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 sections provide an introduction to Cisco ANA terminology and client applications:

- Basic Cisco ANA Terminology, page 1-1—Describes the terms used throughout the Cisco ANA clients and documentation.
- Cisco ANA Security: Permissions, Roles, and Scopes, page 1-3—Describes how Cisco ANA functions and device access are controlled by assigning users specific roles and scopes.
- Cisco ANA NetworkVision, page 1-5—Describes Cisco ANA NetworkVision, including the Cisco ANA PathTracer, Cisco ANA Soft Properties Manager, and the Cisco ANA Command Builder.
- Cisco ANA EventVision, page 1-6—Describes Cisco ANA EventVision, including a description of event types and categories.

Note For information about the Cisco ANA Manage application, see the *Cisco Active Network Abstraction 3.6.6 Administrator Guide*.

Basic Cisco ANA Terminology

This section provides a brief explanation of the terms used in the Cisco ANA clients and documentation.

Table 1 Definitions

Term	Description
event	An event is a representation of a distinct incident occurring at a specific point in time, such as port status change, connectivity loss between protocol processes on peer routers, device reset, device unreachable by management station.
alarm	An alarm represents a scenario which involves a fault in the network, the managed element, or the management system. An alarm is characterized by a sequence of related events, such as port-down and port-up.

Table 1 Definitions (continued)

Term	Description
ticket	A ticket represents the complete hierarchy of correlated alarms representing a single specific fault scenario. A ticket points to the root cause alarm that is the top-most alarm in the correlation hierarchy. The attributes of the ticket, such as short description, are derived from the root cause alarm. Both Cisco ANA NetworkVision and Cisco ANA EventVision display tickets and allow drilling 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.
severity propagation	The network objects' calculated status is propagated from the source/children (the network element component) to the final destination (the network element and tree) via defined relationships.
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.
physical element	A user-named physical component/device existing in the network.
logical element	A user-named logical component; for example, a routing table.
business element	A mapping of service-related information to a network resource. This mapping is achieved using a business element that is a wrapper to a network element or service. 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.
managed element	Anything managed by the system, usually a component managed by the VNE; for example, a device, cloud, ICMP VNE.
link	A physical or logical link between: • Two devices in the network • A device and an aggregation • Two aggregations
physical link	A link between physical network objects; for example, a connection between two physical ports.
logical link	A service-based link between two logical elements (based on a chain of physical elements); for example, a tunnel.

Table 1 Definitions (continued)

Term	Description
business link	An *association* (as opposed to a link) between the following types of network elements: • A logical (protocol-oriented configuration) network element and a physical network element • A logical network element and another logical network element • A business link and anything else An example for a VPN would be an association between the physical IP interface and VRF (which is the associated routing table). A business link is not considered a topological link.
device/network element (NE)	A user-named physical component/device existing in the network.
device/network element components	A component of a network element; for example, a port, routing table and so on.
network object	Network objects include network element components, network elements and links.
virtual cloud/ unmanaged network	Virtual clouds are used for representing unmanaged network segments and are displayed as a cloud. Cisco ANA establishes if network problems emanate from the unmanaged network (the cloud).
VPN	The VPN is a business element, which represents a set of interconnected sites forming a single virtual private network over a public network.
business tag	A business tag is a record that points to a network object. Each business tag has a key field, which is a unique identifier for the entity and its name. There are three types of tags: subscriber, provider, and label. Business tags are stored in the Cisco ANA gateway database.
provider	The party providing the service.
subscriber	The party receiving the service.

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, which enable 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—The default permission only applies to the activities that are related to GUI functionality, 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 3.6.6 Administrator Guide*.

- Network Element—The NE-related permission enables the administrator to group a collection of managed network elements together (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 3.6.6 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 accounts creation, multiple network element scope definition, and a set of five predefined roles for security and access control to allow different system functions (listed from the lower to the higher security level):

- 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 the user's 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 3.6.6 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 for Cisco ANA. It is a surveillance tool providing total visibility for multivendor, multitier, multitechnology networks. It also 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 in order 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 multilayer 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.

The Cisco ANA NetworkVision maps based on Cisco ANA's representation of Virtual Network Elements (VNEs) provides a graphic display of active faults and alarms and serves as an easy access point for activation of services. Cisco ANA provides rich functionality for displaying and managing the 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.
- Every NE (either from the tree or map) allows mouse point-and-click drill-down, providing detailed internal physical and logical inventory information.

For specific details on using Cisco ANA NetworkVision when working with MPLS VPN service network maps, see the *Cisco Active Network Abstraction 3.6.6 MPLS User Guide*.

Cisco ANA NetworkVision is also the launch point for Cisco ANA PathTracer, Cisco ANA Soft Properties Manager, and Cisco ANA Command Builder, which are described as follows.

Cisco ANA PathTracer

Cisco ANA PathTracer enables end-to-end route tracing to be performed with informative performance information displayed simultaneously for the multiple networking layers. Upon receiving a path's start and endpoint, Cisco ANA PathTracer visually traces the route through the network. For more information about Cisco ANA PathTracer, see Chapter 9, "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 SNMP, Telnet/SSH, or TL-1.

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

The Cisco ANA Soft Properties Manager tool is typically used by integrators and any other users who want to manage the soft properties and threshold-crossing alarms (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 3.6.6 Customization User Guide*.

Cisco ANA Command Builder

The Cisco ANA Command Builder enables you to execute a programmable sequence of SNMP or Telnet command lines. These commands can include data properties taken from the Cisco ANA information model (built-in), as well as 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, it can be published and attached to a wider scope of managed elements.

For more information on the Cisco ANA Command Builder, see the *Cisco Active Network Abstraction 3.6.6 Customization User Guide*.

Cisco ANA EventVision

Cisco ANA EventVision is the intuitive 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 (default is 50).
- Number of events to be exported to a file.
- Display previous dated events (in weeks).
- Filter options.
- What information 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 3.6.6 Administrator Guide*.