# Cisco Active Network Abstraction High Availability User Guide
# Version 3.6

# C O N T E N T S

# Preface

This guide describes the high availability (redundancy) and protection options available for the units and gateways in Cisco Active Network Abstraction (ANA) 3.5.2.

# Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New* in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

# Cisco ANA Architecture

This chapter briefly describes the Cisco Active Network Abstraction (ANA) platform's three layer architecture comprising the Cisco ANA Gateway and Cisco ANA fabric, introducing Cisco ANA Units as a prelude to describing the Cisco ANA high availability functionality.

## Architecture

The Cisco ANA platform architectural diagram and functional blocks are displayed below:

*Figure 1-1* **Cisco ANA Architecture**
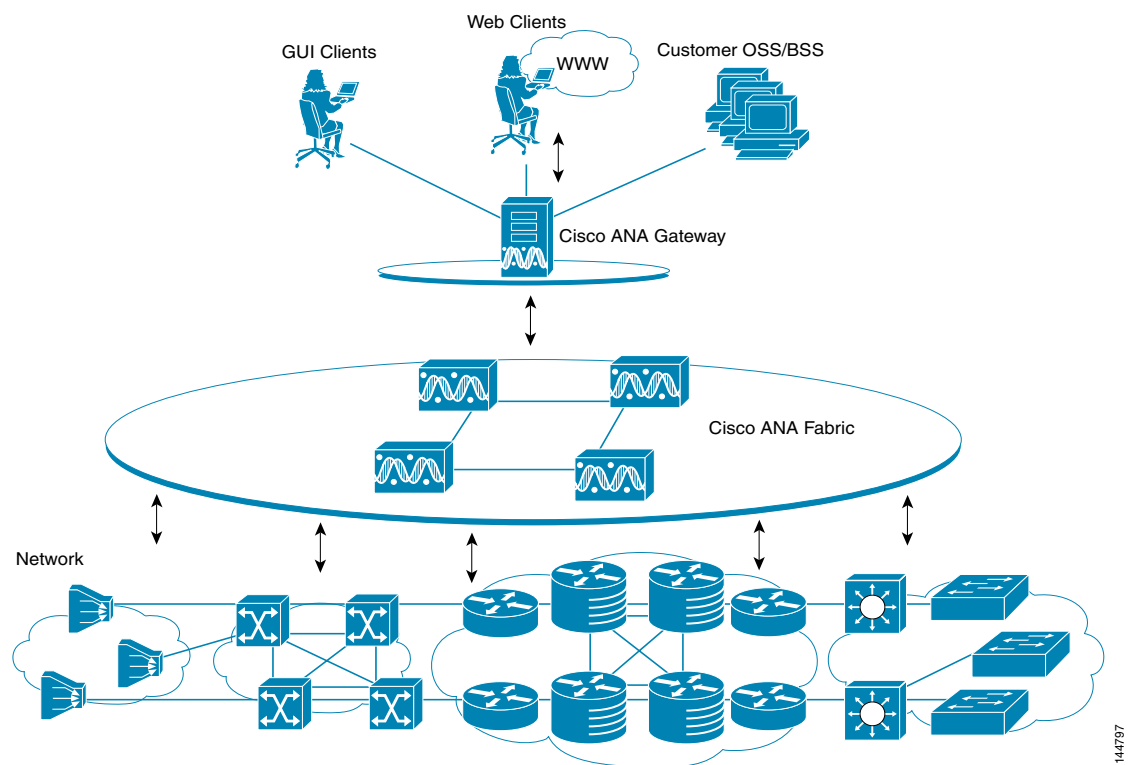
The top layer is comprised of the commercial and/or legacy OSS/BSS applications, as well as the Cisco ANA Client application suite. The Cisco ANA solution enables OSS/BSS applications to integrate with the platform, via a set of well-defined standards based APIs.

The second layer is comprised of the gateway, through which all the OSS/BSS applications and our clients access the Cisco ANA fabric. Each client connects to its designated gateway server.

The third layer is comprised of the interconnected fabric of units, each managing a subset of the Network Elements (NE) in the network. The units are distributed in a way that ensures proximity to their NEs.

# Cisco ANA Gateway

The gateway serves as the gateway through which all clients, including any OSS/BSS applications as well as the clients access the system. It enforces access control and security for all connections and manages client sessions. In addition it maintains a repository for keeping system settings, topological data and snapshots of active alarms and events.

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. In addition, the gateway contains the alarms and events in the system.

# Cisco ANA Units

The main purpose of the units is to host the autonomous Virtual Network Elements (VNEs). The units are interconnected to form a fabric of VNEs, which can inter-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 and VNE type). The units also allow for optimal VNE distribution, ensuring geographic proximity between the VNE and its managed NE.

# Cisco ANA Clients

Cisco ANA provides a comprehensive suite of GUI applications to manage the network using the Cisco ANA platform.

- **Cisco ANA NetworkVision**—The main GUI application of Cisco ANA, used to visualize every management function supported by the system. For more information see 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 see the Cisco Active Network Abstraction EventVision User Guide.

- **Cisco ANA Manage**—System administration and configuration tool for managing the entire Cisco ANA platform. For more information see the Cisco Active Network Abstraction Administrator Guide.

# Introduction to High Availability

This chapter describes the high availability (redundancy) and protection options available for units and gateways:

- High Availability Overview, page 2-1—Provides an overview of high availability in the Cisco ANA fabric.
- Watchdog Protocol, page 2-2—Describes the Watchdog protocol that monitors the processes on the units.
- Unit N+m High Availability, page 2-2—Describes the clustered N+m high availability mechanism within the Cisco ANA fabric designed to handle the failure of units.
- Limitations and Restrictions, page 2-3—Describes the restrictions and limitations relating to high availability.

# High Availability Overview

High availability is the provision of multiple interchangeable components to perform a single function to cope with failures and errors.

The high availability architecture is designed to ensure continuous availability of assurance and fulfillment functionality, by detecting, and recovering from a wide range of hardware and software failures, such as failures in the server machines, connectivity, software breakdowns and so on.

The distributed design of the system enables the "impact radius" caused by a single fault to be confined. This prevents all types of fault from setting into motion the "domino" effect, which can lead to the meltdown of all the management services.

The high availability of the server backbone is achieved at several complementing levels, namely:

- NEBS-3 compliant carrier-class server hardware.
- Internal watchdog within each unit, in charge of monitoring (and if necessary automatically reloading) failed processes. For more information see Watchdog Protocol, page 2-2.
- N+m warm standby protection for units clusters. For more information see Unit N+m High Availability, page 2-2.

# Watchdog Protocol

Each unit executes several processes: one control process and several Agent Virtual Machine (AVM) processes that execute Virtual Network Elements (VNEs). Each process within the unit is completely independent. The isolation concept is tailored throughout the design: a failure of a single process does not affect other processes on the same machine. The exact number of processes on each unit depends on the capacity and computation power of the unit.

The control process executes a Watchdog protocol, which continuously monitors all other processes on the unit. This Watchdog protocol requires each AVM process to continuously handshake with the Control process. A process that fails to handshake with the control process after a number of times (namely, is "stuck") will be automatically killed and reloaded. All the Watchdog protocol parameters are configurable by the operator.

The dynamic design of the control process implements runtime adaptation and escalation. The escalation procedure moves the AVM to suspended mode, namely, the process is suspended. An example of an escalation procedure is to stop reloading a process that has crashed more than **N** times within a given period, as it is suspected of having a recurring software problem.

The reload process is local to the unit, and thus very rapid, with a minimal amount of downtime. Since the process can use its previous cache information (temporary persistency used to improve performance), once the stuck process is detected, reloading the process takes only a few seconds with no data loss.

All Watchdog activity is logged, and an alarm is generated and sent when the watchdog reloads a process.

# Unit N+m High Availability

The clustered N+m high availability mechanism within the Cisco ANA fabric is designed to handle the failure of a unit. Such failures include hardware failures, operating system failures, power failures, or network failures, which disconnect a unit from the Cisco ANA fabric.

Unit availability is established in the gateway, running a Protection Manager process, which continuously monitors all the units in the network. Once 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 network elements. This design provides many possibilities for trading off protection and resources. These possibilities range from just segmenting the network into clusters without any extra machines, up to having a warm-swappable empty unit for each and every unit in the setup. It is recommended that units are clustered according to geography and that an additional empty unit is added to heavily loaded clusters.

The switchover of 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. Hence, the redundant standby unit relearns all the information from the network elements, with no danger of persistent information corruption. Furthermore, where there is cluster saturation (namely, more than one unit in a cluster fails at the same time and there are no extra machines), the remaining units will continue to operate and manage their network scope normally.

When a unit is configured it can be designated as being an active or standby unit. The active  units (excluding the standby unit) that are connected to the gateway are known as a protection group. The standby unit that is configured for the gateway is linked to that protection group. The administrator can define more than a single protection group. Each protection group defined has a set of protected units and a protecting standby unit.

The following example shows a protection group (cluster) of units, controlled by a gateway with one unit configured as the standby for the protection group.

*Figure 2-1*        *Cisco ANA Architecture*

Cisco ANA Gateway

Cisco ANA unit    Cisco ANA unit    Cisco ANA unit    Cisco ANA unit    Cisco ANA unit (standby)
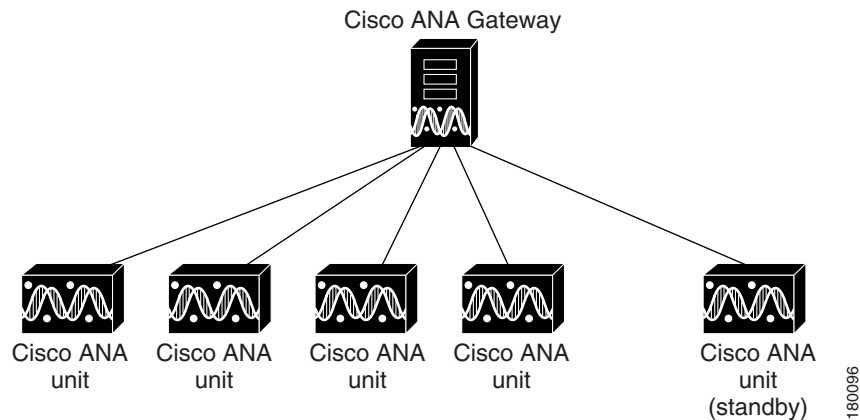
In the above configuration, when the gateway determines that one of the units in the protection group has failed, it notifies the protection group's standby unit to immediately load the configuration of the failed unit. The standby unit loads the configuration of the failed unit, including all its AVMs and VNEs, and functions as the failed unit.

These events are all recorded in the EventVision system log, which enables the user to take the necessary action to bring the failed unit up again. When the failed unit becomes operational, the user can decide whether to configure it as the new standby unit or to reinstate it to the protection group and configure another unit as the standby unit.

# Limitations and Restrictions

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

# Related Documentation

For more detailed information see the following publications:

- Cisco Active Network Abstraction Administrator Guide
- Cisco Active Network Abstraction NetworkVision User Guide
- Cisco Active Network Abstraction EventVision User Guide

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

# Getting Started

This chapter provides instructions for launching the Cisco ANA Manage application. In addition, it describes the steps that must be performed to configure high availability in the Cisco ANA fabric and provides cross-references to the relevant sections in this user guide:

- Starting Manage, page 3-1—Describes how to open the Manage application.
- Workflow, page 3-3—Describes the steps required to configure units for high availability in the Cisco ANA fabric.

## Starting Manage

This section provides instructions for launching the Manage application. Manage is password protected to ensure security. Before you start working with Manage, make sure you know the username, password and the gateway IP address that is required.

To start Manage:

**Step 1** From the Start menu, select the **Programs** folder, then **Cisco ANA/Cisco ANA Manage**. The Manage - Login dialog box is displayed.

**Step 2** Enter your **User Name**, **Password** and **Host** (gateway IP address).

> **Note** The gateway IP address that was used when the user last logged in is automatically displayed in the Host field.

**Step 3** Click **OK**. The Cisco ANA Manage window is displayed.

*Figure 3-1        Cisco ANA Manage Window*
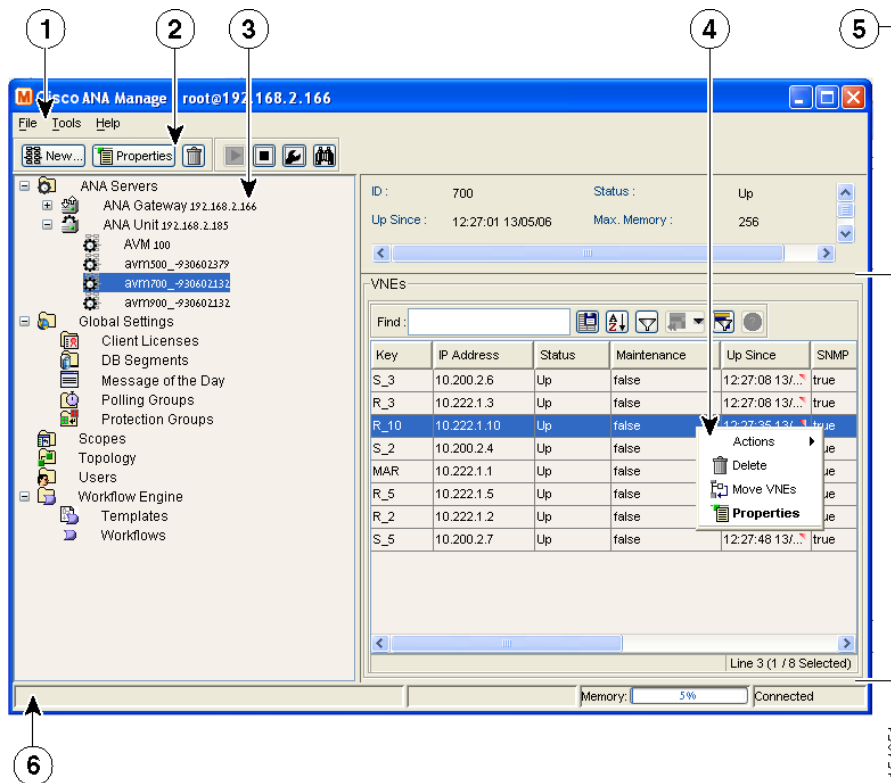


*Table 3-1*

| 1 | Menu bar |
|---|---|
| 2 | Toolbar |
| 3 | Tree pane |
| 4 | Shortcut menu |
| 5 | Workspace |
| 6 | Status bar |

The Manage window is divided into two areas, as follows:

- The tree pane
- The workspace

**Note**    For a detailed description of the Manage application see the Cisco Active Network Abstraction Administrator Guide.

# Workflow

The workflow below describes the steps required to configure units for high availability in the Cisco ANA fabric using Manage and the order in which they must be performed.

*Figure 3-2        Configuring Units Workflow*
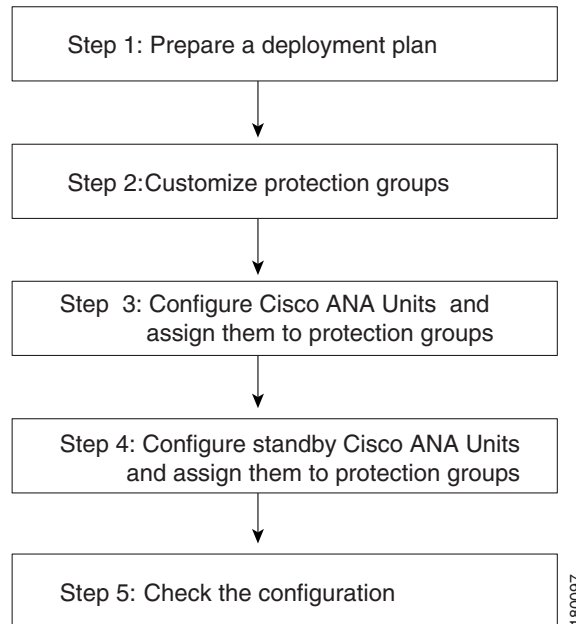
1. **Prepare a deployment plan**—The administrator must decide the following:

   • How many units are going to be deployed

   • How many protection groups there are going to be and how the units are going to be grouped together in the protection groups (cluster), based on the following considerations:

     – Device type

     – Geographical location

     – Importance of device

     – Number of devices

   • How many standby units are going to be deployed

   • How the units, standby units and protection groups are going to be deployed and allocated

2. **Customize protection groups**—Enables the administrator to define the protection groups (clusters) for the units. For more information see Customizing Protection Groups, page 4-1.

3. **Configure units and assign them to protection groups**—Enables the administrator to configure units for high availability and assign the units to protection groups. For more information see Configuring a Unit's Protection Group and High Availability, page 4-2.

✎
**Note**    For a detailed description on configuring units see the Cisco Active Network Abstraction Administrator Guide.

**4.** Configure standby units and assign them to protection groups—Enables the administrator to configure standby units and assign the standby units to protection groups. For more information see Configuring Standby Units, page 4-4.

**5.** Check the configuration**—**Enables the administrator to view the current allocation of the units to protection groups. For more information see Checking the Assignment of Units to Protection Groups, page 4-5.

C H A P T E R **4**

# Configuring Cisco ANA Units

This chapter describes customizing protection groups, configuring units for high availability and configuring standby units.

- Customizing Protection Groups, page 4-1—Describes how to customize protection groups for units.
- Configuring a Unit's Protection Group and High Availability, page 4-2—Describes how to assign a unit to a protection group and enable the unit for high availability.
- Configuring Standby Units, page 4-4—Describes how to create standby units and assign them to protection groups.
- Checking the Assignment of Units to Protection Groups, page 4-5—Describes how to view the current assignments of units to protection groups.
- Changing a Unit's Protection Group, page 4-5—Describes how to change the protection group allocation of a unit.
- Viewing and Editing Protection Group Properties, page 4-6—Describes how to view or edit the properties of a protection group.
- Manually Switching to the Standby Unit, page 4-6—Describes how to manually switch to the standby unit.
- Automatically Switching to a Standby Unit, page 4-7 —Describes how a high availability enabled gateway transfers data from a failed unit.

## Customizing Protection Groups

By default all the units in the Cisco ANA fabric belong to one big cluster. The administrator can change the default setup of the units by customizing protection groups (clusters) and then assigning units to these groups.

To customize a protection group:

**Step 1** Select the Global Settings branch in the Cisco ANA Manage window's tree pane. The Global Settings branch is displayed.

**Step 2** Expand the Global Settings branch and select the Protection Groups sub-branch.

**Step 3**    Right-click to display the shortcut menu and select **New Protection Group**,

or

On the toolbar click **New Protection Group**,

or

From the File menu select **New Protection Group**.

The New Protection Group dialog box is displayed.

**Step 4**    Enter the name of the protection group in the **Name** field.

**Step 5**    Enter a description for the protection group in the **Description** field (optional).

**Step 6**    Click **OK**. The new protection group is displayed in the workspace of the Cisco ANA Manage window.

The workspace displays all the currently defined protection groups.

> **Note**    The **default-pg** protection group displayed in the workspace is the default protection group (cluster), to which, by default, all the units in the Cisco ANA fabric belong.

# Configuring a Unit's Protection Group and High Availability

The administrator can change the default settings of a unit and assign it to a customized protection group. For more information about customizing protection groups see Customizing Protection Groups, page 4-1.

In addition, the administrator can enable or disable high availability for a unit. In other words, these settings enable the administrator to define to which protection group a unit is assigned and whether it is enabled for high availability.

> **Note**    By default, all the units in the Cisco ANA fabric belong to one big cluster, namely, the **default-pg** protection group, and High Availability is enabled.

Advanced configurations can be found in the registry to:

- Enable or disable the Watchdog protocol for each process, including timeouts for discovery when the process is down.
- Control the timeouts for detecting when a unit is down.

For further information, contact your nearest Cisco representative.

To configure a unit:

**Step 1**    Select the Cisco ANA Servers branch in the Cisco ANA Manage window's tree pane. The Cisco ANA Servers branch is displayed.

**Step 2**   Right-click to display the shortcut menu and select **New Cisco ANA Unit**,

or

On the toolbar click **New Cisco ANA Unit**

or

From the File menu select **New Cisco ANA Unit**.

The Cisco ANA Unit dialog box is displayed.

**Step 3**   Enter the IP address of the new unit in the **IP Address** field.

> ✎
> **Note**    For a detailed description on configuring units see the Cisco Active Network Abstraction Administrator Guide.

The **Enable Unit Protection** checkbox enables the administrator to define whether a unit is enabled (checkbox is selected) for high availability. This option is selected by default.

> ✎
> **Note**    It is highly recommended that the user does not disable this option.

The **Standby Unit** checkbox enables the administrator to define whether a unit is defined (checkbox is selected) as a standby unit.

The **Protection Group** dropdown list displays the current list of customized protection groups. For more information about defining a new protection group see Customizing Protection Groups, page 4-1.

**Step 4**   Confirm the **Enable Unit Protection** checkbox is selected to enable high availability.

**Step 5**   Select the required protection group from the **Protection Group** dropdown list.

**Step 6**   Confirm the real IP address of the gateway appears in the **Gateway IP** field.

**Step 7**   Click **OK**. The new unit is displayed in the tree pane and the workspace of the Cisco ANA Manage window.

If the new unit is installed and reachable it will start automatically. The unit is registered with the gateway. Specifically, the command creates the configuration registry for the new unit in the Golden Source. (For more information on the Golden Source registry see the Cisco Active Network Abstraction Administrator Guide.)

For information about changing a unit's protection group see
Changing a Unit's Protection Group, page 4-5.

> ✎
> **Note**    To make an active unit a standby unit:
> 1  Shutdown all the (Virtual Network Elements) VNEs of the active unit
> 2  Remove all the configurable (Agent Virtual Machines) AVMs of the active unit (AVMs below a value of 100 cannot be deleted)
> 3  Delete (remove) the active unit from the setup
> 4  Configure the new standby unit. For more information see Configuring Standby Units, page 4-4.

# Configuring Standby Units

Manage enables the administrator to configure standby units and assign the standby units to protection groups.

To configure a standby unit:

**Step 1**   Select the Cisco ANA Servers branch in the Cisco ANA Manage window's tree pane. The Cisco ANA Servers branch is displayed.

**Step 2**   Right-click to display the shortcut menu and select **New Cisco ANA Unit**,

or

On the toolbar click **New Cisco ANA Unit**

or

From the File menu select **New Cisco ANA Unit**.

The New Cisco ANA Unit dialog box is displayed.

> **Note**   For a detailed description on configuring units see the Cisco Active Network Abstraction Administrator Guide.

The **Enable Unit Protection** checkbox enables the administrator to define whether a unit is enabled (checkbox is selected) for high availability. This option is selected by default.

> **Note**   It is highly recommended that the user does not disable this option.

The **Standby Unit** checkbox enables the administrator to define whether a unit is defined (checkbox is selected) as a standby unit.

**Step 3**   Enter the IP address for the standby unit in the **IP Address** field.

**Step 4**   Select the **Standby Unit** checkbox to define the unit as a standby unit.

The **Protection Group** dropdown list displays the currently customized protection groups. For more information about defining a new protection group see Customizing Protection Groups, page 4-1.

**Step 5**   Select the protection group from the **Protection Group** dropdown list for which the newly created standby unit will act as a standby unit.

**Step 6**   Click **OK**.

> **Note**   Important standby units are not displayed anywhere in the Cisco ANA Manage window.

For information about changing the protection group to which a unit is assigned see Changing a Unit's Protection Group, page 4-5.

# Checking the Assignment of Units to Protection Groups

The administrator can view the protection groups to which the units are currently assigned. In so doing, the administrator can, at a glance, check that the configuration or assignment matches the initial deployment plan.

To check the units-protection groups assignments, select the Cisco ANA Servers branch in the Cisco ANA Manage window's tree pane. The properties of the Cisco ANA Servers branch are displayed in the workspace, including the details of the protection group to which each unit and standby unit currently belongs.

# Changing a Unit's Protection Group

The administrator can easily and quickly change the protection group to which a unit has been assigned.

To change the protection group setting of a unit:

**Step 1**   Select the Cisco ANA Servers branch in the Cisco ANA Manage window's tree pane. The Cisco ANA Servers branch is displayed.

**Step 2**   Expand the Cisco ANA Servers branch and select the required Cisco ANA Unit sub-branch.

**Step 3**   Right-click on the required unit to display the shortcut menu and select **Properties**,

or

On the toolbar click **Properties**

or

From the File menu select **Properties**. The Cisco ANA Unit Properties dialog box is displayed.

> **Note**   For a detailed description on configuring units see the Cisco Active Network Abstraction Administrator Guide.

The **Protection Group** dropdown list displays the currently customized protection groups. For more information about defining a new protection group see Customizing Protection Groups, page 4-1.

The **Enable Unit Protection** checkbox enables the administrator to define whether a unit is enabled (checkbox is selected) for high availability.

> **Note**   It is recommended that the user does not disable this option.

**Step 4**   Select the protection group from the **Protection Group** dropdown list to which you want to assign the unit.

**Step 5**   Click **OK** to save the updated protection group settings for the selected unit. The Cisco ANA Manage window is displayed.

# Viewing and Editing Protection Group Properties

The administrator can view the properties of a protection group, for example, the description. In addition, the administrator can edit the description of the protection group.

To view and edit a protection group's properties:

**Step 1**  Select the Global Settings branch in the Cisco ANA Manage window's tree pane. The Global Settings branch is displayed.

**Step 2**  Expand the Global Settings branch and select the Protection Groups sub-branch.

**Step 3**  Select the required protection group in the Cisco ANA Manage window's workspace.

**Step 4**  Right-click to display the shortcut menu and select **Properties**,

or

On the toolbar click **Properties**,

or

From the File menu select **Properties**.

The Properties dialog box is displayed.

**Step 5**  View the properties of the protection group and/or edit the description.

**Step 6**  Click **OK**. The Cisco ANA Manage window is displayed.

# Manually Switching to the Standby Unit

Manage enables the administrator to manually switch to the standby unit, for example, when a unit needs to be temporarily shut down for maintenance.

To manually switch to the standby unit:

**Step 1**  Select the Cisco ANA Servers branch in the Cisco ANA Manage window's tree pane. The Cisco ANA Servers branch is displayed.

**Step 2**  Expand the Cisco ANA Servers branch and select the required Cisco ANA Unit sub-branch.

**Step 3**  Right-click on the required unit to display the shortcut menu and select **Switch**.

A confirmation message is displayed.

**Step 4**  Click **Yes**. The standby unit becomes the active unit and is displayed in the Cisco ANA Servers branch. The original unit is removed from the setup and can be safely shutdown (it is no longer displayed in the Cisco ANA Servers branch of the Cisco ANA Manage window).

> **Note**  In the event of unit failover, the gateway will randomly select a redundant unit (when there are more than one Cisco ANA N+m redundant units).

# Automatically Switching to a Standby Unit

When the gateway discovers that one of the active units has, for example, timed out (see High Availability Events, page A-1 for more information), Cisco ANA will automatically transfer all data from the failed unit to a standby unit in the same protection group.

C H A P T E R **5**

# Managing the Watchdog Protocol

This chapter describes how Manage enables the administrator to define (Agent Virtual Machines) AVMs for units and enable or disable the watchdog protocol on the AVM.

- Configuring AVMs for High Availability, page 5-1—Describes how to enable or disable the watchdog protocol on the AVM.

- Viewing and Editing the Watchdog Protocol Settings, page 5-2—Describes how to view or edit the properties of an AVM.

## Configuring AVMs for High Availability

Every AVM in the Cisco ANA fabric is by default managed by the watchdog protocol. Manage enables the administrator to define AVMs for units and enable or disable the watchdog protocol on the AVM. For more information about the watchdog protocol see Watchdog Protocol, page 2-2.

**Note** It is highly recommended that the user does not disable this option.

In order to define an AVM:

- The unit must be installed.
- The unit must be connected to the transport network.
- The default AVMs, namely, AVM 0 (the switch AVM), AVM 99 (the management AVM) and AVM 100 (the trap management AVM) must be running.
- The new AVM must have a unique id within the unit.

To define an AVM:

**Step 1** Select the Cisco ANA Servers branch in the Cisco ANA Manage window's tree pane. The Cisco ANA Servers branch is displayed.

**Step 2** Expand the Cisco ANA Servers branch and select the required Cisco ANA Servers Entity sub-branch.

**Step 3** Right-click on the required unit to display the shortcut menu and select **New AVM**,

or

On the toolbar click **New AVM**,

or

From the File menu select **New AVM**.

The New AVM dialog box is displayed.

> ✎ **Note**     For a detailed description on defining AVMs see the Cisco Active Network Abstraction
> Administrator Guide.

The **Enable AVM Protection** checkbox is displayed in the New AVM dialog box, Select this option to enable the watchdog protocol on the AVM.

> ✎ **Note**     It is highly recommended that the user does not disable this option.

**Step 4**    Define the properties of the AVM.

**Step 5**    Click **OK**. The new AVM with the watchdog protocol enabled is added to the selected unit and is displayed in the workspace.

Adding the new AVM creates the registry information of the new AVM in the specified unit and the AVM can now host VNEs.

# Viewing and Editing the Watchdog Protocol Settings

The administrator can view the properties of an AVM, for example, its status and location. In addition, the administrator can edit some of the properties of the AVM, including enabling or disabling the watchdog protocol.

To view and edit an AVM's settings:

**Step 1**    Select the Cisco ANA Servers branch in the Cisco ANA Manage window's tree pane. The Cisco ANA Servers branch is displayed.

**Step 2**    Expand the Cisco ANA Servers branch and select the required AVMs sub-branch in the tree pane.

**Step 3**    Right-click to display the shortcut menu and select **Properties**,

or

On the toolbar click **Properties**,

or

From the File menu select **Properties**.

The AVM Properties dialog box is displayed.

> ✎ **Note**     For a detailed description on defining and editing AVMs see the Cisco Active Network
> Abstraction Administrator Guide.

**Step 4**    Edit the details of the AVM, as required.

**Note**    It is highly recommended that the user does not disable this option.

**Step 5**    Click **OK**. The AVM's new properties are displayed in the workspace.

A P P E N D I X **A**

# High Availability Events

This appendix provides a list of the high availability events displayed inEventVision and provides the defaults for the failover parameters. (For more information see the Cisco Active Network Abstraction EventVision User Guide.)

Cisco ANA has the following pre-configured defaults for failover:

| # | Description | Measured in milliseconds | Entry Name in Registry |
|---|---|---|---|
| 1 | Grace period (time from system startup in which events are not raised) | 1800000 (30 minutes) | Delay |
| 2 | Timeout for AVMs | 300000 (5 minutes) | Timeout |
| 3 | Timeout for units | 300000 (5 minutes)<br><br>**Note**    This is the initial recovery period defined in minutes, which includes device polling and inventory build-up. End-to-end services such as RCA and topology may take longer before they become available. | Timeout |
| 4 | AVMs repeatedly not responding | Tries a maximum of 5 times to restart the AVM within 10800000 ms (180 minutes) (if more will suspend the AVM). | maxTimeoutReloadTime<br>maxTimeoutReloadTries |

The grace period defines the amount of time that the system will not perform any high availability operations on the configured target (either the AVM, or the unit). There is one exception to this, namely, when the configured target responds for the first time with ping, then the grace period is over.

A list of the high availability events is provided in the following table:

| Event | Message | Severity |
|---|---|---|
| **Watchdog Protection** | | |
| The AVM times out (see # 2 in the above Pre-configured default table) | AVM 107 not responding: ANA Unit = 1.1.1.1 AVM = 107<br><br>This is followed by: | Major |
| | AVM 107 is shutting down. ANA Unit = 1.1.1.1 | Minor |
| | AVM 107 is starting. ANA Unit = 1.1.1.1 | Minor |
| The AVM repeatedly does not respond (see # 4 in the Pre-configured default table) | AVM 107 suppressed: ANA Unit = 1.1.1.1 AVM = 107 | Major |
| **Unit Protection** | | |
| The unit times out (when a standby unit is available) (see # 3 in the Pre-configured default table) | Server 1.1.1.1 not responding. Raising Redundant machine = 3.3.3.3 | Major |
| A unit times out (without a standby unit being available) (see # 3 in the Pre-configured default table) | Server 1.1.1.1 not responding. No Redundant machine available | Major |
| Manually switching to the standby unit | Server 1.1.1.1 manual failover initiated No Redundant machine available | Major |
| | Server 1.1.1.1 manual failover initiated Raising Redundant machine = 3.3.3.3 | Major |