CHAPTER 1

Cisco ANA Client Overview

Cisco ANA provides a suite of GUI tools that offer an intuitive interface for managing the network and services, and for performing required system administration activities. The Cisco ANA client application suite comprises Cisco ANA NetworkVision, Cisco ANA EventVision, and Cisco ANA Manage.

The following topics provide an introduction to Cisco ANA terminology and client applications:

Note For information about the Cisco ANA Manage application, see the *Cisco Active Network Abstraction 3.7.1 Administrator Guide*.

Basic Cisco ANA Terminology

Table 1-1 provides a brief explanation of the terms used in the Cisco ANA clients and documentation.

Table 1-1 Definitions

Term	Description
aggregation, aggregated node	A user-defined collection of network elements. For example, an aggregation can contain devices, links, VPNs, and other aggregations. In Cisco ANA NetworkVision maps, aggregations are called aggregated nodes.
alarm	Sequence of event notifications that share the same source, cause, or fault. For example, if a single port goes up and then down, these two events in a related sequence may result in a single alarm. An alarm is stateful and is opened when a fault is first detected. Event notifications may be added to the alarm, and it is archived when it is fixed.

Table 1-1 Definitions (continued)

Term	Description
association	A relationship between the following types of network elements: • A logical (protocol-oriented) network element and a physical network element • A logical network element and another logical network element • An existing association and anything else An example for a VPN would be an association between the physical IP interface and Virtual Routing and Forwarding (VRF) table, which is the associated routing table. An association is not considered a topological link.
business element	Construction or organization of certain network elements and their properties into a logical entity, to provide the ability to track them in a way that makes sense from a business perspective. A virtual private network (VPN) is a business element, which represents a set of interconnected sites that form a single network over a public network. Cisco ANA organizes the business elements in a way that creates a containment hierarchy that reflects the VPN structure.
business tag	A string that is meaningful to the business, and that can be used to label a component of a network element for use in Cisco ANA screens and reports. There are three types of business tags: subscriber, provider, and label. Business tags are stored in the Cisco ANA gateway database.
event	In the context of network management, a discrete activity that occurred at a specific point in time.
link	A physical or logical connection between: • Two devices in the network • A device and an aggregation • Two aggregations
logical link	An association between two network elements (based on a chain of physical links between the elements); for example, a tunnel.
managed element	A network element that is managed by Cisco ANA; for example, a device, cloud, or Internet Control Message Protocol (ICMP) VNE.
network element (NE)	Any physical component or device in the network that can be managed through an IP address.
physical link	A link between physical network objects; for example, a connection between two physical ports.
provider	The party providing a service.
subscriber	The party receiving a service.

Table 1-1 Definitions (continued)

Term	Description
ticket	Object that represents an attention-worthy root alarm whose type is marked in the registry as "ticketable." A ticket has the same type as the root alarm it represents, and it has a status, which represents the entire correlation tree. A ticket can be acknowledged by the user. Both Cisco ANA NetworkVision and Cisco ANA EventVision display tickets and allow you to navigate down to view the consequent alarm hierarchy. From an operator's point of view, a fault is always represented by a complete ticket. Operations such as Acknowledge or Remove are applied to the whole ticket.
virtual cloud or unmanaged network	Network, or part of a network, that is not managed by Cisco ANA. An unmanaged network is often represented in network diagrams by a cloud symbol or image.
VLAN	virtual local-area network (LAN). Group of devices on one or more LANs that are configured (using management software) so that they can communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments. Because VLANs are based on logical instead of physical connections, they are extremely flexible.
VPN	Virtual Private Network. Enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another. A VPN uses *tunneling* to encrypt all information at the IP level.

Cisco ANA Security: Permissions, Roles, and Scopes

Cisco ANA provides enhanced security when working with and managing the Cisco ANA system. Users are assigned permission levels for an operational scope, enabling them to perform only the functions assigned to the scope and defined security level. A user can be assigned more than one security level.

Permission

The user's ability to perform certain tasks. There are two types of permissions: default and NE-related.

- Default—Applies only to the activities that are related to GUI functionality, and not the activities related to network elements. For example, a user with the default permission Viewer can view maps and the device list. For more information, see the *Cisco Active Network Abstraction 3.7.1 Administrator Guide*.
- NE-Related—Enables the administrator to group a collection of managed network elements (in Cisco ANA Manage) to allow the user to view and manage the NEs based on the user's role or permission. After the user is allocated a scope (list of network elements) and a role, the user can then perform various activities on the network elements, such as managing alarms in Cisco ANA NetworkVision. For more information, see the *Cisco Active Network Abstraction 3.7.1 Administrator Guide*.

Roles

Cisco ANA implements a security engine that combines a role-based security mechanism that is applied on scopes of network elements granted per user. The system supports:

- User account creation
- Network element scope definition
- A set of five predefined roles for security and access control that allow different system functions. The roles, listed from the lowest security level to the highest security level, are:
  - Viewer—Have read-only access to the network and to nonprivileged system functions.
  - Operator—Configure business tags and perform most day-to-day operations.
  - Operator Plus—Fully control alarm life cycle and create maps.
  - Configurator—Activate services and configure the network.
  - Administrator—Manage the system configuration and security.

Note Viewer is the lowest security level, and Administrator is the highest. A user with a higher security level can perform all the Cisco ANA functions assigned to a user with a lower security level.

Each user is assigned a permission level for an operational scope, which enables the user to perform certain tasks. Every user has a private username and password. A user can log in from any workstation with their own set of permissions and operational scope. When a user does not have the required permission level to perform a function, the appropriate menu option or button is disabled.

The administrator is responsible for defining the types of activities that the user can view and perform using Cisco ANA Manage. For more information about user security and defining operational scopes, see the *Cisco Active Network Abstraction 3.7.1 Administrator Guide*.

A user's role (their default permissions) applies only to the activities that are related to GUI functionality, not the activities related to NEs (which are controlled by scopes). Default permissions control Cisco ANA functions.

Scopes

A scope is a named collection of managed network elements that have been grouped together to allow a user to view or manage the network elements, based on their access role. Grouping can be based on geographical location, network element type (such as DSLAM, router, or software), network element category (such as access or core), or any other division according to the network administrator's requirements.

For example, using Cisco ANA NetworkVision, a user who has been assigned a scope can view or manage the NEs within this scope, according to the role assigned to the user for that scope. The user cannot view any information regarding NEs that are outside their scope, including basic properties, inventory, and alarms.

Cisco ANA NetworkVision

Cisco ANA NetworkVision is the main GUI application used to visualize the network through network and service maps, to view device physical and logical inventories and connectivity, and to manage device configuration and software images. It provides total visibility for multiple-tier, multiple-technology networks, and supports fault and configuration functionality. The highly optimized, customizable GUIs enable constant, system-wide surveillance of the network and service states, down to the node level.

Cisco ANA NetworkVision supports the creation of multiple network maps to represent specific network views. Views can cover specific network segments, customer networks, or any other mix of network elements desired. Once the maps have been created, they are available for all connecting clients (with support for fine-grained access privileges).

Cisco ANA NetworkVision enables you to:

- View network inventory and multiple-layer connectivity.
- Troubleshoot, monitor, and manage network elements (NEs).
- Model and view network maps, maintaining up-to-date topological information on device connections, traffic, and routes.

Cisco ANA NetworkVision maps based on Cisco ANA's representation of VNEs provide a graphic display of active faults and alarms, and serve as an easy access point for activation of services. Cisco ANA provides rich functionality for displaying and managing network maps by providing:

- Multiple concurrent maps per user.
- Easily customizable hierarchy of nested submaps, aggregations, and business tags with easy navigation up and down the hierarchy.
- Dual views of the network in a hierarchical tree, as well as in topological maps, including all network connections.
- NEs and links using color cues and graphic symbols to indicate status and alarms.
- Mouse point-and-click drill-down from every NE (either from the tree or map), providing detailed internal physical and logical inventory information.

For details on using Cisco ANA NetworkVision when working with specific technologies, see the following topics:

- Carrier Ethernet services—Chapter 12, "Monitoring Carrier Ethernet Services"
- Carrier Grade NAT properties—Chapter 13, "Monitoring Carrier Grade NAT Properties"
- Dense wavelength division multiplexing (DWDM) services—Chapter 14, "Monitoring DWDM Properties"
- Ethernet Operations, Administration, and Maintenance (E-OAM) tool properties—Chapter 15, "Viewing Ethernet Operations, Administration, and Maintenance Tool Properties"
- IPv6 and 6VPE technologies—Chapter 16, "IPv6 and IPv6 VPN over MPLS"
- Multiprotocol Label Switching (MPLS) services—Chapter 17, "Monitoring MPLS Services"
- Mobile Transport over Packet services—Chapter 18, "Monitoring MToP Services"

Cisco ANA NetworkVision is also the launch point for:

- Cisco ANA PathTracer
- Cisco ANA Soft Properties Manager
- Cisco ANA Command Builder
- Cisco ANA Report Manager
- Cisco ANA Configuration and Image Management
- Cisco ANA Network Service Activation

Cisco ANA PathTracer

Cisco ANA PathTracer enables you to perform end-to-end route tracing with informative performance information displayed simultaneously for the multiple networking layers. Upon receiving a path's starting point and end point, Cisco ANA PathTracer visually traces the route through the network. For more information about Cisco ANA PathTracer, see Chapter 11, "Using Cisco ANA PathTracer to Diagnose Problems."

Cisco ANA Soft Properties Manager

The Cisco ANA Soft Properties Manager enables you to manage soft properties and threshold-crossing alarms (TCAs).

The Cisco ANA Soft Properties Manager allows you to extend the set of supported properties for each NE by adding soft properties to the VNEs. These properties extend the Cisco ANA Information Model Object (IMO) and are available through the client GUI as well as through the Broadband Query Language (BQL) API.

Soft properties are retrieved from the NE using Simple Network Management Protocol (SNMP), Telnet, Secure Shell Protocol (SSH), or Transaction Language One (TL-1).

In addition, alarm thresholding enables you to constantly monitor selected properties and generate an alarm each time they cross a user-defined threshold or violate a condition.

The Cisco ANA Soft Properties Manager tool is typically used by integrators or other users who want to manage the soft properties and TCAs that are executed within the Cisco ANA platform.

For more information on the Cisco ANA Soft Properties Manager, see the *Cisco Active Network Abstraction 3.7.1 Customization User Guide*.

For more information about using BQL with Cisco ANA, see the *Cisco Active Network Abstraction 3.7.1 Integration Developer Guide.*

Cisco ANA Command Builder

The Cisco ANA Command Builder enables you to execute a programmable sequence of SNMP or Telnet command lines. These command lines can include data properties taken from the Cisco ANA information model (built-in) or user-defined input parameters entered during runtime.

The Cisco ANA Command Builder is launched from a managed element (Cisco ANA-modeled VNE) such as a port, typically from the Cisco ANA NetworkVision inventory window. The managed element is then used to develop and test the command. Once the command has been completed, you can publish it and attach it to a wider scope of managed elements.

For more information on the Cisco ANA Command Builder, see the *Cisco Active Network Abstraction 3.7.1 Customization User Guide*.

Cisco ANA Report Manager

The Cisco ANA Report Manager enables you to generate, customize, view, and export a variety of reports about events, traps, tickets, syslogs, software versions, and devices. The Report Manager, available from Cisco ANA Manage, Cisco ANA NetworkVision, and Cisco ANA EventVision, provides out-of-the-box reports for events and inventory.

The Report Manager enables you to:

- Produce reports on demand.
- Save generated reports in PDF, CSV, HTML, XLS, or XML format.
- Customize reports for your environment.
- Generate reports for the nonactionable events that are not displayed in Cisco ANA EventVision.

For information about reports and Report Manager, see Chapter 10, "Working with Reports."

You can also retrieve reports using BQL. For more information, see the *Cisco Active Network Abstraction 3.7.1 Integration Developer Guide.*

Cisco ANA Configuration and Image Management

Cisco ANA Configuration and Image Management provides tools that allow you to manage the software and device configuration changes that are made to devices in your network. Device configuration management tools are provided by the Configuration Management (CM) function, and software image management tools are provided by the Network Element Image Management (NEIM) function.

For more information on the Cisco ANA Configuration and Image Management, see the *Cisco Active Network Abstraction 3.7.1 Configuration and Image Management User and Administrator Guide*.

Cisco ANA Network Service Activation

Cisco ANA Network Service Activation (NSA) is a Cisco ANA service activation extension for users wanting to deploy Carrier Ethernet, IP Radio Access Network (RAN), and Mobile Transport over Pseudowire (MToP) services using a service activation wizard launched from the Cisco ANA NetworkVision GUI. Cisco ANA NSA provides:

- A predefined collection of service activation wizards, workflows, and scripts that allow you to begin activating services on Cisco network elements after Cisco ANA NSA is installed.
- The ability for service designers, network planners, and service integrators to customize the wizards and workflows to address service activation needs not provided in the delivered Cisco ANA NSA package.

Cisco ANA NSA provides a visual mechanism for end-to-end service activation on network elements. In addition, Cisco ANA NSA open APIs allow it to be integrated with northbound provisioning systems. Cisco ANA NSA therefore provides a GUI-based service activation solution that can also be integrated into existing operational support system (OSS) environments.

For more information about Cisco ANA NSA, see the *Cisco Active Network Abstraction Network Service Activation 1.1 User Guide*.

Cisco ANA EventVision

Cisco ANA EventVision is the interface used by administrators for viewing system events and tickets that are generated within the Cisco ANA system.

Cisco ANA EventVision is a GUI application that serves as a browser for viewing and retrieving detailed information about the different types of system events and tickets that are generated. Monitoring with Cisco ANA EventVision helps predict and identify the sources of system problems, which in turn assists in preventing future problems.

You can configure Cisco ANA EventVision to display the following information:

- Number of events per page.
- Number of events to be exported to a file.
- Previous dated events (in weeks).
- Filter options.
- The information that appears in Cisco ANA EventVision tabs, such as the Audit tab.

System managers or administrators periodically review and manage the events list using Cisco ANA EventVision. In addition, when an event occurs in the Cisco ANA system, the details become available in Cisco ANA EventVision.

All administrator activities in Cisco ANA Manage are logged and available in Cisco ANA EventVision. For more information on Cisco ANA Manage, see the *Cisco Active Network Abstraction 3.7.1 Administrator Guide*.