CHAPTER 2

Fault Detection and Isolation

This chapter describes unreachable network elements and the sources of alarms on devices. In addition, it describes alarm integrity and the integrity service:

- Unreachable Network Elements—Describes how the various VNEs use reachability to check connectivity with the NEs.
- Sources of Alarms On a Device—Describes the four basic alarm sources that indicate problems in the network.
- Alarm Integrity—Describes what happens when a VNE with associated open alarms shuts down.
- Integrity Service—Describes the integrity service tests that run on the gateway and/or the units.

Unreachable Network Elements

Reachability used by the VNEs (checks the reachability between the VNEs and NEs) depends on the configuration of the VNE, and involves multiple connectivity tests, using SNMP, Telnet/SSH and/or ICMP, as appropriate.

The table describes the various situations below when a NE fails to respond to the protocols:

Table 2-1 Unreachable Network Elements

VNE Type	Checks reachability using	When the NE fails to respond	When the NE is reachable
ICMP VNE	ICMP only. During the ICMP test the unit pings the NE every configured interval.	ICMP ping is suspended, and a *VNE Unreachable* alarm is sent to the Cisco ANA Gateway. Only the reachability tests are executed thereafter to detect when the device is reachable again.	ICMP ping is restarted, and the alarm is cleared.

Table 2-1 Unreachable Network Elements (continued)

VNE Type	Checks reachability using	When the NE fails to respond	When the NE is reachable
Generic VNE	• SNMP only (default). During the SNMP test the unit's "`SNMP get`" the sysoid of the NE and expects to receive a response or • SNMP only (default), and adding an ICMP test.	General polling is suspended, and a *VNE Unreachable* alarm is sent to the Cisco ANA Gateway. Only the reachability tests are executed thereafter to detect when the device is reachable again. If more than one protocol is used, it is enough for one of them to become unreachable in order to generate the alarm. The alarm is generic to all the protocols.	• General polling is restarted. • The first time the VNE is started, all the commands are submitted to the queue, and the collector initiates an immediate session with the NE. The commands are sent to the NE in a serial fashion. • The alarm is cleared.
Full VNE	• SNMP only (default). During the SNMP reachability test, the VNE polls the device's SysOID MIB using a standard "`SNMP Get`" command, and expects to receive a response or • SNMP only (default), and adding ICMP and Telnet. During the Telnet test the unit sends "`Enter`" via the open session and expects to get a prompt back.	General polling is suspended, and a *VNE Unreachable* alarm is sent to the Cisco ANA Gateway. Only the reachability tests are executed thereafter to detect when the device is reachable again. If more than one protocol is used, it is enough for one of them to become unreachable in order to generate the alarm. The alarm is generic to all the protocols.	• The first time the VNE is started, all the commands are submitted to the queue and the collector initiates an immediate session with the NE. The commands are sent to the NE in a serial fashion. • The alarm is cleared.

Each of these scenarios have two possible settings in the registry, namely:

- track reachability (true/false). The default is true.

  When this parameter is true reachabilty is tracked according to the specific protocol, for example, ICMP, SNMP, Telnet, and so on.

  When this parameter is false then the test is not performed.

- lazy reachability (true/false). The default is false. This parameters determines whether there is a dedicated reachability command 'in-charge' of tracking reachability or whether reachability is determined by the regular polled commands.

  When this parameter is true reachability is based on polling, and a dedicated command not activated.

  When this parameter is false a dedicated SNMP command is activated, and this test verifies the response from a specific SNMP oid (sysoid is the default that can be changed).

Note Changes to the registry should only be carried out with the support of Cisco Professional Services.

Sources of Alarms On a Device

The following basic sources of alarms exist in the system which indicate a problem in the network:

- Service Alarms—Alarms generated by the VNE as a result of polling (for example SNMP, Telnet). Usually such alarms (for example link down, card out, device unreachable and so on) are configured in such a way that they can become root cause alarms, according to the correlation algorithms. Service alarms can also be generated by the gateway, for example. the vpn leak alarm.
- SNMP Traps—Traps sent by the network elements and captured by the Cisco ANA platform. The platform supports SNMP v1, v2 and v3 traps. The traps are then forwarded to the specific VNEs for further processing and correlation logic. In addition, reliable traps (inform commands) are supported, when configured in the registry, where the VNE acknowledges that a trap was received.
- Syslogs—Syslog messages sent by the network elements and captured by the Cisco ANA platform. The Syslogs are then forwarded to the specific VNEs for further processing and correlation logic.
- TCA—Cisco ANA can be used to set a TCA for soft properties. The TCA can be enabled to assign a condition to the property which will trigger an alarm when violated. The alarm conditions could be:
  - Equal or not equal to a target value.
  - Exceeding a defined value range (defined by maximum and minimum thresholds, including hysteresis), for example CPU level of a device.
  - Exceeding a defined rate (calculated across time), for example bandwidth or utilization rate of a link.
- System Alarms—Alarms generated by the gateway and/or the units, for example, disk full, database full, unit unreachable and so on. For more information see Integrity Service.

For information about TCAs see the Cisco Active Network Abstraction Customization User Guide.

Alarm Integrity

When the VNE shuts down while it still has open alarms associated with it, “fixing” events which occur during the down period will be consolidated when the VNE is reloaded.

Integrity Service

The integrity service is an internal service that runs on the gateway and/or the units, which is responsible for the stability of the system by running integrity tests in order to maintain the database and eliminate clutter in the system. In order to prevent the session from stopping, the integrity service tests are run on a different thread in a separate directory called *integrity*.

The service integrity tests are run:

- Manually—The integrity service tests are accessed as part of the Cisco ANA Shell management services, and they can be accessed by telneting the gateway.

  To run a test, the user should cd to the integrity dir, and then enter `executeTest` followed by the test name. The user can pass parameters to the tests using Cisco ANA Shell.
- Automatically—The integrity service tests are scheduled as crontab commands, to run specific tests at specific intervals. By default the integrity service tests run automatically every 12 hours.

For example, this line in crontab runs the file every_12_hours.cmd at 11:00AM and 11:00PM:

```
0 11,23 * * * local/cron/every_12_hours.cmd > /dev/null 2>&1
```

The integrity service tests can be defined inside the cmd file, for example:

```
echo "`date '+%d/%m/%y %H:%M:%S -'` running integrity.executeTest alarm"
cd ~/Main ; ./mc.csh localhost 8011 integrity.executeTest alarm >& /dev/null
```

The first line prompts the user when a test starts to run, the next line runs the test.

The integrity service test parameters are defined in the registry. The registry entries responsible for the integrity service can be found at:

```
mmvm/agents/integrity
```

Note Changes to the registry should only be carried out with the support of Cisco Professional Services.

The integrity service tests include, for example, the following:

- Alarm—Deletes *cleared* alarms if the alarm count is above the defined threshold.
- businessObject—Checks for invalid OIDs in business objects.
- Capacity—Checks the disk space capacity.
- archiveLogs—Deletes Oracle logs.
- tablespace—Checks that there is enough disk space for tablespace growth.
- workflowEngine—Deletes all complete workflows that started before a configured period of time.