EtherXtend 30x4 Release Notes

This document provides information for the ETHX-30x4 Firmware release 1.3.1.114   and includes the following information:

- Summary

- New Features

- Problems Fixed

- Known issues or limitations

- Upgrade procedure

- Contacting Global Service and Support

Summary

The EtherXtend 30x4 is a family of SHDSL EFM Network Extenders.   These devices support IEEE 802.3ah loop bonding to create a WAN uplink connection up to 22 Mbps.   Each EtherXtend device provides 4 local Ethernet ports for connection to customer equipment.

Typical applications include leased line replacement, transparent LAN services, Branch-to-Headquarters connectivity, and Internet Access.

R1.3.1 is a major feature release for the ETHX-30xx product line. It includes the following new features, described in more detail in the next section:

- Static Routing on a per-VLAN basis
- Dynamic Route Table updates via RIP or BGP
- NAT (Network Address Translation)/IP Masquerading per VLAN
- DHCP Server per VLAN
- Basic Firewall
- Port Forwarding
- Login Session Inactivity Timer
- SHDSL Link Up Counter and Timer
- Extended SHDSL rates
- Exec-replay scripts now support embedded comments

New Features added since R1.2.2.123 release

(1.3.1.111) SNMP Enhancements

◊   Extensions were made to the following Zhone Enterprise MIBs:
   NP-SYSTEM-MIB.mib
   ZHN-SYSTEM-MIB.mib
   ZHN-SYSMON-MIB.mib

The full suite of Zhone Enterprise MIBs supported by the R1.3.1 release of SW for the ETHX-30xx products is available at www.zhone.com/support/downloads/mibs .

(1.3.1.111) Dynamic Routing

◊   Support for RIP and BGP has been added, enabling dynamic Route Table updates. The maximum size of the Route Table is 128 entries. This feature enables an ETHX-30xx unit to share its statically configured Route Table entries with its peer Provider Edge Router in an MPLS network, and to dynamically update its Route Table with entries that are pushed to the ETHX-30xx unit from its peer router.

(1.3.1.107) Static Routing

◊   When adding a new VLAN (or modifying an existing VLAN), a new configuration option is used to select Routing or Bridging of the traffic on that VLAN.

When Bridging is selected for a VLAN, traffic will be forwarded based on MAC address lookups in the Bridge. The Bridge table is automatically updated based on MAC address learning.

When Routing is selected for a VLAN, traffic will be forwarded based on Route Table and VLAN membership lookups.   The Route Table must be Statically Configured.

This is different from traditional Routers that forward traffic from any port to any port based on Route Table lookups, with no VLAN awareness.   The purpose of the VLAN-aware "Secure Routing" feature supported by R1.3.1 is to provide the same level of traffic isolation that is provided by "Secure Bridging" mode.

If there is no need for traffic isolation, then all LAN and WAN interfaces can be members of the same VLAN.   If traffic isolation is required, then a different VLAN can be assigned for each IP Subnet to provide that isolation.

An added advantage of Secure Routing vs. Secure Bridging is that IP Masquerading / NAT can be used to conserve Routable IP Addresses in the WAN Network and provide increased security for the client devices located behind the NAT Firewall.

A configuration example is provided later in this document that details the procedure that must be followed to properly configure a Routed Mode connection.

(1.3.1.107) NAT (IP Masquerade)

◊ Traditional Network Address Translation (NAT) is a one-to-one method of sharing Internet IP addresses among many computers on a private network. NAT works completely on the network level, meaning that NAT operates by changing IP packets. NAT does not modify higher level protocol information, such as TCP, UDP, ICMP, etc.

IP Masquerade is a variation of NAT that uses a one-to-many translation technique: it allows many private IP addresses to simultaneously share a single Internet IP address. IP Masquerade operates at the network and transport level: it changes both the IP and TCP (or UDP) header information at Layer 3 and Layer 4.

R1.3.1 includes support for IP Masquerade, but since most users are familiar with the term "NAT", that is the term used on the Web and CLI interfaces. NAT may be enabled per WAN-side VLAN (i.e. eth0.1).

Related background information:

After NAT is enabled on a WAN-side interface, the corresponding interface(s) on the LAN side must be assigned an IP address.

The address on the LAN side interface is what the client devices on the LAN will use as their Gateway IP address.   As an example, the eth1:0.1 interface could be assigned 192.168.1.254 with a subnet mask of 255.255.255.0.

After eth1:0.1 has been configured, a client device with a statically configured IP address of 192.168.1.100 could plug into the eth1:0 port and successfully PING the 192.168.1.254 gateway address. If the client is also statically configured with the IP address of a valid DNS server on the WAN, it could launch a browser and access the Internet.

(1.3.1.107) DHCP Server

◊ The DHCP feature provides a means for dynamically assigning private IP Addresses to LAN client devices, along with the IP Addresses of the primary and secondary DNS servers in the WAN that should be used for Domain Name resolution.

(1.3.1.107) Firewall

◊ R1.3.1 includes support for basic firewall security, including the ability to disable (block) or enable (allow) the following services to traverse the NAT function:
- Ping (icmp)
- ssh
- telnet
- http
- https
- tftp
- ftp
- syncookies

In addition, any of the LAN-side or WAN-side firewall interfaces can be configured as a "Router Management Interface" to enable that IP address as a management interface for the device.

◊   In the "Advanced" Firewall configuration screen, Port Forwarding may be configured. Port Forwarding allows remote computers (e.g. public machines on the Internet) to connect to a specific computer within a private LAN. This allows you to setup servers on your private LAN and make them available externally.

DNAT or Destination Network Address Translations is used to implement Port Forwarding. DNAT translates the destination public IP address to a private IP address. When configuring Port Forwarding, you must specify a port (or a range of ports), the network protocol, the public IP address and the IP address of the server on the private LAN to forward to. To specify a range of ports, enter the first port number for Start Port and the last port number for End Port. If only one port number is to be forwarded, enter the same number for the Start Port and End Port.

Note that NAT must be enabled for Port Forwarding to work correctly.
The previous paragraphs need a couple of screen captures to make this clear to the average user.

(1.3.1.107) Login Session Inactivity Timer

◊   User login sessions (HTTP, HTTPS, Telnet, SSH) will be automatically disconnected upon expiration of the inactivity timer. The default value is 300 seconds (5 minutes). A value of 0 disables the inactivity timeout feature.

(1.3.1.107) SHDSL Link up counter and timer

◊   A link up counter is now provided for each SHDSL link, reporting the total number of retrains since the port was last reset or disabled (admin down). In addition, a link up timer now reports how long the link has been up since the last retrain event.

(1.3.1.107) Extended SHDSL Rates

◊   The SHDSL link can now be configured for rates of 32kb/s up to 12Mb/s. Previously, the SHDSL link could be configured for rates from 192kb/s to 5.7Mb/s.

Standard SHDSL uses TCPAM-16 and TCPAM-32 encoding, at symbol rates from 64K symbols/sec to 1424K symbols/sec.

TCPAM-16 provides 3 bits of information per symbol, and TCPAM-32 provides 4 bits per symbol. Since TCPAM-32 has twice as many levels as TCPAM-16, it requires 3dB more SNR to operate at an equivalent error rate.

At the 64K symbol rate, TCPAM-16 provides a data rate of 64K x 3 = 192Kbps, and TCPAM-32 provides a data rate of 256Kbps.   At the 1424K symbol rate, TCPAM-16 provides a data rate of 4272Kbps, and TCPAM-32 provides a data rate of 5696Kbps.

The Extended SHDSL Rates include TCPAM-4 (1 bit per symbol) and TCPAM-8 (2 bits per symbol) encoding, which provide lower data rates but require less SNR, enabling them to operate on longer loops (less signal) and/or noisier loops. The SNR requirement for TCPAM-4 is 6 dB less than TCPAM-16, and the SNR requirement for TCPAM-8 is 3dB less than TCPAM-16.

The extended rates also include TCPAM-64 (5 bits per symbol) and TCPAM-128 (6 bits per symbol) encoding, which provide higher data rates but require better SNR. TCPAM-64 and TCPAM-128 require 3dB more and 6dB more (respectively) SNR than TCPAM-32.

As such, these higher density TCPAM levels can only operate on shorter loops (more signal) and/or quieter loops (less noise).

When the standard SHDSL Symbol Rates are used, but TCPAM-4/8/64/128 levels are used instead of the standard TCPAM-16/32 levels, there is no change to the PSD of the transmit signals -- they continue to comply with all of the standard SHDSL masks, however the rates supported by each Mask will vary.

In addition to adding lower density and higher density TCPAM levels, the Extended Rates feature also adds some higher symbol rates (up to 2048K symbols/sec). These go beyond the SHDSL transmit masks, and may require special regulatory testing and approvals as a result. At the 2048K symbol rate, TCPAM-128 provides 12,280Kbps per pair.

The Extended Rates are not available when Autorating is enabled. The Extended Rate must be manually configured on a line by line basis on the CO device, and the CP device will automatically detect the configured rate and will attempt to connect at that rate. If a rate is configured that cannot be supported due to loop length or noise, the unit will not train up on that loop until the rate has been reconfigured for a reduced rate that the loop can support.

(1.3.1.107) Exec-Replay Scripts with Comments

◊ The EtherXtend 30xx series products support a powerful configuration scripting feature called "Exec-Replay". A configuration script file can be created with any standard ASCII text editor (i.e. Windows Notepad or Wordpad) consisting of any number of CLI commands that must be edited to configure the unit.

Exec-Replay scripts are the ONLY officially supported mechanism for using automated configuration scripts with the EtherXtend 30xx devices.

The sample configuration script provided below begins with a unit that has been reset to the factory default configuration. It includes all CLI commands needed to configure the unit as required for a sample customer application, and at the end of the script the configuration is Saved and a Reset is initiated.

```
#1 Default VLANS are removed
    #The default vlans are deleted by first removing member ports then the vlans:

    /config vlan vlanconfig removeport interface eth0 vlanid 1
    /config vlan vlanconfig removeport interface eth0 vlanid 7
    /config vlan vlanconfig removeport interface eth1:0 vlanid 1
    /config vlan vlanconfig removeport interface eth1:1 vlanid 1
    /config vlan vlanconfig removeport interface eth1:2 vlanid 1
    /config vlan vlanconfig removeport interface eth1:3 vlanid 1
    /config vlan vlanconfig removevlan vlanid 1
    /config vlan vlanconfig removevlan vlanid 7


#2. New VLAN configuration

    /config vlan vlanconfig addvlan vlan_name VLAN145_temporary_management_access vlanid 145 mode bridging
    /config vlan vlanconfig addvlan vlan_name VLAN146_high_priority vlanid 146 mode bridging
    /config vlan vlanconfig addvlan vlan_name VLAN147_tagged_only_service vlanid 147 mode bridging
    /config vlan vlanconfig addvlan vlan_name VLAN148_inband_management_dhcp vlanid 148 mode bridging


    #Ports must be added to the vlans
```

```
    #145 named VLAN145_temporary_management_access interfaces-tagged eth0(dsl EFM group) and
        # untagged eth1:3(LAN port 4) priority 0

    /config vlan vlanconfig addport interface eth0 vlanid 145 tagged
    /config vlan vlanconfig addport interface eth1:3 vlanid 145 untagged
    /config vlan portdefaults vlanport eth1:3 pvid 145 priority 0

    #146 named VLAN146_high_priority interfaces-tagged eth0(dsl EFM group) and untagged
        # eth1:0(LAN port 1) priority 7

    /config vlan vlanconfig addport interface eth0 vlanid 146 tagged
    /config vlan vlanconfig addport interface eth1:0 vlanid 146 untagged
    /config vlan portdefaults vlanport eth1:0 pvid 146 priority 7

    #147 named VLAN147_tagged_only_service interfaces-tagged eth0(dsl EFM group) and
        # tagged eth1:1(LAN port 2)

    /config vlan vlanconfig addport interface eth0 vlanid 147 tagged
    /config vlan vlanconfig addport interface eth1:1 vlanid 147 tagged

    #148 named VLAN148_inband_management_dhcp interfaces-tagged eth0(dsl EFM group)

    /config vlan vlanconfig addport interface eth0 vlanid 148 tagged



#3. Management address configuration:

    /config if mgmt-addrmode brvlan145 static
    /config if mgmt-addrmode brvlan148 dhcp
    /config if interface brvlan145 ip 10.10.10.10 mask 255.255.255.0 broadcast 10.10.10.255

#4. Management user configuration

    /config usrmgmt add-user user-name admin_1 passwd 1asdfjkl! confirm-passwd 1asdfjkl! role admin
    /config usrmgmt change-password user-name admin old-password zhone new-password !_#j99x confirm-password !_#j99x


#5. SNMP and trap manager configuration

    /config snmp community-info add asdf1234JKLM read-only
    /config snmp community-info delete public
    /config snmp trap-managers add 10.100.77.66 v1 community something port 162

#6. Configuration is saved

    /config admin-tools save running-config

#7. System is rebooted

    /config system reboot
```

◊   Exec-Replay scripts are saved to a directory in Flash memory and are retained through power cycles and resets until the next SW Upgrade. Flash memory is erased during the SW upgrade process, and as a result any Exec-Replay scripts that were stored in Flash will need to be re-downloaded after the upgrade.

◊   Exec-Replay scripts are executed one command line at a time, and automatically begin execution of the next command when the previous command has been fully completed. Depending on the command and the reconfiguration actions it specifies, the time required to complete execution will vary. For this reason, it is not feasible to use a terminal emulator to blindly push CLI commands at the unit with a pre-defined wait time between commands.

6

◊   The Exec-Replay feature was initially supported in R1.2.2 versions of SW. In R1.3.1 versions, this feature was enhanced ignore any lines in the script that begin with a # character, enabling the addition of comments to the script files for improved usability.

◊   In addition, R1.3.1 adds support for CR/LF end-of-line characters to enable script editing with any standard ASCII text editor. R1.2.2 SW only supported CR as the end-of-line character, requiring the use of a special text editor such as VI to create and edit scripts.

◊   Once the script file has been created using a PC, terminal or workstation and saved on a TFTP or FTP server as a .txt file, it will need to be downloaded into the EtherXtend device and stored in the /alias directory.

To initiate the transfer of an exec-replay script to an EtherXtend 30xx device via TFTP:

1. login to the EtherXtend device as admin/zhone from the CLI
2. `EtherXtend > /shell` to drop from the CLI to the BusyBox Shell prompt
3. `~ $ tftp -g -l /alias/script.txt -r script.txt 192.168.1.254`
4. `~ $ exit` to exit the Shell and return to the CLI prompt

Notes:
- File permissions for the source file on the TFTP server must be accessible for the admin/zhone userid to access the file.
- The script file is called "script.txt" in this example, but it can be called anything.
- The 192.168.1.254 address used in the above example is the IP address of the TFTP server where the script file is located

To initiate the transfer of an exec-replay script to an EtherXtend 30xx device via FTP:

1. login to the EtherXtend device as admin/zhone from the CLI
2. `EtherXtend > /shell` to drop from the CLI to the BusyBox Shell prompt
3. `~ $ ftpget -u anonymous -p passwd 192.168.1.254 /alias/script.txt script.txt`
4. `~ $ exit` to exit the Shell and return to the CLI prompt

Notes:
- This command will "get" the file from the user's default home directory, as specified in /etc/passwd. For example, most Linux machines map the user login "anonymous" to the /var/ftp directory.
- The script file is called "script.txt" in this example, but it can be called anything.
- The 192.168.1.254 address used in the above example is the IP address of the FTP server where the script file is located

After the Exec-Replay script file has been downloaded into the /alias directory, the following CLI command will initiate execution:

```
EtherXtend > /exec-replay /alias/script.txt
```

◊   Multiple Exec-Replay scripts (each with a unique filename) may be stored in the `/alias` directory, and invoked one at at time using the above CLI command.

7

IP Routing Interface Diagram

Router interfaces may be "unconfigured" (no IP address assigned), "static" (static address assigned), or "DHCP" (DHCP client requests address from upstream server on that VLAN).

LAN-side Router Interface IP is the Gateway for LAN-side client devices.

WAN-side Router Interface IP is the DA for downstream packets on that VLAN

NAT should be enabled for WAN-side (eth0) Router interfaces.

DHCP Server may be enabled on any LAN-side primary Router interface (eth1.x) to assign IP Addresses within the configured range to client devices connecting to that network. The secondary Router interfaces (eth1.x.net0 – eth1.x.net3) provide additional subnets for statically assigned clients.

If "Secure Routing" is enabled, all traffic will be forwarded to the Default GW for that VLAN, even if there is a local route to that subnet defined.

If "InterVLAN Routing" is enabled, the router will allow local routing between VLANs. When disabled, local routing is limited to subnets within each VLAN.

NOTE:
Every configured VLAN will be assigned a virtual interface on the bridge, creating a vlan bridge interface. Up to 24 VLANs may be configured, using any of the available 4096 VLAN IDs. The **Bridge Interfaces** status screen will display all configured VLAN bridge interfaces. The VLAN bridge interfaces that may be use for management access to the EtherXtend unit must have an IP address assigned to them. **brvlan1** is the default VLAN bridge interface with a static IP address that may be used to gain management access into the EtherXtend unit. **brvlan7** is the default VLAN bridge interface with a dynamic (DHCP client) IP address that may be used to gain management access.
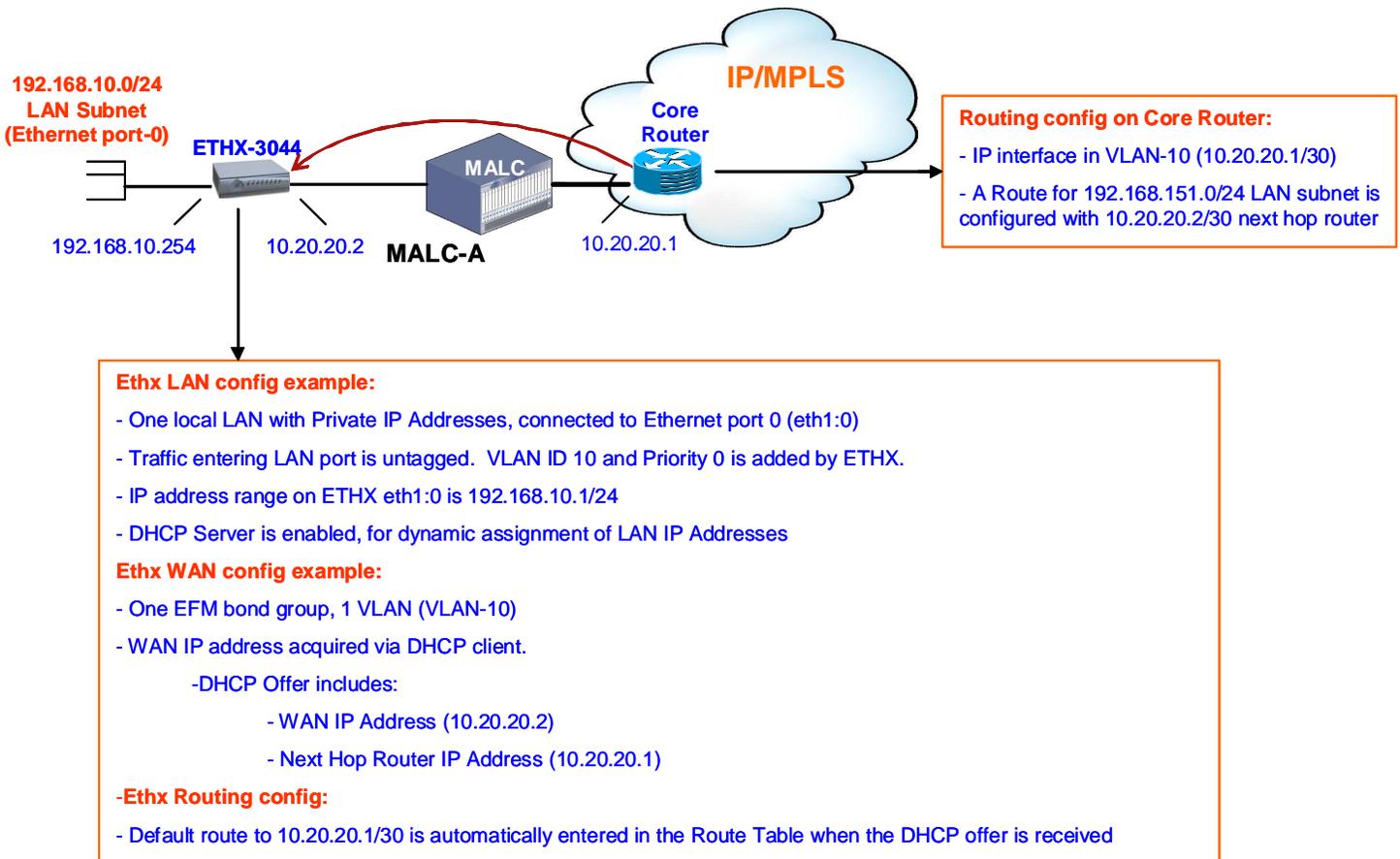
IP Routing Configuration Example

VLAN-aware IP Routing

◊ When a VLAN is configured for Routing mode, traffic will be forwarded based on Route Table and (optionally) VLAN membership lookups.

This is different from traditional Routers that forward traffic from any port to any port based solely on Route Table lookups, with no VLAN awareness. By restricting Route Table lookups and forwarding to stay within the configured VLAN, the ETHX-30xx products can support multiple simultaneous routers, with one router per VLAN, each having its own WAN IP Address and LAN subnet range. This sample configuration diagram on the preceding page illustrates this capability.

The diagram below is a simple NAT Routed configuration. Instructions regarding how to configure the ETHX-30xx unit for this configuration using the Web GUI or using an Exec-Replay script are provided in the pages that follow.

192.168.10.0/24 LAN Subnet (Ethernet port-0)

ETHX-3044

IP/MPLS

Core Router

MALC

MALC-A

192.168.10.254   10.20.20.2   10.20.20.1

Routing config on Core Router:

- IP interface in VLAN-10 (10.20.20.1/30)

- A Route for 192.168.151.0/24 LAN subnet is configured with 10.20.20.2/30 next hop router

Ethx LAN config example:

- One local LAN with Private IP Addresses, connected to Ethernet port 0 (eth1:0)

- Traffic entering LAN port is untagged. VLAN ID 10 and Priority 0 is added by ETHX.

- IP address range on ETHX eth1:0 is 192.168.10.1/24

- DHCP Server is enabled, for dynamic assignment of LAN IP Addresses

Ethx WAN config example:

- One EFM bond group, 1 VLAN (VLAN-10)

- WAN IP address acquired via DHCP client.

    -DHCP Offer includes:

        - WAN IP Address (10.20.20.2)

        - Next Hop Router IP Address (10.20.20.1)

-Ethx Routing config:

- Default route to 10.20.20.1/30 is automatically entered in the Route Table when the DHCP offer is received

The sequence of Web configurations steps required to configure Ethernet port 0 for NAT Router mode on VLAN 10 (as illustrated in the diagram on the previous page) are detailed in the 8 steps that follow.   The equivalent CLI command sequence is also provided as an Exec-Replay script.

1. Web: select, under "Configuration", VLAN Settings,
    a. - unassign Ethernet port 0 (**eth1:0**) from VLAN 1

2. Web: Select, under "Configuration", VLAN Settings, select "Add"
    a. -add VLAN **10** and change "VLAN Mode" to **routing**

3. Web: Select, under "Configuration", VLAN Settings, highlight VLAN ID 10 and select **assign ports**
    a. - add eth0 tagged and eth1.0 untagged.

4. Web: Select, under "Configuration", Port Defaults
    a. - change eth1:0 to PVID 10
    b. – select desired Priority level (i.e. 0)

Note: If you try to configure NAT at this point on the Web, you will only have the option of selecting eth1.10 - not eth0.10, which is required for the WAN side.

The next sequence that is required for eth0.10 to become available in the NAT screen is configuring the Router interface from "unconfigured" to dhcp or static.

---

5. Web:Select, under "Configuration", Router
    a. - modify interface eth0.10 address mode to dhcp or static (dhcp in this example)

6. Web:Select, under "Configuration", Router
    a. - modify interface eth1.10 address mode to dhcp or static (static in this example) with ip address of 192.168.10.254 as the LAN address

7. Web:Select, under "Configuration", NAT
    a. - Apply Router Interface **eth0.10**

8. Web:Select, under "Configuration", DHCP Server
    a. - enable Service

    Select **add** under eth1.10 interface
    b. add start and end IP range (i.e. 192.168.10.1 -- 192.168.10.253)

Equivalent Exec-Replay Script:

```
#1  Remove Ethernet Port 0 from VLAN1 (factory default configuration)

/config vlan vlanconfig removeport interface eth1:0 vlanid 1


#2  Create new VLAN10 and set VLAN Mode to "Routing"

/config vlan vlanconfig addvlan vlan_name vlan10 vlanid 10 mode routing


#3  Assign eth1:0 (LAN Port 0) as an untagged member of VLAN10, and eth0 (WAN uplink) as a tagged member of
VLAN10

/config vlan vlanconfig addport interface eth1:0 vlanid 10 untagged
/config vlan vlanconfig addport interface eth0 vlanid 10 tagged


#4  Set default tag and priority level for untagged traffic on eth1:0 to PVID=10, Priority Tag=0

/config vlan portdefaults vlanport eth1:0 pvid 10 priority 0


#5  Configure eth0.10 interface (VLAN10 on the eth0 WAN uplink) to request a management IP address via DHCP
client

/config if mgmt-addrmode eth0.10 dhcp


#6  Configure eth1.10 interface (VLAN10 on LAN side of NAT router) with a static IP address 192.168.10.254,
and a default gateway of 192.168.10.254

/config if interface eth1.10 ip 192.168.10.254 mask 255.255.255.0 broadcast 192.168.10.255 default-gateway
192.168.10.254


#7  Enable NAT on the routed eth0.10 (VLAN10 on the eth0 WAN uplink) interface

/config nat interface eth0.10


#8  Configure DHCP Server for NAT routed eth1.10 (VLAN10 on LAN side of NAT Router) interface with an IP
Address range of 192.168.10.1 to 192.168.10.253

/config dhcp server enable
/config dhcp server-params lease-period 86400
/config dhcp enable interface eth1.10 ipaddr-range start 192.168.10.1 end 192.168.10.253


#9. Configuration is saved

/config admin-tools save running-config
```

11

R1.2.2.x Features

(1.2.2.122) Ethernet Port Status follows EFM Group Status

◊   A new Ethernet port configuration option has been added called "Follow WAN Uplink Status". When enabled, the Ethernet port will be forced to a physical down state when the WAN uplink is down, and will be restored to a normal operational state when the WAN comes back up.

(1.2.2.122) DHCP refresh on VLAN7 upon EFM bond group activation

◊   When DHCP client is enabled on VLAN7 (which is the factory default condition) the current IP address will be cleared when the EFM bond group goes down, and a new DHCP address request will be issued when the EFM bond group is restored to an active state. In prior releases, a new DHCP request was not issued until the lease time was 50% expired. This new behavior provides a mechanism to clear an IP address and force an immediate request for a new address.

(1.2.2.122) SW Upgrade MIB Support

◊   An Enterprise MIB enables support for SW downloads and activations. This feature is used by the Zhone Management System for ZMS-initiated SW Upgrades

```
genSystem.mib
        zhoneSysSwLogin
        zhoneSysSwPassword
        zhoneSysSwAdmin
                downLoadSw
                abortDownLoadSw
                imageFlashActive
        zhoneSysSwStatus
        zhoneSysSwPriLoadServer
        zhoneSysSwSecLoadServer
        zhoneSysSwRemoteFilePath
```

> **NOTE:**   **The Enterprise MIBs supported by the ETHX devices are available at http://www.zhone.com/support/downloads/mibs/**

(1.2.2.115) DHCP Client for Mgt IP Address Assignment (default enabled)

◊   EtherXtend 30x4 units ship from the factory with DHCP Client enabled on VLAN 7, to support automatic IP Address assignment when connected to the MALC.   If a static IP Address is desired, the console connection can be used to provision a static IP Address. To do this, set your terminal emulator for 9600 N 8 1 mode and log in to the unit using the default ID (admin) and password (zhone).   At the CLI prompt, enter the following command to configure static IP address 192.168.2.1 on the default data path (VLAN1, untagged):

```
/config if interface brvlan1 ip 192.168.2.1 mask 255.255.255.0 broadcast 192.168.2.255

/config admin-tools save running-config
```

(1.2.2.115) CO Mode
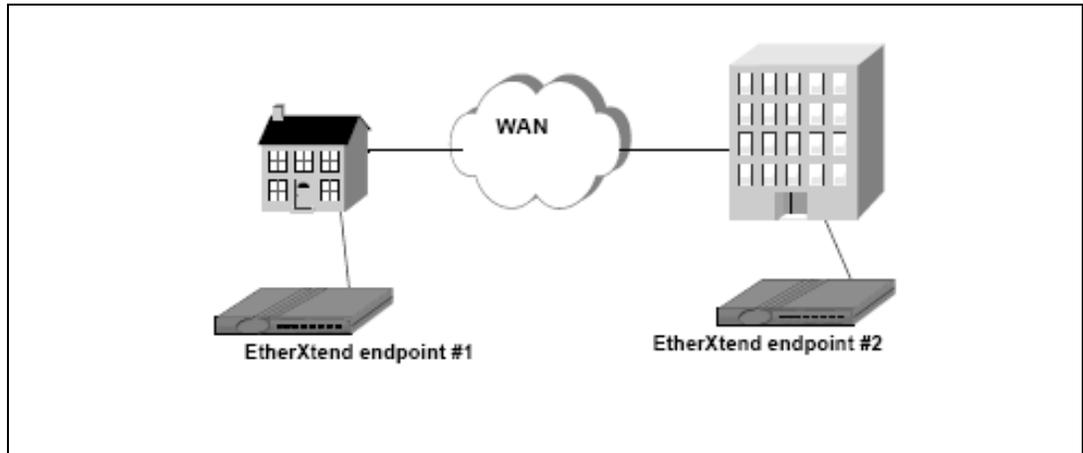
◊ Two EtherXtend 30xx CPE devices can be configured to operate "back to back", with one unit configured for CO mode and the other unit configured for CP mode.

◊ The "CO Mode" LED on the front of the 30xx modem will be illuminated when CO Mode is active.

◊ One EFM bond group is supported by 30xx CPE devices in CO Mode, so only one CPE device can be connected to it. Unused SHDSL EFM links cannot be used to connect a second CPE device.

◊ The CO Mode unit can be configured for fixed rate operation at any supported data rate, with no configuration changes to the CP Mode device required. The default configuration is Adaptive mode with a target SNR Margin of 6dB.

The EtherXtend defaults to CPE mode. When connecting two EtherXtends together across SHDSL loops, one (1) EtherXtend must be configured as a CO, while the other EtherXtend remains in the default CPE mode.

1. To set the modem to CO for back to back operations:

```
/config efm group mode CO
```

2. Save your changes

```
/config admin-tools save running-config
```

(1.2.2.107) SNMP MIB2 Support

MIB-2 RFC1213
SNMP V1 and V2c Support
Unlimited number of trap managers and configurable trap communities

(1.2.2.107) SNMP Alarms and Traps

Standard traps:

Cold Start	OID = .1.3.6.1.6.3.1.1.5.1
Link Down	OID = .1.3.6.1.6.3.1.1.5.3
Link Up	OID = .1.3.6.1.6.3.1.1.5.4
Authentication failure	OID = .1.3.6.1.6.3.1.1.5.5

13

Enterprise traps:

Zhone Alarm-Set   OID = `.1.3.6.1.4.1.5504.2.5.1.0.1`
Zhone Alarm-Clear   OID = `.1.3.6.1.4.1.5504.2.5.1.0.2`
Zhone Test-Start   OID = `.1.3.6.1.4.1.5504.2.5.1.0.3`
Zhone Test-Stop   OID = `.1.3.6.1.4.1.5504.2.5.1.0.4`
Zhone Ready   OID = `.1.3.6.1.4.1.5504.2.5.1.0.7`
Zhone Persistent Config Changed   OID = `.1.3.6.1.4.1.5504.2.5.13.0.1`

(1.2.2.107) PING utility

From the BusyBox shell, a "ping-like" utility (zhnping) can be invoked for diagnostic purposes. After entering the shell, execute the following for additional information on the usage and command syntax for the zhnping:

```
EtherXtend login: admin
Password:
EtherXtend> shell
BusyBox v1.00 (2007.10.18-20:25+0000) Built-in shell (ash)
Enter 'help' for a list of built-in commands.
~$ zhnping
Try zhnping --help' for more information.
QUICK START:
simple ICMP ping: zhnping -1 <host>
simple TCP ping: zhnping <host>
simple Port Scan: zhnping --scan 1-30,70-90 -S <host>

~ $ zhnping -1 10.112.3.254
HPING 10.112.3.254 (brvlan1 10.112.3.254): icmp mode set, 28 headers +
0 data bytes
len=28 ip=10.112.3.254 ttl=255 id=65445 icmp_seq=0 rtt=0.8 ms
len=28 ip=10.112.3.254 ttl=255 id=61655 icmp_seq=1 rtt=0.9 ms

--- 10.112.3.254 hping statistic ---
2 packets tramitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 0.8/0.8/0.9 ms
~ $ exit
```

(1.2.2.107) VLAN Priority and Rate Limiting

By default a first level of priority queuing is enforced on the physical LAN ports. Weighted round robin queuing is used to ensure the queues have access to at least some of the uplink bandwidth. The eight IEEE 802.1p priorities are mapped to the four queues according to the rules defined in Clause 7.7.3 and table 7-2 of the IEEE 802.1D standard. The queue mapping is defined as follows:

802.1p priority value	Internal Priority Queue
7	Critical
6	Critical
5	High
4	High
3	Medium
2	Low
1	Low
0	Medium

14

The weights are distributed as follows.
Queue1 (critical) = 50%
Queue2 (high) = 25%
Queue3 (medium) = 15%
Queue4 (low) = 10%

On a single service round, Queue1 can send 50% of the bandwidth, Queue2
can send 25%, etc. If there is only traffic on Queue1, it will take two rounds for it to
reach 100% of the bandwidth. Likewise if there is only traffic on Queue2, it will take 4 rounds
for it to each 100% of the bandwidth, etc.

VLANs can be configured for rate limiting. Rate limited VLANs can be configured for a second
level of priority queuing. The second level of queuing is strict priority queuing where a queue is
serviced until it is empty.

Using the CLI to configure VLAN 1 rate limited 1000kbps queuing enabled:

```
EtherXtend> /config vlan vlanconfig rate-limit vlanid 1 enable rate 1000 queuing enable
```

Problems Fixed

◊ (1.3.1.114) Unable to backup the configuration file using the web GUI. This issue was
introduced in R1.3.1.111 as a result of changes made to support SNMP-initiated
configuration backups.

◊ (1.3.1.111) The "add vlan" CLI command was modified in R1.3.1.107 to include an
additional argument to specify bridged or routed. In R1.3.1.111 this argument is now
optional and will default to bridged mode if it is not included. This has been done to
resolve compatibility issues with configuration scripts created for R1.3.0 and prior SW
releases.

◊ (1.3.1.111) An intermittent issue that prevented the "Save Running Config" command from
executing has been resolved.

◊ (1.3.1.111) Unable to use ZMS CPE Manager to restore the config database.

◊ (1.3.1.107) A bug that could result in some corrupt RAM memory locations was resolved.
It is unclear what the symptoms of this issue would be if it occurred in the field. There are
no known problem reports from the field related to this issue -- the bug was identified
during a code inspection.

◊ (1.3.1.107) Continuous SNMP pings using an invalid community string caused a slow
memory depletion.

◊ (1.2.2.123) The Web Browser compatibility issue with Mozilla FireFox version 3.05

◊ (1.2.2.122) Authentication trap will be sent when option is disabled

◊ (1.2.2.122) CLI command "help-config admin-tools" describes restore as config only and
does not mention previous bank of software

◊ (1.2.2.122) CLI show syslog command does not always work.

◊ (1.2.2.115) Latest revision of SHDSL driver SW included, with improved operation under
excessive noise conditions

◊ (1.2.2.115) The size of the Tx buffer used for queuing upstream traffic is now adjusted
automatically to a total size = 600msec X aggregate EFM Bond Group rate.

> For example, when the aggregate EFM Bond Group rate is 500,000 bps, the Tx buffer
> size is configured for 300,000 bits (37,500 bytes).

Prior SW Releases used a fixed Tx buffer size of 1,200,000 bytes.

This provides 600msec of buffering when the aggregate EFM Bond Group rate is 20,000,000 bps, but at lower rates the buffer is much larger than it needs to be. At lower rates, it was possible for a burst of traffic to introduce a queuing delay of 1 second or more, causing some client-server applications to time out.

◊ (1.2.2.115) Incorporates new SW for the Infineon SHDSL transceiver that resolves an issue with occasional CRC errors at line rates of 512Kbps and lower.

Known Issues

◊ EtherXtend CPE ifOperStatus always up even when a LAN connection is down

◊ Link up/down traps are sent for the EFM bond group, but not when individual SHDSL links go up or down.

◊ Configure Interface Ethernet modify command does not refresh web page when using MicroSoft IE to modify Eth1. You get a pop up of "Make changes to the page and then click apply". The pop up does not close and the Configure Interfaces Ethernet web page is not updated until you re-enter the page

Features not supported in this release

◊ VLAN Secure Forwarding mode is not supported but there is a CLI command for it.

Upgrade Procedure

This section describes the SW Upgrade and Bank Switch features of the EtherXtend 30xx CPE devices, and provides a detailed SW Upgrade Procedure.

SW Upgrades

EtherXtend has two banks for software with a dedicated set of configuration files associated with each bank. Only one bank of software and its associated configuration database is active at a time (called the "current" bank). The second bank is used to hold an alternate software revision and configuration. (called the "alternate" bank).

Upgrading the SW of an EtherXtend unit is a two step process.

1. Download the new SW image into EtherXtend temporary memory.
2. Upgrade the EtherXtend to the SW image that is in the temporary memory.

An Upgrade causes the following actions:
   a. The Alternate software bank is erased and reformatted
   b. The new SW image that has been downloaded into temporary memory is uncompressed and written to the Alternate bank.
   c. The configuration database in the Current bank is migrated over to the Alternate bank.
   d. A bank switch is performed, with the Current Bank now containing the new SW revision and migrated configuration database.

Warning:	**A reset to Factory Defaults and reconfiguration is required when downgrading to an older SW revision. However, the Bank Switch feature can be used to switch between the current and previous SW revisions with no need to Factory Default. This is because a copy of the configuration database is saved in the alternate bank that was used with that SW revision.**
Warning:	**Exec-Replay script files stored in the /alias directory will be erased during the SW upgrade process. Be sure to backup all Exec-Replay script files in a central location, so they can be loaded into the /alias directory after the upgrade has completed.**

Upgrade example:
   o EtherXtend with 1.2.2.122 in the Current Bank and 1.2.2.115 in the Alternate Bank
   o EtherXtend unit is upgraded to R1.3.1.114

Before Firmware Download

Bank #	Status	Release	Configuration File
1	Current	R1.2.2.122	Configuration B
2	Alternate	R1.2.2.115	Configuration A

After Firmware Download (R1.3.1.114) but before pressing Upgrade button

Bank #	Status	Release	Configuration File
1	Current	R1.2.2.122	Configuration B
2	Alternate	R1.2.2.115	Configuration A
Temp		R1.3.1.114 (compressed)	none

After pressing Upgrade button

Bank #	Status	Release	Configuration File
1	Alternate	R1.2.2.122	Configuration B
2	Current	R1.3.1.114	Configuration C (see note)

IMPORTANT NOTE: During the Upgrade, Configuration B is migrated from the SW revision in Bank #1 to be compatible with the new SW revision that is in Bank #2. The migrated configuration database is called Configuration C.

The upgraded EtherXtend unit is now running the new firmware and the previously active configuration database was migrated to the new firmware.

Any additional configuration changes that are made will be applied only to the Current bank (Config C) and will not be applied to the Alternate bank (Config B).

Firmware Bank Switching

The bank switch feature may be used to toggle the Current bank between Bank 1 and Bank 2. Since each bank contains the configuration database associated with the SW revision in that bank, switching between a newer SW revision and an older SW revision is fully supported. Alternatively, the bank switch feature can be used to support switching between two different configurations for the same SW revision.

IMPORTANT NOTE: No database migration occurs as a result of a bank switch – the configuration stored in the alternate bank becomes active.

Bank Switch example:
- o   EtherXtend unit with release 1.3.1.114 in the Current Bank and 1.2.2.122 in the Alternate Bank
- o   A Bank Switch is performed

Before Bank Switch

Bank #	Status	Release	Configuration File
1	Alternate	R1.2.2.122	Configuration B
2	Current	R1.3.1.114	Configuration C

After Bank Switch

Bank #	Status	Release	Configuration File
1	Current	R1.2.2.122	Configuration B
2	Alternate	R1.3.1.114	Configuration C

You can switch the active firmware bank. The command will force the unit to load the version of firmware that resides in the other "alternate" firmware bank. The Configuration database that is in the alternate bank will become active as well.

IMPORTANT NOTE: When a Bank Switch is performed, the currently active configuration will not be migrated to the newly active bank. The only time that the configuration file is migrated is during a SW Upgrade.

```
EtherXtend> /config admin-tools restore previous-bank
```

WARNING: This command will cause the unit to reboot.

The following command will display the firmware on the EtherXtend unit:

```
EtherXtend> /show system general-info
```

Upgrading EtherXtend software

The EtherXtend CPE provides a built-in mechanism for upgrading its software image without losing customer configurations and settings. To upgrade the software image, use a software image file pre-downloaded to your PC's disk drive.

> ✅ **Note:** Mozilla Firefox is the recommended internet browser for web access to the EtherXtend product. It is strongly recommended that Firefox be used. If using Internet Explorer then see the note referring to **Clearing Web Browser Cache** at the end of this section.

The following is an example of upgrading an EtherXtend CPE, which is running firmware version 1.2.2.103 to firmware version 1.2.2.107. A PC is connected directly to the EtherXtend CPE's LAN port.

To upgrade the EtherXtend CPE's software image using a locally available *.img* file:

1   Viewing the current firmware revision
(here you can see firmware version 1.2.2.103):

> ✅ **Note:** Only files with an *.img* extention can be used for upgrading the firmware of an EtherXtend unit

2   In the **System Software Upgrade Manual** section enter the path of the software image file, or press the **Browse** button to browse for the file on the PC, then click **Download**.
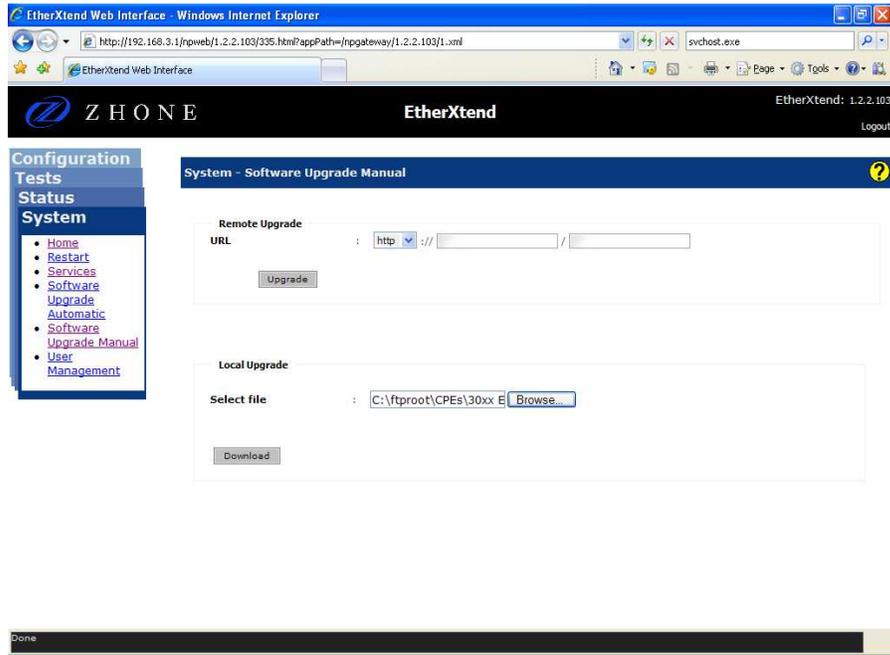
The file will start loading from the PC to the EtherXtend CPE. The word "Loading" will appear on the bottom of the web page. When loading is completed you will be prompted to log in again.

3   Verify from the Configuration Restore screen that the new code was loaded into the Current Software bank. To install this new release into both banks repeat step 2 above.
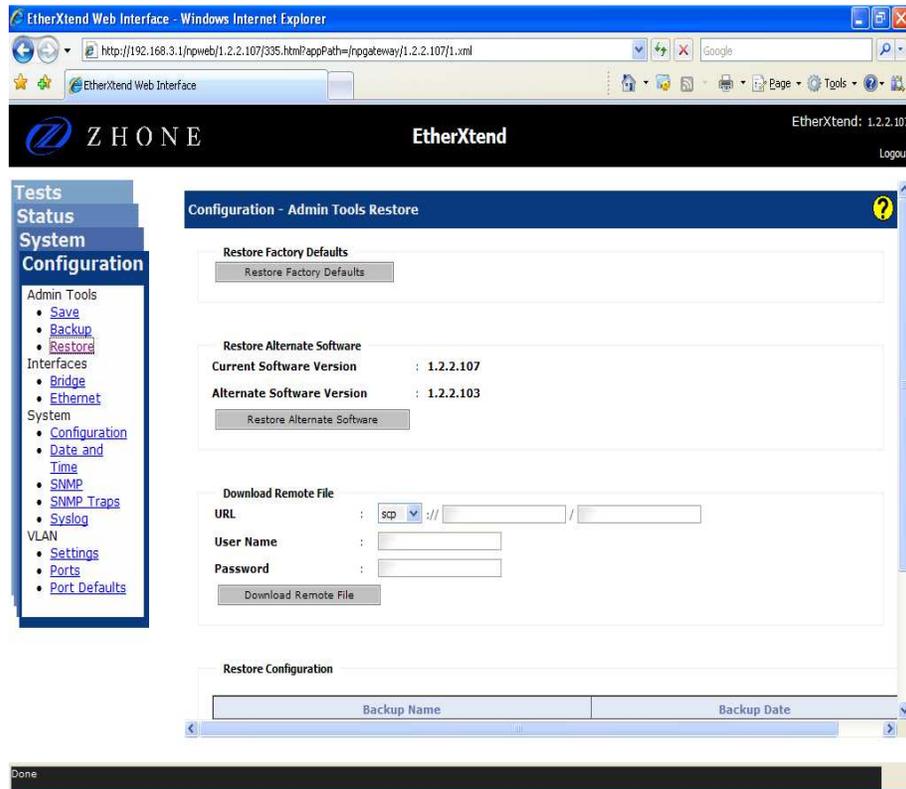
> ✅ **Note:** After loading new firmware you may have to clear your web browser's cache. See **Clearing Web Browser Cache** below.

Clearing Web Browser Cache

There are two options for avoiding stale web pages after an upgrade. You can configure your web browser to load the new page for every page visit, or you can clear the web browser's cache. The following procedure is for Internet Explorer. If you are using another web browser there should be similar settings available.

Load New Page For Every Visit

1. From you web browser select Tools and then Internet Options.
2. From the General tab on the Browsing history section click Settings. Then select the "Every time I visit the web page" radio button

Clear Cache

1. From the web browser select Tools and then Internet Options.
2. In the Browsing history section click **Delete**. Then in the Temporary Internet Files section click **Delete files**

Contacting Global Service and Support

Contact Global Service and Support (GSS) if you have any questions about this or other Zhone products. Before contacting GSS, make sure you have the following information:

- Model number for the Zhone product you are using
- System configuration
- Software version running on the system
- Description of the issue

Technical Support

If you require assistance with the installation or operation of your product, or if you want to return a product for repair under warranty, contact GSS. The contact information is as follows:

E-mail	support@zhone.com
Telephone (North America)	877-ZHONE20
Telephone (International)	510-777-7133
Internet	www.zhone.com/support

If you purchased the product from an authorized dealer, distributor, Value Added Reseller (VAR), or other third part, contact that supplier for technical assistance and warranty support.

Service Requirements

If the product malfunctions, all repairs must be performed by the manufacturer or a Zhone-authorized agent. It is the responsibility of users requiring service to report the need for service to GSS.

Release History

Date Released	Release #	Notes
12/15/2009	1.3.1.114	Bug fix – config file backup using Web / CLI
8/12/2009	1.3.1.111	Added support for dynamic routing (BGP, RIP), minor bug fixes
4/16/2009	1.3.1.107	Initial R1.3.1 SW Release, with support for L3 features, extended SHDSL rates, misc bug fixes.
2/25/2009	1.2.2.123	Resolved Mozilla FireFox v3.06 compatibility issue.
12/4/2008	1.2.2.122	Bug fixes as documented in the Release Notes, plus support for SNMP-initiated SW Upgrades, and LAN Port Status follows EFM Bond Group Status.
7/9/2008	1.2.2.115	Bug fixes as documented in Release Notes, plus support for SHDSL CO mode for back-to-back configurations.
4/24/2008	1.2.2.107	New features: DHCP client, VLAN priorities, SNMP MIPB2, Traps, PING utility, FW bank switching.
2/10/2008	1.1.9	Bug Fixes, primarily related to SHDSL performance
12/12/2007	1.1.3	Initial Production Release