ZyXEL

A Powerful EMS Solution for Enterprise Networks

- Auto Discovery and Device Viewer
- Templates provisioning for efficient configuration
- Traffic/Performance monitoring and management
- Alarm and event management
- Batch Firmware Upgrade
- Feature-rich Layer2 and Layer3 configuration
- Tight access control and log management
- Allow up to10 concurrent users

Enterprise Network Element Management System

NETATLAS™ ENTERPRISE EMS

Benefits

Centralized Network Management Platform

To achieve greater business successes, networks must adapt well with ever-evolving applications and business environment. Stability and top service quality are the fundamental for daily business operation. As network size grows, it can be a challenge to maintain the network and react to possible network failures promptly. Especially when multiple switching devices are spread across different sub networks.

To simplify network management, ZyXEL NetAtlas™ Enterprise EMS (Element Management System) provides a centralized remote management platform that allows administrators to easily maintain and monitor each switch on the network from a single computer. This allows efficient network management and lightens the load off the administrators who can better use the time for other value-added tasks.

Intuitive Hassle-free Operation Interface

No more entering cryptic commands! With intuitive and user-friendly graphical user interface (GUI), NetAtlas™ Enterprise EMS polls network element status and presents the graphical topology in the Map Viewer. Furthermore, double-click an icon in the Device Viewer to see the front panel graphical view and get real-time element status updates.

Configuration templates reduces manual, repetitive configuration time. You can apply a template to multiple ports or devices. With template provisioning, configuration changes are just simple mouse clicks away.

Network Health Monitoring and Management

It is vital to monitor network traffic to be aware any abnormal activity. NetAtlas™ Enterprise EMS allows you to monitor network traffic and generate graphical report down to the port level. Detailed items such as TX/RX, Error packets, collision packets and packet size, etc. can be displayed for further analysis. In addition, event and alarm management tools can issue SNMP trap and log the event in detail for prompt alert. Event logs are displayed in different colors to indicate the event severity level. Actions can be triggered by trap automatically without manual initiation; thus leaves flexibility and convenience to network managers.

## Complete Screen-Based Network Management

With NetAtlas™ Enterprise EMS, network maintenance is just a few simple mouse clicks away. Multi-site network operation and maintenance become easier than ever before. You can remotely perform general device maintenance (such as firmware upgrade and configuration file backup/restore) on more than one device on the network. With complete Layer2 switching, Layer3 IP routing, and system management features, efficient device monitoring and configuration allow for better network quality and can be cost-effective.

Strict Secure Access Management

Tight access control is essential for a secure network. In the NetAtlas™ Enterpise EMS, access to configuration screens and/or status screens are strictly based on user name, password, user's computer IP address and user account category. The three user categories give login accounts different administration authority. The NetAtlass™ Enterprise EMS allows up to 10 users to log in at a time. Information such as the user ID, user group, IP address, configuration actions and time is logged for security reasons. So network managers know who logged in, when and did what.
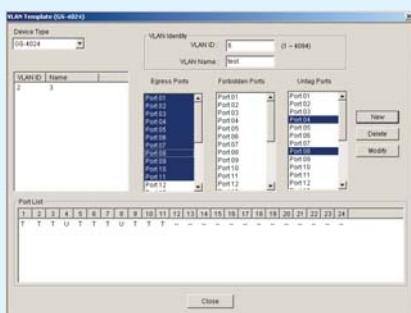
Features at a Glance

Map Viewer/Device Viewer
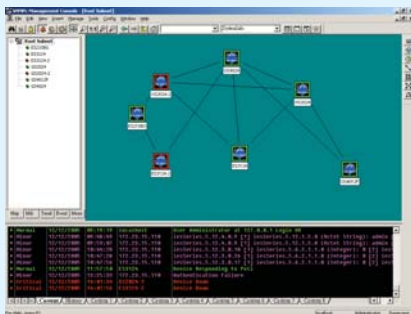
- **Tree View**

  Shown in a tree structure of up three layers: root map node, submap node, device node.
- **Device View**
  - Add/delete a submap or device node and update the device topology.
  - Query the status of a managed network element.

Template Provisioning

- To save configuration templates for future use.
- Templates can apply on multiple network elements or device ports.

Performance Management
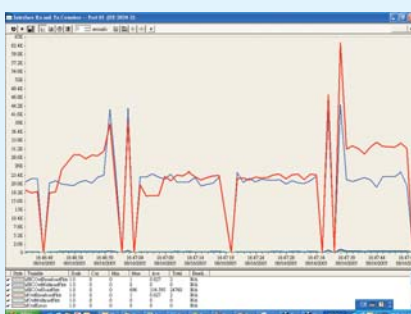
- RX Packets Counters (RX Packets, Multicast, Broadcast, Pause and Control)
- TX Packet Counters (TX Packet, Multicast, Broadcast and Pause)
- TX Collision Counters (Single, Multiple, Excessive and Late)
- Error Pkts counters (RX CRC, Length and Runt)
- Distribution counters (64, 65~127, 128~255, 256~511, 512~1023, 1024~1518 Kbytes and Giant)

Alarm/Event Management
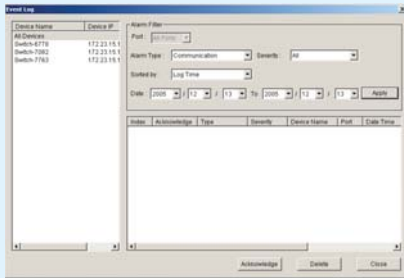
- Event category: Communication Alarm, Equipment Alarm and QoS Alarm.
- Event severity: Critical, Major, Minor, Warning, and Normal.
- Event source: IP address of managed device and port ID
- Time Stamp: time at which the event is generated
- Problem: A description about the event

System Management

- Display basic system information
- SNMP parameter configuration
- Access Control
- Remote management
- Time server setting
- Firmware upgrade
- Firmware upgrade
- Device reset
- Network element configuration backup and restore (automatic or manual), Load Factory Default
- Loopback Test
- 802.1d (MAC Table, ARP Table)

L2/L3 Feature Configuration
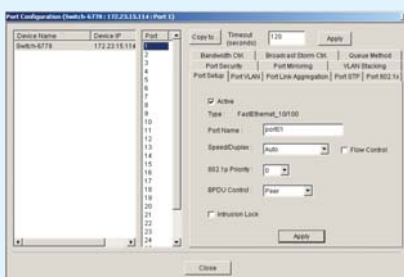
- **Port level setting**
  Port Setup, VLAN Port Configuration, LACP, STP, 802.1x, Port Security, Mirror Ports, VLAN Stacking, Bandwidth Control, Broadcast Storm Control, Query Method
- **System wide Layer 2 settings**
  VLAN Type, Enable/Disable IGMP snooping, Enable/Disable Bridge control protocol transparency, MAC Address Learning, GARP Timer, Priority Queue Assignment, STP/RSTP configuration, Enable/Disable Bandwidth control, Enable/Disable Broadcast storm control, Enable/Disable Mirroring, Enable/Disable LACP, System Priority, Group T1~T6, Enable/Disable 802.1x, RADIUS Setting, Enable/Disable Port Security, Queuing Method, VLAN Stacking, Static VLAN configuration, DHCP Relay, Classifier, Policy Rule, DiffServ
- **System wide Layer 3 settings**
  Static Routing, IP Setup, RIP, OSPF, IGMP, DVMRP, IP Multicast, VRRP

Secure management
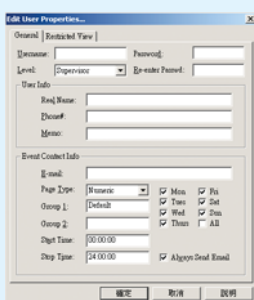
- **Access control**
  3 levels System-Administrator, Operator-Read/Write and Operator-Read Only.
- **Access Log Management**
  Log includes user name, access level, real user name, phone number, e-mail address and additional information.
- **Log Filter**
  Track and locate access by filtering logs (User Name, access level, …, e-mail, etc)

Network Protocol and Standard

- RFC 1157 SNMP
- RFC 1905 SNMPv2c
- RFC 1213 MIB II
- RFC 1493 Bridge MIB
- RFC 2674 P-Bridge MIB, Q-Bridge MIB
- RFC 3621 POWER-ETHERNET-MIB
- RFC 1757 RMON
- RFC 1643 Ethernet MIB
- RFC 2233 ifVHCPacketGroup

Specifications

System Requirements

- Hardware
  - CPU: Intel Pentium 4, 1.6 GHz (or above)
  - 1 GB RAM (or above)
  - 10 GB Hard Disk (or above)
  - 1024 x 768 Graphical Adapter (or above)
  - 10/100 Mbps Ethernet Adaptor

- Software
  - Windows 2000, Windows 2003 Server or Windows XP
  - CastleRock's SNMPc Network Manager
  - Database System: PostgreSQL 8.0

For more product information, visit us on the web www.ZyXEL.com

65-100-102409G   01/06