Security and Timing

This chapter provides information about Cisco ONS 15454 users and SONET timing. To provision security and timing, refer to the *Cisco ONS 15454 Procedure Guide*.

Note The terms "Unidirectional Path Switched Ring" and "UPSR" may appear in Cisco literature. These terms do not refer to using Cisco ONS 15xxx products in a unidirectional path switched ring configuration. Rather, these terms, as well as "Path Protected Mesh Network" and "PPMN," refer generally to Cisco's path protection feature, which may be used in any topological network configuration. Cisco does not recommend using its path protection feature in any particular topological network configuration.

Chapter topics include:

9.1 Users and Security

The CISCO15 ID is provided with the ONS 15454 system, but this user ID is not prompted when you sign into CTC. This ID can be used to set up other ONS 15454 users. (To do this, complete the “Create Users and Assign Security” procedure in the *Cisco ONS 15454 Procedure Guide*.)

You can have up to 500 user IDs on one ONS 15454. Each Cisco Transport Controller (CTC) or TL1 user can be assigned one of the following security levels:

- Retrieve—Users can retrieve and view CTC information but cannot set or modify parameters.
- Maintenance—Users can access only the ONS 15454 maintenance options.
- Provisioning—Users can access provisioning and maintenance options.
- Superusers—Users can perform all of the functions of the other security levels as well as set names, passwords, and security levels for other users.

By default, multiple concurrent user ID sessions are permitted on the node, that is, multiple users can log into a node using the same user ID. However, you can provision the node to allow only a single login per user and prevent concurrent logins for all users.

Note You must add the same user name and password to each node the user accesses.

9.1.1 Security Requirements

Table 9-1 shows the actions that each user privilege level can perform in node view.

Table 9-1 ONS 15454 Security Levels—Node View

CTC Tab	Subtab	[Subtab]:Actions	Retrieve	Maintenance	Provisioning	Superuser
Alarms	—	Synchronize/Filter/Delete Cleared Alarms	X	X	X	X
Conditions	—	Retrieve/Filter	X	X	X	X
History	Session	Filter	X	X	X	X
	Node	Retrieve/Filter	X	X	X	X
Circuits	—	Create/Edit/Delete	—	Partial[1]	X	X
		Filter/Search	X	X	X	X
Provisioning	General	General: Edit	—	—	Partial[2]	X
		Power Monitor: Edit	—	—	X	X
	EtherBridge	Spanning trees: Edit	—	—	X	X
	Network	General: All	—	—	—	X
		Static Routing: Create/Edit/ Delete	—	—	X	X
		OSPF: Create/Edit/Delete	—	—	X	X
		RIP: Create/Edit/Delete	—	—	X	X
	Protection	Create/Delete/Edit	—	—	X	X
		View	X	X	X	X
	BLSR	All	—	—	X	X
	Security	Users: Create/Change/Delete	—	—	—	X
		Users: Change password	Same user	Same user	Same user	All users
		Active Logins: Logout	—	—	—	X
		Policy: Edit	—	—	—	X
		Access: Edit	—	—	—	X
		Legal Disclaimer: Edit	—	—	—	X
	SNMP	Create/Delete/Edit	—	—	X	X
		Browse trap destinations	X	X	X	X
	DCC/GCC/OSC	SDCC: Create/Edit/Delete	—	—	X	X
		LDCC: Create/Edit/Delete	—	—	X	X
		GCC: Create/Edit/Delete	—	—	X	X
		OSC: Create/Edit/Delete	—	—	X	X
	Timing	Edit	—	—	X	X
	Alarm Profiles	Alarm Profiles: Edit	—	—	X	X
		Alarm Profiles Editor: Load/Store/Compare	—	—	X	X

Table 9-1 ONS 15454 Security Levels—Node View (continued)

CTC Tab	Subtab	[Subtab]:Actions	Retrieve	Maintenance	Provisioning	Superuser
Provisioning (continued)	Defaults	Edit	—	—	—	X
	UCP	Node: Edit/Provision	—	—	X	X
		Neighbor: Create/Edit/Delete	—	—	X	X
		IPCC: Create/Edit/Delete	—	—	X	X
		Interface: Create/Edit/Delete	—	—	X	X
		Neighbor: Create/Edit/Delete	—	—	X	X
	WDM-ANS	Circuit: Create/Edit/Delete	—	—	X	X
		Connections: Create/Edit/Delete/Commit/ Calculate	—	—	X	X
		Services: Launch	—	—	X	X
		NE update: Edit/Reset/Import/Export	—	—	X	X
Inventory	—	Delete	—	—	X	X
		Reset	—	X	X	X
Maintenance	Database	Backup	—	X	X	X
		Restore	—	—	—	X
	EtherBridge	Spanning Trees: View	X	X	X	X
		MAC Table: Retrieve	X	X	X	X
		MAC Table: Clear/Clear All	—	X	X	X
		Trunk Utilization: Refresh	X	X	X	X
		Circuits: Refresh	X	X	X	X
	Protection	Switch/Lock out operations	—	X	X	X
	BLSR	Ring/Span Switches	—	—	X	X
	Software	Download	—	X	X	X
		Upgrade/Activate/Revert	—	—	—	X
	Cross-Connect	Protection Switches	—	X	X	X
	Overhead XConnect	Read only	—	—	—	—
	Diagnostic	Retrieve/Lamp Test	—	Partial	X	X
	Timing	Source: Edit	—	X	X	X
		Timing Report: View/Refresh	—	X	X	X
	Audit	Retrieve	—	—	—	X
	Routing Table	Read-only	—	—	—	—
	RIP Routing Table	Refresh	X	X	X	X

Table 9-1 ONS 15454 Security Levels—Node View (continued)

CTC Tab	Subtab	[Subtab]:Actions	Retrieve	Maintenance	Provisioning	Superuser
Maintenance (continued)	Test Access	Read-only	X	X	X	X

1. Maintenance user can edit path protection circuits.
2. Provisioner user cannot change node name, contact, daylight savings, or AIS-V insertion on STS-1 signal degrade (SD) parameters.

Table 9-2 shows the actions that each user privilege level can perform in network view.

Table 9-2 ONS 15454 Security Levels—Network View

CTC Tab	Subtab	[Subtab]: Actions	Retrieve	Maintenance	Provisioning	Superuser
Alarms	—	Synchronize/Filter/Delete cleared alarms	X	X	X	X
Conditions	—	Retrieve/Filter	X	X	X	X
History	—	Filter	X	X	X	X
Circuits	—	Create/Edit/Delete/Filter	—	Partial	X	X
		Search	X	X	X	X
Provisioning	Security	Users: Create/Change/Delete	—	—	—	X
		Active logins: Logout	—	—	—	X
		Policy: Change	—	—	—	X
	Alarm Profiles	Load/Store/Delete	—	—	X	X
		Compare/Available/Usage	—	X	X	X
	BLSR	Create/Delete/Edit/Upgrade	—	—	X	X
Overhead Circuits		Create/Delete/Edit/Merge	—	—	X	X
		Search	X	X	X	X

9.1.2 Security Policies

Users with Superuser security privilege can provision security policies on the ONS 15454. These security policies include idle user timeouts, password changes, password aging, and user lockout parameters. In addition, a Superuser can access the ONS 15454 through the TCC2 RJ-45 port, the backplane LAN connection, or both.

9.1.2.1 Idle User Timeout

Each ONS 15454 CTC or TL1 user can be idle during his or her login session for a specified amount of time before the CTC window is locked. The lockouts prevent unauthorized users from making changes. Higher-level users have shorter default idle periods and lower-level users have longer or unlimited default idle periods, as shown in Table 9-3. The user idle period can be modified by a Superuser; refer to the *Cisco ONS 15454 Procedure Guide* for instructions.

Table 9-3 ONS 15454 Default User Idle Times

Security Level	Idle Time
Superuser	15 minutes
Provisioning	30 minutes
Maintenance	60 minutes
Retrieve	Unlimited

9.1.2.2 User Password, Login, and Access Policies

Superusers can view real-time lists of users who are logged into CTC or TL1 user logins by node. Superusers can also provision the following password, login, and node access policies.

- Password expirations and reuse—Superusers can specify when users must change and when they can reuse their passwords.
- Locking out and disabling users—Superusers can provision the number of invalid logins that are allowed before locking out users and the length of time before inactive users are disabled.
- Node access and user sessions—Superusers can limit the number of CTC sessions one user can have, and they can prohibit access to the ONS 15454 using the LAN or TCC2 RJ-45 connections.

  In addition, a Superuser can select secure shell (SSH) instead of Telnet at the CTC Provisioning > Security > Access tabs. SSH is a terminal-remote host Internet protocol that uses encrypted links. It provides authentication and secure communication over unsecure channels. Port 22 is the default port and cannot be changed.

Note The superuser cannot modify the privilege level of an active user. The CTC displays a warning message when the superuser attempts to modify the privilege level of an active user.

9.1.2.3 Audit Trail

The ONS 15454 maintains a 640-entry, human-readable audit trail of user or system actions such as login, logout, circuit creation or deletion, and user- or system-generated actions. You can move the log to a local or network drive for later review. The ONS 15454 generates an event to indicate when the when the log is 80 percent full, and another event to indicate that the oldest log entries are being overwritten.

9.2 Node Timing

SONET timing parameters must be set for each ONS 15454. Each ONS 15454 independently accepts its timing reference from one of three sources:

- The building integrated timing supply (BITS) pins on the ONS 15454 backplane.
- An OC-N card installed in the ONS 15454. The card is connected to a node that receives timing through a BITS source.
- The internal ST3 clock on the TCC2 card.

You can set ONS 15454 timing to one of three modes: external, line, or mixed. If timing is coming from the BITS pins, set ONS 15454 timing to external. If the timing comes from an OC-N card, set the timing to line. In typical ONS 15454 networks:

- One node is set to external. The external node derives its timing from a BITS source wired to the BITS backplane pins. The BITS source, in turn, derives its timing from a primary reference source (PRS) such as a Stratum 1 clock or global positioning satellite (GPS) signal.
- The other nodes are set to line. The line nodes derive timing from the externally timed node through the OC-N trunk (span) cards.

You can set three timing references for each ONS 15454. The first two references are typically two BITS-level sources, or two line-level sources optically connected to a node with a BITS source. The third reference is usually assigned to the internal clock provided on every ONS 15454 TCC2 card. However, if you assign all three references to other timing sources, the internal clock is always available as a backup timing reference. The internal clock is a Stratum 3 (ST3), so if an ONS 15454 node becomes isolated, timing is maintained at the ST3 level.

The CTC Maintenance > Timing > Report tabs show current timing information for an ONS 15454, including the timing mode, clock state and status, switch type, and reference data.

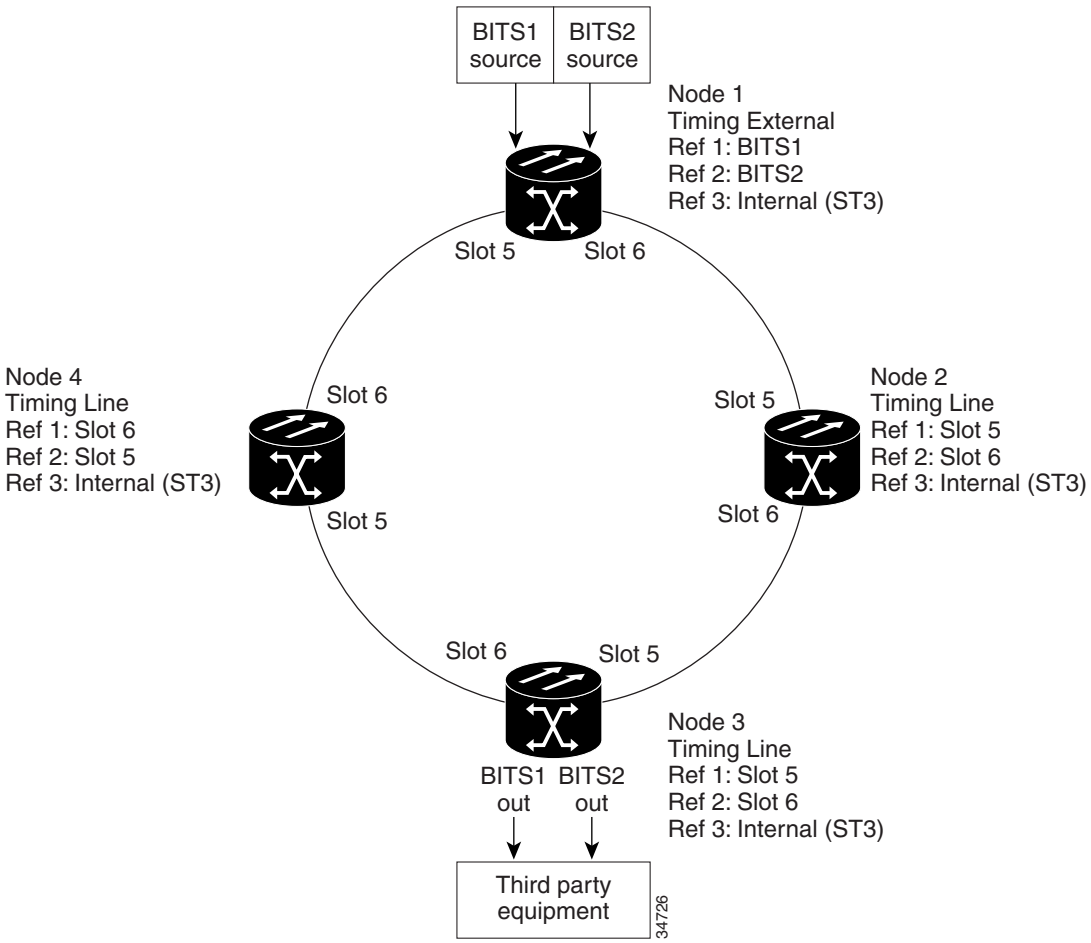
Caution Mixed timing allows you to select both external and line timing sources. However, Cisco does not recommend its use because it can create timing loops. Use this mode with caution.

9.2.1 Network Timing Example

Figure 9-1 shows an ONS 15454 network timing setup example. Node 1 is set to external timing. Two timing references are set to BITS. These are Stratum 1 timing sources wired to the BITS input pins on the Node 1 backplane. The third reference is set to internal clock. The BITS output pins on the backplane of Node 3 are used to provide timing to outside equipment, such as a digital access line access multiplexer.

In the example, Slots 5 and 6 contain the trunk (span) cards. Timing at Nodes 2, 3, and 4 is set to line, and the timing references are set to the trunk cards based on distance from the BITS source. Reference 1 is set to the trunk card closest to the BITS source. At Node 2, Reference 1 is Slot 5 because it is connected to Node 1. At Node 4, Reference 1 is set to Slot 6 because it is connected to Node 1. At Node 3, Reference 1 could be either trunk card because they are equal distance from Node 1.

Figure 9-1 ONS 15454 Timing Example



9.2.2 Synchronization Status Messaging

Synchronization status messaging (SSM) is a SONET protocol that communicates information about the quality of the timing source. SSM messages are carried on the S1 byte of the SONET Line layer. They enable SONET devices to automatically select the highest quality timing reference and to avoid timing loops.

SSM messages are either Generation 1 or Generation 2. Generation 1 is the first and most widely deployed SSM message set. Generation 2 is a newer version. If you enable SSM for the ONS 15454, consult your timing reference documentation to determine which message set to use. Table 9-4 and Table 9-5 on page 9-8 show the Generation 1 and Generation 2 message sets.

Table 9-4 SSM Generation 1 Message Set

Message	Quality	Description
PRS	1	Primary reference source—Stratum 1
STU	2	Synchronization traceability unknown
ST2	3	Stratum 2

Table 9-4 SSM Generation 1 Message Set (continued)

Message	Quality	Description
ST3	4	Stratum 3
SMC	5	SONET minimum clock
ST4	6	Stratum 4
DUS	7	Do not use for timing synchronization
RES		Reserved; quality level set by user

Table 9-5 SSM Generation 2 Message Set

Message	Quality	Description
PRS	1	Primary reference source—Stratum 1
STU	2	Synchronization traceability unknown
ST2	3	Stratum 2
TNC	4	Transit node clock
ST3E	5	Stratum 3E
ST3	6	Stratum 3
SMC	7	SONET minimum clock
ST4	8	Stratum 4
DUS	9	Do not use for timing synchronization
RES		Reserved; quality level set by user