



## **Cisco Active Network Abstraction Servers Installation 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



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 NON-INFRINGEMENT 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](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](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](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](mailto: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](mailto: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](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>



## About This Guide

This Installation Guide describes the typical installation of the Sheer Dynamic Network Abstraction (DNA).

This guide also provides a checklist for the user to ensure that the Sheer DNA Gateway and Sheer DNA Units have been installed successfully. This list provides the user with a framework for checking the following:

- The correct versions of the setup have been installed
- All Third Party software is running the correct version
- The directory structure is correct and nothing is missing
- The Web Server is properly configured and running
- The Golden Source is properly configured

This guide is intended for use by network administrators and anyone else responsible for the management, fulfillment, planning and assurance of the integrity of network resources.

It includes the following chapters:

**Chapter 1, Introduction**, describes the Sheer™ DNA platform architecture and functional blocks.

**Chapter 2, System Requirements**, provides the hardware and software installation requirements of the Sheer DNA Gateway and Sheer DNA Unit. In addition, it describes the connectivity requirements.

**Chapter 3, Before Installing**, describes the CDs that cover the installation of all the system components.

**Chapter 4, Installing the Sheer DNA Gateway**, describes the typical installation of a single Sheer DNA Gateway.

**Chapter 5, Installing the Sheer DNA Unit**, describes the steps required to install the Sheer DNA Unit.

**Chapter 6: Checking the Sheer DNA Gateway Installation**, describes how to check the installation of the Sheer DNA Gateway Server.

**Chapter 7: Checking the Sheer DNA Units Installation**, describes how to check the installation of the Sheer DNA Units Server.

**Appendix A, Sheer DNA Folders**

**Appendix B, Security Considerations**, provides brief notes regarding how the installation changes the .rhosts file of the Sheer user.

**Appendix C, Regenerating a Root Password**, explains how to regenerate a Sheer DNA root password.

---

# Table of Contents

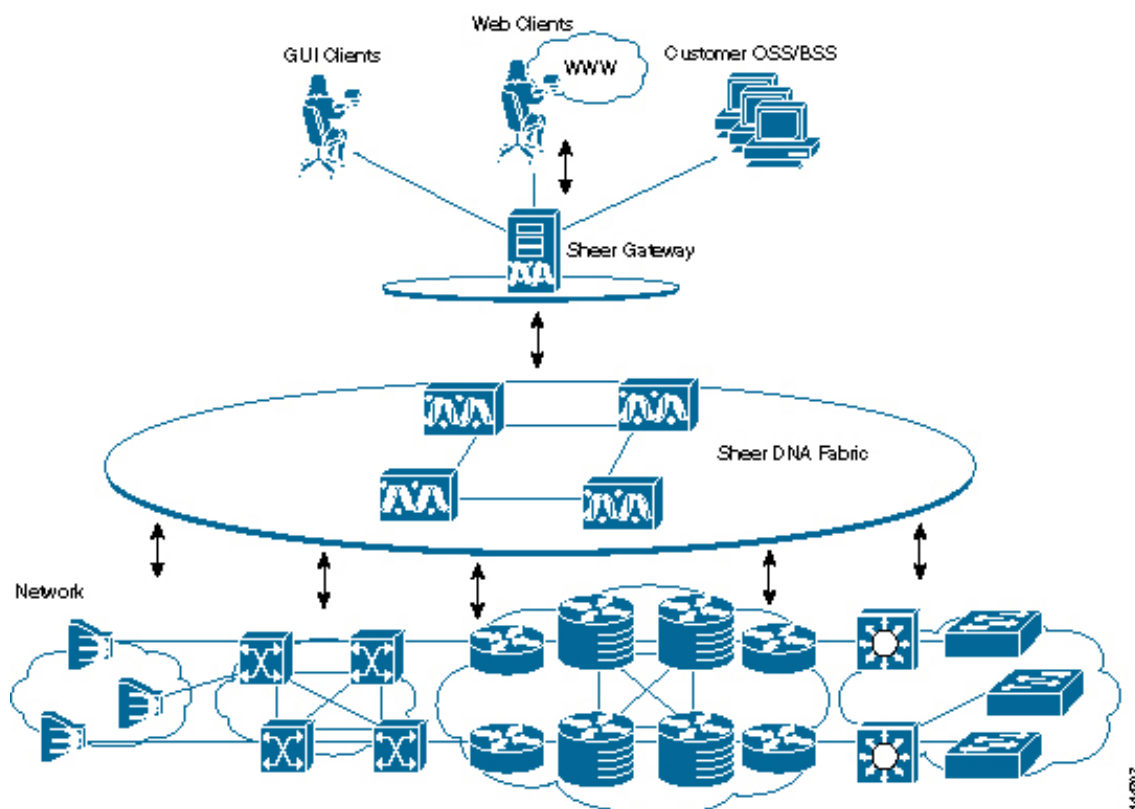
<b>1</b>	<b>Introduction .....</b>	<b>1</b>
1.1.	<b>Sheer DNA Servers .....</b>	<b>2</b>
	Sheer DNA Gateway .....	2
	Sheer DNA Unit .....	2
	Sheer DNA Clients .....	2
1.2.	<b>Sheer DNA Server Ports .....</b>	<b>3</b>
<b>2</b>	<b>System Requirements .....</b>	<b>5</b>
2.2	<b>Sheer DNA Unit.....</b>	<b>6</b>
2.3	<b>Communications .....</b>	<b>7</b>
<b>3</b>	<b>Before Installing .....</b>	<b>9</b>
<b>4</b>	<b>Installing the Sheer DNA Gateway .....</b>	<b>11</b>
4.1	<b>Installing DNA Gateway Server System: Step 1.....</b>	<b>12</b>
4.2	<b>Launching the DNA Gateway: Step 2.....</b>	<b>14</b>
4.3	<b>Verifying the Gateway Installation: Step 3.....</b>	<b>15</b>
4.4	<b>Post-Installation .....</b>	<b>15</b>
4.4.1	Environment Variables .....	17
4.4.2	Aliases .....	17
4.4.3	Users .....	18
4.5	<b>Install the DNA Management Tool: Step 4.....</b>	<b>18</b>
<b>5</b>	<b>Installing the Sheer DNA Unit .....</b>	<b>19</b>
5.1	<b>Installing the DNA Unit System: Step 1 .....</b>	<b>20</b>
5.2	<b>Add the DNA Unit to the DNA Platform: Step 2.....</b>	<b>21</b>
5.3	<b>Launching the DNA Unit: Step 3.....</b>	<b>21</b>
5.4	<b>Verifying the DNA Unit Installation: Step 4.....</b>	<b>22</b>
5.5	<b>Configuring the DNA Unit: Step 5.....</b>	<b>23</b>
5.6	<b>What's Next?.....</b>	<b>23</b>

<b>6</b>	<b>Checking the Sheer DNA Gateway Installation.....</b>	<b>25</b>
6.1	SQL Plus Configuration.....	25
6.2	Sheer Version Information .....	26
6.3	Drools Rules Configuration.....	27
6.4	Web Server and Webstart Configuration .....	28
6.5	Graph Mechanism Configuration .....	29
6.6	Sheer Configuration Files.....	29
6.7	What's Next?.....	30
<b>7</b>	<b>Checking the Sheer DNA Unit Installation.....</b>	<b>31</b>
7.1	Sheer Version Information .....	31
7.2	Key Directories and File Configuration.....	32
7.3	Registry Configuration .....	33
7.4	Golden Source Configuration .....	33
7.5	What's Next?.....	34
<b>A</b>	<b>Sheer DNA Folders .....</b>	<b>35</b>
<b>B</b>	<b>Security Considerations.....</b>	<b>37</b>
<b>C</b>	<b>Regenerating a Root Password.....</b>	<b>39</b>
C.1	Regenerating a lost Sheer DNA root password .....	39

# 1 Introduction

Welcome to the *Cisco Active Network Abstraction Servers Installation Guide, 3.5*. This guide will walk you through a typical Sheer Dynamic Network Abstraction (DNA) installation.

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 Sheer DNA 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.

## 1.1. Sheer DNA Servers

Sheer DNA uses two distinct server types, each performing different activities.

### 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 that 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, 3.5*.

- **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, 3.5*.
- **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, 3.5*.

## 1.2. Sheer DNA Server Ports

The Sheer DNA Server uses the following ports:

Scope	Protocol	Port
<b>Sheer DNA Gateway Northbound</b>		
Sheer NetworkVision	TCP	9770
Sheer NetworkVision	TCP	9771
Sheer NetworkVision - Webstart Edition	TCP	1310
Sheer EventVision	TCP	1521
SSH (for Sheer DNA Shell)	TCP	22
Telnet (for Sheer DNA Shell)	TCP	23
BQL	TCP	9002
Secured remote BQL connections	TCP	9003
Registry Editor	TCP	8011
Registry Editor	TCP	8099
<b>Sheer DNA Gateway Southbound and Intra-Unit Communication</b>		
Transport	TCP	9390
High Availability & Registry Synchronization	TCP	8099
System Administration and Scripts	TCP	512
System Administration and Scripts	TCP	513
System Administration and Scripts	TCP	514
Secure connectivity for System Administration and Scripts	TCP	1101
Time Synchronization (NTP)	UDP	123



## 2 System Requirements

### 2.1 Sheer DNA Gateway

The hardware and software installation requirements are provided below.

**Note:** In the following table, two hardware options are available:

**Minimum** – This is the minimum hardware which is required to install the Sheer DNA Gateway.

**Preferred** – This is the recommended hardware specification, and will also be suitable for future releases of the software.

The hardware recommendations are provided under the assumption and recommendation that Cisco ANA 3.5 will not share the hardware with additional applications.

Item	Specifications
<b>Hardware Requirements (minimum)</b>	
Sun Fire V240	<ul style="list-style-type: none"> <li>• 2 × 1 GHz UltraSPARC® IIIi processors</li> <li>• 8 Gb memory</li> <li>• 2 × 73 Gb HDD space</li> <li>• 1 × DVD drive</li> <li>• 2* 10/100M Ethernet ports</li> </ul>
<b>Hardware Requirements (preferred)</b>	
Sun Fire V490	<ul style="list-style-type: none"> <li>• 4 × 1.5-GHz UltraSPARC IV Processors</li> <li>• 8 Gb memory</li> <li>• 2 × 73 Gb HDD space</li> <li>• 1 × DVD drive</li> <li>• 2* 10/100M Ethernet ports</li> </ul>
<b>Software Requirements</b>	
Operating System	<ul style="list-style-type: none"> <li>• Solaris™ 2.8</li> <li>• Recommended revision 23* kernel patches</li> <li>• Recommended Java™ patch bundle *</li> </ul>
Database	<ul style="list-style-type: none"> <li>• Customer supplied and installed Oracle 9i Enterprise Edition Release 9.2.0.6.0 with partitioning option</li> </ul>

## 2.2 Sheer DNA Unit

The hardware and software installation requirements are provided below.

**Note:** In the following table, two hardware options are available:

**Minimum** – This is the minimum hardware which is required to install the Sheer DNA Gateway.

**Preferred** – This is the recommended hardware specification, and will also be suitable for future releases of the software.

The hardware recommendations are provided under the assumption and recommendation that Cisco ANA 3.5 will not share the hardware with additional applications.

Item	Specifications
<b>Hardware Requirements (minimum)</b>	
Sun Fire V240	<ul style="list-style-type: none"> <li>• 2 × 1GHz and above UltraSPARC ® IIIi processors</li> <li>• 8 Gb memory</li> <li>• 2 × 73 Gb HDD space</li> <li>• 1 × DVD drive</li> <li>• 2* 10/100M Ethernet ports</li> </ul>
<b>Hardware Requirements (preferred)</b>	
Sun Fire V490	<ul style="list-style-type: none"> <li>• 4 × 1.5 GHz UltraSPARC® IV processors</li> <li>• 16 Gb memory</li> <li>• 1 × 73 Gb HDD space</li> <li>• 1 × DVD drive</li> <li>• 2* 10/100M Ethernet ports</li> </ul>
<b>Software Requirements</b>	
Operating System	<ul style="list-style-type: none"> <li>• Solaris™ 2.8</li> <li>• Recommended revision 23*kernel patches</li> <li>• Recommended Java™ patch bundle*</li> </ul>

**Note:** The Sheer DNA Server is fully functional on original Solaris™ 2.8. Cisco recommends you run revision 23\* and Java™ patch bundle\* to ensure security and performance.

## 2.3 Communications

The DNA Platform requires connectivity to all of its tiers as follows:

- DNA Gateway ↔ DNA Units:

The DNA Units Servers have out band management; therefore the DNA Gateway Server needs to have connectivity to all of the DNA Unit Servers.

For further information regarding the ports used, refer to the *Cisco Active Network Abstraction Administrator's Guide, 3.5*.

- DNA Gateway ↔ DNA Clients:

The DNA Clients communicate with the DNA Gateway only, therefore connectivity between the DNA Clients and the DNA Gateway is required.

For further information regarding the ports used, refer to the *Cisco Active Network Abstraction Administrator's Guide, 3.5*.

- DNA Units ↔ Network Elements:

The DNA Unit hosts the VNEs, which require connectivity to the Network Elements (SNMP, Telnet).

For further information regarding the ports used, refer to the *Cisco Active Network Abstraction Administrator's Guide, 3.5*.



### 3 Before Installing

The installation DVD covers the installation of all the system components:

Installation DVD	Description
Gateway Server System and Sheer DNA Servers	<ul style="list-style-type: none"> <li>• Apache Server 2.0.54 hardening based on xianshield apache 2 hardening guide</li> <li>• Sun JDK 1.4.2_06</li> <li>• OpenSSH_4.2p1 hardening based on <a href="http://non-gnu.uvt.nl/pub/uvt-unix-doc/ssh-harden.txt">http://non-gnu.uvt.nl/pub/uvt-unix-doc/ssh-harden.txt</a> guide</li> <li>• ActiveState Active Perl 5.8.6</li> <li>• Cisco ANA Gateway v3.5</li> <li>• Cisco ANA Unit v3.5</li> </ul>
Web Start DNA Clients	<ul style="list-style-type: none"> <li>• Sheer™ DNA Manage v4.0.1</li> <li>• Sheer™ NetworkVision v4.0.1</li> <li>• Sheer™ EventVision v4.0.1</li> </ul>
Configurable Device Management Platform (CDMP)	<ul style="list-style-type: none"> <li>• Includes ALL other Cisco ANA software</li> </ul>
Activation Server	<ul style="list-style-type: none"> <li>• Includes only the Verity Activation Server (formerly Dralasoftware)</li> </ul>
Workflow Client	<ul style="list-style-type: none"> <li>• Includes only the Verity Workflow Client (formerly Dralasoftware)</li> </ul>

Before starting the installation procedure verify the following:

- The installation DVD described above is available.
- The Server machines that are going to be installed comply with the minimum system requirements as specified in the relevant chapter.

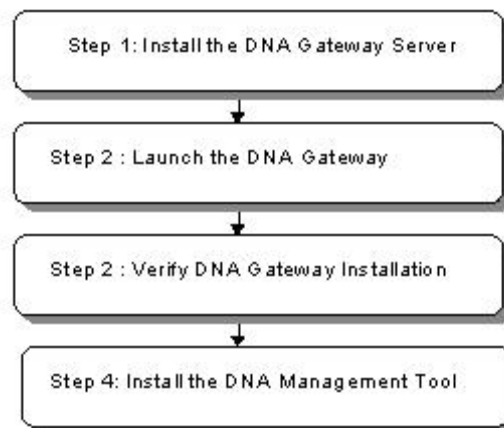
**Note:** The customer supplied Oracle 9i Enterprise Edition Release 9.2.0.6.0 with partitioning option must be installed on the Gateway server before starting the Sheer DNA installation.



## 4 Installing the Sheer DNA Gateway

This chapter covers the typical installation of a single Sheer DNA Gateway. For information about redundancy or multiple installations of the Sheer DNA Gateway, please consult Professional Services.

The workflow below describes the steps required to install the Sheer DNA Gateway in the order in which they should be performed.



**Step 1:** Install the DNA Gateway Server System (specific system installation for the Sheer DNA Gateway), refer to *Section 4.1, Installing the Sheer DNA Gateway*.

**Step 2:** Launch the DNA Gateway, refer to *Section 4.2, Launching the DNA Gateway*.

**Step 3:** Verify the DNA Gateway Installation, refer to *Section 4.3, Verifying the Gateway Installation: Step 3*.

**Step 4:** Install the DNA Management Tool, refer to *Section 4.5*.

**Note:** Only a user with **root** privileges on the Unix box can perform the Sheer DNA Gateway installation.

## 4.1 Installing DNA Gateway Server System: Step 1

During this Step we are going to install tools that are required for the Gateway functionality. These tools include the Apache Web Server and the Third Party Tools, namely, Java™ v1.4.2\_06 and Active Perl v5.8.3.

**Note:** The Server installation script checks for existing 4.x.x version packages, and removes them in a pre-installation phase.

### To install DNA Gateway Server System

1. Verify DVD is in the DVD drive.
2. Open a Telnet/SSH session to the Sheer DNA Gateway machine and login into the machine as “root” user.
3. Check the system prerequisites such as required disk space. For more information, refer to *Chapter 2, System Requirements*.
4. Back up and remove the old version of the Sheer DNA Gateway (if an older version already exists).
5. Change the directory to the CD root directory by executing the following command:

```
cd /cdrom/cdrom0/
```

6. Install the Gateway Server system by invoking the following command:

```
perl install.pl -local_main ./sheer-dna-main.pkg
```

**Note:** Sheer DNA Gateway will install itself to the default directory /export/home/sheer 4.

If you wish to change the installation directory, add the “-dir [desired directory]” switch at the end of the “perl install.pl -local\_main ./sheer-dna-main.pkg” command. For example: “perl install.pl -local\_main ./sheer-dna-main.pkg -dir /opt/sheer”

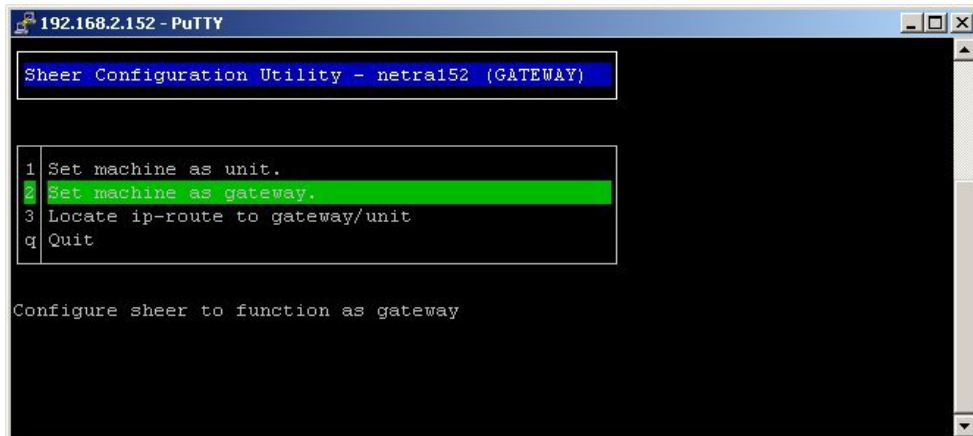
The installation of the DNA Gateway is taking place now. The installation procedure is automatic and requires no interference.

**Note:** This process may take a while. For a further explanation about the DNA environment created during installation, refer to *Appendix A, Sheer DNA Folders*

7. Open a Telnet/SSH session to the Sheer DNA Gateway machine and login into the machine with username **sheer** and password **sheer**.

8. On the first login, the system will prompt you to change the default password. This is highly recommended.
9. Continue installing the gateway Server system by invoking the following command:

```
sheer-conf.pl
```



10. Select **set machine as gateway**. The Sheer DNA configuration utility launches the following post installation utilities:

- a. Database configuration tool - The tool will prompt for Oracle information. In order to attach the system to a local/remote database you will need to supply the Database configuration utility with the following information:
  - i. Oracle home directory location
  - ii. Oracle SID
  - iii. Oracle listener port
  - iv. Schema name
  - v. Schema password
  - vi. Where would you like to save the Data files.

If the Sheer scheme does not exist, the Database configuration utility will prompt the user for:

- i. Oracle admin username: system
- ii. Oracle admin password:
- iii. Password for scheme sheer:

```

Telnet 172.25.127.41
success
success
-----
writing log to /tmp/dblog-1143470728
-----
The system uses Oracle Sqlplus in order to configure the db
Please enter Oracle home directory (E.G: /export/home/oracle/Ora920/) /opt/oracle/Ora920
Please enter Oracle sid: sid
Please enter Oracle admin username: system
Please enter Oracle admin password:
Please enter Password for scheme sheer:
Please enter data files location: /opt/oracle/Ora920/oradata
Please enter Oracle Listener port: 1521
-----
Oracle home directory: /opt/oracle/Ora920
DB address: 127.0.0.1
Oracle SID: sid
Oracle User: sheer
Oracle Port: 1521
Oracle Password: *****
DataFiles location: /opt/oracle/Ora920/oradata
Is this information correct? (y or n) [default y] y

```

- b. Password initiator tool – The tool will ask the user to set all system built-in account passwords.
- c. Time server configuration tool – This tool will configure the XNTP daemon to act as a time server for all units. In order to do so, the tool will prompt the user for the user “root” password.

For information on how to configure the Sheer DNA Gateway for high availability, refer to the *Cisco Active Network Abstraction High Availability User’s Guide, 3.5*.

## 4.2 Launching the DNA Gateway: Step 2

After installing the Server System and the Sheer DNA Gateway software we are ready to launch the Sheer DNA Gateway.

### To launch the Sheer DNA Gateway

1. Open a Telnet/SSH session to the Sheer DNA Gateway machine and login into the machine as user “sheer”, default password “sheer”.
2. Launch the DNA Gateway by executing the initialization command:

```
mvm.csh
```

The DNA Gateway process is now loading.

**Note:** The DNA Gateway loading process may take a while.



```
set autolist
set autoexpand
set autocorrect
set color
set history=5000
set savehist=5000
set notify
set complete="enhance"
set savehist
set correct=cmd
set autologout=0
set color
set colorcat

# --- env settings
setenv SHEERHOME ~sheer
setenv PAGER less
setenv JAVA_HOME $SHEERHOME/java
setenv PERL_HOME $SHEERHOME/perl
setenv PERL_VER "5.8.6"
setenv MANPATH /usr/local/mrtg-2/man:/usr/local/net-
snmp/man:/usr/local/man:/usr/local/ActivePerllocal/samba/man:/usr/local/ActiveP
erl-5.6/man:/usr/local/ssl/man
setenv EDITOR vi
setenv LD_LIBRARY_PATH $SHEERHOME/local/lib/gen:$SHEERHOME/Third_Party/lib
setenv SHEERPATH
.:$SHEERHOME/perl/bin:$SHEERHOME/local/lib/gen:$SHEERHOME/local/bin:$SHEERHOM
Eain/scripts:$SHEERHOME/python/bin:$SHEERHOME/Main/setup

setenv PATH
${SHEERPATH}:/usr/bin:/usr/sbin:/usr/etc:/usr/ucb:/usr/local/bin:/usr/local/
net-sn

setenv PERLLIB
"../${SHEERHOME}/local/lib/perl/gen:${SHEERHOME}/local/lib/perl/sheer:${SHEER
HOMperl/lib/${PERL_VER}:${SHEERHOME}/perl/lib/site_perl/${PERL_VER}/sun4-
solaris-thread-multi:${SHite_perl}:${SHEERHOME}/Main"

setenv SHEER_LOGIN_INFO 1
setenv SHEER_COMMUNICATION_METHOD ssync

# --- other settings
```

```

limit descriptors 1024

# --- sourcing
if ( -f $SHEERHOME/.aliases ) then
    source $SHEERHOME/.aliases
endif
if ( -f $SHEERHOME/db/.db ) then
    source $SHEERHOME/db/.db
endif
if ( -f $SHEERHOME/Main/.sheer ) then
    source $SHEERHOME/Main/.sheer
endif

```

For details on checking the Sheer DNA Gateway installation, see *Chapter 6, Checking the Sheer DNA Gateway Installation*.

#### 4.4.1 Environment Variables

The installation script automatically defines the following environment variables:

Variable Name	Content
SHEER_HOME	/export/home/sheer4
JAVA_HOME	/export/home/sheer4/java
SHEER_COMMUNICATION_METHOD	rcp

**Note:** The SHEER\_HOME variable content "/export/home/sheer4" will change according to the DNA Gateway installation directory. (For details, see *Step 1* in the *Install DNA Gateway Server System* section on page 12).

#### 4.4.2 Aliases

The installation script automatically defines the following aliases:

Table Alias	Content
sheer	Changes directory to: ~sheer/Main
reg	Changes directory to: ~sheer/Main/registry
main	Changes directory to:

Table Alias	Content
	~sheer/Main
logs	Changes directory to: ~sheer/Main/logs

### 4.4.3 Users

The installation script automatically creates a Unix user called “sheer” with a default password “sheer”. This user is privileged to launch the Sheer DNA and to perform all required Sheer functionality.

## 4.5 Install the DNA Management Tool: Step 4

Sheer DNA Manage is the GUI tool used for performing various system administration activities. It provides an interface to perform the following:

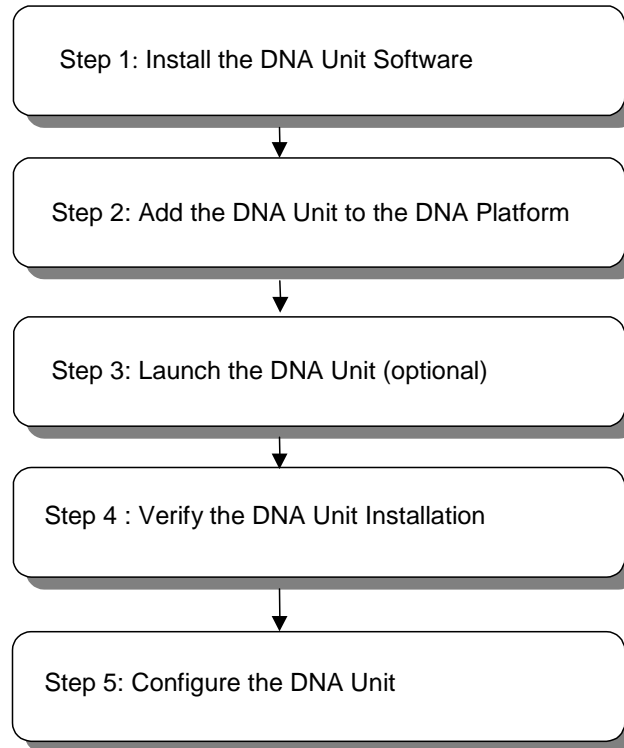
- **Sheer DNA Unit Management:** Adding and removing Units, and setting up Sheer DNA Unit redundancy.
- **Agent Virtual Machines (AVMs) and VNEs Management:** Adding and removing AVMs and VNEs for the different Sheer DNA Units. Starting and stopping VNEs, setting polling information per VNE.
- **Global Settings Management:** Setting up polling groups to be used by the VNEs and defining a service disclaimer (message of the day).
- **Scope, User and Security Management:** Setting up scopes of devices, system users and security levels.
- **Topology Management:** Managing static and persistent topology links.

For more information about installing the Sheer DNA Manage tool, refer to the *Cisco Active Network Abstraction Client Installation Guide, 3.5*.

**Note:** The installation procedure changes the .rhosts file of the Sheer user. For more information, refer to *Appendix B, Security Considerations*.

## 5 Installing the Sheer DNA Unit

The workflow below describes the steps required to install the Sheer DNA Unit in the order in which they should be performed.



**Step 1:** Install the DNA Unit System, refer to *Section 5.1, Installing the DNA Unit System: Step 1*.

**Step 2:** Add the DNA Unit to the DNA Platform, refer to *Section 5.2, Add the DNA Unit to the DNA Platform: Step 2*.

**Step 3:** Launch the DNA Unit (optional), refer to *Section 5.3, Launching the DNA Unit: Step 3*.

**Step 4:** Verify the DNA Unit Installation, refer to *Section 5.4, Verifying the DNA Unit Installation: Step 4*.

**Step 5:** Configure the DNA Unit, refer to *Section 5.5, Configuring the DNA Unit: Step 5*.

For information about restarting the Sheer DNA platform, refer to the *Cisco Active Network Abstraction Administrator's Guide, 3.5*.

## 5.1 Installing the DNA Unit System: Step 1

During this Step we are going to install tools that are required for the DNA Unit functionality, namely, Java™ v1.3.1\_09 and Active Perl v5.6.1.

### To install DNA Unit System

1. Verify the DVD is in the DVD drive.
2. Open a Telnet/SSH session to the Sheer DNA Gateway machine and login into the machine as “root” user.
3. Check the system prerequisites such as required disk space. For more information, refer to *Chapter 2, System Requirements*.
4. Back up and remove the old version of the Sheer DNA Gateway (if an older version already exists).
5. Change the directory to the CD root directory by executing the following command:

```
cd /cdrom/cdrom0/
```

6. Install the Unit system by invoking the following command:

```
perl install.pl -unit -local_main ./sheer-dna-main.pkg
```

**Note:** If you used the “-dir [desired directory]” switch to change the directory at the Sheer Gateway, you must install the DNA Unit to the same directory.

To change the installation directory, add “-dir [desired directory]” switch at the end of the “perl install.pl -unit -local\_main ./sheer-dna-main.pkg” command. For example: “perl install.pl -unit -local\_main ./sheer-dna-main.pkg -dir /opt/sheer”

**Important:** If you did not use the “-dir [desired directory]” switch when you installed the Sheer Gateway, **DO NOT** use it here.

The installation of the DNA Unit is taking place now. The installation procedure is automatic and requires no interference.

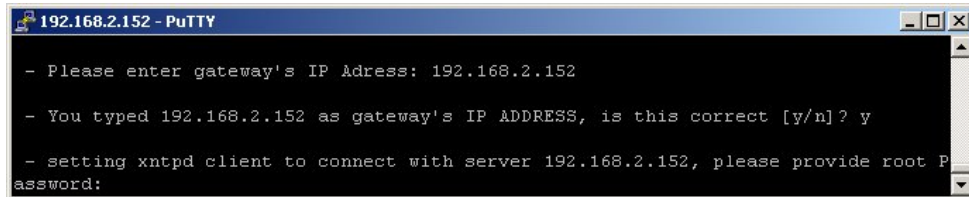
**Note:** This process may take a while. For a further explanation about the DNA environment created during installation, refer to *Appendix A, Sheer DNA Folders*.

7. Open a Telnet/SSH session to the Sheer DNA Unit machine and login into the machine as “sheer” user.

8. Continue installing the Unit system by invoking the following command:

```
sheer-conf .pl
```

9. Select “set machine as unit” and the Sheer DNA configuration utility will request the IP address of the Gateway machine and verify input (y).



```
192.168.2.152 - PuTTY
- Please enter gateway's IP Address: 192.168.2.152
- You typed 192.168.2.152 as gateway's IP ADDRESS, is this correct [y/n]? y
- setting xntpd client to connect with server 192.168.2.152, please provide root Password:
```

10. Insert user “root” password and Unit installation is complete.

For information on how to configure the Sheer DNA Gateway for high availability, refer to the *Cisco Active Network Abstraction High Availability User's Guide, 3.5*.

## 5.2 Add the DNA Unit to the DNA Platform: Step 2

Adding a DNA Unit to the DNA platform entails defining that Unit in the system (so that the DNA Gateway is aware of it). When the DNA Unit is added it automatically connects to the transport fabric so that it is able to communicate with the other elements in the system.

### To add the DNA Unit

Add the DNA Unit using Sheer DNA Manage; refer to the *Cisco Active Network Abstraction Administrator's Guide, 3.5*. Sheer DNA Manage automatically registers the DNA Unit in the registry and creates a transport uplink between the DNA Unit and the Gateway.

## 5.3 Launching the DNA Unit: Step 3

After installing the DNA Unit, you can launch the Sheer DNA Unit (optional). The Sheer DNA Gateway automatically verifies that the DNA Unit is up when it is added to the setup and if it is down the Sheer DNA Gateway starts it.

### To launch the DNA Unit

1. Open a Telnet/SSH session to the Sheer DNA Unit machine and login into the machine as user “sheer”, default password “sheer”.

2. Launch the DNA Unit by executing the initialization command:

```
mvm.csh
```

The DNA Unit process is now loading.

**Note:** The DNA Unit loading process may take a while.

## 5.4 Verifying the DNA Unit Installation: Step 4

This Step enables you to verify that the DNA Unit processes are up and running. The Gateway Server processes are as detailed below:

- AVM 0: transport switch process
- AVM 99: management process
- AVM XXX: any AVM defined on the Unit to load upon VNEs. At this installation Step, no AVMs were added yet.
- Webserver daemon: Client connection process
- Sheer\_secured daemon

### To verify the Sheer DNA Unit process

- Check that the status of all processes and daemons by executing the following command:

```
status
```

The output will list all of the processes:

```

192.168.2.152 - PuTTY
sheer@netra152 [~]# status
# # ##### ##### ## # ##### #####
## # # # # # # # # # #
# # # ##### # # # # # # ##### #####
# # # # # ##### ##### # # #
# ## # # # # # # # # # #
# # ##### # # # # # # ##### #####

Welcome to netra152 running sheer UNIT, version 4.0.0.

- Checking for xntp daemon... [OK]
- Checking for sheer_secured daemon... [OK]
- Checking for webserver daemon... [OK]

sheer@netra152 [~]#

```

## 5.5 Configuring the DNA Unit: Step 5

At this step the Unit is installed and ready to host VNEs. For information about setting up AVMs and VNEs using Sheer DNA Manage, refer to the *Cisco Active Network Abstraction Administrator's Guide, 3.5*.

**Note:** Before creating any AVMs on the Sheer DNA Unit the transport uplinks should be in place.

## 5.6 What's Next?

After installing the DNA Gateway Server and the DNA Units Servers, the system is up and ready to use. The client application can now be installed to enable the user to view the network. For detailed information, refer to the *Cisco Active Network Abstraction Client Installation Guide, 3.5*.

**Note:** The installation procedure changes the .rhosts file of the Sheer user. For more information, refer to *Appendix B, Security Considerations*.



## 6 Checking the Sheer DNA Gateway Installation

This chapter describes how to check the installation of the Sheer DNA Gateway Server.

**SQL Plus Configuration**, Page 25 describes how to check that the Server is available and properly configured.

**Sheer Version Information**, Page 26 describes how to check the version of Sheer installed on the Server.

**Drools Rules Configuration**, Page 27 describes how to check the Drools rules files that are being used.

**Web Server and Webstart Configuration**, Page 28 describes how to check the Web Server and Sheer Webstart mechanism.

**Graph Mechanism Configuration**, Page 29 describes how to check that the graph mechanism.

**Sheer Configuration Files**, Page 29 describes how to check the Sheer configuration files.

**What's Next?** , Page 30 describes the next step after completing the check of the Sheer DNA Gateway.

### 6.1 SQL Plus Configuration

#### Description

This step checks that the Server is available and properly configured. In addition, it checks that the database is up and running, and has been configured properly.

#### Steps

1. On the Server run the following command:

```
sqlplus USER/PASSWORD
```

2. Check that the SQL client can connect to the database.

## Successful Result

The following prompt appears:

```
SQL*Plus: Release 9.2.0.1.0 - Production
on Sun Apr 10 09:40:01 2005

Copyright (c) 1982, 2002, Oracle
Corporation. All rights reserved.

Connected to:

Oracle9i Enterprise Edition Release
9.2.0.1.0 - Production

With the Partitioning option

JServer Release 9.2.0.1.0 - Production

SQL>
```

## Failure

Test failure indicates Database error, please contact your local Database administrator and repeat the test.

## 6.2 Sheer Version Information

### Description

This step checks the version of Sheer DNA installed on the Server. In addition, it also checks that the major parts of the Sheer DNA system are properly located and running.

Note: This test also checks a few additional characteristics of the installation such as directories, classes and so on.

If there are any files missing or problems with the configuration, this step will fail.

### Steps

1. On the Server run the following command:

```
runavm.csh -version
```

2. Check that the correct version of Sheer has been installed.

**Successful Result**

The version, build, and customer information installed on the setup is displayed.

**Actual Sample Result**

```
AVM OS v3.4.0 (045) (BC-VPN)
```

**Failure**

Rerun the installation.

## 6.3 Drools Rules Configuration

**Description**

This step checks that the five Drools rules files that are being used have been properly created.

**Steps**

1. On the Server make sure that the following directory exists:

```
~/Main/data
```

2. Check that the directory contains the following five files:
  - alarms.bom
  - alarms.ilr.clearn
  - alarms.ilr.full
  - post.ilr
  - pre.ilr

**Successful Result**

The five Drools rules files exist in the directory.

**Failure**

Rerun the installation.

## 6.4 Web Server and Webstart Configuration

### Description

This step checks that the:

- Web Server has been properly configured and is running.
- Sheer Webstart mechanism has been properly configured.

### Steps

1. Open a web browser on the PC client connected to the Server.
2. Enter the following URL in order to try and connect to the Sheer DNA Gateway URL:

```
http://<GW-  
IP>:1310/webstart/networkvision.jnlp
```

For example, if the Sheer DNA Gateway IP address is 192.168.2.152, enter the following URL:

```
http://192.168.2.152:1310/webstart/netwo  
rkvision.jnlp
```

### Successful Result

- The networkvision.jnlp file is found.
- The web browser locates the file and tries to open or save (download) the file depending on the configuration of the web Server.
- The Webstart directory and Apache have been properly installed.

**Note:** The jnlp file will return the following error from the webserver. This is an expected error.

*An error occurred while launching/running the application.*

*Category: Launch File Error*

*The field <jnlp><information><homepage>href has an invalid value: home.html*

### Failure

- Check that the Apache Server is running on the Sheer DNA Gateway.

Check that the webserver daemon is up and running by typing the command “status” on the Sheer DNA Gateway server:

If the webserver daemon is down, load it by typing the command “startWeb.cmd”:

- Check that the directory ~/Main/webstart and all of its sub-directories and files have execute privileges.

## 6.5 Graph Mechanism Configuration

### Description

This step checks that the graph mechanism is working properly.

### Steps

1. Open a web browser on the PC client connected to the Server.
2. Enter the following URL in order to try and connect to Sheer DNA Graph:

```
http://<GW-IP:1310>/graphs/
```

### Successful Result

The graphs are properly opened in the web browser.

### Failure

Check the configuration of the web browser.

## 6.6 Sheer Configuration Files

### Description

This step checks the Sheer configuration files, namely, the following:

- What AVMs should run
- What Units are configured

### Steps

1. On the Server browse to the following directory:

```
~/Main/registry/ConfigurationFiles
```

2. Check that the directory contains the following two sub-directories.
  - 127.0.0.1
  - 0.0.0.0



# 7 Checking the Sheer DNA Unit Installation

This chapter describes how to check the installation of the Sheer DNA Units Server.

**Sheer Version Information**, page 29, describes how to check the version of Sheer installed on the Server.

**Key Directories and File Configuration**, page 30, describes how to check that several key directories and files exist in the setup.

**Registry Configuration**, page 31, describes how to check that the Registry directory has been properly created.

**Golden Source Configuration**, page 31, describes how to check that the Golden Source has been properly configured.

**What's next?**, page 32, describes the next step after completing the check of the Sheer DNA Units.

## 7.1 Sheer Version Information

### Description

This step checks the version of Sheer installed on the Server. In addition, it also checks that the major parts of the Sheer system are properly located and running.

Note: This test also checks a few additional characteristics of the installation such as directories, classes and so on.

If there are any files missing or problems with the configuration, this step will fail.

### Steps

1. On the Server run the following command:

```
runavm.csh -version
```

2. Check that the correct version of Sheer has been installed.

### Successful Result

The version, build, and customer information installed on the setup is displayed.

### Actual Sample Result

```
AVM OS v3.4.0 (045) (BC-VPN)
```

### Failure

Rerun the installation.

## 7.2 Key Directories and File Configuration

### Description

This step checks that several key directories and files exist in the setup.

### Steps

1. Check that the license.jar file exists on the Server in the following directory:

```
~/Main
```

2. Check that there is a scheme sub-directory in the following directory and that it contains the proper scheme files:

```
~/Main
```

3. Check that the scripts and unix sub-directories were properly created in the following directory:

```
~/Main
```

### Successful Result

- The license.jar file exists in the directory.
- The scheme sub-directory exists.
- The scripts and unix sub-directories exist.

### Failure

Rerun the installation.

## 7.3 Registry Configuration

### Description

This step checks that the Registry directory has been properly created and contains the necessary files.

### Steps

- On the Server browse to the following directory:

```
~/Main/registry/
```

### Successful Result

The Registry directory exists and contains the necessary files.

### Failure

Rerun the installation.

## 7.4 Golden Source Configuration

### Description

This step checks that the Golden Source has been properly configured on the Unit.

### Steps

1. On the Server locate and open the following file:

```
~/Main/registry/avm99.xml
```

2. Check that the file contains an entry for the key “parent”, which is the value of the IP of the Sheer DNA Gateway.

### Successful Result

The file contains an entry for the key “parent”, which is the value of the IP of the Sheer DNA Gateway.

### Failure

Rerun the installation.

## 7.5 What's Next?

After the installation of the Sheer DNA Units has been checked, the system is up and ready to use. The client application can now be installed to enable the user to view the network. For detailed information, refer to the *Cisco Active Network Abstraction Client Installation Guide, 3.5*.

## A Sheer DNA Folders

This appendix provides a list of the folders created in Sheer DNA.

<code>~sheer/Main/bosconfig</code>	DNA configuration files. These files contain the syntax of the DNA Commands, the errors supported by the DNA and the DNA connection configuration.
<code>~sheer/Main/bosconfig/bos_shell_scripts</code>	DNA user-created scripts.
<code>~sheer/Main/data</code>	Drools configuration files and user-defined scripts.
<code>~sheer/Main/logs</code>	Log output files. Each AVM has its own output file named using the convention <code>&lt;AVM-ID&gt;.out</code> , for example, <code>0.out</code> or <code>11.out</code> .
<code>~sheer/Main/registry</code>	Local copy of registry files.
<code>~sheer/Main/registry/ConfigurationFiles</code>	Golden Source configuration files in Sheer DNA Gateway.
<code>~sheer/Main/registry/templates</code>	Registry file templates used by Sheer DNA Gateway for global system changes.
<code>~sheer/Main/RPC/XML</code>	XML RPC configuration files.
<code>~sheer/scripts</code>	Maintenance scripts of the Sheer DNA Unit.
<code>~sheer/Main/Third_Party</code>	Third-party files.
<code>~sheer/Main/unix</code>	Unix maintenance scripts and utilities.



## **B Security Considerations**

### **B.1 Automatically Generating the .rhosts File**

The installation procedure sets up access privileges for the Sheer DNA Gateway and the Sheer DNA Units. These privileges are defined in the .rhosts file of the root account in each machine. These files must remain intact.

The current configuration for Sheer users in all machines is + + which means any user from any machine. If the user's security policy prohibits such promiscuous behavior, then be advised that remote access is required between the Sheer DNA Gateway and all of its Sheer DNA Units in both directions.

If any changes are made to the .rhosts files in the machine please verify (using rlogin or similar software) that access is enabled for the Sheer user from the Sheer DNA Unit to the Sheer DNA Gateway and vice-versa.



## C Regenerating a Root Password

### C.1 Regenerating a lost Sheer DNA root password

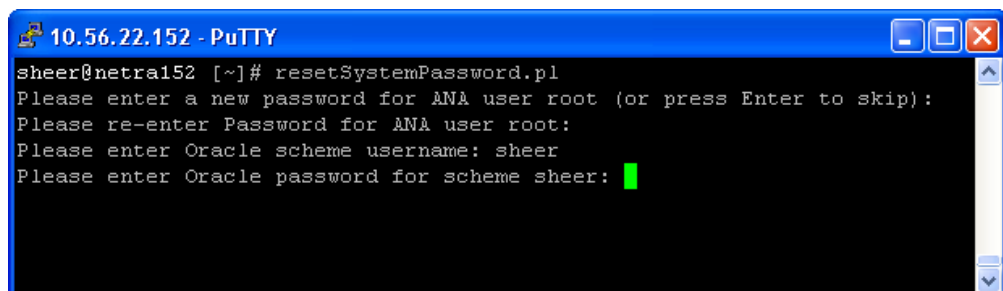
The system allows you to regenerate a lost Sheer DNA root password, as follows:

1. Open a Telnet/SSH session to the Sheer DNA Gateway machine and login with username **sheer** and password **sheer**.
2. Run the system password reset tool by invoking the following command:

```
resetSystemPassword.pl
```

Note: The Sheer DNA database should be up and running before running the system password reset tool.

3. The tool will prompt for the following parameters:
  - a. New password for ANA user root.
  - b. Oracle scheme username.
  - c. Oracle scheme password.



```
10.56.22.152 - PuTTY
sheer@netra152 [~]# resetSystemPassword.pl
Please enter a new password for ANA user root (or press Enter to skip):
Please re-enter Password for ANA user root:
Please enter Oracle scheme username: sheer
Please enter Oracle password for scheme sheer: █
```

4. In any case of failure, check the Oracle scheme username and password provided and try again.

