TN2-86400-434PS
Issue 5.0
October 2011

TN1U
SDH Multiplexer

86434 SERVICE UNIT / IP SERVICE UNIT

Technical Practice and Installation Manual

TN1U

SDH Multiplexer
Technical Practice and Installation Manual

TABLE OF CONTENTS

SECTION PAGE

1. INTRODUCTION.....6
Related Publication and Documentation Support.....6
Product Colour and Nomenclature.....6
Handling and Packing.....7
Revision History.....7

2. UNIT OVERVIEW.....8
Service Unit and IP Service Unit.....8
IP Service Unit (IPSU).....10
IPSU Operations.....12
Support Package.....13
SNMP Support.....14
VistaNET Server Function.....15

3. FRONT PANEL FEATURES.....17
LED Indications.....17
ACO button.....17
ACK button.....17
Craft Interface (C.I.) Jack.....18
Extractor.....19

4. UNIT DESCRIPTION.....20
Intra-Node Communication Channels.....21
SU/IPSU to STM-N Aggregate and SYNC Unit Communication.....21
STM-N Aggregate Unit to TIF Level Unit Communication.....21
TIF to Channel Unit Communication.....21
Intra-Ring Communication.....22
Ring-to-Ring Communications.....22
SU/IPSU-to-VistaNET Workstation Communications.....23
Communication Channels' Traffic.....23
TBOS Interface.....24

SECTION PAGE

IPSU's Ethernet Interface 25

5. INSTALLATION 26

Pre-installation 26
Shelf Position 26
Paddleboard Connections 28
Office Alarms 28
Power Monitor 28
Sync-Tie Connections 28
Ext Sync Unit Connection 30
Orderwire CBUS 31
NMS-Tie Connections 31
Rear Craft Interface 32
Modem Lockout Configuration 33
Ethernet Port on 86434-81 Paddleboard 34
Paddleboard Installation 34
Replacing a Service Unit in a system in-service 34
Installing MIB Files 35

6. CONFIGURATION 36

VistaNET Unit View Information 37
General Information 37
Context-Sensitive Help 37
Configure button 37
Undo button 37
Cancel button 38
Copy and Paste buttons 38
Status Tab 39
Service Unit / IP Service Unit 39
NMS 40
Alarm Summary 41
IPSU-Specific Info 42
Setup Tab 42
Overhead Allocation 42
Service Unit / IP Service Unit 44
Equipped Units 46
Network Setup 46
Date and Time Stamp 48
Software Version and Licensing 49

SECTION *PAGE*

TBOS Monitor Tab *50*
Network Element Display Sub-Tab *50*
TBOS Setup Sub-Tab *51*

7. MAINTENANCE and TROUBLESHOOTING 52
Context-Sensitive Help *52*
Alignment *52*
Troubleshooting *52*

8. NMS FEATURES 55
Features *55*
VistaNET Features *55*

9. SPECIFICATIONS 56

10. ORDERING INFORMATION 58
Equipment and Option Code List *58*

APPENDIX A 59
SNMP *59*
MIB *60*
SNMP Commands *61*

APPENDIX B 62
List of Figures *62*
List of Tables *62*

APPENDIX C 63
List of Acronyms *63*

1. INTRODUCTION

The 86434-02 Service Unit and 86434-03 IP Service Unit are two members of a family of common units in the Lentronics Multiplexers' digital transport/access systems (JungleMUX, TN1U and TN1Ue) designed specifically for the requirements of the utility (Power, Transportation, Pipelines, Oil & Gas, etc.) industry.

This manual explains how to operate, install and maintain the Service Unit and IP Service Unit. An overview of their operation is also included.

Engineering documentation includes EAS schematics for all unit circuitry.

Related Publication and Documentation Support

Additional information is provided in the *TN1U Technical Overview and Reference Manual* for system planning and engineering. The user may also find useful information in *Technical Practice and Installation Manuals* (TPIMs) for other TN1U units.

Customer inquiries for information contained in this manual should be directed to TN1U Product Line Management. GE Multilin appreciates notification of any possible errors or omissions contained herein.

Shipped with each purchased TN1U node is a Node Assignment Drawing (NAD), which provides necessary configuration details for the units and shelf location.

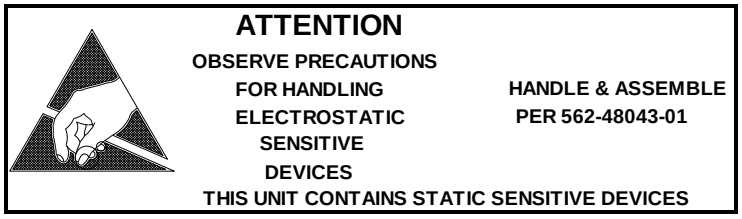
Product Colour and Nomenclature

The product line has undergone a transition to a new coloured package. To distinguish between legacy grey and new black, a "B" prefix is added to all black shelf and unit code numbers to identify the item colour. Note that there is no difference in the internal electronics and therefore the functioning of this equipment, whether it be grey or black. To simplify the information within this TPIM, all unit code numbers will be stated without any colour prefix. The ordering information (Section 10), however, does include the available colour options.

Handling and Packing

Equipment with Electrostatic Discharge Sensitive (ESDS) devices or components must be shipped in protective containers and necessary handling precautions observed otherwise all warranties, expressed or implied, will be considered null and void.

The following Electronic Industries Association (EIA) attention label appears on all GE Multilin EAS schematics and should be attached on all containers used for ESDS items to alert personnel that the contents requires special handling.



Revision History

Issue No.	Issue Date	Details of Change
1	June 2001	Document originated.
2	Mar 2002	General update.
3	Oct 2004	Added IP Service Unit. General update.
4	Jan 2005	General update.
5	Oct 2011	Updated to reflect IPSU with Linux OS and VistaNET 4.00+. Removed appendix with legacy TLCI software information. General update.

2. UNIT OVERVIEW

Service Unit and IP Service Unit

The 86434-02 Service Unit (SU) and 86434-03 IP Service Unit (IPSU) have the capabilities to monitor units at the TN1U node and to provide both Form-C Major and Minor office alarms.

Each SU/IPSU is equipped with alarm indicators, which summarize the alarms from the local node. These alarms are reported by two front panel red LEDs (for Major and Minor alarm conditions) whose states are also reflected on the respective Form-C contacts accessible through the rear-mounted interconnect paddleboard installed on the shelf backplane.

The SU/IPSU can be programmed to operate in Sentinel Alarm Mode, which allows enhanced operation of the on-board Minor and Major Form-C relays. If this mode is enabled, Form-C relays will reflect the alarm state of both local and remote nodes. By configuring the Sentinel Alarm Mode to “Ring” or “System”, the Form-C relays will activate when an alarm condition is encountered at any other node in the same ring or in the entire TN1U system respectively. Sentinel Alarm Mode is useful for high-level SCADA/Alarm gathering systems that use contact closure detection as a 'First Alert' functionality.

The SU/IPSU allows alarms to be sent to a TBOS (Telemetry Byte Oriented Serial) compatible system. The unit’s TBOS port provides visibility of any 16 Network Elements (TN1U nodes) in a TN1U system.

Connections to external equipment are made on a paddleboard installed on the shelf backplane. In a TN1U system, the SU can be used with either legacy 86434-80 paddleboard (discontinued in October 2005) or 86434-81 paddleboard (see Table 3: Equipment and Option Code List). The IPSU can be used with 86434-81 paddleboard only.

The SU/IPSU craft interface (a serial 9600-baud asynchronous RS-232 interface) available on the unit’s faceplate allows for local unit configuring and monitoring through a PC running VistaNET software. In addition, the SU/IPSU craft interface provides an NMS gateway between the TN1U network and a PC running VistaNET software, thus providing the VistaNET user with full NMS visibility of the network.

A VistaNET connection to the SU craft interface can be made through:

- the RJ-11 connector on the unit's faceplate (typically used for temporary hardwire connections), or
- the RJ-11 connector on 86434-8X paddleboard (typically used for permanent hardwire or modem connections), or
- the terminal block connector TB2 on 86434-8X paddleboard (typically used for permanent connections over Data-LS circuit).

The VistaNET functions relevant to monitoring and configuring the SU/IPSU are explained later in this manual. More information on VistaNET software is available in the *VistaNET User Guide*.

The SU/IPSU also provides the communication bus (CBUS format) for the 86471 Orderwire units and the 86474 4W VF Partyline units. Up to seven independent Orderwire and/or 4W VF Partyline systems are supported.

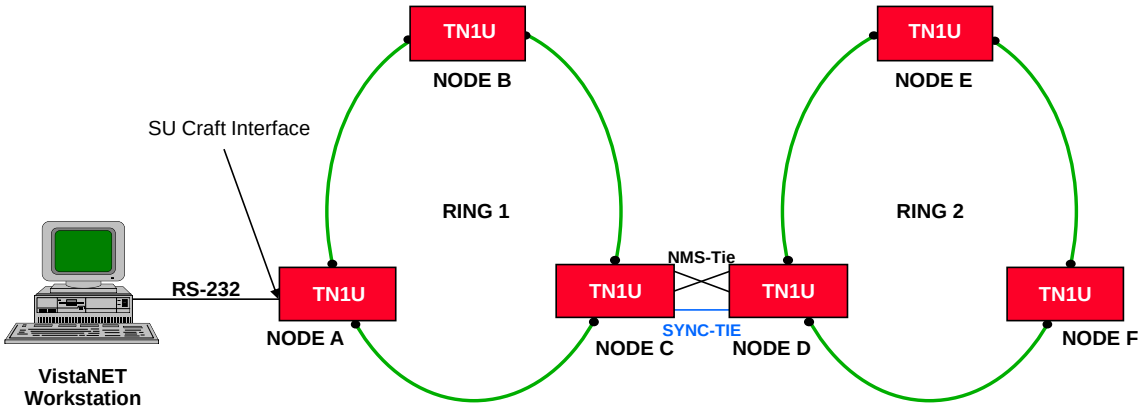


Figure 1: Visibility of two TN1U rings on one VistaNET workstation

Figure 2 shows two separate TN1U systems (NMS domains[1]), each with two TN1U rings. NMS information between the two rings in each system is passed via NMS-Tie cables that are interconnecting the two SU/IPSU paddleboards. These two systems are visible on a single VistaNET platform.

[1] All nodes within a ring or linear network belong to the same NMS domain if they are configured to use the same overhead bytes for NMS communications. The NMS domain can be extended across multiple rings and/or linear networks by means of NMS-Tie cables.

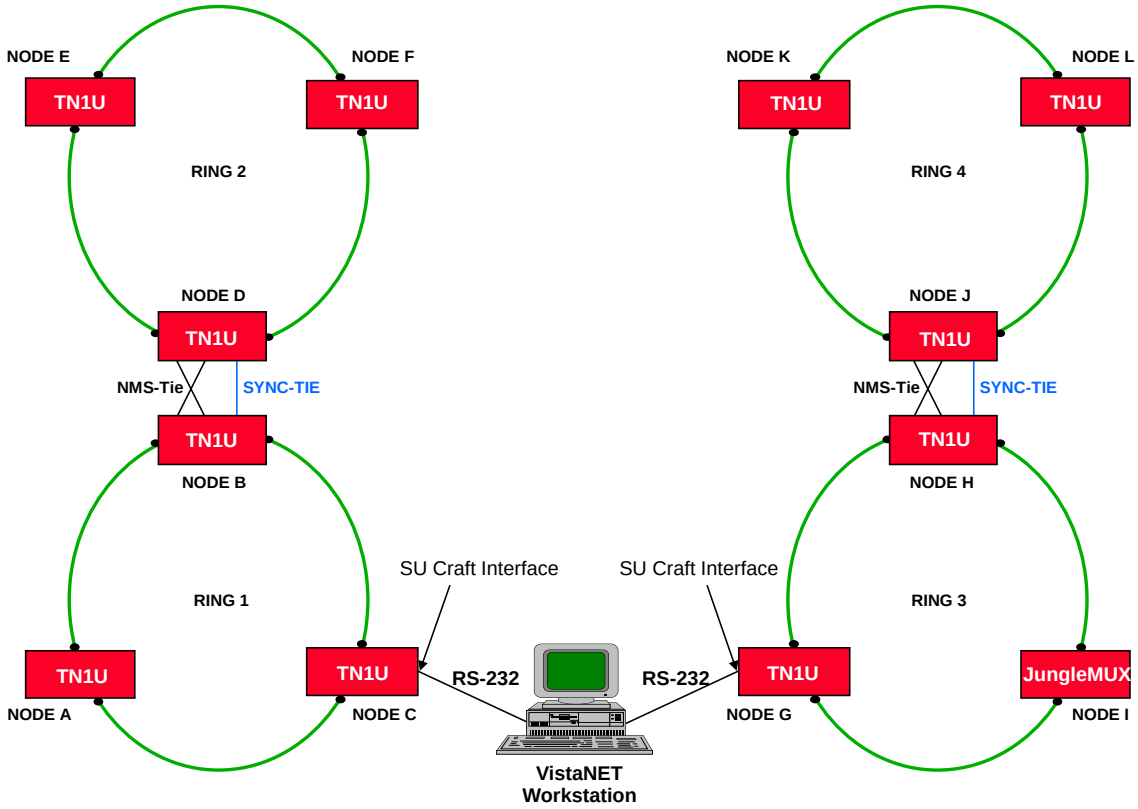


Figure 2: Visibility of two separate TN1U systems on one VistaNET PC

IP Service Unit (IPSU)

The IPSU, in addition to the standard Service Unit features described above, provides an IP network interface for advanced NMS solutions like VistaNET client-server network management and an industry-standard SNMP (Simple Network Management Protocol) interface.

Note: *The IPSU Support Package v4.00 (released in June 2011) allows the unit to simultaneously operate as a VistaNET server and SNMP agent. For the VistaNET server function, the version of the support package installed on the unit must match the VistaNET version installed on the client PCs. For more information on the support package go to page 13.*

Each IPSU can be configured with a static IP address or can subscribe to a DHCP server for dynamic IP address allocation. The IPSU's host name may

also be used for addressing the unit where DNS (Domain Name System) support is available.

Note: *If a DHCP server is not available, to establish an IP connection to an IPSU, certain IP parameters in the unit need to be specified locally (through the unit's craft interface). Alternatively, this can be done remotely if the unit's NMS visibility through the SDH overhead channel has been established.*

The deployment of an IPSU into a TN1U common equipment shelf takes the place of a standard Service Unit. The network operator can choose to have one or multiple IPSUs (for redundancy) used in each TN1U NMS domain to provide NMS visibility of TN1U equipment over an IP network. An Ethernet LAN should be brought to the site with IPSU and connected to the IPSU's paddleboard.

If an Ethernet connection cannot be established to a TN1U ring, the IPSU functionality can be provided by a dedicated PC. In that case, a serial RS-232 connection[1] is established between a standard Service Unit and PC. Refer to the VSA server and VSNMP functions described in the *VistaNET User's Guide* for details.

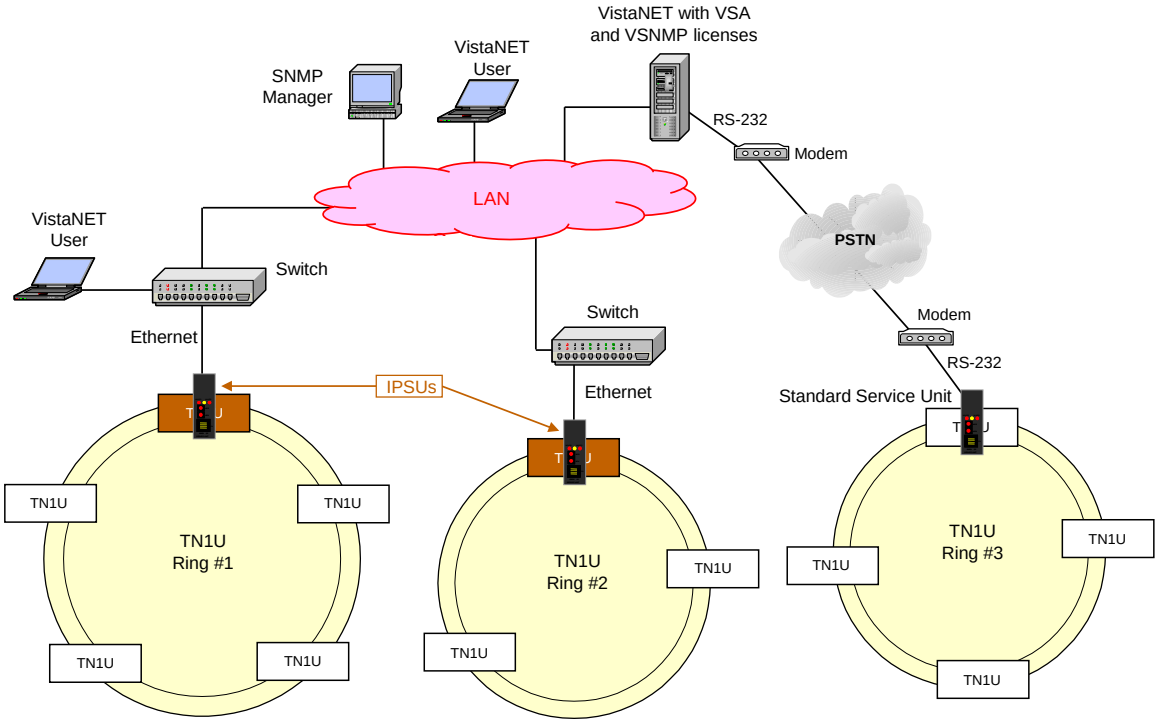


Figure 3: Control of two separate TN1U systems with IPSUs installed

[1] This could be a local or remote connection extended via modem, Data-LS circuit or IP network.

The IPSU is capable of time-stamping and storing TN1U alarms for up to 60 days. When network connections to the IPSU are lost due to outages on the LAN, the IPSU will continue to store events locally. Whenever a connection to the IPSU is re-established, the remote NMS application (SNMP manager or VistaNET PC) can be used to download these saved events. The unit's internal clock can be referenced to an NTP clock.

The unit's standard 10Base-T Ethernet connection (RJ-45 port on 86434-92 paddleboard) provides a fast and secure data transfer port to remote computers.

The IPSU is capable of discovering the local TN1U network inventory. The IPSU possesses a modified "local passport" file, which is used to store the results of the network discovery and results from synchronization with remote VistaNET services.

IPSU Operations

An IPSU must first be connected to an Ethernet LAN. The unit is designed to obtain its IP address either statically or dynamically (DHCP). A Dynamic IP address allocation is assumed for this section. Configuring a Static IP address is described in the *Configuration* section.

Upon powering the IPSU, the unit will attempt to connect with a DHCP server to obtain its IP address. Concurrently, the unit detects nodes within the NMS domain (single or multiple ring/linear network). The unit then attempts to connect to remote VistaNET services (remote VistaNET PCs and/or IPSUs). If the SNMP agent functionality is enabled on the unit[1], it will also try to connect to remote SNMP Manager(s) using the IP address or DNS name previously obtained through the synchronization process with remote VistaNET services.

The IPSU will then start a local VistaNET session, restore the previously discovered inventory (if any), and synchronize the inventories and other resources stored in the passport files on remote VistaNET PCs and IPSUs with its own. At the same time, it (re)discovers all "visible" nodes in the NMS domain to which it belongs. The discovery process takes approximately 1 – 2 minutes per node. Once the discovery has concluded, the discovered inventory is stored/updated within the unit and then uploaded to remote VistaNET sessions and retrieved by SNMP Managers.

[1] In VistaNET v4.00, the SNMP agent functionality cannot be selectively disabled. That is, if the VSNMP license is obtained and the SNMP parameters are set (i.e. entered on one VistaNET PC and then synchronized between VistaNET PCs and IPSUs), all IPSUs and the VistaNET PCs with serial connections to the TN1U network(s) will be performing as SNMP agents.

The discovery process builds a hierarchical tree of TN1U units that are bound together by traffic paths (Ring, Node, Side, Port, TU and Channel) for each ring and node number in the IPSU's NMS domain. Any traffic path change(s) will not be automatically captured once the discovery has concluded. A new discovery must be initiated by the user every time a new unit is added, a unit is replaced, or whenever traffic paths change in any node of the IPSU's NMS domain. Individual unit parameters that do not affect the traffic path are stored in individual units and retrieved when requested.

An IPSU can be reset by right-clicking on the node in the System Tree and selecting the "Reset Service Unit" option. This reset must be carried out each time any of the unit's IP-related configurable parameters have been altered through VistaNET. Removing and re-inserting the IPSU into the shelf, as described in the *Installation* section of this manual, will also reset the unit.

Note: *The IPSU will NOT reboot automatically after a configurable change is made to the unit. The unit must be reset by the user from the VistaNET System Tree after an IP-related configurable parameter has been modified.*

Establishing a serial connection to the IPSU's craft interface while the unit is re-discovering the network will prolong the discovery process. It may take a while for the VistaNET to connect to the IPSU when the IPSU is discovering the network or processing requests on its Ethernet interface.

The IPSU v4.00+ supports NMS communication through its CI interface. That is, it can perform as an NMS gateway to a serially connected VistaNET PC. However, maintaining a permanent serial connection from an IPSU to a VistaNET PC is not recommended, as it will slow down NMS communication with remote VistaNET/SNMP sessions as well as degrade alarm monitoring performance.

Support Package

The IPSU support package is a bin file whose name indicates the corresponding VistaNET software version. For example, IPSU0402.bin is the support package that matches VistaNET version 4.02.

Note: *Starting from June 2011, the IPSU is shipped from the factory with a support package that matches the latest released VistaNET version. The latest support package and VistaNET program can be obtained from the TN1U website at www.JMUX.com.*

Note: *The customers whose IPSUs are running an older version of the support package (compatible with VistaNET 2.24 or earlier) must perform a one-time upgrade with a core software that includes the Linux operating system. Please contact GE Lentronics for more information. Note that this upgrade can be carried out only locally (through the craft interface).*

Note: *An IPSU running the support package version ≥4.00 can be upgraded to a newer package using either an IP connection or the craft interface connection to a PC running VistaNET. The latter one is rather slow and is therefore not recommended. If IP connection is used, the IPSU must be visible in the VistaNET system tree so that the user can open the IPSU's Unit View and initiate the upgrade process (explained in the Configuration section of this manual). If only IP connection to the unit exists, the IPSU must be upgraded before upgrading the VistaNET installation on the PC from which the upgrade is being carried out.*

SNMP Support

An IPSU will act as an SNMP proxy (v1 or v2c) agent for all TN1U units within its NMS domain. SNMP (Simple Network Management Protocol) is an application layer protocol used to manage networks, and works by sending messages, called Protocol Data Units (PDUs) to different parts of a network. In TN1U, the following PDUs are supported:

- GetRequest (retrieves a single SNMP object)
- GetNextRequest (retrieves the next logical SNMP object)
- GetBulk (retrieves multiple SNMP objects)
- Traps (sends an alarm event to a manager)

Note: *The IPSU loaded with software version 4.00 does not support accessing data points (individual unit parameters) from the SNMP manager.*

Like other commercially available SNMP agents, the IPSU stores data about itself and the devices they monitor/control in a MIB (Management Information Base) file and forward this data to the SNMP manager. The MIB can therefore be considered as an "information warehouse" and an example has been included in Appendix A. Since the MIB defines properties of the managed devices (TN1U), it must be available to both the SNMP Agent and the Manager to synchronize the SNMP information. The MIB file is available on www.jmux.com for customer download.

The IPSU connects to the SNMP manager via the rear paddleboard RJ-45 connector. The IPSU and SNMP manager communicate via the UDP protocol. The SNMP agent listens for incoming requests on port 161, while the traps are sent on port 162.

VistaNET Server Function

VistaNET servers allow remote VistaNET PCs without serial connection to a TN1U network (so called "VistaNET clients") to perform network monitoring and unit configuration functions over an IP network. VistaNET servers come in two forms (see Figure 4):

- a PC running VistaNET service with a VistaNET Server Application (VSA) license applied to its RS-232 connection[1] to the standard Service Unit. This is called a *VSA server*.
- an IPSU loaded with the support package matching the VistaNET version used on the client PCs. This is called *an IPSU server*.

A VistaNET server streams alarms from nodes managed by the server to remote VistaNET services (clients) through an Ethernet LAN and allows them to monitor and configure various unit parameters (data points) through the LAN.

[1] Hardwire, modem, Data-LS circuit or Ethernet (using serial-to-Ethernet media converter).

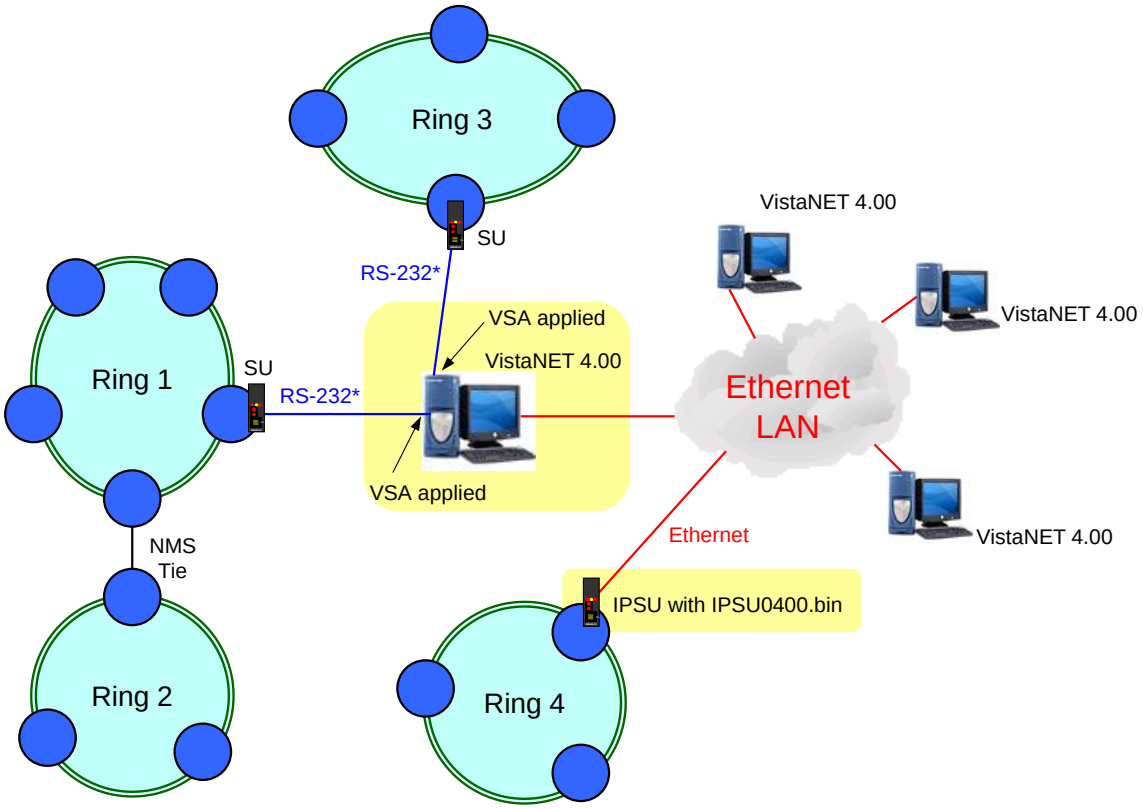


Figure 4: VSA server, IPSU server and VistaNET clients

CAUTION
If routers are used to connect an IPSU with remote VistaNET services, the routers must be configured to allow multicast messages to pass. Otherwise, the remote VistaNET services may not connect with the IPSU.

Note: *Router must enable the TDP/UDP port 8644 (for system tree synchronization) and TCP port 8633 (for remote data download).*

Refer to the VistaNET User Guide for more information on VistaNET.

3. FRONT PANEL FEATURES

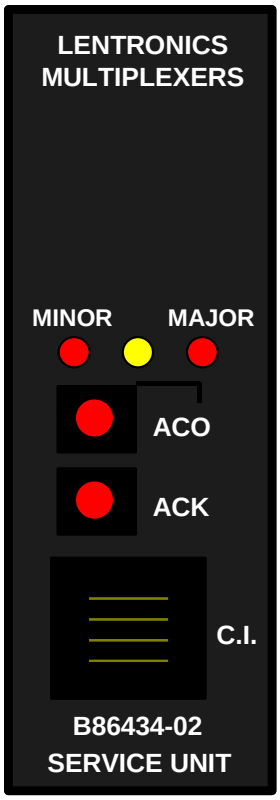


Figure 5: Front Panel Layout

LED Indications

LED indications are provided for Minor and Major alarm conditions at the local node. Generally, Minor is classified as non-service affecting and Major as service affecting, e.g. if a local STM-N Aggregate Unit was to fail, a minor alarm condition would be reported. If both STM-N Aggregate Units were to fail, a Major alarm would be reported. However, there are some Minor alarm conditions that are service affecting (e.g. loss of a 64 kb/s channel unit) and some Major ones that are not service affecting (e.g. loss of one Left and one Right TIF-level unit belonging to different TIF-level unit pairs).

The alarm LED is latched on by any alarm and may be cleared by pressing the ACK button.

***Note**: When a Major alarm is present, both Minor and Major red LEDs are lit.*

***Note**: The LEDs reflect only the alarm state of the local node even if the Sentinel Alarm Mode is enabled.*

ACO button

The Alarm Cut-Off button is provided to temporally silence the alarms (not implemented).

ACK button

The main use of the ACK button is to acknowledge all local alarm conditions after they have cleared. Pressing the ACK button will turn the Amber LED off only if both red LEDs are extinguished.

The second use of the ACK button is a LED and microprocessor test. If the SU/IPSU is operating normally, holding the front panel pushbutton down causes all the LEDs to light. The main use for this test is to verify that the front panel

LEDs are functional and that the microprocessor firmware code is running normally (microprocessor is not locked up).

***Note**: The microprocessor test does not disrupt normal SU/IPSU operation.*

Craft Interface (C.I.) Jack

This is a serial asynchronous RS-232 9600 b/s port that enables communication to a PC running VistaNET. VistaNET's local mode is used to configure unit parameters and monitor the unit's status. VistaNET's network mode enables the user to configure and monitor units that belong to the entire TN1U system.

NOTE

An IPSU loaded with a support package v4.00+ can be used to provide network management of the TN1U network through the unit's CI port. However, this is not recommended for permanent use because the unit's microprocessor would have to manage the activity of both the CI port and support package resulting in significantly slower CI port performance (compared to a standard Service Unit).

In addition to the CI port available on the unit's front panel, two additional CI ports are available on the 86434-81 and legacy 86434-80 paddleboards. The front panel CI port is typically used only for temporary VistaNET connections to the unit. Refer to the *Paddleboard Connections* in the *Installation* section for information on the paddleboard's CI port.

***Note**: Although the CI is available on three physically separate ports, only one of them can be used at a time. It is not possible to run multiple VistaNET sessions through the same Service Unit.*

The reader should refer to *Section 8* for details regarding the features of the Network Management System (NMS).

NOTE

The IPSU can simultaneously support both Serial (CI) and Network (Ethernet) interfaces. However, maintaining a permanent serial connection from an IPSU to a VistaNET PC is not recommended as it will slow down NMS communication with remote VistaNET/SNMP sessions as well as degrade alarm monitoring performance.

Extractor

Located at the bottom of the unit's face plate is the extractor, which is an integral part of the unit's casing. As the name implies, it allows for easy extraction of the unit from the shelf.

WARNING
Do not use the extractor to force the unit into the shelf as this could result in damage to the extractor.

4. UNIT DESCRIPTION

The description that follows is common for both 86434-02 Service Unit (SU) and 86434-03 IP Service Unit (IPSU) unless explicitly stated otherwise.

The SU monitors alarms from individual units and provides Major and Minor office alarm relays. The unit also provides a Network Management interface allowing remote configuration, monitoring and diagnostics of the entire system. Both SU and IPSU process SDH overhead traffic for the 86471 Orderwire Unit and the 86474 VF Partyline Unit via the CBUS interface.

The SU has two assembly boards. The 087-86434-04 is the main assembly board housing the Field Programmable Gate Array (FPGA) U4 and micro-processor U1. The 087-86434-05 sub-assembly board provides the interface to either the legacy 86434-80 (discontinued in October 2005) or 86434-81 paddleboard assembly.

The IPSU has three assembly boards. The 087-86434-08 is the main assembly board housing the Field Programmable Gate Array (FPGA) U8 and micro-processor U2. The 087-86434-07 provides the interface to the 86434-92 paddleboard assembly. Finally, the 087-8634-09 is the StrongARM or X-Scale microcomputer that interfaces an on-board Ethernet controller with the paddleboards RJ-45 and the main board's microprocessor.

The legacy 86434-80 paddleboard assembly can be used only with SU at nodes without External Sync Units. It provides the necessary external connections for Major and Minor alarm relay contacts, TBOS interface, CBUS interface, multi-ring connections for NMS and power monitor input for monitoring Power units.

The 86434-81 paddleboard assembly can be used with either SU or IPSU. It provides the necessary external connections for Major and Minor alarm relay contacts, TBOS interface, CBUS interface, multi-ring connections for NMS, power monitor input for monitoring Power units, and Ethernet interface (used with IPSU only).

Both SU and IPSU have access to the entire SDH overhead information via the Serial Peripheral Interface (SPI) shelf bus. This bus is duplicated to accommodate traffic for both East (left) and West (right) STM-N directions. The following sections provide information on how the SU/IPSU communicates to various equipment and what information is contained in the traffic.

Intra-Node Communication Channels

SU/IPSU to STM-N Aggregate and SYNC Unit Communication

The SU/IPSU, at each node, constantly polls the local STM-N Aggregate and External Sync units for their presence and summary status bits, generating a "node-view" packet for the node. This polling of the STM-N Aggregate and External Sync units is done over a half-duplex 1 Mb/s SPI microprocessor bus.

In addition to this constant polling, the SPI bus is used for requests to both STM-N Aggregate units and External Sync units for more detailed status information of each unit. The response from the units back to the SU/IPSU can be anywhere from 6 to 400 bytes. This information can be for any of the operating parameters of the unit (i.e. received optical level), for any of the configuration bytes (i.e. priority direction) or status of a reconfiguration command.

STM-N Aggregate Unit to TIF Level Unit Communication

This communication uses the Overhead channel in the TIFport data link.

For a TIFport in TU-11 mode of operation, seven TU-11s on the TIFport use 12.096 Mb/s (7 x 27 bytes/frame x 8 bits/byte x 8000 frames/sec) of the 12.960 Mb/s TIFport capacity, leaving 864 kb/s for the NMS channel.

For a TIFport in TU-12 mode of operation, seven TU-12s on the TIFport use 16.128 Mb/s (7 x 36 bytes/frame x 8 bits/byte x 8000 frames/sec) of the 19.440 Mb/s TIFport capacity, leaving 3312 kb/s for the NMS channel.

For each assigned TU-1, each STM-N Aggregate unit polls the appropriate TIFport to check that a TIF level unit is properly configured and healthy. The STM-N Aggregate unit keeps a 21-entry table for these responses plus a summary TU-1 level status byte for the NMS System View icons.

When the VistaNET network operator desires more information on a local TIF level unit, the request/response path will also use this channel.

TIF to Channel Unit Communication

These communications use the overhead channel in the CBUS data link that connects these units. A TU uses 1.728 Mb/s while the CBUS serial clock operates at 2.592 Mb/s. (This is done by taking the 12.96 Mb/s TIFport signal and dividing by five). The remaining 864 kb/s bandwidth is used for NMS data and multi-frame synchronization. (NMS data is actually around 10 kb/s.)

Each on-line CMUX unit polls each of the 24 channel slots on each CBUS port to maintain a database of the equipped channel units and their status.

Further specific information is obtained as required by VistaNET's network channel unit commands.

Intra-Ring Communication

The SU/IPSU can, at each node, communicate with SUs/IPSUs at other nodes in the same ring/linear network using overhead bytes in the STM-N signal (each byte provides 64kb/s). These bytes, depending on the user's selection, can be DCC bytes in the STM-1 Section Overhead (recommended by ITU-T Recommendation G.707 for NMS transport), unused (stuff) bytes of any terminated VC-4, or unused (stuff) bytes of any TU-12 carrying no E1 (2.048 Mb/s) traffic (i.e. any TU-12 that is either unused or carrying traffic originated from any TIF level unit of TU-11 type). The last two options allow the NMS and Orderwire information to be passed through non-TN1U SDH transport nodes or cross-connects that may be used with TN1U in the same network. This is because the TN1U-originated SOH bytes are not passed through non-TN1U SDH nodes, whereas the 'stuffed' TU-12s are.

Since the same NMS packets are sent out on both left and right fibres, the destination node in a ring network normally receives each NMS packet twice. It is the responsibility of the destination site to resolve the arrival of duplicate packets. The receipt of every command packet "destined-for-here" has a sequence number and CRC. Prior to acting upon a command, the history memory is searched for a matching unique ID and, if found, the packet will be discarded.

The Service Unit multiplexes all bytes used for Orderwire/Partyline communication from both left and right fibres into a "standard" CBUS-format signal, which is cabled to selected shelf slot positions in the same manner as the "normal" CBUS-to-channel-unit cabling. This provides an "Orderwire CBUS" into which can be plugged Orderwire units and/or 4W VF Partyline units.

Ring-to-Ring Communications

For multiple ring/line NMS communications, each SU/IPSU has two bidirectional NMS-tie ports, which connect to the corresponding ports on a collocated SU/IPSU belonging to another ring or linear network. These two ports provide micro-to-micro communications at the 2.592 Mb/s CBUS port rate. They are

labelled as NMSTIE-M and NMSTIE-S on the paddleboard. At the site with collocated TN1U nodes, the NMS-tie ports are connected via NMS-Tie cables (035-86430-4X).

SU/IPSU-to-VistaNET Workstation Communications

Each SU/IPSU has a standard 9600-baud serial port for connection to a standard COM port on a PC, running VistaNET software (a Microsoft Windows™ based program).

For convenience, a choice of RJ-11 connectors is available on the front of the unit or on the unit paddleboard. This port may be extended to other locations using a standard 9600-baud Hayes-compatible modem or a TN1U DATA-LS circuit.

Communication Channels' Traffic

There are two types of traffic activity:

One is the transmission of autonomous NODE-ICON bytes; this comprises a string of more than a dozen bytes containing the summary status of each node. These are generated at each node and broadcast throughout the system so that all nodes know the status of all other nodes.

The SU/IPSU at each node assembles all the NODE-ICON bytes into a Service Unit database to which VistaNET has access. (To reduce the response times, only the changed information is sent.)

The other traffic activity is the transmission of requests from the NMS workstations to a specific unit and the transmission of responses from the unit back to the workstation. These may be as a result of an action by the workstation operator or from the workstation's "alarm engine" being activated by a change in a NODE-ICON byte to find the source of a new alarm.

All inter-node packets are 35 bytes long comprising 21 bytes of data preceded by a 13-byte header and followed by a CRC check byte. See Figure 6 for the 13-byte header details.

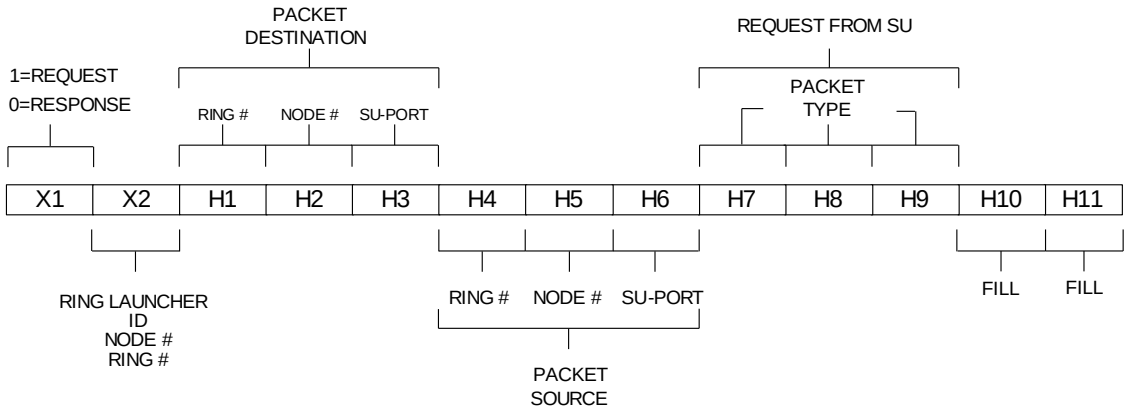


Figure 6: 13-Byte Header Details

TBOS Interface

TBOS (Telemetry Byte Oriented Serial) is a protocol for transmitting alarm, surveillance and control data between monitoring and monitored equipment. The SU/IPSU supports the TBOS interface via a rear access interface port to report alarm and status conditions.

The TBOS port on each SU/IPSU is capable of providing alarm/status information for up to 16 Network Elements (nodes) in the TN1U system. The set of nodes whose status information will be provided is determined by the assignments (Ring and Node numbers) programmed in the TBOS tab (see *Configuration* section). The information is transmitted in the form of 16 displays with each display containing 32 alarm or status points. Each display represents information from one Network Element. At present, in each display, 12 points are used and the remaining points are reserved for future expansion.

The TBOS Interface on the SU/IPSU forms a point-to-point half-duplex transmission over two pairs of 26-gauge 100-ohm twisted pair wire. The TBOS port is accessible on the Paddleboard through connector TB3. The TBOS interface baud rate may be programmed (using VistaNET) to 1200, 2400, 4800, 9600 or 19200 baud. The initial default setting is 2400 baud, 2 stop bits with odd parity. Matching of displays to network elements is carried out through the configuration table in the SU/IPSU.

The TBOS serial interface complies with Bell System Technical PUB49001 section 3.0 and section 4.0.

IPSU's Ethernet Interface

The IPSU makes use of a 400MHz cERFboard equipped with a RISC X-Scale processor and Ethernet controller[1]. This cERFboard offers an interface to the standard Service Unit features processed by the unit's main board and to an IP interface available on the unit's paddleboard. From the customer's perspective, an RJ-45 available on the paddleboard is used to establish a connection to an external Ethernet network.

To communicate with an external SNMP manager, a connectionless oriented transport session (UDP) is established. The network layer protocol is IP (UDP/IP). The IPSU operates as an SNMP agent to the manager and permits data (in SMI format) to pass over this network. SNMP is an application protocol and hence the IP stack required to establish to connection is contained in the IPSU. The IPSU and SNMP manager communicate via the UDP protocol. The SNMP agent listens for incoming requests on port 161, while the traps are sent on port 162.

For communication with remote VistaNET sessions (VistaNET PCs and/or IPSUs), the transport layer protocol used is TCP, while the network layer protocol is IP (TCP/IP). This connection-oriented protocol ensures that data destined for a unit arrives as intended. TCP/IP ports 8644 and 8633 must be enabled within the enterprise network. UDP/IP port 8644 must be enabled for multicast packets used to detect all VistaNET services.

[1] Older IPSU cERFboards are equipped with a 200MHz StrongARM CPU.

5. INSTALLATION

The following section provides information for installing Service Units (SUs) and IP Service Units (IPSUs). The unit is shipped from the factory configured as per the NAD for the purchased system. All spare units or loose units are shipped with factory default settings in memory.

CAUTION

The SU and IPSU have ESDS components and therefore standard static protection precautions should be observed when handling, packing or shipping the unit.

Pre-installation

Visually check the unit for damage. Ensure that screws are firmly tightened and in place. Keep the shipping containers and packing materials for future use. If a unit is damaged, file a claim with the shipping agent or the local GE Multilin representative.

Shelf Position

A SU/IPSU occupies one shelf slot and must be located in position 13 of the Common Equipment Shelf. Only one Service Unit (either 86434-02 or 86434-03) is needed at a node. That is, if multiple Common Equipment Shelves are needed at a node, only the shelf equipped with STM-N Aggregate unit(s) houses a SU/IPSU. Other Common Equipment shelves at the node are equipped with a Blank unit in position 13.

Figure 7 shows a typical rack layout for a ring configured system as it appears on a NAD.

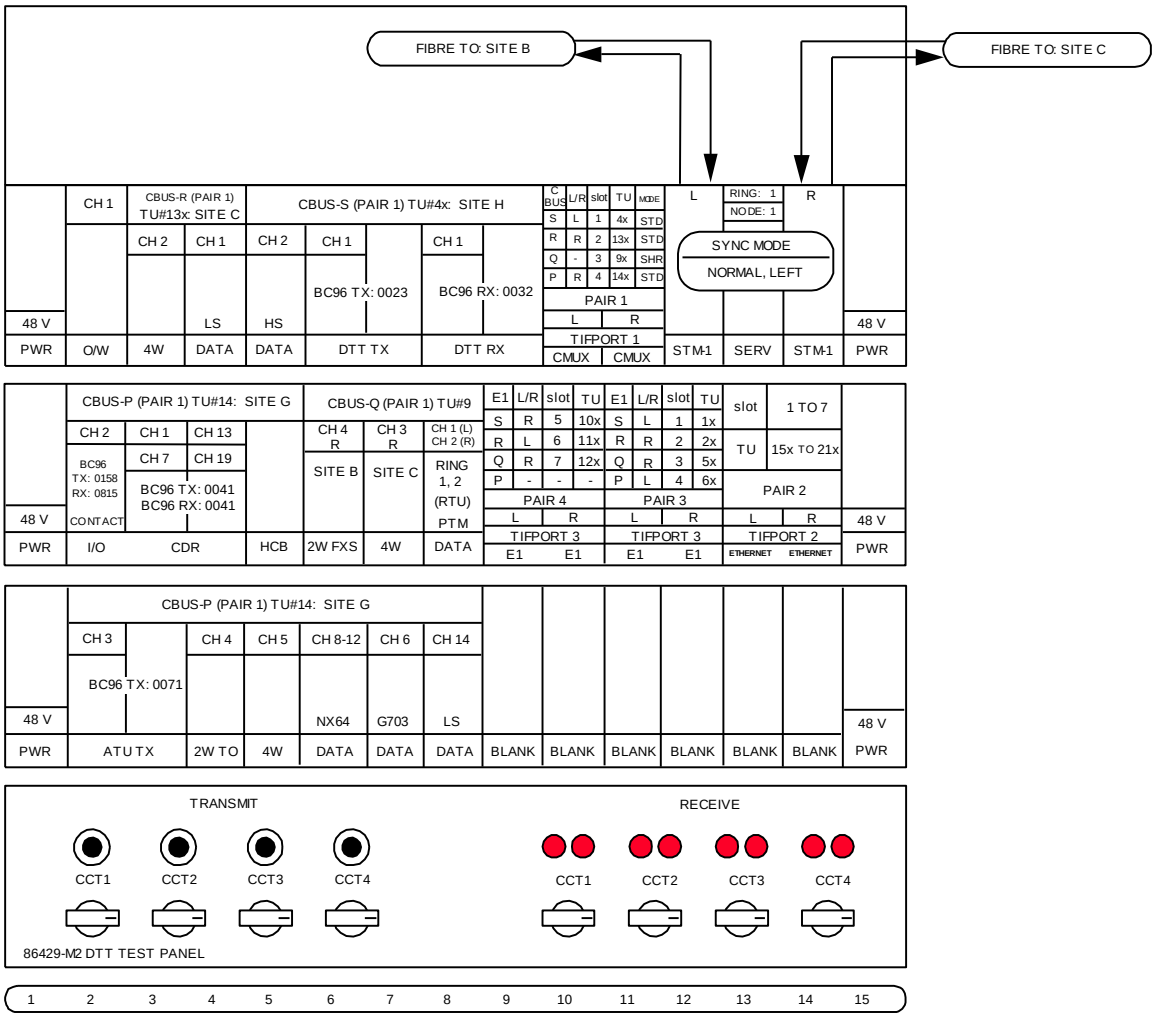


Figure 7: Typical Rack Layout for a TN1U SDH Node

The Service Unit can be inserted and removed from the shelf with shelf power applied.

WARNING

Whenever power to the IPSU is interrupted, the IPSU will reboot. On reboot, IPSU rediscovers all TN1U inventory within the NMS domain where it resides.

Paddleboard Connections

The paddleboard assembly enables customer connections to the unit. The 86434-02 Service Unit is used with either legacy 86434-80 (discontinued in October 2005) or 86434-81 paddleboard, while the 86434-03 IPSU is used with the 86434-81 paddleboard. Figure 8 and Figure 9 detail the paddleboard connections.

Office Alarms

The paddleboard connector TB1 provides the customer connections to Major and Minor alarm relay contacts. These reflect either the status of the local node (default) or the Sentinel Alarm status (if enabled through the VistaNET software). The user is referred to *Configuration* section for more information on Sentinel Alarm configuration.

Note: *Relay contacts provide typical 23 ohm (max 35 ohm) resistance when the relay contact is closed. The maximum load current and voltage are 120 mA (continuous, at 25ºC)[1] and 350V (peak), respectively.*

Power Monitor

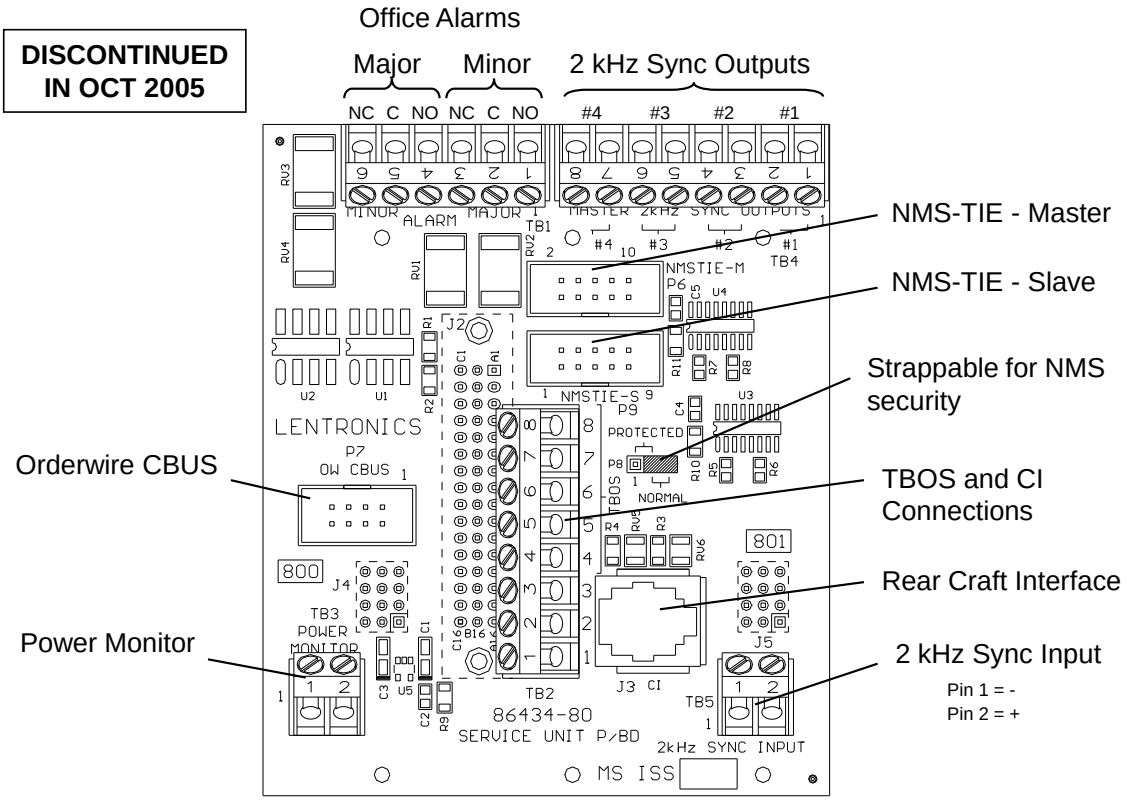
A Power Monitor on TB3 connects to the 86425 AC Power and 86431 DC Power Unit Paddleboards to provide alarm reporting in the case of Power Unit failure (the NO and C contacts on all Power Unit paddleboards residing at this node are paralleled and wired to this connector).

Sync-Tie Connections

One node usually supplies the system clock for all nodes in the network. If a TN1U system comprises multiple rings and/or linear networks, the system clock is usually passed to those rings/linear networks as well. Each Service Unit paddleboard provides a balanced 2kHz input and four balanced 2kHz outputs for connections to multiple rings (see Figure 8). No interconnect Sync tie cable is available through GE Multilin. The user shall use a standard twisted pair with a length of up to 10 meters.

[1] At +60ºC, the maximum load current drops to 90mA for Form A (normally open) and 100 mA for Form B (normally closed).

DISCONTINUED IN OCT 2005



TB2 connector pin designations:

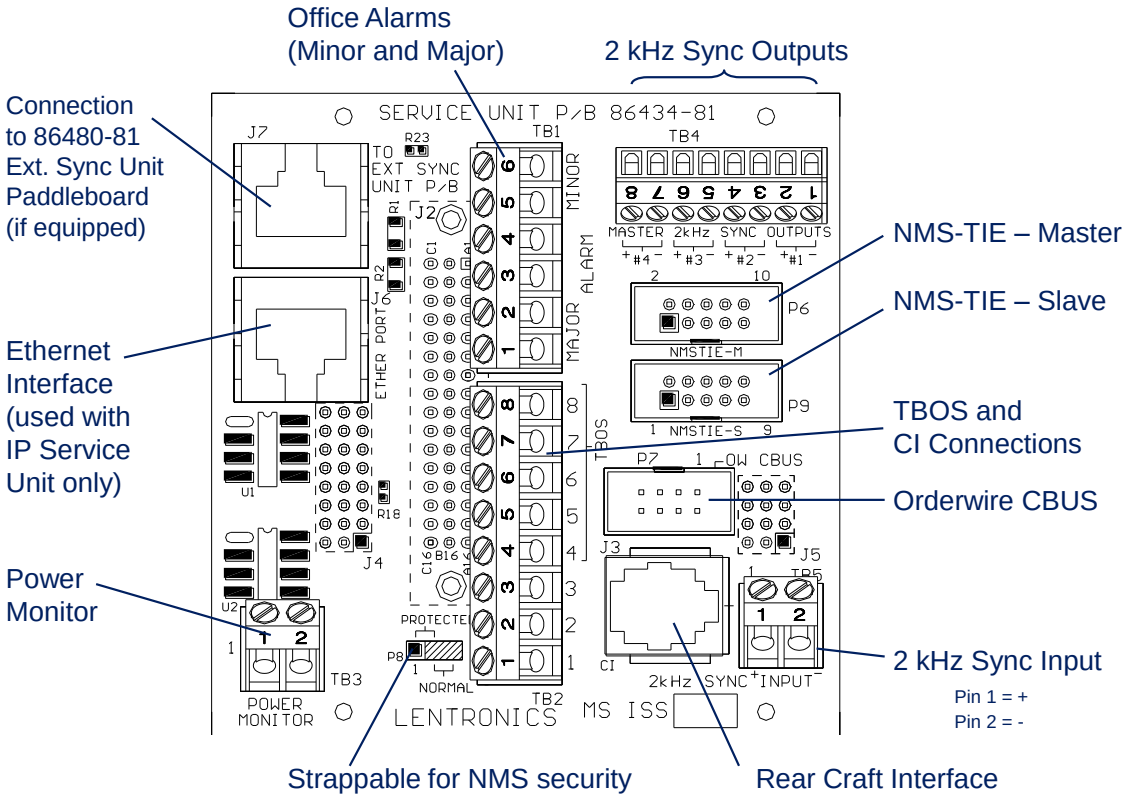
TBOS Transmit (signal from external equipment)	TB2 pins 7 (-) & 8 (+)
TBOS Receive (signal to external equipment)	TB2 pins 5 (-) & 6 (+)
Craft Interface	TB2 pin 1 (xmt), pin 2 (rcv), pin 3 (gnd)

Office Alarms:	Major Alarm	TB1 pin 1 (NO), pin 2 (C), pin 3 (NC)
	Minor Alarm	TB1 pin 4 (NO), pin 5 (C), pin 6 (NC)
2kHz Sync Outputs:	#1	TB4 pin 1 (+), pin 2 (-)
	#2	TB4 pin 3 (+), pin 4 (-)
	#3	TB4 pin 5 (+), pin 6 (-)
	#4	TB4 pin 7 (+), pin 8 (-)

Note: NO = Contact Open when Energized and Alarm Free.

NOTE: This paddleboard was discontinued in October 2005.

Figure 8: 86434-80 Service Unit Paddleboard Connections



*** TB3 connector pin designations:**

TBOS Transmit (signal from external equipment)	TB3 pins 7 (-) & 8 (+)
TBOS Receive (signal to external equipment)	TB3 pins 5 (-) & 6 (+)
Craft Interface	TB3 pin 1 (xmt), pin 2 (rcv), pin 3 (gnd)

Office Alarms:	Major Alarm	TB1 pin 1 (NO), pin 2 (C), pin 3 (NC)
	Minor Alarm	TB1 pin 4 (NO), pin 5 (C), pin 6 (NC)
2kHz Sync Outputs:	#1	TB4 pin 1 (-), pin 2 (+)
	#2	TB4 pin 3 (-), pin 4 (+)
	#3	TB4 pin 5 (-), pin 6 (+)
	#4	TB4 pin 7 (-), pin 8 (+)

Note: NO = Contact Open when Energized and Alarm Free.

Figure 9: 86434-81 Service Unit Paddleboard Connections

Ext Sync Unit Connection

If 86480-31 External Sync units are installed at the node, the connector J7 (n/a to 86434-80 paddleboard) connects to the 86480-81 External Sync Unit Paddleboard connector J13. Refer to the respective TPIM for more information.

Orderwire CBUS

The CBUS port (P7) provides the Orderwire and 4W VF Partyline interface. A 17" ribbon cable (035-86430-15) is used to interconnect this port to the position in the shelf where the first (usually the closest to the Service Unit) Orderwire and/or 4W VF Partyline unit is inserted. Additional Orderwire and/or 4W Partyline units may be installed in adjacent shelf slot positions by extending the CBUS (refer to the *Equipment Shelf TPIM*).

NMS-Tie Connections

Connectors P6 (NMS-TIE-Master) and P9 (NMS-TIE-Slave) allow NMS connectivity between collocated TN1U nodes that do not belong to the same ring/linear network so that the NMS packets can be passed across multiple rings and/or linear networks. The NMS-Tie connections at sites with two and three TN1U nodes are shown in Figure 10. If more than three Service Units must be connected, the NMS-Tie Master-to-Slave configuration would be continued for all Service Units. For each NMS-Tie Master-to-Slave connection one 035-86430-4X ribbon cable is required. These cables are available in different lengths (24", 30", 36", 42", 48", 60", 72", 142" for 035-86430-40 through -47, respectively). Refer to the CA86450 document for more information on these cables.

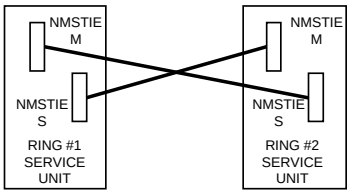
Note: *Presence of 2kHz sync-tie connection between collocated nodes is necessary for proper operation of NMS-Tie connections. The lengths of cables used for these connections shall be approximately the same.*

Removing NMS-TIE connections

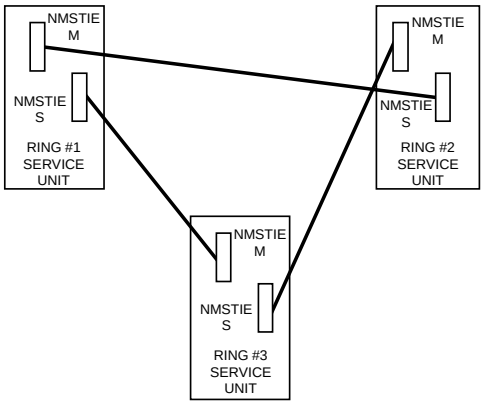
Reducing the size of NMS domains can sometimes provide considerable improvement to NMS efficiency as it reduces the amount of NMS traffic that is sent around the network. Reducing traffic carried on the SDH overhead bytes reserved for NMS equates to performance gains in the Service Unit and NMS engine (VistaNET). Furthermore, if the available resources (SUs and IPSUs) are managing smaller segments of the network, they are better positioned to handle bursts of NMS traffic like those experienced during alarm storms.

Removing the NMS-Tie naturally creates more independent NMS domains. Each NMS domain requires a separate NMS connection to a 24/7 VistaNET PC. Ethernet can be used to provide a shared medium that not only serves to provide NMS connectivity to individual NMS domains, but also allows all VistaNET services to remain synchronized. Synchronized data reduces discovery attempts, simplifies administration, provides a common database of information,

imposes security policies and ensures all VistaNET sessions retain the same look and feel of the TN1U network.



TWO-RING NMS-TIE CONNECTION



THREE-RING NMS-TIE CONNECTION

Figure 10: NMS-TIE Connections

Rear Craft Interface

The rear craft interface port (labelled as "CI") is typically used when a PC running VistaNET is permanently connected to the local Service Unit CI, either directly (hardwire) or through an external modem[1]. An RJ-11 connector provides the interface to a standard VistaNET cable.

Note: *The front panel craft interface port is typically used for temporary VistaNET connections to the unit.*

The craft interface on the connector TB2 pins 1, 2, 3 is used only if the local Service Unit craft interface is to be accessed from another TN1U site (using 86448 DATA-LS unit[2]). This may be needed in order to:

[1] An external modem is used to enable remote dial-up VistaNET connections. The reader is referred to 86456 VistaNET User's Guide for more information on establishing modem connections to the Service Unit.
[2] Use DATA-LS data circuit #4 set for "Service Unit CI" mode.

- route NMS traffic from one of the two non-NMS-Tied rings to a VistaNET PC located at one of the other ring's sites, or
- connect an external modem (located at a site where the local Service Unit CI is hardwired to a 24/7 VistaNET PC) to a remote Service Unit CI.

***Note**: Although the craft interface is available on three physically separate ports (front panel CI port, Paddleboard CI port, and Paddleboard TB3 connector pins 1, 2, 3), only one of them can be used at a time. It is not possible to run multiple VistaNET sessions through the same Service Unit.*

CAUTION

Only one CI connection to the unit may be established. In a situation where a VistaNET connection has been made to the paddleboard CI port (RJ-11 or TB2 pins 1,2,3) and then inadvertently another VistaNET connection is made to the front-panel CI port, both VistaNET sessions will experience loss of transmission packets.

WARNING

The IPSU can simultaneously support both CI (local VistaNET) and Ethernet port communications. However, maintaining a permanent serial connection from an IPSU to a VistaNET PC is not recommended as it will slow down NMS communication with remote VistaNET/SNMP sessions and degrade alarm monitoring performance.

NOTE

The user must initiate IPSU reboot through the VistaNET System Tree (right-mouse-click on the respective node and select Reset Service Unit) after any IP-related configurable parameter on the unit has been changed.

Modem Lockout Configuration

The paddleboard provides a jumper (P8) for selecting the modem lockout configuration (Normal or Protected). The primary purpose of this jumper is to prevent any VistaNET users from performing configuration changes on the TN1U system via an external modem connected to this unit's CI (although the setting will apply to other types of VistaNET connections to the CI). If the jumper on the paddleboard is set to Protected (pins 1 and 2 strapped), then the Service Unit will not permit any configuration requests from a VistaNET program connected to the TN1U system via this Service unit; only monitoring capabilities are supported. The default setting is Normal (pins 2 and 3 strapped).

Ethernet Port on 86434-81 Paddleboard

An RJ-45 connector (J6) on the 86434-81 paddleboard is functional only when this paddleboard is used with IPSU. It is provided to allow network communications between the IPSU and a network application like SNMP manager or VistaNET clients. Several network layer protocols such as TCP and UDP are supported and are carried over IP. The Ethernet port supports a 10Base-T interface.

Paddleboard Installation

1. If a Service Unit is to operate in Protected mode (refer to *Modem Lockout Configuration*), change the strapping on the paddleboard.
2. Place the paddleboard onto the designated slot position ensuring that the rear connectors are fully mated. Ensure correct orientation of the paddleboard prior to insertion.
3. Secure the paddleboard in position using the retaining screws provided.

Replacing a Service Unit in a system in-service

Removing a Service Unit

1. Use a local VistaNET connection to display the unit configuration.
2. Click on *Copy* button (available at the bottom of the Unit View). This copies the local unit's configurable parameters to the VistaNET clipboard.
3. Use the extractor on the face plate of the unit to ease the unit from the shelf.

Note: *Traffic is not affected by removal of the Service Unit but can be affected by removal of the paddleboard if 2 kHz Sync Input/Outputs are used or External Sync Units are installed.*

WARNING
Removing the Service Unit or Service Unit paddleboard affects Orderwire / Partyline communication, Major & Minor relay contacts' operation, TBOS communications and NMS visibility of the node. In addition, if the unit is connected to a VistaNET PC, the visibility of all nodes in the NMS domain may be lost. In the case of IPSU, connection to the Ethernet network would be also lost (effectively killing the VistaNET server and/or SNMP agent functionality). Finally, in the case of Service Unit Paddleboard removal, traffic can be affected if 2 kHz Sync Input/Outputs are used or External Sync Units are installed.

Inserting a Service Unit

WARNING

Do not use the extractor to force the unit into the shelf as this could result in damage to the extractor.

1. Insert the unit to the point of resistance.
2. Gently seat the unit into the shelf by pressing the front panel. (Ensure the extractor is not preventing the unit from insertion.)
3. Establish a local VistaNET connection to the unit. (Note that in the case of IPSU, it may take a while for the unit to respond to VistaNET polls.) In the Unit View, click on Paste button (available at the bottom of the Unit View).

NOTE

It may take a while for the VistaNET to connect to the IPSU when the IPSU is discovering the network or processing requests on its Ethernet interface.

NOTE

The IPSU will begin discovery of all TN1U nodes in its NMS domain immediately upon insertion into the shelf. This process takes approximately 1 – 2 minutes per node in a ring. Complete access to all data-points will not be available until discovery is complete.

4. Click on the Configure button (available at the bottom of the Unit View).
5. To ensure that all the parameters got properly stored into the unit, go to the Setup tab, click on the *Paste* button again and check if the Configure button remains inactive. If not, click on the *Configure* button again. Repeat this sequence until the *Configure* button remains inactive upon the *Paste* action.

Installing MIB Files

The MIB (Managed Information Base) file is a text file in SNMP (SMIv2) that describes the TN1U system. The SNMP manager must compile this list before it can manage the agent and gain access to the information. General Electric provides the MIB in ASN.1 format that is compatible with existing commercial SNMP managers (HP Openview, DEC PolyCenter, IBM AIX Netview etc…) and it is available for customer download from www.jmux.com (customer login credentials are required). Refer to Appendix A for details on the MIB file.

6. CONFIGURATION

To configure the Service Unit (SU) or IP Service Unit (IPSU) locally, connect a PC running VistaNET software to the CI jack at the front of the unit through a COM port.[1] An 84910-05 RJ-11 cable and an 84910-06 (9-pin adapter) are required. In the VistaNET System Tree, click on the COM port connected to the unit.[2] The unit's programmable fields, information about the unit and the summary status of the node are displayed once the communication to the unit is established.

Most of the unit parameters can also be configured remotely through the network management system using VistaNET (if initialized with VNI license); however, some parameters must be configured locally prior to establishing the NMS connection to the unit. The capabilities and features of VistaNET network management software are described in the *VistaNET User's Guide.*

The units that are shipped as part of a purchased TN1U SDH node have their programmable fields set as per the Node Assignment Drawing (NAD) for the node. The SU and IPSU do not have any hardware adjustable options except for modem lockout strapping covered in the *Installation* section. All SU/IPSU configurations are performed through the software.

Note: *The descriptions related to IPSU are applicable only to the IPSU loaded with Linux OS and running VistaNET version 4.00+.*

WARNING

The user needs to reboot the unit after any of the IP-network-related configurable fields has been changed through VistaNET. This can be carried out using the Reboot Service Unit option in the System Tree menu.

NOTE

It may take a while for the VistaNET to connect to the IPSU when the IPSU is discovering the TN1U network or processing requests on its Ethernet interface.

[1] VistaNET must be initialized with either VNI (VistaNET Network Interface) or VLA (VistaNET Local Access) right-to-use license. For VistaNET installation and PC requirements refer to the VistaNET User's Guide.

[2] Only the COM ports provisioned for VistaNET use will appear in the System Tree. See VistaNET User's Guide for more information.

NOTE

After an IPSU reboots, the IPSU will begin a rediscovery process of the connected TN1U network. This process may take 1 –2 minutes per node in the TN1U network.

VistaNET Unit View Information

General Information

The VistaNET Unit View for the SU and IPSU (Figure 11) comprises various configurable and read-only fields grouped in three tabs[1]. Located below the tabs, are the context-sensitive help text-box and action buttons.

The VistaNET title bar (not shown in this manual) indicates the NMS path to the unit and is displayed in the following format:

// R<*Ring#*> / N<*Node#*>

Context-Sensitive Help

When the mouse-pointer is positioned over a specific field label, the text-box located at the bottom of this view will provide general information on the field. Also, for some fields, when the mouse-pointer is positioned over the field itself, more info is provided on that specific reading/selection.

Configure button

Writes the changes made in configurable fields to the unit.

Note*: Any changes made in the configurable fields will not take effect until after the Configure button is pressed. Multiple fields may be configured simultaneously.*

Undo button

Undoes the configuration changes written to the unit when the Configure button was pressed last time. It is possible to keep undoing previously performed configuration changes until the Undo button becomes disabled.

Note*: Upon moving to a different unit, VistaNET will forget the information on the last applied configuration changes. Therefore, the Undo action is possible only for the same unit to which the Configuration changes have been applied.*

[1] The third tab (TBOS Monitor) is available only if the user is connected to the unit locally.

Cancel button

Cancels the changes made in configurable fields and refreshes them with the previously displayed values.

***Note**: Only the changes made after the last Configure (or Undo) action can be cancelled.*

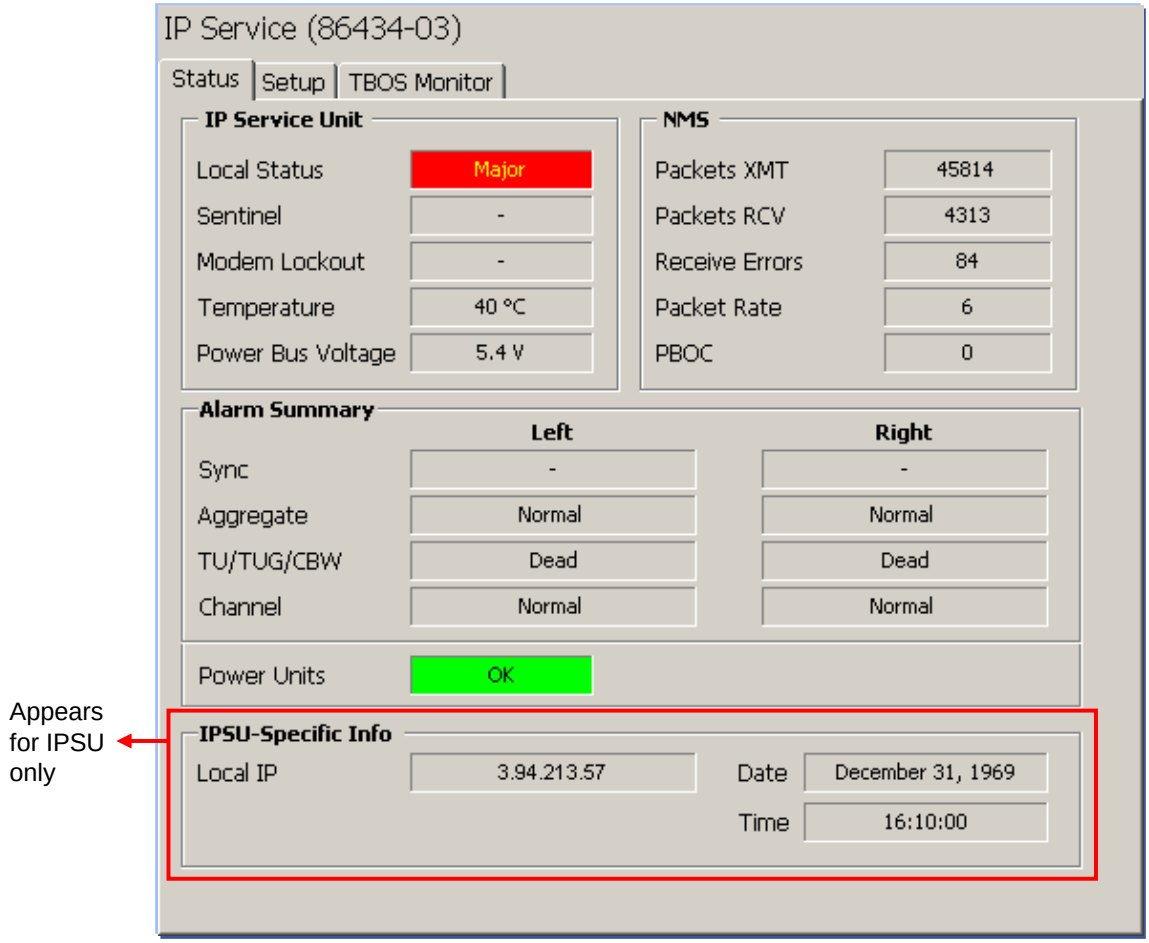


Figure 11: VistaNET Unit View for IP Service Unit – Status Tab

Copy and Paste buttons

These fields allow the user to copy the unit configuration settings to another unit of the same type. Click on *Copy* at the source unit, move the cable to the destination unit, and click on *Paste*. All the fields whose configurations are about to be changed are highlighted. Click on the *Configure* button to write the changes to the destination unit.

Note: *The source unit configuration settings are stored in the "clipboard" and may be applied to unlimited number of destination units of the same type.*

Note: *The user is allowed to modify the selections prior to pressing the Configure button.*

Note: *The user may opt not to apply the changes to the destination unit in which case the Cancel button shall be selected after the Paste action.*

Status Tab

When a VistaNET connection (local or network) to the unit is established, the Unit View is displayed with its Status tab selected. The content of the Status tab is shown in Figure 11.

Service Unit / IP Service Unit

Local Status

The status of the local node is reported in this field. May be MAJOR (red), MINOR (red) or OK (green or yellow). A MAJOR alarm will be reported if alarms are reported from both Left and Right STM-N Aggregate, TUG-3, or TIF level units. Typically, major alarms are reported for service affecting conditions.

A MINOR alarm is reported on any single alarm from the STM-N Aggregate units, TUG-3 units, TIF level units, Power units, or 64kb/s level units. Typically, minor alarms are reported for non-service affecting conditions.

The unit's front panel amber LED remains illuminated (latch) after a minor alarm condition clears which is reflected by OK (yellow) in this field. The latched alarm can be cleared through VistaNET by pressing the ACK button (Figure 5). The ACK button only appears if a latched alarm condition exists.

OK (green) indicates that no alarms (neither active nor latched) exist at the node.

Sentinel

Shows a summary of the Sentinel system or ring status. Sentinel Mode is configured in the SETUP tab.

When set to '-' (Disabled), '-' is displayed (grey background).

When set to RING, this field displays RING OK (green), RING-MINOR (orange) or RING-MAJOR (red).

When set to SYSTEM, this field displays SYSTEM OK (green), SYSTEM-MINOR (orange) or SYSTEM-MAJOR (red).

Modem Lockout

Displays the position of the paddleboard jumper (P8). Displays '-' when the lockout is disabled (P8 jumper set to Normal position) or 'Enabled' when the paddleboard jumper has been positioned in protected mode.

Temperature

Displays the current temperature of the Service Unit.

Power Bus Voltage

Displays the DC voltage on the power bus

NMS

Packet XMT

This field can be used to determine how many NMS packets this Service Unit has transmitted since this unit last reboot.

Packet RCV

This field can be used to determine how many NMS packets this Service Unit has received since this unit last reboot.

Receive Errors

This field can be used to determine how many NMS packets were received with errors since this Service Units last reboot.

Packet Rate

This field can be used to determine how many NMS packets this Service Unit is processing in a 32-second interval. This rate will depend on the number of nodes in the TN1U system – the more nodes, the higher the packet rate. Packet rates of a 1000 or less are considered normal. Packet rates above 1500 indicate that there is excessive NMS traffic and PBOC counts may begin to register.

PBOC (Packet Buffer Overflow Count)

The Service Unit has a receive packet buffer capable of storing 32 NMS packets. As the NMS packets arrive, they are queued in this buffer. The Service Unit's microprocessor processes the packets from the buffer. If the packets arrive at a rate faster than the micro

can process them, the packet buffer will overflow and lose some incoming packets. An increment in the PBOC field indicates that the buffer has overflowed and a packet has been lost. This further indicates that the NMS traffic is too high in the present TN1U system, i.e. the system needs to be broken into smaller systems.

***Note**: The Service Unit may encounter some PBOCs at boot-up, so there should only be cause for concern if this counter is incrementing.*

Alarm Summary

This section in the Status tab displays the overview status of the Left and Right External Sync units (if equipped), the Left and Right STM-N Aggregate units, the summary status for all Left and Right TU/TUG-3/CBW level units and the summary status for all 64kb/s level units and Power units at the local node.

Sync

-	The unit is not equipped.
Dead	The unit is faulty or is not present in the shelf.
Alarm	An alarm condition is detected on the unit.
Normal	The unit is alarm-free.

Aggregate

-	The left/right unit is not equipped.
Dead	The left/right unit is faulty or has been removed from the shelf.
Alarm	An alarm condition is detected at the left/right unit.
Yellow	An RDI is received on the left/right unit (the far-end unit is in alarm).
Test	A test condition is detected on the left/right unit.
Normal	No alarms or tests detected on the left/right unit.

TU/TUG/CBW

-	No left/right TU/TUG-3/CBW level units equipped.
Dead	At least one of the left/right TU/TUG-3/CBW level units is faulty or has been removed from the shelf.
Alarm	An alarm condition is detected on at least one of the left/right TU/TUG-3/CBW level units.
Yellow	An RDI is received on at least one of the left/right TU/TUG-3/CBW level units (the far-end unit is in alarm).
Test	A test condition is detected on at least one of the left/right TU/TUG-3/CBW level units.

Normal No alarms or tests at the left/right TU/TUG-3/CBW level units.

Channel

- No channel units reporting their status through a Left/Right CMUX unit are equipped.

Dead At least one of the previously detected channel unit is non-responsive (either faulty or removed from the shelf).

Alarm An alarm condition on at least one channel unit.

Test A test condition on at least one channel unit.

Normal No alarms or tests at the channel units.

Power Units

Summary status of the Power units at this node. May be ALARM or OK (no alarms).

IPSU-Specific Info

(Applicable to IPSU only.)

Local IP

Displays the IP address of the IPSU.

Date

Displays the current date as per the IPSU's internal clock.

Time

Displays the current time as per the IPSU's internal clock. Time is displayed to one minute accuracy (full minutes only).

Setup Tab

The Service Unit VistaNET Setup Tab (Figure 12) allows the user to configure the majority of the Service Unit parameters. There are some additional configurations that are specific to the IPSU (see Figure 13).

Overhead Allocation

NMS Location

This field identifies the STM-N overhead bytes that are used to carry the Orderwire, 4W VF Partyline and NMS information. May be set to either SOH (Section Overhead) or STUFF (stuffing bytes of one of the TUG-3-structured VC-4s, or the stuffing bytes of a TU-

12 carrying TU-11 traffic, or a dedicated TU-12). SOH is the default selection. STUFF is selected if it is required to ensure that TN1U NMS and Orderwire/Partyline information is passed through a foreign (non-TN1U) SDH system separating parts of the same TN1U network.

Note: *This setting must match the setting in the local STM-N Aggregate units' "NMS Location" field. Refer to the STM-N Aggregate Unit TPIM for more information.*

Note*: This field must be programmed identically at all Service Units within the same ring or linear TN1U network.*

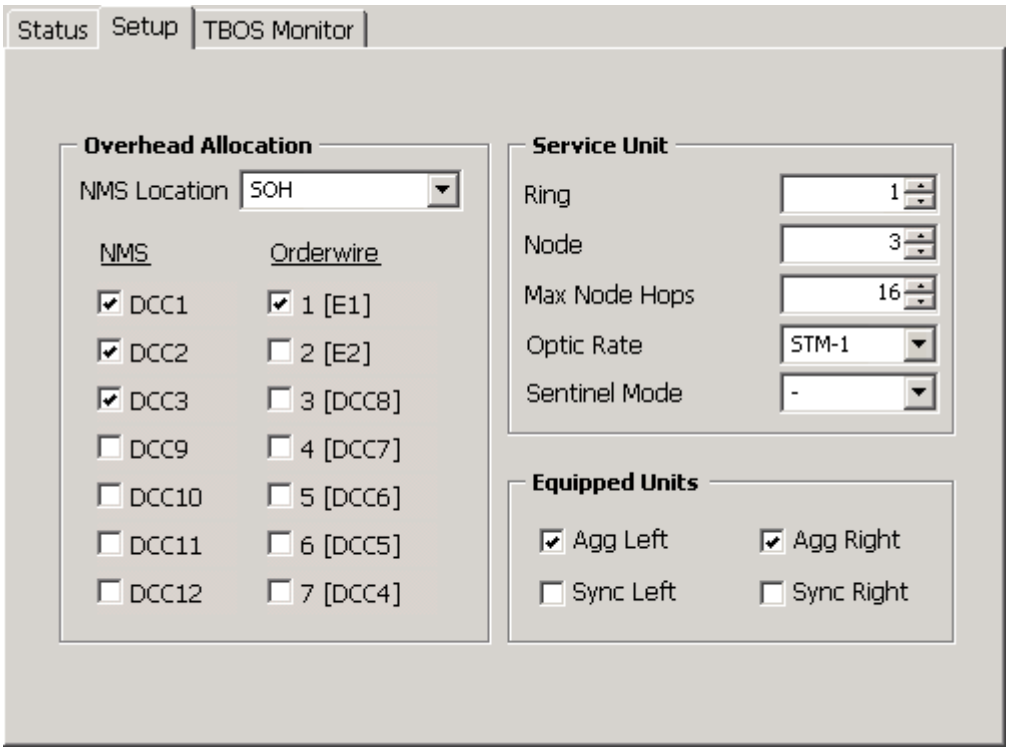


Figure 12: Service Unit Setup Tab

NMS

This field identifies the bytes in either the Section Overhead or the Path Overhead area (depending on selection made in the "NMS Location" field) that are used by the NMS for inter-node communication. Up to three contiguous SOH or VC-4/TU-12 stuff bytes may be used. To maximize the bandwidth available for NMS transport, it is recommended that three contiguous NMS bytes be selected.

The following NMS bytes are available:

In TOH: DCC12, DCC11, DCC10, DCC9, DCC3, DCC2, DCC1
In STUFF: R9, R8, R7

When STUFF bytes are used, the bytes R8, R7 and R6 are selected automatically (not user-selectable).

***Note**: The same NMS byte(s) must be assigned in all Service Units within the same ring or linear TN1U network.*

Orderwire

This field identifies the channels (bytes) in either the Section Overhead or VC-4/TU-12 stuff bytes (depending on the selection made in the "NMS Location" field) that are dropped at this node. The following channels are available:

Chan.	1	2	3	4	5	6	7
TOH	E1	E2	DCC8	DCC7	DCC6	DCC5	DCC4
STUFF	R16	R15	R14	R13	R12	-	-

Each of the seven/five channels may be assigned to an independent Orderwire/Partyline system. Only the channels assigned to the Orderwire/Partyline systems that are to be accessed at this node should be selected.

Service Unit / IP Service Unit

Ring #

The Ring # identifies the network (ring or linear network) in which this node is connected. All nodes in a network must have the same Ring Number. The Ring Number can be any value from 1 to 255 and it must be unique from other networks in the TN1U system. The Ring and Node numbers define the node address used for NMS communication.

Node #

The Node # identifies the node number in this ring or linear network. The Node Number can be any value from 1 to 255 and it must be unique within a ring or linear network. The Ring and Node numbers define the node address used for NMS communications.

Max Hops

This parameter is used to limit the lifetime of NMS packets in multiple ring/linear networks. It is normally set to the total number of Service Units (nodes) in the NMS domain. However, if the

number of nodes is less than 16, Max Hops parameter should be programmed to 16.

***Note**: This field must be programmed identically at all Service Units belonging to the same NMS domain.*

Optic Rate

May be set to STM-1, STM-4 or STM-16. The Service Unit must be programmed in accordance with the type of STM-N Aggregate units installed at this node. If the programming of this field does not match the type of STM-N Aggregate units, VistaNET will not discover inventory correctly.

Sentinel

May be configured to '-' (disabled), RING or SYSTEM. The appearance of the field is different for each of these modes of operation.

When the Sentinel Alarm Mode is configured to DISABLED, the Form-C relays will activate only if there are alarms at this local node. This alarm mode is indicated by a "-" reading in this field.

When the Sentinel Alarm Mode is configured to RING, the Form-C relays will activate if there is a local alarm or if any other node that is in the same network (ring or linear network) as this Service Unit has an alarm. Therefore, if a node in a different ring has an alarm, it will not activate the Local Form-C relays. The Sentinel Ring status is displayed in the Sentinel field of the Status tab, and may be RING-MAJOR, RING-MINOR or RING OK (no ring alarms).

When the Sentinel Mode is configured to SYSTEM, the Form-C relays will activate if there is a local alarm or if any other node in the same NMS domain has an alarm. (All ring or linear networks interconnected with NMS-Tie cables belong to the same NMS domain.) The Sentinel System status is displayed in the Sentinel field of the Status tab, and may be SYSTEM-MAJOR, SYSTEM-MINOR or SYSTEM OK (no system alarms).

***Note**: If a valid remote alarm is present at one node in a TN1U network/system and during this alarm state the ACK button on the Service Unit (at the node in alarm) is pressed, then this remote alarm is masked at the Sentinel node (node with the Sentinel Alarm Mode enabled) as long as the ACK button is pressed. During the remote alarm mask state, the Form-C relay at the Sentinel node will deactivate.*

Valid remote alarms at multiple TN1U nodes will be reflected at the Sentinel node even if the ACK button is pressed at any one remote node in alarm.

***Note**: Since the Sentinel alarm operation uses NMS packets to transport the alarm status information of remote nodes, the prerequisite for its proper operation is correct setup of all Service Units in the TN1U system.*

Equipped Units

Agg Left/Right

May be set to 'Equipped' (checked) or 'Not Equipped' (unchecked) to indicate whether the Left and Right STM-N Aggregate units are equipped at this node (default is 'Equipped'). If a node is equipped with only one STM-N Aggregate unit (e.g. terminal nodes in a linear network) the checkbox corresponding to the missing unit must be unchecked, otherwise, the Service Unit will generate alarms for the missing STM-N Aggregate unit.

***Note:** If the Left/Right checkbox is mistakenly unchecked, VistaNET will not attempt to discover the respective STM-N Aggregate unit nor any other units connected to its TIF/TUG-3/CBW ports. Any alarms produced by these units will neither be reflected on the Service unit nor reported to NMS.*

Sync Left/Right

May be set to 'Equipped' (checked) or 'Not Equipped' (unchecked) to indicate whether the Left and Right External Sync Units are equipped at this node (default is 'Not Equipped').

***Note:** If the left/right External Sync Unit is installed and the respective checkbox is mistakenly kept unchecked, the unit will remain undiscovered by VistaNET. Any alarms produced by this unit will neither be reflected on the Service unit nor reported to NMS.*

Network Setup

(Applicable to IPSU only.)

The IP Service Unit's Setup Tab is slightly different to that of its Service Unit counterpart. In addition to all the fields described above, the IPSU has some additional ones as shown in Figure 13.

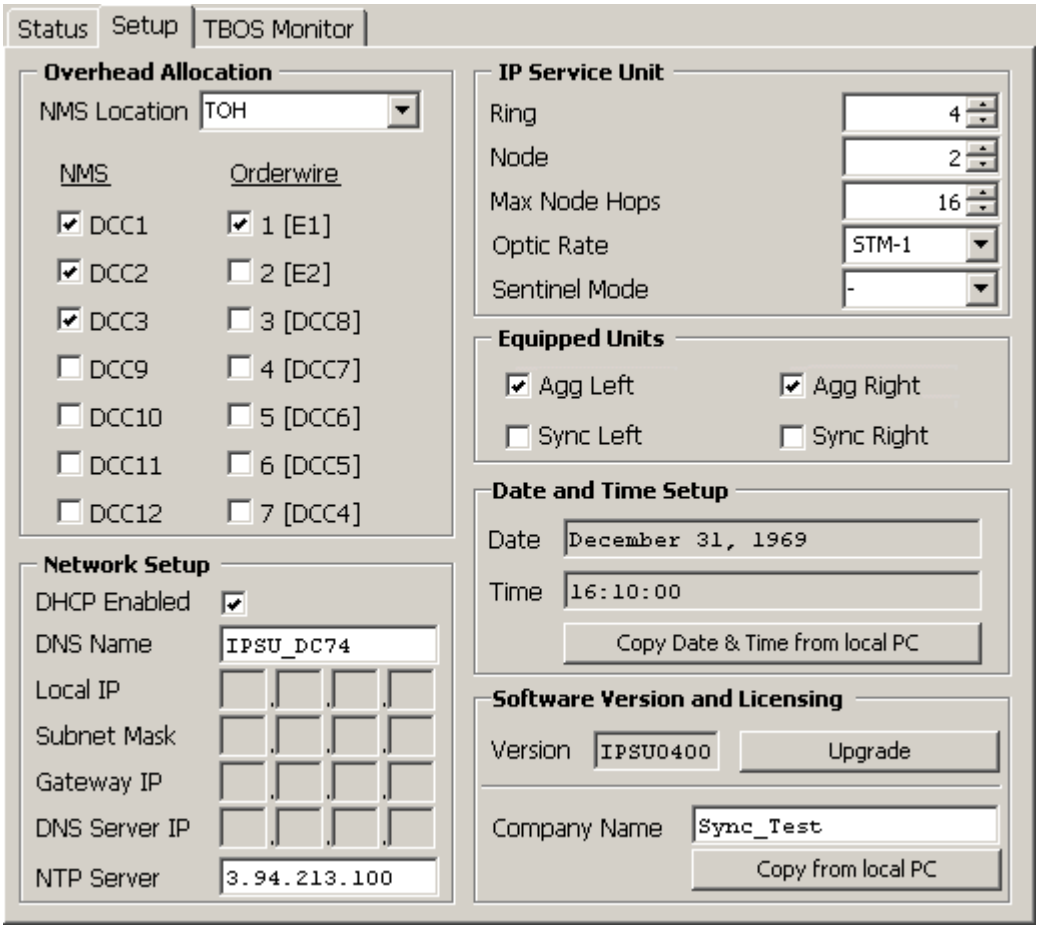


Figure 13: IP Service Unit Setup Tab

DHCP Enabled

Check if a DHCP server is present on the network and the IP address is to be assigned dynamically. Uncheck if the IP address is to be assigned statically.

DNS Name

Allows the user to configure the DNS Name of the IPSU. The default factory setting is unique for each IPSU. The maximum string length is 15 characters.

Local IP

The IPSU is designed to obtain its IP address statically or dynamically (via DHCP). When the DHCP Enabled check box is ticked, the unit's IP address is assigned dynamically. Otherwise a valid IP address must be entered into this unit.

Note: *If a static IP address is assigned, the SUBNET MASK, GATEWAY IP and DNS SERVER IP fields should be configured (if applicable).*

Note: *If the IPSU is programmed to use DHCP without an available DHCP server, the IPSU will be assigned an IP address of 127.0.0.1 in accordance with TCP/IP convention.*

Subnet Mask

A Subnet is a segment of a network that shares a common address. A sub-mask is used within networks to simplify the routing tables of gateway routers used to manage IP traffic, to add security and improve network performance. When a sub-mask is applied, the Network ID and Host ID is modified according to the mask applied. No sub-mask is required when a DHCP server is used.

Gateway IP

LAN's are typically managed by devices that limit the MAC domains to improve the dependability and efficiency of the LAN. Gateway Routers provide this functionality and therefore must be assigned an IP address. All hosts on a LAN (including an IPSU) must establish a connection with this gateway to communicate with devices external to its LAN. No Gateway IP is required when a DHCP server is used.

DNS Server IP

The DNS server translates DNS names into IP Addresses. If DNS names are supported, then a DNS server must be positioned into the network. This server must also have a valid IP address. No DNS Server IP is required when a DHCP server is used.

NTP Server

Allows the user to enter the NTP server's IP address. This is required if the unit is expected to synchronize its internal clock with the NTP server's clock.

Date and Time Stamp

(Applicable to IPSU only.)

Displays the current date and time as per the IPSU's internal clock. When the unit is provisioned, the user is expected to set the date and time (along with the local time zone) using the "Copy Date & Time from local PC" button. From that point on, the unit will synchronize from the NTP Server (if the NTP server

is available and its IP address is entered in the respective field). Otherwise, the unit's internal clock will be free-running but it can be occasionally adjusted using the "Copy Date & Time from local PC" button. This "copy" function can be carried out either locally or remotely.

Note: *Time is displayed to one minute accuracy (full minutes only).*

Software Version and Licensing

(Applicable to IPSU only.)

Version

Indicates the version of the VistaNET program loaded into the IPSU. The format is IPSUnnnn, where nnnn indicates the VistaNET version. For example, IPSU0400 indicates VistaNET version 4.00.

Upgrade [to nn.nn]

Allows the user to load the newer VistaNET version into the IPSU. The reading "Upgrade to nn.nn" appears if the newer version of VistaNET is detected on the local PC. Otherwise, it reads "Upgrade" in which case the button is greyed out and inactive.

Note: *In order for the IPSU to synchronize with remote VistaNET services, their installed support package / VistaNET versions need to match.*

Note: *When upgrading an IPSU to which only IP connection exists, the IPSU must be upgraded before upgrading the VistaNET installation on the PC from which the upgrade is being carried out.*

Company Name

The displayed company name must match the one used by remote VistaNET services to allow the IPSU to synchronize with them. Normally, all VistaNET PCs used by any given customer organization are using the same customer name (as defined by GE when the Master Passport file for the customer was created).

Although the user is allowed to enter the company name manually, it is strongly recommended to copy this parameter from the local PC using the "Copy from local PC" button.[1]

[1] Manual editing of the Company Name will not be allowed in future VistaNET releases.

TBOS Monitor Tab

(Requires local VistaNET connection to the unit.)

The TBOS Monitor Tab comprises two sub-tabs, the Network Element sub-tab (Figure 14) and the TBOS Setup sub-tab (Figure 15). This tab is used only when the TBOS interface is used with external equipment.

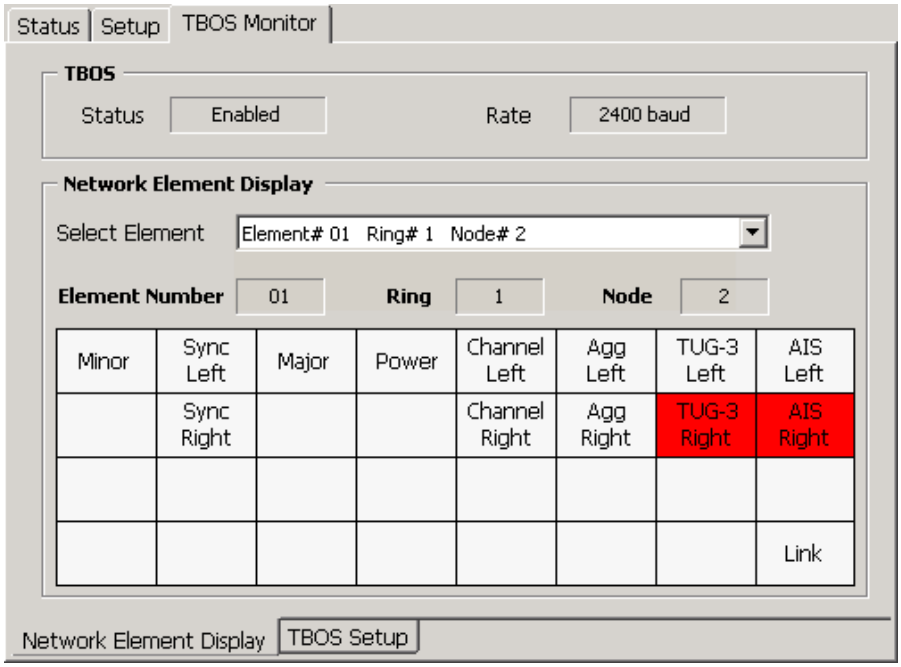


Figure 14: TBOS Monitor Tab – Network Element Display Sub-Tab

Network Element Display Sub-Tab

TBOS Status

May be ENABLED or DISABLED. Go to TBOS Setup sub-tab to configure.

TBOS Rate

Displays the current TBOS interface baud rate. Go to TBOS Setup sub-tab to configure.

Select Element

Each element defined in the TBOS Setup sub-tab is added to this drop down list for convenient retrieval of nodal information.

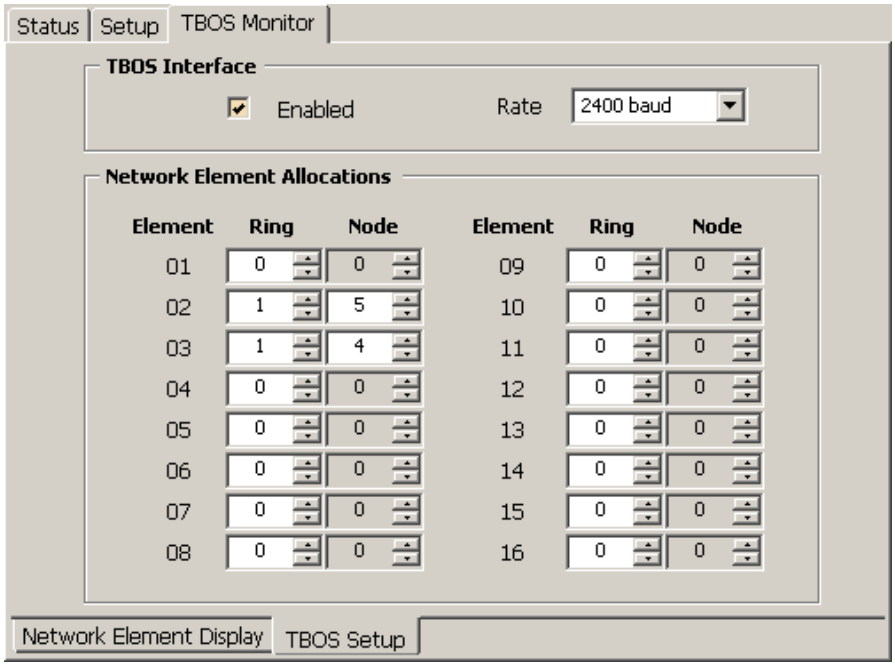


Figure 15: TBOS Monitor Tab – TBOS Setup Sub-Tab

TBOS Setup Sub-Tab

TBOS Status

May be ENABLED or DISABLED. If the TBOS output is not used, it should be OFF (disabled). This preserves the unit's processing capacity. The TBOS output should be activated only on the Service Units connected to TBOS RTUs.

TBOS Rate

Displays the current TBOS interface baud rate. May be programmed to 1200, 2400, 4800, 9600 or 19200 baud.

NOTE
The Service Unit must be reset (removed and reinserted) after changing the TBOS baud rate! Otherwise, the change will NOT take effect.

Element / Ring / Node

Users can define up to 16 network elements by allocating the Ring number and Node number to each of them. When Ring 0 and Node 0 is allocated to an element, the element is not used.

Note: *The node number field becomes enabled when the ring number is changed to some value other than 0.*

7. MAINTENANCE and TROUBLESHOOTING

Context-Sensitive Help

When the mouse-pointer is positioned over a specific field label in the VistaNET Unit View, the text-box located at the bottom of the view will provide general information on the field. Also, for some fields, when the mouse-pointer is positioned over the field itself, more info is provided on that specific reading/selection. This is a useful tool for explaining the capabilities and options of both programmable fields and read-only fields of the unit.

Alignment

The Service Unit must be correctly configured as per the Node Assignment Drawing. All software adjustable fields are detailed in the Configuration section of this manual. The user must ensure that all external connections to the paddleboard are correct.

Troubleshooting

If a Service Unit or IP Service Unit is suspected of being defective, substitute it for a known-good unit and if the replacement unit functions properly return the original to GE Multilin for repair or replacement. Ensure that the substitute unit is configured correctly.

The following table is intended to provide the user with possible solutions to problems that may be encountered during normal unit operation.

Symptom	Probable Cause / Solution
Local Power unit alarm is not reported on Service Unit	Verify that the Power Monitor on the Service Unit Paddleboard is properly wired to Alarm Relay contacts on all Power unit Paddleboards at the node.
Unit LEDs do not illuminate when the ACK button is pressed	The unit's microprocessor may have locked up. Reseat the Service Unit, or restart the IPSU through the unit's web-server.

PBOC increments	When NMS domains become very large (greater than 100 nodes NMS-tied together), the Service Unit may not be able to process all packets, especially during alarm bursts. Break large NMS domains into smaller groups by removing some NMS-tie connections and use multiple VistaNET com ports to connect with the multiple groups. Alternatively, optimize the NMS domains and deploy a network of VistaNET servers, one for each.
Service Unit not-responding	After a Service Unit has been rebooted, the device can take between 60 – 90 seconds to show up in VistaNET.
SNMP Manager or VistaNET Client cannot connect with an IPSU	There is no visual indication on the IPSU that he unit is connected to a LAN. VistaNET and the SNMP manager do provide connectivity status, therefore, if problems exist, do the following: - Check the IP address of the IPSU, IPSU's gateway router using ICMP (PING) or network analyzer to identify the network problem. - Ensure the correct Sub-Mask has been applied and the IPSU (Host ID) has not been statically assigned an invalid Subnet ID. - Attempt to ping the DNS name. Replace a DNS name with an IP address (of the IPSU) if the DNS name is not responding to a ping. - Verify that the IPSU has been loaded with a valid support package by plugging into the IPSU CI port with a PC (com port) running VistaNET. Select the Setup tab of the IPSU and check the "Version" field. If none is displayed, then install a package (see *Configuration* section of this manual). - Ensure that any personal or corporate firewalls are configured to allow these services to pass. - Replace cable or switch from crossover cable to straight-through (or vice versa).
SNMP-specific troubleshooting	• After restarting an IPSU, the SNMP manager should receive a COLD START trap within seconds after it boots. If not, then: - Check that the SNMP agent uses UDP port 161 to listen for incoming requests and port 162 to send traps. While these are standard ports, they must be configured to allow traffic over these ports. - Ensure trap destinations and community string have been configured on a VistaNET PC that is capable to synchronize with IPSU. The IPSU must be restarted (through the VistaNET system tree) after a change in any of these settings has been synchronized and applied. • The SNMP manager must compile the TN1U MIB. • Ensure the IPSU has been configured for SDH or Mixed system. This can be done by making a proper selection in VistaNET (running on a PC) and then synchronizing with the IPSU.

VistaNET-server-specific troubleshooting	• Check VistaNET error log for connection problems with the IPSU. Follow the error log message (i.e. restart VistaNET or restart the IPSU through the unit's web-server). • Check the network availability is high. Excessive collisions and high utilization can cause loss of network connection between the IPSU and VistaNET. • IPSU's responsiveness is considerably slower than normal. If an IPSU has been disconnected from a LAN for extended periods, this condition can be observed. The IPSU should be restarted through the web-browser if the condition does not improve. • The IPSU is also running a watchdog program that will reboot the IPSU automatically if available memory becomes critically low or if the server code stops running. • Router must enable UDP port 8644 (Multicast) as well as TCP ports 8644(Synchronization) and 8633 (Remote Data). • Network Administrators should ensure all IPSU's are 'ready' before a system discovery is attempted and MUST check that the discovered results returned contain inventory from all services. • The version of the VistaNET Support Package loaded onto the IPSU must be aligned with the version of the VistaNET program installed on PCs. Upgrade the IPSU or VistaNET installation on PCs, as applicable. NOTE: When upgrading an IPSU to which only IP connection exists, the IPSU must be upgraded before upgrading the VistaNET installation on the PC from which the upgrade is being carried out.

Table 1: Service Unit and IPSU Troubleshooting Table

8. NMS FEATURES

Features

The NMS allows remote monitoring, testing, forced path switching and reconfiguration of any node from any other node in the system. This includes multiple rings plus linear/spur configurations. A "check-back" is done before any actual reconfiguration to protect against incorrect configuration commands.

The NMS provides simultaneous monitoring and configuration from more than one node. By allowing multiple user access, maintenance personnel have real time information of the network for testing and troubleshooting, as well as the potential of back-up control centres.

An industry standard graphical user interface (Microsoft Windows) for displaying the desired level of detail is used. The user can access all unit levels from the STM-N Aggregate unit down to the 64kb/s channel unit level. For example, this allows displays of information all the way from the STM-N Aggregate optical receive power level, to the state of DTT relaying channels and to the current/voltage levels on the pilot wire interfaces.

A user's choice of TOH bytes or POH bytes for NMS transmission through a foreign SDH system is provided.

In ring networks, NMS communication channel is protected against ring failures.

VistaNET Features

For detailed information, refer to the *VistaNET User's Guide (86456) or VistaNET help engine (available in VistaNET v4.00+)*.

9. SPECIFICATIONS

Type	Parameter	Service Unit Specification	IPSU Specification
Physical	Height	89 mm (3.5 in.)	89 mm (3.5 in.)
	Width	29 mm (1.135 in.)	29 mm (1.135 in.)
	Depth	203 mm (8.0 in.)	203 mm (8.0 in.)
	Weight	226 g (8 oz)	236 g (8.5 oz)
Electrical	Voltage (Supplied from the Common Equipment Shelf)	5.2 VDC ±5%	5.2 VDC ±5%
	Current	160 mA @ +5 VDC	510 mA @ +5 VDC
	Power Consumption	0.8 W	2.55 W
TBOS Interface	Transmission Rate (programmable)	1200, 2400, 4800, 9600, or 19200 baud; 2 stop bits with odd parity	1200, 2400, 4800, 9600, or 19200 baud; 2 stop bits with odd parity
	Transmission Type	Half Duplex	Half Duplex
	Transmission Medium	26 gauge 100 ohm twisted pair	26 gauge 100 ohm twisted pair
Form-C Relays' Rating at 25ºC		120 mA, 350 V On Resistance: 15 – 35 Ohms	120 mA, 350 V On Resistance: 15 – 35 Ohms
Environmental	Temperature: Guaranteed Performance	-20º to +60º C (-4º to +140º F)	-20º to +60º C (-4º to +140º F)
	Temperature: Storage	-40º to +70º C (-40º to +158º F)	-40º to +70º C (-40º to +158º F)
	Relative Humidity	5 to 95% @ 40º C, Non-condensing, 10 days	5 to 95% @ 40º C, Non-condensing, 10 days
	Shipping Altitude	15,000 m; (50, 000 feet)	15,000 m; (50, 000 feet)

Type	Parameter	Service Unit Specification	IPSU Specification
Mechanical	Vibration	per MIL-STD 810E	per MIL-STD 810E
	Bench Handling	per TS 1-00446.06	per TS 1-00446.06
RFI		Meets ANSI/IEEE C37.90.2	Meets ANSI/IEEE C37.90.2
Isolation		Meets ANSI/IEEE C37.90.1, for surge withstand and fast transients on alarm leads	Meets ANSI/IEEE C37.90.1, for surge withstand and fast transients on alarm leads
Reliability		MTBF = 350,000 Hours (40 years) Calculated per TR-NWT-000332	MTBF = 200,000 Hours (22 years) Calculated per TR-NWT-000332
Network	Protocol		TCP/IP, UDP/IP, ICMP, DHCP, SNMPv2c
	Interface	RS-232C	10Base-T Ethernet (RJ45), RS-232C
	IPSU Client		VistaNET Network Interface (VNI), SNMP managers

Table 2: Service Unit and IPSU Specifications

10. ORDERING INFORMATION

This section covers the ordering information for a single Service Unit or IP Service Unit and is not intended to replace standard engineering documentation or drawings.

Please contact the Account Manager for your area regarding ordering the Service Unit/ IP Service Unit.

Equipment and Option Code List

Equip-ment	Option Code	Description
B86434	-02	Service Unit. Provides major and minor office alarms, Orderwire channels' access and capabilities to monitor and configure all TN1U nodes in the same NMS domain via a serial RS-232 connection. Black faceplate. Used with 86434-8X paddleboard.
86434	-02	(DISCONTINUED IN JUNE 2008) Same as B86434-02 but with grey faceplate.
B86434	-03	IP Service Unit. Same as B86432-02 but also provides SNMP agent functionality and VistaNET server functionality for TN1U nodes within its NMS domain.[1] Black faceplate. Used with 86434-81 paddleboard.
86434	-03	(DISCONTINUED IN JUNE 2008) Same as B86434-03 but with grey faceplate.
86434	-80	(DISCONTINUED IN OCTOBER 2005) Service Unit Paddleboard assembly. Provides connections for office alarms, Orderwire / 4W VF Partyline units and NMS-Tie interfaces. One required per (B)86434-02 unit.
86434	-81	Service Unit / IP Service Unit Paddleboard assembly. Provides connections for office alarms, Orderwire / 4W VF Partyline units, NMS-Tie interfaces and Ethernet 10Base-T interface[2]. One required per (B)86434-02 or (B)86434-03 unit.

Table 3: Equipment and Option Code List

Note: For NMS-Tie connections, the 035-86430-4X cables are required (refer to *NMS-Tie Connections* on Page 31 for more information). For connecting Orderwire/Partyline units, the cable 035-86430-15 (17") is required (refer to *Orderwire CBUS* on page 31).

[1] Requires use of support package 4.00+. Authorized users can download the latest support package onto their PCs from www.jmux.com and then download it onto the IPSU.
[2] Ethernet interface is not functional when the paddleboard is used with (B)86434-02 unit.

APPENDIX A

SNMP

As previously discussed in Section 2 of this manual, SNMP (Simple Network Management Protocol) is an internetworking management tool that has seen tremendous popularity since its inception in 1988. The reason being is its simplicity, although don't confuse "Simple" with "Trivial". SNMP compared to other networking protocols is simple, yet its feature set is sufficiently powerful in managing diverse commercial networks through the exchange of management information.

SNMP uses an Agent / Manager model to pass information between managed devices and the network administrator who performs network management functions (i.e. network performance, finding and solving network problems and planning for future growth). An SNMP agent interfaces to managed devices (i.e. router), which contain managed objects. A managed object is a device or characteristic of something that can be managed, like a configuration parameter, or performance statistic and relates directly to the current operation of the device. In TN1U, the IPSU is a proxy SNMP agent that manages all TN1U units within the same NMS domain. The Managed objects within TN1U system are the data points for each TN1U unit. The figure below shows the SNMP Agent / Manager model.

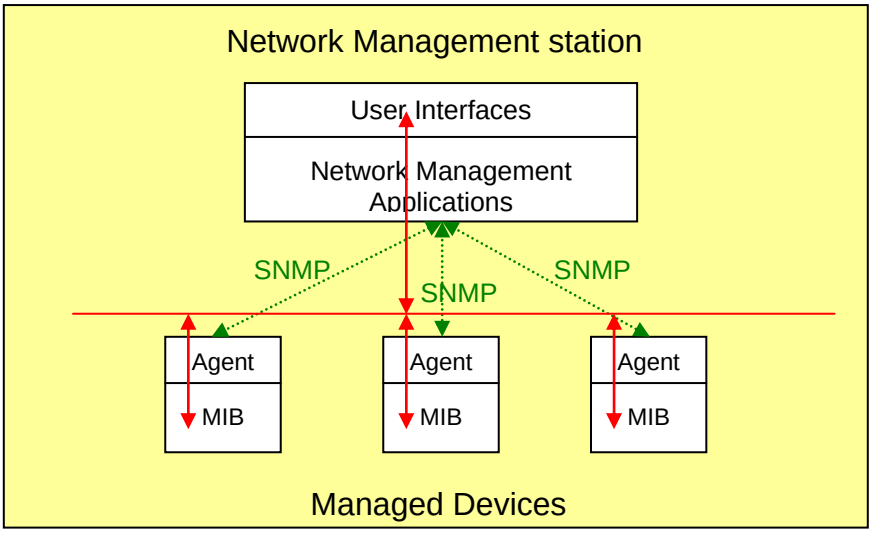


Figure 16: SNMP Model

MIB

The SNMP agent (residing in the IPSU) manages TN1U units and stores their data points (managed objects) in grouped tables within in a MIB (Management Information Base) file. Within the MIB file, Managed Objects must have a standardized name, syntax and an encoding method so that any computer can share the information. OSI have defined SMI (Structure of Management Information) as this standard language. The SMI defines the name of each managed object as an Object Identifier (OID), the syntax (ASN.1) defines the data type, and the encoding (in Basic Encoding rules) describes how the data within the managed objects is serialised for transmission between machines. MIB files can be viewed directly by a MIB browser (i.e. MG-Soft™) and is depicted as a hierarchical tree, with individual data items making up the leaves of the tree (see Figure 17 for the Lentronics Multiplexers MIB Tree which include the OIDs).

Figure 17: Lentronics Multiplexers MIB file

Vendors (i.e. GE Lentronics) can define their own private branches within the Enterprise sub-tree to include instances of their own product. "Lentronics" is a registered object with ID 1.3.6.1.4.1.11134. This tree has been grouped into 7 tables, each includes a table name and specific table column headings, all of which having unique OIDs. The data points that are discovered during the IPSU discovery process are referenced to a unit ID and stored into these tables.

SNMP Commands

To keep SNMP simple, a simple set of commands must be supported. The Management system issues Protocol Data Units (PDU's) like GET, GETNEXT and GETBULK to retrieve single or multiple object variables and a SET commands (although the IPSU agent only supports a single SET command as described earlier in this document). The Managed Agent (IPSU) can also send a TRAP (Alarm) to the management system to identify occurrences of conditions that have exceeded a predefined threshold.

Each SNMP message sent follows the following format and must include:

- Version Number (ensure that the same SNMP version is used)
- Community name (kind of password for weak authentication and is set to "public" although can be changed through the IPSU's Web-Server to match the community domains of the manager)
- One or more SNMP PDU's (Get, GetNext etc…) where all PDU's (except trap) include the following message construct
    - Request ID
    - Error status
    - Error Index
    - List of OIDs and Values (for Get requests, the value is zero).

When access to the data points is required, a PDU is sent that must include a unique OID(s). The OID(s) must rely on information in other tables (Structure to obtain Unit ID) and Subscription to obtain a group name etc…) before the specific data point value can be returned.

For SNMPv2, an "envelope" is applied to the aforementioned SNMP message and included additional authentication and privacy information for the destination and source parties.

APPENDIX B

LIST OF ILLUSTRATIONS

List of Figures

FIGURE #	DESCRIPTION	PAGE

Figure 1: Visibility of two TN1U rings on one VistaNET workstation 9
Figure 2: Visibility of two separate TN1U systems on one VistaNET PC 10
Figure 3: Control of two separate TN1U systems with IPSUs installed 11
Figure 4: VSA server, IPSU server and VistaNET clients..... 16
Figure 5: Front Panel Layout..... 17
Figure 6: 13-Byte Header Details 24
Figure 7: Typical Rack Layout for a TN1U SDH Node 27
Figure 8: 86434-80 Service Unit Paddleboard Connections..... 29
Figure 9: 86434-81 Service Unit Paddleboard Connections..... 30
Figure 10: NMS-TIE Connections 32
Figure 11: VistaNET Unit View for IP Service Unit – Status Tab..... 38
Figure 12: Service Unit Setup Tab 43
Figure 13: IP Service Unit Setup Tab..... 47
Figure 14: TBOS Monitor Tab – Network Element Display Sub-Tab..... 50
Figure 15: TBOS Monitor Tab – TBOS Setup Sub-Tab 51
Figure 16: SNMP Model..... 59
Figure 17: Lentronics Multiplexers MIB file..... 60

List of Tables

TABLE #	DESCRIPTION	PAGE

Table 1: Service Unit and IPSU Troubleshooting Table 54
Table 2: Service Unit and IPSU Specifications..... 57
Table 3: Equipment and Option Code List..... 58

APPENDIX C

LIST OF ACRONYMS

- ACK Acknowledge
- ACO Alarm Cut-Off
- ANSI American National Standards Institute
- ASN.1 Abstract Syntax Notation One
- BER Bit Error Rate
- CBUS Channel Bus
- CI Craft Interface
- COM Communication
- CRC Cyclic Redundancy Check
- DC Direct Current
- DCC Data Communication Channel
- DHCP Dynamic Host Configuration Protocol
- DOS Disk Operating System
- DNS Dynamic Name System (or Service)
- DTT Direct Transfer Trip
- EAS Equipment Assembly Schematic
- EIA Electronic Industries Association
- ESDS Electrostatic Discharge Sensitive
- FPGA Field Programmable Logic Gate Array
- ID Identification
- ICMP Internet Control Message Protocol
- IEEE Institute of Electrical and Electronics Engineers
- IP Internet Protocol
- IPSU IP Service Unit
- LAN Local Area Network
- LED Light Emitting Diode
- LS Low Speed
- MIB Management Information Base
- MTBF Mean Time Between Failure
- NAD Node Assignment Drawing

- NMS Network Management System
- NTP Network Timing Protocol
- OAM&P Operations, Administration, Maintenance and Provisioning
- OID Object Identifier
- PBOC Packet Buffer Overflow Count
- PC Personal Computer
- PDU Protocol Data Units
- PLM Product Line Management
- RCV Receive
- RTU Remote Terminal Unit
- SCADA Supervisory Control and Data Acquisition
- SDH Synchronous Digital Hierarchy
- SMI Structure of Management Information
- SNMP Simple Network Management Protocol
- SOH Section Overhead
- SPI Serial Port Interface
- STM Synchronous Transport Module
- SU Service Unit
- SYNC Synchronous
- TBOS Telemetry Byte Oriented Serial
- TCP Transmission Control Protocol
- TLCI TN1U Local Craft Interface
- TIF TN1U Intermediate Format
- TOH Transport Overhead
- TPIM Technical Practice and Installation Manual
- TU Tributary Unit
- TUG Tributary Unit Group
- UDP User Datagram Protocol
- VC Virtual Container
- VF Voice Frequency
- VNI VistaNET Network Interface
- VSA VistaNET Server Application
- WAN Wide Area Network
- XMT Transmit