



Cisco Active Network Abstraction High Availability User's Guide, 3.5

Corporate 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: 408 526-4100

Text Part Number: OL-8839-01



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.

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, The Fastest Way to Increase Your Internet Quotient, and TransPath 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. (0601R)

Important Notice

Cisco ANA 3.5 is a carrier-class, multi-vendor network and service management platform which builds a real-time virtual model of the network, serving as a live information base for value-added tools and applications for integration into an existing OSS environment.

Cisco ANA 3.5 is a limited release by Cisco Systems of the existing features and functions of the Sheer DNA 4.0.1 software.

As this is a limited release, the naming of the product in the software and the user documentation remains as Sheer DNA.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

<http://www.cisco.com/techsupport>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from Cisco Marketplace at this URL:

<http://www.cisco.com/go/marketplace/>

Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

<http://www.cisco.com/go/marketplace/>

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

Report security vulnerabilities in Cisco products.

Obtain assistance with security incidents that involve Cisco products.

Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

Emergencies — security-alert@cisco.com

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

Nonemergencies — psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

1 877 228-7302

1 408 525-6532

We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.x through 8.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the Tools & Resources link under Documentation & Tools. Choose Cisco Product Identification Tool from the Alphabetical Index drop-down list, or click the Cisco Product Identification Tool link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting show command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

<http://www.cisco.com/go/marketplace/>

Cisco Press publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

<http://www.ciscopress.com>

Packet magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

<http://www.cisco.com/packet>

iQ Magazine is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

<http://www.cisco.com/go/iqmagazine>

or view the digital edition at this URL:

<http://cisoiq.texterity.com/cisoiq/sample/>

Internet Protocol Journal is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

<http://www.cisco.com/ipj>

Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

<http://www.cisco.com/en/US/products/index.html>

Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

<http://www.cisco.com/discuss/networking>

World-class networking training is available from Cisco. You can view current offerings at this URL:

<http://www.cisco.com/en/US/learning/index.html>

Table of Contents

1	Sheer DNA Architecture	1
	Sheer DNA Architecture	1
2	Introduction to High Availability.....	5
2.1	Sheer DNA High Availability Overview	5
2.2	Watchdog Protocol	6
2.3	Sheer DNA Unit N+m High Availability.....	7
2.4	Related Documentation	8
3	Getting Started	9
3.1	Starting Sheer DNA Manage.....	9
3.2	Workflow	11
4	Configuring Sheer DNA Units.....	13
4.1	Customizing Protection Groups	14
4.2	Configuring a Sheer DNA Unit's Protection Group and High Availability....	15
4.3	Configuring Standby Sheer DNA Units	17
4.4	Checking the Assignment of Sheer DNA Units to Protection Groups	19
4.5	Changing a Sheer DNA Unit's Protection Group	19
4.6	Viewing and Editing Protection Group Properties.....	21
4.7	Manually Switching to the Standby DNA Unit.....	22
4.8	Automatically Switching to a Standby DNA Unit	22
5	Managing the Watchdog Protocol.....	23
5.1	Configuring AVMs for High Availability	23
5.2	Viewing and Editing the Watchdog Protocol Settings	25
A.	High Availability Events	27

1 Sheer DNA Architecture

About this chapter:

This chapter briefly describes the Sheer™ DNA platform's three layer architecture comprising the DNA Gateway and Sheer DNA Fabric, introducing Sheer DNA Units as a prelude to describing Sheer's DNA high availability functionality.

Sheer DNA Architecture

The Sheer™ DNA Dynamic Network Abstraction platform architectural diagram and functional blocks are displayed below:

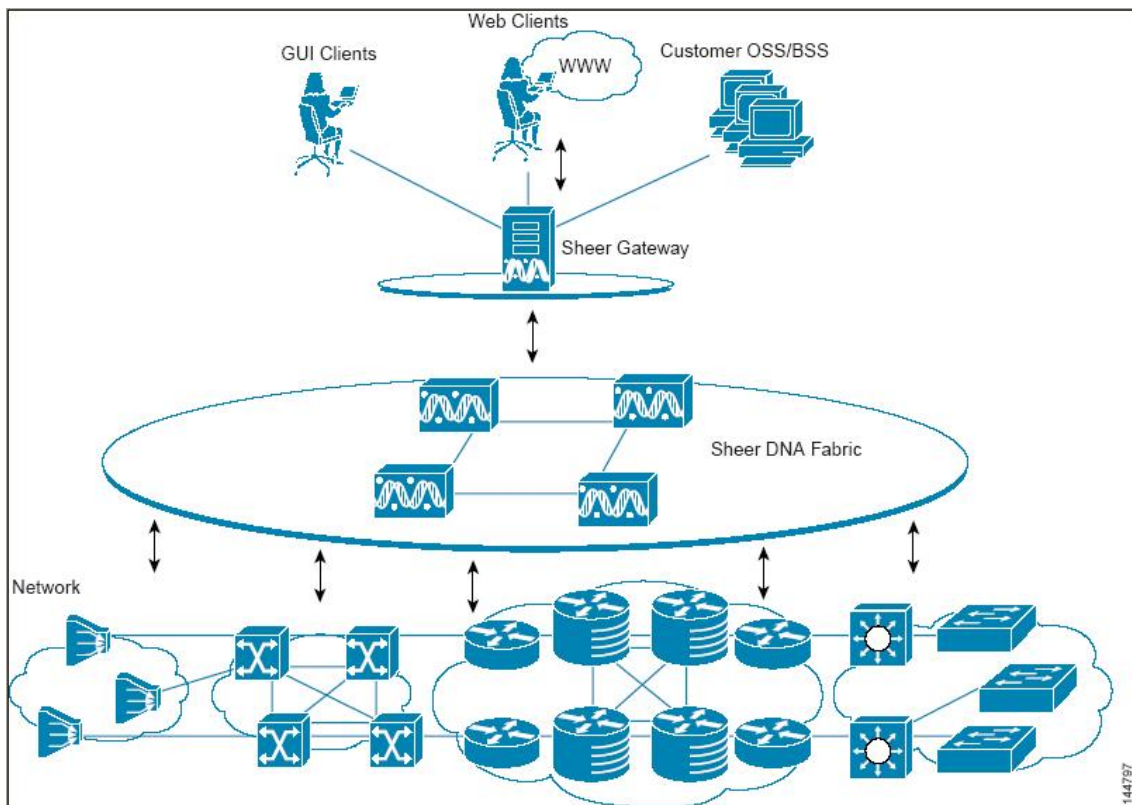


Figure 1: Sheer DNA Architecture

The top layer is comprised of the commercial and/or legacy OSS/BSS applications, as well as the Sheer Client Application Suite. The Sheer DNA 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 **Sheer DNA Gateway**, through which all the OSS/BSS applications and our clients access the Sheer DNA Fabric. Each client connects to its designated Sheer DNA Gateway server.

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

Sheer DNA Gateway

The Sheer DNA Gateway serves as the gateway through which all clients, including any OSS/BSS applications as well as the Sheer DNA 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 Sheer DNA Gateway is to map network resources to the business context. This enables Sheer DNA 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 Sheer DNA Gateway contains the alarms and events in the system.

Sheer DNA Unit

The main purpose of the Sheer DNA Units is to host the Autonomous Virtual Network Elements (VNEs). The Sheer DNA 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 Sheer DNA Unit can host thousands of Autonomous VNE processes (depending on the server system size and VNE type). The Sheer DNA Units also allow for optimal VNE distribution, ensuring geographic proximity between the VNE and its managed NE.

Sheer DNA Clients

Sheer provides a comprehensive suite of GUI applications to manage the network using the Sheer DNA platform.

Sheer NetworkVision – The main GUI application of Sheer DNA, used to visualize every management function supported by the system. For more information, refer to the *Cisco Active Network Abstraction NetworkVision User's Guide*.

Sheer EventVision – A tool for viewing all historical events detected by the Sheer DNA system. For more information, refer to the *Cisco Active Network Abstraction EventVision User's Guide*.

Sheer DNA Manage – System administration and configuration tool for managing the entire Sheer DNA platform. For more information, refer to the *Cisco Active Network Abstraction Administrator's Guide*.

2 Introduction to High Availability

About this chapter:

This chapter describes the high availability (redundancy) and protection options available for Sheer DNA Units and Sheer DNA Gateways.

Sheer DNA High Availability Overview, provides an overview of high availability in the Sheer DNA Fabric.

Watchdog Protocol, page 6, describes the Watchdog protocol that monitors the processes on the Sheer DNA Units.

Sheer DNA Unit N+m High Availability, page 7, describes the Sheer DNA clustered N+m high availability mechanism within the Sheer DNA Fabric designed to handle the failure of Sheer DNA Units.

2.1 Sheer DNA High Availability Overview

High availability is the provision of multiple interchangeable components to perform a single function to cope with failures and errors. In the Sheer DNA system there are two server types to which high availability applies:

- Sheer DNA Units
- Sheer DNA Gateways

The Sheer DNA 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 of the management services.

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

- NEBS-3 compliant carrier-class Server Hardware.
- Internal watchdog within each Sheer DNA Unit, in charge of monitoring (and if necessary automatically reloading) failed processes and/or Virtual Network Elements (VNEs). For more information, refer to *Section 2.2*.
- N+m warm standby protection for Sheer DNA Units clusters. For more information, refer to *Section 2.3*.

2.2 Watchdog Protocol

Each Sheer DNA Unit executes several processes: one *Control* process and several *Agent Virtual Machine* (AVM) processes that execute Virtual Network Elements (VNEs). Each process within the Sheer DNA 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 Sheer DNA Unit depends on the capacity and computation power of the Sheer DNA Unit.

The *Control* process executes a *Watchdog protocol*, which continuously monitors all other processes on the Sheer DNA 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 Sheer DNA 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.

2.3 Sheer DNA Unit N+m High Availability

The clustered N+m high availability mechanism within the Sheer DNA Fabric is designed to handle the failure of a Sheer DNA Unit. Such failures include hardware failures, operating system failures, power failures, or network failures, which disconnect a Sheer DNA Unit from the Sheer DNA Fabric.

Sheer DNA Unit availability is established in the Gateway, running a *Protection Manager* process, which continuously monitors all the Sheer DNA Units in the network. Once the *Protection Manager* detects a Sheer DNA 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. Sheer recommends 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 Sheer DNA Unit does not result in any loss of information in the system, as all of the information is auto-discovered from the network, and no persistent storage synchronization is required. Hence, the redundant standby Sheer DNA Unit relearns all of the information from the Network Elements, with no danger of persistent information corruption. Furthermore, where there is cluster saturation (namely, more than one Sheer DNA Unit in a cluster fails at the same time and there are no extra machines), the remaining Sheer DNA Units will continue to operate and manage their network scope normally.

When a Sheer DNA Unit is configured it can be designated as being an active or standby unit. The active Sheer DNA Units (excluding the standby unit) that are connected to the Sheer DNA 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 Sheer DNA Units, controlled by a Sheer DNA Gateway with one Sheer DNA Unit configured as the standby for the *Protection Group*.

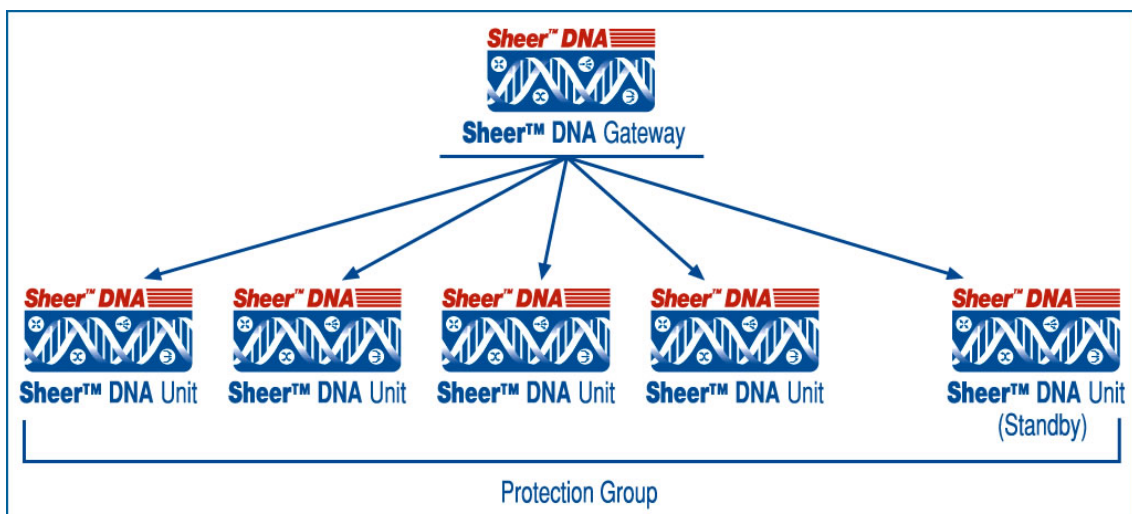


Figure 2: Sheer DNA Architecture

In the above configuration, when the Sheer DNA Gateway determines that one of the Sheer DNA Units in the Protection Group has failed, it notifies the Protection Group's standby Sheer DNA Unit to immediately load the configuration of the failed Sheer DNA Unit. The standby Sheer DNA Unit loads the configuration of the failed Sheer DNA Unit, including all of its AVMs and VNEs, and functions as the failed Sheer DNA 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 Sheer DNA Unit as the standby unit.

2.4 Related Documentation

For more detailed information, refer to the following publication:

- *Cisco Active Network Abstraction Administrator's Guide*
- *Cisco Active Network Abstraction NetworkVision User's Guide*
- *Cisco Active Network Abstraction EventVision User's Guide*

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

3 Getting Started

About this chapter:

This chapter provides instructions for launching the Sheer DNA Manage application. In addition, it describes the steps that must be performed to configure high availability in the Sheer DNA Fabric and provides cross-references to the relevant sections in this User's Guide.

Starting Sheer DNA Manage, below, describes how to open the *Sheer DNA Manage* application.

Workflow, page 11, describes the steps required to configure Sheer DNA Units for high availability in the Sheer DNA Fabric.

3.1 Starting Sheer DNA Manage

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

To start Sheer DNA Manage

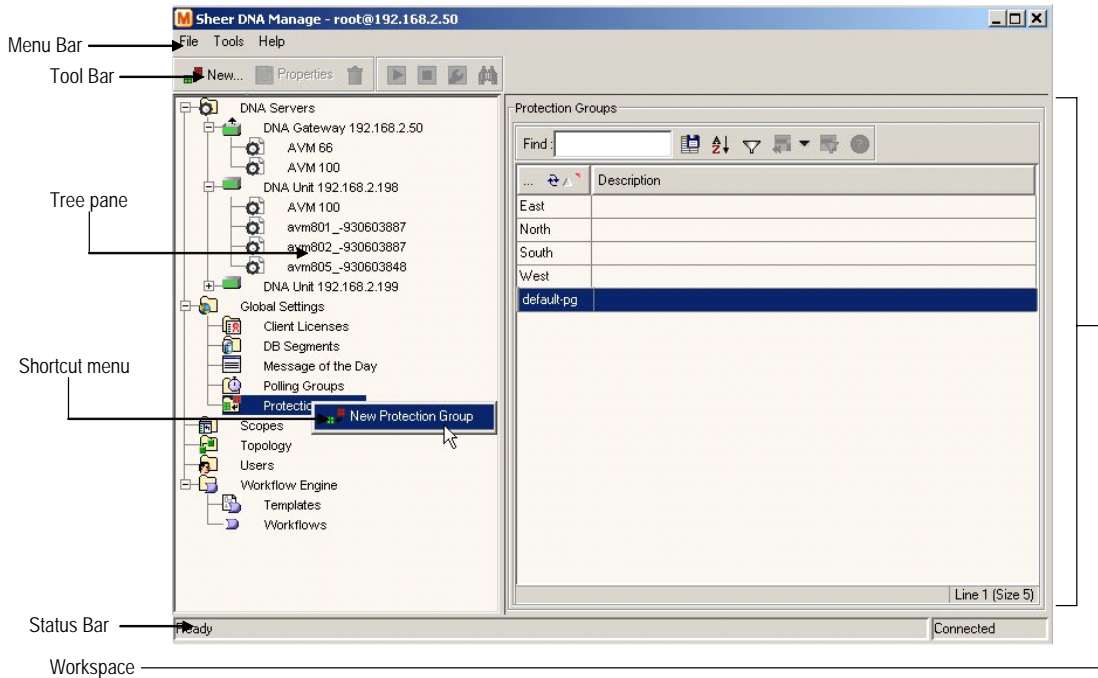
1. From the *Start* menu, select the **Programs** folder, then **Sheer DNA/Sheer DNA Manage**. The *Sheer DNA Manage - Login* dialog box is displayed.



2. Enter your **User Name**, **Password** and **Host** (Sheer DNA Gateway IP address).

Note: The Sheer DNA Gateway IP address that was used when the user last logged in is automatically displayed in the **Host** field.

3. Click **OK**. The *DNA Manage* window is displayed below.



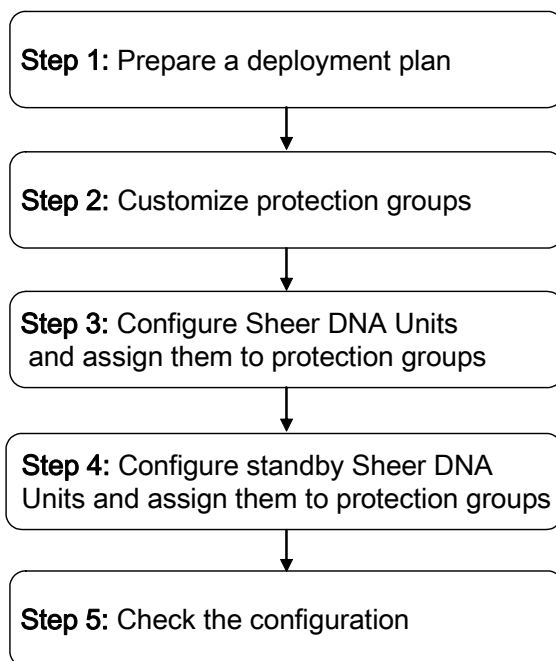
The *DNA Manage* window is divided into two areas, as follows:

- The *Tree* pane
- The *Workspace*

Note: For a detailed description of the Sheer DNA Manage application, refer to the *Cisco Active Network Abstraction Administrator's Guide*.

3.2 Workflow

The workflow below describes the steps required to configure Sheer DNA Units for high availability in the Sheer DNA Fabric using Sheer DNA Manage and the order in which they must be performed.



Step 1: Prepare a deployment plan: The administrator must decide the following:

- How many Sheer DNA Units are going to be deployed
- How many protection groups there are going to be and how the Sheer DNA 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 Sheer DNA Units are going to be deployed
- How the Sheer DNA Units, standby Sheer DNA Units and protection groups are going to be deployed and allocated

Step 2: Customize protection groups: Enables the administrator to define the protection groups (clusters) for the Sheer DNA Units. For more information, refer to *Section 4.1*.

Step 3: Configure Sheer DNA Units and assign them to protection groups: Enables the administrator to configure Sheer DNA Units for high availability and assign the Sheer DNA Units to protection groups. For more information, refer to *Section 4.2*.

Note: For a detailed description on configuring Sheer DNA Units, refer to *Chapter 5, Managing Sheer DNA Units* in the *Cisco Active Network Abstraction Administrator's Guide*.

Step 4: Configure standby Sheer DNA Units and assign them to protection groups: Enables the administrator to configure standby Sheer DNA Units and assign the standby Sheer DNA Units to protection groups. For more information, refer to *Section 4.3*.

Step 5: Check the configuration: Enables the administrator to view the current allocation of the Sheer DNA Units to protection groups. For more information, refer to *Section 4.4*.

4 Configuring Sheer DNA Units

About this chapter:

This chapter describes customizing protection groups, configuring Sheer DNA Units for high availability and configuring standby Sheer DNA Units.

Customizing Protection Groups, page 14, describes how to customize protection groups for Sheer DNA Units.

Configuring a Sheer DNA Unit's Protection Group and High Availability, page 15, describes how to assign a Sheer DNA Unit to a protection group and enable the Sheer DNA Unit for high availability.

Configuring Standby Sheer DNA Units, page 17, describes how to create standby Sheer DNA Units and assign them to protection groups.

Checking the Assignment of Sheer DNA Units to Protection Groups, page 19, describes how to view the current assignments of Sheer DNA Units to protection groups.

Changing a Sheer DNA Unit's Protection Group, page 19, describes how to change the protection group allocation of a Sheer DNA Unit.

Viewing and Editing Protection Group Properties, page 21, describes how to view or edit the properties of a protection group.

Manually Switching to the Standby DNA Unit, page 22, describes how to manually switch to the standby Sheer DNA Unit.

Automatically Switching to a Standby DNA Unit, page 22, describes how a high availability enabled Sheer DNA Gateway transfers data from a failed DNA Unit.


4.1 Customizing Protection Groups

By default all the Sheer DNA Units in the Sheer DNA Fabric belong to one big cluster. The administrator can change the default setup of the Sheer DNA Units by customizing protection groups (clusters) and then assigning Sheer DNA Units to these groups.

To customize a protection group

1. Select the *Global Settings* branch in the *DNA Manage* window's *Tree* pane. The *Global Settings* branch is displayed.
2. Expand the *Global Settings* branch and select the *Protection Groups* sub-branch.
3. Right-click to display the shortcut menu and select **New Protection Group**,

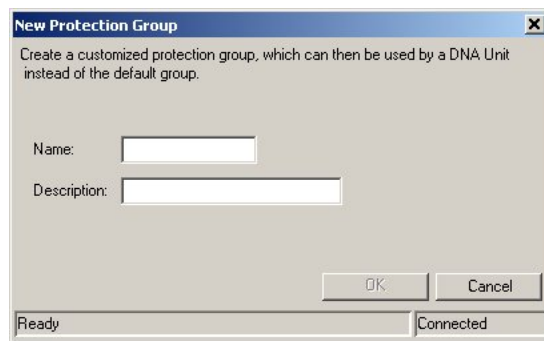
or

In the toolbar click ,

or

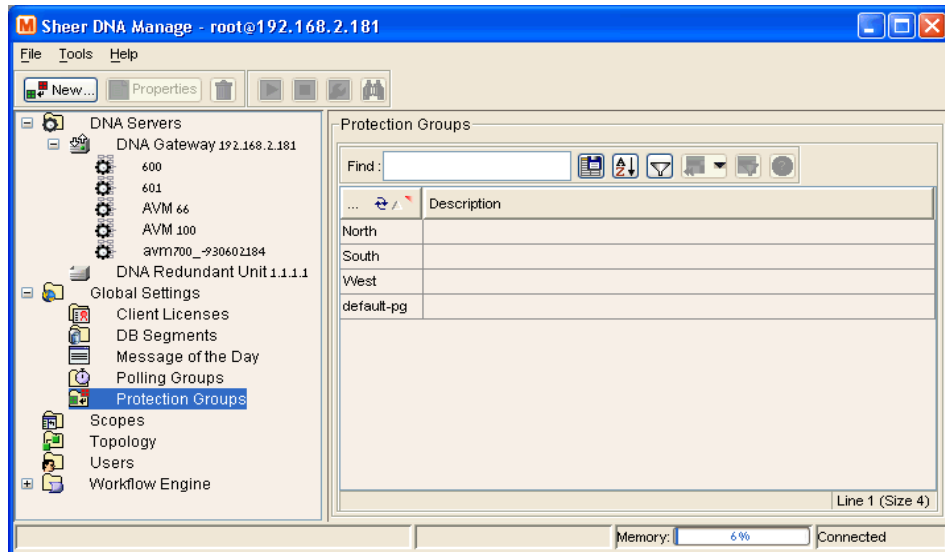
From the *File* menu select **New Protection Group**.

The *New Protection Group* dialog box is displayed.



4. Enter the name of the protection group in the **Name** field.
5. Enter a description for the protection group in the **Description** field (optional).

6. Click **OK**. The new protection group is displayed in the *Workspace* of the *Sheer DNA Manage* window.



The *Workspace* displays all of 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 Sheer DNA Units in the Sheer DNA Fabric belong.

4.2 Configuring a Sheer DNA Unit's Protection Group and High Availability

The administrator can change the default settings of a Sheer DNA Unit and assign it to a customized protection group. For more information about customizing protection groups, refer to *Section 4.1*.

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

Note: By default, all the Sheer DNA Units in the Sheer DNA Fabric belong to one big cluster, namely, the **default-pg** protection group, and High Availability is enabled.

Advanced configurations can be found in the Sheer DNA 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 Sheer DNA Unit is down.

For further information, contact your nearest Sheer Networks representative.

To configure a Sheer DNA Unit

1. Select the *DNA Servers* branch in the *DNA Manage* window's *Tree* pane. The *DNA Servers* branch is displayed.

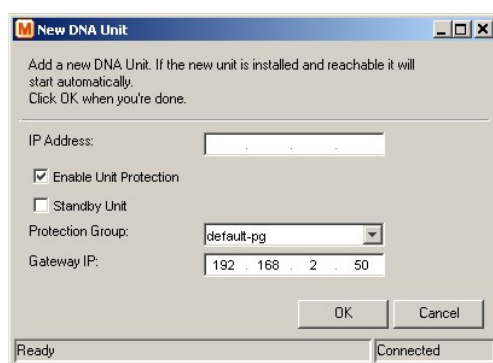
2. Right-click to display the shortcut menu and select **New DNA Unit**,
or

In the toolbar click 

or

From the *File* menu select **New DNA Unit**.

The *New DNA Unit* dialog box is displayed.



3. Enter the IP address of the new Sheer DNA Unit in the **IP Address** field.

Note: For a detailed description on configuring Sheer DNA Units, refer to *Chapter 5, Managing Sheer DNA Units* in the *Cisco Active Network Abstraction Administrator's Guide*.

The **Enable Unit Protection** checkbox enables the administrator to define whether a Sheer DNA 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 Sheer DNA 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, refer to *Section 4.1*.

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

5. Select the required protection group from the **Protection Group** dropdown list.
6. Confirm the real IP address of the Sheer Gateway appears in the **Gateway IP** field.
7. Click **OK**. The new Sheer DNA Unit is displayed in the *Tree* pane and the *Workspace* of the *Sheer DNA Manage* window.

If the new Sheer DNA Unit is installed and reachable it will start automatically. The Sheer DNA Unit is registered with the Sheer DNA Gateway. Specifically, the command creates the configuration registry for the new Sheer DNA Unit in the Golden Source. (For more information on the *Golden Source Registry*, see *Appendix B* in the *Cisco Active Network Abstraction Administrator's Guide*.)

For information about changing a Sheer DNA Unit's protection group, refer to *Section 4.5*.


Note: To make an active Sheer DNA Unit a standby Sheer DNA Unit:

- Shutdown all the (Virtual Network Elements) VNEs of the active Sheer DNA Unit
- Remove all the configurable (Agent Virtual Machines) AVMs of the active Sheer DNA Unit (AVMs below a value of 100 cannot be deleted)
- Delete (remove) the active Sheer DNA Unit from the setup
- Configure the new standby Sheer DNA Unit. For more information, refer to *Section 4.3*.

4.3 Configuring Standby Sheer DNA Units

Sheer DNA Manage enables the administrator to configure standby Sheer DNA Units and assign the standby Sheer DNA Units to protection groups.

To configure a standby Sheer DNA Unit

1. Select the *DNA Servers* branch in the *DNA Manage* window's *Tree* pane. The *DNA Servers* branch is displayed.
2. Right-click to display the shortcut menu and select **New DNA Unit**,
or
In the toolbar click  **New...**
or
From the *File* menu select **New DNA Unit**.

The *New DNA Unit* dialog box is displayed.

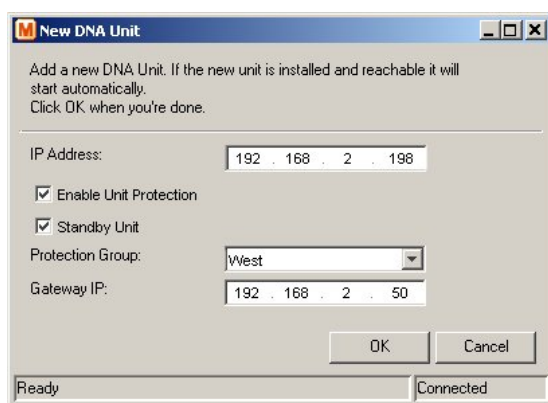
Note: For a detailed description on configuring Sheer DNA Units, refer to *Chapter 5, Managing Sheer DNA Units* in the *Cisco Active Network Abstraction Administrator's Guide*.

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

3. Enter the IP address for the standby Sheer DNA Unit in the **IP Address** field.



4. Select the **Standby Unit** checkbox to define the Sheer DNA 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, refer to *Section 4.1*.

5. Select the protection group from the **Protection Group** dropdown list for which the newly created standby Sheer DNA Unit will act as a standby unit.
6. Click **OK**.

Important Note: Standby Units are not displayed anywhere in the *DNA Manage* window.

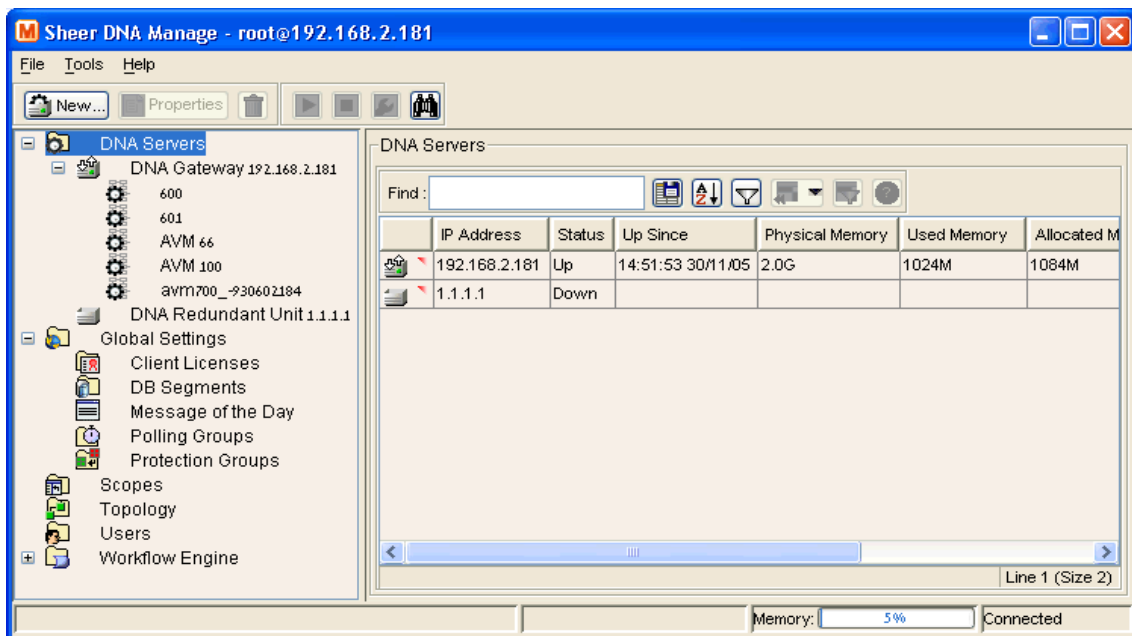
For information about changing the protection group to which a Sheer DNA Unit is assigned, refer to *Section 4.5*.

4.4 Checking the Assignment of Sheer DNA Units to Protection Groups

The administrator can view the protection groups to which the Sheer DNA 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 Sheer DNA Units-protection groups assignments

- Select the *DNA Servers* branch in the *Sheer DNA Manage* window's *Tree* pane. The properties of the *DNA Servers* branch are displayed in the *Workspace*, including the details of the protection group to which each Sheer DNA Unit and standby Sheer DNA Unit currently belongs.



4.5 Changing a Sheer DNA Unit's Protection Group


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

To change the protection group setting of a Sheer DNA Unit

1. Select the *DNA Servers* branch in the *DNA Manage* window's *Tree* pane. The *DNA Servers* branch is displayed.
2. Expand the *DNA Servers* branch and select the required *DNA Unit* sub-branch.

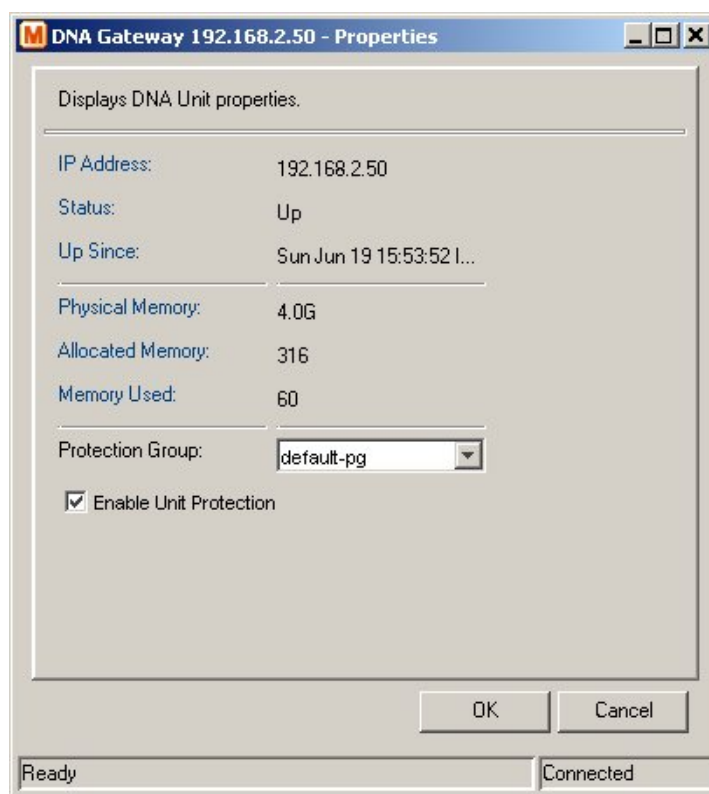
3. Right-click on the required Sheer DNA Unit to display the shortcut menu and select **Properties**,

or

In the toolbar click  Properties

or

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



Note: For a detailed description on configuring Sheer DNA Units, refer to *Chapter 5, Managing Sheer DNA Units* in the *Cisco Active Network Abstraction Administrator's Guide*.

The **Protection Group** dropdown list displays the currently customized protection groups. For more information about defining a new protection group, refer to *Section 4.1*.

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

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

4. Select the protection group from the **Protection Group** dropdown list to which you want to assign the Sheer DNA Unit.
5. Click **OK** to save the updated protection group settings for the selected Sheer DNA Unit. The *Sheer DNA Manage* window is displayed.

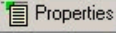
4.6 Viewing and Editing Protection Group Properties

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

1. Select the *Global Settings* branch in the *DNA Manage* window's *Tree pane*. The *Global Settings* branch is displayed.
2. Expand the *Global Settings* branch and select the *Protection Groups* sub-branch.
3. Select the required protection group in the *DNA Manage* window's *Workspace*.
4. Right-click to display the shortcut menu and select **Properties**,

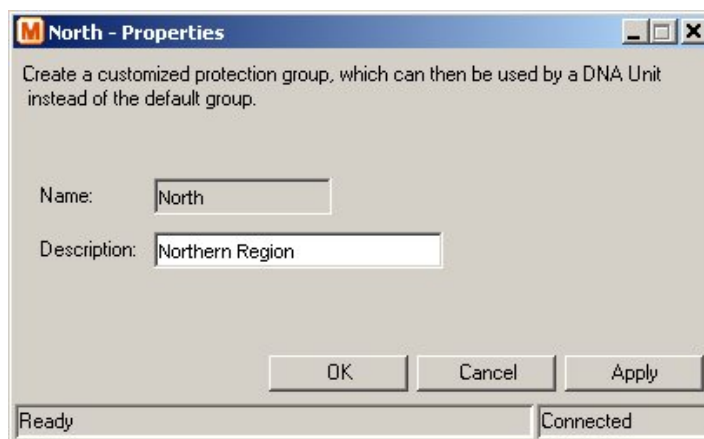
or

In the toolbar click ,

or

From the *File* menu select **Properties**.

The *Properties* dialog box is displayed.



5. View the properties of the protection group and/or edit the description.
6. Click **OK**. The *Sheer DNA Manage* window is displayed.

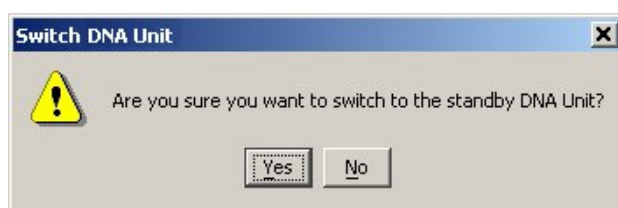
4.7 Manually Switching to the Standby DNA Unit

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

To manually switch to the standby DNA Unit

1. Select the *DNA Servers* branch in the *DNA Manage* window's Tree pane. The *DNA Servers* branch is displayed.
2. Expand the *DNA Servers* branch and select the required *DNA Unit* sub-branch.
3. Right-click on the required Sheer DNA Unit to display the shortcut menu and select **Switch**.

The following message is displayed:



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

Note: In the event of DNA Unit failover, the Sheer Gateway will randomly select a redundant unit (when there are more than one DNA N+m redundant units).

4.8 Automatically Switching to a Standby DNA Unit

When the Sheer DNA Gateway discovers that one of the active DNA Units has, for example, timed out (see *Appendix A High Availability Events* on page 27 for more information), Sheer DNA will automatically transfer all data from the failed DNA Unit to a Standby Unit in the same Protection Group.

5 Managing the Watchdog Protocol

About this chapter:

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

Configuring AVMs for High Availability, below, describes how to enable or disable the watchdog protocol on the AVM.

Viewing and Editing the Watchdog Protocol Settings, page 25, describes how to view or edit the properties of an AVM.

5.1 Configuring AVMs for High Availability

Every AVM in the Sheer DNA Fabric is by default managed by the watchdog protocol. Sheer DNA Manage enables the administrator to define AVMs for Sheer DNA Units and enable or disable the watchdog protocol on the AVM. For more information about the watchdog protocol, refer to page 6.

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

In order to define an AVM:

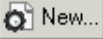
- The Sheer DNA Unit must be installed.
- The Sheer DNA Unit must be connected to the transport network.
- The default AVMs, namely, AVM 0 (the switch AVM), AVM 99 (the management AVM) and AVM 100 (the trap management AVM) must be running.
- The new AVM must have a unique id within the Sheer DNA Unit.

To define an AVM

1. Select the *DNA Servers* branch in the *DNA Manage* window's *Tree* pane. The *DNA Servers* branch is displayed.
2. Expand the *DNA Servers* branch and select the required *DNA Servers Entity* sub-branch.

3. Right-click on the required Sheer DNA Unit to display the shortcut menu and select **New AVM**,

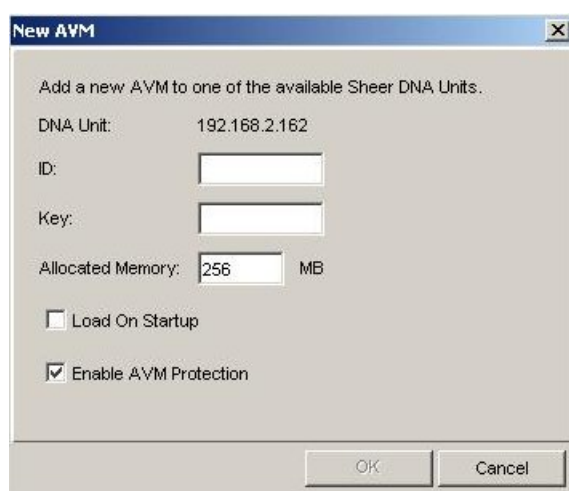
or

In the toolbar click ,

or

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

The *New AVM* dialog box is displayed.



Note: For a detailed description on defining AVMs, refer to *Chapter 6, Managing AVMs and VNEs* in the *Cisco Active Network Abstraction Administrator's Guide*.

The following checkbox is displayed in the *New AVM* dialog box:

- **Enable AVM Protection:** Select this option to enable the watchdog protocol on the AVM.

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

4. Define the properties of the AVM.
5. Click **OK**. The new AVM with the watchdog protocol enabled is added to the selected Sheer DNA Unit and is displayed in the *Workspace*.

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

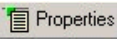
5.2 Viewing and Editing the Watchdog Protocol Settings

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

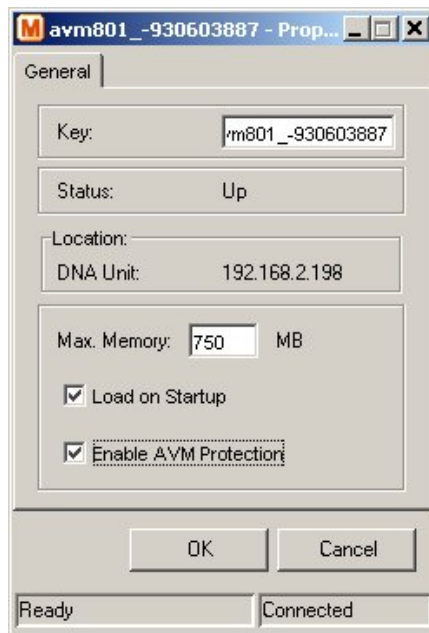
1. Select the *DNA Servers* branch in the *DNA Manage* window's *Tree* pane. The *DNA Servers* branch is displayed.
2. Expand the *DNA Servers* branch and select the required *AVMs* sub-branch in the *Tree* pane.
3. Right-click to display the shortcut menu and select **Properties**,

or

In the toolbar click ,

or

From the *File* menu select **Properties**.

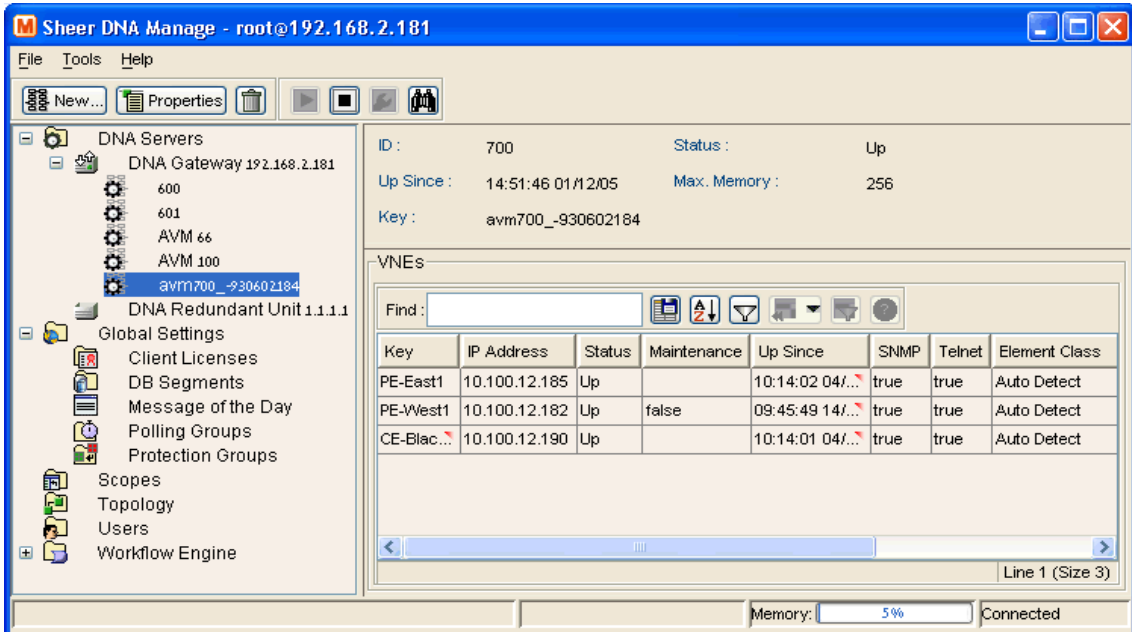


Note: For a detailed description on defining and editing AVMs, refer to the *Chapter 6, Managing AVMs and VNEs* in the *Cisco Active Network Abstraction Administrator's Guide*.

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

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

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



A. High Availability Events

This appendix provides a list of the high availability events displayed in Sheer EventVision and provides the defaults for the failover parameters. (For more information, refer to the *Cisco Active Network Abstraction EventVision User's Guide*.)

Sheer DNA 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) 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 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 DNA 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: DNA Unit = 1.1.1.1 AVM = 107 This is followed by:	Major
	AVM 107 is shutting down. DNA Unit = 1.1.1.1	Minor
	AVM 107 is starting. DNA Unit = 1.1.1.1	Minor
The AVM repeatedly does not respond (see # 4 in the Pre- configured Default Table)	AVM 107 suppressed: DNA 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