



Transients Conditions

This chapter gives a description, entity, SNMP number, and trap for each commonly encountered Cisco ONS 15454 transient condition.

3.1 Transients Indexed By Alphabetical Entry

Table 3-1 alphabetically lists all ONS 15454 transient conditions and their entity, SNMP number, and SNMP trap.



Note

The CTC default alarm profile might contain conditions that are not currently implemented but are reserved for future use.

Table 3-1 ONS 15454 Transient Condition Alphabetical Index

| Transient Condition | Entity | SNMP Number | SNMP Trap |
|---|--------|-------------|-----------------------------------|
| 3.3.1 ADMIN-DISABLE, page 3-4 | NE | 5270 | disableInactiveUser |
| 3.3.2 ADMIN-DISABLE-CLR, page 3-4 | NE | 5280 | disableInactiveClear |
| 3.3.3 ADMIN-LOCKOUT, page 3-4 | NE | 5040 | adminLockoutOfUser |
| 3.3.4 ADMIN-LOCKOUT-CLR, page 3-4 | NE | 5050 | adminLockoutClear |
| 3.3.5 ADMIN-LOGOUT, page 3-4 | NE | 5020 | adminLogoutOfUser |
| 3.3.6 ADMIN-SUSPEND, page 3-4 | NE | 5340 | suspendUser |
| 3.3.7 ADMIN-SUSPEND-CLR, page 3-5 | NE | 5350 | suspendUserClear |
| 3.3.8 AUTOWDMANS, page 3-5 | NE | 5690 | automaticWdmAnsFinished |
| 3.3.9 BLSR-RESYNC, page 3-5 | OCN | 2100 | blsrMultiNodeTableUpdateCompleted |
| 3.3.10 DBBACKUP-FAIL, page 3-5 | EQPT | 3724 | databaseBackupFailed |
| 3.3.11 DBRESTORE-FAIL, page 3-5 | EQPT | 3726 | databaseRestoreFailed |
| 3.3.12 EXERCISING-RING, page 3-6 | OCN | 3400 | exercisingRingSuccessfully |
| 3.3.13 FIREWALL-DIS, page 3-6 | NE | 5230 | firewallHasBeenDisabled |

Table 3-1 ONS 15454 Transient Condition Alphabetical Index (continued)

| Transient Condition | Entity | SNMP Number | SNMP Trap |
|--|------------------------------|-------------|--|
| 3.3.14 FRCDWKSWBK-NO-TRFSW, page 3-6 | OCN | 5560 | forcedSwitchBackToWorkingResultedInNoTrafficSwitch |
| 3.3.15 FRCDWKSWPR-NO-TRFSW, page 3-6 | OCn | 5550 | forcedSwitchToProtectResultedInNoTrafficSwitch |
| 3.3.16 INTRUSION, page 3-6 | NE | 5250 | securityIntrusionDetUser |
| 3.3.17 INTRUSION-PSWD, page 3-6 | NE | 5240 | securityIntrusionDetPwd |
| 3.3.18 IOSCFG-COPY-FAIL, page 3-7 | — | 3660 | iosConfigCopyFailed |
| 3.3.19 LOGIN-FAILURE-LOCKOUT, page 3-7 | NE | 5080 | securityInvalidLoginLockedOutSeeAuditLog |
| 3.3.20 LOGIN-FAILURE-ONALRDY, page 3-7 | NE | 5090 | securityInvalidLoginAlreadyLoggedOnSeeAuditLog |
| 3.3.21 LOGIN-FAILURE-PSWD, page 3-7 | NE | 5070 | securityInvalidLoginPasswordSeeAuditLog |
| 3.3.22 LOGIN-FAILURE-USERID, page 3-7 | NE | 3722 | securityInvalidLoginUsernameSeeAuditLog |
| 3.3.23 LOGOUT-IDLE-USER, page 3-7 | — | 5110 | automaticLogoutOfIdleUser |
| 3.3.24 MANWKSWBK-NO-TRFSW, page 3-8 | OCN | 5540 | manualSwitchBackToWorkingResultedInNoTrafficSwitch |
| 3.3.25 MANWKSWPR-NO-TRFSW, page 3-8 | OCN | 5530 | manualSwitchToProtectResultedInNoTrafficSwitch |
| 3.3.26 PARAM-MISM, page 3-8 | OTS, OMS, OCH, AOTS | 5840 | pluginModuleRangeSettingsMismatch |
| 3.3.27 PM-TCA, page 3-8 | — | 2120 | performanceMonitorThresholdCrossingAlert |
| 3.3.28 PS, page 3-8 | EQPT | 2130 | protectionSwitch |
| 3.3.29 PSWD-CHG-REQUIRED, page 3-8 | NE | 6280 | userPasswordChangeRequired |
| 3.3.30 RMON-ALARM, page 3-8 | — | 2720 | rmonThresholdCrossingAlarm |
| 3.3.31 RMON-RESET, page 3-9 | — | 2710 | rmonHistoriesAndAlarmsResetReboot |
| 3.3.32 SESSION-TIME-LIMIT, page 3-9 | NE | 6270 | sessionTimeLimitExpired |
| 3.3.33 SFTWDOWN-FAIL, page 3-9 | EQPT | 3480 | softwareDownloadFailed |
| 3.3.34 SPANLENGTH-OUT-OF-RANGE, page 3-9 | OTS | 6150 | spanLengthOutOfRange |
| 3.3.35 SWFTDOWNFAIL, page 3-9 | EQPT | 3480 | softwareDownloadFailed |

Table 3-1 ONS 15454 Transient Condition Alphabetical Index (continued)

| Transient Condition | Entity | SNMP Number | SNMP Trap |
|---|---|-------------|----------------------------|
| 3.3.36 USER-LOCKOUT, page 3-9 | NE | 5030 | userLockedOut |
| 3.3.37 USER-LOGIN, page 3-10 | NE | 5100 | loginOfUser |
| 3.3.38 USER-LOGOUT, page 3-10 | NE | 5120 | logoutOfUser |
| 3.3.39 WKSWBK, page 3-10 | EQPT, OCN | 2640 | switchedBackToWorking |
| 3.3.40 WKSWPR, page 3-10 | 2R, TRUNK, EQPT, ESCON, FC, GE, ISC, OCN, STSMON, VT-MON | 2650 | switchedToProtection |
| 3.3.41 WRMRESTART, page 3-10 | NE | 2660 | warmRestart |
| 3.3.42 WTR-SPAN, page 3-10 | — | 3420 | spanIsInWaitToRestoreState |

3.2 Trouble Notifications

The ONS 15454 system reports trouble by using standard condition characteristics that follow the rules in Telcordia GR-253 and graphical user interface (GUI) state indicators.

The ONS 15454 uses standard Telcordia categories to characterize levels of trouble. The system reports trouble notifications as alarms and reports status or descriptive notifications (if configured to do so) as conditions in the CTC Alarms window. Alarms typically signify a problem that you need to remedy, such as a loss of signal. Conditions do not necessarily require troubleshooting.

3.2.1 Condition Characteristics

Conditions include any problem detected on an ONS 15454 shelf. They can include standing or transient notifications. You can retrieve a snapshot of all currently raised conditions on the network, node, or card in the CTC Conditions window or by using the RTRV-COND commands in TL1.


Note

Some cleared conditions are found on the History tab.

For a comprehensive list of conditions, refer to the *Cisco ONS SONET TL1 Command Guide*.

3.2.2 Condition States

The History tab state (ST) column indicates the disposition of the condition, as follows:

- A raised (R) event is active.
- A cleared (C) event is no longer active.

- A transient (T) event is automatically raised and cleared in CTC during system changes such as user login, log out, and loss of connection to node view. Transient events do not require user action.

3.3 Transient Conditions

This section lists in alphabetical order all the transient conditions encountered in Software Release 6.0. The description, entity, SNMP number, and SNMP trap accompany each condition.

3.3.1 ADMIN-DISABLE

The ADMIN-DISABLE (Disable Inactive User) condition occurs when the administrator disables the user or the account is inactive for a specified period.

This transient condition does not result in a standing condition.

3.3.2 ADMIN-DISABLE-CLR

The ADMIN-DISABLE-CLR (Disable Inactive Clear) condition occurs when the administrator clears the disable flag on the user account.

This transient condition does not result in a standing condition.

3.3.3 ADMIN-LOCKOUT

The ADMIN-LOCKOUT (Admin Lockout of User) condition occurs when the administrator locks a user account.

This transient condition does not result in a standing condition.

3.3.4 ADMIN-LOCKOUT-CLR

The ADMIN-LOCKOUT-CLR (Admin Lockout Clear) condition occurs when the administrator unlocks a user account or the lockout time expires.

This transient condition does not result in a standing condition.

3.3.5 ADMIN-LOGOUT

The ADMIN-LOGOUT (Admin Logout of User) condition occurs when the administrator logs off a user session.

This transient condition does not result in a standing condition.

3.3.6 ADMIN-SUSPEND

The ADMIN-SUSPEND (Suspend User) condition occurs when the password for a user account expires.

This transient condition does not result in a standing condition.

3.3.7 ADMIN-SUSPEND-CLR

The ADMIN-SUSPEND-CLR (Suspend User Clear) condition occurs when the user or administrator changes the password.

This transient condition does not result in a standing condition.

3.3.8 AUTOWDMANS

The AUTOWDMANS (Automatic WDM ANS Finish) condition indicates that an automatic node setup command has been initiated. It normally occurs when you replace DWDM cards; the condition is an indication that the system has regulated the card.

This transient condition does not result in a standing condition.

3.3.9 BLSR-RESYNC

The BLSR-RESYNC (BLSR Multinode Table Update Completed) condition might occur when you create or delete circuits on a bidirectional line switched ring (BLSR), change a ring topology (for example, add or delete a BLSR node), or change the BLSR circuit state and ring ID.

This transient condition does not result in a standing condition.

3.3.10 DBBACKUP-FAIL

The DBBACKUP-FAIL (Database Backup Failed) condition occurs when the system fails to back up the database when the backup command is initiated.

This condition can occur when the server is not able to handle the backup operation due to network or server issues. Repeat the same operation again and check to see if it is successful. If the backup fails, it could be due to a network issue or software program failure. Contact TAC for assistance; see the [“Obtaining Documentation and Submitting a Service Request”](#) section on page 1 as needed.

3.3.11 DBRESTORE-FAIL

The DBRESTORE-FAIL (Database Restore Failed) condition occurs when the system fails to restore the backed up database when the restore command is initiated.

This condition can be due to server issues, network issues, or human error (pointing to a file that does not exist, wrong file name, etc.). Retrying the database restore with the correct file will usually succeed. If the network issue persists, you must contact network lab support. If the condition is caused by a network element (NE) failure, contact TAC for assistance. See the [“Obtaining Documentation and Submitting a Service Request”](#) section on page 1 as needed.

3.3.12 EXERCISING-RING

The EXERCISING-RING (Exercising Ring Successfully) condition occurs whenever you issue an Exercise-Ring command from CTC or TL1. This condition indicates that a command is being executed. You must issue another command to clear the exercise and the condition.

3.3.13 FIREWALL-DIS

The FIREWALL-DIS (Firewall Has Been Disabled) condition occurs when you provision the firewall to Disabled.

This transient condition does not result in a standing condition.

3.3.14 FRCDWKSWBK-NO-TRFSW

The FRCDWKSWBK-NO-TRFSW (Forced Switch Back to Working Resulted in No Traffic Switch) condition occurs when you perform a Force Switch to the working port/card and the working port/card is already active.

This transient condition might result in a Force Switch (Ring or Span) standing condition for a BLSR.

3.3.15 FRCDWKSWPR-NO-TRFSW

The FRCDWKSWPR-NO-TRFSW (Forced Switch to Protection Resulted in No Traffic Switch) condition occurs when you perform a Force Switch to the protect port/card, and the protect port/card is already active.

This transient condition does not result in a standing condition.

3.3.16 INTRUSION

The INTRUSION (Invalid Login Username) condition occurs when you attempt to log in with an invalid user ID.

This transient condition does not result in a standing condition.

3.3.17 INTRUSION-PSWD

The INTRUSION -PSWD (Security Intrusion Attempt Detected) condition occurs when you attempt to login with an invalid password.

This transient condition does not result in a standing condition.

3.3.18 IOSCFG-COPY-FAIL

The IOSCFG-COPY-FAIL (IOS Config Copy Failed) condition occurs on ML-Series Ethernet cards when the software fails to upload or download the Cisco IOS startup configuration file to or from an ML-Series card. This condition is similar to the “SFTWDOWN-FAIL” condition on page 3-9, but the IOSCFG-COPY-FAIL condition applies to ML-Series Ethernet cards rather than the TCC2/TCC2P card.

3.3.19 LOGIN-FAILURE-LOCKOUT

The LOGIN-FAILURE-LOCKOUT (Invalid Login–Locked Out) condition occurs when you attempt to log into a locked account.

This transient condition does not result in a standing condition.

3.3.20 LOGIN-FAILURE-ONALRDY

The LOGIN-FAILURE-ONALRDY (Security: Invalid Login–Already Logged On) condition occurs when you attempt to log in with an existing session and SUPN policy.

This transient condition does not result in a standing condition.

3.3.21 LOGIN-FAILURE-PSWD

The LOGIN-FAILURE-PSWD (Invalid Login–Password) condition occurs when you attempt to log in with an invalid password.

This transient condition does not result in a standing condition.

3.3.22 LOGIN-FAILURE-USERID

The LOGIN-FAILURE-USERID (Invalid Login–Username) condition occurs when a user login (CTC, CTM, or TL1) fails because the login username is not present on the node database. You must log in again with an existing user ID.

This transient condition is equivalent to a security warning. You must check the security log (audit log) for other security-related actions that have occurred.

3.3.23 LOGOUT-IDLE-USER

The LOGOUT-IDLE-USER (Automatic Logout of Idle User) condition occurs when a user session is idle for too long (the idle timeout expires) and the session terminates as a result. You must log in again to restart your session.

3.3.24 MANWKSWBK-NO-TRFSW

The MANWKSWBK-NO-TRFSW (Manual Switch Back To Working Resulted in No Traffic Switch) condition occurs when you perform a Manual switch to the working port/card and the working port/ card is already active.

This transient condition does not result in a standing condition.

3.3.25 MANWKSWPR-NO-TRFSW

The MANWKSWPR-NO-TRFSW (Manual Switch to Protect Resulted in No Traffic Switch) condition occurs when you perform a Manual switch to the protect port/card and the protect port/card is already active.

This transient condition results in a BLSR Manual Switch (Span or Ring) standing condition.

3.3.26 PARAM-MISM

The PARAM-MISM (Plug-in Module Range Settings Mismatch) condition occurs when the parameter range values stored on a small-form factor pluggable (SFP) device are different from the parameters stored in the TCC2/TCC2P database.

The transient condition is not user-serviceable. Refer to the [“Obtaining Documentation and Submitting a Service Request”](#) section on page 1.

3.3.27 PM-TCA

The PM-TCA (Performance Monitor Threshold Crossing Alert) condition occurs when network collisions cross the rising threshold for the first time.

3.3.28 PS

The PS (Protection Switch) condition occurs when the traffic switches from a working/active card to a protect/standby card.

3.3.29 PSWD-CHG-REQUIRED

The PSWD-CHG-REQUIRED (User Password Change Required) condition occurs when you are denied login for a shell function such as telnet or FTP because you did not change the login password. You can change the password through CTC or TL1.

3.3.30 RMON-ALARM

The RMON-ALARM (RMON Threshold Crossing Alarm) condition occurs when the remote monitoring variable crosses the threshold.

3.3.31 RMON-RESET

The RMON-RESET (RMON Histories and Alarms Reset Reboot) condition occurs when the time-of-day settings on the TCC2/TCC2P card are increased or decreased by more than five seconds. This invalidates all the history data and remote monitoring (RMON) must restart. It can also occur when you reset a card.

3.3.32 SESSION-TIME-LIMIT

The SESSION-TIME-LIMIT (Session Time Limit Expired) condition occurs when a login session exceeds the time limit and you are logged out of the session. You must login again.

3.3.33 SFTWDOWN-FAIL

The SFTWDOWN-FAIL (Software Download Failed) condition occurs when the system fails to download the required software.

An incorrect input that points to the wrong place or file, network issues, or a bad (corrupt) package can cause this failure. Retrying the operation with the correct name/location will usually succeed. If network issues persist, you must contact the network lab support. If the package is corrupt, contact Cisco TAC. See the [“Obtaining Documentation and Submitting a Service Request”](#) section on page 1 for details.

3.3.34 SPANLENGTH-OUT-OF-RANGE

The SPANLENGTH-OUT-OF-RANGE (Span Length Out of Range) condition occurs when the measured span loss does not fall within the limits of minimum and maximum expected span loss. It can also occur when the difference between MaxExpSpanLoss and MinExpSpanLoss is greater than 1dB.

When you perform a Calculate Span Loss operation on a DWDM node, the software measures the real span loss in the field by comparing the far-end POSC power and the near-end OSC power.

3.3.35 SWFTDOWNFAIL

The SFTWDOWN-FAIL (Software Download Failed) condition occurs when the system fails to download the required software.

An incorrect input that points to the wrong place or file, network issues, or a bad (corrupt) package can cause this failure. Retrying the operation with the correct name/location will usually succeed. If network issues persist, you must contact the network lab support. If the package is corrupt, contact Cisco TAC. See the [“Obtaining Documentation and Submitting a Service Request”](#) section on page 1 for details.

3.3.36 USER-LOCKOUT

The USER-LOCKOUT (User Locked Out) condition occurs when the system locks an account because of a failed login attempt. To proceed, the administrator must unlock the account or the lockout time must expire.

3.3.37 USER-LOGIN

The USER-LOGIN (Login of User) occurs when you begin a new session by verifying your User ID and password.

This transient condition does not result in a standing condition.

3.3.38 USER-LOGOUT

The USER-LOGOUT (Logout of User) condition occurs when you stop a login session by logging out of your account.

This transient condition does not result in a standing condition.

3.3.39 WKSWBK

The WKSWBK (Switched Back to Working) condition occurs when traffic switches back to the working port/card in a non-revertive protection group.

This transient condition does not result in a standing condition.

3.3.40 WKSWPR

The Switched to Protection (WKSWPR) condition occurs when traffic switches to the protect port/card in a non-revertive protection group. This transient condition does not result in a standing condition. The (WKSWPR) is raised as a standing condition in a revertive protection group.

The Switched to Protection (WKSWPR) condition also occurs after the protection switch in a 1+1 non-revertive protection group as a transient condition. When the protection group is changed to revertive, the (WKSWPR) is not raised as a standing condition or as a new transient condition. However, after a protection switch in a 1:1 protection group, the user will not be allowed to configure the protection group from non-revertive to revertive.

3.3.41 WRMRESTART

The WRMRESTART (Warm Restart) condition occurs when the node restarts while powered up. A restart can be caused by provisioning, such as database-restore and IP changes, or software defects. A WRMRESTART is normally accompanied by MANRESET or AUTORESET to indicate whether the reset was initiated manually (MAN) or automatically (AUTO).

This is the first condition that appears after a TCC2/TCC2P card is powered up. The condition changes to COLD-START if the TCC2/TCC2P card is restarted from a physical reseal or a power loss.

3.3.42 WTR-SPAN

The WTR-SPAN (Span is in Wait To Restore State) condition occurs when a BLSR switches to another span due to a Signal Failure-Span command or a fiber is pulled from a four-fiber BLSR configuration. The condition is raised until the WaitToRestore (WTR) period expires.

This transient condition clears when the BLSR returns to a normal condition or the IDLE state.

