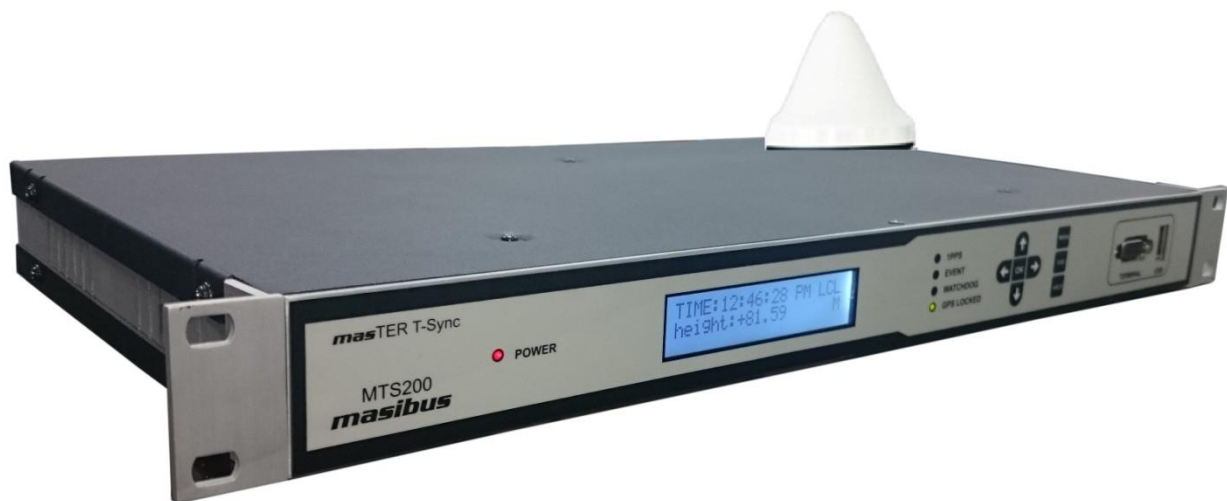


User's Manual

masTER T-Sync



Masibus Automation And Instrumentation Pvt. Ltd.

B/30, GIDC Electronics Estate,
Sector-25, Gandhinagar-382044, Gujarat, India

☎ +91 79 23287275-79 📠 +91 79 23287281-82

Email: support@masibus.com

Web: www.masibus.com

LIMITED WARRANTY

Masibus Automation and Instrumentation Pvt. Ltd. Provides limited warranty for its manufactured product against the defects in material shipped, workmanship under normal use and service for the period of 12 months or as per the warranty period terms agreed, from the date of shipment of product. This warranty shall not apply if the product is used contrary to the instructions in its manual or is otherwise subject to misuse, abnormal operations, accident, lightning or transient surges, repairs or modifications not performed by Masibus Automation and Instrumentation Pvt. Ltd.

Necessary items packed with *masTER* T-Sync such as antenna, lightening arrestor, antenna line amplifier and other accessories are also provided with limited warranty of 12 months from the date of shipment.

Masibus Automation and Instrumentation Pvt. Ltd. Obligation under this warranty are limited to in-factory service and repair, of the product or the component thereof, which is found to be defective. If the defect for which Masibus Automation and Instrumentation Pvt. Ltd. Is found not responsible for the defect or the cause of defect in product, the service or repair will be done on the charge basis.

For warranty service or repair, products if returned to a service facility at Masibus Head Office, buyer shall prepay all shipping charges to Masibus. Masibus highly recommends that prior to returning equipment for service work, our technical/Customer support department be contacted to provide trouble shooting assistance while the equipment is still installed.

EXCEPT FOR THE LIMITED WARRANTY STATED ABOVE, MASIBUS AUTOMATION AND INSTRUMENTATION PVT. LTD. DISCLAIMS ALL WARRANTIES OF ANY KIND WITH REGARD TO ITS PRODUCTS OR OTHER MATERIALS PROVIDED BY MASIBUS, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTY OR MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Masibus Automation and Instrumentation Pvt. Ltd. shall have no liability or responsibility to the original customer or any other party with respect to any liability, loss, or damage caused directly or indirectly by its product, material, or software sold or provided, replacement parts or units, or services provided, including but not limited to any interruption of service, excess charges resulting from malfunctions of hardware or software, loss of business or anticipatory profits resulting from the use or operation of the Masibus product or software, whatsoever or howsoever caused. In no event shall Masibus be liable for any direct, indirect, special or consequential damages whether the claims are grounded in contract, tort (including negligence), or strict liability.

SAFETY PRECAUTIONS

The product and the instruction manual describe important information to prevent possible harm to users and damage to the property and to use the product safely.

Understand the following description (signs and symbols), read the text and observe descriptions.

DESCRIPTION OF SIGNS / SYMBOLS / CHARACTERS



OPERATION RELIABILITY

Disregard may cause damages to person or material.

This Indicates a danger that may result in death or serious injury if not avoided.



WARNING

This indicates a danger that may result in minor or moderate injury or only a physical damage if not avoided.



FUNCTIONALITY

Disregard may impact function of system/device.



INFORMATION

Notes and Information.

Table of Contents

1	Unpacking <i>mas</i>TER T-Sync Model MTS200	9
1.1	Standard Items	9
1.2	Optional Items	9
2	Introduction	10
3	GPS Fundamentals	11
4	Specification	13
5	Unit Front and Rear Panel Description	18
5.1	<i>mas</i> TER T-Sync Model MTS200 Front Panel	18
5.2	<i>mas</i> TER T-Sync Model MTS200 Rear Panel	19
5.3	Mechanical Dimensions Layout	23
6	Installation	24
6.1	GPS Antenna Installation	25
6.1.1	GPS Antenna Installation	25
6.1.2	Mounting the Antenna	26
6.1.3	Verifying Antenna and Cable Operation	28
6.1.3.1	Checking the Antenna Voltage	28
6.1.3.2	Power Supply Check	28
6.1.3.3	Checking the Antenna Resistance	28
6.1.4	Antenna Surge Suppressor	28
6.1.5	Technical Details on GPS Antennas and Cables	29
6.2	Unit Installation	30
6.3	Wiring Diagram	31
7	Hardware Jumper Setting	32
7.1	Relay Contact Output Configurations:	33
7.1.1	POWER relay contacts:	33
7.1.2	GPS LOST relay contacts:	33
7.1.3	WATCHDOG relay contacts:	34
7.2	COM1 terminal RS232 / RS485 output configurations:	34
7.3	COM2 terminal RS232 / RS485 output configurations:	35
8	Start-Up Operation	36
8.1	Receiver Boot-up mode	36
8.2	Battery Backup RTC and GPS receiver RAM Configurations:	37
8.3	Startup Operation	37
8.4	Basic Normal Run Mode Operation	39
9	Unit Setup Configuration	42
9.1	Keypad based configuration	42
9.2	Console based configuration	66
9.2.1	General Settings:	68
9.2.2	NTP Settings:	70
9.2.3	SNMP Settings:	75
9.2.4	Ethernet Settings:	80
9.2.5	Network Security Settings:	86
9.2.5.1	SSHv1/v2 Security Keys menu:	87

9.2.5.2	HTTPS Security Certificate menu:	88
9.2.5.3	NTP Autokey menu:	90
9.2.5.3.1	NTP Autokey PC Scheme:.....	91
9.2.5.3.2	NTP Autokey IFF Scheme:	94
9.2.6	Default / Restore Settings:	98
9.2.7	Administration Settings Menu:	99
9.3	SNMP based configuration	101
9.4	Webserver based configuration	101
10	Serial Communication and Configuration	102
10.1	Steps to Set Putty for serial communication with MTS200:	103
10.2	Steps to Set Hyperterminal for serial communication with MTS200:	105
11	Timing Outputs – Serial, IRIG-B / IEEE 1344, NTP	108
11.1	Timing Output – Serial	108
11.1.1	NMEA-0183 RMC Time frame output	108
11.1.2	T-Format Time frame output:	108
11.1.3	NGTS Time frame output:	109
11.1.4	GPZDA Time frame output:.....	110
11.1.5	GPGGA Time frame output:.....	110
11.2	Timing Output – IRIG-B / IEEE 1344 C37.118-2005	111
11.2.1	Introduction:.....	111
11.2.2	Time Code Output:.....	111
11.2.2.1	Standard IRIG-B Output:.....	112
11.2.2.2	Abstract of IRIG-B Time Code:	112
11.2.2.3	IRIG-B AM & IRIG-B DCLS signals:.....	112
11.2.2.4	IRIG-B IEEE 1344 Extension:	113
11.2.2.5	Generated IRIG-B Time Codes:.....	114
11.2.2.6	Selection/configuration of IRIG-B Time Codes:	114
11.2.2.7	Connecting IRIG-B Time Code:	115
11.2.2.7.1	Connecting IRIG-B DCLS:	115
11.2.2.7.2	Connecting IRIG-B AM:.....	115
11.3	Timing Output – NTP	116
11.3.1	NTP Introduction:	116
11.3.2	NTP Output:	116
11.3.3	NTP Server Installations and Configurations:	118
11.3.3.1	NTP General Settings	118
11.3.3.2	NTP Local Clock.....	119
11.3.3.3	NTP Broadcast / Multicast.....	120
11.3.3.4	NTP Authentication	123
11.3.3.4.1	Symmetric Key Mechanism	123
11.3.3.4.2	NTP AutoKey Mechanism:.....	125
11.3.3.5	NTP Service & Status.....	140
11.3.4	NTP Client Synchronization:	142
11.3.5	NTP Hierarchical Time Distribution:	143
12	Relay and Pulse Outputs	146
12.1	Relay Contact Outputs	146
12.2	Pulse Outputs.....	146
12.2.1	1PPS Output	146
12.2.2	Event Output (PPM/PPH).....	147
12.2.3	Additional Event Outputs (Programmable Pulse Outputs).....	147
13	Ethernet Communications: Telnet, SNMP	148
13.1	Telnet	148

Model: MTS200 (1U)

Doc. Ref. no. : m08/om/201

Issue no. : 03

13.2	SSH	148
13.3	SNMP	149
13.3.1	SNMP Addressing:	149
13.3.2	Protocol Detail:	149
13.3.3	SNMP Operation:	150
13.3.4	SNMP Traps:	164
13.4	Webserver	165
13.5	Syslog	180
13.6	DHCP	181
13.7	Auto configuration	181
14	Holdover Mode	182
15	Options	183
15.1	Optional Input Power Supply	184
15.1.1	Option 1: AC/DC Power Input	184
15.1.2	Option 2: DC Power Input	184
16	Appendix List	185
17	Troubleshooting	186
18	Abbreviations	194

Table of Figures

Figure 3-1 The Basis of GPS 11

Figure 4-1 **masTER** T-Sync Model MTS200 Model 13

Figure 5-1 **masTER** T-Sync Model MTS200 Front Panel Description 18

Figure 5-2 **masTER** T-Sync Model MTS200 Rear Panel Description 19

Figure 5-3 Power supply terminal 20

Figure 5-4 Relay and Standard Event terminal 20

Figure 5-5 Additional Events terminal 20

Figure 5-6 Ethernet ETH terminal 21

Figure 5-7 1PPS BNC terminal 21

Figure 5-8 IRIG-TTL,AM BNC terminal 21

Figure 5-9 COM1 terminal 22

Figure 5-10 COM2 terminal 22

Figure 5-11 SWITCH 23

Figure 5-12 GPS Antenna terminal 23

Figure 5-13 **masTER** T-Sync Model MTS200 Mechanical Dimensions 23

Figure 6-1 Antenna Mounting 26

Figure 6-2 Antenna Mounting with Lightning Arrestor 26

Figure 6-3 **masTER** T-Sync Model MTS200 Wiring Diagram 31

Figure 7-1 **masTER** T-Sync Model MTS200 Main board (Top View) 33

Figure 9-1 Front Panel Keypad Layout 42

Figure 9-2 Display Main Menu layout 44

Figure 9-3 Console based Program main menu layout 67

Figure 10-1 COM2/Serial Console terminal Cable Connections 102

Figure 10-2 Putty Software 103

Figure 10-3 Putty (serial) Settings for console port 104

Figure 10-4 Path of HyperTerminal 105

Figure 10-5 HyperTerminal View 105

Figure 10-6 HyperTerminal Configuration 106

Figure 11-1 IRIG-B waveforms 113

Figure 11-2 NTP frame format 117

Figure 11-3 NTP Settings Menu on Console based utility 118

Figure 11-4 NTP Settings Menu on Webserver 119

Figure 11-5 NTP Security Setings on Webserver 125

Figure 11-6 NTP Autokey – PC Scheme Settings on Webserver 127

Figure 11-7 NTP Autokey – IFF Scheme Settings on Webserver 133

Figure 11-8 NTP Server Status on Webserver 141

Figure 11-9 NTP Server Statistics plot on Webserver 142

Figure 11-10 NTP Time distributions in Hierarchical Arrangement 144

Figure 13-1 MTS200 webserver login page 167

Figure 13-2 MTS200 webserver home page 167

Figure 13-3 MTS200 webserver General page 169

Figure 13-4 MTS200 Webserver Network configuration with IPv4 170

Figure 13-5 MTS200 Webserver Network Configuration with IPv6 171

Figure 13-6 MTS200 Webserver Network Status Page 172

Figure 13-7 MTS200 Webserver SNMP Page 173

Figure 13-8 MTS200 Webserver Security Page 174

Figure 13-9 MTS200 Webserver Administration Page 177

Table of Tables


Table 5-1 mas TER T-Sync Model MTS200 Front Panel Key Definitions.....	19
Table 6-1 Antenna Mounting.....	30
Table 7-1 Power Relay Configuration	33
Table 7-2 GPS LOST Relay Configuration	34
Table 7-3 WATCHDOG Relay Configuration.....	34
Table 7-4 COM1 terminal RS-232/RS-485 Configuration.....	35
Table 7-5 COM2 terminal RS-232/RS-485 Configuration.....	35
Table 9-1 Key Functions	43
Table 11-1 NMEA-0183 Time string format	108
Table 11-2 T-format Time string format	109
Table 11-3 NGTS Time string format.....	110
Table 11-4 GPZDA Time string format	110
Table 11-5 GPGGA Time string format.....	111
Table 11-6 Assignment of CF Segment for IEEE 1344(C37.118-2005).....	114
Table 12-1 Relay Contact Status Chart during Operation	146

1 Unpacking *mas*TER T-Sync Model MTS200

1.1 Standard Items

*mas*TER T-Sync device model MTS200 model is shipped with below standard items.

- *mas*TER T-Sync model MTS200 unit
- Antenna Cable RG6/RG8 as per specified cable length in Customer Order / quote.
- GPS Antenna and Antenna Clamp integrated
- 2 meters RG58 BNC Cable – Qty: 2
- 2 meters RJ45 Ethernet Cable – Qty: 1
- 2 meters RS-232 GPS Configuration Cable – Qty: 1
- Documents – User Manual and supporting Appendix manuals, Test Report, Test Certificates(On Customer Request only)
- CD for Masibus NTP Utility Software – Qty: 1

	INFORMATION <ul style="list-style-type: none">• Antenna Cable type (RG6 / RG8) and antenna cable length (15 meters / 30 meters / 50 meters / customized) is shipped only as per customer order. RG8 cable is provided if antenna cable length requirement is more than 50 meters.
---	--

1.2 Optional Items

*mas*TER T-Sync device model MTS200 model can also be shipped with below optional items only as per customer order.

- Unit Power Supply Cord
- Antenna Cable type and Antenna Cable length
- Lightening Arrestor
- In-Line Antenna Amplifier
- Antenna Splitter
- Antenna holding Mast (of specified length) and its holding clamps
- Antenna Cable GI Conduit

Model: MTS200 (1U)

Doc. Ref. no. : m08/om/201

Issue no. : 03

2 Introduction

masibus MTS200 **masTER** T-Sync has been developed for the time synchronization requirements in various industries like power, process, IT, telecommunications. Masibus next-generation GPS clock provides enhanced performance and security. It is the most featured and cost-effective GPS time synchronization solution available in 1U compact size. MTS200 is Reliable and provides time accuracy of 150nsec at basic level.

To begin with, **masTER** T-Sync model MTS200 offers precise timing accuracy using GPS satellites; it generates accurate output pulses and time codes in multiple formats. It's necessary every time to Lock GPS once after power ON in order to ensure the better accuracy.

masTER T-Sync Model MTS200 synchronizes a wide variety of microprocessor-based power system equipment including: SCADA systems, remote terminal units (RTUs), protection relays, sequence of event recorders, digital fault recorders, tariff meters, Slave Display Units, Data Loggers and other Intelligent Electronic Devices (IEDs). Being a Field programmable device using HyperTerminal / Putty, a very common application in Windows or 8 key Keypad provided on the front panel, **masTER** T-Sync Model MTS200 allows the user to alter the settings or choose from Time codes. Each output can feed directly to different areas through electrically isolated ports which ensure reliable operation in a harsh substation environment.

masTER T-Sync Model MTS200 generates a wide range of timing signals via seven output ports. Standard configurations of **masTER** T-Sync Model MTS200 is equipped with two serial ports, a 1PPS Port, 1 IRIG-B TTL / IEEE 1344 (field configurable) and three PFC relay outputs for POWER, WATCHDOG, GPS LOST alarm and standard PMOS relay based pulse output of PPM/PPH or RTC ON event.

masTER T-Sync Model MTS200 is available with optional feature outputs such as additional 1Gbps eth1 port, 4 additional PMOS relay based pulse outputs each configurable from a second to a day period time, two IRIG-B127 / IEEE 1344/C37.118-2005 Amplitude modulated output (field configurable) or 1 IRIG TTL + 1 IRIG-AM (field configurable) output. Com1 Serial port provides NMEA-GPRMC format. Com2 serial port is configurable for either NGTS or T-format or GPZDA or GPGGA.

MTS200 is a full featured NTP Server (NTPv2/v3/v4) with all available NTP authentication methods available. MTS200 provides time synchronization to different network Clients which are supporting NTP protocols. In addition NTP unicast, MTS200 can be configured with broadcast or multicast mode.

masTER T-Sync Model MTS200 units feature a front panel display, giving both installation teams and users visual feedback about the time data being generated on the outputs. LED indicators provide "at a glance" status information. It also hosts various protocols such as Telnet, SSH, HTTP, HTTPS, SNMP for its own monitoring and configuration management. MTS200 is capable to log alarms internally as well as on remote server through syslog protocol and generate various alarms over syslog and SNMP traps.

The optimized Receiver/Antenna system employed in **masTER** T-Sync Model MTS200 provides time information from the GPS satellite constellation. Dynamic T-RAIM processing is used to eliminate any aberrant satellite signals from the timing solution. The result is timing precision on all outputs with accuracy similar to that normally seen only in laboratory instruments.

masTER T-Sync Model MTS200 unit is Rack Mount and its mechanical dimensions are 482.6(W) x 44(H) x 241(D) mm (IP 20 Enclosure). It is supplied complete with all hardware and software required for the installation, including the Antenna, Antenna mounting kit, 10 meters Antenna cable, 3 meters RS-232 cable and 10 meters RG58 Co-axial cable. (Depends upon commercial terms & condition)

3 GPS Fundamentals

masTER T-Sync Model MTS200 device is a GPS/GNSS based receiver clock device which provides accurate time output with 1PPS signal. Satellite Navigation system is a system of satellites that provide autonomous geo-spatial positioning with global coverage. It allows small electronic receivers to determine their location (longitude, latitude, and altitude) to high precision (within a few meters) using time signals transmitted along a line of sight by radio from satellites. GNSS is a satellite navigation system that is used multiple navigation systems mainly GPS and GLONASS. GNSS also include satellite navigation systems of SBAS, QZSS, Galileo systems etc.

GPS satellite navigation system is maintained by United States of America since 1994 which consists of at-least 24 operational satellites out of 32 satellites in six orbital planes orbiting at an altitude of approximately 20,200 km. In typical GPS operation, four or more satellites must be visible to obtain an accurate result. Satellite-based navigation systems use a version of triangulation to locate the user, through calculations involving information from a number of satellites.

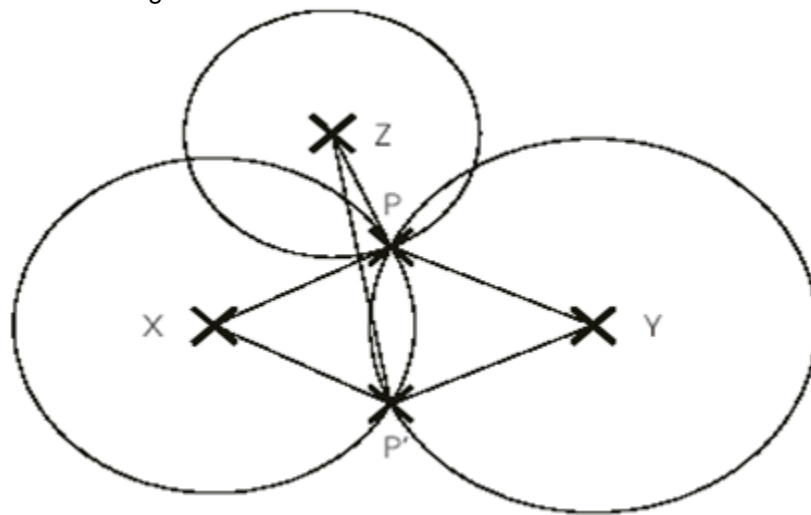


Figure 3-1 The Basis of GPS

If one considers Figure 1 which shows a flat plane. X and Y are two known fixed points on the plane. P is an unknown point. If the distances PX and PY can be measured, then the position of point P can be calculated. Actually there is an ambiguity in that point P' would also fit the measurements. This can be resolved if the position of a third fixed point Z is known since PZ is different to P'Z. This can be summed up by saying that the unknown point P lies at the intersection of three circles based on the known points X, Y and Z.

When the plane becomes three dimensional spaces, the circles become spheres. The intersection of two sphere is a circle, and the intersection of three spheres is a pair of points analogous to the points P and P' of the flat plane case. As for the flat plane case a measurement from an extra fixed point is required to absolutely resolve the ambiguity, although in many cases the ambiguous point would be below the surface of the world. Thus to achieve the objective, GPS must provide accurate measurement of distance from the unknown location of the receiver to 4 known points.

GLONASS based satellite navigation system is maintained by Russia, a fully functional navigation constellation in 1995. After the collapse of the Soviet Union, it fell into disrepair, leading to gaps in coverage and only partial availability. It was recovered and fully restored in 2011. It provides an alternative to Global Positioning System (GPS) and is the second alternative navigational system in operation with global coverage and of comparable precision.

A fully operational GLONASS constellation consists of 24 satellites, with 21 used for transmitting signals and three for in-orbit spares, deployed in three orbital planes. The three orbital planes' ascending nodes are separated by 120° with each plane containing eight equally spaced satellites. The orbits are roughly

Model: MTS200 (1U)

Doc. Ref. no. : m08/om/201

Issue no. : 03

circular, with an inclination of about 64.8°, and orbit the Earth at an altitude of 19,100 km, which yields an orbital period of approximately 11 hours, 15 minutes. The overall arrangement is such that, if the constellation is fully populated, a minimum of 5 satellites are in view from any given point at any given time. This guarantees for continuous and global navigation for users world-wide.

A characteristic of the GLONASS constellation is that any given satellite only passes over the exact same spot on the Earth every eighth sidereal day (1 sidereal day = 23 hours, 56 minutes, 4.0916 seconds). However, as each orbit plane contains eight satellites, a satellite will pass the same place every sidereal day. For comparison, each GPS satellite passes over the same spot once every sidereal day. So opposed to the GPS the ground-track of the GLONASS satellites do not repeat after one day. This avoids the resonance effects which makes station keeping of GPS satellites difficult and expensive.

In GPS navigation system, all satellites operates at same frequency at 1.57542 GHz (as L1 signal) and 1.2276 GHz (as L2 signal) using CDMA technique whereas GLONASS navigation system, all satellites operate on different frequencies using originally a 25-channel frequency FDMA technique spanning from 1602.5625 MHz to 1615.5 MHz, known as the L1 band.

As GNSS uses navigation satellite system of GPS, GLONASS and other available systems in space, GNSS receivers can easily observe 10 to 12 satellites at a time. As more number of satellites are visible, more accuracy in receivers output signals are achieved.

Each visible satellite broadcast two types of information in its message format i.e. Almanac and Ephemeris. Almanac data is coarse orbital parameters for all visible satellites. Each visible satellite broadcasts Almanac data for all visible satellites. This Almanac data is not very precise and is considered valid for up to several months. Ephemeris data by comparison is very precise orbital and clock correction for each visible satellite and is necessary for precise positioning. Each visible satellite broadcasts only its own Ephemeris data. The ephemeris is updated every 2 hours and is usually valid for 4 hours.

4 Specification



Figure 4-1 *masTER* T-Sync Model MTS200 Model

<p>RECEIVER CHARACTERISTICS</p>	<p>Timing Accuracy <15 ns with GPS receiver (the receiver is locked on a fixed position). <±0.1 ppm (OCXO) accuracy while GPS Is Unlock* <±5.0 ppm (TCXO) accuracy while GPS Is Unlock*</p> <p>Positioning Accuracy <10mts SEP (with Selective Availability [SA] Disabled).</p> <p>Receiver Input 1575.42 MHz L1 C/A Code.</p> <p>Tracking 12 parallel channels.</p> <p>Acquisition Time Hot Start : <5 s Warm Start: <38 s Cold Start : <45 s</p> <p>Memory Backup Internal 17mAh cell, Sufficient for 2 weeks of backup time Needs 72 hours run for full charging.</p> <p>Antenna Active L1 GPS, 30 dB Gain Cable: RG 6 / RG 8 (Optional coaxial cable) Maximum Length: 100 meters (Up-to 400 meters using additional line amplifier) Coverage: 360 Degree Ingress Protection: IP67 * If GPS is supplied with OCXO/ TCXO and available on request.</p>
<p>FIXED OUTPUTS</p>	<p>Pulse</p> <p>1 PPS Accuracy: ±500 ns Accuracy with GPS locked</p>

	<p>Output: TTL into 250 Ω Pulse Width: 200 (200 mS High & 800 mS Low signal) Interface: BNC Female connector(Rear Panel) No. of Ports: 1</p> <p>Alarms Three Isolated Dry Contacts to 230 VAC / 24VDC, 10 A: <ol style="list-style-type: none">1. GPS Lost2. Watchdog3. Power FailInterface: 8-Way Terminal Strip</p> <p>Event/RTC ON One Event per minute or per hour or RTC ON/OFF (Configurable) Interface: 8-Way Terminal Strip (Rear Panel) Event contact capacity: 350V DC, 120mA maximum</p> <p>IRIGB-TTL - DC Level Shift / IEEE 1344/C37.118-2005 Format: IRIG-B(007) [IRIGB TTL] or IEEE 1344/C37.118-2005 (field selectable) Output: TTL into 50 Ω Interface: BNC Female connector (Rear Panel) No. of Ports: 1</p> <p>Serial</p> <p>COM1 Protocol: NMEA-0183 (RMC) Port Settings: 9600-8-N-1 Output: RS232/RS485** (Factory Configurable) Interface: DB9 Female Connectors (Rear Panel) No. of Ports: 1</p> <p>COM2 Protocol: NGTS / T-Format / GPZDA / GPGGA Port Settings: 1200/2400/4800/9600/19200-7/8-N/E/O-1/2 (Configurable) Output: RS232/RS485** (Factory Configurable) Interface: DB9 Female Connectors (Rear Panel) No. of Ports: 1</p> <p>** RS232 is factory set</p>
<p>OPTIONAL OUTPUTS</p>	<p>IRIGB-TTL - DC Level Shift / IEEE 1344/C37.118-2005 Format: IRIG-B(007) [IRIGB TTL] or IEEE 1344/C37.118-2005 (field selectable) Output: TTL into 50 Ω Interface: BNC Female connector (Rear Panel) No. of Ports: 1</p> <p>IRIGB-Modulated / IEEE 1344/C37.118-2005 Format: IRIG-B(127) or IEEE 1344/C37.118-2005 (field selectable)</p>

	<p>Signal: 1 KHz AM Signal Modulation Ratio: 3:1 Output: 3.3Vp-p to 10Vp-p, into 100Ω Interface: BNC Female connector (Rear Panel) No. of Ports: 2</p> <p>Ethernet Output No. of Ports: 2 (1x10/100 Mbps + Optional 1 Gbps) Auto Negotiation support Time Synchronization protocols: NTP/SNTP Server [Factory settable] NTP: Version v2 / v3 / v4 with Symmetric and Autokey Authenticaiton RFC: RFC-1119, RFC-1305, RFC-5905 Protocols: TCP, UDP, SNMP v1/v2/v3 with Traps, SSH, SCP, Telnet, Syslog, HTTP/HTTPS Internet protocol: IPv4, IPv6 with Autoconf, DHCP Mode: NTP Server Time format: UTC Interface: RJ-45 Connector (Rear Panel)</p> <p>Additional Event Outputs Four independent configurable Event outputs Configuration: Individual configurable time period and pulse ON time Time Period: 1 to 86400 seconds (24 Hr.) max ON Time: min. 50 milliseconds and max 50% of period time set for particular event Event contact capacity: 350 VDC, 120mA maximum Interface: 8-Way Terminal Strip (Rear Panel)</p>
<p style="text-align: center;">INTERFACE</p>	<p>Display 2x20 LCD with Backlit, 85x19.8 mm with Backlight</p> <p>Displayed data Time of Day (HH:MM:SS) with Local/UTC information Date (DD/MM/YY) with Day of week Day of Year LOCK / UNLOCK status Latitude, Longitude, Height Number of satellites available Data Format on COM2 Parameters of COM2 serial ports Timezone information, DST ON//OFF status Internal Offset</p>

Keypad

KEY	FUNCTION
MENU	For Entering into Configuration mode.
HELP	To Display help about every parameter configurations.
OK	To save the final Configurations.
ESC	To come back into Run mode.
UP	Scroll between various parameters in ascending order in main menu and to change parameters value in submenu.
DOWN	Scroll between various parameters in descending order in main menu and to change parameters value in submenu.
LEFT	To select various available options for the particular parameter in main menu and scroll between various parameters in submenu.
RIGHT	To select various available options for the particular parameter in main menu and scroll between various parameters in submenu.

Status LED

Power: Red
 1 PPS : Red
 Event : Red
 Watchdog : Red
 GPS Locked : Bi Color: Green(GPS LOCK) Red (GPS UNLOCK)

Configuration Modes

Front Keypad
 Front panel RS-232 DB9 serial console port
 SSH, Telnet, Webserver, SNMP

Programmable parameters:

Global Time zone correction
 12/24 Hrs Format of Time
 COM2 serial port setting
 COM2 data format selection (NGTS / T-FORMAT / GPZDA / GPGGA)
 Duration of Programmable repetitive event generation output via dry contact (Per Minute or Hour).
 Eth0 and ETH1 Network Settings
 DST Settings
 Manual Time Setting
 Default Settings
 NTP Settings
 Ethernet Services [SSH, NTP, SNMP, HTTP, HTTPS) Settings
 Password Protection

POWER SUPPLY	AC: 90 to 264 V, 47-63 Hz DC: 100-300 V Power Consumption: 15W max.
OPTIONAL POWER SUPPLY	DC: 18 – 72 V

<p>PHYSICAL DIMENSIONS</p>	<p>19" Rack Mountable Width:482.6 mm (19") Depth:241 mm (9.488") Height: 1 U – 44 mm (3.46") Weight: 2.1 Kg Ingress Protection: IP20 enclosure</p>
<p>ENVIRONMENT</p>	<p>Temperature Operating: 0° C to 50° C Storage: -20° C to +80° C Humidity 20 - 90%(Non-condensing)</p>
<p>EXTRA MODULES (OPTIONAL)</p>	<p>RS232-to-RS485 Converter LINE AMPLIFIER, SURGE ARRESTOR Time Distribution Rack (TDR-4) Time Signal Repeater (TSR-4) Time Display Unit (TDU-64) Netser (NGTS to NTP Converter)</p>
<p>TYPE TEST</p>	
<p>Isolation (Withstanding voltage)</p>	<p>Between primary terminals* and secondary terminals**: At least 1500 V AC for 1 minute</p> <p>Between primary terminals* and grounding terminal: At least 1500 V AC for 1 minute</p> <p>Between grounding terminal and secondary terminals**: At least 1500 V AC for 1 minute</p> <p>Between secondary terminals**: At least 500 V AC for 1 minute</p> <p>* Primary terminals indicate power terminals and relay output terminals. ** Secondary terminals indicate Output Ports.</p> <p>Insulation resistance: 20MΩ or more at 500 V DC between power terminals and grounding terminal.</p> <p>Note: No Isolation between IRIGB-TTL and PPS Output</p>

5 Unit Front and Rear Panel Description

This section provide description of *masTER* T-Sync Model MTS200 unit front panel and back panel user applicable interface.

5.1 *masTER* T-Sync Model MTS200 Front Panel

Below image shows *masTER* T-Sync Model MTS200 model front panel. The front panel is equipped with 20 x 2 line LCD display, 4 LED status indicators, Power LED indicator and keypad interface.

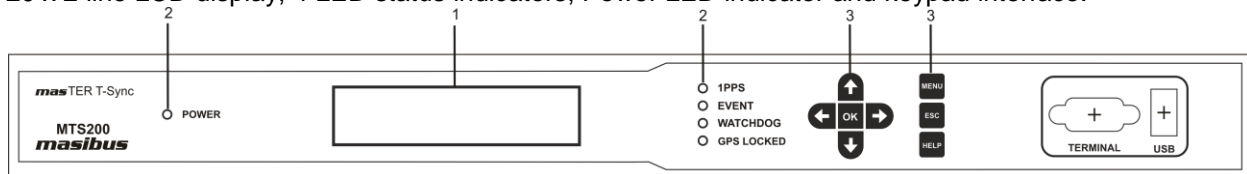


Figure 5-1 *masTER* T-Sync Model MTS200 Front Panel Description

1. **LCD Display:** *masTER* T-Sync Model MTS200 model is equipped with 20 character x 2 line display. This displays various parameters such as Clock parameters (time, date, day of year, day of week, NTP status, Time zone, DST status etc), GPS LOCK/UNLOCK status, GPS satellites data (latitude, longitude, antenna height, total number of satellites available), Keypad configurable parameters etc
2. **LED status Indicators:** There are total 5 LED indicators including power led indication and four other status indicators.
 - **POWER:** This LED illumination is RED color. This LED indicates the presence of power to unit.
 - **1PPS:** This LED indicates the presence of 1PPS signal from GPS receiver module. It blinks at every one second. The illumination is of RED color.
 - **EVENT:** This LED illumination is RED color. This LED indication functionality depends on the type of feature available with ordered *masTER* T-Sync Model MTS200 device.
 1. If the customer has ordered unit with EVENT output, this LED illuminates as per the configured Standard Event period. If the configuration of EVENT output is PPM (Pulse per Minute), this LED blinks at every 1 minute with respect to time on LCD display and will remain ON for 1 second. If the configuration of EVENT output is PPH (Pulse per Hour), this LED blinks at every 1 hour with respect to time on LCD display and will remain ON for 1 second. Configuration can be done through front panel keypad or through COM2 terminal on rear panel.
 2. If the customer has ordered unit with RTC ON feature, this LED will blink when there is no GPS signal present (in UNLOCK condition) and unit is running on its internal clock.
 - **WATCHDOG:** This LED illumination is RED color. This LED is ON when the unit becomes unhealthy due to GPS receiver module failure or internal failure.
 - **GPSLOCKED:** This LED illuminates GREEN color if the GPS satellites signal are available and GPS is LOCKED otherwise LED illuminates RED color if no GPS satellites are available.

3. **KEYPAD:** *masTER* T-Sync Model MTS200 device is equipped with keypad buttons to configure various parameters of Unit. Functionality/usage of each key is described below:









	KEY	FUNCTION
	MENU	To enter in Configuration mode.
	HELP	To Display help about every parameter configurations.
	OK	To save the final configurations changes done.
	ESC	To come back into Run mode or main menu.
	UP	Scroll between various parameters in ascending order in main menu and to change parameters value in submenu.
	DOWN	Scroll between various parameters in descending order in main menu and to change parameters value in submenu.
	LEFT	To select various available options for the particular parameter in main menu and scroll between various parameters in submenu.
	RIGHT	To select various available options for the particular parameter in main menu and scroll between various parameters in submenu.

Table 5-1 *masTER* T-Sync Model MTS200 Front Panel Key Definitions

4. **Terminal / USB:** *masTER* T-Sync Model MTS200 device is equipped with Front serial console terminal RS-232 port for serial based device configurations.

5.2 *masTER* T-Sync Model MTS200 Rear Panel

Below figure 5.2 shows *masTER* T-Sync Model MTS200 model rear panel.

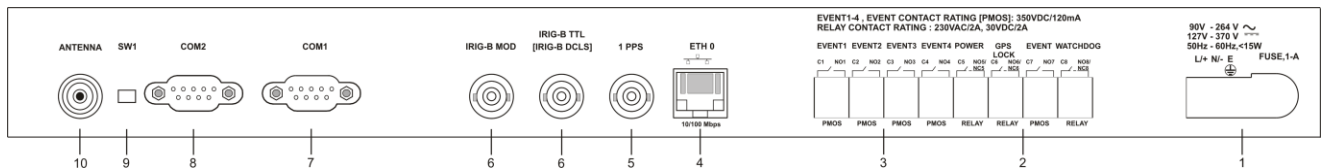


Figure 5-2 *masTER* T-Sync Model MTS200 Rear Panel Description

Various outputs of *masTER* T-Sync Model MTS200 device is provided at rear panel of unit. Below is the description of all possible outputs as per *masTER* T-Sync Model MTS200 configurations with 1 ethernet output (ETH1) with 1 Gbps support, 1 IRIG-B AM output, 1 IRIG TTL/AM and 4 additional pulse outputs. There may be other optional outputs present (as per ordered configuration) apart from standard outputs.

Model: MTS200 (1U)
 Doc. Ref. no. : m08/om/201
 Issue no. : 03

1. Power Input and Fuse Connector:

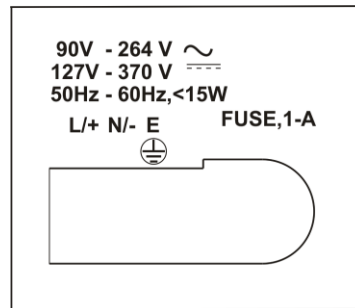


Figure 5-3 Power supply terminal

2. Relay and Event contacts:

masTER T-Sync Model MTS200 provide three relay outputs for Power, Watchdog, GPS LOST alarm and a PMOS pulse output through 8 pin female connector. Factory set Relay contact provided on rear panel connector are C-NO terminals.

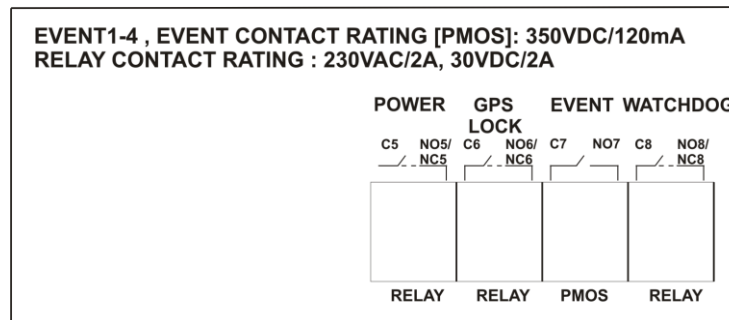


Figure 5-4 Relay and Standard Event terminal

Please refer Relay output section 12.1 for various configurations.

3. Additional Event outputs:

masTER T-Sync Model MTS200 has the capability to provide multiple event outputs in addition to standard PPM/PPH event output. The single event output provides pulse at configured event interval with pre-configured pulse width. This pulse outputs are OptoMOS output (optically coupled solid state Relay output) provided through 8 pin female connector.

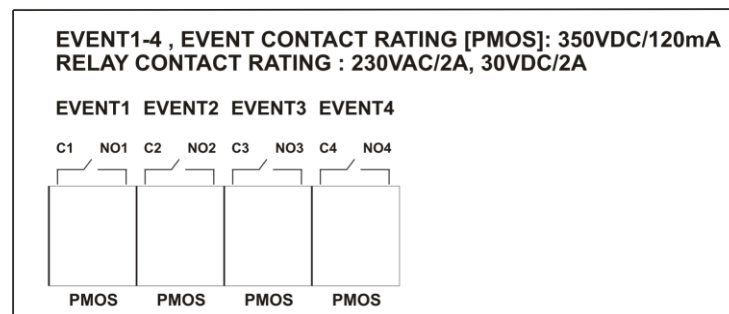


Figure 5-5 Additional Events terminal

masTER T-Sync Model MTS200 model is available with optional Additional Event Outputs.

4. Ethernet Output Connector:

masTER T-Sync Model MTS200 is equipped with 10/100 Mbps Ethernet output for NTP, SNMP, SSH, Webserver and Telnet communication as shown in figure 5.6.

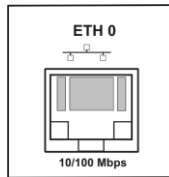


Figure 5-6 Ethernet ETH terminal

masTER T-Sync Model MTS200 model is available with max. 2 ETH optional outputs.

5. 1PPS Connector:

masTER T-Sync Model MTS200 provides 1PPS output at TTL signal level through BNC connector on rear panel of unit as shown in figure 5.7.

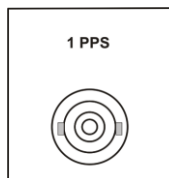


Figure 5-7 1PPS BNC terminal

masTER T-Sync Model MTS200 model is available with 1 x1PPS output as standard option.

6. IRIG-B output:

masTER T-Sync Model MTS200 provides IRIG-B TTL [DCLS] / IEEE-1344 TTL and IRIG-B AM / IEEE 1344 AM output through their respective BNC connector on rear panel of unit as shown in figure 5.8.

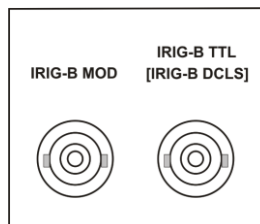
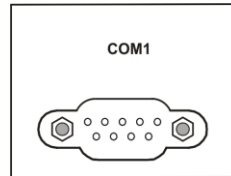


Figure 5-8 IRIG-TTL,AM BNC terminal

masTER T-Sync Model MTS200 model is available with 1 x IRIG-B / IEEE 1344 TTL as standard option with 2 x IRIG-B / IEEE 1344 AM or [1 x IRIG-B / IEEE 1344 AM + 1 x IRIG-B / IEEE 1344 TTL] as an optional output.

7. COM1 terminal:

COM1 terminal on back plane is RS-232/RS-485 electrical standard DB-9 female connector as shown in figure 5.9.

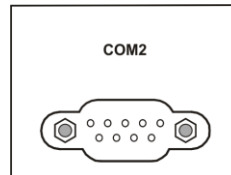
**Figure 5-9 COM1 terminal**

masTER T-Sync Model MTS200 provides serial time frame NMEA format on its COM1 terminal. This terminal provides NMEA time output either in RS-232 electrical standard or RS-485 electrical standard as per specified during unit order. If nothing specified, the factory set settings of COM1 terminal is as per RS-232 electrical standard output.

If Configuration of COM1 terminal is as per RS-232 standard, cross cable (having connection on Pin2, 3 and Pin5) can be used to provide NMEA serial time frame to other peripherals. Pin 4 of COM1 connector is used to provide 1PPS signal in RS-232 format.

If Configuration of COM1 terminal is as per RS-485 standard, Pin 7 of DB-9 connector will act as D+ line and Pin 8 will be D- line.

masTER T-Sync Model MTS200 model is available with 1 NMEA serial output as standard option.

8. COM2 terminal:**Figure 5-10 COM2 terminal**

COM2 terminal on back plane is RS-232/RS-485 electrical standard DB-9 female connector as shown in figure 5.10. *masTER* T-Sync Model MTS200 provides serial time frame T-format / NGTS format on its COM2 terminal and can also be used for *masTER* T-Sync Model MTS200 configuration. This terminal connection will be as per RS-232 electrical standard or RS-485 electrical standard as per specified during unit order. If nothing specified, the factory set settings of COM2 terminal is as per RS-232 electrical standard output.

If Configuration of COM2 terminal is as per RS-232 standard, cross cable (having connection on Pin2, 3 and Pin5) can be used for configuration and to provide serial time frame to other peripherals. Pin 4 of COM2 connector is used to provide 1PPM signal in RS-232 format.

If Configuration of COM1 terminal is as per RS-485 standard, Pin 7 of DB-9 connector will act as D+ line and Pin 8 will be D- line.

9. **SWITCH:**

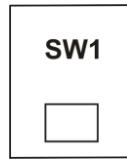


Figure 5-11 SWITCH

Switch “SW1” should be positioned towards the COM1 connector for accessing the time frame on COM2 terminal. If switch “SW1” notch is towards the GPS Antenna, then the system will enter into firmware upgrade mode.

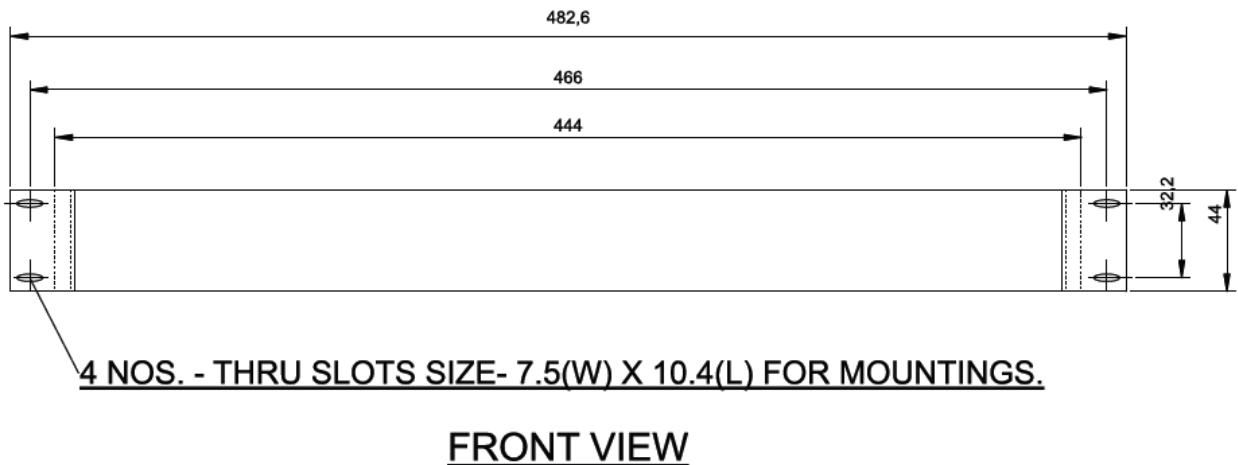
10. **GPS Antenna connector:**



Figure 5-12 GPS Antenna terminal

masTER T-Sync Model MTS200 device have a BNC female connector at its rear panel for connecting GPS antenna as shown in figure 5.11. This connector provides 5 VDC supply to antenna. Refer Antenna Installation section 6 for connecting GPS Antenna.

5.3 Mechanical Dimensions Layout








FRONT VIEW


Figure 5-13 *masTER* T-Sync Model MTS200 Mechanical Dimensions

6 Installation

Before beginning with unit installation, please follow important safety statements for avoiding installation practices causing malfunctioning of the device as mentioned below.

	<p>OPERATION RELIABILITY</p> <p>To minimize the possibility of fire or shock hazards, do not expose this instrument to rain or excessive moisture</p> <p>Do not use this instrument in areas under hazardous conditions such as excessive shock, vibration, dirt, moisture, corrosive gases or oil. The ambient temperature of the areas should not exceed the maximum rating specified</p>
	<p>WARNING</p> <p>It is recommended to get the installation of this product to be done by authorized service personnel of the manufacturing company or by the trained and qualified operator in co-ordination with authorized service personnel of the manufacturer company.</p> <p>Installation of the equipment is to be complied in accordance with local and national electrical codes.</p>
	<p>This equipment is sensitive to Electrostatic Discharge (ESD). Observe all ESD safeguards while using this equipment.</p>
	<p>OPERATION RELIABILITY</p> <p>This equipment can be damaged if incorrect power source voltage is applied.</p> <p>This equipment can be damaged if power source is applied with incorrect polarity on its respective terminal.</p> <p>Never plug unit power supply connector or power supply cables in terminal while main power source is ON.</p>
	<p>WARNING</p> <p>This equipment should be always used with earth grounded. Never defeat the ground connector or operate the equipment in the absence of suitable earth ground connection.</p> 

	<p>WARNING</p> <p>Never work on open unit when power of unit is ON.</p>
---	--

	<p>WARNING</p> <p>Unit is equipped with internal fuse. If it is blown up or blowing again on its replacement, it is highly probable that either power source is incorrect or power source connection is improper.</p> <p>Internal fuse should be only replaced with same fuse type and same fuse rating as supplied from manufacturer factory. Replacement of Fuse should be done in unit Power OFF condition only.</p>
---	--

6.1 GPS Antenna Installation

GPS Antenna and Cable Information

masTER T-Sync Model MTS200 comes complete with the necessary hardware to be able to receive GPS signals: 50-feet of RG-6 cable and a GPS antenna. The antenna cable is connected between the female N connector on the antenna and the female BNC connector at the rear panel of the clock.

This section should help you with installing the GPS antenna and antenna cable(s) and connecting them to the model MTS200 series clocks. It should also be a source of information if you should need to troubleshoot the antenna cable system. These clocks achieve their accuracy. By comparing and adjusting the Internal clock signal to the incoming GPS signal.

6.1.1 GPS Antenna Installation

Refer steps for installation of GPS antenna and antenna cable as described below.

Selecting a GPS Antenna Site Outdoors

Select a site or antenna mounting position that...

- Is the highest point available
- Offers a full 360° view horizontally, to within 10° vertically of the horizon
- Is higher than neighboring buildings/obstructions
- Is protected from strong radio frequency (RF) and microwave transmissions
- Is set away from RF-reflective surfaces that cause multipath interference
- Is set 3 ft. (1 m) away from other GPS antennas

Avoid...

- Mounting the antenna between tall buildings or next to walls and equipment
- Cable type and cable length which runs from the antenna to the receiver that exceed the specified length
- Patching multiple cables together to make a single cable run
- Running the cable through bulkheads and alongside high-energy cables
- Crimping or damaging the cable

Blocked signals and multipath cancellation may significantly increase GPS signals acquisition time. Multipath Cancellation is caused by reflected signals that reach the antenna out of phase with the direct signal due to vertical reflective objects positioned to the side and above the antenna. To solve these problems, user must mount the antenna at least 1 meter away from and above the reflecting surface. To properly receive GPS signals, the GPS antenna needs to be mounted clear of buildings as surrounding elements or heightened obstacles may block the GPS signals transmission done with the satellites. For complete antenna signals coverage, the antenna needs to have a clear view of the sky and if the antenna is mounted in a less favourable location, it may work however GPS antenna signals reception capability may be somewhat limited/deteriorated during certain hours of the day.

6.1.2 Mounting the Antenna



Figure 6-1 Antenna Mounting

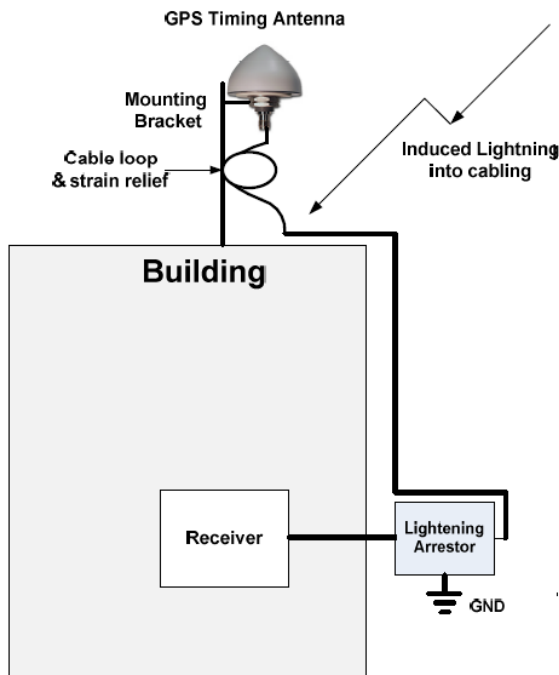


Figure 6-2 Antenna Mounting with Lightning Arrestor

Mount the GPS antenna on an antenna mast (recommended) or on the peak of a building. The GPS antenna kit (P/N no.: m-MK-AMC-40-1) includes special mounting brackets. For the mast, use 1-inch (2.54-cm) diameter water pipe which is rigid enough to withstand high speed winds without flexing. The steps needed to assemble the kit are as follows (as per given figure):

1. Clamp the GPS antenna on the mounting bracket with a retaining nut.
2. Attach the mounting bracket to the pole (P/N: m-AR-01-01) using two guillotine-style U bolts and four hex nuts.
3. Connect the Type N male connector (antenna cable) to the antenna connector.
4. To ensure a trouble free installation the strain must be taken off the Cable by looping the cable.



FUNCTIONALITY

- Use GPS antenna cable supplied from factory or as per recommended in manual. If antenna cable other than recommended is to be used, contact Masibus Customer Service representative.
- Do not cut the antenna cable to shorter its length. Instead, bundle the excess cable to shorten antenna cable length.
- The model MTS200 requires a 5 Volt-compatible antenna. Antennas not rated for 5 V will be damaged.
- Use a splitter to connect a single GPS antenna to multiple *masTER* T-Sync Model MTS200 units. Avoid using BNC "T" connectors.

GPS-related Accessories

The following options/accessories can be ordered:

1. Protect against lightning and field-induced electrical surges.
2. Connect multiple *masTER* T-Sync Model MTS200 receivers to a single antenna.
3. Extend the range of the GPS antenna cable.

1. Lightning Arrestor

Lightning may damage GPS system components and receiving equipment, even without a direct hit, resulting in costly repairs and critical interruption of service. The lightning arrestor is designed to work in conjunction with a low-resistance, low-inductance ground to protect your GPS receiver and elements of the antenna system from lightning discharges and field-induced electrical surges. In-line lightning arrestors are mounted between the antenna and the point where the cable enters the building and require no additional power or wiring except the ground lead.


2. Antenna Splitter


An antenna splitter may be used to drive multiple GPS receivers using a single antenna. With built-in amplification to overcome splitter losses, the Active Splitters may be conveniently cascaded without adding separate amplifiers and bias-tees between splitters. Power is conveniently obtained from the GPS receiver(s) connected to the amplifier, eliminating the need for a separate dc power supply and wiring.

3. In-Line Antenna Amplifier

In-line amplifiers overcome signal attenuation in by amplifying the GPS signal. Use the in-line amplifier for cable runs of 100 to 200 meter. Please contact a masibus Sales Representative for information on how to extend the distance from the antenna to the receiver.

6.1.3 Verifying Antenna and Cable Operation

	<p>WARNING</p> <p>Please ensure that while doing below mentioned procedure for checking antenna voltage/current while unit is in POWER ON condition, do not short the antenna supply +5 Vdc and GND, in any case, failure of which will damage the unit internal electrical supply.</p>
---	---

	<p>This equipment is sensitive to Electrostatic Discharge (ESD). Observe all ESD safeguards while using this equipment. Otherwise, there is danger that the unit may get damaged through ESD.</p>
---	---

6.1.3.1 Checking the Antenna Voltage

masTER T-Sync Model MTS200 unit provides +5 Vdc to the GPS antenna through its Antenna connector on unit rear panel, which is carried through the antenna cable. Nominal antenna current is 10 mA. Check the voltage at the antenna connector on the unit rear panel antenna connector. Without the +5Vdc supply on antenna connector of unit, the antenna and *masTER* T-Sync Model MTS200 will not synchronize with the GPS satellites signal and can generate an GPS UNLOCK alarm.

6.1.3.2 Power Supply Check

The Antenna Voltage test (mentioned above in section 6.1.3.1) actually tests the main power supply voltage for all models of *masTER* T-Sync Model MTS200's. This voltage should be between 4.9 and 5.1 Vdc.

6.1.3.3 Checking the Antenna Resistance

Checking the internal resistance of the GPS antenna is not as useful as verifying the antenna current mentioned above in section 6.1.3.1. Antenna resistance measures several megohms with Multi-meter probes at one polarity and less so if you change the Multi-meter probe polarity.

6.1.4 Antenna Surge Suppressor

If GPS Surge Suppressor kit is available with purchase order, user should mount it in line with the antenna cable. Additional information on grounding GPS antennas, and grounding in general, are available from masibus Customer Support division (Kit P/N :m-LA-01).

6.1.5 Technical Details on GPS Antennas and Cables

Antenna Cable

Length and Loss Considerations

Standard Antenna Cable

The standard antenna cable assembly included with *masTER* T-Sync Model MTS200 is constructed using a 15-meters (50-foot) length of RG-6 type low-loss coaxial cable, terminated with male Type N connector and BNC male connector. Optional lengths of RG-6 coax are separately available for longer runs; see Table 4.2, Cable Data and Accessory Information.

Effects of Cable Parameters

To receive GPS signals and properly operate the clock, the type and length of the cable are important. Due to their effect on specific parameters described in the following paragraphs, any changes to the length and/or type of antenna cable should be made carefully. Damaged cables may also affect performance.

Cable Delay

The velocity factor and the physical length of the cable determine cable delay. User has to enter delay value according to antenna cable length.

For cable options, the delay is tabulated below. The formula for calculating cable delay is:

$$T = \lambda \frac{1}{CKv} + 1ns$$

Where:

T = Cable delay, in nanoseconds;

λ = Cable length, in meters;

C = Speed of light (3 _ 108 meters per second);

Kv = Nominal velocity of propagation (0.85).

One nanosecond is added to the calculated value to account for the length and velocity factor of the short connecting cable inside of the clock.

Attenuation

Attenuation depends upon the cable length, and the loss per unit length. The total attenuation must be limited to 30 dB (maximum) at the GPS L1 frequency of 1575.42 MHz

DC Resistance

The cross-sectional area and length of the conductors in the cable determine the dc resistance. Since power to the RF preamplifier in the antenna is supplied via the antenna cable, excessive dc resistance will degrade performance. Because of the above factors, changes to the length and/or type of antenna cable should be made carefully. Damaged cables may also affect performance.

Model: MTS200 (1U)

Doc. Ref. no. : m08/om/201

Issue no. : 03

Available Antenna Cables and Accessories for Longer Runs

masibus offers longer antenna cables for use with all models of clocks when the standard 15 meters (50-foot) cable is inadequate. RG-6 cable runs up to 50 meter, RG-8 cable is available for 100 meters (328 foot) without the in-line preamplifier. *masibus* offers in-line amplifier, (P/N: m-LA-01) for long antenna cable requirement up to 200 meters (656 foot).

Description	Delay, ns	Signal Level, dB
15-m (50-ft) cable, RG-6	60 ns	5dB
30-m (100-ft) cable, RG-6	120 ns	9dB
50-m (164-ft) cable, RG-6	200 ns	15dB
100-m (328-ft) cable, RG-8	393 ns	17dB

Table 6-1 Antenna MountingConnection to Antenna

The male Type N connector on one end of the antenna cable mates with the female Type N connector on the antenna.

Connection to *masTER* T-Sync

The male Type BNC connector on the opposite end of the antenna cable connects to the female Type BNC connector on the rear panel of the GPS Clock.

6.2 Unit Installation

After GPS Antenna installation is complete, *masTER* T-Sync Model MTS200 unit can be installed as per below procedures.

1. It is necessary to provide correct power supply to unit as per specified order or as per power supply specification mentioned at the unit's rear panel.
2. Ensure that the power supply polarity connections are done as per mentioned Label on specific power supply connector terminal on rear panel.
3. It is recommended to not connect the NTP outputs in installation site ethernet network till proper network settings are done in unit.
4. It is recommended to first get the unit LOCK before using all outputs for time synchronization to client device in order to avoid time difference of *masTER* T-Sync w.r.t. UTC time due to POWER ON in Unlock conditions or battery discharged due to long period (as per section 8.2) of unit in Power OFF conditions.
5. After the power supply is connected properly, Power ON the unit. After unit is Power ON, there are specific messages displayed on the screen till the time and date are displayed on unit display screen. Refer section 8.3 for the Unit Power ON status.
6. At startup, the clock of unit in Unlock conditions may not be correct if the unit was in Power OFF condition for long duration. Refer section 8.1 and 8.2.
7. It is necessary to change the Ethernet addresses of unit NTP output ports individually (connecting NTP port directly with PC using Ethernet cable) before using GPS as NTP server. Refer section 13.1 and Appendix E.
8. User can configure other configurable parameters of *masTER* T-Sync Model MTS200 using keypad and serial terminal or Ethernet based configuration as explained in section 9.
9. After unit settings and configuration is done, user should provide power restart to unit.
10. After unit Power ON, unit should be kept for warm up duration in LOCK condition.

11. Once unit is Power ON, it is necessary to keep the unit in warm up condition for minimum 1 hour in antenna LOCK condition for precise and accurate timing outputs during unit LOCK and Holdover conditions.

6.3 Wiring Diagram

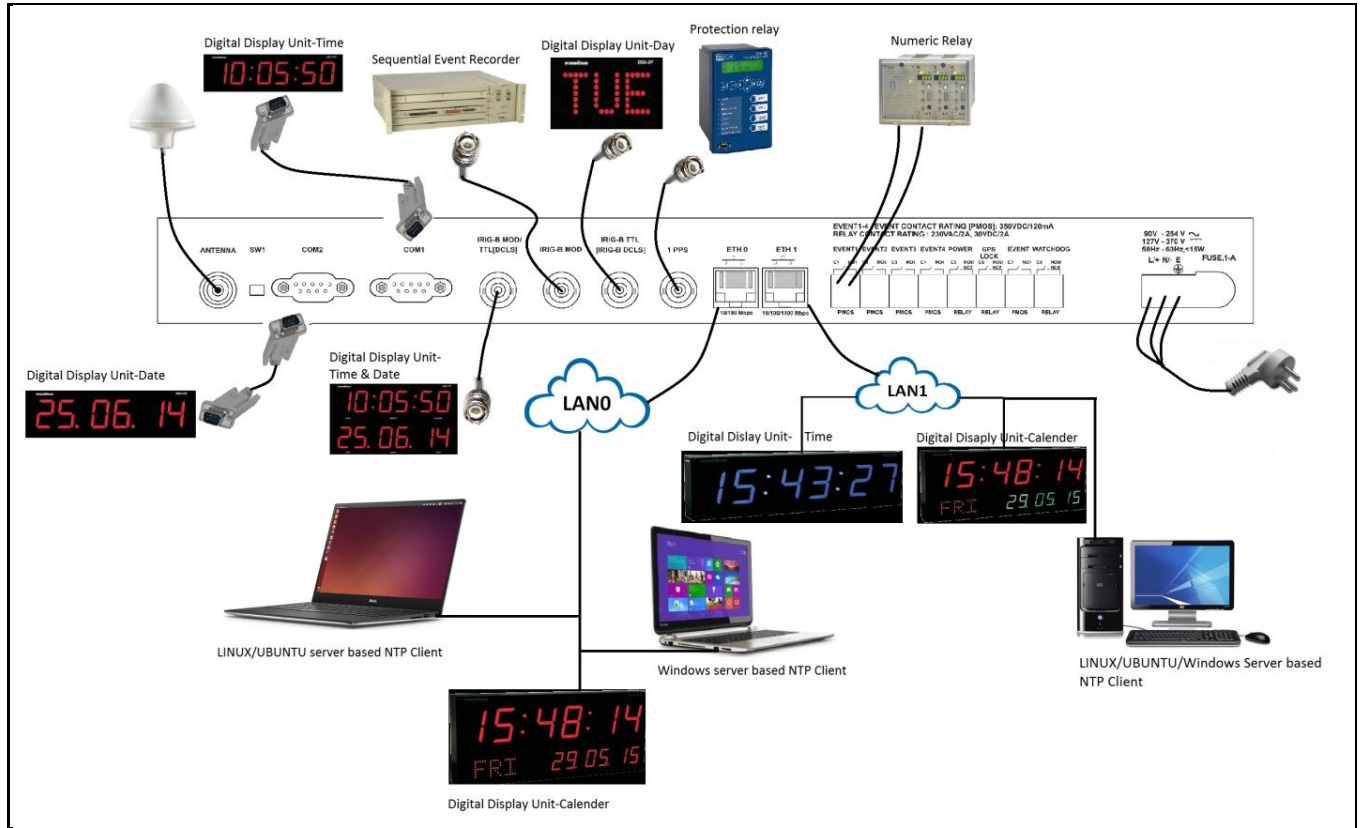




Figure 6-3 masibus MASTER T-Sync Model MTS200 Wiring Diagram

7 Hardware Jumper Setting

	<p>FUNCTIONALITY</p> <p>Hardware jumper settings inside the unit should be done while unit is in POWER OFF condition.</p>
---	--

	<p>This equipment is sensitive to Electrostatic Discharge (ESD). Observe all ESD safeguards while using this equipment. Otherwise, there is danger that the unit may get damaged through ESD.</p>
---	---

masTER T-Sync Model MTS200 device comes with complete system configurations as per factory set settings and if any, as per specified ordered configurations. There are few output options available that can be changed by operator at its end i.e. Relay contacts configuration from C-NO to C-NC contacts and COM1, COM2 terminal RS-232 to RS-485 electrical configurations. However, it is recommended to change the hardware settings after contacting Masibus Customer Support department.

For changing above mentioned settings, jumpers are provided on the main card inside the unit. For changing any configuration, follow below procedure step by step.

1. Power OFF the unit from supply. Remove all the output connections / cables connected on the rear panel of *masTER* T-Sync Model MTS200 unit.
2. If the unit is mounted inside the panel, please remove the unit from panel.
3. Open the top black cover of the unit by unscrewing screws on top cover. After removing the screws, remove the top cover.
4. Change the jumpers settings as described in respective applicable section 7 as explained.
5. After changes are done, please refit the top black cover with screws.
6. After restarting the unit on Power ON, user should take care about the cable connections done on rear panel connectors specifically about those whose output configurations have been changed through internal jumpers.

Below Figure shows the location of Jumpers CN20, CN22, CN23 for Relay contacts, CN12, CN13 for COM1 terminal and CN16, CN18 for COM2 terminal on the main card (front top view).

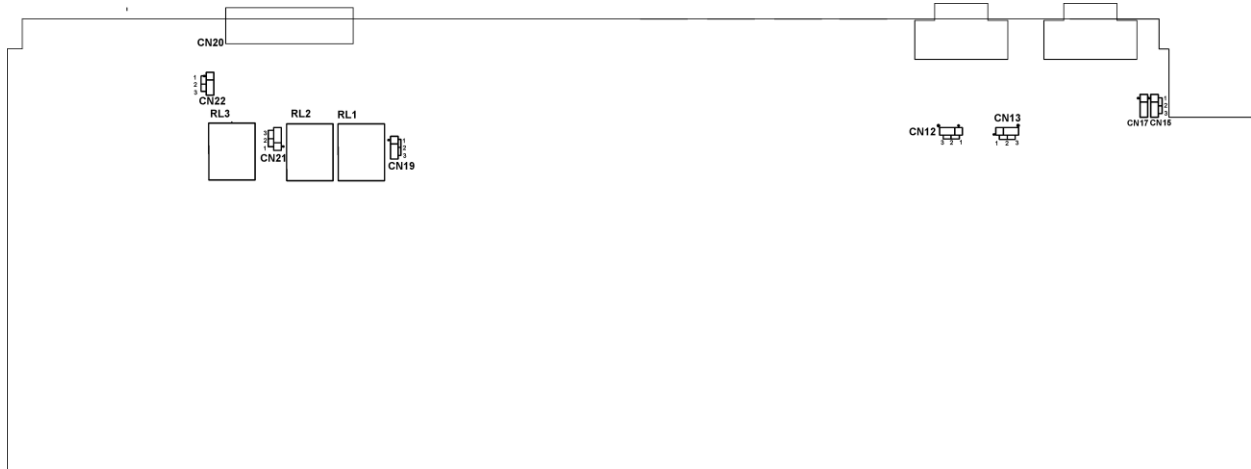


Figure 7-1 masTER T-Sync Model MTS200 Main board (Top View)

7.1 Relay Contact Output Configurations:

The factory default settings of Relay contacts for Power, Watchdog and GPS LOST alarm, available on rear panel of unit are as per C-NO contacts (if any special request is not provided for setting relay output contacts configuration). If required, operator can change the relay contact from C-NO to C-NC contact as explained in below details.

7.1.1 POWER relay contacts:

CN20 3-pin jumper on main card is used to change the relay contact for POWER relay contacts. Operator has to remove black jumper from its current position to required position as explained in below images. Refer below figure for C-NO jumper position configuration and C-NC jumper position configuration.



















C-NO Configuration:	C-NC Configuration:																		
<p>CN19</p> <table style="margin-left: auto; margin-right: auto;"> <tr> <td>NO</td> <td style="text-align: center;">  </td> <td>1</td> </tr> <tr> <td>C</td> <td style="text-align: center;">  </td> <td>2</td> </tr> <tr> <td>NC</td> <td style="text-align: center;">  </td> <td>3</td> </tr> </table>	NO		1	C		2	NC		3	<p>CN19</p> <table style="margin-left: auto; margin-right: auto;"> <tr> <td>NO</td> <td style="text-align: center;">  </td> <td>1</td> </tr> <tr> <td>C</td> <td style="text-align: center;">  </td> <td>2</td> </tr> <tr> <td>NC</td> <td style="text-align: center;">  </td> <td>3</td> </tr> </table>	NO		1	C		2	NC		3
NO		1																	
C		2																	
NC		3																	
NO		1																	
C		2																	
NC		3																	

Table 7-1 Power Relay Configuration

7.1.2 GPS LOST relay contacts:

CN22 3-pin jumper on main card is used to change the relay contact for GPS LOST relay contacts. Operator has to remove black jumper from its current position to required position as explained in below images. Refer below figure for C-NO jumper position configuration and C-NC jumper position configuration.







C-NO Configuration:	C-NC Configuration:
CN21 NO  1 C  2 NC  3	CN21 NO  1 C  2 NC  3

Table 7-2 GPS LOST Relay Configuration

7.1.3 WATCHDOG relay contacts:

CN23 3-pin jumper on main card is used to change the relay contact for Watchdog relay contacts. Operator has to remove black jumper from its current position to required position as explained in below images.

Refer below figure for C-NO jumper position configuration and C-NC jumper position configuration.







C-NO Configuration:	C-NC Configuration:
CN22 NO  1 C  2 NC  3	CN22 NO  1 C  2 NC  3

Table 7-3 WATCHDOG Relay Configuration

7.2 COM1 terminal RS232 / RS485 output configurations:

COM1 terminal provides serial based NMEA time frame at every second once after unit boots. COM1 terminal can configured to provide NMEA time frame on RS-232 electrical standard or RS-485 electrical standard. A COM1 terminal is configured as RS-232 output as factory default. CN12 and CN13 jumpers on main board of unit are used to change the configuration between RS232 to RS485 standard. Please refer below table showing the jumpers position required for RS232 and RS485 configuration.

RS-232 Configuration:	RS-485 Configuration:
<p style="text-align: center;">RS232</p> <p style="text-align: center;">3 2 1</p> <p style="text-align: center;">RS232</p> <p style="text-align: center;">1 2 3</p>	<p style="text-align: center;">RS485</p> <p style="text-align: center;">3 2 1</p> <p style="text-align: center;">RS485</p> <p style="text-align: center;">1 2 3</p>

Table 7-4 COM1 terminal RS-232/RS-485 Configuration

7.3 COM2 terminal RS232 / RS485 output configurations:

COM2 terminal provides serial based T-format, NGTS time frame at every minute once after unit boots. This terminal is also used for GPS configuration. COM2 terminal can be configured for RS-232 electrical standard or RS-485 electrical standard based communication. A COM2 terminal is configured as RS-232 output as factory default. CN16 and CN18 jumpers on main board of unit are used to change the configuration between RS232 to RS485 standard. Please refer below table showing the jumpers position required for RS232 and RS485 configuration.

RS-232 Configuration:	RS-485 Configuration:
<p style="text-align: center;">CN17</p> <p style="text-align: center;">RS232</p> <p style="text-align: center;">1 2 3</p> <p style="text-align: center;">CN15</p> <p style="text-align: center;">RS232</p> <p style="text-align: center;">1 2 3</p>	<p style="text-align: center;">CN17</p> <p style="text-align: center;">RS485</p> <p style="text-align: center;">1 2 3</p> <p style="text-align: center;">CN15</p> <p style="text-align: center;">RS485</p> <p style="text-align: center;">1 2 3</p>

Table 7-5 COM2 terminal RS-232/RS-485 Configuration

8 Start-Up Operation

8.1 Receiver Boot-up mode

When *masTER* T-Sync Model MTS200 unit is power up, the time of unit depends on the GPS receiver RTC data. At every Power ON, unit is in UNLOCK mode initially. If GPS antenna is connected after Power ON or was already connected while powering up the unit, the time to getting unit LOCK depends on the duration for which the unit was in Power OFF condition. Also, if the unit was in UNLOCK condition during the normal operation of unit, the time taken by unit to get LOCK after antenna is connected depends on the duration for which unit was in UNLOCK condition.

Refer below explanation for time taken by unit to get LOCK after Power off or UNLOCK condition.

For a receiver to obtain a position fix, it must download the almanac and ephemeris information from the satellite through a satellite frame. The receiver must download almanac and ephemeris information to achieve a position fix. Depending on the parameters such as valid almanac, ephemeris data of previous visible satellites, last position of receiver and time stored, the boot process (Cold start / Warm start / Hot start) mode is determined.

Cold start: If the GPS receiver does not have any initial data regarding current almanac, ephemeris data (case when backup battery is discharged) or it has invalid data for almanac and ephemeris information, on boot up the receiver will enter in Cold start mode. In order to get current almanac data, GPS receiver should receive at least one satellite frame. Typically, TTFF (Time to First Fix) for position in Cold start is less than <45 seconds (when GPS Antenna is placed in open sky conditions without any obstacle interference) because each GPS receiver may take few seconds time to get initialized on boot up and as each satellite frame takes 30 seconds to transmit single frame.

Since each satellite transmits total 25 frames as satellite complete broadcast message, complete almanac data is transmitted by satellite in 12.5 minutes. So, in order to have very highly accurate position and time data, to reach 90% confidence level after acquiring complete almanac data from each satellite, Cold start for TTFF (Time to First Fix) can be < 15 minutes, it will acquire almanac and ephemeris data for visible satellites and thereafter receiver will enter in its normal operation mode. In this case, it is necessary that antenna should be located in open environment having no immediate obstacles.

If the device is moved to very far location in hundreds of kilometers from its last operation position and system is made ON, then receiver will try to identify visible satellites data and compare it with previously stored almanac data. If this does not match, receiver will start as in Cold start mode.

Warm or Normal start: In the warm start mode, when the receiver boots and if the information of current almanac satellite data, time which receiver knows is within 20 seconds from the satellite time, receiver position to within 100 kms but do not have ephemeris information or ephemeris information may be invalid, the receiver enters Warm start mode. Typically, time required for position fix in Warm mode is less than 38 seconds (when GPS Antenna is placed in open sky conditions without any obstacle interference) as each satellite transmits its ephemeris data at every 30 seconds.

If the receiver does not have valid almanac data, it enters the Cold start mode.

Hot start: When receiver boots up, if the information/data of current almanac, position, current time is stored and are valid, receiver enter Hot start mode and provides accurate time within few tens of seconds.


8.2 Battery Backup RTC and GPS receiver RAM Configurations:

Backup batteries are used to keep the RAM and the Real-Time Clock (RTC) in the receiver running even after unit Power OFF to retain setup and status information, Time, Date, Last Calculated Receiver Position, Almanac and Ephemeris information along with receiver specific parameters allowing resumption of GPS operation automatically once unit mains power is restored. In this “Warm Start” scenario when the unit power is restored, the receiver scans the RTC to check how much duration has elapsed since power was removed, calculates which satellites should be visible using the previous stored almanac information and then proceeds to develop fix information providing data.

The battery is a maintenance-free rechargeable Manganese lithium type. A built-in battery charging circuit is used when the unit is powered on, eliminating the need for maintenance.

Battery Specification:

Manganese lithium, 3.6 volts, 17 mAh,
 Memory Retention Time: 15 days (approx.)

	<p>FUNCTIONALITY</p> <p>It is recommended that if <i>masTER T-Sync</i> Model MTS200 unit was in Power off condition for the duration more than specified Memory retention time, user should allow to keep unit in Power ON condition for 72hours to charge the RTC backup battery to full level.</p>
---	---

Non Volatile Memory Configuration:

The GPS clock maintains its all configuration parameters internally in non-volatile memory, even when the power is off.

8.3 Startup Operation

Before powering up *masTER T-Sync* Model MTS200 device, user has to ensure that power supply connections are done properly. When power is applied, below is basic start up sequence of *masTER T-Sync* Model MTS200 Device.

- While GPS is in Power off, all the outputs are disabled.
- As soon as Power is applied, GPS Display and GPS POWER LED in “Red” color on front panel illuminates and as the GPS is in unlock condition at startup, GPS LOCKED LED illuminates in RED color.
- There is sequence of messages on LCD which are display one after another as mentioned below.

SYSTEM
INITIALIZING

Masibus Auto. &
Inst. Pvt. Ltd.

Model: MTS200 (1U)

Doc. Ref. no. : m08/om/201

Issue no. : 03

- MTS200 is operating system based product so it takes few seconds for bootup which may vary from 15 to 40 seconds to start the main application. During initial bootup period, above two messages are displayed in sequence. Once main application starts, below messages continue to start display.

```
Com 1: 9600-N-8-1
Com 2: 9600-N-8-1
```

```
masTER T-Sync
Connecting...
```

```
Time: 09: 00: 00 AM LCL
Date: 22/09/15 TUE
```

- Few seconds after GPS unit is powered up, 1PPS LED will start flashing in RED color which indicates the Pulse per second output available.
- When the time gets displayed on unit display, all other outputs will become active.
- Since this unit uses standard ntp source in its system, the time on display will be corrected once the ntp program synchronize with internal GPS receiver module.
- If the antenna to the device is not connected and the gps receiver is in cold boot mode due to RTC battery discharged or it unit is moved by several hundred kilometres from last sync position, the time of *masTER T-Sync* Model MTS200 device will get reset to **default time** (Time: 23:59:59 and Date: 21/8/99), in such case all outputs such as time on display, NTP, IRIG-B, serial time outputs, all event outputs will be according to the default time. The time will only be corrected once the antenna is connected to MTS200. In such case, operator can set the system time manually by front panel keypad as explained in section 9.1 "Calender Settings".
Note: NTP clients time will be unaffected because MTS200 will raise "Unsynchronized" flag in its ntp response to clients, as a result ntp clients time will not get disturbed till MTS200 internal clock is synchronized with gps receiver by ntp driver.
- If the device has entered in cold boot mode, then message will be displayed on front LCD (as shown in below image) as well as ntp not sync trap will be send on SNMP manager and syslog if configured. Also, the GPS LOCK LED in front will be "red" color till internal ntp driver synchronizes with gps receiver which may take approx. 12.5 to 13 minutes in cold boot mode after power up.

```
Time: 09: 00: 00 AM LCL
COLD BOOT MODE
```

- Once the internal clock get synchronize with gps receiver, message will occur on display as shown in below figure.

```
Time: 09: 00: 00 AM LCL
NTP[PPS]: 1.000 ms
```

- Internal ntp driver in operating system takes certain minutes to get the internal clock synchronized within 1 millisecond w.r.t. gps receiver satellite time as ntp driver adjust (using skew method) its internal clock using complex PLL clock sync. method.

- Once device internal clock is synchronized with gps receiver, ntp driver will always maintain internal clock accuracy with few hundred microseconds w.r.t gps receiver time in lock conditions and holdover conditions (as per holdover ppm accuracy of internal rtc) during normal run of device.
- Also, the GPS LOCK led will glow “green” color and gps lock status will be updated on other outputs as well.
- All messages showing unit LOCK/UNLOCK status, position information, day of year, day, COM2 terminal time frame format are displayed in rotation in last line of LCD.
- There are other 4 status LED’s on front panel of *masTER* T-Sync Model MTS200 device. When Power is applied to the device, GPS LOCKED indication illuminates in RED color. If GPS Antenna is connected, after few minutes, GPS will get Lock and will be indicated by GREEN indication on GPS LOCKED led. The time taken to get GPS lock will depend on start mode of GPS receiver whether GPS receiver is in Cold start or Warm Start or Hot start mode.
- *masTER* T-Sync Model MTS200 device provides relay contacts on its terminal at back panel of unit for Power, GPS Lost and Watchdog output. Factory set configuration for relay contacts for all three mentioned outputs is C-NO terminal.
- After device is Power ON, Power relay output is energized.
- After time is displayed on device display, watchdog relay contact gets energized after 5 to 6 seconds. Watchdog relay status indicates the healthy functionality of unit. If unit becomes unhealthy, the watchdog relay output will be off after few seconds and watchdog LED in front panel will be ON. It will maintain its output status till the unit regains its healthy status.
- If device is in LOCK condition, GPS LOST relay will be in energized condition and GPS LOCK led on front panel will be ON.
- All other event outputs including standard event output and additional event outputs (optional) are ON as per respective event time configured. Standard event output is configured at every 1 minute event and 1 sec event ON period.
- Factory set setting of all additional event outputs (optional) are set as 60 seconds event time with 50 milliseconds event ON period.
- Time and date displayed on unit will be in I.S.T. format (UTC + 5:30 hrs)- Indian Standard Time format and all other parameters such as gps lock status, gps parameters and other will be display in sequence at 5 or configurable seconds interval. If the parameter on display
- Once unit is Power up and time is displayed, unit will start transmitting serial NMEA frame on COM1 terminal located at back panel of unit. NMEA output communication settings will be at 9600, 8, N, 1. NTP outputs will be at configured factory set factory IP address and will be active once NTP client request are received on particular NTP port. IRIG-TTL output will be at TTL voltage level i.e. 0(low level) and 5V(high level) and IRIG-AM (Amplitude Modulated) output will be available at 3.6Vpp.

8.4 Basic Normal Run Mode Operation

- After unit is boot up completely and time is available on display, all the outputs of unit i.e. event pulse outputs, IRIG, NTP and serial time outputs will be available as per unit clock.
- MTS200 size unit display supports 20 x 2 lines LCD which displays parameters such as time with local/UTC information, date with day of week, GPS LOCK/UNLOCK status, position information, day of year, type of serial frame format on COM2 terminal, ntp pps offset value, configured timezone, DST ON/OFF status.
- Parameter such as Time is always displayed on First line of LCD display.
- Other parameters such as Date, GPS LOCK/UNLOCK status and total satellites visible by receiver, as position information, day of week, day of year, type of serial frame format on COM2 terminal, ntp pps offset, timezone and dst information are display on 2nd line of display. These parameters are displayed in rotation as per configured interval or can be stopped by configuring parameter “Display Update Rate” to 0 using front panel keypad.
- During normal run mode of device, there are several messages displayed on LCD screen of unit as per condition prevail. Below are messages which are available on display screen of unit.
- Each Ethernet port Live / Not-Live status will be display on LCD screen. If RJ-45 cable is connected from MTS200 rear panel “ETH0” connector to end device or PC, it will shown as “Live” status, if and

Model: MTS200 (1U)

Doc. Ref. no. : m08/om/201

Issue no. : 03

only if the Eth interface is set as "UP" in device. If Eth interface is disable using "DOWN" configuration or if GPS rear-panel ETH0 connector is open, "Not-Live" status will be display for that particular Ethernet port.

Status Display: Local Time and date with Day of week

```
Time: 09:00:00 AM LCL
Date: 22/09/15 TUE
```

Status Display: Time and date with Day of week as per UTC

```
Time: 03:30:00 AM UTC
Date: 22/09/15 TUE
```

Status Display: Day of Year

```
Time: 09:00:00 AM LCL
Day of Year: 265
```

Status Display: Time frame available on Unit COM2 terminal

```
Time: 09:00:00 AM LCL
Format: $n9ts
```

Status Display: LOCK/UNLOCK information

```
Time: 09:00:00 AM LCL
GPS SIGNAL LOST
```

```
Time: 09:00:00 AM LCL
GPS LOCKED
```

Status Display: Total No. of Satellite available

```
Time: 09:00:00 AM LCL
Satellite avail:10
```

Status Display: Receiver Position information

```
Time: 09:00:00 AM LCL
Latt: 2314.9194 N
```

```
Time: 09:00:00 AM LCL
Long: 07237.8437 E
```

```
Time: 09:00:00 AM LCL
Height: +83.90 M
```

Status Display: NTP (of internal clock) offset with PPS in milliseconds unit

```
Time: 09:00:00 AM LCL
NTP[PPS]: 0.004 ms
```


Status Display: Timezone and DST parameter

```
Time: 09: 00: 00 AM LCL  
TZ: +05: 30 DST: STOP
```

Status Display: Eth0 Port Connection Status

```
Time: 09: 00: 00 AM LCL  
Eth0 : Live
```

Status Display: Eth1 Port Connection Status

```
Time: 09: 00: 00 AM LCL  
Eth1 : Live
```

9 Unit Setup Configuration

masTER T-Sync **Model MTS200** setup can be done using front panel keypad buttons or front panel RS-232 based serial console or via Ethernet port eth0 or eth1 using Telnet, SSH, webserver and SNMP. Keypad options provided all basic general settings, network settings for eth0 and eth1 port, network services configuration, GPS receiver related settings and limited NTP server settings.

Complete device configuration settings is provided through console based configuration utility (named as “**start**” application file) which can be run through front serial console or Telnet or SSH. Also, webserver and SNMP management in MTS200 provides complete device configuration facility.

9.1 Keypad based configuration

masTER T-Sync **Model MTS200** can be configured for parameters related to serial port COM2, time Format on LCD, Ethernet network settings for eth0 and eth1 port, NTP server configurations, GPS receiver, manual time as well as Events period through its 8 key keypad on device front panel. Below are few key parameters which can be configured through keypad.

- The COM2 output communication parameters baud rate, number of stop bits and parity.
- Serial frame on COM2 port at rear panel of device i.e. NGTS / T-Format/ GPZDA / GPZDA.
- The LCD Display Format includes Hour Mode and Time Format (UTC/LOCAL), 12Hour/24 Hour mode.
- Standard Event Mode can be either configured for event per minute or event per hour.
- Configuring four additional Event’s period & Event On time.
- Network settings include DHCP service, IP address, subnet mask, default gateway for each Ethernet port as well as eth0, eth1 can be enabled or disable using UP/DOWN option.
- Configuration of various network services such as Telnet, SSH, SNMP, HTTP, HTTPS, FTP.
- NTP server settings include local clock service, local clock stratum during device UNLOCK and NTP service start/stop option.
- Calendar settings include manual time, universal time-zone and Daylight Saving time options.
- On IRIG o/p port, user can configure it for either IRIG-B122/120 or IEEE-1344 format and with UTC/LOCAL time option in IRIG frames.
- The user can also reset entire unit using RESET UNIT option.
- Factory default/Restore of all parameters of GENERAL Settings, NTP settings, SNMP Settings, Ethernet network settings.
- Configuration of display parameters rate for second line on LCD display.

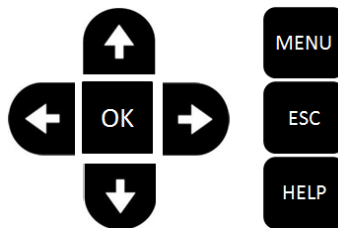


Figure 9-1 Front Panel Keypad Layout


KEY	FUNCTION
MENU	For Entering into Configuration mode.
HELP	To Display help about every parameter configurations.
OK	To save the final Configurations.
ESC	To come back into Run mode.

UP	Scroll between various parameters in ascending order in main menu and to change parameters value in submenu.
DOWN	Scroll between various parameters in descending order in main menu and to change parameters value in submenu.
LEFT	To select various available options for the particular parameter in main menu and scroll between various parameters in submenu.
RIGHT	To select various available options for the particular parameter in main menu and scroll between various parameters in submenu.

Table 9-1 Key Functions

For all main menu parameters, go to that parameter using “UP” / ”DOWN” key till the parameter you want to change is available on display. After that using “LEFT” / “RIGHT” keys go to desired option of that parameter and press “OK” key to save changed parameter. “OK” key is required to save the changes configured by user. Once “OK” key is pressed, on display "Configuring....." message will be displayed which indicates MTS200 is saving your configurations. Wait till this message is there on display.

There are two passwords for configuring *masTER* T-Sync **Model MTS200** through keypad. One is user-defined password (0001 to 9999.), which can be changed by the user. By factory set, this password is '0001'. Another is Immortal Password that cannot be changed by any user and it kept confidential to Masibus Service Engineers. Users are recommended to change the user-defined password as per there requirement.

	<p>INFORMATION</p> <ul style="list-style-type: none"> • Password of configuration through keypad and password of configuration through serial terminal are independent. • It is operator’s responsibility to remember the configured password if it is changed from factory set password. • It is necessary to press OK key after changing any previous configuration through keypad, failing of which the particular parameter will restore to its previous setting. • If no option is selected or keypad button is pressed for 60 seconds interval, device will exit from keypad menu and display run mode parameters.
---	---

Flowchart of Keypad Menu represented in below figure.

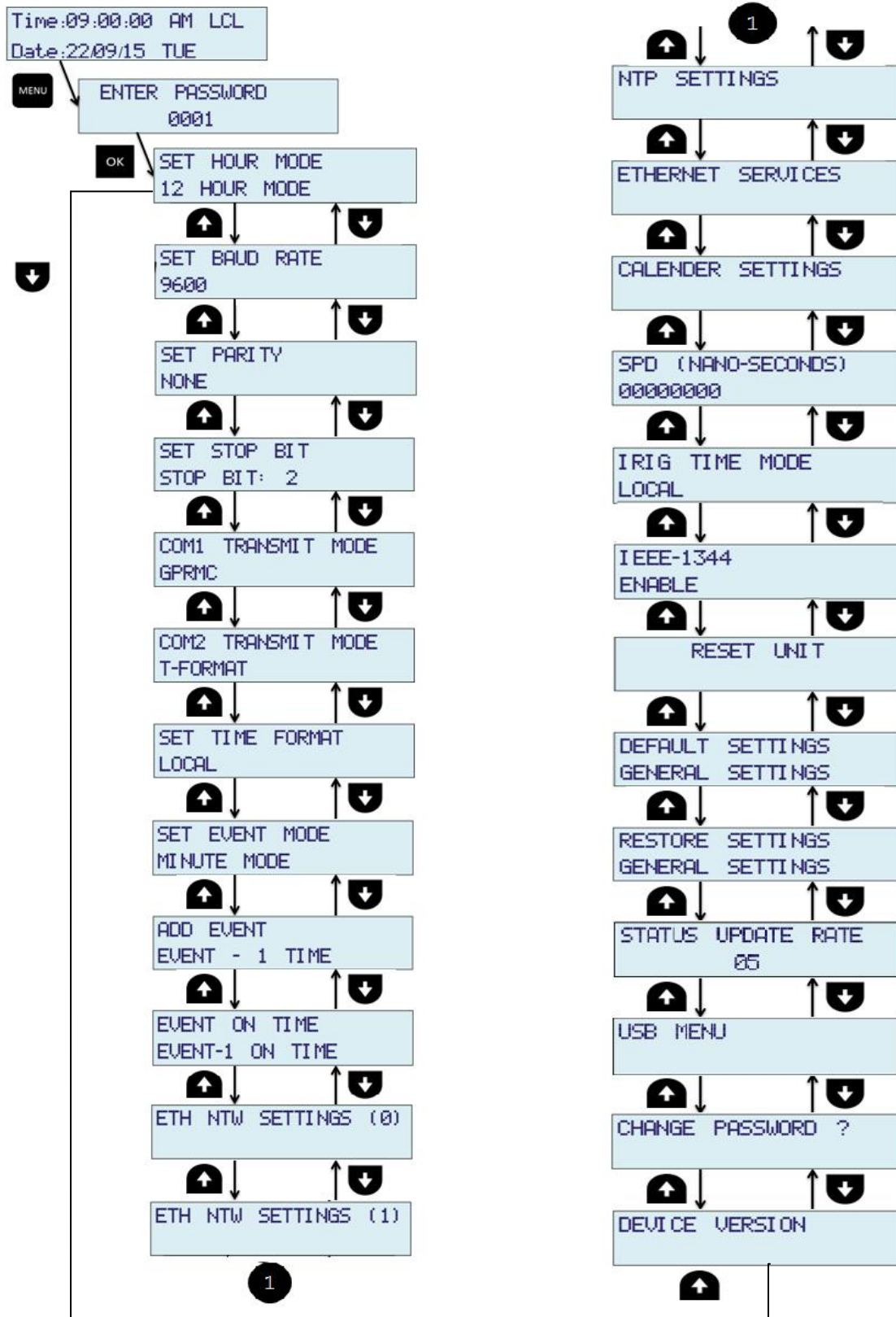


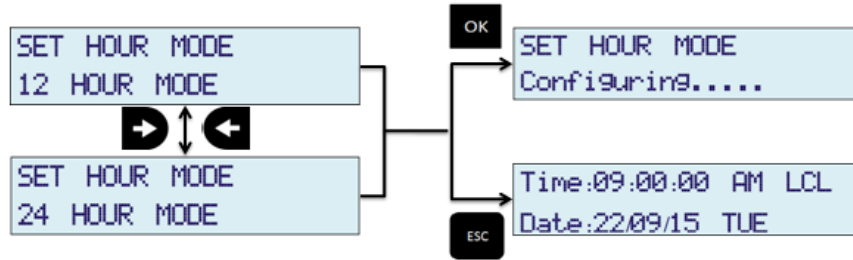
Figure 9-2 Display Main Menu layout

GENERAL SETTINGS:

To enter the configuration mode of MTS200 using front keypad, user need to press “MENU” key and then enter appropriate password. This will allow user to enter configurable parameters option and this parameters can be configured as explained in below section.

1. SET HOUR MODE

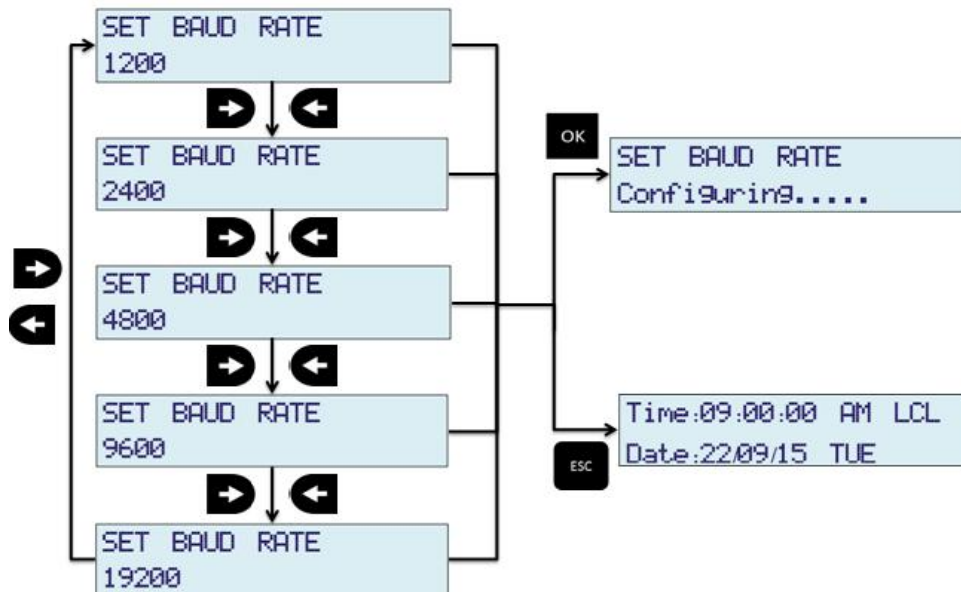
MTS200 provides its internal clock time information on LCD display, SNMP status and webserver home page. This time information can be configured for 12 hour or 24 hour format. Whenever user selects 12 hour format, AM/PM information is displayed in time information.



As shown above, “LEFT” and “RIGHT” key are used to change setting of HOUR MODE. “OK” key will save the setting and “ESC” key will reject new setting and keep old value of this parameter in effect and come out of configuration MENU mode to RUN mode.

2. SET BAUD RATE

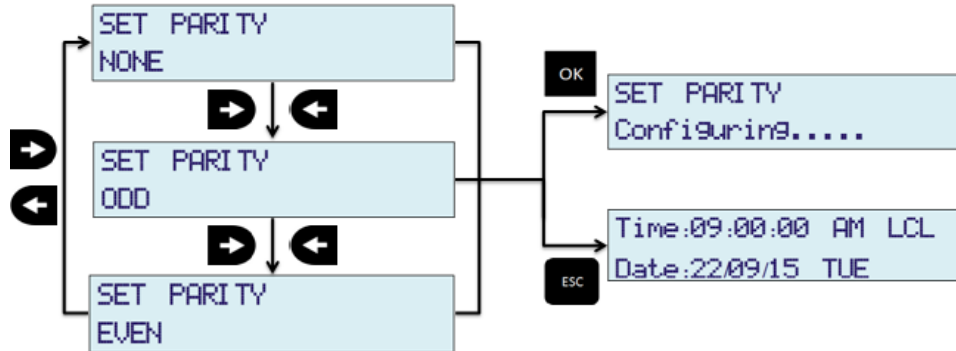
COM2 serial port output baudrate at rear panel of MTS200 can be set by using this option. MTS200 is capable to provide serial time frame on COM2 terminal at configurable baud rates of 1200 / 2400 / 4800 / 9600 / 19200.



As shown above, “LEFT” and “RIGHT” key are used to change setting of HOUR MODE. “OK” key will save the setting and “ESC” key will reject new setting and keep old value of this parameter in effect and come out of configuration MENU mode to RUN mode.

3. SET PARITY

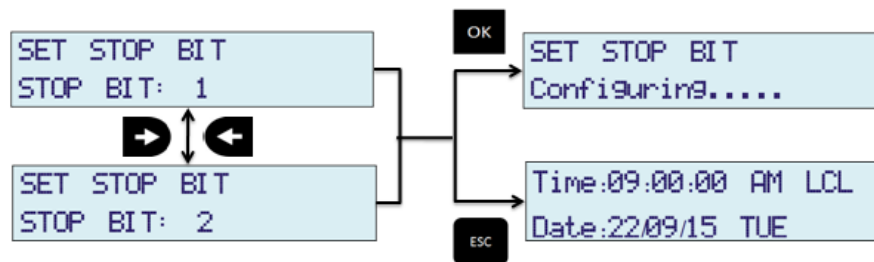
COM2 serial port output parity bit at rear panel of MTS200 can be set by using this option. MTS200 is capable to provide serial time frame on COM2 terminal at configurable parity options of NONE / ODD / EVEN.



As shown above, “LEFT” and “RIGHT” key are used to change setting of HOUR MODE. “OK” key will save the setting and “ESC” key will reject new setting and keep old value of this parameter in effect and come out of configuration MENU mode to RUN mode.

4. SET STOP BIT

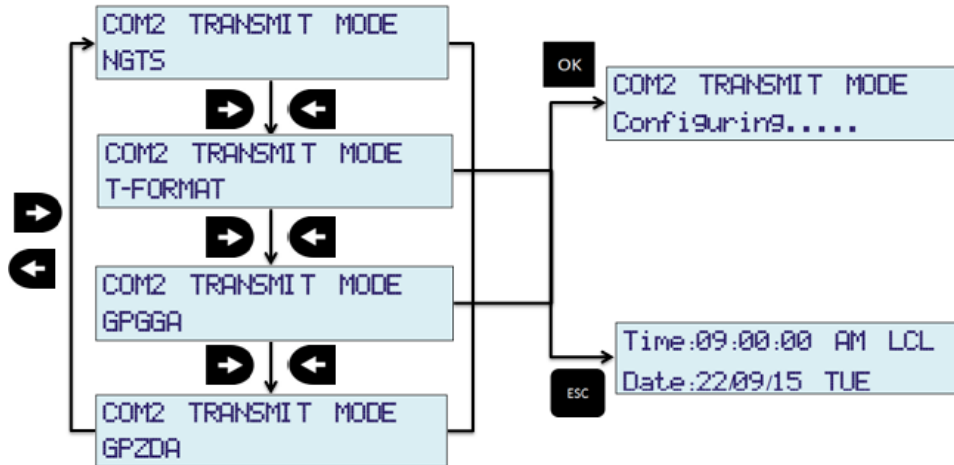
COM2 serial port output stop bit at rear panel of MTS200 can be set by using this option. MTS200 is capable to provide serial time frame on COM2 terminal at configurable stop bit options of 1 / 2 stop bits.



As shown above, “LEFT” and “RIGHT” key are used to change setting of HOUR MODE. “OK” key will save the setting and “ESC” key will reject new setting and keep old value of this parameter in effect and come out of configuration MENU mode to RUN mode.

5. COM2 TRANSMIT MODE

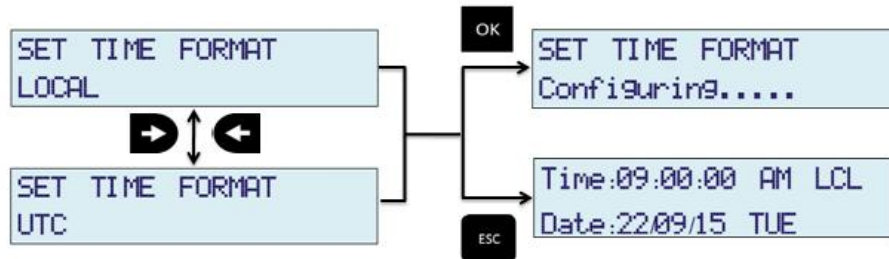
COM2 serial port output serial time string can be set by using this option. MTS200 is capable to provide different types of serial time string such as T-format, NGTS, GPZDA, GPGGA on COM2 terminal.



Serial Time frame T-format, GPZDA and GPGGA are transmitted at every 1 second while NGTS time frame is transmitted at every 1 minute. Refer section 11.1 for detail description of each time string. As shown above, “LEFT” and “RIGHT” key are used to change setting of HOUR MODE. “OK” key will save the setting and “ESC” key will reject new setting and keep old value of this parameter in effect and come out of configuration MENU mode to RUN mode.

6. SET TIME FORMAT

MTS200 provides its internal clock time information on LCD display, SNMP status and webserver home page. This time information can be set for UTC or LOCAL timezone. LOCAL time depends on UTC time + timezone set.

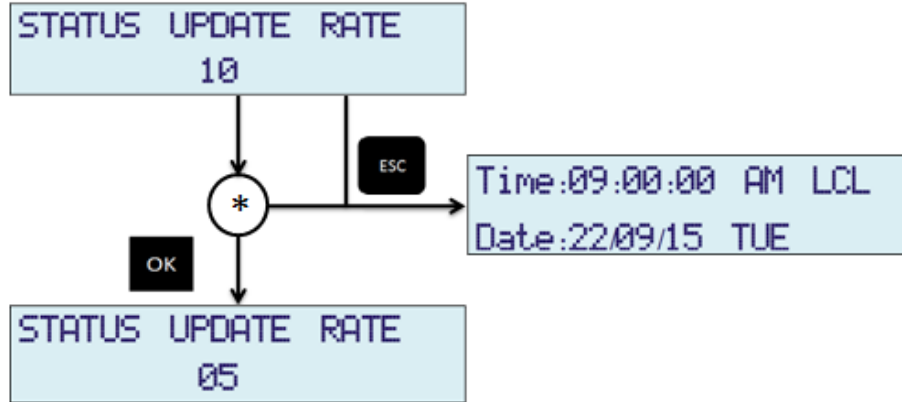


As shown above, “LEFT” and “RIGHT” key are used to change setting of HOUR MODE. “OK” key will save the setting and “ESC” key will reject new setting and keep old value of this parameter in effect and come out of configuration MENU mode to RUN mode.

7. DISPLAY UPDATE RATE

MTS200 displays time information on first line of LCD display whereas other various parameters such as date, COM2 terminal serial format, GPS receiver information, LOCK/UNLOCK status, set timezone , DST ON/OFF status, Day of Year are displayed on second line of LCD display in fixed in rotation at a fixed interval. This interval is configured in seconds and can be changed by user. If this interval is set to value “0”, then the auto-rotation of parameters on second line of LCD display will stop and only Date information will be displayed on second line of LCD display.

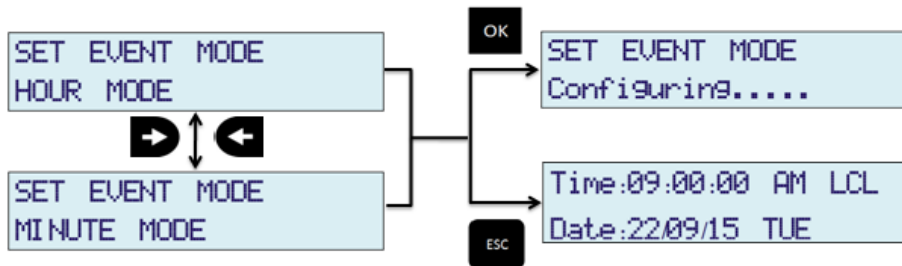
Below method explains to configure this Display Update Rate.



* : After DISPLAY UPDATE RATE option is displayed, press OK key to change its value. After OK key is pressed, cursor will blink which indicates now you can change the value. Its minimum value is 1 second and maximum value is 10 seconds. Values can be changed using UP/DOWN arrow of single digit on which cursor is blinking and use LEFT/RIGHT arrow keys to change position of blinking cursor.

8. Standard EVENT Output

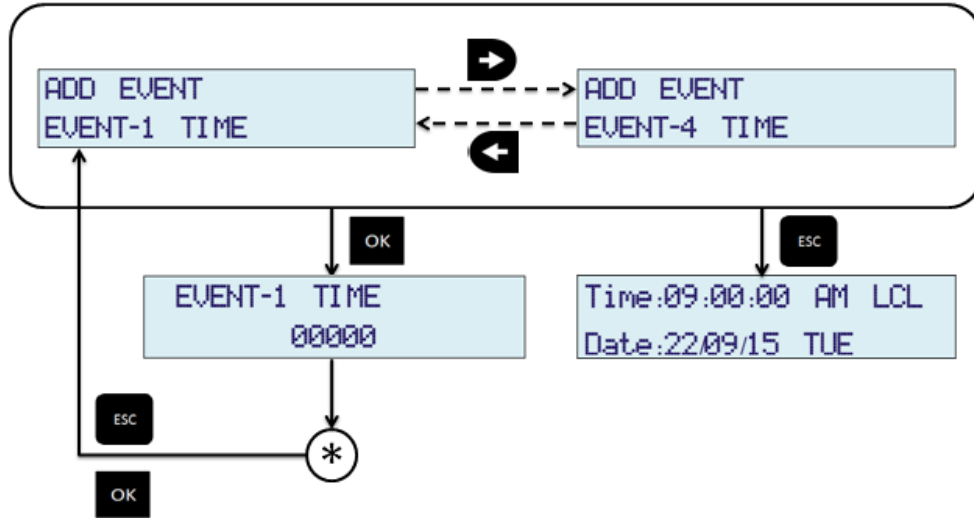
MTS200 provides standard Pulse event output at every minute or every hour. The pulse output present would of 200 ms ON time.



As shown above, “LEFT” and “RIGHT” key are used to change setting of HOUR MODE. “OK” key will save the setting and “ESC” key will reject new setting and keep old value of this parameter in effect and come out of configuration MENU mode to RUN mode.

9. ADDITIONAL EVENT [1 to 4]

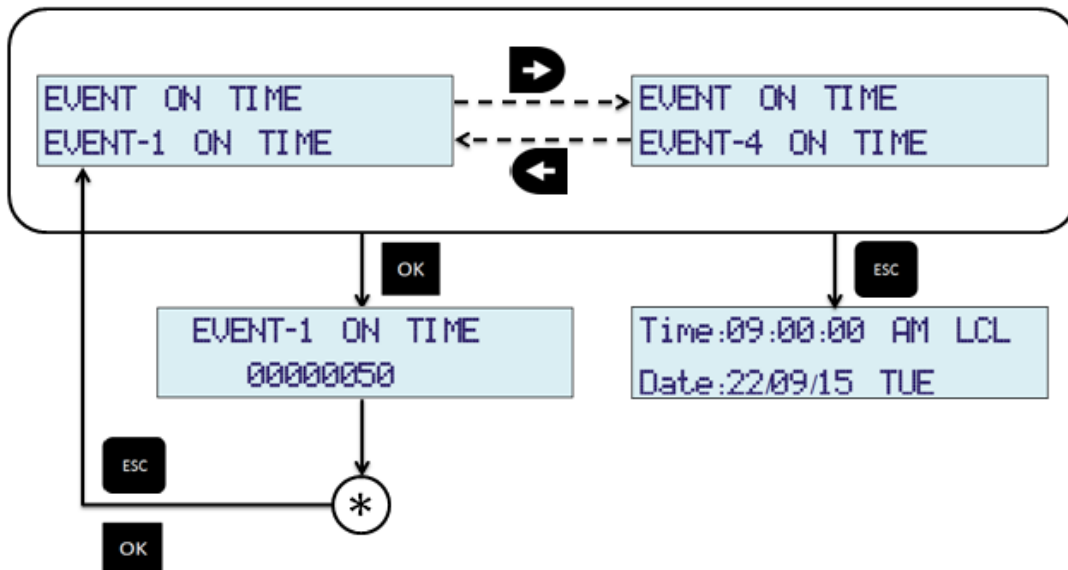
In addition to standard event output, MTS200 also provides 4 additional event outputs. This events output can be configured from 1 second period to 86400 seconds (1 day) period. If this events are configured with 0 value, that particular event output will be disabled and hence no pulse output will be on that particular event. User can also configure duty cycle (ON time) of each event output as explained in next section 12.2.3.



* : Cursor will start blinking once user enters this mode by pressing “OK” key. To change specific digit, use “UP” / “DOWN” arrow keys and to change the position of blinking cursor use “LEFT” / “RIGHT” arrow keys. UP/DOWN arrow keys will update the digit on which cursor is blinking. After value is edited, press “OK” again to save the parameter. After user presses “OK” key, user will return to main menu again. User can switch between EVENT1, EVENT2, EVENT3 and EVENT4 menu using “LEFT” and “RIGHT” key and follow above steps to configure the parameter.

10. EVENT ON TIME

ALL additional events 1 to 4 outputs can be also configured for ON duration time (duty cycle) for above configured respective event period time. The ON time can be configured from 50 milliseconds to maximum 50% of configured respective EVENT period in milliseconds. Units of EVENT ON Time for EVENT 1 to 4 is in milliseconds.



Model: MTS200 (1U)

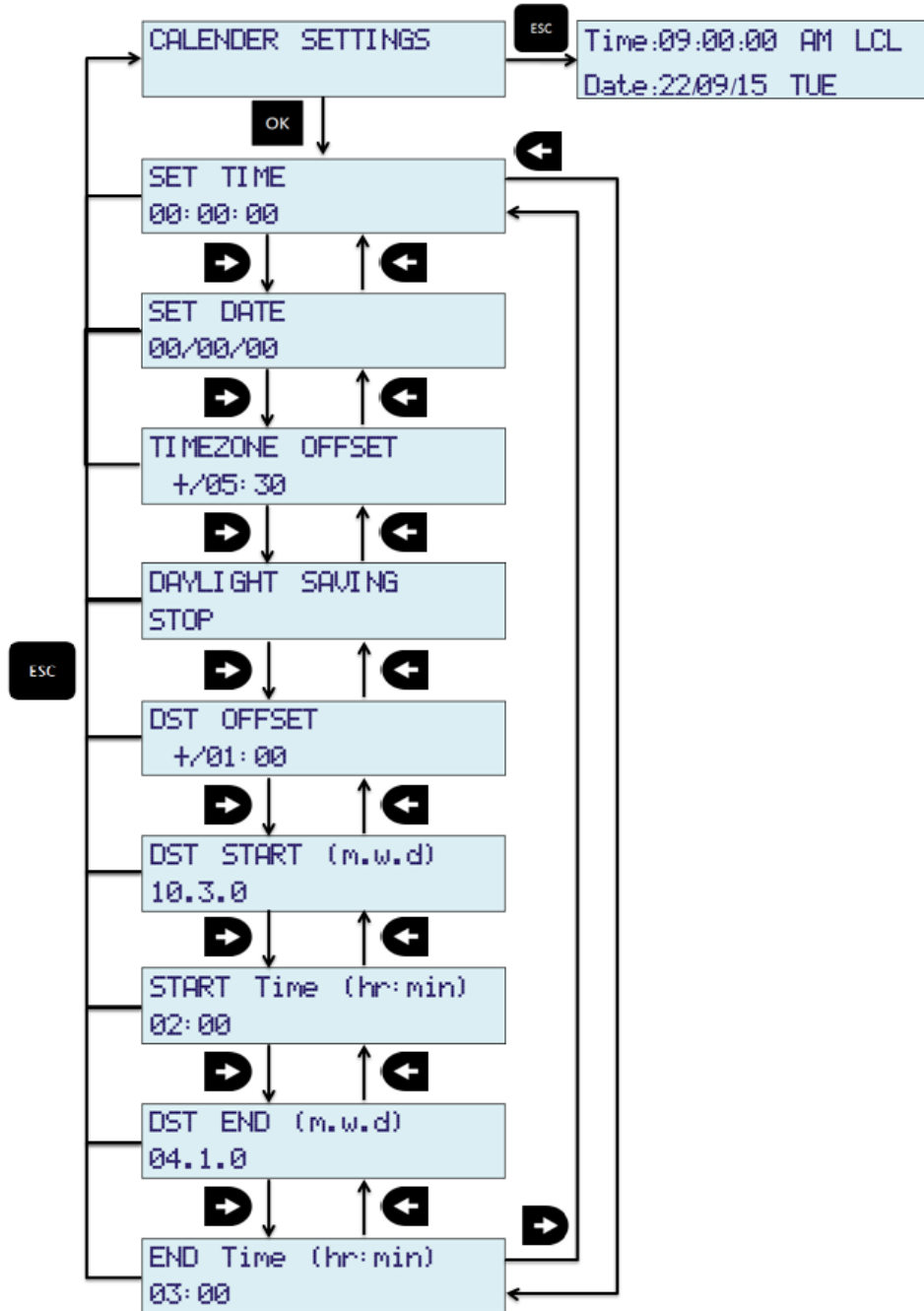
Doc. Ref. no. : m08/om/201

Issue no. : 03

* : Cursor will start blinking once user enters this mode by pressing “OK” key. To change specific digit, use “UP” / “DOWN” arrow keys and to change the position of blinking cursor use “LEFT” / ”RIGHT” arrow keys. UP/DOWN arrow keys will update the digit on which cursor is blinking. After value is edited, press “OK” again to save the parameter. After user presses “OK” key, user will return to main menu again. User can switch between EVENT1, EVENT2, EVENT3 and EVENT4 menu using “LEFT” and “RIGHT” key and follow above steps to configure the parameter.

CALENDER SETTINGS:

User can set the internal clock time of MTS200 device in UNLOCK condition only. The internal clock time setting may be required when the internal RTC battery backup is drained and internal RTC reset to its default time. In such case, NTP output will not be in sync with actual time. So, if user needs correct time on all outputs In such condition, it is recommended to set the internal clock time [in UTC] first and then use all outputs of MTS200 for clients devices. Whenever user sets the internal clock time, GPS receiver is configured with new entered clock data and ntp service is restarted automatically.



Other options in calendar settings are timezone setting for setting the local time, Daylight Settings. **All the calendar settings will only become effective once user come out of configuration mode of keypad menu to normal run mode.**

1. TIMEZONE SETTING

Timezone setting is used to set the LOCAL time of device. LOCAL time can be different from UTC time. MTS200 internal clock operates on UTC time so, it is necessary to set the timezone for configuring the local time of internal clock for LCD display, serial frame (T-format, NGTS) outputs. Local time is derived

Model: MTS200 (1U)

Doc. Ref. no. : m08/om/201

Issue no. : 03

by setting the timezone offset configured in device with respect to UTC time. Timezone format is **+/-:hr:min.**


+/- is the offset polarity

hr=hours, -12 to +12

min = minutes, 0 to 59

Default timezone set from factory is +05:30.

Refer below image for timezone setting:



TIMEZONE OFFSET
+/05:30

In above figure, user can enter the Timezone setting option in Calendar setting mode by using “LEFT” or “RIGHT” key. The value displayed in Timezone option is the current configured timezone offset. To modify this value, press “OK” key and then UP/DOWN key to edit the value at cursor and LEFT/RIGHT key to shift the cursor. After value is set, press “OK” key to save the settings.

As soon as value is saved, the change in offset will be reflected on all outputs configured to show local time.

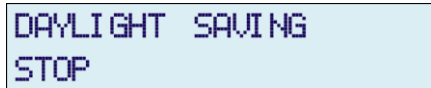
User should check the settings of DST since if DST is ON, it can affect the Local time display which again depends on DST time parameters set.

Note:

- **All the calendar settings will only become effective once user come out of configuration mode of keypad menu to normal run mode.**

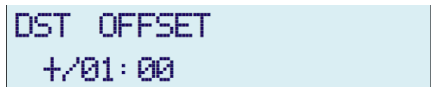
2. DST (DAYLIGHT SETTINGS)

MTS200 can be configured for Daylight settings and selectable option to set DST ON or OFF though keypad. Daylight offset works with respect to UTC. So, user needs to enter the daylight offset w.r.t. UTC time as timezone offset is neglected during daylight start and end time.



DAYLIGHT SAVING
STOP

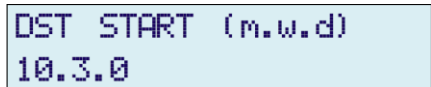
User can start or stop daylight saving feature by option DST ON / OFF setting. For saving daylight parameters, user need to enter all below parameters for correct local time effect for DST. Following are parameters need to set correctly for correct local time for DST.



DST OFFSET
+/01:00

“DST Offset” = **format (+/-:hr:min)**. This is DST offset w.r.t. UTC time.

+/-:hr:min = +/- DST offset polarity w.r.t UTC, hr is hour 0 to 12 and min is minutes 0 to 59.



DST START (m.w.d)
10.3.0

“DST Start” = **Format (m.w.d)**. This is DST start day on which the DST offset will come into effect.

m.w.d = month.week of month.day of week of month. This specifies day *d* ($0 \leq d \leq 6$) of week *w* ($1 \leq w \leq 5$) of month *m* ($1 \leq m \leq 12$). Week 1 is the first week in which day *d* occurs and week 5 is the last week in which day *d* occurs. Day 0 is a Sunday.

```
START Time (hr:min)
02:00
```

“DST Start Time” = Format (hr:min). This the time on DST start day when DST effect should start.
 Hr:min = hour form 0 to 12 and minute from 0 to 59

```
DST END (m.w.d)
04.1.0
```

“DST End” = Format (m.w.d). This is DST endday on which the DST effect will lapse.
 m.w.d = month.week of month.day of week of month. This specifies day *d* ($0 \leq d \leq 6$) of week *w* ($1 \leq w \leq 5$) of month *m* ($1 \leq m \leq 12$). Week 1 is the first week in which day *d* occurs and week 5 is the last week in which day *d* occurs. Day 0 is a Sunday.

```
END Time (hr:min)
03:00
```

“DST End Time” = Format (hr:min). This the time on DST end day when DST will lapse.
 Hr:min = hour form 0 to 12 and minute from 0 to 59

e.g.:

Here is an example for New Zealand, where the standard time (NZST) is 12 hours ahead of UTC, and daylight saving time (NZDT), 13 hours ahead of UTC, runs from the first Sunday in October to the third Sunday in March, and the changeovers happen at the default time of 02:00:00:

- DST Offset = -13:00
- DST Start = 10.1.0
- DST Start Time = 02:00
- DST End = 03.3.0
- DST End Time = 02:00

Note:

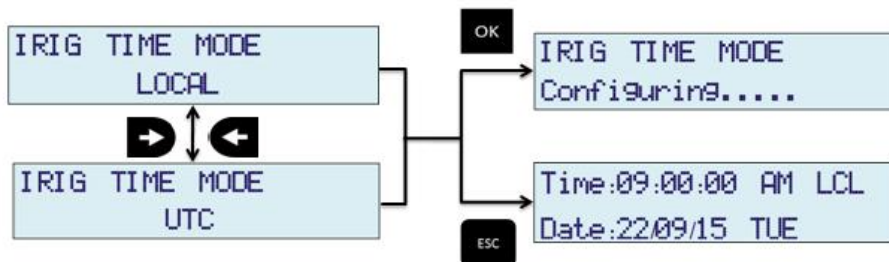
- All the calendar settings will only become effective once user come out of configuration mode of keypad menu to normal run mode.

IRIG O/P PARAMETERS

1. IRIG TIME MODE

MTS200 provides IRIG-B / IEEE 1344 output through BNC connector available on rear panel of device. MTS200 provides the output in DCLS as well as AM output. For further details regarding IRIG-B / IEEE 1344, refer section 11.2.

The time information in IRIG-B and IEEE 1344 output can be local time or UTC time information which can be configured by this parameter. The local time in IRIG-B / IEEE 1344 output will be as per configured timezone and DST settings.



Model: MTS200 (1U)

Doc. Ref. no. : m08/om/201

Issue no. : 03

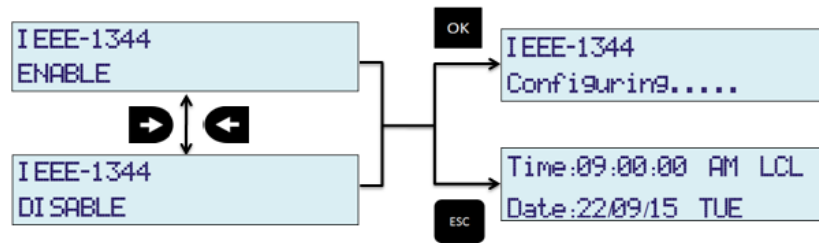
As shown above, “LEFT” and “RIGHT” key are used to change setting of HOUR MODE. “OK” key will save the setting and “ESC” key will reject new setting and keep old value of this parameter in effect and come out of configuration MENU mode to RUN mode.

Note:

- **Settings will only become effective once user come out of configuration mode of keypad menu to normal run mode.**

2. IEEE-1344

MTS200 provides time output in IRIG-B or IEEE 1344 format on same BNC terminal available on rear panel of device. The output type can be configured using this option as described below. For further information, refer section 11.2.



As shown above, “LEFT” and “RIGHT” key are used to change setting of HOUR MODE. “OK” key will save the setting and “ESC” key will reject new setting and keep old value of this parameter in effect and come out of configuration MENU mode to RUN mode.

Note:

- **Settings will only become effective once user come out of configuration mode of keypad menu to normal run mode.**

ETHERNET PARAMETERS:

MTS200 is equipped with standard 10/100 Mbps eth0 port and optional 10/100/1000 Mbps eth1 port on rear panel of device. The network settings for these ports can be done through front panel keypad as shown in below figure. Also, network services such as Telnet, SSH, HTTPS, HTTPS, FTP can be configured through keypad.

MTS200 displays live current applicable network settings of each ethx interface such as IP address, Subnet Mask, Gateway and MAC Address on the main menu on LCD display in ETH NTW SETTINGS (0) for eth0 and ETH NTW SETTINGS (1) for eth1. However, MAC Address is fixed for each eth port and cannot be configured manually. Live settings for specific Ethernet port in case of IPv4 addressing scheme are displayed with " * " sign at end of parameter value. User can configure any parameter related to Ethernet port individually.

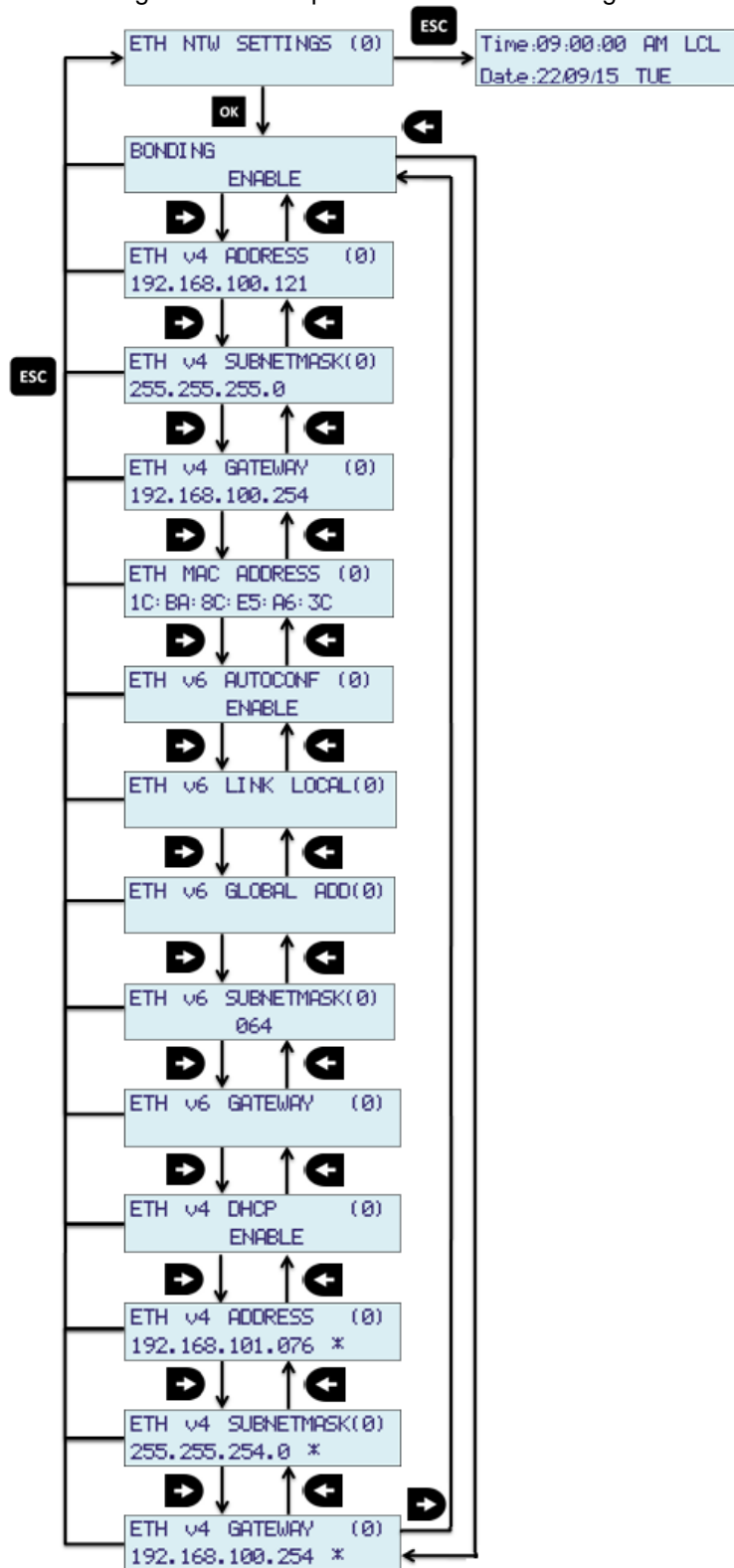
DHCP is Dynamic Host configuration Protocol, for IPv4 addressing scheme, in which respected Ethernet port will acquire the network parameters IP address, Subnet Mask and Gateway from DHCP server. However, DHCP feature can be used to fast track the configuration of MTS200 device through Ethernet communications like Telnet, SSH or Webserver. Network address acquired by DHCP can be viewed on LCD display while navigating to ETH NTW SETTINGS menu.

Autoconfiguration is for IPv6 addressing scheme, in which respected Ethernet port will acquire IPv6 address, Subnet Mask and Gateway from network automatically, if the LAN supports IPv6 infrastructure. Network address acquired by AUTOCONF can be viewed on LCD display while navigating to ETH NTW SETTINGS menu.

As on every Power UP of device, if Ethernet port is configured for DHCP, it will re-acquire network parameters for respected Ethernet port which can result in different IP address as compare to previous.

So, it is recommended to use DHCP mainly for initial network communication and thereafter configure static address of Ethernet port.

User can view the network settings for both eth port as shown in below figure.

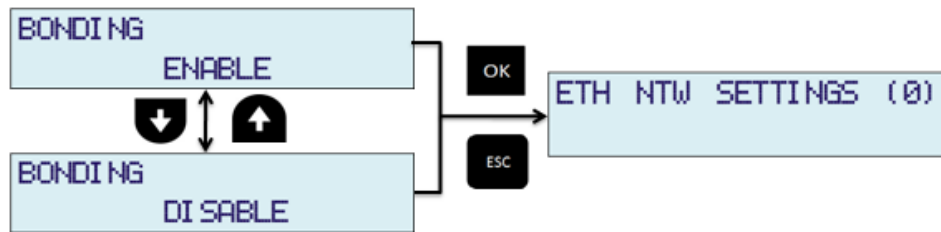


Configuration of Eth0 (EthX) Parameters

1. Bonding

Here, user can configure bonding if MTS200 is with two Ethernet ports. In case of bonding "ENABLE", only configurations of Ethernet port 0 will be applicable to bonding.

To configure bonding of Ethernet port 0 and 1, user have to select "ENABLE" for BONDING and press OK key to save changes as shown in figure.



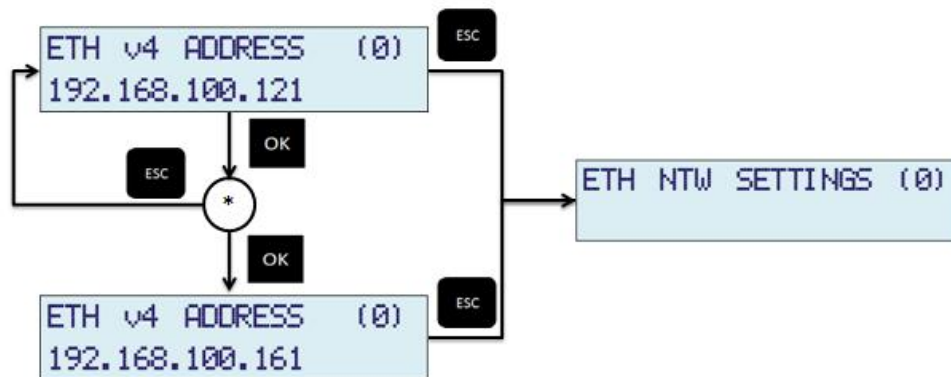
In case of bonding both Ethernet port will be using common IP address and other network setting for IPv4 as well as IPv6. MAC address of interface will be same as particular Ethernet port's MAC address which one is active.

Note:

- To configure bond, user need to configure Ethernet 0's configuration parameters.
- User can view active Ethernet port for bonding on display in RUNMODE.
- Bonding is preferred when user want both Ethernet port to be worked in same network.

2. ETH v4 ADDRESS

Her, user can configure IPv4 address for specific port as shown in figure. If DHCP is "ENABLE" for respective port, this configurations will not affect IPv4 address.

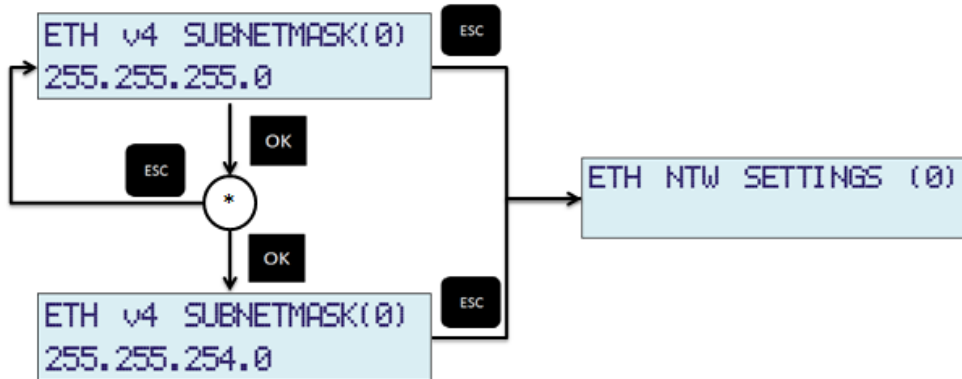


* : Cursor will start blinking once user enters this mode by pressing "OK" key, user can see blinking cursor on 1st position of 2nd line. To change specific digit, use "UP" / "DOWN" arrow keys and to change the position of blinking cursor use "LEFT" / "RIGHT" arrow keys. UP/DOWN arrow keys will update the digit on which cursor is blinking.

After value is edited, press "OK" again to save the parameter or "ESC" to restore parameter value. After user presses "OK" key, user can view changed IPv4 address.

3. ETH v4 SUBNETMASK

Her, user can configure IPv4 subnetmask for specific port as shown in figure. If DHCP is "ENABLE" for respective port, this configurations will not affect IPv4 address.

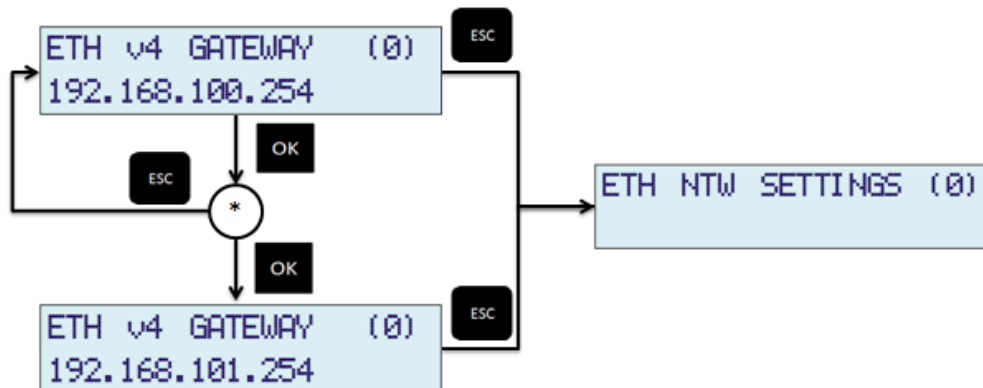


* : Cursor will start blinking once user enters this mode by pressing "OK" key, user can see blinking cursor on 1st position of 2nd line. To change specific digit, use "UP" / "DOWN" arrow keys and to change the position of blinking cursor use "LEFT" / "RIGHT" arrow keys. UP/DOWN arrow keys will update the digit on which cursor is blinking.

After value is edited, press "OK" again to save the parameter or "ESC" to restore parameter value. After user presses "OK" key, user can view changed IPv4 subnetmask.

4. ETH v4 GATEWAY

Her, user can configure IPv4 gateway for specific port as shown in figure. If DHCP is "ENABLE" for respective port, this configurations will not affect IPv4 address.



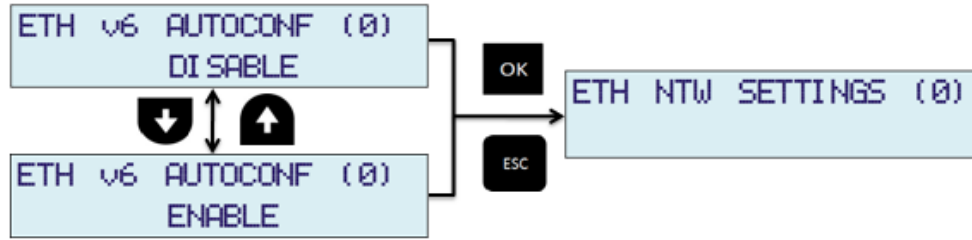
* : Cursor will start blinking once user enters this mode by pressing "OK" key, user can see blinking cursor on 1st position of 2nd line. To change specific digit, use "UP" / "DOWN" arrow keys and to change the position of blinking cursor use "LEFT" / "RIGHT" arrow keys. UP/DOWN arrow keys will update the digit on which cursor is blinking.

After value is edited, press "OK" again to save the parameter or "ESC" to restore parameter value. After user presses "OK" key, user can view changed IPv4 gateway.

5. ETH v6 AUTOCONF

Here, user can configure autoconfiguration mode for IPv6 addressing for specific port. By setting it as "ENABLE", user is configuring respected Ethernet port to receive IPv6 address from network

automatically. For automatic allocation for IPv6 address, user have to select ENABLE for ETH v6 AUTOCONF and press OK key to save changes as shown in figure.



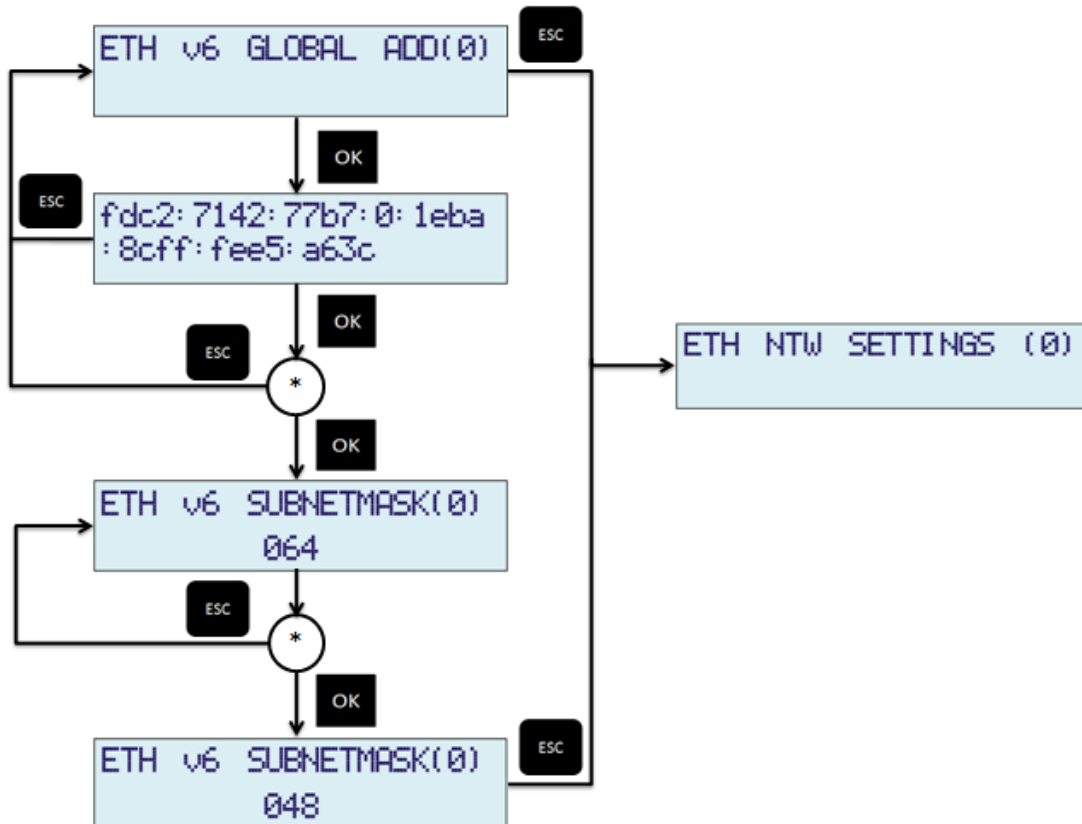
Once, user set AUTOCONF as ENABLE, user need to wait till respected Ethernet port receives IPv6 address from network. User can view allocated IPv6 address in ETH v6 GLOBAL ADD menu.

Note:

- Once, AUTOCONF is set to ENABLE, user can view allocated IPv6 address, subnetmask and gateway address in "ETH v6 GLOBAL ADD", "ETH v6 SUBNETMASK" and "ETH v6 GATEWAY" respectively. Till the IPv6 address is not allocated "ETH v6 ADDRESS" filed will display ":::" and "ETH v6 SUBNETMASK" field will display "000". Till the IPv6 default gateway is not defined by network, "ETH v6 GATEWAY" field will display "::".
- In case of bonding, displayed address is based on active Ethernet port.

6. ETH v6 GLOBAL ADD, ETH v6 SUBNETMASK

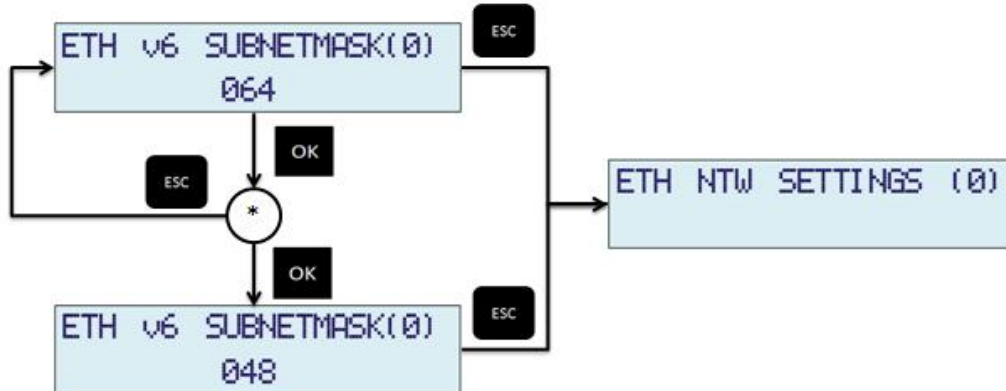
Her, user can configure IPv6 address and it's subnetmask for specific port as shown in figure. If AUTOCONF is ENABLE for respective port, user cannot configure it. IPv6 addresses are 128 bits long in 8 group of 16 bits.



* : Cursor will start blinking once user enters this mode by pressing “OK” key, user can see blinking cursor on 1st position of 2nd line. To change specific digit, use “UP” / “DOWN” arrow keys and to change the position of blinking cursor use “LEFT” / ”RIGHT” arrow keys. UP/DOWN arrow keys will update the digit on which cursor is blinking. User has to set " " for ending digits whenever changed IPv6 address length is less than previous set IPv6 address.

After value is edited, press “OK” again to save the parameter or "ESC" to restore parameter value. After user presses “OK” key, user can view changed IPv6 address and subnetmask at specific field in menu.

User can also configure only IPv6 subnetmask for specific port as shown in figure.

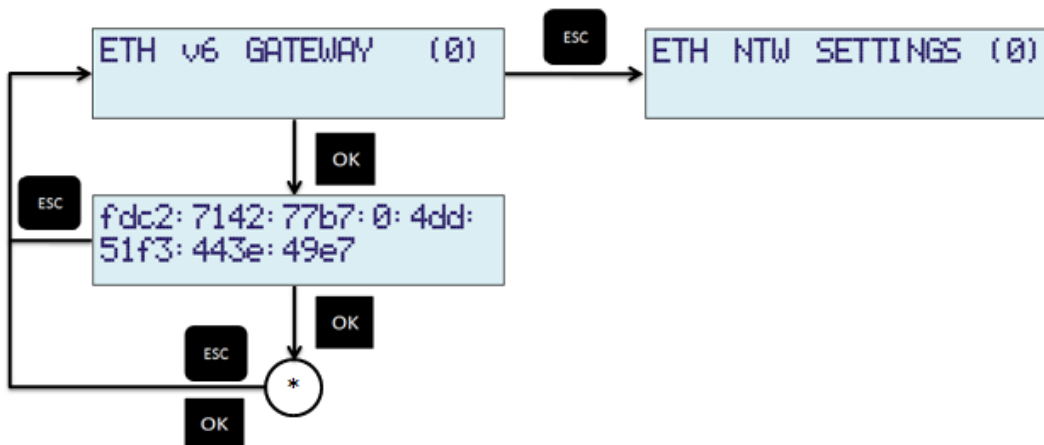


* : Cursor will start blinking once user enters this mode by pressing “OK” key, user can see blinking cursor on 1st position of 2nd line. To change specific digit, use “UP” / “DOWN” arrow keys and to change the position of blinking cursor use “LEFT” / ”RIGHT” arrow keys. UP/DOWN arrow keys will update the digit on which cursor is blinking.

After value is edited, press “OK” again to save the parameter or "ESC" to restore parameter value. After user presses “OK” key, user can view changed IPv6 subnetmask.

7. ETH v6 GATEWAY

Her, user can configure IPv6 gateway for specific port as shown in figure. If AUTOCONF is ENABLE for respective port, user cannot configure it.



* : Cursor will start blinking once user enters this mode by pressing “OK” key, user can see blinking cursor on 1st position of 2nd line. To change specific digit, use “UP” / “DOWN” arrow keys and to change

Model: MTS200 (1U)

Doc. Ref. no. : m08/om/201

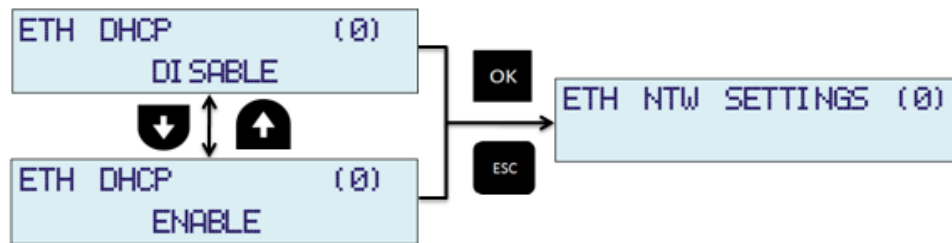
Issue no. : 03

the position of blinking cursor use "LEFT" / "RIGHT" arrow keys. UP/DOWN arrow keys will update the digit on which cursor is blinking.

After value is edited, press "OK" again to save the parameter or "ESC" to restore parameter value. After user presses "OK" key, user can view changed IPv6 gateway.

8. DHCP

Here, user can configure both Ethernet ports to be dynamically configured using DHCP protocol for IPv4. For dynamic allocation of network address, user have to select ENABLE for ETH DHCP and press OK key to save changes as shown in figure.



Note:

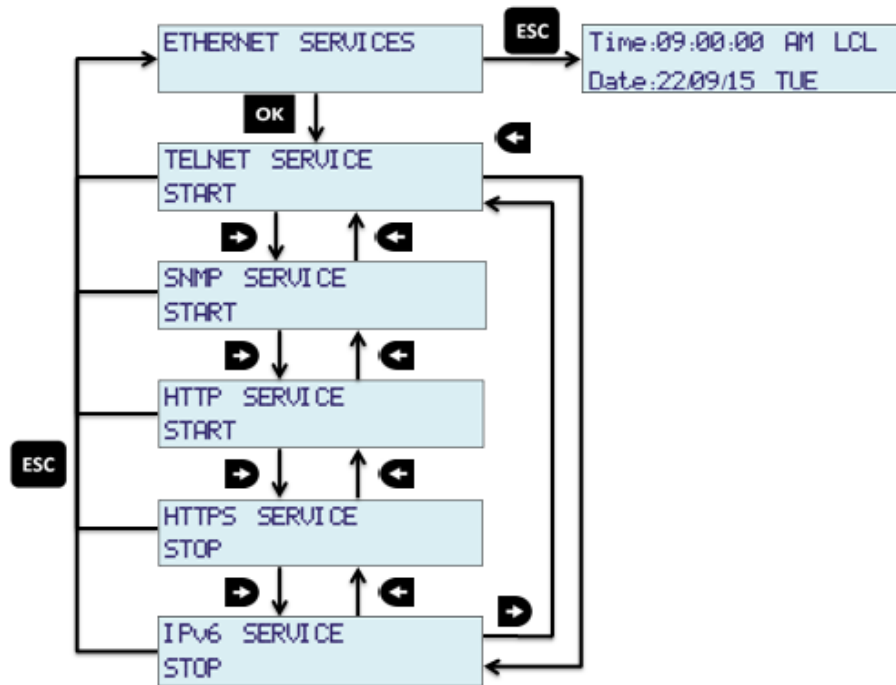
- Once DHCP service is enabled, device will start communication with available DHCP server in network and as a result, it may take few seconds for getting dynamic IP address from DHCP server. User can check the allocated DHCP IP address in "IP Address" menu on LCD display.
- If bonding is enabled, eth0 DHCP will only be effective in use.
- Refer section 13.6 for further details

NOTE :

1. If MTS200 is provided with only single Ethernet option, the other Ethernet port related parameters/configurations will be disabled and not accessible by operator.

Ethernet Services

As explained above, various network services such as Telnet, SSH, HTTP, HTTPS, FTP, SNMP can be set through keypad. Refer below figure.



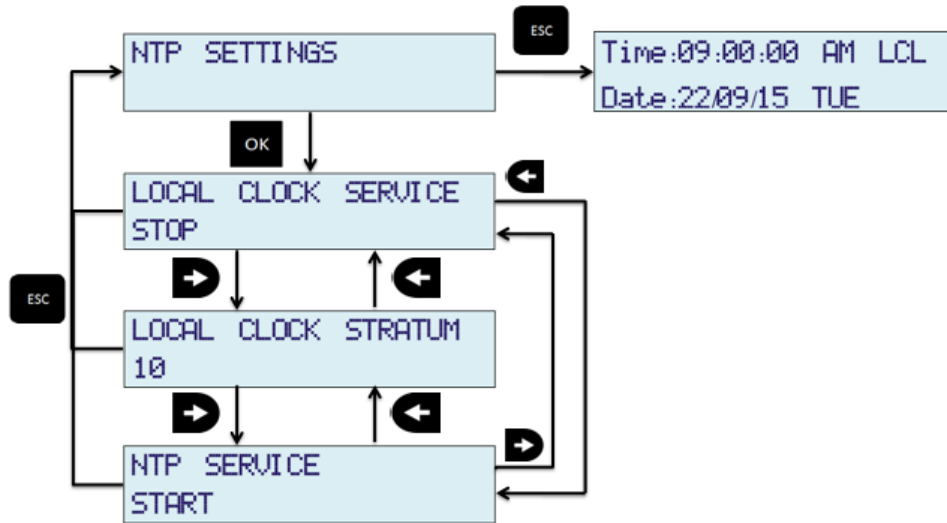
To START/STOP any service follow steps:

1. Go to specific service
2. Press OK key
3. Using UP/DOWN key change START/STOP option.
4. Press OK key

User need to restart the particular service if there is any change in those particular service configurations.

NTP PARAMETERS:

MTS200 act as stratum 1 NTP Server for NTP clients in network. However, during UNLOCK conditions, user can configure internal stratum from 0 to 15 value. Also, User can make local internal clock disable if not required. However, it is always recommended to keep internal LOCK clock enabled because during unlock conditions, MTS200 works on internal clock. If internal clock is disabled, MTS200 may not give correct time.



1. LOCAL CLOCK SERVICE:

MTS200 works on internal clock during Unlock conditions or when internal ntp driver is not synchronized with GPS receiver. User, cannot restart the NTP service during unlock conditions if this parameter is disabled. It is recommended to keep local service enabled. Local clock stratum in unlock conditions will come in effect only when local clock is enabled.

2. LOCAL CLOCK STRATUM:

Local clock stratum can be configured from 0 to 15. This can act as a alert to ntp clients whenever MTS200 is in unlock conditions. As internal ntp driver always provides stratum +1 value in ntp response to ntp clients, it is necessary to configure the stratum value -1 to whatever stratum is required at ntp client end.

3. NTP SERVICE:

NTP Service can be restarted using this option. It is necessary to restart NTP service whenever this change in any parameter related to NTP settings such as local clock enable/disable. Stratum, authentication keys, broadcast etc.

To change configuration of above parameters, follow below steps :

1. Go to specific parameter which want to be modified.
2. Press OK key.
3. Modify the parameter value.
4. Again press OK key.

GPS RECEIVER PARAMETERS:

1. SPD: (Antenna Cable Propagation delay compensation).

The internal GPS receiver outputs a 1PPS signal, the rising edge of which is placed at the top of the GPS or UTC one second time mark epoch as specified by the Time Mode command. The 1PPS Cable Delay Correction command allows the user to offset the 1PPS time mark in one nanosecond increments relative to the measurement epoch.

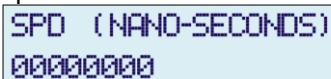
This parameter instructs the GPS receiver to output the 1PPS output pulse earlier in time to compensate for antenna cable delay. Up to 100 microseconds of equivalent cable delay can be removed. Zero cable delay is set for a zero-length antenna cable.

The user should consult a cable data book for the delay per unit length for the particular antenna cable used in order to compute the total cable delay needed for a particular installation.

This parameter may also be employed by the user to adjust the position of the 1PPS to compensate for other system delays.

Range: 0 to 99999 ns
Default value: 0 ns
Resolution: 1 ns

To modify value of SPD, follow below steps:



```
SPD (NANO-SECONDS)
00000000
```

1. Go to SPD menu using UP/DOWN arrow keys.
2. Press OK key.
3. You can see blinking cursor on last digit.
4. Change the value of specific digit using UP/DOWN arrow keys and change the position of blinking cursor using LEFT/RIGHT arrow keys.
5. Press OK key.
6. Wait till "Configuring....." message is there on display.

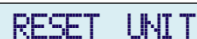


FUNCTIONALITY

This change in the value of this parameter will bring shift in 1PPS and other output signal timing.

RESET UNIT :

This mode will do software reboot of MTS200 device. For that just go to RESET UNIT menu using UP/DOWN arrow keys. After reaching at that menu, only press OK key.



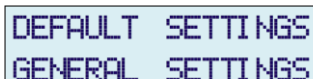
```
RESET UNIT
```

Device will be restart. Wait till time and date are there on Display.

DEFAULT SETTINGS :

Here, user can configure all factory default settings individually for GENERAL, ETHERNET, NTP and SNMP SETTINGS. For that just follow below steps:

1. Go to DEFAULT SETTINGS menu using UP/DOWN arrow keys as shown in figure.



```
DEFAULT SETTINGS
GENERAL SETTINGS
```

Model: MTS200 (1U)

Doc. Ref. no. : m08/om/201

Issue no. : 03

2. Go to option for which you want to configure default settings using LEFT/RIGHT arrow keys.
3. Press OK key.
4. Wait till "Configuring....." message is there on display. Message indicates device is saving new configurations.

User need to take care while configuring any type of settings to default factory as the settings will affect the already running particular communication such as SNMP, NTP, Network.

If user defaults the Network settings, the network settings of eth0 and eth1 such as IP Address, Subnet Mask and gateway will go on factory default and hence affect other network services such as Telnet, SSH, NTP, SNMP, Webserver.

User need to restart the particular Ethernet service such as NTP, SNMP if their settings are defaulted to factory settings.

Note:

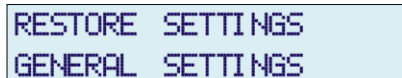
- **Settings will only become effective once user come out of configuration mode of keypad menu to normal run mode.**

RESTORE SETTINGS:

Here, user can restore previous settings of (GENERAL, ETHERNET, NTP and SNMP SETTINGS) once they are done factory default by user. This mode will only restore previous settings before default.

For that just follow below steps :

1. Go to RESTORE SETTINGS menu using UP/DOWN arrow keys as shown in figure.



```
RESTORE SETTINGS
GENERAL SETTINGS
```

2. Go to option for which you want to configure restore settings using LEFT/RIGHT arrow keys.
3. Press OK key.
4. Wait till "Configuring....." message is there on display. Message indicates DEVICE is saving new configurations.

User need to take care while configuring any type of settings to restore as the settings will affect the already running particular communication such as SNMP, NTP, Network.

If user restore the Network settings, the network settings of eth0 and eth1 such as IP Address, Subnet Mask and gateway will go on factory default and hence affect other network services such as Telnet, SSH, NTP, SNMP, Webserver.

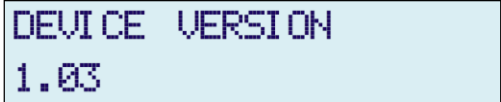
User need to restart the particular Ethernet service such as NTP, SNMP if their settings are restored to factory settings.

Note:

- **Settings will only become effective once user come out of configuration mode of keypad menu to normal run mode.**

SYSTEM INFORMATION

This option displays the MTS200 device system version information.

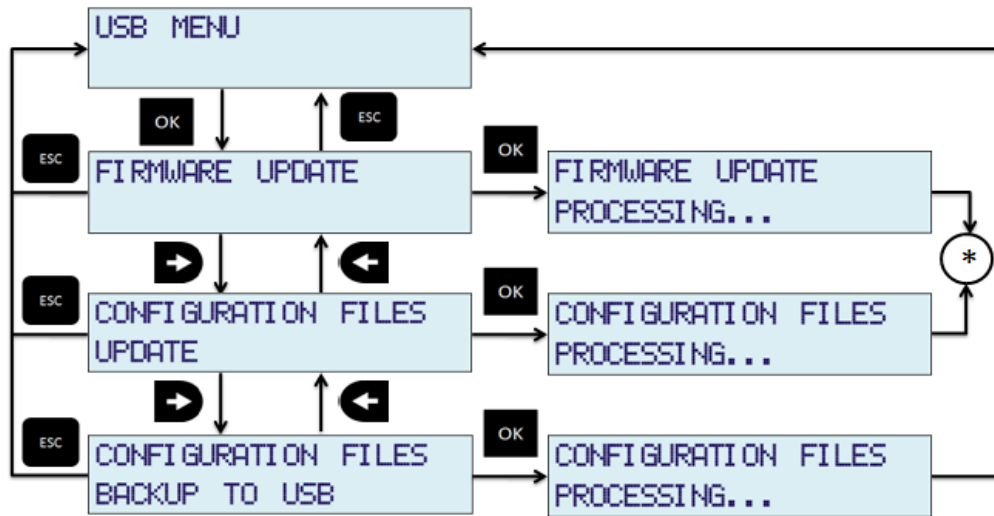


USB Menu

User can enter in this menu only if USB Pendrive is connected to USB port of MTS200 at front panel. If USB Pendrive is not connected, MTS will blink "NO DEVICE DETECTED". User can do following operations:

- 1) Firmware Update
- 2) Configuration Files Update
- 3) Configuration Files backup to USB


Using options 2 and 3, user can configure same settings in number of MTS200 devices.



* : MTS will be reboot after copying respected files from USB device to MTS for it's operation with new firmware/configurations.

Note:

- To update configuration files, files should be kept in a folder named "MTS200" in USB Pendrive. This folder should be present in USB device.
- Configuration files backup to USB option will transfer configuration files to "MTS200" folder in USB device.
- In any option if respected files are not found in USB device, MTS200 will display "FILES NOT FOUND" message and if USB stick is not found, "NO DEVICE DETECTED" message will be display on LCD.
- In case of firmware update, files should be kept in compressed format with named mts200_boot.tar. Make sure that final updated files are present in the mts200_boot.rar

	<p>INFORMATION</p> <ul style="list-style-type: none"> • Password of configuration through keypad and password of configuration through serial terminal are independent. • It is operator's responsibility to remember the configured password if it is changed from factory set password. • It is necessary to press OK key after changing any previous configuration through keypad, failing of which the particular parameter will restore to its previous setting.
---	---

Note:

1. If “MENU” key is pressed while configuring this parameter and before saving the new change of this parameter, user will be jumped to “ENTER PASSWORD” option again without saving new settings.

9.2 Console based configuration

masTER T-Sync Model MTS200 device can be configured remotely using Serial port, SSH, Telnet and webserver mode. However, the configuration through Serial port, SSH and telnet is done by running “start” utility after taking access of unit console command line interface.

Console based configuration means that user need to access the console of MTS200 which can be done through front serial console port or Telnet or SSH.

For configuration through Telnet or SSH, it is necessary to first configure the IP address of unit and connect the eth port of device in network.

- For serial port session with MTS200, connect front console port with DB-9 Male to female cross cable as explained in section 10 and follow below steps.
Set the communication software in remote PC system with 115200 (baudrate), 8 (data bits), none (parity), 1(stop bit).
After communication established, press enter in PC and then give below password if asked for,
password: MTS200LAMBDA

- For Telnet session with MTS200, following commands are to be entered in host system command terminal of unix/linux or windows based PC:

Command

1. telnet 192.168.100.153 on IPv4
2. telnet fe80::1eba:8cff:fee5:c115%**eth0** on IPv6 with Link local address
Here eth0 is the interface-id of your pc's interface-id. Use ifconfig command in your pc to determine interface identifier. If you are using wlan0 to take interface then write **wlan0** as an interface.
3. telnet fdc2:7142:77b7:0:1eba:8cff:fee5:c115

Here fdc2:7142:0:1eba:8cff:fee5:c115 is the Global IPv6 address of the MTS200. It can be viewe

user: root

password: MTS200LAMBDA

- For SSH session with MTS200, following commands are to be entered in host system or user system command terminal of unix/linux or windows based PC:

Command:

4. ssh root@192.168.100.153 on IPv4
5. ssh root@fe80::1eba:8cff:fee5:c115%**eth0** on IPv6 with Link local address
Here eth0 is the interface-id of your pc's interface-id. Use ifconfig command in your pc to determine interface identifier. If you are using wlan0 to take interface then write **wlan0** as an interface.
6. ssh root@fdc2:7142:77b7:0:1eba:8cff:fee5:c115

Here fdc2:7142:0:1eba:8cff:fee5:c115 is the Global IPv6 address of the MTS200. It can be viewed on LCD, Webserver, SNMP and on console based configuration utility.

user: root
password: MTS200LAMBDA

Note: Operator can also use “putty” software for windows based system for establishing telnet or ssh communication with MTS200 unit. Please refer section 10.1 for steps to use “putty” software for establishing telnet or ssh session.

After operator have entered the login of MTS200, then give below command to start the application program:

Command: /usr/sbin/start

And then press enter, start menu will be display as shown in below figure

```
*****
masTER T-Sync
*****

*****
Main Page
*****

GEN . General Settings.
NTP . NTP Settings.
SNMP . SNMP Settings.
ETH . Ethernet settings.
SEQ . Network Security Configurations.
D . Factory Default Settings.
ADM . Administration Settings.
E . Exit

*****

Enter command: █
```

Figure 9-3 Console based Program main menu layout

Above menu is the start menu of application code, which list out the entering code for different applicable modes such as “GEN” for General settings, “ETH” for device network settings etc. After entering any one of given mode and pressing “enter” will make device enter into that particular mode.

In all modes described in main menu image as per figure, user can check the current configurations using “View settings” option in respective modes and also user can change the current settings by using “configure settings” option in their respective modes. All parameters command number are obtained from left most column when “View settings” option is used.

Whenever operator do configuration, operator can save the set parameters using “0” command and then press “y” or “Y” (yes) when prompted for saving. Whenever user is in middle of configuration mode option and want to check the command options of other parameters of same mode, user can press “H” for help. This list out all command values of other parameters of same mode.



INFORMATION

- If no data is entered for more than 5 minutes timeout interval, console program “start” will be stopped automatically. After program being stopped, user need to again start the program by above mentioned command to configure device.
- The console based program “**start**” should be run only one at a time from any of the existing ssh or telnet session. If one SSH/TELNET session is already running “**start**” program from any configured device user, other session or other user cannot run the same program at same time.

9.2.1 General Settings:

```
*****  
          General Settings  
*****  
          1 . View General Settings.  
          2 . Configure General Settings.  
          B . Back  
  
*****  
  
          Enter command: █
```

In above menu for general settings, Option “1” list outs all the current settings of GPS general parameters and option “2” allows to individually configure all parameters and save them for permanent usage. Enter 1 or 2 option and then press “enter” key.

When option “1” is used, below figure resembles the output in this option.

```

General Settings
*****
1 . View General Settings.
2 . Configure General Settings.
B . Back
*****

Enter command: 1
PRESENT SETTINGS
-----
NO  COMMAND  MODE NAME  MEANING  Value(x)
-----
1   STx      Hour Mode  12 Hour Mode  = 1
2   SBx      Baud Rate  1200 Baud Rate  = 12
3   SPx      Parity      Parity NONE     = 0
4   SSx      Stop Bit    1 Stop Bit      = 1
5   SUx      Time Format  LOCAL time      = 2
6   TC1x     COM1 Tx Mode  GPRMC Mode     = 1
7   TC2x     COM2 Tx Mode  GPGGA Mode     = 4
8   Ex       Event Mode   Min. Mode       = 1
9   ET1      Addi. Event1 Second Mode     = 00060
10  ET2      Addi. Event2 Second Mode     = 00060
11  ET3      Addi. Event3 Second Mode     = 00060
12  ET4      Addi. Event4 Second Mode     = 00060
13  EW1      Event1 ON Time m.second Mode  = 0000050
14  EW2      Event2 ON Time m.second Mode  = 0000050
15  EW3      Event3 ON Time m.second Mode  = 0000050
16  EW4      Event4 ON Time m.second Mode  = 0000050
17  SPD      Prop. Delay  n.second Mode  = 000000
18  Z        Time zone    Hour:Minute     = +05:30
19  DST      DST Mode     ON/OFF          = 0
20  DSTZ     DST Offset   Hour:Minute     = +01:00
21  DSTS     DST Start    m.w.d           = 10.3.0
22  DSTST    DST Start Time hr:min         = 02:00
23  DSTET    DST End      m.w.d           = 04.1.0
24  DSTET    DST End Time hr:min         = 03:00
25  IRIGM    IRIG Mode    IEEE1344        = 2
26  IRIGT    IRIG Time    Local           = 2
-----
    
```

Option “2” will allow configuring all parameters mentioned in above figure, as shown in below image.

Example: Refer below steps to configure Hour Mode parameter,

Step 1: Enter Command number for Hour Mode as given in left most column in above figure, and then press “enter”.

Step 2: Now, enter the value of Hour mode when prompted for, as show in below image.

```

*****
General Settings
*****
1 . View General Settings.
2 . Configure General Settings.
B . Back
*****

Enter command: 2

!! Note: Enter '0' to return 'H' for Help !!
-> Enter command: 1

Note: Time Hour Mode (1=12 Hour/2=24 Hour).
-> Enter Hour Mode (1 / 2):█
    
```

Step 3: After value being given, device will again prompt asking for any other parameter to be changed in general settings. If there are other parameters to be modified, then proceed as per Step 1 and step 2.

Step 4: If there are no parameters to be modified, then enter “0” in “Enter command:” prompt. Thereafter it will ask to save modified parameters. Enter “y” or “Y” for yes and “n” or “N” for not saving them. Once saved, check the parameters update by using option “1” in general settings main menu.

```

*****
General Settings
*****
1 . View General Settings.
2 . Configure General Settings.
B . Back
*****

Enter command: 2

!! Note: Enter '0' to return 'H' for Help !!
-> Enter command: 1

Note: Time Hour Mode (1=12 Hour/2=24 Hour).
-> Enter Hour Mode (1 / 2):1

!! Note: Enter '0' to return 'H' for Help !!
-> Enter command: 0

-> Enter 'Y' to Save or any other character to restore:y█
  
```

9.2.2 NTP Settings:

Operator can modify NTP protocol related settings after selection “ntp” mode from main menu only. Give command “ntp” or “NTP” when prompted for in main menu. Please refer section 11.3 for detailed explanation of each NTP configurable parameter and complete MTS200 as ntp server functionality.

```

*****
NTP Main Page
*****
1 . Show NTP Configuration File.
2 . Configure NTP.
3 . View NTP Symmetric Keys.
4 . Edit NTP Symmetric Keys.
5 . Add Trusted Key.
6 . Delete Trusted Key.
7 . Restart NTP.
8 . NTP Output Status.
B . Back.

*****

Enter command: █
  
```

In above menu for ntp settings, below is the explanation of each option:

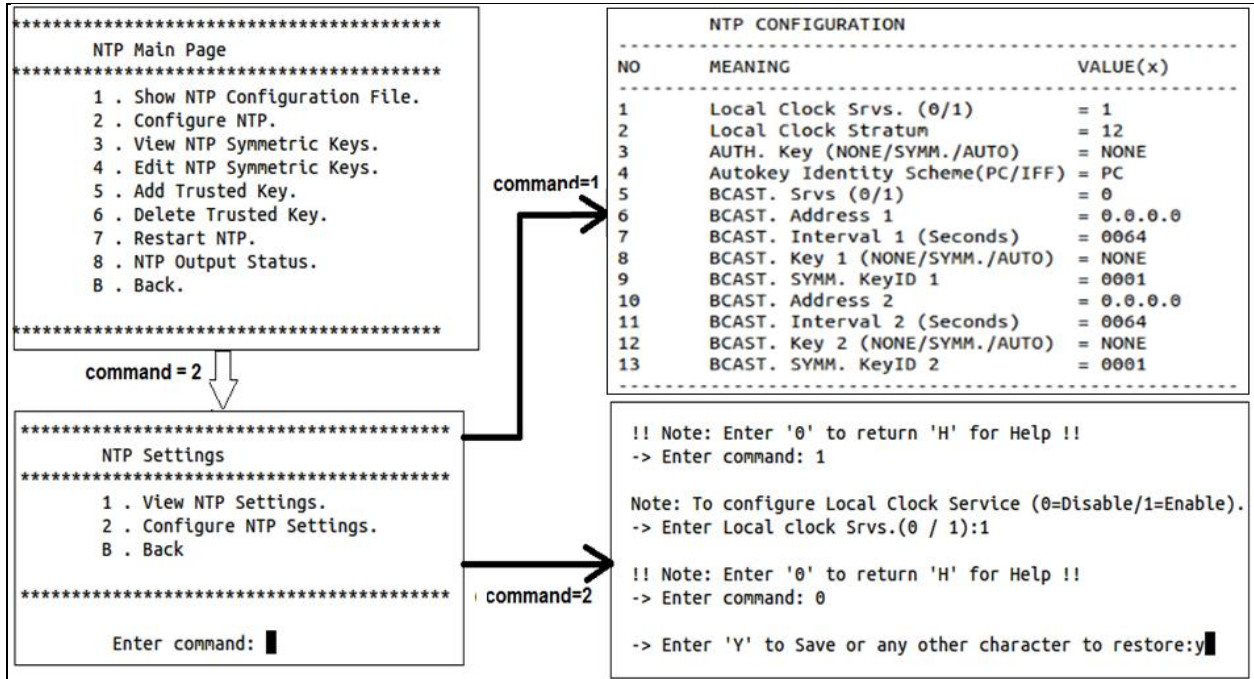
- 1 = Displays current ntp.conf file. This is main configuration file for ntp driver in device.
- 2 = This option is used to view and configure ntp setting options.
- 3 = To view ntp symmetric key file. This file is used for provide ntp symmetric key based authentication.
- 4 = To edit and add ntp symmetric key in the ntp.keys file. This file is used for provide ntp symmetric key based authentication.
- 5 = To add key id in ntp.conf file. NTP symmetric key may contain many number of key id and their password. This options gives user flexibility to use selected symmetric key id and add them to ntp configuration files.
- 6 = To delete trusted key id in ntp.conf file. This options gives user flexibility to delete selected symmetric key id and add them to ntp configuration files.
- 7 = this options restart the ntp service whenever any change to ntp settings or ntp authentication id id done by operator. If ntp service is not restarted, new changes done will not be effective till ntp service is restarted.

8 = To check MTS200 ntp driver output status. This provides ntp driver status equivalent to status generated by “ntpq -p” command in ntp client systems.

To configure basic NTP settings:

For configuring basic NTP settings, operator have to select option “2” in command and then press “enter” from NTP main menu page.

After giving above option, user have to select option “1” to view current NTP settings or option “2” to change current NTP settings. Please refer below figure for more details.




Command	Parameter	Applicable Value	Description
1	Local Clock Srvs.	0 / 1	Disable(0) or enable(1) local clock configuration
2	Local Clock Stratum	0 to 15	Stratum applicable during MTS200 unlock conditions
3	AUTH. Key	NONE/SYMM/AUTO	NTP authentication type for ntp service
4	Autokey Identity Scheme	PC / IFF	Authentication Identity scheme applicable for Autokey [AUTO] type authentication as per parameter 3
5	BCAST. Srvs.	0 / 1	Disable(0) or enable(1) ntp broadcast / multicast
6	BCAST. Address 1	xxx.xxx.xxx.xxx	NTP v4 broadcast/multicast address or v6 multicast address 1
7	BCAST. Interval 1	16/32/64/128/256/512/1024	NTP broadcast interval time in seconds for BCAST. Address 1
8	BCAST. Key. 1	NONE/SYMM/AUTO	NTP authentication type applicable for ntp broadcast. This can be NONE or has to be same as AUTH. Key

			parameter. It is for BCAST. Address 1
9	BCAST. SYMM. KeyID 1	1 to 9999	Broadcast key symmetric ID for Broadcast Symmetric key authentication type SYMM for BCAST. Address 1. This parameter is required only if parameter 3 and 7 are of type.
10	BCAST. Address 2	xxx.xxx.xxx.xxx	NTP v4 broadcast/multicast address or v6 multicast address 2
11	BCAST. Interval 2	16/32/64/128/ 256/512/1024	NTP broadcast interval time in seconds for BCAST. Address 2.
12	BCAST. Key. 2	NONE/SYMM/AUTO	NTP authentication type applicable for ntp broadcast. This can be NONE or has to be same as AUTH. Key parameter. It is for BCAST. Address 2.
13	BCAST. SYMM. KeyID 2	1 to 9999	Broadcast key symmetric ID for Broadcast Symmetric key authentication type for BCAST. Address 2. This parameter is required only if parameter 3 and 7 are of type SYMM.

After value being given, device will again prompt asking for any other parameter to be changed in NTP settings configuration menu. If there are no parameters to be modified, then enter “0” in “Enter command:” prompt. Thereafter it will ask to save modified parameters. Enter “y” or “Y” for yes and “n” or “N” for not saving them. Once saved, check the parameters update by using option “1” in general settings NTP main menu. Refer above figure.

For detailed understanding of each NTP parameter functioning, refer NTP operation section 11.3.

	<p>FUNCTIONALITY</p> <p>It is necessary to restart NTP service using option “7” in NTP main menu in order for new changes to take effect. Refer section 11.3 for complete understanding of NTP operation.</p>
---	--

To configure NTP Symmetric Key based Authentication

NTP Authentication between server and client can be provided using Symmetric key based authentication or Autokey based authentication using PC and IFF scheme. Detailed explanation of NTP authentication is provided in section 11.3.3.4.

MTS200 provides only NTP symmetric key based authentication configuration using SSH, Telnet, serial console port and webserver. However, NTP Autokey based authentication configuration is only provided using webserver access.

In order to configure NTP for symmetric key based authentication, it is necessary to configure key Id number and key string (which will be the key identification password) for authentication in ntp.keys file

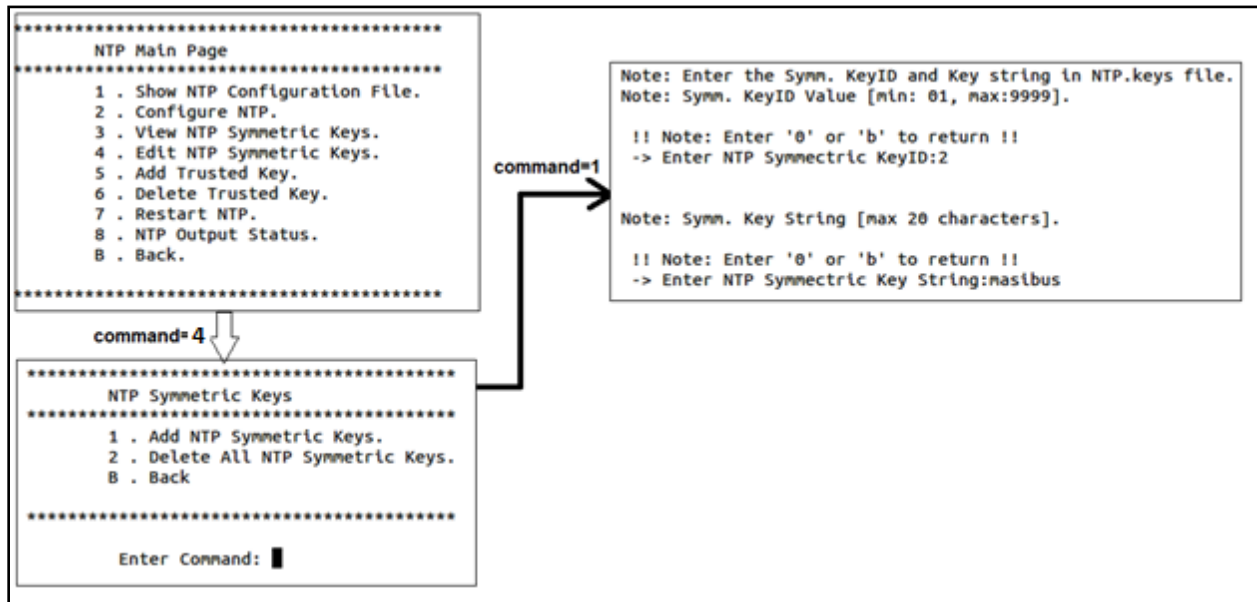
and then configure the added ntp key ID number as trusted key in ntp.conf file. Thereafter, when ntp process is restarted, ntp driver will read the updated keys and .conf file and provide the authentication based on authentication type configured in ntp.conf file.

Symmetric key id and string can be entered using the option “4” in NTP main menu. User can also view existing keys in ntp.keys file using option “3” in NTP main menu as shown in below figure.

```
*****
NTP Main Page
*****
1 . Show NTP Configuration File.
2 . Configure NTP.
3 . View NTP Symmetric Keys.
4 . Edit NTP Symmetric Keys.
5 . Add Trusted Key.
6 . Delete Trusted Key.
7 . Restart NTP.
8 . NTP Output Status.
B . Back.
*****

Enter command: 3
# ntp keys
1      M      masibus
```

In order to add new key string or replace any existing key in ntp.keys file, user should use option “4” in NTP main menu page and then option “1” as shown in below figure.



As shown above, after selection option “1” in “NTP Symmetric Key” menu, device will prompt for entering key ID number and then Key ID string. Key ID number should be between value 1 to 9999 and Key string should be max. 20 character’s only. If the user gives key ID number which is already existing in ntp.keys file, the previous key string will be changed according to new key string entered for that particular key ID number.

Model: MTS200 (1U)

Doc. Ref. no. : m08/om/201

Issue no. : 03

User can also delete all existing keys entry from ntp.keys file using option “2” in NTP Symmetric Keys menu. This will delete all keys but make a default entry of key id number with 2 and key string as “masibus”.

Note:

1. It is necessary to restart NTP service using option “7” in NTP main menu or using ntp restart options via front keypad or via webserver in order for new key changes to take effect. Refer section 11.3 for complete understanding of NTP operation.
2. Default key is provided from factory shipment with key ID number as “1” and key string as “masibus”. However, user can change the key string as per his requirement.

Option “5” and “6” in NTP main menu refers to add any key entry already present in ntp.keys file as trusted key in ntp.conf or to delete any key from ntp.conf as trusted key. NTP process will provide NTP authentication for keys only which are configured as trusted key provided in ntp.conf file.

Refer below for using option “5” to add a trusted key.

```
!! Note: Enter '0' or 'b' to return !!
-> Enter Trusted KeyID to Add:█
```

Remember, that the value to be entered as trusted key should be one of the keys configured as symmetric key number in ntp.keys file. User can configure only maximum 10 trusted key entries in ntp.conf file in MTS200. If user wants to view existing trustkey keys entry in ntp.conf, user can use option “1” in NTP main menu to view existing ntp.conf file.

Note:

1. It is necessary to restart NTP service using option “7” in NTP main menu or using ntp restart options via front keypad or via webserver in order for new key changes to take effect. Refer section 11.3 for complete understanding of NTP operation.

NTP Restart and status output:

User can restart NTP process at any time during MTS200 normal operation by using option “7” in NTP main menu. User should always restart NTP process using this option whenever there is any change in ntp configuration or any change in ntp trusted key entries or if any Symmetric key ID is replaced in ntp.keys file using “Edit NTP Symmetric Keys” option in NTP main menu. Unless NTP process is not restarted using this option, the changes done in ntp all configurations will not be in effective in NTP Server output.

User can also check NTP server ntp process status using option “8” in NTP main menu. Below figure shows the example output of NTP status output.

remote	refid	st	t	when	poll	reach	delay	offset	jitter
0127.127.30.0	.GPS.	0	l	15	16	377	0.000	0.000	0.002
192.168.100.255	.XFAC.	16	u	-	1024	0	0.000	0.000	0.002

NTP STATUS OUTPUT.

- **remote** = list of all ntp and time servers available as per defined in /etc/ntp.conf file.
- **refid** = reference name as per individual time servers
- **st** = current stratum value of the ntp server
- **when** = seconds since last ntp request
- **poll** = current applicable ntp query poll interval (in seconds) with respective ntp server as per defined in /etc/ntp.conf file.

- **reach** = The value displayed in column reach is octal, and it represents the reachability register. One digit in the range of 0 to 7 represents three bits. The initial value of that register is 0, and after every poll that register is shifted left by one position. If the corresponding time source sent a valid response, the rightmost bit is set.
During a normal startup the registers values increment in stages as per 0, 1, 3, 7, 17, 37, 77, 177, and 377.
- **delay** = this indicates the delay (In milliseconds) in ntp query and response
- **offset** = time difference (in milliseconds) between client and ntp server.
- **jitter** = variance of time offset (in milliseconds).

9.2.3 SNMP Settings:

MTS200 SNMP parameters required to configure MTS200 as SNMP agent can be configured via console based configuration utility through serial console port on front panel, Telnet, SSH mode as well as through Webserver mode.

In this section, method to configure MTS200 as SNMP agent for v1/v2 or v3 and steps to configure V3 authentication will be described via console based configuration utility.

To configure MTS200 as snmp agent, user need to enter SNMP mode from main menu in configuration utility as described below.

```
*****  
SNMP settings  
*****  
1 . View SNMP Parameters.  
2 . Configure SNMP Parameters.  
3 . Restart SNMP Service.  
B . Back.  
*****  
  
Enter command: █
```

After user enters in SNMP mode, Option “1” will display all current SNMP settings and Option “2” will allow user to configure SNMP parameters.

Refer below image for Option “1” in SNMP menu which represents list of all applicable SNMP agent parameters.

SNMP CONFIGURATION		
NO	MEANING	VALUE(x)
1	Manager1 IP Address	= 0.0.0.0
2	Manager1 Version	= 0
3	RO Community1 string (v1/v2c)	= public
4	RW Community1 string (v1/v2c)	= public
5	Manager1 Permission	= rw
6	Manager1 Trapenable	= 0
7	Manager1 Trapcommunity(v1/v2c)	= public
8	Manager1 v3 username	= username
9	Manager1 EngineId (v3)	= 0x123456789123456789
10	Manager1 Auth. Type (v3)	= NONE
11	Manager1 Auth. Passphrase	= public
12	Manager1 Priv. Type (v3)	= NONE
13	Manager1 Priv. Passphrase	= public
14	Manager2 IP Address	= 0.0.0.0
15	Manager2 Version	= 0
16	RO Community2 string (v1/v2c)	= public
17	RW Community2 string (v1/v2c)	= public
18	Manager2 Permission	= rw
19	Manager2 Trapenable	= 0
20	Manager2 Trapcommunity(v1/v2c)	= public
21	Manager2 v3 username	= username
22	Manager2 EngineId (v3)	= 0x123456789123456789
23	Manager2 Auth. Type (v3)	= NONE
24	Manager2 Auth. Passphrase	= public
25	Manager2 Priv. Type (v3)	= NONE
26	Manager2 Priv. Passphrase	= public
27	SNMP Contact	= masibus
28	SNMP Location	= gandhinagar

Option “2” in SNMP menu is for configuring each parameter. After pressing option “2”, user will be prompted for command value of each parameter shown in above figure. The command number of each parameter are mentioned in left most column of parameters list. User can do configuration of multiple values at a time by entering the command value of required parameter. User will remain in the configuration menu till user enters “0” in command prompt. User can use “H” for displaying list of all parameters in middle of configuration stage.

Once all required parameters are configured, operator can save the set parameters using “0” command and then press “y” or “Y” (yes) when prompted for saving. Whenever user is in middle of configuration mode option and want to check the command options of other parameters of same mode, user can press “H” for help.

Below table provide each parameter description for SNMP parameters.

Command	For SNMP Version	Parameter	Applicable Value	Description
1	v1 & v2c	Manager 1 IP address	Valid IPv4/IPv6 address	SNMP Manager1 v4/v6 IP address Default: 0.0.0.0
2	v1 & v2c	Manager 1 Version	0 / 1 / 2 /3	This should be set according to SNMP Version of Manager 1.

				“0” is special case to disable SNMP agent configuration for SNMP Manager1. Default: 0
3	v1 & v2c	RO Community String (v1 / v2c)	public	SNMP ro community name for Manager 1 Note: Min – 4 chars, Max – 30 chars. No special characters allowed Default: public
4	v1 & v2c	RW Community String (v1 / v2c)	public	SNMP rw community name for Manager 1 Note: Min – 4 chars, Max – 30 chars. No special characters allowed Default: public
5	v1, v2c, v3	Manager1 Permission	ro / rw	Read only or Read-write permission to SNMP Manager1 in MTS200. Default: ro
6	v1, v2c, v3	Manager1 Trapenable	0 / 1	SNMP trap status for Manager1. Default: 0
7	v1 & v2c	Manager1 Trapcommunity(v1/v2c)	public	Community string for SNMPv1/v2 if trap is enabled. Note: Min – 4 chars, Max – 30 chars. No special characters allowed Default: public
8	v3	Manager1 username v3	User defined string	SNMP v3 USM security name Note: Min – 4 chars, Max – 30 chars. No special characters allowed Default: username
9	v3	Manager1 Engineid (v3)	User defined value	SNMP v3 Manager engine ID. Note: Min – 4 chars, Max – 40 chars. No special characters allowed Must begin with 0x format Default:

				0x123456789123456789
10	v3	Manager1 Auth. Type (v3)	NONE / MD5 / SHA	SNMP v3 Authentication Technique Default: MD5
11	v3	Manager1 Auth. Passphrase	User defined password	SNMP v3 Authentication passphrase or password Note: Min – 4 chars, Max – 30 chars. No special characters allowed
12	v3	Manager1 Priv. Type (v3)	DES / AES	SNMP v3 Encryption Priv. Technique Default: DES
13	v3	Manager1 Priv. Passphrase	User defined password	SNMP v3 Encryption Priv. passphrase or password Note: Min – 4 chars, Max – 30 chars. No special characters allowed
14	v1 & v2c	Manager 2 IP address	Valid IPv4/IPv6 address	SNMP Manager2 v4/v6 IP address Default: 0.0.0.0
15	v1 & v2c	Manager 2 Version	0 / 1 / 2 / 3	This should be set according to SNMP Version of Manager 2. “0” is special case to disable SNMP agent configuration for SNMP Manager2. Default: 0
16	v1 & v2c	RO Community String (v1 / v2c)	public	SNMP ro community name for Manager 2 Note: Min – 4 chars, Max – 30 chars. No special characters allowed Default: public
17	v1 & v2c	RW Community String (v1 / v2c)	public	SNMP rw community name for Manager 2 Note: Min – 4 chars, Max – 30 chars. No special characters allowed Default: public
18	v1, v2c, v3	Manager2 Permission	ro / rw	Read only or Read-write permission to SNMP Manager2 in MTS200. Default: ro
19	v1, v2c,	Manager2 Trapenable	0 / 1	SNMP trap status for

	v3			Manager2. Default: 0
20	v1 & v2c	Manager2 Trapcommunity(v1/v2c)	public	Community string for SNMPv1/v2 if trap is enabled. Note: Min – 4 chars, Max – 30 chars. No special characters allowed Default: public
21	v3	Manager2 username v3	User defined string	SNMP v3 USM security name Note: Min – 4 chars, Max – 30 chars. No special characters allowed Default: v3username1
22	v3	Manager2 EngineId (v3)	User defined value	SNMP v3 Manager engine ID. Note: Min – 4 chars, Max – 40 chars. No special characters allowed Must begin with 0x format Default: 0x123456789123456789
23	v3	Manager2 Auth. Type (v3)	NONE / MD5 / SHA	SNMP v3 Authentication Technique Default: MD5
24	v3	Manager2 Auth. Passphrase	User defined password	SNMP v3 Authentication passphrase or password Note: Min – 4 chars, Max – 30 chars. No special characters allowed
25	v3	Manager2 Priv. Type (v3)	DES / AES	SNMP v3 Encryption Priv. Technique Default: DES
26	v3	Manager2 Priv. Passphrase	User defined password	SNMP v3 Encryption Priv. passphrase or password Note: Min – 4 chars, Max – 30 chars. No special characters allowed
27	-	SNMP Contact	User defined string	SNMP system contact information Note: Min – 4 chars, Max – 38

				chars. No special characters allowed except _ . , [] Default: masibus
28	-	SNMP Location	User defined string	SNMP system location information Note: Min – 4 chars, Max – 38 chars. No special characters allowed except _ . , [] Default: Gandhingar

After the SNMP Manager parameters are configured, it is necessary to restart the SNMP service using SNMP failing to which SNMP communication will be according to old or previous settings. SNMP service operation depends on snmpd.conf configuration file contents which are automatically created according to SNMP settings as per above table once SNMP service is restarted or started after being stop.

9.2.4 Ethernet Settings:

MTS200 Ethernet network parameters required to configure MTS200 eth0 and eth1 (optional) network IP parameters. This parameters need to setup whenever there is change in IP address of device eth0 or eth1 port or if any service in MTS200 is to be restarted. This mode is also used to configure syslog server address in MTS200.

User need to enter “ETH” or “eth” in main menu of console based configuration utility as shown in below figure.

```

*****
Main Page
*****
GEN . General Settings.
NTP . NTP Settings.
SNMP . SNMP Settings.
ETH . Ethernet settings.
SEQ . Network Security Configurations.
D . Factory Default Settings.
ADM . Administration Settings.
E . Exit

*****

Enter command: eth

*****
ETH0/1 Network settings
*****
1 . Current ETHx Settings.
2 . View ETHx Parameters.
3 . Configure ETHx Parameters.
4 . Restart Ethernet Services.
5 . View Log Messages.
B . Back

*****

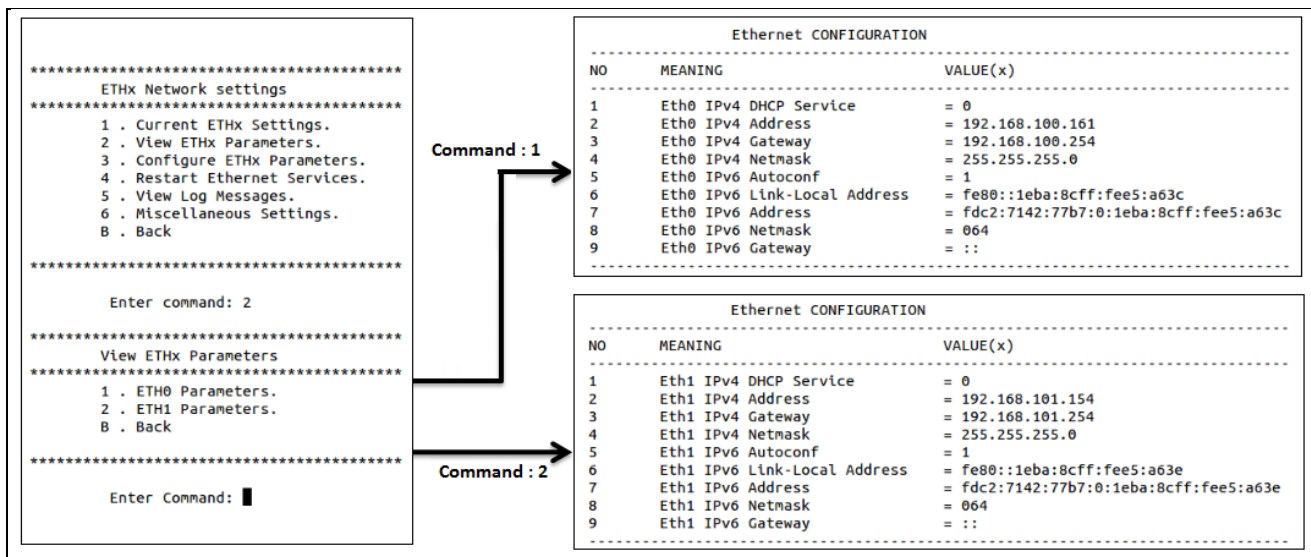
Enter command: █
  
```


Once user have entered in Ethernet menu “ETH0/1 Network Settings”, below is explanation of various options:

- 1 = To check current live network settings of Eth0 and Eth1. This are network settings which are alive in system. This mode is helpful mainly to check network settings when Ethernet port is in DHCP mode or in Autoconf mode or when user wants to check live system IP.
- 2 = To view current configured Ethernet settings
- 3 = To configure network parameters of eth0, eth1, syslog server address and enabling/disabling network services.
- 4 = This option is to restart all Ethernet services at a single option. This may be required when user have to restart all services at one go.
- 5 = To view internal logged messages in /var/log/messages file.
- B = to return to main menu.

To View configured network parameters of Eth0 and Eth1:

Option “2” in Ethernet main menu is used to view configured eth0, eth1 settings. In case of single Ethernet, user can view respected single Ethernet port parameters directly. For dual Ethernet, user need to give 1 or 2 command to view Ethernet port 0 or Ethernet port 1 parameter respectively as shown in below figure.



To configure network parameters:

Option “3” in Ethernet main menu is used to configure eth0, eth1 parameters as shown in below image.

After pressing option “3”, user will be prompted for command value of each parameter shown in above figure. The command number of each parameter are mentioned in left most column of parameters list. User can do configuration of multiple values at a time by entering the command value of required parameter. User will remain in the configuration menu till user enters “0” in command prompt. User can use “H” for displaying list of all parameters in middle of configuration stage.

Once all required parameters are configured, operator can save the set parameters using “0” command and then press “y” or “Y” (yes) when prompted for saving. Whenever user is in middle of configuration mode option and want to check the command options of other parameters of same mode, user can press “H” for help.

Note:

SSH and TELNET Communication will get disconnected and console application “start” code will **stop** whenever operator will change the Ethernet network settings parameters by using SAVE option using the start program.

So, it is necessary that user should again connect MTS200 by SSH or TELNET communication with the applicable IP address and start the console program “/usr/sbin/start” again.

Below table provide each parameter description for Ethernet0 network parameters.

Command	Parameter	Applicable Value	Description
1	Eth0 IPv4 DHCP Service	0 / 1	To enable DHCP on eth0 network. Configure this parameter will enable eth0 to acquire dynamic IPv4 address from DHCP server in network. This mode is mainly helpful whenever MTS200 is connected in network for first time before installation complete. If DHCP server is not present, configure this as “0”. Setting eth0 to DHCP will make static configuration of IPv4 eth0 network address meaningless. Default: 1
2	Eth0 IPv4 Address	xxx.xxx.xxx.xxx	This is v4 format IP address for eth0 port. Default: 0.0.0.0
3	Eth0 IPv4 Gateway	xxx.xxx.xxx.xxx	This is v4 format gateway address for eth0 port. Default: 0.0.0.0
4	Eth0 IPv4 Netmask	xxx.xxx.xxx.xxx	This is v4 format subnet mask address for eth0 port. Default: 255.255.255.0
5	Eth0 IPv6 Autoconf	0 / 1	To enable Autoconf on Eth0 network. Configure this parameter will enable eth0 to acquire IPv6 address from network. This mode is mainly helpful whenever MTS200 is connected in IPv6 network for first time. Setting eth0 to Autoconf will make static configuration of IPv6 eth0 network address unusable and will be replaced by automatically acquired IPv6 addresses. Default: 1
6	Eth0 IPv6 Link-Local Address	Non-configurable	Eth0 will have this address whenever IPv6 service is enabled and link for Eth0 is live. Default : ::
7	Eth0 IPv6 Address	Valid IPv6 address	This is v6 format IP address for eth0 port.

			Default: ::
8	Eth0 IPv6 Netmask	0 to 128	This is v6 format subnet mask address for eth0 port. Default: 0
9	Eth0 IPv6 Gateway	Valid IPv6 address	This is v6 format gateway address for eth0 port. Default: ::

Below table provide each parameter description for Ethernet1 network parameters.

Command	Parameter	Applicable Value	Description
1	Eth1 IPv4 DHCP Service	0 / 1	To enable DHCP on eth1 network. Configure this parameter will enable eth0 to acquire dynamic IPv4 address from DHCP server in network. This mode is mainly helpful whenever MTS200 is connected in network for first time before installation complete. If DHCP server is not present, configure this as "0". Setting eth0 to DHCP will make static configuration of IPv4 eth1 network address meaningless. Default: 1
2	Eth1 IPv4 Address	xxx.xxx.xxx.xxx	This is v4 format IP address for eth1 port. Default: 0.0.0.0
3	Eth1 IPv4 Gateway	xxx.xxx.xxx.xxx	This is v4 format gateway address for eth1 port. Default: 0.0.0.0
4	Eth1 IPv4 Netmask	xxx.xxx.xxx.xxx	This is v4 format subnet mask address for eth1 port. Default: 255.255.255.0
5	Eth1 IPv6 Autoconf	0 / 1	To enable Autoconf on Eth1 network. Configure this parameter will enable eth1 to acquire IPv6 address from network. This mode is mainly helpful whenever MTS200 is connected in IPv6 network for first time. Setting eth0 to Autoconf will make static configuration of IPv6 eth1 network address unusable and will be replaced by automatically acquired IPv6 addresses. Default: 1
6	Eth1 IPv6 Link-Local Address	Non-configurable	Eth1 will have this address whenever IPv6 service is enabled and link for Eth1 is live. Default : ::
7	Eth1 IPv6 Address	Valid IPv6 address	This is v6 format IP address for eth1 port. Default: ::

8	Eth1 IPv6 Netmask	0 to 128	This is v6 format subnet mask address for eth1 port. Default: 0
9	Eth1 IPv6 Gateway	Valid IPv6 address	This is v6 format gateway address for eth1 port. Default: ::

Below table provide each parameter description for Ethernet network Services.

Command	Parameter	Applicable Value	Description
1	Telnet Service	0 / 1	Disable(0) or enable(1) telnet service in MTS200. This change will make telnet service effective on both eth0 & eth1 port. Note: Service can be restarted only though Option “4” in Network main menu. Default: 1
2	HTTP Service	0 / 1	Disable(0) or enable(1) HTTP Webserver service in MTS200. This change will make HTTP service effective on both eth0 & eth1 port. At a time, either HTTP or HTTPS will be active. If HTTPS was set previously and user set HTTP enable, then HTTPS will automatically be disabled internally. Note: Service can be restarted only though Option “4” in Network main menu. Default: 1
3	HTTPS Service	0 / 1	Disable(0) or enable(1) HTTPS Webserver service in MTS200. This change will make HTTPS service effective on both eth0 & eth1 port. At a time, either HTTP or HTTPS will be active. If HTTP was set previously and user set HTTPS enable, then HTTP will automatically be disabled internally. Note: Service can be restarted only though Option “4” in Network main menu. Default: 0
4	SNMP Service	0 / 1	Disable(0) or enable(1) SNMP service in MTS200. This change will make SNMP service effective on both eth0 & eth1 port. Note: Service can be restarted only though Option “4” in Network main menu. Default: 0

5	IPv6 Service	0 / 1	Disable(0) or enable(1) IPv6 service in MTS200. This change will make IPv6 service effective on both eth0 & eth1 port. Note: Service can be restarted only though Option “4” in Network main menu. Default: 0
---	--------------	-------	---

Below table provide each parameter description for Ethernet network Miscellaneous parameters.

Command	Parameter	Applicable Value	Description
1	Syslog1 Address	Valid IPv4/IPv6 address	Syslog server1 v4/v6 format IP address. Default: 0.0.0.0
2	Syslog2 Address	Valid IPv4/IPv6 address	Syslog server1 v4/v6 format IP address. Default: 0.0.0.0
3	Bonding Enable	0 / 1	Disable(0) or enable(1) Bonding in MTS200. This change will make bonding applicable and configurations for bond0 are same as Eth0. Note: Configurable only for dual Ethernet MTS200. Default : 1

Option “5” is used to view MTS200 log messages. The device is cable to log the internal system messages, alarms in /var/log/messages file. New log is created on Power reboot of MTS200 and old records are deleted automatically on Power reboot. Also, MTS200 can store log messages of maximum 100Kbytes after which old logs will be deleted automatically.

If user wants the system to transmit log messages to remote syslog server on UDP layer, user need to configure the required Syslog1 and Syslog2 server address. This will cause syslog service is restart and thereafter, MTS200 will start transmitting all new messages in /var/log/messages and alarm to remote syslog servers and this messages will be stored in remote PC syslog message file automatically. For remote logging of syslog messages transmitted by MTS200, it is necessary that syslog configuration file on Server PC should be configured for accepting syslog frames over UDP layer and syslog service should be running on server PC.

Note:

1. If MTS200 is provided with only single Ethernet option, the other Ethernet port related parameters/configurations will be disabled and not accessible by operator.
2. As unit is shipped with DHCP settings on eth0 and eth1 port, user need to set static IP as DHCP IP on network may change on every Power ON/OFF of the device.
3. Eth1 port is any optional port to server different network in same industry. So, the domain of eth0 and eth1 should be separate.
4. Option “1” always displays live running all network settings of eth0 and eth1. However, gateway of any one of eth0 or eth1 is only displayed due to single entry in device IP routing table.
5. To make effect of change in any Ethernet port related parameter, user should press “y” or “Y” when start application asks to REBOOT device. Otherwise all parameters will be restored to last saved configuration settings.

9.2.5 Network Security Settings:

MTS200 provides secure communication to remote machines through SSH and HTTPS mode for its own status monitoring and configurations. However, SSH and HTTPS provide security layer through their respective security keys and certificates. MTS200 is shipped with default factory SSH v1 and SSH v2 keys as well as with self-signed HTTPS certificate. But, MTS200 also provided flexibility to user to generate their own SSH v1 and SSHv2 keys as well as HTTPS certificates through console based configuration utility and Webserver mode.

It is always recommended to generate security keys and certificates in MTS200 through secured means such as SSH and HTTPS. Other communication modes with MTS200 such as serial console, Telnet and HTTP are not secured and prone to network intruders.

Below is the explanation for methods to generate SSH and HTTPS security keys through SSH based console configuration utility application.

To go to security menu, user need to enter “SEQ” or “seq” in main menu of application utility as shown in below image.

```
*****
Main Page
*****
GEN . General Settings.
NTP . NTP Settings.
SNMP . SNMP Settings.
ETH . Ethernet settings.
SEQ . Network Security Configurations.
D . Factory Default Settings.
ADM . Administration Settings.
E . Exit

*****

Enter command: seq

*****
Network Security Configuration
*****
1 . SSH Settings.
2 . HTTPS Settings.
3 . NTP Autokey Settings.
B . Back

*****

Enter command: █
```

- 1 = To view and generate SSH related security keys
- 2 = To view and generate HTTPS related security certificate
- 3 = To view, generate, remove and update NTP autokeys

9.2.5.1 SSHv1/v2 Security Keys menu:

Option “1” in security main menu, user can select SSH security menu page. Below image shows the SSH menu page in security settings. This menu allows user to view existing SSH key details, to generate new SSH keys for verison1 and 2, view generated new SSH keys and option to save new generated keys. For more details regarding SSH v1 and v2 explanation, refer section 13.2.

```

*****
SSHv1/v2 Settings
*****
1 . View Current SSHv1/v2 Key.
2 . Generate SSHv1/v2 Key.
3 . View Generated SSHv1/v2 Key.
4 . Save SSHv1/v2 Key.
B . Back

*****

Enter command: █
    
```

Option “1” will show current existing SSH v1 and v2 keys present. This are keys which are currently used for SSH communication. This are different from option “3” as keys viewed using option “3” shows new generated keys which will only come in effect once saved. Below image shows the SSH key details.

```

SSHv1 Key Not Found.
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQCAwEhRkPshYm3h5CUC0haZYbC5/11z0KPkUOfpML0Zn5C50Vn4y5Zj/175Fok6grsLsdQovwonn7Lz8PTlFDE2cY3hZyvvRpe9bMDn8Pn
Q5aroAelvbchSerLYFnMfAy8kJfI2XRwLFFjJfT0HQV8I+eQ5CTrvNjNycN2tGKc0xT9NI2C78bnNy9hh8Gauxv8pWn5QZ698kocPrDo5xHwRe5qIfa5afG8shUSK58f1ArMUK193MjILv
rUCPrPS+/ixznI4eflgr0pPPBrhM+bcYsgntzGjv489J364PNJ0ae+v5YPvktSVrYVvaTHTnRQ9wMlGn/fyIqPX root@MTS200
SSHv2 [ssh_host_rsa_key] Key:
ssh-dss AAAAB3NzaC1kc3MAAACBANggSJK2o1+UftZp9A9PHS14c7aInjVyst7ZQ8E+bvQ2bT7gdXHYgaIQuZns+R1Fr7zqvdxRgxeWlkyL7KAT8ZDan5LyDj0gYns5h2n4w8d3z3n5o+
IEr/DeTh1QYqw1(+b2Jp0hupLPk9hw2PIJfTe+lsqhb1RLP0+7ZfwAAAAAQCMUNxJd+xyes2zt/UeTMSycZFwAAAIbCN4s1T+3sxP0TjV9NcNTLjJfL3Q4k71Q+cR284CShoe9r0d4
YFIN3Juk+nnuqXNcNT+r8MYBTa0v8hoalIoTVV4RU7dVqD1MkVBCsMBIsZbkpp2MPubKzCYwGNC3ndkLMunxV7hKYYU1ehTs/SQvZPX0VBfE54Dz7Dv6AEMgAAAIb0SM3by+Nv4+anJ
VbQanp7zyleUUAU2Vc4Kzxta0Pp0hyZAy00MHSa+H9CRT/fv1/4s3gwanrLOTlHgaM9qAdn8ZRprrk3xaun7L8h182feBy1JY3dLZ13srTA3wLthTW1XLlreTyr0qSonJL38rUL09A+0
EHZf7b4GK9= root@MTS200
SSHv2 Tssh host dsa key1 Key:
    
```

Option “2” is used to generate new keys for SSH v1 and SSHv2 keys. SSHv1 uses default RSA type private and public keys while SSH v2 uses RSA and DSA type private and public key for authentication purpose. DSA keys are of fixed 1024 bits based keys while RSA keys can of 768 or 1024 or 2048 bits to create keys. It is recommended to use 2048 bits RSA key sized because 2048 bits is considered more robust authentication key size for ssh communications.

For further details, refer section 13.2.

MTS200 is capable to generate DSA keys of 1024 bits as well as RSA keys with configurable bits size. When option “2” is selected, user is prompted to enter bits size to generate keys as shown in below figure.

Note: Enter bits required to generate rsa SSH key.Default is 2048.
 -> Enter total bits for RSA based SSH key(768 / 1024 / 2048):

After entering required bits, SSHv1 RSA and SSHV2 DSA and RSA keys are generated automatically. The new generated keys can be viewed by using option”3”. The new generated keys will only be effective when they are save using option “4” in SSH menu. This option will replace existing SSH keys with new generated SSH v1 and v2 keys automatically. However, new keys can be experienced a new SSH login with MTS200 as existing SSH login with MTS200 will continue till the existing SSH session is closed.

Note:

Model: MTS200 (1U)

Doc. Ref. no. : m08/om/201

Issue no. : 03

1. Whenever new SSH keys are generated and saved in MTS200, user need to remove old keys for MTS200 particular IP address at remote PC and then connection with MTS200 new keys can be established.

9.2.5.2 HTTPS Security Certificate menu:

Option “2” in security main menu, user can select HTTPS security menu page. Below image shows the HTTPS menu page in security settings. This menu allows user to view existing HTTPS certificate details, to generate new HTTPS certificate, view generated new HTTPS certificate and option to save new generated certificate. HTTPS security certificate in MTS200 are self-signed SSL security certificate of X509 type.

```
*****  
                HTTPS Settings  
*****  
    1 . View Current SSL Certificate Key.  
    2 . Generate SSL Certificate Key.  
    3 . View Generated SSL Certificate Key.  
    4 . Save SSL Certificate Key.  
    B . Back  
*****
```

Option “1” will show current existing HTTPS certificate present. This is security certificate which are currently used for HTTPS communication. This are different from option “3” as certificate viewed using option “3” shows new generated security certificate which will only come in effect once saved. Below image shows the HTTPS certificate details. Below image shows the truncated part of HTTPS SSL certificate.


```
Certificate:
Data:
  Version: 3 (0x2)
  Serial Number:
    bd:22:9e:39:6b:db:60:5f
  Signature Algorithm: sha1WithRSAEncryption
  Issuer: C=IN, ST=Gujarat, L=Gandhinagar,India, O=MAIPL, OU=Rnd, CN=www.masibus.com/emailAddress=support@masibus.com
  Validity
    Not Before: Jan 1 00:06:27 1970 GMT
    Not After : Dec 30 00:06:27 1979 GMT
  Subject: C=IN, ST=Gujarat, L=Gandhinagar,India, O=MAIPL, OU=Rnd, CN=www.masibus.com/emailAddress=support@masibus.com
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    Public-Key: (2048 bit)
    Modulus:
      00:c8:b3:8b:c7:39:68:e8:cb:b6:74:d3:b2:15:cc:
      1f:99:f6:13:6e:a5:76:28:6a:53:39:e9:f3:92:3a:
      91:a1:a2:ea:4b:d7:8a:4d:9b:d1:ff:e9:1d:60:26:
      de:cf:c7:a1:13:d0:86:6b:ba:62:47:be:8b:6d:45:
      6e:2b:cb:05:1e:53:82:84:e9:8b:cd:26:87:d9:42:
      00:79:8b:31:26:5a:e5:ce:1b:a9:1c:f6:f0:72:33:
      2f:6a:53:4c:b9:53:46:ba:89:1e:aa:dd:ca:f2:9f:
      41:a0:5e:c1:03:88:a2:8b:4b:8d:60:be:c8:bc:72:
      77:c1:fa:e9:12:fc:63:7e:3f:97:75:db:3d:d8:a0:
      bb:29:e8:6c:78:d5:85:fd:1b:92:8f:42:98:ef:e2:
      cc:9a:77:7b:d9:fd:37:f6:a8:7d:03:81:c4:f9:f0:
      9b:8d:2b:a5:a8:d1:4c:f7:5c:dd:25:f5:6a:2d:3f:
      23:aa:30:0d:63:12:99:9b:a3:51:50:08:63:7d:e4:
      8e:a1:e2:c8:1d:67:de:4c:65:36:86:9f:7b:fd:67:
      03:bc:09:38:e0:2b:26:6b:9d:13:e0:94:73:fa:42:
      0c:27:3e:bd:21:11:58:17:59:b0:93:25:3c:bb:b2:
      c7:c5:bf:39:57:a5:42:c3:ec:ab:a0:10:b2:3d:d1:
      03:45
    Exponent: 65537 (0x10001)
  X509v3 extensions:
    Netscape Cert Type:
      SSL Server
  Signature Algorithm: sha1WithRSAEncryption

  Signature Algorithm: sha1WithRSAEncryption
    70:a0:f3:c4:1b:4c:ec:b3:fa:e6:ef:04:b6:d8:98:9c:3b:
    9d:a5:1c:2b:3d:e8:9d:ca:fc:d3:43:27:8a:3a:c8:ea:2c:5a:
    1d:1b:88:82:fd:0f:d6:5b:88:2e:ec:99:07:8a:b4:fe:72:7a:
    e6:ba:ae:a6:48:87:93:0e:7c:65:dc:83:94:52:f6:6f:b4:b5:
    6a:df:0d:df:47:1b:7c:6a:85:f7:82:5f:f5:ab:16:c3:4c:fa:
    6b:44:19:f7:ac:ef:59:fc:4c:09:e8:f8:fa:83:57:ea:82:7a:
    4c:03:eb:24:55:c2:5c:89:36:04:d0:e5:3d:f9:24:77:47:a8:
    35:c7:0a:11:34:53:94:8e:98:de:91:d9:91:a9:27:1e:74:d1:
    f5:96:f1:80:0c:48:7e:71:30:be:0a:cd:c3:24:cd:a1:0d:e5:
    f5:3e:37:a6:5a:8c:39:e9:6d:5d:3c:13:ef:49:7c:a7:c6:23:
    b2:9d:86:12:41:a9:00:59:2c:9b:0a:28:71:cf:68:e8:c0:8b:
    86:ba:0d:66:fc:4e:46:5b:a4:21:6f:7d:46:f3:fa:62:62:9b:
    38:2d:34:b7:1f:ee:16:ad:93:93:fa:b2:6e:b2:6c:38:ae:15:
    fc:86:aa:2c:c0:fd:7f:71:07:a1:a0:49:76:d7:19:9a:60:a1:
    c5:2f:00:fa
  -----BEGIN PUBLIC KEY-----
  MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAYL0Lxzl06Mu2dN0yFcfw
  mFYTbqV2KGPtOenzkjqRoalQs9eKTzVr/+kdYCbz8ehE9CGa7p1R76LbUvUk8sF
  HLOCh0mLzSaH2UIAeYsxJlrlzhupHPbwcjMvaLNmuVNGuoqeqt3K8p9BoF7BA4ii
  i0uNYL7IvHJ3wfrpEvxjFj+Xdds92KC7KehseNWF/Rusj0KY7+LMnd72Fu39qh9
  A4HE+fCbJsuLqNFM91zdJfVqLT8jqjANYxKZm6NRUAhJjfeS0oeLIHWfETGU2hp97
  /WCDvAk44Csma50T4JRz+kIMJz69IRFYF1mwkyU8u7LHxb85V6VCw+yro8CyPdED
  RQIDAQAB
  -----END PUBLIC KEY-----
  -----BEGIN CERTIFICATE-----
  MIIDyDCCARcGAWIBAgIJAL0injlR22BFMA0GCSqGSIb3DQEBBQUAMIGXMQswCQYD
  VQGEWJTTjEQMA4GA1UECBMHR3VqYXJhdEaMBGGA1UEBxMRR2FuZGhpbmFnYXIs
  SW5kaWExdJAMBGNVBAoTBU1BSVBMMQwwCgYDVQQLLEwNSbmqxGDAWBgNVBAMTD3d3
  dy5tYXNpYnVzLmNvbTEiMCAgCSqGSIb3DQEJARYTc3VvcG9ydEBtYXNpYnVzLmNv
  bTAEfW03MDAxMDAwMDA2MjdaFw030TEyMzAwMDA2MjdaMIGXMQswCQYDVQGEWJTTj
  EQMA4GA1UECBMHR3VqYXJhdEaMBGGA1UEBxMRR2FuZGhpbmFnYXIsSW5kaWExdJ
  AMBGNVBAoTBU1BSVBMMQwwCgYDVQQLLEwNSbmqxGDAWBgNVBAMTD3d3dy5tYXNp
  YnVzLmNvbTEiMCAgCSqGSIb3DQEJARYTc3VvcG9ydEBtYXNpYnVzLmNvbTCCASIw
  DQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMiZi8c5a0jLtnTTshXMH5n2E26L
  dIhqZnp85I6kaGi6kvXik2b0f/pHWAm3s/HoRPQhmu6Yke+i21FbivLBR5TgoTp
  i80mh9lCAHnLMSZa5c4bqRz28HIzL2pTTLTRrQJHrdyVkfQaBewQ0IootLjWc+
  yLxYd8H66RL8Y34/L3XbPdIguynobhJvhf0bko9Cm0/izp3e9n1N/aofQ0BxPnw
  m40rpaJRTPdc3SX1ai0/I6owDWMsZuJUVAIY33kjHlyB1n3kxLNoafe/1nA7wJ
  00ArJmudE+CUC/pCDCC+vSERWbDz5JMlPLuyx8W/OveLQsPsq6AQsJ3RA0UCAwEA
  AaMVBMMwEQYJYIZIAyB4QgEBBAQDAgZAMA0GCSqGSIb3DQEBBQUAA4IBAQBwoPPE
```

Option “2” is used to generate new HTTPS SSL certificate. MTS200 is capable to generate user defined data based HTTPS certificate. When option “2” is selected, user is prompted to enter few details required for generating security certificate as shown in below figure.

Below Fields are required for generate SSL certificate.

Country Name [2 letter code].
 State or Province Name (full name). [min=2, max=20 characters].
 Locality Name (eg, city). [min=2, max=20 characters].
 Organization Name (eg, company). [min=2, max=25 characters].
 Organizational Unit Name (eg, section). [min=2, max=15 characters].
 Common Name (e.g. server FQDN or YOUR name) [min=2, max=25 characters].
 Email Address [max. 25 characters].

-> Enter Country Name [2 letter code]:

Below table represents the special characters details for parameters required to generate HTTPS Certificate.

Parameter Name	Value	Special Characters applicable
Country Name	Only characters allowed (a-z, A-Z).	No special characters allowed
State or Province Name	Characters (a-z, A-Z) and numeric (0 to 9) allowed.	Only “.” Allowed in special characters.
Locality Name	Characters (a-z, A-Z) and numeric (0 to 9) allowed.	Only “.” Allowed in special characters.
Organization Name	Characters (a-z, A-Z) and numeric (0 to 9) allowed.	Only “.”,“-” Allowed in special characters.
Organization Unit Name	Characters (a-z, A-Z) and numeric (0 to 9) allowed.	Only “.”,“-” Allowed in special characters.
Common Name	Characters (a-z, A-Z) and numeric (0 to 9) allowed.	Only “.”,“-”,“_”,“@” Allowed in special characters.
Email Address	Characters (a-z, A-Z) and numeric (0 to 9) allowed.	Only “.”,“-”,“_”,“@” Allowed in special characters.

After entering above data, security certificate generation process starts and take few seconds for generating certificate. During this, user should not stop the process in between and wait till certificate is generated. After new certificate is generated, user can use Option “3” to view the certificate contents and then option “4” to save the certificate.

After new certificate is saved, user need to restart HTTPS service from “Network Setting page”. User will be asked to accept new HTTPS SSL certificate in web browser software’s as previous downloaded certificate in web based browser will become invalid for this particular MTS200.

9.2.5.3 NTP Autokey menu:

For detailed description of NTP Autokey please refer section **11.3.3.4.2**

User can generate NTP Autokey for PC and IFF scheme based authentication files in MTS200 using webserver and using SSH. To generate keys, user need to take SSH of MTS200 and run the application code.

```

Enter command: seq
*****
Network Security Configuration
*****
1 . SSH Settings.
2 . HTTPS Settings.
3 . NTP Autokey Settings.
B . Back
*****
Enter command:
    
```

User need to enter 3 for NTP Autokey settings in console based configuration utility. Once user has entered in the NTP Autokey settings it will ask for the certificate type. Enter '1' for trusted server.

```

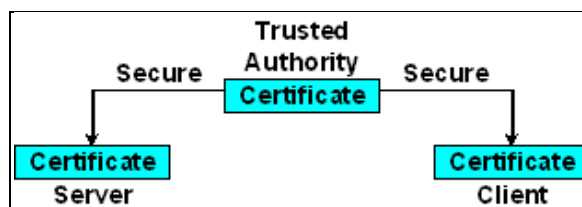
Enter command: 3
-> Enter Certificate Type (1 = Trusted Server / 0 = Server) : 1
*****
NTP Autokey Settings
*****
1 . Generate NTP Autokey.
2 . View NTP Autokey.
3 . Remove Old NTP Autokey.
4 . Update NTP Autokey.
B . Back
*****
    
```

In above menu below options are available.

- 1) Generate NTP Autokey – This option is used to generate NTP PC/IFF Auto key. User need to enter password and copy respected keys in the client.
- 2) View NTP Autokey: - This option is used to view generated NTP autokey either it is from PC or from IFF scheme.
- 3) Remove Old NTP Autokey:- This option is used to remove old generated key in the MTS200
- 4) Update NTP Autokey.

9.2.5.3.1 NTP Autokey PC Scheme:

The PC scheme uses a private certificate (X509.3 type certificate) generated by Trusted host as the group key and is distributed to all ntp group clients by secure means such as HTTPS or SCP. It is owner or operator responsibility to reveal this group key outside the ntp group. This scheme is cryptographically strong as long as the private certificate is kept secured. Refer below figure for further understanding of PC scheme.



Whenever a new private certificate is generated by Trusted host, it is necessary to distribute new key to all ntp clients for successful associations.

Model: MTS200 (1U)

Doc. Ref. no. : m08/om/201

Issue no. : 03

For detailed description please refer section 11.3.3.4.2.1

- Procedure to Generate NTP Autokey PC Scheme keys in MTS200:

User need to enter in the NTP Autokey configuration menu in the Security menu in the console based configuration utility. Select trusted server and PC scheme. In NTP Autokey PC scheme user need to enter password to generate private key and private certificate.

```

Enter command: 1

-> Enter Identity Scheme (PC/IFF) : pc

-> Enter Password (Only Digits/Letters) (Max. Length = 20) : masibus

-> Re-Enter Password : masibus
    
```

As soon as password entered in the it will start the process for generating autokey. User need to wait till the NTP autokey pc scheme private key and certificate get generated.

```

-> Enter Password (Only Digits/Letters) (Max. Length = 20) : masibus

-> Re-Enter Password : masibus

Please Wait...!!

Using OpenSSL version OpenSSL 1.0.2d 9 Jul 2015
Using host MTS200 group MTS200
Generating RSA keys (512 bits)...
RSA 0 0 1RSA 0 1 2RSA 0 2 3RSA 0 3 4RSA 0 4 5RSA 0 5 6RSA 0 6 7RSA 0 7 8RSA      1 0 1RSA      1 1 2RSA      1 2
3RSA      1 3 4RSA      1 4 5RSA      1 5 6RSA      1 6 7RSA      1 7 8RSA      1 8
9RSA      1 9 10RSA      1 10 11RSA      1 11 12RSA      3 0 1RSA 0 0 9RSA 0 1
10RSA      1 0 13RSA      1 1 14RSA      1 2 15RSA      1 3 16RSA      1 4 17RSA      1 5
18RSA      1 6 19RSA      1 7 20RSA      1 8 21RSA      1 9 22RSA      1 10 23RSA      1 11
24RSA      3 1 2

Generating new host file and link
ntpkey_host_MTS200->ntpkey_RSAhost_MTS200.3687833896
Using host key as sign key
Generating new certificate MTS200 RSA-MD5
X509v3 Basic Constraints: critical,CA:TRUE
X509v3 Key Usage: digitalSignature,keyCertSign
X509v3 Extended Key Usage: private
Generating new cert file and link
ntpkey_cert_MTS200->ntpkey_RSA-MD5cert_MTS200.3687833896
    
```

Keys generated in the PC scheme in MTS200 are as follows

PC Private Key: "ntpkey_host_MTS200

PC Private Certificate: "ntpkey_cert_MTS200"

Generated key and certificate can be viewed as explained. Select option 2 in the NTP Autokey settings options to view the generated NTP auto key.

```
Enter command: 2

-> Enter Key Type (1 = Private Key / 2 = Certificate / 3 = Group Key) : 1

# ntpkey_RSAAhost_MTS200.3687833896
# Fri Nov 11 06:18:16 2016

-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIBBozA9BgkqhkiG9w0BBQ0wMDABBgkqhkiG9w0BBQwwDgQImyEarm2m3EUCAggA
MBEGBSs0AwIHBAhYoJ4tfK0xYgSCAWCFyVtVmtMTYeA+omAH6aK4PHWAwHe0piI2
x+AkB03h9RPsSMz6WwatLurduWi4NEJqPtIqCzGW8qm54NbfEzWzG3R20NflttvM
L1W8clPxgKNUP/WZ7llqz5UAFKGGKWhdJ7j1NrP1dn5t6LBapMwAt2oLRVWuxTS5
AWE2++feK4qXMD62LSIpLXB3hbhLkZjRRbUVbpeiXWbdmPeUBeYBB9M4e8YDTQDK
TJMesCbosCiKjTciWlsQvapWGQadexbL0+A25Iywn+H68bCdw9IYVNejym2W63M4
DcJzaU0q+bJ8VuFFe/30eHAMARxRHaDYNQSCe6dMvbcowccci9hNCZeMtv5xtQZ
c1gDrXtpnrNJavLpP8ZZF84/80x/HtAprdV5ocMpc8EjFVY3XxvdmL4uuELY+9NK
D692Bk4wgwz4t4SZwpPXaw+FJJz0/HIhu9t3SEerC3mg5SXHCjFu
-----END ENCRYPTED PRIVATE KEY-----
```

```
Enter command: 2

-> Enter Key Type (1 = Private Key / 2 = Certificate / 3 = Group Key) : 2

# ntpkey_RSA-MD5cert_MTS200.3687833896
# Fri Nov 11 06:18:16 2016

-----BEGIN CERTIFICATE-----
MIIBRDCB76ADAgECAGTbz+EoMA0GCSqGSIb3DQEBAUAMBExDzANBgNVBAMMBk1U
UzIwMDAeFw0xNjExMTEwNjE4MTZaFw0xNzExMTEwNjE4MTZaMBExDzANBgNVBAMM
Bk1UuzIwMDBaMA0GCSqGSIb3DQEBAQUAA0kAMEYCCQDZNauBJHU7U0AmSjix6Xaf
xPPVoYACb0KnlhQB38orXjm7LtQ1LQ+Kwhkt/vLYenz7UeCtpKF9TOMGYMofRbxj
AgEDozEwLzAPBgNVHRMBAf8EBTADAQH/MASGA1UdDwQEAwIChDAPBgNVHSUECDAG
BgQrBgEEMA0GCSqGSIb3DQEBAUAA0EAJfMNUg91EBN1HYgvTaPqCTiHUEBFhLCO
DSfb6U0+7u4+AndyRT1Fj1TKQwHbDkBnnv84mvt34j7BZAHso0/00Q==
-----END CERTIFICATE-----
```

- Procedure to use NTP Autokey PC Scheme as ntp associations between MTS200 and ntp clients

Procedure for NTP associations between MTS200 and client is same as explained in the 11.3.3.4.2.1 section.

- Procedure to transfer Trusted server MTS200 keys in other MTS200 units

Step 1: To use NTP Auto key for MTS200 as server user need to go to the NTP Autokey settings menu in the security menu of the user based configuration utility. To generate PC scheme NTP Autokey user need to follow the same procedure as it is used for trusted server only change is user need to select Server for certificate type.

```
Enter command: 3

-> Enter Certificate Type (1 = Trusted Server / 0 = Server) : 0

*****
NTP Autokey Settings
*****
1 . Generate NTP Autokey.
2 . View NTP Autokey.
3 . Remove Old NTP Autokey.
4 . Update NTP Autokey.
B . Back

*****
```

Step 2: Enter the password used to generate the Trusted Server PC keys in password field. After entering password wait for some time. Now copy private key and certificates from trusted server.

```

Enter command: 1
-> Enter Identity Scheme (PC/IFF) : pc
-> Enter Password (Only Digits/Letters) (Max. Length = 20) : masibus
-> Re-Enter Password : masibus

Please Wait...!!

*****
Message :: Copy Private Key and Certificate from Trusted Server.
*****
  
```

Step 3: To transfer NTP key from trusted server to server please follow 11.3.3.4.2.1.

Step 4: After the NTP auto key is transferred from trusted server to server again go to the NTP autokey settings menu in the security menu of console based configuration utility. Now select option 4 to update NTP autokey. If NTP auto key is successfully updated message will be there as shown below.

```

*****
NTP Autokey Settings
*****
 1 . Generate NTP Autokey.
 2 . View NTP Autokey.
 3 . Remove Old NTP Autokey.
 4 . Update NTP Autokey.
 B . Back

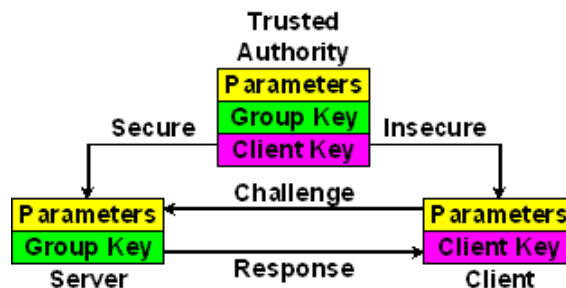
*****

Enter command: 4
-> Enter Identity Scheme (PC/IFF) : pc

Message :: Updating... Please Wait
  
```

9.2.5.3.2 NTP Autokey IFF Scheme:

In IFF scheme, there is Trusted Authority (TA) which generated the IFF parameters, private key and public key for IFF based ntp network. User can make MTS200 as TA by using Trusted Server option in webserver and console based configuration utility and selecting IFF scheme in webserver security page or any one of multiple MTS200 connected in a single network as TA.



For detailed description please refer 11.3.3.4.2.2

- Procedure to Generate NTP Autokey IFF Scheme keys in MTS200 which will act as Trusted Authority in NTP network:

User can generate Autokey for PC and IFF scheme in MTS200 using webserver and console based configuration utility. To generate PC schemes keys, user need to go NTP Autokey settings in the Security menu of the console based configuration utility.

Step 1: User need to select trusted server as a certificate type and select IFF option in the identify scheme. Now procedure will be same as it is done in the NTP Auto key PC Scheme.

```

Enter command: 1

-> Enter Identity Scheme (PC/IFF) : iff

-> Enter Password (Only Digits/Letters) (Max. Length = 20) : masibus

-> Re-Enter Password : masibus

Please Wait...!!

Using OpenSSL version OpenSSL 1.0.2d 9 Jul 2015
Using host MTS200 group MTS200
Generating RSA keys (512 bits)...
RSA 0 10 14 1 11 24 3 1 2
Generating new host file and link
ntpkey_host_MTS200->ntpkey_RSAAhost_MTS200.3687849566
Using host key as sign key
Generating IFF keys (256 bits)...
IFF 0 379 408 1 49 167 2 1 2 3 1 4
Confirm g^(q - b) g^b = 1 mod p: yes
Confirm g^k = g^(k + b r) g^(q - b) r: yes
Generating new iffkey file and link
ntpkey_iffkey_MTS200->ntpkey_IFFkey_MTS200.3687849566
Generating new certificate MTS200 RSA-MD5
X509v3 Basic Constraints: critical,CA:TRUE
X509v3 Key Usage: digitalSignature,keyCertSign
X509v3 Extended Key Usage: trustRoot
Generating new cert file and link
ntpkey_cert_MTS200->ntpkey_RSA-MD5cert_MTS200.3687849566
    
```

Step 2: After required keys are generated, user can check the key contents using “VIEW” option and selecting key type in field “Contents of” as shown in below images. Same as Private key user can view certificate as well as Group key.

```

*****
NTP Autokey Settings
*****
1 . Generate NTP Autokey.
2 . View NTP Autokey.
3 . Remove Old NTP Autokey.
4 . Update NTP Autokey.
B . Back

*****

Enter command: 2

-> Enter Key Type (1 = Private Key / 2 = Certificate / 3 = Group Key) : 1

# ntpkey_RSAAhost_MTS200.3687849566
# Fri Nov 11 10:39:26 2016

-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIBmZA9BqkqhkiG9w0BBQ0wMDABBgkqhkiG9w0BBQwwDgQIWP3A/23TLP4CAgga
MBEGBS0AwIHBAj2UJvktNPNswSCAVioU034Vji8NLir8dC++BpGL4uU+f5KKKeS
j+qK3P+s6UFSK41DIIfIq6dG08GbwFZUo4zT6C60ExmPLwvZUFhKwYXRktPrTrl8
bZhtAutExF+Xh5FE8HXjPpLCH7jIAIF2ExKL2Y7kIA2uUft8VSw2T+zUIgCC/vHK
Lm0DuDCT5EqcVcIqZPLM5ZinbXkp/Yz7B9Q5sc+zdPnvezag1KMQIrUFMP64m32I
/urtzSjl0a4ZDfHZwf1Lks6/hK3I9/B+/w2CoPGn/AZoB3R5LvcRq9JfJb5nGqpt
IFB013emL6TGwZ9hXXDkGPT/ruyo8EDWYnGnwI7bkMdJMjsstRbo4CG7CwKtHX4i
DbtmJMprRtBILSbHaYtLEaYWHJ1T9e2yutViM83YRiJrWFmt+v4p+4ZeiY8D005
N4HS696a7KN9tdrBD+4L4CgikbDTI+/xwLS0esKEVQ==
-----END ENCRYPTED PRIVATE KEY-----
    
```

The keys generated in PC scheme in MTS200 are as follows:

IFF Parameter key: "ntpkey_iffkey_MTS200"
IFF Private Key: "ntpkey_host_MTS200"
IFF Private Certificate: "ntpkey_cert_MTS200"

- Procedure to use IFF scheme as ntp associations between MTS200 trusted authority and ntp clients:

Step 1: Procedure to use IFF scheme between MTS200 trusted authority and ntp client is same as explained in the 11.3.3.4.2.2.

- Procedure to transfer Trusted Authority MTS200 IFF key in other MTS200 units:

There will be only one MTS200 device in complete NTP group network which will act as Trusted Authority with trusted server functionality. Other MTS200 units in same NTP network will only be acting as trusted server mode.

Step 1: To use NTP Auto key for MTS200 as server user need to go to the NTP Autokey settings menu in the security menu of the user based configuration utility. To generate IFF scheme NTP Autokey user need to follow the same procedure as it is used for trusted server only change is user need to select Server type for certificate type.

```
Enter command: 3
-> Enter Certificate Type (1 = Trusted Server / 0 = Server) : 0
*****
NTP Autokey Settings
*****
1 . Generate NTP Autokey.
2 . View NTP Autokey.
3 . Remove Old NTP Autokey.
4 . Update NTP Autokey.
B . Back
*****
```

Step 2: Before generating new key remove the old keys. Now select the IFF scheme as Identify scheme and enter the password. Password can be different from the MTS200 trusted server password and generate key and certificate.

```
ubuntu:~
NTP Autokey Settings
*****
1 . Generate NTP Autokey.
2 . View NTP Autokey.
3 . Remove Old NTP Autokey.
4 . Update NTP Autokey.
B . Back
*****
Enter command: 1
-> Enter Identity Scheme (PC/IFF) : iff
-> Enter Password (Only Digits/Letters) (Max. Length = 20) : masibus
-> Re-Enter Password : masibus
```



```
-> Re-Enter Password : masibus

Please Wait...!!

Using OpenSSL version OpenSSL 1.0.2d 9 Jul 2015
Using host MTS200 group MTS200
Generating RSA keys (512 bits)...
RSA 0 3 14      1 11 24                      3 1 2
Generating new host file and link
ntpkey_host_MTS200->ntpkey_RSАhost_MTS200.3687858494
Using host key as sign key
Generating new certificate MTS200 RSA-MD5
X509v3 Basic Constraints: critical,CA:TRUE
X509v3 Key Usage: digitalSignature,keyCertSign
X509v3 Extended Key Usage: trustRoot
Generating new cert file and link
ntpkey_cert_MTS200->ntpkey_RSA-MD5cert_MTS200.3687858494

*****
Message :: Copy Group Key from Trusted Server.
*****

*****
NTP Autokey Settings
*****
```

Step 3: Transfer NTP IFF group key from trusted server to server please follow 11.3.3.4.2.2.

Step 4: After the NTP auto key is transferred from trusted server to server again go to the NTP autokey settings menu in the security menu of console based configuration utility. Now select option 4 to update NTP autokey.

9.2.6 Default / Restore Settings:

MTS200 settings related to General settings, NTP settings, SNMP Settings and Ethernet network settings can be resetting to factory default and/or restore using “D” or “d” command in console based configuration utility. User can restore last settings if user has done factory default and want to revert to settings which were before doing default.

MTS200 settings which can be done to factory default or restore is shown in below image.

```
*****
Main Page
*****
GEN . General Settings.
NTP . NTP Settings.
SNMP . SNMP Settings.
ETH . Ethernet settings.
SEQ . Network Security Configurations.
D . Factory Default Settings.
ADM . Administration Settings.
E . Exit

*****

Enter command: d

*****
Factory Default Settings
*****
1 . General Settings.
2 . NTP Settings.
3 . SNMP Settings.
4 . Ethernet Settings.
B . Back

*****

Enter command: █
```

Options explained in above figure, below are explanation:

- 1** = to configure General settings as explained in section 9.2.1 to factory default or restore before default settings.
- 2** = to configure NTP settings as explained in section 9.2.2 to factory default or restore before default settings.
- 3** = to configure SNMP manager related settings as explained in section 9.2.3 to factory default or restore before default settings.
- 4** = to configure Ethernet network eth0 and eth1 settings as explained in section 9.2.4 to factory default or restore before default settings.
- B** = to return to previous menu.

If user wants to change general setting to factory default, user should give “1” in command and then press ENTER. This will lead to below figure type index which will have options for factory default or restore. Refer below image.

```
*****  
Settings  
*****  
1 . Factory Default.  
2 . Restore bkp.  
3 . View Current Settings.  
*****  
!! Note: Enter '0' to return 'H' for Help !!  
-> Enter command: █
```

Option “1” will default General setting to factory default. If user wants to revert to settings which were before default being done, user can use Option “2” to restore the settings. Option “3” will let user view the current settings of General parameters which will be applicable.

Same method is applicable for other settings for NTP, SNMP and Ethernet. By doing default settings of Ethernet Network, all network settings of eth0 and eth1 will go to default. Due to this other clients connected with MTS200 Ethernet communication will break due to change in network addresses of eth0 and eth1.

Whenever user change the settings of NTP and SNMP, it is necessary for user to restart the respective service for “Ethernet Settings” option in main menu for new changes to take effect.

9.2.7 Administration Settings Menu:

```
*****  
Administration settings  
*****  
1 . View Process List.  
2 . View Device Version.  
3 . Reboot Device.  
4 . User Management.  
B . Back  
*****  
Enter Command: █
```

Option “1” in above menu is for Process list and it shows the current process running in MTS200 device.

Option “2” shows Device Version which give details about the MTS200 version information.

Option “3” “Reboot Device” option can be used to reboot the device through webserver. While this option will cause reboot, all outputs of MTS200 will be halted till the units get started again. All log messages will be cleared and all Ethernet services will be restarted again.

Option “4” “User Management” option can create/modify/delete system username as explained below.

```
*****
User Management
*****
 1 . View Current Users.
 2 . Add New User.
 3 . Change Password.
 4 . Delete User.
 B . Back

*****

Enter Command: █
```

Multiple Users can be created for MTS200 device with categories as Super-User, Administrator and Info. Maximum 10 username are allowed within system including “root” user. “root” is default super-user of MTS200 device which cannot be deleted or its username or password modified.

Users created through webserver or console based configuration program are applicable only for webserver login and SSH, Telnet and serial console session. The users created through webserver or console based program are different from front panel keypad password access.

New Users can be created or deleted only by Super-user and administrator type of users. Info user login to webpage can neither create user nor delete any user.

Super-user have all read-write access for system configuration, have rights to start/stop restart any system through webserver or console based program and even can check the ntp status data on webserver or console based program.

Administrator also have all read-write access for system configuration, have rights to start/stop restart any system through webserver or console based program and even can check the ntp status data on webserver or console based program. But, Administrator do not have access to console of MTS200 through SSH or Telnet or serial mode. If Administrator tries to have SSH, Telnet or serial session with MTS200, console based configuration utility “start” program will run automatically and session will expire or close on exit of the program.

Info User can only view configuration status but cannot modify device configuration and also cannot make any changes to system services status. Info user also does not have access to ntp service status.

Option “1” will show details and list of current existing system users as show below.

No.	Username	Group Membership
0	root	Super-User
1	masibus	Super-User
2	user3	Info-User

Option “2” will create new system user as shown below.

```
NOTE :: Only a-z,0-9 and '_'
-> Enter Username [min=1, max=20 characters]:
-> Enter Password [min=1, max=20 characters]:
-> Enter Group Membership (1=Super-User/2=Administrator/3=Info-User):█
```

Option “4” can delete existing user as shown below. “root” user cannot be modified or deleted.

```
NOTE :: Make sure before ENTER. User will be permanently deleted.
-> Enter Username [min=1, max=20 characters]:█
```

Default factory settings for user are below:

Username: root
Password: MTS200LAMBDA

9.3 SNMP based configuration

masTER T-Sync Model MTS200 support SNMP v1/v2c/v3 protocol for its monitoring and configuration with SNMP Manager. This device act as SNMP agent and can support upto two SNMP Manager with independent SNMP versions. Refer section 13.3 for complete explanation of device configuration through SNMP protocol.

9.4 Webserver based configuration

For MTS200 configuration through webserver using HTTP or HTTPS protocol, refer section 13.4 for detailed explanation.

10 Serial Communication and Configuration

masTER T-Sync Model MTS200 device has console terminal at front panel of instrument which is female DB-9 connector operating on RS-232 electrical standards. This terminal can be used to configure device parameters when console terminal of device is connected to RS-232 terminal of computer using 9 pin CROSS Cable (refer below section for cable connections)

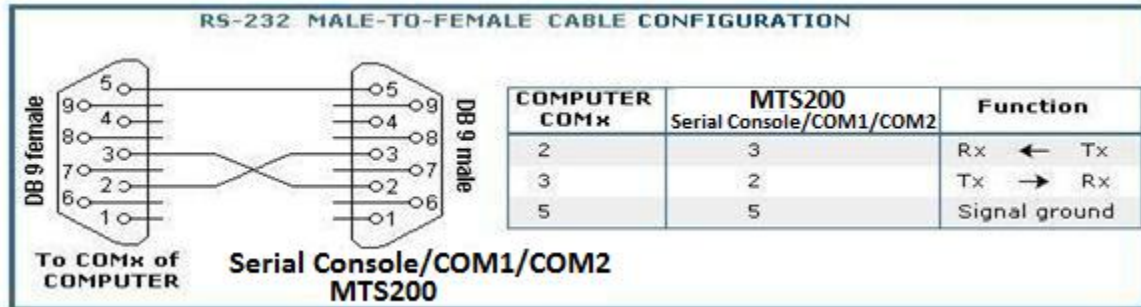


Figure 10-1 COM2/Serial Console terminal Cable Connections

Connect one end of the cross cable to the serial console terminal of device and other end to an available serial port on your local computer. (If there is no RS-232 terminal in user’s computer, user can use USB-To-Serial convertor. Masibus do not provide USB-To-Serial convertor as part of accessories supplied with masTER T-Sync Model MTS200 device).

It is recommended to use **putty.exe** for communicating with MTS200 through front serial console port or SSH or Telnet medium from windows based PC or Server. Putty.exe can be downloaded from <http://www.putty.org/> website. It is free and reliable software.

In windows based PC, hyperterminal can also be used but user may encounter problems of limited hyperterminal screen size when list of any mode is larger than provided screen size. This problem will not be faced through putty software.

10.1 Steps to Set Putty for serial communication with MTS200:

1. Run putty.exe file. Below image will appear when putty software is started.

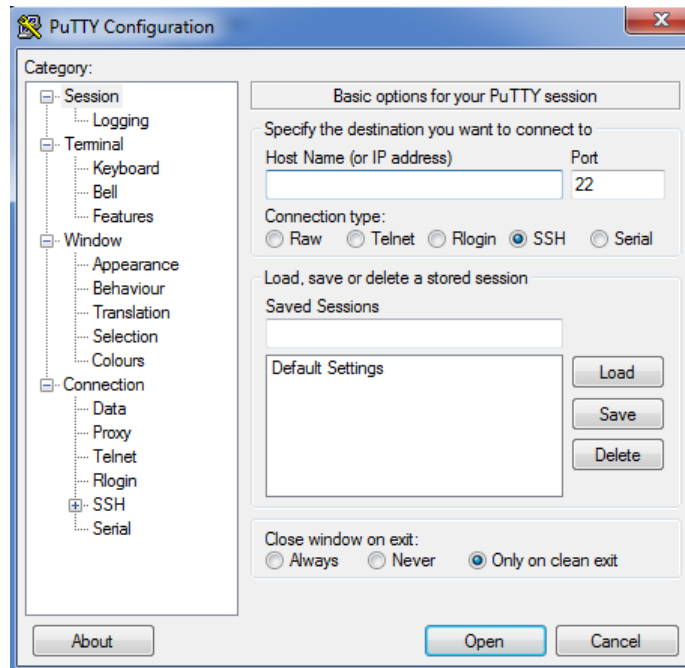
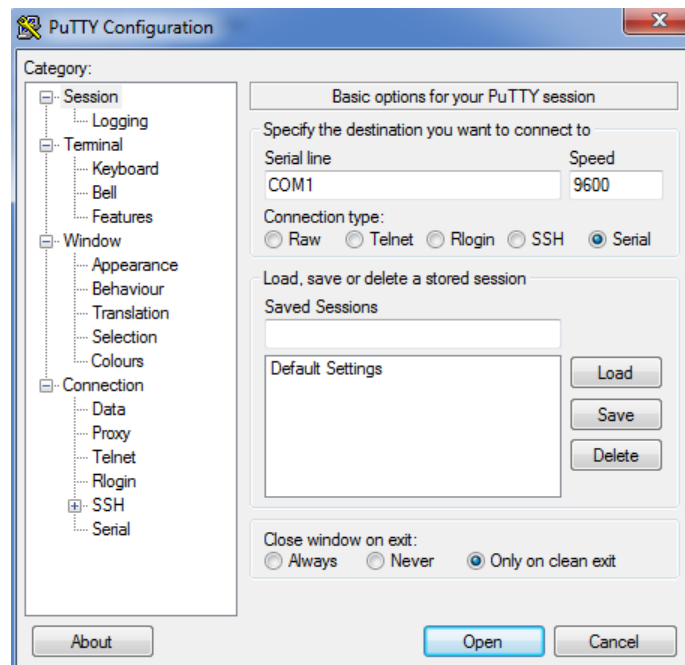


Figure 10-2 Putty Software

2. User need to select “Serial” in field “Connection type” as shown in below image.



- Now, user need to enter comport number e.g. COM22 in field “Serial line” and baudrate 115200 in field “Speed”. Then click on “Open” which will establish serial communication with MTS200 device as shown in below figures. After serial communication screen appears, user need to press ENTER, which will shown login menu of MTS200 device.

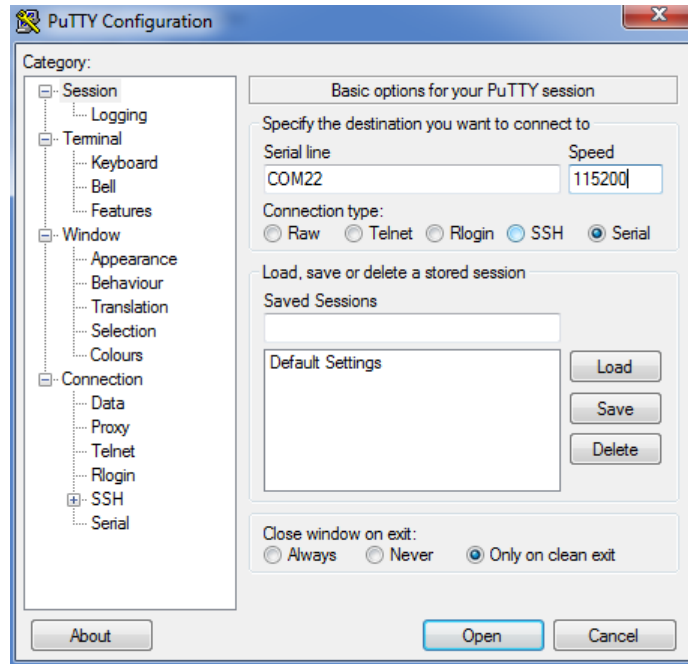
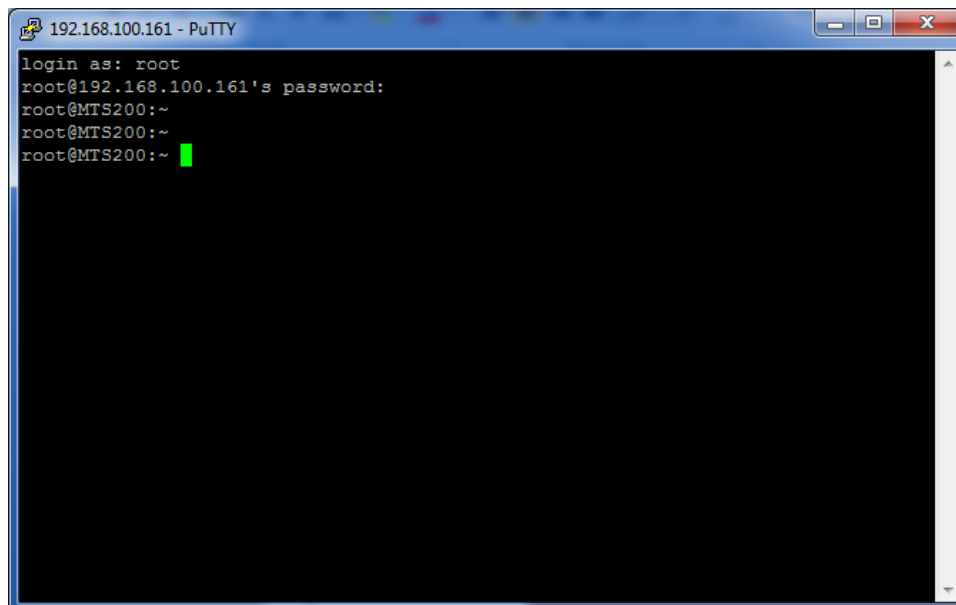


Figure 10-3 PuTTY (serial) Settings for console port



- Now, user should login with password and run the configuration utility program command: **/usr/sbin/start**. If user is already logged in the device, then user need to only run the command for configuration utility program.

10.2 Steps to Set Hyperterminal for serial communication with MTS200:

Configuration requires a standard 9-way D-type RS-232 cable and standard serial communication software in the PC, such as **HyperTerminal**.



Figure 10-4 Path of HyperTerminal

Open the **HyperTerminal** and start **new connection** on **COMx** of your PC. (x can be any available serial RS232 port number) as shown in below figure. User can enter any name in "NAME" option.

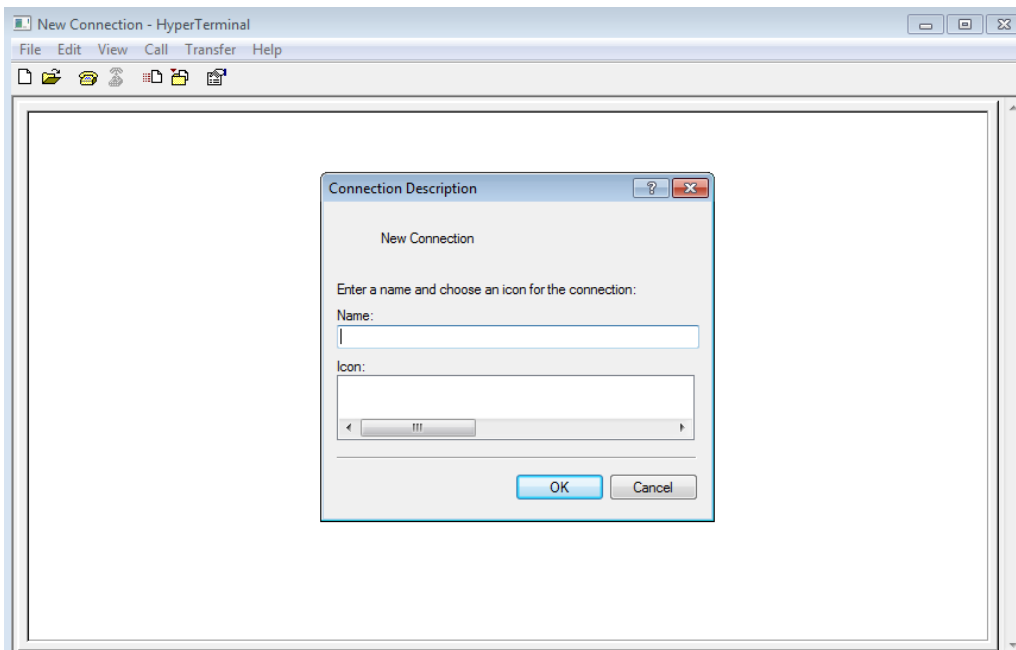



Figure 10-5 HyperTerminal View

In using **HyperTerminal**, it is recommended to select **File\Properties\Settings** and set **Emulation to ANSI**, to avoid auto-detect making unwanted changes to the settings.

	<p>INFORMATION</p> <ul style="list-style-type: none">• Cross cable connection as mentioned in above figure is necessary to communicate with COM2 terminal.• It is recommended to use putty instead of hyperterminal because of limited visible screen size in hyperterminal.• Ensure serial console port communication setting done in <i>masTER T-Sync Model MTS200</i> unit and end device should be same for proper communication.
---	--

The port settings in **HyperTerminal** and the serial console port of unit must match each other for fruitful communication. The factory set settings of serial console of unit are set 115200(baud rate), 8 (data bits), N(Parity-None),2 (stop bit) and may be checked by observing the LCD on boot up.

It is necessary that user have to select "NONE" option in "Hardware Flow Control" option while doing communication parameters settings in HyperTerminal. User can check unit serial console communication settings from Keypad Menu available on front panel of unit.

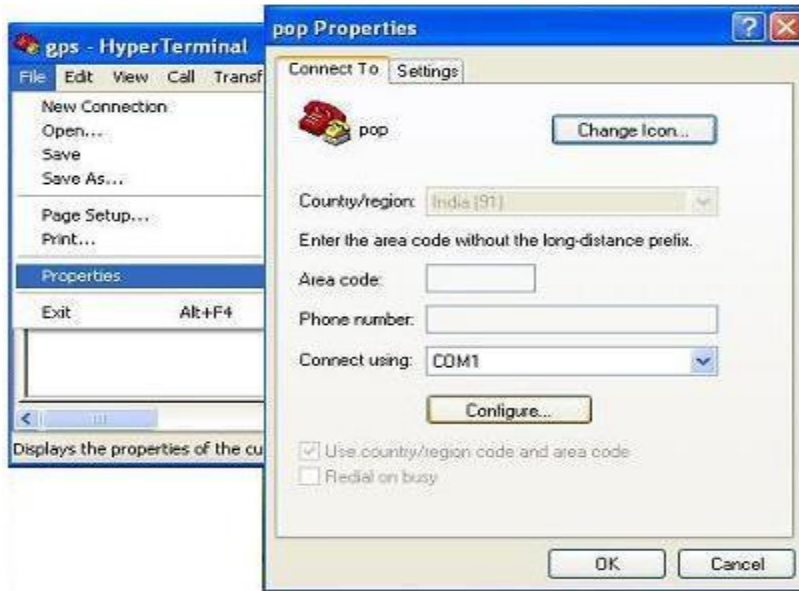


Figure 10-6 HyperTerminal Configuration

After connection is setup successfully, user will get prompt of log in menu of MTS200 unit or may be directly to console prompt, if user have already login previously in MTS200 through serial or telnet or ssh.

Refer section 9.2 in manual for device configuration through console based utility application program.



INFORMATION


User should log out when the configuration through serial console utility is finished by pressing key on PC keyboard Ctrl + d. This command will log out the console and prevent unauthorized access to MTS200 system. This is important because changes done in system files due to unauthorized access can create unexpected performance of device for which user is solely responsible for the consequences.

11 Timing Outputs – Serial, IRIG-B / IEEE 1344, NTP

11.1 Timing Output – Serial

11.1.1 NMEA-0183 RMC Time frame output


masTER T-Sync Model MTS200 transmits NMEA time frame from COM1 terminal at rear panel of unit at every 1 second at 9600 (baud rate), 8 (Data bits), N (NONE parity), 1 (1 stop bit). The NMEA-0183 \$GPRMC serial time string contains time and date of position fix, speed and course information.

	<p>INFORMATION</p> <p>The serial communication settings of COM1 terminal including type of frame, baud rate, parity and stop bit are fixed and cannot be changed.</p>
---	--

The full data message of this format shall consist of data fields as follows:

Field	Example	Comments
String ID	\$GPRMC,	
UTC Time	130525.00,	hhmmss.ss,
Status	A,	A = Valid/V = Invalid,
Latitude	4250.5589,	ddmm.mmmm,
N/S Indicator	S,	N = North/S = South,
Longitude	14518.5084,	dddmm.mmmm,
E/W Indicator	E,	E = East/W = West,
Speed over ground	000.1,	Knots,
Course over ground	245.0,	Degrees,
UTC Date	291206,	DDMMYY,
Magnetic variation	,	Degrees,
Magnetic variation	,	E = East/W = West,
Checksum	*25	*CC
Terminator	<CR>,<LF>	Non-displayable characters

Table 11-1 NMEA-0183 Time string format

	<p>INFORMATION</p> <p>The serial communication settings of COM1 terminal including type of frame, baud rate, parity and stop bit are fixed and cannot be changed.</p>
---	--

11.1.2 T-Format Time frame output:

masTER T-Sync Model MTS200 transmits T-format time frame from COM2 terminal at rear panel of unit at every 1 second at 9600 (baud rate), 8 (Data bits), N (NONE parity), 1 (1 stop bit). User can change the serial communication settings using keypad on unit front panel as explained in section 9 or console base configuration utility as explained in section 9.2 or webserver as per section 13.4 or snmp as per section 13.3.

Note: Device can be configured to transmit T-format, NGTS, GPZDA or GPGGA time frame through its COM2 terminal at rear panel. Configuration of frame type can be done via keypad, via console based configuration utility through serial console terminal or Telnet or SSH, via SNMP or via Webserver. Refer respective sections in manual for further details.

Description	Number of Characters	Character Position	Range of Value/Information
Code Identification	1	1	Capital T
Divider	1	2	:
Year in Century	2	3,4	0 to 99
Divider	1	5	:
Month	2	6,7	1 to 12
Divider	1	8	:
Day of Month	2	9,10	1 to 31
Divider	1	11	:
Day of Week	1	12	1 to 7
Divider	1	13	:
Hours	2	14,15	0 to 23
Divider	1	16	:
Minutes	2	17,18	0 to 59
Divider	1	19	:
Seconds	2	20,21	0 to 59
Divider	1	22	:
GMT Marker	1	23	0 or 1
Validity Marker	1	24	0 or 1
CR [Carriage return]	1	25	Non displayable character
LF [Line Feed]	1	26	Non displayable character

Table 11-2 T-format Time string format

11.1.3 NGTS Time frame output:

masTER T-Sync Model MTS200 transmits NGTS time frame from COM2 terminal at rear panel of unit at every 1 minute at 9600 (baud rate), 8 (Data bits), N (NONE parity), 1 (1 stop bit). User can change the serial communication settings using keypad on unit front panel as explained in section 9 or console base configuration utility as explained in section 9.2 or webserver as per section 13.4 or snmp as per section 13.3.

Note: Unit can be configured to transmit T-format, NGTS, GPZDA or GPGGA time frame through its COM2 terminal at rear panel. Configuration of frame type can be done via keypad, via console based configuration utility through serial console terminal or Telnet or SSH, via SNMP or via Webserver. Refer respective sections in manual for further details.

The NGTS time string shall consist of 14 printable characters and a concluding CR, LF as follows:

Description	Number of Characters	Character Position	Range of Value/Information
Code Identification	1	1	Capital T
Year in Century	2	2,3	0 to 99
Month	2	4,5	1 to 12

Day of Month	2	6,7	1 to 31
Day of Week	1	8	1 to 7
Hours	2	9,10	0 to 23
Minutes	2	11,12	0 to 59
GMT Marker	1	13	0 or 1
Validity Marker	1	14	0 or 1
CR [Carriage return]	1	15	Non displayable character
LF [Line Feed]	1	16	Non displayable character

Table 11-3 NGTS Time string format

11.1.4 GPZDA Time frame output:

masTER T-Sync Model MTS200 transmits GPZDA time frame from COM2 terminal at rear panel of unit at every 1 second at 9600 (baud rate), 8 (Data bits), N (NONE parity), 1 (1 stop bit). User can change the serial communication settings using keypad on unit front panel as explained in section 9 or console base configuration utility as explained in section 9.2 or webserver as per section 13.4 or snmp as per section 13.3.

Note: *masTER* T-Sync Model MTS200 can be configured to transmit T-format, NGTS, GPZDA or GPGGA time frame through its COM2 terminal at rear panel. Configuration of frame type can be done via keypad, via console based configuration utility through serial console terminal or Telnet or SSH, via SNMP or via Webserver. Refer respective sections in manual for further details.

The full data message of this format shall consist of data fields as follows:

Field	Example	Comments
String ID	\$GPZDA,	
UTC Time	130525.00,	hhmmss.ss,
UTC Date	29,	Utc date dd
UTC Month	09,	Utc month mm
UTC year	2015,	Utc year yyyy
Local Timezone polarity	+,	Local timezone offset w.r.t. UTC
Local Timezone hours	05,	Local timezone hour w.r.t. UTC
Local Timezone minutes	30,	Local timezone minutes w.r.t. UTC
*cs	xx,xx	Two bytes crc
Terminator	<CR>,<LF>	Non-displayable characters

Table 11-4 GPZDA Time string format

11.1.5 GPGGA Time frame output:

masTER T-Sync Model MTS200 transmits GPGGA time frame from COM2 terminal at rear panel of unit at every 1 second at 9600 (baud rate), 8 (Data bits), N (NONE parity), 1 (1 stop bit). User can change the serial communication settings using keypad on unit front panel as explained in section 9 or console base configuration utility as explained in section 9.2 or webserver as per section 13.4 or snmp as per section 13.3.

Note: *masTER* T-Sync Model MTS200 can be configured to transmit T-format, NGTS, GPZDA or GPGGA time frame through its COM2 terminal at rear panel. Configuration of frame type can be done via keypad, via console based configuration utility through serial console terminal or Telnet or SSH, via SNMP or via Webserver. Refer respective sections in manual for further details.

The full data message of this format shall consist of data fields as follows:

Field	Example	Comments
String ID	\$GPGGA,	
UTC Time	130525.00,	hhmmss.ss,
Latitude	4250.5589,	ddmm.mmmm,
N/S Indicator	S,	N = North/S = South,
Longitude	14518.5084,	dddmm.mmmm,
E/W Indicator	E,	E = East/W = West,
Position Fix	1,	0=Unlock / 1=lock
Satellites tracked	12,	Total number of satellites available
HDOP	hhh.h,	Horizontal Dilution of Precision
Antenna Height	+0091.00,	Antenna height MSL value
Antenna Height units	M,	Antenna heights units In meters
Geoid Separation height	Ggg.g,	Geoid Separation
Geoid Height units	M,	Geoid height units
*cs	xx,xx	Two bytes crc
Terminator	<CR>,<LF>	Non-displayable characters

Table 11-5 GPGGA Time string format

11.2 Timing Output – IRIG-B / IEEE 1344 C37.118-2005

11.2.1 Introduction:

This section should help you with understanding, choosing and connecting the correct output from the *masTER* T-Sync model MTS200 to synchronize equipments, such as relays, breakers, meters etc. Often, questions arise about how output port should be connected, and how to connect cabling between model MTS200 and the relay. Certain protective relays or digital fault recorders may use a different style connector than available at model MTS200 outputs. This section will help to answer some common questions, like which type of cabling should be used? Coaxial or a twisted pair etc.

The steps involved in getting your devices synchronized to the model MTS200 are fairly simple and should not take long to complete. To expedite the process, make sure that you know:

1. The type of timing signal each piece of equipment requires, and
2. How to enable the equipment to receive the timing signal.

Various methods are used to configure equipment for IRIG-B including setting a physical jumper, or setup program. Some equipment can auto detect the timing signal, so that nothing else is required other than connecting the cable.

11.2.2 Time Code Output:

This section will describe IRIG-B Time Code also availability of the same in model MTS200 also configuration for the same. *masTER* T-Sync model MTS200 can generate different no of digital as well as analog signals as described in this section. Model MTS200 has also the facility to have optional card in model. Optional cards will have the same IRIG-B Time Code output, as on the standard output port.

Model: MTS200 (1U)

Doc. Ref. no. : m08/om/201

Issue no. : 03

11.2.2.1 Standard IRIG-B Output:

As per figure 5.2, *masTER* T-Sync model MTS200 model has two BNC connectors each for TTL and AM + one optional BNC connector for TTL/AM that supply timing signals to external equipment. Figure 5.8 shows the same two ports referenced as IRIG-B TTL. Where IRIG-B AM and other BNC port (which can be hard configured for TTL/AM) output is optional.

Note: On the back terminal plate of model MTS200 IRIG-B DCLS time code signal is referred as IRIG-B TTL.

11.2.2.2 Abstract of IRIG-B Time Code:

The transmission of coded timing signals began to take on widespread importance in the early 1950's. Especially the US missile and space programs were the forces behind the development of these time codes. The definition of time code formats was completely arbitrary and left to the individual ideas of each design engineer due to that hundreds of different time codes were formed, some of which were standardized by the "Inter Range Instrumentation Group" (IRIG) in the early 60's.

Today electronic systems such as communication system, data handling systems require time of day/year for data correlation of data with time. IRIG-B is a serial time code that occurs once per second and depending protocol it contains day of year, hour, minute, seconds, year and other important information. Except these, "IRIG Time Code" other format like IEEE1344 code which is an IRIG coded extended by information for time zone, leap second, etc.

IRIG-B fully described in IRIG Standard 200-04, released by RANGE COMMANDERS COUNCIL of the US Army White Sands Missile Range. IRIG-B format standard allows number of configurations that designated as IRIG-Bxyz, where x indicates the modulation technique, y indicates carrier signal frequency and z indicates data contained in the signal. IRIG-B timecode consists of 100 bits out of 74 bit used for time, date, and control functions. The 74 time code bits divided into:

30 bits for BCD value of Seconds, Minutes, Hours, and current day of the year

9 bits for year information

17 bits for binary value of current day seconds

18 bits for control functions Also unused bits are filled with logical zero.

11.2.2.3 IRIG-B AM & IRIG-B DCLS signals:

Figure illustrates primary difference between AM-Amplitude Modulated Signal and DCLS- (Pulse Width Modulated Signal). IRIG-B AM is distinctive because of the 1 KHz sine wave carrier. It is similar to IRIG-B DCLS, since Pick-Pick values of the carrier signal follow the same form as IRIG-B DCLS, which contains information.

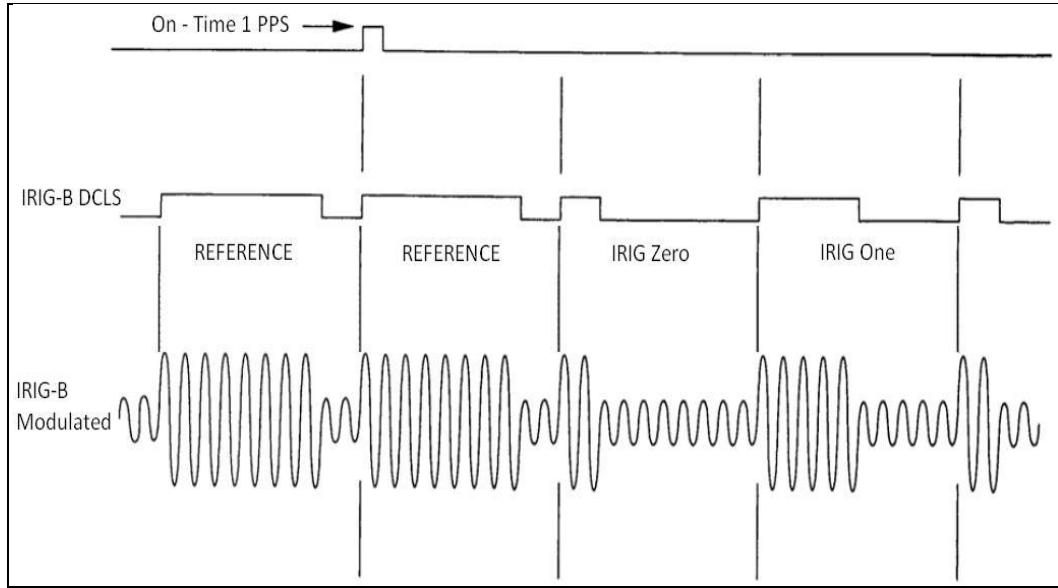


Figure 11-1 IRIG-B waveforms

11.2.2.4 IRIG-B IEEE 1344 Extension:

IEEE 1344 protocol has two versions available of which model MTS200 supports is IEEE 1344-2005 which defined in IEEE 1344.C37.118TM-2005 document. IEEE 1344.C37.118TM-2005 extends the Range Commanders Council document by using CF bits of IRIG 200-04. These CF bits are contains information like Time quality, Time offset to get UTC time from frame etc.

Bit no	Designation	Description
50	Year BCD Encoded, BCD 1	Low nibble of BCD encoded Year
51	Year BCD Encoded, BCD 2	
52	Year BCD Encoded, BCD 4	
53	Year BCD Encoded, BCD 8	
54	Separator always Zero	
55	Year BCD Encoded, BCD 10	High nibble of BCD encoded Year
56	Year BCD Encoded, BCD 20	
57	Year BCD Encoded, BCD 40	
58	Year BCD Encoded, BCD 80	
59	P6	Position Identifier #6
60	Leap Second Pending (LSP)*	Becomes 1 up to 59 Sec before leap second inserted
61	Leap Second (LS)*	0 = add leap sec, 1 = Delete leap Sec
62	Daylight Saving Pending (DSP)*	Becomes 1 up to 59 Sec before DST change
63	Daylight Saving Time (DST)*	Becomes 1 during DST
64	Time-zone Offset Sign	Time-zone Offset Sign :- 0=+, 1=-
65	Time-zone Offset BCD encoded, BCD 1	Offset from coded IRIG-B time to UTC time. IRIG coded time plus time offset (Including sign) Equals UTC time.
66	Time-zone Offset BCD encoded, BCD 2	
67	Time-zone Offset BCD encoded, BCD 4	
68	Time-zone Offset BCD encoded, BCD 8	

69	P7	Position Identifier #7
70	Time Zone Offset 0.5 Hour	0 = none, 1=additional 0.5 hour time-zone offset
71	Time Quality	4-bit code representing approx. clock time error. 0000 =MTS200 Locked, maximum accuracy 1111 =MTS200 failed, data unreliable
72	Time Quality	
73	Time Quality	
74	Time Quality	
75	Parity	Parity on All preceding data bits including time of year
76	Not Used	Unassigned, Zero Value
77	Not Used	Unassigned, Zero Value
78	Not Used	Unassigned, Zero Value
79	P8	Position Identifier #8

Table 11-6 Assignment of CF Segment for IEEE 1344(C37.118-2005)

To use these extra bits of information, protective Relays, RTU's and other equipment receiving the time code must be able to decode them.

	<p>INFORMATION</p> <p>In IEEE 1344 C37.118-2005 Leap Second, Leap Second Pending bits are not supported in this firmware version.</p>
---	--

11.2.2.5 Generated IRIG-B Time Codes:

masTER T-Sync model MTS200 supports different IRIG-B 00x/IRIG-B12x protocols. Supported protocols are listed below.

- a) IRIG-B007 : 100 pps, DCLS Signal, No carrier Frequency
BCD TOY, BCDYR, SBS (Time of Day)
- b) IRIG-B127 : 100 pps, AM Signal, 1 KHz carrier Frequency
BCD TOY, BCDYR, SBS (Time of Day)
- c) IEEE 1344 (C37.118-2005) : 100 pps, AM Signal, with 1 KHz Carrier frequency
BCD TOY, BCDYR, SBS, IEEE1344 assignment of CF bits (Refer Section 11.2.2.4)
: 100 pps, DCLS Signal, No Carrier Frequency
BCD TOY, BCDYR, SBS, IEEE1344 assignment of CF bits (Refer Section 11.2.2.4)

11.2.2.6 Selection/configuration of IRIG-B Time Codes:

The time code generated can be selected/configured using Telnet menu available on model MTS200 Ethernet port NTP1.

IRIG-B time code for model MTS200 can be configured for

- 1) IEEE 1344 C37.118 – 2005 protocol enabling
- 2) UTC time on IRIG-B time code or Local time on IRIG-B time code.

IRIG-B DCLS time codes (IRIG-B 00x) and IRIG-B AM time codes (IRIG-B 12x) are always generated simultaneously. Using telnet if we configure the IRIG-B output for IEEE 1344 protocol than both IRIG-B00x and IRIG-B12x gives IEEE 1344 protocol CF bits output. Similarly, we can configure IRIG-B output

for UTC time/ Local time effect of configuration will be on both IRIG-B 00x and IRIG-B 12x. To configure IRIG-B please refer Telnet Appendix.

11.2.2.7 Connecting IRIG-B Time Code:

masTER T-Sync model MTS200 time code outputs are designed to handle multiple loads. The output terminals of IRIG-B time code are BNC type. Input devices have different type of IRIG-B time code input connectors. Co-axial cables can be connected directly from model MTS200 to end device. To adapt twisted pair cabling with model MTS200, use BNC Breakout or other similar adapter.

Note: In case of shielded twisted pair cabling do not connect shielding of cable to model MTS200, ground it at the receiver end.

Following factors come into effect by transmitting time code to multiple/single devices over long distance,

- 1) Resistive loss in cabling
 - 2) Electromagnetic interference
 - 3) Propagation delay
 - 4) Input impedance of end device
- 1) **Resistive loss in cabling:** -Resistive loss in cabling affects the available output voltage at the input device. Wire has a certain resistivity associated with it that is determined by its metallic composition, and resistance determined by the diameter and length.
 - 2) **Electromagnetic interference:** -Electromagnetic interference (EMI) includes a variety of sources of interfering signals, ranging from dc and low-frequency (50 or 60 Hz) all the way up through the RF (Radio Frequency) and microwave region. All of these signals have the potential to interfere in one way or another with the accurate and reliable distribution of timing signals.
 - 3) **Propagation Delay:** -Electromagnetic waves travel at the speed of light (C) in free space/vacuum and a fraction of that speed through cabling which cause delay in IRIG-B Time code output.
 - 4) **Input impedance of end device:** -By connecting, multiple devices to *masTER* T-Sync MTS200 results in decrease of drive voltage due to increase in load current. In many cases, model MTS200 time code output are "fanned out" to a no of devices. The exact no of possible load can be determine from input impedance of each connected devices. To know input impedance of connected devices please refer specific device manual.

11.2.2.7.1 Connecting IRIG-B DCLS:

To drive multiple loads from IRIG-B DCLS output connects all end devices in parallel. To determine load current for one IRIG-B DCLS output.

- Determine no of load devices to be connected
 - Determine input impedance of each load devices (Rdev)
 - Calculate load current of each device ($I_{dev} = 5V \div R_{dev}$)
 - Sum all the load device current and compare with model MTS200 load capacity current
- masTER* T-Sync model MTS200 IRIG-B DCLS time code output impedance is 50Ω @ 5V.

11.2.2.7.2 Connecting IRIG-B AM:

The main difference in computing the load capacity for IRIG-B AM and IRIG-B DCLS is that some of the modulated IRIG-B decoders are sensitive to the peak-to-peak voltage. Connecting multiple devices with MC-1 IRIG-B AM output causes increase in current flow which affects the Pick-Pick output voltage to decrease. *masTER* T-Sync MTS200 IRIG-B AM Time code signal output impedance is 100Ω.

11.3 Timing Output – NTP

11.3.1 NTP Introduction:

NTP (Network time protocol) is a common method for synchronization of hardware clocks in local and global Ethernet networks. The software package NTP is an implementation of the actual version 3, based on the specification RFC-1305. NTP protocol is used to synchronize and maintain the time among distributed networks of servers and clients. NTP protocol is evolved from Time protocol but is designed to maintain accuracy and robustness even on the networks involving multiple gateways, high network path delays and unreliable nets. NTP protocol is applied on the application layer on UDP based IP layer.

The purpose of NTP is to convey timekeeping information (in terms of UTC) from NTP servers to other time clients via the Internet and also to cross-check clocks and mitigate errors due to equipment or propagation failures. In NTP basic model, NTP client device sends the NTP packet message over wire to NTP server (time source) at prefixed/defined interval (as per NTP standard). The NTP server interchanges IP addresses and ports, overwrites certain fields in the message, inserts current timestamp in packet, recalculates the checksum and returns the message immediately to NTP client. Information included in the NTP message allows the client to determine the server time with respect to local time and adjust the local clock accordingly. After NTP message is received, NTP client calculates time offset, own local clock frequencies and update in its database at regular intervals to maintain the clock time synchronization with NTP server time. This may result in either a step-change or a gradual phase adjustment in time of the NTP client's local clock to reduce the offset to zero or as minimum as possible. The accuracies achievable by NTP client depend strongly on the precision of the local-clock frequency and stringent control of device and process latencies.

NTP architecture model consists of number of primary reference sources, synchronized by wire or radio clock. There are other several multiple secondary time sources/clients which are arranged in hierarchal manner in network which request time from primary reference sources. Under normal circumstances it is intended that the synchronization subnet of primary and secondary servers assumes a hierarchical-master-slave configuration with the primary servers at the root and secondary servers of decreasing accuracy at successive levels toward the leaves.

11.3.2 NTP Output:

masTER T-Sync Model MTS200 device is equipped with 10/100 Mbps based Ethernet output port which provides the functionality of NTP server. This NTP output is capable to synchronize time of various NTP clients such as windows PC, Unix/Linux machines and other clients which support NTP protocol. This unit operates at stratum 1 level which is the highest level (in terms of accuracy) after atomic clock providing the NTP timestamp output resolution in milliseconds. Stratum level 1 indicates that a device synchronizes its own clock from radio clock or satellite clock. *masTER T-Sync* Model MTS200 NTP output operates in Unicast mode in which NTP server responds only when there is NTP request from NTP clients. MTS200 is also capable to operate in ntp broadcast as well as multicast mode in which MTS200 will send ntp server frame at configured interval in seconds. NTP clients operating at stratum level lower than 1 (i.e. 2 to 15) can synchronize their time from *masTER T-Sync* Model MTS200 NTP output.

MTS200 continuous to provide NTP output even under Unlock conditions (when there is no satellite signal available) depending on its internal RTC clock time and accuracy. If required, user can configure stratum level (2 to 15) of NTP output only for holdover conditions which is applicable when device is in Unlock condition. This feature provides the indication to NTP client devices whenever device enters holdover mode during ideal run conditions. Under Lock conditions, MTS200 NTP output will always operate at stratum level 1 which cannot be changed.

User should change the stratum level of device carefully, after having knowledge of its NTP Server-Client network hierarchical level architecture. Stratum level decreases by 1 at every NTP server-client level stages with respect to GPS Clock device stratum level.(Stratum at the topmost level (primary GPS servers) is assigned as one and each level downwards (secondary servers) in the hierarchy assigned as one greater than the preceding level). If the stratum level of device is configured at 15 under Unlock

conditions, no NTP client will synchronize its time with NTP server output as level 15 is the last limit of stratum as per NTP standard.

```

Network Time Protocol
  Flags: 0x1c
    00.. .... = Leap Indicator: no warning (0)
    ..01 1... = Version number: NTP Version 3 (3)
    .... .100 = Mode: server (4)
  Peer Clock Stratum: primary reference (1)
  Peer Polling Interval: 14 (16384 sec)
  Peer Clock Precision: 0.000001 sec
  Root Delay:      0.0000 sec
  Root Dispersion: 0.0000 sec
  Reference Clock ID: Global Positioning Service
  Reference Clock Update Time: Feb  7, 2036 06:28:18.2679 UTC
  originate Time Stamp: Feb  7, 2036 06:28:18.2679 UTC
  Receive Time Stamp: Oct 15, 2009 11:33:29.3930 UTC
  Transmit Time Stamp: Oct 15, 2009 11:33:29.3930 UTC
    
```

Figure 11-2 NTP frame format

Below are the list of some of all NTP packet parameters which are functionally significant with respect to NTP server.


Mode: 3-bit integer representing the mode with value “4”, means that this device act as NTP server device and can provide time output for synchronization to NTP client devices but will never be synchronized by clients.

Peer clock stratum:8-bit integer representing the stratum with value “1”, which means that *masTER* T-Sync act as primary reference source. Stratum value will be fixed at 1 during device Lock conditions. However, it can be configured between 2 to 15 (via telnet/SSH/keypad/Webserver/serial console terminal) which will only be applicable during device Unlock conditions.

Clock precision:This is an eight-bit signed integer indicating the precision of the local clock, in seconds to the nearest power of two. *masTER* T-Sync MTS200 is having its internal clock precision of 1 us (1 microseconds = 0.000001s).

Reference Clock identifier: This is a 32-bit code identifying the particular reference clock. As *masTER* T-Sync Model MTS200 is stratum 1 primary reference source, it's reference identifier is designated as “GPS”.

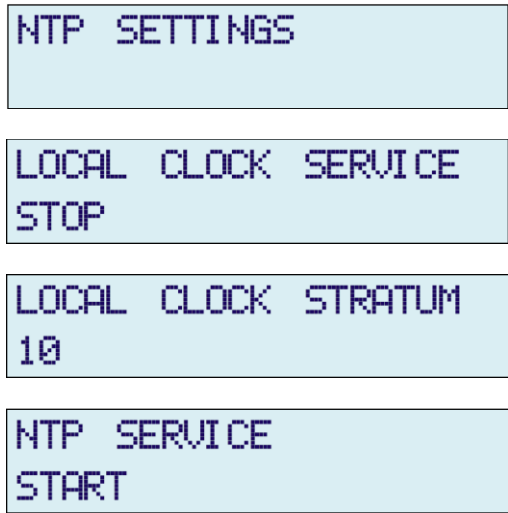
Transmit Timestamp:Time of the server when the NTP response left for the NTP client, in NTP timestamp format. NTP timestamps are represented as a 64-bit unsigned fixed-point number, in seconds relative to 0h on 1 January 1900 in terms of UTC. The integer part is in the first 32 bits and the fraction part in the last 32 bits. *masTER* T-Sync Model MTS200 provides time format in seconds and fractional timestamp with a millisecond resolution.

	<p>FUNCTIONALITY</p> <p>If the stratum level of <i>masTER</i> T-Sync Model MTS200 device is configured at 15 under Unlock conditions, no NTP client will synchronize its time with NTP server output as level 15 is the last limit of stratum as per NTP standard</p>
---	--

11.3.3 NTP Server Installations and Configurations:

11.3.3.1 NTP General Settings

NTP Settings through front panel keypad:



NTP Settings through SSH / Telnet / Serial Console Mode:

NTP CONFIGURATION		
NO	MEANING	VALUE(x)
1	Local Clock Srvs. (0/1)	= 1
2	Local Clock Stratum	= 12
3	AUTH. Key (NONE/SYMM./AUTO)	= NONE
4	Autokey Identity Scheme(PC/IFF)	= PC
5	BCAST. Srvs (0/1)	= 0
6	BCAST. Address 1	= 0.0.0.0
7	BCAST. Interval 1 (Seconds)	= 0064
8	BCAST. Key 1 (NONE/SYMM./AUTO)	= NONE
9	BCAST. SYMM. KeyID 1	= 0001
10	BCAST. Address 2	= 0.0.0.0
11	BCAST. Interval 2 (Seconds)	= 0064
12	BCAST. Key 2 (NONE/SYMM./AUTO)	= NONE
13	BCAST. SYMM. KeyID 2	= 0001

Figure 11-3 NTP Settings Menu on Console based utility

NTP Settings through Webserver Mode:

NTP Configurations:

Authentication Type:

Trusted Key: Add Delete (1-9999)

Disable Local Clock:

Local Clock Stratum: (0-15)

Disable Broadcast Address:

Broadcast Address 1: Key Type: Key ID: (1-9999)

Broadcast Interval 1 (sec):

Broadcast Address 2: Key Type: Key ID: (1-9999)

Broadcast Interval 2 (sec):

*Use "Ctrl+F5" to Refresh Page

NTP Configurations:

NTP Configurations

```
driftfile /home/root/ntp/ntp.drift
statsdir /home/root/ntp/ntpstats/
statistics loopstats
filegen loopstats file loopstats type day enable
pidfile /home/root/ntpdpid.txt

disable auth

server 127.127.30.0 minpoll 4 maxpoll 4 prefer
fudge 127.127.30.0 flag3 1

server 127.127.1.0 # local clock
fudge 127.127.1.0 stratum 12 refid GPS # local clock

restrict -4 default kod notrap nomodify nopeer noquery
restrict -6 default kod notrap nomodify nopeer noquery

restrict 127.0.0.1
restrict ::1

broadcast ff08::101 minpoll 04 maxpoll 04 # broadcast
```

Figure 11-4 NTP Settings Menu on Webserver

11.3.3.2 NTP Local Clock

MTS200 is capable to operate on internal local clock whenever there is no GPS Antenna connected to the unit. Ntp service in MTS200 can be configured for local clock and local stratum value when the unit is in unlock conditions. Local clock settings can be done by front panel keypad or SSH application or Telnet

Model: MTS200 (1U)

Doc. Ref. no. : m08/om/201

Issue no. : 03

application or webserver or front panel serial console port. Stratum can be configured from 0 to 15 value range. Local clock cannot be disable in GPS Unlock conditions because in unlock conditions, unit is running on its internal clock.

Note:

1. The stratum of local clock should be configured as required stratum – 1 because ntp driver always transmit stratum as configured + 1 value.
2. Refer section 11.3.4 and 11.3.5, for detail understanding of stratum value implementation on ntp clients in network.

Refer section 11.3.3 for method to configure ntp settings through SSH, Telnet, serial console mode and refer 11.3.3 for method to configure ntp settings through webserver mode.

11.3.3.3 NTP Broadcast / Multicast

NTP Configurations:

Authentication Type:

Trusted Key: (1-9999)

Disable Local Clock:

Local Clock Stratum: (0-15)

Disable Broadcast Address:

Broadcast Address 1: Key Type: Key ID: (1-9999)

Broadcast Interval 1 (sec): (64 is selected)

Broadcast Address 2: Key Type: Key ID: (1-9999)

Broadcast Interval 2 (sec):

MTS200 is capable to broadcast NTP packets at configured & defined interval in seconds. This device can send regular ntp packets over particular defined broadcast address or set NTP multicast address (IPv4 - 224.0.1.1) which is fixed v4 address and (IPv6 – ff08::101,ff05::101,ff02:101) assigned by IANA for ntp multicast.

Operator have to set the broadcast address or above specified multicast address in Broadcast Address field as “BCAST. Address” in console configuration utility or “Broadcast Address” in webserver mode. Also , user have to select the broadcast/multicast interval in seconds defined as “BCAST. Interval(seconds)” in console based configuration utility or “Broadcast Interval” in webserver NTP page.

If NTP broadcast or multicast mode is not required, users can use this mode by setting parameter “BCAST/ Srvs (0/1)” in console based configuration utility NTP menu to 0 or selecting “Disable Broadcast Address” option in webserver NTP page.

It is always recommended to use NTP Broadcast or NTP multicast only with using any of NTP Authentication technique (symmetric key based / Autokey) in order to avoid accidental or malicious disruption in this mode.

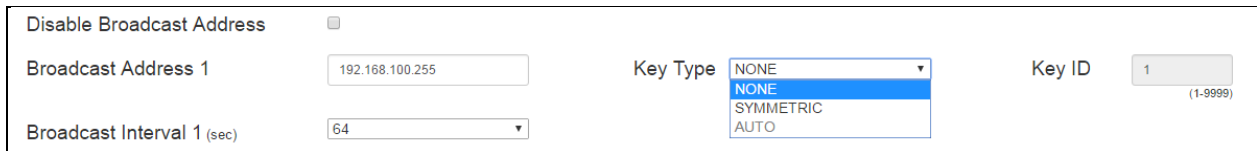
User can configure NTP broadcast Authentication via console based utility in Symmetric key mode only and in Symmetric and Autokey authentication via webserver mode.

Broadcast Authentication – Symmetric key:

Before configuring NTP Broadcast Authentication, user need to configure NTP main Authentication mode to required Broadcast Authentication mode (SYMM / AUTO) for symmetric key and Autokey because ntp driver can be configured only in one authentication mode either Symmetric key or Autokey, at a time for complete ntp authentication and ntp broadcast authentication.

However, NTP broadcast Authentication is optional as user can set NTP main Authentication mode to SYMM or AUTO but broadcast authentication can be made NONE if no authentication is required for NTP broadcast/multicast, but it is recommended to always use ntp broadcast/multicast with either of authentication technique.

1. In Console based configuration utility: For configuration NTP broadcast / multicast with symmetric key authentication, user need to set field “BCAST. Key” parameter to SYMM mode and “BCAST. SYMM KeyID” parameter to applicable trusted key configured.
2. In Webserver mode: For configuration NTP broadcast / multicast with symmetric key authentication, user need to set the field “Key Type” to “SYMMETRIC” and field “Key ID” to trusted key value as shown in below figure.



The screenshot shows a configuration window for NTP broadcast authentication. It includes a checkbox for 'Disable Broadcast Address', a text field for 'Broadcast Address 1' with the value '192.168.100.255', a dropdown for 'Broadcast Interval 1 (sec)' with the value '64', a dropdown for 'Key Type' with 'SYMMETRIC' selected, and a text field for 'Key ID' with the value '1' and a range '(1-9999)'.

Broadcast Authentication – Autokey Mode:

Before using NTP Autokey (AUTO) authentication for NTP broadcast/multicast, user need to generate or should have the ntpkeys in MTS200 for configured PC or IFF scheme. Please refer section 11.3.3.4 for method for NTP Autokey Authentication process.

Broadcast – NTP Client modifications:

1. For Broadcast without authentication :

User have to do below changes in client ntp.conf file for receiving ntp broadcast packets.

```
disable auth  
  
broadcastclient yes  
broadcastdelay 0.01
```

Ordinarily, upon receiving a message for the first time, the broadcast client measures the nominal server propagation delay using a brief client/server exchange with the server, after which it continues in listen-only mode. If the **broadcastdelay** command is not used, the default is 4.0 ms or user can specify their own **broadcastdelay** depending on their network architecture.

2. For Broadcast with symmetric key authentication :

User have to do below changes in client ntp.conf file for receiving ntp broadcast packets.

```
# disable auth
keys /etc/ntp/ntp.keys # symmetric key file
trustedkey 1 2 8 10 # total trusted keys list

broadcastclient key 8 # 8 is key id number required from trusted keys
broadcastdelay 0.01
```

3. For Broadcast with Autokey authentication :

User have to do below changes in client ntp.conf file for receiving ntp broadcast packets.

```
# disable auth
crypto pw password #Autokey
keysdir /etc/ntp # public keys directory path
crypto randfile /dev/urandom

broadcastclient autokey
broadcastdelay 0.01
```

4. For multicast without authentication :

User have to do below changes in client ntp.conf file for receiving ntp broadcast packets.

```
disable auth
multicastclient 224.0.1.1
multicastclient ff08::101
```

This command enables reception of multicast server messages to the multicast group address(es) (type **m**) specified. Upon receiving a message for the first time, the multicast client measures the nominal server propagation delay using a brief client/server exchange with the server, then enters the broadcast client mode, in which it synchronizes to succeeding multicast messages. Note that, in order to avoid accidental or malicious disruption in this mode, both the server and client should operate using symmetric key or public key authentication

5. For multicast with symmetc key authentication :

User have to do below changes in client ntp.conf file for receiving ntp broadcast packets.


```
# disable auth
keys /etc/ntp/ntp.keys # symmetric key file
trustedkey 1 2 8 10 # total trusted keys list

multicastclient 224.0.1.1 key 8 # 8 is key id number required from trusted keys
multicastclient ff08::101 key 8 # 8 is key id number required from trusted keys and ff08::101 is NTP
#multicast address
```

6. For multicast with Autokey authentication :

User have to do below changes in client ntp.conf file for receiving ntp broadcast packets.

```
# disable auth
crypto pw password          #Autokey
keysdir /etc/ntp           # public keys directory path
crypto randfile /dev/urandom
multicastclient 224.0.1.1 autokey
```

	<p>FUNCTIONALITY</p> <ul style="list-style-type: none"> • NTP Broadcast or multicast should always be used with authentication to avoid accidental or malicious disruption in this mode. Also, if there are multiple MTS200 devices connected in same LAN, use any of the MTS200 for ntp broadcast/multicast. • After changes to NTP broadcast parameters are done, NTP service need to be restarted in order to changes to be in effect. User can check the configuration by using “show ntp.conf” file option in webserver or option “1” in NTP main menu in console based configuration utility. • For MTS200 dual Ethernet output operating in different network domain, ntp driver will enable broadcast on second Ethernet output on broadcast address as xxx.xxx.xxx.255 automatically if broadcast feature is not disabled in configuration. Broadcast interval seconds and security feature will be same as configured. • Multicast address always will be IP address “224.0.1.1” which is fixed and reserved for NTP by IANA. If user configures any other reserved multicast address other than mention, ntp driver will not start NTP multicast considering this as fault address. • FF08::101 is the NTP Ipv6 Multicast address. User can configure FF05::101, FF02::101. These are the IPv6 multicast address reserved for Ipv6. • User need to take special care while configuring ntp clients operating in NTP unicast and NTP broadcast mode at a time considering timing accuracy requirement at ntp clients internal clock.
---	---

11.3.3.4 NTP Authentication

Authentication support allows the NTP client to verify that the server is in fact known and trusted and not an intruder intending accidentally or on purpose to masquerade as that server. The NTPv3 specification RFC-1305 defines an scheme which provides cryptographic authentication of received NTP packets. Originally, this was done using the Data Encryption Standard (DES) algorithm operating in Cipher Block Chaining (CBC) mode, commonly called DES-CBC. Subsequently, this was augmented by the RSA Message Digest 5 (MD5) algorithm using a private key, commonly called keyed-MD5.

11.3.3.4.1 Symmetric Key Mechanism

The original RFC-1305 specification allows any one of possibly 65,534 keys, each distinguished by a 32-bit key identifier, to authenticate an association. The servers and clients involved must agree on the key and key identifier to authenticate their messages. Keys and related information are specified in a key file, usually called ntp.keys, which should be exchanged and stored using secure procedures beyond the scope of the NTP protocol itself. When ntpd is first started, it reads the key file specified in the keys command and installs the keys in the key cache. However, the keys must be activated with the trusted command before use.

Model: MTS200 (1U)

Doc. Ref. no. : m08/om/201

Issue no. : 03

When authentication is specified, a message authentication code (MAC) is appended to the NTP packet header. The MAC consists of a 32 bit key identifier (key ID) followed by a 128- or 160 bit message digest. On receive, the message digest is computed and compared with transmitted MAC. The packet is accepted only if two MACs are identical.

MTS200 provides support for Symmetric key mechanism based NTP authentication using user define key ID and key password. MTS200 supports only MD5 Key. MTS200 uses ntp.keys file to store the key ID and key password. However, the password should be transferred to ntp clients using secure means.

Below is truncated part of ntp.keys file format:

#ntp.keys		
1	M	masibus
2	M	test1
3	M	key1

M refers to MD5 key notation.

User can add or replace existing key string using console based configuration utility or webserver. User can add 1 to 9999 key ID values in MTS200 and key string of max. 20 characters only. Factory default key id will be set at ID number 1 and Key string "masibus".

ntp driver will authenticate the ntp messages with symmetric key for only those keys which are defined as trustedkey in ntp.conf file. This can be also be done using console based configuration utility and webserver mode. Remember, the trustedkey should be one of the keys defined in ntp.keys file, failing to which ntp association between MTS200 and ntp clients will not complete.

Also, for successful NTP secure communication between MTS200 and ntp clients, it is necessary to define same key ID and key string in ntp.keys file in ntp client device. Apart from adding key ID and string in clients ntp.keys file, same key ID has to be defined in client ntp.conf file as trustedkey.

Using Console based configuration utility:

Refer section 9.2.2 for method to edit NTP symmetric key and add/delete trusted key using console based configuration utility.

Using Webserver:

1. For editing NTP symmetric key file ntp.keys, go to Security page -> "NTP Symmetric Key" section in below image.

In this section, enter Key id number in field "Key ID" and password in field "Key String" and then click on "ADD" button. This will add key in ntp.keys file. To check the existing or new added keys, click on "View Symm. Keys" button.

Figure 11-5 NTP Security Settings on Webserver

- Now, to configure any key in ntp.keys file as trustedkey in ntp.conf file, go to menu NTP-> NTP Configurations.

If trusted key field is to be modified, then user have to ensure the NTP filed “Authentication Type” should be already set as “SYMMETRIC”. If not, set it as “SYMMETRIC” and then apply “SAVE” button. Then only user can modify trusted key as explained below.

Now, Enter the required trustedkey value in field “Trusted Key” and then click on “ADD” button. If user wants to remove any key as trusted key, enter the required trustedkey value in field “Trusted Key” and then click on “DEL” button.

After doing above changes, user have to restart the ntp service in order to new trusted key to be in effect.

11.3.3.4.2 NTP AutoKey Mechanism:

NTPv4 included support for NTP symmetric key as well as NTP Autokey mechanism specified in RFC-5606. NTP Symmetric key was less secure than NTP Autokey due to easy access to password form ntp.keys file. However, Autokey mechanism provided more robust mode of authentication between ntp server and clients by generating private key, public key and group key. Also, ntp Autokey reduce the extra work of changing the key in all ntp clients whenever there is change in private key at trusted server.

Model: MTS200 (1U)

Doc. Ref. no. : m08/om/201

Issue no. : 03

Autokey involves public and private key in which public key cryptography is based on a private key known only to creator or trusted server and a public key known to all participants. NTP client can verify the originator has the private key using the public key and any of several digital signature algorithms.

Autokey subnet includes three main type of NTP devices as follows:

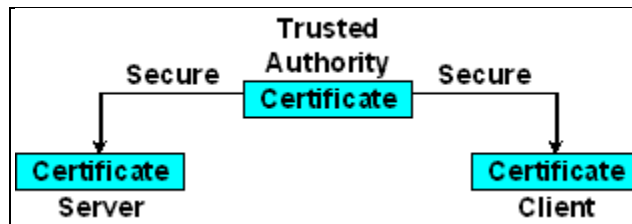
1. **Trusted Server/Trusted Authority:** This are lowest stratum server in NTP network which can generate self-certified certificate marked as trusted and group key.
2. **Server:** This are the secondary NTP servers which do not own trusted certificate but only self generate certificate which are not trusted marked.
3. **Clients:** These are normal ntp clients which uses only public keys to authenticate trusted server and servers.

The group key or public key has to be transferred to other ntp clients and server using secure means only such as HTTPS, SSH or SCP.

MTS200 is a stratum 1 server so it can act as Trusted Server in ntp network. Also, there are multiple MTS200 units installed in a network, user can make one unit as Trusted server and others as normal Server. MTS200 supports two type of Autokey Identity schemes which are PC (Private Certificate) scheme and IFF (Schnorr) Cryptosystem scheme.

11.3.3.4.2.1 NTP Autokey PC Scheme:

The PC scheme uses a private certificate (X509.3 type certificate) generated by Trusted host as the group key and is distributed to all ntp group clients by secure means such as HTTPS or SCP. It is owner or operator responsibility to reveal this group key outside the ntp group. This scheme is cryptographically strong as long as the private certificate is kept secured. Refer below figure for further understanding of PC scheme.



Whenever a new private certificate is generated by Trusted host, it is necessary to distribute new key to all ntp clients for successful associations.

- Procedure to Generate NTP Autokey PC Scheme keys in MTS200:

User can generate Autokey for PC and IFF scheme based authentication files in MTS200 using webserver only. To generate PC schemes keys, user need to go device webserver page Security, in which NTP Autokey section is provided.

Step 1: Then, user need to select PC option in field “Identity Scheme” and mark Certificate Type as “Trusted Server”. Autokey PC scheme need password to be entered to generate private key and private certificate. User need to remember this password to set in ntp client ntp.conf file while starting PC scheme based ntp associations between server and client.

NTP Autokey:

Identity Scheme: PC

Certificate Type: Trusted Server Server

NTP Autokey Password: [masked]

Re-enter NTP Autokey Password: [masked]

Buttons: Submit Password, Generate NTP Autokey, Remove Old Keys

Contents Of: Private Key (selected), Certificate, Group Key

Buttons: Add Key, View

Figure 11-6 NTP Autokey – PC Scheme Settings on Webserver

Step 2: After password is entered, click on “Submit Password”. This option will configure the crypto password in MTS200 ntp configuration file automatically. “Generate NTP Autokey” option will only be enable after “Submit Password” is done.

NTP Autokey:

Identity Scheme: PC

Certificate Type: Trusted Server Server

NTP Autokey Password: [masked]

Re-enter NTP Autokey Password: [masked]

Buttons: Submit Password, Generate NTP Autokey, Remove Old Keys

Contents Of: Private Key

Buttons: Add Key, View

Step 3: “Generate NTP Autokey” option will generate the NTP Autokey PC scheme private key and private certificate automatically. It is necessary to delete any old NTP autokey files from MTS200 before generating new keys, use option “Remove Old Keys” option. While the keys are being generated, the background of webserver will be hidden till all keys are generated.

NTP Autokey:

Identity Scheme: PC

Certificate Type: Trusted Server Server

NTP Autokey Password: [masked]

Re-enter NTP Autokey Password: [masked]

Buttons: Submit Password, Generate NTP Autokey, Remove Old Keys

Contents Of: Private Key

Modal Dialog: ...
PROCESSING. PLEASE WAIT...

Model: MTS200 (1U)
 Doc. Ref. no. : m08/om/201
 Issue no. : 03

Step 4: PC scheme generates two different Autokey files i.e. Private key file and Certificate file. After required keys are generated, user can check the key contents using “VIEW” option and selecting key type in field “Contents of” as shown in below images.

NTP Autokey:

Identity Scheme:

Certificate Type: Trusted Server Server

NTP Autokey Password:

Re-enter NTP Autokey Password:

Buttons:

Contents Of:

Buttons:

```
# ntpkey_RSAbost_MTS200.2208990457
# Thu Jan 1 00:27:37 1970

-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIBozA9BgkqhkiG9w0BBQ0wMDAbBgkqhkiG9w0BBQwwDgQIoHXyDu+jHMACAggA
MBEGBSsOAwIHBAgTyosv5k4pjjSCAWAdfRhTH8kkpQPMJF2WlxmauHeqamvRVx5S
wvf++Bp9jZR0M83otxC7sh4Bul3eLMYTgoAml2laWlmAtShcugL5ttGrL23mhQX
Y639S0LKVTUndQp/zlisHIO0pXGXUHMaQAT12LvdhKHILL0An6yw95fLEYFP0fZV
bzHXoFtv/E/XWTysWR4tMw0K/56zHHA+OUFp/RhbpCtBF3WPFdhU7MGas+EYIKxy
dfIPRNngGC7FUqhDPCECfjBfaZT5a+ubDpjgAwais9ghyYMNcV6WGfutJNR+Ap0m4
wZLghpz27qIOkksWQozaf9Stof3dzQLI/FJeUX56sJY0KyvQuyKLMqw4W40h82+X
XyoLIWAndNzxUVa/dITvdlcwE3KvXEyRMXwCVx6x+1cEq5kMrL0Amy/gq6SEefx
JGzOjLX1AF9llrktatm6OrtgINTe4YYPzCLzfs7voJbS3KkAx9Y
-----END ENCRYPTED PRIVATE KEY-----
```

Contents Of:

Buttons:

```
# ntpkey_RSAbost_MTS200.2208990457
# Thu Jan 1 00:27:37 1970

-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIBozA9BgkqhkiG9w0BBQ0wMDAbBgkqhkiG9w0BBQwwDgQIoHXyDu+jHMACAggA
MBEGBSsOAwIHBAgTyosv5k4pjjSCAWAdfRhTH8kkpQPMJF2WlxmauHeqamvRVx5S
wvf++Bp9jZR0M83otxC7sh4Bul3eLMYTgoAml2laWlmAtShcugL5ttGrL23mhQX
Y639S0LKVTUndQp/zlisHIO0pXGXUHMaQAT12LvdhKHILL0An6yw95fLEYFP0fZV
bzHXoFtv/E/XWTysWR4tMw0K/56zHHA+OUFp/RhbpCtBF3WPFdhU7MGas+EYIKxy
dfIPRNngGC7FUqhDPCECfjBfaZT5a+ubDpjgAwais9ghyYMNcV6WGfutJNR+Ap0m4
wZLghpz27qIOkksWQozaf9Stof3dzQLI/FJeUX56sJY0KyvQuyKLMqw4W40h82+X
XyoLIWAndNzxUVa/dITvdlcwE3KvXEyRMXwCVx6x+1cEq5kMrL0Amy/gq6SEefx
JGzOjLX1AF9llrktatm6OrtgINTe4YYPzCLzfs7voJbS3KkAx9Y
-----END ENCRYPTED PRIVATE KEY-----
```

The keys generated in PC scheme in MTS200 are as follows:

PC Private key: “ntpkey_host_MTS200”
 PC Private Certificate: “ntpkey_cert_MTS200”

- Procedure to use Autokey PC Scheme as ntp associations between MTS200 and ntp clients :

Step 1: User should transfer the generated key and certificate to all other ntp clients using secure means such as SCP or HTTPS (using download section) or doing copy & paste option from MTS200 webserver/SSH mode.

To transfer MTS200 ntp keys using SCP method, user need to take console of MTS200 using SSH (only by super-user or administrative user of MTS200) from remote host PC, mentioned as below commands.

On Remote Host PC: **ssh root@192.168.100.153**

Where, root = is the default super-user of MTS200,
192.168.100.153 = is the IP address of MTS200 ethernet port

If operator has successfully taken the console session of MTS200, then user can give below commands to transfer the ntp keys to remote Host PC.

scp /home/root/ntp/ntpkey_cert_MTS200 user@192.168.100.231:/etc/ntp

scp /home/root/ntp/ntpkey_host_MTS200 user@192.168.100.231:/etc/ntp

Where, user = is the username of remote Host PC where keys are to be transferred,
192.168.100.231 = IP address of remote Host PC where keys are to be transferred
/etc/ntp = it is the destination folder where ntp keys are copied. This can be different as per remote Host PC ntp client setup

Now, user should close the SSH session with MTS200, as given below command:

exit

User should avoid using Telnet mode to transfer keys as Telnet in unsecure way for communication.

After keys are transferred, user need to copy keys in ntp clients keys folder (as mentioned in ntp.conf file) and make links to the transferred keys as follows:

Format:

ln -s /etc/ntp/ntpkey_host_MTS200 ntpkey_host_username*
ln -s /etc/ntp/ntpkey_cert_MTS200 ntpkey_cert_username*

here, username = should be the username of the ntp client unix or linux host machine

e.g.

ln -s /etc/ntp/ntpkey_host_MTS200 ntpkey_host_ubuntu
ln -s /etc/ntp/ntpkey_cert_MTS200 ntpkey_cert_ubuntu

Step 2: Once, key is transferred to ntp clients and links made as per step1, user should configure ntp client **ntp.conf** file for NTP Autokey PC scheme as explained below.

First, add below lines in **ntp.conf** file.


```
crypto pw password #keys password
keysdir /etc/ntp # directory where autokey is stored
crypto randfile /dev/urandom

server 192.168.100.153 minpoll 6 autokey
```

password = in ntp.conf file is the password used to generate the NTP PC Autokeys in MTS200 device using webserver.

keysdir = is the directory in ntp clients where PC private key and private certificate are stored.

User need to add “autokey” keyword in server address line in ntp.conf which will ensure the ntp communications between MTS200 and ntp client is through PC based Autokey.

	INFORMATION
	<ul style="list-style-type: none">• After changes to NTP Autokey IFF parameters are done, NTP service need to be restarted in ntp client by user.• NTP takes few minutes to get synchronized when using Autokey PC authentication and also depending on time difference between NTP server and NTP client.• NTP client will only sync with NTP server with autokey PC keys only if password and autokey options in ntp.conf file are correct as per server and ntp service at client side is restarted after keys setup done at client side.

- Procedure to transfer Trusted Server MTS200 keys in other MTS200 units:

Step 1: User should transfer the generated key and certificate to PC using secure means such as HTTPS (using download section).

Step 2: Now, Open https communication with MTS200 device which user wants to configure as only Autokey GPS server mode. Remember, this device cannot act as “Trusted Server”


Step 3: Enter the password used to generate the Trusted Server PC keys in password field and then select “Submit Password” option.

Step 4: It is necessary to delete any old NTP autokey files from MTS200 before generating new keys, use option “Remove Old Keys” option.

Step 5: Now, select the option of “Private key” in field “Contents Of” -> copy the contents of “ntpkey_host_MTS200” file in Dialog box -> click “ADD” option.

Similarly, select the option of “Certificate” in field “Contents Of” -> copy the contents of “ntpkey_cert_MTS200” file in Dialog box -> click “ADD” option.

This will copy the contents of keys of Trusted server MTS200 in Server MTS200 Autokey modes.

	INFORMATION
	<p>After changes to NTP Autokey PC parameters are done, NTP service need to be restarted at MTS200 which is acting as server only, in order to changes to be in effect. User can check the configuration by using “show ntp.conf” file option in webserver or option “1” in NTP main menu in console based configuration utility.</p>

Apart from using Webserver mode to transfer the Trusted Server MTS200 PC scheme Autokeys, user can also use SSH mode to accomplish the same as explained below:

Step 1: User should transfer the generated key and certificate to PC using secure means such as SCP. User should avoid using Telnet mode to transfer keys as Telnet in unsecure way for communication.

Step 2: Now take SSH connection of server MTS200 where keys are need to be installed and create the required links for key.

For establishing SSH connection,
ssh root@192.168.100.xxx

Then, remove old autokeys files if any ntp folder,
rm -rf /etc/ntp/ntpkey*

Step 3: Now, transfer the files from trusted server MTS200 to normal server MTS200.

To transfer Trusted Server MTS200 ntp keys using SCP method, user need to take console of MTS200 using SSH (only by super-user or administrative user of MTS200) from server MTS200, mentioned as below commands.

Below example is provided by considering that Trusted Server MTS200 IP address is 192.168.100.153 and server MTS200 IP address is 192.168.100.154.

On Remote Host PC, take the console of trusted server MTS200: **ssh root@192.168.100.153**

Where, root = is the default super-user of trusted server MTS200,
192.168.100.153 = is the IP address of trusted server MTS200 ethernet port

If operator has successfully taken the console session of trusted server MTS200, then user can give below commands to transfer the ntp keys to server MTS200 device.

scp /home/root/ntp/ntpkey_cert_MTS200 root@192.168.100.154:/etc/ntp

scp /home/root/ntp/ntpkey_host_MTS200 root@192.168.100.154:/etc/ntp

scp /home/root/ntp/ntpkey_cert_MTS200 root@192.168.100.154:/home/root/ntp

scp /home/root/ntp/ntpkey_host_MTS200 root@192.168.100.154:/home/root/ntp

Where, user = is the username of remote Host PC where keys are to be transferred,
192.168.100.154 = IP address of Server MTS200 where keys are to be transferred
/etc/ntp = it is the destination folder where ntp keys are copied.
/home/root/ntp = it is the destination folder where ntp keys are copied.

Now, user should close the SSH session with trusted server MTS200, as given below command:


exit

User should avoid using Telnet mode to transfer keys as Telnet in unsecure way for communication.

Step 4: User need to set the crypto password in ntp.conf file. This crypto password should be same as the password used to generate autokey PC keys in MTS200 Trusted Server side.

This can be set by webserver mode in Security page in filed “NTP Autokey Password” and then click on “Submit Password”.

Step 6: Now restart the NTP service using console based configuration utility or webserver.

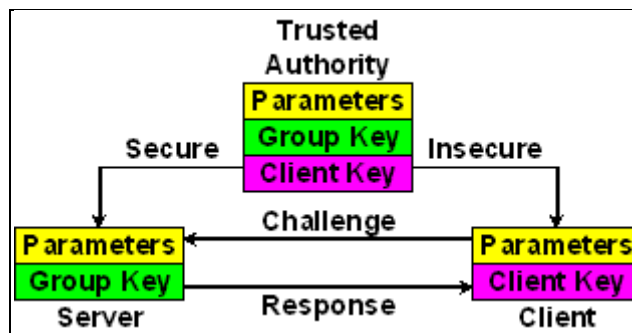
	<p>INFORMATION</p> <ul style="list-style-type: none"> After changes to NTP Autokey PC parameters are done, NTP service need to be restarted in order to changes to be in effect. User can check the configuration by using “show ntp.conf” file option in webserver or option “1” in NTP main menu in console based configuration utility. NTP client will only sync with MTS200 only server when autokey password at MTS200 server is same as autokey password at MTS200 trusted server side.
---	---

11.3.3.4.2.2 NTP Autokey IFF Scheme:

In IFF scheme, there is Trusted Authority (TA) which generated the IFF parameters, private key and public key for IFF based ntp network. User can make MTS200 as TA by using Trusted Server option in webserver and selecting IFF scheme in webserver security page or any one of multiple MTS200 connected in a single network as TA.

Now, the IFF parameters key has to be copied to ntp clients machine using secure means. Without a private key, a client cannot masquerade a TA and hence, could not create threat to TA NTP server response.

Below figure represents the general architecture of NTP IFF TA, server and client keys generation and distribution network.



Using IFF scheme, three types of keys are generated at MTS200 acting as TA. This are Private key, public certificate and IFF parameter file. The IFF parameter key generated by MTS200 acting as TA has to be distributed to all other servers and clients in network and user need to install the soft link in normal ntp server and ntp clients to this TA IFF key file.

After that, user need to generate the IFF private key and public key at each normal NTP server and ntp client using password same or different as used in MTS200 TA unit.

As the IFF parameter key file is independent of keys and certificates, the private and public key at each normal NTP server and NTP clients can be refreshed or recreated as needed.

There will be only one MTS200 device in complete NTP group which will act as Trusted Authority with trusted server functionality. Other MTS200 units in same NTP network will only be acting as trusted server mode.

In below explanation, Group Key in IFF scheme refers to IFF parameter key which should be shared among Trusted NTP servers, NTP servers and NTP clients.

- Procedure to Generate NTP Autokey IFF Scheme keys in MTS200 which will act as Trusted Authority in NTP network:

User can generate Autokey for PC and IFF scheme in MTS200 using webserver only. To generate PC schemes keys, user need to go device webserver page Security, in which NTP Autokey section is provided.

Step 1: Then, user need to select IFF option in field “Identity Scheme” and mark Certificate Type as “Trusted Server”. Autokey IFF scheme need password to be entered for generate private key and private certificate. User need to remember this password to set in ntp client ntp.conf file while starting IFF scheme based ntp associations between server and client.

The screenshot shows the 'NTP Autokey' configuration page. It includes the following elements:

- Identity Scheme:** A dropdown menu set to 'IFF'.
- Certificate Type:** Radio buttons for 'Trusted Server' (selected) and 'Server'.
- NTP Autokey Password:** A text input field with masked characters.
- Re-enter NTP Autokey Password:** A second text input field with masked characters.
- Buttons:** 'Submit Password', 'Generate NTP Autokey', and 'Remove Old Keys'.
- Contents Of:** A dropdown menu with options 'Private Key', 'Private Key', 'Certificate', and 'Group Key'. Below it are 'Add Key' and 'View' buttons.

Figure 11-7 NTP Autokey – IFF Scheme Settings on Webserver

Step 2: After password is entered, click on “Submit Password”. This option will configure the crypto password in MTS200 ntp configuration file automatically. “Generate NTP Autokey” option will only be enable after “Submit Password” is done.

Step 3: Selecting “Generate NTP Autokey” option, it will generate the NTP Autokey IFF scheme private key, private certificate and group key automatically. While the keys are being generated, the background of webserver will be hidden till all keys are generated.

The screenshot shows the 'NTP Autokey' configuration interface. It includes fields for 'Identity Scheme' (set to IFF), 'Certificate Type' (radio buttons for 'Trusted Server' and 'Server'), 'NTP Autokey Password', and 'Re-enter NTP Autokey Password'. There are three buttons: 'Submit Password', 'Generate NTP Autokey', and 'Remove Old Keys'. A 'Contents Of' dropdown is set to 'Private Key'. A modal dialog box is centered on the screen with the text 'PROCESSING. PLEASE WAIT...' and a loading spinner.

Step 4: After required keys are generated, user can check the key contents using “VIEW” option and selecting key type in field “Contents of” as shown in below images.

This screenshot shows the same 'NTP Autokey' configuration page, but now with the 'Contents Of' dropdown set to 'Private Key'. The 'View' button is highlighted. Below the dropdown, a text area displays the generated private key content:

```
# ntpkey_RSAhost_MTS200_2208993935
# Thu Jan 1 01:25:35 1970

-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIBoZA9BqkqhkiG9w0BBQ0wMDAbBgkqhkiG9w0BBQwwDgQI8YOeSOasn0QCAGgA
MBEGBSsOAwIHBAnsValbk3qohQSCAWDs6PJpcCp5FrRuS5qxbEudH2CRRdNzUJVI
19dT48wWwI4WJpqrSx0D/UwafLpBRc4Qjz8KvY6N7M1G2XzNMPF8qga5M7B35kY
40INaEhDasIdS0RjvbejGc0juWTTAlzmm7f9eggSs/SJPHnpwpslR2CfvZYCGx
atvGIQPM93P5qGs9z9KRYm6rY4bE04U985hldoEb3H05aY/SAwRplKpZJq27W1tx
aNej/pYQQGcfoChKuu7q9JwN+TepU4tAQKvsnC2safKkBRw9spio2DvjHgmBHAr
hiGlnYdikEU3HeeAXA5OzplDc18YEQQ8khkpcSpvqnDhHnGD6RpA4BnVeZ3Ww7+V
ErgvQJyG247Zlg6AJ15WU6oZArRcbEZZw3QPfh1s/b1wNf+S95tGR6g2zvBXH8C
ZZdNI/V2ivGq2BISizi45ctGhvgTEvyp5gkMFsg2o+1rTTeFdtC9
-----END ENCRYPTED PRIVATE KEY-----
```

NTP Autokey:

Identity Scheme:

Certificate Type: Trusted Server Server

NTP Autokey Password:

Re-enter NTP Autokey Password:

Contents Of:

```
# ntpkey_RSA-MD5cert_MTS200.2208993935
# Thu Jan 1 01:25:35 1970

-----BEGIN CERTIFICATE-----
MIIBSTCB9KADAgECAGSDqpKpMA0GCSqGSIb3DQEBAUAMBExDzANBgNVBAMTBk1U
UzlwMDAeFw03MDAxMDEwMTI1MzVaFw03MTAxMDEwMTI1MzVaMBExDzANBgNVBAMT
Bk1UzlwMDBaMA0GCSqGSIb3DQEBAQUAA0kAMEYCOQDCcmkhocPynKRJW9VFwN8RR
Ns4U1o2aBxihW68swhGjQ8DTf5HsVsus2+mG2wigpnQyT0j8ngmkb0sbu9B0scX
AgEDoZyWNDAPBgNVHRMBAf8EBTADAQH/MAAsGA1UdDwQEAwIChDAUBgNVHSUEDTAL
BgkrBgEFBQcwAQswDQYJKoZIhvcNAQEEBQADQDDFzNDqVF0B8aGG74agDt38ExyN
s/T8z4bQKGP0bXq9LQwS6iyauhD96SR6EwajFUuSU1UspJ0XnMrpccFuCLU+
-----END CERTIFICATE-----
```

NTP Autokey:

Identity Scheme:

Certificate Type: Trusted Server Server

NTP Autokey Password:

Re-enter NTP Autokey Password:

Contents Of:

```
# ntpkey_IFFkey_MTS200.2208993935
# Thu Jan 1 01:25:35 1970

-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIBEJA9BgkqhkiG9w0BBQ0wMDAbBgkqhkiG9w0BBQwwDgQI4EVNY3jyZ0QCaggA
MBEGBSsOAwHBAi8n7EiISMHhgSB0OdX4bKA0xVAUJ+n7dEOioBQHk4Myicf7u55
14RU+EMTReEfnlssQ1HeSkXpoP2Vw84CTGLMkvK44z8srReXeXND0OlxS1ENp3B
chkAnjhbmoSYzSrDBqjCcs05jQoE2Mfy6EsNO7k53RoFSm2izoZWY+hllMgfdmfMK
MRKsVaGFxzEp00aC5JEdp3ceJqLmLBubb3QP6SUFmmk5oC7Jm8M3e7DJ4v1wo1qX
3kvRfogoAAmdnhGWuxP2Nk2PH0kajo6r9jmAdml5tzLRs3O/W8Q=
-----END ENCRYPTED PRIVATE KEY-----
```

The keys generated in PC scheme in MTS200 are as follows:

IFF Parameter key: "ntpkey_iffkey_MTS200"
 IFF Private key: "ntpkey_host_MTS200"
 IFF Private Certificate: "ntpkey_cert_MTS200"

- Procedure to use IFF Scheme as ntp associations between MTS200 Trusted Authority and ntp clients :

Step 1: User should transfer the generated IFF parameter Group Key from Trusted MTS200 to all other ntp clients using secure means such as SCP or HTTPS (using download section). User should avoid using Telnet mode to transfer keys as Telnet in unsecure way for communication.

Model: MTS200 (1U)

Doc. Ref. no. : m08/om/201

Issue no. : 03

To create IFF private and public key file of ntp client system, first, user should enter the folder (e.g. /etc/ntp/) where ntp keys are needed to be generated using cd command and delete all old ntp autokey files to avoid conflict and confusion with new keys.

Then, give below command to generate ntp client IFF keys.

```
ntp-keygen -H -p cryptopasswd
```

Where, cryptopasswd is the password used to generate the ntp clients keys and same password should be entered in client ntp.conf file as explained in next step.

After Group Key IFF file is transferred from MTS200 trusted server to NTP clients, user need to copy this IFF parameter key in ntp clients keys folder (as mentioned in ntp.conf file) and make links to the transferred group key in ntp client keys folder as follows:

User should now use IFF group key of Trusted Server MTS200 and transfers it to NTP client PC using either webserver method OR SSH method as described below:

TO TRANSFER GROUP KEY (ntpkey_ iffkey_ MTS200) USING WEBSERVER:

Open MTS200 webserver and go to "Security Page" and download "[NTP Autokey IFF Group Key](#)" downloads section in local drive. Now copy this group key in folder where previous keys were generated. i.e. /etc/ntp folder.

Now, at NTP client side, user should enter in folder where ntp client autokey files are generated.

```
cd /etc/ntp
```

and then,

```
In -s /path*/ntpkey_ iffkey_ MTS200 ntpkey_ IFFkey_ username*
```

here, username = is the username of the ntp client unix or linux system

path* = is the path of folder where MTS200 trusted server IFF key is present

e.g.

```
In -s /etc/ntp/ntpkey_ iffkey_ MTS200 ntpkey_ IFFkey_ ubuntu
```

TO TRANSFER GROUP KEY (ntpkey_ iffkey_ MTS200) USING SSH:

On Remote Host PC: **ssh [root@192.168.100.153](#)**

Where, root = is the default super-user of MTS200,
192.168.100.153 = is the IP address of MTS200 ethernet port

If operator has successfully taken the console session of MTS200, then user can give below commands to transfer the ntp keys to remote Host PC.

```
scp /home/root/ntp/ntpkey_ iffkey_ MTS200 user@192.168.100.231:/etc/ntp
```

Where, user = is the username of remote Host PC where keys are to be transferred,
192.168.100.231 = IP address of remote Host PC where keys are to be transferred
/etc/ntp = it is the destination folder where ntp keys are copied. This can be different as per remote Host PC ntp client setup

Now, user should close the SSH session with MTS200, as given below command:

exit

Now, at NTP client side, user should enter in folder where ntp client autokey files are generated.

cd /etc/ntp

and then,

In -s /path*/ntpkey_iffkey_MTS200 ntpkey_iffkey_username*

here, username = is the username of the ntp client unix or linux system
 path* = is the path of folder where MTS200 trusted server IFF key is present

e.g.

In -s /etc/ntp/ntpkey_iffkey_MTS200 ntpkey_iffkey_ubuntu

Step 2: Once, key is transferred to ntp clients and links made as per step1, user should configure ntp client **ntp.conf** file for NTP Autokey IFF scheme as explained below.

First, add below lines in **ntp.conf** file.

```
crypto pw cryptpasswd #keys password
keydir /etc/ntp # directory where autokey is stored
crypto randfile /dev/urandom

server 192.168.100.153 minpoll 6 autokey
```

cryptpasswd = in ntp.conf file is the password used to generate the NTP IFF Autokeys in ntp clients.

keydir = is the directory in ntp clients where all IFF schemes related keys are stored.

User need to add “autokey” keyword in server address line in client ntp.conf which will ensure the ntp communications between MTS200 and ntp client is through IFF based Autokey.



INFORMATION

- User should only transfer IFF group key from MTS200 trusted server to other group members. Other keys of certificate and private key of MTS200 trusted server is not required by other group members.
- After changes to NTP Autokey IFF parameters are done, NTP service need to be restarted at ntp client side by user.
- NTP takes few minutes to get synchronized when using Autokey authentication and also depending on time difference between NTP server and NTP client.
- NTP client will only sync with NTP server with autokey keys only if password and autokey options in ntp.conf file are correct as per server and ntp service at client side is restarted after keys setup done at client side.

- Procedure to transfer Trusted Authority MTS200 IFF key in other MTS200 units:

There will be only one MTS200 device in complete NTP group network which will act as Trusted Authority with trusted server functionality. Other MTS200 units in same NTP network will only be acting as trusted server mode.

Step 1: User should transfer generated IFF parameter Group Key to computer using secure means such as SCP or HTTPS (using download section). User should avoid using Telnet mode to transfer keys as Telnet in unsecure way for communication.

Step 2: Now, Open https communication with MTS200 device which user wants to configure as only Autokey GPS server mode. Remember, this device cannot act as “Trusted Server”.

Step 3: Now select the IFF scheme and Server mode in field “Certificate Type”. Enter the password used to generate the Server IFF keys in password field and then select “Submit Password” option. The password can be different from the MTS200 trusted Server password.


Step 4: Remove any old autokey files by using option “Remove Old keys”.

Step 5: Now, generate ntp client IFF keys using “Generate NTP Autokey” tab. This will only generate IFF private Key and Certificate file only which is particular for this MTS200 server only.

Step 6: Now, open the webserver of MTS200 which is Trusted Server. Select the option of “Group key” in field “Contents Of” -> click “VIEW” option -> copy the contents of “**Group key**” file in Dialog box.

Step 7: Now, open the webserver of MTS200 which is only acting as Server. Select the option of “Group key” in field “Contents Of” -> paste the contents of trusted server group key in Dialog box, then -> click “ADD” option. This will copy the IFF group key of Trusted Server into MTS200 Only Server.

Step 8: Now, Restart NTP Service at normal server MTS200 which is acting as only IFF Server.

	<p>INFORMATION</p> <ul style="list-style-type: none"> • It is necessary to remove OLD keys before generating new autokey keys. • After changes to NTP Autokey IFF parameters are done, NTP service need to be restarted in order to changes to be in effect. User can check the configuration by using “show ntp.conf” file option in webserver or option “1” in NTP main menu in console based configuration utility. • Only IFF Group key need to copied from MTS200 as Trusted Server/Authority to MTS200 as Server. Other keys (private key and certificate) are not required as they are different for all group members in IFF ntp network. • Password used to generate IFF key in MTS200 server and other NTP clients can be different as compare to MTS200 trusted server password.
---	--

Apart from using Webserver mode to transfer the Trusted Server MTS200 IFF parameter key, user can also use SSH mode to accomplish the same as explained below:

Step 1: User should transfer generated IFF parameter Group Key to PC using secure means such as SCP. User should avoid using Telnet mode to transfer keys as Telnet in unsecure way for communication.

Step 2: Now, transfer the files from PC where IFF key is stored to MTS200 where keys are to be installed by below command.

```
scp /path*/ntpkey_iffkey_MTS200 /etc/ntp/ntpkey_iffkey_MTS200
```

where, path is the local folder path where Trusted Server MTS200 keys are stored.

Step 3: Now take SSH connection of MTS200 where keys are need to be installed and create the required links for key.

For establishing SSH connection,
ssh root@192.168.100.153

Then, remove old autokeys files if any ntp folder,
rm -rf /etc/ntp/ntpkey*

Now, create MTS200 server ntp IFF private and public key using below command in ntp keys folder as given below.

```
ntp-keygen -H -p cryptopasswd
```

when, cryptopasswd is the password used to generate the ntp clients keys and same password should be entered in client ntp.conf file as explained in next step.

and then to create link with Trusted server keys, follow below commands.

```
ln -s /etc/ntp/ntpkey_iffkey_MTS200 /etc/ntp/ntpkey_iffkey_MTS200
```

Step 4: Now restart the NTP service using console based configuration utility or webserver.



INFORMATION

- After changes to NTP Autokey IFF parameters are done, NTP service need to be restarted in order to changes to be in effect. User can check the configuration by using “show ntp.conf” file option in webserver or option “1” in NTP main menu in console based configuration utility.
- NTP client will only sync with MTS200 only server when autokey password at MTS200 server is same as autokey password at MTS200 trusted server side.

Model: MTS200 (1U)

Doc. Ref. no. : m08/om/201

Issue no. : 03


11.3.3.5 NTP Service & Status**NTP Service:**

As MTS200 provides many configuration related to NTP operation, user need to restart the ntp service after any change done in ntp configurations. This is required as ntp will not update the changed configuration till service is restarted.

NTP Service in MTS200 can be restarted through front panel keypad or console based configuration utility or webserver.

For restarting NTP through front keypad, refer section 9.1 and through console based configuration utility, refer section 9.2.2.

For restarting ntp service through webserver, refer section 13.4.

	<p>INFORMATION</p> <ul style="list-style-type: none">• Whenever ntp service is started or restarted, the internal system re-configures the gps receiver using ntp driver which takes few seconds for internal clock to synchronize with gps receiver. As a result, whenever ntp is restarted, display seconds update, serial, event and IRIG output may see some jump in output for 3 to 4 seconds.• NTP service cannot be restarted during unlock conditions if local clock in ntp settings is disabled.• When NTP service is stopped, internal clock is running freely on its own clock PPM and is not synchronized with gps receiver. In such conditions, the accuracy of GPS receiver which is higher than internal clock PPM accuracy will not be in effect and all time outputs including NTP will operate on internal Clock PPM which may be around 20 -30 PPM.• Whenever there are modifications in ntp related keys in ntp clients, it is necessary to restart the ntp service in ntp clients for new changes to take effect.
---	--

NTP Status:

MTS200 is capable to generate internal ntp driver status information and the internal clock accuracy statistics. User can check ntp status output through webserver and console based configuration utility. MTS200 is also capable to store the record of ntp statistics for 10 days after which they are auto removed but maintaining the last 10 days records.

In Webserver, NTP Status menu in NTP menu, display all ntp status as well as ntp statistics graph output as shown in below figures.

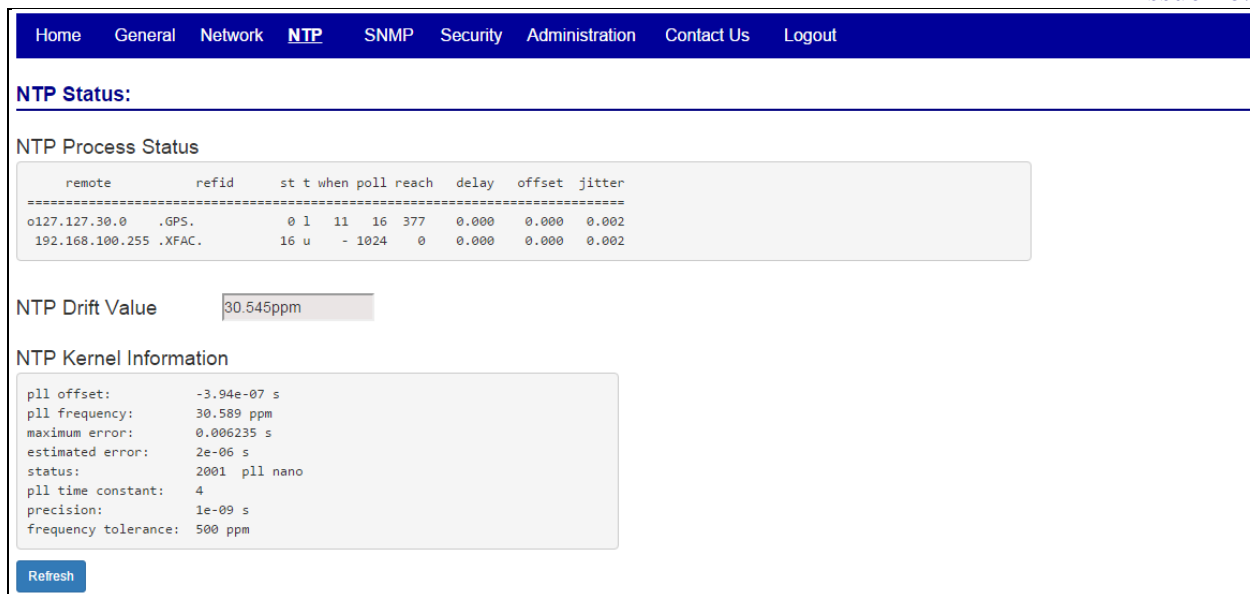


Figure 11-8 NTP Server Status on Webserver

“NTP Process Status” field in above image indicates the output of ntp driver as similar as ntpq -p command output. Below are description of each parameters.

- **remote** = list of all ntp and time servers available as per defined in /etc/ntp.conf file.
- **refid** = reference name as per individual time servers
- **st** = current stratum value of the ntp server
- **when** = seconds since last ntp request
- **poll** = current applicable ntp query poll interval (in seconds) with respective ntp server as per defined in /etc/ntp.conf file.
- **reach** = The value displayed in column reach is octal, and it represents the reachability register. One digit in the range of 0 to 7 represents three bits. The initial value of that register is 0, and after every poll that register is shifted left by one position. If the corresponding time source sent a valid response, the rightmost bit is set.
 During a normal startup the registers values increment in stages as per 0, 1, 3, 7, 17, 37, 77, 177, and 377.
- **delay** = this indicates the delay (In milliseconds) in ntp query and response
- **offset** = time difference (in milliseconds) between client and ntp server.
- **jitter** = variance of time offset (in milliseconds).

“NTP Drift value” shows the current PPM of internal NTP driver in kernel which is syncing with ntp server. This PPM value is not the PPM accuracy of GPS unit as basic MTS200 supplied is with TCXO or optional OCXO based.

“NTP Kernel Information” is the ntp driver output generated by kernel of internal operating system. This output provides more detail information regarding ntp kernel information.

Below image shows the ntp “loopstats” statistics information in graphical format. NTP driver is storing this statistics information each day of normal ntp operation and provides output of same with information of offset, ntp clock PPM at every configured poll interval. Maximum of latest 10 days of statistics files are logged in internal system. The graph shows the ntp offset with server in blue line and ntp clock PPM value with red line both with respect to UTC time in statistics file.

User can check the ntp statistics output of current running date by selecting option “Show Graph of Current date”. As the ntp statistics of current data is not complete, the same time scale will be shown till the data is recorded. If user wants to check the statistics of previous 10 days, user can select the date in field “Date of Logfile” and then “Show Graph” option. Please refer below figure

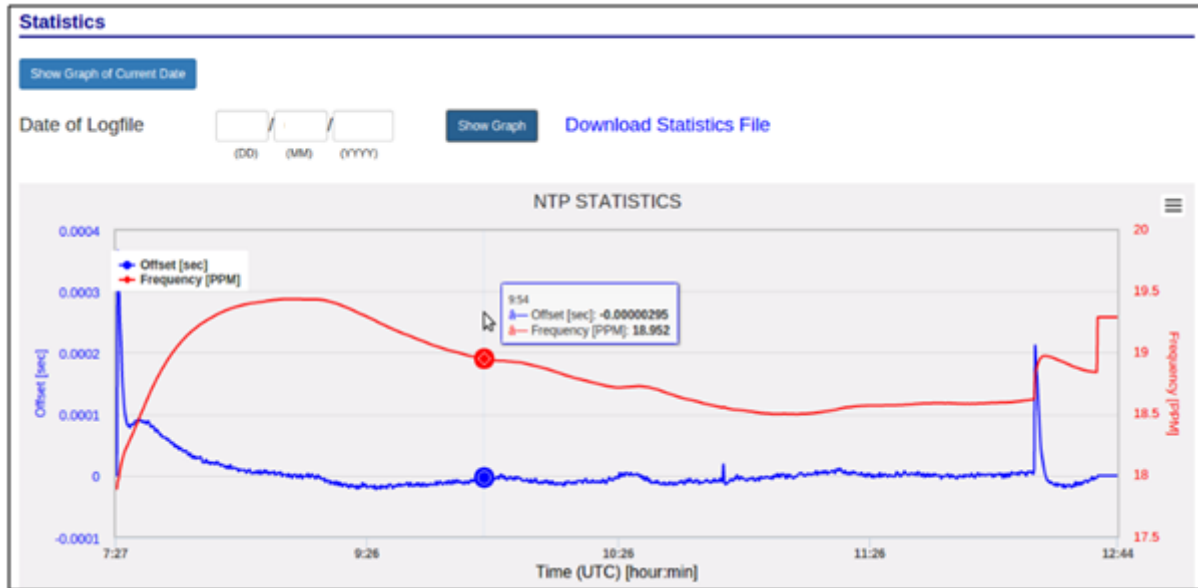
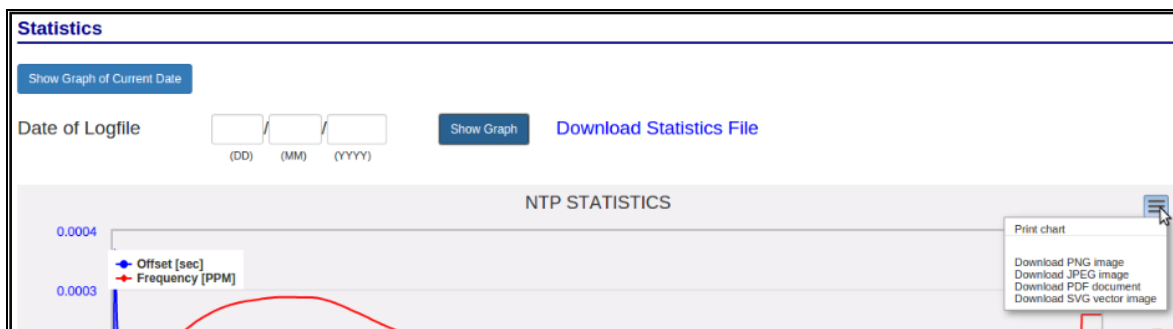


Figure 11-9 NTP Server Statistics plot on Webserver

User can also download the plotted Graph in jpg or png or pdf format by selecting option on right side corner of graph as shown in below figure.



11.3.4 NTP Client Synchronization:

masTER T-Sync Model MTS200 NTP output port can be used to synchronize of Windows PC or Unix/Linux based PC in networks. Please refer **Appendix C** for procedure/settings for making PC to operate as NTP client. It is recommended to visit website www.ntp.org for installing and configuring Unix/Linux based PC as NTP client.

To making Unix/Linux based PC as NTP client with IPv6 address user has to use global Ipv6 address. Add below lines in the respected file

```
server fdc2:7142:77b7:0:1eba:8cff:fee5:c115 minpoll 4 maxpoll 4
```

Note: Link local Ipv6 address cannot be used for NTP time synchronization.

masTER T-Sync Model MTS200 is available with NTP Utility software which can be used to synchronize Windows PC as NTP client device. If NTP Utility software is used, there is no need to do regedit settings in Windows PC for NTP client configuration.

NTP Client time accuracy depends on multiple factors such as Client local clock frequency ppm, network load and congestion, type of clock synchronization algorithm in NTP Client devices other than Unix/Linux PC, hierarchical arrangement of NTP servers and NTP clients in network and *masTER* T-Sync Model MTS200 NTP Clock output accuracy during holdover conditions (when device is Unlock as per ppm of internal clock crystal) etc.

Since NTP client sends NTP request to NTP server at fixed intervals which can be from few seconds to minutes, as during the interval, time of NTP client depends on its own local clock ppm. If there is too much network load and congestion, there is possibility that NTP request as well as NTP responses to and fro from NTP clients to NTP servers can be delayed by significant milliseconds at irregular intervals or NTP packets may be discarded by network (as NTP packet is UDP based transmission packet) since it may cross packet TTL (Time To Live) value in network.

11.3.5 NTP Hierarchical Time Distribution:

NTP architecture model consists of number of primary reference sources, synchronized by wire or radio clock. There are other several multiple secondary time sources/clients which are arranged in hierarchal manner in network which request time from primary reference sources. Under normal circumstances it is intended that the synchronization subnet of primary and secondary servers assumes a hierarchical-master-slave configuration with the primary servers at the root and secondary servers of decreasing accuracy at successive levels toward the leaves.

NTP Server-client architecture are generally arranged in hierarchical arrangement in network. Refer below figure 11.3 to understand time distribution model in hierarchical arrangement.

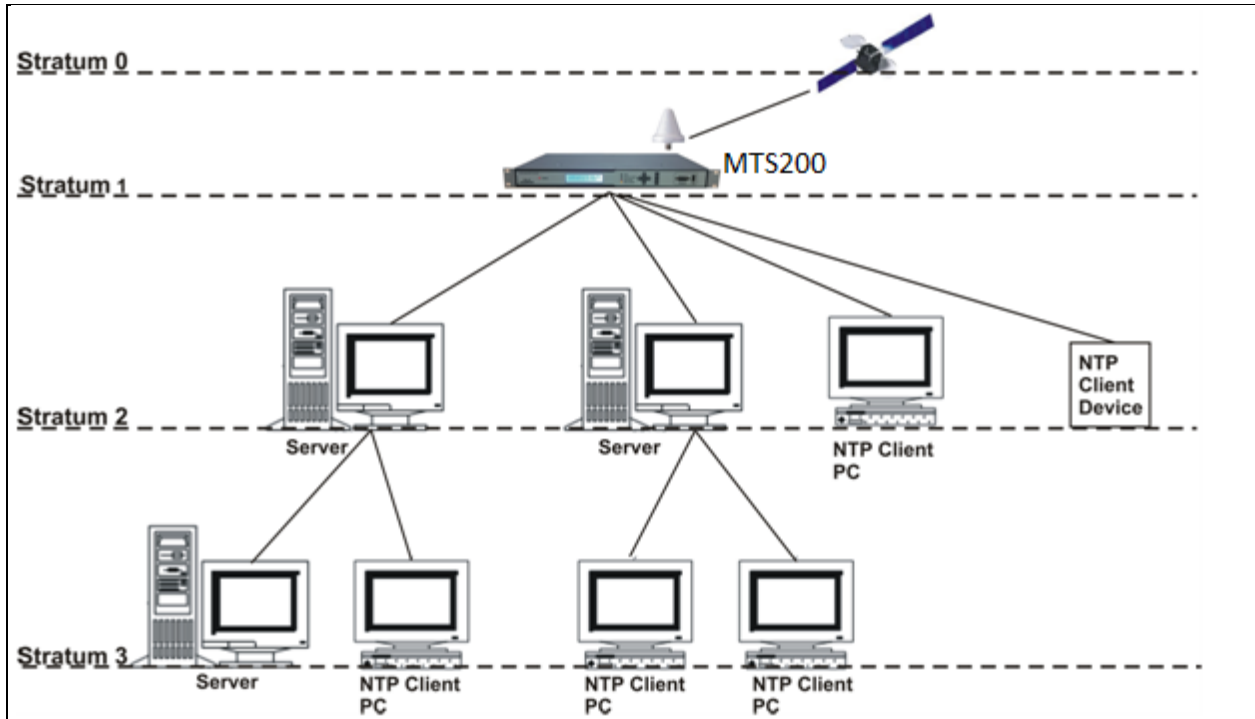



Figure 11-10 NTP Time distributions in Hierarchical Arrangement

As shown in figure 11.3, *masTER* T-Sync receives time form GPS Satellites. According to NTP protocol, GPS satellites are considered to be operating at stratum level 0 as most accurate time source. As the devices passes down to other levels of network architecture, stratum level increases by 1. *masTER* T-Sync MTS200 model operates at stratum level 1 which is considered next accurate time source to GPS Satellites. Other NTP clients stratum level increases by 1 as NTP devices goes downwards in network layers. Stratum level can be upto maximum 14 to be considered as valid NTP time source. NTP client accuracy also depends on the hierarchical arrangement of NTP servers and NTP clients in network because the stratum value increases by 1 at every hierarchical stage in network and as stratum value increases, the accuracy of NTP client decreases depending on the type of NTP server's clock accuracy in hierarchy, processing capabilities of multiple NTP requests and transmission delays.

	<p>FUNCTIONALITY</p> <ul style="list-style-type: none"> • If the stratum level of <i>masTER</i> T-Sync Model MTS200 device is configured at 15 under Unlock conditions, no NTP client will synchronize its time with NTP server output as level 15 is the last limit of stratum as per NTP standard. • Stratum of <i>masTER</i> T-Sync MTS200 under Unlock conditions should be such that last NTP client in hierarchical arrangement should be at stratum level 15 so that can be continuously synchronized with its superior level NTP source device.
	<p>INFORMATION</p> <ul style="list-style-type: none"> • I.P. address of two NTP ports in GPS should not be same if both NTP ports are to be used in same network domain.



- It is recommended that NTP output in network should be used only when once device is Lock after being power UP. If device was in Power OFF condition for very long duration, RTC battery may get discharged and RTC time will reset to its default time. (Please check the applicable battery backup period mentioned in RTC section).

Note:

- I.P. address of two NTP ports in GPS should not be same if both NTP ports are to be used in same network domain.
- Among all applicable NTP parameters in NTP packet format, only stratum value can be modified for Unlock condition only. If NTP output stratum value is configured as 15, all NTP clients in network will continue to ignore NTP output as valid time source.
- As NTP protocol is based on UDP transmission protocol (as UDP is a connectionless protocol as there is no acknowledgment for failed packet delivery), NTP requests from NTP clients to NTP servers and NTP responses from NTP servers to NTP clients can be delayed at irregular intervals or rarely discarded if there too much Ethernet packets load/congestion in network.
- It is recommended that NTP output in network should be used only when once device is Lock after being power UP. If device was in Power OFF condition for very long duration, RTC battery may get discharged and RTC time will reset to its default time. (Please check the applicable battery backup period mentioned in RTC section).
- If unit was Lock for once after being Power UP, it will retain accurate NTP output in holdover conditions (according to its local clock ppm accuracy).
- NTP Client time accuracy depends on multiple factors such as Client local clock frequency ppm, network load and congestion, type of clock synchronization algorithm in NTP Client devices other than Unix/Linux PC, hierarchical arrangement of NTP servers and NTP clients in network and *masTER T-Sync* Model MTS200 NTP Clock output accuracy during holdover conditions (when device is Unlock as per ppm of internal clock crystal) etc.

12 Relay and Pulse Outputs

12.1 Relay Contact Outputs

masTER T-Sync Model MTS200 device is equipped with 3 Relay contact outputs for indication of POWER failure alarm, WATCHDOG alarm and GPS LOCK status alarm on back panel of unit. Factory set configuration for relay contacts for all three mentioned outputs is C-NO terminal. The relay output configuration can be changed to C-NC if required through hardware jumpers only (refer section 7 and 7.1). Below table represents the relay contact status in various modes.

Relay Contact Configuration: C – NO

MODE	Contact on Terminal	POWER RELAY STATUS	WATCHDOG RELAY STATUS	GPS LOST RELAY STATUS
Unit Power OFF	C-NO	Contact Open	Contact Open	Contact Open
At Power ON	C-NO	Contact Close	Contact Close only after 6 seconds once time is displayed on unit Screen	Contact Close (if GPS is LOCK) or Contact Open (if GPS is UNLCOK)
Power fail	C-NO	Contact Open	--	--
Unit Healthy	C-NO	Contact Close	Contact Close	Contact Close (if GPS is LOCK)
GPS LOCK	C-NO	--	--	Contact Close

Relay Contact Configuration: C – NC

MODE	Contact on Terminal	POWER RELAY STATUS	WATCHDOG RELAY STATUS	GPS LOST RELAY STATUS
Unit Power OFF	C-NC	Contact Close	Contact Close	Contact Close
At Power ON	C-NC	Contact Open	Contact Close but Contact Open only after 6 seconds once time is displayed on unit Screen	Contact Close (if GPS is UNLOCK) or Contact Open (if GPS is LCOK)
Power fail	C-NC	Contact Close	--	--
Unit Healthy	C-NC	Contact Open	Contact Open	Contact Open (if GPS is LOCK)
GPS LOCK	C-NC	--	--	Contact Open

Table 12-1 Relay Contact Status Chart during Operation

12.2 Pulse Outputs

12.2.1 1PPS Output

masTER T-Sync Model MTS200 device provides 1PPS output at every 1 second through its BNC terminal on rear panel of unit. This is TTL signal of 0(low level) to 5V (high level) value. The Pulse width of 1PPS signal is 20% duty cycle i.e. 200 milliseconds (high level) and 800 milliseconds (low level).

12.2.2 Event Output (PPM/PPH)

masTER T-Sync Model MTS200 device is equipped with the standard feature of providing event output at every PPM (Pulse per Minute) / PPH (Pulse per Hour) with fix pulse width of 1 second. This event provides pulse output according to configured time interval i.e. Minute / Hour through front panel keypad or console based configuration utility or webserver or snmp. Please refer section 9 for method of configure standard event output through console based configuration utility and to configure through keypad on device or section 13.3 for snmp or section 13.4 for webserver. Refer technical specification section 4 for electrical characteristics of event output.

12.2.3 Additional Event Outputs (Programmable Pulse Outputs)

masTER T-Sync Model MTS200 device is equipped with the (optional) feature of providing 1 to 4 additional event outputs. These events provide pulse output according to configured time interval and ON time. Each event time can be configured with time interval ranging from 1 sec to 86400 seconds and pulse ON time (pulse width) from min. 50 milliseconds to max. 50% of configure time interval of that particular event in terms of milliseconds through front panel keypad or console based configuration utility or webserver or snmp. Please refer section 9 for method of configure additional event outputs through console based configuration utility and keypad or section 13.3 for snmp or section 13.4 for webserver on device. Refer technical specification section 4 for electrical characteristics of additional event outputs.

13 Ethernet Communications: Telnet, SNMP

13.1 Telnet

Telnet is a session layer protocol to provide bilateral communication using command line interface with remote host. MTS200 support telnet protocol (PORT: 23) for its own configuration of device. User can connect with MTS200 device using telnet command from windows or unix/linux based systems.

For windows based PC/Server, user need to go command prompt by typing “cmd” in run mode and then give command: **telnet 192.168.100.121**. When telnet communication is established, MTS200 console port will prompt.

Now, once user has accessed MTS200 console through Telnet, user can run console based configuration utility program “start” as explained in section 9.2.

User can also use software “putty” software for windows based system. Select “telnet” in “connection type” field and enter MTS200 IP address in “Host name” field and then click on “Open”. This will start telnet communication with MTS200.

After, user finished MTS200 configuration over telnet, user should close the telnet session by giving command “exit” on MTS200 console. This will close telnet session with MTS200. This is necessary to prevent unauthorized access to device because if telnet session is not closed, user who is not authorized can take access and change the device configurations without the knowledge of operator.



- It is recommended to avoid using telnet communication with MTS200 because it is very unsecure protocol as it is transmitting username and password as simple texts over net.
- It is always recommended to use SSH instead of Telnet as SSH is very high secured protocol.

13.2 SSH

SSH is a secure protocol to provide bilateral communication using command line interface with remote host. MTS200 support SSH protocol (PORT: 22) for its own configuration of device. User can connect with MTS200 device using ssh command from windows or unix/linux based systems.

MTS200 supports ssh v1 and sshv2 communication. SSHv1 security uses RSA key of size 768 bits / 1024 bits / 2048 bits while SSHv2 security uses DSA of 1024 bits (fixed) and RSA key of size 768 bits / 1024 bits / 2048 bits. The RSA key sized can be configured using console based configuration utility program as explained in section 9.2 or webserver as explained in section 13.4. It is recommended to use RSA key of size 2048 bits as it provides maximum level of security as compare to 768 and 1024 bits key size.

For windows based PC/Server, User need to use software “putty” software for windows based system. Select “ssh” in “connection type” field and enter MTS200 IP address in “Host name” field and then click on “Open”. This will start ssh Session with MTS200.

For Unix/Linux based system, open terminal and then follow below command:

Command: ssh root@192.168.100.121

Now, once user has accessed MTS200 console through ssh, user can run console based configuration utility program “start” as explained in section 9.2.

After, user finished MTS200 configuration over ssh, user should close the ssh session by giving command “exit” on MTS200 console. This will close ssh session with MTS200. This is necessary to prevent unauthorized access to device because if ssh session is not closed, user who is not authorized can take access and change the device configurations without the knowledge of operator.

13.3 SNMP

SNMP protocol is capable of managing multiple network devices remotely via devices configuration and its monitoring. SNMP communication is operated on application layer in network devices. SNMP architecture mostly resembles server-client architecture as SNMP devices are configured as either SNMP Manager or SNMP agent device. SNMP Manager can configure as well as monitor SNMP agent as per configured parameter in SNMP MIB files. MIB (Management Information Base) files are the configuration files which contain details about variables (identified as OID-object identifiers) which can be configured and monitored by SNMP Manager in SNMP agent device. SNMP protocol also provides the flexibility to send the alarms as SNMP traps from SNMP agent to the configured SNMP Manager.

masTER T-Sync device act as SNMP agent and support SNMP version 1, 2 and 3 for its configuration and monitoring of run time variables. Also, it can send SNMP traps in mentioned versions to configured SNMP managers. It is capable to handle single or multiple variables walk, get or set requests. It also provides the flexibility to configure max. 2 SNMP managers each in either of version with read / read-write options. It has its own customized MIB database for variables allowed to be configured in device.

The elements (objects / variables) are organized in data structures called Management Information Base (MIB).The agent is also responsible for controlling the database of control variables defined in the product's MIB.

13.3.1 SNMP Addressing:

SNMP addressing is structured as a very large tree database. A root node address is an integer value that ranges from 0 to some very large number. Conceptually, there are no limits to the numbers of sub nodes either. SNMP addressing is written in “dotted decimal” notation. For example, the address of *masTER* T-Sync model MTS200 product name Enterprise MIB variable is “1.3.6.1.4.1.38306.1.1.0”, this is also known as OID (Object Identifier). The address fragment 1.3.6.1.4.1 is fixed by the IANA (Internet Assigned Number Authority) and is the address of the SNMP Private Enterprise MIB's. The 38306 is the address assigned by IANA to *masibus* for our Enterprise MIB's. *masibus* assigns the addresses after that at our discretion and design.

13.3.2 Protocol Detail:

SNMP operates in the Application Layer of the Internet Protocol Suite. The manager may send requests from any available source port to port 161 to the agent. The agent will response back to the manager address on port 162. The manager receives notifications (Traps and Inform-Requests) on port 162. SNMPv1 specifies five core protocol data units (PDUs). Two other PDUs, Get-Bulk-Request, and Inform-Request were added in SNMPv2. The seven SNMP protocol data units (PDUs) are as follows:

- i) **GET-Request:** This PDU is used to get the values of a list of variables from a particular host.
- ii) **Get-Next-Request:** This PDU is used to Get the next value for multi-valued data-items (for example the entries in a routing table). The manager specifies one or more variables for value, and the agent returns the current value for each of the requested variables.
- iii) **Set-Request:** This PDU is used to set the values of a list of variables for a particular host.
- iv) **Get-Bulk-Request:** This PDU is optimized version of Get-Next-Request, used to request multiple iteration of Get-Next-Request. It allows the caller to specify – non-repeaters, range of variables which are single valued, max-repetition, no of values to be returned by the call.

Model: MTS200 (1U)

Doc. Ref. no. : m08/om/201

Issue no. : 03

- v) **Response:** Agent returns this PDU in response to above all PDUs. It contains the requested data items along with a result code.
- vi) **Trap:** This PDU is quite different from other PDUs. Agent generates it in response to particular important events. An agent only at the request of an SNMP manager application generates a trap PDU.
- vii) **Inform-Request:** This PDU introduces a new pattern of communication (Manager to Manager communication). In manager to manager communication, one manager sends information from a MIB view to another manager.

13.3.3 SNMP Operation:

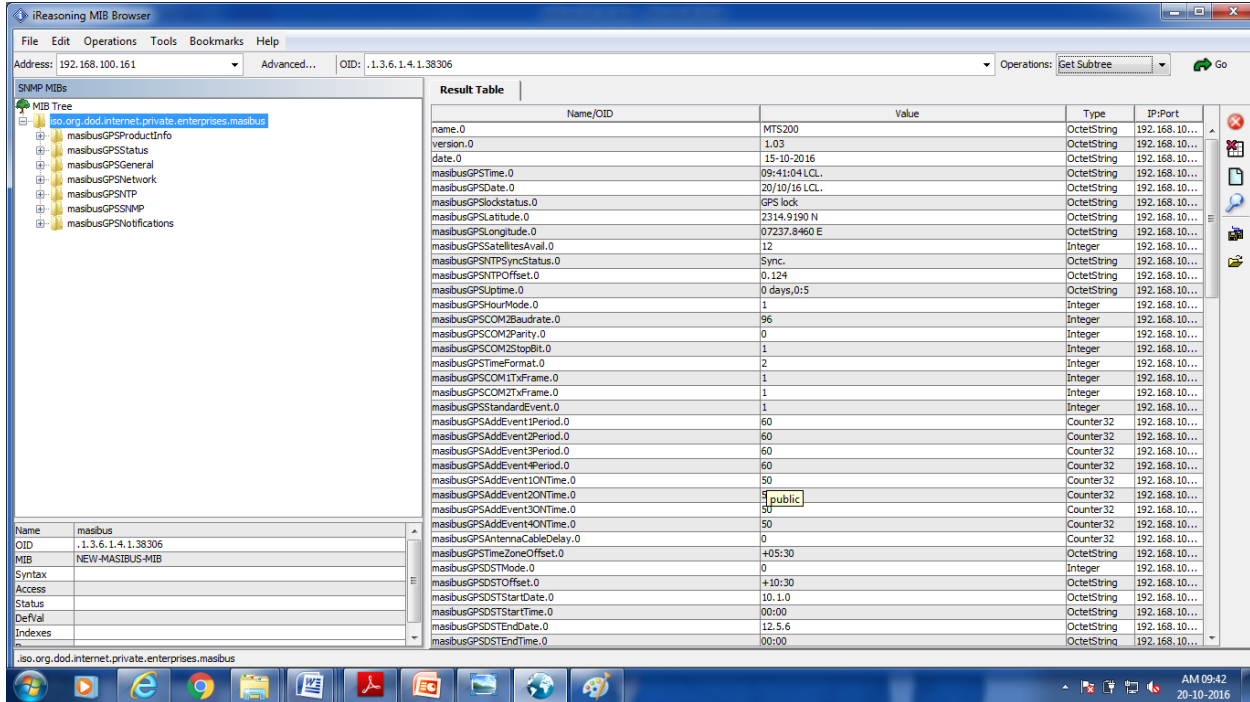
Below are few details about SNMP package installed in *masTER* T-Sync device:

SNMP Versions Supported:	1 2c 3
Net-SNMP Version:	5.7.2.1
Network transport support:	Callback Unix Alias TCP UDP IPv4Base TCPBase UDPIPV4Base UDPBase
SNMPv3 Security Modules:	usm
Agent MIB code:	masibusGPSProductInfo, masibusGPSStatus, masibusGPSGeneral, masibusGPSNTP, masibusGPSNetwork, masibusGPSSNMP, masibusGPSNotifications, default_modules, snmpv3mibs, mibII, ucd_snmp, agent_mibs, agentx utilities
Authentication support:	MD5, SHA1
Encryption support:	DES, AES

For this device to work as SNMP agent in network device, it is necessary that SNMP service should be active/ON and SNMP manager1 and SNMP manager2 parameters to be actively configured in device. SNMP service can be started through front keypad or SSH/Telnet application program or webserver.

SNMP Manger can read all variables applicable in MIB files of this device with below given single command from linux/unix based systems or from SNMP graphical based management software such as MIB Browser or others on windows or unix based platform.

To get/walk variables from *masTER* T-Sync using SNMP MIB Browser software:



To get/walk variables from *masTER* T-Sync on unix/linux based SNMP Manger systems:

Command for SNMP v1

1. snmpwalk -v 1 -c public 192.168.100.121 .1.3.6.1.4.1.38306 on IPv4
2. snmpwalk -v 1 -c public udp6:[fdc2:7142:77b7:0:1eba:8cff:fee5:bb52] .1.3.6.1.4.1.38306 on IPv6
3. snmpwalk -v 1 -c public udp6:[fe80::1eba:8cff:fee5:bb52] .1.3.6.1.4.1.38306 on IPv6

Command for SNMP v2

1. snmpwalk -v 2c -c public 192.168.100.121 .1.3.6.1.4.1.38306
2. snmpwalk -v 2c -c public udp6:[fdc2:7142:77b7:0:1eba:8cff:fee5:bb52] .1.3.6.1.4.1.38306 on IPv6
3. snmpwalk -v 2c -c public udp6:[fe80::1eba:8cff:fee5:bb52] .1.3.6.1.4.1.38306 on IPv6

Command for SNMP v3

1. snmpwalk -v 3 -n "" -u usernamesnmpv33333 -l authPriv -a MD5 -A passphrase222 -x DES -X passphrase222 -e 0x123456789123456789 192.168.100.162 .1.3.6.1.4.1.38306
2. snmpwalk -v 3 -n "" -u usernamesnmpv33333 -l authPriv -a MD5 -A passphrase222 -x DES -X passphrase222 -e 0x123456789123456789 udp6:[fdc2:7142:77b7:0:1eba:8cff:fee5:bb52] .1.3.6.1.4.1.38306
3. snmpwalk -v 3 -n "" -u usernamesnmpv33333 -l authPriv -a MD5 -A passphrase222 -x DES -X passphrase222 -e 0x123456789123456789 udp6:[fe80::1eba:8cff:fee5:bb52].1.3.6.1.4.1.38306

Note: Help regarding possible options applicable for snmpwalk and other snmp related commands and their explanation can be found on <http://net-snmp.sourceforge.net/wiki/index.php/Tutorials> or <http://net-snmp.sourceforge.net/tutorial/tutorial-5/> or <http://net-snmp.sourceforge.net> webpage.

Response from *masTER* T-Sync for above query is given below: (Note this is the truncated output of complete data for only easy understanding of response)

```

iso.3.6.1.4.1.38306.2.1.0 = STRING: "16:58:19"
iso.3.6.1.4.1.38306.2.2.0 = STRING: "19/09/15"
iso.3.6.1.4.1.38306.2.3.0 = STRING: "GPS lock"
iso.3.6.1.4.1.38306.2.4.0 = STRING: "2314.9194 N"
iso.3.6.1.4.1.38306.2.5.0 = STRING: "07237.8437 E"
iso.3.6.1.4.1.38306.2.6.0 = INTEGER: 11
iso.3.6.1.4.1.38306.2.7.0 = STRING: "Sync."
iso.3.6.1.4.1.38306.2.8.0 = STRING: "0.000"
iso.3.6.1.4.1.38306.2.9.0 = STRING: "0 days,1:43"
.
.
.
.
.
.
iso.3.6.1.4.1.38306.6.11.0 = STRING: "DES"
iso.3.6.1.4.1.38306.6.12.0 = STRING: "passphrase1"
iso.3.6.1.4.1.38306.6.13.0 = STRING: "192.168.100.231"
iso.3.6.1.4.1.38306.6.14.0 = INTEGER: 3
iso.3.6.1.4.1.38306.6.15.0 = STRING: "allreadwrite"
iso.3.6.1.4.1.38306.6.16.0 = STRING: "rw"
iso.3.6.1.4.1.38306.6.17.0 = INTEGER: 1
iso.3.6.1.4.1.38306.6.18.0 = STRING: "trapcommunity2"
iso.3.6.1.4.1.38306.6.19.0 = STRING: "username SNMPv33333"
iso.3.6.1.4.1.38306.6.20.0 = STRING: "0x123456789123456789"
iso.3.6.1.4.1.38306.6.21.0 = STRING: "MD5"
iso.3.6.1.4.1.38306.6.22.0 = STRING: "passphrase222"
iso.3.6.1.4.1.38306.6.23.0 = STRING: "DES"
iso.3.6.1.4.1.38306.6.24.0 = STRING: "passphrase222"
iso.3.6.1.4.1.38306.6.25.0 = STRING: "masibus"
iso.3.6.1.4.1.38306.6.26.0 = STRING: "Sector"
iso.3.6.1.4.1.38306.6.27.0 = INTEGER: 0
  
```

masTER T-Sync device can be configured by multiple modes such as front panel keypad, SSH, Telnet, HTTP/HTTPS and SNMP Managers. This device provides the flexibility to configure both SNMP managers in read-only mode or read-write mode or read/read-write access with public community. Public community makes it possible for multiple SNMP managers to configure *masTER* T-Sync. SNMP managers need to copy *masTER* T-Sync customized MIB in their respective mib folder before running any snmp operation on this agent device.

SNMP variables in *masTER* T-Sync can be configured using respective variable OID address using snmpset command from unix/linux based systems. Also, some graphical based SNMP manager software such as MIB Browser allows menu based options for configuring SNMP agent variables. Refer below examples for configuring using snmpset command.

FOR SNMP v1:

To set single integer variable with IPv4:

```
user@ubuntu:~$ snmpset -v 1 -c comm_name 192.168.100.121 .1.3.6.1.4.1.38306.3.1.0 i 1
```

To set single integer variable with IPv6 Link-local:

```
user@ubuntu:~$ snmpset -v 1 -c comm_name udp6:[fe80::1eba:8cff:fee5:bb52] .1.3.6.1.4.1.38306.3.1.0 i 1
```


To set single string variable:

```
user@ubuntu:~$ snmpset -v 1 -c comm_name 192.168.100.121 .1.3.6.1.4.1.38306.6.25.0 s "masibus"
```

To set multiple variables:

```
user@ubuntu:~$ snmpset -v 1 -c comm_name 192.168.100.121 .1.3.6.1.4.1.38306.6.25.0 s "masibus" .1.3.6.1.4.1.38306.6.26.0 s "gandhinagar"
```

Note: In above snmpset command, “-c comm_name” indicates that –c option is used to provide SNMP v1 community name in *masTER T-Sync* device, 192.168.100.121 is the SNMP agent IP address, .1.3.6.1.4.1.38306.6.25.0 is the OID of the agent variable which is to be configured, s indicates string and i indicated integer depending on variable data type, “masibus” indicated value of OID in string format. User can use IPv6 address to set string variable as well as multiple variables.

FOR SNMP v2:

To set single integer variable:

```
user@ubuntu:~$ snmpset -v 2c -c comm_name 192.168.100.121 .1.3.6.1.4.1.38306.3.1.0 i 1
```

```
user@ubuntu:~$ snmpset -v 2c -c comm_name udp6:[fe80::1eba:8cff:fee5:bb52] .1.3.6.1.4.1.38306.3.1.0 i 1
```

```
user@ubuntu:~$ snmpset -v 2c -c comm_name udp6:[fdc2:7142:77b7:0:1eba:8cff:fee5:bb52] .1.3.6.1.4.1.38306.3.1.0 i 1
```

To set single string variable:

```
user@ubuntu:~$ snmpset -v 2c -c comm_name 192.168.100.121 .1.3.6.1.4.1.38306.6.25.0 s "masibus"
```

To set multiple variables:

```
user@ubuntu:~$ snmpset -v 2c -c comm_name 192.168.100.121 .1.3.6.1.4.1.38306.6.25.0 s "masibus" .1.3.6.1.4.1.38306.6.26.0 s "gandhinagar"
```

Note: In above snmpset command, “-c comm_name” indicates that –c option is used to provide SNMP v1 community name in *masTER T-Sync* device, 192.168.100.121 is the SNMP agent IP address, .1.3.6.1.4.1.38306.6.25.0 is the OID of the agent variable which is to be configured, s indicates string and i indicated integer depending on variable data type, “masibus” indicated value of OID in string format. User can use IPv6 address to set string variable as well as multiple variables.

FOR SNMP v3 [for authPriv case]:

To set single integer variable:

```
user@ubuntu:~$ snmpset -v 3 -n "" -u usernamesnmp -l authPriv -a MD5 -A passphrase -x DES -X passphrase -e 0x12345678912345 192.168.100.121 .1.3.6.1.4.1.38306.3.1.0 i 2
```

```
user@ubuntu:~$ snmpset -v 3 -n "" -u usernamesnmp -l authPriv -a MD5 -A passphrase -x DES -X passphrase -e 0x12345678912345 udp6:[fdc2:7142:77b7:0:1eba:8cff:fee5:bb52] .1.3.6.1.4.1.38306.3.1.0 i 2
```

```
user@ubuntu:~$ snmpset -v 3 -n "" -u usernamesnmp -l authPriv -a MD5 -A passphrase -x DES -X passphrase -e 0x12345678912345 udp6:[fe80::1eba:8cff:fee5:bb52] .1.3.6.1.4.1.38306.3.1.0 i 2
```

Model: MTS200 (1U)

Doc. Ref. no. : m08/om/201

Issue no. : 03

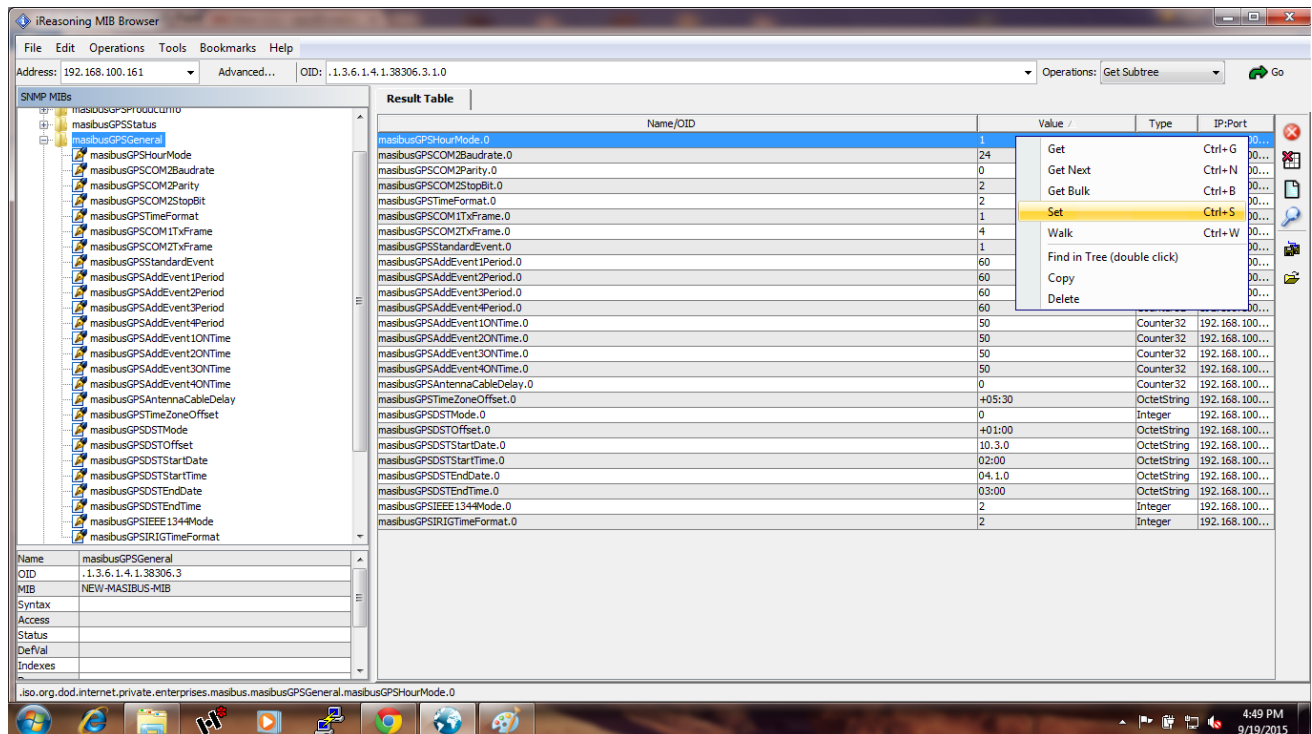
To set single string variable:

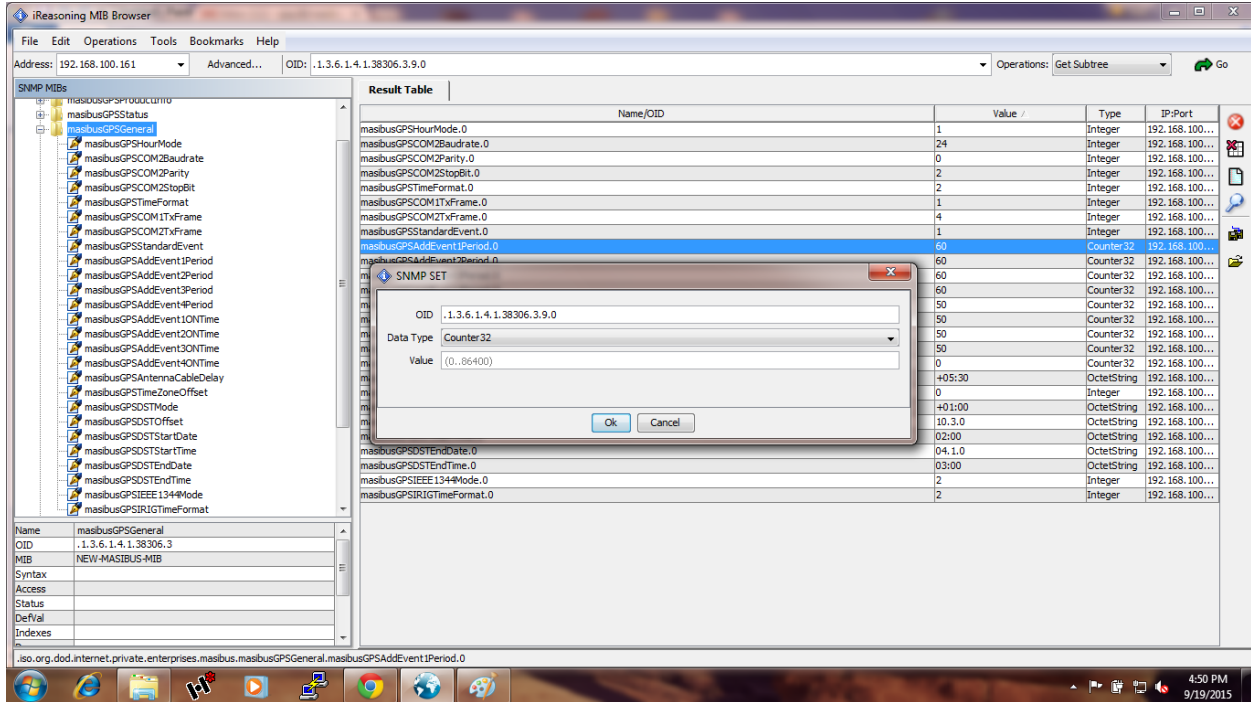
```
user@ubuntu:~$ snmpset -v 3 -n "" -u usernamesnmp -l authPriv -a MD5 -A passphrase -x DES -X passphrase -e 0x12345678912345 192.168.100.121 .1.3.6.1.4.1.38306.6.25.0 s "masibus"
```

To set multiple variables:

```
user@ubuntu:~$ snmpset -v 3 -n "" -u usernamesnmpv33333 -l authPriv -a MD5 -A passphrase222 -x DES -X passphrase222 -e 0x123456789123456789 192.168.100.121 .1.3.6.1.4.1.38306.6.25.0 s "masibus" .1.3.6.1.4.1.38306.6.26.0 s "Gujarat"
```

Using MIB Browser software:





OID of masTER T-Sync device is 1.3.6.1.4.1.38306.

masTER T-Sync SNMP Main branches are given below:

Branch	OID	Description
masibusGPSProductInfo	.1.3.6.1.4.1.38306.1	Device basic Information
masibusGPSStatus	.1.3.6.1.4.1.38306.2	Status of run time device parameters
masibusGPSGeneral	.1.3.6.1.4.1.38306.3	GPS general parameters
masibusGPSNetwork	.1.3.6.1.4.1.38306.4	GPS ethx network and services settings
masibusGPSNTP	.1.3.6.1.4.1.38306.5	NTP related parameters
masibusGPSSNMP	.1.3.6.1.4.1.38306.6	SNMP related parameters
masibusGPSNotifications	.1.3.6.1.4.1.38306.7	SNMP Trap parameters

Below are descriptions of MTS200 SNMP MIB variables.

SNMP Branch : masibusGPSProductInfo

Variable	OID	Data Type [read/write]	Description [Values]
name	.1.3.6.1.4.1.38306.1.1.0	String [read only]	GPS Timeserver identification name
version	.1.3.6.1.4.1.38306.1.2.0	String [read only]	Software Version
date	.1.3.6.1.4.1.38306.1.3.0	String [read only]	Software Version Date

SNMP Branch : masibusGPSStatus

Variable	OID	Data Type [read/write]	Description [Values]
masibusGPSTime	.1.3.6.1.4.1.38306.2.1.0	String [read only]	Current Device display time (will be according to system)

			configurations) [format: minute:hour:seconds]
masibusGPSDate	.1.3.6.1.4.1.38306.2.2.0	String [read only]	Current Device display Date (will be according to system configurations) [format: dd/mm/yyyy]
masibusGPSlockstatus	.1.3.6.1.4.1.38306.2.3.0	String [read only]	Unit LOCK / UNLOCK status [GPS LOCK / GPS UNLOCK]
masibusGPSLatitude	.1.3.6.1.4.1.38306.2.4.0	String [read only]	Current Latitude position of unit in LOCK condition and last Latitude position of unit in UNLOCK condition
masibusGPSLongitude	.1.3.6.1.4.1.38306.2.5.0	String [read only]	Current longitude position of unit in LOCK condition and last longitude position of unit in UNLOCK condition
masibusGPSSatellitesAvail	.1.3.6.1.4.1.38306.2.6.0	String [read only]	Current satellites available
masibusGPSNTPSyncStatus	.1.3.6.1.4.1.38306.2.7.0	String [read only]	System Clock synchronization status with GPS receiver using ntp daemon. [SYNC . / NOT SYNC.]
masibusGPSNTPOffset	.1.3.6.1.4.1.38306.2.8.0	String [read only]	Internal system clock offset with respect to GPS receiver. Units in milliseconds.
masibusGPSUptime	.1.3.6.1.4.1.38306.2.9.0	String [read only]	Duration since the device is Power up.

SNMP Branch : masibusGPSGeneral

Variable	OID	Data Type [read/write]	Description [Values]
masibusGPSHourMode	.1.3.6.1.4.1.38306.3.1.0	Integer [read-write]	Hour Mode [1 / 2] Note: 12 / 24 hour mode resp
masibusGPSCOM2Baudrate	.1.3.6.1.4.1.38306.3.2.0	Integer [read-write]	COM2 port Baud rate [12 / 24 / 48 / 96 / 19] Note: 1200 / 2400 / 4800 / 9600 / 19200 baud rate resp.
masibusGPSCOM2Parity	.1.3.6.1.4.1.38306.3.3.0	Integer [read-write]	COM2 port parity bit [0 / 1 / 2] Note: none / odd / even parity value set
masibusGPSCOM2StopBit	.1.3.6.1.4.1.38306.3.4.0	Integer [read-write]	COM2 port Stop bit [1 / 2] Note: 1 / 2 stop bit
masibusGPSTimeFormat	.1.3.6.1.4.1.38306.3.5.0	Integer	COM2 port serial time format

		[read-write]	[1 / 2] Note: 1 = utc / 2 = local time
masibusGPSCOM1TxFrame	.1.3.6.1.4.1.38306.3.6.0	Integer [read-write]	COM1 port serial time string type [1] Note: fix value
masibusGPSCOM2TxFrame	.1.3.6.1.4.1.38306.3.7.0	Integer [read-write]	COM2 port serial time string type [1 / 2 / 3 / 4] Note: 1=ngts / 2=tformat / 3=GPZDA / 4=GPGGA string
masibusGPSStandardEvent	.1.3.6.1.4.1.38306.3.8.0	Integer [read-write]	PPM/PPH standard pulse output [1 / 2] Note: 1=PPM / 2=PPH
masibusGPSAddEvent1Period	.1.3.6.1.4.1.38306.3.9.0	Integer [read-write]	Additional Event1 pulse total time output in seconds. [0 to 86400]
masibusGPSAddEvent2Period	.1.3.6.1.4.1.38306.3.10.0	Integer [read-write]	Additional Event2 pulse total time output in seconds. [0 to 86400]
masibusGPSAddEvent3Period	.1.3.6.1.4.1.38306.3.11.0	Integer [read-write]	Additional Event3 pulse total time output in seconds. [0 to 86400]
masibusGPSAddEvent4Period	.1.3.6.1.4.1.38306.3.12.0	Integer [read-write]	Additional Event4 pulse total time output in seconds. [0 to 86400]
masibusGPSAddEvent1ONTime	.1.3.6.1.4.1.38306.3.13.0	Integer [read-write]	Additional Event1 pulse duty cycle in milliseconds. [50 to 4320000]
masibusGPSAddEvent2ONTime	.1.3.6.1.4.1.38306.3.14.0	Integer [read-write]	Additional Event2 pulse duty cycle in milliseconds. [50 to 4320000]
masibusGPSAddEvent3ONTime	.1.3.6.1.4.1.38306.3.15.0	Integer [read-write]	Additional Event3 pulse duty cycle in milliseconds. [50 to 4320000]
masibusGPSAddEvent4ONTime	.1.3.6.1.4.1.38306.3.16.0	Integer [read-write]	Additional Event4 pulse duty cycle in milliseconds. [50 to 4320000]
masibusGPSAntennaCableDelay	.1.3.6.1.4.1.38306.3.17.0	Integer [read-write]	GPS receiver antenna cable compensation in nanoseconds [0 to 99999]
masibusGPSTimeZoneOffset	.1.3.6.1.4.1.38306.3.18.0	string [read-write]	Time zone w.r.t. UTC time. Max chars: 7 Format: +/-hr:min Note: hr: 0 to 12, min: 0 to 59 e.g.: +05:30
masibusGPSDSTMode	.1.3.6.1.4.1.38306.3.19.0	Integer [read-write]	DST Mode ON or OFF [0 / 1] Note: 0=OFF, 1=ON
masibusGPSDSTOffset	.1.3.6.1.4.1.38306.3.20.0	string [read-write]	DST offset w.r.t. UTC time. Max chars: 7 Format: +/-hr:min Note: hr: 0 to 12, min: 0 to 59

masibusGPSDSTStartDate	.1.3.6.1.4.1.38306.3.21.0	string [read-write]	e.g.: +05:30 DST start date Max chars: 7 Format: mm.w.d Mm(month): 01 <= mm <= 12, w(week): 1 to 5, D(day of week): 0 to 6 Day 0 is a Sunday. e.g.:05.2.4 as Thursday of 2 nd week of May month.
masibusGPSDSTStartTime	.1.3.6.1.4.1.38306.3.22.0	string [read-write]	DST start time on start date Max chars: 6 Format: hr:min Hr: 0 to12 Min: 0 to 59 e.g. 06:30
masibusGPSDSTEndDate	.1.3.6.1.4.1.38306.3.23.0	string [read-write]	DST end date Max chars: 7 Format: mm.w.d Mm(month): 01 <= mm <= 12, w(week): 1 to 5, D(day of week): 0 to 6 Day 0 is a Sunday. e.g.:05.2.4 as Thursday of 2 nd week of May month.
masibusGPSDSTEndTime	.1.3.6.1.4.1.38306.3.24.0	string [read-write]	DST end time on end date Max chars: 6 Format: hr:min Hr: 0 to12 Min: 0 to 59 e.g. 06:30
masibusGPSIEEE1344Mode	.1.3.6.1.4.1.38306.3.25.0	Integer [read-write]	Selection for IRIG-B or IEEE1344 output on BNC ports [1 / 2] Note: 1=IRIG-B / 2=IEEE1344
masibusGPSIRIGTimeFormat	.1.3.6.1.4.1.38306.3.26.0	Integer [read-write]	Selection of UTC or local time in IRIG/IEEE1344 output [1 / 2] Note: 1=UTC / 2=local time

SNMP Branch : masibusGPSNetwork

Variable	OID	Data Type [read/write]	Description [Values]
masibusGPSEth0v4DHCP	.1.3.6.1.4.1.38306.4.1.0	Integer [read-write]	Enable DHCP on eth0 port. [0 / 1] Note: 0=off, 1=on

masibusGPSEth0v4IP	.1.3.6.1.4.1.38306.4.2.0	string [read-write]	Eth0 v4 IP address Max chars: 16 Format: xxx.xxx.xxx.xxx
masibusGPSEth0v4GTY	.1.3.6.1.4.1.38306.4.3.0	string [read-write]	Eth0 v4 gateway address Max chars: 16 Format: xxx.xxx.xxx.xxx
masibusGPSEth0v4MASK	.1.3.6.1.4.1.38306.4.4.0	string [read-write]	Eth0 v4 subnet mask address Max chars: 16 Format: xxx.xxx.xxx.xxx
masibusGPSEth0v6AUTOCONF	.1.3.6.1.4.1.38306.4.5.0	Integer [read-write]	Enable Autoconf on eth0 port. [0 / 1] Note: 0=off, 1=on
masibusGPSEth0v6LinkAddr	.1.3.6.1.4.1.38306.4.6.0	string [read-only]	Eth0 v6 link-local address
masibusGPSEth0v6GlobalAddr	.1.3.6.1.4.1.38306.4.7.0	string [read-write]	Eth0 v6 IP address Max chars: 39 Format: Valid IPv6 address
masibusGPSEth0v6MASK	.1.3.6.1.4.1.38306.4.8.0	Integer [read-write]	Eth0 v6 subnet mask [0 to 128]
masibusGPSEth0v6GTY	.1.3.6.1.4.1.38306.4.9.0	string [read-write]	Eth0 v6 gateway address Max chars: 39 Format: Valid IPv6 address
masibusGPSEth1v4DHCP	.1.3.6.1.4.1.38306.4.10.0	Integer [read-write]	Enable DHCP on eth1 port. [0 / 1] Note: 0=off, 1=on
masibusGPSEth1v4IP	.1.3.6.1.4.1.38306.4.11.0	string [read-write]	Eth1 v4 IP address Max chars: 16 Format: xxx.xxx.xxx.xxx
masibusGPSEth1v4GTY	.1.3.6.1.4.1.38306.4.12.0	string [read-write]	Eth1 v4 gateway address Max chars: 16 Format: xxx.xxx.xxx.xxx
masibusGPSEth1v4MASK	.1.3.6.1.4.1.38306.4.13.0	string [read-write]	Eth1 v4 subnet mask address Max chars: 16 Format: xxx.xxx.xxx.xxx
masibusGPSEth1v6AUTOCONF	.1.3.6.1.4.1.38306.4.14.0	Integer [read-write]	Enable Autoconf on eth1 port. [0 / 1] Note: 0=off, 1=on
masibusGPSEth1v6LinkAddr	.1.3.6.1.4.1.38306.4.15.0	string [read-only]	Eth1 v6 link-local address
masibusGPSEth1v6GlobalAddr	.1.3.6.1.4.1.38306.4.16.0	string [read-write]	Eth1 v6 IP address Max chars: 39 Format: Valid IPv6 address
masibusGPSEth1v6MASK	.1.3.6.1.4.1.38306.4.17.0	Integer [read-write]	Eth1 v6 subnet mask [0 to 128]
masibusGPSEth1v6GTY	.1.3.6.1.4.1.38306.4.18.0	string [read-write]	Eth1 v6 gateway address Max chars: 39 Format: Valid IPv6 address
masibusGPSTelnetopt	.1.3.6.1.4.1.38306.4.19.0	Integer [read-write]	To stop/start telnet service in device. [0 / 1] Note: 0=stop, 1=start
masibusGPSHTTPOpt	.1.3.6.1.4.1.38306.4.20.0	Integer	To stop/start http service in device.

		[read-write]	[0 / 1] Note: 0=stop, 1=start
masibusGPSHTTPOpt	.1.3.6.1.4.1.38306.4.21.0	Integer [read-write]	To stop/start https service in device. [0 / 1] Note: 0=stop, 1=start
masibusGPSSNMPOpt	.1.3.6.1.4.1.38306.4.22.0	Integer [read-write]	To stop/start snmp service in device. [0 / 1] Note: 0=stop, 1=start
masibusGPSIPv6opt	.1.3.6.1.4.1.38306.4.23.0	Integer [read-write]	To stop/start IPv6 service in device. [0 / 1] Note: 0=stop, 1=start
masibusGPSSyslog1Addr	.1.3.6.1.4.1.38306.4.24.0	string [read-write]	First Syslog server v4/v6 IP address Max chars: 39 Format: Valid v4/v6 address Note: 0.0.0.0 is to disable remove syslog logging facility
masibusGPSSyslog2Addr	.1.3.6.1.4.1.38306.4.25.0	string [read-write]	Second Syslog server v4/v6 IP address Max chars: 39 Format: Valid v4/v6 address Note: 0.0.0.0 is to disable remove syslog logging facility
masibusGPSBonding0opt	.1.3.6.1.4.1.38306.4.26.0	Integer [read-write]	To stop/start Bonding in device. Only for dual Ethernet. [0 / 1] Note: 0=stop, 1=start
masibusGPSEthxSaveOrRestore	.1.3.6.1.4.1.38306.4.27.0	Integer [read-write]	To save or restore all parameters. [0 / 1] Note: 0=restore, 1=save and reboot
masibusGPSCurrentAddrEth0	.1.3.6.1.4.1.38306.4.28.0	string [read-only]	Display live IPv4 address and netmask for Eth0 port
masibusGPSCurrentAddrEth1	.1.3.6.1.4.1.38306.4.29.0	string [read-only]	Display live IPv4 address and netmask for Eth1 port

Note: If MTS200 is provided with only single Ethernet option, the other Ethernet port related parameters/configurations will be disabled and not accessible by operator.

SNMP Branch : masibusGPSNTP

Variable	OID	Data Type [read/write]	Description [Values]
masibusGPSNTPLclCik	.1.3.6.1.4.1.38306.5.1.0	Integer [read-write]	System internal Local clock status [0 / 1] Note: 0=disable, 1=enable
masibusGPSNTPLclStratum	.1.3.6.1.4.1.38306.5.2.0	Integer	Applicable stratum during unit

		[read-write]	unlock conditions [0 to 15] Note: stratum applicable on ntp output will be stratum+1 during unlock.
masibusGPSNTPAuthType	.1.3.6.1.4.1.38306.5.3.0	string [read-write]	NTP authentication type [NONE / SYMM / AUTO] Note: Autokey settings can be done only by webserver.
masibusGPSNTPBCTEnable	.1.3.6.1.4.1.38306.5.4.0	Integer [read-write]	Ntp broadcast status [0 / 1] Note: 0=disable, 1=enable
masibusGPSNTPBCTAddr1	.1.3.6.1.4.1.38306.5.5.0	string [read-write]	Broadcast v4/v6 IP address used by ntp broadcast/multicast. Max chars: 39 Format: Valid v4/v6 address
masibusGPSNTPBCTInterval1	.1.3.6.1.4.1.38306.5.6.0	Integer [read-write]	NTP broadcast interval in seconds for broadcast address 1 [16 / 32 / 64 / 128 / 256 / 512 / 1024] Note: units in seconds
masibusGPSNTPBCTAuth1	.1.3.6.1.4.1.38306.5.7.0	string [read-write]	NTP authentication type for NTP broadcast address 1 [NONE / SYMM / AUTO] Note: This will depend on masibusGPSNTPAuthType parameter always.
masibusGPSNTPBCTkey1	.1.3.6.1.4.1.38306.5.8.0	Integer [read-write]	NTP broadcast key id value if broadcast is configured for SYMM key for broadcast address 1. [1 to 9999] Note: keyid entered should be a valid key in ntp.keys file of GPS Clock unit.
masibusGPSNTPBCTAddr2	.1.3.6.1.4.1.38306.5.5.0	string [read-write]	Broadcast v4/v6 IP address used by ntp broadcast/multicast. Max chars: 39 Format: Valid v4/v6 address
masibusGPSNTPBCTInterval2	.1.3.6.1.4.1.38306.5.6.0	Integer [read-write]	NTP broadcast interval in seconds for broadcast address 2 [16 / 32 / 64 / 128 / 256 / 512 / 1024] Note: units in seconds
masibusGPSNTPBCTAuth2	.1.3.6.1.4.1.38306.5.7.0	string [read-write]	NTP authentication type for NTPbroadcast address 2 [NONE / SYMM / AUTO] Note: This will depend on

			masibusGPSNTPAuthType parameter always.
masibusGPSNTPBCTkey2	.1.3.6.1.4.1.38306.5.8.0	Integer [read-write]	NTP broadcast key id value if broadcast is configured for SYMM key broadcast address 2. [1 to 9999] Note: keyid entered should be a valid key in ntp.keys file of GPS Clock unit.
masibusGPSNTPService	.1.3.6.1.4.1.38306.5.9.0	Integer [read-write]	To stop/start ntp service in device. [0 / 1] Note: 0=stop, 1=start Note: local clk should be enabled if ntp started in unlock conditions

SNMP Branch : masibusGPSSNMP

Variable	OID	Data Type [read/write]	Description [Values]
masibusGPSSNMPMgr1IP	.1.3.6.1.4.1.38306.6.1.0	string [read-write]	SNMP Manager1 v4/v6 IP address. Max chars: 39 Format: Valid v4/v6 address
masibusGPSSNMPMgr1Ver	.1.3.6.1.4.1.38306.6.2.0	Integer [read-write]	SNMP version for Manager 1 [0 / 1 / 2 / 3] Note: 0 is special case to disable SNMP communications with SNMP Manager1.
masibusGPSSNMPROCommunity1	.1.3.6.1.4.1.38306.6.3.0	string [read-write]	SNMP Manager1 community string for SNMP v1, v2c read only [walk, get] operation. min chars: 4, max chars: 30
masibusGPSSNMPRWCommunity1	.1.3.6.1.4.1.38306.6.4.0	string [read-write]	SNMP Manager1 community string for SNMP v1, v2c read/write [walk, get, set] operation. min chars: 4, max chars: 30
masibusGPSSNMPMgr1Permission	.1.3.6.1.4.1.38306.6.5.0	string [read-write]	SNMP Manager1 community read/write permissions for SNMP v1, v2c read/write [walk, get, set] operation. max chars: 2 [ro / rw]
masibusGPSSNMPMgr1TrapEnable	.1.3.6.1.4.1.38306.6.6.0	Integer [read-write]	SNMP trap enable for SNMP Manager1 for v1/v2/v3. [0 / 1] Note: 0=disable, 1=enable
masibusGPSSNMPMgr1TrapCommunity	.1.3.6.1.4.1.38306.6.7.0	string [read-write]	Community string applicable for trap receiving Manager for v1/v2 only. min chars: 4, max chars: 30
masibusGPSSNMPMgr1v3User	.1.3.6.1.4.1.38306.6.8.0	string	SNMPv3 username for

		[read-write]	Manager1. min chars: 4, max chars: 30
masibusGPSSNMPMngr1v3engin eld	.1.3.6.1.4.1.38306.6.9.0	string [read-write]	SNMPv3 engineid value with Manager1. min chars: 4, max chars: 40 Note: String must start with 0x format.
masibusGPSSNMPMngr1v3Auth Type	.1.3.6.1.4.1.38306.6.10.0	string [read-write]	SNMP v3 Authentication Type for Manger1. [NONE / MD5 / SHA] max chars: 4
masibusGPSSNMPMngr1v3Pass phrase	.1.3.6.1.4.1.38306.6.11.0	string [read-write]	SNMP v3 Authentication passphrase[password] for Manger1. min chars: 4, max chars: 40
masibusGPSSNMPMngr1v3PrivT ype	.1.3.6.1.4.1.38306.6.12.0	string [read-write]	SNMP v3 Priv Encryption Type for Manger1. [NONE / DES / AES] max chars: 4
masibusGPSSNMPMngr1v3Privp hrase	.1.3.6.1.4.1.38306.6.13.0	string [read-write]	SNMP v3 Priv Encryption passphrase[password] for Manger1. min chars: 4, max chars: 40
masibusGPSSNMPMngr2IP	.1.3.6.1.4.1.38306.6.14.0	string [read-write]	SNMP Manager1 v4/v6 IP address. Max chars: 39 Format: Valid v4/v6 address
masibusGPSSNMPMngr2Ver	.1.3.6.1.4.1.38306.6.15.0	Integer [read-write]	SNMP version for Manager2 [0 / 1 / 2 / 3] Note: 0 is special case to disable SNMP communications with SNMP Manager1.
masibusGPSSNMPROCommunit y2	.1.3.6.1.4.1.38306.6.16.0	string [read-write]	SNMP Manager2 community string for SNMP v1, v2c read only [walk, get] operation. min chars: 4, max chars: 30
masibusGPSSNMPRWCommunit y2	.1.3.6.1.4.1.38306.6.17.0	string [read-write]	SNMP Manager2 community string for SNMP v1, v2c read/write [walk, get, set] operation. min chars: 4, max chars: 30
masibusGPSSNMPMngr2Permiss ion	.1.3.6.1.4.1.38306.6.18.0	string [read-write]	SNMP Manager2 community read/write permissions for SNMP v1, v2c read/write [walk, get, set] operation. max chars: 2 [ro / rw]
masibusGPSSNMPMngr2TrapEn able	.1.3.6.1.4.1.38306.6.19.0	Integer [read-write]	SNMP trap enable for SNMP Manager2 for v1/v2/v3. [0 / 1] Note: 0=disable, 1=enable
masibusGPSSNMPMngr2TrapCo mmunity	.1.3.6.1.4.1.38306.6.20.0	string	Community string applicable for trap receiving Manager for

		[read-write]	v1/v2 only. min chars: 4, max chars: 30
masibusGPSSNMPMgr2v3User	.1.3.6.1.4.1.38306.6.21.0	string [read-write]	SNMPv3 username for Manger2. min chars: 4, max chars: 30
masibusGPSSNMPMgr2v3engineId	.1.3.6.1.4.1.38306.6.22.0	string [read-write]	SNMPv3 engineid value with Manger2. min chars: 4, max chars: 40 Note: String must start with 0x format.
masibusGPSSNMPMgr2v3AuthType	.1.3.6.1.4.1.38306.6.23.0	string [read-write]	SNMP v3 Authentication Type for Manger2. [NONE / MD5 / SHA] max chars: 4
masibusGPSSNMPMgr2v3Passphrase	.1.3.6.1.4.1.38306.6.24.0	string [read-write]	SNMP v3 Authentication passphrase[password] for Manger2. min chars: 4, max chars: 40
masibusGPSSNMPMgr2v3PrivType	.1.3.6.1.4.1.38306.6.25.0	string [read-write]	SNMP v3 Priv Encryption Type for Manger2. [NONE / DES / AES] max chars: 4
masibusGPSSNMPMgr2v3Privphrase	.1.3.6.1.4.1.38306.6.26.0	string [read-write]	SNMP v3 Priv Encryption passphrase[password] for Manger2. min chars: 4, max chars: 40
masibusGPSSNMPContact	.1.3.6.1.4.1.38306.6.27.0	string [read-write]	GPS Clock contact information. min chars: 4, max chars: 38 Note: special characters not allowed except <i>,/ _/ / []</i>
masibusGPSSNMPLocation	.1.3.6.1.4.1.38306.6.28.0	string [read-write]	GPS Clock device location information. min chars: 4, max chars: 38 Note: special characters not allowed except <i>,/ _/ / []</i>
masibusGPSSNMPRestartSrvs	.1.3.6.1.4.1.38306.6.29.0	Integer [write only]	To restart the SNMP service in GPS Clock. [1] Note: Fixed value only.

13.3.4 SNMP Traps:

masTER T-Sync device can send snmp traps to up to two SNMP managers with configured customized trap community over version 1, 2 or 3. Below is the list of SNMP traps which masTER T-Sync is capable to generate over respective alarm generated in device.

1. GPS LOCK / UNLOCK trap [OID:- .1.3.6.1.4.1.38306.7.1.1.0]

Message: "GPS LOCK – Date/Time" or "GPS UNLOCK-Date/Time" [OID:- .1.3.6.1.4.1.38306.7.1.2.0]

Description: Whenever this device GPS is in sync or out of sync with GPS satellites, this trap is generated whenever there is change of state with lock/Unlock time.

2. NTP Sync Loss [OID:- .1.3.6.1.4.1.38306.7.1.3.0]

Message: "NTP Sync." or "NTP Not Sync."

Description: Whenever ntpd daemon in device loses sync with internal gps receiver, *masTER T-Sync* will generate this alarm on every change of state. This may happen at every power up of device or ntp service restart of stop/start or internal accuracy loss or manual change of internal system clock.

3. NTP service restart/start/stop trap [OID:- .1.3.6.1.4.1.38306.7.1.4.0]

Message: "NTP Srvs. Stop" or "NTP Srvs. Start" or "NTP Srvs. Restart"

Description: Whenever the ntp service is restarted or stopped or started manually through front panel keypad or SSH/Telnet application program or SNMP application or at power-up when device comes in LOCK from unlock condition, this trap is generated.

4. Unit configuration change alarm [OID:- .1.3.6.1.4.1.38306.7.1.5.0]

Message: "Config. Changed"

Description: This alarm is generated whenever there is any change in configuration of device done through front panel keypad or SSH/Telnet application program or SNMP application.

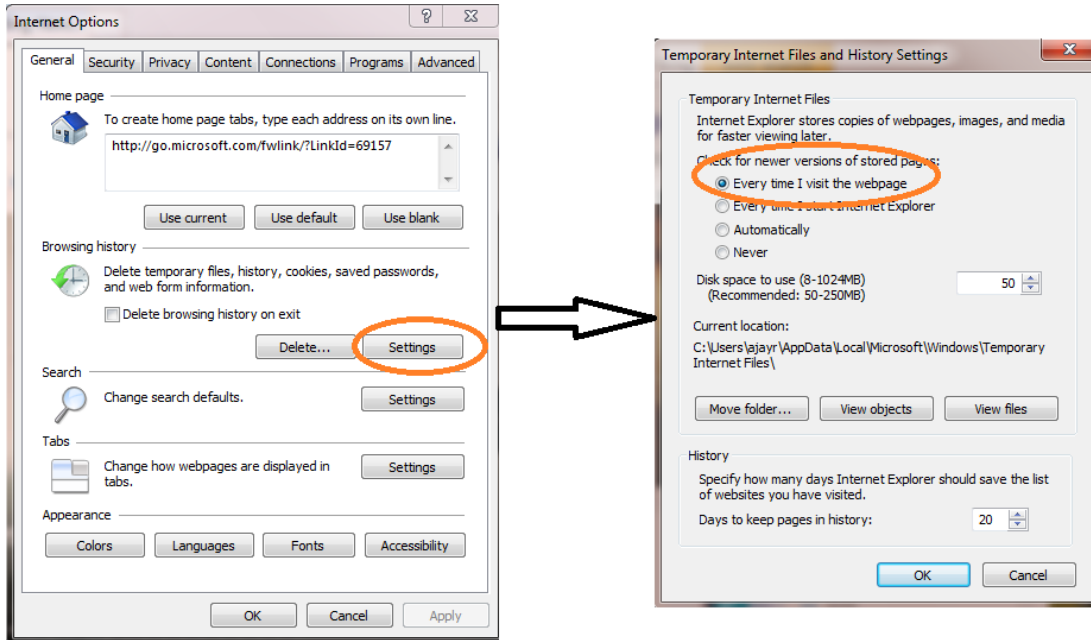
SNMP traps can be received through running snmptrapd utility in unix/linux based systems or configuring SNMP MIB Browser software on windows based systems.

13.4 Webserver

User/Operator need to carefully read and apply applicable notes before using MTS200 webserver.

Note:

1. MTS200 configuration through webserver should be accessed through a single computer at a time to avoid any configuration conflict through multiple computer systems.
2. It is recommended to use IE 9.0+, Mozilla Firefox 46+ web-browser software for MTS200 webserver. Use shortcut "Ctrl + F5" instead of F5 key to refresh the webpage.
3. If user is using "Google Chrome" or any other web-browser software, it is recommended to clear cache and cookies before starting MTS200 webserver.
4. It is recommended to clear cookies and cache files from web browser after power on of MTS200 unit. This will avoid any user conflict with old caches files of MTS200 device in web-browser with current MTS200 data.
5. As, MTS200 uses cookies for some of its webserver page features, user should not block the cookies settings for MTS200 webserver pages.
6. If user is using IE (Internet Explorer) for webserver, user need to do following changes in IE settings. Go to **Internet Options** -> **Browsing history** -> **Settings** -> **select option "Every Time I Visit the Webpage"** -> **OK**. This option will make web browser to load latest webpage from MTS200 webserver. Refer below two images for detail.



masTER T-Sync Model MTS200 device can be configured remotely using Serial port, SSH, Telnet and Webserver mode. However, the configuration through Serial port, SSH and telnet is done by running “start” utility after taking access of unit console command line interface.

For configuration through Webserver, user need to enter the IP address in web browser software as explained below:

For HTTP connection with

1. MTS200: <http://192.168.100.153> on IPv4
2. MTS200: [http://\[fdc2:7142:77b7:0:1eba:8cff:fee5:c115\]](http://[fdc2:7142:77b7:0:1eba:8cff:fee5:c115]) on IPv6

For HTTPS connection with

1. MTS200: <https://192.168.100.153> on IPv4
2. MTS200: [https://\[fdc2:7142:77b7:0:1eba:8cff:fee5:c115\]](https://[fdc2:7142:77b7:0:1eba:8cff:fee5:c115]) on IPv6

For HTTPS connection, user will be prompted for accepting SSL certificate of MTS200, which user have to accept as SSL certificates for https in MTS200 are self signed certificate.

Once, user give above address in web browser software, login page of MTS200 page will open as shown below.



Figure 13-1 MTS200 webserver login page

User need to enter the username and password in login page to gain access to other web pages of MTS200. Users can be created through “Administration” webpage of MTS200. Maximum 9 users can be created.

- **“HOME” Webpage:**

Once user login in webserver, MTS200 home web page will be displayed as below.

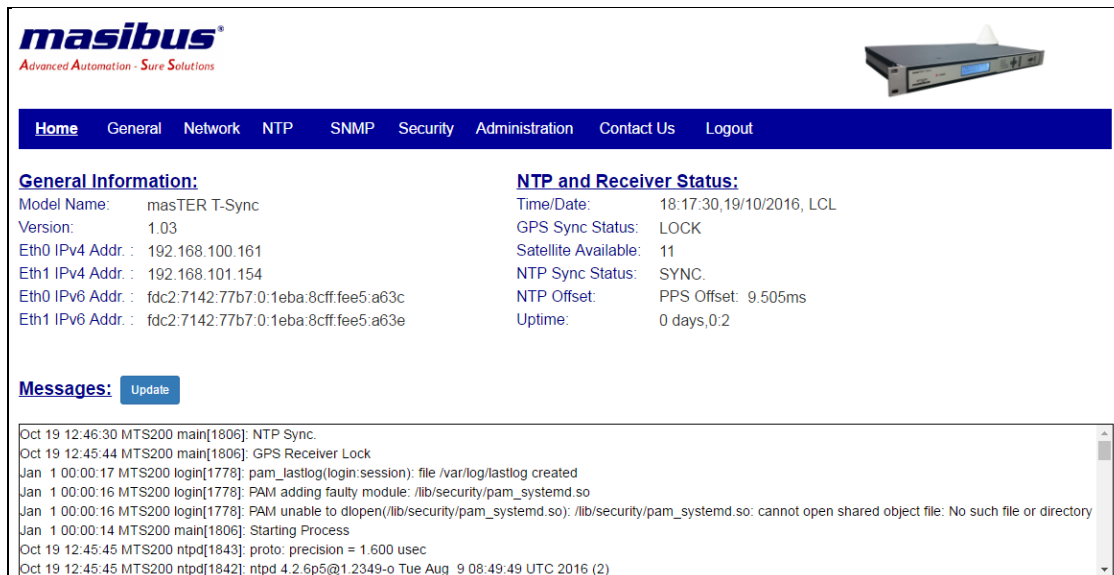


Figure 13-2 MTS200 webserver home page

Model: MTS200 (1U)

Doc. Ref. no. : m08/om/201

Issue no. : 03

Home page is updated only at every loading or refresh of page. This can be done either by selecting menu option in menu index or by pressing refresh button on web browser.

Home page display top menu line have link to Home page, General Settings menu, Network Settings, NTP options, SNMP menu, Security page, Device Administration page and logout index. User can navigate through several menu options and selected menu will be marked with background "GREEN" colour.

Once any main menu is selected, that particular menu is indicated by *Bold and Underlined Text* in that particular page as shown in below example.

E.g. If user in Network page in webserver, it will highlighted as below.



Network

MTS200 home page displays status of few mentioned parameters. On left side, the device version number, IPv4/IPv6 address of both eth port are displayed. If unit is configured with single eth port, field "Eth2 IP Address" will be marked as "N.A.".

On Right side of page, gives status about GPS receiver and NTP status output of MTS200. Below is the description of parameters:

Time/Date - Displays the time and date with LOCAL/UTC timezone mode information

GPS Sync Status – Display "LOCK" and "UNLOCK" information of MTS200.

Satellite Available – Number of Satellites during unit LOCK condition. If Unit is in UNLOCK condition, it will be displayed as 0.

NTP Sync Status – "SYNC" or "NOT Sync". This indicates if the internal clock of device is synchronized with GPS receiver module.

NTP Offset – Represents the offset of internal ntp driver clock with GPS receiver in milliseconds units.

Uptime – This represents the duration since the device is power up.

Below Section in home page displays the log messages (/var/log/messages) file of accessed MTS200 unit. This file is created newly at every Power ON and is cleared when the size of log file exceeds 100Kbytes. User can check the updated log file by clicking on "Update" field as shown in below image.



Messages:

Only latest 50 messages from /var/log/messages file will be displayed in Messages section in home page. For complete log file, user can download the log messages file from Administration Page in webserver.

- **"GENERAL" Webpage:**

For MTS200 basic settings, user need to navigate and select the "GENERAL" option in menu index. After, selecting below webpage will be displayed.



Advanced Automation · Sure Solutions



Home
General
Network
NTP
SNMP
Security
Administration
Contact Us
Logout

Time:

Time Format Hour Mode

Time Zone Offset :
(Hour) (Min.)

Com1 Configuration:

Time Code Format

Com2 Configuration:

Baud Rate Parity

Stop Bit Transmit Mode

Events:

Standard Events

Event 1	On Time(millisecond)
Period(sec) <input type="text" value="60"/> <small>(Max. : 86400)</small>	<input type="text" value="50"/> <small>(Min. : 50 ms, Max. : 50% of Period)</small>
Event 2	On Time(millisecond)
Period(sec) <input type="text" value="60"/> <small>(Max. : 86400)</small>	<input type="text" value="50"/> <small>(Min. : 50 ms, Max. : 50% of Period)</small>
Event 3	On Time(millisecond)
Period(sec) <input type="text" value="60"/> <small>(Max. : 86400)</small>	<input type="text" value="50"/> <small>(Min. : 50 ms, Max. : 50% of Period)</small>
Event 4	On Time(millisecond)
Period(sec) <input type="text" value="60"/> <small>(Max. : 86400)</small>	<input type="text" value="50"/> <small>(Min. : 50 ms, Max. : 50% of Period)</small>

Antenna Cable Length Compensation:

SPD (nanoseconds)
(Max. : 99999)

DayLight Saving:

DST Mode

DST Offset :
(Hour) (Min.)

DST Start Date / / DST Start Time :
(Month) (Week Of Month) (Day Of Week) (Hour) (Min.)

DST End Date / / DST End Time :
(Month) (Week Of Month) (Day Of Week) (Hour) (Min.)

IRIG Output:

IRIG Mode IRIG Time

*Use "Ctrl+F5" to Refresh Page

Figure 13-3 MTS200 webserver General page

Model: MTS200 (1U)

Doc. Ref. no. : m08/om/201

Issue no. : 03

As shown in above figure, user can configure general settings of device in webserver. Please refer section 9.1 for each parameter description. Once user modify the required data, click on “Save” options provided at end of page. This will save the changed parameters in MTS200.

Other options provided at end of page include “Default Configurations” used to default the settings of GENERAL parameters, “Restore Configurations” which is used to restore previous saved settings if user have defaulted all parameters and “View Configurations” to view the current GENERAL parameters values. User need to click on “Save” option after doing “Default Configurations” or “Restore Configurations” or change on any parameter.

- **“Network” Webpage:**

For MTS200 eth0 and eth1 network settings, user need to navigate and select the “NETWORK” option in menu index. After, selecting below webpage will be displayed.

The screenshot displays the Masibus webserver interface for network configuration. At the top, there is a navigation menu with options: Home, General, **Network**, NTP, SNMP, Security, Administration, Contact Us, and Logout. The main content area is divided into sections for Eth0, Eth1, Misc. Settings, and Network Services.

Eth0: This section allows configuration for the Eth0 interface. It includes radio buttons for IPv4 and IPv6. The IPv4 configuration shows an IP Address of 192.168.100.161, a Subnet Mask of 255.255.254.0, and a Gateway of 192.168.100.254. There is a checkbox for DHCP, which is currently unchecked.

Eth1: This section is similar to Eth0, with radio buttons for IPv4 and IPv6.

Misc. Settings: This section includes Syslogserver1 and Syslogserver2, both set to 0.0.0.0. There is a checkbox for Bonding (unchecked) and a checkbox for IPv6 (checked).

At the bottom of the configuration area, there are three buttons: Save, Default Configurations, and View Configurations.

Network Services: This section shows a table of services with their status:

Status	Telnet	HTTP	HTTPS	SNMP
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

A "Save Status" button is located to the right of the Network Services table. At the bottom left, there is a note: *Use "Ctrl+F5" to Refresh Page.

Figure 13-4 MTS200 Webserver Network configuration with IPv4

The screenshot shows the Masibus webserver interface for network configuration. At the top, there is a navigation menu with options: Home, General, **Network**, NTP, SNMP, Security, Administration, Contact Us, and Logout. Below the menu, there are sections for configuring network interfaces:

- Eth0:** Includes checkboxes for IPv4 and IPv6. The IPv6 configuration is active, showing:
 - Autoconf:
 - Link Local Address: fe80::1eba:8cff:fee5:a83c
 - IPv6 Address: fd02:7142:77b7:0:1eba:8cff:fee5:a83c
 - IPv6 Subnet Mask: 64
 - Gateway Address: ::
- Eth1:** Similar to Eth0, with IPv4 and IPv6 checkboxes.
- Misc. Settings:**
 - Syslogserver1: 0.0.0.0
 - Syslogserver2: 0.0.0.0
 - Bonding:
 - IPv6:

At the bottom of the configuration section, there are buttons for "Save", "Default Configurations", and "View Configurations". Below this is the "Network Services" section, which includes a table for service status:

Status	Telnet	HTTP	HTTPS	SNMP
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

A "Save Status" button is located to the right of the table. At the very bottom, a red note reads: "*Use 'Ctrl+F5' to Refresh Page".

Figure 13-5 MTS200 Webserver Network Configuration with IPv6

To configure network parameters of eth0 and eth1 of MTS200, user need to enter respective data in mentioned field in network webpage. In order to configure network settings of eth0 and eth1, first select the tickbox of respective eth interface and then settings of that eth can be edited. However, if user wants DHCP option on eth0 and eth1, user need to just tick the checkbox in DHCP field respective interface.

For each eth interface, IP address, Subnet Mask, gateway can be configured in v4 format. If DHCP is enabled in any of the interface, MTS200 will automatically acquire IP address and other network parameters of that interface from DHCP server in network. IP acquired by DHCP can be viewed on front panel LCD display via keypad or “Network Status” webpage or it can be viewed in SNMP.

To configure network parameters of eth0 and eth1 of MTS200 with IPv6, user need to enter respective data in mentioned filed in network webpage. In order to configure network settings of eth0 and eth1, first select the tick box of respective eth interface and then settings of that eth can be edited. If user want Autoconf option then tick the checkbox in autoconf field of respective interface.

If autoconf is enabled , MTS200 will automatically acquire IP address and other parameter of that interface. User can view live ethernet parameter in “Network Status” webpage on the webserver.

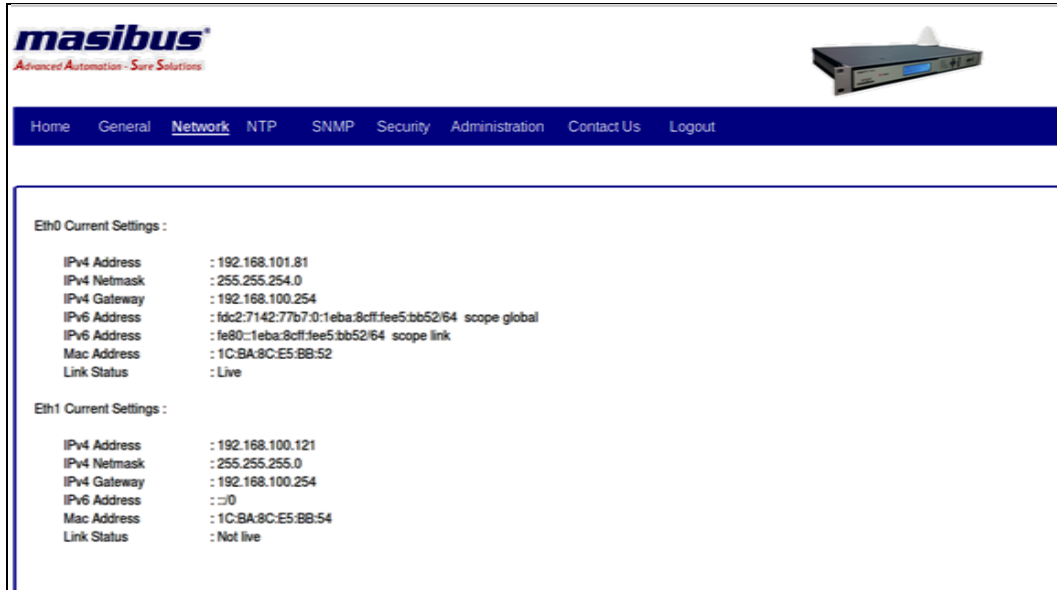


Figure 13-6 MTS200 Webserver Network Status Page

User can configure syslog server1 and syslog server2 IP address in their respective files. For further explanation, refer section 13.5.

Once user modifies the required data, click on “Save” options provided at the end of the page. This will save the changed parameters in MTS200. Other options provided at the end of the page include “Default Configurations” used to default the settings of GENERAL parameters, “Restore Configurations” which is used to restore previous saved settings if user has defaulted all parameters and “View Configurations” to view the current GENERAL parameters values. User needs to click on “Save” option after doing “Default Configurations” or “Restore Configurations” or change on any parameter.

Apart from setting network parameters, network services such as Telnet, SSH, HTTP, HTTPS, SNMP can be enabled or disabled in “Network Services” field. Once configuration is done, select “Save Status” to save the network services status.

Note:

1. MTS200 will automatically reboot if there is a change in any parameter related to ETH0, ETH1 and bonding.
2. If MTS200 is provided with only a single Ethernet option, the other Ethernet port related parameters/configurations will be disabled and not accessible by the operator.
3. Use static instead of dynamic IP for both ETHx connectors as dynamic IP may change on every power reboot of the device or on making eth0 service disable/enable.
4. User cannot stop HTTP and HTTPS service when configuring through the webserver. At a time, HTTP or HTTPS service will be active to avoid complete disabling of webserver service.

- **“NTP” Webpage:**

For MTS200 NTP settings and internal ntp driver status, user needs to navigate and select the “NTP -> NTP Configurations” for ntp configurations and “NTP->NTP Status” for ntp driver status in the menu index.

For detailed explanation, refer section 11.3.3.

- **“SNMP” Webpage:**

For MTS200 SNMP settings, user need to navigate and select the “SNMP” option in menu index. After, selecting below webpage will be displayed.

Figure 13-7 MTS200 Webserver SNMP Page

MTS200 can be configured as SNMP agent communicating with two different SNMP Manager’s. MTS200 settings for both managers can be different with different snmp versions. SNMP Manager version 1 / 2c and 3 are supported in MTS200.

For Detailed understanding of each parameter, refer section 13.3.

Also, SNMP Traps can be made enabled or disabled for each SNMP Manager, refer section 13.3.4.

Model: MTS200 (1U)

Doc. Ref. no. : m08/om/201

Issue no. : 03

Once user modify the required data, click on “Save” options provided at end of page. This will save the changed parameters in MTS200. Other options provided at end of page include “Default Configurations” used to default the settings of GENERAL parameters, “Restore Configurations” which is used to restore previous saved settings if user have defaulted all parameters and “View Configurations” to view the current GENERAL parameters values. User need to click on “Save” option after doing “Default Configurations” or “Restore Configurations” or change on any parameter.

- **“Security” Webpage:**

For MTS200 Security settings for NTP, HTTPS and SSH, user need to navigate and select the “Security” option in menu index. After, selecting below webpage will be displayed.

NTP Authentication:

MTS200 provides ntp output compatible with verison 2/3/4. NTP version 3 authentication is supported through NTP Symmetric key based method while NTPv4 supports NTP symmetric key as well as Autokey based PC and IFF scheme authentication.

For complete understanding of NTP Authentication using both methods, refer section 11.3.3.4.

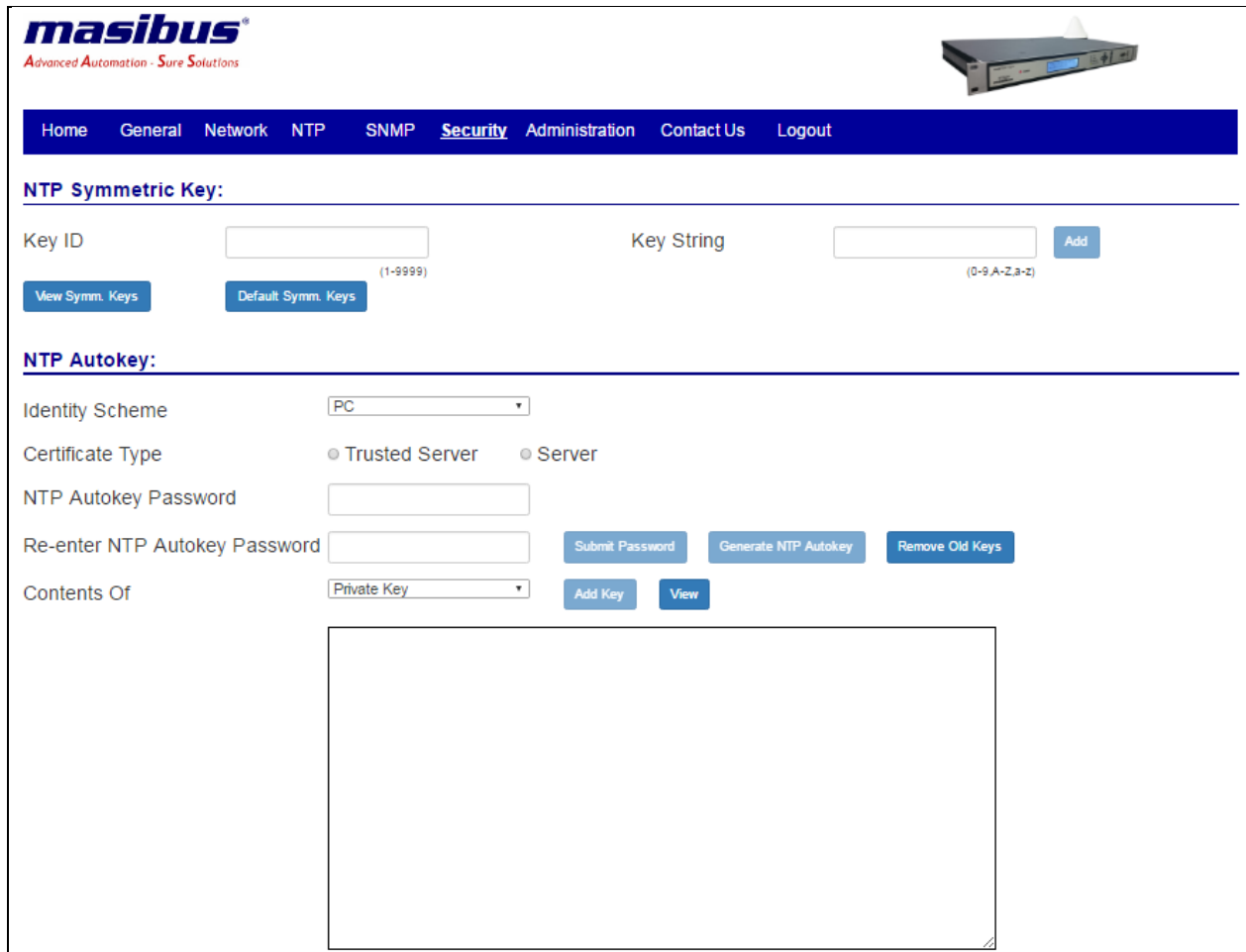


Figure 13-8 MTS200 Webserver Security Page

HTTPS Certificate:

MTS200 can be remotely configured using secured HTTP service i.e. HTTPS with remote PC Web browser. HTTPS security certificate in MTS200 are self-signed SSL security certificate of X509 type.

Remote PC can connect with MTS200 using https with address: <https://192.168.100.153> or the IP address configured in device.

For first time, the remote PC Web browser will ask to accept the MTS200 certificate, user should check the contents of certificate and then accept. After that https communication is established.

Apart from the standard certificate provided by shipped unit, user can generate their own certificate by entering required fields as shown in below image.

HTTPS [SSL] Certificate:

Country Name (2 letter code,A-Z,a-z)

State Name (A-z,a-z) Organization Unit (@,0-9,A-z,a-z)

Locality Name (A-z,a-z) Organization Name (A-z,a-z,.)

Email Address (@,.0-9,A-z,a-z,_) Common Name (@,0-9,A-z,a-z)

After all fields are entered, “Generate SSL Certificate” tab will be highlighted. Now, click on the “Generate SSL Certificate” will save entered parameters.

Now, click on “Save” will start generating SSL certificate for HTTPS communication. This process will take some while and while generating certificate, background will be disabled as shown in below figure.

HTTPS [SSL] Certificate

Country Name (2 letter code)

State Name

Locality Name

Email Address

Organization Unit

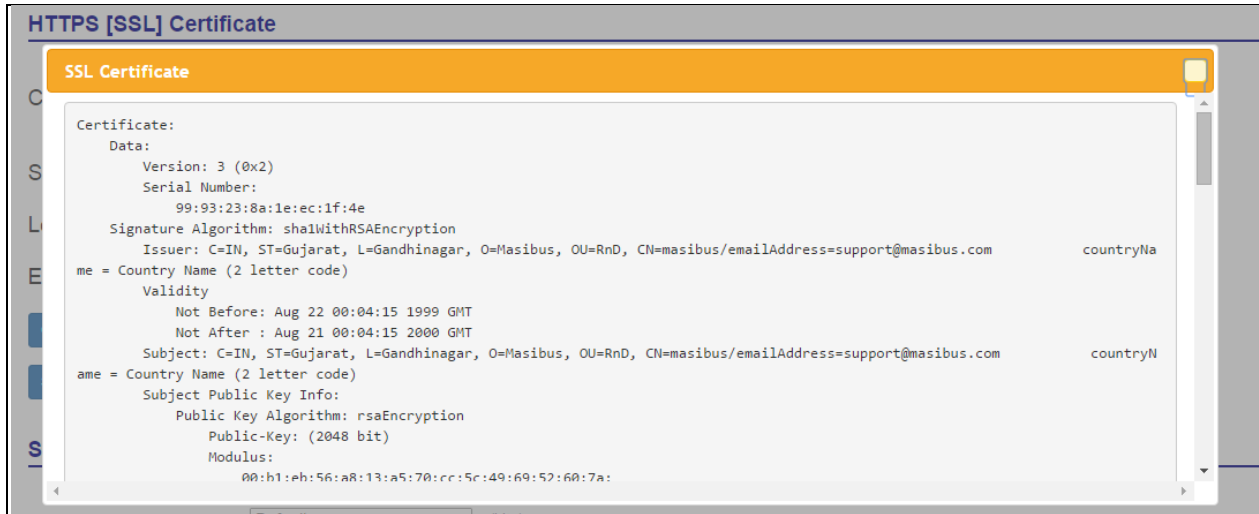
Organization Name

Common Name

PROCESSING. PLEASE WAIT...

Once certificate generation process is completed, new HTTPS certificates will be saved in device and HTTPS communication will start with newly generated certificate.

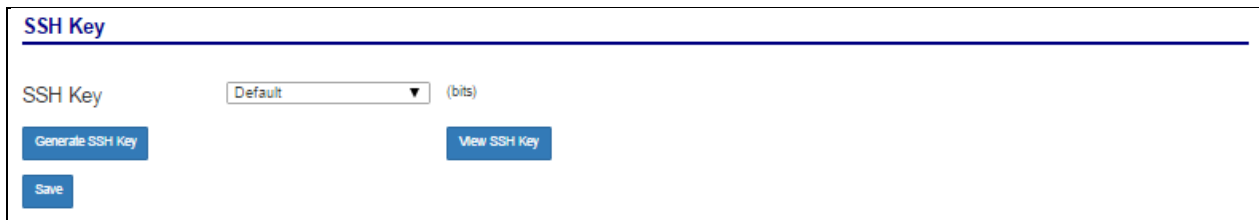
User can also view current or generated HTTPS certificate details using “View SSL Certificate” option. This option will pop up new window displaying certificate contents as shown in below figure and this pop up window can be closed by right corner close option.



SSH v1/v2 keys:

MTS200 can be configured and monitored using console based configuration utility. This utility can be executed through SSH communication mode with MTS200. MTS200 supports SSHv1 and SSHv2 protocol. SSHv1 key is based on RSA key with 768 / 1024 / 2048 bits for key generation while SSHv2 uses DSA key of fix 1024 bits and RSA key with 768 / 1024 / 2048 bits for key generation. It is recommended to use 2048 bits RSA key sized because 2048 bits is considered more robust authentication key size for SSH communications.

MTS200 webserver mode allows configuring and generating SSH v1 and v2 keys. Also, user can view SSH key contents. After selecting SSH key bits size, click on “Generate SSH Key” will start generating the SSH v1 and v2 keys.



Generating SSH key process will take some while and while generating keys, background will be disabled. Once keys are generated, users need to select “Save” option to save the new keys and delete old keys.

Using “View SSH key” user can view the generated SSH keys or previous SSH keys as shown in below figure. The pop up window will appear and display SSH v1 and v2 keys in pop up window.


```

SSH Key:
SSH v1 v2 public key
768 65537 116244802276789437198008732807309169626669080153902637570831479788590443676795133259049219014451396955273
3874078346070697712927855758452935663831913222753139805507621413374338930594163598462410958854924157527322405187785
716777200267 root@MTS200

SSHv2 rsa key:768 65537 1162448022767894371980087328073091696266690801539026375708314797885904436767951332590492190
1445139695527338740783460706977129278557584529356638319132227531398055076214133743389305941635984624109588549241575
27322405187785716777200267 root@MTS200

SSHv2 dsa key:ssh-dss AAAAB3NzaC1kc3MAAACBANGLkywzaMrvzu/8+oFN5LNmBtKuIF3tR+TSycwkeS0chc56GEIEjkiWm3ES2TJ2AYZnWtCsG
ZTdee/kYu8PX0wVcCgBq6RCyq/7Bn1TfNt9M1f8jgoDTY2+p17/Y5Yr/223V4FptI99xqUptsoML8PYwR7S8L4CLNP08YE0ncgLAAAFQDaZ8F0pK70
5+LFKxayMhNfxOk5zQAAAEIeAsQasyCyrU11ncFCGudbqkBOHjIR9ZRT8ClD0K2QTiAt9EKNV0oqTbB30s2onJP4zevA5/ZIwDcAONJ4WiH4KZVdTzZ
E0401Cy1m23BTC/28i/1cdHksow94wgNI4PRg+Sj9rG0k0sGJ02cuM0ZEKcCiwkXYvTltMRLKY9HozEAAACAXjd1F191urA8ZVpk4/V5tDATuJ2pj0
ps0U9fW37H2hc263kPHcflj+VFhxG/AYx7KhR9iwiYvR3iuG0fVwXrv7D7epa1TIc37G40ehAxsuIj7NvkhoN1101xSd13ATnFV21YaNKxKPp9R1vKav1
    
```

When user communicate with MTS200 using ssh for first time or when new keys are generated, user will be prompt to accept new keys, which should be accepted by user to start ssh communication with MTS200.



Downloads:

User can download all required keys and certificates from MTS200 in “Downloads” section in “Security” page of webserver.

Downloads

[NTP Symmetric Key](#)
[NTP Autokey PC Certificate](#) [NTP Autokey PC Key](#)
[NTP Autokey IFF Group Key](#) [NTP Autokey IFF Certificate](#) [NTP Autokey IFF Key](#)
[SSH v1 Key](#) [SSH v1 RSA Key](#) [SSH v1 DSA Key](#)
[SSL Certificate](#)

• “Administration” Webpage:

Home
General
Network
NTP
SNMP
Security
Administration
Contact Us
Logout

System Configurations:

Process List

Device Version

Reboot Device

Device Update

Figure 13-9 MTS200 Webserver Administration Page

Model: MTS200 (1U)

Doc. Ref. no. : m08/om/201

Issue no. : 03

System Configurations:

Process list shows the current process running in MTS200 device. The process list is only refreshed on the loading of webpage. User need to refresh this webpage to see current list of process running in system.

Device Version give details about the MTS200 version information.

Reboot Device option can be used to reboot the device through webserver. While this option will cause reboot, all outputs of MTS200 will be halted till the units get started again. All log messages will be cleared and all Ethernet services will be restarted again.

Device Update:

User can have below page from “Administration” page by clicking on “Device Update” button at on “Administration” page.

masibus®
Advanced Automation - Sure Solutions

Home General Network NTP SNMP Security **Administration** Contact Us Logout

Device Update:

Firmware (Only .tar file) No file chosen

Configuration Files (Only .txt files)

General	<input type="button" value="Choose file"/>	No file chosen
Eth0	<input type="button" value="Choose file"/>	No file chosen
Eth1	<input type="button" value="Choose file"/>	No file chosen
Eth Misc.	<input type="button" value="Choose file"/>	No file chosen
Eth Services	<input type="button" value="Choose file"/>	No file chosen
NTP	<input type="button" value="Choose file"/>	No file chosen
SNMP	<input type="button" value="Choose file"/>	No file chosen

Others No file chosen

*Use "Ctrl+F5" to Refresh Page

Here user can update number of files at a time. User has to select respected files to upload.

Three options are available in the Device update.

- 1) Firmware Update
- 2) Configuration Files.
- 3) Others.

To update firmware or configuration files click on the choose file button, it will prompt user to select the respected file. Select that file and click on submit button. It will take some time and device will reboot.

Note:

- In case of firmware update, files should be kept in compressed format with named mts200_boot.tar. Make sure that final updated files are present in the mts200_boot.rar.
- For configuration file update, select the respected configuration text file.

* : MTS will be reboot after clicking submit button

Device Configurations:

Device Configurations:

View Configurations General ▼ Submit

Change User's Password

Username General
 Network
 NTP
 SNMP
 ntp conf File
 snmp conf File
 ntp.keys

Using Device configurations, user can view the current applicable settings for General settings, Network settings, NTP settings, SNMP settings, ntp.conf file, snmp.conf file and NTP symmetric keys values. User need to select the option and click on “Submit” button. After submit button is clicked, pop up window will open showing the settings for selected file.

User Management:

User Management:

Username (Only a-z, 0-9 and '_')

Password

Group Membership Super-User Administrator Info Add Show Current Users

Username Delete

Multiple Users can be created for MTS200 device with categories as Super-User, Administrator and Info. Maximum 10 username are allowed within system including “root” user. “root” is default super-user of MTS200 device which cannot be deleted or its username or password modified.

Users created through webserver or console based configuration program are applicable only for webserver login and SSH, Telnet and serial console session. The users created through webserver or console based program are different from front panel keypad password access.

New Users can be created or deleted only by Super-user and administrator type of users. Info user login to webpage can neither create user nor delete any user.

Super-user have all read-write access for system configuration, have rights to start/stop restart any system through webserver or console based program and even can check the ntp status data on webserver or console based program.

Administrator also have all read-write access for system configuration, have rights to start/stop restart any system through webserver or console based program and even can check the ntp status data on webserver or console based program. But, Administrator do not have access to console of MTS200 through SSH or Telnet or serial mode. If Administrator tries to have SSH, Telnet or serial session with MTS200, console based configuration utility “start” program will run automatically and session will expire or close on exit of the program.

Info User can only view configuration status but cannot modify device configuration and also cannot make any changes to system services status. Info user also does not have access to ntp service status.

Details and list of current existing system users can be viewed through “Show Current Users” option as shown in below image.

No.	Username	Group Membership
0	root	Super-User
1	masibus	Super-User
2	user2	Administrator
3	user3	Info-User

In order to make any modification to existing user and its password, “Change Current User Password” option can be used. This applicable username and new password is required to entered. Refer below image. “root” user can neither be modified or deleted.

Change User's Password:

Username

New Password

Downloads:

Downloads

- [SNMP MIB File](#)
- [Manual](#)
- [System Log Messages](#)

User can download MTS200 SNMP MIB file, Product manual and log messages file from “Download” Section.

- **“Contact Us” Webpage**

Provides Details regarding “Masibus Automation And Instrumentation Pvt. Ltd.” Contact details.

13.5 Syslog

MTS200 is capable to send internal logging messages of /var/log/messages file to configured two remote syslog servers.

For this, user need to configure IPv4/IPv6 address of required syslog server in the Ethernet Network settings. This can be done by console based configuration utility through front serial console port, Telnet, SSH and Webserver.

For setting syslog server IP address through serial console port, Telnet, SSH, refer section 9.2.
For setting syslog server IP address through webserver, refer section 13.4.

If operator does not require the log messages at any remote syslog server, user can set syslog server address for server1 and server2 as 0.0.0.0. or :: This will stop sending log messages to remote server but continue maintain log messages in internal /var/log/messages file.


The log messages file will continue log messages till the size of log file do not exceed 100Kbytes. If size exceed this limit, the file will be cleared automatically and restart logging new messages. This file will also be cleared at every Power ON of device. So, in order to maintain the log of messages, user can configure remote syslog server to keep the record for long time or can also download the file using webserver "Administration Page".

13.6 DHCP

MTS200 can acquire dynamic IP address through DHCP Server available in LAN. At every power reboot if DHCP option is enabled or ETH services restart or DHCP service restart, MTS200 will re-initiate the process of acquiring IP address and other network related parameters from available DHCP Server in LAN. It may take few seconds or minutes for acquiring the network settings by MTS200 and during this period. If there is no DHCP server available, no network address will be acquired by MTS200 device.

DHCP option in MTS200 can be enabled / disabled via front panel keypad menu or console based configuration utility or SNMP or Webserver.

Once IP address and other network parameters acquired, user can view the acquired network parameters on LCD display in respected Ethernet port menu option. Thereafter, user can use the allocated IP address to do completed configuration of MTS200 using console based configuration through SSH, Telnet or Webserver.

	<p>INFORMATION</p> <ul style="list-style-type: none">• DHCP is applicable for both the interface• If there is no DHCP server available in network, IP address will be mentioned as some garbage value or invalid address.• It is necessary that ethernet RJ-45 cable should be connected in network before making DHCP enable. If eth0/eth1 cable is not connected before making DHCP enable, user need to connect Ethernet cable and then restart DHCP service or eth0/eth1 service from device keypad.• DHCP network for both the interface eth0 and eth1 must be different. If both the interfaces are connected in the same DHCP server than eth0 and eth1 comes in same network which is only supported via Bonding option.
---	--

13.7 Auto configuration

Model: MTS200 (1U)

Doc. Ref. no. : m08/om/201

Issue no. : 03

MTS200 can be configured with IPv6 based network settings.

Autoconf option in MTS200 can be enabled / disabled via front panel keypad menu or console based configuration utility or SNMP or Webserver. Once IP address and other network parameters acquired, user can view the acquired network parameters on LCD display in respected Ethernet port menu option.

MTS200 can acquire two types of IPv6 address i.e. link-local and Global IPv6 address, if Autoconf feature is enabled. Global IPv6 address will be acquired only if IPv6 router is available in network. Link Local address will be acquired automatically even if Autoconf feature is disabled. Link-Local address is not configurable.

Example:

Link local address format: **fe80::1eba:8cff:fee5:a63c**

Global IPv6 address format: **fdc2:7142:77b7:0:1eba:8cff:fee5:a63c**

In case of Ethernet in different subnet, both Ethernet interface will have different IPv6 address as per isolated network in which Ethernet port is connected. In case of bonding between both Ethernet port, global IPv6 address will be according to the current active Ethernet port.



INFORMATION

- If unit doesn't find any IPv6 address it will show :: on the display as well as on the webserver.
- Any change in IPv6 address status is automatically scanned at every minute interval till the new IPv6 address is acquired. This condition may occur only if there is any change in Ethernet port link connection status or on Power ON.

14 Holdover Mode

If *masTER* T-Sync Model MTS200 is Power ON in Unlock conditions, the unit will provide time output depending on the data of its internal RTC clock time which is available with battery backup (refer section 8). However, if the provided battery backup to RTC is discharged due to very long Power OFF period of this device, at Power ON conditions in unlock conditions; all outputs of device will have factory set time value and not the correct time. Once unit gets locked, all outputs will get proper time data.

masTER T-Sync Model MTS200 device enter Holdover mode, when unit goes into Unlock condition from Lock condition and thereafter provides time output depending on the internal clock crystal accuracy. The accuracy of all time outputs (including 1PPS output) of unit will degrade depending on the duration during which unit is in Holdover mode and also on the internal clock crystal frequency accuracy. If the Unit again enter the Lock condition from Unlock condition, all the time outputs will become accurate as per UTC time. Holdover mode conditions do not exist if unit gets power reboot while unit was in Unlock condition. *masTER* T-Sync Model MTS200 outputs will regain its accuracy only when unit gets in lock condition once after Power ON.

15 Options

masTER T-Sync Model MTS200 model can be configured for Optional Power Supply.

Model: MTS200 (1U)

Doc. Ref. no. : m08/om/201

Issue no. : 03

15.1 Optional Input Power Supply

masTER T-Sync MTS200 model is available with optional power input connects to Plug in screw terminal. For AC supply operation connect LINE to (L) terminal, Neutral to (N) terminal and safety ground earth to "E" terminal, where as for DC Supply operation connect the positive lead to the (+) Positive terminal, connect the negative lead to the (-) Negative terminal and safety ground to "E" terminal when viewing instrument from rear.

15.1.1 Option 1: AC/DC Power Input

Input voltages are 90-264 Vac, 47-63 Hz or 125-300Vdc, less than 15 VA typical.

Input Power

AC Voltage Range	:	90 – 264 V _{AC}
Frequency	:	47 – 63 Hz
DC Voltage Range	:	125 – 300 V _{DC}

Fuse

Current Rating	:	1 Ampere
Voltage Rating	:	250 Volt

15.1.2 Option 2: DC Power Input

Input voltages are 18-72Vdc, less than 15 VA typical.

V _{DC} DC Power Supply Input :	18 – 72 V _{DC}
---	-------------------------

Fuse

Current Rating	:	1 Ampere
Voltage Rating	:	250 Volt

Note: This power consumption is for MTS200 without optional output.

16 Appendix List

Below is the list of *masTER* T-Sync Model MTS200 supported manuals.

Appendix C – Procedure to configure Windows / Linux PC as NTP Client

Appendix D – Procedure to configure Unix PC as NTP Client

Appendix H – NET T-Sync Tool software as NTP Client Utility

17 Troubleshooting

17.1 Unit not getting Power ON

Below mention, points need to be check to troubleshoot this problem.

- 1) Check Power input cable connected properly
- 2) Check Power input cable connected to respective terminal as described in section 14.1
- 3) Check Input power is available.
- 4) Check fuse is melted or not, if fuse is melted please contact masibus support department.

17.2 Wrong time at Unit Power ON

If the unit was kept in Power OFF conditions for the duration more than 15 days, as per mentioned in section 8.2, the battery back of internal RTC will get discharged completely. As a result, at unit Power ON, time displayed on LCD and time provided in all time outputs will be according to default internal time till the unit gets LOCKED after GPS antenna is connected to unit.

If the battery is discharged as per mentioned above, it is necessary to keep unit in Power ON condition for duration mentioned in section 8.2, for full charging of internal battery. Full charging is necessary to avoid possibility of wrong time output at unit Power ON.

17.3 masTER T-Sync Model MTS200 display time not as per Local time

If *masTER* T-Sync Model MTS200 time on display, NGTS & T-format time output, all event outputs is not as per Local time, the timezone offset w.r.t UTC may not be set as per required time offset for the region/country where unit is installed. Please refer section 9.1 to set timezone offset through serial configuration. Also, ensure that DST Mode if ON, there are proper settings of DST parameters.

Apart from timezone offset, it is necessary that the setting of time format (UTC/LOCAL) should be set to LOCAL. For setting this parameter to LOCAL, user can set it through front panel keypad (parameter: "SET TIME FORMAT" as per section 9) or console based configuration utility as section 9.2 or webserver as section 13.4 and snmp as per section 13.3 .

17.4 Cannot establish Serial communication with COM1

RS-232 cable used for serial communication with COM1 terminal should be cross cable as per figure 10.1. The serial communication of end device should be 9600 (baud rate), 8 (Data bits), N (NONE parity), 1 (1 stop bit). COM1 is used only to transmit NMEA serial time frame every second. The device which will be using NMEA time frame from *masTER* T-Sync Model MTS200 unit should comply with serial frame format as per table11.1.

17.5 Not able to receive time frame on COM1 terminal at every second

Refer troubleshoot index 17.4.

17.6 Cannot establish Serial communication with COM2

RS-232 cable used for serial communication with COM2 terminal should be cross cable as per section 10.

Also, the serial communication parameters such as baudrate, parity, stop bits of COM2 terminal are configurable through unit front panel keypad (refer section 9.1). It is necessary to match the end device serial communication parameters as per configured in *masTER* T-Sync Model MTS200 unit.

17.7 Not able to do configuration through front panel Serial Console terminal

The serial communication parameters such as baudrate, parity, stop bits of console terminal are fixed at 115200 baudrate, 8 data bits, Parity None, 1 stop bit. Also, set hardware flow control to None. It is necessary to match the end device serial communication parameters as per configured in *masTER* T-Sync Model MTS200 unit.

In order to configure *masTER* T-Sync Model MTS200 unit through serial configuration Front panel serial console terminal, it is necessary to enter correct password (when asked for, refer section 10.2.1.) in serial communication terminal software of remote PC.

Note: Password used for unit parameters configuration through keypad and serial communication are different. If user have forgot its own configured password for keypad menu or serial configuration menu, user should contact Masibus Service department.

17.8 Problem with getting unit LOCK to GPS satellites

- 1) It is always recommended to use factory provided antenna cable shipped with *masTER* T-Sync Model MTS200 unit. If antenna cable used for installation is other than provided with *masTER* T-Sync Model MTS200 unit, please contact Masibus Service department for assistance.
- 2) GPS Antenna must be installed properly as per suggested in section 5.1.1 and 5.1.2.
- 3) GPS Antenna cable must be connected at the antenna connection on rear panel of *masTER* T-Sync Model MTS200 device.
- 4) Refer section 5.1.5 for antenna cable technical details.
- 5) Check Antenna cable continuity. Unplug the antenna cable connection from GPS Antenna and antenna connector on *masTER* T-Sync Model MTS200 rear panel. Short the Antenna cable at any one end and check the continuity at other end using Digital Multimeter. If there is any break in continuity, contact Masibus service department for rectification.
- 6) If antenna cable is proper, refer section 5.1.3 for further diagnostics.
- 7) If *masTER* T-Sync Model MTS200 device is able to capture very less number of satellites even if the weather and sky is clear, try to re-orient the GPS antenna or relocate the GPS antenna so that maximum number of GPS satellites is visible.
- 8) NTP service should be ON because internal clock is synchronized by GPS receiver using ntp driver.

17.9 IRIG-B / IEEE 1344 client synchronization fail

Following steps are to be checked for issues of IRIG-B synchronization failure or loss.

- 1) IRIG-B BNC cable should be tightly connected and locked at GPS rear panel IRIG terminal and at IRIG-B client device terminal.
- 2) If IRIG client device terminal is other than BNC type connector, ensure that IRIG connection is done with correct polarity at client device terminal end.
- 3) Total number of IRIG-B/IEEE 1344 compatible devices connected on the IRIG TTL or IRIG-AM terminal of *masTER* T-Sync Model MTS200 should be determined considering the maximum electrical load capacity as specified in *masTER* T-Sync Model MTS200 specification. Refer product specifications and section 11.2.2.7 for further details.

17.10 No response to Ping Command

Below steps are to be checked for troubleshooting the mentioned issue:

Model: MTS200 (1U)

Doc. Ref. no. : m08/om/201

Issue no. : 03

- 1) *masTER* T-Sync Model MTS200 is shipped with factory set Ethernet configuration (IP, gateway and subnet address) or DHCP. For DHCP to work properly there should be DHCP server available in network.
- 2) Check the connection route from *masTER* T-Sync Model MTS200 Ethernet port to end device and configuration of intermediate Ethernet switches and gateways. *masTER* T-Sync Model MTS200 Ethernet port addresses of subnet and gateway should be configured as per network domain architecture.
- 3) If the unit is directly connected to remote PC using RJ-45 cable, it is recommended to connect unit through Ethernet switch or using cross RJ-45 cable configuration.
- 4) User should configure the IP address of all Ethernet outputs as per network domain configurations where *masTER* T-Sync Model MTS200 device is to be installed. User can configure IP address of Ethernet port using telnet connection with respective Ethernet NTP port. It is recommended to Power recycle the unit after all Ethernet NTP ports are configured with new IP address.

17.11 NTP client not synchronizing with GPS NTP output port

Following steps are to be checked for issues of NTP communication failure or NTP client time not synchronizing with GPS NTP Server port.

- 1) IP address of GPS NTP port and NTP client device should be same network domain.
- 2) Please verify the Ethernet connection between GPS NTP port and NTP server device by pinging the IP address of GPS NTP port. If IP address of GPS NTP port is not reachable, NTP communication will be failed.
- 3) GPS NTP Server port IP address should be properly configured in NTP client device.
- 4) MTS200 internal ntp driver must have synchronized with GPS Receiver.
- 5) If Authentication settings are done in MTS200, then user need to configure ntp client device with similar type of authentication if and only if authentication is required at client side. Refer section 11.3.3.4 for details regarding NTP Authentication.
- 6) Various NTP parameters should be configured properly in NTP client device.
- 7) If ntp client device is a computer machine based on Windows or Unix based or Linux based, please refer manual Appendix C for proper configuration and time synchronization method of client device.
- 8) Please refer section 11.3.4 and manual Appendix C for understanding NTP client time synchronization method.

17.12 Loss of time synchronization by NTP Client during GPS Unlock

If NTP client loses time synchronization when *masTER* T-Sync Model MTS200 is in Unlock condition and resume when *masTER* T-Sync Model MTS200 comes in LOCK condition, check the configured NTP stratum value in *masTER* T-Sync Model MTS200 device. It should be less than 15 or applicable value depending on NTP hierarchical architecture arrangement as explained in section 11.3.

17.13 Loss of time accuracy in NTP, IRIG-B, event outputs during Unit Power ON in Unlock conditions

When *masTER* T-Sync Model MTS200 comes in UNLOCK condition from LOCK condition during normal operation, unit enters in holdover mode. Refer section 14 for technical explanation of holdover mode.

17.14 Cannot establish telnet communication

- 1) IP address of GPS ethernet port and telnet device should be same network domain.
- 2) Please verify the Ethernet connection between GPS ethernet port and telnet device by pinging the IP address of GPS ethernet port. If IP address of GPS ethernet port is not reachable, telnet connection will fail.
- 3) Provide correct IP address of GPS Ethernet port while trying to establish telnet connection. Refer manual Appendix E for procedure for telnet connection with GPS Ethernet port.
- 4) Telnet service should be ON/START in MTS200 unit.
- 5) Telnet service should be ON in PC from which telnet session is required with MTS200.
- 6) Enter correct password of MTS200 when prompted for password filed while starting telnet session with MTS200. Refer section 13.1 for details.

17.15 Cannot establish SNMP communication

- 1) IP address of GPS ethernet port and SNMP manager should be in the same network domain.
- 2) Please verify the Ethernet connection between GPS ethernet port and SNMP manager by pinging the IP address of GPS ethernet port. If IP address of GPS ethernet port is not reachable, SNMP connection will fail. Refer troubleshooting index 17.10 and 17.11.
- 3) SNMP Manager should be able to work on SNMPv1 and SNMPv2c protocol.
- 4) MIB file at manager side for model MTS200 agent should be the same provided at the time of commissioning.
- 5) Read or Write Community of SNMP manager and model MTS200 agent should be same.

17.16 Not able to receive SNMP traps

- 1) IP address of GPS ethernet port and SNMP manager should be in the same network domain.
- 2) Please verify the Ethernet connection between GPS ethernet port and SNMP manager by pinging the IP address of GPS ethernet port. If IP address of GPS ethernet port is not reachable, SNMP connection will fail. Refer troubleshooting index 17.10 and 17.11.
- 3) SNMP version should not be set as 0 in MTS200.
- 4) SNMP Manager version should be as per set in MTS200 snmp settings.
- 5) SNMP manager IP should be configured in model MTS200 agent.
- 6) Trapenable for respective SNMP Manager Variable should be enabled in MTS200.
- 7) After doing any modification, restart SNMP service in MTS200.
- 8) Trapcommunity name and Manager IP address should be same at MTS200 and manager side for Manager to receiver traps.
- 9) User need to configure PC snmptrapd.conf file for authentication disable or enable and trapcommunity settings if required for v1, v2 and v3.

17.17 Not Able to set SNMP parameter

- 1) IP address of GPS ethernet port and SNMP manager should be in the same network domain.
- 2) Please verify the Ethernet connection between GPS ethernet port and SNMP manager by pinging the IP address of GPS ethernet port. If IP address of GPS ethernet port is not reachable, SNMP connection will fail.
- 3) SNMP version should not be set as 0 in MTS200.
- 4) SNMP Manager version should be as per set in MTS200 snmp settings.
- 5) For SNMPv3, authentication parameters should be correct at MTS200 and Manager side.
- 6) User need to configure PC snmptrapd.conf file for authentication disable or enable and trapcommunity settings if required for v1, v2 and v3.
- 7) MIB file at manager side for model MTS200 agent should be the same provided at the time of commissioning.
- 8) Write Community of SNMP manager and model MTS200 agent should be same.

17.18 Cannot establish SSH communication

- 1) IP address of GPS ethernet port and telnet device should be same network domain.
- 2) Please verify the Ethernet connection between GPS ethernet port and telnet device by pinging the IP address of GPS ethernet port. If IP address of GPS ethernet port is not reachable, telnet connection will fail.
- 3) Provide correct IP address of GPS Ethernet port while trying to establish telnet connection. Refer manual Appendix E for procedure for telnet connection with GPS Ethernet port.
- 4) SSH service should be ON/START in MTS200 unit.
- 5) SSH service should be ON in PC from which telnet session is required with MTS200.
- 6) Enter correct password of MTS200 when prompted for password filed while starting SSH session with MTS200. Refer section 13.2 for details.
- 7) SSH version 1 and 2 and their keys must be supported at PC side from where SSH session with MTS200 is required.
- 8) User should accept the MTS200 keys if prompted for in PC console. If PC warns to remove old keys with that particular IP address, user should remove old keys and then again give SSH command to have access with MTS200.

17.19 Cannot start Webserver

- 1) IP address of GPS ethernet port and telnet device should be same network domain.
- 2) Please verify the Ethernet connection between GPS ethernet port and telnet device by pinging the IP address of GPS ethernet port. If IP address of GPS ethernet port is not reachable, telnet connection will fail.
- 3) Provide correct IP address of GPS Ethernet port while trying to establish telnet connection. Refer manual Appendix E for procedure for telnet connection with GPS Ethernet port.
- 4) HTTP or HTTPS service should be ON/START in MTS200 unit.
- 5) Enter correct password of MTS200 when prompted for password filed while starting webserver session with MTS200. Refer section 13.4 for details.
- 6) If HTTP service is ON in MTS200, then user cannot have HTTPS connection for webserver. Also, If HTTPS service is ON in MTS200, then user cannot have HTTP connection for webserver
- 7) User should accept the MTS200 Webserver certificate if prompted for in PC web based browser for having HTTPS connection.

17.20 Alarms/Notification being not received on remote Syslog Server

- 1) In MTS200, syslog server IP address should be properly configured in Network settings.
- 2) At PC server side, syslog service should be ON and should accept packets from MTS200 on UDP layer.
- 3) Syslog server should be in same network domain and connected in LAN in which MTS200 is connected.

17.21 NTP Broadcast / Multicast messages not received at NTP client side

- 1) If NTP client is a Unix or Linux or Solaris or Red-Hat system, user need to configure ntp.conf file in unix based system for receiving broadcast/multicast ntp messages and then restart the ntp service in those systems.
- 2) If ntp client is configured for ntp authentication, then ntp authentication type should be same as authentication type configured for broadcast in MTS200.
- 3) If NTP broadcast is configured with NONE Authentication type in MTS200 and ntp clients are configured with broadcast authentication, then configure NTP broadcast in MTS200 with same type of settings.

17.22 NTP Client Not synchronized with MTS200 using Symmetric Key Authentication

- 1) ntp.keys file of MTS200 and ntp client should have same Keyid-string pair at both sides. The required keyid-pair should be configured in ntp.conf file at MTS200 and client side.
- 2) ntp service at server and client side, should be restarted after configuring ntp.keys and ntp.conf file.
- 3) ntp.keys file path of ntp client should be properly configured in client ntp.conf file.
- 4) NTP client should have symmetric authentication enabled in configuration file.

17.23 NTP Client Not synchronized with MTS200 using PC scheme AutoKey association with MTS200 as trusted Server

Below options can be possible reasons affecting the process.

- 1) Autokey password used to generate autokey file, mismatch at server and client side.
- 2) NTP client ntp.conf is configured for disable authentication or symmetric key authentication.
- 3) NTP client ntp.conf is wrongly configured for autokey parameters.
- 4) NTP client ntp.conf server address of MTS200 should have "autokey" keyword appended in its line.
- 5) Old keys not deleted at MTS200 side or ntp client side.
- 6) NTP service should be restarted at server and client side after configuration done.
- 7) Wrong autokey files transferred to ntp client
- 8) NTP client side autokey file names improper.
- 9) NTP client autokey files directory path and path defined in client ntp.conf should be same.

17.24 NTP Client Not synchronized with MTS200 using PC scheme AutoKey association with multiple MTS200 units.

Below options can be possible reasons affecting the process.

- 1) Autokey password used to generate autokey file, mismatch at server and client side.
- 2) NTP autokey files Private key and certificate contents of MTS200 as trusted server should be copied and pasted as Private key and certificate contents of MTS200 as server only.
- 3) Autokey password should be same of MTS200 trusted server, MTS200 server and other ntp autokey clients.
- 4) NTP client ntp.conf is configured for disable authentication or symmetric key authentication.
- 5) NTP client ntp.conf is wrongly configured for autokey parameters.
- 6) NTP client ntp.conf server address of MTS200 should have "autokey" keyword appended in its line.
- 7) Old keys not deleted at MTS200 side or ntp client side.
- 8) NTP service should be restarted at all MTS200 servers and client side after configuration done.
- 9) Wrong autokey files transferred to ntp client
- 10) NTP client side autokey file names improper.
- 11) NTP client autokey files directory path and path defined in client ntp.conf should be same.

17.25 NTP Client Not synchronized with MTS200 using IFF scheme AutoKey association with MTS200 as trusted Server

Below options can be possible reasons affecting the process.

Model: MTS200 (1U)

Doc. Ref. no. : m08/om/201

Issue no. : 03

- 1) Autokey password used to generate autokey files at client side should be added in client ntp.conf file. This password can be different from autokey password of MTS200 trusted server.
- 2) NTP client ntp.conf is configured for disable authentication or symmetric key authentication.
- 3) NTP client ntp.conf is wrongly configured for autokey parameters.
- 4) NTP client ntp.conf server address of MTS200 should have "autokey" keyword appended in its line.
- 5) Old keys not deleted at MTS200 side or ntp client side.
- 6) NTP service should be restarted at server and client side after configuration done.
- 7) Wrong autokey files transferred to ntp client
- 8) NTP client side autokey file names improper.
- 9) NTP client autokey files directory path and path defined in client ntp.conf should be same.

17.26 NTP Client Not synchronized with MTS200 using IFF scheme AutoKey association with multiple MTS200 units.

Below options can be possible reasons affecting the process.

- 1) Autokey password used to generate autokey file, mismatch at MTS200 trusted server and MTS200 as server side.
- 2) NTP autokey group key IFFkey contents of MTS200 as trusted server should be copied and pasted as Group key contents of MTS200 as server only and other ntp clients.
- 3) Autokey password used to generate autokey files at client side should be added in client ntp.conf file. This password can be different from autokey password of MTS200 trusted server.
- 4) NTP client ntp.conf is configured for disable authentication or symmetric key authentication.
- 5) NTP client ntp.conf is wrongly configured for autokey parameters.
- 6) NTP client ntp.conf server address of MTS200 should have "autokey" keyword appended in its line.
- 7) Old keys not deleted at MTS200 side or ntp client side.
- 8) NTP service should be restarted at all MTS200 servers and client side after configuration done.
- 9) Wrong autokey files transferred to ntp client
- 10) NTP client side autokey file names improper.
- 11) NTP client autokey files directory path and path defined in client ntp.conf should be same.

17.27 NTP association between MTS200 and ntp clients working with old NTP settings.

Below options can be possible reasons affecting the process.

- 1) NTP Service need to be restarted in MTS200 after any NTP related configurations change done in MTS200.
- 2) NTP Service need to be restarted in NTP client after any NTP related configurations change done.

17.28 NTP client not synchronize with NTP broadcast/Multicast frames from MTS200.

Below options can be possible reasons affecting the process.

- 1) NTP service need to restarted in MTS200 after broadcast or multicast settings changes done in MTS200 device.

- 2) Need to configure broadcast option in NTP client ntp settings and then restart NTP service at client side.
- 3) Authentication type should be same at MTS200 and client side if ntp authentication is used for ntp broadcast/multicast.
- 4) Multicast frames may be blocked by network IT routers or gateways.

17.29 Not able to create ntp autokey files in MTS200.

Below options can be possible reasons affecting the process.

- 1) Autokey files in MTS200 will be created only in PC scheme as MTS200 trusted Server mode or IFF scheme.

17.30 MTS200 webserver showing old configuration data.

Below options can be possible reasons affecting the process.

- 1) Old cookies or cache file stored in web browser settings. Delete old history files.
- 2) It is recommended to use IE 9.0+ web browser.
- 3) To disable MTS200 IP address in Web browser settings from storing any cookies or cache files.

17.31 IPv6 address showing “::”.

Below options can be possible reasons affecting the process.

- 1) IPv6 feature may be disabled.
- 2) IPv6 autoconf feature is disabled and not static IPv6 address is set by user.
- 3) Respective Ethernet port cable is not connected in network.

17.32 IPv6 address changed while MTS200 in operation.

Below options can be possible reasons affecting the process.

- 1) This will happen when both Ethernet ports are configured in Bonding mode. This can occur only when current active Ethernet port cable is disconnected from LAN and MTS200 internally switches to other Ethernet port connected in LAN. This will result in update in IPV6 global address according to current active Ethernet port.

17.33 IPv6 Link-Local address acquired but IPv6 Global address not acquired

Below options can be possible reasons affecting the process.

- 1) Autoconf feature is disabled.
- 2) IPv6 enabled router is not available in network.

17.34 Both Ethernet port showing same IPv6 Link-local and global address

Below options can be possible reasons affecting the process.

- 1) Bonding feature is enabled if both Ethernet port are connected in same network.

18 Abbreviations

1PPS	:	1 Pulse Per Second
AM	:	Amplitude Modulation
AC	:	Alternate Current
BNC	:	Bayonet Neill–Concelman Connector
BCD	:	Binary Coded Decimal
BCDYR	:	Binary Coded Decimal Year
BCDTOY	:	Binary Coded Decimal Time of Year
CE	:	Conducted Emission
CISPR	:	International special committee on Radio Interference
CF	:	Control Function
CR	:	carriage return
CRO	:	Cathode Ray Oscillator
CDMA	:	code division multiple access
DB9	:	D-Subminiature connectors, and houses 9 pins
dB	:	Decibels
DC	:	Direct Current
DCLS	:	Direct Current Level Shift
DHCP	:	Dynamic Host Configuration Protocol
DST	:	Day-Light Saving Time
DSP	:	Day-light Saving Pending
ESD	:	Electrostatic discharge
EMI	:	Electro-Magnetic interference
FDMA	:	Frequency Division Multiple Access
GMT	:	Greenwich Mean Time
GPS	:	Global Positioning System
GNSS	:	Global Navigation Satellite System
HTTP	:	Hypertext Transfer Protocol
HTTPS	:	Secure Hypertext Transfer Protocol
IPv4	:	Internet Protocol version 4
IRIG	:	Inter Range Instrumentation Group
IP67	:	Ingress Protection Marking - 67
IED	:	Intelligent Electronic Device
IEC	:	International Electrotechnical Commissions
IST	:	Indian Standard Time
IEEE	:	Institute of Electrical and Electronics Engineers
IANA	:	Internet Assigned Numbers Authority
LCD	:	Liquid-Crystal Display
LED	:	light-emitting diode
LF	:	Line Feed
LSP	:	Leap Second Pending
LS	:	Leap Second
MIB	:	Management Information Base
mAh	:	milliAmpere Hour
mS/msec	:	milliseconds
Mbps	:	Megabits per Second
NTP	:	Network Time Protocol
NMEA	:	National Marine Electronics Association
OCXO	:	Oven Controlled Crystal Oscillator
OID	:	Object Identifier
PC	:	Personal Computer
ppm	:	Parts per million
PPH	:	Pulse Per Hour
PPM	:	Pulse Per Minute

PTP	:	Precision Time Protocol
UTC	:	Coordinated Universal Time
UDP	:	User Datagram Protocol
RCC	:	Range Commanders Council
RTC	:	Real Time Clock
RFC	:	Request For Comments
RE	:	Radiated Emission
RG-6/RG-8	:	Radio Grade - 6
RF	:	Radio Frequency
SA	:	Selective Availability
SBS	:	Straight Binary Second
SNTP	:	Simple Network Time Protocol
SNMP	:	Simple Network Management Protocol
SSH	:	Secure Shell
SSL	:	Secure Sockets Layer
TCP	:	Transmission Control Protocol
TCXO	:	Temperature Compensated Crystal Oscillator
TDR-4	:	Time Distribution Rack – 4
TDU-64	:	Time Display Unit - 64
Telnet	:	Telecommunication Network
TSR-4	:	Time Signal Repeater - 4
TTL	:	Transistor Transistor Logic