CTP Series Circuit to Packet Platform

Managing CTP Devices

Release
7.2

Modified: 2015-11-17

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Managing CTP Devices, CTPOS and CTPView Release 7.2

Revision History
December 2015—Managing CTP Devices, CTPOS and CTPView Release 7.2

The information in this document is current as of the date on the title page.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at http://www.juniper.net/support/eula.html. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

CHAPTER 1

Managing CTP Devices Overview

Synchronizing CTP Devices Using External Clocks Overview

CTP devices can use an external clock as a reference input to the system. The reference can be input on a port or on the external reference input. You can configure and prioritize up to five references depending on the CTP model. The device automatically uses the highest priority reference available, and switches to a holdover mode if all the references are lost. The following ports can be used for reference inputs:

CTP2008, CTP20024, CTP2056: P0–P3

The CTP2000 external reference input is provide by the CLK-RTM module through a DB-25 connector.

An interface module must be present in slot one of the CTP2000 chassis to provide reference synchronization throughout the device.

You can define multiple clocks as references, each with a priority, to ensure that a reference with lower priority is available if the primary clock reference fails. The reference inputs to the CTP device must be 32 Kbps, an n x 64 Kbps (up to 4096), or 1.544 Mbps. The CTP device provides a reference holdover with an accuracy of approximately 100 parts per billion if the reference is lost and no backup is defined or available.

Related Documentation

Ethernet Media Configuration Overview

You can configure the CTP Ethernet media to autonegotiate and set the speed to either 100 or 10 Mbps. By default, autonegotiation is enabled and the speed is to 1000 Mbps. If you choose to disable autonegotiation, the system prompts you to configure the desired speed.

The Ethernet configurations on CTP must match the configuration of the connected router or switch. Mismatched configurations, such as setting the CTP system to autonegotiate and the router to full duplex, will result in a misconfiguration and dropped

packets. You must disable Cisco Discovery Protocol on the Fast Ethernet port connected to the CTP system.

Table 1 on page 6 lists the valid Ethernet media configuration settings that CTP Series supports.

Table 1: Valid Ethernet Media Configuration Settings for CTP

Speed	Autoneg Status	Mode (Duplex)	MTU (up to 1500)
1000	ON	Full	any
100	OFF	Full	any
10	OFF	Full	any

NOTE: **The CTP system supports only full duplex mode.**

Related Documentation

- Configuring Ethernet Media (CTP Menu) on page 28
- Displaying Ethernet Media Information (CTP Menu) on page 28

CHAPTER 2

Configuring the CTP Device

Configuring the Date and Time on CTP Devices (CTP Menu)

This topic describes how to configure the date and time on CTP devices. CTP devices must be set to UTC time or CTPView software will not gather and display statistics graphs properly.

To configure the date and time on a CTP device using the CTP Menu:

1. From the Main Menu, select **5) Node Operations**.
2. Select **1) Change Node Date/Time** and configure the date and time as described in Table 2 on page 8.

Table 2: CTP Device Date and Time Settings in the CTP Menu

Field	Function	Your Action

Change Node Date/Time	Specifies the date and time setting on the CTP device	Answer y to change the date and time, and fill in the following parameters:
		
		`Do you want to change it? y[n]:`
		`Enter new Month:  (1-12)[1]:`
		`Enter new Day:  (1-31)[5]:`
		`Enter new Year:  (1-2037)[2011]:`
		`Enter new Hour:  (0-23)[14]:`
		`Enter new Min:  (0-59)[28]:`
		`Enter new Sec:  (0-59)[46]:`

Related Documentation

Configuring a Default Ethernet Interface (CTP Menu)

You are required to reboot the CTP device when you finish this configuration procedure.

To configure the default Ethernet interface by using the CTP Menu:

1. From the Main menu, select **5) Node Operations**.
2. Select **3) Configure network settings**.
3. Select **2) IPv4 Configuration** or **3) IPv6 Configuration**.
4. Follow the onscreen instructions to select and specify a default Ethernet interface.
5. Configure the options as described in Table 3 on page 8.

NOTE: **Do not add a route to the default Ethernet interface.**

Table 3: Ethernet Interface Parameter Settings in the CTP Menu

Field	Function	Your Action
Please input the hostname	Specifies the hostname for the CTP device.	Enter a name.

Table 3: Ethernet Interface Parameter Settings in the CTP Menu *(continued)*

Field	Function	Your Action
Please input the ip/ipv6	Specifies the IP address of the Ethernet interface.	Enter an IP address.
Please input the netmask	For IPv4 interfaces, specifies the network mask.	Enter the network mask.
Please input the gateway	On the default Ethernet interface, specifies the IP address of the default next-hop gateway, which is the Ethernet interface on the router.	Enter an IP address.
Please input the mtu in bytes	Specifies the maximum transmission unit (MTU) for the Ethernet interface.	For IPv4 networks, enter a number from 64 through 1500. For IPv6 networks, enter a number of at least 1280.

Related Documentation

- Ethernet Media Configuration Overview on page 5
- Configuring Ethernet Media (CTP Menu) on page 28
- Displaying Ethernet Media Information (CTP Menu) on page 28

Adding a VLAN Interface to a Node (CTP Menu)

This topic describes how add a VLAN interface to a node. Adding VLAN interfaces to a node comprises two steps:

- Adding a VLAN ID to the System on page 9
- Configuring VLAN Interface by Using the VLAN ID on page 10

Adding a VLAN ID to the System

When you add a VLAN to a node, the network and CTP devices are restarted to update the network parameters. The node is not restarted.

NOTE: **For VLAN switchover to function correctly, VLANs must be configured on the primary Ethernet interface (for example, eth1) that has IPv4 configured and Ethernet switchover enabled.**

To add a VLAN ID to the system from the CTP Menu:

1. From the Main Menu, select **5) Node Operations** > **3) Configure network settings** > **8) VLAN Configuration**.

```
==============================================================================
= (ctp_90 05/08/14 23:03:48 WST) | Network Configuration Menu
==============================================================================
Please select a number from the following list:
------------------------------------
0) Back to Previous Menu
1) Supported Protocols: IPv4 only
```

```
2) IPv4 Configuration
3) IPv6 Configuration
4) Virtual IP addresses
5) OAM port (IPv4): 16
6) CTP Bndl Data pkt protocol: 47
7) CTP Bndl OAM port (IPv6): 32
8) VLAN Configuration
9) Current Configuration (active on reboot)
10) Port operations (PBS/bridge)
11) Config port operational mode (CE/PBS/bridge)
12) Config access ip filtering
13) SNMP Configuration
------------ Your choice [0]: 8
***
*** You are about to modify a system parameter that will require
*** a network restart when complete.
***
*** If you decide to continue, the network will automatically
*** restart upon leaving the menu, existing menu session will be
*** terminated and active circuits will take traffic hits. For
*** further configuration re-initiate the menu session.
***
*** Note: If these parameters are changed incorrectly,
*** system may not be reachable via the network
*** after the network restarts.
***
Are you sure? y[n]: y
Exsisting VLAN interfaces :
No VLAN is configured yet
How do you want to change VLANs (add/delete/quit) ? (rtn for show): add
Which ethernet port the new VLAN will be added on? (0-3)[0] 1
What is the new VLAN id? (0-4095)[0] 111
Exsisting VLAN interfaces :
eth1.111: Vlan ID 111 on ethernet port 1
How do you want to change VLANs (add/delete/quit) ? (rtn for show): quit
```

2. Follow the onscreen instructions and configure the options as described in Table 4 on page 10.

Table 4: Configuring a VLAN Interface

Field	Function	Your Action
How do you want to change VLANs ?	Enter **add** to add a new VLAN, **delete** to remove a VLAN, and **rtn** to show existing VLANs.	Enter **add** to create a new VLAN.
Which ethernet port the new VLAN will be added on ?		Specify the ethernet port number. The default value is 0 (zero).
What is the new VLAN id ?		Assign the VLAN ID for the newly created VLAN in the range 0–4095. The default value is 0 (zero).

Configuring VLAN Interface by Using the VLAN ID

1. From the Main Menu, select **5) Node Operations** > **3) Configure network settings** > **2) IPv4 Configuration** to assign an IP address for the VLAN.

```
=============================================================================
= (ctp_90 05/08/14 23:09:40 WST) | Network Configuration Menu
=============================================================================
Please select a number from the following list:
-----------------------------------
0) Back to Previous Menu
1) Supported Protocols: IPv4 only
2) IPv4 Configuration
3) IPv6 Configuration
4) Virtual IP addresses
5) OAM port (IPv4): 16
6) CTP Bndl Data pkt protocol: 47
7) CTP Bndl OAM port (IPv6): 32
8) VLAN Configuration
9) Current Configuration (active on reboot)
10) Port operations (PBS/bridge)
11) Config port operational mode (CE/PBS/bridge)
12) Config access ip filtering
13) SNMP Configuration
------------ Your choice [8]: 2
***
*** You are about to modify a system parameter that will require
*** a network restart when complete.
***
*** If you decide to continue, the network will automatically
*** restart upon leaving the menu, existing menu session will be
*** terminated and active circuits will take traffic hits. For
*** further configuration re-initiate the menu session.
***
*** Note: If these parameters are changed incorrectly,
*** system may not be reachable via the network
*** after the network restarts.
***
Are you sure? y[n]: y
There are 2 ethernet devices available for use. The default device
is the device through which the default gateway can be accessed.
Ctp circuits can run over any ethernet device, default or not.
A default device must be configured, other devices may be configured
and enabled, or disabled. Here is a list ot the available devices
and their descriptions:
Copyright © 2014, Juniper Networks, Inc. 3
eth0: 10/100/1000 Copper (right back)
eth1: 10/100/1000 Copper (left back)
List of VLAN interface :
eth1.111: Vlan ID 111 on ehternet port 1
What device would you like to make the IPV4 default device? (rtn for eth1):
OK, eth1 (10/100/1000 Copper (left back)) will be configured as IPV4 default
device.
Please input the hostname (return for ctp_90):
===== Configuration for eth0:
Activate IPV4 interface eth0 on boot [n]
===== Configuration for eth1 (default device):
Please input the ip (return for 10.216.118.90):
Please input the netmask (return for 255.255.254.0):
Please input the gateway (return for 10.216.119.254):
Please input the mtu in bytes (return for 1500):
Add route to interface eth1 [n]
IPV4 configuration for VLAN interfaces :
===== Configuration for eth1.111:
Activate IPV4 interface eth1.111 on boot [n] y
Please input the ip (return for 10.0.0.1): 1.1.1.1
```



```
Please input the netmask (return for 255.255.255.0):
Please input the mtu in bytes (return for 1500):
Add route to interface eth1.111 [n]
```

2. Follow the onscreen instructions and configure the options as described in Table 5 on page 12.

Table 5: IP Parameters for Configuring a VLAN

Field	Your Action
What device would you like to make the IPv4 default device ?	Select the default Ethernet device.
Please input the hostname.	Specify the host name. Press **Enter** to select the default hostname.
Activate the IPv4 interface eth0 on boot.	Enter **n**. Ethernet failover may not work correctly if multiple Ethernet interfaces are activated or the active Ethernet interface is configured as the secondary interface.
Configuration for eth1 (default device)	Enter the IP address, network mask, gateway, and MTU for eth1.
Activate the IPv4 interface eth1.111 on boot.	Enter **y**.
Configuration for eth1.111	Enter the IP address, network mask, and MTU for eth1.111.

Separate Interfaces for Management and Circuit Traffic Overview

Until CTPOS and CTPView Release 7.1, only one network device (the default device) is used for both management and circuit data. In certain network topologies, a segregation is required between the circuit or Ethernet traffic and management traffic. Therefore, separate interfaces need to be used for the management and circuit networks so that traffic segregation can be achieved at the physical interface level. Starting with CTPOS Release 7.2, support for configuring two default gateways, one for management traffic and the other for circuit device, is available, which enables circuit and management traffic to be segregated.

The functionality to segregate management and circuit traffic requires at least two Ethernet devices—one for circuit traffic and the other for management traffic. When this feature is enabled, both management and circuit interfaces are required to be configured. Segregation of traffic is performed on the basis of the management and circuit device or interface. CTP devices that support two default gateways are required—one for management device and other for circuit device. Each interface replies to incoming packets via its own default gateway. All incoming and outgoing packets in the circuit network traverse through the circuit device gateway (main default gateway). All incoming and outgoing packets in the management network traverse through the management device gateway.

For having two default gateways, policy-based routing is required. Policy-based routing enables the creation of multiple routing tables, one for each interface. Policy-based

routing provides a flexible mechanism for forwarding data packets based on polices configured by a network administrator. This capability enables you to implement policies that selectively cause packets to take different paths. For circuit traffic, the main routing table, inet.0 is referred and for management traffic, the newly-created policy-based routing table is referred. The policy-based routing table is used, based on a set of rules. Using the main routing table for circuit device enables any IP table-related changes for the SAToP and CESoPSN bundles to be avoided. An entry of this newly created policy-based routing table is stored at **/etc/iproute2/rt_tables**.

The “IPV4 configuration” under “Config Network Settings” menu is modified to enable the configuration of different interfaces for management traffic and circuit or Ethernet traffic. The Display network settings menu is modified to display the circuit and management network devices. A separate conf file is implemented to indicate the status of this feature (whether it is enabled or not). Apart from feature status, this configuration file also stores information related to circuit and management device. With this feature to distinguish management and circuit traffic, Ethernet failover is supported only on the circuit interface and not on the management interface. This feature cannot be activated during the first boot process.

After the management device is selected, a new policy based routing table is created for this device. For example, if the routine table is named 10 tab-eth0, 10 denotes the route table number and tab-eth0 signifies the route table name created for management device eth0. This table is referred according to the rule specified in the rule-eth0 file.

The following command displays the main route table and the newly created policy based route table “tab-eth0”:

```
[root@ctp_90 ctp_cmd 2]# ip route show  tab main
1.1.1.0/24 dev eth0  scope link
10.216.118.0/23 dev eth1  scope link
169.254.0.0/16 dev eth1  scope link
127.0.0.0/8 dev lo  scope link
default via 10.216.119.254 dev eth1

[root@ctp_90 ctp_cmd 3]# ip route show  tab tab-eth0
1.1.1.0/24 dev eth0 scope link
default via 1.1.1.3 dev eth0
```

The following command displays the rules added for the policy-based route table:

```
[root@ctp_90 ctp_cmd 4]# ip rule show
0:      from all lookup local
32764:  from all to 1.1.1.1 lookup tab-eth0
32765:  from 1.1.1.1 lookup tab-eth0
32766:  from all lookup main
32767:  from all lookup 253
```

When this feature is disabled, the IP config/query section in the CTP Menu does not display the option for segregating management and circuit traffic.

Operations Performed When Management and Circuit Traffic Are Segregated

When you activate the feature to separate management and circuit traffic, you are prompted to enter the default circuit and default management device. If you enter the same device for both management and circuit devices, an error message is displayed stating that you need to define different devices for circuit and management traffic. When you enter a correct management device (say ethX), a reference for the policy-based routing table is created for management device. An entry of its route-table number and route-table name is added in /etc/iproute2/rt_tables. This route table is referred for the management device according to the rule specified by its rule file (rule-ethX).

After you configure the management device, a route entry for its own subnet and a default gateway route for that device is added to the route- ethX file. Rules are added to rule-ethX file to handle the inbound and outbound packets through this network. The rule-ethX file contains the rules such that if any packet arrives for the management network or if any packet is originated from the management network IP address, then such a packet is transmitted through the management device gateway. An existing configuration file, **/etc/sysconfig/ctp**, is used to store this feature configuration. The configuration of this feature contains the status of this feature, circuit device name, and management device name.

The following example illustrates the contents of the **/etc/sysconfig/ctp** file:

```
[root@ctp_90 ctp_cmd 5]# cat /etc/sysconfig/ctp
CTP=yes
TARGET=yes
CTP_IP_PROTO=0
status=1
ckt_dev=eth0
mgmt_dev=eth1
```

When you disable this feature, the policy-based route table and the rules corresponding to that route table are deleted from the system and the system is configured as it was configured previously (with one default gateway). The route-ethX file and rule-ethX files are also be deleted from the system after the feature is disabled.

This feature is not supported with IPv6-only or independent IPv6 (and not a combination of IPv4 and IPv6) configuration. This limitation denotes that with IPv6 configuration settings specified on a CTP device, the option to separate management and circuit traffic is not available for configuration. If this feature is enabled on CTP150 devices, Ethernet failover cannot be activated because CTP150 devices contain only two Ethernet devices and the PCI mezzanine card (PMC) is not supported on such devices.

Configuring Separate Interfaces for Management and Circuit Traffic (CTP Menu)

In certain network topologies, a segregation is required between the circuit or Ethernet traffic and management traffic. Therefore, separate interfaces need to be used for the management and circuit networks so that traffic segregation can be achieved at the physical interface level. Starting with CTPOS Release 7.2, support for configuring two default gateways, one for management traffic and the other for circuit device, is available, which enables circuit and management traffic to be segregated.

NOTE: This feature is not supported with IPv6-only or independent IPv6 (and not a combination of IPv4 and IPv6) configuration. This limitation denotes that with IPv6 configuration settings specified on a CTP device, the option to separate management and circuit traffic is not available for configuration. If this feature is enabled on CTP150 devices, Ethernet failover cannot be activated because CTP150 devices contain only two Ethernet devices and the PCI mezzanine card (PMC) is not supported on such devices.

To configure separate interfaces for management traffic and circuit traffic on a CTP device using the CTP Menu:

1. From the Main Menu, select **5) Node Operations**.
2. Select **3) Configure network settings** to specify the network configuration parameters.
3. Select **2) IPv4 Configuration** to define the IPv4 attributes.
4. A message is displayed stating that you are about to modify a system parameter that requires a network restart when the configuration settings are modified. If you proceed with the configuration settings, the network automatically restarts after you complete specifying the parameters, the existing menu session is terminated, and active circuits undergo traffic drops. You must reopen a new CTP Menu session to perform additional configuration changes.

   The message alerts you that if the parameters are incorrectly defined, the system might be unreachable over the network after the system restarts. Therefore, you must exercise caution while entering the attributes. Enter **y** to proceed with defining the interfaces for management and circuit traffic.

```
Please select a number from the following list:
-------------------------------------
 0) Exit to Shell
 1) Bundle Operations
 2) Node Synchronization
 3) Node Summary
 4) Node Diagnostics
 5) Node Operations
 6) Save Running Database to Flash
------------ Your choice [3]: 5


=====================================================================
= (ctp_90 06/29/16 23:04:38  UTC) | Node Operations Menu
```

```
=========================================================================

Please select a number from the following list:
-------------------------------------
 0) Back to Previous Menu
 1) Change Node Date/Time/TimeZone
 2) Display network settings
 3) Configure network settings
 4) Initialize Database
 5) Ping IP address
 6) Traceroute IP address
 8) System descriptor field:
 9) Reboot Node
10) Powerdown Node
11) Display ethernet media
12) Config ethernet media
13) Set your password
14) Config security profile
------------ Your choice [0]: 3


=========================================================================
= (ctp_90 06/29/16 23:04:38  UTC) | Network Configuration Menu
=========================================================================

Please select a number from the following list:
-------------------------------------
 0) Back to Previous Menu
 1) Supported Protocols:        IPv4 only
 2) IPv4 Configuration
 3) IPv6 Configuration
 4) Virtual IP addresses
 5) OAM port (IPv4):            16
 6) CTP Bndl Data pkt protocol: 47
 7) CTP Bndl OAM port (IPv6):   32
 8) VLAN Configuration
 9) Current Configuration (active on reboot)
10) Port operations (PBS/bridge)
11) Config port operational mode (CE/PBS/bridge)
12) Config access ip filtering
13) SNMP Configuration
------------ Your choice [0]: 2

***
*** You are about to modify a system parameter that will require
*** a network restart when complete.
***
*** If you decide to continue, the network will automatically
*** restart upon leaving the menu, existing menu session will be
*** terminated and active circuits will take traffic hits. For
*** further configuration re-initiate the menu session.
***
*** Note: If these parameters are changed incorrectly,
***       system may not be reachable via the network
***       after the network restarts.
***
        Are you sure? y[n]: y

There are 4 ethernet devices available for use. The default device
is the device through which the default gateway can be accessed.
Ctp circuits can run over any ethernet device, default or not.
```

```
A default device must be configured, other devices may be configured
and enabled, or disabled. Here is a list ot the available devices
and their descriptions:

        eth0: 10/100/1000 Copper (right back)
        eth1: 10/100/1000 Copper (left back)
        eth2: 1000 Fiber (left)
        eth3: 1000 Fiber (right)

Do you want to segregate circuit and management traffic (y/n)? [n]  y

Which device would you like to make the IPV4 default circuit device? (rtn for
 eth1):
OK, eth1 (10/100/1000 Copper (left back)) will be configured as IPV4 default
circuit device.

Which device would you like to make the IPV4 default management device? (rtn
for eth0): eth1
**** Management and Circuit Device cannot be same ****
You will be asked to enter management and circuit devices again

Which device would you like to make the IPV4 default circuit device? (rtn for
 eth1):
OK, eth1 (10/100/1000 Copper (left back)) will be configured as IPV4 default
circuit device.

Which device would you like to make the IPV4 default management device? (rtn
for eth0):
OK, eth0 (10/100/1000 Copper (right back)) will be configured as IPV4 default
 management device.

Please input the hostname (return for ctp_90):

===== Configuration for eth0 (default management device):
Please input the ip (return for 127.0.0.1): 1.1.1.1
Please input the netmask (return for 255.255.255.0):
Please input the gateway (return for 127.0.0.1): 1.1.1.3
Please input the mtu in bytes (return for 1500):

Add route to interface eth0 [n]

===== Configuration for eth1 (default circuit device):
Please input the ip (return for 10.216.118.90):
Please input the netmask (return for 255.255.254.0):
Please input the gateway (return for 10.216.119.254):
Please input the mtu in bytes (return for 1500):

Add route to interface eth1 [n]

===== Configuration for eth2:

Activate IPV4 interface eth2 on boot [n]

===== Configuration for eth3:

Activate IPV4 interface eth3 on boot [n]
```

Follow the onscreen instructions and configure the options as described inTable 6 on page 18.

Table 6: Configuring Separate Interfaces for Management and Circuit Traffic

Field	Function	Your Action
Do you want to segregate circuit and management traffic (y/n)?	Specifies whether you want to enable the capability to configure separate interfaces for management and circuit traffic. Lists the previously configured Ethernet devices that are available for use in the system. The default device is the device through which the default gateway can be accessed. CTP circuits can run over any Ethernet device, such as the default or non-default devices. A default device must be configured, while other devices might be configured and enabled or disabled.	Specify **y** or **n**.
Which device would you like to make the IPV4 default circuit device?	Specifies the device or interface that you want to configure as the default circuit device for IPv4.	Specify an interface from the list of available interfaces that were previously displayed in the CTP Menu as the default circuit interface. Specify **rtn** to set the interface that is prompted by the system to be specified as the default IPv4 circuit device. For example, if the prompt displays **(rtn for eth1)**, and if you specify **rtn**, **eth1** is set as the default circuit device.
Which device would you like to make the IPV4 default management device?	Specifies the device or interface that you want to configure as the default management device for IPv4.	Specify an interface from the list of available interfaces that were previously displayed in the CTP Menu as the default management interface. Specify **rtn** to set the interface that is prompted by the system to be specified as the default IPv4 management device. For example, if the system prompt displays **(rtn for eth0)**, and if you specify **rtn**, **eth0** is set as the default management device. NOTE: You must not specify the same device for both management and circuit traffic. Otherwise, the system prompts you to enter the default circuit device and default management device again. For example, if you specify **eth1** as the default interface for both circuit and management traffic, the system prompts you to enter the settings again.
Please input the hostname	Specifies the hostname of the CTP device.	Enter the hostname of the CTP device. Press **Enter** to specify the default hostname.
Please input the ip	Specifies the IP address of the Ethernet interface.	Enter an IP address.
Please input the netmask	For IPv4 interfaces, specifies the network mask.	Enter the network mask.
Please input the gateway	Specifies the IP address of the next-hop gateway (the router).	Enter an IP address.

Table 6: Configuring Separate Interfaces for Management and Circuit Traffic *(continued)*

Field	Function	Your Action
Please input the mtu in bytes	Specifies the maximum transmission unit (MTU) for the Ethernet interface.	For IPv4 networks, enter a number from 64 through 1500.
Add route to interface eth	Specifies whether or not to add static routes to the Ethernet configuration.	Specify **yes**.
Activate IPV4 interface eth on boot	Specifies whether you want to activate the particular IPv4 interface during the boot operation.	Enter **y** or **n**.

Displaying the Management and Circuit Interface Settings (CTP Menu)

To display the configured network settings using the CTP Menu:

1. From the CTP Main Menu, select **5) Node Operations**.
2. Select **2) Display network settings**.

```
Hostname: ctp_90

Protocols supported:   IPV4 ONLY

Segregation between management and circuit traffic: ON

Default management device (eth0: 10/100/1000 Copper (right back)) IPV4
parameters:
        ipaddress:  1.1.1.1
        netmask:    255.255.255.0
        gw:              1.1.1.3
        mtu:        1500 bytes

Default circuit device (eth1: 10/100/1000 Copper (left back)) IPV4 parameters:

        ipaddress:  10.216.118.90
        netmask:    255.255.254.0
        default gw: 10.216.119.254
        mtu:        1500 bytes
```

Table 7 on page 19 describes the fields corresponding to the configured network settings, including the status of the capability to segregate management and circuit traffic, displayed in the output.

Table 7: CTP Network Settings Display in the CTP Menu

Field Name	Field Description
Hostname	Hostname of the CTP device..
Protocols supported	Displays the protocols supported on the CTP device, such as IPv4 or IPv6.
Segregation between management and circuit traffic	Displays whether the functionality to segregate management and circuit traffic is configured (**ON**) or not (**OFF**).

Table 7: CTP Network Settings Display in the CTP Menu *(continued)*

Field Name	Field Description
Default management device (eth) IPV4 parameters	
ipaddress	Displays the IP address of the Ethernet interface set as the default management interface.
netmask	Displays the network mask of the Ethernet interface set as the default management interface.
gw	Displays the IP address of the next-hop gateway for the Ethernet interface set as the default management interface.
mtu	Displays the maximum transmission unit (MTU) of the Ethernet interface set as the default management interface.
Default circuit device (eth) IPV4 parameters	
ipaddress	Displays the IP address of the Ethernet interface set as the default circuit interface.
netmask	Displays the network mask of the Ethernet interface set as the default circuit interface.
gw	Displays the IP address of the next-hop gateway for the Ethernet interface set as the default circuit interface.
mtu	Displays the maximum transmission unit (MTU) of the Ethernet interface set as the default circuit interface.

Loss Of Signal Detection Capability on CTP Bundles and SAToP Bundles

A loss of signal (LOS) alarm indicates that there is a physical link problem with the connection to the router receive port from the neighboring SONET equipment transmit port. An LOS alarm occurs when the port on the card is in service but no signal is being received. The cabling is not correctly connected to the ports, or no signal exists on the line. Possible causes for a loss of signal include upstream equipment failure or a fiber cut.

The CTP devices support a both-ended redundancy mechanism, in which two identical CTP circuit bundles are combined using Y cables at each end, enabling one bundle to act as a backup for the other. One of the bundles is in use (online), while the other is in the standby state (offline). Only the online bundle is allowed to drive the Y cable towards the user equipment, while the offline bundle is tristate. A communications channel (such as redundancy by using a hardware link that uses a special Y cable or redundancy based on a software link that does not depend on a signaling hardware like the Y cable) between ports at each end determines which of the two ports on the Y cable is currently online. When one bundle fails, the failed bundle transitions to the offline and places the other bundle in the online state.

Consider a sample configuration scenario in which two CTP bundles (four CTP ports) are used in a Y-cable redundancy format. Software-based redundancy is enabled. In this

type of configuration, 172.25.62.51:te-0/0(B0) is the left primary link and 172.25.62.51:te-0/1(B1) is the left secondary link. 172.25.62.52:te-0/0(B0) is the right primary link and 172.25.62.52:te-0/1(B1) is the right secondary link. In this redundant configuration, the circuit is very robust, protecting against many types of failures, such network failures, power failures, and equipment failures. However, one type of failure is not detected, which is when a cable is pulled out.

Starting with CTPOS Release 7.2R1, CTP devices support the detection of a loss of signal, which denotes a physical link problem. The following conditions are supported:

- In a serial both-ended Y-cable redundancy configuration (hardware-based redundancy or software-based Y cable link protocol), removal of Y cable leg from the CTP port of the online bundle must be able to force a switch to the standby bundle.
- In a T1/E1 both-ended Y cable configuration (hardware-based redundancy or software-based Y cable link protocol), removal of Y cable leg from the CTP port of the online bundle must be able to force a switch to the standby bundle.

The way in which CTP redundancy works is by using the bundle state to make decisions. When a bundle is in the RUNNING state, the following processes occur:

1. The remote CTP is operational and is able to generate and send packets into the IP network (towards us).
2. The network is able to transport bundle OAM and payload packets from the remote CTP to the local CTP.
3. A sufficient percentage of the bundle payload packets fills packet delay variation (PDV buffers) and maintain circuit data transport towards the locally connected user equipment.

Therefore, when a bundle is in the RUNNING state, it is “usable” and can be online in a redundant configuration.

Consider a network topology in which a failure occurs in the circuit path that does not cause the circuit to exit the RUNNING state. This phenomenon can be the case when the cable is pulled from the CTP port of a redundant online bundle. Although this condition might not typically be considered an actual failure, and instead more of a configuration error, this symptom can nevertheless be classified in the failure category. Therefore, a mechanism to be able to detect this condition in redundant setups and provide an online circuit switch to offline when the cable is removed is beneficial. CTP devices support the evaluation of LOS conditions on serial interfaces and T1E1 interfaces in CTP bundles and SAToP bundles.

- Detection of LOS on Serial Interfaces on page 21
- Detection of T1/E1 Interfaces on page 22

Detection of LOS on Serial Interfaces

For serial interfaces, the determination of LOS condition is already performed in CTPOS releases earlier than Release 7.2R1. When a serial circuit is configured to use the TT input (on a data communication equipment [DCE] interface) for at least one of its five configured port clocks (for example, “Cfg Rate - Ext Clk), the external clock frequency is

examined by the CTP device before the local bundle can go to the running state. If there is no external clock present or it is not the correct frequency, then the bundle transitions to the TtFAIL state and never go to RUNNING. Also, if the bundle is already in the RUNNING state, the external clock is verified every second to ensure that its frequency is still present and within range. If not, the bundle transitions from RUNNING to TtFAIL.

In the TtFAIL state, the bundle periodically transitions back to the EVAL state, where the external clock is checked again. If the clock fails or a bad frequency occurs, the bundle returns to the TtFAIL state. If the clock is properly functional, then the bundle transitions to the various states that eventually end in the RUNNING state. Such a method of change of states enable a graceful (if not instantaneous) recovery of a circuit where a cable is disconnected, but subsequently reconnected. Because removal of the cable on a serial port that is using an external clock can cause the bundle to exit the RUNNING state, that bundle switches offline, if currently online in a Y-cable redundancy setup.

Detection of T1/E1 Interfaces

The clock and data signals are embedded together on a T1/E1 interface in a single AMI (alternate mark inversion) electrical signal. The hardware line interface unit (LIU) that recovers the composite AMI signal into its component clock and data signals recovers a clock from the incoming AMI signal, even when none is present because it is based on a free running phase-locked loop (PLL) that generates a clock, even when it is not locked to an incoming signal. As a result, the CTP port interface receives an incoming external clock from the LIU, whether a valid T1/E1 signal is connected to the CTP or not. The LIU, however, cannot determine when it has a valid incoming T1/E1 signal, and in such a condition, the LIU indicates as a LOS status bit. This indication serves as the basis for detecting a cable disconnect in a Y-cable redundant configuration.

To use LOS as a way to take down a RUNNING bundle, the effective method implemented is to treat a T1/E1 LOS condition exactly the same as a serial port with a bad or missing external clock. When the CTP device performs its “check external clock” function, instead of returning an automatic success on T1/E1 ports, the LOS status bit is analyzed to determine whether it is a T1/E1 port. If the LIU LOS status indicates that there is no incoming signal, then the function returns a failure, which causes the bundle to move to the TtFAIL state. This state is the same as a missing external clock processing for a serial port. In this manner, the T1/E1 ports behave exactly the same way as serial ports.

Guidelines for Configuring LOS Detection

Keep the following points in mind when you configure the capability to detect LOS conditions on T1E1 interfaces:

- A cable disconnection of a serial port cannot be detected when no external clock is being used by the port. The following clock configurations use an external clock:
  - DCE/DTE: Cfg Rate – Ext Clk
  - DCE/DTE: All Clock – Ext Clk
  - DCE/DTE: Adap Rate – Ext Clk
  - DCE/DTE: Auto Rate – Ext Clk

  - DTE: All clocked by Ext Clk (ST/RT)
  - DTE: All clocked by User Clk (RT)
  - Any custom clock config that uses “TT”
- For any other serial clock configuration, a cable removal on the online port does not cause it to exit the running state.
- For T1/E1 ports, the recovered clock (which is equivalent to the external clock of a serial port) from the incoming T1/E1 AMI signal is used in all available T1/E1 preconfigured or canned clock configurations.
- The T1 LOS checking technique was primarily intended for CTP bundles. Because the T1/E1 SAToP bundle state machine also supports the bundle EVAL state as part of its bundle state machine, it can also benefit from the LOS checking functionality provided by this feature. However, the LOS detection feature on SAToP bundles is not useful for both ended redundancy, since both-ended Y-cable redundancy configurations only supports CTP bundles.
- CESoPSN and VCOMP bundles are not supported for detecting LOS conditions because their bundle state machines do not support an EVAL state.
- You can configure the LOS detection mechanism for T1/E1 ports in the same function that checks the external input clock. In addition, this T1/E1 LOS detection capability is processed under the control of a separate port configuration flag so that this LOS checking occurs only when this flag is active. Although this menu option to enable or disable the LOS detection functionality is shown regardless of the port type, such as serial interfaces or T1E1 interfaces, this setting becomes effective on a T1/E1 port only when it is connected to a CTP or SAToP bundle. If the LOS detection functionality is enabled on a serial port or other bundle types, the setting is not processed.
- Also, when you run the bundle query for CTP bundles and SAToP bundles, the T1E1 port type displays port configuration flags that are relevant to a T1E1 port. In the PortConfigFlags field displayed in the output of the bundle query, T1LoSCheck denotes that LOS detection is specified on a T1 port connected to a CTP bundle or a SAToP bundle, E1LoSCheck denotes that LOS detection is specified on a E1 port connected to a CTP bundle or a SAToP bundle, and the NoRdReclk flag signifies that the redundancy receiving (RX) clock is disabled. The NoRdReclk flag is also displayed because this flag is default enabled for a T1/E1 port, whereas it is usually not enabled for a serial port.

Configuring LOS Detection on CTP and SAToP Bundles (CTP Menu)

Starting with CTPOS Release 7.2R1, CTP devices support the detection of a loss of signal, which denotes a physical link problem. The following conditions are supported:

- In a serial both-ended Y-cable redundancy configuration (hardware-based redundancy or software-based Y cable link protocol), removal of Y cable leg from the CTP port of the online bundle must be able to force a switch to the standby bundle.
- In a T1/E1 both-ended Y cable configuration (hardware-based redundancy or software-based Y cable link protocol), removal of Y cable leg from the CTP port of the online bundle must be able to force a switch to the standby bundle.

A CTP series device provides two types of Y-cable redundancy.

- Redundancy by using a hardware link that uses a special Y cable
- Redundancy by using a software link that does not depend on a signaling hardware like the Y cable

The CTP devices support a both-ended redundancy mechanism, in which two identical CTP circuit bundles are combined using Y cables at each end, enabling one bundle to act as a backup for the other. One of the bundles is in use (online), while the other is in the standby state (offline). Only the online bundle is allowed to drive the Y cable towards the user equipment, while the offline bundle is tristate. A communications channel (such as redundancy by using a hardware link that uses a special Y cable or redundancy based on a software link that does not depend on a signaling hardware like the Y cable) between ports at each end determines which of the two ports on the Y cable is currently online. When one bundle fails, the failed bundle transitions to the offline and places the other bundle in the online state.

Before you begin:

- Disable the bundle before you modify the bundle options.

To configure the capability to detect LOS alarms in a Y-cable redundancy configuration for CTP and SAToP bundles by using the CTP Menu:

1. From the Main Menu, select **1) Bundle Operations**.
2. Select **1) CTP**.
3. Select a bundle from the list.

   If you select an active bundle, you are prompted to disable the bundle before configuring it.
4. Select **3) Port Config**.
5. Select **4) Advanced Options** to configure advanced attributed for the CTP bundle.

6. Select **20) LOS checking (T1E1 only)** to configure the functionality to detect LOS for the T1E! interfaces in a CTP bundle or SAToP bundle.
7. Follow the onscreen instructions and configure the options as described Table 8 on page 25.

Table 8: LOS Settings in the CTP Menu

Field	Function	Your Action
Check LOS on T1/E1 ports for CTP/SAToP bundles? y[n]	Specifies that the capability to identify LOS alarms on T1E1 interfaces in SAToP or CTP bundles needs to be enabled. A loss of signal (LOS) alarm indicates that there is a physical link problem with the connection to the router receive port from the neighboring SONET equipment transmit port. An LOS alarm occurs when the port on the card is in service but no signal is being received. The cabling is not correctly connected to the ports, or no signal exists on the line. Possible causes for a loss of signal include upstream equipment failure or a fiber cut.	Enter **y** or **n** to enable or disable the LOS detection capability. NOTE: Although this menu option to enable or disable the LOS detection functionality is shown regardless of the port type, such as serial interfaces or T1E1 interfaces, this setting becomes effective on a T1/E1 port only when it is connected to a CTP or SAToP bundle. If the LOS detection functionality is enabled on a serial port or other bundle types, the setting is not processed.

Initializing the CTP Database (CTP Menu)

Initializing the database clears nonvolatile configuration of the local CTP system. It returns the node settings to their factory defaults and disables all the ports.

To initialize the database by using the CTP Menu:

1. From the Main Menu, select **5) Node Operations**.
2. Select **4) Initialize Database**.

CAUTION: **Initializing the database resets the ports to factory defaults, and the ports will be disabled.**

Related Documentation

Pinging an IP Address (CTP Menu)

This topic describes how to ping an IP address.

To ping an IP address using the CTP Menu:

1. From the Main Menu, select **5) Node Operations**.
2. Select **5) Ping IP address**.
3. Specify the options as described in Table 9 on page 26

Table 9: Parameters for Ping IP Address Option

Field	Function	Your Action
Enter IP address to ping	Specify the IP address of the host you want to ping.	Enter an IP address.
Enter ping count	Specify the ping count in the range 1-100. The default value is 5	Enter the ping count.
Enter packet size	Specify the packet size in the range 28-65515. The default value is 64.	Enter the packet size.

Specifying a Traceroute IP Address (CTP Menu)

This topic describes how to specify an IP address and get a traceroute to that address.

To get a traceroute to an IP address by using the CTP Menu:

1. From the Main Menu, select **5) Node Operations**.
2. Select **6) Traceroute IP address**.
3. Specify the options as described in Table 10 on page 26

Table 10: Options for Traceroute

Field	Function	Your Action
Enter IP address for traceroute	Specify the IP address of the host.	Enter an IP address.
Enter max hops	Specify a value for maximum hops in the range 1-40. The default value is 10.	Enter the maximum number of hops.
Enter packet size	Specify a value for packet size in the range 38-65535. The default value is 38.	Enter the packet size.

SSH to Another Host (CTP Menu)

You can do an SSH to a remote host from the CTPMenu by specifying the IP address of the remote host. You can also use the CTPView Node Maintenance window to establish an SSH session to a host. This topic describes how to SSH to remote host from the CTPMenu.

To SSH to a remote host from the CTP Menu:

1. From the Main Menu, select **5) Node Operations**.
2. Select **7) ssh to another host**.
3. When prompted, specify the IP address of the host.

Configuring the CTP Bundle Data Packet Protocol and OAM Port (CTP Menu)

To configure the CTP Bundle Data Packet Protocol using the CTP Menu:

1. From the Main Menu, select **5) Node Operations**.
2. Select **3) Configure network settings**.
3. Select **6) CTP Bndl Data pkt protocol**. The following warning message is displayed.

```
***
*** You are about to modify a system parameter that will require
*** a system reboot when complete.
***
*** If you decide to continue, the system will automatically
*** reboot upon leaving these menus.
***
*** Note: If these parameters are changed incorrectly,
***       system may not be reachable via the network
***       after the system reboots.
***
        Are you sure? y[n]:
```

4. When prompted, specify a value for the protocol ID for data packets in the range 2-254. The default value is 46.

To configure a CTP Bndl OAM port (IPv6):

1. From the Main Menu, select **5) Node Operations**.
2. Select **3) Configure network settings**.
3. Select **7) CTP Bndl OAM port (IPv6)**.
4. When prompted, specify a port number for OAM packets in the range 2 through 254.

   The default value is 16.

Rebooting a Node (CTP Menu)

This parameter allows you to reboot the CTP system. You can also reboot the CTP system from the CTPView Node Maintenance window.

To initialize the database using the CTP Menu:

1. From the Main Menu, select **5) Node Operations**.
2. Select **9) Reboot Node**.

Powering Off the CTP Platform

Use one of the following methods to power off the device:

- Using the **halt** Command at the CTP Command Line

- Using the CTP Menu

To power off the CTP platform from the CTP command line:

Before you power off the device, enter the **halt** command to temporarily suspend the device's operation.

CAUTION: If you do not use the **halt** command before removing or powering down the device, the device's CompactFlash card might become corrupted.

To power off the device from the CTP Menu:

1. From the Main Menu, select **5) Node Operations**.
2. From the Node Operations Menu, select **10) Powerdown Node**.

Displaying Ethernet Media Information (CTP Menu)

This topic describes how to display the supported link modes (speed and duplex) and the configuration of the Ethernet media on CTP devices.

To display Ethernet interface information on a CTP device using the CTP Menu:

1. From the Main Menu, select **5) Node Operations**.
2. Display the current Ethernet configuration by selecting **11) Display ethernet media**.

   A list a of available Ethernet devices and is displayed.
3. Specify the Ethernet device whose details are to be displayed.

   The CTP system displays the details of the Ethernet device that you selected.

Related Documentation

- Ethernet Media Configuration Overview on page 5
- Configuring Ethernet Media (CTP Menu) on page 28

Configuring Ethernet Media (CTP Menu)

You can configure the CTP Ethernet media to autonegotiate the duplex mode and speed and to set the speed to either 100 or 10 Mbps. The Ethernet configurations on the CTP device must match the configuration of the connected router or switch. Mismatched configurations, such as setting the CTP system to autonegotiate and the router to full duplex, may result in a misconfiguration and dropped packets. You must disable Cisco Discovery Protocol on the Fast Ethernet port connected to the CTP system.

To configure Ethernet interfaces on a CTP device using the CTP Menu:

1. From the Main Menu, select **5) Node Operations**.
2. Display the current Ethernet configuration by selecting **12) Config ethernet media**.

```
***
*** You are about to modify a system parameter that will require
*** a system reboot when complete.
***
*** If you decide to continue, the system will automatically
*** reboot upon leaving these menus.
***
*** Note: If these parameters are changed incorrectly,
***       system may not be reachable via the network
***       after the system reboots.
***
        Are you sure? y[n]: y
Here is a list of the available ethernet devices and their descriptions:
        eth0: 10/100/1000 Copper (right)
        eth1: 10/100/1000 Copper (left)
Please input the device to configure the media for: eth0


Configure eth0 (e1000) for autonegotiation? [y] n

Configure eth0 for 100 Mbps [y] n
OK, setting speed to 10 Mbps.
```

Autonegotiation is enabled by default and the speed is set to 1000 Mbps

Field	Function	Your Action
Please input the device to configure the media for	Specifies the Ethernet port	Specify an Ethernet port from the list.
Configure eth0 (e1000) for autonegotiation	Specifies whether autonegotiation is enabled. The default speed for autonegotiation is 1000 Mbps.	Specify **y** or **n**. If you specify **y**, autonegotiation is enabled and the speed is set to 1000 Mbps. If you specify **n**, the system prompts you to set the speed to 100 Mbps.
Configure eth0 for 100 Mbps	Specifies the speed. This field is not displayed if autonegotiation is enabled.	Specify **y** or **n**. If you specify **y**, the system sets the speed to 100 Mbps. If you specify **n**, the speed is set to 10 Mbps.

3. Specify the Ethernet device you want to configure, and follow the onscreen instructions.

Related Documentation

- Ethernet Media Configuration Overview on page 5
- Displaying Ethernet Media Information (CTP Menu) on page 28

NTP Authentication Overview on CTP Devices

Network Time Protocol (NTP) is a UDP protocol for IP networks. It is a protocol designed to synchronize the clock on client machines with the clock on NTP servers. NTP uses Coordinated Universal Time (UTC) as the reference time.

The implementation of NTP requires separate client and server applications. Superficially, NTP is a software daemon operating in a client mode and server mode. Using NTP packets, the client and server exchange time stamp data, ultimately setting the clock on the client machine similar to that of the NTP server. Starting with CTPOS Release 7.2R1, NTP authentication is supported. NTP authentication checks the authenticity of NTP server before synchronizing local time with server. This phenomenon helps you to identify secure servers from unauthorized or illegal servers. NTP authentication works with a symmetric key configured by user. The key is shared by the client and an external NTP server. The servers and clients must agree on the key to authenticate NTP packets. Currently NTP is already supported in CTP devices but NTP authentication is not supported. 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 following are the different operating modes used by NTP:

- Client/Server—In a common client/server model, a client sends an NTP message to one or more servers and processes the replies as received. The server interchanges addresses and ports, overwrites certain fields in the message, recalculates the checksum, and returns the message immediately. Information included in the NTP message allows the client to determine the server time with respect to local time and adjust the local clock.
- Symmetric Active/Passive—Configuring a peer in symmetric-active mode indicates remote server that one wish to obtain time from the remote server and that one is also willing to supply time to the remote server if necessary. This mode is appropriate in configurations involving a number of redundant time servers interconnected through diverse network paths. Symmetric modes are most often used between two or more servers operating as a mutually redundant group.
- Broadcast—The advantage is that clients do not need to be configured for a specific server, as this mode is intended for configurations involving one or a few servers and a possibly very large client population. Broadcast mode requires a broadcast server on the same subnet. Since broadcast messages are not propagated by routers, only broadcast servers on the same subnet are used. Since an intruder can impersonate a broadcast server and inject false time values, this mode should always be authenticated.

In the CTPView server, the Client/Server mode is implemented, which is the use case of the CTP device and CTPView or any other Linux machine within the same network as that of the CTP device will act as NTP servers for authentication.

Although you can configure NTP using the CTPView server in CTPView releases earlier than Release 7.2, you can configure NTP authentication starting from CTPView Release 7.2R1. NTP can only be configured from the CTPView server by using the **System**

Configuration > Node Settings page of the CTPView server. NTP authentication allows the NTP client to verify that servers are known and trusted. Symmetric key authentication will be used to authenticate the packets. It is assumed that the shared secret key is already being communicated between client and server and it is the responsibility of the server to have the shared secret keys already configured in their configuration and keys files. The client then adds the required key id and shared secret key to their configuration and keys files through CTPView or through syscfg commands. The **Key ID** and **Key Value** fields must be left blank in CTPView to disable NTP authentication.

NTP Authentication Procedure

It is assumed that the shared secret key is already being communicated between client and server and it is the responsibility of the server to have the shared secret keys already configured in their configuration and keys files. Also, the "trustedkey keyid" attribute must be mentioned in the server's ntp.conf file and the NTP process (ntpd) must be started in the server side for successful authentication.

The user provides the communicated key id and key values through the CTPView server or syscfg commands. The CTPView server adds the key value and key id to the conf and keys files of the CTP device and starts the NTP daemon. The NTP servers and clients involved must agree on the key, key ID, and key type to authenticate the NTP packets.

When the NTP daemon is started, it reads the key file specified by the keys command and installs the keys in the key cache. It then exchanges packets with its configured servers at poll intervals. The NTP authentication packet adds the key ID and the MAC address in its header, and the packets are accepted by the server only if the key ID matches a trusted key and the message digest is verified with this key. After authentication is successful, the NTP server stores its own timestamp and a transmit timestamp into the packet and send it back to the client. In the case of authentication failure, time is not synchronized.

The following is the example of NTP authentication assuming that the key received from NTP server is 12345 and the key number and corresponding key value is added to the conf and key files of the CTP device.

```
Command - ntpdate -d –a <Key Id> -k /etc/ntp/keys <Server Ip>

Example - ntpdate -d –a 12345 -k /etc/ntp/keys 10.216.118.101


[root@ctp_74 ctp_cmd 36]# ntpdate -d -a 12345 -k /etc/ntp/keys 10.216.118.101
27 May 16:13:41 ntpdate[11935]: ntpdate 4.2.8@1.3265-o Tue Jan  6 05:50:59 UTC
2015 (3)
Looking for host 10.216.118.101 and service ntp
host found : 10.216.118.101
transmit(10.216.118.101)
receive(10.216.118.101)
receive: authentication passed
transmit(10.216.118.101)
receive(10.216.118.101)
receive: authentication passed
transmit(10.216.118.101)
receive(10.216.118.101)
receive: authentication passed
transmit(10.216.118.101)
```

```
receive(10.216.118.101)
receive: authentication passed
server 10.216.118.101, port 123
stratum 11, precision -21, leap 00, trust 000
refid [10.216.118.101], delay 0.02577, dispersion 0.00006
transmitted 4, in filter 4
reference time:    d9101e66.08f2fe3d  Wed, May 27 2015 10:43:50.034
originate timestamp: d9101e68.fbd8b5c6  Wed, May 27 2015 10:43:52.983
transmit timestamp:  d9106bbb.82aca793  Wed, May 27 2015 16:13:47.510
filter delay:  0.02580  0.02579  0.02577  0.02579
         0.00000  0.00000  0.00000  0.00000
filter offset: -19794.5 -19794.5 -19794.5 -19794.5
         0.000000 0.000000 0.000000 0.000000
delay 0.02577, dispersion 0.00006
offset -19794.526903

27 May 16:13:47 ntpdate[11935]: step time server 10.216.118.101 offset
-19794.526903 sec
```

The preceding command, when run without “-d” option, synchronizes the time of CTP device with the NTP server. The “-d” option runs in debug mode, prints the intermediate results, and does not adjust the clock. If the key number or key value are not correct, then the message “authentication passed” is replaced with “authentication failed” and time is not synchronized.

Configuring NTP Authentication Using the System Query Page (CTPView)

NTP authentication enables the CTP device, which functions as the NTP client, to verify that servers are known and trusted. Symmetric key authentication will be used to authenticate the packets. It is assumed that the shared secret key is already being communicated between client and server and it is the responsibility of the server to have the shared secret keys already configured in their configuration and keys files. The client then adds the required key id and shared secret key to their configuration and keys files through CTPView or through syscfg commands. The **Key ID** and **Key Value** fields must be left blank in CTPView to disable NTP authentication.

To configure NTP authentication using the System Query page of CTPView:

1. In the side pane, select **System** > **Query**.

   

   TIP: Alternatively, you can specify the key ID and key value for NTP authentication from the System Configuration page by selecting **System** > **Configuration** in the side pane.

2. Click **Node Settings** tab.

   The NTP Settings page is displayed. The hostname and IP address of the CTP device are displayed under the Device table, which is shown to the left of the NTP Settings table.

3. Configure the parameters described in Table 11 on page 33 and click **Submit Settings**.
4. (Optional) Click **System** > **Query** > **Node Settings** to verify the NTP configuration details.

Table 11: NTP Server Authentication Settings on the System Query Page in CTPView

Field	Function	Your Action
Server IP	Specifies the IPv4 or IPV6 address of the NTP server. Adds NTP servers to the server list (IP addresses or hostnames). You can configure a maximum of two NTP servers. NTP authentication is started from the first server in the list and if the first server fails or becomes unavailable, the second server in the list is used.	Enter the IPv4 or IPv6 address of the NTP server to be used for authentication.
Key ID	Specifies the key ID to authenticate the NTP packets received from the server by the NTP client. The servers and clients involved must agree on the key and key identifier to authenticate NTP packets. Keys and related information are specified in a key file. Key ID is used to prove authenticity of data received over the network. During the synchronization of time, the client requests the key ID with the “NTP Client” packet and server sends the response with the “NTP Server” packet. If the key ID differs in both the packets, then the time does not synchronize. The time is synchronized and modified for the client only when the two key IDs are the same. The IP address with the secret key is configured in the “/etc/ntp.conf” NTP configuration file on the CTP device. The following is the example for the ntp.conf file: ‘server x.x.x.x key 123’ where: x.x.x.x is the NTP server IP address Key is the secret key id which is shared by both the client and server.	Enter a 32-bit integer in the range of 1 through 65534.

Table 11: NTP Server Authentication Settings on the System Query Page in CTPView *(continued)*

Field	Function	Your Action
Key Value	Specifies the value of the NTP key used for NTP authentication between the NTP server and the NTP client. NTP uses keys to implement authentication. This key is used while exchanging data between the client and server. The following three key types are present: • An A key is just a sequence of up to eight ASCII characters. • An M key is a sequence of up to 31 ASCII characters. • An S key is a 64 bit value with the low order bit of each byte being odd parity. CTP devices support the M key (MD5) for NTP authentication. All the keys must be defined in the "/etc/ntp/keys" file. The following is an example for the keys file: '123 M pass' where: 123 is the key id (range 1 to 65534) M designates the key type (M means MD5 encryption) Pass denotes the key itself	Enter the key value as a sequence of up to 31 ASCII characters.
Status	Specifies whether you want to enable or disable the NTP process on the CTP device.	Select one: • Enabled—Enables the NTP process on the CTP device. • Disabled—Disables the NTP process on the CTP device.

Support for Multiple Master Nodes to Associate With a Single Backup Node in NetRef

Network node reference (NetRef) is an extension of the CTP adaptive port clocking. NetRef can be used to provide node level synchronization across a network. When NetRef is configured for primary or backup operation, the primary node sends clocking information to the backup node. The backup node uses an algorithm similar to that used for adaptive port clocking to control the local node clock so that it follows the clocking of the remote node. To operate in primary or backup mode, the remote primary node must be configured as a NetRef primary node with the IP address of the NetRef slave configured. The backup node must be configured as a NetRef backup node with the IP address of the NetRef primary node configured. You can configure up to four master modes, each of which can send their clocking information to a maximum of 10 slaves and the slave node can receive clocking information from the configured master nodes.

You can configure the four master nodes using CTP Menu or the CTPView web server during Netref slave configuration. As a result, a single slave node can use the IP address of up to four master nodes while you configure Netref slave node settings.

Each master node is assigned a priority during Netref slave configuration. The master node with the highest priority is assigned Priority 1, the second highest priority for the

master node is Priority 2, and so on. You cannot configure the priority of the master nodes. The priorities assigned are unique for each masters while configuring Netref slave nodes. The slave nodes synchronize their local clock with the clock of the highest priority master node (Priority 1 master node). After the highest priority master goes down or when a problem occurs during the clock synchronization phase, the CTP device switches to its next highest priority master (Priority 2 master node). The slave nodes synchronize their clock with the clock of Priority 2 master node. The priorities of the master nodes are also switched in the backend, after switching of the master nodes takes place. In the case of flapping between the masters, the primary master (high priority) is retained or binding with the master that contains a good clock quality is maintained.

When switching of the masters takes place, an event of mastership change is logged into the syslog messages. The slave node synchronization query provides the details of the master node to which the slave is locked and the details of the configured master nodes along with their assigned priorities. You cannot configure the lowest priority masters until its higher priority masters are configured. Similarly, you cannot disable the highest priority masters until its lower priority masters are disabled.

When a node is configured as NetRef Master, it starts generating the NetRef packets and send them to the slave nodes. The slave node accepts the packets from the highest priority master node and the NetRef state of the slave node is changed to wait state. If 16 sequenced packets are received by the slave nodes, the NetRef state is changed from **Wait** state to **Aggressive** state. At this stage, if 8 packets are missed continuously, the NetRef state again moves back to the **Wait** state. These NetRef packets are processed and slope is calculated. Based on the slope, the clock of the slave node is in synchronization with the master node and the state changes to the **Maintain** state. The state changes from **Maintain** or **Aggressive** to **Starvation** when no NetRef packet is received in last 20 seconds. As soon as the node goes to **Starvation** state, switching of the master takes place. The packets are processed by the slave nodes to synchronize their clock with the next highest priority master node. Flapping of the masters occurs if you continuously “round robin” to each master and wait for 20 seconds for an incoming NetRef packet.

The LED becomes red when NetRef is in **Wait** or **Aggressive** state. The LED is green when NetRef is in **Maintain** state. The switching of the masters occurs as described in the following table:

Slave Nodes	Assigned Priority	Assigned Priority After First Failure	Assigned Priority After Second Failure	Assigned Priority After Third Failure	Assigned Priority After Fourth Failure
Master 1	1 (primary)	4	3	2	1 (primary)
Master 2	2	1 (primary)	4	3	2
Master 3	3	2	1 (primary)	4	3
Master 4	4	3		1 (primary)	4

If all the four master nodes goes down, the NetRef state remains in **Starvation** state and no switching will take place. When the NetRef state of the slave node is Maintain and the primary master goes down, the slave node is unable to receive the packets within the last 20 seconds. Therefore, the NetRef state of the slave node moves from **Maintain** state to **Starvation** state and switching takes place. When the NetRef state of the slave node is **Aggressive** and the primary master goes down, the slave node is unable to receive the packets within the last 20 seconds. Therefore, the NetRef state of the slave node transitions from **Aggressive** state to **Starvation** state and switching will take place.

When the NetRef state of the slave node is in **Wait** state (waiting for NetRef packets from the primary master node) and the primary master node is disabled but the secondary master nodes are sending NetRef packets to the slave node, switching will take place.

Revert option is not supported; when the primary node comes up, the slave node remains locked to the secondary master node and does not become locked to the primary master node.

Without multiple master nodes support, when a node is configured as slave, the node www_db string is

"23|0,0,0,0,0,0,0,0,0,0,5|5|5|5|5|5|5|2|64|127.0.0.1/127.0.0.1/127.0.0.1/127.0.0.1/127.0.0.1/127.0.0.1/127.0.0.1/127.0.0.1/127.0.0.1/0|255|0;"

This www_db string is not different when multiple master nodes are configured for a backup node. The first IP address in the www_db string contains a priority of 1, the second contains a priority of 2, and so on, as shown as follows:

"23|0,0,0,0,0,0,0,0,0,0,5|5|5|5|5|5|5|2|64|10.216.187.3/10.216.188.6/10.216.189.0/10.216.188.8/127.0.0.1/127.0.0.1/127.0.0.1/127.0.0.1/127.0.0.1/0|255|0;"
When node is configured as master, the node www_db string will remain same as it is there in the earlier releases.

Configuring NetRef Multiple Master Nodes (CTP Menu)

NetRef primary backup operation involves a new packet flow from the primary node to all the backup nodes. These timing packets are sent at a rate of approximately 4.5 packets per second.

NOTE: In this topic, the terms *Primary* and *Backup* refer to master and slave operations or nodes, respectively.

To configure network node reference with multiple master nodes:

1. From the Main Menu, select **2) Node Synchronization**
2. Select **6) NetRef** to configure NetRef configuration parameters.

NOTE: You can select **1) 1st Priority, Reference 0**, **2) 2nd Priority, Reference 1**, **3) 3rd Priority, Reference 2**, **4) 4th Priority, Reference 3**, and **5) 5th Priority, Reference** to specify the prioritized node clock references. An external reference input and any of the serial interfaces may be used for the node reference clock. Reference frequencies must be 32 KHz, n x 64 KHz, or 1,544 KHz up to a maximum of 4096 KHz (2048 KHz maximum on the CTP1002).

3. From the NetRef Menu, **1) NetRef** to enable NetRef on the CTP device..

```
Enable NetRef (0=Off, 1=Master, 2=Slave, 3=Adaptive Bundle)? (0-3)[2]:
```

4. Enter **2** to select Slave mode.
5. From the NetRef Menu, select **2) NetRef Master IP (Priority 1)**. and specify the IP address of the NetRef master node, which is assigned a priority of 1.
6. From the NetRef Menu, select **3) NetRef Master IP (Priority 1)**. and specify the IP address of the NetRef master node, which is assigned a priority of 2.
7. From the NetRef Menu, select **4) NetRef Master IP (Priority 1)**. and specify the IP address of the NetRef master node, which is assigned a priority of 3.
8. From the NetRef Menu, select **5) NetRef Master IP (Priority 1)**. and specify the IP address of the NetRef master node, which is assigned a priority of 4.

```
Please select a number from the following list:
-------------------------------------
 0) Exit to Shell
 1) Bundle Operations
 2) Node Synchronization
 3) Node Summary
 4) Node Diagnostics
 5) Node Operations
 6) Save Running Database to Flash
------------ Your choice [3]: 2

=============================================================================
= (ctp_74 06/24/15 19:25:18  UTC) | Node Synchronization Menu
=============================================================================

Please select a number from the following list:
-------------------------------------
 0) Back to Previous Menu
 1) 1st Priority, Reference 0: Disabled
 2) 2nd Priority, Reference 1: Disabled
 3) 3rd Priority, Reference 2: Disabled
 4) 4th Priority, Reference 3: Disabled
 5) 5th Priority, Reference 4: Disabled
 6) NetRef:                    Disabled
 7) 32 kHz Ref Output:         NO
 8) Query Node Sync Status
 9) Measure Ref Inputs
10) Calibrate Node to Current Reference
------------ Your choice [6]: 6


=============================================================================
```

```
= (ctp_74 06/24/15 19:25:38  UTC) | NetRef Menu
================================================================================

Please select a number from the following list:
-------------------------------------
 0) Back to Previous Menu
 1) NetRef:             Disabled
------------ Your choice [1]: 1
Enable NetRef (0=Off, 1=Master, 2=Slave, 3=Adaptive Bundle)? (0-3)[0]: 2


================================================================================
= (ctp_74 06/24/15 19:25:42  UTC) | NetRef Menu
================================================================================

Please select a number from the following list:
-------------------------------------
 0) Back to Previous Menu
 1) NetRef:             Slave
 2) NetRef Master IP (Priority 1):  127.0.0.1
 3) NetRef Master IP (Priority 2):  127.0.0.1
 4) NetRef Master IP (Priority 3):  127.0.0.1
 5) NetRef Master IP (Priority 4):  127.0.0.1
------------ Your choice [2]: 2

Configure a NetRef Master?  n[y]: y

Enter remote node IP address for NetRef:(rtn for 127.0.0.1)? 10.216.118.73


================================================================================
= (ctp_74 10/30/15 12:22:08  UTC) | NetRef Menu
================================================================================

Please select a number from the following list:
-------------------------------------
 0) Back to Previous Menu
 1) NetRef:             Slave
 2) NetRef Master IP (Priority 1):  10.216.118.73
 3) NetRef Master IP (Priority 2):  127.0.0.1
 4) NetRef Master IP (Priority 3):  127.0.0.1
 5) NetRef Master IP (Priority 4):  127.0.0.1
------------ Your choice [2]: 3

Configure a NetRef Master?  n[y]: y

Enter remote node IP address for NetRef:(rtn for 127.0.0.1)? 10.216.118.86


================================================================================
= (ctp_74 10/30/15 12:48:56  UTC) | NetRef Menu
================================================================================

Please select a number from the following list:
-------------------------------------
 0) Back to Previous Menu
 1) NetRef:             Slave
 2) NetRef Master IP (Priority 1):  10.216.118.73
 3) NetRef Master IP (Priority 2):  10.216.118.86
 4) NetRef Master IP (Priority 3):  127.0.0.1
 5) NetRef Master IP (Priority 4):  127.0.0.1
```



```
------------ Your choice [3]: 4

Configure a NetRef Master?  n[y]: y

Enter remote node IP address for NetRef:(rtn for 127.0.0.1)? 10.216.118.90


================================================================================
= (ctp_74 10/30/15 12:49:04  UTC) | NetRef Menu
================================================================================

Please select a number from the following list:
-----------------------------------
 0) Back to Previous Menu
 1) NetRef:             Slave
 2) NetRef Master IP (Priority 1):  10.216.118.73
 3) NetRef Master IP (Priority 2):  10.216.118.86
 4) NetRef Master IP (Priority 3):  10.216.118.90
 5) NetRef Master IP (Priority 4):  127.0.0.1
------------ Your choice [4]: 5

Configure a NetRef Master?  n[y]: y

Enter remote node IP address for NetRef:(rtn for 127.0.0.1)? 10.216.118.88


================================================================================
= (ctp_74 10/30/15 12:49:12  UTC) | NetRef Menu
================================================================================

Please select a number from the following list:
-----------------------------------
 0) Back to Previous Menu
 1) NetRef:             Slave
 2) NetRef Master IP (Priority 1):  10.216.118.73
 3) NetRef Master IP (Priority 2):  10.216.118.86
 4) NetRef Master IP (Priority 3):  10.216.118.90
 5) NetRef Master IP (Priority 4):  10.216.118.88
------------ Your choice [5]:
```

NOTE: When a node is configured for NetRef backup operation, the remote address must be configured to that of the primary node. Likewise, the NetRef primary node must be configured with the IP address of the NetRef backup node. A NetRef primary node can be configured to send data packets to up to 10 NetRef backup nodes.

Rate selection and clock configuration allow the serial interface rate to be configured through the software. Rates supported range from less than 300 bps to 12.288 Mbps (in subhertz increments). You can configure the CTP systems by using the menu interface to provide multiple prioritized node clock references. An external reference input and any of the serial interfaces may be used for the node reference clock. Reference frequencies must be 32 KHz, n x 64 KHz, or 1,544 KHz up to a maximum of 4096 KHz (2048 KHz maximum on the CTP1002).

Follow the onscreen instructions and configure the options as described inTable 12 on page 40.

Table 12: Configuring Multiple NetRef Master Node IP Addresses

Field	Function	Your Action
NetRef Master IP (Priority)	Specifies whether you want to configure multiple master nodes with priorities, which can be used to transmit clocking information to the backup nodes in NetRef.	Enter **2**, **3**, **4**, and **5** to configure NetRef master nodes with priorities 1, 2, 3, and 4, respectively.
Configure a NetRef Master? n[y]	Specifies whether you want to configure a NetRef master node.	Specify **y** or **n**.
Enter remote node IP address for NetRef	Specifies the IP address of the NetRef master node..	Specify IP address of the NetRef master node assigned with different priorities. Specify **rtn** to set the IP address of 127.0.0.1 interface that is prompted by the system to be specified as the default IPv4 address of the master node. For example, if the prompt displays **(rtn for 127.0.0.1)**, and if you specify **rtn**, **127.0.0.1** is set as the default IP address.

Related Documentation

- *Configuring NetRef for Adaptive Bundle Operation*
- *Network Node Reference Overview*

Unlocking User Accounts for Which Password Has Expired

To support the U.S. Department of Defense Joint Interoperability Test Command (JITC) requirements, when the security level of the CTP Series platforms is set as high, the JITC high security mode requires that the CTP device must automatically disable accounts after a 35-day period of account inactivity. This requirement- standard denotes that the password of all those user accounts that do not login to the CTP device or CTPView server for the past 35 days. You can unlock those user accounts in compliance with the JITC specification.

A lockout warning message is displayed only for System Administrator and CTP Administrator accounts and not for other user accounts. The lockout warning messages are recorded in the network syslog file to inform the list of those system administrator accounts, which are due to be locked in next 10 days.

All the users authorized to access the syslog file can view the lockout warning messages. The lockout warning messages are started to be sent from 10 days before the date on which the account is bound to be locked. For example, when an account is due to be locked because of not having been accessed for the last 25 days, the first warning message is sent on 25th day, the second warning message is sent on the 26th day, and so on, until the 35th day is reached and the account is locked. All the users whose accounts are locked can request the system administrators or root access-privileged users to unlock the accounts for them.

A script “reset_pw_lock <user>” is added on the CTP device and the CTPView server.

Script to Monitor the Duration of Inactivity of User Accounts

The “activity_check” script file that is already available on the CTP Series platforms and CTPView server at the /etc/cron.daily/activity_check path is enhanced to send the lockout warning messages to the network syslog. Currently, this file is used to lock the user accounts after a 35-day period of account inactivity.

The following sequence of events occur with the “activity_check” script that is used for sending the lockout warning messages.

1. If the user account is not already locked, then the script identifies the date on which the user was logged in. If the user has not logged in for the last 25 days, and if the user is a system administrator, then a warning message is generated and transmitted to the syslog with the severity level of the log greater than 8.
2. If the user account is not already locked, then the script determines the date on which the user account was created. If the user has not logged in for the last 25 days, and if the user is a system administrator, then a warning message is generated and transmitted to the syslog with the severity level of the log greater than 8.

Script to Reset the Expired User Accounts

The reset_pw_lock script is added to the CTP device CTP Box and CTPView server in the /bin folder. This script can also be run in shell or CLI mode. With locked user accounts (in which the user cannot log in to shell), the user needs to manually change to single-user mode to run this script. The script can be run by entering the reset_pw_lock <user> command. The script unlocks the password of only the user specified in the command. With multiple users, you can enter the command as reset_pw_lock <user1> <user2> .... When you run this script, it unlocks the password of the specified user account, performs the mounting operations, and reboots the system. The activity_check script file is modified to send the lockout warning message to the network syslog. The reset_pw_lock script is added to unlock the password of disabled user accounts.