services. Servers usually have more memory, more disk storage, and a more advanced processor than a single-user desktop PC.

Where Entuity manages an application, Entuity can manage the application server as a device.

#### Services

Services is a method of grouping together collections of ports that provide a service and associating with them other ports which use that service. For example, a service maybe email, with one port designated as the provider of the service and all others in the group defined as consumers.

## SLA

A Service Level Agreement (SLA) is a set of rules and metrics which can be used to measure the efficiency and performance of an object. That object may be a department, a server, a

network or any other functional component of an organization. If an object adheres to its associated set of rules and metrics, then it can be said to be conforming to its SLA. Similarly, if the object breaches the set of rules and metrics, then this means that it is no longer conforming to its SLA.

#### SNMP

Standardized method of managing and monitoring network devices on TCP/IP based internets. SNMP defines the formats of a set of network management messages, and the rules by which those messages are exchanged. The network management messages are used to make requests for performing network management functions and to report on events that occur in the network. Also, SNMP defines the allowable data types for MIBs, they way in which MIBs can be structured, and a set of standard objects that can be used in implementing a MIB.

#### **Spanning Tree**

Spanning tree provides a vendor neutral technology for visibility into your network. When correctly implemented Entuity discovers bridge links, switch to switch relationships, through polling the Bridge MIB. Complete spanning tree connectivity relies on a contiguous set of Entuity managed devices.

#### **Spare Ports**

By default Entuity spare port calculations include ports that have been unused for forty days or more, include ports that have system uptime of less than forty days and are currently unused and exclude ports that have been unused for less than forty days but have a system uptime of forty days or more.

By default Entuity spare port calculations:

- Include ports that have been unused for forty days or more.
- Include ports that have system uptime of less than forty days and are currently unused.
- Exclude ports that have been unused for less than forty days but have a system uptime of forty days or more.

The forty day threshold is configurable through the reporting section of entuity.cfg. Entuity distinguishes between physical and virtual ports using interface type. If required System Administrators can amend the virtual port identifier.

#### **SNMP** Agent

Management code that resides in the device, controls the operation of the device, and responds to SNMP requests.

#### SSL

An SSL Certificate consists of a public key and a private key. The public key is used to encrypt information and the private key is used to decipher it. When a browser points to a



secured domain, an SSL handshake authenticates the server and the client and establishes an encryption method and a unique session key. They can begin a secure session that guarantees message privacy and message integrity.

#### Startup-config

The initial configuration when a piece of Cisco hardware starts-up. If there have been no changes to the configuration since start-up, this will be the same as the running-config. The startup-config is also referred to as the saved config. The startup-config is held in NVRAM.

#### Static Thresholds

Static threshold settings allow you to configure the trigger points which when crossed cause Entuity to raise events. You can set thresholds against an individual event, a managed object, view or all objects on an Entuity server.

#### StormWorks

Entuity Configurable Framework is the internal Entuity engine, also known as the Data Management Kernel (DMK). It runs as the **DsKernelStatic** process.Entuity Configurable Framework enables the delivery of functionality through a highly configurable set of core services. The configuration files, found in *entuity\_home*\etc, prefixed with **sw**\_ define and configure Entuity Configurable Framework services.

Entuity assigns all of the objects it manages their own Entuity Configurable Framework identifier. Entuity Configurable Framework identifiers are sequentially assigned, do not consider the object type and are unique within each Entuity server. *StormWorks ID* is visible from the object's web UI Advanced tab, and is used in creating dashboards to the user, for example during Data Export, Map Export, running of Flex Reports.

#### **Stream Attributes**

Information Entuity collects from your network is stored within Entuity as an attribute of the managed object, for example a port's name, a port's utilization are stored as attributes. Stream attributes are to maintain a history of a metric, for example Entuity maintains a history of port utilization.

#### SVG

Scalable Vector Graphics (SVG) is a graphics file format and Web development language based on XML. SVG is used by Entuity's reports to dynamically generate, high-quality graphics from real-time data.

#### Switch

A switch is a network device that selects a path or circuit for sending a unit of data to its next destination. It is usually simpler and faster than a router, which requires knowledge about the network to determine the route.

A switch may also include the function of the router, a device or program that can determine the route and specifically what adjacent network point the data should be sent to.

#### SynOptics Network Management Protocol (SONMP)

SONMP is also known as the Nortel Discovery Protocol (NDP), a Data Link Layer network protocol for discovery of Nortel (Avaya and Ciena) devices. It is available as a technology link type for the Entuity maps.

#### System Capabilities

Entuity determines the switching capability of a device by checking the group dot1dtp, specifically the mandatory scalar value dot1dTpLearnedEntryDiscards. dot1dtp is only present when the device supports transparent bridging, which implies it has Ethernet switching capability.

Entuity determines the routing capability of a device by checking for the ip-forwarding variable from the ip group in the MIB of the device. When ip-forwarding has a value of 1, this implies the device is acting as a gateway and so has routing capability.

Entuity determines whether the device type is hub by comparing its type to device types detailed in the vendor files.

#### TCP

Connection-oriented protocol that provides a reliable byte stream over IP. A reliable connection means that each end of the session is guaranteed to receive all of the data transmitted by the other end of the connection, in the same order that it was originally transmitted without receiving duplicates.

#### TCP/IP

Combination of TCP and IP protocols common to many different computer systems and so often used for communication between them.

#### TFTP

Trivial File Transfer Protocol (TFTP) is a very simple file transfer protocol, with the functionality of a very basic form of FTP. It uses UDP as its transport protocol and has no authentication or encryption mechanisms.

#### Ticker

Ticker allows you to view real time output at the device and port level, viewing data changes as they occur. You can select to view data activity for one or more client devices or ports. For monitored:

- Ports you can select from a list of MIB variables the particular variable(s) you want to use to monitor the port. Entuity is supplied with a default number of MIB variables for use with ports and you can also add your own MIB variables to this list.
- Devices you can create your own list of MIB variables on which to monitor the device.

#### traceroute

Entuity includes two types of traceroute functionality, identified in the Entuity client as TraceRoute from Client and TraceRoute from Server.

TraceRoute from Entuity Client, calls the traceroute utility installed on the Entuity client machine and performs a live traceroute from the Entuity client to the target IP address.

TraceRoute from Entuity Server, uses data collected by applicationMonitor. This traceroute information is updated every two minutes, so calling TraceRoute from Server does not initiate a live traceroute but instead interrogates the data returned from the last applicationMonitor traceroute.

applicationMonitor uses Entuity's own implementation of traceroute functionality. This implementation performs ICMP pings in a similar way to a standard traceroute but with this key difference. When performing a traceroute applicationMonitor increments TTL values by one, until the pings reach the edge of an invisible cloud. At this point applicationMonitor increase the TTL value to 32. When this results in the ping reaching its target, the response from the target includes the actual number of hops required to reach target.

#### Traps

Traps can be used by network components to signal abnormal conditions. Entuity can both receive and forward SNMP traps.

Entuity can be configured to:

- Generate events in Event Viewer then traps are received.
- Forward traps to up to six concurrent recipients.



Entuity also supply a more advanced SNMP trap forwarding integration module. Contact your Entuity sales representative for details.

#### **Trivial Change**

A difference between a current-configuration file and a previously archived one that is not considered important by the system because it matches a set of rules codified as patterns in an "ignore file". Trivial changes may include comments such as timestamps in a configuration file.

#### Root Cause Analysis (RCA)

RCA isolates IT related problems using vector differencing. This involves the building of a dependency chain of objects and monitoring the object states in that chain. In the event of

state changes (where each object state change is a vector), differencing the dependency chain state vectors enables Entuity to determine the true cause of the event. Entuity can then raise the appropriate event.

For example, if an application becomes unavailable because a switch has failed then Entuity raises an event relating to the switch failure in Event Viewer. Entuity does not raise events for the application being unavailable as changes in state in the dependency chain are attributed to the switch failure.

#### **Trunk Ports**

Trunk ports, i.e. ports connecting switches together.

Entuity identifies a trunk port by:

- reading the MIB.
- macman identifying the switch port as having more than ten MAC addresses and also having associated VLANs.
- using CDP Trunk Port Discovery, a CISCO proprietary method.

When one or more of these methods identifies a trunk port, Entuity also considers it as a trunk port.

#### **Unclassified Devices**

Entuity managed devices for which Entuity does not have a device support dataset, provided through individual vendor, bin.vendor or newbin.vendor files, are included to Entuity as Unclassified devices under Full Management, or Unclassified devices under Ping-only and Basic Management.

Unclassified generically managed devices use an Uncertified device type, created by Entuity and held in newbin.vendor. These are Entuity managed devices and do incur a license charge. System Administrators should contact their Entuity support representative for a vendor file which would ensure Entuity fully manages these devices.

#### Unicast

Unicast is network communication between a single sender and a single receiver.

## **Uplink Detection**

Entuity considers an uplink as trunking on a connection to a router or layer 3 switch, which is visible through spanning tree. This technology attempts to link layer 3 with layer 2.

Where links between switches and routers are not done using VLAN trunking and spanning tree then the spanning tree technology will not detect them. This is typically at smaller satellite offices, which do not need the greater port density and much greater speed available from router on a stick and even greater speed available from layer 3 switching.

## Uplinks

Ports connecting routers with switches.

#### Uptime

By default Entuity polls devices every five minutes, retrieving device *sysuptime*. Entuity checks as to whether the device has been continually up since the last poll, and modifies the device's uptime value accordingly.

When *sysuptime* indicates the device has been down during the polling interval but is now up, from *sysuptime* alone Entuity cannot identify for how long the device was down. Entuity takes this unknown time, and adds fifty percent of it to the known uptime value, with the remaining fifty percent considered UNKNOWN. For example where *sysuptime* has a value of two minutes. Entuity cannot determine the state of the device over the first three minutes of the polling interval. Entuity adds ninety seconds to the *sysuptime* value, giving an uptime value of two hundred and ten seconds and records the device state as UNKNOWN for ninety seconds.

Device uptime is visible through Component Viewer, and is used in many reports, e.g. Routing Summary, Switching Summary.

## Utilization

In Entuity port utilization is expressed as a percentage of actual traffic volume against the maximum volume that can be handled by the port.

## UUID (Universally Unique ID)

A 16 byte value written to a system's planar at manufacturing time to uniquely identify a system across time and space.

## Variable Binding

A variable binding, or VarBind, refers to the pairing of the name of a MIB variable to the variable's value. A VarBindList is a simple list of variable names and corresponding values. Some PDUs are concerned only with the name of a variable and not its value (e.g., the GetRequest-PDU). In this case, the value portion of the binding is ignored by the protocol entity. However, the value portion must still have valid ASN.1 syntax and encoding. It is recommended that the ASN.1 value NULL be used for the value portion of such bindings.

## VCC (Virtual Channel Connection)

A VCC is an association established at the ATM Layer between two or more endpoints for the purpose of user-user, user-network, or network-network information transfer. The points at which the ATM cell payload is passed to the AAL for processing signify the endpoints of a VCC. Virtual Circuit is a more generic, non-ATM specific term.

## VCI (Virtual Channel Identifier)

VPI and VCI together identify a virtual channel link on an ATM interface.

#### **Vendor Files**

Entuity identifies the device type of discovered devices by matching their sysoid to that held against the device support datasets. Device support dataset definitions are held in, listed here in order of precedence, individual vendor files, bin.vendor file, newbin.vendor file, and then uncertified file.

**vendinfo** identifies the vendor information available to Entuity and the decisions made when more than one vendor file is available for a particular sysoid; which vendor device definition Entuity uses to manage that device type.

File Type	Description
individual vendor files	When Entuity does not currently manage a device that you require it to, you can request your Entuity support representative for an appropriate vendor file. Those non-standard definitions are listed in entuity_home/etc/ exotica. Only when a vendor file is moved to entuity_home/etc does Entuity use that definition.
bin.vendor file	File includes the default vendor file definition
newbin.vendor file	File includes device type definitions generated by earlier versions of Entuity.
uncertified file	File includes device type definitions created by Entuity, using proliferate with the -g parameter. Devices of this type are considered as Unclassified Devices.

#### View

All network objects within Entuity are displayed through views. View filters allow you to restrict the displayed objects in the view to the ones you are interested in. You can also use user profiles to control access to different views.

## Virtual Channel Links (VCLs)

A VCC consists of the concatenated VCLs. A VCL is a means of unidirectional transport of ATM cells between the points where a VCI value is assigned and the point where the value is translated or removed. The VPI and VCI within the ATM cell header associates each cell with a particular VCL over a given physical link.

#### Virtual Circuit

A Virtual Circuit is a generic term for an association established between two or more endpoints for the purpose of user-user, user-network, or network-network information transfer. An example would be ATM's VCC.

#### Virtual Port

Entuity distinguishes between physical and virtual ports using interface type. If required System Administrators can amend the virtual port identifier.

#### VLAN

A logical association that allows users to communicate as if they were physically connected to a single LAN, independent of the actual physical configuration of the network.

## **VM Platforms**

Entuity currently manages Oracle and VMware VMs through its VM Platform device type. Entuity communicates with VMs and their hypervisors through the VM's SDK. This requires specification of different connection attributes when compared to devices of other types. It also requires that all VMs are added to Entuity with a **Ping Only** management level, as this allows the selection of the VM Platform type and its connection configuration. When adding VMs using autoDiscovery care must be taken to ensure candidate device VMs are always added as **Ping Only**.

## VPD (Vital Product Data)

VPD is information about a device that is stored on a computer's hard disk (or the device itself) that allows the device to be administered at a system or network level. Typical VPD information includes a product model number, a unique serial number, product release level, maintenance level, and other information specific to the device type. Vital product data can also include user-defined information, such as the building and department location of the device. The collection and use of vital product data allows the status of a network or computer system to be understood and service provided more quickly.

## VPI (Virtual Path Identifier)

VPI identifies a virtual path leg on an ATM interface.

## VRF (Virtual Routing and Forwarding)

VRF allows multiple instances of a routing table to co-exist within the same router at the same time. Because the routing instances are independent, the same or overlapping IP addresses can be used without conflicting with each other.

## VTP (VLAN Trunk Protocol) Domain

A VTP domain consists of one or more connected switches that share the same VTP domain name. A switch can be configured to be in one and only one VTP domain. The vtpDomainTool generates a view that groups devices and VLANS by this VTP domain name.

## Wireless Controller (WC)

A network attached device that coordinates traffic to and from Lightweight Wireless Access Points (LAPs). It provides centralized control over the configuration and dynamic behavior of potentially many LAPs.

# Index

# Α

Access Control web server 94 Access Groups 127 Access Lists definition 126 packet classification 127 Access Points 168 Alias 15 Amazon Web Services (AWS) access keyname 45 details 44 VM platforms 39 Application details 54 **Application Server** details 55 **Application Status** access control 94 URL alerts 95 applicationMonitor log files 181 reachability 184 traceroute 189 Applications viewing 53 AR System 168 ARs 168 Attached Applications 53 autoDiscovery proliferate 195 Availability Monitor see also Application Availability see also WAN Availability AvailMonitor High Latency Reaching Application 54 AWAP 162

#### В

BGP overview 140 peer state 141 Remote AS 141 BladeCenter Blades inventory 37 rail voltages 38 state 37 temperature 37 BladeCenter Blowers 31 BladeCenter Chassis rail voltages 36 temperature management 37 BladeCenter Management Module 31 BladeCenter Media Tray polling 36 BladeCenter Power Supplies 31 BladeCenter Switch Bays 31 BladeCenters gateway IP address 32 subnet mask 32 BMC Remedy Action Request System (AR System) 168 **Business Views** see Views

## С

CCM Group 61 CDP neighbor discovery 17 trunk port discovery 170 CIO Perspective Component Availability Report 15 Cisco Nexus 1000v 5 Cisco Unified Computing System (UCS) 74 device support 75 licensing 76, 77 Manager 76 Class Maps associated access groups 129 definition 126

status 129 Community String setting for firewalls 89 Component Availability Report 15

Configuration Management transfer server override 3

Congestion Avoidance WRED 133

CUCM Groups 60

CUCMs data retention 59 event thresholds 71

# D

Descriptive Alias 15 dev.txt see Device File Device Management Level 181 **Device Sensor Warning Value** thresholds 86 Device Status 60, 62, 63, 66, 68, 69, 72 Device Support Datasets 173, 181 Device Types 174 device support datasets 173 Devices locating 3 types 3 uptime 6, 149 Discards rollups 24 DMK 172 DsKernelStatic 187 Dynamic Application Profiling 94

# E

EIGRP local interface details 142 overview 142 peer state 142 Enterprise Ports 29 Entuity BladeCenter 31 Entuity CUCM troubleshooting 71 Entuity Remedy AR System 176 entuity\_home 175 Events resource thresholds 71 External Authentication see also User Authentication

# F

F5 Labs Big IP 6400 Load Balancer 27, 180 Faults rollups 24 Firewall Servers community string 89 packages 90 SNMP UDP port 89 total memory 89

## G

Gateway IP Address 32 Generically Managed Devices 190, 192

## Н

Hello Suppression 144 Hosted Applications 53 HSRP 26

# 

inSight Center see also Green IT Perspective IP Addresses ports 152 web server 94 IP Precedence setting 135

IPSO SNMP port 89

# Κ

Key Metrics gauge 179

# L

Latency Threshold applications 54 Layer 2 uplink detection 190 Layer 3 core ports 172 IP Links 179 uplink detection 190 Link Layer Discovery Protocol 180 Load Average 149 Load Balancer device support 27, 180 port details 27 port traffic 28 port utilization 28 Load Balancers current sessions 97 local pools 103 real servers 104 session statistics 100 virtual servers 106 virtual services 105

#### Μ

MAC Addresses 25 history 25 Managed Hosts 56 match evaluation statement 129 Match Statements definition 126 Matrix Switch enterprise ports 29 Mobility Controllers 156 Monitored Servers ip address 94 name 94 operational status 94

# Ν

Not Classified Devices 190

## 0

Operation Status web server 94 OSPF overview 143 priority 144 status 144

#### Ρ

Packet Dropping **WRED 133** Packet Marking overview 135 Packet Rate 24 **PoE Midspan Injectors** manufacturer details 123 overview 122 port status 124 power configuration 124 status 123 Policy Maps associated class maps 130 definition 126 Ports alias 15 Details 13 interface speed 15, 20, 23, 152 IP Address 152 spare port status 16 VLANs 17 **Power Configuration** PoE Midspan Injectors 124 proliferate see also autoDiscovery

## Q

QoS components 126 simple example 126

QoS Groups packet marking 135 Queue Management 132

## R

r\_matrix 29 Remedy Help Desk 184 Remote CUCMs 73 Resources load balancers 98 Rollup trend data 172 Routing CTI Devices 59

# S

Security see also User Authentication Service Desk application 184 Service Policies 130 definition 126 SNMP Port setting for IPSO agent 89 Spanning Tree Network see STP Spare Status 16 SSL 186 SSL Proxy Servers 148 StormWorks 187 Switched Network Early Warning System see SNFWS Switches matrix 29 System Capabilities 188

# Т

Tail Drops avoiding 132 Temperature Sensor events 86 traceroute 189 TraceRoute from Client 189 TraceRoute from Server 189 Traffic Policing definition 130 performance 131 Traffic Shaping overview 138 status 139 Traps see also SNMP Troubleshooting CUCM performance 71 Trunk Ports CDP discovery 170

# U

Uncertified Device 174 Unclassified Device Types 174 Universal Unique Identifier Virtual Machine 40, 42, 43, 45 Uptime device 6, 149 URL Alerts application status 95 User Actions see also Extensible Menus User Authentication

## V

Vendor Files 192 Virtual Machines hypervisor 178 operating system 40, 45 Universal Unique Identifier 40, 42, 43, 45 VLANs ports 17

#### W

Wireless Access Points 168

WRED congestion avoidance 133

# Χ

XML API Data Collection credential set 5