



Release Notes for Cisco Active Network Abstraction, 3.5.1

13 November 2006

These release notes support the release of Cisco Active Network Abstraction 3.5.1.



Note

See Cisco.com for the most up to date version of the Release Notes for Cisco Active Network Abstraction, 3.5.1.

Contents

This document includes the following topics:

- [Introduction](#)
- [Installation Notes](#)
- [Limitations and Restrictions](#)
- [Important Notes](#)
- [Open Caveats - Release Cisco ANA 3.5.1](#)
- [Resolved Caveats - Release Cisco ANA 3.5](#)
- [Open Caveats - Release Cisco ANA 3.5](#)
- [Documentation Updates](#)
- [Related Documentation](#)
- [Obtaining Documentation](#)
- [Documentation Feedback](#)
- [Cisco Product Security Overview](#)
- [Product Alerts and Field Notices](#)
- [Obtaining Technical Assistance](#)
- [Obtaining Additional Publications and Information](#)



Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 1999 - 2006 Cisco Systems, Inc. All rights reserved.

Introduction

These Release Notes support the release of Cisco Active Network Abstraction, 3.5.1 (Cisco ANA 3.5.1).

Cisco ANA 3.5.1 is a carrier-class, multi-vendor network and service management platform providing the flexibility for carriers and service providers to efficiently respond to the constant market demand for new, reliable and more sophisticated services.

Cisco ANA 3.5.1 understands network characteristics and builds a real-time virtual model of the network, serving as a live information base for value-added tools and applications capable of seamless integration within a customer's existing OSS environment.

Cisco ANA 3.5.1 provides a unified solution for diverse network environments and applications. Implemented with a highly-scalable distributed architecture, Cisco ANA 3.5.1 offers integrated configurable device management, network and service discovery, network and service fault isolation and a highly flexible service activation engine. These integrated applications enable correlated management of global scale networks supporting millions of subscribers and customers.

Cisco ANA 3.5.1 is a unified, fully-integrated solution offering:

- Multi-vendor device support
- Multi-Technology coverage: IP, L2/L3 VPN, xDSL, ATM, FR, GigE, Ethernet, 802.1Q, ISL, PPP and routing protocols (e.g. OSPF, BGP)
- Integrated device, network and service management functionality
- Open interfaces for integration with multiple OSS/BSS applications

Cisco ANA 3.5.1 dynamically discovers and identifies basic network components, while obtaining end-to-end visibility of the network resources, connections and dependencies, enabling Cisco ANA 3.5.1 to manage and analyze network behavior. Cisco ANA 3.5.1 builds its end-to-end understanding of the network structure and interoperability, across vendors, technologies and network layers, into a customer-specific virtual network model for each and every installation.

The virtual network model within Cisco ANA 3.5.1 is an always maintained up-to-date enabling powerful device, network and service management functionality, including:

- Configurable Device Manager: Basic FCAPS features for multi-vendor devices
- Network and Service Discovery: Physical and logical discovery with multi-layer network & service connectivity
- Network and Service Fault Isolation: End-to-end, topology-based fault isolation, monitoring & root cause analysis
- Service Activation
- And a series of product options including Northbound APIs, Path Tracing and Client UIs

Installation Notes

Refer to the Cisco Active Network Abstraction Server's Installation Guide, 3.5.1 and the Cisco Active Network Abstraction Client Installation Guide, 3.5.1.

Limitations and Restrictions

Cisco ANA NetworkVision

Cisco ANA NetworkVision with a configuration 512MB of free-non virtual memory per running instance, supports across all of the maps that are open, a maximum of 10K objects (devices, VPNs, VRFs and sites) 12K links and 10K tickets (if the same tickets are displayed in different maps, each instance will be counted separately).

One map in Cisco ANA NetworkVision, supports a maximum of 5K objects, 6K links and 5K tickets.

The maximum number of maps that can be opened for Cisco ANA NetworkVision is five (default), regardless of the number of devices, links and tickets, but this number is configurable assuming that the overall number of links and devices per application do not exceed the maximum limits. For information about customizing the maximum number of maps, contact Cisco Professional Services.

Cisco ANA Fault Management

The maximum number of open tickets (other tickets can be correlated to them) for the system is 5K. For a definition of an open ticket, refer to the Cisco ANA Fault Management Guide, 3.5.1. The operator should ensure that tickets are closed on time.

Cisco ANA Workflow Editor

The following restriction applies to the names of Workflow templates.

The user should not include the "_" and "%" characters (wildcard characters) in Workflow template names when executing a workflow or referencing a subflow as this can lead to ambiguity. The execution will fail and the following message will be displayed in the AVM66 log:

```
"WARN [13 21:00:08,248] - dralasoft.workflow - Task aborted. Task: 245886, Workflow:
245885 java.lang.IllegalArgumentException: Template AA_BB.template is ambiguous, templates
ids are: 245874 , 245873"
```

"_" denotes any single character

"%" denotes a zero or many characters

The following examples depict workflow template names that can lead to ambiguity if they are deployed together:

In this example the WFTLM_MUESTRA.template leads to ambiguity with the WFTLM#MUESTRA.template when they are deployed together.

In this example the WFTLM%MUESTRA.template leads to ambiguity with the WFTLM###MUESTRA.template when they are deployed together.

The ambiguity only occurs if the template containing the wild characters is executed.

HSRP

Note in order for correlation to work, the path through which the HSRP signaling passes must be modeled (exist) in the system.

Important Notes

The following table lists the Solaris services and components that are being used by the Cisco ANA system and must not be removed:

Table 1 *Solaris Services and Components used by Cisco ANA*

Name	Description of function	Configuration information	TCP and UDP port numbers	Traffic classification
Xntpd	Time server	/etc/inet/ntp.conf	123	ntp
/bin/tcsh	Unix shell	None	None	None
/usr/bin/tcsh	Unix shell	None	None	None
Perl	Scripting language	None	None	None
/bin/sh	Unix shell	None	None	None
Rsh/rexec	Remote shell	None	512,513,514	None

The following table lists the product services that are installed with the Cisco ANA system:

Table 2 *Product Services Installed with Cisco ANA*

Name	Description of function	Configuration information	TCP and UDP port numbers	Dynamic TCP and UDP port ranges	Inter-dependencies with other features, applications and services	Traffic classification
Avm[1-999]	Main app	Main/registry/Avm[NUM].xml		2000-3000, 8000-9000	Java,Perl,Tcsh	Inner protocol
Udp2icmp	Icmp redirector	-	10001	-	Perl	-
redirectUdp	Udp redirector	-	162,1162,514, 1514	-	Perl	-
Sheer_secured	Secured connectivity between gateway and unit	local/sheer_secured /sheer_config	1101	-	-	ssh
webserver	Serves the client webstart and the system troubleshooting tools.	utils/apache/conf/ sheer.conf	1310	-	-	http
Machine interface	BQL machine to machine interface	-	9002	-	Java	-

Table 2 *Product Services Installed with Cisco ANA*

Name	Description of function	Configuration information	TCP and UDP port numbers	Dynamic TCP and UDP port ranges	Inter-dependencies with other features, applications and services	Traffic classification
secure machine interface	Secured BQL machine to machine interface	-	9003	-	Java	-
transport switch	Gateway/Unit internal message bus	-	9290	-	Java	-
Client Transport	Client/Gateway message bus	-	9771	-	Java	-
Syslog redirector	Redirects syslog messages	-	1162	-	-	-
Traps redirector	Redirects trap events	-	1512	-	-	Snmp

Online Help

Note that the online help for Cisco ANA 3.5.1 has been tested using the following browsers:

- Microsoft Internet Explorer version 6
- Firefox version 2.0
- Avant Browser version 11 build 25

Open Caveats - Release Cisco ANA 3.5.1

Table 3 *Open Caveats - Release Cisco ANA 3.5.1*

Identifier	Title	Impact	Workaround
CSCsd12788	Path tool doesn't open when the path should pass through IMA topology	The Cisco ANA PathTracer does not open when the path goes through IMA	None.
CSCsd27001	Asam 1000 new alarms Persistency don't work	When an alarm occurs in the ASAM VNE and the VNE goes down (for any reason), if the alarm is fixed during the down time, then when the VNE goes up again the alarm is not cleared.	Clear the alarm manually.
CSCsd34847	Missing link between the ASAM <-> CBX	There is no link between ASAM version 4.2.1.0 and CBX 500 version 04.02.01.00	Create static links manually.

Table 3 Open Caveats - Release Cisco ANA 3.5.1

Identifier	Title	Impact	Workaround
CSCsd59865	VRF isn't displayed in a map as deleted although it was deleted	The VRF is displayed on the VPN map and it appears as though everything is OK, but the VRF has already been deleted.	Open and close the client.
CSCsd61127	Able to add a VNE in UP state to an AVN that is down	A VNE is transferred from an Up state to a down state unintentionally.	Pay attention to the move action before moving a VNE.
CSCsd84445	Overlay does not work with aggregations - aggregations color issue	The overlay does not work well in a case where the map contains aggregations. The aggregation's color is not in sync with its relevancy to the overlay: if it is closed, it is always grayed out, and if it is opened as a thumbnail it is always colored, even if none of the devices that it contains are relevant to the overlay.	None.
CSCsd84449	Overlay and link properties-missing selection sensitive menu	The map contains an aggregation of a device and an overlay is run that is relevant to the device. Select show aggregation as thumbnail, and right-click on the links of the device, that are relevant to the overlay. No context sensitive menu (no popup) is displayed.	None.
CSCse66308	Cannot load VNE against Cisco 10K with 15,000 Ip int.	When loading a Cisco router 10K device with a lot of sessions (~15000) the AVM may crash due to out of memory.	Decrease the polling interval for the encapsulations command and increase the amount of memory available for the AVM
CSCse70636	System installation is not verifying that server swap size is at least 2xMemory size	If the SWAP size is insufficient the Unit or Gateway may fail to load.	Make sure that the UNIX machine has at least two times the swap area of the physical memory of the machine.
CSCse78912	AVM 100 does not start on gateway.	No traps will be received by this trap manager instance.	This issue is caused by an Oracle ftp service that uses port 2100, to which AVM 100 is supposed to bind. This service should not be installed on the Unit or Gateway. If this service is installed remove it.

Table 3 *Open Caveats - Release Cisco ANA 3.5.1*

Identifier	Title	Impact	Workaround
CSCse82338	Physical Inventory is missing	For some network elements there is no physical inventory. This may occur with network elements that do not respond well to SNMP or Telnet requests.	Stopping and restarting the affected VNEs solves this issue.
CSCse85009	Cisco ANA Gateway receive no response for UtStarcom VNE	No physical or logical components are visible when loading a UTStarcom VNE on the IP/VPN scheme.	Load this VNE with the ATM/DSL scheme.
CSCse97220	Drop messages in avm 100	After loading AVM 100 many messages from the VNEs were dropped (Trap/Syslogs manager)	This is normal behavior on large scale setups, and the situation will be resolved and the traps/syslogs will arrive normally after the system has stabilized. The time that it takes the system to stabilize depends on the size of the setup. For 15000 VNEs it will take approximately 20 minutes.
CSCsf02136	Allocated memory calculation is wrong	Over allocation of the memory can be made to the unit causing the unit to work slower than intended.	When calculating the memory add 50MB for each AVM that is created (including AVM0, AVM66 and AVM99). The operating system memory is not accounted for (included) either.
CSCsf05415	Can't delete multiple WorkFlow rows	Multiple workflow rows in Cisco ANA Manage cannot be deleted.	Delete the workflow rows one by one.
CSCsf13264	Publishing fails in high scale	Problem with publishing the command to the highest hierarchies in setup, which includes many devices in real-time.	One of the following: <ul style="list-style-type: none"> • Publish to lower hierarchies. • Publish during maintenance window when all units are down.
CSCsf31904	Information in Business tab is missing	When the Cisco ANA PathTracer is opened, Layer1, Layer2 and Layer3 tabs display the correct information but the Business tab is empty.	None.
CSCsg08522	General Error Dialog when removing tickets twice	A general error dialog box is displayed when the user attempts to manipulate (clear, remove, or clear and remove) tickets that are already in the process of being removed (as this action may take a few minutes).	Close the general error dialog box. The tickets are manipulated as initially requested. The user should wait for this to happen.

Table 3 Open Caveats - Release Cisco ANA 3.5.1

Identifier	Title	Impact	Workaround
CSCsg26028	Unusable gateway when there is a duplicate entry/key in alarm-types.xml	Gateway is unusable if the alarm-types.xml file is corrupted.	Make sure that file is not corrupted and that its related site.xml entry is also correct and not corrupted.
CSCsg26227	Deadlock in Workflow Editor	The workflow editor hangs sometimes when executing a workflow.	Restart the workflow.
CSCsg28927	Problem with load topology persistency on VNE connected to the Cloud	After restarting the Cloud VNE, which was connected to an adjacent VNE, some cloud ports may be connected to the incorrect VNE ports.	<ol style="list-style-type: none"> 1. Disable topology persistency for the VNE which should connect to the cloud. Open the Registry Editor. Connect to the golden source. Open <code><AVM ID>/agents/da/<VNE ID>/amsi/topology/common</code>, and define the "persistency" entry as "false". 2. Disable the topology persistency for the Cloud VNE in the same way as you did for the VNE. 3. Remove the topology persistency folder. Go to the <code>Main/topology</code> directory and remove the folders for the IP Addresses of the appropriate VNEs and Cloud VNE. 4. Restart the VNE and Cloud VNE.
CSCsg29273	Acknowledge Alarm message in the history tab should be formatted.	An unformatted event is displayed in the history tab.	None.
CSCsg36976	Modeling of sub-sub-module in GSR	Modular cards on GSR devices are not modeled.	None, this is a limitation in this version.
CSCsg39235	A workflow fails if there is no output	In a special case when the workflow does not have an output it fails. A workflow that does not have an output does not interact with the Gateway and does not print to its output stream.	None.
CSCsg45530	Workflow editor fails to run BQL tasks - GUI Issue	Cannot execute the BQL task in the Cisco ANA Workflow Editor	<p>Deploy the workflow in Cisco ANA Manage.</p> <p>Run the workflow template.</p>
CSCsg45747	ICMP VNE can't be used - GUI issue	Cannot use the ICMP agent in Cisco ANA NetworkVision	<p>None for ICMP.</p> <p>If you want to ping the VNE use BQL with a ping command.</p>

Table 3 Open Caveats - Release Cisco ANA 3.5.1

Identifier	Title	Impact	Workaround
CSCsg48454	VC Removed is not scale	Not supported in this version.	None.
CSCsg48456	Events are dropped when doing high scale alarm manipulation	Events are dropped when doing high scale alarm manipulations.	Avoid performing alarm manipulation actions in high scale. Check Cisco ANA EventVision for reports of the dropped events.

Resolved Caveats - Release Cisco ANA 3.5

The table below lists the open caveats from Cisco ANA 3.5 that have now been resolved.

Table 4 Resolved Caveats - Release Cisco ANA 3.5

Identifier	Summary	Explanation
CSCsc72986	No HSRP group modelled	Fixed.
CSCsc94544	The cloud VNE isn't supported in the default scheme	Fixed.
CSCsd15988	Physical links not discover between Ethernet Cloud to others VNEs	Fixed.
CSCsd30408	CDP Topology: Link not disconnecting when CDP is disabled	Fixed.
CSCsd34516	Affected Parties do not change their severity status to Real/Recovered	Fixed.
CSCsd36144	Frame Relay cross connect is missing in Cloud VNE	Fixed.
CSCsd46264	No GRE tunnel modelled	Fixed.
CSCsd66920	Client memory problem	No workaround is needed. The memory is automatically freed when another map is opened.
CSCsd74121	C not run bean shell script in Command Builder	Apply patch name "CSCsd74121_patch.jar" to system after installation. The patch must be installed by Professional Services.
CSCsd74144	An ISDN backup interface goes up but no alarm appears in the system.	An alarm is now generated in this case.
CSCsd75036	Memory/CPU problem when opening few service paths.	Do not open multiple service paths on the same client simultaneously.
CSCsd77828	No alarm is created in the ASAM VNE when a card is pulled out.	The problem was not reproducible in the lab. When pulling out a card on this device an alarm was received.
CSCsd78156	Adding VC cross connect causes exceptions - Unreproducible	A translator that was omitted from a merge activity was added.
CSCsd78530	ASAM v5: ADSL port status is missing	This bug was junked because it was reported on the wrong scheme file.
CSCsd78874	Potential affected does not change state to recovered in a link down scenario.	Fixed.

Table 4 Resolved Caveats - Release Cisco ANA 3.5

Identifier	Summary	Explanation
CSCsd78894	BGP Affected functionality is not working correctly.	Fixed.
CSCsd79340	Scalability issue with command creation in Command Builder	This must be done by Cisco Professional Services. To workaround this performance issue there is a need to break the site.xml file into several files. to do so just copy a section inside site.xml into a new xml file and add a "default" entry pointer to the new xml file where the section was previously inside site.xml.
CSCsd79361	CDP: Physical topology not discovered for POS & Serial links.	Fixed.
CSCsd80788	Restore script does not work with an external database	<p>This is a workaround for the restore problem:</p> <ul style="list-style-type: none"> • Login to the system as user sheer • Create a directory named /tmp/db_back • Copy the backup content into /tmp/db_back • Change the directory permission by running the following command: <code>chmod -R 775 /tmp/db_back</code> • Change dir to <code>\$(SHEERHOME)/Main/scripts/misc/backup</code> • In the following command, switch the red painted oradata part with the oracle directory which holds the database data (as entered on sheer-conf.pl while configuring the product for the first time) and type it: <pre>cat orarestore.sh sed s"/data/MCDB"/"/oradata/MCDB"/g > /tmp/restore.sh</pre> • Change the permission of /tmp/restore.sh by typing : <code>chmod 777 /tmp/restore.sh</code> • Switch to user oracle • Type the following command: <code>/tmp/restore.sh /tmp/db_back</code> • For security purposes, erase dir /tmp/db_back
CSCsw12683	Frame-Relay Cloud: Static topology doesn't work.	Fixed.
CSCsw13304	Ethernet Cloud does not support switchport trunk and access properly.	Fixed.

Open Caveats - Release Cisco ANA 3.5

Table 5 Open Caveats - Release Cisco ANA 3.5

Identifier	Title	Impact	Workaround
CSCsd61046	Limited support of L2TP.	L2TP information will include only basic L2TP information. No support of alarms, LAC/LNS distinguishing and path tool available for L2TP.	None.
CSCsd63693	IMA is not supported.	IMA agregations are not discovered.	None.
CSCsw09406	Link connect/disconnect between CE and PE which are directly connected.	When two devices are configured one as CE and one as a PE in a MPLS network and are connected directly (no switches between them), the link in the VNES will connect and disconnect periodically. The reflection of this problem is the link blinking on and off in the GUI.	Create a static link between the PE and CE.
CSCsw12670	Creating static link between Clouds to VNE reports failure.	When running the BQL command for creating static link between cloud VNE and a VNE, the command reports failure even if it succeeded.	None. Creating a static link between the Cloud and the VNE succeeds but a failure is erroneously reported. This error can be ignored. The link can be seen in Cisco ANA NetworkVision.

Documentation Updates

This section of the Release Notes includes updates to the Cisco Active Network Abstraction 3.5.1 documentation set.

Cisco ANA Administrator's Guide, 3.5.1

The option to search for a ANA Unit according to specifically defined search criteria is no longer available.

The option to search for an AVM/VNE is still available. When searching for an AVM the following search criteria are displayed:

- ID
- Status
- Key
- Loaded patches

When searching for a VNE the following search criteria are displayed:

- Key
- IP address
- Status
- Element type
- Maintenance
- Polling group

System Configuration

Two new parameters were added to the system configuration. These parameters control the behavior of the polling of the sysoid command and the software version command.

Previously when the VNE could not poll the sysoid or the software version, it did not attempt to retry to poll the sysoid or the software version, and the status became "Device Unsupported" or "Initializing".

Now two separate parameters have been added for the sysoid command and the software version command in order to add the option to attempt to retry to poll this information. The following two parameters were added:

- interval—This parameter states the time in milliseconds required to wait before each poll. The default value is 30000 (30 seconds).
- retries—This parameter states how many retries are required to be performed before discontinuing the poll. The default is -1 which means that the retry is unlimited (always). If a positive value is defined, for example, 10 then this is the number of retries that will occur before the VNE discontinues retrying.



Note

There is an option to override the default settings, if the customer so requires. Changing these settings must be done with the support of Cisco Professional Services.

VNE Persistency Mechanism in Cisco ANA

This section describes the VNE Persistency mechanism in Cisco ANA.

[Introducing Persistency](#)

[Alarm Persistency](#)

[Configuring Alarm Persistency](#)

[Instrumentation Persistency](#)

[Configuring Instrumentation Persistency](#)

[Topology Persistency](#)

[Configuring Topology Persistency](#)



Note

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

Introducing Persistency

This section includes a description of:

- Alarm persistency
- Instrumentation persistency
- Topology persistency

Persistency is the ability to store information in the Unit for later use. This information persists (is stored) across Unit/AVM/VNE restarts.

Instrumentation persistency is used mainly to:

- Shorten the starting time of VNEs for devices (using the information from the local file system, the device's response time and network latency is eliminated, thus the VNE finishes modeling its first state very quickly).
- Provide information about the old state of the VNE in order to initiate alarms if the status has changed (if the VNE was unloaded for any reason). For example, a port-down alarm is initiated only if the port status was "up" and was changed to "down" to make sure that an alarm is not issued on ports which should be "down". By maintaining information about the old state of the port, the system understands whether the current state is valid or not.
- Help lower the CPU load on the device when starting and there are lots of get commands that are generated. In addition, when persistence data is loaded from the Unit the traffic bandwidth between the Unit and device is much lower than when the system is loaded ordinarily (using "ordinary" device discovery/modulation).

Topology persistency is used mainly to:

- Create topology between devices on startup when the VNE is loaded, instead of performing the entire discovery process. Afterwards verification of the links is performed.

Alarm persistency is used mainly to:

- Save information about the VNE components that send alarms, namely, when a VNE sends an alarm it can be configured to save this information (that it has sent an alarm of type X). This information can then be used by the VNE components after restarts to verify whether it needs to send clearing alarms in a case where changes have occurred in the device when the VNE was down.

How is VNE data persisted:

- During runtime when a VNE polls data from a device, it updates the files in the file system for changes in the device's response (according to the persistency variables)
- The reading from these files is done only once, when the VNE starts. Every polling that takes place (normal or due to refresh) after this first time, will read the data from the device itself and not from the files.

Alarm Persistency

Alarm persistency enables the system to clear alarms which relate to events which have occurred while the system was down. For example, a "link down" alarm is generated and then the system goes down. While the system is down a "link up" event occurs in the network, but the system is down and does not monitor the network. When the system goes up, the alarm will be cleared because the system "remembers" that a "link down" alarm exists and needs to be cleared by sending a corresponding alarm.

Persisting events are held in the AlarmPersistencyManager. Each VNE contains an AlarmPersistencyManager object. Alarms are added and removed from the AlarmPersistencyManager object, in order to maintain the status of an event (whether existing in the repository or not), namely, whether an “up” alarm has been generated, or whether a “clearing” alarm has been generated. Two copies of alarm persistency information are maintained, one in the memory and the other on disk.

At startup, the AlarmPersistencyManager retrieves the events persisting for the containing VNE.

Event data in the files is updated:

- At shutdown or
- After a change (a new event is added or removed) or
- After a specific interval of time has passed. This prevents data from being rewritten to the persistency file when a stream of events is added or removed during a short period of time because the data is saved only after the specified period of time has elapsed.

Initialization

The AlarmPersistencyManager reads the following configurable items:

- Enabled—is the mechanism enabled for this VNE.
- Writing delay—the interval between the arrival of a new event (or a removal of an existing event) and the writing activity of the persistency file.
- Maximum age—how long an event remains in the persistency files before it becomes obsolete.



Note This only applies when trying to retrieve data from the persistency files.

Retrieving Events

At startup, each VNE calls its AlarmPersistencyManager to load the persisting events.

If the file does not exist or is corrupt no events are loaded. Faulty event objects are not be loaded. Events which have been in the file for longer then the configured amount of maximum age are not loaded (no age tests are held during ordinary runtime).

Storing Events

At shutdown, events are saved to the VNE's event persistency file as a safety precaution in case the events have not been saved.

Removing an Event

An event will be searched for and removed using the same information which was used to add it. The event is removed from the memory because an “up alarm” (for example, a “link up” alarm) has been generated and the persistency information is no longer required. After the removal, the AlarmPersistencyManager stores the events after a writing delay as specified in the Registry.

Removing an Event and Clearing an Alarm

The AlarmPersistencyManager is able to search for and remove an event and send a clearing alarm for this event if it is found because this information is no longer required as the alarm has been cleared.

After an event has been added or removed from the AlarmPersistencyManager, a delayed message is sent to the AlarmPersistencyManager which triggers, upon its arrival, a storing of the events to the file.

Configuring Alarm Persistency

The user can define for each sub-event whether to have a persisting or unpersisting alarm (define both or none). An example of the "card out" alarm is displayed.

```
<key name="card out">
  ...
  <key name="card in">
    ...
    <key name="alarm">
      <entry name="alarm-persistency">unpersist</entry>
      ...
    </key>
  </key>
</key>
<key name="card out">
  ...
  <key name="alarm">
    <entry name="alarm-persistency">persist</entry>
    ...
  </key>
</key>
</key>
```

Alarm Persistency Default Configuration

The following alarms are configured to be persistent:

- Card Out
- Device unreachable
- CPU over utilized
- Dropped packets
- Discarded packets
- Duplicate route entries (alarm is disabled OOB)
- Link down
- Route entry removed entries (alarm is disabled OOB)
- Memory over utilized
- Port down
- Port flapping
- Rx over utilized
- Tx over utilized

Instrumentation Persistency

The instrumentation layer persists the information that was collected from the device to the file system. When the VNE restarts, it uses this information to emulate the device's response and thus the VNE can be modeled according to its last persistent state. The next polling instance is performed against the real device.

Configuring Instrumentation Persistency

The following instrumentation parameters can be configured:

- persistencydir
- persistencylevel
- persistencystorageenabled
- persistencystorageinterval
- persistencytimeout

persistencydir

This is the directory in which the persistency information is saved on the local file system. This is a relative path.

Allowed Values—A string representing the relative directory in the file system

Default Value—instrumentor-persistency

persistencylevel

This is the level of persistency to be used. Off means it will not persist. Full means it will persist. Do not use “partial”.

These values may be on certain commands to make sure some are persistent by some not.



Note

This is a “command” level parameter, meaning you can decide that one command is persisted using “full” and another is not (using “off”).

Allowed Values—Full or OFF or partial

Default Value—Full

persistencystorageenabled

This defines whether to enable the whole mechanism or not.

Allowed Values—True / false

Default Value—True

persistencystorageinterval

This is the interval, in milliseconds, for which the data to be persisted is accumulated and then written to the persistent storage in bulk, in order to use less IO operations.

Allowed Values—Within the user’s discretion.



Note

Small intervals cause more IO operations on the local file system. Very long intervals means that the information that is stored is less up to date.

Default Value—600000 (10 minutes)

persistencytimeout

If the persistency mechanism is enabled, when the instrumentation layer starts, it loads all the data from the files and this data can be used as data for the commands only the first time they are executed. Some commands can be used for the first time, long after all the other commands have finished multiple cycles (for example, commands which run only when the status on the device has changed), this initial data is marked as obsolete after the "persistency timeout" has passed, and commands after this time, even if they are run for the first time, will be executed directly on the device. The time is defined in milliseconds.

Allowed Values—Within the user's discretion, should however usually be at least one minute.

**Note**

A small value causes the instrumentation layer to ignore the persistent data. A large value causes old data to be retrieved long after the VNE has finished loading.

Default Value—60000 (1 minute)

Topology Persistency

Cisco ANA supports persistency for topology, namely, Layer 1 topological connections. Layer 1 topology supports one connection per DC, namely, the physical topology reflects a single port connected via a single link.

The following topologies are persisted:

- Layer 1 counter-based topologies
- Static topologies
- Path-based topologies for B-STDX, GX and CBX

Static topology, which identifies physical links configured by the user is persisted once a user configures the static link between the two entities. This link is then stored in the Registry in the AVM key that contains the specific VNE registrations.

For other topology, every time a link is created the persistency mechanism writes the link to this file. When a link is disconnected the file representing the link is removed.

Configuring Topology Persistency

Physical topology persistency can be enabled or disabled via the Registry. Topology has a Registry entry entitled "Persistency":

- The entry can be defined as true or false value
- In order to enable topology persistency the value should be defined as true
- The default value is true

**Note**

Topology persistency assumes that the XID (unique device component ID) will be persistable. For example, the port XID should remain the same (will not be dependent on whether the ifIndex is changed from time to time) XID after the device reboots or after the VNE reboots.

Cisco ANA NetworkVision User's Guide, 3.5.1

When adding a new device to a map, all the devices that are managed by the system are displayed.

When viewing the Device View in the Cisco ANA NetworkVision window only the devices displayed in the map are listed.

The following columns have been removed from the Device View:

- System Description
- Location
- Contact



Warning

There is an option to add the System Description, Location and Contact columns to the Device View, however, this will increase memory consumption. Changing these settings must be done with the support of Cisco Professional Services.

Cisco ANA Client Installation Guide, 3.5.1

In Chapter 2, System Requirements, the minimum Cisco ANA Client hardware requirements were updated as follows:

- The Cisco ANA Client requires 512 MB of free non-virtual memory



Note

The minimum client configuration, remains a 1GB. When several memory intensive applications are running at the same time, the user may experience sluggish in the user interface response time and a slow refresh rate. If the user encounters latency problems, the user must close the other applications running on the desktop.

When planning available memory space the user should consider that the application does not work well with paging. When paging is used, this leads to degradation in the application's performance.

In Chapter 2, System Requirements on page 2-1 should read as follows:

The minimum hardware requirements for an IBM or PC compatible work station is a Pentium IV, 2.66 GHz Processor or better, and not a Pentium IV, 2.66 MHz Processor or better.

Cisco ANA NetworkVision with a configuration 512MB of free-non virtual memory per running instance, supports across all of the maps that are open, a maximum of 10K objects (devices, VPNs, VRFs and sites) 12K links and 10K tickets (if the same tickets are displayed in different maps, each ticket will be counted separately).

One map in Cisco ANA NetworkVision, supports a maximum of 5K objects, 6K links and 5K tickets.

The other Cisco ANA applications require 256MB of free non-virtual memory.



Note

It is possible to reconfigure Cisco ANA NetworkVision to use only 256 MB, however this may result in reduced functionality. To modify the memory parameters, right click on the Cisco ANA Network Vision short cut properties. In the "Target" text box, remove the texts -vmargs -Xmx512m, and re-launch the application.

**Note**

The maximum number of maps that can be opened for Cisco ANA NetworkVision is five (default), regardless of the number of devices, links and tickets, but this number is configurable assuming that the overall number of links and devices per application do not exceed the maximum limits. For information about customizing the maximum number of maps, contact Cisco Professional Services.

**Note**

The maximum number of open tickets (other tickets can be correlated to them) for the system is 5K. For a definition of an open ticket, refer to the Cisco ANA Fault Management Guide, 3.5.1. The operator should ensure that tickets are closed on time.

In Chapter 3, Before Installing, the following warning was added:

**Warning**

Before installing the Cisco ANA Client 3.5.1 the user must uninstall the previous version.

In Chapter 4, Installing the Cisco ANA Client, the default installation location on page 4-1 has been updated as follows:

- The default installation location is:
C:/Program Files/Cisco Systems/ANA

In Chapter 4, Installing the Cisco ANA Client, the default Program Manager Group on page 4-2 has been updated as follows:

- The default Program Manager Group is: Cisco ANA.

Cisco ANA MPLS User's Guide, 3.5.1

In Chapter 6, Fault Management In MPLS Networks, the following note was added:

**Note**

The MPLS black hole feature is only supported when the PEs are managed by the system.

Cisco ANA Fault Management Guide, 3.5.1

The “VC removed” alarm is not supported in this version.

Related Documentation

User Guides

Cisco Active Network Abstraction NetworkVision User's Guide, 3.5.1

Cisco Active Network Abstraction EventVision User's Guide, 3.5.1

Cisco Active Network Abstraction MPLS User's Guide, 3.5.1

Cisco Active Network Abstraction Fault Management User's Guide, 3.5.1

Administrator Guides

- Cisco Active Network Abstraction Servers Installation Guide, 3.5.1
- Cisco Active Network Abstraction Client Installation Guide, 3.5.1
- Cisco Active Network Abstraction Administrator's Guide, 3.5.1
- Cisco Active Network Abstraction Error Messages, 3.5.1
- Cisco Active Network Abstraction Shell User's Guide, 3.5.1
- Cisco Active Network Abstraction High Availability User's Guide, 3.5.1

Developer Guides

- Cisco Active Network Abstraction Customization User's Guide, 3.5.1
- Cisco Active Network Abstraction Command Builder User's Guide, 3.5.1
- Cisco Active Network Abstraction Workflow User's Guide, 3.5.1
- Cisco Active Network Abstraction BQL User's Guide, 3.5.1
- Cisco Active Network Abstraction Registry Editor User's Guide, 3.5.1

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. This section explains the product documentation resources that Cisco offers.

Cisco.com

You can access the most current Cisco documentation at this URL:

<http://www.cisco.com/techsupport>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

The Product Documentation DVD is a library of technical product documentation on a portable medium. The DVD enables you to access installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the HTML documentation and some of the PDF files found on the Cisco website at this URL:

<http://www.cisco.com/univercd/home/home.htm>

The Product Documentation DVD is created and released regularly. DVDs are available singly or by subscription. Registered Cisco.com users can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at the Product Documentation Store at this URL:

<http://www.cisco.com/go/marketplace/docstore>

Ordering Documentation

You must be a registered Cisco.com user to access Cisco Marketplace. Registered users may order Cisco documentation at the Product Documentation Store at this URL:

<http://www.cisco.com/go/marketplace/docstore>

If you do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>

Documentation Feedback

You can provide feedback about Cisco technical documentation on the Cisco Technical Support & Documentation site area by entering your comments in the feedback form available in every online document.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you will find information about how to do the following:

- Report security vulnerabilities in Cisco products
- Obtain assistance with security incidents that involve Cisco products
- Register to receive security information from Cisco

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For emergencies only — security-alert@cisco.com

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For nonemergencies — psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532



Tip

We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.x through 9.x.

Never use a revoked encryption key or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT to find other means of encrypting the data before sending any sensitive material.

Product Alerts and Field Notices

Modifications to or updates about Cisco products are announced in Cisco Product Alerts and Cisco Field Notices. You can receive Cisco Product Alerts and Cisco Field Notices by using the Product Alert Tool on Cisco.com. This tool enables you to create a profile and choose those products for which you want to receive information.

To access the Product Alert Tool, you must be a registered Cisco.com user. (To register as a Cisco.com user, go to this URL: <http://tools.cisco.com/RPF/register/register.do>) Registered users can access the tool at this URL: <http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en>

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day at this URL:

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>



Note

Use the **Cisco Product Identification Tool** to locate your product serial number before submitting a request for service online or by phone. You can access this tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link, clicking the **All Tools (A-Z)** tab, and then choosing **Cisco Product Identification Tool** from the alphabetical list. This tool offers three search options: by product ID or model name; by tree view; or, for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.



Tip

Displaying and Searching on Cisco.com

If you suspect that the browser is not refreshing a web page, force the browser to update the web page by holding down the Ctrl key while pressing F5.

To find technical information, narrow your search to look in technical documentation, not the entire Cisco.com website. On the Cisco.com home page, click the **Advanced Search** link under the Search box and then click the **Technical Support & Documentation** radio button.

To provide feedback about the Cisco.com website or a particular technical document, click **Contacts & Feedback** at the top of any Cisco.com web page.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411

Australia: 1 800 805 227

EMEA: +32 2 704 55 55

USA: 1 800 553 2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—An existing network is “down” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of the network is impaired while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The Cisco Online Subscription Center is the website where you can sign up for a variety of Cisco e-mail newsletters and other communications. Create a profile and then select the subscriptions that you would like to receive. To visit the Cisco Online Subscription Center, go to this URL:

<http://www.cisco.com/offer/subscribe>

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco channel product offerings. To order and find out more about the *Cisco Product Quick Reference Guide*, go to this URL:
<http://www.cisco.com/go/guide>
- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:
<http://www.cisco.com/go/marketplace/>
- Cisco Press publishes a wide range of general networking, training, and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:
<http://www.ciscopress.com>
- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the *Internet Protocol Journal* at this URL:
<http://www.cisco.com/ipj>
- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:
<http://www.cisco.com/en/US/products/index.html>
- Networking Professionals Connection is an interactive website where networking professionals share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:
<http://www.cisco.com/discuss/networking>
- “What’s New in Cisco Documentation” is an online publication that provides information about the latest documentation releases for Cisco products. Updated monthly, this online publication is organized by product category to direct you quickly to the documentation for your products. You can view the latest release of “What’s New in Cisco Documentation” at this URL:
<http://www.cisco.com/univercd/cc/td/doc/abtunicd/136957.htm>
- World-class networking training is available from Cisco. You can view current offerings at this URL:
<http://www.cisco.com/en/US/learning/index.html>

This document is to be used in conjunction with the documents listed in the “[Related Documentation](#)” section.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 1999-2006 Cisco Systems, Inc. All rights reserved.