CHAPTER 1

Introducing Cisco ANA

This chapter describes the Cisco Active Network Abstraction (ANA) platform and architecture. In addition, it provides a brief explanation of the terms used throughout this guide. The Cisco ANA Manage maintenance application is part of an overall Cisco solution; therefore, in order to better understand the Cisco ANA Manage environment, a brief overview of Cisco ANA is required.

- Introduction—Provides an overview of the Cisco ANA, its platform architecture and functional blocks.
- Cisco ANA Components—Describes the Cisco ANA system's key components.
- Cisco ANA Manage—Describes how Cisco ANA Manage serves as a tool to manage the Cisco ANA, which enables the addition, removal and modification of Cisco ANA information.
- Additional Concepts and Terms—Explains any additional terms used within Cisco ANA Manage and this guide.
- Conventions Used In This Guide—Describes the conventions used in this guide. In addition, it provides a list of related documentation.

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

Introduction

Cisco ANA is a carrier-class network management platform, designed to serve as an active mediation layer between the operation and network layers. It provides a set of easy-to-use applications as well as well-defined APIs for Operation Support Systems (OSS), enabling carriers and service providers to efficiently respond to the constant market demand for new, reliable and more sophisticated services, while hiding the complexity of large, multivendor, mixed technology networks.

Cisco ANA provides solutions for diverse network environments and applications. It offers an integrated network and service auto-discovery for network modeling, intelligent fault analysis, and a highly flexible network configuration and activation engine.This enables fully correlated management of global scale networks supporting millions of subscribers and customers.

Cisco ANA is a network management solution that provides a fully integrated service-oriented solution offering:

- Multivendor, hybrid device support.
- Mixed technology (IP, VPN, MPLS, Ethernet, ATM, DSL).
- Multifunction (network discovery, fault, activation and configuration).
- Vertical integration with multiple OSS/BSS applications.

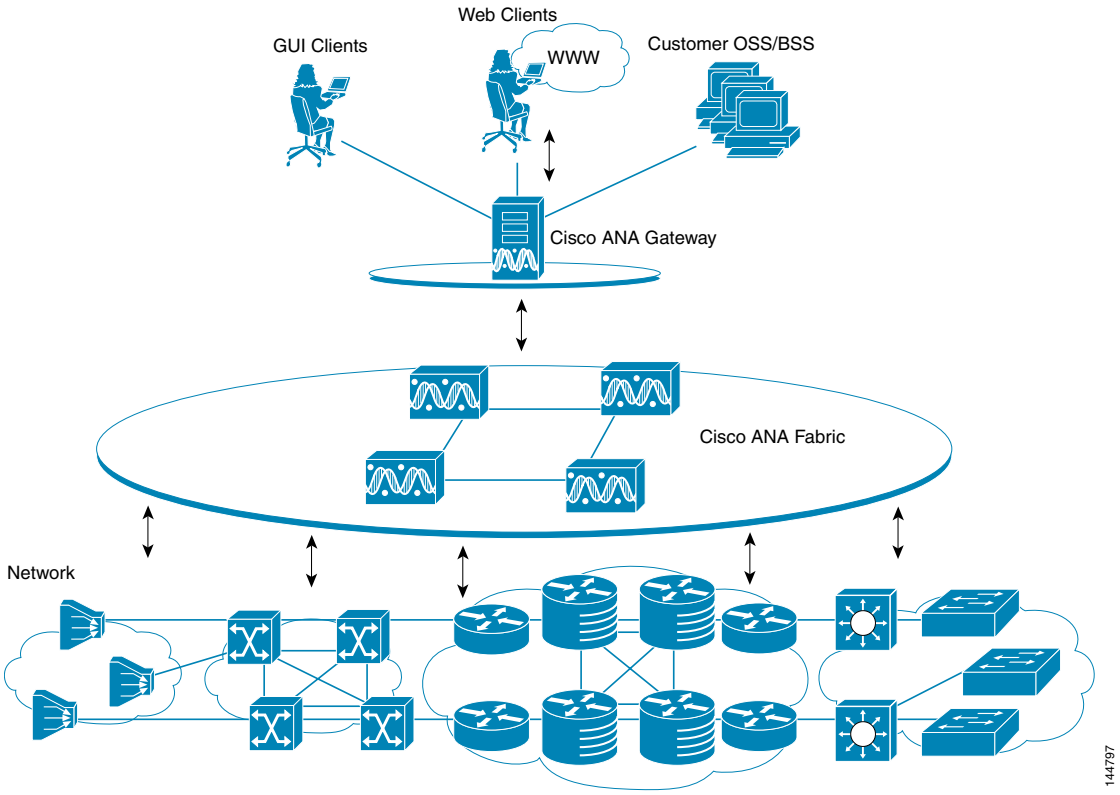
Based on a patented innovative architecture of distributed autonomous virtual network elements (VNE), Cisco ANA enables integrated management for hybrid network environments while being scalable to support network growth and evolution.

The Cisco ANA includes the following functionality:

- **Network (horizontal) Integration—**Supporting NEs from multiple vendors, across multiple technologies, forming a unified, end-to-end synthesis of the network.
- **Network and Service Discovery, Real-time Inventory and Topology—**Discovery of network inventory, services and multi-layer connectivity to form an accurate, up-to-date network information model.
- **Network Fault Intelligence—**Using the auto-discovered network model for fault correlation and root-cause analysis.
- **Service Impact—**Analysing of various network faults showing affected VPNs and sites.
- **Activation and Configuration—**The activation engine supports many device configurations.
- **Service Verification—**Real-time verification of configuration health and consistency.
- **Service Path Analysis—**Dynamic isolation and tracing of service paths, end-to-end across technologies and network layers.
- **GUI Client Applications—**User applications for managing assurance, fulfillment and performance.
- **OSS/BSS (Vertical) Integration—**Open, flexible northbound adaptation framework to OSS/BSS applications in a wide variety of APIs, protocols, and information models.
- **Scalability—**A fully distributed solution implementing parallel processing that inherits the scaling properties of the network by creating a virtual model of it. Adding more autonomous VNEs and units supports network growth.

The Cisco ANA platform architectural diagram and functional blocks are displayed in the figure that follows.

Figure 1-1 Cisco ANA Architecture



Cisco ANA Components

The Cisco ANA system includes key components, as follows:

- Autonomous VNEs
- Cisco ANA Servers
- Cisco ANA Clients

Autonomous VNEs

The autonomous VNEs are software entities that run as a completely autonomous process within the Cisco ANA units. Each VNE is assigned to manage a single network element (NE) instance using whatever southbound management interfaces the NE implements (for example, SNMP or Telnet). The autonomous VNEs are the entities that maintain a live model of each NE and of the entire network.

As the VNE loads, it starts investigating the NE and automatically builds a live model of the NE, including its physical and logical inventory, its configuration and its status. Following the device investigation, the VNEs begin to negotiate with peer VNEs, which represent the peer NEs determining the connectivity and topology at different layers. This model of the network topology, device state, and device inventory is constantly being updated by the VNEs, which track every change that occurs in the NE or in the network.

Messaging between VNEs is used for running different end-to-end flows in order to provide information for root-cause and impact analysis, service path tracing, and more.

Cisco ANA Servers

Cisco ANA uses two server types, each performing different activities:

- Cisco ANA Gateway
- Cisco ANA Unit

Cisco ANA Gateway

The Cisco ANA gateway serves as the gateway through which all clients, including any OSS/BSS applications as well as the Cisco ANA clients can access the system. The gateway is an extended Cisco ANA unit. It enforces access control and security for all connections and manages client sessions. In addition it functions as a repository for storing configuration, network and system events and alarms.

Another important function of the gateway is to map network resources to the business context. This enables Cisco ANA to contain information that is not directly contained in the network (such as VPNs and subscribers) and display it to northbound applications.

Cisco ANA Unit

The main purpose of Cisco ANA units is to host the autonomous VNEs. The units are interconnected to form a fabric of VNEs that can communicate with other VNEs regardless of which unit they are running on. Each unit can host thousands of autonomous VNE processes (depending on the server system size). The units also allow for optimal VNE distribution, ensuring geographic proximity between the VNE and its managed NE.

Cisco ANA includes a clustered N+m high-availability mechanism. Unit availability is established in the gateway, running a protection manager process, which continuously monitors all the units in the network. After the protection manager detects a unit that is malfunctioning, it automatically signals one of the m servers in its cluster to load the configuration of the faulty unit (from the system registry), taking over all its managed NEs. The switchover to the redundant standby unit does not result in any loss of information in the system, as all the information is auto-discovered from the network, and no persistent storage synchronization is required. When a unit is configured, it can be designated as being an active or a standby unit.

For more information about high availability refer to the *Cisco Active Network Abstraction High Availability User Guide*.

Cisco ANA Clients

Cisco ANA provides a comprehensive suite of GUI applications to manage the network:

- **Cisco ANA NetworkVision—**The main GUI application of Cisco ANA, used to visualize every management function supported by the system. For more information refer to the *Cisco Active Network Abstraction NetworkVision User Guide*.
- **Cisco ANA EventVision—**A tool for viewing all historical events detected by the Cisco ANA system. For more information refer to the *Cisco Active Network Abstraction EventVision User Guide*.
- **Cisco ANA Manage—**A system administration and configuration tool for managing the entire Cisco ANA platform, as described in this chapter.
- **Cisco ANA Registry Editor—**A tool used for viewing and configuring the registry.

The clients support automatic client updates from the gateway using Web Start. When connecting with a gateway application, the system verifies that the client version is the latest available and if an upgrade is required, the system automatically updates the clients from the gateway.

Cisco ANA Manage

Cisco ANA Manage is the GUI tool used for performing various system administration activities for simple system control. It provides an interface to perform the following:

- **Cisco ANA Units—**Adding and removing units.
- **Autonomous Virtual Machines (AVMs) and Virtual Network Elements (VNEs)—**Adding and removing AVMs and VNEs for the different units. Starting and stopping VNEs, and setting polling information per VNE.
- **Global Settings**:
  - **Clients Licenses—**Installing and managing Cisco ANA client licenses .
  - **Database Segments—**Viewing the storage allocated for all the database segments.
  - **Messages of the Day—**Generating a message of the day (service disclaimer).
  - **Polling Groups—**Customizing polling groups.
  - **Protection Groups—**Customizing protection groups.
- **Topology—**Managing static and persistent topology links.
- **Workflow Engine—**Enables the administrator to manage workflow templates and running workflows in runtime.
- **Scopes—**Enables the administrator to group a collection of managed NEs together so that the user can view and manage the NEs based on the user's role.
- **Users—**Enables the administrator to define and manage user accounts.

Additional Concepts and Terms

The sections below include additional concepts and terms used in Cisco ANA Manage and throughout this guide.

AVM

Cisco ANA units are divided into AVMs (Autonomous Virtual Machines). These AVMs are Java processes that provide the necessary distribution support platform for executing and monitoring multiple VNEs. AVMs and VNEs should reside on a Cisco ANA unit (as a common configuration) but they can also reside on a Cisco ANA gateway.

Some types of AVMs run on the server, but do not run VNEs. These AVMs have reserved ID numbers (AVM 0-100) and these cannot be used. In addition, there are other reserved AVM ID numbers. The following AVMs have special roles assigned to them:

- AVM 0 (the switch AVM)
- AVM 11 (the gateway)
- AVM 66 (the workflows AVM)
- AVM 99 (the management AVM)
- AVM 100 (the trap management AVM)

Element Management

The base configuration for the creation of the managed element. Cisco ANA Manage enables the user to create VNEs, for example, by entering the IP address, SNMP and polling rate information and so on. This is element management.

License

Cisco ANA client applications and BQL connectivity is based on installed license files. Cisco ANA Manage enables the administrator to control and monitor the number of client and BQL connections over a limited or unlimited period of time based on the client licenses installed. Two types of licenses are supported: fixed (the number of installed users are identified by usernames or IP addresses or both) or floating (the number of installed users operating concurrently).

Managed Element

After Cisco ANA Manage installs and runs the process, samples the device, and collects the data a VNE (Managed Element) is created. The VNE includes logical inventory (for example, forwarding tables) and physical inventory (for example, modules and ports). The managed element can be accessed using NetworkVision.

Network Element

A network component existing in the network, for example, the devices displayed in Cisco ANA and in NetworkVision.

Network Element Components

Components of an NE, such as ports, blades, contexts and so on.

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 NEs. For example, a user with the default permission Viewer can view maps and the device list. For more information, see Default Permissions, page 10-2.
- **Network Element—**The NE-related permission enables the administrator to group a collection of managed NEs together (in Cisco ANA Manage) in order to enable 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 NEs) and a role, the user can then perform various activities on the NEs, for example, manage alarms in NetworkVision. For more information, see Scopes, page 10-1.

Polling Group

A polling group is defined as a group of polling rates that can be specified for a device. For more information, see Polling Groups Overview, page 7-5.

Polling Intervals

The unit servers poll the NEs to discover and display accurate and up-to-date information of the network. The system periodically triggers polling at set intervals. Cisco ANA provides three out-of-the-box polling intervals for the VNEs, see Polling Groups Overview, page 7-5.

Protection Group

A protection group is a cluster to which units and standby units are related. In case of unit failover then the redundant unit will be taken from the same protection group.

Redundant Unit

The Cisco ANA unit comes with built-in redundancy for maximum up-time and automatic switching. A threshold configurable watchdog constantly monitors the units and gateway, and can make an automatic or manual (operator approved) switchover when there is no response from the monitored entity. The system is always up-to-date via real-time investigation of the network. The redundancy mechanism ensures synchronization of the active and backup units. Once activated, the standby node is immediately synchronized with the network.

Roles

Cisco ANA implements a security engine that combines a role-based security mechanism that is applied on scopes of NEs granted per user. The system supports user accounts creation, multiple NE scope definition, and a set of five pre-defined roles for security and access control to allow different system functions:

- **Administrator—**Manages the system configuration and security.

- **Configurator—**Activates services, and configures the network.
- **Operator Plus—**Controls alarm life cycle and create maps.
- **Operator—**Configures business tags and performs most day-to-day operations.
- **Viewer—**Has read-only access to the network and to non-privileged system functions.

Roles can be granted per scope or at an application level (default permission) for all the activities that are related to GUI functionality, not the activities related to devices. The default permission includes:

- Application login.
- Manage alarms in NetworkVision.
- Manage maps—Creating, deleting, and opening.
- Map manipulation—Arrange map, including aggregations, adding NEs, NE placement in map, map background and so on.
- Business tag management.

Scopes

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

Using NetworkVision, a user that has been assigned a scope can view and manage the NEs within this scope according to the role assigned to the user as per the scope. The user cannot view any information regarding NEs, including basic properties, inventory, and alarms, that are outside the user's scope.

Static Link

A static link is a physical link that is not automatically discovered by the system. The user manually creates the static link between NEs by selecting the two end ports from the NE physical inventories.

Transport Link

A transport link is a logical link used for communication between the units and for transferring information.

Users

In order for a user to work with Cisco ANA the following requirements must be met:

- The user must have a valid license installed.
- The user must have a defined Cisco ANA user account.
- The user must have an assigned permission.

For more information about users see Chapter 10, "Managing Security".

Workflow

A workflow consists of several tasks grouped together and arranged in a flowchart. All workflows are stored on the gateway. After a workflow is deployed, it can be accessed using Cisco ANA Manage in order to view its properties and status. Deployed workflow templates can be invoked with the Cisco ANA API using BQL. In addition, the user can view a history of the invoked workflows using EventVision. For more information refer to this guide and the *Cisco Active Network Abstraction Workflow User Guide*.

Conventions Used In This Guide

Command syntax descriptions use the following conventions:

Convention	Description
boldface	Boldface text indicates commands and keywords that the user enters literally as shown.
italics	Italic text indicates arguments for which the user supplies values.
[x]	Square brackets enclose an optional element (keyword or argument).
|	A vertical line indicates a choice within an optional or required set of keywords or arguments.
[x | y]	Square brackets enclosing keywords or arguments separated by a vertical line indicate an optional choice.
{x | y}	Braces enclosing keywords or arguments separated by a vertical line indicate a required choice.

Nested sets of square brackets or braces indicate optional or required choices within optional or required elements. For example:

Convention	Description
[x {y | z}]	Braces and a vertical line within square brackets indicate a required choice within an optional element.

Examples use the following conventions:

Convention	Description
screen	Examples of information displayed on the screen are set in Courier font.
Boldface screen	Examples of text that the user must enter are set in Courier bold font.
< >	Angle brackets enclose text that is not printed to the screen, such as passwords.
[ ]	Square brackets enclose default responses to system prompts.
{ }	Curly brackets group mandatory parameters together where there are options.

Related Documentation

For more detailed information see the following publications:

- *Cisco Active Network Abstraction NetworkVision User Guide*
- *Cisco Active Network Abstraction EventVision User Guide*
- *Cisco Active Network Abstraction Servers Installation Guide*
- *Cisco Active Network Abstraction Client Installation Guide*
- *Cisco Active Network Abstraction High Availability User Guide*
- *Cisco Active Network Abstraction Error Messages*
- *Cisco Active Network Abstraction Workflow User Guide*