

SSU-2000 PackeTime Supplement

This document provides information on the PackeTime module designed for operation in Symmetricom's SSU-2000 and SSU-2000e. It covers hardware and software operation associated with Release 5.0 and includes new TL1 commands that apply to the cards. For information on installing, operating, and provisioning the SSU-2000, refer to the *SSU-2000 User's Guide*, part number 12713020-002-2 and the *SSU-2000 Technical Reference*, part number 12713020-002-3, or the *SSU-2000e Users's Guide*, part number 12713148-002-2 and the *SSU-2000e Technical Reference*, part number 12713148-002-3.

In This Supplement

- [Overview](#)
- [PackeTime Module](#)
- [Maintenance Port Adapters](#)
- [TL1 Commands](#)
- [Ordering Information](#)
- [Technical Support](#)

Overview

The PackeTime module supports Network Time Protocol (NTP) with the Release 5.0 of firmware for the SSU-2000 and SSU-2000e. This module supports IEEE 1588 Precision Time Protocol (PTP) in the future with Release 6.0.

NTP is used to synchronize the time of any device running an NTP client, such as a GPS receiver or local timing source. The Symmetricom SSU-2000 and SSU-2000e with the PackeTime module provides NTPv3 functions, as described in RFC 1305. The SSU-2000/e acts as an NTP *server*, and distributes an accurate time packet to *clients* able to reach it via the IP network. For security reasons, the NTP packets are sent on a network separate from the SSU-2000 maintenance network.

With Release 5.0, the SSU-2000 supports up to six non-redundant PackeTime modules per Main shelf and up to ten non-redundant PackeTime modules per Expansion shelf. The SSU-2000e supports up to three non-redundant PackeTime modules per Main shelf and up to five non-redundant PackeTime modules per Expansion shelf.

Stratum 1 NTP servers are connected directly to a UTC (Universal Time Coordinated) time source, such as a GPS receiver. The SSU-2000 is a Stratum 1 NTP server when it is equipped with a GPS Input module that provides Time of Day (TOD) to the PackeTime module.

The SSU-2000 acts as a Stratum 2 NTP server when no GPS Input module is installed. Once the NTP time function has its time set by the Stratum 1 NTP server, a Stratum 2 NTP server provides UTC-traceable time to any requesting NTP client. The SSU-2000 is a Stratum 2 NTP server when it is no more than one “hop” from a Stratum 1 NTP server. In this case, the SSU-2000 is both an NTP client (of the Stratum 1 NTP server) and an NTP server (to connected clients). This is known as *peering*.

Security Considerations for a SSU-2000 Installation

- The SSU-2000 should be installed in a significantly robust physical security, e.g. inside a mantrap.
- The SSU-2000's Communication Module's Ethernet port should be installed behind the company's firewall to prevent public access.
- The SSU-2000's PackeTime Module's Maintenance port should be installed behind the company's firewall to prevent public access.
- Whenever possible, the SSU-2000's PackeTime Module's NTP Service ports should be installed behind the company's firewall to prevent public access.

Security Features of the SSU-2000's PackeTime Module

The introduction of the PackeTime Module into the SSU-2000 requires the design of the Ethernet interfaces to provide the highest level system security available and provide extremely accurate time of day, due to the fact that the PackeTime service (NTP or PTP) ports could be on public networks. The protocols running on the PackeTime module run behind an internal firewall on the module, this allows access to UDP ports to be limited or completely inaccessible by other systems. The PackeTime Module supports NTPv3, RFC 1305, NTP modes 3 (client), 4 (server), hardware timestamping of NTP packets for extremely accurate time transfer, and NTP authentication

For PackeTime providing NTP services, there are three TCP/UDP protocols active: ntp is on the two service ports, and ssh client and sftp client are on the maintenance port. For the initial release of PackeTime, the ssh client and sftp client are only active during module firmware upgrades. The TCP/UDP ports are opened for file transfer and once the firmware image has been successfully transferred from a host the TCP/UDP ports are closed and the upgrade process continues on the module. Each of the two Service ports only allow ntp UDP port (123) to be opened while ntp is active; ntp access can be enabled or disabled via user command.

The two service Ethernet ports on the PackeTime module operate in one of two modes, independent or bonded. In the Bonded mode (available in a future release), only one of the two ports is active at any given time, since bonding requires both ports to share the same IP address. They cannot be allowed to be active simultaneously or packet routing issues would occur. In the Independent mode, the two ports are each assigned unique IP addresses and can each serve time to independent networks. From a security perspective, the important thing to note about the Independent mode is that the PackeTime Module does not support routing protocols between the two service ports or between the service ports and the maintenance port. This prevents a malicious attack on Port A (network A) to be used to send a malicious attack via Port B (network B) or vice-versa, or between Port A or B networks and the Maintenance Port's network.

The PackeTime module supports a maximum ntp transaction rate of approximately 1500 request transactions per second. The requests can be on a single interface or split across both interfaces. If this maximum is exceeded the PackeTime module will continue to service 1500 requests per second, but it will not respond to requests above the maximum rate.

If the number of transactions (any type of TCP or UDP packet) per second exceeds 2500 per second, the PackeTime module will generate a notification to the user interface indicating excessive traffic is being seen on the Service ports. This could be an indication of a malicious attack or it could also be a large number of NTP clients requesting time from the server. The Service ports will remain active and simply provide an indication of excessive traffic.

If the PackeTime service ports do come under attack, only the module under attack will be affected due to the system's architecture, which prevents this module from corrupting the system 4 kHz clocks. The Comms Module will continue to provide all management facilities for the system during this type of attack. During system validation, the vulnerability tool Nessus was used to validate the PackeTime module's ability to defeat undesired access.

If a malicious attack was able to gain access to the SSU's PackeTime module via an Ethernet attack on either the service ports or the maintenance port:

- Gaining shell access would be extremely unlikely
 - The SSH shell is only active on the Maintenance port during module's firmware upgrades
 - The user should use the capabilities of SSH to use encrypted/secure access, this would be an additional deterrent.

If the attacker was able to gain shell access, in order to gain control of the system:

- They would then be required to know the memory location of the SPI driver to allow the SPI Slave to request service and send information to the system.
- Then they would have to know the SSU's proprietary SPI commands and protocol in order to send commands to system components to gain control of the system functions.

Security Attributes of the PackeTime's NTP implementation

As discussed above the PackeTime Module monitors for excessive traffic on the two service port interfaces. The cause of excessive traffic could be there are too many NTP clients requesting time from the server(s), if this is the case the load on the NTP server will need to be reduced by configuring some of the NTP clients to request time from another server. The other possible cause of excessive traffic is due to malicious attack(s). The PackeTime Module will generate an event to indicate to the user that the module may be under attack and action should be taken to resolve the issue.

With SSU Release 5.1, the PackeTime Module will support NTP authentication for both server and client modes of operation. NTP message authentication provides a mechanism to increase the confidence in the server or client that the NTP request or response did originate from a system within the authenticated domain. Authentication cannot 100% guarantee the received NTP datagram has not been spoofed or modified, but the probability of the authenticated message not being spoofed or modified is 99.999%. PackeTime has implemented hashing algorithms that can be used with NTP authentication, MD5 or SHA1, the standard is MD5 but due to some vulnerabilities with MD5 Symmetricom choose to add SHA1 as a hashing option as well.

Conclusions

- The SSU's architecture isolates functional areas such as user interfaces, the module-to-module interface, and output signal generation to minimize the possible corruption of time and frequency outputs.
- The SSU's Comms Module design provide isolation of the Ethernet interfaces to the system control plane via the SPI protocol.
- The SSU's PackeTime Module design provides the same type of Ethernet firewall via the SPI protocol that is implemented by the Comms Module.
- The PackeTime Module's Carrier-Class implementation of NTP provides extremely accurate time to clients (<10uS accuracy) as well as port bonding and module redundancy for failure recovery.
- The PackeTime Module can be configured to use authentication NTP messages for either Server or Client modes of operation, while continuing to provide a high transaction rate.
- Only service specific UDP protocols are enabled (running) on either the Comms or PackeTime Modules.
- From a system security perspective the SSU-2000 with PackeTime provides the highest level of security while providing a very accurate time of day output, but it also requires that the user implement best-practice security safeguards in their networks for the most robust levels security.

PackeTime Module

This section describes the PackeTime module (part number 23413325-000-0). It provides details on operation, configuration, alarms, events, and specifications.

Functional Block Diagram

A simplified block diagram of the PackeTime module is shown in [Figure 1-1](#).

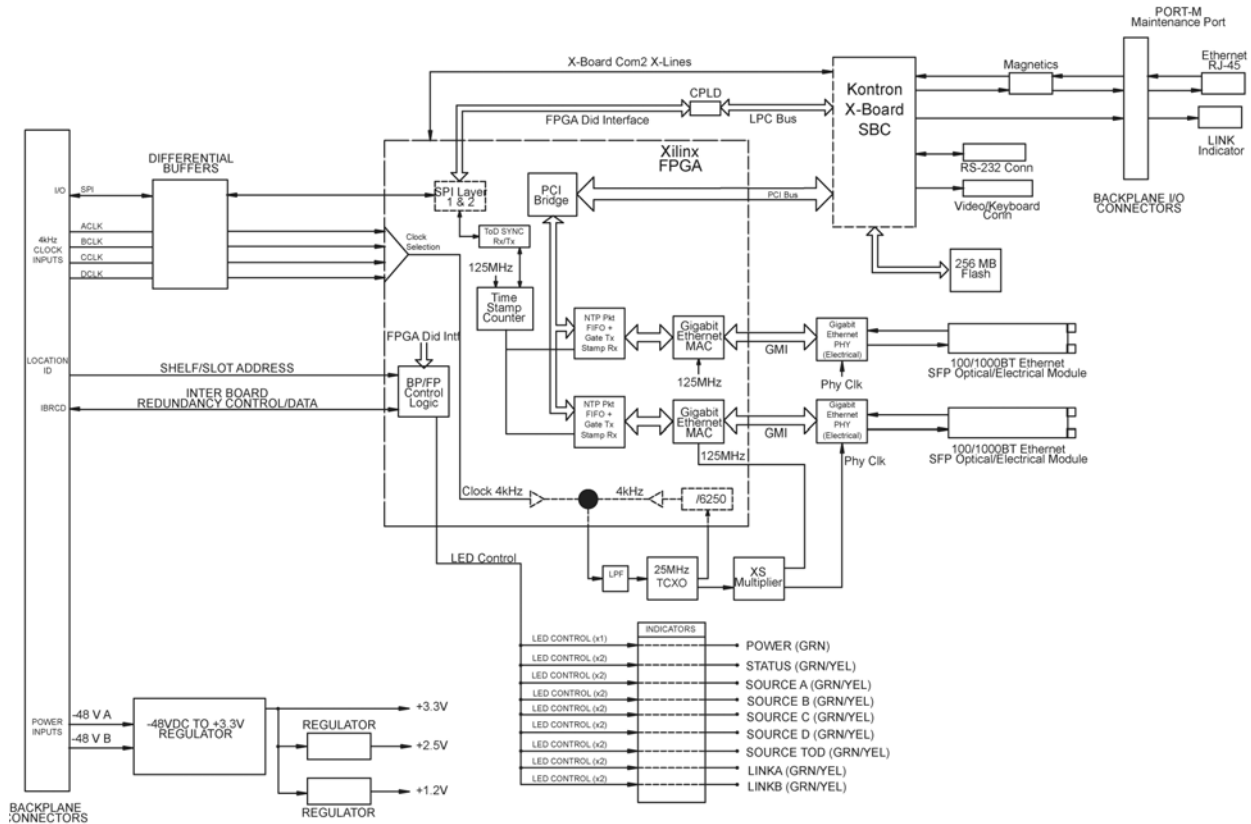


Figure 1-1. Block Diagram of the PackeTime Module

Alarms

Table 1-1 lists the alarm and event autonomous messages generated by the PackeTime module to report conditions. The Alarm category of autonomous messages reported by the Retrieve-Event-Alarm command are associated with conditions that have been identified as alarms (“CR”, “MJ”, “MN” and “CL”). All alarms are written into the event log. The severity of each alarm is fixed and cannot be provisioned to a different severity level.

Table 1-1. PackeTime Alarms

Alarm ID	Description of Alarm Condition	Alarm Delay	Default Alarm Severity
000 – 001	Loss of Clock source A, B	Immediate	Minor
002 – 003	Loss of Clock source C, D	20 s	Minor
004	Clock module selected	Immediate	Major
005	TOD no longer traceable to UTC	Immediate	Minor
006 – 007	NTP Service port A, B failure	10 s	Report
008	NTP Maintenance port failure	5 s	Minor

Table 1-1. PackeTime Alarms (Continued)

Alarm ID	Description of Alarm Condition	Alarm Delay	Default Alarm Severity
009	PackeTime module FPGA program error	Immediate	Major
010	PackeTime module PLL unlock	Immediate	Major
011	Loss of communication with redundant NTP port	Immediate	Report
012	Peer time	Immediate	Minor
013	Excess traffic on service port	Immediate	Minor

Table 1-2 lists the PackeTime alarm and event messages and a description or corrective action that you can take.

Table 1-2. PackeTime Module Alarm and Event Messages

Alarm/ Event/ Trap ID	Typical Alarm/Event/Trap Response	Description/ Corrective Action
000	CLK-A, Fault	Loss of Clock (source) A
001	CLK-B, Fault	Loss of Clock (source) B
002	CLK-C, Fault	Loss of Clock (source) C
003	CLK-D, Fault	Loss of Clock (source) D
004	Clk Selected, Fault	Clock source has been selected as reference
005	TOD Traceable, Fault	Time of Day is traceable to UTC
006	Link PA, Fault	Loss of link (connectivity) on Port A
007	Link PB, Fault	Loss of connectivity on Port B
008	Link PM, Fault	Loss of connectivity on Port M(aintenance)
009	FPGA, Fault	Loss of communication to FPGA
010	PLL, Fault	25 MHz PLL has unlocked
011	Redundant, Fault	Loss of communication with redundant module
012	Peer Time, Fault	Peer Mode only; Time error >1 second between module and Peer
013	Excess Traffic	Traffic load in excess of 2500 requests per second
129	Install, PackeTime	The module has been installed.
130	Remove, PackeTime	The module has been removed.
131	Enable, PackeTime	The module has been enabled.
132	Disable, PackeTime	The module has been disabled.
133	Restart, PackeTime	Module re-boot.

Table 1-2. PackeTime Module Alarm and Event Messages (Continued)

Alarm/ Event/ Trap ID	Typical Alarm/Event/Trap Response	Description/ Corrective Action
134	Cannot Enable, PackeTime	Internal firmware conflict. Restart module; if the problem persists, call SGS.
144	UTC Time, Set	Module's TOD has been set to UTC
145	Download, Successful	
146	TOD Set, by GPS	
147	TOD Set, by NTP	
148 ¹	Leap Sec, Pending	NTP will apply a leap second at midnight June 31 or December 31
149 ¹	Leap Sec, Inserted	NTP has applied a leap second at midnight June 31 or December 31
150 ¹	Bonding, PA Active, COML	Service ports have been configured in Bonded mode of operation
151	Slot, Active, COML	PackeTime module in specified slot is the Active module in a redundant NTP pair
152	Req Reboot, This Module	
153 ¹	Ports Network Setup, Requires Bonding	Provisioning two PackeTime modules to operate in redundant mode requires Bonding to be enabled
193	Image, 0, COML	Indicates that the firmware image 1 0 that is active
194	EthPort, ETH1, changed, COML	Ethernet port configuration change
195	TODSRC Prefer, TODSRC, COML	The Preferred Time of Day can be TODSRC or PEER
196	TODSRC Priority, 2, COML	TODSRC Priority set for this Module
197 ¹	Broadcast, DEL, 1, COML	NTP Mode of operation
198	Peer, ADD, 1, COML	NTP peer added
199	Prefer, Peer, 1, COML	NTP Peer added as preferred peer
200	Auth, 1, 2000	NTP Authentication key defined
201	PortAWeight, -1, COML	Load balancing configuration defined between NTP Port A and B
202	Committed, Set	Configuration stored in non-volatile memory
203	NTPd Service, Disable, COML	NTP Daemon has been disabled
204 ¹	Bond State, Enable, COML	Port bonding enabled
205 ¹	Bond Mode, ACTSTBY, COML	Module is in Active Standby
251	Err Delay, (1), 300 sec, COML	Modified error delay

Table 1-2. PackeTime Module Alarm and Event Messages (Continued)

Alarm/ Event/ Trap ID	Typical Alarm/Event/Trap Response	Description/ Corrective Action
252	Alm Level, (2), Maj, COML	Modified alarm level
253	Elevate Time, 7200 sec, COML	Modified alarm elevation time
254	Setup, User Default, COML	Changed the user-saved module configuration

Note:

¹Available in a future release.

TL1 Commands

Table 1-3 lists the new TL1 commands that are associated with Release 5.0 the SSU-2000 firmware. For details, refer to [TL1 Commands](#), on page 21 in this supplement and the *SSU-2000 Technical Reference*.

Table 1-3. PackeTime TL1 Commands

Command	Function
Load Program	Downloads the firmware to the specified PackeTime module
Retrieve Image	Retrieves the current firmware image from the specified module
Set Image	Provisions the specified PackeTime ports
Retrieve Ping	Pings a specified remote host via TCP/IP
Set Commit Parameters	Commits all uncommitted provisioned parameters in the specified module to become the active parameters
Retrieve IP Parameters	Retrieves the IP settings for the specified module
Set IP Parameters	Sets the IP parameters for the specified module
Retrieve NTP Module Parameters	Retrieves the current Source used by the specified PackeTime module
Set NTP Module Parameters	Sets the source for the specified PackeTime module
Retrieve NTP Peer Parameters	Retrieves the currently-assigned NTP servers, identified by index and IP address
Set NTP Peer Parameters	Sets up to eight NTP servers as peers.
Retrieve TOD Source	Retrieves the modules that are provisioned as TOD sources and their priorities
Set TOD Source	Sets the specified modules as TOD sources
Retrieve NTP Module Status	Displays the status information for the specified PackeTime module

Table 1-3. PackeTime TL1 Commands (Continued)

Command	Function
ACT-MODULE	Activates the specified module
DISC-MODULE	Deactivates the specified module
RST-MODULE	Resets the specified module
RTRV-INV	Displays the inventory information for the specified module

Status LED Indicators

The front panel of the PackeTime module contains eight status LEDs as shown in Figure 1-2. They are described in Table 1-4.



Figure 1-2. Front Panel of the PackeTime Module

Table 1-4. Status LED Indicators on the PackeTime Module

Indicator	Color	Description
POWER	Green	Off = Power is not present on the module On = The module is receiving power
STATUS	Green / Amber	Green = No module issues Amber = Module has detected a problem
Source A	Green / Amber / Off	Green = Clock source A is present and is selected. Amber = Clock source A is not present. Off = Clock source A is present, but not selected, or Clock source A is not selectable.
Source B	Green / Amber / Off	Green = Clock source B is present and is selected. Amber = Clock source B is not present. Off = Clock source B is present, but not selected, or Clock source B is not selectable.
Source C	Green / Amber / Off	Green = Clock source C is present and is selected. Amber = Clock source C is not present. Off = Clock source C is present, but not selected, or Clock source C is not selectable.
Source D	Green / Amber / Off	Green = Clock source D is present and is selected. Amber = Clock source D is not present. Off = Clock source D is present, but not selected, or Clock source D is not selectable.
Source TOD	Green / Amber	Off = Module is booting Green = Synchronized to TOD source Amber = No TOD source is available
Ethernet Link A	Green / Amber / Off	Green = Ethernet/Link activity (flickers with 1000 Mbps traffic) Amber = Ethernet/Link activity (flickers with 100 Mbps traffic) Off = No Ethernet connection
Ethernet Link B	Green / Amber / Off	Green = Ethernet/Link activity (flickers with 1000 Mbps traffic) Amber = Ethernet/Link activity (flickers with 100 Mbps traffic) Off = No Ethernet connection

Specifications

[Table 1-5](#) lists specifications for the PackeTime module with Release 5.0.

Table 1-5. PackeTime Specifications

Performance Characteristic	Specification
Network Protocol	NTP v3 – RFC1305 compliant IPv4
Time Stamping	Hardware Time Stamping
Inputs	Stratum 1: Time-of-Day feed from GPS Input module Stratum 2: Full NTP Client with peering
NTP Service Ports	2 Ethernet Small Form-factor Pluggable (SFP) Optical: 1000BaseX Electrical 100/1000BaseT
NTP Transaction Rate	1000/s fully authenticated, up to 1500/s unauthenticated
Authentication	MD5 (RFC1321) (available in a future release)
Protection	1+1 Protection (available in a future release)
Maintenance port	Used for firmware upgrades
Accuracy	10 μ s

Configuration Options and Default Settings

The configuration settings for the PackeTime module are listed in [Table 1-6](#).

Table 1-6. PackeTime Configuration Settings

Configuration Setting	Factory Default	Range
Alarm elevation time	86 400 s	60 – 500 000
Maintenance port		
IP address	10.0.0.100	Valid IPv4 address
Mask	255.255.255.0	Valid IPv4 address
Gate	0.0.0.0	Valid IPv4 address
Port A		
IP address	10.0.0.101	Valid IPv4 address
Mask	255.255.255.0	Valid IPv4 address
Gate	0.0.0.0	Valid IPv4 address
Port B		
IP address	10.0.0.101	Valid IPv4 address
Mask	255.255.255.0	Valid IPv4 address
Gate	0.0.0.0	Valid IPv4 address

Table 1-6. PackeTime Configuration Settings (Continued)

Configuration Setting	Factory Default	Range
TODSRC Preferred mode Priority	GPS 0 (No priority)	GPS PEER 0 ... 8
Bonding	Disable	Disable Enable
Port Weight	-1	-1 0 ... 100
External Peer list	None	Valid IPv4 address
Broadcast	None	Valid IPv4 address
Trusted Key	None	

Maintenance Port Adapters

You must install a Maintenance Port Adapter on the I/O ports associated with the slot in which the PackeTime module is installed. This adapter provides an Ethernet maintenance port separate from the NTP network. You use this maintenance port to upgrade the firmware in the PackeTime module. Three Maintenance Port Adapters are available, as shown in [Figure 1-3](#).

- Non-redundant operation, ANSI shelf (part number 22013323-000-0)
- Redundant operation, ANSI shelf (part number 220113324-000-0)
- Redundant operation, ETSI shelf (part number 22013326-000-0)

[Table 1-7](#) describes the Link LED on every adapter.

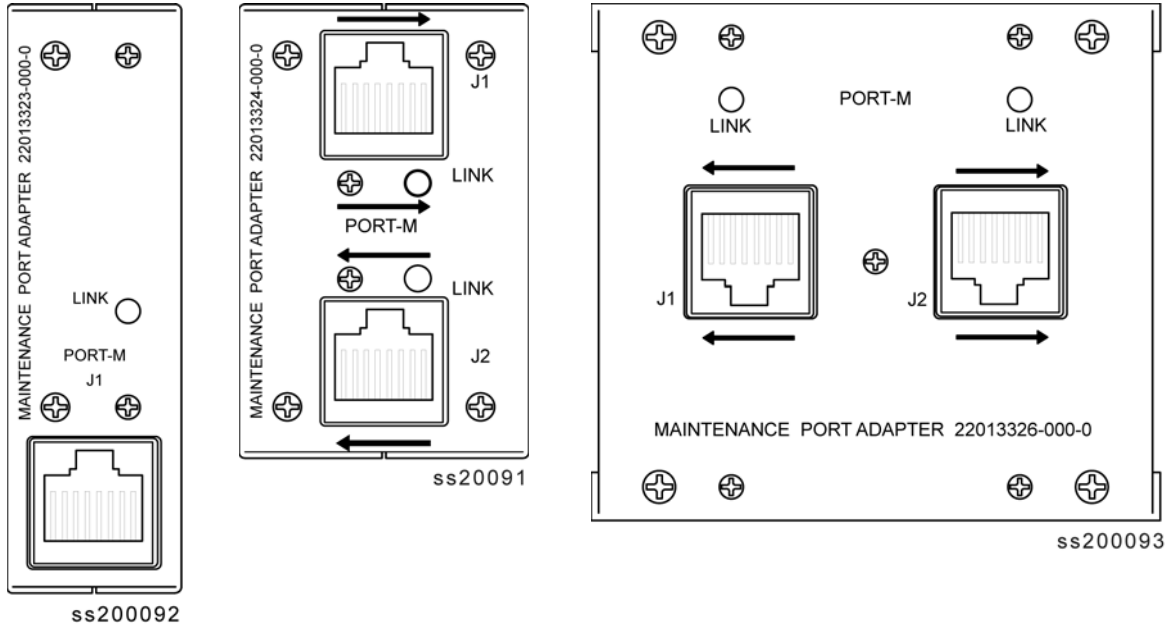


Figure 1-3. PackeTime Maintenance Port Adapters

Table 1-7. Status LED Indicator on the Maintenance Port Adapters

Indicator	Color	Description
Link	Green/Yellow	Green = Link is valid Green and flashing yellow = Link is valid and there is traffic Off = Link is not valid

Connectors

J1 and J2

These connectors are used to download firmware to the PackeTime module. Refer to [Downloading Firmware to the PackeTime Module](#), on page 16 for the procedure.

Handling Modules



Caution: To avoid equipment damage due to poor ventilation and EMI considerations, each slot in the SSU-2000 must contain either a module or blank filler panel. Filler panels are available for unpopulated slots.

Take the following precautions when handling any of the modules:

1. Use proper static control precautions when handling modules! Protect the equipment against ESD (electrostatic discharge) by using a grounded protective wrist strap and normal equipment grounding. Two ground connectors are provided on the side of the unit to connect these straps to frame ground (one on each mounting bracket).
2. Avoid touching component leads and edge connectors.
3. Avoid placing the module on an ungrounded surface.
4. Avoid allowing the module to come in contact with insulated surfaces.

Installing a Module

You can install a PackeTime module in the following slots:

- SSU 2000 Main shelf: slots A4 through A9 on a SSU-2000 Main shelf
- SSU-2000 Expansion shelf: slots A1 through A14
- SSU-2000e Main shelf: Either slot in a pair (A6 or A7, A8 or A9, A10 or A11)
- SSU-2000e Expansion shelf: Either slot in a pair (A1 or A2 through A9 or A10)

This procedure is common for all modules.



Note: Modules can be removed and inserted while system power is supplied without damaging modules or affecting system operation.



Caution: For continued EMC compliance, replace all deformed module gaskets with the same type. Clean gaskets and mating surfaces. Secure all modules with captive screws.

To install a module:

1. Align the module card edges with the plastic card guides of the selected slot.
2. Slide the module into the shelf until it seats fully into its rear panel edge connector.
3. Tighten the captive screws located at the top and bottom of the module front panel.



Caution: To avoid possible damage and intermittent failures, ensure that you have completely inserted the module into the system and that you have securely tightened the captive screws.

Downloading Firmware to the PackeTime Module

Downloading firmware to the PackeTime module involves a file transfer from an FTP server to the Maintenance port. The TL1 command LOAD-PROGRAM contains the parameters necessary to download a new firmware load to the PackeTime module. See [Load Program](#), on page 28 for more details.

Making Connections

Connecting the PackeTime Module to the Network

You can use either an optical or electrical network cable with the PackeTime module. Install the appropriate SFP interface module (optical or electrical) into Port A or Port B on the front panel of the PackeTime module, then attach the appropriate network cable. If you are using only one of the ports, you must use Port A.

To provide optimum NTP service levels, you must place the Maintenance port and Service port(s) on separate physical networks.

Provisioning the NTP Addresses

You must assign an IP address and mask for each port on the PackeTime module.

1. Establish a serial connection to the SSU-2000 shelf using the procedures in the *SSU-2000 User's Guide*.
2. Use the following example commands to provision the addresses:

```
SET-PRMTR-IP::SxAy-A:SSU::<ip_address>,<mask>,<gate>;  
SET-PRMTR-IP::SxAy-B:SSU::<ip_address>,<mask>,<gate>;  
SET-PRMTR-IP::SxAy-M:SSU::<ip_address>,<mask>,<gate>;
```

Provisioning the TOD Source

You must assign the TOD source for the PackeTime module.

1. Establish a serial connection to the SSU-2000 shelf using the procedures in the *SSU-2000 User's Guide*.
2. Use the following example command to provision the TOD source:

```
SET-TODSRC::S1A5::SSU::0;
```

This command sets the GPS module in slot A5 as the TOD source, and sets the priority to 0.

Testing the PackeTime Module

Perform the tests in this section to verify that the PackeTime module is operating correctly.

LED Indications

The LEDs on the PackeTime module illuminate in the following sequence when you install the PackeTime module:

- The Status LED illuminates after approximately 60 seconds, then blinks during the boot process. The LED then turns solid green, indicating that the PackeTime module has successfully booted and that it is the active module.
- The Source TOD LED illuminates when the PackeTime module is receiving a valid ToD signal.
- The SFP A and B LEDs are off when there is no connection. When connected to a network, they blink in one of two colors: amber for 100 Mbps activity or green for 1000 Mbps (1 Gbps) activity.

Verifying the IP Addresses

This test sets the IP address, mask, and gateway for the PackeTime module Port-A and Port-B and verifies that the addresses are functioning properly.

1. Open a TL1 session with the SSU-2000 using terminal emulation software such as Procomm Plus or TeraTerm Pro, or from a Windows command line. If you are already logged in, skip to step 4.
2. Type `telnet <ssu_ip_address> 2000`.
3. Log in to the SSU-2000 with a valid username and password:

```
ACT-USER:[tid]:uid:ctag::pwd;
```

where `<uid>` is a valid username and `<pwd>` is the valid password for that username.

4. Set the PackeTime module's Port-A IP address, mask and gateway:

```
SET-PRMTR-IP::SxAy-A:SSU::<ip_address>,<mask>,<gate>;
```

where

`<ipaddress>` = desired IP address for NTP port A

`<mask>` = desired subnet mask

`<gate>` = desired gateway IP address

5. Verify the Port-A IP settings:

```
RTRV-PRMTR-IP::SxAy:SSU;
```

where *SxAy* is the location of the PackeTime module.

6. Send a ping command to the Port-A IP address: Open a command window in Windows XP (click Start, select Run, type `cmd` and click **OK**. Type `ping <ip_address>` and click **OK**.
7. Verify that a reply is received from Port-A. If a “Request timed out” message is received, ensure that the computer is correctly connected to the network that Port-A is connected to.
8. Repeat steps 4 through 7 for the Port-B address.

Verifying the In-Service Function

This test sets the administrative state of the PackeTime module to In-Service. When in the In-service state, the module responds to NTP requests received on the NTP Service port.

1. Open a TL1 session with the SSU-2000 using terminal emulation software such as Procomm Plus or TeraTerm Pro, or from a Windows command line. If you are already logged in, skip to step 4.
2. Type `telnet <ssu_ip_address> 2000`.
3. Log in to the SSU-2000 with a valid username and password:

```
ACT-USER:[tid]:uid:ctag::pwd;
```

where *<uid>* is a valid username and *<pwd>* is the valid password for that username.

4. Verify the current state of the PackeTime module:

```
RTRV-STATUS-NTPMOD::SxAy:SSU;
```

The module's current state may be ENA or DIS.

5. Change the state of the PackeTime module to In-service:

```
ACT-MODULE::SxAy:SSU;
```

6. Verify that the PackeTime module is ready to receive NTP requests:

```
RTRV-STATUS-NTPMOD::SxAy:SSU;
```

The module's current state should be ENA.

Verifying the NTP Server Function

This test verifies that the PackeTime module is functioning and sending NTP packets.



Note: This procedure resets the clock in your computer to the time in the specified NTP server. If you do not wish to reset the time in your computer, then skip this procedure.

This procedure uses the SymmTime™ application available at www.ntp-systems.com. Follow the on-line instructions to download and install the application. You must have administrator rights on the computer in order for SymmTime to function properly.

Procedure

1. Start the SymmTime application.
2. Right-click anywhere in the SymmTime window and select **Sync Servers...** The Sync Servers window appears similar to the example shown in [Figure 1-4](#).

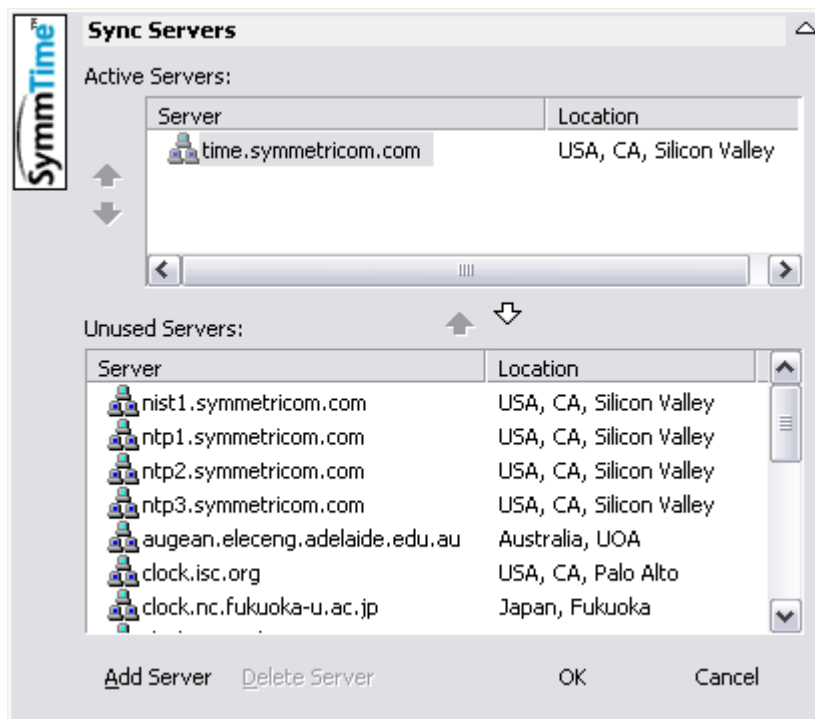


Figure 1-4. The Sync Server Window in SymmTime

3. Highlight all server names in the Active Servers: pane and click the down arrow. This moves them to the Unused Servers: pane.
4. Click **Add Server**. The New Server window appears, as shown in [Figure 1-5](#).

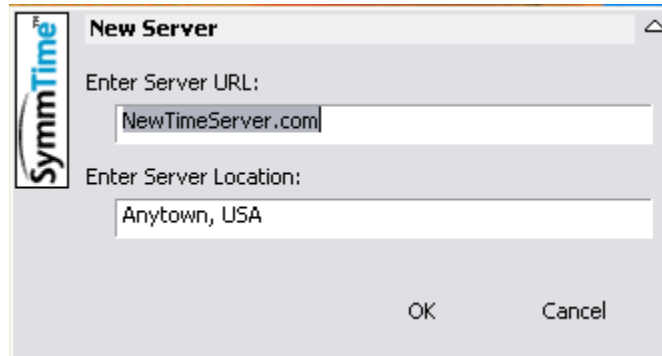


Figure 1-5. The New Server Window in SymmTime

5. Enter the IP address of the PackeTime module in the **Enter Server URL:** field.
6. Type a name for the PackeTime module in the **Enter Server Location:** field. This step is optional.
7. Click **OK** to close the New Server window. The PackeTime module URL or IP address and Location appear in the Active Servers pane of the Sync Servers window.
8. Click **OK** to close the Sync Servers window.
9. Right-click anywhere in the SymmTime window and select Sync Status... The Synchronization Status window appears as shown in [Figure 1-6](#).

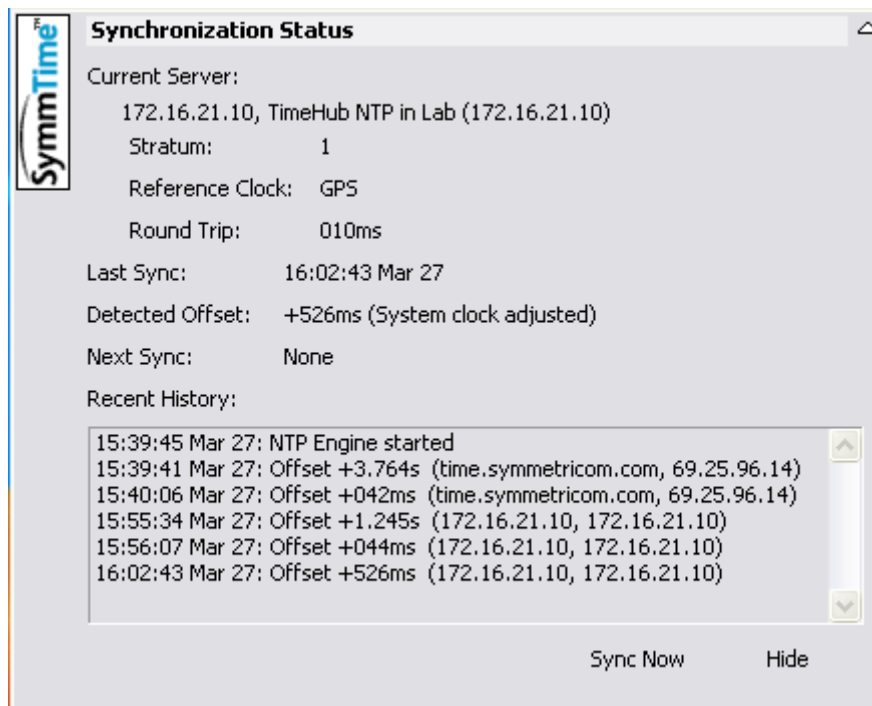


Figure 1-6. The Synchronization Status Window in SymmTime

10. Click **Sync Now**. The new time and any offset from the PackeTime module appears. This verifies that the PackeTime module and the connection to the card is operating properly.

If the PackeTime module or the connection to the PackeTime module is not working, a message appears that says SymmTime cannot connect to the server. Troubleshoot the connection first, then the PackeTime module.

TL1 Commands

This section lists TL1 commands associated with the PackeTime module. Refer to the *SSU-2000 Technical Reference* for details on TL1 command syntax.

Retrieve NTP Module Parameters

This command returns the current ToD source used by the PackeTime module designated by the aid.

Syntax

RTRV-PRMTR-NTPMOD:[tid]:aid:ctag;

Parameter	Value	Description
aid	SxAy	Retrieves the ToD source from the specified PackeTime module

Response Format

^^^"aid:<preferred>,(weight)" <cr><lf>

where:

- aid = module access identifier
- preferred = TODSCR | PEER
- weight = -1 | 0 | ... | 100 and is the load (bandwidth) distribution between port-A and port-B. See [Set NTP Module Parameters](#), on page 21, for further details.

Related Commands

[Set NTP Module Parameters](#)

Set NTP Module Parameters

This command selects the source of the ToD used by the PackeTime module designated by the aid. To make the changes selected by this command, you must execute the SET-PRMTR-COMMIT command after executing this command.

Syntax

SET-PRMTR-NTPMOD:[tid]:aid:ctag::<preferred>,<weight>;

Parameter	Format	Description
aid	SxAy	Aid for the PackeTime module.
preferred	TODSRC PEER	TODSRC sets the GPS module as the source PEER selects a Peer if operating in Client or Broadcast Client mode. Setting the PREFERRED keyword to TODSRC selects the GPS module as the TOD source. For Release 5.0, it uses the GPS Priority to determine which GPS Input has priority. If the TOD source fails, the PackeTime module will failover to the Peer List. When you set PREFERRED to PEER, then the servers on the Peer List are used until exhausted of valid NTP servers, and then it would failover to GPS if available. Both modes are Auto-Revertive: they switch back to the primary source once it has been validated as good.
weight	-1 0 ... 100	Sets the load (bandwidth) distribution between port-A and port-B as a percentage. For example, 70 means port-A get 70% of total bandwidth, port-B gets the remaining 30%. If port-A reaches 70% of total bandwidth but port-B has no traffic, the 30% of bandwidth is wasted, because port-A cannot use it. To allow either port to use all the bandwidth, weight can be set to -1, indicating no limit between port-A and port-B (either port-A or port-B can get all the bandwidth, based on first-come, first-serve). Thus the range of this parameter -1 to 100. For bonding mode, this parameter must be forced to -1, so the active port can use 100% of the bandwidth. For non-bonding mode, you can set any value between -1 and 100.

Related Commands

- [Retrieve NTP Module Parameters](#)
- [Set Commit Parameters](#)

Retrieve NTP Peer Parameters

This command returns the currently-assigned NTP servers; they are identified by index and IP address.

Syntax

RTRV-PRMTR-NTPPEER:[tid]:aid:ctag;

Parameter	Value	Description
aid	SxAy	Aid for PackeTime modules

Response Format

```
^^^"aid:index,ip,min,max"<cr><lf>
^^^...<cr><lf>
^^^"aid:preferindex"<cr><lf>
```

where:

- `index` = defines a value of 1 through 8 to provide an index of the NTP server(s); the default is 1
- `ip` = the ip address used by the server
- `min` = 16 | 32 | 64 | 128 | 256 | 512 | 1024 and is the minimum request rate in seconds for Client mode; the default is 16
- `max` = 16 | 32 | 64 | 128 | 256 | 512 | 1024 and is the maximum request rate in seconds for Client mode; the default is 1024
- `preferindex` = the Preferred Peer index, where 0 = no preferred server and 1 – 8 indicates the preference value (lower number = higher preference)

Related Commands

[Set NTP Peer Parameters](#)

Set NTP Peer Parameters

This command allows you to define up to eight NTP Servers (defined by their IP address), allowing the PackeTime module to operate in NTP Mode 3, NTP Client. To make the changes selected by this command, you must execute the `SET-PRMTR-COMMIT` command after executing this command.

Syntax

```
SET-PRMTR-NTPPEER:[tid]:aid:ctag::<function>,<index>[,<ip>,<min>,<max>];
```

Parameter	Value	Description
aid	SxAy	Aid for PackeTime modules
<function>	ADD DEL PREFER	Adds or deletes the NTP server at the specified IP address, or sets it to the Preferred server
<index>	0 1 - 8	When <function> = PREFER, sets an arbitrary index value to the NTP server at the specified IP address; 0 = no preference, default is 1
<ip>		Defines the IP address of the NTP server
<min>	16 32 64 128 256 512 1024	Sets the minimum request rate in seconds in Client mode; default is 16
<max>	16 32 64 128 256 512 1024	Sets the maximum request rate in seconds in Client mode; default is 1024

Related Commands

[Retrieve NTP Peer Parameters](#)

Retrieve TOD Source

This command displays the aid of each SSU-2000 module that is provisioned as a ToD source, and its assigned priority.

Syntax

```
RTRV-TODSRC:[tid]:[aid]:ctag;
```

Response Format

```
^^^"aid:priority1"<cr><lf>  
^^^...<cr><lf>  
^^^"aid:priority8"<cr><lf>
```

Related Commands

[Set TOD Source](#)

Set TOD Source

This command allows you to provision appropriate SSU-2000 modules (either GPS or PackeTime) as ToD sources, and to set their assigned priority. To make the changes selected by this command, you must execute the `SET-PRMTR-COMMIT` command after executing this command.

Syntax

```
SET-TODSRC:[tid]:aid::ctag::priority;
```

Parameter	Value	Description
aid	SxAy	Aid of a module that can deliver ToD
priority	0 1 - 8	Priority level of the ToD source module

Related Commands

[Retrieve TOD Source](#)

Retrieve Ping

This command allows you to ping a remote host via TCP/IP. Use this command to verify that the SSU-2000 is communicating over a network.

Syntax

```
RTRV-PING::[aid{-A | B | M}]:ctag::<ip>;
```

Parameter	Value	Description
aid	S1A2	Default aid if no aid specified
	SxAy{-A B M}	Aid for PackeTime modules
ip	####.####. ####.####	Specifies the host address, given in IPv4 format, where ### is a number between 0 and 255

Response Format

The response message is COMPLD if the ping was successful or DENY (SDNR) if unsuccessful.

Set Commit Parameters

This command commits all uncommitted provisioned parameters to become the active parameters for the specified PackeTime module. This command also commits the parameters to non-volatile memory.



Note: You *must* execute this command after setting NTP/PackeTime parameters using the [Set NTP Module Parameters](#) and/or [Set NTP Peer Parameters](#) commands. Failure to execute this command leaves the original parameters unchanged.

Syntax

```
SET-PRMTR-COMMIT:[tid]:aid:ctag;
```

Parameter	Value	Description
aid	SxAy	Aid for PackeTime modules

Related Commands

All PackeTime commands

Retrieve NTP Module Status

This command displays the status of the specified PackeTime module.

Syntax

```
RTRV-STATUS-NTPMOD:[tid]:aid:ctag;
```

If no aid is specified, then ALL is assumed.

Response Format

```
^^^"aid:mstat"<cr><lf>
```

where:

- `mstat` = ENA | DIS as set by the ACT-MODULE and DISC-MODULE commands

Related Commands

ACT-MODULE, DISC-MODULE

Retrieve NTP Peer Status

This command displays the current NTP status of the specified PackeTime module.

Syntax

```
RTRV-STATUS-NTPPEER:[tid]:aid:ctag;
```

Response Format

```
^^^SYS: syspeer, leap, stratum, precision, rootdelay, rootdispersion,  
offset"<cr><lf>
```

```
^^^REFTIME: reftime"<cr><lf>
```

```
^^^PEER:peer1, refid, stratum, poll, reach, delay, offset, jitter"<cr><lf>
```

```
.
```

```
^^^PEER:peer8, refid, stratum, poll, reach, delay, offset, jitter"<cr><lf>
```

where:

- `syspeer` = IP address of peer selected by server as most likely to provide best timing information
- `leap indicator` = The NTP server leap indicator (0, +1, -1, or NOSYNC)
- `precision` = Measure of the number of significant bits in NTP timestamp
- `rootdelay` = The calculated root delay value to primary source
- `rootdispersion` = The NTP system Root Dispersion (max error relative to the primary reference source at the root of the synchronization subnet, in seconds)
- `reftime` = The local time
- `peern` = IP address of NTP peer *n*
- `refID` = The NTP system Reference
- `stratum` = The NTP server stratum level
- `poll` = The NTP server poll interval
- `reach` = The NTP server reachability
- `offset` = The client's calculated time offset value for the specified server

Related Commands

[Set NTP Peer Parameters](#)

Retrieve IP Parameters

This command returns the current Internet Protocol settings for the specified module. The default aid (if not included in the command) specifies the Communications module.

Syntax

```
RTRV-PRMTR-IP:[tid]:[aid]:ctag;
```

Response Format

```
^^^"S1A2:addr,mask,gate,mac<cr><lf>
```

or

```
^^^"aid-A:addr,mask,gate,mac"<cr><lf>
```

```
^^^"aid-B:addr,mask,gate,mac"<cr><lf>
```

```
^^^"aid-M:addr,mask,gate,mac"<cr><lf>
```

where:

- aid-A = NTP Port A
- aid-B = NTP Port B
- aid-M = Maintenance port
- addr = the port's IP address
- mask = the port's IP mask
- gate = the port's IP gateway
- mac = the Media Access Control address

All IP numbers are in the IPv4 format (###.###.###.###).

Related Commands

[Set IP Parameters](#)

Set IP Parameters

This command sets the Internet Protocol parameters. To provide optimum NTP service levels, you must place the Maintenance port and Service port(s) on separate physical networks.

Syntax

```
SET-PRMTR-IP:[tid]:aid[-A|B|M]:ctag::[addr],[mask],[gate];
```

Parameter	Format	Description
<aid>	S1A2	Specifies the Communications module
	SxAy[-A B M]	Specifies the PackeTime module [port-A, port-B, or Maintenance port]

Parameter	Format	Description
addr		Sets the IP address for the specified module
mask		Sets the IP mask for the specified module
gate		Sets the IP gate for the specified module

where:

- `aid-A` = NTP Port A
- `aid-B` = NTP Port B
- `aid-M` = Maintenance port
- `addr` = the port's IP address
- `mask` = the port's IP mask
- `gate` = the port's IP gateway

All IP numbers are in the IPv4 format (###.###.###.###).

Related Commands

[Retrieve IP Parameters](#)

[Set Commit Parameters](#)

Load Program

This command downloads the firmware to a PackeTime module. The command is invoked through the Ethernet port on the Communications module, and the file is transferred through the Maintenance port on the PackeTime module. During the transfer, a Progress code is issued. An event notification is generated to report the success or failure of the command.

The PackeTime module has memory locations for two firmware versions. This command loads the firmware into the location (0 or 1) that is not currently active. When you reboot the module, it loads the most recent firmware version.

To determine the location (0 or 1) of the currently-active firmware, issue the RTRV-IMAGE command (described below).

To determine the version number of the currently-active firmware, issue the RTRV-INV or the RTRV-IMAGE command. Refer to the *SSU-2000 Technical Reference* for details.

Syntax

```
LOAD-PROGRAM:[tid]:aid:ctag:<filename>,<ftp-server>,<user>,<passwd>,<reboot>;
```

where:

- `filename` = the image file to be downloaded. The file path may be required as part of the filename.
- `ftp-server` = the server IP address in IPv4 format (`###.###.###.###`)
- `user` = the username requiring access to the server
- `passwd` = the password associated with the user
- `reboot` = `REBOOT` | `MANUAL` for the firmware to reboot after the download. If not specified, the default value is `REBOOT`.

Example

The following is an example firmware upgrade command, where the PackeTime module is installed in slot S1A6, the cTag is 100, the filename is /17313325-000-5_Rev_A00.rpm, the ftp server address is 172.16.21.107, the username is `austinuser`, and the password is `austinpsw`.

The format of the Progress code is:

```
IP ctag <cr><lf>
```

When the download process is complete, the PackeTime module reboots.

```
LOAD-PROGRAM::S1A6:100::"/17313325-000-5_Rev_A00.rpm", "ftp:172.16.21.208", "austinusr", "austinpsw", REBOOT;
```

```
SSU_2000 07-10-17 14:12:12
M 100 COMPLD
IP 100
<IP 100
<IP 100
. . .
. . .
<IP 100
<  "\"COMPLETED, MODULE RESTART\""
```

```
SSU_2000 07-10-17 14:16:41
A 000003 REPT EVT
"S1A06:NA,145,NSA,07-10-17,14-16-40:\"Download, Successful\""
```

```
SSU_2000 07-10-17 14:16:41
A 000004 REPT EVT
"S1A06:NA,133,NSA,07-10-17,14-16-40:\"Restart, in process, SYS\""
```

Retrieve Image

This command returns the location of the current firmware image in use by the specified PackeTime module.

Syntax

```
RTRV-IMAGE:[tid]:aid:ctag;
```

Response Format

```
^^^"aid:current_partition,reboot_partition"<cr><lf>  
^^^"PARTITION-0,revision,date"<cr><lf>  
^^^"PARTITION-1,revision,date"<cr><lf>
```

where:

- current_partition = 0 | 1
- reboot_partition = 0 | 1

Example Response

```
SSU-2000 07-07-10 12:58:32  
M 100 COMPLD  
"PARTITION-0,A.00,09JUL2007"  
^^^"PARTITION-1,A.00,09JUL2007"
```

Related Commands

[Set Image](#)

Set Image

This command selects which of two firmware images is loaded when the PackeTime module reboots.

Syntax

```
SET-IMAGE:[tid]:aid:ctag::image;
```

where:

- image = 0 | 1

Related Commands

[Load Program](#), [Retrieve Image](#)

Other Commands

```
ACT-MODULE:[tid]:aid:ctag;
```

Valid aid codes: SxAy

This command activates (enables) a module (not a specific port).

DISC-MODULE:[tid]:aid:ctag;

Valid aid code; SxAy

This command disconnects (disables) a module (not a specific port).

RST-MODULE:[tid]:aid:ctag;

Valid aid code: SxAy

This command restarts (reboots) the specified module.

RMV-MODULE:[tid]:aid:ctag;

Valid aid code: SxAy

This command removes the module configuration information from the database.

ACT-USER:[tid]:uid:ctag::pwd;

Valid aid code: none; requires user name (uid) instead.

This command logs in the username `uid` with password `pwd`.

CANC-USER:[tid]::ctag;

Valid aid code: none

This command logs off the current TL1 user and returns the unit to security level 0 (Idle).

EXIT:[tid]::ctag;

Valid aid code: none

This command logs off the current user and returns an RS-232 port to ASCII mode, or disconnects an Ethernet session to end TL1 communication.

Ordering Information

The order numbers for the SSU-2000 PackeTime parts and accessories are listed in [Table 1-8](#).

Table 1-8. SSU-2000 PackeTime Parts and Accessories

Description	Part Number
PackeTime module	23413325-000-0
Maintenance Port Adapter Non-redundant ANSI	22013323-000-0
Ethernet SFP modules	
Optical LX 1310 nm (single mode)	121-20621-10-2
Optical SX 850 nm (multimode)	121-20621-11-2
Electrical 100/1000BaseT (autosensing)	121-20621-12-2
PackeTime Kits	
PackeTime Kit without SFPs	990-13325-00
PackeTime Kit with LX 1310 nm single mode optical SFPs	990-13325-01
PackeTime Kit with SX 850 nm multimode optical SFPs	990-13325-02
PackeTime Kit with autosensing 100/1000Base T electrical SFPs	990-13325-03

The order numbers for the SSU-2000e PackeTime parts and accessories are listed in [Table 1-9](#).

Table 1-9. SSU-2000e PackeTime Parts and Accessories

Description	Part Number
PackeTime module	23413325-000-0
Maintenance Port Adapters Redundant ETSI	22013326-000-0
Ethernet SFP modules	
Optical LX 1310 nm (single mode)	121-20621-10-2
Optical SX 850 nm (multimode)	121-20621-11-2
Electrical 100/1000BaseT (autosensing)	121-20621-12-2
PackeTime Kits	
PackeTime Kit without SFPs	990-13325-05
PackeTime Kit with LX 1310 nm single mode optical SFPs	990-13325-06
PackeTime Kit with SX 850 nm multimode optical SFPs	990-13325-07
PackeTime Kit with autosensing 100/1000Base T electrical SFPs	990-13325-08

Reference Information

Acronyms

- GPS Global Positioning System
- IPTV Internet Protocol Television
- NTP Network Time Protocol
- PTP Precision Time Protocol
- PRS Primary Reference Source
- RPS Requests per second (NTP requests)
- SSU Synchronization Supply Unit
- TOD Time Of Day

References

- RFC 1305
- RFC 2030
- NTPv4 (IETF WG draft expiring 9/2/06)
- IEEE 1588
- IEEE 802.3-1998

- IEEE 802.3ab, 1999, 1000BaseT GE (metallic)
- IEEE 802.3z, 1998, 1000BaseX GE (fiber)
- IEEE 802.3u, 1995, 100BaseT FE

Technical Support

If you encounter any difficulties installing the update or operating the product, contact Symmetricom Global Services:

U.S.A. Call Center (for USA, Canada, Latin America including Caribbean, Pacific Rim including Asia, Australia, and New Zealand)
Symmetricom, Inc.
2300 Orchard Parkway
San Jose, CA 95131-1017

Toll-free in North America: 888-367-7966
Telephone: 408-428-7907
Fax: 408-428-7998
E-mail: support@symmetricom.com

Europe, Middle East, and Africa (EMEA) Call Center:
Symmetricom Global Services EMEA
Fichtenstr. 25
85649 Hofolding Germany

Telephone: +49 700 3288 6435
Fax: +49 810 4662 433
E-mail: emeasupport@symmetricom.com

Internet: www.symmetricom.com

