

ATX LAN Switch
ATX User's Guide Addendum
For Release 3.2

9032020

CABLETRON
SYSTEMS

The Complete Networking Solution™

A.1 INTRODUCTION

The ATX LAN Switch Release 3.2 provides the ATX platform with a number of new features. These features include:

- Virtual Workgroups - This feature allows you to create broadcast domains to enhance network performance.
- Local and Remote Port Mirroring - This feature allows you to designate a local or remote ATX port for diagnostics.
- Unique Trap IDs - This feature provides for unique Trap IDs that provide detailed information about traps.
- IPX Routing over Source Route - This feature gives the ATX the ability to cache RIF information when a source routed IPX frame needs to be routed to a transparent network.
- Trace Route and PING - These features allow the ATX to perform trace route and ping functions.
- Event Logging - This feature allows the ATX to display events, filter events, and send events as traps to SNMP managers.

In addition to these features for the ATX, a translation enhancement was made to the Token Ring Module for the ATX, which adds the StripRif ALL parameter to the StripRif protocol set.

A.2 ATX LAN SWITCH WORKGROUPS

A.2.1 Overview

Virtual workgroups allow you the flexibility to control broadcasts in the network. By reducing broadcasts throughout the network, it preserves network bandwidth for important user data and frees up valuable end station processing. By defining virtual workgroups, broadcasts will only be seen by other end stations within the same virtual workgroup. With the functionality to define workgroups by port grouping, IP network address and/or IPX network number, a station can be part of multiple workgroups based on their location and protocol.

Each workgroup can be defined by port, IP network address and/or IPX network number (see command format below). A total of 100 virtual workgroups can be defined on each ATX LAN Switch. The ATX LAN Switch can route between IP workgroups but all other workgroups will need an external router (See Workgroup to Workgroup Communication).

A.2.2 Management

LCM

The LCM command format is:

workgroup **name ports type info**

name 1-16 characters; identifies the workgroup

ports range of ports separated by (-) or (,)

type ALL or IP or IPX

info ip address\mask or ipx network number (hex or decimal); NA for type ALL

Examples:

```
workgroup eng 3-7 all
workgroup sales 10,11,12,13 ip 134.141.141.0 255.255.255.0
workgroup mktg 11,12-18 ipx 0x1234
```

Classification

When a broadcast packet is received on a workgroup defined port, the packet is classified as being IP(IP, ARP or RARP), IPX(SAP, RIP, SPX or NCP) or ALL (any protocol type). Based on this classification, the broadcast will only be forwarded to the ports within that workgroup. If there is no workgroup defined for the receiving port the broadcast is forwarded out all other ports regardless of the exiting port's workgroup configuration.

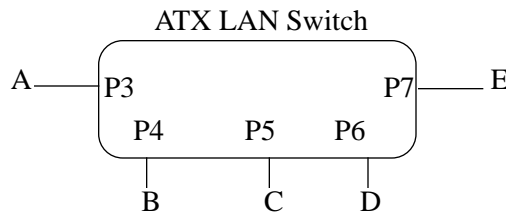
Workgroup of Type ALL

When a broadcast of any protocol type is received by a port with only an ALL workgroup defined, the packet will be broadcast out every port in the ALL workgroup (see Example #1).

Example #1

Defined workgroups:

```
workgroup red 3-5 ALL
workgroup blue 5-6 ALL
```



- Broadcast from A will only be seen by B and C
- Broadcast from B will only be seen by A and C
- Broadcast from C will only be seen by A, B and D
- Broadcast from D will only be seen by C
- Broadcast from E will be seen by all forwarding ports

Workgroup of Type IP

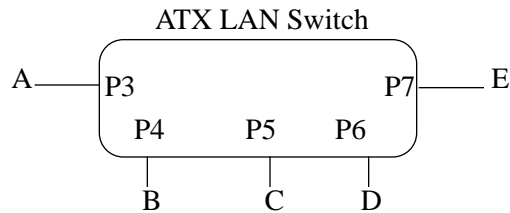
The destination IP address within the broadcast packet is used to determine the workgroup (see Example #2). This IP address is matched against the IP network address and IP network mask defined in the workgroup for the receiving port. If the destination IP address does not match the IP workgroup defined the packet is forwarded out all other ports. If the destination IP address is a broadcast address, the source IP address is used to determine the correct workgroup. If there is no destination IP address(i.e. RARP), then the packet is forwarded out all of the IP workgroups for the receiving port. If the packet is an IP multicast but not broadcast (i.e. class D address) the workgroups are ignored and the normal forwarding criteria is applied.

ATX LAN SWITCH WORKGROUPS

Example #2

Defined workgroups:

workgroup red 3-5 All
workgroup blue 5-6 IP 100.100.1.0 255.255.255.0
workgroup green 6-7 IP 100.100.2.0 255.255.255.0



An ARP from:

A or B destined for 100.100.1.xxx will only be seen by A, B and C

A or B destined for 100.100.2.xxx will only be seen by A, B and C

A or B destined for 100.100.3.xxx will only be seen by A, B and C

C destined for 100.100.1.xxx will only be seen by D

C destined for 100.100.2.xxx will be seen by all forwarding ports

C destined for 100.100.3.xxx will be seen by all forwarding ports

D destined for 100.100.1.xxx will only be seen by C

D destined for 100.100.2.xxx will only be seen by E

D destined for 100.100.3.xxx will be seen by all forwarding ports

E destined for 100.100.1.xxx will be seen by all forwarding ports

E destined for 100.100.2.xxx will only be seen by D

E destined for 100.100.3.xxx will be seen by all forwarding ports

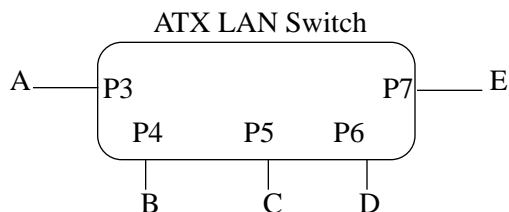
Workgroup of Type IPX

To determine the workgroup of an IPX broadcast the destination IPX network number is used (see Example #3). If the destination IPX network number is zero, the packet is forwarded out all of the IPX workgroups for the receiving port. If the broadcast has a non-zero IPX network number, there are a few possibilities. The IPX workgroup with the same IPX network number is used. If the destination IPX network number does not match the workgroup defined and a default IPX workgroup (IPX network number 0) is defined the that workgroup is used (see Example #4). If destination IPX network number does not match the defined workgroup and there is no default IPX workgroup, the packet is forwarded out all other forwarding ports.

Example #3

Defined workgroups:

- workgroup red 3-5 all
- workgroup blue 5-6 ipx 0x1234
- workgroup green 7 ipx 0x999



A SAP from:

- A or B destined for the 0x1234 network will only be seen by A, B and C
- A or B destined for the 0x999 network will only be seen by A, B and C
- A or B destined for the 0x000 network will only be seen by A, B and C

- C destined for the 0x1234 network will only be seen by D
- C destined for the 0x999 network will be seen by all forwarding ports
- C destined for the 0x000 network will only be seen by D

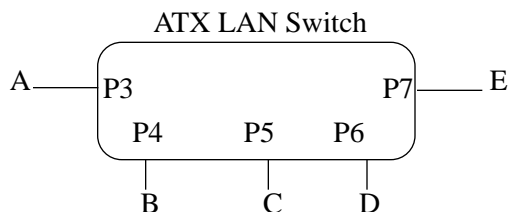
- D destined for the 0x1234 network will only be seen by C
- D destined for the 0x999 network will be seen by all forwarding ports
- D destined for the 0x000 network will only be seen by C

- E destined for the 0x1234 network will be seen by all forwarding ports
- E destined for the 0x999 network will stay local to E
- E destined for the 0x000 network will stay local to E

Example #4

Defined workgroups:

- workgroup red 3-5 all
- workgroup blue 5,6,7 ipx 0
- workgroup green 7 ipx 0x999



A SAP from:

- A or B destined for the 0x1234 network will only be seen by A, B and C
- A or B destined for the 0x999 network will only be seen by A, B and C
- A or B destined for the 0x000 network will only be seen by A, B and C

ATX LAN SWITCH WORKGROUPS

C destined for the 0x1234 network will only be seen by D and E
C destined for the 0x999 network will only be seen by D and E
C destined for the 0x000 network will only be seen by D and E

D destined for the 0x1234 network will only be seen by C and E
D destined for the 0x999 network will only be seen by C and E
D destined for the 0x000 network will only be seen by C and E

E destined for the 0x1234 network will only be seen by C and D
E destined for the 0x999 network will stay local to E
E destined for the 0x000 network will only be seen by C and D

Same Port in Multiple Workgroups

In the event that a port is defined in workgroups of ALL and IP or IPX, the forwarding criteria for IP packets or IPX packets will be based on IP workgroup or IPX workgroup respectively. If the IP\IPX broadcast does not match the IP or IPX workgroup the packet will be forwarded out every other port. It will NOT revert back to the criteria set for the ALL workgroup defined on that port. For instance, in Example #2 port 5 is a member of two workgroups, RED of type ALL and BLUE of type IP. When station C sends an IP packet destined for any network other than 100.100.1.0 the broadcast is forwarded out every other forwarding port. Even though port 5 is a member of two workgroups it does not fall back to the RED workgroup's criteria.

Workgroup to Workgroup Communication

This type of communication can only be achieved by routing. With the ATX LAN Switch having the ability to route IP packets, it will route between IP workgroups (See Example #5). However, the ATX LAN Switch will NOT be able to route between IPX workgroups. The reason is that the ATX LAN Switch does not have the ability to enable IPX routing on multiple ports with the SAME IPX network number. Therefore, communication between IPX and ALL workgroups can only be achieved via an external router.

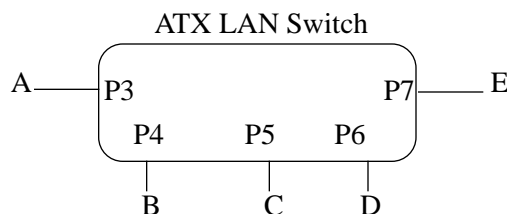
Example #5

Defined workgroups:

```
workgroup red 3-5 ip 134.141.100.0 255.255.255.0  
workgroup blue 6-7 ip 134.141.200.0 255.255.255.0
```

IP Configuration with IP enabled on all ports:

```
ipaddress P3 134.141.100.3 255.255.255.0  
ipaddress P4 134.141.100.4 255.255.255.0  
ipaddress P5 134.141.100.5 255.255.255.0  
ipaddress P6 134.141.200.6 255.255.255.0  
ipaddress P7 134.141.200.7 255.255.255.0
```



Results:

1. Stations A, B and C IP communication will be switched between ports 3, 4 and 5 since they are on the same subnet of 100.
2. Stations D and E IP communication will be switched between ports 6 and 7.
3. If A, B or C needs to communicate with D or E and vice versa. The receiving port will have the ability to route the packet to the 200 or 100 subnet respectively since routing is enabled on all ports.

A.3 ATX LOCAL AND REMOTE PORT MIRRORING

A.3.1 Overview

Port mirroring allows the ATX LAN Switch to redirect network traffic (excluding MAC layer errors) from one or more ports to any other port, in effect “mirroring” all network traffic to a selected port. This feature allows customers who have existing investments in external analyzers, external RMON probes, or devices like Network General's Distributed Sniffer System to continue to receive expert analysis and packet decode functions in a switched environment -- simply use the port mirroring function to mirror switched traffic to the designated “diagnostic” port to which the analyzer is attached.

The ATX LAN Switch supports local and remote port mirroring. Local port mirroring is when the diagnostic port is on the same ATX as the mirrored ports. Remote port mirroring is when the diagnostic port is on a different or remote ATX from the mirrored ports. The mirrored ports have to be either local or remote to the diagnostic port, not both. In the case of remote port mirroring, the traffic from the mirrored ports is encapsulated into an IP packet and sent to the IP destination defined (the diagnostic port).

A.3.2 Management

LCM

The LCM command format for Local Port Mirroring is:

mirror port-range off

port-range range of mirrored ports
off to turn local port mirroring off on the ports specified

mirror port-range to port# oversize

port-range range of mirrored ports
port# the diagnostic port on the local ATX
oversize discard or truncate; what to do with oversized packets

The LCM command format for Remote Port Mirroring is:

Local ATX (in reference to the diagnostic port)

mirror remote off
off to turn remote port mirroring off

ATX Local and Remote Port Mirroring

mirror remote to **port# oversized**

port# the diagnostic port on the local ATX

oversized discard or truncate; what to do with oversized packets

Remote ATX (in reference to the diagnostic port)

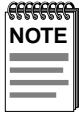
mirror **port-range off**

off to turn remote port mirroring off

mirror **port-range to Ipaddr**

port-range range of mirrored ports on remote ATX

Ipaddr ip address of the local ATX where the diagnostic port resides



Both ATX LAN Switch's have to have port mirroring turned off in order to fully disable the remote port mirroring function.

Types of Media and Framing

Mirrored and diagnostic ports have no restrictions and can be any of the ATX LAN Switch's interfaces, Token Ring, Ethernet, Fast Ethernet or FDDI. However, it is recommended that the diagnostic port and mirrored ports are of the same media type and framing. This is because in an intermixed mode, due to the differences in the physical layers, mirrored packets may be translated or dropped. For example, when an 802.5 packet is mirrored out to an 802.3 interface, the MAC addresses are translated (big endian to little endian) and the length field is added to the original frame. Furthermore, mirroring traffic of a higher speed interface out to a lower speed interface may impose a strain on performance (e.g. capturing FDDI traffics to a 4 Mbps Token Ring). When the size of the mirrored packet exceeds the size of the maximum transport unit (MTU) of the diagnostic port, the packet is labeled as oversized. As an option for local mirroring in an intermixed mode, the ATX can be configured to truncate or discard oversized packets.

Packet Capturing and Mirroring

The mirroring of network traffic is performed by the ATX LAN Switch software, and the mirror image reflects the ATX LAN Switch internal representation of the packets. Certain physical layer information (such as Access Control and Frame Control in 802.5 frames) will not be available. The difference in the physical layers are minor, and should not impair the normal usage of the port mirroring as it is mostly used in MAC and network layers.

The ATX LAN Switch mirror software attempts to minimize any differences between the internal and external formats when the frame is mirrored out the diagnostic port. Other than the possible framing translation, MAC layer should have only minor or no differences between the mirrored image and the raw frame on the wire. On the network layer, there should be no alteration. For example, when an inbound routed packet is mirrored, the image reflects the packet prior to any changes made by the ATX LAN Switch routing software.

The ATX LAN Switch mirror software maintains the original packet ordering of bridging frames between the inbound and outbound interfaces. The bridging packets include the Transparent, Source Routed and Transparent Source Routed frames. Network layer routing traffic is not subject to this requirement, and the sequence of routed packets may occasionally be out of order (as in the cases without port mirroring).

Mirrored Filters

The ATX also allows you -- via the existing port filtering feature (Chapter 5 in the ATX LAN Switch User's Guide)-- to establish "mirror filters" which can help reduce the amount of traffic seen by the diagnostic port. Using a "mirror filter," you can restrict the amount of monitored traffic by filtering inbound or outbound packets according to source and destination addresses, packet types, frame protocols and offsets within the data field.

In port filters, there are currently two types you can select from: Entry and Exit. With the addition of port mirroring, there are now four types: Entry, Exit, PMEntry and PMExit. PMEntry applies to any packet entering the port and PMExit is any packet leaving the port. See Configuration Examples for implementation. The rest of the parameters for setting up filters are the exact same independent of what the type is.

There are two major differences between mirror filter and packet filter:

- A mirrored filter has the exact opposite affect as a port filter. Mirrored filters will pass the traffic matching the filter rather than being blocked as in packet filtering.
- Both inbound packets to the ATX and outbound packets generated by the ATX are subject to the mirror filtering.

Example #1: LOCAL Port Mirroring

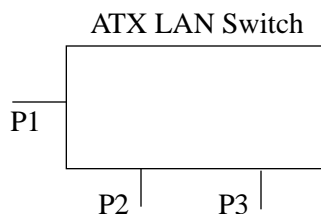
Port 1 is the diagnostic port where the analyzer resides

Ports 2 and 3 are the mirrored ports

mirror 2-3 to 1 discard

or

mirror 2-3 to 1 truncate



Mirror Filters with LOCAL Port Mirroring:

Desired: analyze IP traffic from station A (on P2) to station B (on P3) and vice versa

Implementation: add a PMEntry and PMExit filter to ports 2 and 3 with Protocol Type of 800(type IP in hex).

The reason for a PMEntry and PMExit filter is when A and B communicate there is communication both ways, i.e. IP packets are transmitted and received by P2.

Example #2: REMOTE Port Mirroring

Port 1 on ATX #1 is the diagnostic port where the analyzer resides

Ports 2 on ATX #2 is the mirrored port

Port 5 on ATX #1 has an ip address of 134.141.100.1

Port 4 on ATX #2 has an ip address of 134.141.100.2

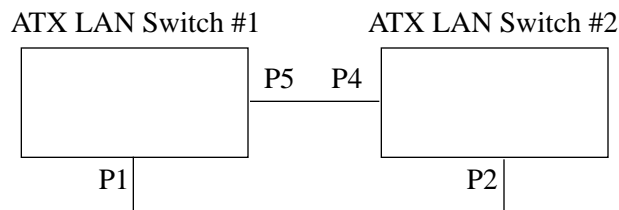
(P4 has to have an ip address assigned so ATX #2 will have an ip to ARP with)

Config on ATX #1

mirror remote to 1 discard

or

mirror remote to 1 truncate



Config on ATX #2

mirror remote 2 to 134.141.100.1

Mirror Filters with REMOTE Port Mirroring:

Desired: to see packets from station A (on P2) only

Implementation: add a PEntry filter to port 2 on ATX #2 with station A's MAC address as the source address in the filter.

A.4 ATX UNIQUE TRAP IDS

The new trap mechanism allows a SNMP Manager (Spectrum Element Manager, Spectrum) to have more control over SNMP Traps. Each trap is given a unique Trap ID, which gives detailed information about the trap and why it was sent. This also gives you the ability to select the traps you want generated and the traps you want to suppress.



With Release 3.2 of the ATX LAN Switch, the following traps replace all traps in previous releases. This section of the addendum replaces section 6.2 of the ATX User's Guide

- Tempok (1) - Sent whenever the module's temperature transitions from too hot to okay, and vice versa.
- Writestatus (2) - Sent when a bank of Flash EPROM has been erased. If swdisWriteStatus indicates success, then the unit is ready to be downloaded with the new software.
- PortFunctions (3) - Sent whenever the current functional state (active protocols) of the port has changed.
- RxQueues (4) - Sent whenever the number of times that the port's receiver has stopped receiving packets due to buffer space shortages has exceeded the port's limit.
- TxStormFlag (5) - Sent whenever multicast storm protection has been invoked for the port.

- TxCongests (6) - Sent whenever packets destined for the unit itself were discarded due to lack of buffer space.
- filterThresh (7) - Sent whenever usage of a port's combination filter has exceeded the filter's limits.
- debugStringId (8) - Send whenever the unit has a debug text string to be displayed. The text strings are sent in a stream-like fashion.
- IpbkOperation (9) - Send whenever the unit has finished a loop back test, or a loop back error has been detected.
- trunkState (10) - A trunking state change transition has occurred. The possible transitions are:
 - CLOSED-ONEWAY
 - ONEWAY-PERTURBED
 - PERTURBED-JOINED
 - JOINED-HELDDOWN
 - CLOSED-HELDDOWN
 - ONEWAY-HELDDOWN
 - PERTURBED-HELDDOWN
- trunkBridgeAddr (11) - The associated trunking MAC address of the bridge ID of the remote bridge has changed.
- trunkIPAddr (12) - The associated trunking IP address of the remote bridge has changed.
- trunkError (13) - An error has occurred in trunking.
- trunkLinkOrdinal (14) - The port's index in the trunking group has changed.
- trunkLinkCount (15) - The number of ports in the trunking group has changed.
- diagUnitBooted (16) - The unit has booted.
- storageFailure (17) - Sent if the unit's Configuration EEPROM has failed. The unit will not be able to reboot, and must be returned to the factory.
- portCongested (18) - Sent whenever outbound congestion control has been invoked for the port.
- topChangeBegun (19) - The spanning tree topology has begun to change.
- topChangeEnd (20) - The spanning tree topology has stopped changing.
- ifErrors (21) - Sent whenever the number of hardware errors in received and transmitted packets has exceeded the port's limit.
- stRootID (22) - The spanning tree root bridge ID for the unit has changed.
- stRootCost (23) - The unit's spanning tree cost to the root bridge has changed.
- stRootPort (24) - The unit's spanning tree root port has changed.
- stMaxAge (25) - The unit's spanning tree maximum age has changed.
- stHelloTime (26) - The unit's spanning tree hello time has changed.
- stForwardDelay (27) - The unit's spanning tree forward delay time has changed.
- stDesigRoot (28) - The Root Bridge ID in received Spanning Tree Configuration BPDUs from the port has changed.

ATX Unique Trap IDs

- `stPortDesigBridge` (29) - The bridge ID of the spanning tree designated bridge of the LAN/WAN to which the port is attached has changed.
- `stPortDesigCost` (30) - The cost to the spanning tree root bridge from the designated port of the LAN/WAN to which the port is attached has changed.
- `stPortDesigPort` (31) - The port ID of the spanning tree designated port of the LAN/WAN to which the port is attached has changed.
- `stPortState` (32) - The spanning tree state of the port has changed.
- `fddimibSMTCFState` (200) - Sent whenever the FDDI port's CFM state has changed. The `fddimibPORTMACIndicated` (one or two instances, depending upon whether the FDDI connection is a SAS or a DAS) is also included.
- `fddimibMACUpstreamNbr` (201) - Sent whenever the FDDI port's upstream neighbor has changed.
- `configPowerAc1` (202) - Sent whenever the AC input to the unit's first power supply transitions from on to off, and vice versa.
- `configPowerAc2` (203) - Sent whenever the AC input to the unit's second power supply transitions from on to off, and vice versa.
- `configPowerDc1` (204) - Sent whenever the DC output of the unit's first power supply transitions from on to off, and vice versa.
- `configPowerDc2` (205) - Sent whenever the DC output of the unit's second power supply transitions from on to off, and vice versa.
- `configPowerPresent1` (206) - Sent whenever the presence of the unit's first power supply transitions from present to not present, and vice versa.
- `configPowerPresent2` (207) - Sent whenever the presence of the unit's second power supply transitions from present to not present, and vice versa.
- `sfddiShortAddressing` (208) - Sent whenever an FDDI packet is received (other than Claim/Beacon packets) with 16 bit MAC addresses.
- `sfddiSmtConditionsStatus` (209) - Sent whenever any of the conditions indicated by the value of the MIB variable `sfddiSmtConditions` has occurred.
- `sfddiSrfConditionsStatus` (210) - Sent whenever any of the conditions indicated by the value of the MIB variable `sfddiSrfConditions` has occurred.
- `sfddiSBFlag` (211) - Sent whenever the FDDI port's optical bypass becomes stuck, or un-stuck.
- `sfddiOBSFuseBad` (212) - Sent whenever the fuse to the FDDI port's optical bypass becomes bad, or switches from bad to good.
- `sfddiStationState` (213) - Sent whenever the FDDI port's Station State has changed.
- `swanActualSpeed` (214) - The actual line speed of the WAN port has changed.
- `fddismtUpstreamRsp` (215) - The upstream neighbor of the requested FDDI device has been learned.
- `hwFatalErr` (216) - Sent whenever a module dies unexpectedly. Since death of the ME or TURBO causes the unit to reboot, a `hwFatalErr` alarm for such a module will never occur.
- `hwDiagModuleFailed` (217) - A module has failed diagnostics.

- hwDiagModMismatch (218) - The type of a module does not match its defined type.
- hwDiagPortMismatch (219) - A type of a port does not match its defined type.
- hwDiagPortStatus (220) - A port of this module has a bad status.
- sfddiDup (221) - Duplicate MAC address found on FDDI ring.
- slog (222) - An event logging message has been generated.
- atRtOvflw (223) - Appletalk routing table overflow.
- atArpOvflw (224) - Appletalk ARP table overflow.
- sipxRtOvflw (225) - IPX routing table overflow.
- sipxSvcOvflw (226) - IPX service table overflow.
- atPortsSameSeg (227) - Appletalk- two ports on same segment.
- iprouteTblOvflw (228) - Routing table overflow.
- arpTblOvflw (229) - ARP table overflow.
- eePromReconfig (230) - The unit's EEPROM has been reconfigured.
- maxNextHop (231) - Maximum number of next hops reached.
- ripBadNet (232) - RIP received with wrong local network number.
- routeAgeOut (233) - Route aged out.
- sipxSAPAgeOut (234) - IPX service aged out.
- ipUnknownDest (235) - IP packet to unknown destination received by host.
- pppLinkOpen (236) - PPP link to open
- pppLinkClose (237) - PPP link to close.
- pppNeighborIpAddrChange (238) - PPP neighbor IP address change.
- dupIP (239) - Duplicate IP address detected.

A.5 IPX WITH TOKEN RING SOURCE ROUTING

A.5.1 Overview

Token ring networks often interconnect with source routing (SR) bridges. Although the source routing is a MAC layer feature, all packets must provide the correct source route information to the bridges in order to traverse the networks. To successfully and efficiently route network traffic in such environments, routers need to have the capability to explore and select routes, cache and age route information, and construct network packets with the proper route information. Support of IPX over source routing (IPX SR) enables the ATX LAN switch to achieve this capability and route IPX packets through the SR bridges.



This feature is valid only for Token Ring and FDDI ports.

A.5.2 LCM Support

Command **ipxroute** is expanded with additional option **sr** to support IPX SR on token ring and FDDI ports. Option **sr** implies **on**. The explorer type and cache aging time can be configured using SNMP with the MIB variables. Refer to the ATX MIB Reference Guide Addendum (902021) for the specific MIB variables. The following is the LCM command format:

```
ipxroute [PORT-RANGE [{off | on | sr}]]
```

A.6 PING AND TRACE ROUTE ON THE ATX

Implementations of ping and trace route have been added to version 3.2 of the ATX firmware, giving the ATX the ability to originate ping and trace route requests from the ATX. These requests can be started from LCM or from SNMP (refer to the MIB Reference addendum for SNMP information). Results for requests originating from LCM are printed out on the LCM console.

A.6.1 Ping

The LCM command for ping is as follows:

```
ping [-rvsxmqw] host_IP [data_size [count]]
```

-r = record route

-v = verbose

-s = send one packet per second continuously

-x = send packets continuously without delay

A.6.2 Trace Route

The LCM command for trace route is as follows:

```
tracert [-m max_ttl] [-q nqueries] [-w wait] host_IP [data_size]
```

A.7 EVENT LOGGING ON THE ATX

Version 3.2 of the ATX firmware provides an Event Log feature to assist in troubleshooting problems on the network. This allows you to turn on logging of some class of networking event, and use the output of the log to be analyzed to assist in diagnosing the problem.

A.7.1 Features of ATX Event Logging

ATX Event logging includes the following features:

- Separate enabling flags for each event or class of events. The enabling flags are symbolic and are thus easily used in troubleshooting the network.
- Continuous monitoring of events is supported.
- Logging entries are easy to add and delete from the source code.
- The framework is integrated with SNMP and easily fits into the anticipated fault/alarm restructuring.

A.7.2 Management from LCM

The Event Log is established using the LCM. New LCM commands have been added in order to manage the event logging. There are 3 new LCM commands:

eventfilter

The LCM command format is:

```
eventfilter [clear | [overwrite | stopwhenfull] [add|delete][allentries ! [filter_name[,filter_name]*] ]]
```

Examples-

eventfilter	-- prints out current eventfilter values
eventfilter arp	-- replaces current eventfilter with arp
eventfilter delete arp_request_timeout	-- deletes entries from current eventfilter
eventfilter allentries	-- turns on all entries in event filter
eventfilter clear	-- turns off event logging
eventfilter stopwhenfull arp	-- replace current eventfilter with arp, and stop -- keeping logging entries when the buffer gets full
eventfilter overwrite	-- keep current eventfilter value, overwrite buffer entries if necessary

The default event filter will be empty, meaning that no event logging entries will be kept. If the eventfilter command is issued without any options, the current eventfilter will be displayed. If the eventfilter command is issued without either an “add” or “delete” option, the entire eventfilter will be replaced. An eventfilter command issued with a “clear” option will turn off event logging. The event logging entries will be kept in a circular buffer, and the logging entries will be overwritten if necessary. If the “stopwhenfull” option is given, the logging mechanism will cease entering logging entries into the event logging queue once it is full. By default, entries will be overwritten.

eventtrap

The LCM command format is:

```
eventtrap on|off
```

The eventtrap command will be used to determine whether event logging entries will trigger SNMP traps. By default, events generating SNMP traps will not be enabled.

eventdisplay

The LCM command format is:

```
eventdisplay [continuous ]
```

The eventdisplay LCM command will get event logging entries that are currently in the event logging queue.

The eventdisplay command will output continuous event log entries, if specified, or the number of entries currently in the event logging queue. The continuous display of the event logging information to the console will be turned off by a Control-C.

A.8 TRANSLATION ENHANCEMENT (STRIPRIF ALL)

A new translation parameter was added to the ATX Token Ring module to complete the StripRif protocol set: StripRif ALL. The current set of protocols that StripRif is used for are: IPX, ARP, NetBIOS and SNA. This feature was added to handle all other protocols that need the RIF stripped before being transmitted out other ATX LAN Switch ports (for example, protocols such as BootP and RIP).

The LCM command format is:

translate port# all [StripRif|passRif|passBoth]

