# OpenWare™

# Introduction to Ethernet Switch Management with OpenWare

Ethernet Switches come in many different guises, and fulfill many different roles. But, apart from very simple plug-n-play devices, they all require some management software to configure and control them.

OpenWare™ is Abaco's switch management environment, available exclusively on our NETernity™ layer 2/3 Ethernet switches. (NETernity, by the way, is one product family in our extensive Ethernet switch selection, which is one of the best you will find anywhere.) OpenWare, on our NETernity switch product line, meets the needs of customers in all types of industries, whether it is commercial or military/aerospace.

OpenWare is GNU/Linux-based firmware, bringing together the best of Open Source and proprietary switch control, routing and protocol implementations. This provides the user with a switch that can be easily configured for any network requirement – from the trivially simple, through to the very complex. The flexible OpenWare environment allows for customization for specific customer requirements and the incorporation of the latest standards – for example, new RFCs (Request For Comments) from the IETF, new standards from the IEEE or new SNMP MIBs (Management Information Bases).

The OpenWare switch management environment provides integrated switch management services, including configuration, monitoring, switching control, addressing, routing and all supported protocols. These can be controlled via a range of interfaces – a CLI (Command Line Interface) either locally through a serial interface, or remotely, using the ubiquitous Telnet or the secure SSH. Alternatively, SNMP (Simple Network Management Protocol) is supported, for customers who require programmatic control. Recently, we have been expanding its simple web interface, allowing "point and click" type access to switch control. No matter which method you use to configure your switch, you can save the configuration so it comes up ready every time it is started.

Increasingly, the support of IPv6 addressing is important to customers in order to provide a future proof path from IPv4 to IPv6 - a Layer 3 OpenWare switch provides support for both IP addressing schemes. Networks are increasingly making use of multicast traffic, for example in IP surveillance systems. It is important that these multicast streams, which may include video, are only forwarded to devices which are registered to receive it. OpenWare provides support for IGMP Snooping, and for IPv6 networks, MLD Snooping. These provide a mechanism for the dynamic management of the multicast forwarding behavior of the switch.

Security is another area which has been increasing in importance to customers – an OpenWare switch provides methods to set up secure access to a network through switch ports, and provide indications and logs of potential security violations to the administrator.

Abaco is almost unique in the industry in developing our switch management software in-house, and we've been doing this for over 15 years. In addition to the OpenWare package, this also gives us particularly strong skills in assisting customers with network solutions. We are able to discuss in great detail all aspects of Ethernet network design and communication applications development.

So, next time you are considering which embedded Ethernet switch is best for your upcoming project, keep in mind the time and hassle you can save with a well-conceived and well-designed toolset like OpenWare.

## OpenWare feature highlights

The following is a list of features supported by OpenWare. Please note this is illustrative of what is provided, but is not exhaustive. There are many other features provided for specific cases, which we have omitted as they may not have general appeal.

### Works "out of the box"
OpenWare configures switches so that they will run on power up in a "plug and play" way. In other words, they will, by default, act as simple layer 2 switches. It is only as you need more complex configurations that you need to touch the management interface. Many customers power up the switch, and have traffic flowing through it for a long time before they even configure the IP address of the switch.

### User Access
OpenWare provides three levels of user at the Operator Console, providing a specified level of access to switch functionality. These are:

• Status-only user
  This user is able to get status information from the switch, but not able to change any configuration settings. Perfect for monitoring operations.

**abaco**
S Y S T E M S

# Introduction to Ethernet Switch Management with OpenWare

- Admin user
  This allows full access to the Operator Console menus – providing configuration control over all normal switch operations.
- Root user
  This allows access to the underlying Linux system, for cases where configuration of specific advanced operations is required, or tasks such as upgrade to the switch software.

Access to these users can be controlled by creation and management of passwords.

## User interfaces

Users can manage an OpenWare switch using a range of access methods:

- Serial console
  This is a physical serial port, which allows access to a terminal, typically a PC, running an ANSI terminal emulator (e.g. Hyperterminal).
- Out-Of-Band network port (OOB)
  This is an Ethernet port that is driven directly by the management processor, and typically sits on a separate network from the one in which the switch resides. Telnet , SSH and HTTP are supported on this interface.
- In-Band network ports
  The switch has an address on the network, so the switch can be managed across that network also. Once again, Telnet, SSH and HTTP are supported.

The interfaces provided to the user are:

- Command Line Interface (accessed via console, telnet, or SSH)
  This is a character-based interface, allowing use of a comprehensive menu-driven command structure, which provides the switch management control. It can also allow access to the Linux command prompt (to the appropriate user.)
- Web interface
  OpenWare provides an HTTP-based set of web pages, with a simple switch management interface that can be accessed from a web browser. This gives point and click control over most switch features.

## Switch protocol features

### Layer 2 Features

- Jumbo frames
  For use in Gigabit networks, frame sizes limited to the original Ethernet size of about 1500 bytes are not efficient. OpenWare allows for Jumbo Frames (typically up to 9K) including for traffic destined to the management software.
- VLANs (port based)
  This allows a user to group sets of ports into logical blocks, separating traffic into "Virtual LANs"
  - IEEE 802.1Q
- VLANs (tagged)
  This is used to separate traffic into VLANs, based on information based in the frame header.
  - IEEE 802.3ac
- GVRP
  This protocol handles the exchange of VLAN registrations between switches, allowing dynamic management of the broadcast domains in a network.
  - IEEE 802.1Q
- Quality of Service
  Information in the header is used to prioritize traffic of different types (e.g. voice or data). A range of capabilities are provided to handle Class of Service, Differentiated Services, and Access Control.
  - IEEE 802.1p, RFC 2474, 2475, 2597, 3246, 3260
- Storm control
  Storm control allows the user to protect the network from "bad things" happening when nodes are wrongly configured, or from malicious attacks.
- Filtering
  Filters can be set up to change the forwarding of certain frames – perhaps to block packets matching particular patterns, or pass traffic from a suspicious address out a certain port. These can also be configured to block particular traffic – matching (or partially matching) certain patterns. This is typically used for firewall type functions.
- Trunking (Link Aggregation)
  Groups of ports can be grouped together to provide combined level of throughput between systems. OpenWare allows this to be set up either manually, or using the

Link Aggregation Control Protocol (LACP).
  - IEEE 802.3ad
- Mirroring
  Traffic from one or more ports can be "copied" to another port. This is typically used to debug network problems.
- Port Configuration
  Ports can be manually or automatically configured in a number of ways: speed, duplex, fiber/copper, flow control, Pause frame generation, MTU settings. Port statistics and configurations are recorded and displayed to the user. Ports can be manually set up or down (enabled/disabled).
- Rate limiting
  The traffic load on specific ports can be limited, to prevent saturation of the network by rogue devices.
- Congestion Control
  Extending the PAUSE frame generation further an administrator can tune the level at which these frames are generated by setting backpressure and internal buffers per port.
- Precision Time Protocol (PTP) support
  OpenWare allows the user to configure use of PTP. Transparent Clock mode is supported on our recent switches, allowing the switch to modify packets with information about latency within the switch.
- Port Statistics
  In addition to the normal traffic statistics, we have recently added specific counters to reflect the traffic loading on each port. this is used by some customers to identify the normal traffic levels in their network, and possibly flag up early indication of developing problems.
- Fiber Optic Power Budgets
  Because military customers often use fiber optics in situations where the signal may suffer problems, we have provided easy access to information about how much of the optical power is being received at each end. This is useful in identifying installation issues.
- Inter-Frame Gap control
  To satisfy requirements of some military protocols, OpenWare can allow the user the ability to adjust the Inter-Frame Gap. This affects the timing of Ethernet frames, and is relevant to a small number of military specifications.

# Introduction to Ethernet Switch Management with OpenWare

## Switch protocol features

### Security Control

Improved security to manage who can connect to and what traffic is permitted to flow through the switch can be carried out using these features. These features also guard against rogue external devices attempting to disrupt the normal switch operation.

- Port Security
  This allows an administrator to configure a set of allowed MAC addresses, or create a limit on the number of allowed connections on particular ports. If a device attempts to connect where the MAC address is not configured as permitted, or the port limit is reached, the device will be denied access to the network through switch ports.
- Port Authorization
  802.1X Port Authorization is supported, allowing specific control over who can be connected to which port. Typically, this makes use of a remote RADIUS server.
  - IEEE 802.1X, RFC 2868, 2866
- Denial of Service Protection
  Once enabled, this feature provides protection from certain types of DoS attacks.
- DHCP Snooping
  This allows an OpenWare switch to filter untrusted DHCP messages and will create an IP-MAC binding table, which can then be used to check the integrity of other switch messaging.
- Dynamic ARP Protection
  This provides a method of confirming that ARP messages are being sent to the NETernity switch from known sources, helping prevent ARP spoofing attacks.
- MAC Notification
  This provides a log of information as device addresses are added to and removed from switch ports – SNMP traps can be configured to provide information to a remote Network Management entity.

### Multicast

The multicast features provide a method of limiting the forwarding of multicast traffic by only sending to devices which have indicated an interest in receiving it. This can be configured dynamically using IGMP and MLD or by addition of static entries.

- IGMP Snooping Querier
  - The switch can react to and generate IGMP protocol messages, which allow an OpenWare switch to dynamically update the internal multicast forwarding database, only forwarding traffic on ports which have expressed a wish to receive it. This makes for efficient use of the overall network bandwidth.
  - Both IGMP Snooping and IGMP Snooping Querier functions are supported.
    > RFC 1112, 2236, 3376, 4541
- MLD (Multicast Listener Discovery) Snooping Querier
  - MLD provides the same scope of multicast data control as IGMP Snooping Querier but in IPV6 networks.
  - Both MLD Snooping and MLD Snooping Querier functions are supported.
    > RFC 3513, 4541
- Static Multicast control
  OpenWare allows the configuration of static multicast entries, providing a method of limiting multicast data forwarding for cases where IGMP or MLD is not available.
- IGMP/MLD Access Groups & Limits
  This feature allows an Administrator the ability to manage access to configured multicast groups, and also limit the number of multicast groups which are able to be joined on defined ports.
- GMRP
  This protocol handles the exchange of information about multicast groups and forwarding mode options between switches.
  - IEEE 802.1D 802.1Q
- PIM-SM (Protocol Independent Multicast – Sparse Mode)
  PIM allows for multicast traffic to be carried over unicast routes. This is applicable in complex networks with heavy multicast use, typically with routing controlled by routing protocols like RIP or OSPF.
  - RFC 4601
- Static Multicast Routing
  This feature provides a method for a User to add static multicast routes so defined multicast traffic can be forwarded across VLANs.

### Configuration

- DHCP Client/Server/Relay for IPv4 and IPv6
  The switch can get its configuration information (e.g. IP address) from another system – or the switch can be configured to give out configuration information to other systems in the network.
  - RFC 951, 1542, 1534, 2131, 2132, 3046, 3315, 3396, 3736, 4242
- DHCP Server (Port Aware)
  The switch has a facility that allows allocation of an IP address for a DHCP Client based on the port on which the DHCP address request was received on.
- Configuration profiles
  Switches may need different configurations, depending on where they are positioned in a network. OpenWare provides the ability for switches to automatically select different configuration files, dependent on pre-defined criteria – for example based on a Geographic Address, set by the cable harness.

### Management Protocol

- SNMP
  OpenWare supports SNMP, allowing for OpenWare switches to be managed and integrated into networks where consolidated control of heterogeneous networks is required. Appropriate standard MIBs are supported for most protocol implementations.
  - RFC 1155, 1157, 1212, 1215, 1901, 1908, 2571, 2573, 2578, 2579, 3410, 3416, 3584

Provision of SNMP Traps in order to provide indications of events to SNMP management entities.

### Redundancy/Failover

OpenWare includes a number of features which provide failover and redundancy support in the event that links fail and the network needs to automatically reconfigure or failover to redundant links.

# Introduction to Ethernet Switch Management with OpenWare

- MSTP (Multiple Spanning Tree)
  - Spanning Tree Protocol is used to provide and manage redundant paths through a network. It prevents loops being formed and reconfigures the network if a link becomes unavailable. MSTP is the latest version of this protocol, and allows for different trees to exist over complex networks, segmenting a network into separate regions and using multiple VLANs to further segment and provide different paths for traffic on different VLANs. This improves the failover performance and allows load balancing to occur through the network.
    - > IEEE 802.1d, 802.1w, 802.1Q-2005
  - MSTP will interoperate with the other Spanning Tree Protocols (STP, or RSTP.)
- Spanning Tree and Link Aggregation
  OpenWare allows combinations of protocols - for example STP can be run over aggregated links.
- VRRP (Virtual Router Redundancy Protocol)
  This standard protocol can be used to provide failover (or load sharing) between switches, routers or hosts. Typically used in large, complex network configurations.
  - RFC 3768
- FailOver Groups (FOG)
  This is a proprietary mechanism, allowing for very fast failover/failback of switches or links in homogeneous networks. This is a building block for High Availability configurations.

## Layer 3
The layer 3 operation of the OpenWare switch provides support for routing of IP traffic between routing domains - this is provided either statically or by the use of routing protocols in order to maintain dynamic routing information.

- Routing
  OpenWare supports manual and protocol-controlled handling of Layer 3 routing, in both IPv4 and IPv6.
  - RFC 1519, 1812
- Routing protocols
  The routing protocols supported include RIP, OSPF and BGP for IPv4 and RIPng, OSPF and BGP for IPv6.
  - RFC 1058, 2453, 2328, 1997, 2439, 3107, 4241, 4456, 5056
- Differentiated Services (DiffServ)
  - Allows classification of packets flowing through the switch and assigns actions based on these – supports wide range of classification, including IP or MAC address (source or destination), port, VLAN, and Ethertype. Actions include, packet dropping, switching, redirection, mirroring or packet counting. Using a combination of these commands will provide a flexible method of traffic management.

## System
- IP Address Control
  The switch management entity can be configured with multiple IPv4 and an IPv6 addresses.
- System control
  Comprehensive tools are provided for management of software version, configurations, debugging, and logging.
- Built In Test (BIT)
  OpenWare provides tools to run tests of the hardware, on startup (pBIT) or on request (iBIT)) or continuously, in the background (cBIT). The types of testing in these BIT operations are configurable, but can even include putting ports into loopback. This provides a high level of confidence in the switch operation.
- System Initialization
  Making use of the flexibility of the underlying Linux system, OpenWare features can be scheduled to be started and configured during the boot process.

- Fast start-up
  One area which OpenWare has pushed the boundaries is the time taken to start up. We measure from power-on to the first frame switched (with a relatively simple configuration.) We achieve under thirty seconds on most of our switches - in some cases, approximately fifteen seconds. For a fully managed switch, that can be an important figure.
- System Security
  A number of features in OpenWare are aimed at providing the types of security control that the military are interested in. Various ways to sanitize non-volatile memory are provided, including the option to network boot OpenWare itself, avoiding the need to hold any sensitive information on the switch. We are well experienced with working in cooperation with our customers to provide the software tools they need.

## VICTORY testing
Switches running OpenWare have been successfully tested against US Army VICTORY (Vehicle Integration for C4ISR/EW Interoperability) specifications. To satisfy this, OpenWare was enhanced in a small number of areas - including a specific set of SNMP MIBs being added.

## Availability
OpenWare is available on a wide range of NETernity switches, with many combinations of form factor, fiber or copper, slow to very fast line speeds, different levels of ruggedness, thermals and packaging.

Please contact your sales representative to determine the appropriate switch you need for your project as the full suite of OpenWare features may be limited on some models.

## WE INNOVATE. WE DELIVER. YOU SUCCEED.

**Americas:** 866-OK-ABACO or +1-866-652-2226     **Asia & Oceania:** +81-3-5544-3973

**Europe, Africa, & Middle East:** +44 (0) 1327-359444

**Locate an Abaco Systems Sales Representative visit:** abaco.com/products/sales

**abaco.com**    @AbacoSys

abaco
SYSTEMS