



APPLICATION NOTE

Cyber Security RFL eXmux[®] 3500 IP Access Multiplexer

The RFL eXmux 3500 is a hardened IP Access Multiplexer engineered for mission critical infrastructures. The eXmux 3500 will seamlessly transport voice, serial, video and Ethernet data communications over Ethernet/IP or MPLS networks. The eXmux 3500 is a Layer 2 device with an integrated managed Ethernet switch which allows the eXmux 3500 to be used either in a private network with other eXmux 3500's or as part of a larger Ethernet/IP/MPLS network. Both fiber (using SFPs) and RJ-45 connections are available for the eXmux 3500; uplink speeds of up to a Gigabit are possible.

This application note describes the implementation of cyber security features in an Ethernet network containing eXmux multiplexers. Once implemented, these features meet or exceed all NERC-CIP requirements.

Cyber Security in an eXmux 3500 Ethernet LAN

The Ethernet LAN has many security weaknesses and can face attacks both internally or externally, these attacks can be unintentional or intentional in nature. The primary weakness with Ethernet is that it is a broadcast system, which means every message sent out by any host on a segment of Ethernet medium reaches all parts of that segment and potentially could be read by any host on the segment. The security risks within an Ethernet network can be classified into several categories as shown below:

- a. **Data leakage** - a freeware packet sniffer; e.g. Wireshark could intercept data streams allowing access to confidential and critical data.
- b. **Data loss** - a wrongly configured router/switch could send your unprotected data to an unintended destination.
- c. **Data theft** - an intruder can launch an attack from a connected Layer 2 WAN to get access to your data.

Thus, measures must be taken to ensure the communications over the Ethernet LAN are secured to minimize the number of successful cyber security attacks; e.g. DOS (Denial of Service), MIM (Man-in-Middle), Broadcast/Multicast/Unicast Ethernet Storms.

Designed into the eXmux 3500 IP Access Multiplexer are cyber security features meeting NERC-CIP requirements and ways of securing the same if installed in an Ethernet network.

Physical Security:

In addition to physically preventing unauthorized access (Company Policies) into an equipment facility, it also makes sense to secure a backup copy of device configurations each time a change is made. The eXmux 3500 can generate back-up configurations both soft (XML format) and hard (pdf, word, excel format) copies. This is not only a security measure but also a recovery method if a device should fail and require replacement.

Port Security:

Enable / Disable Ports - the eXmux 3500 integrated managed switch can have its ports administratively enabled or disabled. Having ports disabled will prevent access by an unauthorized device attempting to insert or intercept network traffic.

MAC-based Port Security

The eXmux 3500 integrated managed switch can administratively configure a port-based hardware address (MAC address). This management feature will deny access to a non-authorized device. Service is only provided for specific MAC address/addresses and prevents a non-configured MAC address communication via that port. This can also be used as a precaution against connecting more than the allotted number of workstations or devices to a port.

Virtual LAN

The eXmux 3500 integrated managed switch provides the ability to logically segregate traffic between predefined ports. This can effectively prevent snooping and sniffing on the network. It also reduces network traffic by limiting messages to only part (within VLAN/Broadcast domain) of the network on which they are needed to improve the efficiency of the whole network.

In the eXmux 3500, the VLAN can effectively separate traffic from other devices; e.g. IP Phone, IP Camera, LAN extension from PLC or SCADA, Current Differential Relay, Real-Time service devices. As these devices may not normally communicate with each other, separating them with a VLAN will allow the two networks to co-exist on the same switch.

The eXmux 3500 supports both Port-Based VLAN and IEEE 802.1Q Tagged-Based VLAN.

User Access Management System

The eXmux 3500 uses a multi-level user access mechanism to ensure appropriate access for each added user and secures the unit against unauthorized configuration. The user access management system is embedded in the unit to prevent intruders from recovering user ID's and passwords in a case where a laptop is stolen.

SNMPv3

The eXmux 3500 Network Management System uses the latest SNMPv3 for authentication and encryption each time the unit is accessed preventing unauthorized access and data theft.

Forward Unknown Packet

The eXmux 3500 integrated managed switch supports “disabling forwarding of unknown unicast frames” feature. If administratively disabled in the eXmux CPU and LAN ports, the switch will not forward any unicast frames not in the MAC-Address Table. This feature prevents unknown traffic inadvertently or intentionally being injected; e.g. Ethernet Random/Unicast Storm (DOS Attack) being propagated in the switch that will degrade the switch performance and ultimately make the switch inoperable and cause a network meltdown.

Rate Limiting

The eXmux 3500 integrated managed switch supports rate limiting for broadcast and multicast traffic. If administratively configured the rate of broadcast and multicast traffic is limited to the configured percentage of the ports speed. This prevents ports from accepting excessive broadcast and multicast traffic in the case of an inadvertent or legitimate attack; e.g. Broadcast and Multicast Storms in the network.

Contact RFL Electronics at 973-334-3100 for further assistance.