



## **Cisco Active Network Abstraction High Availability User Guide**

Version 3.6 Service Pack 4  
January 2009

**Americas Headquarters**  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
<http://www.cisco.com>  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 527-0883

Text Part Number: OL-17257-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo 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. (0809R)

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.

*Cisco Active Network Abstraction High Availability User Guide Version 3.6 Service Pack 4*  
© 1999-2009 Cisco Systems, Inc. All rights reserved.



# CONTENTS

## **Preface** v

[Obtaining Documentation and Submitting a Service Request](#) v

---

### **CHAPTER 1**

## **Cisco ANA Architecture** 1-1

[Architecture](#) 1-1  
[Cisco ANA Gateway](#) 1-2  
[Cisco ANA Units](#) 1-2  
[Cisco ANA Clients](#) 1-2

---

### **CHAPTER 2**

## **Introduction to High Availability** 2-1

[High Availability Overview](#) 2-1  
[Watchdog Protocol](#) 2-2  
[Unit N+m High Availability](#) 2-2  
[Estimating Down Time in Case of Failure](#) 2-3  
[Catastrophic Process Failure](#) 2-4  
[Timeout Process Failure](#) 2-5  
[Timeout Machine Failure](#) 2-7  
[Related Documentation](#) 2-8

---

### **CHAPTER 3**

## **Getting Started** 3-1

[Starting ANA Manage](#) 3-1  
[Workflow](#) 3-3

---

### **CHAPTER 4**

## **Configuring Cisco ANA Units** 4-1

[Customizing Protection Groups](#) 4-2  
[Configuring a Unit's Protection Group and High Availability](#) 4-2  
[Configuring Standby Units](#) 4-4  
[Checking the Assignment of Units to Protection Groups](#) 4-5  
[Changing a Unit's Protection Group](#) 4-5  
[Viewing and Editing Protection Group Properties](#) 4-6  
[Manually Switching to a Standby Unit](#) 4-7  
[Automatically Switching to a Standby Unit](#) 4-7

---

**CHAPTER 5**

**Managing the Watchdog Protocol 5-1**

Configuring AVMs for High Availability 5-2

Viewing and Editing Watchdog Protocol Settings 5-3

---

**APPENDIX A**

**High Availability Events A-1**



## Preface

---

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

## Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, 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>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.





# CHAPTER 1

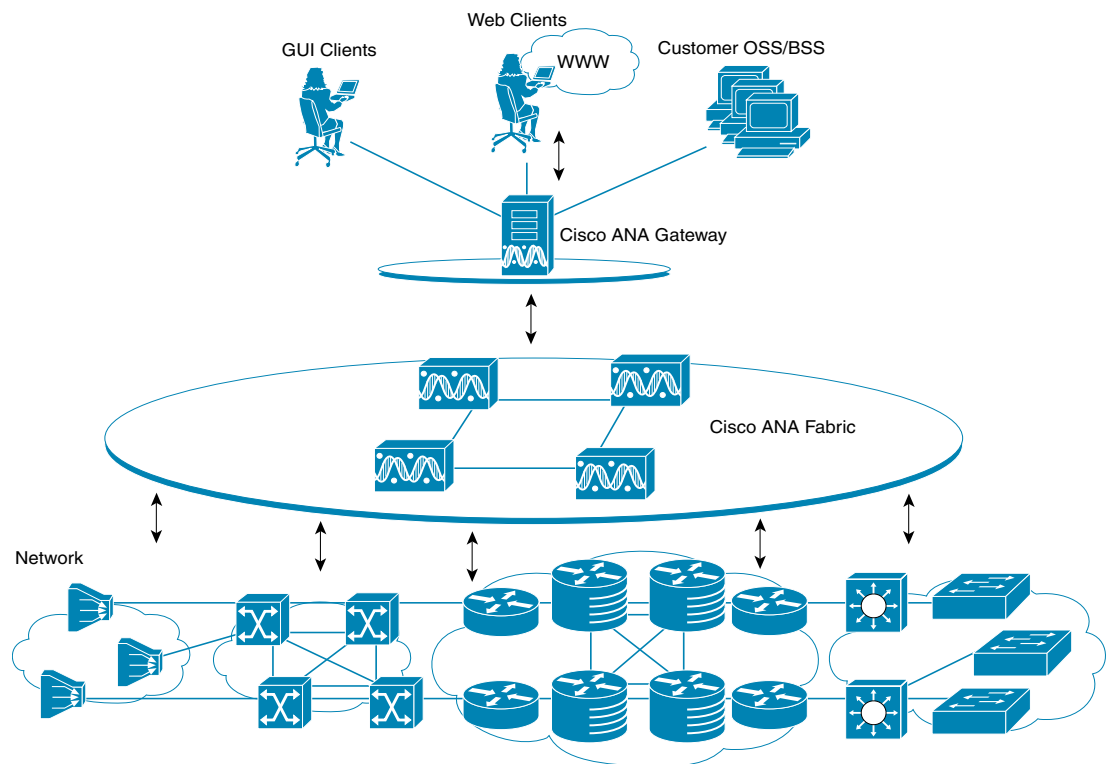
## Cisco ANA Architecture

This chapter briefly describes the Cisco Active Network Abstraction (Cisco 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 portal through which all clients, including any OSS/BSS applications, 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.

## Cisco ANA Clients

Cisco ANA provides a comprehensive suite of GUI applications that 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 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 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*.



# CHAPTER 2

## 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.
- [Estimating Down Time in Case of Failure, page 2-3](#)—Describes how to estimate how long a unit or AVM is down in the event of failure, and the recovery period.

## 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](#).



### Note

Cisco ANA does not provide a solution for the configuration of high availability for a Cisco ANA gateway. For information on configuring high availability for a Cisco ANA gateway using Veritas, please contact the Cisco Project Manager or Cisco Account Team.

---

## 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.

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.



### Note

An alarm persistency mechanism enables the system to clear alarms which relate to events that occurred while a VNE, AVM, unit, or the whole system was down, thus preserving system integrity. For more information about alarm persistency, see the *Cisco Active Network Abstraction Administrator Guide*.

All the watchdog protocol parameters, such as “pulse interval” and “retry times” are configurable in the registry by the operator. The higher these parameter values are, the longer the AVM or unit failure lasts, but this increases the certainty that a failure has actually occurred. Configuring these parameters with lower values may shorten the AVM or unit recovery, but might result in a “false positive” which could unnecessarily restart an AVM or revert to a standby unit, when the AVM is just busy or the unit currently processing a heavy load of data.

## 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.

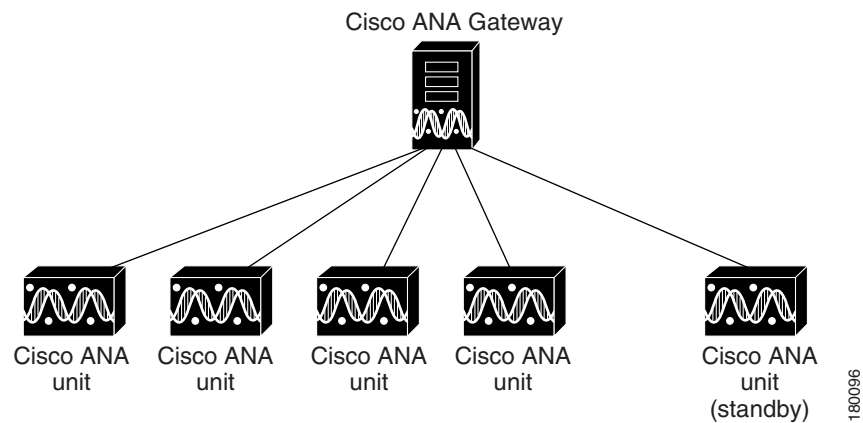
Unit availability is established in the gateway, running a Protection Manager process, which continuously monitors all the units in the network. Once the Protection Manager detects a unit that is malfunctioning, it automatically signals one of the  $m$  servers in its cluster to load the configuration 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**



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.

## Estimating Down Time in Case of Failure

When a failure occurs in a unit or AVM, the length of time that the system is down depends on the type of failure, how long it takes to detect that the component is not working, and the length of the recovery period (during which the unit or AVM reloads and the system begins to function normally again).

Three types of failure can occur, as described in the following sections:

- [Catastrophic Process Failure](#)
- [Timeout Process Failure](#)
- [Timeout Machine Failure](#)

## Catastrophic Process Failure

Each AVM has a log file which is constantly monitored by a Perl process for log messages about catastrophic failures, such as AVM processes running out of memory. When such a failure occurs, the Perl process restarts the AVM almost immediately, so the Mean Time To Repair (MTTR) is based on the AVM loading life cycle.

Table 2-1 describes the impact on different AVMs when experiencing such a failure:

**Table 2-1** *Catastrophic Process Failure Impact on AVMs*

Process	Impact	MTTR	Probability of Failure
AVM 0 (switch AVM)	Loss of messages to and from the machine.	1 minute to reach bootstrap.	Messages are constantly being sent and received in the system, so the probability of failure is high.
AVM 99 (management AVM)	Loss of registry notifications on changes made to the Golden Source.	1 minute to reach bootstrap.	Registry modifications are made only when the VNE is first loaded into the system, so the probability of failure is low. Modifications are rarely made while the system is up and running.
AVM 100 (trap management AVM)	Loss of traps and syslogs from devices.	1 minute to reach bootstrap, plus time for all the VNEs to re-register for traps and syslogs.	Traps and syslogs are constantly received in a live, scaled system, so there is a high probability of losing traps and syslogs during the reloading period.
AVM 11 (gateway)	Loss of persistency of any kind.	6-10 minutes to reach bootstrap on a scale.	Since AVM 11 handles Oracle communication and various gateway functions such as alarm processing, there is a high probability of loss of event persistency during this period.
AVM101-999	Loss of management to a section of devices managed by the AVM.	1 minute to reach bootstrap, plus time to load the VNEs depending on the number and type of VNEs.	No alarm processing occurs when the AVM is down, so traps and syslogs sent to the VNEs are lost. The loss of traps and syslogs for a period of 1 minute is high.

## Timeout Process Failure

Each AVM is constantly monitored by the management AVM (AVM99) using a watchdog protocol pulse message sent to the AVM at a preconfigured interval. When the AVM fails to respond to the pulse message after a preconfigured number of attempts, the management AVM restarts the process.

The management process also keeps a history of the number of times it has restarted the AVM. When it reaches the maximum number of preconfigured restart times, the management AVM stops restarting the AVM, because this indicates a serious problem with the AVM. Each restart is logged as a system event (except when AVM11 is restarted, because this AVM handles all persistency).

Failures on AVMs in the system are measured in a similar way to a catastrophic process failure (see [Table 2-1](#)), with the addition of the watchdog protocol overhead. This is measured by the pulse interval multiplied by the number of restart attempts.



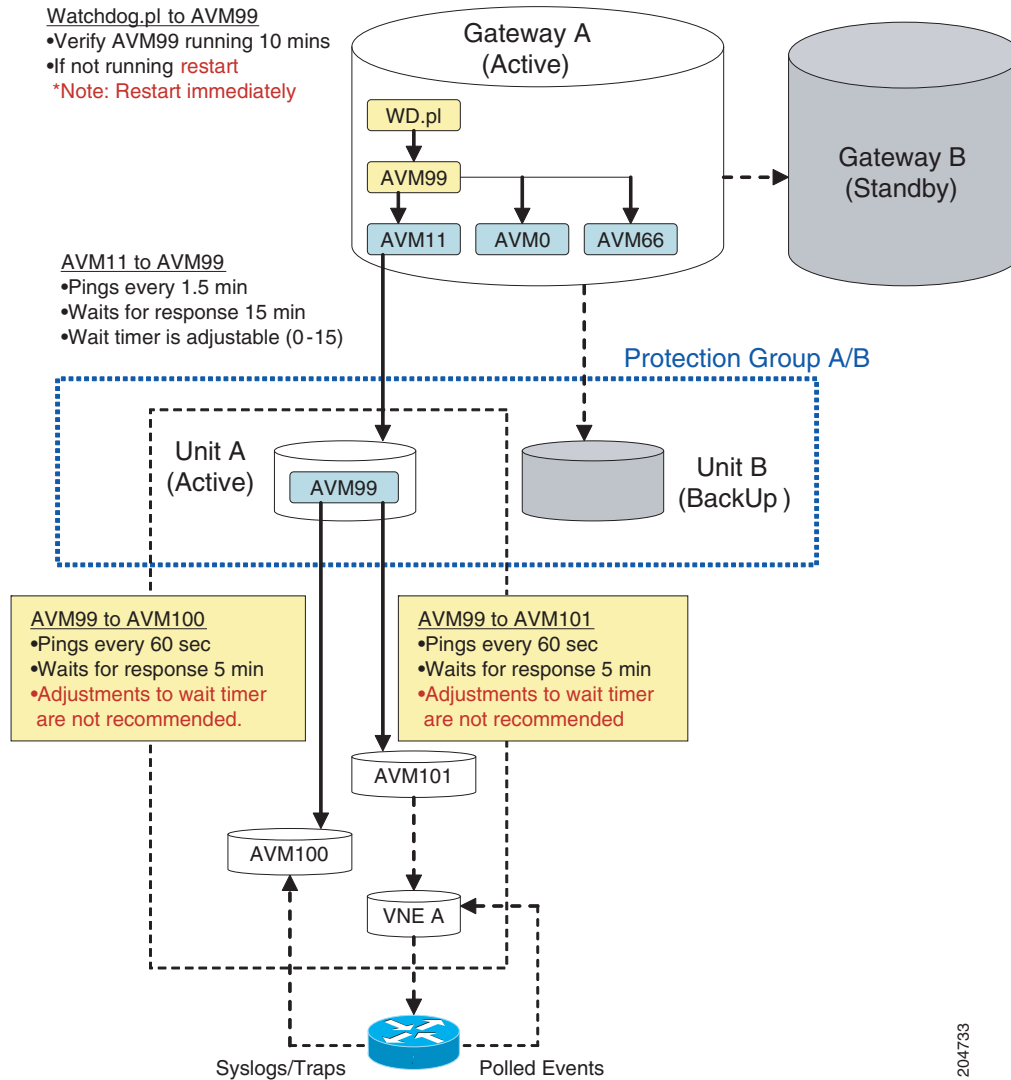
---

**Note**

- The maximum number of preconfigured restart times is five, after which the management process will not try to reload the AVM.
  - It takes approximately 1 minute for the system to detect that an AVM (including AVM100) is not working.
  - The recovery period during which an AVM (including AVM100) reloads and the system starts to function normally again is approximately 5 minutes, depending on the number of VNEs per AVM, and the complexity of each.
-

Figure 2-2 provides a typical example of how the High Availability timer parameters work while monitoring the AVMs.

**Figure 2-2 HA Parameter Timers and AVM Monitoring Example**



### Measuring Ticket Processing Down Time

When a failure occurs on an AVM, the time during which ticket processing is down is measured as the sum of the following factors:

- The time it takes to determine that the AVM has failed.
- The time it takes for the AVM to reload, depending on its number of VNEs.
- The time it takes to pass syslogs or traps to the VNEs (in the case of an AVM100), or to pass events to the gateway (in the case of an AVM101-999).



#### Note

For the first 30 minutes after an AVM99 (the management AVM) has started, there is no monitoring of the system to find high availability issues. This allows the system enough time to get up and running.

## Timeout Machine Failure

The Cisco ANA gateway constantly monitors the units by sending a watchdog protocol pulse message to the units' management AVM at a preconfigured interval. If the units' management AVM fails to respond to the pulse message after a preconfigured number of retries, the gateway loads the standby unit to replace it.

The impact of such a failure on the system is that the unresponsive unit does not manage the devices for a period of time. This "unmanaged" period of time is measured by the pulse interval multiplied by the number of retry times, plus the unit load time.

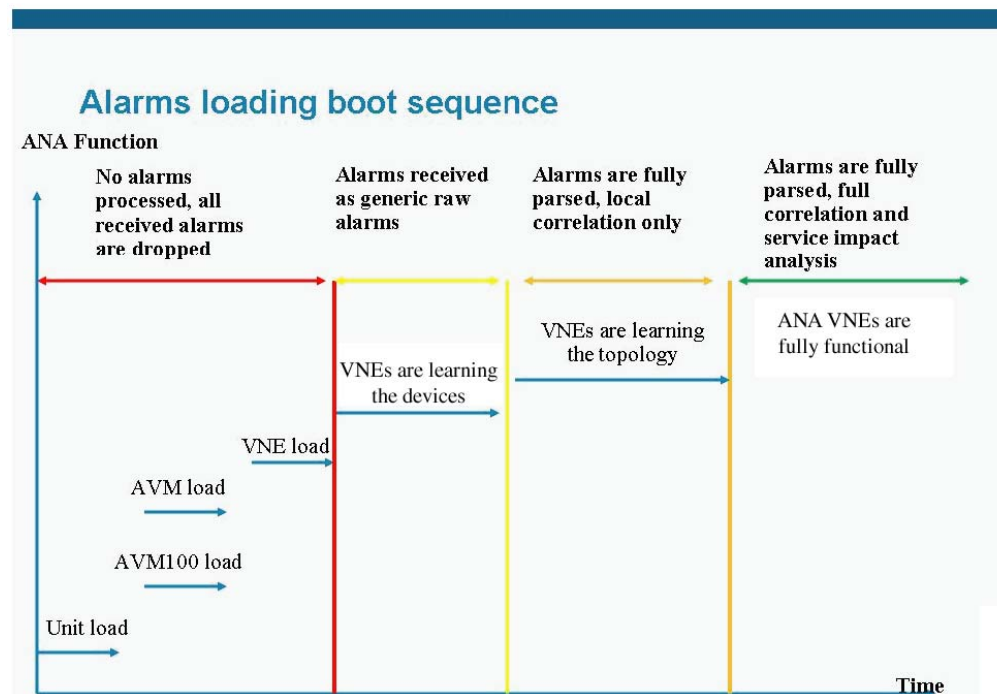


### Note

The unit load time depends on the AVMs and the load time taken for the VNEs to complete their modeling, as described in [Table 2-1](#).

[Figure 2-3](#) illustrates how the unit handles events during the loading time.

**Figure 2-3 Stages in Event Handling through System Restart**



### Measuring Ticket Processing Down Time

When a failure occurs on a unit, the time during which ticket processing is down is measured as the sum of the following factors:

- The time it takes to determine that the unit has failed (depending on the ping interval).
- The time it takes for the unit to reload, depending on the number of AVMs and VNEs in the unit.
- The time it takes to pass correlated events to the gateway (a minimum of 5 minutes to get some device history, plus a variable time depending on the number of VNEs per AVM).

## Related Documentation

For more detailed information see the following publications:

- *Cisco Active Network Abstraction Administrator Guide*
- *Cisco Active Network Abstraction User Guide*

**Note**

---

Changes to the registry should be performed only with the support of Cisco. For details, please contact your Cisco Project Manager or Cisco Account Team.

---



## CHAPTER 3

# 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 guide:

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

## Starting ANA Manage

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

To start Manage:


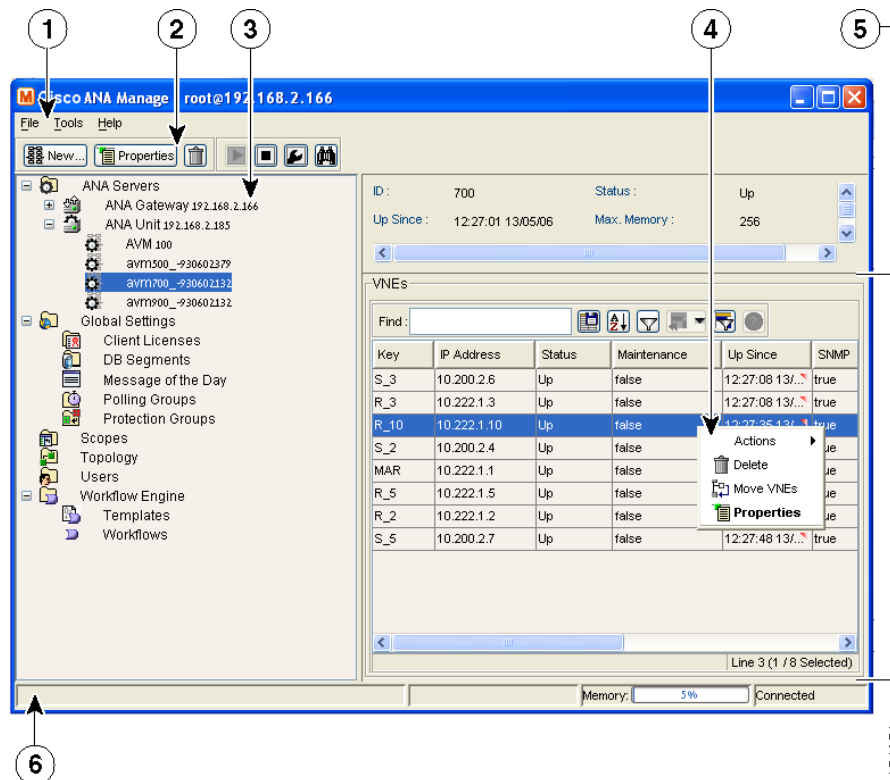
- 
- Step 1** Select **Start > Programs > Cisco ANA > Cisco ANA Manage**. The ANA Manage Login window is displayed.
- Step 2** Enter your **User Name**, **Password** and **Host** (gateway IP address).
-  **Note** The gateway IP address that was used when the user last logged in is automatically displayed in the Host field.
- 
- Step 3** Click **OK**. The ANA Manage window is displayed.
-

Figure 3-1 ANA Manage Window



The ANA Manage window is divided into two areas:

- The tree pane
- The workspace

Table 3-1 identifies the principal features of the window.

**Table 3-1 ANA Manage Window Features**

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



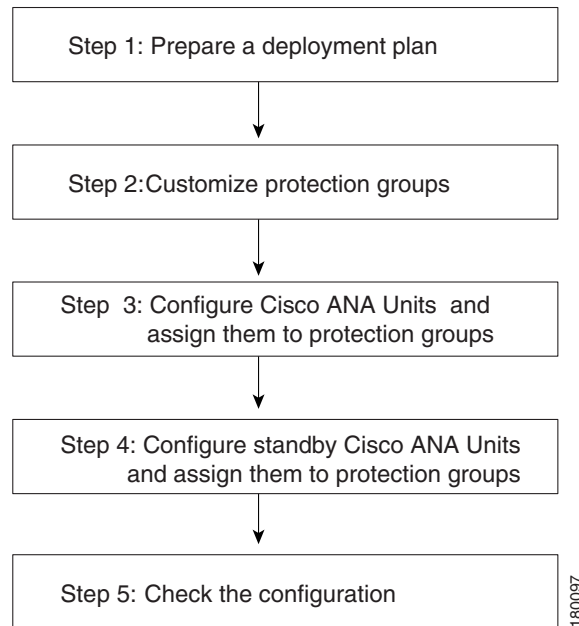
**Note**

For a detailed description of the ANA 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 ANA 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 will be deployed?
  - How many protection groups will there be and how will they be clustered? The administrator must base these answers on the following considerations:
    - Device types
    - Geographical locations
    - Importance of devices
    - Number of devices
  - How many standby units will be deployed?
  - How will the units, standby units and protection groups 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 4-2](#).
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](#).



## CHAPTER 4

# Configuring Cisco ANA Units

---

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

- [Customizing Protection Groups, page 4-2](#)—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 a Standby Unit, page 4-7](#)—Describes how to manually switch to the standby unit.
- [Automatically Switching to a Standby Unit, page 4-7](#)—Describes how a high-availability 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 ANA Manage window. The Global Settings branch is displayed.

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

**Step 3** Open the New Protection Group dialog box:

- Right-click the Protection Groups sub-branch, then select **New Protection Group**.
- Or
- Click **New Protection Group** in the toolbar.
- Or
- Select **File > 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 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 4-2](#).

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.

For information about how long a unit or AVM is down when switching to a standby unit, see [Estimating Down Time in Case of Failure, page 2-3](#).



**Note**

---

By default, all the units in the Cisco ANA fabric belong to one big cluster (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 ANA Manage window. The Cisco ANA Servers branch is displayed.

**Step 2** Open the New ANA Unit dialog box:

- Right-click the Cisco ANA Servers branch and select **New Cisco ANA Unit**.
- Or
- Click **New Cisco ANA Unit** in the toolbar.
- Or
- Select **File > New Cisco ANA Unit**.

The New 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*.

---

When selected, the **Enable Unit Protection** checkbox enables the unit's high-availability functions.



---

**Note** **Enable Unit Protection** is selected by default. We strongly recommended that you do not disable this option.

---

When selected, the **Standby Unit** checkbox identifies the unit 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 4-2](#).

**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 that the real IP address of the gateway appears in the **Gateway IP** field.

**Step 7** Click **OK**. The new unit is displayed in the 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 on this task, see [Configuring Standby Units, page 4-4](#).

## Configuring Standby Units

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

For information about how long a unit or AVM is down when switching to a standby unit, see [Estimating Down Time in Case of Failure, page 2-3](#).

To configure a standby unit:

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

**Step 2** Open the New ANA Unit dialog box:

- Right-click the Cisco ANA Servers branch and select **New Cisco ANA Unit**.
- Or
- Click **New Cisco ANA Unit** in the toolbar.
- Or
- Select **File > New New Cisco ANA Unit**.

The New ANA Unit dialog box is displayed.

**Note**

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

When selected, the **Enable Unit Protection** checkbox enables the unit's high-availability functions.

**Note**

**Enable Unit Protection** is selected by default. We strongly recommended that you do not disable this option.

When selected, the **Standby Unit** checkbox identifies the unit as a standby unit.

**Step 3** Enter the IP address of the new 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 4-2](#).

- 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 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 ANA Manage window. 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** Open the Cisco ANA Unit Properties dialog box:
- Right-click the Cisco ANA Servers branch and select **Properties**.
  - Or
  - Click **Properties** in the toolbar.
  - Or
  - Select **File > Propertiest**.

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 4-2](#).

When selected, the **Enable Unit Protection** checkbox enables the unit's high-availability functions.



**Note** **Enable Unit Protection** is selected by default. We strongly recommended that you do not disable this option.

- Step 4** In the **Protection Group** dropdown list, select the protection group to which you want to assign the unit.
- Step 5** Click **OK** to save the updated protection group settings for the selected unit. The 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 ANA Manage window. 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 workspace.
- Step 4** Open the Properties dialog box:
- Right-click the protection group and select **Properties**.
  - Or
  - Click **Properties** in the toolbar.
  - Or
  - Select **File > Properties**.
- The Properties dialog box is displayed.
- Step 5** View the properties of the protection group, or edit the description.
- Step 6** Click **OK**. The ANA Manage window is displayed.

## Manually Switching to a Standby Unit

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

To manually switch to a standby unit:

- 
- Step 1** Select the **Cisco ANA Servers** branch in the ANA Manage window. 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, then 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 shut down (it is no longer displayed in the **Cisco ANA Servers** branch of the ANA Manage window).



---

**Note** In the event of unit failover, the gateway randomly selects 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** automatically transfers all data from the failed unit to a standby unit in the same protection group. The original unit is removed from the standby setup and is no longer displayed in the **Cisco ANA Servers** branch of the ANA Manage window.





## CHAPTER 5

# Managing the Watchdog Protocol

---

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

[Configuring AVMs for High Availability, page 5-2](#)—Describes how to enable or disable the watchdog protocol on the AVM.

[Viewing and Editing Watchdog Protocol Settings, page 5-3](#)—Describes how to view or edit the properties of an AVM.

For a detailed description of how the watchdog protocol monitors the processes on the units, see [Watchdog Protocol, page 2-2](#).

## Configuring AVMs for High Availability

Every AVM in the Cisco ANA fabric is, by default, managed by the watchdog protocol. ANA Manage enables the administrator to define AVMs for units and enable or disable the watchdog protocol on each AVM.

In order to define an AVM:

- The unit must be installed.
- The unit must be connected to the transport network.
- The following default AVMs must be running:
  - AVM 0 — The switch AVM
  - AVM 99—The management AVM
  - AVM 100—The trap management AVM
- The new AVM must have a unique ID within the unit.



### Note

For detailed information on defining AVMs, see the *Cisco Active Network Abstraction Administrator Guide*.

To define an AVM:

- 
- Step 1** Select the Cisco ANA Servers branch in the ANA Manage window. 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** Open the New AVM dialog box:
- Right-click the required unit and select **New AVM**.
  - Or
  - Click **New AVM** in the toolbar.
  - Or
  - Select **File > New AVM**.

The New AVM dialog box is displayed.

- Step 4** The **Enable AVM Protection** checkbox is displayed in the New AVM dialog box. Select this checkbox to enable the watchdog protocol on the AVM.



### Note

We strongly recommended that you do not uncheck the **Enable AVM Protection** option.

- Step 5** Define the properties of the AVM.
- Step 6** 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 for the new AVM in the specified unit. The AVM can now host VNEs.
-

# Viewing and Editing 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.

**Note**

---

For detailed information on defining and editing AVMs, see the *Cisco Active Network Abstraction Administrator Guide*.

---

To view and edit an AVM's settings:

---

**Step 1** Select the Cisco ANA Servers branch in the ANA Manage window. 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** Open the AVM Properties dialog box:

- Right-click and select **Properties**.

Or

- Click **Properties** in the toolbar.

Or

- Select **File > Properties**.

The AVM Properties dialog box is displayed.

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

**Note**

---

We strongly recommend that you do not uncheck the **Enable AVM Protection** option.

---

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

---





# APPENDIX A

## High Availability Events

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

[Table A-1](#) shows Cisco ANA's pre-configured failover defaults.

**Table A-1** Failover Defaults

#	Description	Measured in milliseconds	Entry Name in Registry
1	Grace period (time from system startup in which events are not raised) <sup>1</sup>	1800000 (30 minutes)	Delay
2	Timeout for AVMs	300000 (5 minutes)	Timeout
3	Timeout for units	300000 (5 minutes) <b>Note</b> This is the initial recovery period defined in minutes,. This period 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, suspends the AVM).	maxTimeoutReloadTime maxTimeoutReloadTries

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

Table A-2 lists Cisco ANA's high availability events.

**Table A-2 High Availability Events**

Event	Message	Severity
<b>Watchdog Protection</b>		
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	Major
	This is followed by:	
	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
<b>Unit Protection</b>		
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