



Release Notes for Cisco Active Network Abstraction, 3.5.2

19 March 2007

These release notes support the release of Cisco Active Network Abstraction, 3.5.2.



Note

See Cisco.com for the most up-to-date version of the Release Notes for Cisco Active Network Abstraction, 3.5.2.

Contents

This document includes the following topics:

- [Introduction](#)
- [New Features in Cisco ANA 3.5.2](#)
- [Changes from the Last Release](#)
- [Installation Notes](#)
- [Limitations and Restrictions](#)
- [Important Notes](#)
- [Open Caveats - Cisco ANA, Release 3.5.2](#)
- [Resolved Caveats - Cisco ANA, Release 3.5.1](#)
- [Open Caveats - Cisco ANA, Release 3.5.1](#)
- [Resolved Caveats - Cisco ANA, Release 3.5.](#)
- [Open Caveats - Release Cisco ANA 3.5](#)
- [Documentation Updates](#)
- [Related Documentation](#)
- [Obtaining Documentation](#)
- [Documentation Feedback](#)



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

© 1999-2007 Cisco Systems, Inc. All rights reserved.

- [Cisco Product Security Overview](#)
- [Product Alerts and Field Notices](#)
- [Obtaining Technical Assistance](#)
- [Obtaining Additional Publications and Information](#)

Introduction

These Release Notes support the release of Cisco Active Network Abstraction, 3.5.2 (Cisco ANA 3.5.2).

Cisco ANA 3.5.2 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 3.5.2 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 3.5.2 provides a unified solution for diverse network environments and applications. Implemented with a highly-scalable distributed architecture, Cisco ANA 3.5.2 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 3.5.2 is a unified, fully-integrated solution offering:

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

Cisco ANA 3.5.2 dynamically discovers and identifies basic network components, while obtaining end-to-end visibility of the network resources, connections and dependencies, enabling Cisco ANA 3.5.2 to manage and analyze network behavior. Cisco ANA 3.5.2 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 3.5.2 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 and 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

New Features in Cisco ANA 3.5.2

The following new features were added in Cisco ANA 3.5.2:

- New VNEs introduced—For more information see [New VNEs Introduced](#).
- Performance improvements—For more information see [Performance Improvements](#).
- Layer 2 tunneling protocol—For more information see [Layer 2 Tunneling Protocol “L2TP”](#).
- Solaris 10—For more information see [Solaris 10](#).
- QoS—The following functionality is supported:
 - Access lists on Cisco routers including access list entries.
 - Rate limit on Cisco routers including detailed parameters.
- New service alarm introduced:
 - Card up/down—Indicates that the card admin status has changed from down to up, and from up to down.
 - Port down—By default, port down alarms are suppressed on xDSL ports. Cisco ANA supports selectively enabling the sending of port down alarms on xDSL ports.
- XML format in BQL error messages—The system API (BQL) returns errors in XML format. The error messages contain the error code, error description and stack trace (if applicable) within the XML tags.
- VNE schemes—The product scheme was added. It is recommended that the user select the product scheme when defining VNEs.

New VNEs Introduced

This section details the Virtual Network Element (VNE) device support information for Cisco ANA 3.5.2.

Table 1 Cisco ANA 3.5.2 VNEs

Vendor	Device Classification	Device Family	Device Type/Modules	Software Version
ADC Teledata	DSLAM		BA-40	
Alcatel	DSLAM	ASAM/DSLAM	1000 R3	4.2 SD
Alcatel	DSLAM	ASAM/DSLAM	7300, 1000 R4	4.2 HD, UD
Alcatel	DSLAM	ASAM/DSLAM	MiniRam 480	4.2 HD, UD
Cisco	Broadband	SCE	1000	3.0.3, 3.0.5
Cisco	Broadband	SCE	2000	3.0.3, 3.0.5
Cisco	Router	12xxx Series	12416	12.0(33)s; 12.0(31)S5; 12.0(31)S4
Cisco	Router	12xxx Series	12000 Series	IOS-XR 3.4
Cisco	Router	7200 Series	7206 VXR/7206	11.1; 12.2(15)T5
Cisco	Router	76xx Series	7609	12.2 SRA; 12.2(18)SXF4
Cisco	Router	76xx Series	7613	12.1

Table 1 Cisco ANA 3.5.2 VNEs (continued)

Vendor	Device Classification	Device Family	Device Type/Modules	Software Version
Cisco	Router	CRS	CRS-1	R 3.4
Cisco	Router	ISR	836	12.3(14T), 12.3(11T)
Cisco	Router	ISR	1841	12.3(14T), 12.3(11T)
Cisco	Router	ISR	2801	12.3(14T), 12.3(11T)
Cisco	Router	ISR	2811	12.3(14T), 12.3(11T), 12.3(11) T6
Cisco	Router	ISR	2851	12.3(14T), 12.3(11T)
Cisco	Router	ISR	3825	12.3(14T), 12.3(11T)
Cisco	Router	ISR	3845	12.3(14T), 12.3(11T)
Cisco	Router	ISR	1801-W	12.3(14T), 12.3(11T)
Cisco	Router	ISR	1802-W	12.3(14T), 12.3(11T)
Cisco	Router	ISR	1803-W	12.3(14T), 12.3(11T)
Cisco	Router	ISR	1811-W	12.3(14T), 12.3(11T)
Cisco	Router	ISR	1812-W	12.3(14T), 12.3(11T)
Cisco	Router	ISR	871-W	12.3(14T), 12.3(11T)
Cisco	Router	ISR	876-W	12.3(14T), 12.3(11T)
Cisco	Router	ISR	877-W	12.3(14T), 12.3(11T)
Cisco	Router	ISR	878-W	12.3(14T), 12.3(11T)
Cisco	Switch	2600 Series	2621	11.3
Cisco	Switch	35xx Series	3550	11.2(8); 12.2(25)SED; 12.1(13)EA1a;12.1(14)EA1a
Cisco	Switch	45xx Series	4507	12.1(12c) EW; 12.2(25)SG
Cisco	Switch	65xx Series	6509	12.2.18-SXF
Cisco	Switch	65xx Series	6513	6.2(2)
ECI Telecom	DSLAM	DSLAM	Miniram	5.8.x
ECI Telecom	DSLAM	DSLAM	Hi-Focus SAM 480	5.8.x; 8.10.x
Juniper	Router	ERX	1440	7.2
Juniper	Router	M-Series	7	7.2
Juniper	Router	M-Series	10i	7.2
Juniper	Router	M-Series	20	7.2
Lucent	ATM switch	CBX	500	8.0.3.7, 9.1.1.14
Lucent	ATM switch	GX	550	8.0.3.22; 8.0.3.7, 9.1.1.14
Redback Networks	BRAS	SMS	1800	7.2

Table 1 Cisco ANA 3.5.2 VNEs (continued)

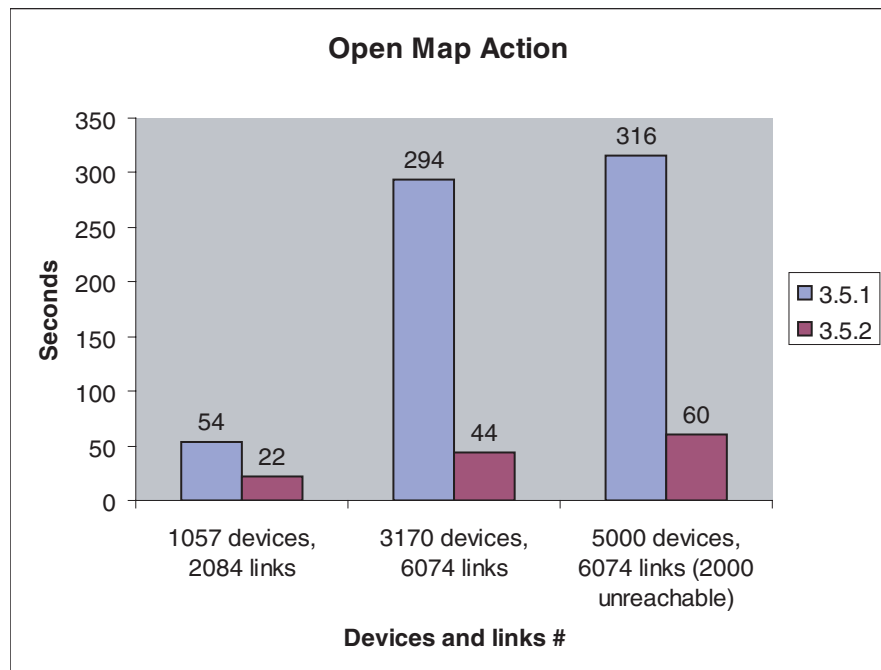
Vendor	Device Classification	Device Family	Device Type/Modules	Software Version
Redback Networks	BRAS	SMS	10000	6.09.18
Redback Networks	Router	SmartEdge SE	800	6.09.18

Performance Improvements

This section details the improvements in performance relating to Cisco ANA 3.5.2.

Opening a Map

The improvement in the performance of the “open map” action is detailed in the graph and table. The graph and table display the details regarding the “open map” action and compare the performance results between Cisco ANA 3.5.2 and Cisco ANA 3.5.1.

Figure 1 Open Map Performance Cisco ANA 3.5.2 vs. Cisco ANA 3.5.1

System Restart and Recovery

After a system restart, the time it takes to open the Cisco ANA Client applications was reduced from approximately 30 minutes to approximately 10 minutes.



Note This applies to a setup of 15000 objects or less.



Note Full VNE modeling to allow complete usage of the system will take longer than 10 minutes.

Layer 2 Tunneling Protocol “L2TP”



Note All the information described in this section is related to Redback devices only.

This section includes the following:

- [Layer 2 Tunnel Protocol Interface \(IL2TPTunnel\)](#)
- [Layer 2 Tunnel Protocol Session Entry \(IL2TPSessionEntry\)](#)
- [Layer 2 Tunnel Protocol Peer \(IL2TPPeer\)](#)
- [Layer 2 Tunnel Protocol Group \(IL2TPGroup\)](#)
- [Layer 2 Tunnel Protocol Domain Entry \(IL2TPDomainEntry\)](#)
- [Faults and Alarm Correlation](#)
- [L2TP Alarm Configuration Parameters](#)
- [Using Cisco ANA PathTracer to View L2TP Path Information](#)
- [Topology](#)

Layer 2 Tunnel Protocol Interface (IL2TPTunnel)

The following Layer 2 Tunnel Protocol Interface object represents one edge of an L2TP Tunnel. It aggregates multiple Layer 2 Tunnel Protocol Session Entries, which it is bound to by its session table attributes, while being aggregated by a Layer 2 Tunnel Protocol Peer, from which it is created or cloned.

Table 2 *Layer 2 Tunnel Protocol Interface (IL2TPTunnel)*

Attribute Name	Attribute Description
Local and Remote Tunnel Identifications	Local and remote tunnel identifications
Local and Remote Tunnel Names	Local and remote tunnel names
Remote Address	Remote IP address
Control Errors	Control errors count
Last Error Code	Last error code value which causes the tunnel disconnection
Tunnel State	Tunnel state (unknown, idle, connecting, established, disconnecting)
Sessions Count	Current sessions count
Sessions Table	Array of Layer 2 tunnel protocol session entries

Layer 2 Tunnel Protocol Session Entry (IL2TPSessionEntry)

The following Layer 2 Tunnel Protocol Session Entry object represents a session within an L2TP Tunnel. It is primarily accessed by the Layer 2 Tunnel Protocol Interface, in which it is contained.

Table 3 Layer 2 Tunnel Protocol Session Entry (IL2TPSessionEntry)

Attribute Name	Attribute Description
Local and Remote Session Identifications	Local and remote session identifications
Subscriber Name	Subscriber name
Session Type	Session type (unknown, LAC, LNS)
Session State	Session state (unknown, idle, connecting, established, disconnecting)
Input and Output Data Counters	Input and output data octets and packets counters

Layer 2 Tunnel Protocol Peer (IL2TPPeer)

The following Redback's Layer 2 Tunnel Protocol Peer object describes a logical component, aggregating multiple Layer 2 Tunnel Protocol Interfaces with their configuration, to which it is being bound by its Logical Sons attribute. It is primarily being used for managing the creation of L2TP Tunnels.

Table 4 Layer 2 Tunnel Protocol Peer (IL2TPPeer)

Attribute Name	Attribute Description
Local and Peer Addresses	Local and peer IP addresses
Local and Peer Names	Local and peer names
Tunnel Type	Tunnel type (unknown, LAC, LNS)
Tunnel Mode	Tunnel mode (null, static, dynamic)
Maximum and Current Tunnels Counts	Maximum and current tunnels counts
Maximum and Current Sessions Counts	Maximum and current sessions counts
Session Authentication Type	Session authentication type (null, none, simple, challenge)
Tunnel Password	Tunnel password for the authentication phase of the tunnel establishment
RADIUS Identification	Remote Authentication Dial In User Service (RADIUS) identification
Hello Time Interval	Time interval in which hello (keep alive) packets should be sent
Control Errors	Control errors count
Media Type	Underlying media type (null, other, none, UDPLP, Frame Relay, ATM)
Group Identification	Object Identification (OID) of Layer 2 Tunnel Protocol Group (IL2TPGroup)

Table 4 Layer 2 Tunnel Protocol Peer (*IL2TPPeer*)

Attribute Name	Attribute Description
Domains Table	Array of Layer 2 tunnel protocol domain entries
Logical Sons	Array of aggregated Layer 2 tunnel protocol interface

Layer 2 Tunnel Protocol Group (IL2TPGroup)

The following Redback's Layer 2 Tunnel Protocol Group describes a logical component, load balancing multiple Layer 2 Tunnel Protocol Peers, which are being grouped by its Peer List attribute. It is being aggregated or contained by a Traffic Descriptor Container object.

Table 5 Layer 2 Tunnel Protocol Group (*IL2TPGroup*)

Attribute Name	Attribute Description
Group Name	Layer 2 tunnel protocol group name
Tunnel Algorithm	Tunnel algorithm
Dead Time	Dead time
RADIUS Identification	Remote Authentication Dial In User Service (RADIUS) identification
Peers List	Array of Layer 2 tunnel protocol peers
Domains Table	Array of Layer 2 tunnel protocol domain entries

Layer 2 Tunnel Protocol Domain Entry (IL2TPDomainEntry)

The following Redback's Layer 2 Tunnel Protocol Domain Entry describes an Internet Domain, to which its members are allowed to open L2TP Sessions within L2TP Tunnels aggregated by either L2TP Peers or further by L2TP Groups containing this Domain. It is being aggregated or contained by a Traffic Descriptor Container object.

Table 6 Layer 2 Tunnel Protocol Domain Entry (*IL2TPDomainEntry*)

Attribute Name	Attribute Description
Domain Name	Layer 2 tunnel protocol domain name
Attached To Object	Object Identifier (OID) of either object L2TPPeer or L2TPGroup to which this domain is attached

Faults and Alarm Correlation

A summary of the L2TP technology alarms are displayed in the alarm summary table:

Table 7 Alarms Summary

Alarm	Severity	Description	Up Alarm
L2TP Peer is Not Established	Major	The state of a statically configured L2TP tunnel is changed from "established" to anything else. Such a failure may be as the result of a configuration or network problem.	L2TP Peer is Established
L2TP Peer was Removed	Info	A dynamically configured L2TP Tunnel was removed from a device	None
L2TP Sessions Count Exceeded	Major	The current sessions count has exceeded its maximum threshold	L2TP sessions count returned to normal

L2TP Peer Is Not Established/Established

An *L2TP peer is not established* alarm is issued when the state of a statically configured L2TP tunnel is changed from "established" to anything else. Such a failure may be as the result of a configuration or network problem. The *L2TP peer is established* alarm is issued when this problem has been fixed.

L2TP Peer Was Removed

An *L2TP peer was removed* alarm is issued when a dynamically configured L2TP tunnel is removed from a device. This is not issued as a ticket; however it invokes a correlation flow and can be viewed in Cisco ANA EventVision. In addition, it also appears in the Cisco ANA NetworkVision application only if correlated to another alarm, like link or port down.

L2TP Sessions Count Exceeded/Return to Normal

An *L2TP sessions count exceeded* alarm is issued when the current percentage of the number of sessions in the L2TP peer has exceeded the maximum configurable threshold. A *L2TP sessions count return to normal* alarm is issued when the current percentage of the number of sessions has returned to below the configured threshold.

The maximum number of sessions allowed for a single peer is defined by the L2TP peer and L2TP tunnel configuration parameters.

L2TP Alarm Configuration Parameters

This section describes the options that exist to modify the alarm behavior for L2TP by editing the appropriate alarm parameters in the system registry.

Table 8 L2TP Service Alarms

Item	Name	is-correlation-allowed	correlate	is-ticketable	severity
1	L2TP peer not established	true	true	true	MAJOR
2	L2TP peer established	false	false	false	CLEARED
3	L2TP peer is removed	true	true	false	INFO
4	L2TP sessions count exceeded	false	false	true	MAJOR
5	L2TP sessions count return to normal	false	false	false	CLEARED

Table 9 Configuration Parameters - L2TP

Parameter Name	Description	Permitted Values
threshold alarm value	The current sessions count has exceeded its maximum threshold (measured as a percentage)	80
threshold clear value	L2TP sessions count returned to normal (measured as a percentage)	70

**Note**

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

For more information about event and alarm configuration parameters, see the Cisco Active Network Abstraction Fault Management Guide.

Using Cisco ANA PathTracer to View L2TP Path Information

This section describes the Cisco ANA PathTracer for L2TP, including viewing tunnel information. For detailed information about the Cisco ANA PathTracer, see the Cisco Active Network Abstraction NetworkVision User Guide.

Cisco ANA uses VC ID encapsulation information to trace the path from one tunnel interface to another over the network. The Cisco ANA's PathTracer tool enables you to:

- View a path for the defined L2TP session across the network.
- For each network element view the relevant parameters for each interface on all layers along the path.

Layer 2 and Layer 3 L2TP information is displayed in the Cisco ANA PathTracer windows when a path is traced over L2TP tunnels for Redback devices.

Layer 3

The following Layer 3 property that may be displayed in the Layer 3 tab relates specifically to L2TP tunnels:

- Name - The peer name is displayed.

Layer 2

The following Layer 2 properties that may be displayed in the Layer 2 tab relate specifically to L2TP tunnels:

- Encapsulation Type—The encapsulation type, for example, PPPoA.
- Binding Information.
- Binding Status—The binding status, namely, bound or unbound.
- Tunnel Session Count—The number of current sessions.
- Tunnel Remote ID—The remote tunnel identifier.
- Tunnel ID—The local tunnel identifier.
- Tunnel Name—The name of the subscriber and the tunnel ID.
- Session ID—The session identifier.
- Traffic -> L2TPSessionCounters—The number of traffic packets passing through the L2TP tunnel.
- Traffic <- L2TPSessionCounters—The number of traffic packets passing through the L2TP tunnel.
- Containing TPs—The underlying termination points (communication or physical).
- Contained Current CTPs—The bound connection termination points and forwarding component.
- Tunnel Ctl Errors—The number of control errors.
- Tunnel State—The tunnel state, namely, unknown, idle, connecting, established, and disconnecting.
- Session Typ—The session type, namely, unknown, LAC, and LNS.
- Peer Name—The peer name.
- Tunnel Remote IP—The remote IP address of the tunnel.
- Last Error Code—The last error code value which caused the tunnel disconnection.
- Session State—The session state namely, unknown, idle, connecting, established, and disconnecting.
- Remote Session ID—The remote session identifier.

Topology

There is no topology based on L2TP technology in Cisco ANA 3.5.2.

Solaris 10

The recommended operating system to run Cisco ANA 3.5.2 on SUN servers is Solaris 10. Cisco ANA 3.5.2 is compatible with the latest patch release as published by Sun on February 13, 2007. This patch release contains the following (13/02/07) SunOS sh-nv210-279 5.10 Generic_118833-36 sun4u sparc SUNW,Sun-Fire-V210 patches:

Table 10 Sun Patch Release (13/02/07)

118371-07	119574-02	120824-07	122640-05
118560-02	119578-30	120849-04	122660-07
118562-11	119593-01	120900-04	122911-02
118712-13	119757-04	121002-03	123186-02
118731-01	119764-05	121004-03	123256-02
118815-05	119903-02	121012-02	123839-04
118833-36	119981-09	121118-10	124188-02
118872-04	119985-02	121133-02	124204-03
118918-24	119986-03	121229-01	124244-01
118959-03	120061-02	121265-03	124457-01
119042-10	120068-02	121296-01	124630-03
119059-20	120085-01	121308-08	124997-01
119081-25	120272-06	121453-02	119130-32
120292-01	121901-01	119254-06	120329-02
122032-03	119254-34	120469-05	122172-06
119317-01	120719-02	122174-03	



Note

For any later patches distributed by Sun, contact Cisco Professional Services.

Changes from the Last Release

This section includes the following:

- [Cisco ANA Client](#)
- [Beanshell Library](#)
- [IMO Changes from Cisco ANA 3.5.1 to 3.5.2](#)

Cisco ANA Client

The Cisco ANA Client is shipped with JDK 1.4.2_12 which is the required version for the client.

Beanshell Library

Cisco ANA 3.5.2 introduces a new beanshell library.

The previous library would box the primitive parameter with the appropriate object and invoke the method. The new library will give an error message stating that there is no such method with a signature that accept the primitive parameter.

This bug will not be solved.

IMO Changes from Cisco ANA 3.5.1 to 3.5.2

The table below lists the IMO changes that occurred from Cisco ANA 3.5.1 and Cisco ANA 3.5.2.

Table 11 IMO Changes from Cisco ANA 3.5.1 to 3.5.2

IMO Name	Method Name	Status	Old Signature	New Signature
IError	setOriginatorEnum	Signature Change	(int enum)	(int
IL2TPSessionEntry	Inheritance	Different	INE	IConnectionTermin
IManagedElement	Inheritance	Different	INE	IMO
ISoftPropertyAlarm	setTriggerEnum	Signature Change	(int enum)	(int triggerEnum)
IWorkflow	setStateEnum	Signature Change	(int enum)	(int stateEnum)
IL2TPGroupOid	Inheritance	Different	IFWComponentOid	ITrafficDescriptorO
IL2TPTunnelOid	getTunnelName	Removed		
IL2TPTunnelOid	setTunnelName	Removed		
ITunnelContainerO	Enum	Changed	S_TUNNEL_TYPE	S_TUNNEL_TYPE
IAuthenticationRul	getMinPunctuation	Removed		
IAuthenticationRul	setMinPunctuation	Removed		
IAuthenticationRul	getMinDigits	Removed		
IAuthenticationRul	setMinDigits	Removed		
IAuthenticationRul	getMinLowercase	Removed		
IAuthenticationRul	setMinLowercase	Removed		
IAuthenticationRul	getMinUppercase	Removed		
IAuthenticationRul	setMinUppercase	Removed		
IL2TPGroup	Inheritance	Different	IFWComponent	ITrafficDescriptor
IL2TPPeer	getLocalType	Removed		
IL2TPPeer	setLocalType	Removed		
IL2TPPeer	getLocalAddress	Removed		
IL2TPPeer	setLocalAddress	Removed		
IL2TPPeer	getPeerAddress	Removed		
IL2TPPeer	setPeerAddress	Removed		
IL2TPPeer	getTunnelLimit	Removed		
IL2TPPeer	setTunnelLimit	Removed		

Table 11 *IMO Changes from Cisco ANA 3.5.1 to 3.5.2*

IMO Name	Method Name	Status	Old Signature	New Signature
IL2TPPeer	getTunnelCount	Removed		
IL2TPPeer	setTunnelCount	Removed		
IL2TPPeer	getSessionsPerTun	Removed		
IL2TPPeer	setSessionsPerTun	Removed		
IL2TPPeer	getControlWindow	Removed		
IL2TPPeer	setControlWindow	Removed		
IL2TPPeer	getSessionAuthType	Removed		
IL2TPPeer	setSessionAuthType	Removed		
IL2TPPeer	setTunnelNumber	Removed		
IL2TPPeer	getTunnelNumber	Removed		
IL2TPPeer	setSessionNumber	Removed		
IL2TPPeer	getSessionNumber	Removed		
IL2TPPeer	getHostnameAlias	Removed		
IL2TPPeer	setHostnameAlias	Removed		
IL2TPPeer	getConfiguredRemo	Removed		
IL2TPPeer	setConfiguredRemo	Removed		
IL2TPPeer	getLocalIpAddress	Removed		
IL2TPPeer	setLocalIpAddress	Removed		
IL2TPPeer	getLac	Removed		
IL2TPPeer	setLac	Removed		
IL2TPPeer	getLns	Removed		
IL2TPPeer	setLns	Removed		
IL2TPPeer	getStaticMode	Removed		
IL2TPPeer	setStaticMode	Removed		
IL2TPPeer	getMaxTunnel	Removed		
IL2TPPeer	setMaxTunnel	Removed		
IL2TPPeer	getMaxSession	Removed		
IL2TPPeer	setMaxSession	Removed		
IL2TPPeer	setDomain	Signature Change	ITrafficDescriptor	ITrafficDescriptor
IL2TPPeer	setGroup	Signature Change	ITrafficDescriptor	ITrafficDescriptor
IL2TPPeer	setSessionCount	Signature Change	(String str)	(int sessionNum)
IL2TPTunnel	getSessionsData	Removed		
IL2TPTunnel	setSessionsData	Removed		
ISonetSdh	Enum	Changed	S_SPECIFIC_TYP	S_SPECIFIC_TYP
ITrafficDescriptorC	Enum	Changed	S_TABLE_TYPE =	S_TABLE_TYPE =
ICiscoRouterBridge	setSubscriberPolic	Signature Change	(String)	(String)

Table 11 *IMO Changes from Cisco ANA 3.5.1 to 3.5.2*

IMO Name	Method Name	Status	Old Signature	New Signature
IEventList	IMO	Added		
ISystemError	IMO	Added		
IAlcatelEssBridge	IMO	Added		
IEventListOid	IMO	Added		
IL2TPTunnelOid	getTunnelId	Added		
IL2TPTunnelOid	setTunnelId	Added		
IRegEntityOid	setVirtualPath	Added		
IRegEntityOid	getVirtualPath	Added		
ISystemErrorOid	IMO	Added		
IAuthenticationRul	getAllowedConsequ	Added		
IAuthenticationRul	setAllowedConsequ	Added		
IAuthenticationRul	getForbiddenComp	Added		
IAuthenticationRul	setForbiddenComp	Added		
IFRTrafficDescriptor	getCir	Added		
IFRTrafficDescriptor	setCir	Added		
IFRTrafficDescriptor	getLmiProfileId	Added		
IFRTrafficDescriptor	setLmiProfileId	Added		
IFRTrafficDescriptor	getPriority	Added		
IFRTrafficDescriptor	setPriority	Added		
IFRTrafficDescriptor	getXlatFlag	Added		
IFRTrafficDescriptor	setXlatFlag	Added		
IFRTrafficDescriptor	getCRC	Added		
IFRTrafficDescriptor	setCRC	Added		
IL2TPPeer	getTunnType	Added		
IL2TPPeer	setTunnType	Added		
IL2TPPeer	getRemIp	Added		
IL2TPPeer	setRemIp	Added		
IL2TPPeer	getTunnCount	Added		
IL2TPPeer	setTunnCount	Added		
IL2TPPeer	getTunnelMode	Added		
IL2TPPeer	setTunnelMode	Added		
IL2TPPeer	getDomains	Added		
IL2TPPeer	setDomains	Added		
IL2TPPeer	getMedia	Added		
IL2TPPeer	setMedia	Added		
IL2TPPeer	getTunnelPass	Added		

Table 11 *IMO Changes from Cisco ANA 3.5.1 to 3.5.2*

IMO Name	Method Name	Status	Old Signature	New Signature
IL2TPPeer	setTunnelPass	Added		
IL2TPPeer	getHelloTimer	Added		
IL2TPPeer	setHelloTimer	Added		
IL2TPPeer	getTunnelCtlErr	Added		
IL2TPPeer	setTunnelCtlErr	Added		
IL2TPPeer	getRadius	Added		
IL2TPPeer	setRadius	Added		
IL2TPTunnel	getTunnelId	Added		
IL2TPTunnel	setTunnelId	Added		
IL2TPTunnel	getPeerName	Added		
IL2TPTunnel	setPeerName	Added		
IL2TPTunnel	getTunnelRemoteId	Added		
IL2TPTunnel	setTunnelRemoteId	Added		
IL2TPTunnel	getLastErrorCode	Added		
IL2TPTunnel	setLastErrorCode	Added		
IL2TPTunnel	getTunnelSessionC	Added		
IL2TPTunnel	setTunnelSessionC	Added		
IL2TPTunnel	getTunnelCtlErrors	Added		
IL2TPTunnel	setTunnelCtlErrors	Added		
IL2TPTunnel	getSessionsTable	Added		
IL2TPTunnel	setSessionsTable	Added		

Installation Notes

Refer to the Cisco Active Network Abstraction Server's Installation Guide, 3.5.2 and the Cisco Active Network Abstraction Client Installation Guide, 3.5.2.

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 10000 objects (devices, VPNs, VRFs and sites) 12000 links and 10000 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 5000 objects, 6000 links and 5000 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 5000. For a definition of an open ticket, refer to the Cisco ANA Fault Management Guide, 3.5.2. The operator should ensure that tickets are closed on time.

Cisco ANA High Availability

The high availability mechanism will attempt to load an AVM, after it crashes, a maximum of seven times. Thereafter, the high availability mechanism will not try to reload this AVM again.

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

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

Important Notes

Solaris Services and Components

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

Table 12 *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 13 *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	-

Table 13 *Product Services Installed with Cisco ANA (continued)*

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
Sheer_secured	Secured connectivity between gateway and unit	local/sheer_secured /sheer_config	1101	-	-	ssh
webservers	Serves the client webstart and the system troubleshooting tools.	utils/apache/conf/sheer.conf	1310, 1311	-	-	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	-	-	Snmp

Online Help

The online help for Cisco ANA 3.5.2 has been tested using the following browsers:

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

Open Caveats - Cisco ANA, Release 3.5.2

Table 14 Open Caveats - Cisco ANA, Release 3.5.2

Identifier	Title	Impact	Workaround
CSCsd61370	UT-Starcom modeling - missing interface under routing entity.	In the logical inventory of a UT-Starcom device, one or more of the IP interfaces may not be shown.	None.
CSCsd85803	Few traps are coming is generic trap (RTT and BGP).	The traps RTT operation timeout, RTT operation threshold violation, bgpBackwardTransition, bgpEstablished will arrive as generic traps in Cisco ANA EventVision.	None.
CSCse08188	Stinger: VC admin status is missing.	When viewing the VC properties of the Lucent stinger, the admin status is not shown.	None.
CSCsg44987	2 properties are missing in the inventory of Cisco routers.	BQL queries for the Cisco device does not show CPU usage history and FlashDeviceSize.	To view CPU usage one open Cisco ANA NetworkVision. No workaround for the FlashDeviceSize.
CSCsg46860	For Cisco 7206VXR, ATM Traffic Profiles entries missing in ANA 3.5.1 NW.	ATM profiles are not shown in the logical inventory of Cisco 7206VXR.	None.
CSCsg50208	ASAM1000: after card_out and card_in, port has no cross connect table.	The cross connect table is not shown after the card is removed.	Restart the VNE, which will result in the remodelling of the VNE, including the cross connect table.
CSCsg84343	Interface description is not displayed in the routing table.	In the logical inventory of Cisco 12012, the interface description is not available in the routing table.	None.
CSCsg87329	Stinger - Port type, Last change and MAX speed are not displayed.	Some of the port properties, like type, last changed and max speed are not displayed in Cisco ANA NetworkVision.	None.
CSCsh42902	Verification topology doesn't work on Lucent trunk	Eventhough the link is removed from the devices (they are no longer connected in the network) the link is still displayed Cisco ANA NetworkVision.	Stop one of the VNEs and restart it.
CSCsh46315	ECI : Values under MCR is not displayed.	The MCR column in the ATM traffic profile is empty.	None.

Table 14 *Open Caveats - Cisco ANA, Release 3.5.2 (continued)*

Identifier	Title	Impact	Workaround
CSCsh47093	Port connector of card type wsx-6524mmmt should be fiber.	The port connector of module wsx-6524mmmt is shown as RJ45 instead of being shown as a fiber.	None.
CSCsh51454	When creating a Soft Property there is a possibility to override system property	When creating a soft property there is a possibility to override the system property by giving the soft property the same name as the system property. The registration will not be overridden, just the property name, which will cause the property to change values whenever one of the registrations (system or soft) pools.	Check in the registry if the property name is already defined before creating the soft property.
CSCsh53017	AVM properties are missing when an AVM down.	<p>If an AVM is down it does not show the devices in the right pane allocated to the AVM. It stays in "Please wait ..." mode and does not timeout.</p> <p>After the AVM goes into the "Please wait ..." state, you cannot see the content in the right pane for any other AVM or unit. It freezes.</p> <p>If you do not touch the down AVM, the other AVMs in any Unit are available for navigation.</p>	Restart the client.
CSCsh54780	Alcatel Mini RAM-480:DS1 port Clocking shown as unknown.	In the physical inventory of the Alcatel miniram device, when choosing a port, the port clocking property is undefined.	None.
CSCsh57305	Client waits for server response if a server BQL response fails.	The Client does not time out when waiting for BQL response.	Restart the client.
CSCsh64220	Cisco 4507- Hardware version is missing in the GUI.	In the physical inventory of the Cisco 4507 device, when choosing a card, the hardware version is missing.	None.

Table 14 Open Caveats - Cisco ANA, Release 3.5.2 (continued)

Identifier	Title	Impact	Workaround
CSCsh69252	VNEs lost their connection with the hierarchy nodes.	<p>When moving a large number of VNEs (150 were tested) from one AVM to another in a different unit, all of the VNEs lost their connection to their hierarchy nodes (the icons of the VNEs appear in Cisco ANA NetworkVision as blue boxes).</p> <p>Once this happens, these devices cannot be managed by the system.</p>	All of the VNEs should be shutdown prior to moving a large number of them to another AVM.
CSCsh71005	NTP doesn't work.	<p>NTP is a process that should sync the date and time between the machines in the setup (gateway and units).</p> <p>This bug indicates a problem in this sync mechanism, which can cause sync problems in the system.</p> <p>For example, a problem with the events time stamp can cause event correlation to fail and to DB mess.</p>	<p>After installation, the system time should be set manually in all of the units.</p> <p>The difference between the clocks on all of the units should not be more than 4 minutes.</p> <p>Once this is done NTP will sync the machines precisely.</p>
CSCsh74067	Changing date/time causes transport disconnection.	When the date is changed in a unit, all of the AVMs in the unit become unreachable (including the unit itself).	<p>The time must not be changed while the product is up and running.</p> <p>If the date or time needs to be adjusted, the entire Cisco ANA product needs to be shutdown prior to making this change.</p>
CSCsh82831	BA40: "Customer ID" is missing on ADSL ports.	In the physical inventory of the BA 40 device, when choosing a port, the customer ID is not shown.	None.
CSCsh85650	Cisco CRS-1 adding support for new interface type dwdm.	Dense Wavelength Division Multiplexing (DWDM) optical technology is not supported, therefore no information relating to these interfaces is shown.	None.

Table 14 Open Caveats - Cisco ANA, Release 3.5.2 (continued)

Identifier	Title	Impact	Workaround
CSCsh96756	Incorrect cross connect in frame-relay cloud	Missing entries in IP interface multi-point table prevent flows from running and stopping properly in the VNE model.	None.
CSCsi03708	Problems with Parser.pm and Cisco.pm residing in the “monitoring” directories.	The scripts Parser.pm and Cisco.pm located under the ./Main/scripts/monitoring/RPC/XML may not work properly.	<p>Post installation—Copy the files from ./Main/RPC/XML to ./Main/scripts/monitoring/RPC/XML</p> <ol style="list-style-type: none"> 1. Login as user sheer 2. cd ~ 3. cp ./Main/RPC/XML/Parser.pm ./Main/scripts/monitoring/RPC/XML/Parser.pm 4. cp ./Main/RPC/XML/Cisco.pm ./Main/scripts/monitoring/RPC/XML/Cisco.pm

Resolved Caveats - Cisco ANA, Release 3.5.1

Table 15 Resolved Caveats - Cisco ANA, Release 3.5.1

Identifier	Summary	Explanation
CSCsd34847	Missing link between the ASAM <-> CBX	Fixed.
CSCsg26210	New Beanshell library not compliant with previous Beanshell scripts	<p>A workaround for this problem is to migrate the beanshell scripts so that they use manual boxing and do not rely on auto-boxing. For example:</p> <ul style="list-style-type: none"> • <code>thisTask.getAttribute("Attr", true)</code>—This script line relies on beanshell to autobox the Boolean primitive and will fail in Cisco ANA 3.5.2. • <code>thisTask.getAttribute("Attr", new Boolean(true))</code>—This script line does manual boxing, and will execute successfully in Cisco ANA 3.5.2.
CSCsd59865	VRF is not displayed in the map as deleted eventhough it was deleted.	Fixed.
CSCse70636	System installation is not verifying that server swap size is at least 2xMemory size	Fixed.

Table 15 **Resolved Caveats - Cisco ANA, Release 3.5.1**

Identifier	Summary	Explanation
CSCse78912	AVM 100 does not start on gateway.	Fixed.
CSCse85009	Product Device-iP_VPN: Sheer Gateway receives no response for UtStarcom VNE.	Fixed.
CSCse97220	Drop messages in avm 100	Fixed.
CSCsf05415	Can't delete multiple WorkFlow rows	Fixed.
CSCsf13264	Publishing fails in high scale.	Fixed.
CSCsf31904	Information in Business tab is missing.	Fixed.
CSCsg08522	General Error Dialog when removing tickets twice	Fixed.
CSCsg26028	Unusable gateway when there is a duplicate entry/key in alarm-types.xml	Fixed.
CSCsg26227	Deadlock in Workflow Editor	Fixed.
CSCsg28927	Problem with load topology persistency on VNE connected to the Cloud.	Fixed.
CSCsg29273	Acknowledge Alarm message in the history tab should be formatted.	Fixed.
CSCsg36976	Sprint POC - modeling of sub-sub-module in GSR.	Fixed.
CSCsg39235	A workflow fails if there is no output.	Fixed.
CSCsg45530	Workflow editor fails to run BQL tasks - GUI Issue	Fixed.

Open Caveats - Cisco ANA, Release 3.5.1

transfer this section to table 3 if still open

Table 16 *Open Caveats - Cisco ANA, Release 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.
CSCsd61127	Able to add a VNE in UP state to an AVM 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
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.

Table 16 Open Caveats - Cisco ANA, Release 3.5.1 (continued)

Identifier	Title	Impact	Workaround
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 AVN that is created (including AVN0, AVN66 and AVN99). The operating system memory is not accounted for (included) either.
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 - Cisco ANA, Release 3.5.

Table 17 Resolved Caveats - Cisco ANA, Release 3.5

Identifier	Summary	Explanation
CSCsd61046	Limited support of L2TP.	Fixed. Duplicate of CSCse01359.

Open Caveats - Release Cisco ANA 3.5

Table 18 Open Caveats - Release Cisco ANA 3.5

Identifier	Title	Impact	Workaround
CSCsd63693	IMA is not supported.	IMA aggregations 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 3.5.2 documentation set.

Cisco Active Network Abstraction Administrator Guide

In Cisco ANA Manage, the VNE Properties dialog box is used to view and edit the properties of a VNE in a unit, for example, the status and Telnet settings. The Telnet/SSH tab in the VNE Properties dialog box now supports masking of password information.

The Telnet/SSH Tab is described in the Cisco ANA Administrator Guide, Chapter 6, Defining VNEs, Telnet/SSH Tab.

In the Telnet/SSH Tab in the VNE Properties dialog box, choose Password from the Prompt drop-down menu, or enter the word 'password' in the prompt field. When you enter the password in the Run field, the password will be hidden. See [Figure 2](#).



Note

If you enter any other variant in the Prompt field, the password will show as clear text in the table and Run text field.

Figure 2 Telnet/SSH Tab

The screenshot shows the 'cmp-3550-3 - Properties' dialog box with the 'Telnet / SSH' tab selected. The 'Enable' checkbox is checked. The 'Protocol' is set to 'Telnet' and the 'Port' is 23. A table with two columns, 'Prompt' and 'Run', contains the following entries:

Prompt	Run
Password:	***
cmp-3550-3>	en
Password:	***
cmp-3550-3#	

Below the table, the 'Prompt' dropdown is set to 'Password' and the 'Run' field contains '***'. There are 'Add' and 'Remove' buttons next to the 'Run' field. At the bottom of the dialog, there are fields for 'User Name', 'Password', 'Cipher' (set to 'DES'), and 'Authentication' (set to 'Password'). The 'OK', 'Cancel', and 'Apply' buttons are at the bottom right. The status bar at the very bottom shows 'Memory: 7%' and 'Connected'.

Workflow User Guide

In Chapter 2, Working With the Task Library, Execute BQL Task, the following note will be added after Step 6:



Note

The Command CID that is to be executed by the BQL Task must not register for notifications. The BQL task process only the initial command response and does not process any later notifications.

In Chapter 2, Gateway Workflow Commands and Operations, Running a Workflow, the following changes will be made:

In the RunWorkflow BQL command CID, the “workflowAttributes” parameters were changed to support new attribute of types other than String.

In the following BQL CID example the attribute types are in **bold**, and the attribute names and values are in **blue**:

```
<?xml version="1.0" encoding="UTF-8"?>
<command name="RunWorkflow">
  <param name="templateOid">
    <value>{ [WorkflowTemplate (Name=bql.template)] }</value>
  </param>
  <param name="workflowAttributes">
    <value>
      <IWorkflowStringAttribute>
        <ID type="Oid">{ [WorkflowAttribute (Name=StringAtt)] }</ID>
        <Value type="String">root</Value>
      </IWorkflowStringAttribute>
      <IWorkflowIntegerAttribute>
        <ID type="Oid">{ [WorkflowAttribute (Name=IntegerAtt)] }</ID>
        <Value type="Integer">5</Value>
      </IWorkflowIntegerAttribute>
      <IWorkflowBooleanAttribute>
        <ID type="Oid">{ [WorkflowAttribute (Name=BooleanAtt)] }</ID>
        <Value type="Boolean">true</Value>
      </IWorkflowBooleanAttribute>
      <IWorkflowLongAttribute>
        <ID type="Oid">{ [WorkflowAttribute (Name=LongAtt)] }</ID>
        <Value type="Long">12345</Value>
      </IWorkflowLongAttribute>
      <IWorkflowDoubleAttribute>
        <ID type="Oid">{ [WorkflowAttribute (Name=DoubleAtt)] }</ID>
        <Value type="Double">12345</Value>
      </IWorkflowDoubleAttribute>
    </value>
  </param>
  <param name="preview">
    <value>false</value>
  </param>
</command>
```



Note

To maintain backward compatibility with existing integrations, the system can be configured to support the previous RunWorkflow CID string by overriding the registry entry. Set the registry entry, **workflowavm/services/workflow/use-workflow-string-param-casting**, to “true”. The default setting is “false”.

Related Documentation

User Guides

Cisco Active Network Abstraction NetworkVision User Guide, 3.5.2

Cisco Active Network Abstraction EventVision User Guide, 3.5.2

Cisco Active Network Abstraction MPLS User Guide, 3.5.2

Cisco Active Network Abstraction Fault Management User Guide, 3.5.2

Administrator Guides

Cisco Active Network Abstraction Servers Installation Guide, 3.5.2

Cisco Active Network Abstraction Client Installation Guide, 3.5.2

Cisco Active Network Abstraction Administrator Guide, 3.5.2

Cisco Active Network Abstraction Error Messages, 3.5.2

Cisco Active Network Abstraction Shell User Guide, 3.5.2

Cisco Active Network Abstraction High Availability User Guide, 3.5.2

Developer Guides

Cisco Active Network Abstraction Customization User Guide, 3.5.2

Cisco Active Network Abstraction Command Builder User Guide, 3.5.2

Cisco Active Network Abstraction Workflow User Guide, 3.5.2

Cisco Active Network Abstraction BQL User Guide, 3.5.2

Cisco Active Network Abstraction Registry Editor User Guide, 3.5.2

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 Support 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 these announcements 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. Registered users can access the tool at this URL:

<http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en>

To register as a Cisco.com user, go to this URL:

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

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Support 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 Support Website

The Cisco Support 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/en/US/support/index.html>

Access to all tools on the Cisco Support 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**

Before you submit a request for service online or by phone, use the **Cisco Product Identification Tool** to locate your product serial number. You can access this tool from the Cisco Support website by clicking the **Get 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. After using the Search box on the Cisco.com home page, click the **Advanced Search** link next to the Search box on the resulting page 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 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, 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/abtnicd/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.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, 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, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, 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. (0711R)

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.

© 1999-2007 Cisco Systems, Inc. All rights reserved.

