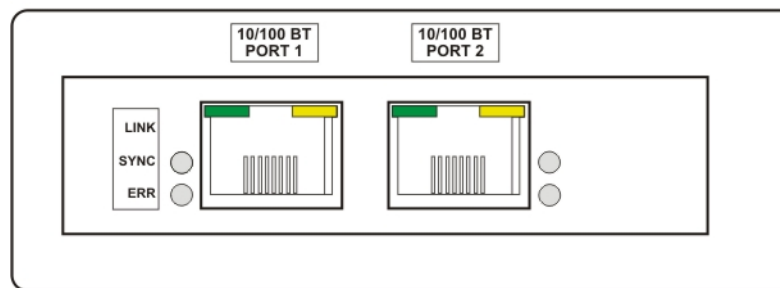


Option 34: NTP/PTP Server Setup and Operating Guidelines



Option 34 - Rear Panel Layout Drawing

Document No. PD0044300B

Arbiter Systems, Inc.
1324 Vendels Circle, Suite 121
Paso Robles, CA 93446 U.S.A.
(805) 237-3831, (800) 321-3831
<http://www.arbiter.com>
[mailto: techsupport@arbiter.com](mailto:techsupport@arbiter.com)

Contents

1 Option 34: NTP/PTP Server	3
1.1 General Description	3
1.2 Option 34 Setup	4
1.3 Glossary of Key Terms and Definitions	8
1.4 Specifications	11
1.5 HTTPS/SSL Certificate	12
1.6 Time Zone Format Strings	14

PRODUCT INFORMATION

This area is for you to write down pertinent information regarding your product. Take time to identify some necessary information, such as the password. In the event that the password is lost, it will be necessary to be returned to the factory to reset it to default settings. See also Section 1.3.

SERIAL NUMBER:	
PASSWORD:	

1 Option 34: NTP/PTP Server

1.1 General Description

Option 34 provides Network Time Protocol (NTP) and Precision Time Protocol (PTP)¹ servers in Arbiter Models 1084A/B/C, 1088A/B and 1093A/B/C GPS series clocks. These instructions will assist you in the setup and configuration of the Option 34 NTP/PTP server. Configure Option 34 using the Web Interface or the SSH Console.

Option 34 has two independent server ports that can access either the NTP (versions 1, 2, 3 or 4 frames) or the PTP servers. This option has been designed in accordance with the latest NTP and PTP standards and may be updated whenever new firmware is available.

PTP with hardware assist offers much better accuracy than with NTP, however to achieve these accuracies requires PTP-enabled network components that provide for latency and jitter to be determined between the clock and each component. When designing for the ultimate in PTP accuracy, evaluate every component in the complete network.

Network Time Protocol (NTP) Server

Option 34 allows the clock to act as network (NTP) time server over an Ethernet network and understands NTP version 1 – 4 frames, while optionally supporting authentication via DES and MD5 cryptographic checksums as defined in RFC 5905². Option 34 supports symmetric key authentication. Time is distributed over the network interface to computers, controllers and other equipment needing the correct time. Option 34 allows a secure connection to configure, using either the preferred HTTPS Web Interface, or using the SSH Console.

Precision Time Protocol (PTP) Server

Option 34 allows the clock to act as a Precision Time Server (PTP) according to Standard IEEE 1588 2008. However for highest accuracy, the entire network where PTP is required must have PTP-enabled network components. Without hardware assist through the physical interface, PTP will provide time with the same accuracy as with NTP. Accuracy with hardware assist using PTP should be better than 1 microsecond. Accuracy without hardware assist should be better than 100 microseconds.

Configuration Protocols

Three types of configuration protocols are allowed on the Option 34: HTTP, HTTPS and Secure Shell (SSH). Of the three, HTTPS and SSH permit secure channels on the network between the user and the Option 34. If a secure channel is required, choose either HTTPS using the Web Interface, or SSH using the Console. HTTPS requires that a valid signed certificate (PEM file) be uploaded into the Option 34. Use of Console does not require a signed certificate. Both of these methods are discussed in the following pages, and both require a Username and Password to open a connection. To access Option 34 using the Web Interface you will need Web browser. To access Option 34 using the Console, you will need an SSH client. These instructions use an SSH client called PuTTY when describing the Console Interface. Option 34 comes by default configured for an HTTP connection, and may be configured to use HTTPS.

¹IEEE 1588v2 – IEEE 1588-2008

²Includes RFC 5906, 5907 and 5908

1.2 Option 34 Setup

This section covers initial setup of the Option 34, NTP/PTP server. Before the Option 34 can serve time accurately, the clock must be locked to the GPS and stable. Once meeting these conditions, the Option 34 can provide reliable time to a network. The three subsections below will guide you through this initial phase of starting up the clock and configuring Option 34.

Option 34 can be ordered with either static IP addresses, DHCP assigned IP addresses, or both static and DHCP. This information should help you decide how to configure the Option 34.

Default Port Addresses

By default, Option 34 comes configured as follows:

```
Port 1 IP address -- STATIC: 192.168.0.232
      Netmask           255.255.255.0
      Gateway           xxx.xxx.xxx.xxx
```

```
Port 2 IP address -- DHCP:   xxx.xxx.xxx.xxx
```

Selecting Option 34 in Clock

Before you can use Option 34 in your clock, make sure that it is selected as an option. Selection may be checked at the front panel for Models 1084B/C, 1088A/B and 1093B/C. For Models 1084A and 1093A, select it through the serial port. These instructions include both methods.

Clocks With a Display

Models 1084 and 1093 are very similar in that they have a main board option and aux board option. For these models, Option 34 is selected in the AUX Board section. Model 1088A/B has two choices: Slot A and Slot B. For Model 1088A/B, select Option 34 in the Slot B section.

1. Press the SETUP key until you reach “SET OPTION CONTROL” and press “ENTER”.
2. Navigate to either AUX Board Option or SLOT B Option, depending on clock model.
3. Use the UP key to select (OPTION) 34 and press “ENTER.”
4. Option 34 should now be selected in the clock.

Clocks Without a Display

Models 1084A and 1093A do not have a keypad or LCD display, so that Option 34 must be selected through the RS-232 port. To select Option 34, use a terminal program (HyperTerminal or Tera Term³) and null-modem cable. Important pins for a null-modem cable are indicated in Table 1 below.

³To download a free copy of Tera Term, see Arbiter website at <http://www.arbiter.com/software/index.php>.

PC Port Pins	Clock Port Pins	Port Function
2	3	Transmit
3	2	Receive
5	5	Ground

Table 1: Null-Modem Cable Connections

1. Make sure that you have the terminal program open at the same baud rate as the clock. For 1084A and 1093A it will be 9600 baud.
2. Type the letter “v” to verify communication. It should return the firmware date code.
3. For Model 1084A, type “1,11,1084XI”.
4. For Model 1093A, type “1,8,1093XI”.
5. Option 34 should now be selected in your clock.
6. To test it, type “IP” and it should return the IP addresses of the two Ethernet ports. With no Ethernet cable connected to a port, the IP command will return dashes for the IP address of that port. The MAC address will still be returned as illustrated below.

```
NET1:192.168.000.232 64:73:E2:XX:XX:XX
NET2:---.---.---.--- 64:73:E2:XX:XX:XX
```

NTP Status Display Indications

GPS Clock and Server Stabilizing

During the stabilization process, the clock will display different status messages that indicate whether the NTP server is ready to serve time. Clock stabilization requires the clock to be locked to the GPS for a period of time after which it will provide its time to the Option 34. Press the STATUS key on the clock to access these status messages.

Server Status – Waiting for clock to lock to satellites

```
NTP: PLEASE WAIT...
PTP: DISABLED
```

Server Status – Waiting for NTP to stabilize (up to 1 hour)

```
NTP: UNLOCKED
PTP: DISABLED
```

Server Status – Normal Operation

```
NTP: SYNCHRONIZED
PTP: DISABLED
```

Server Status – Synchronization problem on Option 34

```
NTP: ERROR
PTP: DISABLED
```

After the Clock and Server Have Stabilized

After the GPS clock and NTP/PTP server have stabilized, press the Status button to view server status, link status and port addresses (IP and MAC address).

Server Status

```
NTP: SYNCHRONIZED
PTP: DISABLED
```

Link Status – indicates whether the network connection is good or bad.

```
NET1: GOOD LINK
NET2: BAD LINK
```

Port Address:

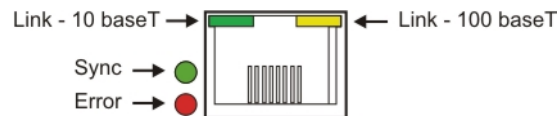
```
NET1:192.168.000.232
64:73:E2:XX:XX:XX
```

To Determine IP Address for 1093A/1084A

For clocks without a display, type “IP” at the terminal window, as explained in Section 1.2, and the clock should return the IP and MAC addresses for both ports in separate lines.

Option 34 LED Indications

To view the Option 34 Status LEDs, see the Option 34 rear panel. The figure and table below describe the indications.



LED Name	Color	Meaning
LINK	Steady Green	Good Link, 10 Mb/s
	Steady Yellow	Good Link, 100 Mb/s
	OFF	Bad Link
SYNC	Steady Green	NTP Server Synchronized
	OFF	NTP Server not Synchronized
ERROR	Red	Startup/Error
	OFF	No Errors

Table 2: Option 34 LED Indications

Using the Web Interface

The Option 34 may be configured through either network port using the Web Interface. See Figure 1 for an illustration of the Web Interface. If either port on the Option 34 is configured to use a Static IP address, you may need to contact your network administrator to help identify the assigned IP address(es), Netmask and Gateway. See Section 1.2 for the default port settings.

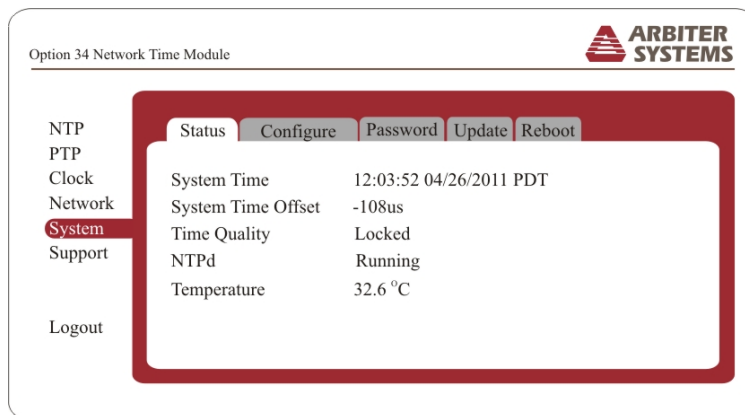


Figure 1: Web Interface – System Status Information

1. Make sure the clock is powered off. Connect a cable between one of the Ethernet ports on the Option 34 and a computer or network⁴. Power On the clock. See Section 1.2 for the default port settings.
2. Log in using the Web Interface – type the server IP address into your web browser address bar. See Section 1.3 for login information.
3. In the Web Interface, select “Network” on the left, then select the Configure tab.
4. Select either DHCP or Static for IP address handling.
5. If choosing Static, enter the desired address, netmask and gateway (if required).
6. If choosing DHCP, no other information is needed.
7. If making any other network or administrative changes, consult the Glossary of Key Terms and Definitions in Section 1.3.
8. Click the Apply button to accept the changes.

Important Configuration Change Notes

Note: Certain configuration changes will cause you to lose the web interface connection. These configuration changes include (1) changing from HTTP to HTTPS, (2) changing a Network configuration, or (3) changing a System configuration **on the port which you are connected**. If you are making changes to another port, the web interface connection will not be dropped. To make the changes persist, you will need to re-log in to the web interface using the new setting(s). To lose changes, reboot the clock. After making any changes to the NTP service, you may experience a delay of up to five minutes for the NTP service to start.

⁴A 4-minute delay in service may result if no network cable is connected to either port during clock startup.

Using the Console Interface

The Option 34 may also be configured using the SSH Console and a Secure Shell (SSH) client like PuTTY™ – see Figure 2. Web and Console terms and definitions are located in Section 1.3.

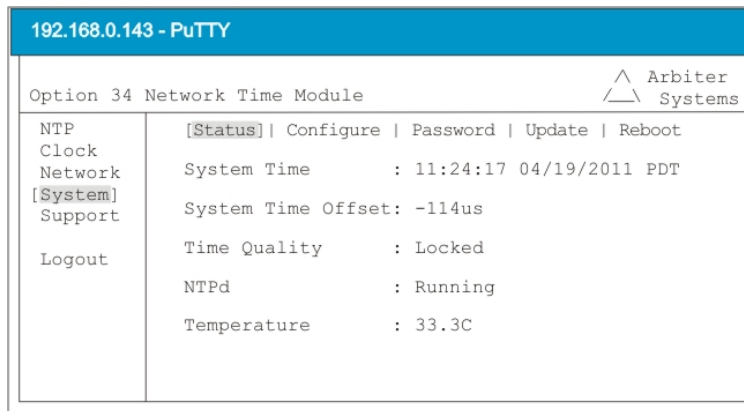


Figure 2: Console Interface – System Status Information

1. Using PuTTY, or other SSH client, open one of the ports using Host name or IP address.
2. When requested, type in the username and press ENTER. Next, type in the password and press ENTER. See Section 1.3 for login information.
3. The Console should appear and mimic the Web Interface in content, simplifying operation using SSH.
4. Use the arrow keys on your keyboard to navigate around the Console.

Useful Keys for Console Navigation

- Arrow Keys – navigate up, down, left, and right
- Enter – accept the current selection
- SPACE – accept the current selection except in edit fields (same as Enter)
- Tab – cancel an edit/change
- Q or q – select the Logout menu item

1.3 Glossary of Key Terms and Definitions

All Option 34 interface terms and definitions are located in this section. To securely configure the server and upload new firmware versions, the preferable method is through the Web Interface using HTTPS or using the SSH Console. HTTPS provides adequate security that the connection is not compromised, and requires that a PEM file be uploaded to the server. HTTP does not require a signed certificate and has no secure transport between the user and the server.

Login

Logging in to the Option 34 requires a fixed Username and a configurable Password. The value for Username is "clockoption" and the default value for Password is "password" (all lower case). The value for Password may be changed in the Web Interface or SSH Console. For more detail on Password, see below under **System – Password**. *Note that to log in to the Web Interface requires your browser be set to accept cookies.*

Username

Password

NTP

Describes the NTP server status, how to configure NTP functions and logging NTP data.

NTP – Status

Describes the operating status of the NTP server.

NTP – Configure

Allows configuration of various NTP functions, such as (1) NTPd Version (1 – 4), (2) Multicast Address, and (3) Broadcast Address for Ethernet Port 1 and Port 2.

NTP – Authentication

Provides for enabling/disabling authentication and a key table. The key table has space for five of the following: (1) ID, (2) Format, (3) Key, and (4) check box to signify a trusted element.

Clock

Clock provides the current time and date with time quality, the number of GPS satellites that are visible and being tracked.

Network

Provides network-specific information, and the ability to configure certain aspects of the Option 34 port, such as whether the network interface uses a static IP address or DHCP. If static, then you will be able to select (1) IP address, (2) netmask, and (3) gateway on both ports.

Network – Status

Describes the IP and MAC address for both ports. It also provides network statistics, such as number of bytes and packets transmitted and received, packet errors and packets dropped.

Network – Configure

Allows independent assignment of an IP address (either DHCP or Static) to either port. When selecting “Static” the menu changes to allow entry of the desired IP address, netmask and gateway address.

WARNING: Please be sure you are aware of advanced networking issues before setting both Ethernet ports on the same subnet.

System

The “System” tab provides a wide range of information and function, including (1) operating status, (2) User Interface, (3) setting a password, (4) updating the Option 34 firmware, and (5) rebooting the (Option 34) system.

System – Status

Provides a number of system variables including, but not limited to, System Time and Date, System Time Offset, Time Quality (locked or unlocked), NTP/PTP Daemon, Clock Temperature.

System – Configure

Allows for selection of (1) HTTP or HTTPS, port number, (2) setting the User Interface timeout intervals, (3) responding to ping requests, and (4) setting the time zone in the web interface.

Be sure to enter a TZ Format string, which represents the time zone you would like the Web UI, Console UI and the internal log files to use. Leaving this field blank will result in the time zone being set to UTC. See Section 1.6 for a list of some of the commonly used TZ Format strings.

In order to enable HTTPS, the Option 34 requires installation of a *decrypted private key* and an *SSL certificate*. These must be uploaded to the Option 34 in the form of a single, base 64 encoded X.509 PEM file. If you have separate files (*.key and *.crt) you can simply concatenate the two files into a single PEM file.

The private key must not be encrypted with a passphrase, as there is no means for an administrator to enter the passphrase whenever the webserver is started on the Option 34.

For more information regarding the PEM File please see Section 1.5.

System – Password

Allows assignment of a new password. Username is fixed.

Password Character Set

The password can have a minimum of one character and a maximum of sixteen characters in length, which may consist of printable ASCII values from 33 – 126 decimal.

Important Password Information

Store and manage the password so that if necessary it can be recovered. *If the password is lost, the option will need to be returned to the factory in order to be reset.* If security is not important, the password should be left alone – unchanged from the default password as it left the factory. If security is important, the password should be changed and managed to minimize the chance that the option would need to be returned.

System – Update

Update allows you to load the latest version of the Option 34 firmware package to your Network Time Module.

1. Download the latest firmware update package from the Arbiter website.
2. In the Web Interface only⁵, select System menu and Update tab. Click the Browse button in the file window and select the update package that you downloaded and click OPEN.
3. A small window will appear that states, “**Are you sure you want to upload and install this package now?**” (Allows OK or Cancel.)
4. Click OK and wait for the upload to complete. **NOTE: DO NOT DISCONNECT ANY CABLES AND DO NOT HALT THE UPDATE PROCESS!**
5. When the update process has finished, follow the on-screen message. Some packages require a different completion process.

⁵Currently, no updates are possible from the SSH Console.

System – Reboot

To restart the service on the Option 34 click the Reboot button. This means that both network connections will be lost until the service has restarted. This is not the same as restarting the GPS clock, and should take less time to regain a connection to the port.

Support and Contact

Arbiter Systems provides support for this product via phone, fax or email. Arbiter Systems is open between 7 a.m. and 5:30 p.m. Pacific Time, Monday through Thursday. Contact information is listed on page 1. Additionally, you may find support documentation on the Arbiter website.

Version

This is the version of the software running on the Option 34, not the clock itself. Check for updates on the Arbiter website under Service/Support and Downloads.

Logout

Allows you to disconnect from the server, with confirmation screen.

1.4 Specifications

Performance

NTP:	< 100 microseconds, depending on network load and clock accuracy
PTP:	< 100 microseconds (software) < 1 microsecond with hardware assist

Interface

Network	Two Ethernet (Version 2.0/IEEE 802.3) 10/100BT or Multi-mode SSF modules
Protocols	NTP, SNTP, PTP (IEEE 1588 TM -2008), UDP, ICMP, SNMP, TCP, SSH, SCP, SSL, HTTP, HTTPS.

Operator Interface

Management	Web and SSH Console
Status LEDs	Sync (green) Fault (red) Link (green – 10baseT, yellow – 100baseT)
Setup	IP number (DHCP or Static) Net Mask Reference Identifier UDP Broadcast parameters MD5 and DES authentication keys are optional

1.5 HTTPS/SSL Certificate

This appendix discusses a method of generating a PEM file for use with HTTPS as discussed in Section 1.3. As is the case with any web server, in order to provide a secure connection via HTTPS, the Option 34 must be configured with an SSL Certificate. The Option 34 uses a single PEM File which includes the private key and the certificate. This guide illustrates a method of creating a PEM File using the free and publicly available OpenSSL package. OpenSSL is merely one of many possible solutions – please see your toolkit documentation for exact instructions. This guide assumes you have already downloaded and installed the OpenSSL tools on a Linux system.

Note: In the following examples, the symbol ‘▷’ denotes the command prompt.

Step 1 - Generate a Private Key

The following command will generate a 1024 bit RSA private key. Please keep this file safe, secure, and not accessible to the public.

```
▷openssl genrsa -out private.key 1024
```

The generated file (private.key) might look like the following:

```
-----BEGIN RSA PRIVATE KEY-----
MIICXgIBAAKBgQDPoNigXmq2JAlw9DrDOP50g5c5xsEnt9bPjfuE7MGkDEGN09sC
...more data...
8Xzzzgu4xizBdLmONkHu7b/h7GL6u5smkWVOCesCCROmKw==
-----END RSA PRIVATE KEY-----
```

Step 2 - Generate a Certificate Signing Request (CSR)

The following command will generate a CSR (certificate signing request) file using the private key generated in Step 1. OpenSSL will prompt for several pieces of information, our example responses are in BOLD text. If you are purchasing a certificate from a commercial vendor, the information provided during this step must match exactly the information you will be providing to the vendor.

```
▷openssl req -new -key private.key -out my.csr
```

```
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter ‘.’, the field will be left blank.
```

```
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:California
Locality Name (eg, city) [ ]:Paso Robles
```

Organization Name (eg, company) [Widgits Pty Ltd]:Arbiter Systems, Inc.
Organizational Unit Name (eg, section) []:Lab
Common Name (eg, YOUR name) []:
Email Address []: techsupport@arbiter.com

Please enter the following 'extra' attributes
to be sent with your certificate request

A challenge password []:

An optional company name []:

The generated file (my.csr) might look like the following:

```
-----BEGIN CERTIFICATE REQUEST-----  
MIIBsDCCARkCAQAwcDELMAkGA1UEBhMCVVMxEzARBgNVBAGTCkNhbG1mb3JuaWEx  
...more data...  
YA/JCw==  
-----END CERTIFICATE REQUEST-----
```

Step 3A - Purchase a Certificate

To prevent web browsers from warning users about untrusted certificates, an SSL Certificate must be purchased from a trusted authority. If you do not require this level of protection, you may go to Step 3B (Generate a Self Signed Certificate).

Most certificate vendors will ask for the generated CSR file (from Step 2) to be pasted into a field in a web page during the purchase procedure. Be sure to copy the entire contents of the file (including the BEGIN and END tags with the dashes) into the vendor's web form.

Once the purchase has been completed, and other verification steps completed (this will vary from vendor to vendor), they will provide you with a certificate file. You may skip to Step 4.

Step 3B - Generate a Self Signed Certificate

If you do not need a commercially purchased certificate, the following command will generate a Self Signed Certificate using the files created from steps 1 and 2. Most web browsers will warn users that the certificate is not trusted or signed by a trusted authority. Also note that the certificate generated will be valid for 365 days. After this period, users will be additionally warned about an expired certificate until a new certificate is generated and uploaded to the Option 34.

```
▷openssl x509 -req -days 365 -in my.csr -signkey private.key -out my.crt
```

The generated file (my.crt) might look like the following:

```
-----BEGIN CERTIFICATE-----  
MIICVzCCAcACCQC7uu43uMF1+jANBgkqhkiG9w0BAQUFADBwMQswCQYDVQQGEwJV  
...more data...  
Jo+H1MXknNISZtcu/xb9gghHG42veveZSg72  
-----END CERTIFICATE-----
```

Step 4 - Create the PEM File

Once you have a purchased or self signed certificate file, the following command will create a single PEM file including the key and the certificate from the previous steps.

```
▷cat private.key my.csr > mycert.pem
```

Please note the “greater than” symbol ‘>’ between ‘my.csr’ and ‘mycert.pem’.

The file mycert.pem can now be uploaded to the Option 34 in order to enable HTTPS.

1.6 Time Zone Format Strings

This section lists some common time zones using the TZ command as discussed in Section 1.3. For further information regarding the time zone format, please go to the following link:

<http://www.gnu.org/s/hello/manual/libc/TZ-Variable.html>.

Some Useful Time Zone Values

“Greenwich Mean Time”	GMT0	–	
“Universal Coordinated Time”	UTC0	“Guam Standard Time”	GST-10
“Fernando De Noronha Std”	FST2FDT	“Eastern Australian Standard”	EAS-10EAD
“Brazil Standard Time”	BST3	“Central Australian Standard”	CAS-9:30CAD
“Eastern Standard (Brazil)”	EST3EDT	“Japan Standard Time”	JST-9
“Greenland Standard Time”	GST3	“Korean Standard Time”	KST-9KDT
“Newfoundland Standard Time”	NST3:30NDT	“China Coast Time”	CCT-8
“Atlantic Standard Time”	AST4ADT	“Hong Kong Time”	HKT-8
“Western Standard (Brazil)”	WST4WDT	“Singapore Standard Time”	SST-8
“Eastern Standard Time”	EST5EDT	“Western Australian Standard”	WAS-8WAD
“Chile Standard Time”	CST5CDT	“Java Standard Time”	JST-7:30
“Acre Standard Time”	AST5ADT	“North Sumatra Time”	NST-7
“Cuba Standard Time”	CST5CDT	“Indian Standard Time”	IST-5:30
“Central Standard Time”	CST6CDT	“Iran Standard Time”	IST-3:30IDT
“Easter Island Standard”	EST6EDT	“Moscow Winter Time”	MSK-3MSD
“Mountain Standard Time”	MST7MDT	“Eastern Europe Time”	EET-2
“Pacific Standard Time”	PST8PDT	“Israel Standard Time”	IST-2IDT
“Alaska Standard Time”	AKS9AKD	“Middle European Time”	MEZ-1MES
“Yukon Standard Time”	YST9YST	“Swedish Winter Time”	SWT-1SST
“Hawaii Standard Time”	HST10HDT	“French Winter Time”	FWT-1FST
“Somoa Standard Time”	SST11	“Central European Time”	CET-1CES
“New Zealand Standard Time”	NZS-12NZD	“West African Time”	WAT-1