



Release Notes for Cisco Active Network Abstraction, 3.5

Corporate Headquarters

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

<http://www.cisco.com>

Tel: 408 526-4000

800 553-NETS (6387)

Fax: 408 526-4100



THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0601R)

Important Notice

Cisco ANA 3.5 is a carrier-class, multi-vendor network and service management platform which builds a real-time virtual model of the network, serving as a live information base for value-added tools and applications for integration into an existing OSS environment.

Cisco ANA 3.5 is a limited release by Cisco Systems of the existing features and functions of the Sheer DNA 4.0.1 software.

As this is a limited release, the naming of the product in the software and the user documentation remains as Sheer DNA.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

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

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from Cisco Marketplace at this URL:

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

Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

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

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

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 can perform these tasks:

- 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 and notices for Cisco products is available at this URL:

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

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from 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 might have identified a vulnerability in a Cisco product, contact PSIRT:

Emergencies — 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.

Nonemergencies — psirt@cisco.com

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

1 877 228-7302

1 408 525-6532

We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.x through 8.x.

Never use a revoked 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.

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>

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the Tools & Resources link under Documentation & Tools. Choose Cisco Product Identification Tool from the Alphabetical Index drop-down list, or click the Cisco Product Identification Tool link under Alerts & RMAs. The CPI 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.

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)—Your 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 operation 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 your network is impaired, but 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.

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>

Packet magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

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

iQ Magazine is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

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

or view the digital edition at this URL:

<http://ciscoiq.texterity.com/ciscoiq/sample/>

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 for networking professionals to 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>

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>

Table of Contents

1	Introduction.....	1
1.1	Installation	2
1.2	Important Notes.....	2
2	Known Caveats With This Release	5
2.1	Open Caveats.....	5
3	Documentation Updates	11
3.1	Cisco ANA Server's Installation Guide, 3.5.....	11
3.2	Cisco ANA Administrator's Guide, 3.5	11
3.2.1	Database Backup and Restore Procedure.....	11
3.2.1.1	Overview.....	12
3.2.1.2	Backed-Up Content.....	12
3.2.1.3	Backup Procedure.....	12
3.2.1.4	Changing Periodic Backup Time	14
3.2.1.5	Restore Procedure.....	14
3.3	Cisco ANA Registry Editor User's Guide, 3.5.....	15
3.3.1	How Changes Affect the Registry	15
3.4	Cisco ANA MPLS User's Guide, 3.5.....	16
3.5	Cisco ANA Workflow User's Guide, 3.5	16
4	Related Documentation	17
4.1	User Guides	17
4.2	Administrator Guides	17
4.3	Developer Guides.....	17

1 Introduction

These Release Notes support the release of *Cisco Active Network Abstraction, 3.5* (Cisco ANA 3.5).

Cisco ANA 3.5 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 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 provides a unified solution for diverse network environments and applications. Implemented with a highly-scalable distributed architecture, Cisco ANA 3.5 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 is a unified, fully-integrated solution offering:

- Multi-vendor device support
- Multi-Technology coverage: IP, L2/L3 VPN, xDSL, ATM, FR, GigE , MetroEthernet, Ethernet\802.1Q\ISL, L2TP and routing protocols (e.g. EIGRP, OSPF, BGP, IS-IS)
- Integrated device, network and service management functionality
- Open interfaces for integration with multiple OSS/BSS applications

Cisco ANA 3.5 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 to manage and analyze network behavior. Cisco ANA 3.5 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 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

1.1 Installation

Refer to the *Cisco Active Network Abstraction Server's Installation Guide, 3.5* and the *Cisco Active Network Abstraction Client Installation Guide, 3.5*.

1.2 Important Notes

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

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 Sheer DNA system:

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 bloodtest.	utils/apache/conf/sheer.conf	1310	-	-	http
Machine interface	BQL machine to machine interface	-	9002	-	Java	-
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	-	-	Snmpp

2 Known Caveats With This Release

2.1 Open Caveats

Identifier Details

- CSCsc72986 **Title:** HSRP Group is not Modeled
- Impact:** 1. We will not see HSRP IP interfaces on the logical inventory.
2. No alarm of type hsrp group status changed will be generated and nothing will correlate to it.
- Conditions:** HSRP is configured on the device.
- Workaround:** None
- CSCsc94544 **Title:** The cloud VNE isn't supported in the default scheme
- Impact:** The cloud VNE will not load properly when created.
- Conditions:** Cloud VNE is required to run in deployment.
- Workaround:** The patch VNE_PATCH_2.jar solves this problem. The patch must be installed by Professional Services.
- CSCsd15988 **Title:** Physical links not discover between Ethernet Cloud to others VNEs
- Impact:** Cloud VNE will load but no links will connect to it even if configured on other VNEs.
- Conditions:** Ethernet Cloud VNE is up and running.
- Workaround:** The patch VNE_PATCH_2.jar solves this problem. The patch must be installed by Professional Services.
- CSCsd30408 **Title:** CDP Topology: Link not disconnecting when cdp is disabled.
- Impact:** When CDP is disabled on a device that was previously running CDP and the device was connected to another device via CDP, the link does not disconnect.
- Conditions:** Cisco devices that have CDP enabled and are connected to each other.
- Workaround:** Restarting one on the VNEs will disconnect the link and cause it to be rediscovered based on other attributes if applicable.
- CSCsd34516 **Title:** Affected Parties do not change their severity status to Real/Recovered
- Impact:** When a link down occurs in a MPLS network its impact analysis report should include affected pairs that have their severity set to either recovered or real according to whether a re-route was found for those services. At this time they are all set with potential severity.
- Conditions:** The problem appears in a MPLS network running services such as VPN and a link down fault occurs.

Identifier **Details**

Workaround: Patch VNE_PATCH_2.jar solves the problem. The patch must be installed by Professional Services.

CSCsd34526 **Title:** BGP neighbor Loss alarm does not always correlate to link down alarm

Impact: BGP Neighbour Loss alarm doesn't correlate to link down in some scenarios.

Conditions: This could happen in one of the following scenarios:

1. Some of the devices that participating in the flow from the source device to its neighbor are not managed.
2. When the information in the VNE cache does not tally with the device timestamp information like routing table and mpls forwarding table.

This could happen when the following is happened:

- a. A VNE is reloaded and accordingly, the new MPLS forwarding table is been changed from the previous mpls forwarding information. This information has not been updated yet in the VNE cache.
- b. The links are not stable: link down / up alarms are reoccurring rapidly on links that located on the path of the flow.

Again here, the new information does not yet update in the VNE cache.

In such cases, the flow starts according to its timestamp which is different from the one that should be there (For ex: different outgoing I/F). Therefore, the flow fails.

Workaround: None.

CSCsd34847 **Title:** Missing link between the ASAM <-> CBX

Impact: Topological link between Alcatel ASAM and Lucent CBX is not discovered.

Conditions: Alcatel ASAM and lucent CBX must be connected to each other and have traffic flowing between them.

Workaround: This problem can be fixed by making the relevant changes in the customer customized scheme. These changes, along with other required customizations, can be done by the Cisco Professional Service team as part of the product deployment process.

CSCsd36144 **Title:** Frame Relay cross connect is missing in Cloud VNE

Impact: Frame-relay cross-connect table is missing the in the cloud VNE. This problem occur for physical interfaces which have multiple frame-relay sub interfaces.

Workaround: The problem is solved by patch VNE_PATCH_2.jar. The patch must be installed by Professional Services. Should the problem persist, specific modification to the deployment scheme need to performed by professional services.

CSCsd46264 **Title:** No GRE tunnel modelled

Impact: GRE tunnels are not modeled, nor their topology is displayed.

"GRE tunnel down" alarm will not be issued, nor any correlation to it will occur.

Identifier	Details
	Workaround: None.
CSCsd61046	Title: Limited support of L2TP. Impact: L2TP information will include only basic L2TP information. No support of alarms, LAC/LNS distinguishing and path tool available for L2TP. Conditions: L2TP support is limited to Redback SMS devices only. Workaround: None.
CSCsd61060	Title: Ethernet physical topology isn't discovered when CDP is not enabled. Impact: Topology links that should have been discovered using IP topology or MAC topology are not discovered. Conditions: This situation may occur when a client is working with Cisco routers and/or Catalyst devices without using CDP.. Workaround: Set the state of the WaitForSpecificSignature flag to false in site.xml and make sure the value is not overriden in license.jar
CSCsd63659	Title: Mac based topology disconnects for no apparent reason. Impact: Topology links between Ethernet ports are connecting and then disconnecting. Workaround: Connect the ports using static topology.
CSCsd63693	Title: IMA is not supported. Impact: IMA agregations are not discovered. Conditions: When working with modules that support IMA aggregation of ports. Workaround: None
CSCsd66920	Title: Client memory problem Impact: NetworkVision's reported memory usage remains high even after closing a large map. Conditions: Using the NetworkVision GUI application, open a large map and then close it. Workaround: No workaround is needed. The memory is automatically freed when another map is opened.
CSCsd74121	Title: C not run bean shell script in Command Builder. Impact: Trying to execute a breanshell script will be resolved in an error. Conditions: No condition, every beanshell script through out the system. Workaround: Apply patch name "CSCsd74121_patch.jar" to system after installation. The patch must be installed by Professional Services.
CSCsd74144	Title: ISDN backup doesn't work with scheme of bc-ces. Impact: An ISDN backup interface goes up but no alarm appears in the system.

Identifier **Details**

Conditions: This occurs in routers that have an interface backed up by an ISDN interfaces. When the primary interface goes down the backup should go up and the VNE should produce and alarm.

Workaround: None

CSCsd75036 **Title:** Memory/CPU problem when opening few service paths.

Workaround: Do not open multiple service paths on the same client simultaneously.

CSCsd77828 **Title:** ASAM missing card-out/card-in alarms

Impact: No alarm is created in the ASAM VNE when a card is pulled out.

Conditions: Pull out a card from an ASAM VNE and wait for a period longer then the configured configuration interval.

Workaround: None

CSCsd78156 **Title:** Adding VC cross connect causes exceptions - Unreproducible

CSCsd78530 **Title:** ASAM v5: ADSL port status is missing

Impact: When loading an ASAM VNE the port status is not updated.

Conditions: Loading an ASAM VNE using either reduno or telmex scheme.

Workaround: None

CSCsd78874 **Title:** Potential affected does not change state to recovered in a link down scenario.

Impact: When a link down occurs in a MPLS network its impact analysis report should include affected pairs that have their severity set to either recovered or real according to whether a re-route was found for those services. At this time they are all set with potential severity.

Conditions: The problem appears in a MPLS network running services such as VPN and a link down fault occurs.

CSCsd78894 **Title:** BGP Affected functionality is not working correctly.

Impact: When performing a link down resulting in:

- a. device unreachable (BGP router)
- b. BGP neighbor loss alarm (Route reflector)

No impact analysis is received, since the route reflector does not hold any services on it and the BGP router is unreachable and is hence not detecting the problem.

Conditions: Any loss of connectivity between route reflectors and BGP routers that become unreachable will cause this problem.

Workaround: Normally Route reflectors hold no services on them therefore no affected pairs are reported. A device that becomes unreachable is not aware of the fact that it has lost BGP neighbors. This is a known limitation since it was not taken into consideration that one of the BGP routers will become unreachable

Identifier **Details**

- CSCsd79340** **Title:** Scalability issue with command creation in Command Builder
- Impact:** Performance issue when doing publishing of a Command created with the command manager.
- Conditions:** When doing customer customizations all data is stored to site.xml file, one of the customized elements inserted into the site.xml is the customer "Script Commands" created via the Command Manager (a tool inside the Vision GUI client). As long as site.xml is getting bigger and bigger, doing a "publishing" (an action designed to enable the new command for several VNE elements base on family, type & etc.) takes longer and longer. The issue was traced to the Registry component and there for the workaround is in the site.xml file.
- Workaround:** 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** **Title:** CDP: Physical topology not discovered for POS & Serial links.
- Impact:** POS and serial links are not being discovered.
- Workaround:** Connect the link statically.
- CSCsd80788** **Title:** Restore Script Is Not Working With An External Db
- Workaround:** This is a workaround for the restore problem
- 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: `chmod -R 775 /tmp/db_back`
- change dir to `$$SHEERHOME/Main/scripts/misc/backup`
- 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:
- `cat orarestore.sh | sed s/"\data\MCDB"/"/oradata\MCDB"/g > /tmp/restore.sh`
- change the permission of /tmp/restore.sh by typing : `chmod 777 /tmp/restore.sh`
- switch to user oracle
- type the following command: `/tmp/restore.sh /tmp/db_back`
- for security purposes, erase dir /tmp/db_back
- CSCsw09406** **Title:** Link connect/disconnect between CE and PE which are directly connected.
- Impact:** When two devices are configured one as CE and one as a PE in a MPLS network

Identifier **Details**

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.

Conditions: The problem will occur in networks that run VPN over MPLS and devices run CDP, and the VNE topology mechanism is configured to run CDP tests

Workaround: Create a static link between the PE and CE.

CSCsw12618 **Title:** Ethernet Cloud: Ethernet port disappear from Cloud.

Impact: Ethernet port disappeared from cloud VNE.

Conditions: Cloud VNE and adjacent VNE should be loaded.

Workaround: Professional services should add in the specific deployment scheme the following:

Cloud VNE should have entry "permissible-subnets" in avm, with ip subnet defined over appropriate Ethernet port.

CSCsw12670 **Title:** Creating static link between Clouds to VNE reports failure.

Impact: When running the BQL command for creating static link between cloud VNE and a VNE, the command reports failure even if it succeeded.

Conditions: Cloud VNE and adjacent VNE should be loaded. Telnet to the GW with port 9002. Login and run bql command for create Ethernet port in Cloud VNE with appropriate vlan.

Workaround: None.

CSCsw12683 **Title:** Frame-Relay Cloud: Static topology doesn't work

Impact: Cross-connect in Frame Relay VNE cloud isn't created when crating the cross-connect statically.

Conditions: Frame Relay VNE cloud is up and running.

Workaround: The patch VNE_PATCH_2.jar solves this problem. The patch must be installed by Professional Services.

CSCsw13304 **Title:** Ethernet Cloud does not support switchport trunk and access properly.

Impact: When Interface to Ethernet cloud is in a trunk, the Cloud VNE does not support it properly.

Conditions: 1. Ethernet VNE cloud is up and running.
2. Port connecting to the cloud is configured as "trunk"

Workaround: None.

3 Documentation Updates

This section of the Release Notes includes updates to the Cisco Active Network Abstraction 3.5 documentation set.

3.1 Cisco ANA Server's Installation Guide, 3.5

In Section 2, System Requirements, 2.1 Sheer DNA Gateway and 2.2 Sheer DNA Unit, the Operating System Software Requirements are detailed as:

- Solaris™ 2.8
- Recommended revision 23* kernel patches
- Recommended Java™ patch bundle *

The specific requirements are as follows:

- Solaris™ 2.8
- Solaris 8 Recommended patch cluster, from December 2005 and above.
- Recommended J2SE patch cluster for Solaris 8, from December 2005 and above.

3.2 Cisco ANA Administrator's Guide, 3.5

3.2.1 Database Backup and Restore Procedure

This section describes the database backup and restore procedure.

Overview, page 12, provides an overview of the backup procedure.

Backed-Up Content, page 12, briefly describes the data that is backed up.

Backup Procedure, page 12, describes how to activate the backup procedure.

Changing Periodic Backup Time, page 14, describes how to change the backup time.

Restore Procedure, page 14, describes the restore procedure.

3.2.1.1 Overview

The following backup procedure is used to perform data backup once a week. It operates through the UNIX cron mechanism. The factory settings entry in the cron table (crontab) executes the backup procedure every Sunday at 1:00 AM. To activate the backup procedure the user needs to remove the comment for the relevant line in the cron table.

The restoration is done manually by executing the `restore.pl` script.

3.2.1.2 Backed-Up Content

The data that has been backed-up is:

- Sheer DNA Database
- Sheer DNA Registry (“Golden Source”)
- cron table (crontab).

3.2.1.3 Backup Procedure

The backup script is a Scheduled task. It operates through cron.

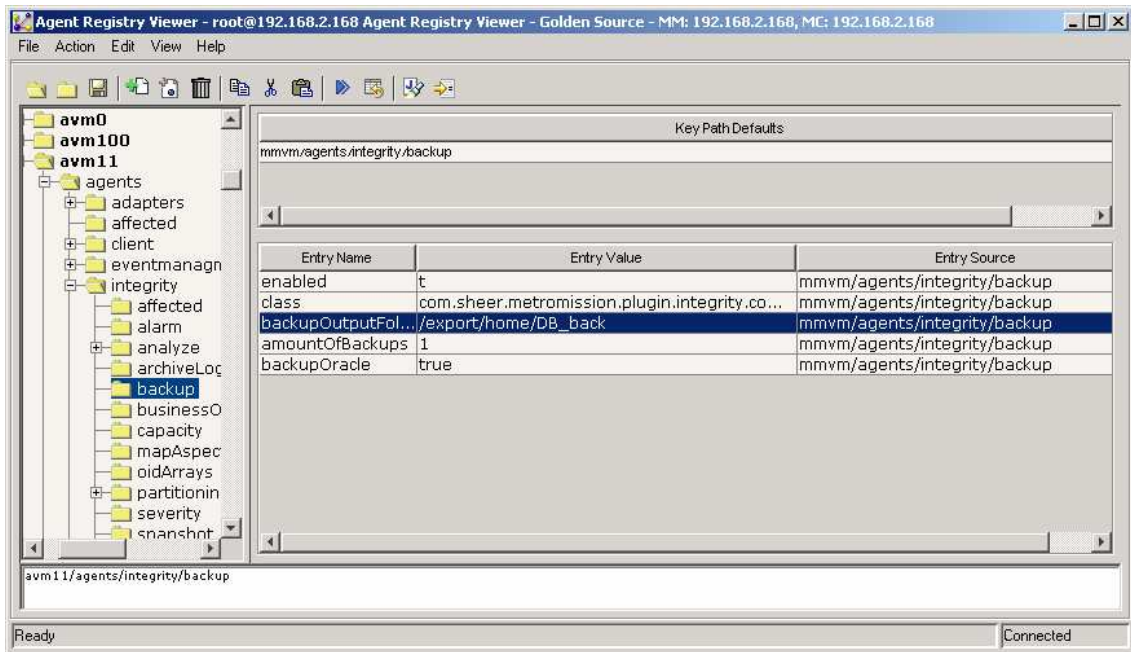
The backup files are stored in the following directory:

```
~sheer/db/db_backup/[date+time].
```

Note: The filler [date+time] is a directory name composed of a date and time of the backup. For example, `~sheer/db/db_backup/200504130404/` is created on 13 April 2005 at 4:04 AM. By default the cron table executes the backup procedure every Sunday at 1:00AM.

The location is configurable through the registry. For more information, refer to registry path: `avm11/agents/integrity/backup`.

The figure below displays the backup registry entries.



The backup is disabled by default.

To enable the backup

1. Telnet the Ana Gateway with sheer user.
2. Edit the cron table as follows:

```
crontab -e
```

3. add the following line to the file and save the change:

```
0 1 * * 0 cd Main;./mc.csh localhost 8011  
integrity.executeTest backup > /dev/null 2>&1
```

Refer to `crontab(1)` in the Solaris documentation for a detailed explanation about the cron table format.

The user can activate the backup procedure on the spot.

To activate the backup procedure on the spot

1. Telnet the Ana Gateway with sheer user.

2. Change the directory to sheer/Main by executing the following command:

```
cd ~/Main
```

3. At prompt execute the following command line:

```
./mc.csh localhost 8011 integrity.executeTest backup
```

3.2.1.4 Changing Periodic Backup Time

A crontab file consists of lines of six fields each. The fields are separated by spaces or tabs. The first five are integer patterns that specify the following:

- minute (0-59)
- hour (0-23)
- day of the month (1-31)
- month of the year (1-12)
- day of the week (0-6 with 0=Sunday)

To specify days using only one field, the other field should be set to *.

For example, 0 0 * * 1 would run a command only on Mondays.

Another example cleans up core files every weekday morning at 3:15 am:

```
15 3 * * 1-5 find $HOME -name core 2>/dev/null | xargs rm -f
```

The sequence 0 0 1,15 * 1 runs a command on the first and fifteenth of each month as well as every Monday.

3.2.1.5 Restore Procedure

Install the Sheer DNA Gateway. For more information, refer to the chapter *Installing the Sheer DNA Gateway* in the *Cisco Active Network Abstraction Servers Installation Guide*. Note you will need to login as root.

To restore from a backup

1. Change the directory /export/home/sheer/Main/scripts by executing the following command:

```
cd ~/sheer/Main/scripts
```

2. Execute the restoration script:

```
restore.pl [backup-files-location]
```

Note: By default the [backup-files-location] is ~sheer/db/db_backup/[date+time] (this is configurable through the registry). The filler [date+time] is a directory name composed of a date and time backup time. For example, ~sheer/db/db_backup/200504130404/ is created on 13 April 2005 at 4:04 AM.

3. Once the restoration is successful, initialize the Sheer DNA Gateway by executing the following command:

```
su - sheer
cd Main
./mvm.csh
```

Note: The default password for the user sheer is sheer.

3.3 Cisco ANA Registry Editor User's Guide, 3.5

3.3.1 How Changes Affect the Registry

The Registry 'Defaults' mechanism has similar behavior to that of inheritance in Object Oriented Programming Languages. In other words, when a Key has a 'default' entry set, this is similar to a Class being extended in Java. A Registry Key Data is therefore composed of two parts: Concrete data (physically written in that key's location) and inherited data (coming from parent key(s)). If to continue with the OO analogy, this is similar to concrete methods and inherited methods in a class. It is important to add that not only entries are inherited, but also sub keys. Since a Key's data is composed of both concrete and inherited data, registering for changes on a specific key will cause implicit registration on inherited keys (so, changes to inherited data will trigger notifications as well).

One special hive in the registry is called 'Site'. Site is the place to concentrate all changes made to the registry on a customer site. Any first level key placed under site will be added to the default path during runtime. For example, if we have a key called Key1, extended by (i.e. has a 'default' entry set to) ParentKey1 (default path: Key1->ParentKey1), and we place under site a key called ParentKey1, the default path will now look like this: Key1->site/ParentKey1->ParentKey1.

3.4 Cisco ANA MPLS User's Guide, 3.5

In the Cisco Active Network Abstraction MPLS User's Guide, Section 6.1.2 "Broken LSP Discovered Alarm" the note on page 68 should read as follows:

Note: The clearing alarm does not activate flows to locate the LSPs that were passing through it in order to issue a clearing alarm for Broken LSPs, but rather uses the auto clear functionality. The Gateway periodically reviews the tickets and checks if all the alarms under each ticket are cleared or configured as auto cleared alarms, and whether the Gateway correlation timeout has passed, and in this case the Gateway closes the ticket.

Using this functionality, once the "MPLS Black hole" alarm is cleared, then after a specific time interval (configured Gateway correlation timeout) has passed, the Gateway will be able to close the ticket since all the alarms correlated to "MPLS Black hole" are "Broken LSP" which are configured as auto cleared.

3.5 Cisco ANA Workflow User's Guide, 3.5

In the Cisco Active Network Abstraction Workflow User's Guide, Section 2.10.2 "Get Workflows" the BQL command on page 28 should read as follows:

```
<?xml version="1.0" encoding="UTF-8"?>  
<command name="GetWorkflows"/>
```

4 Related Documentation

4.1 User Guides

Cisco Active Network Abstraction NetworkVision User's Guide, 3.5

Cisco Active Network Abstraction EventVision User's Guide, 3.5

Cisco Active Network Abstraction MPLS User's Guide, 3.5

Cisco Active Network Abstraction Fault Management User's Guide, 3.5

4.2 Administrator Guides

Cisco Active Network Abstraction Servers Installation Guide, 3.5

Cisco Active Network Abstraction Client Installation Guide, 3.5

Cisco Active Network Abstraction Administrator's Guide, 3.5

Cisco Active Network Abstraction Error Messages, 3.5

Cisco Active Network Abstraction Shell User's Guide, 3.5

Cisco Active Network Abstraction High Availability User's Guide, 3.5

4.3 Developer Guides

Cisco Active Network Abstraction Customization User's Guide, 3.5

Cisco Active Network Abstraction Command Builder User's Guide, 3.5

Cisco Active Network Abstraction Workflow User's Guide, 3.5

Cisco Active Network Abstraction BQL User's Guide, 3.5

