

## PowerConnect™ 34xx Feature Overview

Feature	Details / Defaults	Administrator Controls
<b>Total Switching Capacity</b>	12.6 Gbps (PowerConnect™ 3424) 17.6 Gbps (PowerConnect™ 3448)	none
<b>Maximum Forwarding Rate</b>	9.52 Mpps	none
<b>Port configuration</b>	Ports are configurable	User can set: <ul style="list-style-type: none"> <li>• Administrative state (enable/disable)</li> <li>• Port speed</li> <li>• Duplex setting</li>   <li>• Flow control</li> </ul>
<b>Auto-negotiation</b>	Enabled for speed and duplex modes. Auto-negotiation of flow control is disabled by default. Auto-negotiation advertisement supported.	User can set auto-negotiation on and set advertisement parameters.
<b>Flow Control, Head of Line Blocking</b>	When flow control is turned on, HOL blocking may be turned off, and vice versa. By default, flow control is disabled. Head of Line Blocking is supported within the same bank of ports.	User can enable / disable flow control
<b>Auto MDI/MDIX</b>	Enabled by default	None
<b>Back Pressure</b>	Enabled by default	User can enable/disable back pressure
<b>Virtual Cable Testing</b>	VCT detects and reports potential cabling issues. Cable analysis can be done when the link is down. Cable length can be measured when the link is operational. Cable length measurements may not work accurately on 10mbps links.	Initiate a cable test operation.
<b>Optical Diagnostics</b>	Finisar optical transceivers provide access to a set of parameters that can be monitored and displayed by the system administrator.	Monitor and display Finisar optical transceiver diagnostics.
<b>Environmental Monitoring</b>	If sensors are provided as part of the hardware design, monitoring of power supply and fans is supported.	The user can view power supply and fan status.
<b>Port counters</b>	The user can view the following statistics:	The user can clear the statistics.

	<ul style="list-style-type: none"> <li>• Inbound Octet Rate</li> <li>• Inbound Unicast Packet Rate</li> <li>• Inbound Non-unicast Packet Rate</li> <li>• Inbound Discard Rate</li> <li>• Inbound Error Rate</li> <li>• Outbound Octet Rate</li> <li>• Outbound Unicast Packet Rate</li> </ul> <p>4-group RMON is supported.</p>	
<b>Spanning Tree</b>	<p>Per device spanning tree (802.1d) Fast Link supported Default settings are per standard. Rapid Spanning Tree. (802.1w) Support for BPDU filtering when STP is disabled.</p>	<p>The user can enable / disable STP. The user can set: Hello Time, Max Age, Forward Delay, Bridge Priority. The user can specify per port priority, cost and fast link parameters.</p>
<b>Multiple Spanning Tree</b>	<p>Multiple Spanning Tree (802.1s) Support of up to 16 instances.</p> <p>Limitations:</p> <ul style="list-style-type: none"> <li>• Ingress filtering is always on.</li> <li>• When transitioning from blocking to forwarding state, learning is not supported.</li> <li>• PVLAN and MSTP cannot both be enabled on the same port.</li> </ul>	<p>The user can create domains, instances and map VLANs to instances The parameters for RSTP can be configured for each instance.</p>
<b>Port Security</b>	<p>Support for learning MAC addresses and then disabling learning to effectively lock the MAC addresses that have access to the network</p> <p>MAC-based port security by number of MACs is supported. A user-configured number of MAC addresses can be learned on a given port, after which no more can be learned, using controlled learning and MAC address shadowing.</p>	<p>Packets received on a locked port, whose source address was not found or previously learned on a different port, are treated in one of the following ways, which can be configured per port:</p> <ul style="list-style-type: none"> <li>• Forward (Frame is forwarded, but its address is not learned)</li> <li>• Discard</li> <li>• Port shutdown</li> </ul>
<b>VLANs</b>	<p>Up to 256 802.1q VLANs, out of full range of 4,096. GVRP is supported</p>	<p>User can assign ports to participate in VLAN. User can assign VLAN as 802.1q or port-based. Using 802.1q-based VLANs, user can set port as tagged or untagged.</p>
<b>Private VLANs</b>	<p>Three types of Private VLAN ports can be defined:</p> <ul style="list-style-type: none"> <li>• promiscuous - communicates with all interfaces</li> </ul>	<p>VLAN can be defined as a private VLAN, in a given mode (promiscuous, isolated, community) An interface can be configured as</p>

	<ul style="list-style-type: none"> <li>Isolated - completely separated from other ports within the same Private VLAN, but not from promiscuous ports</li> <li>Community - communicate among themselves and with promiscuous ports, but not with ports in other communities or with isolated ports.</li> <li>PVLAN will not work with priority-tagged packets.</li> </ul>	a private VLAN mode.
<b>MAC-based VLAN</b>	The user can define VLANs based upon the MAC address. A port joins a VLAN after the first MAC is learned	The user can assign a port to a VLAN, based on the source MAC address of the device connected to the port.
<b>Broadcast Control</b>	<p>The threshold for the number of broadcast packets that are sent over a port can be set, to prevent broadcast storms. Storm control can be enabled per port, and limitation can be based on:</p> <ul style="list-style-type: none"> <li>Unknown unicast, multicast broadcast</li> <li>Multicast &amp; broadcast</li> <li>Broadcast only</li> </ul>	User can define the threshold per port, or apply to all ports.
<b>MAC Access Control Lists</b>	Up to 128 MAC Access Control Lists are supported as MAC filtering. The ACL is attached to a VLAN.	User can configure ACLs to filter out specific MAC destination addresses. The rule action could be drop/drop and disable. Forward is the default action.
<b>Class of Service (IEEE 802.1p)</b>	Traffic prioritization.	Port can be prioritized per 4 queues DSCP tags (up to 64) can be used.
<b>MAC Multicast Support</b>	Up to 256 multicast groups	User can define static multicast groups
<b>IGMP Snooping</b>	IGMP snooping can be enabled globally. Up to 128 multicast groups can be learned, on any defined VLAN.	User can enable / disable IGMP snooping
<b>Link Aggregation (LAGs)</b>	Up to 8 ports in up to 8 LAGs. LAG is not supported on stacking ports. LACP is supported.	User can assign a port to be a member of a LAG and can configure it as a whole with port parameters
<b>Port Mirroring</b>	Port mirroring can be enabled on a many-to-one basis.	User can enable / disable port mirroring. User defines a single target port and mirrored ports
<b>IP Addressing</b>	Static and dynamic (DHCP/BootP)	User can select IP address management method (Static / BootP / DHCP) User can define static IP address, subnet mask and gateway Default assignment of an IP address is supported

<b>Telnet access</b>	Up to five sessions	Security paramaters can be configured
<b>Web access</b>	Multi-session	Security paramaters can be configured
<b>Management security</b>	Management Access Control Lists. User-name and Password protection.	User can configure Management ACLs. User can configure username and password.
<b>RADIUS</b>	Management security using a RADIUS server.	Server parameters can be configured.
<b>TACACS+</b>	Management security using a TACACS+ server.	Server parameters can be configured.
<b>802.1x Port Authentication</b>	Using external RADIUS server as authenticator. Support of Guest VLAN. Support of unauthenticated VLAN and single/multiple host.	User can define external RADIUS server. User defines shared secret authentication
<b>SNMPv1, SNMPv2, SNMPv3</b>	Per RFC 1517 Up to eight community strings can be defined, with combinations of GET, SET and TRAP. Hosts can be defined with these access rights. Default GET community string for the switch is 'public', and the host table is empty	User can define community strings. User can enable / disable traps globally SNMPv3 - users, groups and views can be defined.
<b>MIB support</b>	Support of MIBs for supported feature. Support of Enterprise MIB	None
<b>RFC 1493 / RFC 2674</b>	The Bridge MIB RFCs are interoperable.	None
<b>Configuration files</b>	Support of running, startup and backup configuration files	User can manipulate configuration files. Display of empty configuration file Upload and download of configuration files. File system management.
<b>Image file and firmware upgrade</b>	Firmware can be uploaded from a TFTP server. Two image files are supported. Firmware is can be copied from stack master to all other units.	Upload and download of configuration files.
<b>CPU Utilization Monitoring</b>	CPU Utilization Monitoring	none
<b>SNTP</b>	External clock server support.	Can configure server polling & authentication
<b>Telnet Client</b>	Allows for telnet from the switch to a remote host	none
<b>DNS Client</b>	Allows for name resolution via remote DNS servers	DNS servers can be configured
<b>Layer 3 Traceroute</b>	Allows for multi-hop ICMP requests	none
<b>MRTG Interoperability</b>	The Multi Router Traffic Grapher (MRTG) is a tool to monitor the traffic load on network links. MRTG generates HTML pages containing PNG	none

	<p>images which provide a LIVE visual representation of this traffic (<a href="http://www.stat.ee.ethz.ch/mrtg/">http://www.stat.ee.ethz.ch/mrtg/</a>) MRTG interoperability is supported on the device</p>	
<b>Management methods</b>	<p>Access to web interface  Secure Web (HTTPS)  Telnet access to Command Line Interface (described in CLI specification).  Secure Shell (CLI over SSH access)  SNMP Interface.  Privilege levels</p>	<p>CLI copy/paste text supported.  Set-up wizard will supported</p>
<b>Power over Ethernet</b>	<p>Complies to the IEEE802.3af standard for poering remote network devices</p>	<p>Power alarms and thresholds</p>