

Transient Conditions

This chapter provides description for each commonly encountered transient condition.

- ADMIN-DISABLE, on page 2
- ADMIN-DISABLE-CLR, on page 2
- ADMIN-LOCKOUT, on page 2
- ADMIN-LOCKOUT-CLR, on page 2
- ADMIN-LOGOUT, on page 2
- ADMIN-SUSPEND , on page 2
- ADMIN-SUSPEND-CLR, on page 3
- AUD-ARCHIVE-FAIL, on page 3
- AUTOWDMANS , on page 3
- DBBACKUP-FAIL, on page 3
- DBRESTORE-FAIL, on page 3
- FIRMWARE-DOWNLOAD, on page 3
- FIRMWARE-UPG, on page 4
- FIRMWARE-UPG-COMPLETE, on page 4
- FIRMWARE-UPG-FAIL, on page 4
- LOGIN-FAIL-LOCKOUT, on page 4
- LOGIN-FAIL-ONALRDY, on page 4
- LOGIN-FAILURE-PSWD, on page 4
- LOGIN-FAILURE-USERID, on page 5
- LOGOUT-IDLE-USER, on page 5
- MASTERKEY-SUCCESS, on page 5
- PM-TCA, on page 5
- PSWD-CHG-REQUIRED, on page 5
- RMON-ALARM, on page 5
- RMON-RESET , on page 5
- SESSION-TIME-LIMIT, on page 6
- USER-LOCKOUT, on page 6
- USER-LOGIN, on page 6
- USER-LOGOUT, on page 6
- WRMRESTART , on page 6
- WKSWBK, on page 6

ADMIN-DISABLE

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

This transient condition does not result in a standing condition.

ADMIN-DISABLE-CLR

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

This transient condition does not result in a standing condition.

ADMIN-LOCKOUT

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

This transient condition does not result in a standing condition.

ADMIN-LOCKOUT-CLR

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

This transient condition does not result in a standing condition.

ADMIN-LOGOUT

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

This transient condition does not result in a standing condition.

ADMIN-SUSPEND

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

This transient condition does not result in a standing condition.

ADMIN-SUSPEND-CLR

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

This transient condition does not result in a standing condition.

AUD-ARCHIVE-FAIL

The Archive of Audit Log Failed (AUD-ARCHIVE-FAIL) condition occurs when the software fails to archive the audit log. The condition normally occurs when the user refers to an FTP server that does not exist, or uses an invalid login while trying to archive. The user must log in again with correct user name, password, and FTP server details.

This transient condition does not lead to a standing condition.

AUTOWDMANS

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

This transient condition does not result in a standing condition.

DBBACKUP-FAIL

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

This condition can occur due to network or server issues. Repeat the operation and check if it succeeds. If it fails again, contact the Cisco Technical Assistance Center (TAC) (1 800 553-2447).

DBRESTORE-FAIL

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

This condition can be due to server or network issues. If the condition is caused by a network element (NE) failure, contact the Cisco Technical Assistance Center (TAC) (1 800 553-2447) for assistance.

FIRMWARE-DOWNLOAD

The Firmware Download (FIRMWARE-DOWNLOAD) condition occurs when the firmware is being downloaded during the firmware upgrade. The firmware upgrade initiates when the download is complete.

This transient condition does not result in a standing condition.

FIRMWARE-UPG

The Firmware Upgrade (FIRMWARE-UPG) condition occurs when the firmware is being upgraded. This condition reflects the upgrade status.

This transient condition does not result in a standing condition.

FIRMWARE-UPG-COMPLETE

The Firmware Upgrade Complete (FIRMWARE-UPG-COMPLETE) condition occurs when the firmware upgrade is successfully completed.

This transient condition does not result in a standing condition.

FIRMWARE-UPG-FAIL

The Firmware Upgrade Fail (FIRMWARE-UPG-FAIL) condition occurs when the firmware upgrade fails. The user must start the firmware upgrade again.

This transient condition does not result in a standing condition.

LOGIN-FAIL-LOCKOUT

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

This transient condition does not result in a standing condition.

LOGIN-FAIL-ONALRDY

The Invalid Login Already Logged On (LOGIN-FAIL-ONALRDY) condition occurs when a user attempts to log in to a node where the user already has an existing session and a Single-User-Per-Node (SUPN) policy exists.

This transient condition does not result in a standing condition.

LOGIN-FAILURE-PSWD

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

This transient condition does not result in a standing condition.

LOGIN-FAILURE-USERID

The Invalid Login Username (LOGIN-FAILURE-USERID) condition occurs when you attempt to log in (SVO web interface) with an invalid username. To log in, use a valid username.

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.

LOGOUT-IDLE-USER

The Automatic Logout of Idle User (LOGOUT-IDLE-USER) condition occurs when a user session remains inactive for a certain period of time. When the idle timeout expires, the user session ends and requires the user to log in again.

MASTERKEY-SUCCESS

The Master Key Exchange Success condition occurs when the primary key is successfully reset and the Threshold Crossing Alert (TCA) has provisioned.

This transient condition does not result in a standing condition.

PM-TCA

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

PSWD-CHG-REQUIRED

The Password Change Required condition occurs when the user password needs to be changed.

This transient condition does not result in a standing condition.

RMON-ALARM

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

RMON-RESET

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

SESSION-TIME-LIMIT

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

USER-LOCKOUT

The User Locked Out (USER-LOCKOUT) condition occurs when an account is locked due to failed login attempts. The account can be unlocked by an administrator or when the lockout time expires.

USER-LOGIN

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

This transient condition does not result in a standing condition.

USER-LOGOUT

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

This transient condition does not result in a standing condition.

WRMRESTART

The Warm Restart (WRMRESTART) condition occurs when the node restarts while it is powered up. A restart can be caused by provisioning, such as a database restore or IP changes, or by 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 control card is powered up. The condition changes to COLD-START if the control card is restarted from a physical reseat or a power loss.

WKSWBK

Default Severity: Warning

Logical Object: Transient

Resource Type: OPT ODUk

The WKSWBK alarm is raised when the protection switch returns the traffic to the nominal working resource.

Clear the WKSWBK Alarm

Procedure

The alarm never clears as it is a transient condition.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/cisco/web/support/index.html for more information or call Cisco TAC (1 800 553-2447).