

TRAINEE GUIDE
FOR
GLOBAL COMMAND AND CONTROL SYSTEM – MARITIME (GCCS-M) 4.0
SYSTEM ADMINISTRATION COURSE

CIN: A-150-0045



Prepared For

COMMANDING OFFICER
CENTER FOR INFORMATION DOMINANCE
53690 TOMAHAWK DRIVE, SUITE 144
SAN DIEGO, CA 92147-5080

Prepared By

NORTHROP GRUMMAN MISSION SYSTEMS
9326 SPECTRUM CENTER BLVD.
SAN DIEGO, CA 92123

January 2006

THIS PAGE INTENTIONALLY LEFT BLANK

CHANGE RECORD

Number and Description of Change	Entered By	Date

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

<u>Contents</u>	<u>Page</u>
Change Record	3
Security Awareness Notice	7
Safety/Hazard Awareness Notice	9
How to Use Your Trainee Guide	11
Terminal Objectives	13
Unit 1 GCCS-M Overview	15
Unit 2 Introduction to Solaris	73
Unit 3 Load, Configure, and Maintain GCCS-M	161
Unit 4 Integrated Imagery and Intelligence Administration	273

THIS PAGE INTENTIONALLY LEFT BLANK

SECURITY AWARENESS NOTICE

 *
 * This course does not contain any classified material. *
 *

THIS PAGE INTENTIONALLY LEFT BLANK

SAFETY/HAZARD AWARENESS NOTICE

This notice promulgates safety precautions to the staff and trainees of the System Administration Course in accordance with responsibilities assigned by the Naval Education and Training Command.

Trainees may voluntarily request termination of training. Any time the trainee makes a statement such as "I QUIT," or "DOR," (Drop on Request), he or she shall be immediately removed from the training environment and referred to the appropriate division or training officer for administrative action. The trainee must then make a written statement, clearly indicating the desire to DOR.

Any time a trainee or instructor has apprehension concerning his or her personal safety or that of another, he or she shall signal for a "**Training Time Out**" to clarify the situation or procedure and receive or provide additional instruction as appropriate. "Training Time Out" signals, other than verbal, shall be appropriate to the training environment.

Instructors are responsible for maintaining situational awareness and shall remain alert to signs of trainee panic, fear, extreme fatigue or exhaustion, or lack of confidence that may impair safe completion of the training exercise, and shall immediately stop the training, identify the problem, and make a determination to continue or discontinue training. Instructors shall be constantly alerted to any unusual behavior which may indicate a trainee is experiencing difficulty, and shall immediately take appropriate action to ensure the trainee's safety.

The safety precautions contained in this course are applicable to all personnel. They are basic and general in nature. Personnel who operate or maintain equipment in support of System Administration Course must be thoroughly familiar with all aspects of personnel safety, and strictly adhere to every general as well as specific safety precautions contained in operating and emergency procedures and applicable governing directives.

Special emphasis must be placed on strict compliance with published safety precautions and on personal awareness of potentially hazardous conditions peculiar to diving.

All personnel must have a comprehensive knowledge of emergency procedures, which prescribe courses of action to be followed in the event of equipment failure or human error as stated in the Pre-Mishap Plan. Strict adherence to approved and verified operating, emergency, and maintenance procedures is MANDATORY. As a minimum, each individual is responsible for knowing, understanding, and observing all safety precautions applicable to the command, school, course, their work, and their work areas. In addition, you are responsible for observing the following general safety precautions:

SAFETY/HAZARD AWARENESS NOTICE (CONT.)

- a. Each individual shall report for work rested and emotionally prepared for the task's at hand.
- b. You shall use normal prudence in all your functions, commensurate with the work at hand.
- c. You shall report any unsafe conditions, or any equipment or material which you consider to be unsafe, and any unusual or developing hazards.
- d. You shall warn others whom you believe to be endangered by known hazards or by failure to observe safety precautions, and of any unusual or developing hazards.
- e. You shall report to the school any mishap, injury, or evidence of impaired health occurring in the course of your work or during non-training environment.
- f. You shall wear or use the protective clothing and/or equipment of the type required, approved, and supplied for the safe performance of your work.
- g. All personnel in the immediate vicinity of a designated noise hazardous area or noise hazardous operation shall wear appropriate hearing protective devices. (NDSTC Instruction 6260.6 series)

HOW TO USE THIS TRAINEE GUIDE

This publication has been prepared for your use while under instruction. It is arranged in accordance with the topics taught, and is in sequence with those topics. By using the table of contents, you should be able to locate the lesson topics easily. By following the enclosed course schedule, you should be able to follow the course of instruction in a logical manner.

Under each topic, there may be the following instruction sheets:

- **OUTLINE SHEETS**: Provide a listing of major teaching points. The outline is consistent with the outline of the discussion points contained on the DDA pages in the lesson plan. It allows the trainee to follow the progress of lesson topic, to take notes as desired, and to retain topic information for future reference.
- **INFORMATION SHEETS**: Amplify supplemental information from the reference materials for the course, from technical manuals, or from instruction books. You may be tested on this material during the course.
- **PROBLEM SHEETS**: Normally used for paperwork troubleshooting when the equipment is not available. Can also be used for drill-and-practice problems related to the topic.
- **JOB SHEETS**: Provide step-by-step instructions for developing your skills in performing assigned tasks and maintaining the equipment when and where the work is assigned, in the laboratory or practical areas.
- **ASSIGNMENT SHEETS**: To assist you in being prepared for the lesson topics and laboratory/practical exercises BEFORE they are presented by the instructor or occur in the course.
- **DIAGRAM SHEETS**: These are used as necessary to simplify the instruction. They are to aid you in understanding the systems, equipment, or topics presented.

All of the instruction sheets are identified by their unit and lesson topic number. They are listed in the order of their use. Each lesson topic will contain at least one Enabling Objective.

The Enabling Objectives listed in this Guide specify the knowledge and/or skills that you will learn during the course, and reflect the performance expected of you on the job. The Enabling Objectives specify the knowledge and/or skills you will learn in a specific lesson topic. You should thoroughly understand the Enabling Objectives for a lesson topic and what these objectives mean to you before you start each lesson topic. Each learning objective contains behavior(s), conditions, and standards.

They are defined as follows:

The behavior is a description of the performance and/or knowledge that you will learn in that lesson topic;

The conditions under which you will be able to perform or use the knowledge;

The standard(s) to which you will be able to perform or use the knowledge.

The objectives provide a means by which you can check your progress during training. The objectives also enable you to evaluate your training when you have finished, so you can ensure that you have satisfied the goals of the course. Your instructor will explain the objectives to you at the start of the course. Feel free to ask for additional information during training if you feel that you are not learning, as you should.

- STUDY TECHNIQUES:

Classroom and laboratory sessions will be conducted by one or more instructors. You will be responsible for completing the material in this guide, some of it before class time. Prior to starting to use this guide, read through the front matter and become familiar with the organization of the material, then follow directions below for each lesson topic:

1. READ the Enabling Objectives for the lesson topic and familiarize yourself with what will be expected of you.
2. STUDY each reading assignment.
3. WRITE any written assignment.

- EXAMINATIONS AND QUIZZES

Exams and quizzes will be administered as required by the Course Master Schedule. A blitz is an informal test used to check for understanding, and may be given by your instructor at any time. These quizzes do not count toward your final grade. In any event, only the material covered will be tested. All written tests will be in the form of multiple choice, completion, or true/false items. Performance tests will be provided to test job skills as appropriate. Success on exams is dependent upon an understanding of the objectives, involvement in class activities, and good study habits.

TERMINAL OBJECTIVES

- 1.0 **DESCRIBE** GCCS-M software components, and how they are managed.
- 2.0 **IDENTIFY** current hardware in the GCCS-M architecture.
- 3.0 **PERFORM** basic Solaris system administration techniques related to GCCS-M.
- 4.0 **PERFORM** GCCS-M software installations, configuration techniques, and administration procedures from a Load Plan.

THIS PAGE INTENTIONALLY LEFT BLANK

ASSIGNMENT SHEET 1-1-1 INTRODUCTION TO GCCS-M

A. Introduction

This assignment sheet is to be completed as homework as assigned.

B. Enabling Objectives

- 1.1 **DISCUSS** applicable safety and security concerns when performing system administration.
- 1.2 **DISCUSS** applicable security requirements for GCCS-M.
- 1.3 **DISCUSS** the history and functionality of GCCS-M.
- 1.4 **DESCRIBE** the purpose of each GCCS-M server.
- 1.5 **ACCESS** the web applications utilized by GCCS-M.
- 1.6 **DISPLAY** the ability to effectively navigate the System Chart.

C. Study Assignment

Read Information Sheet 1-1-2, 1-1-4

Complete Job Sheet 1-1-3

D. Study Questions

1. What different security classifications are associated with GCCS-M?

2. List each of the Sun Servers and the aliases used for GCCS-M.

3. List the major functions of each GCCS-M server onboard a large deck ship
 - a. Communications (comms1 / comms2)-
 - b. Intelligence (intel)-
 - c. Web server (websvr)-
4. List all web applications on the websvr and the corresponding hyperlink.
5. Under which Chart toolbar is the declutter icon located?
6. Describe the functions performed by the UCP master.
7. Which server is responsible for providing access to the Intel databases?

INFORMATION SHEET 1-1-2

INTRODUCTION TO GCCS-M

A. **Introduction**

This lesson will provide the trainee a basic understanding and background of the history of Global Command and Control System – Maritime (GCCS-M) as well as an introduction to technologies and methods used in GCCS-M 4.x.

B. **References**

1. Embedded Online Documentation

C. **Information**

1. History of GCCS-M
 - a. GCCS-M provides a complete command and control solution to the Fleet, with interfaces to a variety of communications and computer systems.
 - b. Program management
 - (1). GCCS-M is the Naval Command and Control system implemented by the Space and Naval Warfare Systems Command (SPAWARSYSCOM).
 - c. GCCS-M evolution
 - (1). Global Command and Control System –Maritime (GCCS-M) provides Joint and Allied Afloat Commanders a single, integrated Command, Control, Communications, Computers and Intelligence (C4I) system that receives, processes, displays and maintains current geo-location information on friendly, hostile and neutral land, sea and air forces with intelligence and environmental information. GCCS-M integrates COTS hardware and software to facilitate network connectivity onboard ships and Battle Group/Amphibious Ready Group (BG/ARG) Joint Task Forces. GCCS-M is currently operational on most surface combatants in the US Navy including Aircraft Carriers, Command ships, Amphibious ships, Cruisers, Destroyers, Frigates, Mine-Sweepers, and Supply ships.

- (2). The GCCS-M model has evolved as a product of initiatives designed to fuse the functionality of multiple C4I systems into a single system architecture and platform. Each of these C4I systems has satisfied a sub set of the Fleet's C4I requirements.
 - (3). In most cases, these systems were nearing the end of their life cycle and were becoming expensive to maintain. Because most systems were based upon proprietary hardware, software and communication standards, the exchange of data was difficult and expensive, generally requiring unique communication interfaces to be developed.
 - (4). Over time, the Joint Operational Tactical System (JOTS) morphed into Navy Tactical Command System-Afloat (NTCS-A) then to Joint Maritime Command Information System (JMCIS) and then into GCCS-M. With the advent of the 4.0 version of software, tactical functions will be accessible from any configured network computer.
2. Security classification of GCCS-M
 - a. GCCS-M is classified at the SECRET level when fully installed with functional SECRET databases. There are also Sensitive Compartmented Information (SCI) and Unclassified variants.
3. The purpose of GCCS-M is to disseminate intelligence and surveillance data in support of warfare mission planning, execution, and assessment.
4. GCCS-M is critical to many different areas, such as strike mission planning, anti-submarine warfare, mine countermeasures, and surface warfare.
5. Standard Afloat Configuration (UNIX servers): Communications server (comms1), Back-up Server (comms2) Intelligence/Imagery server and Web Server.
 - a. Communications server (comms1 or comms2).
 - (1). (As Configured) Universal Communications Processor (UCP) Master.
 - (2). (As Configured) Track Management Server (TMS) Master.
 - (3). (As Configured) Accounts and Profiles Manager (APM) Master and NIS + Master.
 - (4). Replaces JOTS 1, 2 and 12
 - (5). The link to incoming and outgoing communications.

- (6). Communications to Naval Message Automated Communications System (NAVMACS) via the Secret Server and Defense Messaging Distribution System (DMDS)
- (7). Manages communication channels such as Officer in Tactical Command Information Exchange System (OTCIXS), Tactical Data Information Exchange System (TADIIXS A), NETWORK, TADIL A, COP Synchronization Tools Transmission Control Protocol (CSTTCP), etc.
- (8). Tactical correlation is accomplished when new incoming track reports are automatically merged with existing tracks and/or records in the database.
- (9). Tactical associations are the links with existing tracks and/or records in the database with other type of tracks, e.g. a LINK track associated with Platform track
- (10). The system contains default track colors for the different order-of-battles, and the analyst/user may customize/change them
- (11). Holds the Master track database
 - (a). Holds the tracks and track information.
 - (b). The track master is also called the TMS.
 - (c). The maximum number of tracks in the database is 20,000.
- b. Intel/Imagery server: (intel, Shared Data Server (SDS), Imagery Transformation Service (ITS))
 - (1). Hosts the Commercial-off-the-Shelf (COTS) Relational Database Management Software (RDBMS), Sybase Server.
 - (a). There are six database server segments that are installed on the ISDS. SYBi3C is installed on the server to create and configure the I3 server. It modifies the settings for each data server, number of connections, and memory. If this segment is removed after the databases have been installed all data will be lost and will result in the removal of the Sybase server. The SYSAM, COTS segment install the Sybase utility to manage the license for all Sybase products. Additional SDS segments will be covered in a later section.

- (b). There are six GCCS-M database segments that are generally installed on the ISDS. GMIDB, NERF, and EPL require a database restore as part of the ISDS configuration.
 - CTDS (Common Track Data Store)
 - EPL (ELINT Parameters List Database)
 - GMIDB (General Military Intelligence DB)
 - ISHOPD (Intelligence Shop Database)
 - NERF (Naval Emitter Reference File)
 - IMDB (Image Management Database)
 - (c). All clients and servers that require access to the Intel server must have the Intelligence Shop Client (ISHOPC) segment installed. Client software provides a means for other machines on the LAN with “run-time” software to communicate with and access the intel/imagery server.
 - (d). Replaces JOTS 19 (Database Server and JOTS 14 (Imagery Server).
- c. Web Server (MEDULA, websvr and appserver)
 - (1). Provides a user friendly interface to each database on the ISDS.
 - (2). Makes up the middle-tier of a three tier architecture model. The COTS, BEA Web Logic Server (BEAWLS) is configured by the I3 Configure Middle Tier (I3CMT) segment.
 - (3). Serves the Modular Embedded Doc Utility Archive (MEDULA). The MEDULA web application provides management and delivery of online user-requested hardware and software documentation and help-files.
<https://appserver/MEDULA/DocMgm>
 - (4). Serves ishop database interface. <https://appserver/ishop>
 - (5). Serves webcop web application. <https://appserver/webcop>
 - (6). Serves ITS_WEB web application. <https://appserver/ITSWEB>
 - (7). Also provides a system management console accessible from the web.
<https://appserver/console>

JOB SHEET 1-1-3

ACCESSING DMI CONTENT

A. Introduction

The Document Management Infrastructure (DMI) is an online documentation system accessed via the browser. DMI is installed by MEDULA (server segment), CSLDD (system wide documentation and training content segment) and SINOPS (client segment). Documentation consists of XML files that are installed (“checked-in”) separately by each segment in GCCS to the DMI. Online documentation is accessed either from a direct URL connection, the System Chart (Help → System Help), or from the Help menu from an application.

B. Equipment Required

A PC connected via LAN to the Application Server.

C. References

Online Embedded Documentation.

D. Safety Precautions:

Review TTO procedures

E. Job Steps:

DMI content can be accessed three ways.

To access DMI Content directly via browser:

1. Log in on the computer as the administrator
2. Open the browser and in the URL box, enter:
 - a. <https://appserver/MEDULA/DocMgm>
 - b. The primary DMI window appears. The Job tab is set to default.

- 1) The left side of the window displays a Job-based tree structure. Under each job, are duties and tasks. In summary, the tree follows this pattern:
Jobs → Duties → Tasks → Sub-Tasks
 - 2) The right side of the window displays specific procedural content related to the Tasks or Sub-Tasks that are opened on the left-side.
 - 3) The Function tab only displays content specific for an application and is not applicable unless you access DMI from an application (see next page).
- c. Navigate through the tree on the left side of the window to display different content on the right side. Note that the Job-based tree on the left side is an evolving structure and will change over time.

To access DMI Content from System Chart:

1. Log in on the machine.
2. Open the System Chart and select Help → System Help
 - a. The primary DMI window appears.

To access DMI Content from an application:

1. Log in on the machine.
2. Open the System Chart and select Intel → Analyst Workshop.
3. Sign-in.
4. After the application starts, go to the Help menu and select Help...(wording can differ).
 - a. The Browser will launch and the Function tab will be the default display. On the left side of the window is a listing of the Functions and Sub-Functions related to the application. The right side displays procedural content

INFORMATION SHEET 1-1-4 **THE APPLICATION FRAMEWORK (AFW)** **CHART WINDOW**

A. Introduction

This lesson will provide a basic understanding of the chart window for those who do not have much experience with the operating functions within the chart.

B. References

Online Embedded documentation

C. Information

Standard features are available from the Chart window. These include the title bar, the menu bar, the toolbar, the map area, and the status bar.

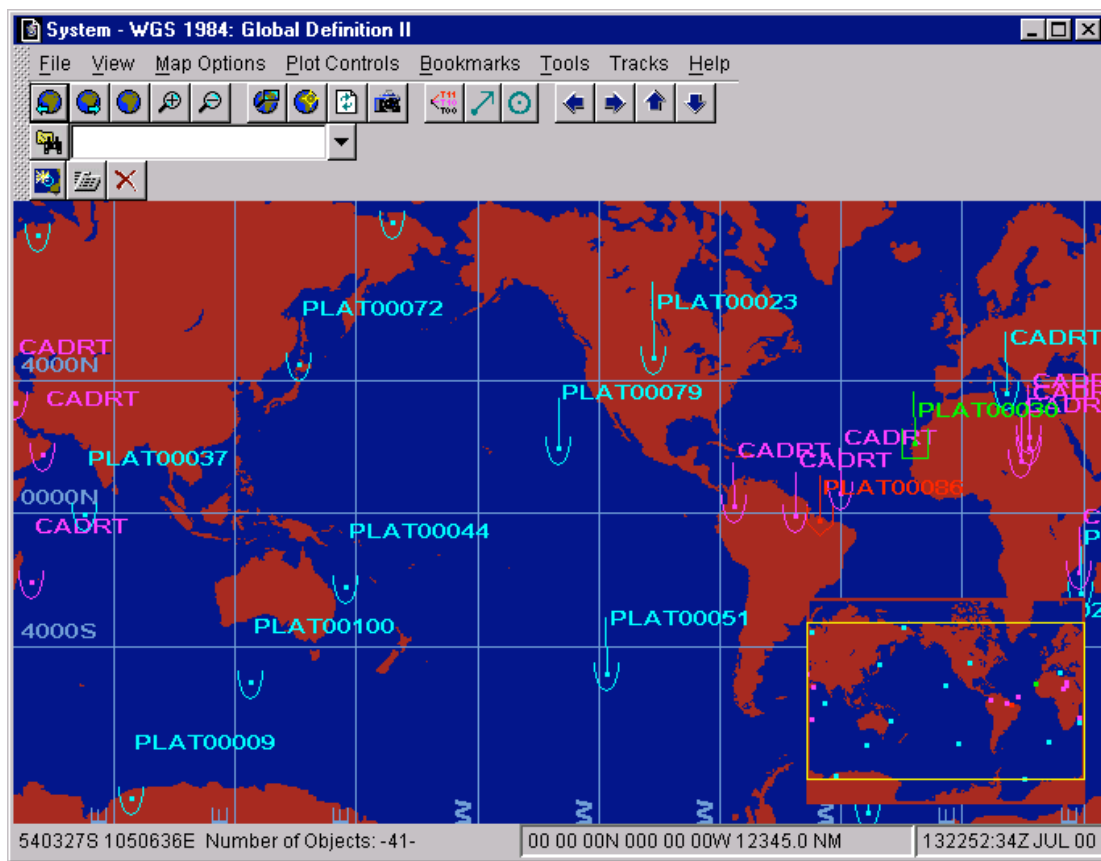


Figure 1-1-1

1. The Titlebar

The titlebar at the top of the Chart window displays the map name, the datum used, and any user-defined title.

2. The Menu Bar

The menu bar contains a group of menus. Each menu on the menu bar can be selected to display a pull-down group of related options to allow you to perform various actions. Using the menu bar and the pull-down options are discussed in detail in the Using the Graphical Interface section located in the on-line documents.

3. The Main Toolbar

- a. The Main Toolbar at the top of any chart window contains buttons that can be used to quickly perform map-related functions. The Main Toolbar can be toggled on or off with the Main Toolbar option, which is located in the View Menu. The Main Toolbar appears as follows.

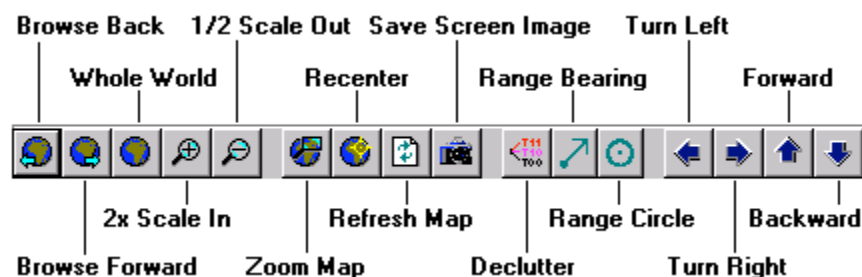


Figure 1-1-2

- b. The Main Toolbar contains the Browse Back, Browse Forward, Whole World, 2x Scale In, 1/2 Scale Out, Zoom Map, Recenter, Refresh Map, Save Screen Image, Declutter, Range Bearing, Range Circle, Turn Left, Turn Right, Forward, and Backward buttons. Some of these buttons have equivalent menu options.

4. Browse Back

If more than one map has been displayed in the chart window, use the **Browse Back** button to view the previous map.

5. Browse Forward

If the **Browse Back** button has been used to view previously displayed maps in the chart window, use the **Browse Forward** button to view the next map in a forward direction.

6. **Whole World**

Click this button to display a whole worldview in the chart window.

7. **2x Scale In**

Click this button to redraw the map around the current center point at half the current horizontal map width. Using this option changes the map, zooming IN by a factor of 2.

8. **1/2 Scale Out**

Click this button to redraw the map around the current center point to reduce the current horizontal map scale by half.

9. **Zoom Map**

- a. Click this button to redraw and plot a zoomed (close-up) view of a specific area of the current tactical display.
- b. To select a ZOOM(ed) area:
 - Click and hold a point to be the upper left-hand corner of the new map.
 - Drag the trackball or mouse outward from the point to encompass the zoom area.
 - Release the **left** button; the area in the zoomed box fills the screen.
 - The smallest zoom width is 0.10 NM across.

10. **Recenter**

- a. Click this button to center the map on a chosen position.
- b. To select a new map center:
 - Click the **Recenter** button. The pointer changes to a crosshairs object.
 - Move the crosshairs pointer to the desired position on the map and click.
 - The map recenters around the chosen position.

11. **Refresh Map**

Click this button to refresh the map on the tactical display. This button is not typically used, as the map automatically refreshes periodically, but it is available if needed to clean up the look of the map.

12. **Save Screen Image**

Click this button to save the current map and all objects displayed on the map to a .bmp file. This file can viewed with the View Saved Snapshots option and can be pasted into other

applications. The first image that is saved is automatically named SnapShot_000.bmp, the second is named SnapShot_001.bmp, etc.

13. **Declutter**

Click this button to declutter the track information.

14. **Range Bearing**

Click this button to toggle on/off the Range Bearing feature. Allows a user to click a hook point and view range and bearing information from that point to another point on the map.

15. **Range Circle**

Click this button to toggle on/off the Range Circle feature. Allows a user to click a hook point and draw a circle around that point, with range and bearing information from that point to the circle displayed.

16. **Turn Left**

Click this button to shift the map view slightly to the left.

17. **Turn Right**

Click this button to shift the map view slightly to the right.

18. **Forward**

Click this button to shift the map view slightly up.

19. **Backward**

Click this button to shift the map view slightly down.

20. **Main Tool Bar**

The Main Toolbar can be displayed with icons, text only, or text and icons. Right click on the gray rectangle to the left of the Main Toolbar to display the **SHOW [MAIN TOOLBAR]** AS menu.

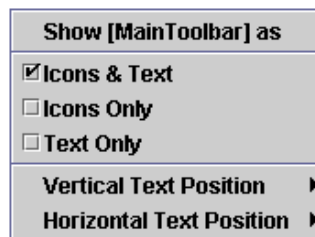


Figure 1-1-3

Choose the **Icons & Text**, **Icons Only**, or **Text Only** check box to display the Main Toolbar in the chosen format.

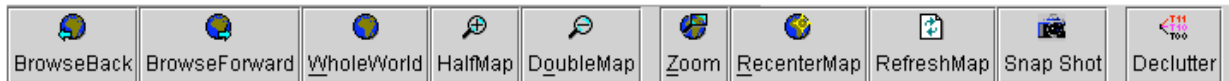


Figure 1-1-4 Main Toolbar in Icons & Text Format



Figure 1-1-5 Main Toolbar in Icons Only Format

21. Main Toolbar in Text Only Format

- a. If Icons & Text is chosen as the format, the Vertical Text Position and Horizontal Text Position options are available from the **SHOW [MAIN TOOLBAR] AS** menu.
- b. The Vertical Text Position option contains a cascading menu with check boxes for **Top**, **Center**, or **Bottom**. Choose one of these check boxes to set the vertical display location of the text in relation to the icon. The Horizontal Text Position option contains a cascading menu with check boxes for **Left**, **Center**, or **Right**. Choose one of these check boxes to set the horizontal display location of the text in relation to the icon.

22. The Map Area

The map area displays a map of the world. The map view can be set to show anywhere in the world and can be zoomed in or out to display a closer or farther view. Tracks and other objects can be plotted on the map.

23. Quick Pan Box

- a. The Quick Pan Box is located in the bottom right part of the map area and shows a larger picture of the map with the current view shown in a **yellow** box. It can be toggled on/off with the **F6** key from the keyboard.

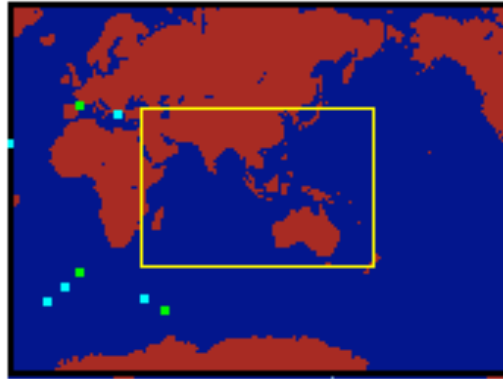


Figure 1-1-6

- b. The Quick Pan Box allows you to see beyond the current map view to get a bigger picture of what is being viewed in the map view.
- c. To change the current map view to a different area within the Quick Pan Box, click anywhere within the Quick Pan Box to **recenter** the **yellow** box around the clicked point. You may also drag the **yellow** box to a different area within the Quick Pan Box to change the map view to that area.

24. The Status Bar

The Status Bar at the bottom of any chart window displays information about the map that is currently being viewed as well as some other status information.



Figure 1-1-7

Separate areas of status information are listed along this bar as follows:

- The left portion of the Status Bar displays the current pointer position.
- The next portion of the Status Bar displays the number of objects plotted on the map. This is the number of tracks, overlay objects, and other objects displayed on the entire map, not just the visible portion. If tracks or other objects are suppressed from view, they are not included in the number displayed.
- The next portion of the Status Bar contains a box showing the current map center and width.
- The far right portion of the Status Bar displays the current date and time.

25. **OnlineDocs**

- a. OnlineDocs is the help system that provides information on how to use the system software and COE documentation on-line, such as user's manuals. It is available in the system at any time because key COE manuals are included in the COE kernel software.
- b. The OnlineDocs system is designed to display system documents and provide easy navigation to the appropriate information. OnlineDocs provides immediate access to the following:
 - View online HTML documentation provided using an intuitive and easy-to-use interface.
 - Access key system information and troubleshooting tips.
 - Step-by-step procedures for completing tasks.
 - Descriptions of fields and menus.
 - Overviews of windows within the system.
 - The OnlineDocs segment provides a framework and set of HTML pages for the Netscape Navigator browser to allow users to view COE documents on-line on a COE platform.
 - All on-line documentation is viewed using the Netscape browser as the presentation engine. When the OnlineDocs segment is installed, the OnlineDocs icon becomes available to all users from the Start menu on Windows machines. Some segments may have OnlineDocs included and available from the pull-down menus with the tactical display.
- c. To access the Online Docs help function:
 - Click on Start.
 - Click on Programs→DII Apps→Online Docs→Online Docs.
 - The Online Docs window opens.
 - Select the manual that you wish to read from the list of documents.

THIS PAGE INTENTIONALLY LEFT BLANK

ASSIGNMENT SHEET 1-2-1 COMMON ADMINISTRATION TASKS

A. **Introduction**

This assignment sheet is to be completed as homework as assigned.

B. **Enabling Objectives**

- 1.7 **IDENTIFY** technical documentation associated with GCCS-M system administration.
- 1.8 **DISCUSS** the overall responsibilities of a GCCS-M System Administrator.

C. **Study Assignment**

Read Information Sheet 1-2-2

D. **Study Questions**

- 1. State the location of the SAM and SECAM documents.
- 2. State seven typical duties of a System Administrator.
- 3. What are some the tasks involved with user account management?
- 4. What methods are typically involved with the recovery process?

THIS PAGE INTENTIONALLY LEFT BLANK

INFORMATION SHEET 1-2-2

COMMON ADMINISTRATION TASKS

A. **Introduction**

This lesson will describe common administrative tasks associated with a GCCS-M administrator.

B. **References**

Embedded Online Documentation

C. **Information**

1. Documentation

Most documentation for the GCCS system can be found on the system. The manuals used for software troubleshooting can be found under the following directories:

/h/COE/data/help/PDF

- System Administration Manual (SAM)
- Security Administration Manual (SECAM)
- System Integrator's Manual (SIG) *Not found in this directory*
- Segment SAMs and Software Version Descriptions (SVD) *Not found in this directory*

2. Typical Duties and tasks of a System Administrator.

a. User and Group account management

- (1). Adding and deleting user accounts with or without account templates
- (2). Manage user account passwords, permissions, restrictions, and assign available resources to groups
- (3). Manage domain security policies for users IAW current DOD INFOSEC policies
- (4). Delegate control of common tasks to trusted users and computers.
- (5). Create and manage folders and directories for users on the network

b. Servers

- (1). Managing Domain Name Service (DNS) to include adding zones and domains

- (2). Assign Dynamic Host Control Protocol (DHCP) scopes as required.
 - (3). Add and configure applications for installation through the application server
 - (4). Allocate disk space to users
- c. Mail Services
 - (1). Move and delete mailboxes for established users through active directory.
 - (2). Provide virus protection for incoming and outgoing mail
- d. Network
 - (1). Configure network properties such as Transmission Control Protocol/Internet Protocol (TCP/IP)
 - (2). Monitor network performance including bandwidth usage, server and client performance and network outages
 - (3). Use Event viewer to investigate problems
 - (4). Prepare reports for chain of command
- e. Backup and Restore
 - (1). Backup the Data Store, Information Store, and Exchange
 - (2). Plan and implement Backup strategies
 - (3). Restore systems using backup data
 - (4). Restore email
- f. Troubleshooting
 - (1). Identify and fix software and certain hardware related problems
 - (2). Utilize online documentation for troubleshooting procedures
 - (3). Investigate user log for problems
 - (4). Troubleshoot network resource problems
 - (5). Maintain and repair hardware by using defrag utilities
 - (6). Examine the registry to find and fix problems
 - (7). Troubleshoot the boot process
- g. Recovery
 - (1). Re-install software as needed to recover a crashed system
 - (2). Use boot recovery procedures to fix boot up problems
 - (3). Configure array controllers

ASSIGNMENT SHEET 1-3-1

GCCS HARDWARE OVERVIEW

A. Introduction

This assignment sheet is to be completed as homework when assigned.

B. Enabling Objectives

- 1.9 **DISCUSS** the functional interface for equipment and systems associated with GCCS-M.
- 1.10 **DESCRIBE** the hardware used for GCCS-M comms, Intel, and websvr UNIX servers to include hard drives, memory, and CPU specifications.
- 1.11 **DESCRIBE** the hardware used for GCCS-M COMPOSE servers to include hard drives, fault tolerance, memory, and CPU specifications.
- 1.12 **DESCRIBE** the hardware used for GCCS-M UNIX clients to include hard drives, memory, and CPU specifications.
- 1.13 **DESCRIBE** the hardware used for GCCS-M COMPOSE clients to include hard drives, memory, and CPU specifications.
- 1.14 **DISCUSS** the differences between each enclave to include Secret and SCI.
- 1.15 **DESCRIBE** the 3-tier computing model.
- 1.16 **DESCRIBE** the connectivity to the other racked equipment.

C. Study Assignment

Read Information Sheets 1-3-2, 1-3-3 and 1-3-4

D. Study Questions

1. What is the Integrated Shipboard Network System (ISNS) in relation to IT-21?
2. What two common network configurations are typically used in an ISNS installation?

3. What type of fault tolerance is provided with the GCCS-M UNIX servers?
4. Where can additional maintenance information be located for GCCS-M hardware?
5. What is the purpose of the keyswitch on the Sun 280R server?
6. How does track data move within GCCS-M between servers and clients?
7. What network port is all track data sent across?
8. What are the three main configuration steps for each ICSF client?
9. Explain how data is routed to an analyst when he or she uses an appserver I3 product.

INFORMATION SHEET 1-3-2
IT-21 OVERVIEW
AND
THE INTEGRATED SHIPBOARD NETWORK SYSTEM (ISNS)

A. Introduction

This lesson will provide a basic overview of IT-21 and ISNS as it relates to GCCS-M.

B. References

Embedded Online Documentation

C. Information

Information Technology for the Twenty First Century (IT-21) is the Navy's lifecycle initiative to establish, operate and maintain a global communication structure that will support seamless command center connectivity. IT-21 is a complete, reliable end-to-end management solution for hardware and software developments to ensure the Navy will have access to the most up-to-date technology. One of the major network structures under the IT-21 initiative is the Integrated Shipboard Network System.

The Integrated Shipboard Network System (ISNS), AN/USQ-153(V) is a high-speed information network that provides instantaneous communications to shipboard personnel via Local Area Networks (LANs) and direct interfaces with other systems and external communication channels. The system consists of a fiber-optic connected backbone of high-speed switches that inter-connect a number of shipboard LANs. Interface connections with the Global Command and Control System - Maritime (GCCS-M) and the Navy Tactical Command Support System (NTCSS) provide users with tactical and support information. ISNS provides off-ship communications by interfacing with various RF and shore-connected communication systems. The standard installation includes a classified and a separate unclassified network.

ISNS currently exists in two common physical arrangements corresponding to the technology employed. It is worth noting here that every installation is different to the extent of the number and connectivity of devices. However, each system can generally be defined by the switching technology used to interconnect the devices making up the network. Switching

technologies are typically based on either Asynchronous Transfer Mode (ATM) or Gigabit Ethernet (GigE) technology.

The Asynchronous Transfer Mode (ATM) infrastructure most often consists of two interconnected backbone switches, each supporting a number of edge switches. Both edge and backbone switches consist of Xylan (Alcatel) OmniSwitch chassis equipped with the appropriate modules. Edge switches act as a connection point for segments of the network, each are redundantly connected to each backbone switch. OmniSwitches are configured to provide connections for ATM and Ethernet connected workstations, servers and peripherals. In this configuration the PDC, BDC and MSSs are usually attached to a backbone switch while most workstations and peripherals are attached to the edge switches.

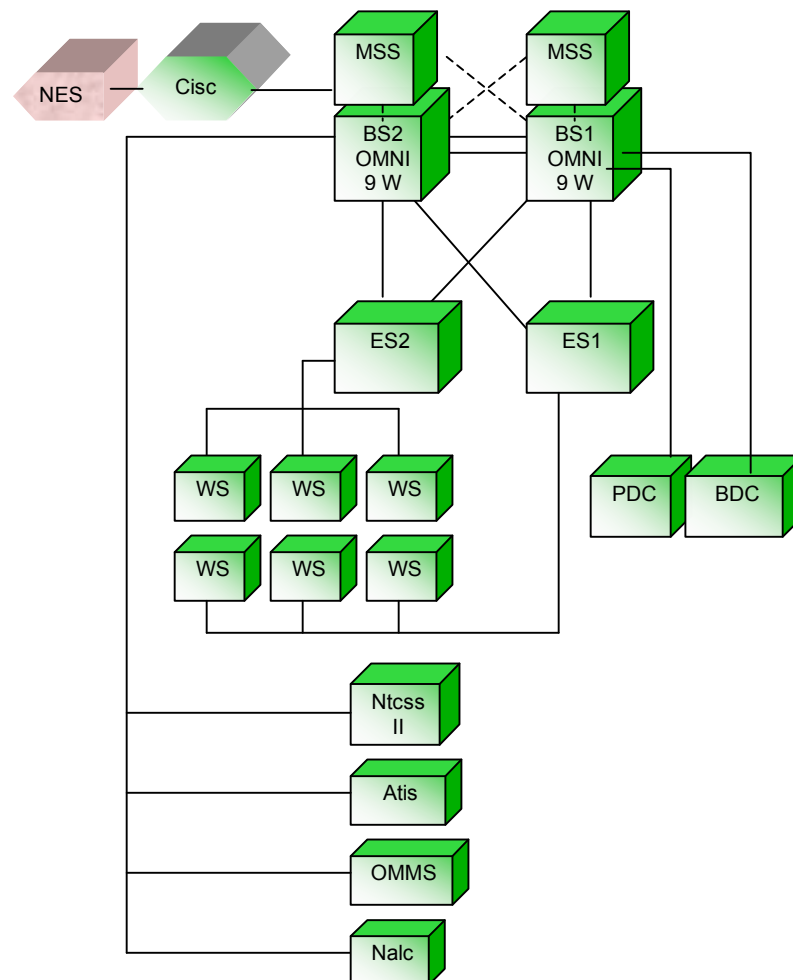


Figure 1-3-1

In an ATM infrastructure, ATM switches and ATM connected devices are interfaced with either OC-3 (155 Mbps) or OC-12 (622 Mbps) connections. Most often, as shown in the figure above, edge and backbone switches are interconnected with OC-3 while backbone switches are OC-12 connected. In some installations, edge and backbone switches interconnect using OC-12. Connectivity speeds are determined by the Cell Switching Modules (CSMs). Each ATM device must be properly configured before it can interface with the network.

The Gigabit Ethernet (GigE) infrastructure most often consists of two or more interconnected backbone switches each supporting a number of edge switches. Backbone switches consist of Alcatel (formerly Xylan) OmniSwitch/Router (OSR) chassis equipped with the appropriate modules. Backbone and Edge switches act similarly to an ATM configuration and provide connectivity for workstations, servers and peripherals depending on the module installed. GigE connections can use either fiber-optic cable or Category-5 (cat.-5) copper wire depending on the module installed. A GigE configuration is similar to an ATM configuration shown in Figure 1-3-1 with the exception of the MSSs.

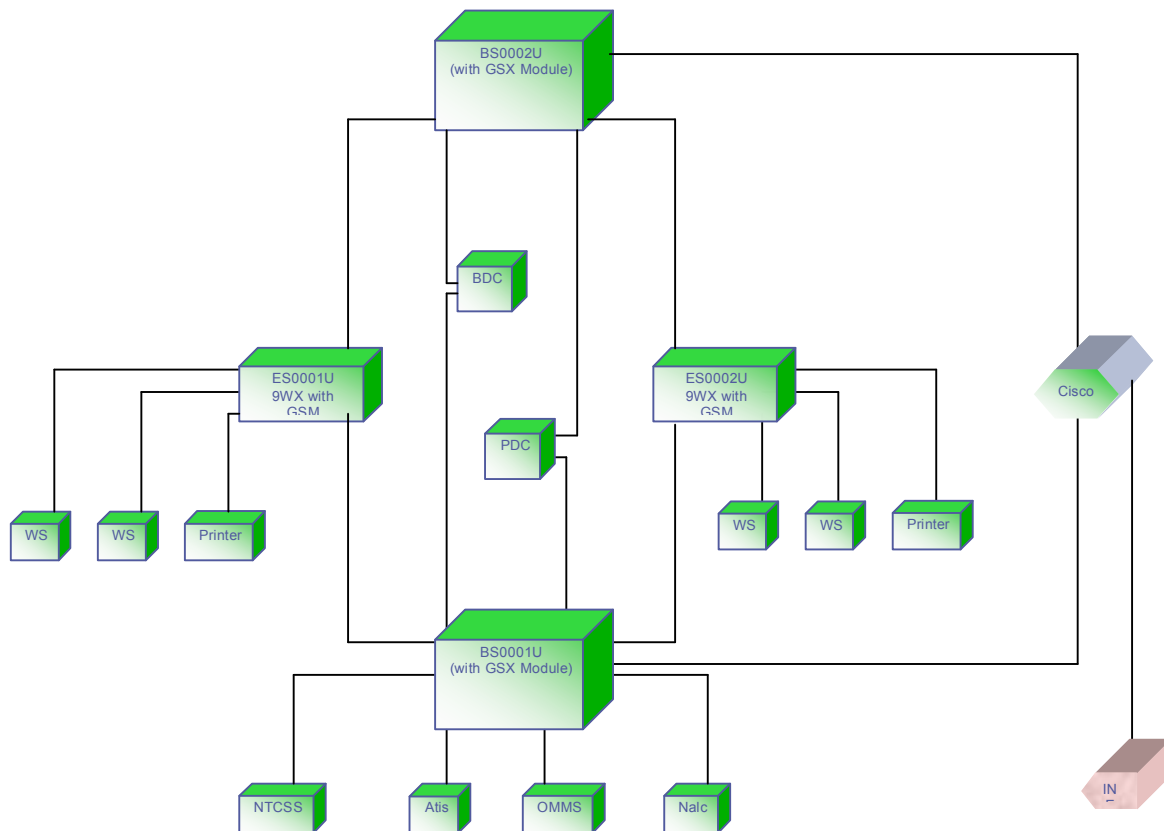


Figure 1-3-2

THIS PAGE INTENTIONALLY LEFT BLANK

INFORMATION SHEET 1-3-3

GCCS-M HARDWARE

A. Introduction

This lesson will provide the trainee a basic overview and material understanding of the hardware used for GCCS-M 4.x servers and clients.

B. References

Embedded Online Documentation

C. Information

1. Communications servers (comms1, comms2), Web Server, and Intel Server
 - a. **Sunfire V240**

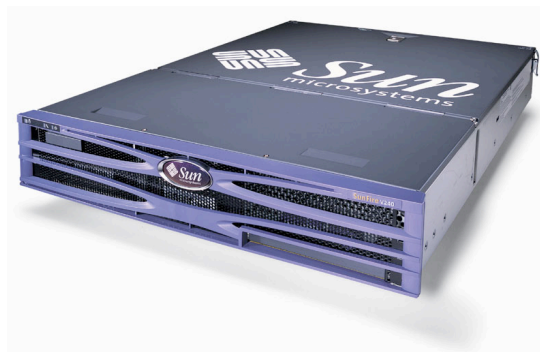


Figure 1-3-3

- (1). One or two 1.34 GHz or 1.4 GHz UltraSPARC® IIIi processors
- (2). Up to Four Ultra 160 SCSI Hard Drives
- (3). Four (4) DDR DIMM slots per processor.
- (4). Fault Tolerance: RAID 0+1, disk mirroring.
 - (a). External Support for 0, 1, 0 +1, and 5.
 - (b). RAID 0 (striping), RAID 1 (mirroring), RAID 0+1 (striping plus mirroring sometimes called RAID 10), and RAID 5 (striping with interleaved parity) configurations can all be implemented using Solstice DiskSuite and VERITAS software.

- (5). Four (4) auto-sensing 10/100/1000 Ethernet ports
- (6). Dual redundant power supplies
- (7). Documentation can be found at <https://appserver/MEDULA/DocMgm> or www.sun.com.
- (8). Refer to the Service Manuals for detailed information on component removal, system specifications and trouble shooting techniques.

b. Sun Fire 280R server (ashore sites)

- (1). One or two 1 GHz or 1.28 UltraSPARC® III processors
- (2). Up to Two Fibre Channel-Arbitrated Loop (FC-AL) Hard Drives
- (3). Fault Tolerance: Disk mirroring. External Support for 0, 1, 0 +1, and 5.
- (4). Eight (8) GB of memory
- (5). Four Industry Standard USB ports, Supports Sun USB Keyboard and Mouse.
- (6). Hot-swappable Power Supplies
- (7). Two separate PCI buses, supporting 33 MHz and 66 MHz.
- (8). Documentation can be found at <https://appserver/MEDULA/DocMgm> or www.sun.com.
- (9). Keyswitch settings:
 - (a). Power On/Off- This setting enables the system's power button to power the server on and off. If the keyswitch is in this position, quickly depressing the power button and releasing it will shut down the system gracefully.
 - (b). Diagnostics position- POST and OpenBoot Diagnostics will run during system startup. All diagnostics messages will be displayed on screen
 - (c). Locked- disables the power button and locks the front doors.
 - (d). Off- Immediately power's off the system.

(10). LED indicators

- (a). Power On/Activity- A green LED continuously on with power applied.
- (b). System fault LED- Lights a steady amber color when a hardware fault is detected.

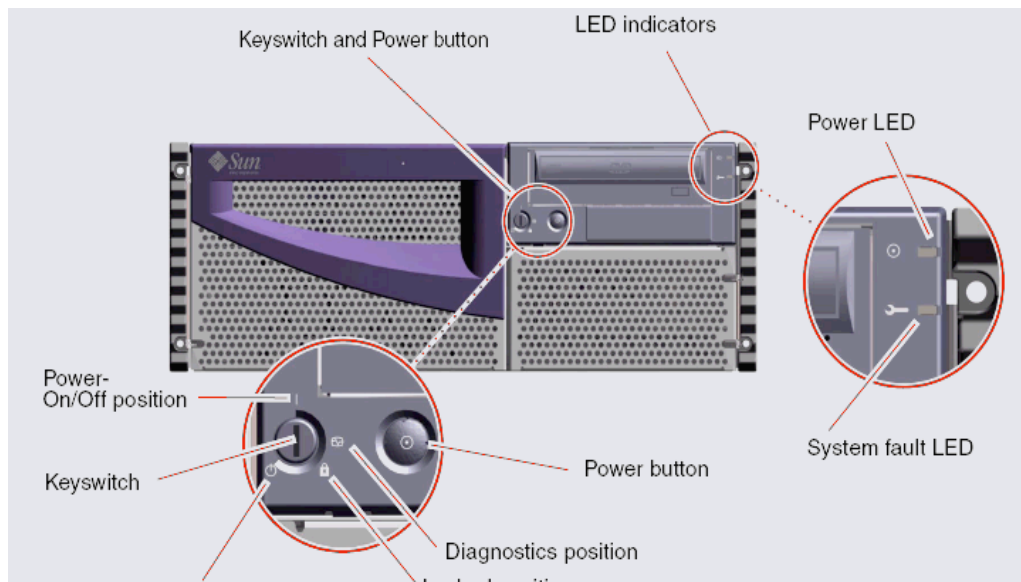


Figure 1-3-4 (Sun Fire 280R)

(11). Gaining access to internal components.

- (a). Figure 1-3-5 shows how to unlock the top cover to gain access to internal components.

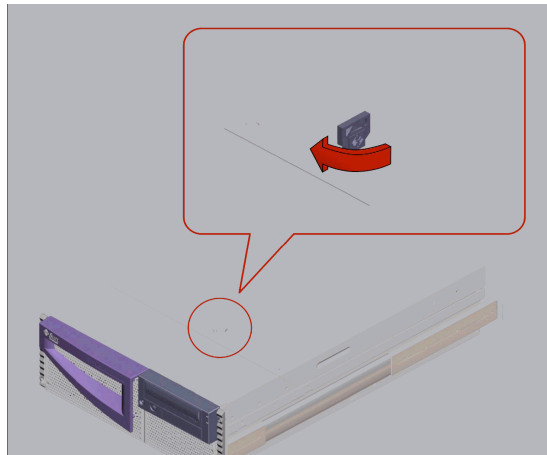


Figure 1-3-5

- (12). Refer to the Sun Fire 280R Service Manual for detailed descriptions on component removal for the 280R server.

c. **EEPROM settings on Sun equipment**

- (1). Sun systems are equipped with flash programmable read-only memory.
- (2). To access the EEPROM the user must stop the boot process by pressing “Stop – A” from a Sun USB keyboard, or if accessing from a terminal press the break key.
- (3). At the *ok* prompt the user can type *printenv* to display the current settings.
- (4). Type *boot* to continue the boot process.
- (5). More information on EEPROM and ALOM can be found in the hardware manuals.

2. COMPOSE Servers (Domain Controllers, Exchange, File Server)

a. **HP Proliant DL -380 G3**

- (1). Up to six - 72 GB SCSI Hard Drives
- (2). 12 GB max memory
- (3). Up to 2 Intel Xeon 3.2GHz processors with 1MB L3 cache in addition to the 512K L2 Cache.
- (4). Fault Tolerance: Ultra3 Smart Array 5i Plus RAID controller
- (5). Documentation can be found at <https://appserver/MEDULA/DocMgm> or via www.HP.com.



Figure 1-3-6

(6). Compaq DL 380 Drive LED Description Status

(1)

Activity status On = Drive activity

Flashing = High activity on the drive or drive is being configured as part of an array.

Off = No drive activity

(2)

Online status On = Drive is part of an array and is currently working.

Flashing = Drive is actively online.

Off = Drive is offline.

(3)

Fault status On = Drive failure

Flashing = Fault-process activity

Off = No fault-process activity

- *Review figure 1-3-7 for LED Status*

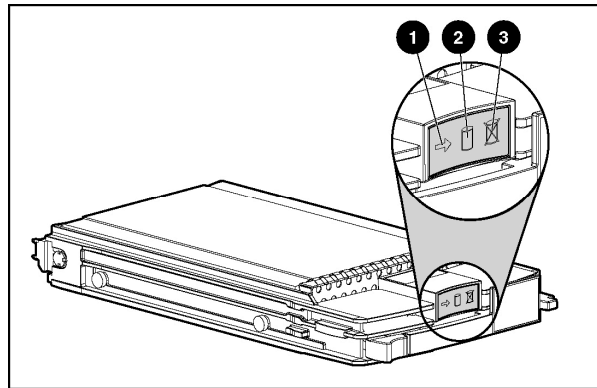


Figure 1-3-7

3. UNIX Clients (Gale Lite, SCI Clients)

a. Sunblade 150

- (1). 550 MHz or 650 MHz UltraSPARC III
- (2). Up to 4 DIMM memory cards.
- (3). Up to Two (2) IDE Hard Drives
- (4). Fault Tolerance: None
- (5). Documentation can be found at <https://appserver/MEDULA/DocMgm> or via Sun's website.
- (6). Refer to the Service manual for detailed information on component removal.

4. COMPOSE/GCCS Clients

- a. Due to the constant upgrade and rapid development of PC technology the manufacture and detailed specifications of each client will be dynamic, the model numbers and specifications should be considered as reference only and may be different depending on each ships configuration.
- b. Each Windows client will have at a minimum
 - (1). 8 GB Hard Drive for COMPOSE
 - (2). 512 MB of memory
 - (3). Pentium processor @ 1GHZ or above.
 - (4). Fault Tolerance: None

5. Digi-mux Realport Etherlite multiplexer

- a. The Digi EtherLite serial concentrator is used as a way of eliminating the installation of several serial adaptors inside each server.
- b. Digi RealPort is a software feature that allows network-based host systems to use the ports of the Digi EtherLite as though they were the host system's own ports, appearing and behaving as local ports to the network-based host, this means that the ports will use standard operating system interfaces that control the baud rate, parity, etc. In short, it makes a connection on a single TCP/IP session from all RS 232 communication ports reducing network and CPU overhead.

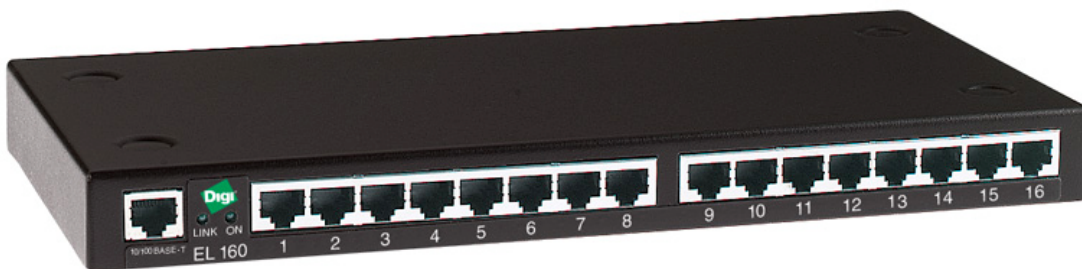


Figure 1-3-8

- c. The EtherLite 160 auto detects the presence of either 10BaseT or 100BaseTX, allowing the unit to work with legacy equipment, while supporting speeds up to 230 Kbps on all serial ports simultaneously. Since the ports are real, local serial devices, they are not slowed down by network overhead common to terminal servers. EtherLite ports appear as local TTYs under UNIX and as native COM ports under Windows NT which allows the administrator to configure the ports in an environment in which they are more familiar. The figure below depicts the connection panel of a GCCS rack. It shows the 16, RS 232, nine pin connections.

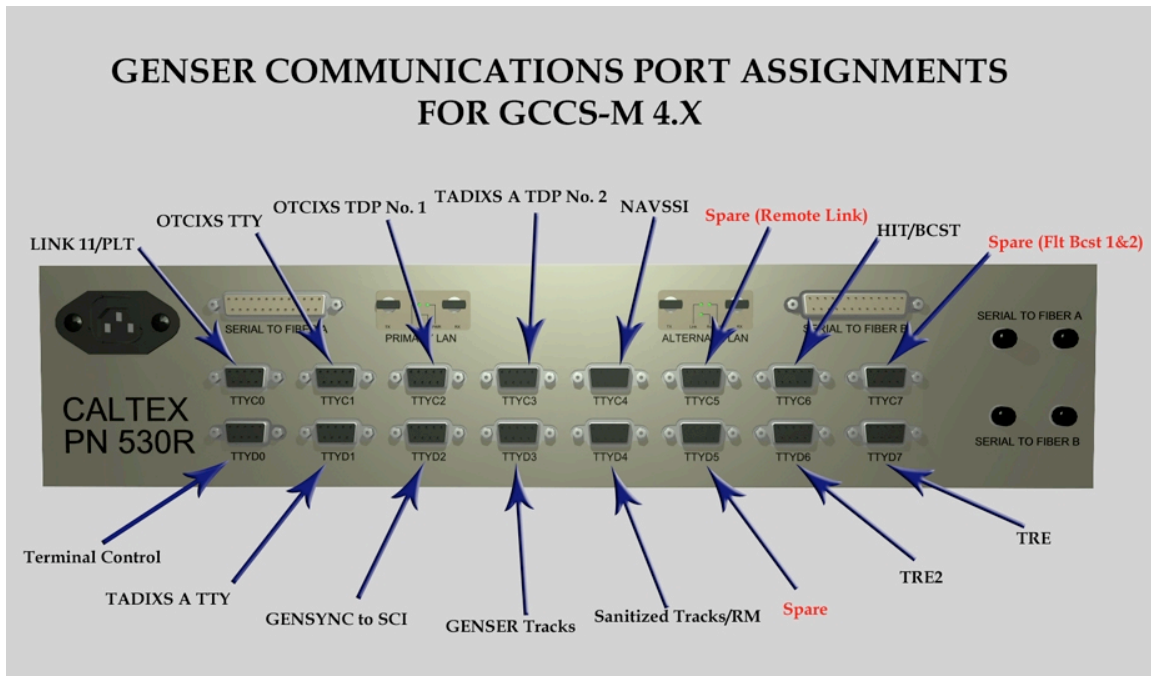


Figure 1-3-9

6. Sun Storedge 3510 FC RAID
 - a. Has the capability for dual controller modules. Each controller module provides six Fibre channel ports that can support one or two gigabit (Gb) data rates.
 - b. Dual hot-swappable redundant power supplies.
 - c. Connects to Intel server via fiber optic cable.



Figure 1-3-10 (Sun Storedge 3510 FC)

INFORMATION SHEET 1-3-4

EQUIPMENT CONNECTIVITY

A. Introduction

This lesson will provide the trainee a basic understanding of data movement between each type of server and across each type of enclave.

B. References

Embedded Online Documentation

C. Information

1. Most of the machines loaded with GCCS-M (servers and clients) will be classified Secret (GENSER). For many ships and shore facilities, this will be the only classification encountered. The standard shipboard Secret enclave will consist of four servers (comms1, comms2, intel, and websvr). The communications servers will transmit and receive GCCS-M network messages through the DMDS and OTCIXS and TADIXS A, if applicable via the LAN multiplexer (DigiMUX), which encapsulates the data and sends it over the network. Additionally, the GENSER enclave will transmit data to the site's Top Secret and/or SCI enclaves, if applicable through a serial line on the DigiMUX.
2. The TS/SCI enclave will have servers configured similar to the GENSER enclave and will receive data from the GENSER system via a one-way serial line as well as transmit data to the GENSER system via a one-way serial line through Radiant Mercury. The GENSER Synchronization (GENSYNC) configuration procedure is used to update owntrack in the SCI network and to setup and configure the channels on both the GENSER and SCI networks.
3. As a part of the COE architecture provided by the Defense Information Systems Agency (DISA), Integrated C4I System foundations (ICSF) provides a framework for C4I systems designed to meet the tactical communications, data fusion, and display needs of joint warfighters across many echelons. The three main configurations for ICSF are IFL, TMS and UCP.

4. **IFL** – ICSF Foundational Libraries and processes that are shared across components
 - a. The IFL component contains a set of utility libraries and services that are used by the other components contained in the ICSF. IFL has a set of libraries files that need to be available to the other segments to ensure full functionality of each segment.
 - b. All other segments in the ICSF Bundle require the IFL segment in order to run properly. Setting up an ICSF LAN Master will assign the master host for the importer and exporter function of TDAs.
5. **TMS** - track correlation and tactical database management services
 - a. The Track Management System (TMS) component provides the correlation engine, including single source, report-to-track, and multi-source track-to-track correlation, and the tactical database management for the COE. The primary responsibility of TMS is to manage track data by providing data correlation, storage, and distribution.
 - b. During the TMS configuration steps, the servers and clients are “pointed” to one server that will act as the TMS master. All track data will be sent to/from the master via port 2000. When an operator double-clicks to view a track, the PC provides the information contained in a local database that has been updated by the master. If the operator edits the track, the PC sends the data to the server on port 2000 and then, after the server accepts the data, the server broadcasts it out to all clients thereby updating all of the local track records. If a new track has been received by the master from an external source, it will immediately broadcast it on port 2000 and all clients listening on that port will receive the update. GCCS-M communicates to external sources via the Universal Communications Processor (UCP) master.
6. **UCP** - communications interfaces, message processing, and message handling
 - a. The UCP component communications infrastructure is derived from several existing communications programs, thereby providing a fairly robust communications framework under the COE. For tactical communications, the UCP uses communications services from the Navy's Joint Maritime Command Information System (JMCIS) program, specifically the Unified Build (UB) Core, and the Army's communications server. For record communications, the UCP uses the communications services from the COE Communications Channel Server (DCCS) program.

- b. The UCP component provides centralized management of all communication channels in a UCP suite (the UCP server and its clients). The primary user interface is the "Channel Manager" window, where the operator can view all communications channels in the suite, the software interfaces which they represent (e.g., Network, Serial), the host on which they reside, the device that they are using (e.g., ttya, network), and their current status (ON/OFF). From this window, the operator can add new channels, choosing from a list of available communications interfaces. The operator can also monitor the current traffic on the channel through a "Raw Data" window.
 - (1). For example, if an operator left clicks the red stop sign icon to stop the CSTTCP (Cop Sync Tools / Transmission Control Protocol) channel, the PC send sends a message to the UCP master requesting that the channel be stopped. The UCP then broadcasts the change to all clients and the change (making the CSTTCP icon red and stopping the channel) is displayed in the UCP dialogue box on all clients.

7. Integrated Imagery and Intelligence (I3)

- a. As discussed, all intelligence functions are web-enabled; therefore intelligence operators will interact with the intel server via the webserv to perform analytical tasks. For example, when an operator submits a query via ISHOPC and ISHOPI, the request is routed via the network to the webserv. If the webserv recognizes the operator as a valid user, then it routes the query to the intel server, which in turn routes the data back to the webserv and finally to the operator. This is called a three tier computing system.

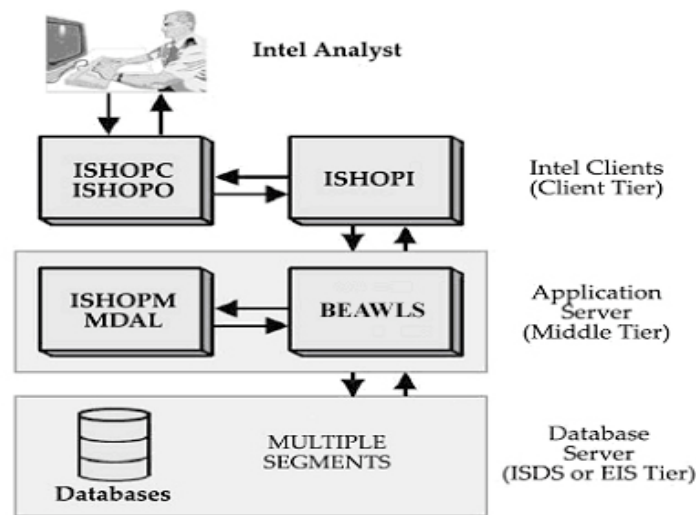


Figure 1-3-12

b. Three-Tier Computing Model.

- (1). In order to web-enable all mission critical and unclassified applications; the traditional 2-tier client/server architecture was modified to a Web-enabled, 3-tier architecture.
- (2). The various applications and databases are split into three logical layers:
 1. Presentation Layer = Workstation with Web Browser.
 2. Data Access Layer = Application Server/Web Server.
 3. Business Logic Layer=Data Server, Data
- (3). Application servers provide the framework for a client to connect to a backend source, execute the applications logic, and return. Application servers, whatever their function, occupy a large chunk of computing territory between database servers and the end user. Typically, this is called “middleware” which in itself says something about what these application servers are providing. First and foremost, application servers connect database information (usually coming from a database server) and the end-user or client program (often running in a Web browser). There are many reasons for having an intermediate player in this connection – among other things, a desire to decrease the size and complexity of client programs, the need to cache and

control the data flow for better performance, and a requirement to provide security for both data and user traffic. The end result of this thinking is what is now called an application server or webservr.

c. Flow of I3 information

- (1). Client Tier Segments like ISHOPC, ISHOPO and ISHOPI provide an interface with the middle tier so that the data can be received in a proper format for the user to be able to view. Use the ISHOP SAM for more detailed information on Client Tier Segments.
- (2). Application Server Segments or middle-tier segments are comprised of the COTS Application Server and the Intelligence business components that include the Data Access Layer (DAL). The COTS application server is installed by the WebLogic Server segment. The WebLogic Server is configured by the I3 Configure Middle Tier (I3CMT) segment. The Intelligence Business Components are installed by Intelligence Shop Middle-Tier (ISHOPM) and DMI segments.
- (3). The BEA WebLogic Server (BEAWS) contains the BEA WebLogic COTS product. The BEA WebLogic Server acts as an intermediary between the Intelligence clients and various data sources. When the Intelligence analyst runs a search, the client machine sends the database requests to the Application Server, which in turn translates the request and routes it to various data sources.
- (4). The I3 Configure Middle Tier (I3CMT) segment is used to configure Middle Tier application server segments. Currently, only BEA WebLogic Server (BEAWS) is supported. I3CMT contains scripts for deploying applications such as ISHOP, MEDULA, and Webcop. It also contains scripts that start the server when the workstation is rebooted.
- (5). The ISHOPM segment provides retrieval, update, formatting, and packaging services within a distributed object-based environment. The Data Access Layer (DAL) encapsulates database access, transactions, and caching for MIDB/GMI, CTDS, TMS, IMDB, and organizational messages. This will be discussed more in detail in later topics.

THIS PAGE INTENTIONALLY LEFT BLANK

DIAGRAM SHEET 1-3-5

DIFFERENT LAN ARCHITECTURES

The following drawing represents a GENSER LAN onboard a typical ship.

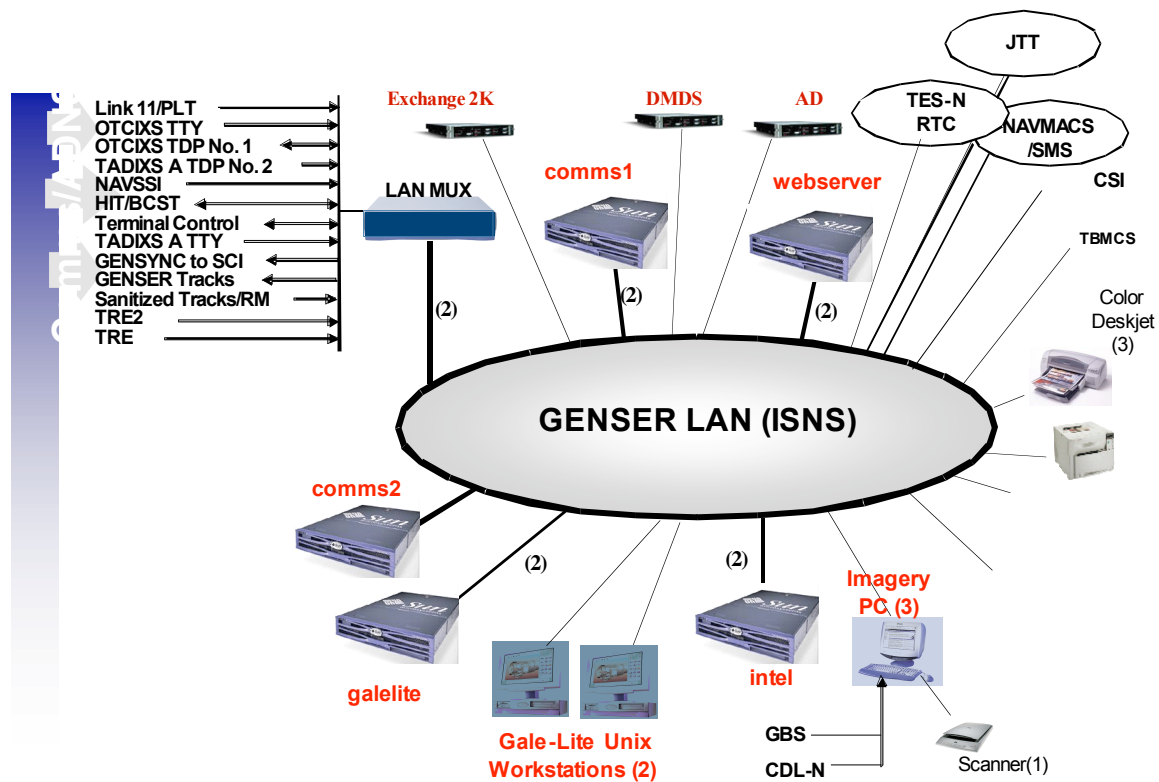


DIAGRAM SHEET 1-3-5 (cont.) SCI LAN ARCHITECTURE

The following drawing represents an SCI LAN onboard a typical ship.

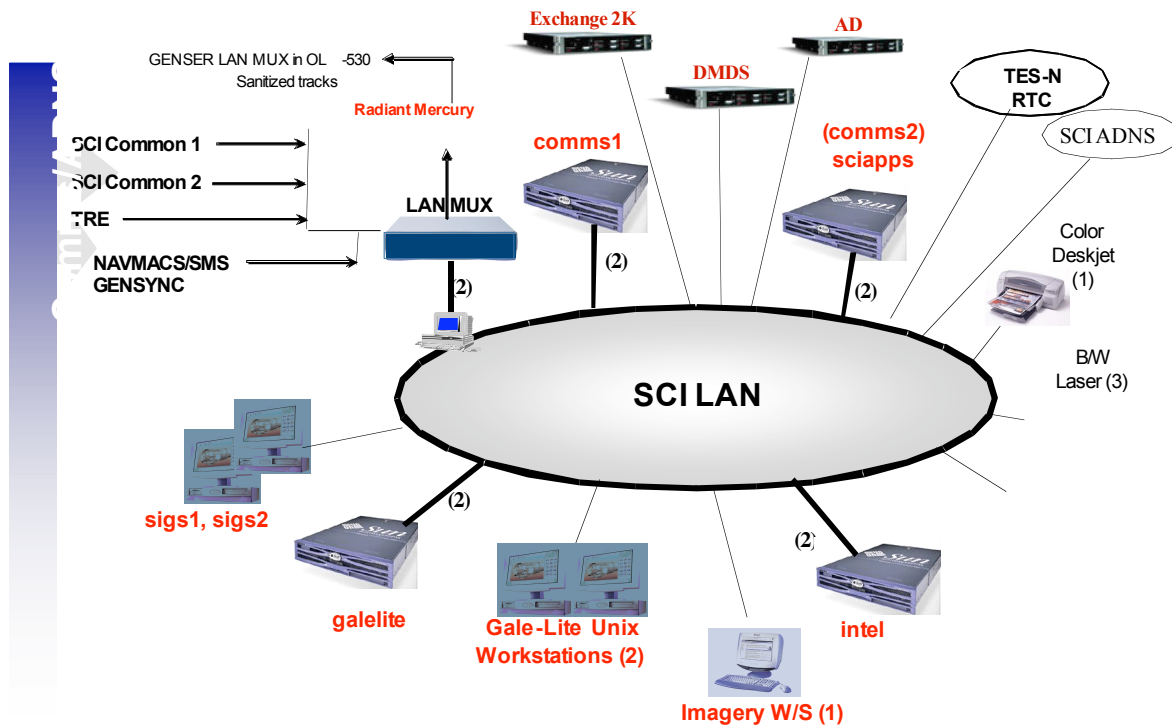
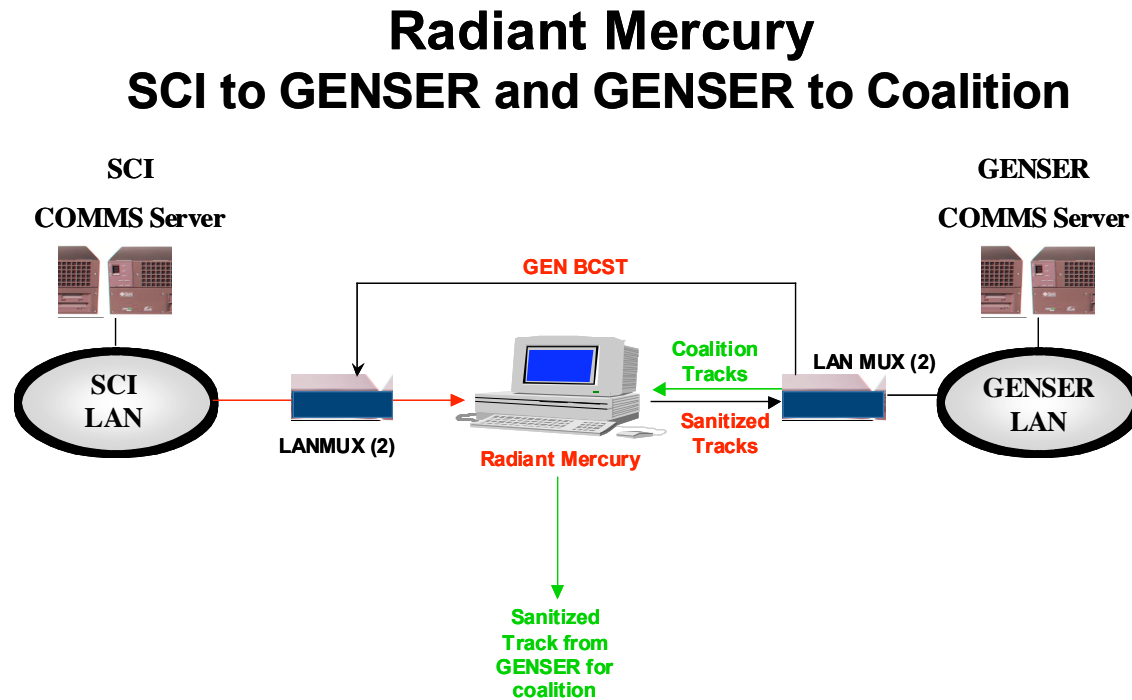


DIAGRAM SHEET 1-3-5 (cont.)
RADIANT MERCURY ARCHITECTURE

The following drawing represents an SCI LAN onboard a typical ship.



THIS PAGE INTENTIONALLY LEFT BLANK

ASSIGNMENT SHEET 1-4-1
DEFENSE INFORMATION INFRASTRUCTURE COMMON
OPERATING ENVIRONMENT (DII COE)

A. Introduction

This assignment sheet is to be completed as homework as assigned.

B. Enabling Objectives

- 1.17 **DISCUSS** the Common Operating Environment (COE) as an infrastructure.
- 1.18 **STATE** the accounts and profiles that are created locally during the flash.
- 1.19 **DISCUSS** the functions of the GCCS-M sysadmin account.
- 1.20 **DISCUSS** the functions of the GCCS-M secman and keyman accounts.
- 1.21 **PERFORM** a system shutdown and reboot via a GUI.
- 1.22 **DEMONSTRATE** the use of the Application Manager to perform basic system administration functions.
- 1.23 **DEMONSTRATE** the use of the Common Desktop Environment.
- 1.24 **DEMONSTRATE** the use of the Common Operating Environment sysadmin Graphical User Interface.

C. Study Assignment

Read Information Sheet 1-4-2

Perform Job Sheet 1-4-3

D. Study Questions

- 1. State the goal of the Defense Information Infrastructure (DII).
- 2. What are the “building blocks” of COE-based systems, and how are they used?

3. Is COE a network-centric system or a platform-centric system?
4. State four features of a COE kernel.
5. What is APM and what is its primary function?
6. What accounts are created on a Solaris machine during the flash?
7. What is the purpose of the keyman account?

INFORMATION SHEET 1-4-2

DEFENSE INFORMATION INFRASTRUCTURE COMMON OPERATING ENVIRONMENT (DII COE) OVERVIEW

A. **Introduction**

This lesson will provide the trainee a basic overview of the Defense Information Infrastructure Common Operating Environment (DII COE).

B. **References**

Embedded Online Documentation

C. **Information**

The goal of the *Defense Information Infrastructure (DII)* program was to provide a seamless end-to-end integration of *Department of Defense (DoD)* information resources. The Common Operating Environment (COE) was a cornerstone to the realization of this goal. To view the COE simply as a *command, control, communications, computers, and intelligence (C4I)* system misses the fundamental idea that the COE is not a system; but merely a *foundation* for building open architecture systems. Building a system such as Global Command and Control System (GCCS) is principally a matter of combining COE components with mission specific software.

The COE infrastructure manages the flow of data through the system, both internally and externally. Mission specific software or applications are designed to request specific data from the COE and present it in a form that is significant to the operator (e.g., as a pie chart, in tabular form, or as a graph). The COE provides the foundation for such data manipulation and has the necessary information about where the requested data is stored – whether locally or across a Local Area Network (LAN) or Wide Area Network (WAN). This frees the system designer to concentrate on data presentation rather than on the mechanics of data manipulation, network communications, database storage, etc. It must be kept in mind, however, that there is only one COE. Each COE system uses:

- The same set of *application program interfaces (APIs)* to access common COE components.

- The same approach to integration.
- The same set of tools for enforcing COE principles.

Systems are built on top of the COE and use precisely the same COE software components for common functions (e.g., communications interfaces and data flow management). This approach to software reuse significantly reduces interoperability problems. By using the same software, two dissimilar mission systems interpret or implement the common APIs and get the same results. The COE concept is best described as:

- An architecture that is fully conformant with the DOD Joint Tactical Architecture.
- An approach for building interoperable systems.
- A reference implementation containing a collection of reusable software components.
- A software infrastructure for supporting mission-area applications.
- A set of guidelines, standards, and specifications.

The COE is a network-centric “plug and play” open architecture, presently designed and implemented around a client/server model. Functionality is easily added to or removed from the target system in small manageable units called *segments*. Segments are defined in terms of functions that are meaningful to operators, not in terms of internal software structure. Structuring the system into segments in this manner allows flexibility in configuring the system to meet specific mission needs or to minimize hardware requirements for an operational site. Site personnel perform field updates by replacing affected segments through use of a simple, consistent, graphically oriented user interface.

Segments are the most basic building blocks from which a COE-based system is built. In COE-based systems, all software and data (except certain portions of the kernel such as the operating system and basic windowing software) are packaged in self-contained units called *segments*. This is true for COE infrastructure software and for mission-application software as well. Segments are defined in terms of the functionality they provide, not in terms of “modules,” and may in fact consist of one or more “modules.” *Segments* are a collection of related functions as seen from the perspective of the end user, not the developer. The reason for defining segments in this way is that it is a more user-oriented way of expressing and communicating what software features or functions are to be included or excluded from the system than by individual process, file name, or data table.

Those segments that are part of the COE are known as *COE-component segments*, or more precisely, as segments that further have the attribute of being contained within the COE. Segments that are built on top of the COE to provide capabilities specific to a particular mission domain are *mission-application segments*. Segments can be data segments, software segments, or patches. Each segment in the system contains a directory with a collection of data files that “self-describe” the segment to the rest of the COE.

The COE is a *superset* of capabilities. It contains far more functionality than would ever be installed on a single platform or even at a specific operational site. Thus, it is important to note and understand that just because a segment is part of the COE; it is not necessarily always present or required. Considerable flexibility is offered to customize the environment so that only the segments required to meet a specific mission-application need are present at runtime. This approach allows minimization of hardware resources required to support a COE-based system.

At the heart of the COE is the kernel. The *COE kernel* is the minimal set of software required on every platform, regardless of how the platform will be used. The COE kernel components include the Operating System, Windowing Services and a collection of other services that properly belong in the Infrastructure Services Layer.

A few local accounts are created during the COE kernel installation that can be used to administer the COE environment. It should be noted that if local accounts cannot reside on a particular server such as a domain controller, the local accounts described below will not be created. A domain controller does not allow for the creation of local accounts so all functions to be performed on the domain controllers will be done with a domain administrator account. With the use of flash technology, the installer does not have to ensure these accounts have been correctly created. The following accounts and profiles will be created with the installation of the Kernel, or during the flash load:

- sysadmin (SA default profile)
- secman (SSO default profile)
- keyman (Auth default profile)
- winadmin (SA default profile)

System Administration Overview (sysadmin / winadmin account)

The COE provides for system administration through:

1. A set of system administration tools with varying availability across the COE platforms.
2. Across all COE platforms, the system administration tools provide the ability to install/remove software segments as well as change a machine's identity (name or IP address). Several additional tools are provided for UNIX platforms only. Windows platforms utilize the native tools available to perform other system administration tasks.
3. System administration tools are described in the table below.

<i>Change Machine ID</i>	Changes the machine name or Internet Protocol address of a machine.
<i>COEInstaller</i>	Installs and/or removes software segments on a local machine.
<i>COESegInstall</i>	A command line interface for installing segments.
<i>Create Action</i> (UNIX only)	Creates a desktop action.
<i>Dtterm</i> (UNIX only)	Opens a Dtterm terminal window to perform tasks that require use of a command line.
<i>Disk Manager</i> (UNIX only)	Perform file system management tasks including mounting and exporting file system partitions, formatting hard drives and hard drive partitions, displaying available hard disk space, and initializing diskettes.
<i>Edit Local Hosts</i> (UNIX only)	Manages the list of computers that can be accessed from a machine.
<i>Network Installation Server</i> (UNIX only)	Loads software segments onto a machine and makes them available for other computers to install.
<i>Reboot System</i> (UNIX only)	Reboots a machine.
<i>Set DNS</i> (UNIX only)	Sets the <i>Domain Service Name (DNS)</i> parameters of a local machine.
<i>Set Routes</i> (UNIX only)	Configures a machine to connect to a wide area network through a default router.
<i>Set System Time</i> (UNIX only)	Sets or changes the system time.

<i>Shutdown System</i> (UNIX only)	Prepares the machine for powering down.
<i>Text Edit</i> (UNIX only)	Invokes a text editor.
<i>Xterm</i> (UNIX only)	Opens an xterm terminal window to perform tasks that require use of a command line.

Security Administration Overview (secman / keyman)

The COE provides for security administration through:

- a. A security lockdown
- b. A security manager account (secman)
- c. A key manager account (keyman)
- d. A set of security administration tools or programs accessible via icons (GUI-based) and the command line with interfaces and functionality consistent across the COE platforms.
- e. The Security Administration function allows authorized users to create, delete, and maintain user accounts. The SSO Default profile allows a Security Administrator to assign sets of applications to users, often according to job responsibilities.
- f. Provides tools listed in the table below:

<i>Edit APM Configuration</i>	This GUI program configures APM settings. The <i>Edit APM Configuration</i> tool is launched from an icon provided in the SSO Default Profile (i.e., the <i>DII_APPS/SecAdm</i> folder in the <i>Application Manager</i>).
<i>Authentication Manager</i>	Both a <i>Command Line Interface (CLI)</i> and GUI program. The <i>Authentication Manager</i> sets authentication keys that the APM uses to validate users of the <i>APM Client</i> and the <i>COEInstaller</i> .
<i>Merge Host</i>	This GUI program makes a workstation or server part of an administrative domain.

<i>Remove Host</i>	This GUI program removes a workstation or server from an administrative domain
<i>Register Host</i>	<p>This GUI program is used to notify APM when the function type – Primary Domain Controller (PDC), Secondary Domain Controller (SDC), Operating System Domain Member (OSDM), or Stand Alone Workstation (SAWS) – of a host is changed.</p> <p>Note: The <i>Register Host</i> tool is not used to add hosts to the APM administrative domain or to remove hosts. Hosts are added to an APM domain through the <i>Merge Host</i> tool and removed from an APM domain through the <i>Remove Host</i> tool.</p> <p>See the <i>SECAM</i> for more information on using the <i>Register Host</i>, the <i>Merge Host</i> and the <i>Remove Host</i> tools.</p>
<i>APM Client</i>	This GUI program is used to view and edit APM information.
<i>APM Key Server</i>	This GUI program stores the master APM authentication key in memory on the <i>Master APM Server</i> to support remote segment installation via <i>COESegInstall</i> .
<i>APM Public Key Manager</i>	This GUI program generates a public/private key pair and that is used to export/import public keys.
<i>APM Server Reload</i>	This GUI program reloads the information in the CDS files into the cached copy kept by the <i>Master APM Server</i> .
<i>APM Server Start</i> (UNIX only)	This GUI program starts the APM Server.
<i>APM Server Stop</i> (UNIX only)	This GUI program stops the APM Server.
<i>Assign Passwords</i>	This GUI program allows a trusted user (i.e., the “secman” account or “root” on UNIX and “Administrator” on Windows) to change a user’s (or set of users’) password(s) to a temporary password that must be changed the next time the user(s) logs in.

<i>Audit Log File Manager</i> (UNIX only)	This GUI program sets alerts when audit files reach a certain size or percentage of disk capacity. The tool can also delete (i.e., clear) log files on the system.
<i>Profile Selector Config</i>	This GUI program controls profile locking (requires the DAZ segment) and determines whether multiple profiles can be assumed at the same time.
<i>SecuritySetup.pl</i> (UNIX only)	This CLI configures system security settings according to the information in <i>Security.conf</i> .
<i>PSM_enable</i> (UNIX only)	This CLI tool enables or disables the “3-strikes” capability.
<i>PSM_unlock</i> (UNIX only)	This CLI tool unlocks (and can lock) accounts that have been disabled via 3-strikes.
<i>SSO Deadman</i>	This GUI program configures the locking screen saver and deadman capabilities.
<i>COE_deadman_enable</i>	This CLI configures the locking screen saver and deadman capabilities.

The Account and Profiles Manager (APM) component provides the capability to establish, maintain, and delete user accounts, groups, and profiles. Profiles are defined and assigned to users by the security administrator. They provide users with levels of access to applications via menus and icons in the Application Manager (UNIX) or Start Menu (Windows). APM provides tools for the security administrator to build APM Administrative Domains (AAD) that allow centralized management of user accounts, groups, and profiles. APM will be covered more in depth throughout the course.

THIS PAGE INTENTIONALLY LEFT BLANK

JOB SHEET 1-4-3
PERFORM TASKS AS AN ADMINISTRATOR

A. Introduction

This job sheet allows the trainee to demonstrate the skills necessary to logon as an administrator and locate function related to tasks that must be performed as an Administrator.

B. Equipment Required

Unix and Windows machines loaded with GCCS.

C. References

Online Embedded Documentation

D. Safety Precaution

Review TTO procedures

E. Job Steps:

Step 1: Login and User Familiarization.

1. Open the System Administrator's Manual for Solaris and follow the instructions to login to a Solaris machine with the "sysadmin" account.
2. Note the available utilities for the SSA profile.
3. Locate and review all functionalities listed in previous topic to include file system administration, Network administration and segment installation.
4. Once you are comfortable with the environment of the sysadmin account, logout.
5. Open the System Administrator's Manual for Windows and follow the instructions to login to a windows machine with the "sysadmin" account.
6. Note the available utilities for the SSA profile and the differences between a Windows sysadmin and a UNIX sysadmin.

Note: GCCS must be booted in the following order: comms1, Intel, websvr, clients. If the system has Compose Domain Controllers, they should be booted in the following order: DC1, DC2, Exchange, clients. Compose and GCCS can be rebooted independently of each other. If both systems are shutdown it is recommended to first power on the compose servers and then power on the GCCS servers and then finally boot all clients. If there is ancillary equipment that is to be used, it must be turned on prior to the serving unit is powered on. ie. The StorEdge Power RAID must be powered on and initialized prior to the intel server.

Step 2: Reboot the GCCS system.

1. Login to comms1 with the sysadmin account.
2. Reboot comms1, monitor and familiarize yourself with the boot process.
 - a. Press Stop-A and verify the EEPROM settings.
3. Login to intel and reboot.
4. Login to websvr and reboot.
5. Once the system is back up, login to a windows client and test the following items:
 - a. Chart
 - b. Add a track to the COP
 - c. Any web application. (ie. webcop, ishop or DMI)
6. Login to a Solaris server at your station and answer the following questions:
 - a. What is the hostname?
 - b. What systems are in the host table? What are the aliases of each?
 - c. What is the current primary DNS server for this system?
 - d. What application is used to export file systems?
 - e. Which file systems are mounted from comms1?

- f. What application changes the classification level of the
7. What tools are available from the sysadmin login, DII applications of a windows client?
8. Use the COE profile selector to verify the profile is selected. Which profile is used for sysadmin? Secman?
9. Access the IFL configuration window and write down the specifics.
10. Access the TMS configuration window and write down the specifics.
11. Access the UCP configuration window and write down the specifics.
12. What system(s) is(are) required to be in all three windows?
13. On the system chart, zoom into the San Diego area.
14. Create a new Hostile, NAV track.
15. Re-center the display to the U.K.

16. Move your new track to this area.
17. Zoom out so that all of the U.K. and France are visible.
18. Display the range and bearing between U.K. and France.
19. Change the map colors so that the land is red and the water is blue.
20. Turn on grid lines.
21. Turn on boundaries.
22. Turn on country colors for U.K. and France.
23. Change the plot symbol labels to large text size with medium symbol size.
24. Declutter the screen.

ASSIGNMENT SHEET 2-1-1

INTRODUCTION TO SOLARIS

A. Introduction

This assignment sheet is to be completed as homework.

B. Enabling Objectives

- 2.1 **DESCRIBE** the System Boot Process for UNIX servers.
- 2.2 **DESCRIBE** the function of the boot PROM on UNIX servers.
- 2.3 **DEMONSTRATE** the use of init commands used to restart and shut down a UNIX server from a command line interface.
- 2.4 **DESCRIBE** emergency server/system shutdown procedures.

C. Study Assignment

Read Information Sheet 2-1-2

D. Study Questions

1. Which Shutdown option allows you to specify a time (in seconds) before the system is shutdown?
2. What is the Sun keyboard sequence that will abort the boot process of a Sun Solaris computer?

3. What is the name of the window in Solaris that contains the icons for executing System Administration applications?

4. Which icon in the SysAdm window allows the System Administrator to change the machine name or Internet Protocol (IP) address on comms1?

5. State and explain the different run levels used in Solaris.

6. What are the different commands that allow a user to change the current run level?

7. What EEPROM command changes the input device from tty to keyboard?

INFORMATION SHEET 2-1-2

BOOT AND SYSTEM SHUTDOWN PROCESSES

A. Introduction

This lesson will provide the trainee a basic understanding of the boot and system shutdown processes.

B. References

Online Embedded documentation

C. Information

Understanding the system startup requires the comprehension of the hardware, software and firmware. This section describes the steps in the boot process. Identifying those steps is a key skill for system administrators who must troubleshoot systems that do not boot successfully. There are four phases to the boot process, as described in the following table:

Boot PROM Phase	<ol style="list-style-type: none"> 1. This phase displays the system identification banner. 2. PROM runs self-test diagnostics. boot device programmed into the PROM. 3. It finds the boot program from the default 4. PROM loads the boot block (bootblk) program.
Boot Program Phase	<ol style="list-style-type: none"> 5. The boot block program loads the secondary boot program (ufsboot). 6. The (ufsboot) boot program loads the kernel.
Kernel Initialization Phase	<ol style="list-style-type: none"> 7. The kernel initializes itself and starts the init process.
The /sbin/init Phase	<ol style="list-style-type: none"> 8. The kernel creates a user process and starts the /sbin/init program. This program uses information found in the /etc/inittab file.

PROM (Programmable Read-Only Memory)

Each SPARC system has a PROM (programmable read-only memory) chip with a program called the **monitor**. The monitor controls the operation of the system before the kernel is available. When a system is turned on, the monitor runs a quick self-test procedure that checks things such as the hardware and memory on the system. If no errors are found, the system begins the automatic boot process. The PROM firmware located in the Sun servers used in this course is called OpenBoot. The OpenBoot firmware contains programs that control the operation of the system prior to the kernel being online.

Occasionally, the user may need to abort the boot process. The specific abort key sequence depends on your keyboard type. For example, press **Stop-A** or on **tty** terminals, press the **BREAK** key. To abort the boot process, type the **abort** key sequence for the system. When the boot process is aborted, the monitor should display the ok prompt. If the terminal shows the **> monitor** prompt, type **n** to get the ok prompt.

The init Program and the /etc/inittab File

When the system is initialized or has had the run levels changed, the init daemon starts processes using the information read from the entries in the **/etc/inittab** file, which defines system initialization states. Each entry in the **/etc/inittab** file has the following fields:

id:runlevel:action:process

The fields are as follows:

id	A unique identifier
runlevel	The run level
action	How and when the process is to be run
process	The name of the command to execute

Run levels and init states

A run level is a software configuration of processes (running programs) and available services that describes how a system is booted or shut down. Run levels are also referred to as init states because the init process starts and stops the system processes that are available at each

run level. A system can be in only one run level at a time. When the system is first booted, the init daemon starts all processes in the inittab file labeled sysinit. The initdefault entry in **/etc/inittab** identifies the default run level. In this example, the default is run level 3. The init daemon runs each process associated with this run level.

The following is an example of a typical **/etc/inittab** file.

1.	ap::sysinit:/sbin/autopush-f /etc/iu.ap	
2.	fs::sysinit:/sbin/rcS	>/dev/console2>&l</dev/console
3.	is:3:initdefault:	> /dev/console 2>&l
4.	p3:sl234:powerfail:/sbin/shutdown -y -i5 -g0	> /dev/console 2>&l </dev/console
5.	s0:0:wait:/sbin/rc0	> /dev/console 2>&l </dev/console
6.	sl:1:wait:/sbin/shutdown -y -iS -g0	> /dev/console 2>&l </dev/console
7.	s2:23:wait:/sbin/rc2	> /dev/console 2>&l </dev/console
8.	s3:3:wait:/sbin/rc3	> /dev/console 2>&l </dev/console
9.	s5:5:wait:/sbin/rc5	> /dev/console 2>&l </dev/console
10.	s6:6:wait:/sbin/rc6	> /dev/console 2>&l </dev/console
11.	fw:0:wait:/sbin/uadmin 2 2	> /dev/console 2>&l </dev/console
12.	of:5:wait:/sbin/uadmin 2 6	> /dev/console 2>&l </dev/console
13.	rb:6:wait:/sbin/uadmin 2 1	> /dev/console 2>&l </dev/console
14.	sc:234:respawn:/usr/lib/saf/sac -t 300	
15.	co:234:respawn:/usr/saf/ttymon -g -h -p "uname -n' console login:" -T sun \-d dev/console -I console -m Idterm,ttcompat	

Explanation:

1. STREAMS module initialization (initializes the keyboard and mouse drivers for use)
2. File system check
3. Defines the default run level (initial state)
4. Power fail shutdown
5. Run level 0 (state **0** - firmware/Prom state)
6. Run level 1 (state **0** - administrative state)
7. Run level 2 (state **0** - multi-user state w/o NFS running)

8. Run level 3 (state **0** - multi-user state w/ NFS running)
9. Run level 5 (state **0** - immediate power off)
10. Run level 6 (state **0** - reboot)
11. Firmware or PROM level
12. Power off
13. Reboot
14. Service Access Controller initialization (start the processes to monitor terminal lines)
15. Console initialization (start the process to monitor the console & issue login prompt)

The Eight Solaris Software Environment Run Levels

The *Solaris* software environment has eight run levels, which are described in the table listed below:

Run States	Description
0	Stops system services and daemons. Terminates all processes.
1	Single-user state Only root is allowed to login at the console
2	Multi-user state (NFS resource-sharing not allowed)
3	Multi-user state (Normal operation & NFS resource-sharing)
4	Alternate multi-user state (This level is currently unavailable.)
5	Power-down state
6	Reboot
s or S	Single-user state Only root is allowed to login at the console

NOTE: Run level "S or s" is not exactly the same as run level 1. All other users will be logged out of the system when in state S,s.

To find the run level for a system, type **who -r** and press **RETURN**. The run level, date and time, process termination status, process id, and process exit status are displayed.

Changing System Run Levels

While the `/etc/inittab` file establishes the default run level, Solaris provides several commands to change the system run level. These different run levels allow a user or

administrator to limit the activity on a system while allowing for performance of certain system administrative tasks.

The **init** Command

Use the **init** command to change system run levels. The **init** command does not send warning messages before changing run levels. The command **syntax** for the **init** command is:

init [run_level]

NOTE: The options for the **init** command are **0-6**, **s**, and **S**, which correspond to the appropriate run levels. You can also use the **Q** or **q** to tell the **init** program to re-read the `/etc/inittab` file.

Shutting Down to the Firmware/PROM Monitor Level

To shutdown to the PROM monitor level, type **init 0** and press **RETURN**. The **init** command runs scripts that bring the system down cleanly. A clean shutdown means all file system changes (writes) are written to the disk and all system services and processes are terminated normally. No warning messages are broadcast.

init 0

There are two modes for this level, one that is more secure (**>** is the prompt) and another that is less secure (**ok** is the prompt). Once the **ok** prompt is displayed, the user is able to set or change the PROM/Firmware password using the **setenv** command. The **printenv** command will display current settings. The environments set here will be stored in the NVRAM.

ok setenv output-device screen

In some cases the alias “screen” does not work and you have to force the resolution.

ok setenv output-device screen:r1280x1024x75

A device alias is a shorthand representation of a device path. For example, the alias disk may represent the complete device path name: (see tables below). Systems usually have predefined device aliases for the most commonly-used devices, so users rarely need to type a full device path name. The alias disk is the commonly-used default boot-device alias. Use the **dev alias** command (from the PROM prompt, 'ok') to display all current device aliases.

ok devalias	- Display all current device alias
ok devalias alias	- Display device path for corresponding alias

The following table represents typical device aliases for a SPARC system:

SPARC

ALIAS	BOOT PATH	DESCRIPTION
disk	/sbus/esp/sd@3,0	SCSI disk at target 3
disk0	/sbus/esp/sd@0,0	SCSI disk at target 0
disk1	/sbus/esp/sd@1,0	SCSI disk at target 1
disk2	/sbus/esp/sd@2,0	SCSI disk at target 2
disk3	/sbus/esp/sd@3,0	SCSI disk at target 3
tape	/sbus/esp/st@4,0	tape drive at target 4
tape0	/sbus/esp/st@4,0	tape drive at target 4
tapel	/sbus/esp/st@5,0	tape drive at target 5
cdrom	/sbus/esp/sd@6,0:c	CD-ROM partition c
cdroma	/sbus/esp/sd@6,0:a	CD-ROM partition a
net	/sbus/le	Ethernet
floppy	/fd	Floppy drive

The NVRAM settings can be changed within the software as well as in the firmware. In some cases like the output-device they have to be checked in both places to ensure the settings have been changed. To set the NVRAM settings within UNIX using the **eeeprom** command:

gccs45% su -	- become root
# eeprom output-device=screen	Using the eeprom command the “=” sign must be used to set the functionality

Both firmware settings and software settings should be the same. If they are not the same you could have problems with the initialization of the system.

Booting a System

If a system is powered off, turning it on starts the default multi-user boot sequence. The following procedures explain how to boot in different states from the **ok** (PROM) prompt. If the PROM prompt is **>**, type **n** to display the **ok** prompt, or use the appropriate **boot** command.

Boot Types

A boot type describes how a system is booted, which may include a shutdown of the operating system as well. As a system administrator, it is required to know the following different boot types:

- **Interactive boot** - This type of boot prompts to provide information about how the system is booted, such as the /etc/system path, kernel path and device path name.
- **Reconfiguration boot** - The system is reconfigured to support newly added hardware or new pseudo devices.
- **Recovery boot** - The system is hung or an invalid entry is prohibiting the system from booting to completion or from allowing users to log in.

The Boot Command

Use the **boot** command to change to a different run level. The command formats follow:

ok boot [device-alias] [option]

>b [device-alias] [option] on SPARCs OR **boot [device-alias] [option]** on ULTRAs

The options for the **boot** command are:

- a Performs an **interactive boot** that prompts for root and swap devices and several important system files.
- r Performs a **reconfiguration boot** where the system probes all attached devices and creates entries for all found devices in the /devices and /dev directories.
- s Brings the system to run level S (single user mode), but prompts first for the root password. (**recovery boot** if device-alias is CDROM)
- v Displays detailed startup messages.

Booting to Multi-User State From PROM Level

To boot into multi-user state, type **boot** and press **RETURN** at the PROM prompt. The automatic boot procedure starts on the default drive, displaying a series of start-up messages. The system is brought up in multi-user state.

Booting to Single-User State from PROM Level

To boot into single-user state, type **boot -s** and press **RETURN** at the PROM prompt. The system boots to single-user mode and prompts for the root password:

ok boot -s

INIT: SINGLE USER MODE

Type **Ctrl-d** to proceed with normal start-up,

(or give root password for system maintenance): **XXXXXXX**

NOTE: To continue the process and bring the system up into multi-user state, press **CONTROL-D**.

Booting a System Interactively

Users may boot interactively in order to make a temporary change to a system file or the kernel. In doing this, changes can be tested and a system recovery can be completed easily if problems are experienced.

1. Boot the system interactively by using the **boot -a** command.
2. Answer the system prompts as described below:

If the System Displays ...	Do the Following ...
Enter filename [kernel/unix]:	Provide the name of another kernel to use for booting. Or, press RETURN to use the default kernel (/platform/`uname -m`/kernel/unix).
Name of default directory for modules [/platform/`uname -m`/kernel /kernel /usr/kernel]:	Provide an alternate path for the modules directory and press RETURN . Or, press RETURN to use the default modules directory path.
Name of system file [/etc/system]:	Provide the name of an alternate system file and press RETURN . Or, press RETURN to use the default /etc/system file.
root filesystem type [ufs]:	Press RETURN to use the default root file system type: UFS for local disk booting or NFS for diskless clients.
Enter physical name of root device [physical-device-name]	Provide an alternate device name and press RETURN . Or, press RETURN to use the default physical name of the root device.

In the following example, the default choices (shown in square brackets) were accepted by pressing **RETURN**:

```
ok boot -a
(Hardware configuration messages)
rebooting with command: -a
Boot device: /iommu/sbus/espdma@4,8400000/esp@4,8800000/sd@3,0
File and args: -a
Enter filename [/kernel/unix]: <return>
```

(Copyright notice)

Name of system file [/etc/system]: <return>

Name of default directory for modules [/kernel /usr/kernel]: <return>

Enter name of device instance number file [/etc/path_to_inst]: <return>

root file system type [ufs]: <return>

Enter physical name of root device

[/iommu@f,e0000000/sbus@f,e0001000/espdma@f,400000/esp@f,
800000/sd@3,0:a]: <return>

swap filesystem type [swapfs]: <return>

Configuring network interfaces: le0.

Hostname: gccsl

(fsck messages)

The system is coming up. Please wait.

(More messages)

gccsl console login:

Run Control Files

The operating system provides a detailed series of run control (rc) scripts to control init state changes. Each run level has an associated rc script/file located in the /sbin directory. Most rc files contain a directory bearing the filename of the rc script plus an A extension. The rc files are located in the /sbin directory, and the corresponding script directories are located in the /etc directory.

For example:

s3:3:wait:/sbin/rc3	> /dev/console 2>&l </dev/console
---------------------	-----------------------------------

The s3 (id - field1) line from the /etc/inittab file invokes the /sbin/rc3 (process - field4) script when the system enters run level 3 (runlevel - field 2). When the init process encounters this line upon entering run level 3, it will start the /sbin/rc3 script and wait until the script finishes. Then the /sbin/rc3 script will scan the /etc/rc3.d directory for scripts to run (in alphabetic, then numeric order). Each script in the rc3.d directory handles a specific system function. The actions of each run control level script are summarized as follows:

The **/sbin/rc0** Script

- Stops system services and daemons
- Terminates all running processes
- Unmounts all file systems

The **/sbin/rc1** Script

- Runs the /etc/rc1.d scripts
- Stops system services and daemons
- Terminates all running processes
- Brings the system up in single-user mode

The **/sbin/rcS** Script

- Runs the /etc/rcS.d scripts to bring the system up to single-user mode
- Mounts /usr, if necessary
- Sets the system name
- Checks the / and /usr file systems
- Mounts pseudo file systems (/proc and /dev/fd)
- If it is a reconfiguration boot, rebuilds the device entries

The **/sbin/rc2** Script

- Runs the /etc/rc2.d scripts
- Mounts all file systems
- Creates device entries in /dev for new disks (only if boot -r is run)
- Configures default router
- Sets the NIS domain and the ifconfig netmask
- Starts inetd, named, and rpcbind, if appropriate
- Starts NIS daemons (ypbind) and NIS+ daemons (rpcnisd), as appropriate
- Starts kerserv, statd, lockd
- Starts the automount, cron, LP, and sendmail daemons

The **/sbin/rc3** Script

- Runs the /etc/rc3.d scripts
- Starts syslogd
- Cleans up sharetab
- Starts nfsds
- Starts mountd
- If boot server, starts rarpd and rpc.bootparamd

The **/sbin/rc4** Script

- Not Used.

The **/sbin/rc5** Script

- Runs the /etc/rc0.d scripts
- Kills the printer daemons
- Unmounts local file systems
- Kills the syslog daemon
- Unmounts remote file systems
- Stops NFS services
- Stops NIS services
- Stops rpc services
- Stops cron services
- Kills all active processes
- Powers off System

The **/sbin/rc6** Script

- Runs the /etc/rc0.d/K*
- Kills all active processes
- Runs the initdefault entries in the /etc/inittab file

/etc/inittab & Run Control Files

A common practice in modifying the boot process is adding entries to the /etc/rc#.d script files such that new processes may be started at specific run levels. Although users can modify the /etc/inittab file to change the final stages of the boot sequence, there are drawbacks to this approach. It would be difficult to test the inittab entries or make the entries conditional upon factors other than run level. Therefore, using run control (rc) files is the preferred method for making boot process modifications. All scripts used by the rc files are actually located in the /etc/init.d directory. A symbolic link is made from the script in the /etc/init.d directory to a file in the appropriate /etc/rc#.d directory. These UNIX links are created using the *ln* command.

The link name or filename generally match the function they perform or the system service that they start or stop. For example, under /etc/init.d is a script called cron which (once invoked) runs others programs at scheduled times.

Scripts contain a case statement and take different actions depending on the argument contained on the command line (stop or start). Remember, the same script can be used at several run levels and the name controls the sequence of execution of several scripts in one directory (S01xxxx before S02xxxx and so on). Also, to avoid multiple copies of a script and to ease maintenance, symbolic links are used.

Shutting down a System.

When preparing to do an administration task, determine which shutdown command is appropriate for the system and the task at hand. There are many commands available to change system run levels:

/usr/sbin/shutdown

/usr/sbin/init

/usr/sbin/halt

/usr/sbin/reboot

/usr/sbin/poweroff

These commands initiate shutdown procedures; kill all running processes, write out any new data to the disk, and shutdown the system software to the appropriate run level. The **init**, **reboot**, and **shutdown** commands are the most preferred methods of changing system states. These commands are the most reliable for shutting down a system because they use a number of rc scripts to kill running processes. The **shutdown** command actually executes the **init** command after sending a warning message and monitoring a grace period.

The shutdown Command

Use the **shutdown** command when shutting down a system with multiple users. The **shutdown** command sends a warning message to all users who are logged in, waits for 60 seconds (default), and shuts down the system to single-user state. The command format follows:

shutdown [-y] [-g seconds] [-i runlevel]

The options for the **shutdown** command are:

- y Use this option to continue with the system shutdown without intervention; a prompt will allow the user to continue the shutdown process.
- g Allows users to specify a time (in seconds) before the system is shutdown.
- i Allows a user to bring the system to a different run level other than the default run level S. Choices are run levels 0, 1, 2, 5, and 6.

NOTE: It is best to bring the system to run level 0 before moving to a new run level. Hence, if the system is currently at run level 3 and run level 1 is desired, first change to run level 0 then to run level 1.

Use the **halt** command when the system must be stopped immediately. The **halt** command shuts down the system without any delay and does not warn any other users on the system. Using the **halt** command will not perform a clean shutdown as it does not run any of the run control scripts and may cause fsck to run.

Use the **poweroff** command to shut down a system that is capable of being powered off by the operating system. The **poweroff** command does not warn users on the system, and it is equivalent to using init 5.

Rebooting the System

To reboot, type **reboot** or **init 6** and press **RETURN**. Information is written to the disk, all active processes are killed, and the system is brought to a power-down state. It is then rebooted to the default run level specified in the /etc/inittab file.

init 6

Use the **reboot** or **init 6** commands to shut down a system that does not have multiple users to bring it back into multi-user state. The reboot command performs an unconditional shutdown of system processes and will tend to be much quicker than using shutdown. Reboot does not run all the rc scripts and is not as graceful as the init or shutdown command. The reboot command does sync file systems so this is not a concern.

If the system does not respond to an init command, the **poweroff** or **halt** command can be used to shut the system down. In worst case scenarios, physically pressing the button will also perform a shutdown. Holding the button longer than five seconds will remove power from the system.

ASSIGNMENT SHEET 2-2-1

UNIX OPERATING SYSTEM REVIEW

A. Introduction

This assignment sheet is to be completed as homework.

B. Enabling Objectives

- 2.5 **DESCRIBE** the UNIX operating system.
- 2.6 **DISCUSS** UNIX directory structure.
- 2.7 **DEMONSTRATE** the ability to launch an X-Term window.
- 2.8 **DISCUSS** UNIX command structure.
- 2.9 **DEMONSTRATE** the use of UNIX directory commands.
- 2.10 **DEMONSTRATE** the use of UNIX file and miscellaneous commands.
- 2.11 **DEMONSTRATE** the use of UNIX system commands.
- 2.12 **DEMONSTRATE** the use of file and directory permissions in UNIX.
- 2.13 **DESCRIBE** the differences between Solaris and HP UNIX.
- 2.14 **DEMONSTRATE** the use of visual editor (vi).

C. Study Assignment

- 1. Read Information Sheet 2-2-2, 2-2-4 and 2-2-5
- 2. Complete Job Sheet 2-2-6 and 2-2-7

D. Study Questions

- 1. What resource is always available for command syntax?

- 2. Describe UNIX's directory structure.

3. What is the difference between the Solaris and HP-UX system administration tools?
4. State the difference between formatting a floppy in Solaris and HP-UX?

Match the definition with the corresponding command and/or option.

- | | | | |
|--------|--|----|--------------|
| 1. ___ | Copies files or directories. | a. | mv |
| 2. ___ | Displays the last number of lines in a file. | b. | mkdir |
| 3. ___ | Moves/renames files. | c. | tail |
| 4. ___ | Creates a new directory. | d. | cp |
| 5. ___ | Displays a list of files and sub-directories for the current directory, including hidden files | e. | more |
| 6. ___ | Searches file system for specified file or directory name. | f. | find |
| 7. ___ | Combines or appends the contents of a file. | g. | ls -a |
| 8. ___ | Searches within files for specified character strings | h. | grep |
| | | i. | cat |
| | | j. | rm |

- | | | | |
|---------|---|----|------------|
| ___ 1. | Moves the cursor to the beginning of the previous paragraph. | a. | J |
| ___ 2. | Changes the case of the letter at the current cursor position. | b. | ~ |
| ___ 3. | Moves the cursor right one character. | c. | x |
| ___ 4. | Moves the cursor to the beginning of the last line of the file. | d. | l |
| ___ 5. | Joins two lines. | e. | { |
| ___ 6. | Deletes a character at the cursor position. | f. | G |
| ___ 7. | Repeats the last command entered. | g. | :q! |
| ___ 8. | Deletes complete line. | h. | I |
| ___ 9. | Inserts text at the beginning of the current line. | i. | dd |
| ___ 10. | Quits the file <u>without</u> saving. | j. | . |

INFORMATION SHEET 2-2-2

SYSTEM HIERARCHY

A. **Introduction**

This information sheet provides a description of the UNIX System Hierarchy.

B. **References**

None

C. **Information**

UNIX is a multi-user and multi-tasking operating system widely used by the military and civilian sectors for data servers. The operating system was developed in the late 1960's by Ken Thompson from Bell Labs and has spawned multiple versions. Some of the more popular are HP-UX, Solaris, and Linux. The 3.X version of GCCS-M onboard ships operates on HP-UX 10.20. The new 4.0 version of GCCS-M afloat operates on Solaris 8. To read more about the history of UNIX, please browse to the following url: <http://cm.bell-labs.com/cm/cs/who/dmr/hist.html>

1. Directory Structure

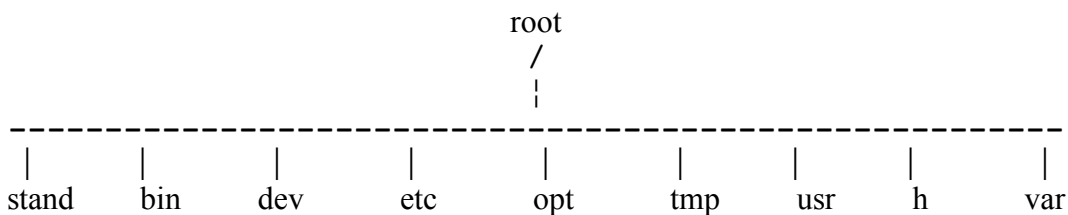
UNIX based systems use a hierarchical file system structure. A hierarchy is an organization of entities or directories and files in UNIX. Directories are logical storage locations. The UNIX hierarchical file system is tree structured and at the base of the tree structure is the root directory. From root it branches out to other directories and files. Root is denoted with a slash (/) and may contain many files and subdirectories, which make up the file system. UNIX establishes some directories and files when installed; these sub-directories contain system and user files necessary for operation.

Each file or subdirectory under the root directory is denoted by its name and pathname. The pathname may be absolute or relative, which describes the route to the file from the root directory for the user. Absolute (Full) Pathname is a list of directories leading to a file or subdirectory, beginning from the root directory (/). E.g., the full pathname of the exec directory is /export/exec. Slash (/) represents the root directory, but also separates directory and filenames. The relative pathname is a series of directory names locating the file in relation to the current

(working) directory. For example, if the user is in the root directory, the relative pathname to the exec directory is export/exec. Note that the name of the current directory is not used. Upon logging in, as sysadmin the System Administrator is placed into a "home" directory, this directory is /h/USERS/local/sysadmin. The Sysadmin user can return to this directory by simply typing **cd**.

All Sub-directories branch from the root directory.

Example:



1. Standard Root Sub-directories:

a. **/bin** directory:

The traditional location for all unix binary (executable) files.

b. **/dev** directory:

Contains the device (terminal/printer) driver files. All UNIX devices whether they are internal or external must have a file entry in this directory. **Warning:**

Never remove files from this directory.

(1). **/dev/rmt** directory:

Contains the device files for raw SCSI devices. For example:

/dev/rmt/3m, stores the device file for the DAT drive.

(2). **/dev/dsk** directory:

Contains the device files for hard and floppy disks. The first number of the device filename identifies the SCSI address of the device; the last number indicates slot number. Slot number 0 is used for the system board.

For example: **/dev/dsk/6s0**: Device file for the boot drive.

- c. **/etc** directory:
Contains maintenance commands and essential data files for system administration, including the password (passwd) file. Other important files are the group and hosts files.
- d. **/lib** directory:
Contains files crucial to UNIX programs.
- e. **/tmp** directory:
Scratchpad area for programs to use. This directory is cleaned out at each bootup.
- f. **/usr** directory:
Traditional location of user oriented files and sub-directories (user home directories).
 - (1). **/usr/bin/x11**:
The X windows binary files. The X windows utilities that come with the X windows Release 11 reside in this directory.
 - (2). **/usr/lib/x11**:
This directory is used for the X windows Systems files.

2. **Shell** (Command Interpreter)

- a. The shell delineates the boundaries of the computer operating system and is a command interpreter that acts as an interface between users and the operating system. It is responsible for interpreting the commands a user enters, calling the required program(s) executing the command, queuing the process into the kernel for processing, and ensuring the programs of the command are processed by the operating system.
- b. Shell commands can be used interactively. They are executed one at a time by the user via a terminal. In this sense, it serves as a direct interface between the user and the operating system.
- c. The shell can also be used as a high-level programming language which supports looping and logic constructs, variables, functions, parameters, and features that are unique to UNIX which allow it to be a true and consistent operating system interface. To use the shell as a high-level programming language, shell commands

are arranged in a file called a shell script. The script is then executed as a high-level program much like a BASIC program.

- d. This dual feature of the shell allows great flexibility for the user. Complex operations can be performed easily with short commands or elaborate programs can be built with little work.
- e. Just as there are many flavors of the UNIX operating system, there are many flavors of the UNIX shell. Three of the most popular are Bourne shell, the C shell, and the Korn shell. Each shell has its own features and set of commands.
- f. More than one shell can reside on a single UNIX system. Different users can use the different shells at the same time. It is also possible for a user to switch from one shell to another while using UNIX. One of the powers of UNIX is the ability to provide a customized user interface which demonstrated the capability of being able to choose various shells.
- g. Types of UNIX Shells
 - (1). **bourne** - This is the standard UNIX System V shell. It was developed by Steve Bourne at AT&T Laboratories. The bourne shell was designed for general- purpose use and is relatively efficient. Two advantages are:
 - The ability to redirect standard error and standard output to different places enabling the user to receive clean output
 - The Bourne shell is more compact and thus is easier to learn
 - (2). **C** - The shell was developed by Bill Joy as part of the Berkley UNIX. It provides the standard System V shell features, plus several features not included in the Bourne shell. The advantages of the C shell are:
 - access to previous commands (command history)
 - protection from accidentally overwriting existing files when you redirect output to them
 - ability to process arrays of numbers and strings and to evaluate logical and numerical expressions
 - command name abbreviation (aliasing)

(3). **Korn** - The Korn shell was developed by David Korn of Bell Laboratories. It was designed so that scripts written in the Bourne shell could be executed under it without having to be modified. It includes most of the features of both the Bourne and C shells (including aliasing). Other features include the following:

- Provides report formatting capabilities
- Supports a wider range of metacharacters (wildcard characters)
- Though considerably larger and more complex than the Bourne shell, it is noticeably more efficient because it has more built-in functions that can be performed directly by the shell.

3. GCCS-M specific directories:

a. **/h/USERS/global:**

This is a shared network file system (NFS) used to merge accounts and profiles.

b. **/h/data/local:**

This is a file system where local GCCS-M and COE directories and files reside.

Examples include: **UB**. This is the Unified Build directory. It contains directories for Overlays, Routes, Screen Kilos, etc.

b. **/h/data/global/UCP:**

This is a shared NFS where globally accessed GCCS-M communication management directories reside.

c. **/ h/COE/Comp/APM/bin**

Directory where all APM related scripts are stored.

THIS PAGE INTENTIONALLY LEFT BLANK

DIAGRAM SHEET 2-2-3

SOLARIS AND UNIX DIFFERENCES

A. Introduction

This information sheet provides comparisons between UNIX and Solaris syntax of many of the common commands.

B. References

<http://www.unixporting.com/quickguide.html>

C. Information

There are a few differences between UNIX operating systems. Some Solaris commands are slightly different than those found in HP versions of UNIX. The information below highlights some (but not all) of these differences:

SOLARIS	HP-UX 10.X/11.X
---------	-----------------

DISK SPACE AND INFORMATION

Solaris 8	HP-UX 10.x 11.x
/usr/sbin/df	/usr/bin/df
/usr/sbin/df -k	/usr/bin/bdf
/usr/sbin/mount, umount	/sbin/mount, umount
/usr/sbin/devinfo	/usr/sbin/diskinfo
	/dev/rdisk/device_file

KERNEL CONFIGURATION

Solaris 8	HP-UX 10.x 11.x
/etc/system	/stand/system

PROCESSES

Solaris 8	HP-UX 10.x 11.x
/usr/bin/ps -ef	/usr/bin/ps -ef
/bin/truss	tusc
/usr/bin/iostat	/usr/bin/iostat
/usr/ucb/users	/usr/bin/users
/usr/bin/prstat	/usr/bin/top

PHYSICAL MEMORY

Solaris 8

/usr/sbin/dmesg | grep mem
/usr/sbin/prtconf | grep memory

HP-UX 10.x 11.x

/etc/dmesg | grep -i phys

HARDWARE STATUS/INFORMATION

Solaris 8

dmesg
/usr/bin/arch -k

HP-UX 10.x 11.x

dmesg
/usr/bin/model

UNIQUE ID

Solaris 8

/usr/sbin/dmesg | grep ether
/usr/bin/hostid

HP-UX 10.x 11.x

/usr/sbin/lanscan
/usr/sbin/lanscan, /usr/bin/uname -I

SWAP

Solaris 8

/usr/sbin/swap -a
/usr/sbin/swap -l
vmstat

HP-UX 10.x 11.x

/usr/sbin/swapon -a
/usr/sbin/swapinfo
vmstat

SYSTEM FILES

Solaris 8

/etc/rc#.d
/etc/rc#.d
/etc/vfstab
/etc/inet/hosts
/etc/shadow
/etc/group

HP-UX 10.x 11.x

/etc/rc#.d
/sbin/init.d
/etc/fstab
/etc/hosts
/etc/passwd
/etc/group, /etc/loggingroup

THE X WINDOW SYSTEM

Solaris 8

/usr/openwin/bin/xterm
/usr/openwin/bin/xhost

HP-UX 10.x 11.x

/usr/bin/X11/xterm
/usr/bin/X11/xhost

HOSTNAME

Solaris 8

/usr/bin/hostname
 /etc/inet/hosts
 /usr/bin/uname -a

HP-UX 10.x 11.x

/usr/bin/hostname
 /etc/hosts
 /usr/bin/uname -a

NETWORKING

Solaris 8

/usr/sbin/showmount
 /etc/dfs/dfstab
 /usr/sbin/share
 /usr/lib/netsvc/yp/ypbind
 /usr/sbin/route
 /usr/sbin/in.routed
 /usr/bin/netstat
 /usr/bin/rsh

HP-UX 10.x 11.x

/usr/sbin/showmount
 /etc/exports
 /usr/sbin/exportfs
 /usr/lib/netsvc/yp/ypbind
 /usr/sbin/route
 /usr/sbin/gated
 /usr/bin/netstat
 /usr/bin/remsh

TAPE COPIES

Solaris 8

/usr/bin/cpio
 /usr/sbin/tar
 tar cvf /dev/rmt/0m
 tar cvf /dev/rmt/0m file
 tar xvf /dev/rmt/0m

HP-UX 10.x 11.x

/usr/bin/cpio
 /usr/sbin/tar
 tar cvf /dev/rmt/0m
 tar cvf /dev/rmt/0m file
 tar xvf /dev/rmt/0m

Tape Devices

Solaris 8

/vol/dev/dsk/cXtXdX (CD-ROM)
 /dev/rmt/0m (tape)
 /usr/bin/eject

HP-UX 10.x 11.x

/dev/dsk/c0tXd0 ("X" is address)
 /dev/rmt/0m
 /usr/bin/tcio -r

SOFTWARE

Solaris 8

/usr/sbin/pkgadd
 /usr/sbin/pkginfo
 /usr/sbin/pkgrm
 /usr/bin/showrev -p
 /usr/sbin/patchadd
 /usr/sbin/patchrm
 /usr/sbin/pkgchk
 /usr/sbin/swmtool

HP-UX 10.x 11.x

/usr/sbin/swinstall
 /usr/sbin/swlist
 /usr/sbin/swremove
 /usr/sbin/swlist | grep PH
 /usr/sbin/swinstall
 /usr/sbin/swremove
 /usr/sbin/swverify
 /usr/sbin/swinstall, /usr/sbin/swremove

/usr/bin/pkgmk

/usr/sbin/swpackage

DAEMONS

Solaris 8

/usr/bin/cron
/usr/bin/atq
/usr/bin/atrm

HP-UX 10.x 11.x

/usr/bin/cron
/usr/bin/at -q
/usr/bin/at -r

BACKUP/RESTORE

Solaris 8

/usr/sbin/ufsdump
/usr/sbin/ufsrestore

HP-UX 10.x 11.x

/usr/sbin/fbackup, dump, rdump
/usr/sbin/frecover, restore, rrestore

CORE FILES

Solaris 8

/usr/bin/savecore
/usr/sbin/crash
/usr/bin/coreadm

HP-UX 10.x 11.x

/sbin/savecrash
/usr/sbin/crashutil
/etc/rc.config.d/savecrash

DISK FORMATTING

Solaris 8

/usr/sbin/format
/usr/sbin/format
/usr/sbin/format

HP-UX 10.x 11.x

/usr/bin/mediainit
/usr/sbin/pvcreate, vgcreate, lvcreate
/usr/sbin/pvremove, vgremove, lvremove,
vgreduce, lvreduce, vgextend, lvextend,
pvdisplay, vgdisplay, lvdisplay

PRINTING

Solaris 8

/etc/printers.conf
/usr/bin/lpstat
/usr/bin/lp
/usr/bin/cancel
/usr/spool/lp/model

HP-UX 10.x 11.x

/usr/lib/lp/model
/usr/bin/lpstat
/usr/bin/lp
/usr/bin/cancel
/usr/lib/lp/model

MISCELLANEOUS

Solaris 8

/usr/ucb/whoami
/usr/bin/dos2unix
/usr/bin/eject
/usr/bin/fdformat

HP-UX 10.x 11.x

/usr/bin/whoami
/usr/bin/dos2unix
/usr/bin/tcio -r
/usr/bin/mediainit -f

/usr/bin/makedev	/usr/sbin/mkno
/usr/bin/mpstat	/opt/perf/bin/glance, /opt/perf/bin/gpm
/usr/bin/pagesize	/opt/perf/bin/glance, /opt/perf/bin/gpm
/usr/bin/setfacl	/usr/bin/chacl
/usr/bin/showrev	/usr/bin/uname -a
/usr/bin/tip	/usr/bin/cu
/usr/sbin/add_drv	/usr/sbin/mknod, /usr/sbin/insf, /usr/sbin/mksf
/usr/sbin/cfgadm	/usr/sbin/ioscan
/usr/sbin/devfsadm	/usr/sbin/mknod, /usr/sbin/insf, /usr/sbin/mksf
/usr/sbin/dhccpconfig	/sbin/auto_parms
/usr/sbin/dhtadm	/usr/sbin/dhcptools
/usr/sbin/disks	/usr/sbin/mknod, /usr/sbin/insf, /usr/sbin/mksf
/usr/sbin/fdisk	/usr/sbin/lvlnboot, /usr/sbin/lvcreate
/usr/sbin/growfs	/usr/sbin/extendfs, /usr/sbin/fsadm, /usr/sbin/lvextend
/usr/sbin/installboot	/usr/sbin/lvlnboot
/usr/sbin/metaparam	/usr/sbin/lvchange, /usr/sbin/vgchange
/usr/sbin/metastat	/usr/sbin/lvdisplay, /usr/sbin/pvdisplay,
	/usr/sbin/vgdisplay
/usr/sbin/metasync	/usr/sbin/lvsync, /usr/sbin/vgsyncr
/usr/sbin/nslookup	/usr/bin/nslookup
/usr/sbin/poweroff	/usr/sbin/shutdown
/usr/sbin/prtconf	/usr/bin/getconf
/usr/sbin/prtconf grep -i memory	/usr/sbin/swapinfo
/usr/sbin/rem_drv	/usr/sbin/rmsf
/usr/sbin/strace	/usr/bin/strace
/usr/sbin/strclean	/usr/bin/strclean
/usr/sbin/strerr	/usr/bin/strerr
/usr/sbin/sysdef	/usr/sbin/ioscan, /usr/sbin/sysdef
/usr/sbin/tapes	/usr/sbin/mknod, /usr/sbin/insf, /usr/sbin/mksf
/usr/ucb/fasthalt	/usr/sbin/reboot -q, /usr/sbin/shutdown

THIS PAGE INTENTIONALLY LEFT BLANK

INFORMATION SHEET 2-2-4 COMMAND FAMILARIZATION

A. Introduction

This information sheet provides many of the common UNIX and Solaris commands.

B. References

UNIX – The Complete Reference

C. Information

1. This lesson is an introduction to the UNIX command structure. Many more commands exist than are being taught in this lesson and is a starting point for system administrators. If a command is unknown or you are unsure of the proper syntax, use the man pages.

- a. **man** utilizes the **more** utility to display its output, so all pattern search and display capabilities of **more** can be used with **man**. Displays information from the online reference manuals one screen at a time.

- (1) Every manual entry follows the same basic organization. The top line of the output includes the name of the utility.
- (2) Name followed by a number enclosed in parenthesis that refers to the section of manual where the entry is located.
- (3) Capitalized words such as NAME and SYNOPSIS introduce the various sections of the entry.
- (4) To see the next line of the manual, press RETURN. To see the next page of the manual, press the space bar.
- (5) To exit man use ctrl-c or “q”.

- b. Command Syntax

- (1) Syntax - a specific way of entering a command.
- (2) **command [options][arguments][filename]**
 - (a). Uses lowercase letters

- (b). Some can be used alone
- (c). Others must use options, arguments, and filenames

(3) Options

- (a). Use both uppercase and lowercase letters
- (b). Are case-sensitive
- (c). Are usually preceded by a hyphen (-)
- (d). Are used to modify a command
- (e). Sometimes can be grouped
- (f). e.g., **ls -al** where **ls** is the command, and **-al**, the options

(4) Arguments

- (a). used in combination with the command and options to complete the function.
- (b). e.g., **grep -i STRING** where **grep** is the command, **-i** is the option, and **STRING** is the argument.
- (c). This example searches a file (grep) for a word (STRING), where the case of STRING is ignored (-i).

(1). Filename

The filename to which the command applies.

4. Directory Commands

- a. **pwd** instructs the computer to print the current working directory. In UNIX, print often means to display. The command **pwd** gives the absolute pathname of the current position in the filetree.
- b. **cd** change directories. The **cd** command allows the system administrator to move around the directory structure.
 - (1) **cd** with no argument moves the current directory to the home directory
 - (2) **cd *directoryname*** moves from the current directory to a sub-directory
 - (3) **cd ..** moves back one directory.

- (4) **cd ../*directoryname*** moves back one directory and then into the specified subdirectory. This command allows the user to move laterally within a directory with only one command.
- (5) **cd /*directoryname/directoryname*** moves into the absolute path of specified directory

c. **cp** copy a file or directory

- (1) **cp /*directoryname/filename*** copies the specified file from the directory into the current directory.
- (2) **cp *directoryname/filename directoryname2*** copies the specified file into the specified subdirectory.
- (3) **cp -r /*directoryname/subdirectory*/*** Copies all subdirectories and their related files from the specified path into the current working directory.
- (4) **cp -rp /*directoryname/sub-directory*/*** performs the same as "cp -r" but maintains ownership of the copied directories and files.
- (5) **cp -i /*directoryname/filename*** prompts the user whenever the "cp" command will overwrite an existing file. Prompts with overwrite y/n?
- (6) **cp *filename1 filename2***
 - *filename1* is the name of the file to copy from.
 - *filename2* is the name of the file to copy to. If *filename2* does not exist will create it with this command.

d. **ls** lists filenames (including directory name) located in the current directory. Lists contents of directories.

- (1) **ls *directory name*** lists filenames (including directories) located in the specified directory
- (2) **ls -a** lists all filenames of hidden files, in addition to the files visible with the regular "ls" command. Hidden files normally set up the system environment and usually do not need to be accessed.
- (3) **ls -l** produces the long directory listing that includes file permissions, file owner, date, and size. HP-UX includes group owner in long listing

- (4) **ls -r** (recursive) lists all files and sub-directories from current directory
 - (5) **ls -g** same as “ls -l”, except that only the group is printed (displayed) and owner is omitted.
 - (6) **ls -f** (mark directories and files).
 - (a). Directories are marked with a trailing slash “/”.
 - (b). Executable files are marked with a trailing asterisk “*”.
 - (c). Symbolic links are marked with a trailing at sign “@”.
 - e. Other directory commands:
 - (1) **mkdir** creates new directories and subdirectories. If a path is not designated, the new directory will be a subdirectory of the current working directory.
 - (2) **mkdir -p newdirectory1/newdirectory2** the **-p** option allows the user to create multiple levels of directories in one command.
 - (3) **rmdir** deletes directories. The directory must be empty, and the **rmdir** command must be run from a directory other than the one being deleted.

3. File commands

 - a. **find** performs a search of the filesystem for a file or directory
 - (1) **find / -name *directory or file* -print** searches the file system **starting with** the root for the file or directory specified, and display the results on the screen.
 - (2) **find . -name *directory or file* -print** searches the filesystem from the **current directory** for the specified file or directory and displays the results on the screen.
 - (3) **find *pathname* -name *filename* -print** performs a search of the filesystem for files/directories starting at the specified path.
 - b. **grep** searches within files for specified character strings.
 - (1) **grep *searchstring filename or directoryname*** searches the specified file or directory for the desired character string.

- (a). When searching directories, `grep` lists each file whose contents have the desired string.
 - (b). When searching a file, `grep` lists each line containing the entered string.
 - (c). To search only the current directory use the `"*"` in place of the directory or filename.
- (2) **`grep "multiple word string" filename or directoryname`** searches the specified directory or filename for the multiple word string. Multiple word strings *must* be enclosed in quotes.
- c. **`rm filename`** removes/deletes files. In most cases a file cannot be retrieved once it has been deleted.
 - `rm -i filename`** deletes a file only after operator confirms deletion at the y/n prompt.
 - `rm -R filename`** deletes a file or directory (and all files in that directory) without prompting the user.
- d. **>(redirect symbol)** The “greater than” symbol is referred to as a **REDIRECT** in UNIX. This symbol allows the user to redirect the output of one command or file to a new or existing file. Use caution with this command; a redirect to an existing file will overwrite the information in the file.
 - `command>filename`** will redirect the output of the command to the file specified, i.e. **`call>date`** will output a calendar to a file by the name of `date`. If this file does not exist, this command will make the file.
- e. **`cat`** combines or appends files.
 - (1) Multiple files can be combined into one new file.
 - (2) Files can be appended to the end of an existing file.
- f. To combine *two* files into *one* new file using **`cat`** and **>**
 - (1) Type **`cat filename1 filename2 > filename3`**.

- (2) *filename1* and *filename2* are the files whose contents will be combined into *filename3*.
 - (3) If *filename3* already exists, it will be overwritten
 - (4) the original *filename1* and *filename2* remain unchanged.

- g. To append a file to the end of another using **cat** and **>>**:
 - (1) Type **cat *filename1* >> *filename2***.
 - (2) The contents of *filename1* are *added to the end of filename2*.
 - (3) The original *filename1* remains unchanged

- h. **more filename** - displays the contents of a file one screen at a time
 - (1) **f** scrolls forward one page
 - (2) the space bar can also be used to advance one screen, or the **<ENTER>** key to advance by single lines.
 - (3) **b** scrolls backwards one page
 - (4) **q** quits the display of the file contents.
 - (5) The **more** command can be used with other commands such as **ls | more**
 - (6) **ls | more** lists the files one page at a time

- i. **head -x filename** is used to view the first *x* lines of a file
 - (1) *x* is the number of lines to be viewed
 - (2) *filename* is the name of the file to be viewed
 - (3) If a numeric value is not entered, a default of 10 is used.

- j. **tail -x filename** is used to view the last *x* lines of a file.
 - (1) *x* is the number of lines to be viewed
 - (2) *filename* is the name of the file to be viewed
 - (3) If a numeric value is not entered, a default of 10 is used.

k. Using **more** with **head** and **tail**

- (1) For example **head -100 filename | more**. This displays the first 100 lines of the file, one "screen" at a time.
- (2) For example, **tail -50 filename | more**. This displays the last 50 lines of the file, one "screen" at a time.

l. **mv** moves/renames files

- (1) **mv** moves the name and contents of one file to another file.
- (2) The original file is renamed; only one copy of the file is maintained.
- (3) Type **mv filename1 filename2**.
- (4) **mv /directoryname1/filename /directoryname2** moves the specified file to a new directory, using the original filename
- (5) **mv /directoryname1/filename1 /directoryname1/filename2** moves the specified file to a different filename in the same directory, without having to change into the source or target directory.

m. **ln** - link

- (1) Creates a link between two files. A Link allows a given file to be accessed by means of two or more different names.
- (2) The alternative names can be located in the same directory as the original file or in another directory.
- (3) If the file appears in the same directory as the one the file is linked with, the links must have different filenames.
- (4) A linked file points to another file. There is no physical copy.

4. Miscellaneous Commands

- a. **clear** - clears the display
- b. **hostname** - displays hostname at the system prompt; e.g., `comms1`
- c. **clear** - Clears the display screen of all data and redisplay the cursor at the top of the page.
- d. **who** displays current system users

- (1) Displays the login name, terminal name, and login time for current system users.
- (2) The node name of the machine from which the user logged in is displayed in parentheses.
- (3) A node name of (:0.0) denotes that the login is from the host CPU.

e. **telnet /ftp**

- (1) allows users to remotely log in to servers and clients.
- (2) ftp allows users to transfer files from one machine to another

5. System Control Commands

a. Viewing and setting the system date (**date**)

- (1) **date** displays and/or resets the system date and time.
- (2) To display the system date and time:
 - (a). Type **date** at the system prompt.
 - (b). Type **date_mmddhhmm yy**
 - (c). *mm* is the month in digits.
 - (d). *dd* is the day in digits
 - (e). *hh* is the hour.
 - (f). *mm* is minutes
 - (g). *yy* is the last two digits of the year

b. Controlling and displaying system processes (**ps**)

- (1) Process - a command running on a CPU.
 - (a). Can only be executed one at a time, in sequence, from the keyboard.
 - (b). One must finish before the next can start.
- (2) Displaying processes (**ps**)
 - (a). **ps**, process status, displays information on the processes that are currently running on the system.
 - (b). Type **ps -ef**
 - (c). **e** displays information about all processes.
 - (d). **f** displays a full listing
- (3) Running a process in the background without having to wait for one to finish before starting the next.

- (a). Add an ampersand (&) to the end of a command to run in background mode.
- (b). For example, **grep "Section A-3" * &** This searches the directory for the string "Section A-3", while enabling other functions to be completed.
- (c). Drawback: (using the same example) the output from this command is displayed as each file is found. This could interrupt other functions being executed.
- (d). To avoid this, redirect the output into a file: e.g., **grep "Section A-3" * > tempfile & tempfile** is the name of the file into which the output is written. When complete, a notification message is displayed. tempfile's contents can be viewed using **more**.

(4) Stopping system processes

- (a). Normally, stop a UNIX-initiated process by pressing **CONTROL** and **C** simultaneously.
- (b). Background processes cannot be stopped with **CONTROL C**.
- (c). To **kill** a background process: Must know the process identification (PID) of the process to be killed.
- (d). Type **kill PID**, where **PID** is the process identification number of the process to be killed. The kill command has many levels, **kill -9** will immediately stop the process.

6. File and Directory Permissions

- a. Restrict access to files and directories for read, write, and execute capabilities.
- b. Indicated by the first ten characters of each line displayed by the **ls -l** command.
- c. The first character indicates the type of file, usually:
 - (1) - indicates an ordinary file.
 - (2) **d** - indicates a directory
- d. Characters 2-4 indicate permissions for the user of the file. The user is the person who created the file

- e. Characters 5-7 indicate permissions for the group users of the file
- f. Characters 8-10 indicate permissions for other users of the file (who are not owners or group members).
 - (1) **r** - indicates that the file can be read
 - (2) **w** - indicates that the file can be written to or edited.
 - (3) **x** - indicates that the file is an executable.
- g. Changing File Permissions (**chmod**)
 - (1) **chmod** changes the permissions of a file.
 - (2) Must be the root (or the file owner) to change permissions for the files:
 - (a). user (u)
 - (b). group (g)
 - (c). others (o)
 - (3) Default values for **chmod** changes permissions for all.
 - (4) To add permissions:
 - (a). Type **chmod 777 filename**.
 - (b). **filename** is the file to which permissions are added

Octal Value	File Permissions	Set Permissions Description
0	---	No permissions
1	--x	Execute permissions only
2	-w-	Write permissions only
3	-wx	Write and execute permissions
4	r--	Read permission only
5	r-x	Read and execute permissions
6	rw-	Read and write permissions
7	rwX	Read, write, and execute permissions

The first number refers to the permissions for the owner and is in binary coded octal notation: 4=Read, 2=Write, and 1=Execute. The second number refers to the permissions for the group and is also in binary coded octal notation.

The second number refers to the permissions for all other users and is also in binary coded octal.

(c). e.g., **chmod 666 progs**

Gives read and write permissions for all users to the "progs" file.

(d). e.g., **chmod 664 progs**

Gives write permissions to only the user and group members of the "progs" file.

(e). E.G. **chmod 777 progs**

Gives read, write, and execute permissions for all users to the "progs" file.

h. Changing ownership of directories and files (**chown**)

(1) **chown** changes the ownership of directories and files.

(2) Must be the owner of the directory or file or root to perform the command.

(3) To change ownership:

(a). Type **chown O filename**

(b). Type **chown O directory**

Note: To change all the directories and files below the intended directory, type **chown -R O directory**.

THIS PAGE INTENTIONALLY LEFT BLANK

INFORMATION SHEET 2-2-5

VI EDITOR

A. Introduction

This lesson will provide the trainee a basic understanding of Visual Text Editor (vi).

B. References

Sun Solaris Man pages

C. Information

1. Cursor Movement Keys:

- h** Moves left one character.
- j** Moves down one line.
- k** Moves up one line.
- l** Moves cursor right one character.

(Note: The arrow keys also work to navigate through the file.)

2. Moving by Words: The administrator may use a number in front of the following commands to multiply the command that many times. Using a number is optional.

- w** Word right.
- e** End of word right.
- b** Moves the cursor back one word.

3. Moving by Sentence

-) Next sentence.
- (Previous sentence.

4. Moving by Paragraph

- { Previous paragraph.
- } Next paragraph.

5. Moving by Screen

<cntrl>b Moves the cursor back one screen.

<cntrl>f Moves the cursor forward one screen.

6. Moving by Line

A Moves to the end of the line and inserts text.

:#<Return> Moves to the specified line number (3) in the document. If no number (#) is supplied, the cursor moves to the first line of the file.

G Moves to the beginning of the last line of the file.

7. Changing Text: Changing text places the analyst in insert mode. The analyst must use the **<ESC>** to exit from insert mode and enter additional commands.

cw Change word.

cc Change line.

r<character> Replaces character at the cursor position with the specified character.

~ Changes the case of the letter at the current cursor position.

R Overwrite.

J joins two lines.

8. Inserting Text: The **<ESC>** key is used with each of these commands. When the administrator is done inserting text he/she must select the **<ESC>** key before continuing with additional commands.

Do not use the cursor movement keys, or other commands while in insert mode.

i Inserts text at the cursor position.

I Inserts text at the beginning of the line.

a Adds text after the current cursor position.

A Inserts text at the end of the current line.

o Inserts a new line below the cursor.

O Inserts a new line above the cursor.

9. Deleting Text: The user may use a number (#) in conjunction with the following commands, to multiply the command that many times. Using a number is optional.
 - #x** Deletes character or specified number (#) of characters at the cursor position.
 - d#<spacebar>** Deletes the specified number (#) of characters from the cursor position. Performs the same function as **#x**.
 - #X** Deletes the specified number (#) of characters to the left of the cursor position.
 - D** Deletes the line from the cursor position to the end of the line.
 - d#w** Deletes the specified number (#) of words from the cursor position.
 - d#d** Deletes the specified number (#) of lines beginning with the line on which the cursor is positioned.
10. Undo and Repeat Commands
 - u** Used to undo the last change made, including the last undo.
 - .** Used to repeat the last *command* entered.
11. vi Search Commands: The analyst may use **n** to repeat the following commands.
 - /search string** Searches forward in the text file for the desired search string.
 - ?search string** Searches backwards in the text file for the desired search string.
12. Exiting/Closing vi
 - Shift ZZ** Saves the file and exits vi.
 - Esc :wq** Same as **ZZ**. Saves the file and exits vi. (Note: if you are root and not the owner of the file, you must add a “!” after the “q”)
 - Esc :q** Quits from an unmodified file.
 - Esc :q!** Quits vi *without saving*.

THIS PAGE INTENTIONALLY LEFT BLANK

JOB SHEET 2-2-6

BASIC AND ADVANCED UNIX COMMANDS

A. Introduction

This Job Sheet provides the student practice with some of the basic UNIX system commands.

B. Equipment Required

GCCS-M UNIX servers or workstations with the COE kernel loaded.

C. References

none

D. Safety Precautions:

Review TTO procedures

E. Job Steps:

1. Launch an xterm and perform the following commands.

2. Display the contents of the **/etc/hosts** file.

Enter the command here:

3. Use a text editor to display the **/etc/hosts** file.

Enter the command here:

4. Quit out of the **/etc/hosts** file **without** saving.

Enter the command here:

5. Determine the present working directory.

Enter this command here:

- a. Look this command up in the man pages. What notes, if any are present for this command?

6. Display the users who are logged into the CPU you are currently using.

What users are logged into the CPU you are using?

7. From the home directory, display the currently running processes one page at a time.

Redirect the output into a temporary file.

Enter the command used here:

8. Change directory to /tmp and create a directory naming it with your *last name*.

- a. Access the directory that has been created.
- b. Create a subdirectory called "*One*."
- c. Access the "*One*" subdirectory.
- d. Display the full pathname of the directory you have currently accessed.
- e. Return to the directory named with *your last name* and list the directory contents in long format. Enter this command here.
- f. Return to the /tmp directory.
- g. Create a directory called "*Two*."
- h. Copy the *lastname* directory and its contents into the "*Two*" directory.

Enter this command here:

- i. Rename the *Two/lastname* directory, using your *first name* as the new directory name.

Enter this command here:

- j. Return to the /tmp directory and perform a search for the "*One*" directory.

Enter this command here:

- k. Delete the directory named with your *first name*.
Enter this command here: (Does anything have to be completed before this?)
9. Change directory to /etc.
 - a. Print a long listing of the files and directories in /etc.
List three files or directories owned by root
10. Write the numeric and symbolic representation for the following permissions in the spaces provided below:
 - a. Read/write for owner, read only for all other users.
 - b. Read/write/execute for owner Read/execute for all other users.
 - c. Execute only for all users.
 - d. Read/write/execute for all users.
 - e. Interpret the following permissions for owner, group and user.
 - -r--r--r--
 - -rwxr-xr-x
 - 711
 - 775

Once the instructor has reviewed your work, delete all files created during this exercise.

Job Sheet completed:

Trainee _____ **Instructor's Initials** _____

THIS PAGE INTENTIONALLY LEFT BLANK

JOB SHEET 2-2-7

VISUAL TEXT (VI) EDITOR

A. Introduction

This Job Sheet provides the student practice with some of the UNIX Visual Text Editor (VI) functions.

B. Equipment Required

GCCS-M UNIX servers with the COE kernel loaded.

C. References:

None

D. Safety Precautions:

Review TTO procedures

E. Job Steps:

1. Launch an xterm.
2. Change directory to /tmp.
3. Create a new file and name it with your *first name*.
4. Change to insert mode and enter:
 UNIX is fun! Hit the enter key, and then type: **This is an exercise using Visual Editor.**
 Visual Editor (vi) is used to view, create, and edit files within UNIX.
5. Return to the Command mode.
 Enter the command used here:
6. Using the arrow keys, return to the beginning of the document.
 - a. Move to the end of the sentence and insert **“HA HA”**.
 - b. Insert **Solaris** in front of the word UNIX.
 Enter the command used here:

- c. Delete the words “Visual Editor” and the parentheses around “vi” in the second sentence.

Enter the command used here:

7. Add the following to the end of the existing text:

The Command Mode allows you to use the keyboard to execute vi commands.

8. Insert the following text at the beginning of the sentence added in Step 10:

The Insert Mode allows you to use the keyboard to enter text.

Enter the command used here:

9. Replace the capital “T” in “The Command Mode . . . “ with a lower case “t”.

Enter the command used here:

10. Use your last name to name the file.

11. Save the document and exit from vi.

Enter the command used here to save and exit the file:

Job Sheet completed:

Trainee _____ **Instructor's Initials** _____

ASSIGNMENT SHEET 2-3-1

FILE AND DIRECTORY STRUCTURE

A. **Introduction**

This assignment sheet is to be completed as homework.

B. **Enabling Objectives**

- 2.15 **DESCRIBE** types of file systems used in GCCS-M.
- 2.16 **DESCRIBE** the process of mounting file systems.
- 2.17 **DEMONSTRATE** the use of Disk Manager Tool to mount devices.
- 2.18 **CREATE** permanent mount entries with the Disk Manager Tool.
- 2.19 **DESCRIBE** GCCS-M specific directories and mount points.
- 2.20 **DESCRIBE** maintenance commands to include du, df, find, quot and tar commands.

C. **Study Assignment**

Read Information Sheet 2-3-2, 2-3-3 and 2-3-4

D. **Study Questions**

1. Which file, read during the boot process, is used to start the Volume Manager?

2. When manually mounting a file system which option would you use to specify mounting a specific file system?

3. Identify the seven fields of the /etc/vfstab file.

4. Which command is used to display the number of 512-byte blocks used per file or directory?

5. Which command may display file system names followed by such parameters as the available free disk space, used disk space, percentage of capacity used and mount points?

6. Which of the following is the correct format for using the find command?
 - a. find [-options] [pathname] [arguments] [output]
 - b. find [-options] [arguments] [pathname] [output]
 - c. find [pathname] [-options] [arguments] [output]
 - d. find [pathname] [arguments] [-options] [output]

INFORMATION SHEET 2-3-2

FILE SYSTEMS

A. **Introduction**

This lesson will provide the trainee a basic understanding of mounting and sharing file systems and devices.

B. **References**

Embedded Online Documentation

C. **Information**

A file system is a logical division or partition of a disk. An example of a file system is /home2 or /home2/scripts. The administrator defines the size and identifies disk resources for each file system on the computer. When adding a new disk to the computer, a new file system must be created in order for that disk to be recognized. In order to access the disk, the file system must first be mounted and if the disk is to be shared, the information must be exported. Administrators perform the following file system management functions:

- Mount and export file system partitions.
- Format hard drives.
- Display hard disk space availability.
- Initialize diskettes.

Types of File Systems

A file system is a grouping of files stored in a particular file system type. File system types support different media and storage devices and are formatted to support the efficient retrieval of data. The Solaris environment supports several file system types:

Disk-Based (Local) File Systems

Disk-based file systems are used to store data on physical media on the local system. The types of media supported are hard drives, floppy disks, CD-ROM drives, and magnetic tape. The available formats are:

ufs The UNIX file system is the default file system. File systems keep track of files by issuing them a number, called an inode. They are like the page listings within a table of contents ("***Inode***" is a contraction for index-node.)

UFS provides the following features.

- File system locking (only if application takes advantage of locking)
- Data blocks are (by default) 8K size with 1 K fragments. This provides a good balance for most needs
- Support for new-generation hard disks by de-referencing variable-length list structures
- Unlimited inodes and cylinders per cylinder group for disks

hfs The High Sierra File System is a file system for CD-ROM drives. It supports the High Sierra CD-ROM file formats and the ISO 9660-88 CD-ROM file formats using the Rock Ridge extension.

NTFS NTFS is a file system developed specifically for Windows NT and carried over to Windows 2000. It uses 64-bit disk addresses and can support disk partitions up to 2^{64} bytes. NTFS also that allows for file level security and compression.

Distributed (Network) File Systems

Distributed file systems are file systems that are accessed over the network. The available distributed file systems are:

nfs The network file system is the standard networking file system for UNIX. NFS file systems are file systems that appear to be in a directory structure, but actually reside on someone else's system. Instead of connecting to the data through disk cables, it is connected through the network.

CIFS The Common Internet File System is a Samba application that allows UNIX to see Windows based directories without TELNET or FTP.

Mounting Resources

In order for resources to be available in the UNIX environment, they must be mounted for use. Mounting is the process of inserting a resource into the UNIX directory structure. This means that the resource is given a directory within the directory structure, and this directory is referred to as its mount point. Most mounting commands will be completed within the Disk Manager utility covered in the next topic.

<u>Device</u>	<u>Mount Point</u>
/dev/dsk/c0t3d0s0/	/
/dev/dsk/c0t3d0s5	/var
/dev/dsk/c0t3d0s3	/security1
/dev/dsk/c0t3d0s7	/h

The physical devices are read as c= controller, t=target, d=disk, s=slice.

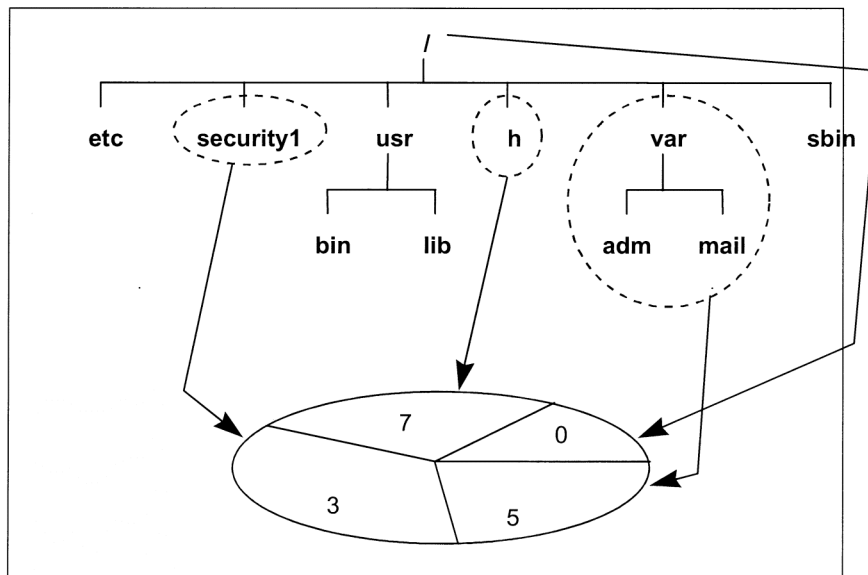


Figure 2-3-1 Hard Drive Partitioning Scheme

The four hard drive slices are each given mount points. Each mount point is a directory in the directory structure, and stored data is part of that directory. For example, the /var mount

point is slice 5. Any files stored in /var or any of its subdirectories will be stored on slice 5. This is also the same for /h and /securityl. Any directories that do not have their own mount point are stored in the / mount point (slice 0). This includes /etc, /usr, and /sbin. Disk slices are connected into the directory structure by mounting them onto a designated directory. By mounting a file system, you can use commands such as cp to copy files to it. When disk slices are unmounted, only a few programs (such as backup programs) can access the data on the slice. The choice of directory names is arbitrary.

The mount Command

The mount command is used to make resources available to the operating system. It takes the given mount point for a resource and inserts it into the directory structure. The command format is:

mount [-F fstype] [-o options] [server:pathname] mount-point

For example:

```
# mount /dev/dsk/c0t3d0s5 /statistics
```

In the above example, **c0t3d0s5** is mounted as the /statistics directory.

```
# mount -F nfs -o rw,bg,soft comms1:/h/data/global
```

In this example, the /h/data/global directory from labserver is mounted as the /h/data/global directory on the local machine with read/write options. The "bg" and "soft" options are normally used with network mounts. These specify to retry the mount in the background if it fails on the first attempt. They also specify to go on without the directory if it times out. In order for a resource to be mounted, the directory that will act as the mount point must already exist. This directory can be created with the **mkdir** command. The following is an example of creating a directory for a resource before mounting it.

```
# mkdir /security2

# mount /dev/dsk/c0t1d0s4 /security2
```

While the file system can be mounted to any directory, it is best to mount only empty directories. When a file system is mounted to a nonempty directory, the files originally in that directory are unavailable until the file system is unmounted.

One other option available with the **mount** command is displaying all of the currently mounted resources. To display a list of mounted file systems, type **mount** and press **RETURN**. All the file systems currently mounted are displayed. This same information is also stored in the `/etc/mnttab` file. The following example shows the output of the **mount** command.

```
#mount
/ on /dev/dsk/c0t3d0s0 read/write on Sun Feb 13 14:52:09 1994
  /usr on /dev/dsk/c0t3d0s6 read/write on Sun Feb 13 14:52:09 1994
/proc on /proc read/write on Sun Feb 13 14:52:09 1994
#
```

The mountall Command

Normally, all of the important file systems are mounted at boot time through entries in the `/etc/vfstab` file. The **mountall** or **mount -a** command allows you to perform this operation at any time. This command will mount all resources from the virtual file system tables that are normally mounted at boot time.

The command format follows:

```
mountall [ -r ] [ -l ] [ -F nfs ]
```

The options for this command are defined as follows:

-r	Limits mounting to networked file resources.
-l	Limits mounting to the local file systems.
-F fstype	Limits mounting to a specific file system type.

In the following example, all remote file systems are mounted.

```
# mountall -r
```

The **umount** command is used to unmount a resource that is currently mounted. This resource will be removed from the directory structure, and it will no longer be available. One critical point to remember with **umount** is that it will not unmount resources that are currently in use. The command format follows:

umount *mount-point*

For example:

```
# umount /statistics
```

The **umountall** command unmounts all currently mounted file systems that are not in use. The command format follows:

umountall [**-r**] [**-l**] [**-F** *nfs*]

The options for this command are defined as follows:

-r	Limits mounting to networked file resources.
-l	Limits mounting to the local file systems.
-F <i>fstype</i>	Limits mounting to a specific file system type.

In the following example, all remote file systems are unmounted.

```
# umountall -r
```

Volume Manager

The Volume Manager is used to mount removable devices (CDs and floppy disks). The Volume Manager automatically detects CD-ROMs and the **volcheck** command checks for floppy

disks. It automates the interaction between you and your removable devices by creating a symbolic name for floppies and CD-ROMs.

The `/etc/vold.conf` file is read during the boot process to start the Volume Manager. It automatically mounts CDs when they are inserted into the CD-ROM drive. The CD-ROM is mounted as `/cdrom/cdrom_name`.

When a floppy disk is inserted into the floppy drive, the user must execute the **volcheck** command in order to access the floppy disk. The **volcheck** command checks drive for installed media. It then mounts the floppy disk to `/floppy/floppy_name`.

Virtual File System Table file

One of the problems with mounting file systems is that all mounts are lost when the machine is turned off. When the machine is booted again later, all of the mounts have to be created again. To accomplish this task, UNIX uses the virtual file system table. This table is kept in the `/etc/vfstab` file. When the computer boots, each entry is read from this table and used to mount a file system.

Virtual File System Table Entries

Each **vfstab** entry is composed of seven fields. These fields are used to specify the resource, mount point, and mount options. The fields are:

Field	Description
device to mount	Specifies the resource that will be mounted.
device to fsck	Specifies the resource for file system checks. This field is only used for local hard drives and contains the "raw" hard drive device pointer.
mount point	Specifies the mount point. This is where the resource will appear in the directory structure.
FS type	Specifies the file system type.

fsck pass	Specifies the order that hard drive partitions will be checked for file system checks at boot time. All entries will be a number between 1 and 9. This field is only used for hard drive entries and will have a corresponding entry in the "device to fsck" field.
mount at boot	Specifies whether or not the resource will be mounted at boot time. All entries will either be <i>"yes"</i> or <i>"no"</i> .
mount options	Specifies the mount options for the resource. The options are explained above with the mount command.

The following example shows entries for two hard drive mount points. In the example, slice 5 on drive 3 is mounted as /filesl. Slice 7 on drive 3 is mounted as /h.

# device	device	mount	FS	fsck	mount	mount
# to mount	to fsck	point	type	pass	at boot	options
/dev/dsk/c0t3d0s5	/dev/rdsk/c0t3d0s5	/h/data/global	ufs	2	yes	-
/dev/dsk/c0t3d0s7	/dev/rdsk/c0t3d0s7	/h	ufs	3	yes	-

The following example shows entries for two-networked mount points. In the example, the /h/data/global directory from labserver is mounted on the local machine with /h/data/global as its mount point. The /usr/data directory from labserver is mounted on the local machine with /data as its mount point. It also uses the background mount options.

# device	device	mount	FS	fsck	mount	mount
# to mount	to fsck	point	type	pass	at boot	options
#						
labserver:/h/data/global	-	/h/data/global	nfs	-	yes	-
labserver:/h/USERS/global	-	/h/USERS/global	nfs	-	yes	bg,soft

When creating vfstab entries, the user must fill in all of the fields. If the field is not saved, it must have a '-' as the entry in that field. It acts as a place holder. The user will also have to specify whether or not the resource should be mounted at boot time.

Creating Permanent Mount Entries with the vfstab file

In order to create a permanent mount point on a file system, there are several things that must be done. Several of these things have already been pointed out in the chapter. The steps are listed in the following section.

1. Become superuser.
2. Edit the /etc/vfstab file with a text editor. Add the entry for the resource and separate each field with spaces or a Tab. If a field does not have an entry, enter a hyphen.
3. Save the changes and exit from the editor.
4. Create the directory for the mount point if it does not already exist. This is done with the **mkdir** command.
5. Type **mount <mount-point>**, and press **RETURN**. The entry is mounted.

Networked File Systems

A network file system is one that can be located and accessed over the network. Before resources can be mounted over the network, they must be shared by the server where they are located.

Sharing is the process of making resources available over the network so that they can be mounted by remote machines. Before network mounting can occur, the following conditions must be met.

1. The machines must know each other's names and IP addresses. This information is stored in the /etc/hosts file and is normally configured or via DNS.
2. The server must share the resource to be mounted.
3. The remote machine must mount the resource.

NOTE: Setting up a network share is detailed in the Installation Procedures and in both SAM documents.

Required NFS Daemons

In order for network mounting to occur, certain daemons must be running on the computer systems.

1. **Server Daemons.** In order for a machine to share resources over the network, it must be running the /usr/lib/nfs/mountd and /usr/lib/nfs/lnfsd daemons. These daemons receive mount requests from other machines over the network and return the file handles for accessing the shared resources. Any machine that shares a resource over the network becomes an NFS server.
2. **Client Daemons.** In order for a machine to mount networked resources, it must be running the /usr/lib/lnfs/lockd and /usr/lib/nfs/statd daemons. These daemons provide locking services and crash/recovery functions.

A user can determine if these daemons are running with the command "ps -ef | grep nfs". These daemons will appear in the output of the ps command if they are running.

Sharing File Systems

The share command allows users to share resources over the network. The share command will share and unshare resources, as well as display what is currently shared. In addition, resource sharing can be made permanent at boot time. This is done with the /etc/dfs/dfstab.

The **share** command makes file resources available for mounting by remote systems. The command format is:

share [option(s)] pathname

The options for this command are:

- F nfs** Specifies the "nfs" file system (the default file system for networking).
- O options** Specifies the share options. Some of these are:
 - rw - Read/write (default share option).
 - ro - Read only.

In the example, the /usr/data directory is shared with read/write access. It is only shared with the machines lab1, lab2, and lab3.

```
# share -F nfs -o rw=lab1:lab2:lab3 /usr/data
```

The **unshare** command makes file resources unavailable for mounting by remote systems. The command format follows:

```
# unshare [ -F nfs ] pathname
```

The options for this command are defined as follows:

-F nfs	Specifies nfs as the file system type.
pathname	Specifies the pathname of the file resource to be unshared.

The following example makes the /statistics file system unavailable for sharing:

```
# unshare /statistics
```

Normally, all of the resources to be shared at boot time are stored in the /etc/dfs/dfstab file. The **shareall** command allows users to share all of these resources at any time. The command format is:

```
shareall [ -F nfs ]
```

The **unshareall** command is used to unshare all of the resources that are currently being shared with the network. The command format is:

```
unshareall [ -F nfs ]
```

The **dfshares** command allows you to display the resources that are currently being shared over the network. The command format is:

```
dfshares [server]
```

When the **dfshares** command is entered by itself, it will display the resources that the machine is sharing with the network. The following is an example of the output of this command.

# dfshares				
RESOURCE		SERVER	ACCESS	TRANSPORT
labl:/statistics	labl	-	-	
labl:/usr/data	labl	-	-	

When the **dfshares** command is entered with the name of another machine, it will display the resources that the specified machine is sharing with other machines. The following example shows the output of this option.

# dfshares labserver				
RESOURCE		SERVER	ACCESS	TRANSPORT
labserver:/h/data/global	amc	-	-	
labserver://h/USERS/global	amc	-	-	

Distributed File System Table

The distributed file sharing table is used to share resources permanently over the network. This table is setup when the computer boots and stays active at all times. The sharing table is kept in the /etc/dfs/dfstab file. The dfstab file stores the **share** commands for resources that are to be shared at boot time. This file is also used when the **shareall** command is entered. The following is an example of the file.

When a system does not have any resources shared, the NFS server daemons will not be running on that system. In order for those daemons to be running, there must be *share* entries in the dfstab when the computer boots. To invoke sharing on a system do the following:

```
# cat /etc/dfs/dfstab
# place share(1M) commands here for automatic execution
```

```
# on entering init state 3.
# share [-F fstype] [-o option] [-d "<text>"] <pathname> [resource]
    e.g.,
    share -F nfs -o rw=engineering -d "home dirs" /export/home
share -F nfs -o ro /usr/data
share -F nfs -o rw=lab1:lab2:lab3 /h/data/global
```

Setting Up the NFS Server

1. Add an entry to the /etc/dfs/dfstab file with a text editor. This entry will be a **share** command.
2. Start the NFS server daemons with the command **"`/etc/init.d/nfs.server start`"**.

The **dfshares** command can be used to verify that the resource has been shared. The entry added to the dfstab will be permanently shared over the network, and sharing will automatically start when the computer is booted.

GCCS-M NFS

GCCS-M has two NFS mount points: /h/USERS/global and /h/data/global/UCP. Both are set up during the installation process. The /h/USERS/global is used to populate accounts and profiles in both Windows and UNIX domains and the /h/data/global/UCP mount point allows global access to communication functions.

THIS PAGE INTENTIONALLY LEFT BLANK

INFORMATION SHEET 2-3-3

FILE SYSTEM ADMINISTRATION WITH THE DISK MANAGER TOOL

A. Introduction

This lesson will provide the trainee a basic understanding of mounting and sharing file systems and devices.

B. References

Embedded Online Documentation

C. Information

The Disk Manager Tool

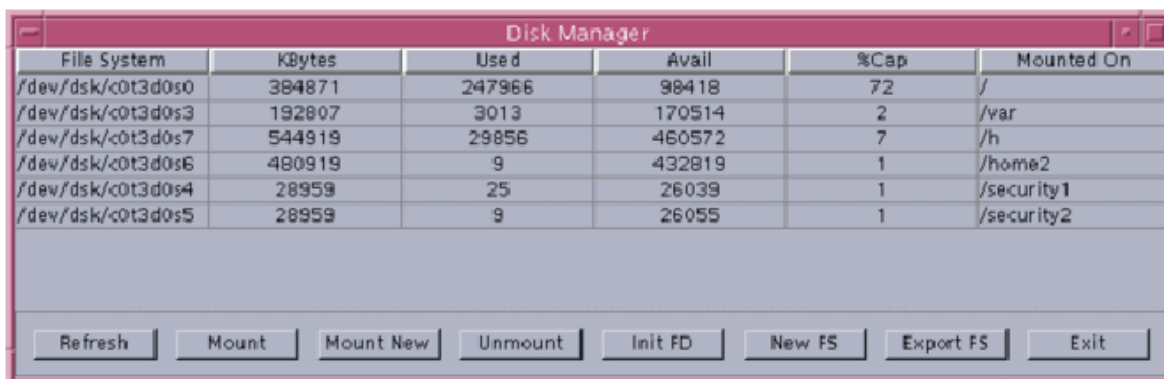
The Disk Manager tool is used to mount and export files, format drives, display disk space availability and initialize disks. From this tool a user can define file systems to be used for specified purposes, such as a designated temp directory or if other systems need to access information from the network.

Most file system operations are performed using the Disk Manager tool.

- Log in as **SysAdmin** and access DII Apps the System Administration utilities.
- Double-click the **Disk Manager** icon. The Disk Manager window appears.

NOTE: When Disk Manager errors occur, they are written to the log file

/h/COE/date/local/SysAdm.log. If no errors have occurred, the file will not be present.



The Disk Manager window contains the following buttons:

Refresh

Updates file system entries in the window.

Mount

Attaches an existing file system in the window to a directory, making the files available to the user.

Mount New

Identifies a new file system and attaches it to a directory, making that directory structure available to the user. Once mounted, the file system appears in the window.

Unmount

Detaches a file system in the window from a directory. When a file system is unmounted, the files become unavailable to the user, yet they remain intact. A file system that someone is accessing cannot be unmounted.

Init FD

Formats a diskette. This option erases the entire contents of the diskette.

New FS

Reformats a selected device to create a new file system. All data on the selected device is deleted.

Export FS

Exports or unexports a file system to allow or deny file system sharing.

Exit

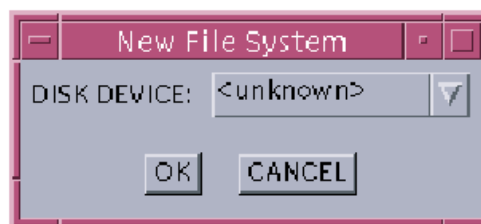
Closes the window.

Create a New File System

Creating a new file system formats the disk and erases all data on the disk. Exercise caution before performing this operation.

WARNING: All data on the selected device will be deleted. No partitions are protected from New FS. Therefore, you should back up any data you want to save before beginning the New FS procedure.

- Click **New FS** button at bottom of Disk Manager window. The New File System window appears.

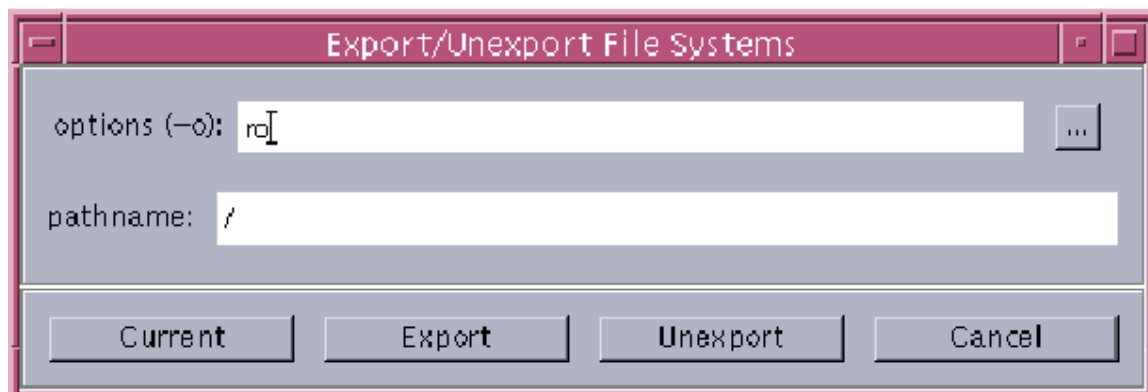


- To select the disk device to reformat, click the **arrow** next to the **DISK DEVICE** field and select **disk device** from the list.
- Click **OK** to reformat the selected device. Otherwise, click **CANCEL** to prevent creating a new file system.

Export a File System

When a file system is to be exported, those computers listed in the local host table or Domain Name Server (DNS) table, to mount the file system.

- Highlight a file from the Disk Manager window list.
- Click **Export FS** button at bottom of Disk Manager window. The Export/Unexport File Systems window appears.



The Export/Unexport File Systems window contains the following buttons.

Current

Views the file systems that are currently exported (shared).

Export

Exports (shares) a selected file system.

Unexport

Unexports (denies file system sharing to) a selected file system.

Cancel

Closes the window.

- To view a list of file system export options, right-click the **ellipsis (...)** button following the **options** field and select an **option** from the list (for example: **read only**, **read/write**). The file system options appear in the options field.
- In the pathname field, type the **pathname** of the directory to share.
- Click **Export** to export the file system. A window appears, prompting to permanently export the file system.



- Click **Yes** to export the file system permanently. Otherwise, click **No** to leave the file system exported until the next system reboot.

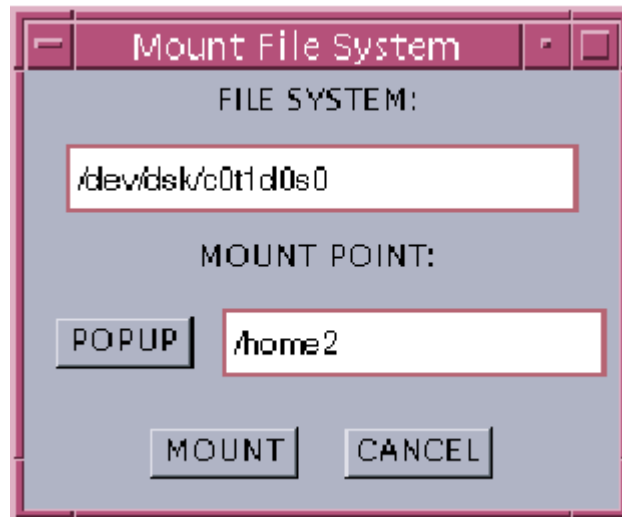
To confirm that the file system was exported, perform the steps below.

- On the Disk Manager window, click **Export FS**. The Export/Unexport File Systems window reappears.
- Click **Current**. The shared directory appears in the list of exported file systems.

Identify a New File System

A new file system must be defined in order to add a new disk to the computer. Then it can be mounted. Follow the procedures below to identify a new file system. Log in as the **System Administrator** and access the System Administration applications.

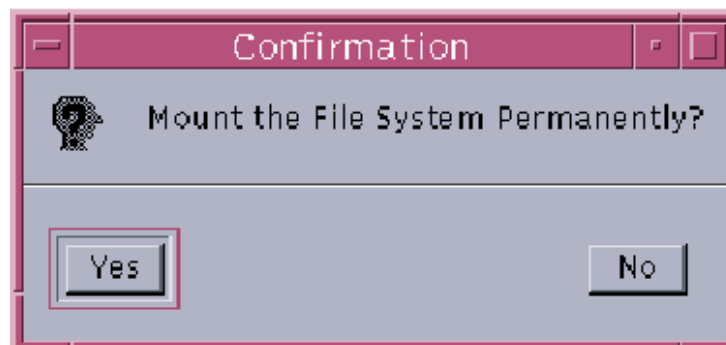
- Click **Mount New** button at bottom of Disk Manager window. The Mount File System window appears.



- In the **FILE SYSTEM** field, enter the new file system name.
- In the **MOUNT POINT** field, enter a mount point to select an unused location to mount the file system using one of the following methods:
 - Enter the location in the **MOUNT POINT** field.
 - Click **POPUP** to open the Choose Mount window. Click a **mount point** in the list and click **OK**. The Mount File System window reappears with the new mount point in the **MOUNT POINT** field.



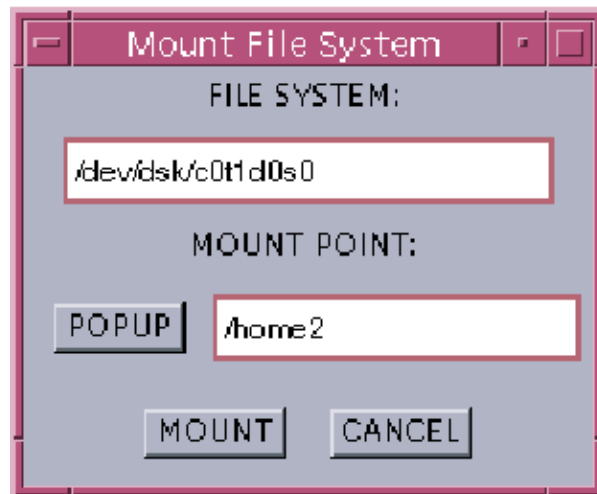
- On the Mount File System window, click **MOUNT**. A window appears prompting if you want to permanently mount the file system. Otherwise, click **CANCEL** to not mount the file system.



- To mount the file system each time the computer is rebooted, click **Yes**. Otherwise, click **No** to mount the file system only once, without remounting it upon reboot.

Mount a File System

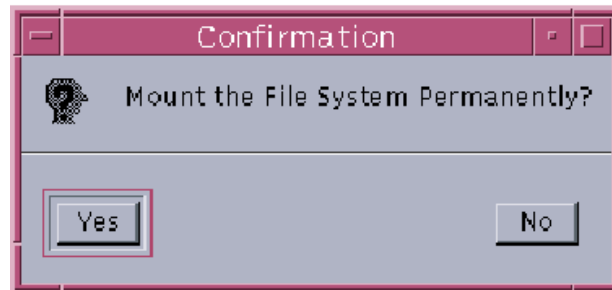
- From the Disk Manager window, select a **file system** to mount. [You must attach a file system to the *Solaris* Operating Environment directory tree at a mount point. A mount point is a directory that is the point of connection for a file system. Use the mounting process to attach individual file systems to their mount points on the directory tree].
- Click the **Mount** button. The Mount File System window appears.



- To select an unused location as a mount point for the file system, enter a mount point in the **MOUNT POINT** field using one of the following methods:
- Type the location in the **MOUNT POINT** field.
- Click **POPUP** to open the Choose Mount window.
- Click a **mount point** in the list and click **OK**. The Mount File System window reappears with the new mount point in the **MOUNT POINT** field.



- On the Mount File System window, click **MOUNT**. A window appears prompting if you want to permanently mount the file system. Otherwise, click **CANCEL** to not mount the file system.

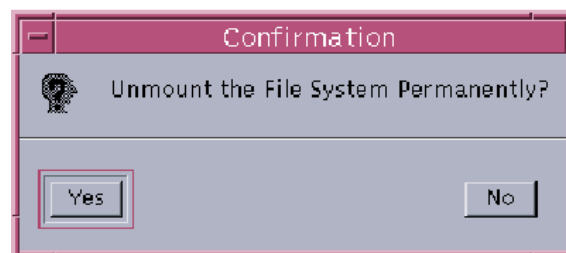


- To mount the file system each time the computer is rebooted, click **Yes**. Otherwise, click **No** to mount the file system only once, without remounting it upon reboot.

Unmount a File System

NOTE: A file system that is in use by an application or user cannot be unmounted.

- From the Disk Manager window, select a file system to unmount. A window appears, prompting if you want to permanently unmount the file system.



- To permanently unmount the file system, click **Yes**. Otherwise, click **No** to unmount the file system only until the computer is rebooted.

NOTE: Once CIFS is configured and /h/USERS/local is mounting, in order to install any segment on a Solaris machine the /h/USERS/local must be temporarily unmounted during installation.

INFORMATION SHEET 2-3-4 MAINTAINING FILE SYSTEMS

A. Introduction

This lesson will provide the trainee a basic understanding of maintaining file systems

B. References

Online Embedded Documentation

C. Information

The commands in this section are designed to assist in management of file system space.

1. Tar command. Backing up and restoring files (**tar**)

- a. **tar** is used to back up and restore files saved to a media device.
- b. **tar** is also used to list the contents of a media device.
- c. File arguments used with **tar**:
 - (1). **c** - creates a backup
 - (2). **t** - lists the contents of the backup media.
 - (3). **f** - specifies a device to backup to or restore from
 - (4). **x** - restores files from the backup media
 - (5). **v** - displays the name of each file
- d. Backing up files.
 - (1). To back up, type **tar cvf device filename**.
 - (2). **filename** is the name of the file to be backed up.
 - (3). If not working in the directory where the file resides, must include the full pathname for the file.
 - (4). To list the contents of a media:
 1. Type **tar tvf device**.
 2. **device** is the name of the device where the media was placed.

- e. To restore a file from the backup media:
 - (1). Login to the computer desired for copying to.
 - (2). Access the directory to copy the file to.
 - (3). Type **tar xvf *device filename***.
 - (4). ***device*** is the name of the device where the media was placed.
 - (5). ***filename*** is the name of the file to restore.
2. The disk usage (**du**) command is used to display the number of 512-byte blocks used per file or directory to include it's subdirectories in the block count, (default is current directory).

The command format is as follows:

du [options] [directoty ...]

The options for this command are:

- s** Silent mode, displays only grand totals.
- k** Display output in kilobytes
- o** Subdirectories not included in total size
- d** Stay within current partition
- a** Display usage for all files, just not subdirectories.

For example:

```
$ cd /h/USERS/global/ftstudent01
$ du -sk
2062    /h/USERS/global/ftstudent01
```

In the example above, the **du** command uses the '**s**' option to generate a summary of the output and the '**k**' for output in kilobytes for the directory /h/USERS/global/ftstudent01. Student01 is using 2062 kilobytes of disc space in *that* directory. Student01 could be using disk space in other location.

3. The disk free (**df**) command may display file system names followed by such parameters as the available free disk space, used disk space, percentage of capacity used and mount points. There are many options that display information in different formats.

The command format follows:

df [options] [argument]

The options for this command are:

- g** Displays total 512-byte blocks and files allocated, used, and free, as well as the type of file system, file system ID, file name length, block size, and fragment size.
- k** Displays the used kilobytes, free kilobytes, and the percent of capacity used. (typically not used with other options)
- F** Report on an unmounted file system specified by type, i.e. tmpfs. Available types may be found in the letclvstab file.
- l** Reports only on local file systems (ufs).

Example:

\$ cd /					
\$ df -k					
Filesystem	Kbytes	Used	Avail Cap		Mount on
/dev/dsk/c0t0d0s0	384847	115489	230878	34%	/
/dev/dsk/c0t0d0s3	96455	1196	85619	2%	/security1
/dev/dsk/c0t0d0s4	96455	112	86703	1%	/security2
/dev/dsk/c0t0d0s5	180495	145979	16476	4%	/var
/dev/dsk/c0t0d0s7	769694	461956	302738	68%	/h

NOTE: Approximately 10% of the disk capacity is reserved for file system proficiency. It is not reflected in the `df -k` output.

In the example below, only one file system type is viewed.

\$ df -F tmpfs

/tmp	(swap):	64800 blocks	3029 files
-------------	--------------	-----------	---------------------	-------------------

Knowing how to correctly display disk information, such as disk usage and location of file systems, is very important to a system administrator.

4. Maintaining orderly and clean file system structures increase performance and reduce wasted space on the storage devices. Proper archiving, moving and/or deleting of files (especially large ones) may increase the system proficiency and defer costly hardware upgrades.

The **find** command is a very useful command for locating files. This command is both powerful and recursive by design. The find command searches for specific files by using different options searching for certain parameters (i.e. search for all files owned by a user). It is designed to start at a given directory and search thoroughly down the hierarchy (i.e. start at root and search every subdirectory and file under root).

The command format follows:

find [pathname] [-options] [arguments] [output]

Here are some search options used to specify what file parameter to find;

-time (+/-)days Finds files that were last accessed by a day parameter.

NOTE: The **find** command will change the access time of directories supplied under the pathnames parameter.

-time (+/-)days	Find files that were last modified by a day parameter.
-group group	Find files belonging to a group, specified by name or GID.
-perm ###	Find files by absolute permission parameters.
-name filename	Find files by specific name.
-inum #	Find files by inode number.
-user username	Find files belonging to a user, specified by name or UID.

The options that utilize (+/-) specify exactly, more or less than a particular number. Example, **+d** (more than # days ago), **d** (exactly # days ago), and **-d** (fewer than # days ago).

The following are output options that can be used with **find**. These specify what to do with the results of the search.

- ok command {};** Runs UNIX commands after a file is found, verifying the action with the user.
- exec command {} \;** Runs UNIX command after a file is found.

A good example of using the **find** command for maintaining file systems is the following: When a workstation has been improperly shutdown the operating systems sends all unsaved information from virtual memory to a file for protection against inadvertent loss. These core files may be large, unwanted and in an unknown location. To find starting at the /(root) directory core files and remove them -interactively, do the following:

```
# find / -name core -exec rm -i {} \;
```

Another good example of the **find** command for maintaining file systems: A user account is no longer required and has been deleted. To ensure complete closure on the account, use the following to **find** from / all files owned by that specific -user and remove them -interactively. (see example below).

```
# find / -user gregory -exec rm -i {} \;
```

To find and interactively remove unwanted empty files do the following:

```
# find / -size 0 -ok rm {} \;
```

To find files belonging to a particular user with a given set of permissions do the following:

NOTE: In this example the results will be every file with "wide open" permissions for the user hacker.

```
# find / -user hacker -perm 777
```

```
# find / -user root -perm -700
```

In the second example above, every file owned by root that has **other than** read, write, execute permissions for the owner will be listed (note the **-700**). **ALSO NOTE;** the find command's results will contain the absolute paths for **all types** of files (regular files, link files, directory files and device/special files)

5. The **quot** command displays the number of kilobytes on the hard drive slice that each user is occupying. This command is often used to find out who is using the largest amounts of disk space.

NOTE: **quot** is a very limited command because it can only be used on local file system mount points. Look at the `/etc/vfstab` file for a list of all local file systems mount points on a system.

The command format follows:

quot [options] file system mountpoint

The options for this command are:

- a** Report on all mounted file systems.
- f** Show the number of files as well as the number of Kbytes owned by the user.

For example: The `/(root)` file system is mounted to `/dev/dsk/c0t0d0s0`.

# quot -f /		
/dev/dsk/c0t0d0s0(st) :		
69984	2451	root
44237	1843	bin
9824	105	adm
147	87	lp
79	19	sys

Files to Monitor

A notable feature of Unix is the way that it keeps logs of almost all system operations. As part of normal system operation, some of these log files can grow quite large. It is important to monitor these files so they do not use too much of the system disk space.

NOTE: If left unchecked these logs may get so large that they interrupt normal system operation. The following is a list of some of these files.

FILE	USE
/var/adm/lastlog	History of last logins
/var/adm/messages	Messages from syslogd
/var/adm/pacct	Per process accounting information
/var/adm/sa/*	System accounting files
/var/adm/sulog	History of su commands
/var/adm/utmp	History of user logins
/var/adm/wtmp	History of system logins
/var/cron/log	History of actions of /usr/sbin/cron

File System Corruption

File systems keep track of files by issuing them a number, called an index-node (inode). The inode numbers make up a table of contents for locating files. Directories simply list the correlation between file names and inode numbers. Each partition has its own set of inode numbers, thus the need for symbolic links versus hard. A slice's inode data is stored in a list

called the inode-list (ilist). The ilist for a slice resides in the superblock. Superblocks contain the instructions and information for controlling the movement and storage of a partition's data.

Inconsistencies in the superblock's synchronization with the data on a disk could result in file system corruption. File systems can be damaged or become unusable because of abrupt termination of the operating system in these ways:

1. Power failure
2. Accidental unplugging of the system
3. Turning the system off without the proper shutdown procedure
4. A software error in the kernel

File system corruption, though serious, is common. When a system is booted, a file system consistency check is done automatically. Most of the time, the file system check (**fsck**) repairs minor problems it encounters. But many times the file system check command (**fsck**) must be run manually. Usually **fsck** will run after receiving a command line warning message during the boot process.

The **fsck** command is used to perform file systems checks to correct problems on the hard drive. This program will repair various problems that can occur in the file systems, superblocks, Inode list, and data blocks.

The **fsck** command should **NEVER** be run on a busy file system. Due to how the script functions, the **fsck** command would report errors and possibly delete files as users were trying to read and/or write their data. Run the **fsck** command in single-user mode or on unmounted file systems only.

The **syntax** for the **fsck** command is:

fsck [option(s)] [device..]

The options for this command are:

- F fstype:** Specify the file system type on which to operate.
- y -Y** Assume a yes response to all questions.
- n -N** Assume a no response to all questions.
- m** Check, but do not repair
- o specific-options** The specific-options can be used in any combination, separated by commas with no spaces. One of the most used options is the *b=#*. Use this option where the # is the superblock number. Block 32 is always one of the alternates.

To determine the location of alternate superblocks, use the **newfs** command with the -N option.

WARNING: Make sure you include the -N or a new file system will be created and destroy all data! For more information and options see the manual pages.

The following table describes some of these important file system structures:

Cylinder Groups	To improve performance, the UNIX operating system groups subsets of inodes and data blocks together into groups of consecutive cylinders called <i>cylinder groups</i> .
Cylinder Group Blocks	The <i>cylinder group block</i> describes the number of used inodes/ blocks and free inodes/blocks. Plus the inode/directory map.
Superblock	The <i>superblock</i> contains information about the entire file system such as the number of blocks and cylinder groups, hardware parameters, and the mount point name. Because the superblock contains critical data, it is replicated in each cylinder group to protect against catastrophic loss.

The state flag specified in the superblock of the file system is checked to see whether the file system is clean or requires checking. If it is omitted, all the local file systems listed in /etc/vfstab with a fsck pass value greater than 0 are checked.

In the example below, the first file system needs checking; the second file system does not:

```
# fsck -m /dev/rdisk/c0t0d0s6
** /dev/rdisk/c0t0d0s6
ufs fsck: sanity check: /dev/rdisk/c0t0d0s6 needs checking
fsck -m /dev/rdisk/c0t0d0s7
/dev/rdisk/c0t0d0s7
ufs fsck: sanity check: /dev/rdisk/c0t0d0s7 okay
```

In the following example, /dev/rdisk/c0t0d0s5 is checked and the incorrect block count is corrected:

```
# fsck /dev/rdisk/c0t0d0s5
checkfilesystem: /dev/rdisk/c0t0d0s5
** Phase 1 - Check Block and Sizes
INCORRECT BLOCK COUNT I=2529 (6 should be 2)
CORRECT? Y
    Phase 2 - Check Pathnames
    Phase 3 - Check Connectivity
    Phase 4 - Check References Counts
    Phase 5 - Cylinder Groups
Dynamic 4.3 FFS
929 files, 8928 used, 2851 free (75 frags, 347 blocks, 0.6%
fragmentation)
/dev/rdisk/c0t0d0s5 FILE SYSTEM STATE SET TO OKAY

***** FILE SYSTEM WAS MODIFIED *****
```

When the **superblock** of a file system becomes damaged, it must be restored, fsck will normally inform the user when a **superblock** is bad. Fortunately, redundant copies of the **superblock** are stored within the file system.

To restore a bad **superblock**, do the following:

1. Become superuser.
2. Change to a directory outside the damaged file system.
3. Type **umount** <mount-point> and press **RETURN**.
4. Type **newfs -N /dev/rdisk/<device>** and press **RETURN**.

WARNING: Be sure to use the **-N** option with the **newfs** command. If you omit this option, you will create a new, empty file system (thus destroying all data on file system).

5. Type **fsck -o b=#** (# is alternate block) /dev/rdisk/<device> and press **RETURN**.

For example:

```
# cd /
# umount /var
# newfs -N /dev/rdisk/c0t0d0s5
/dev/rdisk/c0t0d0s5:      163944 sectors in 506 cylinders of 9 tracks,
36 sectors
83.9 MB in 32 cyl groups (16 c/g,      2.65MB/g, 1216 i/g)
super-block backups (for fsck -b #) at:
32, 5264, 10496, 15728, 20960, 26192, 31424, 36656, 41888, 47120, 52332, 57584, 62816,
  68048, 72143, 76563, 82976, 84132, 93440, 98672, 103904, 109316, 114368, 116754,
119600, 124832, 135296,
#fsck -o b=32 /dev/rdisk/c0t0d0s5
Alternate superblock location: 32.
/dev/rdisk/c0t0d0s5
** Last Mounted on
** Phase 1 - Check Block and Sizes
** Phase 2 - Check Pathnames
** Phase 3 - Check Connectivity
** Phase 4 - Check References Counts
** Phase 5 - Check Cyl groups
FREE BLK COUNT(S) WRONG IN SUPERBLK
```

SALVAGE ? y

36 files, 867 used, 75712 free (16 frags, 9462 blocks, 0.0%
fragmentation)

/dev/rdisk/c0t0d0s5 FILE SYSTEM STATE SET TO OKAY

***** FILE SYSTEM WAS MODIFIED *****

ASSIGNMENT SHEET 3-1-1

INSTALLATION OF GCCS-M SOFTWARE

A. Introduction

This assignment sheet is to be completed as homework.

B. Enabling Objectives

- 3.1 **IDENTIFY** the documentation to be used when performing install procedures.
- 3.2 **DISCUSS** the GCCS-M Installation process to include the Flash and segment installation.
- 3.3 **DEMONSTRATE** the use of the Segment Installer Tool to properly install segments.
- 3.4 **DISCUSS** the core software that is loaded during the flash with the use of an official Load Plan.
- 3.5 **PERFORM** a flash software load of the web server with the use of an official Load Plan and Installation Procedure.
- 3.6 **PERFORM** a flash software load of the communications servers with the use of an official Load Plan and Installation Procedure.
- 3.7 **PERFORM** a flash software load of the intelligence server with the use of an official Load Plan and Installation Procedure.
- 3.8 **CONFIGURE** the web server, communications servers, and intelligence server in accordance with the loan plan and installation procedures.
- 3.9 **PERFORM** the configurations steps for IFL, TMS and UCP with Installation Procedures.
- 3.10 **INSTALL** software segments on COMPOSE workstations with the use of an official Load Plan and Installation Procedure.

C. Study Assignment

Review Information Sheets 3-2-2 and 3-2-3

D. Study Questions

1. Which Documents are utilized during a standard flash load of GCCS-M?
2. Is the root password predefined by the flash or set by the installer?
3. What is the sa password?
4. What is the proper command for starting the flash from the boot prompt?
5. Which Compose machines will have the DII COE Kernel loaded?
6. What COMPOSE diagnostic tool is used to list installed programs?
 - a. Where is this command located?
7. What application is used to configure IFL?
8. In TMS, what are the different configuration types?
9. Can a Windows Machine be the TMS Master?

INFORMATION SHEET 3-1-2

INSTALLATION OF GCCS-M SOFTWARE

A. **Introduction**

This Information Sheet will provide the trainee with information needed during the installation of GCCS-M servers.

B. **References**

Online Embedded documentation

4.0.1.0 Consolidated Load Plan and Installation Procedures

C. **Information**

1. The GCCS installation documentation is broken down into two main documents. The Load plan is a spreadsheet that lists the order for installing software segments. There are several segments and procedures that must be done in particular order. The document is broken down into sections so that the installers complete the install in the proper order. The Installation Procedure documentation provides the installer with a step-by-step process for each line item found in the Load Plan.
 - a. Installation Procedures (IP)
 - (1). Detailed instructions designed to assist an installer and administrators are located in Installation Procedures (IP).
 - (2). Ensure that the latest procedures are followed in order to reduce the possibility of installing or configuring software or segments incorrectly.
 - b. Load Plans (LP)
 - (1). Some segments must be installed and/or configured before subsequent segments can be loaded, therefore a system administrator cannot load a full machine from start to finish, and then install the next machine.
 - (2). Each segment should be loaded or configured following a horizontal pattern across the row of the load plan. In conjunction with the Installation Procedures.

2. At this point, read sections one (1) through four (4) in the Installation Procedures document. Close adherence to this document is crucial to the successful load of the GCCS-M software.
3. Flash load for the communications server
 - a. When starting the flash, the installer will be installing a previously created Flash Image of the operating system, kernel, core ICSF, and Maritime application segments onto the system.
 - b. Certain machines will require a name change after this portion of the load.
 - c. It is imperative to enter the correct hostname and IP address at the specified prompts.
 - d. The comms server, also known as the UCP Master, is the machine to which most communications channels are connected.
 - e. Processes the communications data being received and transmitted over various channels. The comms server is often also used as the TMS/Track Master
 - f. UCP/TMS Master Server – the UCP and the TMS can be on the same machine or on separate servers: named –UCP Master (comms processor) and one named the Track Management Server (TMS) Master, with a backup TMS loaded on the UCP Master.
4. Flash load for the web server (websvr)
 - a. In addition to web services, this machine contains the documentation management infrastructure (DMI) segments and is the server for all system documentation.
 - b. The Flash load establishes a Solaris server with other GCCS-M related software allowing the administrator to follow the Installation Procedure and Load Plan from the Initial Configuration point forward.
5. Flash load for intelligence server
 - a. The intel server is the intelligence database storage machine. All imagery data is also stored and processed on this machine.
6. Server Configuration
 - a. Not all segments will be loaded on each server. Some segments that are loaded on the comms server might not be loaded on the intel server or the websvr.
 - b. The customized Load Plan will indicate which segments to install.

7. The COMPOSE Windows network

- a. COMPOSE is short for Common PC Operating System Environment. Depending on the configuration will install Windows 2000 Advanced Server on the Domain Controllers, Exchange server, and a File Server. All clients are configured as a Windows 2000 Professional. COMPOSE consists of modules that allow an unattended installation with minimum user interface. Compose is beyond the scope of this course and therefore will only be covered as an overview.

- **Server Baseline Configuration Module (BCM)** produces a Windows 2000 Advanced Server with a baseline server load.
- **Domain Configuration Module (DCM)** identifies each of the server roles and their functionality within a COMPOSE domain environment.
- **Core Services Installation Module (CISM)** finalizes the server role assignments and then performs the installations of the services and the applications on all servers and workstations to establish a fully functional Windows 2000 network.
- **Security Configuration Module (SCM)** used to apply local security to the servers and workstations in the newly created Windows 2000 network

NOTE: All servers must be installed and configured before installing and configuring any workstations and the COMPOSE installation guide must be strictly adhered to or the installation may have to be restarted.

- b. Core Services Installation Module (CSIM) Wizard is used to refine the list of software (also known as “roles”) to be installed on either a server or workstation. A server’s software list is based on the server’s functionality defined by the System Administrator during the DCM. The CSIM Wizard displays a default workstation software list as a base from which the System Administrator can customize the installations for various groups of workstations. Once the System Administrator has finalized server or workstation roles in the CSIM Wizard, the settings are saved and the CSIM automatically installs the appropriate software on the server or workstation. During the server software installation, the CSIM also disables server services on servers where they are not needed. Since the BCM installed all basic

server services (DNS, DHCP, WINS) on all servers by default, the CSIM must configure each server according to its DCM defined domain server functionality. If a server is assigned to function as a domain controller, Active Directory is installed and configured at the start of this server's software installation.

- c. After executing the CSIM to install COMPOSE software on all COMPOSE servers, the System Administrator should follow the "Post-CSIM Deploy to Server Steps" found in the "COMPOSE Manual Configurations Guide" to finalize the configuration for various servers. Once the server installation and configuration stage is complete, the System Administrator can begin installation of the workstations.

NOTE: The System Administrator should **NOT** change the administrator's default password on any server prior to the initial COMPOSE software installation and configuration on all servers. The installation of critical COMPOSE executables require the default administrator password setting.

- d. After the System Administrator has executed the CSIM on a workstation, the System Administrator should perform the manual configuration steps on all COMPOSE workstations. These steps should be performed after the System Administrator has executed the CSIM to deploy COMPOSE software on a workstation. The System Administrator should perform these steps as soon as possible after the workstation has received the COMPOSE software using the CSIM
- e. Compose includes several tools to help administer the Compose environment.
 - (1). COMPOSEINSTALLINFO.exe

DCI\E:\Compose\Client\bin: There is an executable program called ComposeInstallInfo.exe. This program will read the registry in real time of the selected machine and provide a list of installed applications. If there is an application such as Acrobat Reader that did not get installed on a client but shows as being installed in ComposeInstallInfo.exe the application can be tagged for reload by clicking on the Tag Application for Reload button within the ComposeInstallInfo.exe application. This action will remove the entry from the registry of the client and Compose will automatically reinstall it.

(2). COMPOSEDIAGNOSTICS.exe

Located on *DCI\E:\Compose\Client\bin*. This tool will gather important information about the Compose install and generate an email attachment as a .zip file. Before running this program, make sure there is an administrator account with email configured for the user. Enter the users email when prompted by ComposeDiagnostics. Once the program finishes the user can save the attachment and rename it as a zip file then browse through the Compose files generated by the program.

8. DII COE Kernel load on a COMPOSE domain controller

- a. After the COMPOSE domain is built and the webservr, intel, and comms servers have been configured up to the final configurations, the installer needs to load the DII COE Kernel on both COMPOSE domain controllers. During the installation of the kernel the system will prompt for an authentication key. The installer will **not** be prompted for a password for the keyman and secman accounts created during the installation of the server.
- b. For the classroom environment, the Compose servers have been preloaded with the appropriate Kernel for the GCCS-M load.

9. DII COE Kernel load on a COMPOSE Workstation

- a. The PC Baseload DVD allows installers to load a windows client from a flash just as the UNIX servers were loaded.
- b. The PC Baseload Load Plan and Installation Procedures will be referenced when building each Windows workstation.
- c. Since the Compose Servers are already preloaded the workstations can be loaded up to "Final Configurations" at any time during the UNIX server installation.

10. Segment Installer

- a. The Segment Installer is used to install, after the Kernel, most segments listed in the Load Plan. The standard installation is from a DVD, but other media devices including the network, CDs, DAT tapes, or floppy disks may be used.
- b. Use of the Segment installer is detailed in the Windows and Solaris SAMs.
- c. It is the responsibility of the trainee to be able to effectively use the segment installer on both Solaris and windows in order to successfully complete the install.

11. IFL / TMS / UCP Configuration

a. ICSF Foundation Libraries (IFL)

- (1). IFL provides an application called ICSFLanHosts that is intended for use by the ICSF administrator user account. To provide the ICSF administrator user access to ICSFLanHosts, the IFLSysAdmin feature must be active in the profile that the ICSF administrator uses. Once the IFLSysAdmin feature is active, the ICSFLanHosts application is available to the user from the icons found in DII_APPS/IFL. Refer to the IP or SAM for more information on the configuration of IFL.
- (2). ICSFLanHosts provides a means of configuring logical groups of hosts within the network. These groups of hosts segregate multiple TMS and UCP masters across the network, creating logical subnets of TMS/UCP master and client workstations. All machines that share the same /h/data/global directory will have access to this "network groups and hosts" definition

b. Track Management System (TMS)

- (1). TMS provides an application call TMS Config that is intended for use by the ICSF administrator. Access to the TMS feature is similar to the IFL feature. It is a best practice to have an account with all three configurations available. Use the TMS Workstation Config utility to set the track database management configuration on each workstation. Refer to the IP or SAM for more information on the configuration of TMS.
- (2). For track database management purposes, the local area network (LAN) can be configured as one or more "virtual" track management LANs. Each virtual track management LAN contains one "master" workstation, which can have gateway and client workstations.
 - **Master:** The master controls the track database and all track management processes. It must be a Unix workstation.
 - **Gateway:** A gateway allows other workstations (gateways and clients) to connect to it in order to receive track data, thus reducing the load on the server because it does not have to service as many workstations. A gateway can be a Unix or Windows workstation, given the following considerations:

- A Unix gateway can be connected to a Unix master or a Unix gateway.
 - A Windows gateway can be connected to a Unix master, a Unix gateway, or a Windows gateway.
 - A gateway's ICSF LAN Host setting must be the same as the ICSF LAN Host setting of the master workstation to which it is connected.
- **Client:** Each client receives its track data from the master, either directly or through a gateway. A client can be a Unix or Windows workstation, given the following considerations:
 - A Unix client can be connected to a Unix master or a Unix gateway, but cannot be connected to a Windows gateway.
 - A Windows client can be connected to a Unix master, a Unix gateway, or a Windows gateway.
 - A client's ICSF LAN Host setting must be the same as the ICSF LAN Host setting of the master workstation to which it is connected.
- (3). The following types of track management configurations are possible:
- One master, with all other workstations being either gateways or clients of that master.
 - Multiple masters, each of which has gateways and/or clients.
 - Multiple masters, some of which have gateways and/or clients and some of which are standalone masters.
 - All masters, where each workstation on the LAN is a standalone master.
- (4). The Master Host specified in the ICSF LAN Host Config utility must be the same as the Master Server specified in the TMS Config utility.
- (5). If a new Master is selected in the TMS Config utility, it is automatically changed in the ICSF LAN Host Config utility when TMS restarts.
- (6). If a new Master is selected in the ICSF LAN Host Config utility, it also must be manually selected in the TMS Config utility and the system must be restarted

The following figure illustrates a LAN containing 4 "virtual" track management LANs (V1, V2, V3, and V4), in various combinations as described above.

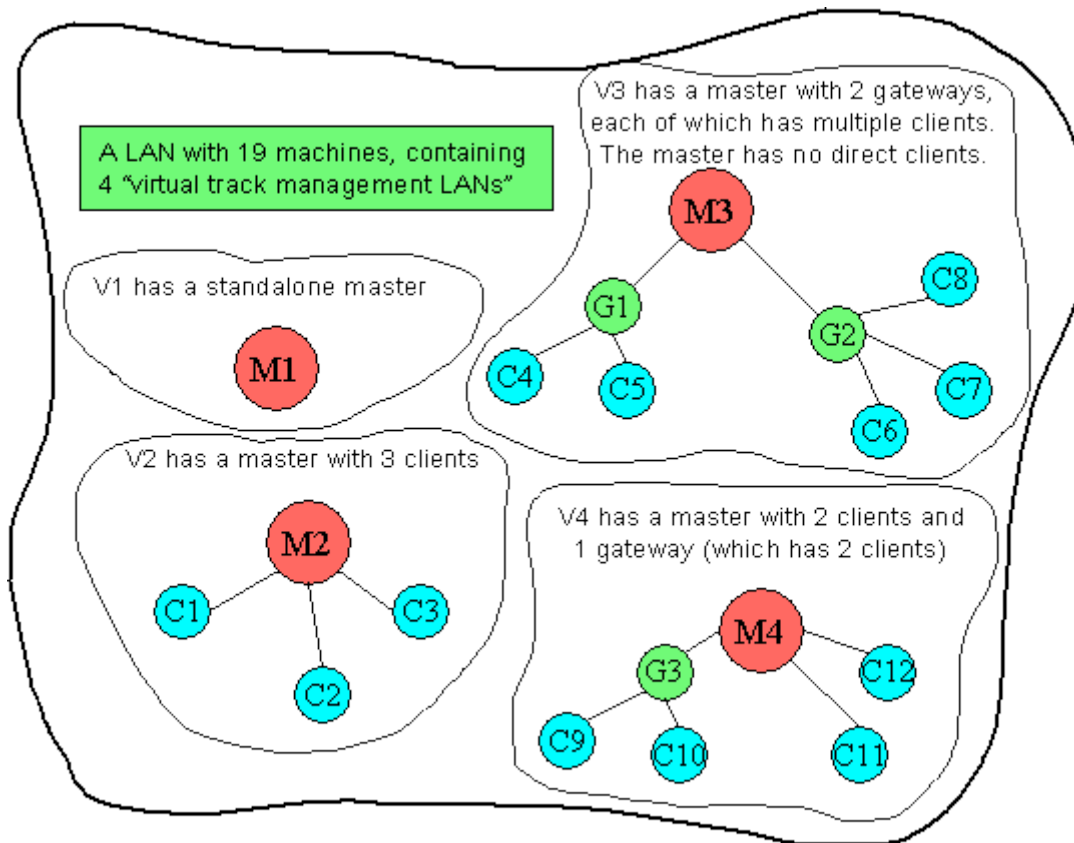


Figure 1-3-11

4. Universal Communication Processor (UCP)

- (1). UCP provides an application call UCP Workstation Config that is intended for use by the ICSF administrator. Access to the UCP feature is similar to the IFL and TMS feature. It is a best practice to have an account with all three configurations available. Use the UCP Workstation Config utility to set the UCP management configuration on each workstation. Refer to the IP or SAM for more information on the configuration of UCP.
- (2). During UCP configuration steps, one of the servers will be configured as the master and all other servers and clients will be "pointed" to it. When operators add, delete, stop, and start communication channels, the UCP is queried and provides data to update the local UCP record so that the UCP dialogue box displays the correct information.

ASSIGNMENT SHEET 3-2-1
ACCOUNT AND PROFILES MANAGER (APM)
AND
INTEGRATED C4I SYSTEM FOUNDATIONS (ICSF)

A. Introduction

This assignment sheet is to be completed as homework.

B. Enabling Objectives

- 3.11 **DESCRIBE** the Account and Profile Manager (APM).
- 3.12 **DISCUSS** the function of each component to the APM architecture.
- 3.13 **DISCUSS** the differences of each possible APM configuration.
- 3.14 **DEMONSTRATE** the ability to merge Windows 200 and Solaris machines into one APM Administrative Domain.
- 3.15 **DISCUSS** the differences between each type of account in APM.
- 3.16 **DEMONSTRATE** the ability to utilize domain and local accounts.
- 3.17 **TROUBLESHOOT** APM related problems with the use of current documentation.
- 3.18 **CONFIGURE** Network Information System Plus (NIS+) with the use of current documentation.
- 3.19 **CONFIGURE** the Common Internet File System (CIFS) with the use of current documentation.
- 3.20 **DEMONSTRATE** the use of APM to create user accounts with the use of current documentation.
- 3.21 **DESCRIBE** the segments integrated into the ICSF bundle.
- 3.22 **DISCUSS** the dependencies of each of the ICSF segments.

C. Study Assignment

Review Information Sheets 3-2-2 and 3-2-3

D. Study Questions

1. What is APM?
2. In what directory are the APM scripts located?
3. What is the CDS?
4. What tools are most often used in relation to APM?
5. What is NIS+? Is it configured before or after the APM merge process?
6. Does CIFS need to be configured before APM and NIS+?
7. What are the most common errors found with APM?
8. State the segments loaded with the ICSF bundle.
9. What type of track is only displayed on the individual workstation?

INFORMATION SHEET 3-2-2

ACCOUNT AND PROFILES MANAGER (APM)

A. **Introduction**

This information sheet is to be used by system administrators and installers in the understanding and troubleshooting of the GCCS-M APM tool. This lesson is not inclusive of all techniques used when working with APM, but can be used in addition to the SECAM and Systems Integrator's Guide.

B. **References**

Online Embedded documentation

4.0.1.0 Consolidated Load Plan and Installation Procedures

Current SECAM and SIG

C. **Information**

1. The APM system provides centralized account and profile management across a collection of UNIX and NT hosts called an *administrative domain*. Within the administrative domain, APM supports the ability for authorized users to create, delete, and maintain user accounts and groups, as well as define profiles that provide users easy access to the executables they need to perform their duties.
2. APM is a management tool provided by the COE Kernel that can be used in the creation and maintenance of user accounts, groups and profiles. APM also maintains a database of the segments installed on each computer that has the COE Kernel loaded on it. This is an important factor in determining a user's ability to access a specific segment's features.
3. APM provides system administrators with a tool to create and manage users and profiles in a heterogeneous computing environment. A heterogeneous environment is one that may include some or all of the following elements:
 - Computers using a UNIX OS (i.e. Sun Solaris)
 - Computers using a Windows OS (i.e. Windows 2000)
 - LAN configurations using W2K Active Directory (AD)
 - LAN configurations using NIS+

4. APM provides an *APM Client GUI*, which can be used to add/delete/modify users, groups, and profiles on COE machines. The *APM Client* connects to the APM Server over a *Transmission Control Protocol/Internet Protocol (TCP/IP)* socket. The APM Server carries out the requests, or *APM transactions*, and sends the status of the operations back to the client.
5. Any computer that is configured to “point” to the APM Master computer can be used to manage users and profiles. APM maintains a Central Data Store (CDS) or a database of each computer in the Administrative APM Domain. This database contains the segments loaded on the computer, the local and/or domain users, groups and profiles and a list of segment features.
6. The following are commonly used Administrative Tools that manage APM.
 - **APM_BecomeOwnMaster.pl** – this utility is used to reset APM back to its pre-merged status.
 - **APM_RegisterHost.pl** – this utility should be launched from a command prompt using the –g option in order to launch the application in a GUI.
 - **APM_EditConfig.pl** – this utility is used to point the client to the APM Master.
 - **APM_AuthMgr.pl** – this utility is used to set the Authentication Key. Authentication Keys must be set on the Master and client machines.
 - **APM_ReloadAPM.pl** - This utility reloads the information in the CDS files into the cached copy kept by the *Master APM Server*.
7. **Common Data Store (CDS) Architecture**
 - a. The CDS is split into *MasterHost*, *LocalHost*, *LocalHostPrivate*, and *User* areas. All areas of the CDS exist on all COE machines. Details on each part of the CDS can be found in the SIG. For general use, the *MasterHost* and *LocalHost* sections will be discussed.
 - b. APM data is stored in the CDS, a repository that provides cross platform user, account, group and profile information, as well as other Kernel information.
 - c. As segments, users, profiles and groups are added to the local computer each tree is updated. If the computer is its own APM Master then the Local Tree will match the Master Tree.

- d. The **/MasterHost** area of the CDS contains APM information for all hosts within the administrative domain. When the Kernel is first installed on a machine, the machine is an administrative domain that consists of one machine (only). The **/MasterHost** area of the CDS is maintained with the information that is relevant to the one host. When a Kernel machine is merged into an administrative domain, that machine's **/MasterHost** area of the CDS is no longer maintained. In an administrative domain, only the *Master APM Server* keeps its **/MasterHost** area of the CDS up to date.
- e. A **/LocalHost** area of the CDS contains machine-specific information (e.g., data on the users, groups, and profiles relevant to that machine). The **/LocalHost** area of the CDS is always maintained on every machine in the administrative domain.

8. APM Architecture

- a. APM is a three-tiered architecture that includes the *Master APM Server*, the *Local APM Server*, and the *APM Client*. All three APM components are present on all COE machines. The following subsections describe each of the components in APM. The figure below provides a graphical representation of the APM subsystem. Figure 3-2-1 shows a *Master APM Server* and a host in the administrative domain. In the figure, the host happens to be a PDC, but that fact has no bearing on the drawing.

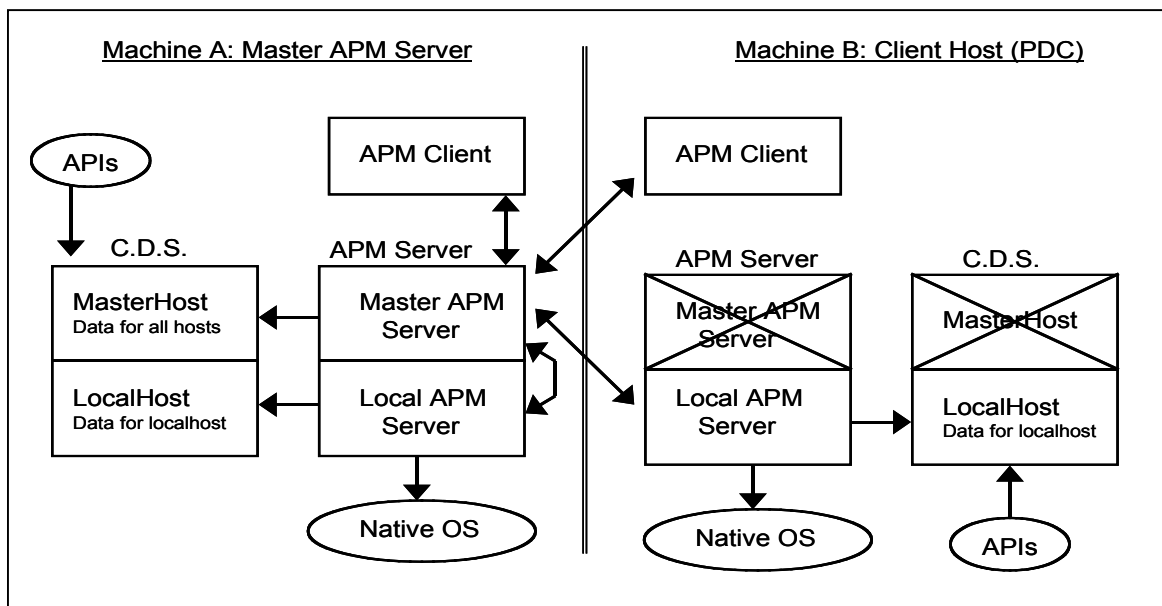


Figure 3-2-1

- b. The **Master APM Server** is present on all Kernel machines. When the Kernel is installed, the *Master APM Server* process is configured to administer only the one machine. In the *Merge Host* process, a machine transfers account and profile information and control to the *Master APM Server* on another machine. The *Master APM Server* is the process (and the machine) that the *APM Client* connects to when reading APM information and sending APM transaction requests. The *Master APM Server* is not involved in the user login process. Users can login and assume a profile even if the connection to the *Master APM Server* is down. The *Master APM Server* performs the following functions:

- Receives transaction requests from the *APM Client*.
- Distributes actions to the *Local APM Servers*.
- Collects status from the *Local APM Servers*.
- Returns the status of operations back to the *APM Client*.
- Maintains the */MasterHost* CDS area information for the administrative domain.
- The */MasterHost* area of the CDS includes information about the NIS+ and Windows domains and all of the hosts that are part of the administrative domain

NOTE: When a Kernel machine is merged into an administrative domain, that machine's */MasterHost* area of the CDS is no longer maintained. In an administrative domain, only the *Master APM Server* keeps its */MasterHost* area of the CDS up to date.

- c. The **Local APM Server** process is present on every COE machine. The *Local APM Server*:

- Receives transaction requests from the *Master APM Server*.
- Uses native operating system interfaces and functions to perform administrative operations, such as adding/deleting/modifying user accounts.
- Collects status information from operations and returns the status to the *Master APM Server*.
- Uses CDS APIs to update information in the */LocalHost* area of the CDS for the local users, groups, and profiles present on that machine.

- d. **APM Client** is a Java-based GUI installed on every 4.x Kernel machine. The APM Client:
 - Retrieves APM information from the Master APM Server and displays the information in GUI windows.
 - Receives user input to build account and profile management transactions.
 - Sends transactions to the Master APM Server for processing.
 - Receives status from operations in the administrative domain and displays the status to the user.
- e. APM Client can only be launched by:
 - Members of the admin group (present on all COE machines).
 - Members of the Administrators and Domain Administrators groups on Windows machines.
 - The “root” user on UNIX

9. **Configuring APM**

- a. The Edit APM Configuration tool is provided to configure the APM subsystem. The Edit APM Configuration tool is documented in the SECAM.
- b. The Edit APM Configuration GUI includes tabs for setting local configuration options, domain configuration options, and password configuration options. The domain and password configuration options only show up on the Master APM Server.
- c. A machine determines whether or not it is a Master APM Server by checking the “Master Host” field in the local configuration options tab. If the machine name is the same as the local hostname, the machine considers itself a Master APM Server.
- d. The password options control the operation of the COE Change Password Tool, and affect the settings in the native operating system. On a Solaris platform, the password configuration settings are in the /etc/default/passwd file. On a Windows platform, the configuration settings are in the Windows OS security accounts manager (SAM) database.

10. APM Authentication

APM authentication is the mechanism that restricts the management of accounts and profiles to authorized personnel. The 4.2 Kernel uses “Keys”, which are essentially re-useable passwords, to authenticate the individual using the *APM Client* and *COEInstaller* and to authenticate the *Master APM Server* to the *Local APM Servers*. Keys are the primary authentication mechanism in APM.

11. APM Authentication Key

- a. There are two keys used in the primary authentication mechanism of APM:
 - The *master APM authentication key*, which is the key that must be entered in the *APM Client* and the *COEInstaller*.
 - The *local authentication key*, which is used to authenticate the *Master APM Server* to the *Local APM Servers*.
- b. The Master APM keys are stored in the CDS as an encrypted value in the CDS under */MasterHost/DII Kernel/Keys/<hostname>*. The encryption mechanism is *Data Encryption Standard (DES)* and the master authentication key is used as the encryption key. (The master APM authentication key can only be decrypted and verified if a user supplies the correct key value.)
- c. The local authentication key is stored in two places:
 - An unencrypted numerical hash value is stored under */LocalHostPrivate/DII Kernel/Keys/<hostname>* on the machine to which the local authentication key belongs. The *Local APM Server* compares this value to the local authentication key that the *Master APM Server* sends with any transactions. Tight permissions are placed on the CDS file in order to protect the local key.
 - An encrypted value is stored with the master APM authentication key on the *Master APM Server* in the CDS under */MasterHost/DII Kernel/Keys/<hostname>*. This is the key that the *Master APM Server* decrypts (using the master APM authentication key as the decryption key) and sends to the *Local APM Server* with APM transactions.
- d. The authentication keys can be changed at any time, and should be changed immediately if they are compromised. Note that if the master APM authentication

key is reinitialized (i.e., a new one is picked), the local authentication keys for every machine in the administrative domain will have to be re-entered.

- e. If a machine is merged into another *Master APM Server*, the master APM authentication key on the machine being merged into the administrative domain is no longer used. In this case, the master APM authentication key for the new *Master APM Server* is the key that must be entered for tools that require an authentication key.
- f. When merging a machine into an administrative domain, the *Master APM Server* must first be informed of the local authentication key for the client host being merged. After setting the local authentication key to a known value on the client host, the new local authentication key must also be entered via the *Authentication Manager* on the *Master APM Server* so that the *Master APM Server* can use the host's local authentication key when sending the host APM transactions. The *SECAM* describes how to set authentication keys more in depth.

12. Network Information System Plus (NIS+)

- a. A Naming Service that allows creation of global accounts and groups in a UNIX domain. NIS+ allows the system administrator to create a UNIX domain and therefore create domain objects for the UNIX servers and clients that are in the AAD. If NIS+ is not implemented, then the system administrator is forced to use only local objects (i.e. profiles and accounts) for the UNIX environment.
- b. Establishes a NIS+ domain ending with .nis. (Example: nimitz.navy.mil.nis)
- c. Configures a NIS+ Master. The NIS+ Master and the APM Master do not need to be the same machine.
- d. If the APM Master is not acting as the NIS+ master then the APM Master must be configured as a NIS+ client.
- e. NIS + must be installed on all machines that will be part of the NIS+ domain.

13. Common Internet File System (CIFS)

- a. Samba, the commercially known term for CIFS, is an application that allows a UNIX file system to be browsed as a Windows share. This allows Windows 2000 clients to use UNIX resources such as files and printers.
- b. CIFS allows user accounts residing in the UNIX environment to access resources (i.e. shared directories and printers) in the W2K environment. This capability allows the system administrator to create a user that can log into either the UNIX environment or the W2K environment.
- c. Only installed on UNIX machines that will share files with Windows machines.
- d. It is independent of APM and NIS+ and does not have to be installed in any order.
- e. CIFS is a segment. After the segment is installed it must be properly configured using the CIFS appendix in the current Installation Procedure.
- f. CIFS daemons are smbd and nmbd.

14. Possible APM Configurations

- a. There are different configuration models that can be deployed and used in APM Administrative Domains (AAD). Each model depends on a specific hardware and software configuration and each model has its own advantages and disadvantages. Implementers and installers must weigh these advantages and disadvantages against the requirements of the site and the hardware and software configurations in use.
- b. **Non-merged APM Domain**
 - (1). In this configuration each computer acts as its own APM Master. Under this configuration, APM does not manage user accounts and profiles on a domain level and all accounts and profiles must be built and maintained on each local computer individually. Figure 1 is a graphical representation of a non-merged APM Domain. Each COE Client maintains its own Master and Local CDS Trees and there are no logical APM connections between the individual clients. Any change to the CDS is reflected in both CDS trees.

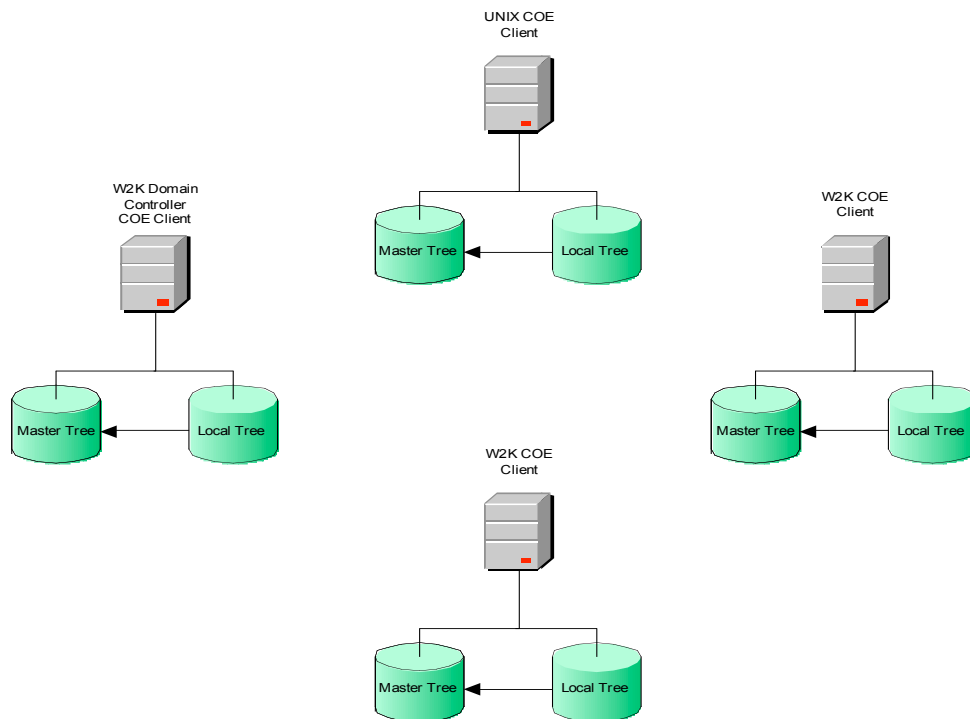


Figure 3-2-2 Non-Merged APM Domain

c. Administrative APM Domains (AAD) – **Fully Merged AAD**

- (1). A merged AAD allows the system administrator to manage both local and domain accounts, groups and profiles across both the UNIX and Windows operating systems from any AAD member.
- (2). The merge process requires that the system administrator change the APM configuration, pointing the client to a new APM Master Server. This task is completed through Edit APM Configuration.
- (3). In order to manage domain objects, a W2K domain controller or a NIS+ Master server must be merged into the AAD. The W2K domain controller must be merged into the AAD prior to any W2K workstations.
- (4). When a workstation is configured to use another computer as the APM Master server, then the workstation's Master CDS Tree is no longer maintained. All APM transactions and updates are applied to the CDS Master Tree of the APM Master Server

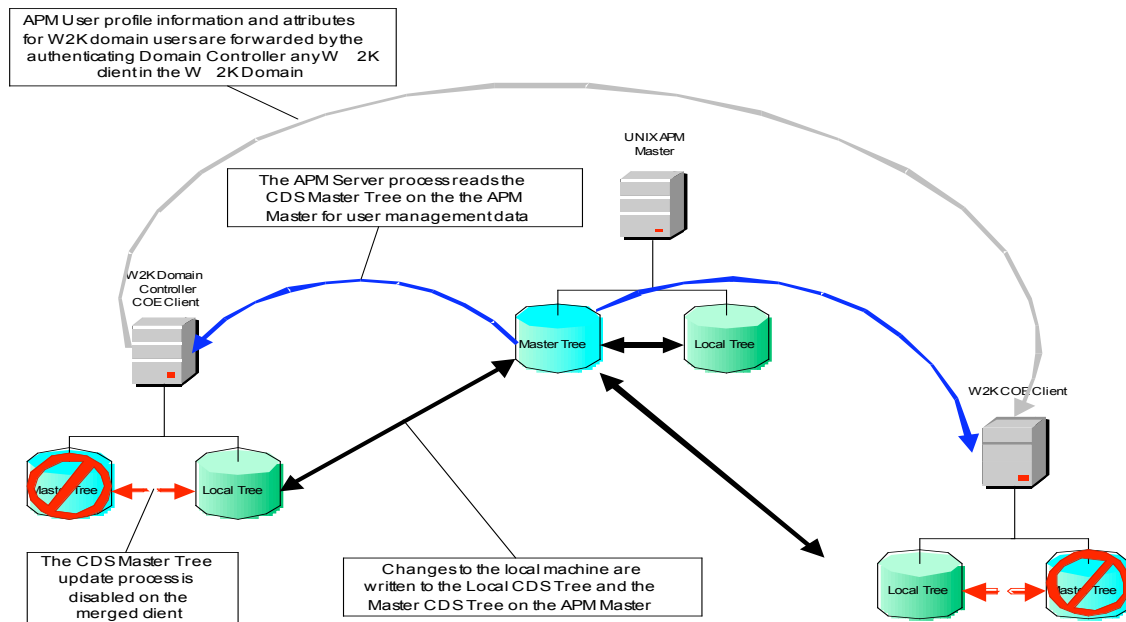


Figure 3-2-3 Merged APM Domain

- (5). All of the clients should have their APM roles checked prior to being merged into the AAD. To check the role of a client, run `APM_RegisterHost.pl -g`. Any domain member client should show up as Operating System Domain Member (OSDM) and the domain name should appear in the Domain field. If not, then select the Auto-Detect and Submit buttons. Objects for domain members are controlled by the domain master server or the domain controller. An object can be a user account, group account or user profile. For NIS+ domain members, the NIS+ master server controls the objects for each of the NIS+ clients. In a W2K domain, the authenticating W2K domain controller handles objects for each of the W2K client workstations.
- (6). In a fully merged AAD, every client is pointed to the AAD Master Server and each Local CDS Tree is merged into the Master CDS Tree of the AAD Master Server. This process is accomplished with the `APM_MergeHost.pl` script. When a change is made to an APM object, that change is transmitted to every client merged into the AAD. If a client is offline (i.e. powered off or no network connection), then that update/change is lost and the APM Master Server flags that object as being out of synch. Most often this flag is cleared

when another update is made to the object and the update is passed on to every AAD client.

d. Representative Client AAD

- (1). In a Representative Client AAD, a small number of client workstations are merged into the AAD. These clients should, in total, contain every segment that a user may require access. These segment features become the basis for building domain managed user profiles. Domain managed objects are stored on the domain master servers. For NIS+ domains, this is the NIS+ Master Server, for W2K domains this is any domain controller for the W2K domain.
- (2). Any changes to domain or locally managed objects only affect the computers that are merged into the AAD. The non-merged clients do not receive any updates but access the domain objects (i.e. profiles) from their respective domain masters.

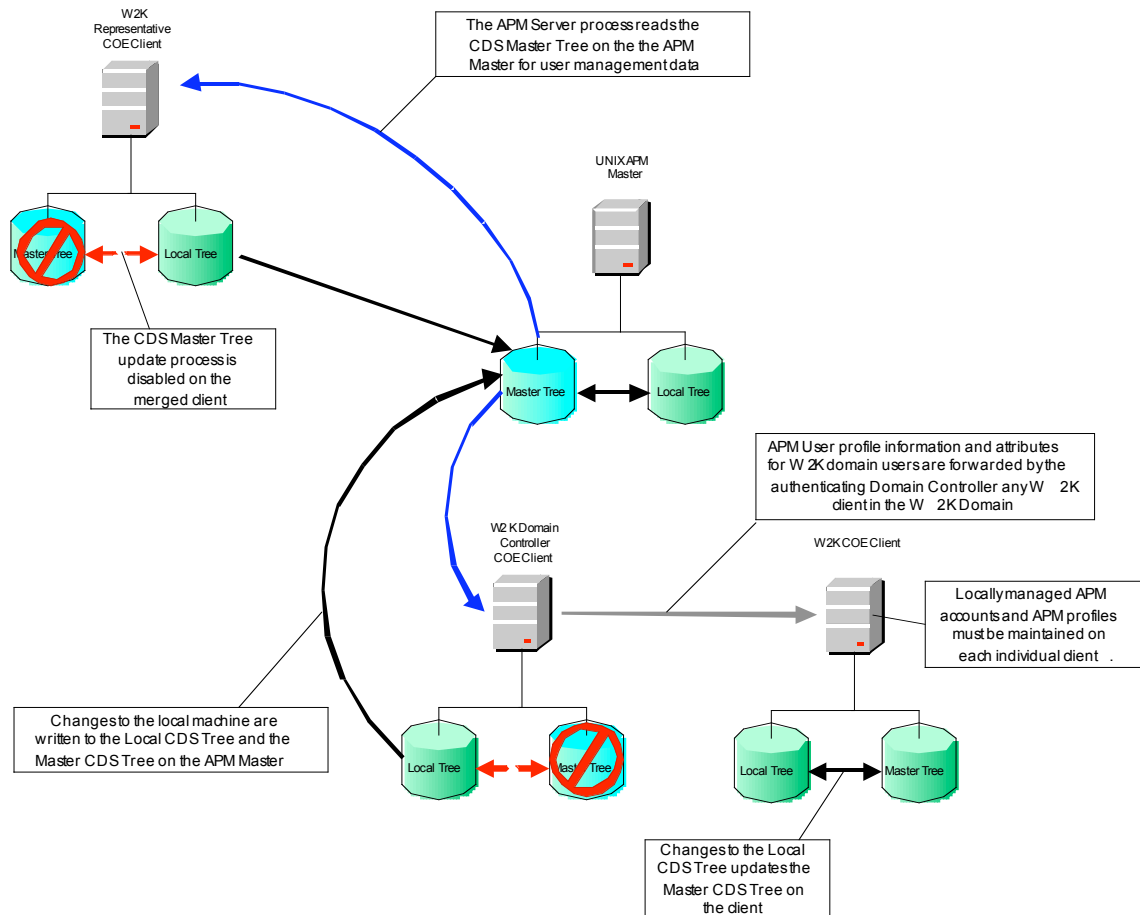


Figure 3-2-4 Representative Client Merged APM Domain

15. System and User Administration in a Representative AAD

- a. In a fully merged AAD user and system administration functions can be ran from any workstation/client in the AAD. This means that the system administrator can run the APM Client (APM_Client.pl) processes on any workstation and update the AAD environment with the changes. This enabled because each workstation/client is configured to use the Master CDS tree on the APM Master Server.
- b. In a Representative AAD, only those clients configured to “point” to the APM Master can update the APM Master’s Master CDS Tree. Each unmerged client can be configured to either point to itself (Fig. 3-2-5 Client A) or configured to point to the APM Master (Fig. 3-2-5 Client B).

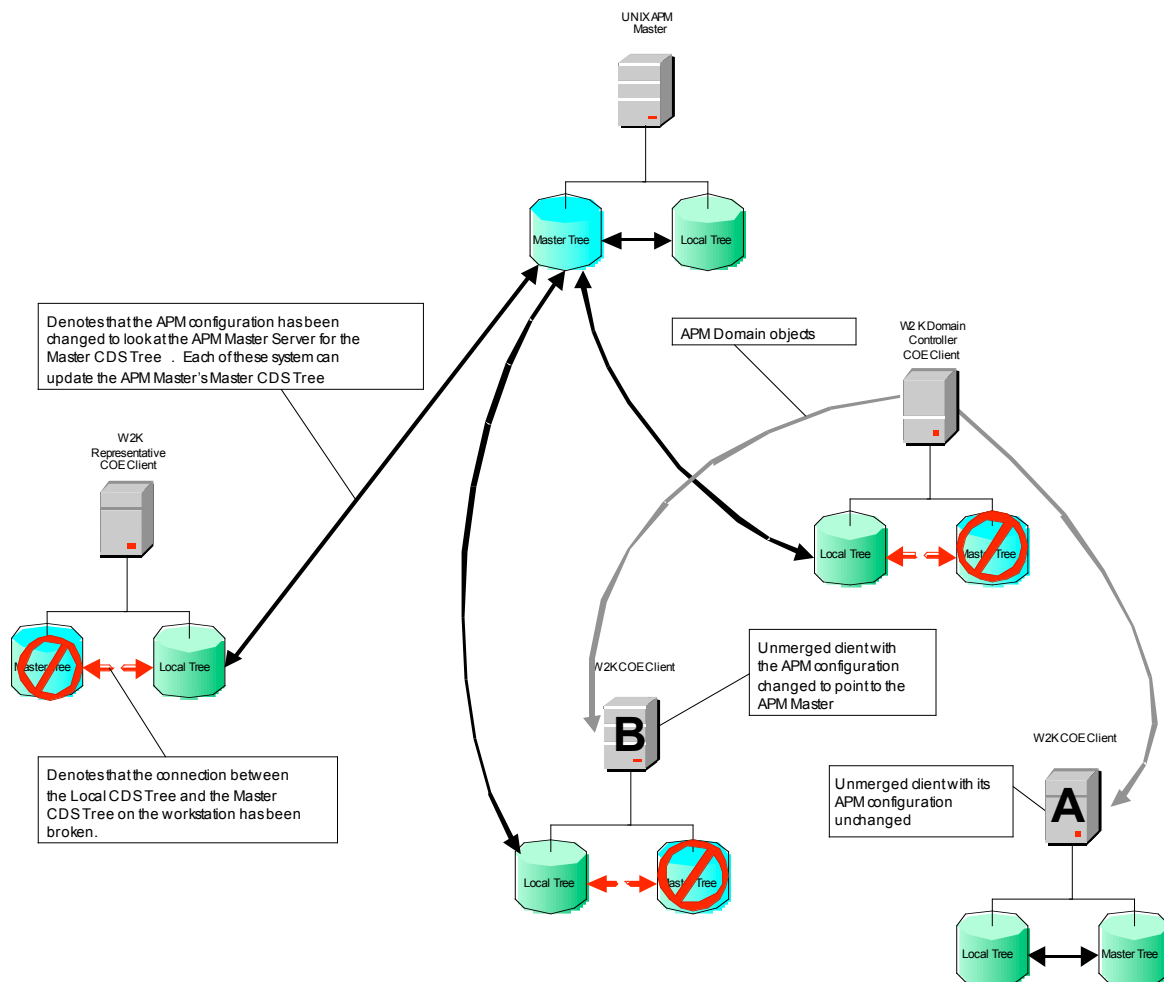


Figure 3-2-5

16. User Accounts and Profiles

User accounts and profiles identify and define the level of access a user has to the GCCS-M system. Accounts and profiles are managed either on the domain level or the local level.

a. Locally Managed

- (1). Local accounts and profiles reside on each individual computer. When a local account is created, the account properties must match the security criteria for the computer's security settings (i.e. password complexity rules). The account then resides in both the operating system user's database/files and in the APM Local CDS tree. Locally managed profiles also reside in the APM Local CDS tree but do not interact directly with the operating system. Local profiles can be created in merged or unmerged AADs.
- (2). In an unmerged AAD, locally managed objects (users, profiles and groups) must be created on each individual workstation or server. In a merged AAD, locally managed objects can be created on any workstation or server in that is a member of the AAD. Once the object is created then it can be "pushed" to any member of the AAD. The push can occur when the object is created by selecting the computer name from the Hosts tab.

b. Domain Managed

- (1). Domain managed objects are controlled by the APM Master Server and the Domain Master Server for each domain. Generally there are only two domains for each AAD, a W2K domain and a NIS+ domain. Domain objects are stored in the Master CDS Tree of the APM Master Server and in the Local CDS Tree of the domain master server (W2K domain controller or NIS+ master server).
- (2). Domain objects can only be created from a merged AAD, either a fully merged AAD or a representative client AAD. The domain master server controls access to any domain object that a domain client is attempting access. A domain client in this case means an operating system domain client; the client does not have to be merged into the AAD in order for it to access a domain object.

17. Profiles and Groups

- a. Profiles and account groups provide a convenient method for implementing discretionary access controls within GCCS-M. Using the Profile Editor, the Security Administrator can create profiles that are tailored to specific user needs, or to the needs of a specific GCCS-M site.
- b. A profile provides a mechanism by which a security administrator can group sets of users, usually by their job responsibilities. Rather than assigning each user a list of applications they are allowed to access, the security administrator can define a profile that provides convenient access to a list of applications, and then assign users to one or more profiles based on user responsibilities. For example, the security administrator may create a profile called GCCSM User, which would contain all of the applications that a typical Global Command and Control System-Maritime (GCCS-M) user would need to access. The administrator could then assign this profile to one or more user accounts.
- c. Similarly, the administrator could create a profile called Backup that would provide access to the applications needed to perform a system backup. This profile could then be assigned to one or more user accounts.
- d. Account groups and profiles are utilized together to enforce access control on the GCCS-M system. Account groups are associated with profiles based on the functionality required by the profile. That is, functions are assigned to users through profiles, but access to the executables underlying the functions is provided by group membership. This membership provides the users access to the file system objects needed to perform their assigned tasks. Therefore, users must be assigned to the appropriate groups based on the functions specified in their assigned profiles. Appendix A, of the Trusted Facilities manual provides a list of Default Profiles, provides a matrix for the System Administrator to determine the interrelation between groups and the functions provided by profiles.

18. Re-building an APM Administrative Domain

- a. The best method to rebuild an AAD is to first reset every computer back to a pre-merge condition. Under certain conditions this may require that the system administrator remove/delete local objects that were created and stored on the client

while it was in the AAD. System administrators need to be familiar with the original state of the users, profiles and groups that were on the system when the COE Kernel was loaded. This “house cleaning” prevents future conflicts we the AAD is re-merged.

- b. The first step in this re-building process is to “break” the AAD. This is accomplished by running the APM_BecomeOwnMaster.pl on every member of the AAD. It is recommended that the APM_BecomeOwnMaster.pl script be ran on all W2K clients first, then W2K domain controllers, UNIX client servers and finally on the APM Master Server. The APM_BecomeOwnMaster.pl script copies the Local APM CDS Tree to the Master APM CDS Tree on that client and re-establishes the link between the computer’s Local CDS and Master CDS Trees. The APM_BecomeOwnMaster.pl script also changes the APM Master Server back to the local machine name.
- c. After APM_BecomeOwnMaster.pl has been ran on all of the computers in the AAD, the system administrator needs to run the APM_Client.pl script on each computer to review all of the users, groups and profiles listed and remove any item that was created or left behind from the merged AAD. This will prevent conflicts from occurring when the AAD is re-merged.

19. Recommendations and Best Practices

The following are recommendations to local system administrator to ensure the smooth and efficient operations of APM.

- a. For large scale networks (larger than 10 clients) the Representative APM Client AAD should be used.
- b. The APM Master should be located on a separate server whenever possible. This prevents APM issues from interfering with other server functions. An example is that the APM Server process locks up on the server and is unusable and requires a reboot. If this server is also the TMS Master Server, than the re-boot will cause a loss of track data.
- c. Use domain managed profiles and accounts. The use of domain objects makes user and profile management easier and is more robust than using locally managed account and profiles.

- d. Prior to beginning the APM Merge process, review the local DNS and ensure that all clients that are going to be merged into the AAD have the correct forward and reverse pointer records.
 - e. Prior to beginning the APM Merge process, ensure that every client is properly registered with APM by running the APM_RegisterHost.pl and verifying that the client's role is correct.
 - f. Backup the **/h/COE/data/CDS** directory on the APM Master Server and any Domain Controllers on a daily/weekly basis. System administrators may wish to save the **/h/COE/data/CDS** directory on individual workstations after major changes/upgrades.
 - g. Prior to merging a workstation perform the following checks:
 - Ensure that the APM Master and the client machine can ping each other.
 - Verify the APM Local Client Key on the APM Master and on the client.
 - Perform an nslookup on the client for the APM Master server and run an nslookup on the APM Master for the client. This validates the DNS and ensures that the authentication process will work.
20. The most common errors with APM are:
 - No COE Profile Selector available after logging in with a domain account built in APM.
 - The Profile is not available in the COE Profile Selector.
 - The Profile is available but when the submit button is clicked an error is generated such as "Cannot write to CDS".
 - The Change Password Utility is not available after logging in with a domain account created in APM.
21. Known APM fixes.
 - a. On a Windows/COMPOSE Clients:
 - (1). Verify **C:\h\COE\Comp\APM\bin** has authenticated users added with **Read & Execute, List Folder Contents, and Read** permissions.
 - (2). Verify the domain name and hostname are correct.
 - (3). Verify the Master Host in Edit APM Configuration (**C:\h\COE\Comp\APM\bin\APM_EditConfig**) is pointed to the APM Master and that Enable Authentication is selected. Verify the Master Port is

set to 2003. Make sure that the Enabled Auditing and Enable Authentication Failure Lockouts boxes are checked.

- (4). Verify the Authentication Key is set and that it matches the Master Authentication key.
 - (5). Browse to **C:\h\COE\Comp\APM\bin**. Open a command prompt and drag and drop **APM_RegisterHost** into the command prompt. At the end of the line, insert a space and type **-g** to get the GUI. Verify that the Function selected is “Operating System Domain Member (OSDM)”. If the function is “Stand Alone Workstation or Server (SAWS)” click the Auto-Detect button and verify that the function changes to OSDM. Click the submit button. If an error is reported, reselect the OSDM function and click the submit button again.
- b. On DC1 and DC2
- (1). Check DNS; verify there are no duplicate entries. Ensure that the IP and hostname in DNS match the actual hostname and IP address of the client. Ensure the reverse lookup zone entries are correct and there are no stale entries in either the forward or reverse lookup zones. Double-check the aliases for the GCCS-M servers.
 - (2). Check on the applicable server to ensure the location of home directory is properly shared. This will either be on DC1/h/Users/global or possibly on the file server, shared out as ComposeUsers.
- c. On DC1 only.
- (1). Browse to **C:\h\COE\Comp\APM\bin\APM_EditConfig**, click on the Advanced Configuration button and verify the two Home Servers entered like the example below:

Home Server	Shared Directory	Share Name	Drive Letter
Comms1	/h/UEERS/global	GlobUser	Y
Default	/h/USERS/global	global	W

NOTE: The W drive will be the shared drive when an accounts home server is set to DC1. The Y drive is used when the home server is set to comms1, as in the example

above. Compose will use H, S, Y, and Z based on configuration files and login scripts. Do not use these drive letters for sharing out /h/USERS/global on DC1. If DC1 is not being used to store GCCS-M user home directories on /h/USERS/global then this step is not applicable.

- (2). Verify the APM Master is added to **Active Directory Users and Computers\COMPOSE Users and Computers\COMPOSE Workstations**. Verify the trusted for delegation box is checked.
 - (3). Verify the Master Host in Edit APM Configuration is pointed to the APM Master and the Enable Authentication is selected. Verify the Master Port is set to 2003.
 - (4). Verify **C:\h\COE\Comp\APM\bin** has **authenticated users** added with **Read & Execute, List Folder Contents, Read, and Write** boxes checked in the Allow column.
 - (5). Verify **C:\h\COE\Comp\APM\bin** has **administrators** added with **Full Control, Modify, Read & Execute, List Folder Contents, Read, and Write** boxes checked in the Allow column.
 - (6). Verify **C:\h\COE\Comp\APM\bin** has **system** added with **Full Control, Modify, Read & Execute, List Folder Contents, Read, and Write** boxes checked in the Allow column.
- d. From DC1
- (1). Verify that the domain name and hostname are correct.
 - (2). Browse to **C:\h\COE\Comp\APM\bin**. Open a command prompt and drag and drop **APM_RegisterHost** into the command prompt. At the end of the line insert a space and then type **-g**. Verify the Function selected is “Primary Domain Controller (PDC)”. If the function is anything else click the Auto-Detect button and verify the function changes to PDC. Click the submit button. The computer will prompt if the operation completed successfully. If an error is reported, reselect the PDC function and click the submit button again.

- e. From DC2
 - (1). Verify that the domain name and hostname are correct.
 - (2). Browse to **C:\h\COE\Comp\APM\bin**. Open a command prompt and drag and drop **APM_RegisterHost** into the command prompt. At the end of the line insert a space and then type **-g**. Verify the Function selected is “Secondary Domain Controller (SDC)”. If the function is anything else click the Auto-Detect button and verify the function changes to SDC. Click the submit button. If an error is reported, reselect the SDC function and click the submit button again.
 - (3). **RegisterHost.pl note:** When the cloning process is used to load GCCS-M clients, the client is removed from the domain and placed in a workgroup; if the kernel is loaded on a client in the domain the cloning process will fail. After an image has been restored to the client and the post image procedures are complete, the client must be registered after joining it to the domain as an Operating System Domain Member OSDM. If the APM configurations are completed prior to registering the host, the APM merge might not succeed and even if it does, the client still requires a correct registration, or no domain profiles, accounts, or groups will be pushed to the client.
- f. On the APM Master
 - (1). Verify the two CIFS processes are running: Open an x-term and type **ps -ef | grep -I cifs**. Verify on the screen: **h/COTS/CIFS/bin/Samba/sbin/smbd** and **h/COTS/CIFS/bin/Samba/sbin nmdb**.
 - (2). To verify /h/USERS/global is exported, from an x-term type: **dfshares** or go to another UNIX server such as webservr, open an x-term and type: **mount -p**
 - (3). Verify the Master Authentication Key is correct in Authentication Manager.
 - (4). Verify the clients are added in the authentication manager and the authentication key matches the Master Authentication key.
 - (5). Since there are some applications in GCCS-M that still use the host file (/etc/hosts), verify proper hostname and aliases are entered.
 - (6). Verify that DNS is set properly.

- g. On the remaining UNIX machines
 - (1). Verify the Master Host in Edit APM Configuration is pointed to the APM Master and Enable Authentication is selected. Verify the Master Port is set to 2003.
 - (2). Verify that the domain name and hostname are correct.
 - (3). Verify the Authentication Key is set and that it matches the Master Authentication key.
 - (4). Open an x-term and change directories to **/h/COE/Comp/APM/bin**. Run the RegisterHost program (**./APM_RegisterHost -g**). Verify the “Operating System Domain Member (OSDM)” is selected. If the function is “Stand Alone Workstation or Server (SAWS)” click the Auto-Detect button and verify the function changes to OSDM. Click the submit button. The system will prompt to continue when the operation is successfully completed. If an error is reported, reselect the OSDM function and click the submit button again.
 - (5). Since some applications within GCCS-M still use the host file (/etc/hosts), ensure that the proper hostname and aliases are entered.
 - (6). Verify proper DNS configuration.

INFORMATION SHEET 3-2-3

INTEGRATED C4I SYSTEM FOUNDATIONS (ICSF)

A. **Introduction**

This information sheet will provide the trainee with an understanding of the ICSF bundle and each segment internal to the ICSF bundle.

B. **References**

Online Embedded documentation

4.0.1.0 Consolidated Load Plan and Installation Procedures

C. **Information**

1. ICSF Bundle

- a. The ICSF 4.x series creates the software framework for the next generation C4I systems to meet field operators' requirements. ICSF operates with a Java-based graphical user interface (GUI) within underlying three-tier architecture. Moreover, the ICSF series supports the services framework for communications, tactical database management, and visualization.
- b. ICSF is composed of four primary COE components-Tactical Management System (TMS), Tactical Management System Visualization (TMSV), Universal Communications Processor (UCP), and Joint Mapping Tool Kit-Visualization (JMV). It also contains two supporting components -Integrated Foundation Library (IFL) and Application Framework (AFW) - whose creation resulted from the decomposition of the software formerly known as the Unified Build (UB).
- c. Together, the ICSF segments provide the foundation for creating a C4I system. Because of operational dependencies, the ICSF segments must be installed, configured, and removed in a particular order. For example, all of the segments depend on the shared libraries that the IFL segment provides; therefore, the IFL segment must be installed before any of the other segments are installed. For the

same dependencies, IFL must be the last segment removed. Figure 3-2-6 provides a view of the other segment's dependencies.

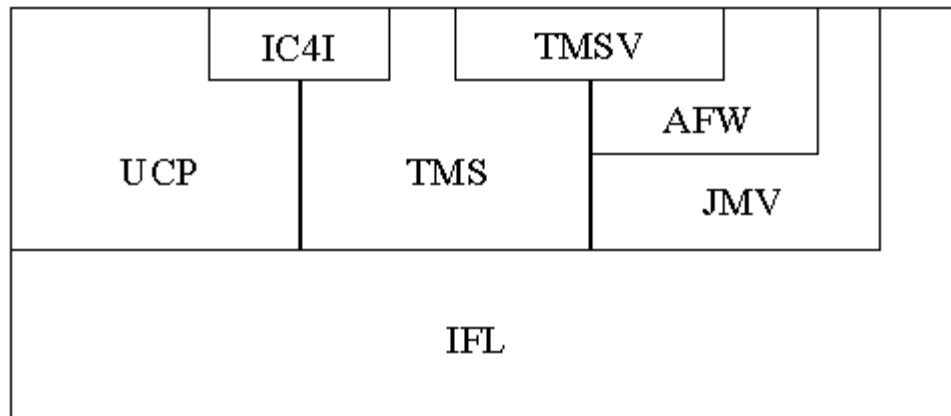


Figure 3-2-6. ICSF Segment Dependencies

- d. IC4I requires UCP on UNIX only. IC4I does not require Tactical Management System-Visualization (TMSV), Application Framework (AFW), or Joint Mapping tool Kit (JMV) however, they are usually loaded to provide track visualization. TMSV does not require UCP; however UCP must be loaded to access communications broadcasts.
2. ICSF Components
 - a. The ICSF software Bundle contains the following core component segments:
 - IFL - Integrated Foundation Library
 - JMV - Joint Mapping Tool Kit-Visualization
 - AFW - Application Framework
 - UCP - Universal Comms Processor
 - TMS - Tactical Management System
 - TMSV - Tactical Management System-Visualization
 - b. In addition to the core components, the following software and data segments are provided with the ICSF Bundle:
 - IC4I - ICSF C4I Configuration
 - JMVMD - JMV Map Data

3. **Integrated Foundation Library (IFL)**

The IFL segment contains a set of utility libraries and services that are used by the other components contained in ICSF. IFL has a set of runtime libraries and JAR files that must be available to the other segments (JMV, AFW, UCP, TMS, and TMSV) to ensure full runtime functionality of each segment. It is also responsible for exporting the TDA's.

4. **Application Framework (AFW)**

- a. The AFW segment is a Joint Mapping Visualization client providing a framework for application segments that share a common tactical display. The AFW Chart supports segment definition and user configuration of menu, toolbar, and hot key actions. Map accessories can be provided to supply a continuous mechanism for drawing objects from a given source. AFW also provides a map accessory called Symplot that offers a framework to provide common plotting of data objects from different databases.
- b. AFW and IFL are the building blocks of the ICSF bundle. The AFW provides the static information for the maps. IFL is the static information library for world wide name and locations.
- c. The Cartographer, part of AFW, provides the framework under which multiple applications can share a single map to create a complex composite picture. This composite picture consists of two distinct conceptual layers: the *Background Map* and the *Foreground Objects*.
- d. The *Background Map* is created by plug-in components known as Draw Modules. Each Draw Module contributes to the background by rendering a map product such as Compressed ARC Digitized Raster Graphics (CADRG) or by drawing particular geographic features such as roads or navigation aids.
- e. *Foreground Objects* consist of graphical objects that are drawn in layers on top of the background by the server. Representative graphic objects are arcs, circles, corridors, boxes and military symbols.
- f. Application programs-Map Accessories-create and manage all objects in a map's display list. Cartographer also provides a number of built-in operations on a map's display list such as selection, highlighting, repainting, and animation. The Map

Accessories create and maintain only their contribution to a map's display list. The mechanics of user interaction with the display list is handled entirely by the Cartographer server.

- g. Map Accessories are run and managed by the map manager program called Chart. Chart keeps track of what Map Accessories should be run and manages which Map Accessory has temporary control of a given map. Chart also provides a number of built-in map actions such as double/half scale, change projection, re-center map, feature controls, and grid line controls. Cartographer contributes the basic mapping capabilities and Chart provides the framework under which applications cooperate to create a composite display.

5. **Joint Mapping Tool Kit-Visualization (JMV)**

- a. The JMV segment is the chart server portion of the Joint Mapping Tool Kit (JMTK). The JMV segment provides a server that creates maps and draws graphic primitives on a geographic display.
- b. JMV Map Data (JMVMD) is a data segment that provides additional map data for JMV. JMVMD is not included as part of the ICSF Bundle but is provided as a separate segment that can be installed after the ICSF Bundle has been installed.

6. **ICSF C4I Configuration (IC4I)**

The ICSF C4I (IC4I) segment provides additional configuration for the ICSF Bundle to finalize the installation for a basic IC4I environment that supports communications, database management, and tactical visualization.

7. **Universal Comms Processor (UCP)**

The UCP segment provides communications interfaces, message processing, and message handling functionality. UCP provides a set of GUI applications and tools to configure, manage, and monitor the communications interfaces and message traffic. It also provides a set of APIs and Tools that can be used by other segments to define and install new communications interfaces, message types, and decoders to process those message types.

8. Tactical Management System-Visualization (TMSV)

The TMSV segment is a client to both the TMS and AFW segments, providing visualization of the track data as well as GUI access to track management functions in the TMS segment. The TMSV segment retrieves the track data from the TMS segment, adapts it to what is required by the Symplot portion of the AFW segment, and passes the data to the AFW segment for display. The track management GUI provided by TMSV can be accessed from the AFW segment via the main Chart menu toolbar or by right clicking on the track symbols on the Chart.

9. Tactical Management System (TMS)

- a. The TMS segment provides the correlation engine, including single source, report-to-track, and multi-source track-to-track correlation, and the tactical database management for COE. The primary responsibility of TMS is to manage track data by providing data correlation, storage, and distribution.
- b. TMS is the component of COE that provides the track database. The track database consists of data that includes-but is not limited to-the identifying attributes and position histories of reported ships, submarines, aircraft, land units, and other moving or fixed objects of interest in the world. TMS also provides specific message parsing and message encoding, and multi-source correlation.
- c. A *track* is a physical or imaginary object whose existence and, possibly, movement have been reported (i.e., "tracked"). A *contact* is a single instance of a position report on an object being tracked.
- d. Tracks in the system appear as symbols on the tactical display representing objects or groups of objects (i.e., ships, submarines, land units, or aircraft). The position of the track on the screen reflects information contained in the latest contact report. Data for each track can enter the system from many sources, including the following:
 - Ship's organic sources, including ACDS, Link-11, Link-14, and Link-16
 - Intelligence (Intel) messages from the Officer in Tactical Command Information Exchange Subsystem (OTCIIXS) or the Tactical Data Information Exchange Subsystem (TADIXS)
 - Repeat, POST, fleet broadcast, or other generic serial, asynchronous RS-232 input sources, which are treated as Intel data

- Navigation inputs received from sources such as Ships Inertial Navigation System (SINS) or Carrier Vehicle Navigation System (CVNS), each of which have their own message format
 - Manual input, for information such as visual sightings
 - External data sources that are registered with TMS
- e. Identity and position data for each currently active track is stored internally as a record, or group of records, in the track database. Some of the track types that TMS supports include:

Platform Tracks	RAYCAS V Tracks
UNIT Tracks	ELINT (Electronic Intelligence) Tracks
Link Tracks	Acoustic Tracks
SPA-25G Tracks	FCS (Fire Control System) Tracks
SI Tracks	Missile Tracks
EOB (Electronic Order of Battle) Tracks	Facility Tracks
General Tracks	

- f. Each of these track record types contains its own (possibly overlapping) data elements. The most comprehensive tracks are:
- Platform Tracks - air and sea objects such as aircraft, ships, and submarines
 - UNIT Tracks - land objects such as tanks
 - Missile Tracks - air objects such as Theater Ballistic Missiles (TBMs)
- g. Link, SPA-25G, RAYCAS V, ELINT and Acoustic tracks represent raw data observations on physical objects. These lesser track types can be associated with Platform tracks so that their positions and attribute updates can be added to the Platform. Only ELINT tracks can be associated with UNIT tracks. An associated track is said to be subordinate to the Platform or UNIT track, but it maintains its identity as a separate track in the database. This permits the track database manager (TMS Master) to perform source-dependent correlation among the lesser tracks, which percolates up into the associated Platform or UNIT track.

- h. The operator sees each track appear on the display in its appropriate geographical position. This position is determined from data that is contained in the track data record. Track symbols and colors in the display indicate the type of object represented by a track and its threat status, both of which are derived from the track record. Track record updates based on contact reports received by a COE-based system automatically cause a plot update in the geographic display to reflect the track's latest position. In addition to storing the most recent contact report in the track record in the track database, a COE-based system also maintains a composite track history of all contact reports that have been correlated to the track and each of its associated tracks.
- i. An operator can request various displays of track information, which the system builds from the contents of the corresponding track database record and the track history. The operator can also perform various functions to clean up, or manage, the track database. TMS Master is designed to operate within a local area network (LAN) of computer workstations using virtual machine architecture. A TMS Master Service is run on each machine in a network. One of the machines is designated the TMS Master, Master Host. Each other TMS Master Service is designated a "slave" on the LAN. The TMS Master process running on the TMS Master, Master Host machine plays the role of network controller and synchronizes the track database management activities of each TMS Master within the network.

10. Track Database

The COE-provided track database is a collection of records, grouped into separate types of track information. Each of these groups contains a different record type. The track database is referenced by some as a "database of databases," since each group may be thought of as a database of a particular track record type. However, the track database is actually a single database. Track record types include the following:

ACOUSTIC	Acoustic tracks consist of subsurface contacts with purely acoustic tonal information and Trademark as attributes for correlation. Special Trademark correlation is performed on these tracks.
ELINT	The ELINT track database consists of tracks reported from all sources with emitter parametric data (ELNOT, PRI, RF, Scan Rate, and Pulse Width). Emitter reports are correlated to ELINT or Electronic Order of Battle (EOB) tracks. ELINT tracks may be associated with Platform or UNIT tracks. EOB tracks may be associated with Facility Tracks. Any number of emitters may be associated with a given Platform or UNIT.
FACILITY	Facility tracks are created by data extracted from the MIDS Intelligence Database (MIDB).
FCS	Fire Control System (FCS) tracks are used to exchange track data with the CCS/Mk2 Submarine Combat System aboard certain U.S. Navy submarines. These tracks are similar to Link tracks except that they have little attribute data. They are reported as a position, course, speed, weather at target, and FCS target number. Correlation is based exclusively on the FCS target number.
General	General Tracks are used to produce track types other than the standard ones in ICSF TMS. Key fields are: Originator, which identifies the actual type. Originator Key, which is used to correlate the tracks; Hierarchy Level, which is used in associating tracks; and Raw Data, which contains additional information to be stored in TMS.
Link	The Link track database consists of tracks created and maintained by several interfaces, including: Link-11, Link-14, Link-16, TADIL A/B, TADIL J, and ACDS. Link tracks are not archived to disk (unless associated to a Platform track) and histories are not maintained. Correlation is performed solely using the NTDS track number as a unique search key. Up to four separate Link databases are supported, which provides the ability to monitor remote Link-11 data sources.

Missile	The Missile tracks represent ballistic missile objects. These missile tracks may be reported over any interface, and history information is maintained. Predicted launch and impact positions are often included.
Platform	The Platform tracks are the most comprehensive tracks in the system. They represent air and sea objects. Any other type of track, except a UNIT track, may be associated with a Platform track. Platform tracks designated as OTH tracks are candidates to be reported over OTCIXS, HIT broadcasts. Platform tracks may be designated as local (LAN) or terminal tracks, in which case they will not be exported over any broadcast.
RAYCAS V	The RAYCAS V track database consists of tracks reported by the RAYCAS V system aboard US Coast Guard vessels. These tracks are similar to Link tracks except that they have almost no attribute data. They are simply reported as a track number plus position, course, and speed.
SI	The SI Track database consists of tracks reported from Communications Intelligence (COMINT) sources.
SPA-25G	The SPA-25G database is similar to the Link database except that the source of data is the SPA-25G system. Up to four simultaneous SPA-25G interfaces and track databases are supported. Each track comes with a unique track number (used for correlation) and system track number (used for display). Histories are maintained on the SPA-25G tracks.
UNIT	The UNIT track database consists mostly of friendly land tracks representing Army, Marine, Navy and Air Force units ashore. Identification includes: organization type, such as administration, engineer; echelon, such as Air Army, command, division, attachment; and platform, such as anti-aircraft gun, bunker and bridge. UNIT tracks designated as OTH tracks are candidates to be reported over OTCIXS, HIT broadcasts. UNIT tracks may be designated as local (LAN) or terminal tracks, in which case they will not be exported over any broadcast.

11. Types of Tracks

- a. Each track database can be further divided into track types.
 - OTH - Displayed on all workstations on a LAN and are candidates for external transmission.
 - LOCAL - Displayed only on the workstations in a local network
 - Terminal - Displayed only on an individual workstation.
- b. There are three additional levels within the different track types:
 - Real-World tracks are those that exist in the real world, such as ships, aircraft, submarines, and land units.
 - Live Training tracks are tracks that exist in the real world, but are being used for exercise purposes. Live Training tracks might be assigned a different identity for exercise purposes, such as a friendly track being identified as hostile.
 - Simulated tracks are those that don't actually exist in the real world, but are being created for exercise and scenario purposes.

12. Track Associations

A key concept of the COE-provided track database is the ability to associate, or link, two or more tracks together. One of the associated track records is considered the *parent record*. Records associated with the parent are called *children* of the parent and serve to provide additional information on the parent. Once an association has been made, position reports for any associated child track automatically update the parent track. For example, say an ELINT track record has been associated with a certain Platform track record. Each time the ELINT track receives a position update that is archived, the associated Platform track receives the same update. Associations are normally manually initiated; however, special cross database correlation provides for automatic associations of (1) an ELINT or Link track to a Platform track and (2) an EOB track to a Facility track. Similarly, an association may be automatically broken when the system determines that it no longer makes sense.

13. Database Management

The operator is provided with a variety of tools to manage the track database.

- Create new tracks for each track database
- Edit track records

- Delete track records
- Merge two records (similar record types)
- Associate two records (dissimilar record types)
- Disassociate subordinate tracks
- Create Platform and associate subordinate in one step (NU-TRK)
- Reprocess ambiguity records
- Turn an ambiguity record into a track
- Promote a terminal track to a local or OTH Platform track
- Copy a local or OTH Platform track into a terminal track. A terminal track may become a local or OTH. A local track may become an OTH.
- Compare tracks to reports
- Compare tracks to tracks
- Create track summaries for each database and for all databases

14. Network Database Management

The TMS Master Server must provide a consistent representation of the central COE-provided track database to all workstations in the local area network. As a system administrator, making sure the COP gets tracks on each client is one of your main jobs. The server does this by exporting data record updates to each workstation so that applications have local copies of the track database for fast access.

15. Correlation

- a. Each contact report that comes into a COE-based system must undergo correlation to determine its assignment in the track database. Correlation determines whether an incoming contact report provides data for either an existing track or a new track; or it may become an ambiguity, if it does not contain enough attribute information to allow positive identification.
- b. TMS Master performs automatic correlation, whenever possible, on the basis of the attribute sets for each track, which specifies the information that identifies that track. If automatic processing cannot correlate the contact report, the operator may be able to assign it correctly to the database.
- c. TMS Master provides the ability to use the COE-provided unique identifier (UID) as its principal correlation element.

THIS PAGE INTENTIONALLY LEFT BLANK

ASSIGNMENT SHEET 3-3-1

GCCS-M ADMINISTRATION

A. Introduction

This assignment sheet is to be completed as homework.

B. Enabling Objectives

- 3.23 **CONFIGURE** peripheral devices connected to a GCCS-M system.
- 3.24 **DISCUSS** the different communications channels that are utilized in GCCS-M.
- 3.25 **DESCRIBE** the term COP Management and how it relates to GCCS-M.
- 3.26 **DISPLAY** the ability to navigate the Communications Channel Manager.
- 3.27 **DESCRIBE** the NAVMACS II/SMS shipboard architecture to the level of detail required to support system administration functions.
- 3.28 **DESCRIBE** the function of CST.
- 3.29 **DISCUSS** proper configurations and settings for CST.
- 3.30 **DEMONSTRATE** the ability to create and modify CST channels.
- 3.31 **DISTINGUISH** the status of a CST node by color indication.
- 3.32 **PERFORM** miscellaneous tasks as related to GCCS-M Administration.
- 3.33 **PERFORM** Track Management System (TMS) administration.
- 3.34 **DISCUSS** backup strategies with GCCS-M.
- 3.35 **DEMONSTRATE** the use of the GBAR utility.

C. Study Assignment

Review Information Sheets 3-3-2

D. Study Questions

1. How many serial ports does the current Digi-Mux support?

2. State the primary interfaces that interact with ICSF
3. What is MTC?
4. What are some functions of CST?
5. What is the difference between CSTTCP and CSTSTCP?
6. How many child nodes can CSTMDP support?
7. What are the two ways to clean the TMS database?
 - a. Which is preferred?
8. What backup tool is utilized on the Solaris GCCS-M servers?

INFORMATION SHEET 3-3-2

COMMUNICATIONS

A. **Introduction**

This information sheet will provide the trainee with an understanding of GCCS-M Communications.

B. **References**

Online Embedded documentation
Current Load Plan and Installation Procedures

C. **Information**

1. Communications Background

- a. DII/COE uses one- and two-way communications channels to receive and transmit data such as track position reports and tactical messages (OPNOTES) between commands. GCCS-M operators control the configuration of the communications channels. However, system administrators also must understand how to configure channels in order to be better prepared to troubleshoot communications problems.
- b. The UCP software segment is a child component of the COE core that provides the Communications (Comms) Services capability. The current UCP implementation focuses on Command, Control, Communications, Computers, and Intelligence (C4I) communications and messaging services. The UCP is constructed on top of the COE Kernel to meet the COE Communications Service requirements, specifically in the area of message-based data exchange for both text and binary messages.
- c. The UCP provides a configurable and extensible framework for communications and message handling services. The UCP provides services for adding/configuring communications interfaces, wrapping/unwrapping messages, logging incoming/outgoing message traffic, and interacting with message handling and message engines.

- d. UCP receives serial data inputs via the DigiMux. The DigiMux replaces the old SCSI-Mux found in the GCCS-M 3.X configurations. The DigiMux supports 16 serial channel interfaces and converts the serial data transmission into a TCP/IP packet. This allows any system on the network to support communication inputs without physically moving any hardware or cabling. The standard configuration is for comms1 to support all serial data inputs. If during operations, the operator or system administrator notes that there is no data coming in on the serial interfaces or that UCP appears "locked-up", this may be an indication that the DigiMux is inoperative. The operator or system administrator should recycle the DigiMux as the first step to troubleshooting UCP or serial communication problems.
2. **Communications Channels** The UCP component provides centralized management of all communication channels in a UCP suite. The operator can add new channels, choosing from a list of available communications interfaces, configure and activate the new channel.
 - a. ICSF uses a number of interfaces to interact with external systems and devices. The primary interfaces are:
 - 1) Officer Tactical Command Information Exchange Subsystem (OTCIXS)
 - 2) Tactical Data Information Exchange Subsystem (TADIXS) A
 - 3) Network
 - 4) Common Operational Picture (COP) Synchronization Tools (CST)
Transmission Control Protocol (CSTTCP)
 - 5) Tactical Receive System (TRS)
 - 6) Serial
 - 7) Advanced Combat Direction System (ACDS)
 - 8) Multi-Tadil Capability (MTC)
3. **Message Logging.** The UCP component provides logging capabilities for the message body and its wrapper, sectioned or collated if necessary, thus providing an accurate depiction of the full message actually transmitted or received. The logs also provide message status (e.g., transmitted, received and decoded, received but no

decoder found, etc.). Multiple log profiles are available for different message types, and the user determines the log profile configuration.

4. Communication interfaces.
 - a. OTCIXS is a two-way Non-DAMA (Demand Assigned Multiple Access) UHF Satellite Communications channel operating at 2400 BPS. The receive system(s) that receives and decodes the information are the ON-143(V)6 or (V)14 and KG-84A Crypto. OTCIXS was at one time the primary means for transmitting and receiving track information between units. It has recently been supplanted by Network and CSTTCP as the primary track distribution interface.
 - b. TADIXS A is a one-way (two-way for flag ships) DAMA UHF Satellite Communications channel operating at 2400 BPS. The receive system(s) that receives and decodes the information are the ON-143(V)6 or (V)14 and KG-84A Crypto. TADIXS A is the primary GENSER intelligence circuit for red and white non-organic data. TADIXS A can be used as a method for transmitting and receiving Mission Data Updates (MDUs) for Tomahawk strikes.
 - c. The Network channel is a TCP/IP based interfaced used to transmit tracks, operator-to-operator notes (OPNOTES), routes, and formations. The speed of transmission is dependent on the network setup and available bandwidth. The Network channel is the primary method of transmitting track data to other units when not using CSTTCP.
 - d. The CSTTCP channel is a TCP/IP based interface used to distribute tracks throughout the COP network when in a Wide Area Network (WAN) configuration. The architecture of nodes resembles a tree with the master machine (TOP COP) at the top and child nodes below. Each COP parent can have up to 5 connections (1 to a parent and 4 to children).
 - e. TRS is a TCP/IP interface and is used to receive Electronic Intelligence (ELINT) tracks from national sensors. Tracks are broadcasted via the Tactical Information Broadcast System (TIBS) and Tactical Related Applications (TRAP) Data Dissemination System (TDDS). If you are on a ship, you will need one of the following pieces of equipment to receive ELINT data, the ON-143(V)11 (old Tactical Receive Equipment (TRE)); OL-444 (new TRE); Commander's Tactical

Terminal (CTT) or the Joint Tactical Terminal (JTT). Certain types of aircraft can receive this data if they have the Multi-mission Advanced Tactical Terminal (MATT). The track types include priority tracks (missiles). The tracks are received in TAB-37 format and decoded by the TMS.

- f. The Serial interface is used for connections to other systems and also to synchronize the GENSER and SCI GCCS-M networks. The channel configuration is dependent on the destination.
 - g. Advanced Combat Direction System (ACDS). The ACDS interface is used on flagships for injecting tracks from the combat direction system into GCCS-M. The tracks come from various systems attached to the Combat Direction System including:
 - 1) LINK 11
 - 2) LINK 16
 - 3) SLQ-32
 - 4) Operator manual entry
 - h. Multi-Tadil Capability (MTC). MTC is used on flag and command ships to provide a means of directly inputting information from multiple types of LINKs into GCCS-M. The MTC channel provides the communication link between GCCS-M and the Air Defense System Integrator (ADSI), the link controller.
5. GCCS-M COP management
- a. Common Operational Picture (COP) Background
 - 1) The Common Operational Picture is a C4I management concept that has been used in several of our military forces for over five years. The concept and responsibilities are detailed in CFCSI 3151.01. It has been mandated by the Joint Chiefs that all U.S. forces now use the COP concept for track management.
 - 2) Each CINC controls his/her Common Operational Picture. The primary software tool used to manage the COP is GCCS, and more specifically, COP Synchronization Tools (CST).
 - 3) CST is a TCP/IP based communications protocol used to distribute tracks and export objects throughout the COP.

- 4) GCCS-M 4.0 uses the latest CST protocol, CSTTCP 5.4.7.0, but can still connect to nodes running legacy interfaces like CSTMDXNET 2.1.
 - 5) GCCS-M COP track management is management by negation. If a node (ship, station, command center, etc.) is given permission to add tracks into the COP, then it is assumed their data is valid. There is no stringent QA of data as in FOTC correlation.
 - 6) The COP architecture resembles a tree or a pyramid. At the top is the CINC, often referred to as the TOPCOP. Below that level are up to 5 children. Below each child can be up to 4 additional children and so on.
 - 7) The parent determines the permissions (add and delete tracks for example) for each child. The TOPCOP decides which of its children may have their own children (Secondary Configuration).
 - 8) The track database is synchronized at the top and bottom of every hour from the lowest child through the TOP COP utilizing DB Sync. In this way, all nodes in the architecture should have the same, or Common Operational Picture. CST will be covered in a later chapter.
6. NAVMACS II _Single Messaging Solution (SMS)
 - a. The Single Messaging Solution (SMS) provides state-of-the-art message store and delivery services for organizational and record message traffic in the GENSER and SCI enclaves.
 - b. The SMS architecture is a mixture of legacy GOTS systems and newer COTS packages.
 - c. SMS is comprised of the following systems: NAVMACS II, Exchange 2000, Outlook 2000, TurboPrep, and the Defense Message Dissemination System (DMDS).
 - d. Messages arrive via the following circuits: legacy circuits, Fleet SIPRNET Messaging (FSM), and the Defense Messaging System (DMS).
 - e. SMS provides eight different API sets for accessing, retrieving, injecting, and searching messages in the message repository. Web access is also supported via MS Outlook Web Access. In addition, the JavaMail API supports message access from Java platforms.

7. Defense Message Dissemination System (DMDS)
 - a. DMDS is a message profiler system used to disseminate a command's organizational messages. The messages can be passed to it by an e-mail system, such as the DMS, and/or passed to it from an AUTODIN Subscriber Terminal (AST), such as GateGuard. The two principle programs that make up DMDS are the Profiler Module and the Database Manager.
 - b. The Profiler Module operates as an automated mail client program, for example, as an automated version of a DMS Client. As a mail client program, the Profiler reads messages as they arrive in a particular account's mail folder and compares them against user provided profiles. The profiles specify where messages with some particular characteristic, such as ones that contain a specific text string, are to be disseminated. Messages passed to the Profiler from an AST are encapsulated into the body of a new e-mail message. Once encapsulated, the same profiles are used to determine dissemination requirements. The Database Manager is used to maintain the database employed by the Profiler Module.
 - c. DMDS is designed to disseminate an organization's military messages that are received at a particular host site. The system can be directed to disseminate newly arrived messages found in an arbitrary number of different disk directories and/or mail folders of an e-mail system. Rules for disseminating messages are defined by a set of profiles that the organization provides. If a particular host site serves more than one organization, each organization can provide the system with its own set of profiles. The system can apply each set of profiles independently to each message that it processes.
 - d. Dissemination is typically accomplished by forwarding individual messages to one or more e-mail addresses but the system can also be directed to copy messages into disk directories. Messages can also be disseminated to public or private mail folders. DMDS operates on a Microsoft Windows host. It interacts with the mail client interface, MAPI, provided by those operating systems. If (and only if) messages are to be disseminated by an e-mail system, then the site must install separately a mail service provider that conforms to the operating system's mail service interface.

DIAGRAM SHEET 3-3-3 **GENSER SMS SHIPBOARD ARCHITECTURE WITH DMS**

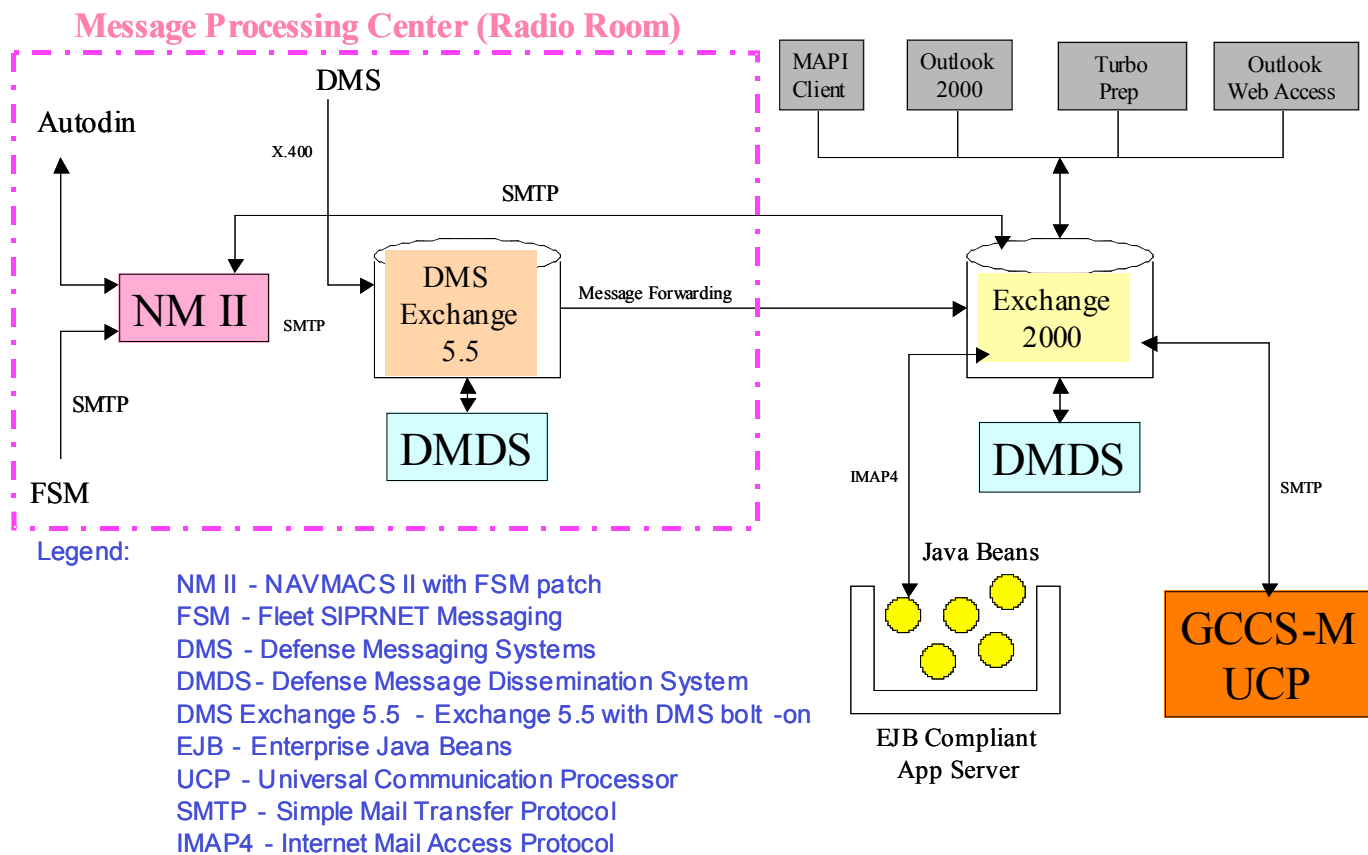


DIAGRAM SHEET 3-3-3 (cont)
GENSER SMS SHIPBOARD ARCHITECTURE WITHOUT DMS

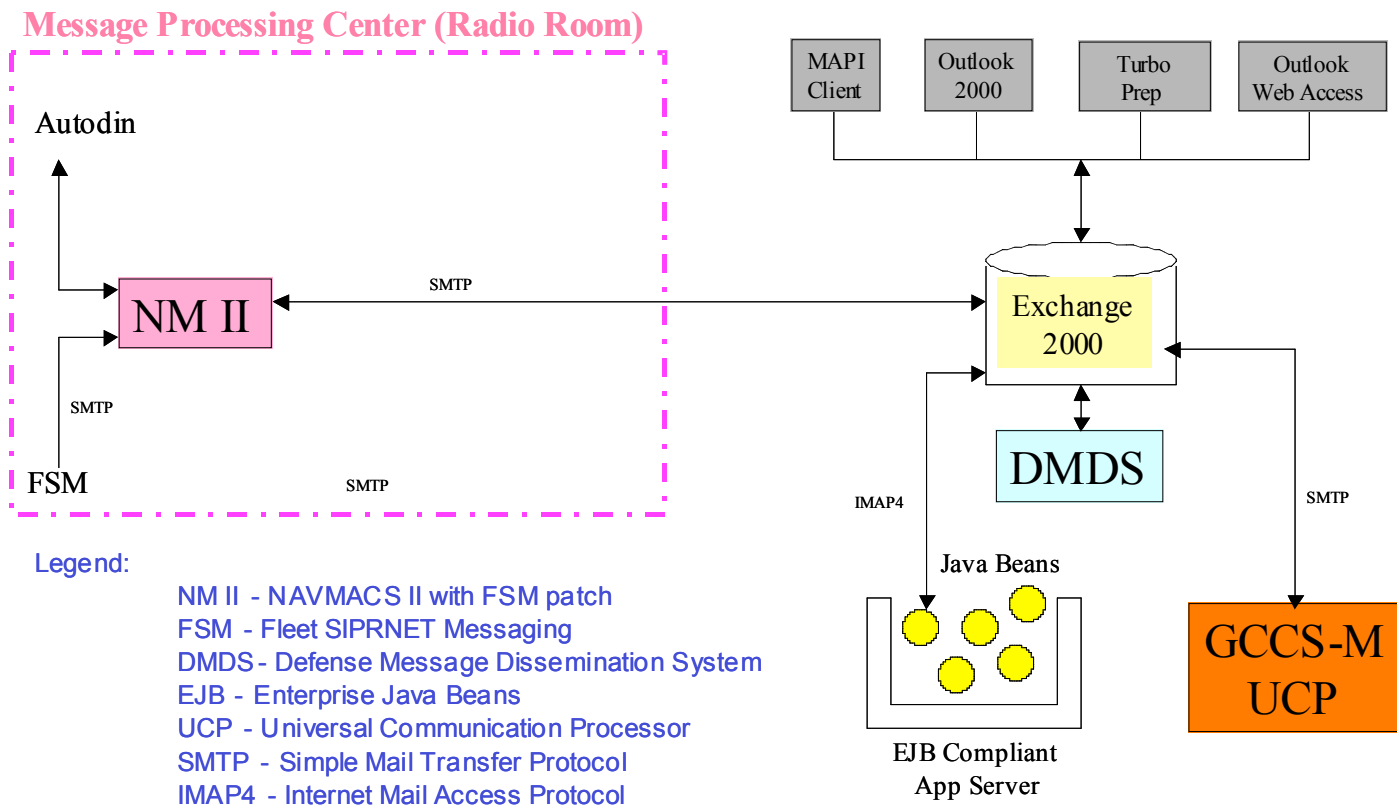


DIAGRAM SHEET 3-3-3 (cont)
GENSER SMS SHIPBOARD ARCHITECTURE
WITHOUT DMS USING NAVMACS V

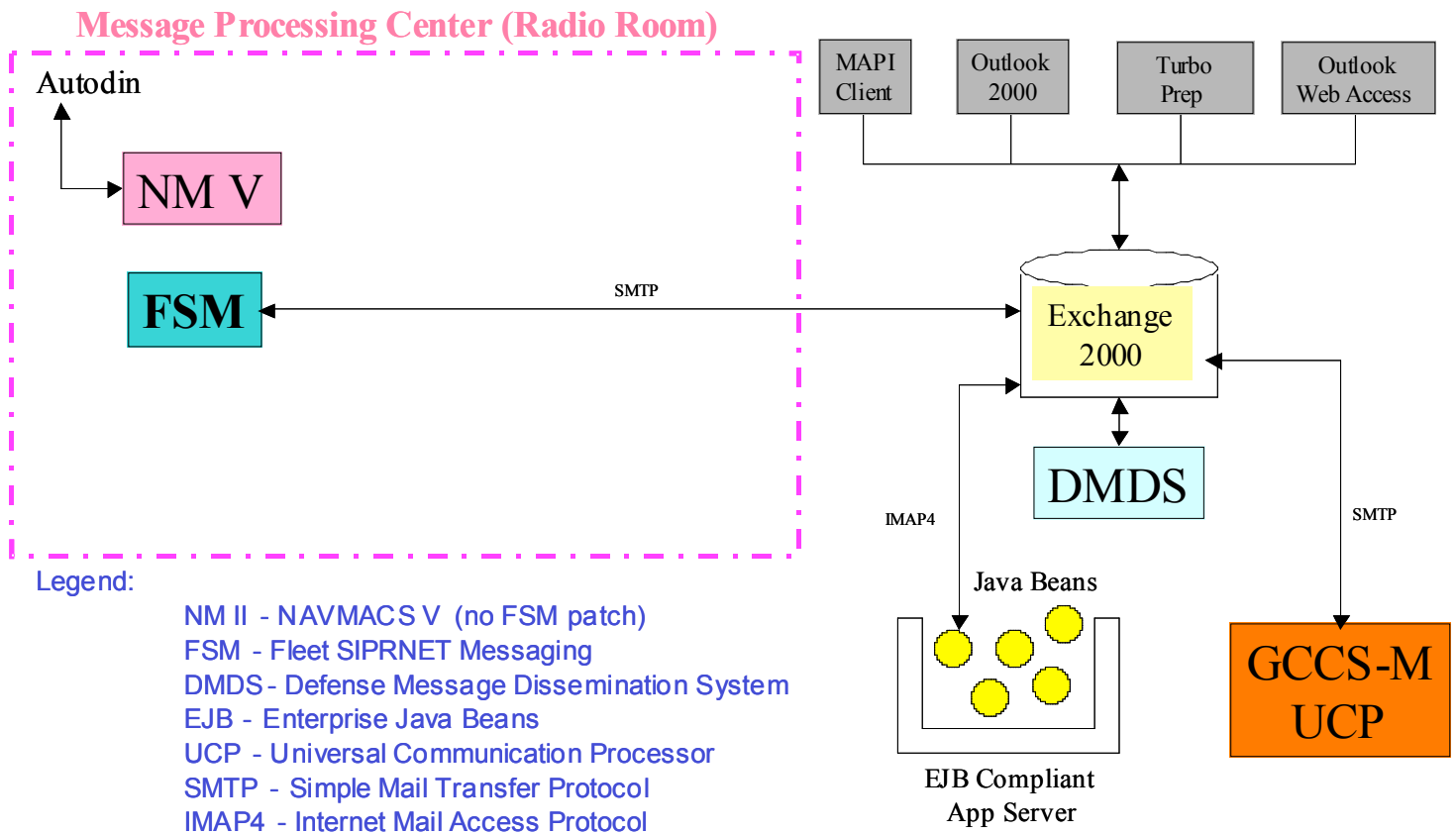
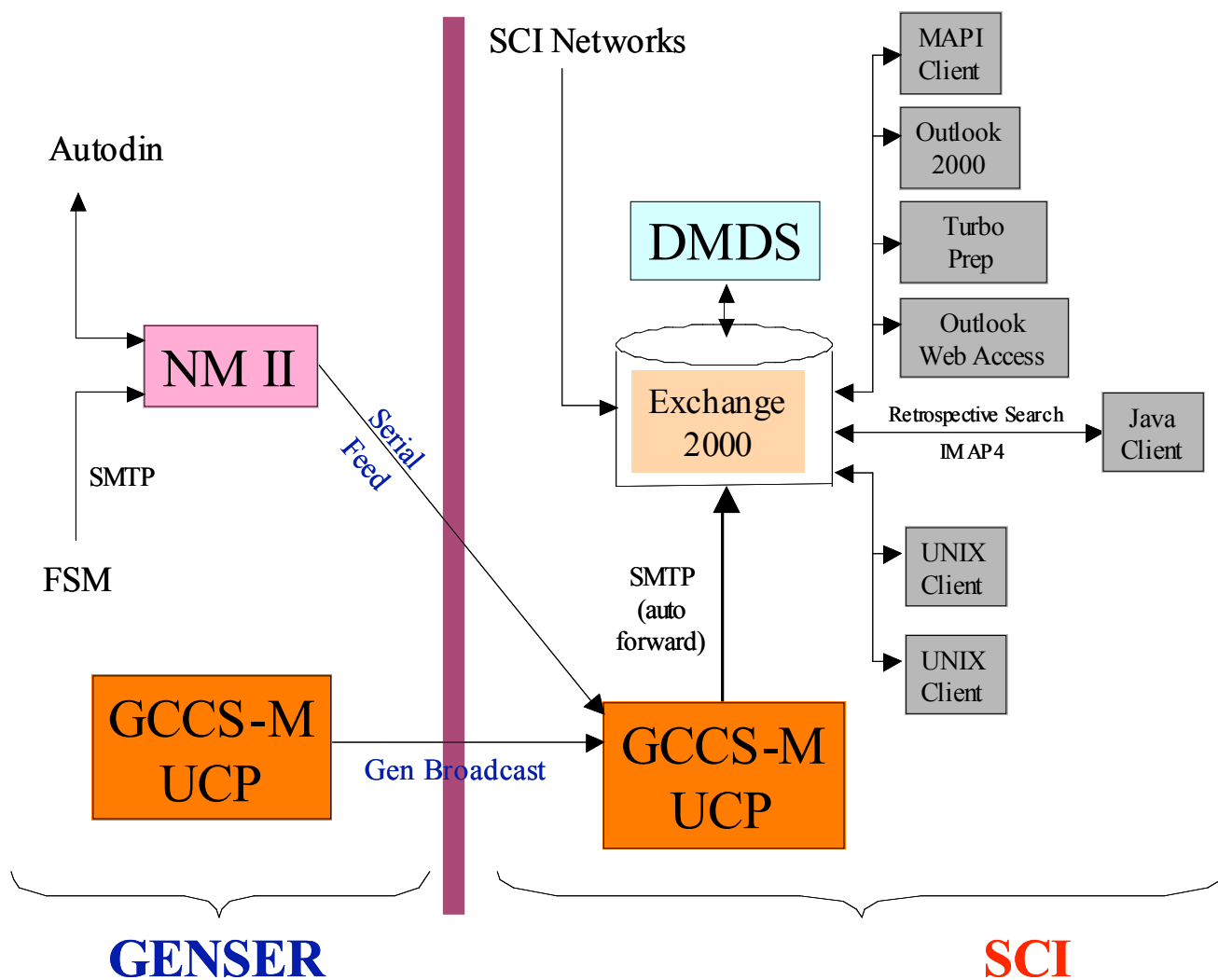


DIAGRAM SHEET 3-3-3 (cont)
SCI SMS SHIPBOARD ARCHITECTURE



INFORMATION SHEET 3-3-4

COMMUNICATIONS CHANNEL MANAGER

A. Introduction

This Information Sheet will provide an understanding of the Communication Channel Manager.

B. References

Online Embedded documentation

C. Information

The Universal Communications Processor (UCP) is the DII COE child component that provides portions of the core communications services capabilities for the COE. The current UCP implementation focuses on C4I communications and messaging services.

UCP provides services for adding/configuring communications interfaces, wrapping/unwrapping messages, logging incoming/outgoing message traffic (including headers), and interacting with a message generation/processing engine.

Five functions of the UCP/ Tactical Communications Processor (TCP) Server.

1. Link to incoming and outgoing communications – communications set-up performed at this server.
2. Communicates directly with NAVMACS.
3. Hosts the track database, Tactical Database Manager TMS MASTER.
4. Hosts the */h/data/global* file system.
 - The */h/data/global* file system is a shared file system that all the servers and clients on the GCCS-M LAN can access.
 - Software applications write files that all the servers and clients require to the */h/data/global* file system.
 - Configuration information is stored in the */h/data/global* file system.

5. As UCP master, serves the Universal Communication Manager.

Communications Channels

The UCP component provides centralized management of all communication channels in a UCP suite (the UCP server and its clients). The primary user interface is the "Channel Manager" window, where the operator can view all communications channels in the suite, the software interfaces which they represent (e.g., Network, Serial), the host on which they reside, the device that they are using (e.g., tty, network), and their current status (ON/OFF). From this window, the operator can add new channels, choosing from a list of available communications interfaces. The operator can also monitor the current traffic on the channel through a "Raw Data" window. The UCP brings with it a number of basic communications channels, including: Serial, Network, Mdx (Message Data Exchange), Email, and STU-III.

Message Handling

The UCP component is responsible for receiving message bodies, appending appropriate headers, queuing, and transmitting the complete message over the appropriate channel. On the incoming side, the header is parsed and the message body is supplied to UCP clients for decoding purposes

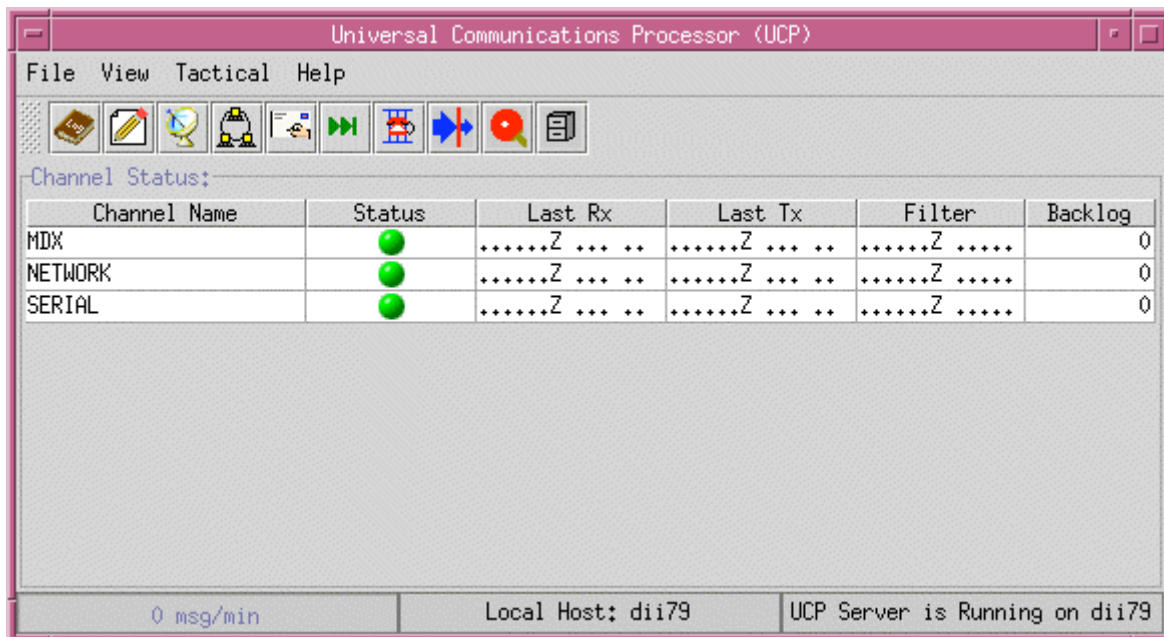


Figure 3-3-1

There are 10 icons available on the UCP main window. These icons provide quick and easy access to the most commonly used UCP applications.

- a. Opens the Incoming Message Log application - used to manage incoming message traffic.
- b. Opens the Message Editor application - used to create and edit messages.
- c. Opens the Channel Manager application - used to manage Comms channels.
- d. Opens the Network Host Table application - stores information about hosts with which the Network channel can communicate.
- e. Opens the Email Directory application - stores information about hosts with which the Email channel can communicate.
- f. Opens the Auto Forward Table application - used to automatically forward specific types of incoming and outgoing messages to selected destinations.
- g. Opens the STU III Directory application - used to view a list of organizations that are set up to receive messages sent with a STU III device.
- h. Opens the InputMessageFilter Table application - used to filter out specific incoming messages based on specific criteria.
- i. Opens the WAN Status application - used to list all responding host names in the system.
- j. Opens the Archive application - used to archive and restore UCP application data.

Channel Status box

The UCP main window displays channel information if the Channel Status option is checked under the View menu. This feature displays the contents of the Channel Status window on the UCP Main window. This feature is for viewing purposes only. You must still run the Channel Status application to interact with the channels.

Status bars (bottom of window)

Far left - displays the number of messages being received per minute

Center - displays the name of the local host machine

Far right - displays the status of the UCP server (Running/Down)

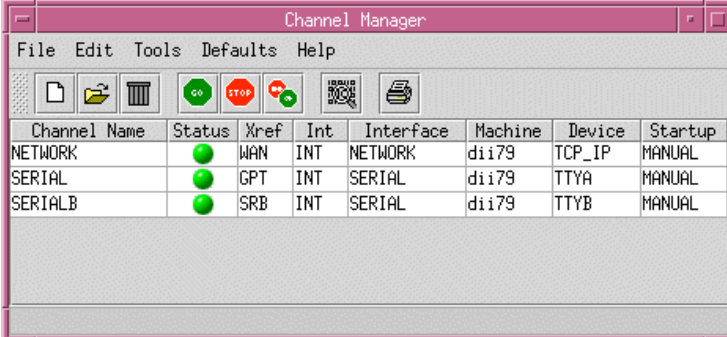
File Menu Options:

Exit: Exit and close the UCP main window.

View Menu Options:

Channel Status: ON (checkbox filled) - The contents of the Channel Status will be displayed in the UCP main window. OFF (checkbox empty) - The UCP main window will be collapse and show only the main-menu bar, the application icons, and the status bars.

Tactical Menu Options: The Tactical menu options consist of—Channel Manager, Channel Tables, Message Log, Message Tables, Message Editor, WAN Status, Channel Status, and Archive. Descriptions of each of these options can be found under the Tactical Comms item on the main UCP Users Manual (UM) index.



The screenshot shows a window titled "Channel Manager" with a menu bar (File, Edit, Tools, Defaults, Help) and a toolbar with icons for file operations and status. Below the toolbar is a table with the following data:

Channel Name	Status	Xref	Int	Interface	Machine	Device	Startup
NETWORK	●	WAN	INT	NETWORK	dii79	TCP_IP	MANUAL
SERIAL	●	GPT	INT	SERIAL	dii79	TTYA	MANUAL
SERIALB	●	SRB	INT	SERIAL	dii79	TTYB	MANUAL

Figure 3-3-2

Channel Manager Window Fields

Channel Name:

Unique channel name

Status:

Green - channel is running (ON); messages are sent or received based on the configuration.

Red - channel is not running (OFF); messages are not sent or received.

Xref:

Unique three-character Comms cross-reference code.

Int: (INTERNAL)

Checked ON for all channels, except a network-based channel being used for a TMS WAN broadcast.

Interface:

Comms interface for the channel.

Machine:

Name of the machine used to transmit or receive messages on this channel.

Device:

Device name used for this channel.

Startup

AUTO - channel started automatically at system startup.

MANUAL- channel started by operator, using the Start menu option.

Network Host Table Window

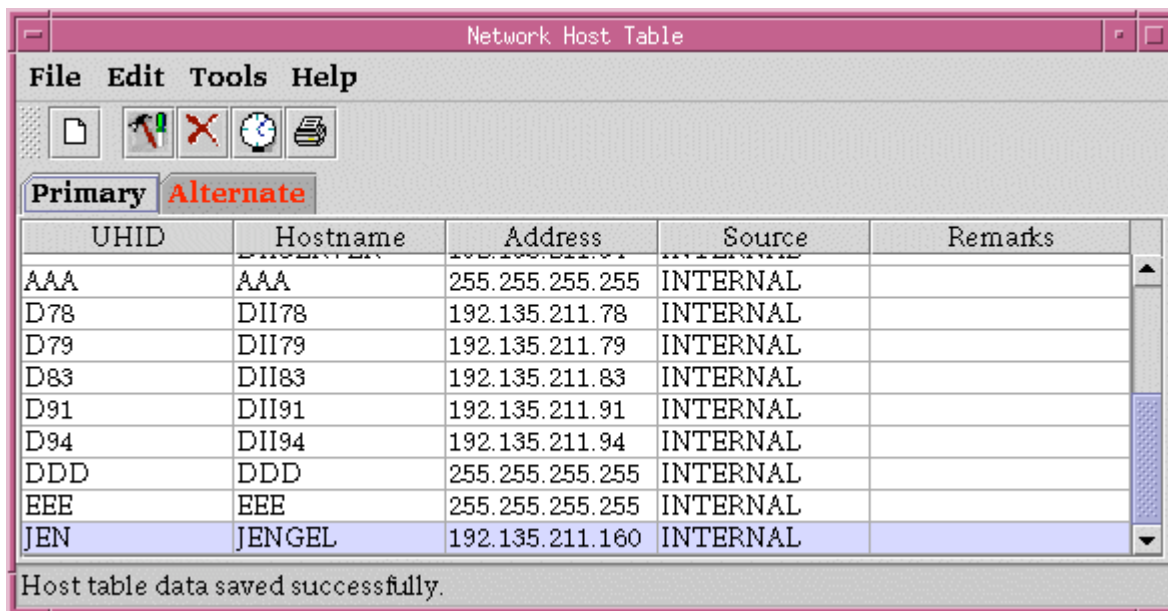


Figure 3-3-3

In order for a machine to communicate to another machine (host), over a Network channel, information about that host must be listed in the Network Host Table. Information that must be included in this table: host's Unique ID (UHID), name, and IP address, and whether the host is internal or external to your site.

When using a Network channel, UCP uses this table to lookup information about a host before receiving/transmitting data to/from that host. The operator may define two tables (Primary

and Alternate) for which UCP may use for lookup. Using the Network Host Table application, a user with sysadmin privileges can manage (i.e., add, edit, delete) these tables. Non-sysadmin users can only view the table information.

Network Host Table Window Fields

UHID

Unique host name ID, a three-character code that *uniquely* identifies the host.

Hostname

The *full* name of the host: each host must be unique.

Address

Numerical address of the host machine.

Source

INTERNAL - hostname is internal to a site.

EXTERNAL - hostname is external to a site.

Remarks

Remarks about the host.

File Menu Options:

NAME

Comms interface.

INTERFACE

Interface Type (examples: SERIAL, AMP, etc.).

MACHINE

Assigned name for the workstation being used for Comms with this interface.

PORT

Workstation port used for Comms for this interface.

BAUD

Baud rate used for Comms on this interface.

PARAMETERS

Data size, followed by the parity, followed by the stop bits for the interface. The data size (a number from 5 to 8) is displayed first, followed by a dash, the parity (N=None, E=Even, O=Odd), another dash, and then the stop bits (1, 1.5, or 2).

DATA

Code for the data type used for the interface. Data type codes are:

Code	Data Type
ASC	ASCII
BAU	BAUDOT
BIN	BINARY

XON/XOFF

Shows whether the XON function is turned ON or OFF, followed by a slash. Whether the XOFF function is turned ON or OFF.

R/X

Shows whether transmissions can be received on this interface (Y = Yes, N = No). Followed by a slash. Whether transmissions can be sent on this interface (Y = Yes, N = No).

A/SRC

Shows whether this interface is set to AUTOSTART (Y = Yes, N = No), followed by a slash, next a code for the source for the interface.

If the source is Intel, two dots are displayed.

If the interface has a Link source, it displays a L1, L2, L3, or L4. Similar abbreviations are used for other sources.

The WAN Status application is used to verify communication status with selected host names.

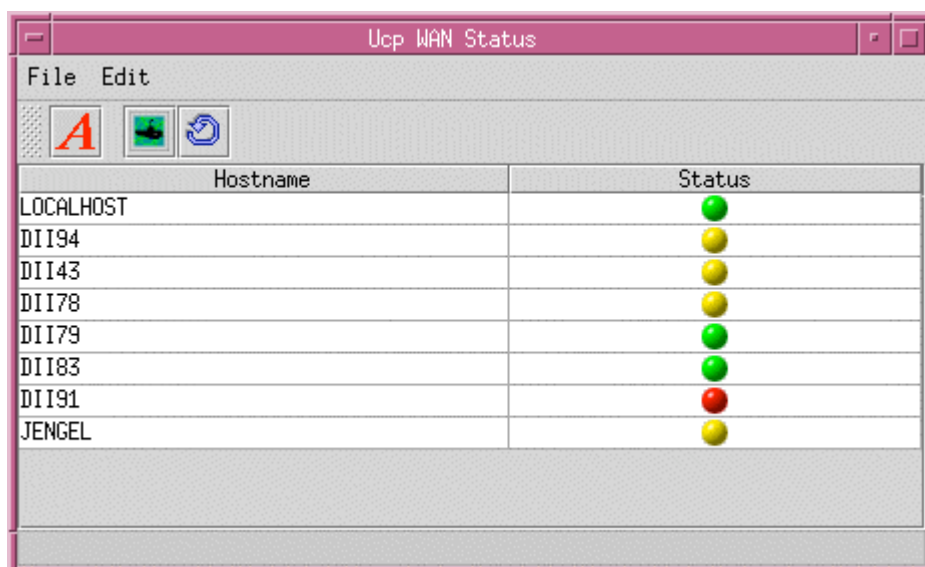


Figure 3-3-4

INFORMATION SHEET 3-3-5

COP SYNC TOOLS (CST)

A. **Introduction**

This information sheet will provide the trainee with an understanding of CST tools.

B. **References**

1. Online Embedded documentation
2. CST 4570P8 User Manual Appendix

C. **Information**

1. COP Synchronization Tools (CST)
 - a. CST supports tactical commanders by providing an automated method of transferring and synchronizing data for a common operating picture across the battle space.
 - b. It uses fielded COE-based systems and conventional Department of Defense (DOD) communications capabilities. CST interfaces allow the near real-time exchange of track data between the sites participating in the CST network over a wide area network (WAN). They enable receipt of raw and processed track information and distribution of track correlation results throughout the CST network.
 - c. The CSTTCP and CSTSTCP channel types work in basically the same way, with the difference in the two being that the CSTSTCP is a secure channel type. Both the CSTTCP and CSTSTCP channel types use TCP/IP as their underlying network transport mechanism. Using TCP/IP requires all connections be distinct point-to-point connections between two points. Due to this and the fact that any one CSTTCP or CSTSTCP interface can have no more than five directly connected child nodes, the flow of information over a CSTTCP or CSTSTCP channel can be represented by an inverted tree diagram, in which the child of one node may itself be the parent of another node. A parent or master node provides data to its child nodes. Child nodes may also provide data to their parent node to transmit data to other participating nodes.

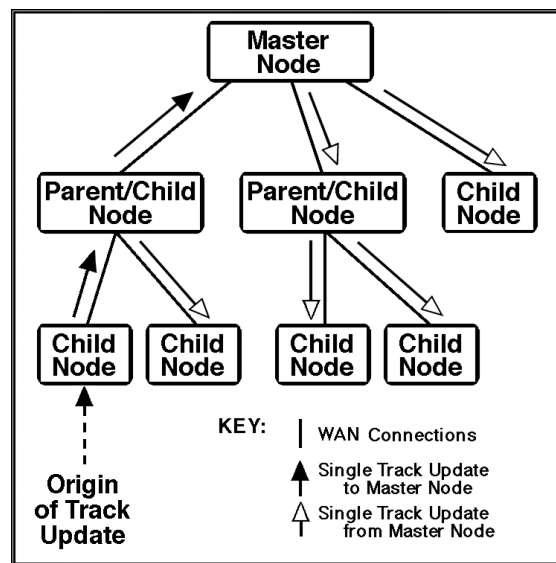


Figure 3-3-5

2. The CSTMDPV2 interface is a multicast-based protocol to send data to and receive data from other nodes participating in the CST network. However, due to the efficiency of the multicast protocol, this interface allows for a maximum of 1000 child nodes to connect to a single parent node, keeping the inverted tree only one level deep

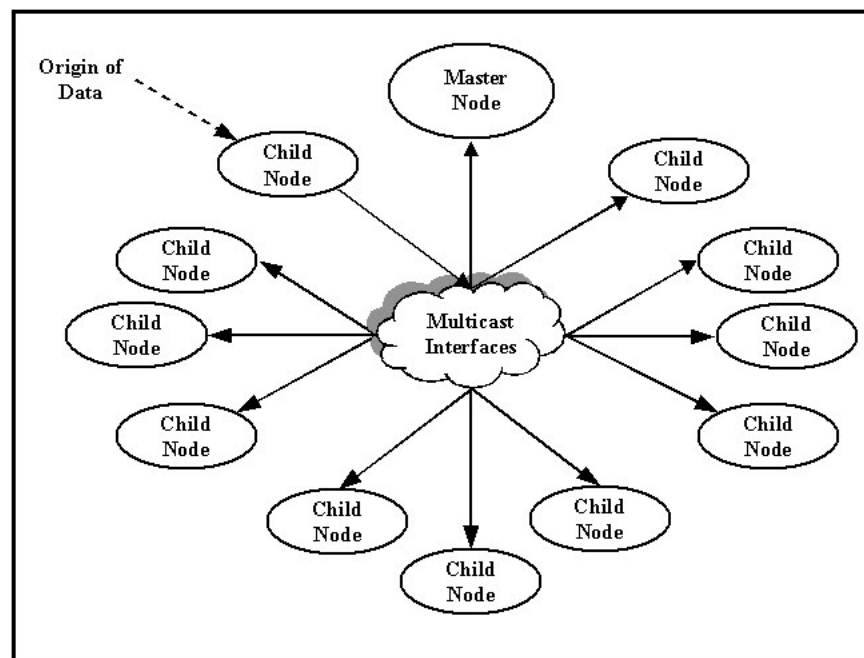


Figure 3-3-6

3. With multicast, when any one node transmits a piece of data, the information is essentially passed to the network and its associated network hardware for proper delivery to all nodes having indicated an interest in the piece of information. Unlike the CSTTCP and CSTSTCP interfaces, which require every piece of data to be passed individually to each participating node, multicast interfaces are efficient because a single transmission of data from one node is automatically delivered to all participating nodes. The various pieces of the network hardware ensure the data is delivered correctly. Because of this lower data transmission overhead requirement, the CSTMDPv2 interface will require significantly less network bandwidth and enable a master or parent node to provide data to a maximum of 1000 child nodes with the same amount of work as if sending to a single TCP/IP site.
4. Unfortunately, at many sites either the network hardware is not modern enough to support the use of multicast as a transmission medium or multicast support has not been enabled. The latter is the case for most wide-area military networks in use today (like SIPRNET). However, in situations where data needs to be transmitted between many nodes within a given command or location, it is usually not difficult to enable multicast support within the network hardware and allow for the use of the multicast interface types. Their use can help to lower the overall network usage levels.
5. SITREP messages are automatically sent out from the child to the parent node every 30 minutes (on the half hour) and are intended to bring the local track picture up to date with other participants on the WAN. However, participating nodes do not send ambiguity tracks, local tracks, or terminal tracks to other participating nodes. When necessary, CST handles deletions of track data via drop-track messages.
 - a. The COP Sync Tools menu enables a user to perform the following tasks:
 - View the configuration and status of each node
 - View graphical representations of local and remote CST network topologies
 - Restrict tracks
 - Distribute tracks
 - Control how often owntrack updates are distributed
 - Down sample link association updates
 - Take ownership of a track

- Import and export an object (Air Tasking Order [ATO], Air Coordination Order [ACO], overlay, stored map, stored plot control, and Position and Intended Movement Track [PIMTRACK])
- Perform a manual track database synchronization
- Set the DFLM LAN master host

6. CST NODE LIST Window

- The CST NODE LIST window is updated dynamically as the CST network adds or deletes a node or as the status of a node changes.

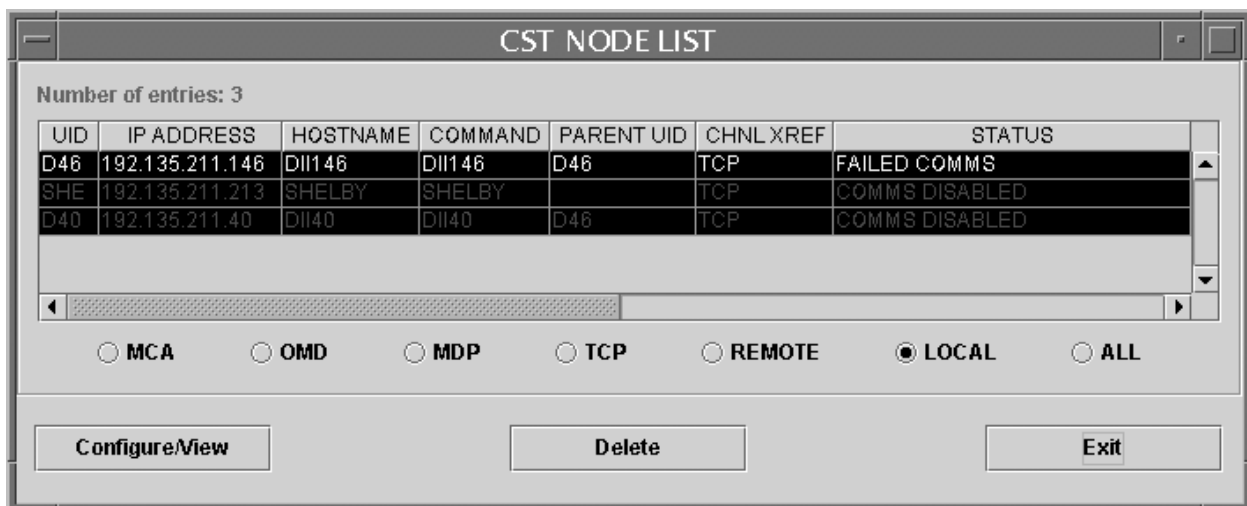
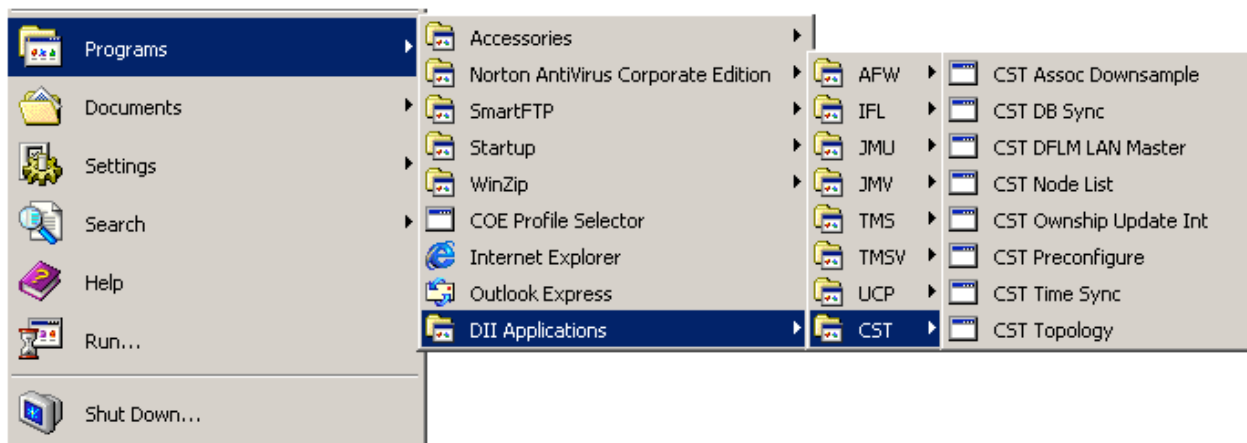


Figure 3-3-7

- b. The CST NODE LIST window displays an entry under the following column headings for each node in the list:

UID

Unique identifier of the node

IP ADDRESS

IP address of the node

HOSTNAME

Host name of the node

COMMAND

Local command of the node

PARENT UID

UID of the parent node

PARENT IP ADDRESS (optional)

IP address of the parent node

CHNL XREF

Unique three-character communications cross-reference code for the channel

STATUS

Status of the node, from among the following:

- COMMS DISABLED – The communication path to the node is disabled (appears red).
- CONFIGURATION PROVIDED – The node has been configured and has requested to log on to the parent node, but the CST node list manager has not received notification that the login was successful (appears yellow).
- ESTABLISHING COMMS – The node is awaiting connection to a node (appears yellow).
- FAILED COMMS – The node has tried for more than 15 minutes to connect to a node that is not accepting the connection (appears white).
- PARTICIPATING – The node is active (appears green).
- REQUESTING CONFIGURATION – The node has requested participation and is awaiting configuration (appears cyan). The node is considered to have

requested participation when it activates one of the following CST channels: CSTTCP, CSTMCAST, or CSTMDPV2.

- STATUS UNKNOWN – The node does not fit into any other category (appears **magenta**).

IN FILTER (optional)

Filter that determines which tracks are received by the node from its parent

OUT FILTER (optional)

Filter that determines which tracks are distributed by the node to its parent

PERMISSIONS (optional)

Operations that the node is allowed to perform, from among the following options. (If **no** permissions are assigned, the node can only view the data distributed by the CST network.)

- A (ADD) – Node can add (distribute) tracks via the CST network.
- D (DELETE) – Node can delete (restrict) tracks from the CST network.
- T (TAKE OWNERSHIP) – Node can assume ownership of tracks created by another node. Once ownership is assumed, the node can modify or delete tracks as if they were its own.
- U (UPDATE) – Node can modify tracks that were created by another node.
- M (MERGE) – Node can merge tracks that were created by another node.
- C (SECONDARY CONFIGURATION MASTER) – Allows the node to configure other nodes below it (child nodes, grandchild nodes, and so on).

PARENT SEND TO (optional)

IP address used in transmitting data to parent node

NODE SEND TO (optional)

IP address used in transmitting data to child node

NOTE: The bottom of the CST NODE LIST window contains several filter options, which enable the user to select the type of node list entries to display. By default, all local channel cross-references are displayed. To choose another filter, select one of the following options:

- MCA – To display only CSTMCAST channel cross-references
- OMD – To display only CSTMDP1WY channel cross-references
- MDP – To display only CSTMDPV2 channel cross-references
- TCP – To display only CSTTCP channel cross-references
- REMOTE – To display only remote channel cross-references
- LOCAL – To display only local channel cross-references
- ALL – To display all channel cross-references

7. CST IE (import/export) CONFIGURATION Window

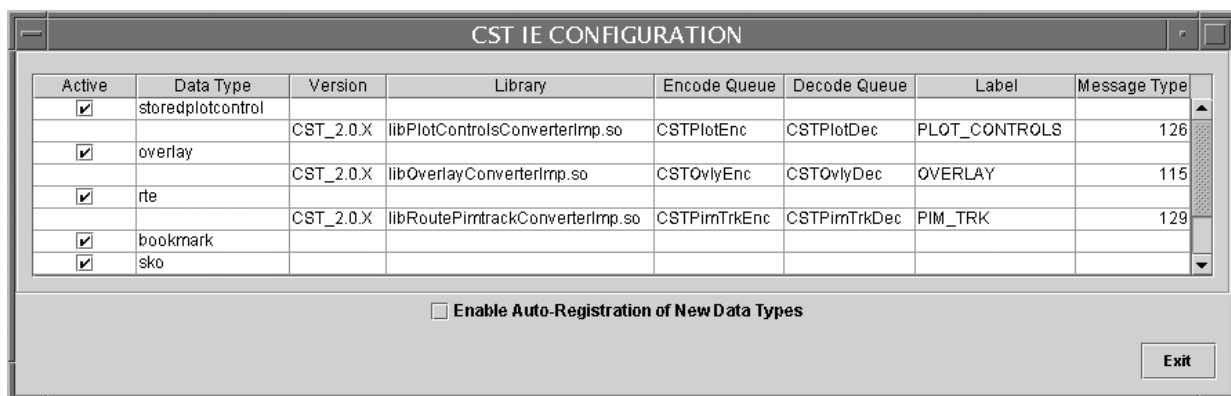


Figure 3-3-8

The object types available for import or export are as follows (as listed in the Label column):

- ATO – Air tasking order (this includes ACOs, which if input into the system separately would not get sent)
- OVERLAY – Overlay
- STMAP – Stored map
- PLOT_CONTROLS – Stored plot control
- PIM_TRK – Position and intended movement track

8. CONFIGURE NODE Window (with CST and TMS Tabs)

The figure shows two screenshots of the 'CONFIGURE NODE' window. The left screenshot is the 'CST' tab, showing 'Node ID Info' with fields for IP ADDR (192.135.211.40), HOSTNAME (DII40), COMMAND (DII40), UID TRIGRAPH (D40), and CHNL XREF (TCP). Below it is 'Parent Node ID Info' with a dropdown for UID TRIGRAPH (D46) and a text field for IP ADDR (192.135.211.146). The right screenshot is the 'TMS' tab, showing 'Filter Attributes' with 'IN COMMS FILTER' and 'OUT COMMS FILTER' both set to '<NONE>', and radio buttons for TBM (RAW, FUSED, ALL). It also has a checkbox for 'Filter Local Tracks Only'. Below is 'Permission Attributes' with checkboxes for UPDATE, DELETE, MERGE, TAKE OWNERSHIP, and SECONDARY CONFIG. Both screenshots have 'OK' and 'Cancel' buttons at the bottom.

Figure 3-3-9

On the CST tab, the fields in the Node ID Info box are not editable; you may wish to verify that the information for each of the following fields is correct.

- IP ADDR – IP address of the node
- HOSTNAME – Host name of the node
- COMMAND – Command of the node
- UID TRIGRAPH – UID trigraph of the node
- CHNL XREF – Channel cross-reference of the node

9. CST PRECONFIGURATION Window

The figure shows the 'CST PRECONFIGURATION' window. It displays 'Number Of Entries: 0001' and a table with the following data:

UID	IP ADDRESS	HOSTNAME	COMMAND	PARENT UID	CHNL XREF	PARENT IP ADDRESS
D58	192.135.211.58	DII58	JOTS37CMD	D60	CST	192.135.211.60

At the bottom of the window are three buttons: 'View', 'Delete', and 'Exit'.

Figure 3-3-10

The CST PRECONFIGURATION window is updated dynamically as entries or changes to entries are added to the CST preconfiguration database. Entries can only be added to the CST preconfiguration database using the CST NODE LIST window. The Number of Entries field indicates the total number of nodes in the list. The CST PRECONFIGURATION window displays an entry for each node in the list under the following column headings.

UID

Unique identifier of the node

IP ADDRESS

IP address of the node

HOSTNAME

Host name of the node

COMMAND

Local command of the node

PARENT UID

UID of the parent node

PARENT IP ADDRESS

IP address of the parent node

CHNL XREF

Unique three-character communications cross-reference code for the channel

IN FILTER (optional)

Filter that determines which tracks are received by the node from its parent

OUT FILTER (optional)

Filter that determines which tracks are distributed by the node to its parent

PERMISSIONS (optional)

Operations that the node is allowed to perform, from among the following options. (If *no* permissions are assigned, the node can only view the data distributed by the CST network.)

- a. A (ADD) – Node can add (distribute) tracks via the CST network.
- b. D (DELETE) – Node can delete (restrict) tracks from the CST network.
- c. T (TAKE OWNERSHIP) – Node can assume ownership of tracks created by another node. Once ownership is assumed, the node can modify or delete tracks as if they were its own.
- d. U (UPDATE) – Node can modify tracks that were created at another node.
- e. M (MERGE) – Node can merge tracks that were created at another node.
- f. C (SECONDARY CONFIGURATION MASTER) – Allows the node to configure other nodes below it (child nodes, grandchild nodes, and so on) and nodes that are requesting configuration.

PARENT SEND TO (optional)

IP address used in transmitting data to parent node

NODE SEND TO (optional)

IP address used in transmitting data to child node

10. CST Topology

NOTE: The CST NODE LIST and CST Topology windows depict CST connectivity. Although these windows may indicate a problem with a node, they do not identify specific network problems, such as down routers.

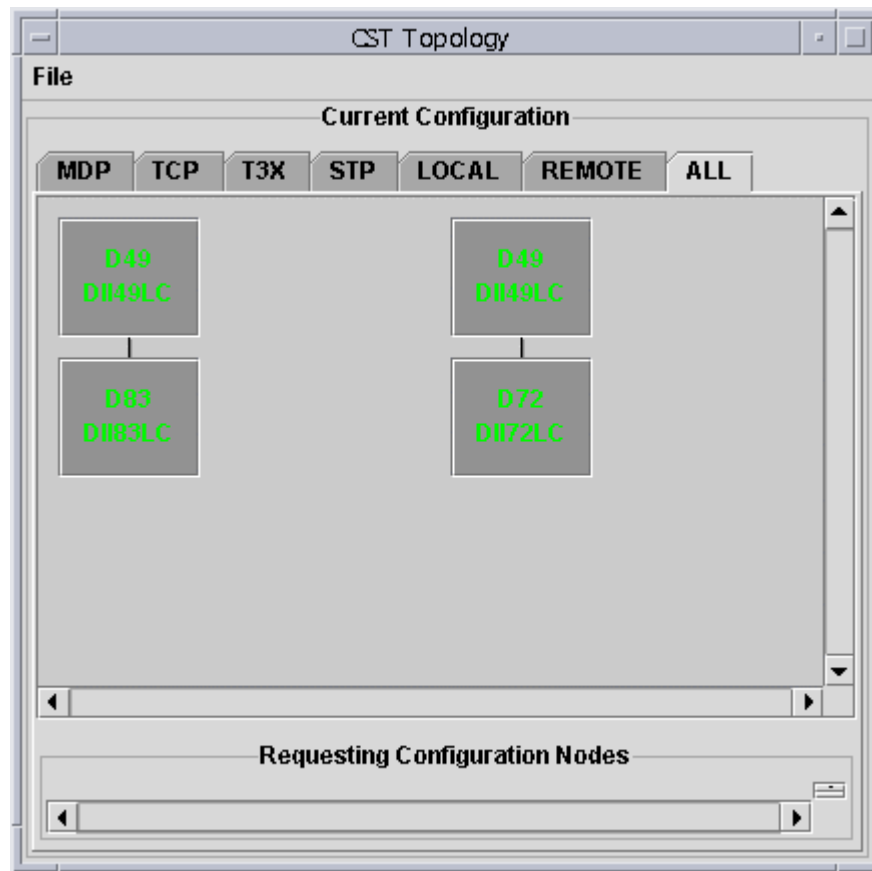


Figure 3-3-11

The CST Topology window is updated dynamically as the CST network adds or deletes a node, or as the status of a node changes.

10. Troubleshoot Tracks Using Node Status Indicators

a. Node Status Indicators

- (1). The color-coding and status information in the CST NODE LIST window can be used to determine whether there is a problem with your CST interface or whether a network problem exists. The color-coding and status indicators are explained in Table 1.

b. Node Status Indicators

Own Node Color/Status	Parent Node Color/Status	Child Node Color/Status	Meaning & Recommended Action
Red/ COMMS DOWN	—	—	CST interface is not running. It is either down or has been turned off and needs to be restarted.
Green/ PARTICIPATING	Red /COMMS DOWN	—	Network connectivity between your node and the parent node is no longer available. Contact the appropriate network or technical personnel.
Green/ PARTICIPATING	—	Red/ COMMS DOWN	Network connectivity between your node and the child node is no longer available. Contact the appropriate network or technical personnel.
Green/ PARTICIPATING	—	—	Your CST interface is working properly, but you have lost general network connectivity. Contact the appropriate network or technical personnel.

11. Adding a CST Channel

- a. To add a CST channel (CSTTCP, CSTSTCP, or CSTMDPv2):
- b. Open the Channel Manager window

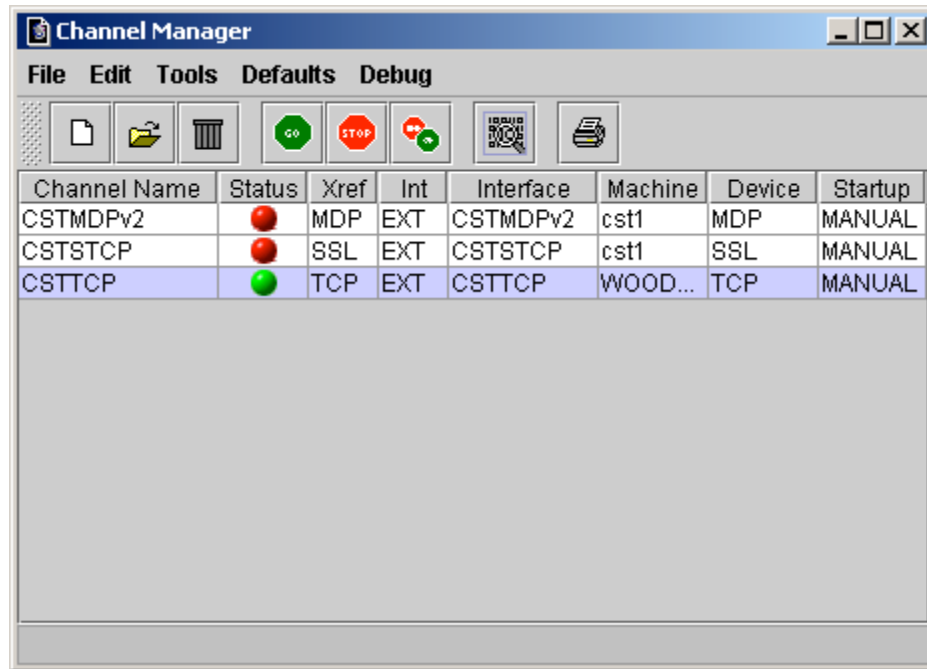


Figure 3-3-12

- c. Click the Add Channel icon . The Add Channel window appears.

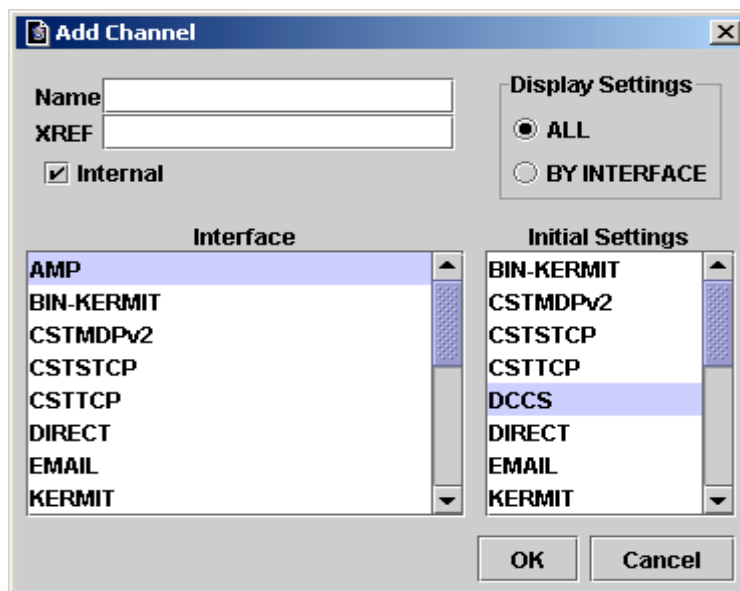




Figure 3-3-13

- d. In the **Name** box, enter a name for the channel. The name is restricted to alphanumeric, underline (_), and hyphen (-) characters.
- e. In the **XREF** box, enter a unique three-character communications cross-reference code for the channel.
- f. Verify that the **Internal** check box is selected.
- g. In the **Display Settings** box, verify that **ALL** is selected.
- h. In the **Interface** list, select a CST channel (CSTTCP, CSTSTCP, or CSTMDPv2).
- i. The type of channel you select automatically determines the selection in the Initial Settings list.
- j. Click **OK**.
- k. The Channel Manager window is updated, listing the new CST channel.
- l. Type of start-up specified for the channel, either AUTO (starts automatically upon system start-up) or MANUAL (must be started manually by selecting the channel and clicking )

12. Configuring and Activating a CSTTCP Channel

CAUTION: When you apply any changes to an active CSTTCP channel (a channel with a green **Status** in the Channel Manager window), the channel is automatically deactivated and then restarted with the updated settings. This action can cause messages that are en route to be lost.

- a. To configure and activate a CSTTCP channel:
- b. Open the Universal Communications Processor (UCP) window.
- c. Click the Channel Manager icon .
- d. The Channel Manager window appears.

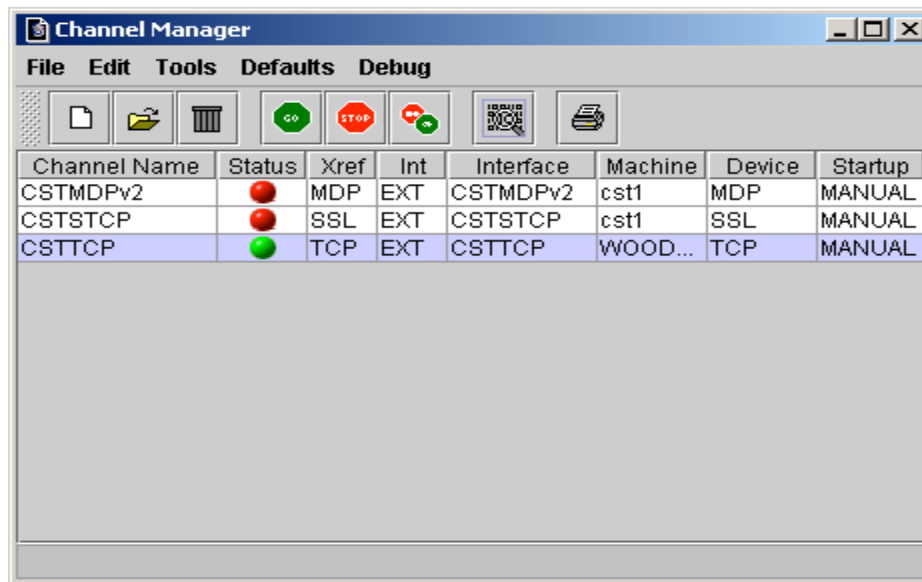


Figure 3-3-14

- e. Select a channel with a CSTTCP interface from the list, then click the Edit Channel



- f. The Edit CSTTCP Channel window appears:

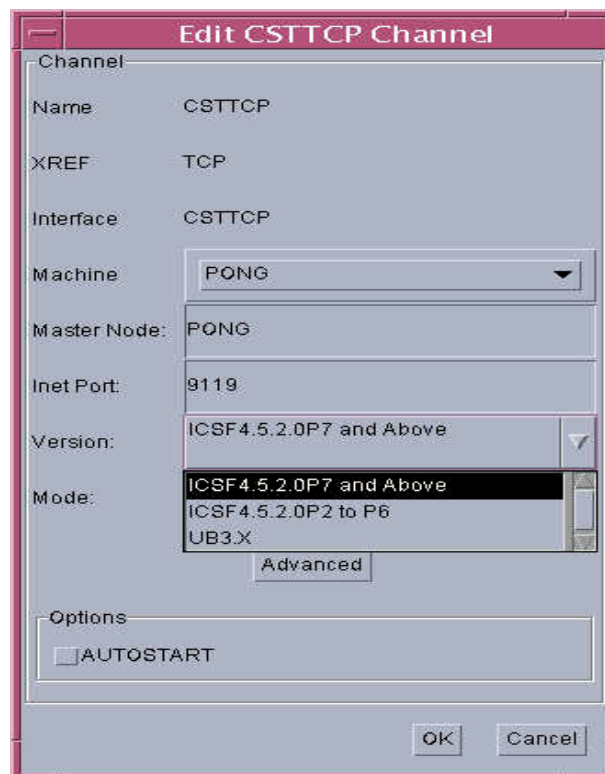



Figure 3-3-15

- g. In the Machine box, click the drop arrow and select the workstation that is running the CSTTCP channel. This could be the workstation name, or if your workstation is a client to another workstation, it would be that workstation's name.
- h. In the Master Node box, enter the host name of your master node. If your node is the master node, the entry in the Master Node box must match the entry in the Machine box. (The Standard Operating Procedures [SOP] at your site should provide information on the role of your node and the host name of the master node.)
- i. To change the INET port value, enter the port value, as designated by the master node, in the Inet Port box. The default value is 9119.
- j. Click the Version drop box and select the version of ICSF or UB software your recipient is using from the list of choices (UB3.X, ICSF 4.5.2.0P2 to P6, or ICSF 4.5.2.0P7 and Above).
- k. Older versions of CST with CST2.X listed in this field can communicate with UB3.X, and CST4.X can communicate with ICSF 4.5.2.0P2 to P6.
- l. To prevent lost data, it's best to run the newest version. For example, if a server with ICSF 4.5.2.0P7 is running the ICSF 4.5.2.0P7 and Above channel, the new data structure for P7 will be preserved and transmitted via this channel. But if this ICSF4.5.2.0P7 server is running the ICSF 4.5.2.0P2 to P6 channel, the other CST nodes connecting to this channel will not get new data such as track URLs, short name for General Tracks, and some other data.
- m. In the Mode box, click the drop arrow and choose the transmission mode. If the version selection is ICSF 4.5.2.0P2 to P6 or ICSF 4.5.2.0P7 and Above, the available modes are Default, Oneway, or NAT. If the version selection is UB3.X, the available modes are Default, Oneway, and TTWCS. Parent and child nodes should always have the same mode selections.
- n. If you choose default, your workstation will be set to send and receive transmissions directly from your parent and child connections.
- o. If you choose Oneway and your workstation is the master node, your workstation will be set to send CST transmissions directly to your child nodes. If you choose Oneway and your workstation is not the master node, your workstation will be set to

receive transmissions from your parent node, but your workstation will not be allowed to send transmissions to the parent node.

- p. Choose NAT (Network Address Translation) if your network is set up to communicate through routers. This choice allows your workstation to send and receive transmissions.
- q. Choose TTWCS to enable additional processing required between a GCCS-M system and a Tactical Tomahawk Weapons Control System (TTWCS). This mode assumes all data originates from GCCS-M and adds history synchronization between GCCS-M and TTWCS.
- r. Do one of the following, depending on whether you want the channel to start automatically or manually:
 - To ensure the CSTTCP channel starts automatically upon system startup, select the **AUTOSTART** check box.
 - To set the CSTTCP channel for manual activation, clear the **AUTOSTART** check box. (To start the CSTTCP channel manually, select the CSTTCP channel from the list of channels in the Channel Manager window and click  from the toolbar.)
- s. Click **OK**.
- t. If the channel is already activated, clicking **OK** automatically deactivates the channel and restarts it with the new settings.
- u. When the CSTTCP channel is activated, your node sends a message to the master node requesting configuration in the CST network. The master node must then configure your node before you are allowed to participate fully in the CST network. To check the status of your node at any time, use the **CST Node List** option.
- v. Once your node is configured, if communication between your node and the parent node is disrupted, CST attempts to reconnect to the parent node for a threshold assigned by the configuring node (default of 5 minutes). If after this threshold has expired CST is still unable to connect to the parent node, CST then attempts to connect to the master node as configured in the Edit CSTTCP Channel window.
- w. If your node becomes out of sync with the master node by five minutes or more, a warning window appears, prompting you to time sync with the master node.

- x. If you turn the CSTTCP channel off and back on or reboot your local machine, your node sends another message to the master node to request configuration.

13. Setting Advanced Configuration Features for a CSTTCP Channel

NOTE: Do not perform any of the following advanced procedures without first coordinating your actions with the CST administrator at the master node and the ICSF system administrator at your node. Failure to do so can produce unexpected results, such as the channel not remaining activated or the system indicating that the channel is properly configured when it is not. In most cases, each node should use the default settings provided in the Advanced CSTTCP Configuration window. (These values are set during CST installation.)

- a. To set advanced configuration features for a CSTTCP channel:

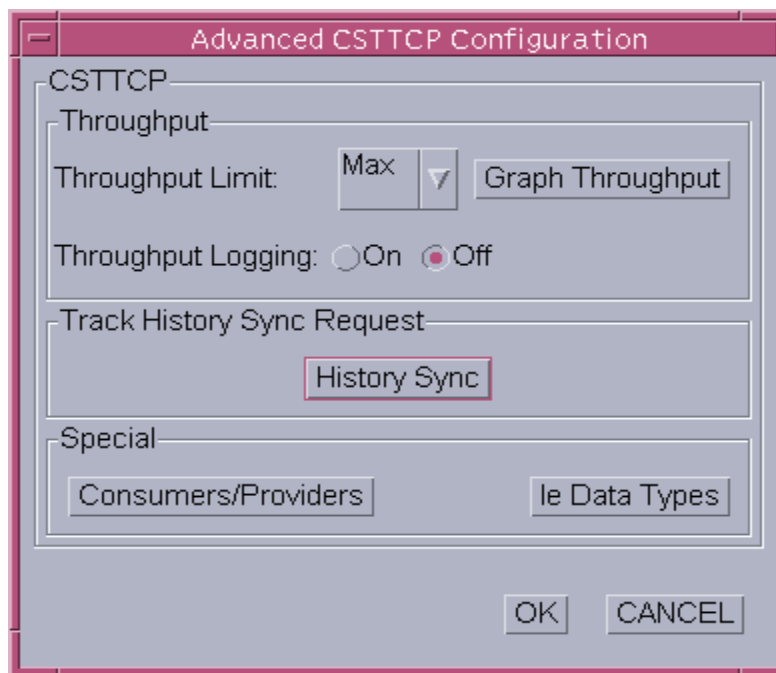


Figure 3-3-16

14. Configuring a Node Requesting Configuration

Note: Configuring a node requesting configuration can only be done by a master node or a secondary master node.

Tip: To check the status of a node listed in the CST NODE LIST window with a status of UNKNOWN, double-click the node and then click **OK** in the CONFIGURE NODE window

without making any changes to the node. If the node is active, the node replies accordingly and updates the CST network with its current status.

15. To configure a node that is requesting configuration:

- a. From the CST menu, select CST Node List.
- b. The CST NODE LIST window appears. Nodes that are requesting configuration appear in blue in the list.
- c. Select a node and click Configure/View.
- d. Depending on whether you have the proper permissions to edit the node, either the VIEW NODE or the CONFIGURE NODE window appears. Each window has a CST and a TMS tab.

CONFIGURE NODE

CST **TMS**

Node ID Info

IP ADDR: 123.123.123.123

HOSTNAME: ACURA

COMMAND: VA LAB

UID TRIGRAPH: ACU

CHNL XREF: TCP

Parent Node ID Info

UID TRIGRAPH: TOY ▼

IP ADDR: 123.123.123.124

PARENT RETRY TIME (MIN): 5

PENALTY BOX: ☐

ADD TO PRECONFIG: ☐

OK Cancel

Figure 3-3-17

- e. From the **CST** tab, do the following as applicable:
- f. Although the fields in the Node ID Info box are not editable, you may wish to verify that the information for each of the following fields is correct.

- IP ADDR – IP address of the node
 - HOSTNAME – Host name of the node
 - COMMAND – Command of the node
 - UID TRIGRAPH – UID trigraph of the node
 - CHNL XREF – Channel cross-reference of the node
- g. Modify the fields in the Parent Node ID Info box as follows:
- (1). In the UID TRIGRAPH box, click the drop arrow and choose the UID trigraph of the parent node from the drop list. Note that only UIDs of nodes in the CST network are available for selection.
 - (2). In the IP ADDR box, verify the IP address of the parent node. (This address is automatically entered upon entering a value in the UID TRIGRAPH field.)
 - (3). In the PARENT RETRY TIME box, enter the amount of time (in minutes) to attempt reconnection with parent node when communications are interrupted. If a connection cannot be re-established with the parent node within this time, the node will then attempt to connect to the master node.
 - (4). Select the PENALTY BOX check box to place the child node into the penalty box. Nodes placed in the penalty box will have no parent node connection. They are still able to exchange data normally with child nodes but will not be able to exchange data with the rest of the CST tree.
 - (5). Select the ADD TO PRECONFIG check box to add the node to the CST preconfiguration database.
- h. Click the TMS tab. The TMS page appears.



Figure 3-3-18

- i. Click the IN FILTER FROM PARENT drop arrow and choose a filter from the list. This filter specifies the tracks that the node can receive from its parent. Note that filters created through this CONFIGURE NODE window and with the Track Database Search window are available for selection. For more information on using the Track Database Search window, see the procedures for using the Database Search option in the User's Manual (UM) for Integrated C4I System Framework (ICSF) Runtime Segments.
- j. To set no filter, select NONE.
- k. To edit an existing filter, select the desired filter from the drop list and click EDIT. To create a new filter, select NONE from the drop list and click EDIT.
- l. The CST IN FILTER EDIT window appears.

Search Filter

Filter Name: USER_DEF_192.135.211.83CST

Description: N/A

Include Tracks that **Match** the Selected Criteria

☐ Center on Selected Tracks

Type/Mode/Scope/Scen/Cat/Thrt

Geolocation

Track Types	All
PLATFORM	<input checked="" type="checkbox"/>
ELINT	<input checked="" type="checkbox"/>
ACOUSTIC	<input checked="" type="checkbox"/>
SPA25	<input checked="" type="checkbox"/>
RAYCAS	<input checked="" type="checkbox"/>
UNIT	<input checked="" type="checkbox"/>
FCS	<input checked="" type="checkbox"/>
SI	<input checked="" type="checkbox"/>
LINK	<input checked="" type="checkbox"/>
EXTERNAL	<input checked="" type="checkbox"/>
EOB MODE	<input checked="" type="checkbox"/>
EOB	<input checked="" type="checkbox"/>
FACILITY	<input checked="" type="checkbox"/>
MISSILE	<input checked="" type="checkbox"/>
Z TRACK	<input checked="" type="checkbox"/>
GENERAL T...	<input checked="" type="checkbox"/>
SPACE	<input checked="" type="checkbox"/>

Attribute

Modes	All
FOTC	<input checked="" type="checkbox"/>
NON FOTC	<input checked="" type="checkbox"/>
AMBG	<input checked="" type="checkbox"/>
NON AMBG	<input checked="" type="checkbox"/>

Timelate

Scopes	All
OTH	<input checked="" type="checkbox"/>
LOCL	<input checked="" type="checkbox"/>
TERM	<input checked="" type="checkbox"/>

Scenarios	All
REAL WORLD	<input checked="" type="checkbox"/>
LIVE TRAINI...	<input checked="" type="checkbox"/>
SIMULATED	<input checked="" type="checkbox"/>

	ALL	AIR	NAV	SUR	MER	FSH	SUB	LND	UNK	SPC
FRD	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
HOS	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
NEU	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
AFD	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
SUS	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
UNK	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
PND	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

OK Cancel Save Recall Export Reset Help

Figure 3-3-19

- m. The CST IN FILTER EDIT window works the same as the Track Database Search window to allow you to specify filter criteria. Use the four tabs in this window to set filter criteria as you want it. Click Save to save the filter and return to the CONFIGURE NODE window. Refer to the User's Manual (UM) for Integrated C4I System Framework (ICSF) Runtime Segments for complete information about creating filters.
- n. To further filter the tracks that the node can receive from its parent, select one of the filter radio buttons below the IN FILTER FROM PARENT list. (The default is RAW. FUSED and ALL are currently unsupported and therefore grayed out.)

- RAW – Allows the node to receive only uncorrelated (raw) theater ballistic missile (TBM) tracks from its parent.
- FUSED – Allows the node to receive only correlated (fused) TBM tracks from its parent.
- ALL – Allows the node to receive both uncorrelated (raw) and correlated (fused) TBM tracks from its parent.

Note: Without the Theater Ballistic Missile Defense Multi-Source Correlator (TMSC) segment to correlate (fuse) TBM tracks, only uncorrelated (raw) TBM tracks exist. For additional information on the TMSC segment, see the Theater Ballistic Missile Defense Multi-Source Correlator (TMSC) Segment User's Manual.

- o. Click the OUT FILTER TO PARENT drop arrow and choose a filter from the list. This filter specifies the tracks that the node can distribute to its parent. The methods for choosing an OUT FILTER TO PARENT are the same as those for choosing an IN FILTER FROM PARENT. See Step 5 above for details about setting a filter.
- p. To apply the OUT FILTER TO PARENT to only those tracks owned by the local node, select the Apply Filter to Local Tracks check box. To apply the filter to all tracks (regardless of ownership), select the Apply Filter To All Tracks check box. These options are only available if an out filter is specified.
- q. In the Permission Attributes area, select any combination of permissions for the node, as applicable:
 - UPDATE allows the node to modify tracks that were created by another node.
 - DELETE allows the node to delete tracks that were created by another node.
 - MERGE allows the node to merge tracks that were created by another node.
 - TAKE OWNERSHIP allows the node to assume ownership of tracks created by another node. (Once ownership is assumed, the node may modify or delete tracks as if they were its own.)
 - SECONDARY CONFIG allows the node to configure other nodes below it (child nodes, grandchild nodes, and so on). This option is only available for CSTTCP and CSTSTCP channels.
- r. Click OK. A message is transmitted to the node that was requesting configuration, indicating the new settings for the node.

THIS PAGE INTENTIONALLY LEFT BLANK

INFORMATION SHEET 3-3-6

MISCELLANEOUS TASKS

A. Introduction

This information sheet will provide the trainee with an understanding of Miscellaneous tasks that the System Administrator is responsible for on the GCCS-M system.

B. References


1. Online Embedded documentation
2. Current Load Plan and Installation Procedures

C. Information

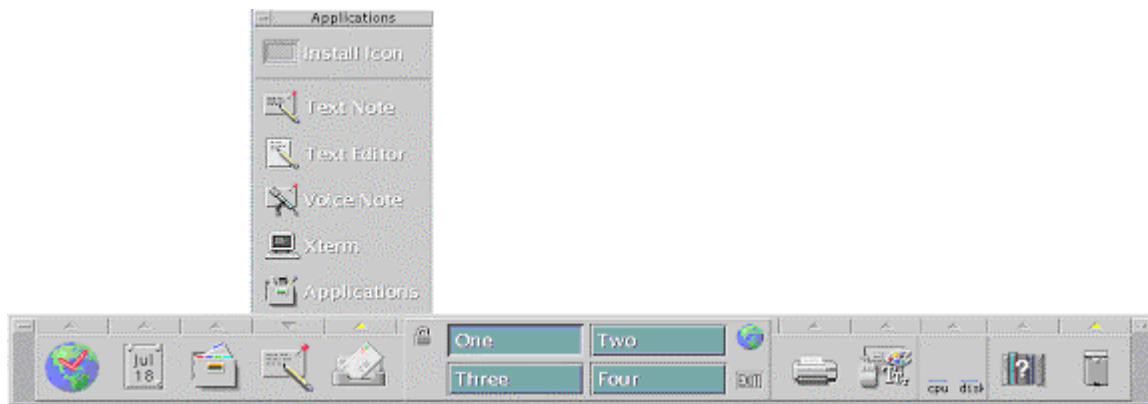
- ## 1. Clean Incoming Logs

This utility enables users to delete all the messages in the Incoming Message Log. Since newer messages replace older messages, once the log capacity (1000 messages) is reached, it is not usually necessary to manually empty it. Emptying this log is generally an activity used in troubleshooting the system.

2. Empty the Incoming Message Log:

- a. Go to the Front Panel, and click the arrow above the **Apps Manager** icon 

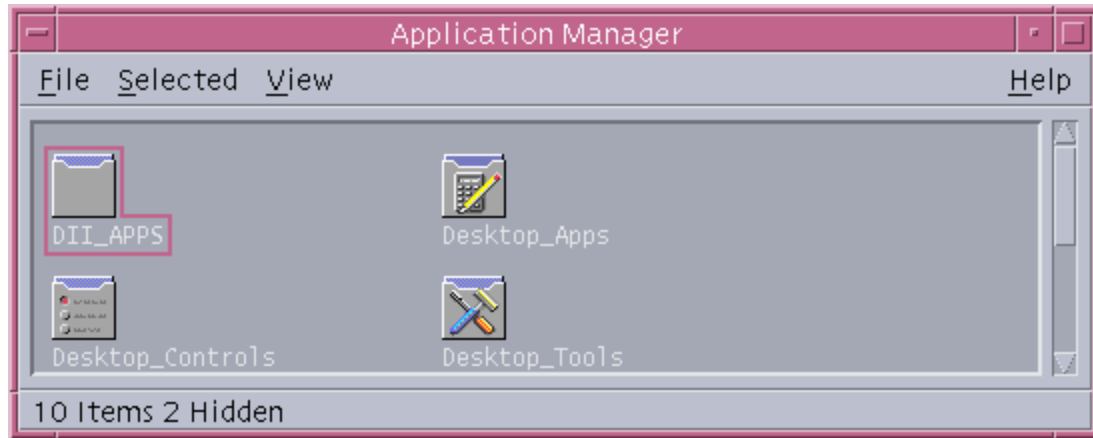
The **Applications** menu appears.



- b. Select **Applications**

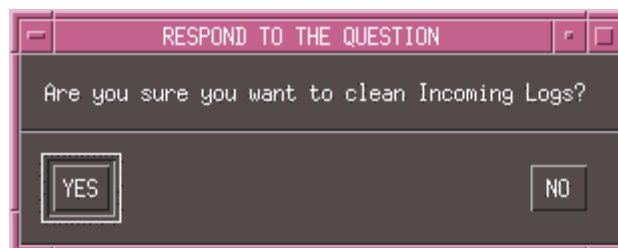


The Application Manager window appears.



- c. In the Application Manager window, double-click the **DII_APPS** folder.
- d. Double-click the **UCP** folder.
- e. Double-click the **Clean Incoming Logs** icon.

The RESPOND TO THE QUESTION confirmation window appears.



- f. Click **YES**.

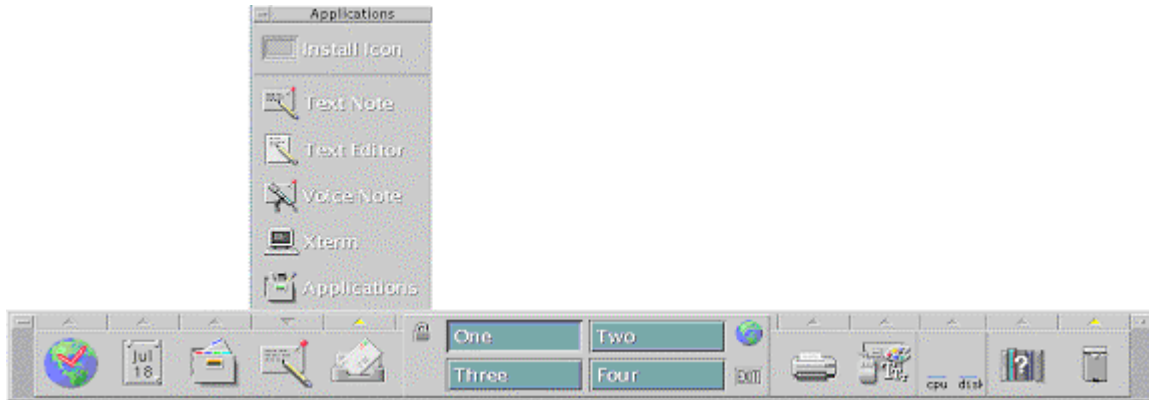
The confirmation window closes and all messages are cleared from all the incoming message logs.

3. To clean outgoing message logs on the UCP Server:

- a. Go to the Front Panel, and click the arrow above the **Apps Manager** icon



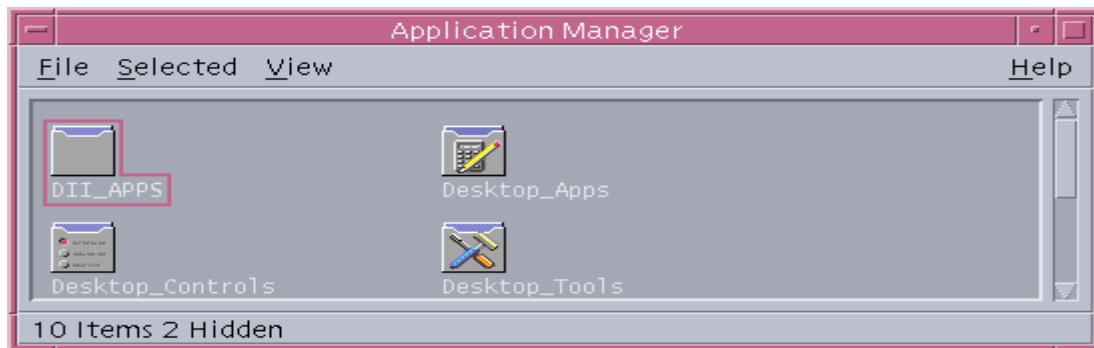
The **Applications** menu appears.



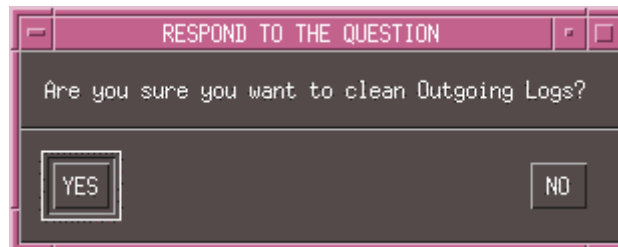
- b. Select **Applications**.



The Application Manager window appears.



- c. In the Application Manager window, double-click the **DII_APPS** folder.
- d. Double-click the **UCP** folder.
- e. Double-click the **Clean Outgoing Logs** icon.
- f. The RESPOND TO THE QUESTION confirmation window appears.



- g. Click **YES**.

The confirmation window closes and all messages are cleared from all the outgoing message logs.

4. Clean Track Database Files (Unix only)
 - a. This utility is available only when the TMS segment is loaded. This utility enables you to remove all TMS track database files while TMS processes are running. It does not remove the database configuration files. It is designed to be used when one or more of the TMS database files are corrupted, causing some or all of the TMS processes to fail soon after starting. Cleaning the track database is usually done only after all other recovery methods fail.
 - b. The TMS P8 feature will also clear the TMS database and is the recommended first step to cleaning the track database prior to using the TMSRun feature.
5. To clean the Track Database:
 - a. Log to the TMS Master as sysadmin.
 - b. From the command line change directories to /h/COE/Comp/TMS/bin and type:
TMSRun –clean

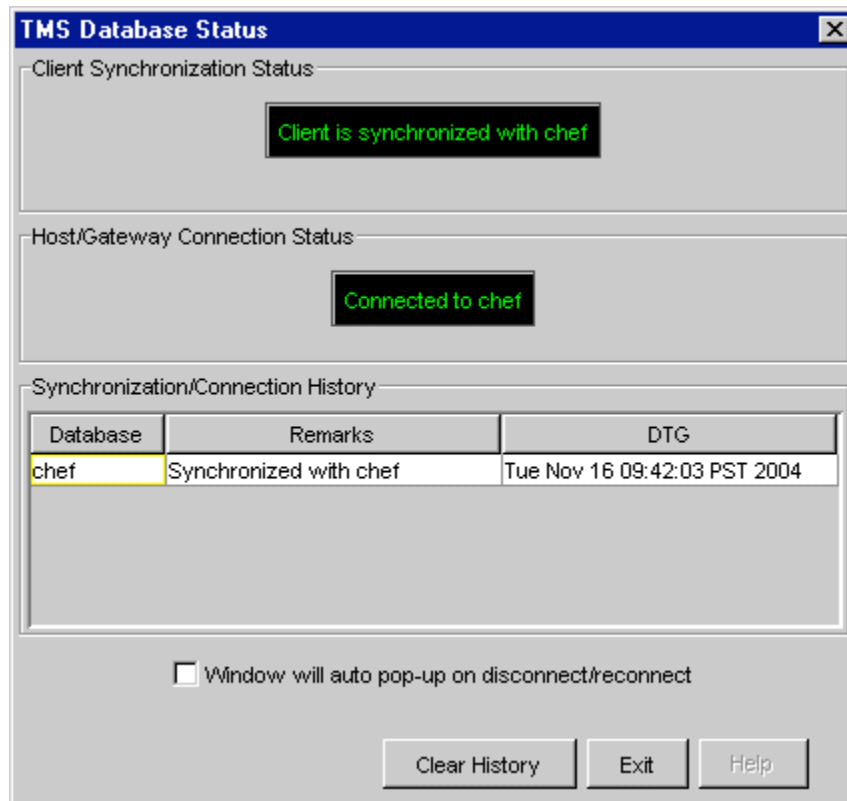
NOTE: After this command has been run, the entire TMS network must be rebooted. Use this as a last resort for troubleshooting.

OR

- c. As a sysadmin or a user with the TMS P8 feature and clean the database from the clean database icon.

Use the **TMS Database Status** option to view the current Client and Gateway connection status. The following TMS Database Status procedures are available:

6. Accessing TMS Database Status
 - a. To open the TMS Database Status window:
 - b. Go to the **Tracks** menu and select **TMS Database Status**.
 - c. The TMS Database Status window appears.



- d. The TMS Database Status window shows whether or not the Client is synchronized with a Host, and also displays information about any lost connections. It also displays a list showing the synchronization/connection history.
- e. To automatically display the TMS Database Status window when the Client becomes disconnected with the Host, or when the Client reconnects with the Host, click the **Window will auto pop-up on disconnect/reconnect** check box.
- f. (Optional) To clear the Synchronization/Connection History list, click **Clear History**.

7. TMS Database Status Window Fields

a. Client Synchronize Status

If the Client is synchronized with a Host, this displays a message telling you the Client is synchronized and the Host name. If the client is not synchronized with a Host, this displays a lost synchronized message.

b. Host/Gateway Connection Status

If the Client is connected to a Host, this will display a message telling you the Client

is connected to the host and the host name. It will display Lost Connections if there are lost connections.

c. **Synchronization/Connection History**

This displays a list of the Synchronization/Connection history between the Client and any hosts. The Database column lists the name of the Host or Server, the Remarks column lists some explanatory text, and the DTG column displays the time of the event.

8. **System backup, recovery, and contingency**

The importance of proper backup, recovery, and contingency procedures cannot be over emphasized. This section discusses:

- The importance of recovering machines to a known state
- What is backed up (i.e., OS, databases, user directories, and file systems)
- What circumstances warrant activation of recovery and contingency procedures
- Sites must develop site-specific procedures, and implement those procedures to ensure that their systems can be recovered in an acceptable timeframe.

Backup Strategy


A comprehensive backup strategy is important to ensure the system can be recovered to a known state and at a certain point in time. A successful recovery process depends upon two processes; 1) The ability to construct, or restore, the system to an initial installation or baseline configuration with segment tapes or original installation media, and 2) The proper selection, or inclusion, of the files designated for archival. The incremental backup only copies those files that have been changed since the last incremental (or full backup if it is the first incremental) backup in the set. Full backups are taken on an infrequent basis in coordination with the Incremental backups. Incremental backups are generally done on a more frequent basis than full backups. Each individual site should determine an appropriate backup schedule and conduct backups on a regular basis. Depending upon the site's backup strategy, it is recommended several backup sets be created. Backup sets may be grouped by any logical classification that is most appropriate for the site. Common ways to logically group backup sets are by: day of the week, week of the month, criticality of files, or any other logical grouping of application, data or user files. Scheduling of different backup sets do not need to be the same between sets. Certain files may



need to be backed up more frequently than others due to operational requirements and/or the timeliness of the data.

9. Global Backup and Restore Utility (GBAR)

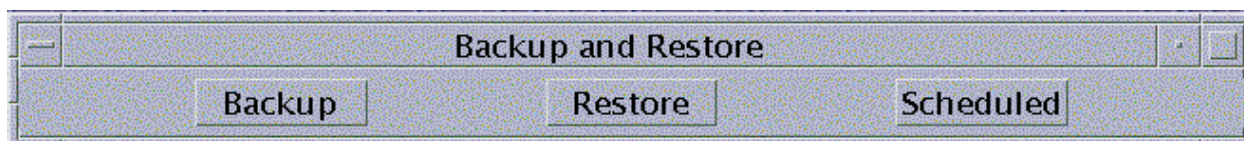
- a. Global Backup and Restore (GBAR) allows system administrators to set workstations to automatically backup data daily. Administrators may also find it useful to sometimes cancel the automatic process and backup data manually, enabling them to specify which data directories should be backed up and which should not be. When backing data up manually, system administrators may choose to add files for backup not included by GBAR, or remove those custom files as needed. Any files added to the “custom” files will also be included in scheduled backups.
- b. The Global Backup and Restore (GBAR) is a simple tool that provides backup and restore capability of file system data that resides on the Solaris host. Each GCCS-M host is installed with GBAR and must be run locally to backup files to the local tape drive. By default, critical files are pre selected and sorted into Application, Log, User and System Data. Users can select which type of data to backup. GBAR is intended to be used as a file backup utility and can not perform incremental or full system backups.
- c. GBAR can also make a backup image of the entire server using *flarcreate*. This backup ability also watches for the existence of Disk Mirroring (DSKMIR), and if it is there, makes sure that the image that will be made is capable of being restored later without needing to de-install DSKMIR from the current system prior to making the image. The user interface for this segment is described in *Appendix D* of the GBAR Software Version Description (SVD).

10. Schedule an Automatic Backup

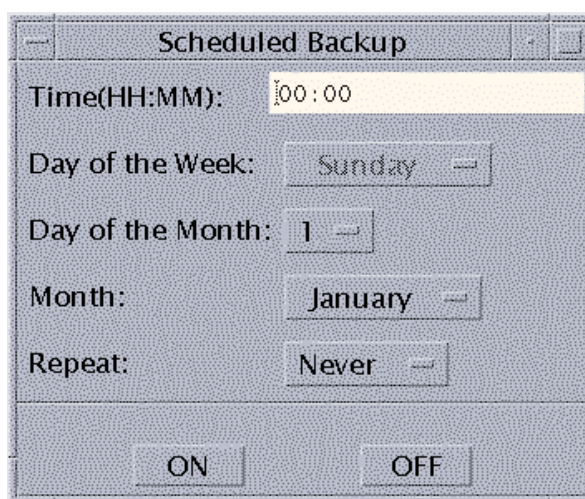
 **NOTE:** Only one backup can be scheduled at any one time. A new scheduled backup overwrites the previous one.

- a. Go to the **Front Panel** and click the arrow above the **Apps Manager** icon .
- b. From the *Applications* menu, select **Applications** .
- c. In the *Application Manager* window, double-click the **DII_APPS** folder.

- d. Double-click the **GBAR** folder.
- e. Double-click the **Global Backup And Restore** icon.




- f. In the *Backup and Restore* window, click **Scheduled**.



- g. In the *Scheduled Backup* window, from the **Repeat** drop list, select the backup frequency. The remaining fields to be set depend on the Repeat value, as indicated in the table below.

Repeat Value	Selectable Fields (others are grayed out)
Never (one-time backup only)	Time, Day of the Month, Month
Daily	Time
Weekly	Time, Day of the Week
Monthly	Time, Day of the Month

- h. If **Time** is selectable, enter it in the format **HH:MM** where HH=hours and MM=minutes. (An improperly formatted time entry results in an error window.)
- i. If **Day of the Week**, **Day of the Month**, or **Month** is selectable, choose a value from its respective drop list.

 **NOTE:** If the system administrator selects an impossible date (for example, February 31), the scheduled backup will not run since that date will never arrive. The program does not stop you from selecting this date, however.

- j. Click **ON**.
- k. In the *RESPOND TO THE QUESTION* window, at the *Backup to a Tape or the File System?* message, click either **Tape** or **File System**.



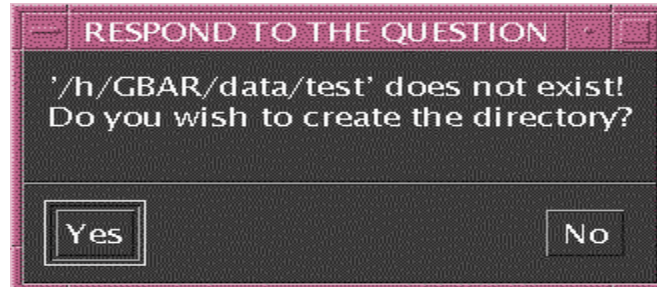
- l. If **Tape** is chosen, do the following:
 - (1). In the *Select Tape Device* window, at the *Device:* prompt, select **<the tape device>** and click **Ok**.



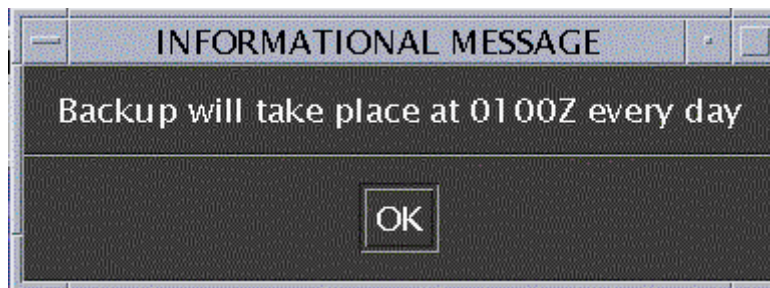
- m. If **File System** is chosen, do the following:
 - (1). In the *ENTER A RESPONSE* window, at the *Please specify a location to store the backup file (example: /h/GBAR/data/backups):* prompt, enter **<the location to store the backup file>**.



- n. If the *RESPOND TO THE QUESTION* window appears, at the '*<the location to store the backup file>*' does not exist! Do you wish to create the directory? message, click **Yes**.



- o. In the *INFORMATIONAL MESSAGE* window, at the *Backup will take place at XXXX XXX XXX* message, click **OK**.



- p. Ensure the appropriate media is prepared for the backup process. For example, ensure a tape drive is connected and that a valid tape is in the drive.

11. **Configure Backup Device**

- a. In the *RESPOND TO THE QUESTION* window, at the *Backup to a Tape or the File System?* message, click either Tape or File System.



- b. If **Tape** is chosen, do the following:

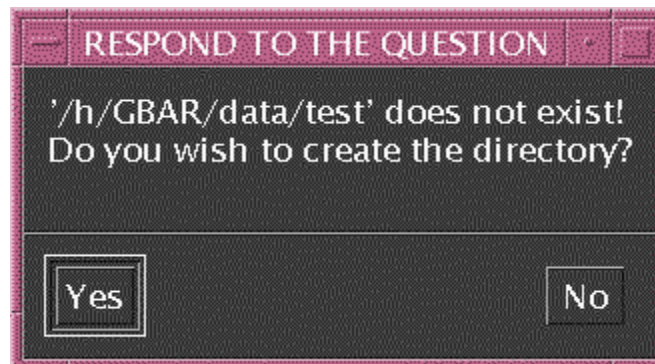
- (1). In the *Select Tape Device* window, at the *Device:* prompt, select **<the tape device>** and click **Ok**.



- c. If **File System** is chosen, do the following:
 - (1). In the *ENTER A RESPONSE* window, at the *Please specify a location to store the backup file (example: /h/GBAR/data/backups):* prompt, enter **<the location to store the backup file>**.




- d. If the *RESPOND TO THE QUESTION* window appears, at the '*<the location to store the backup file>* does not exist! Do you wish to create the directory?' message, click **Yes**.



12. Backup local and global data manually

Prepare the appropriate media for the backup process. For example, ensure a tape drive is connected and that a valid tape is in the drive.

- a. Go to the **Front Panel**, as shown below, and click the arrow above the **Apps**

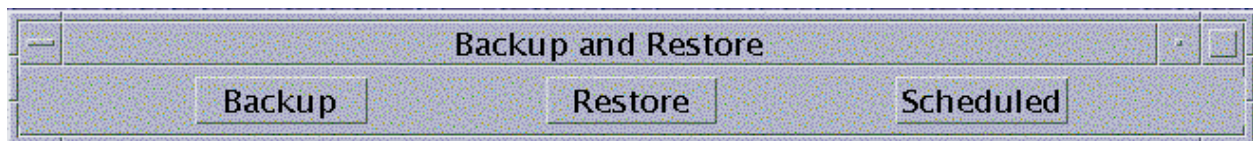
Manager icon .

- b. From the Applications menu, select **Applications** .


- c. In the *Application Manager* window, double-click the **DII_APPS** folder.

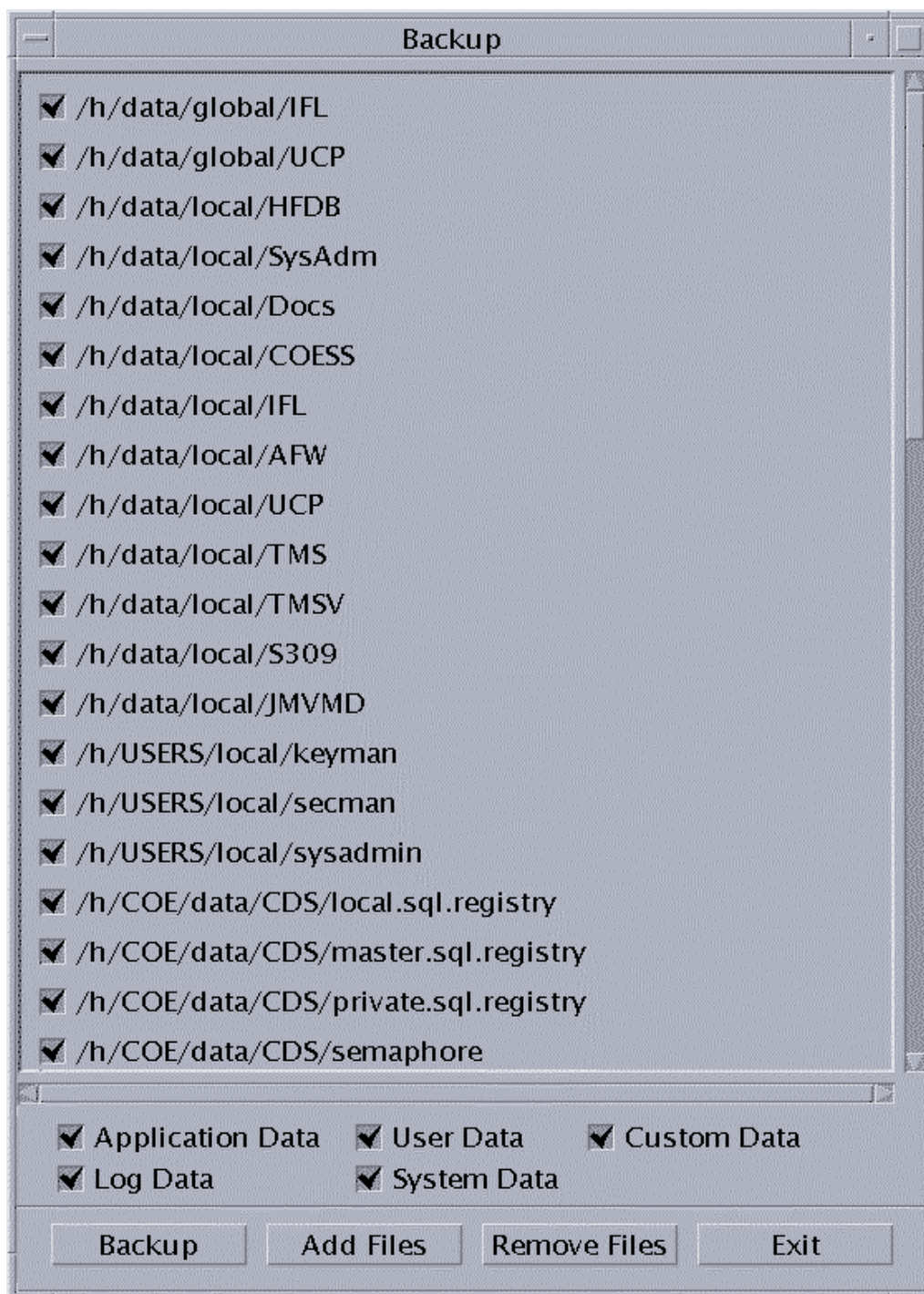
- d. Double-click the **GBAR** folder.

- e. Double click the **Global Backup And Restore** icon.




- f. In the *Backup and Restore* window, click **Backup**.

 **NOTE:** The Backup window appears displaying a list of available directories to backup. All available directories/files are automatically selected for backup.




- g. Deselect any directories/files to **not** include in the backup.
- h. If a system administrator clicks on (uncheck) one or more of the check boxes at the bottom of the window (Application Data, User Data, Log Data, System Data, or Custom Data), **all** files associated with the unchecked group(s) will disappear from the list. They will not be included in the backup.

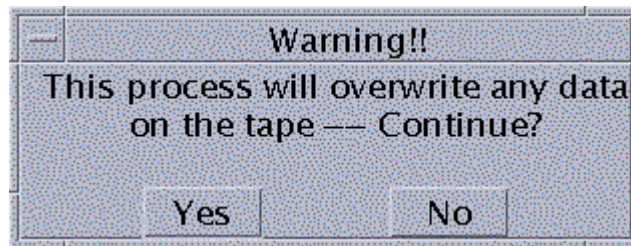
- i. To append data to the backup tape versus overwriting the data on the tape, select the **Log Data** checkbox. With the **Log Data** checkbox selected, system administrators can also select the Custom Data checkbox and include new custom data to the data appended on the backup tape. However, selecting any other group of files (such as Application Data, User Data, or System Data), then GBAR will rewind and overwrite the data already on the tape.

 **NOTE:** Clicking on (check) one or more of these groups after deselecting them, all files associated with the group(s) appear again and are checked on. The **Custom Data** checkbox represents all files added for backup. To remove the files from a backup a system administrator added, click (uncheck) the **Custom Data** checkbox or remove the files added.

- j. After determining which group(s) of files to exclude from the backup, click on (uncheck) any of the remaining individual files in the list to exclude them from the backup.

 **NOTE:** All the directories/files with a checkmark will be included in the backup process.

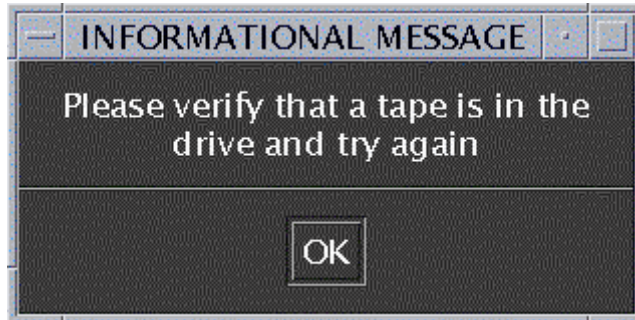
- k. When the appropriate directories are selected for backup, click **Backup**.
- l. If the *Warning!!* window appears, click **Yes** to continue with the backup as indicated.




- j. If the backup process is successfully completed, in the *INFORMATIONAL MESSAGE* window, at the *Backup Completed Successfully* message, click **OK**.



- k. If an error occurs during the backup process, in the *INFORMATIONAL MESSAGE* window, at the *Please verify that a tape is in the drive and try again* message, click **OK**, check the tape drive and tape, and try the backup process again.




13. Restore local and global data

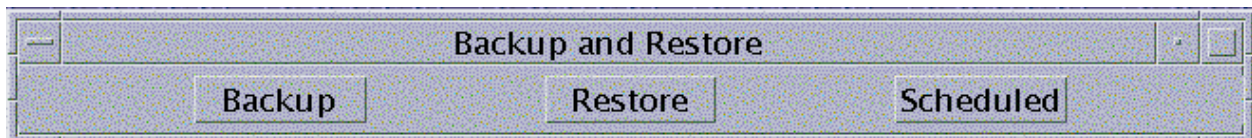
 **NOTE:** If restoring data to a different machine, change the current machine's hostname to match the hostname of the machine on the backup tape. Ensure the machine is configured with the same settings as the machine on the backup tape.

- a. Prepare the appropriate media for the restore process. For example, ensure a tape drive is connected and that a valid tape of backup data is in the drive.
- b. Go to the **Front Panel**, as shown below, and click the arrow above the **Apps**

Manager icon



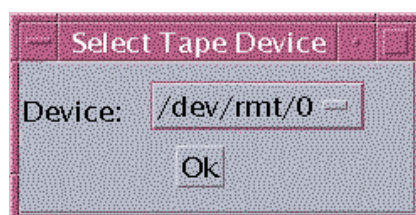
- c. From the Applications menu, select **Applications** .
- d. In the *Application Manager* window, double-click the **DII_APPS** folder.
- e. Double-click the **GBAR** folder.
- f. Double click the **Global Backup And Restore** icon.



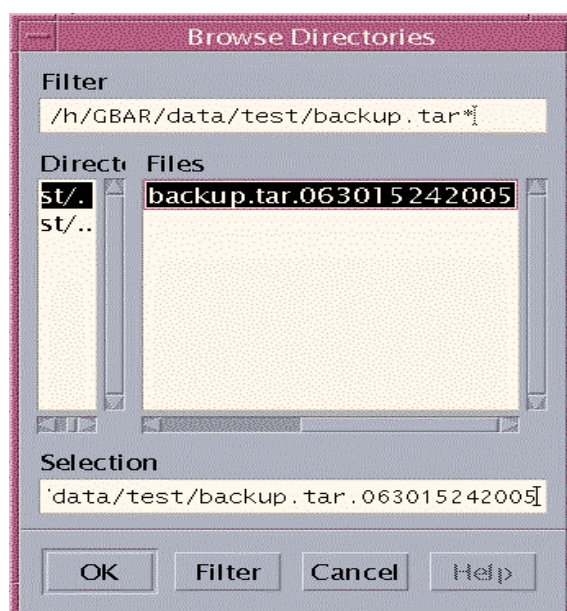
- g. In the *Backup and Restore* window, click **Restore**.
- h. In the *RESPOND TO THE QUESTION* window, at the *Choose the media to restore from:* prompt, click **Tape** or **File System**.



- i. If **Tape** is chosen, the following window may appear:
- j. In the *Select Tape Device* window, at the *Device:* prompt, select **<the tape device>** and click **Ok**.



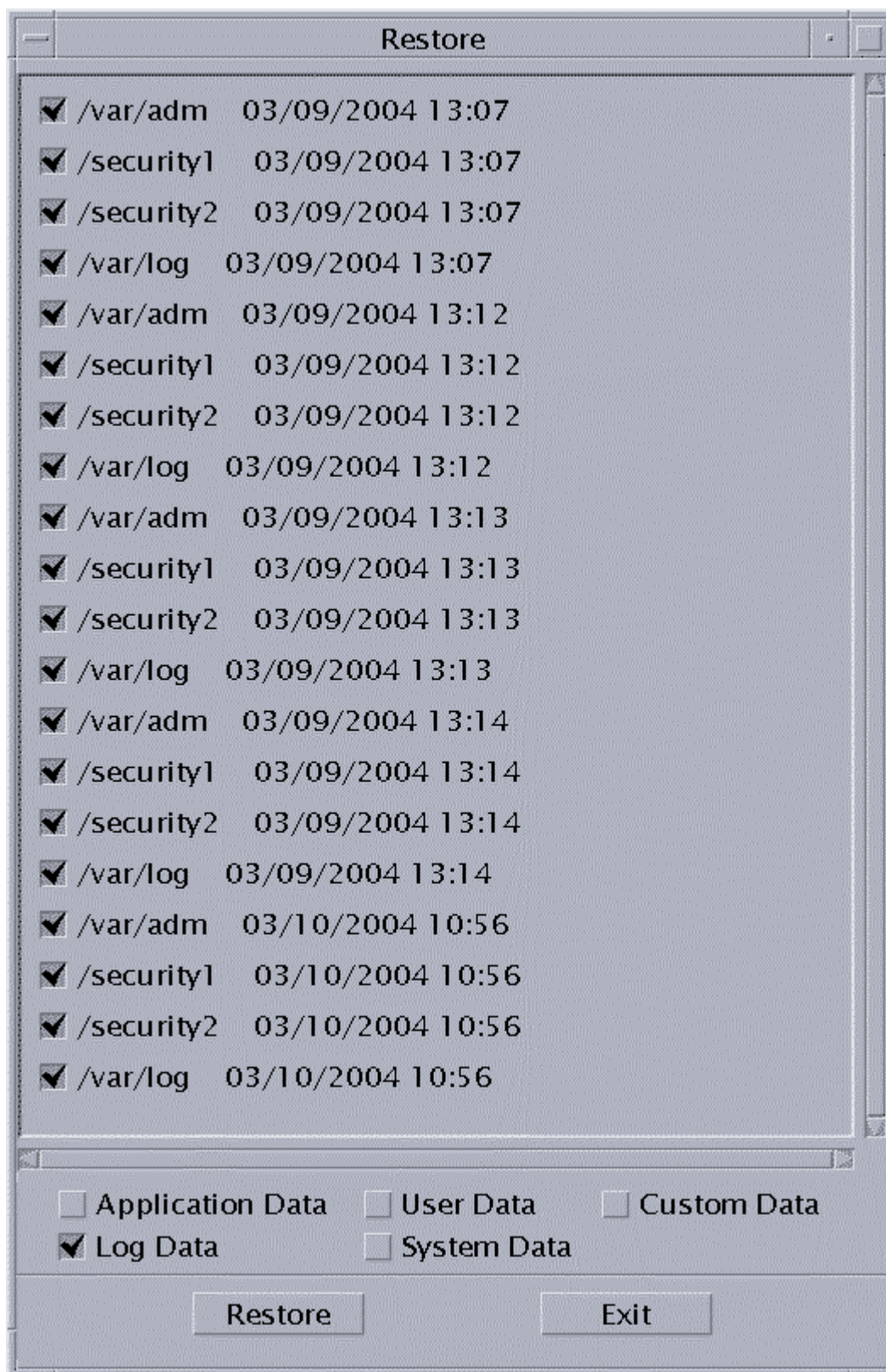
- k. If **File System** is chosen, do the following:
 - (1). In the *Browse Directories* window, browse to the location of the backup file to be restored, highlight the file name, and click **OK**.






NOTE: The Restore window appears displaying a list of available directories to restore. All available directories are automatically selected for restoration. The Restore window may take a few minutes to appear because the backup tape is being read to create a list of available items to restore.

- l. Deselect any directories/files you do **not** wish to include in the restore.
- m. If the system administrator clicks on (unchecks) one or more of the checkboxes at the bottom of the window (Application Data, User Data, Log Data, System Data, or Custom Data), **all** files associated with the unchecked group(s) will disappear from the list. They will not be included in the restore.
- n. If the system administrator clicks on (checks) one or more of these groups after deselecting them, all files associated with the group(s) appear again and are checked on.
- o. The **Custom Data** checkbox represents all files added for backup. If the system administrator does not want to restore the files added, click (uncheck) the **Custom Data** checkbox.
- p. If the tape being restored was backed up using the append method (with the **Log Data** checkbox selected) versus the overwrite method, then files in the Restore window display the date and time of the backup, as shown below.




- q. After determining which group(s) of files to exclude from the restore, click on (uncheck) any of the remaining individual files in the list to exclude them from the restore.

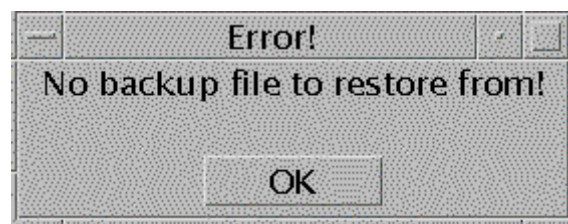
 **NOTE:** All the directories/files with a checkmark will be included in the restore process.

- r. Click **Restore**.
- s. If the following warning window appears, click **Yes**.

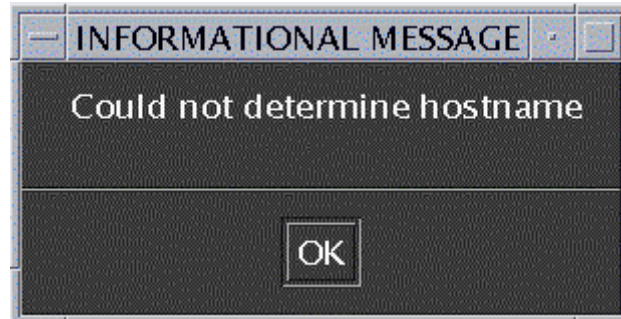


 **NOTE:** If a valid backup tape is not in the tape drive when you click **Restore**, one of the following error windows appears.

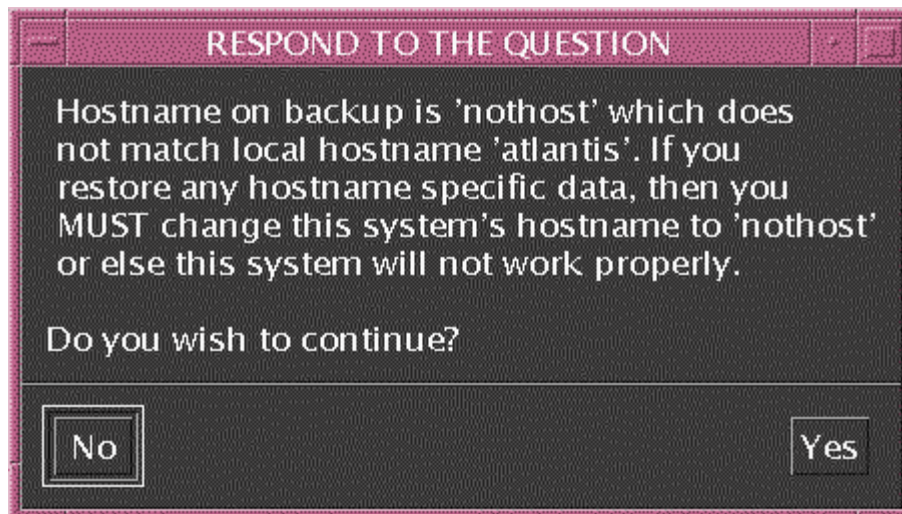
- t. In the *Error!* window, at the *No backup file to restore from!* Message, click **OK**, ensure a backup tape is in the connected tape drive, and start the restore process again.



- u. If this error message appears, either the hostname of the current machine, or the hostname that was stored on the backup tape could not be determined. Generally, at this error, the backup tape does not have the hostname of the machine from which data was stored. Click **OK** and begin the restore with a backup tape, which indicates the machine's hostname.



- v. If this message appears, the hostname of the machine to which you are restoring data does **not** match the hostname of the machine indicated on the backup tape. Either click **No** and start the restore again with the correct tape (a tape with the same hostname as your machine), or click **Yes** and change the hostname of your machine once the restore is completed. If you change the hostname of your machine, ensure the other configuration settings on your machine match that of the machine indicated on your backup tape.



- w. Another warning window appears, allowing you to (either individually or as a group) confirm the data directories for restoration.




- x. To confirm all the data directories for restoration, click **Yes All**.
- y. To confirm each selected data directory individually, click **Yes**, or click **No** if you do not want a particular selected directory to be restored.
- z. To cancel the entire restore process, click **No All**.
- aa. In the *Restore Complete* window, click **Yes** to reboot the machine and restart any stopped processes.



14. Backup Entire System to tape or file system

- a. Go to the **Front Panel**, as shown below, and click the arrow above the **Apps**

Manager icon .

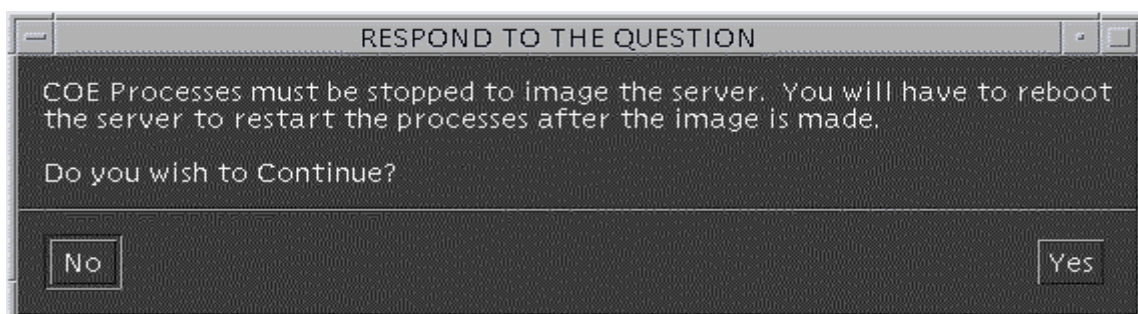
- b. From the Applications menu, select **Applications** .

- c. In the *Application Manager* window, double-click the **DII_APPS** folder.

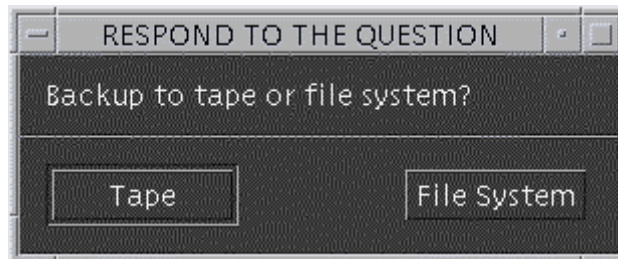
- d. Double-click the **GBAR_P3** folder.

- e. Double click the **Image Server** icon.


- f. In the *RESPOND TO THE QUESTION* window, at the *COE Processes must be stopped to image the server. You will have to reboot the server to restart the processes after the image is made. Do you wish to continue?* prompt, click **No** to quit or **Yes** to continue.




- g. In the *RESPOND TO THE QUESTION* window, at the *Backup to tape or file system?* prompt, do the following:
- h. To place the image on the local hard disk, select **File System**.
- i. To place the image on a tape, select **Tape**.



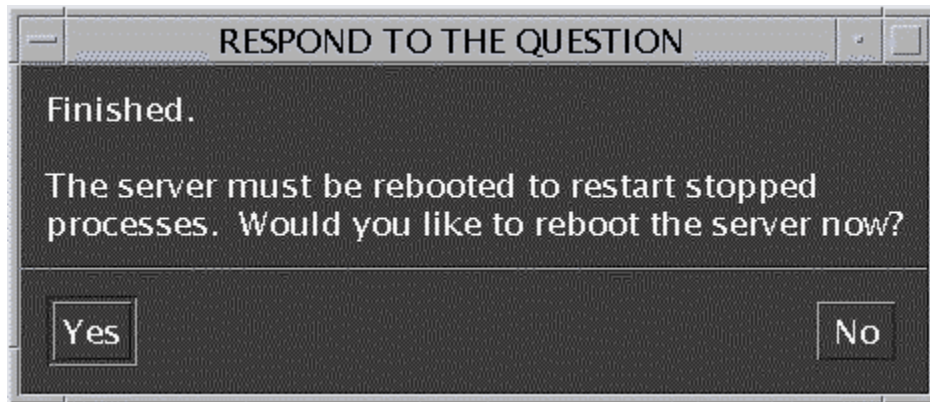
- j. In the *ENTER A RESPONSE* window, at the *Enter the directory where the server archive can be stored. This directory will NOT be included in the archive* prompt, enter **<the directory to store the image>**.


 **NOTE:** The directory chosen will not be included in the image made of the server. This is to avoid the image trying to archive itself. It is recommended to create a directory specifically to hold images so that this feature does not affect the backup (e.g. /h/images). If the system administrator fails to supply a valid directory 3 times, the program will exit.



 **NOTE:** At this point, the program is making an image of the server. This can take several hours depending on how much data is on the system that needs to be backed up.

- k. When the backup is complete, in the *RESPOND TO THE QUESTION* window, at the *Finished. The server must be rebooted to restart stopped processes. Would you like to reboot the server now?* prompt, click **Yes**.



 **NOTE:** For information on how to restore the image, see the latest *System Administrator Guide (SAG) for Global Command and Control System-Maritime (GCCS-M) Integration Product 4.0.XX*.

THIS PAGE INTENTIONALLY LEFT BLANK

ASSIGNMENT SHEET 4-1-1

INTEGRATED INTELLIGENCE AND IMAGERY (I3)

A. **Introduction**

This assignment sheet is to be completed as homework or as assigned.

B. **Enabling Objectives**

- 4.1 **DESCRIBE** the GCCS-M I³ databases and servers to support system administration functions.
- 4.2 **PERFORM** administrative tasks of the Intelligence Shared Database Server (ISDS).
- 4.3 **DESCRIBE** the four Intelligence Groups required with the Intelligence Shop Applications on the GCCS-M I³ system.
- 4.4 **PERFORM** Imagery Transformation Server (ITS) administration.

C. **Study Assignment**

- 1. Read Information Sheet 4-1-2

D. **Study Questions**

- 1. What type of COTS database is used for GCCS-I³ management?
- 2. Which Database Server segment provides utilities for the maintenance and configuration of the Sybase server and data?
- 3. What are 6 Database segments installed on the ISDS?

4. What Intel Client segment provides the capability to geographically display general military intelligence?
5. What is the purpose of ISHOP?
6. What does MEDULA provide?
7. What server, formerly known as jots14, hosts the images that have been imported to the GCCS-M side from outside sources?

INFORMATION SHEET 4-1-2

SERVER ADMINISTRATOR FUNCTIONS

A. Introduction

This Information Sheet will provide the trainee with information about the databases and associated segments loaded with GCCS-M 4.0.

B. References

Online Embedded documentation

C. Information

Solaris ISDS Server							Solaris Middle Tier		Solaris/W2K Client Workstation		Solaris Intelligence Parser Server	
GDUS 4.7.0.1	I3GMI 4.7.1.2	GMIDB 4.7.0.1 (Dublin)	CTDS 4.7.1.2	EPL 4.7.1.2	IMDB 4.7.1.2	NERF 4.7.1.2	ISHOPM 4.7.1.2 (DAL and Intel Shop Web App Components)	MDAL 4.7.0.5	ISHOPO 4.7.1.2 (Intel Office / W2K)	ISHOPC 4.7.1.2 (Intel Shop Java App)	ISHOPP 4.7.1.2 (Tactical Message Parser)	ISHOPI 4.7.1.2
SYBADM 4.7.1.2							Application Client BEAJAR 4.7.1.0/8.1 (WebLogic 8.1 COTS client)		ISHOPI 4.7.1.2 (Client Interface to ISHOPM)			
SYBI3C 4.7.1.2							I3CMT 4.7.1.2 (I3 Configure Middle Tier)		XIC 4.5.3.0			
SYBADP 12.5.0.0 & 12.5.0.0P1							Application Server BEAWLS 4.7.1.1/8.1 (WebLogic 8.1 COTS)		Application Client BEAJAR 4.7.1.1/8.1 (WebLogic 8.1 COTS client)		Application Client BEAJAR 4.7.1.1/8.1 (WebLogic 8.1 COTS client)	
SYSAM 1.0.1.0/1.0.0.0												
DBAdmR 4.0.0.0, DBAdmS 4.0.0.0												
JAVA2 4.7.0.1, JMTK 4.7.0.0, JMV 4.5.2.0, NSWEB 4.7.0.1/7.0												
ICSF 4.5.2.0.P4												
Kernel 4.2.0.10												
Solaris 8 (v12/02) or Windows 2000 w/SP2 OS												

****Note** – Solaris recommended patches are required for ISDS to create properly. Please see load plan.

GCCS-M Build 11.1 Intelligence Architecture (12 Dec 2003)

1. GCCS-I³ (Integrated Intelligence and Imagery) Database Management
 - a. GCCS-I³ database administration is performed on the Intelligence Shared Data Server (ISDS), formerly jots19. The ISDS uses Sybase, COTS (Common Off-The-Shelf), Relational Database Management System (RDBMS).
 - b. Six (6) Database Server segments installed on ISDS:
 - (1). **SYSAM** installs the Sybase COTS utility to manage the licenses for Sybase products.
 - (2). **DBAdmR** provides APIs and database maintenance GUI for identifying storage, server control, password control, and error logging.
 - (3). **DBAdmS** provides APIs for creating and dropping data stores, starting and stopping the server, and extending database sizes.
 - (4). **SYBADP** contains the components for deploying the Sybase Adaptive Server Enterprise RDBMS and backup server, and provides related applications and libraries.
 - (5). **SYBI3C** creates the Sybase server and contains components to configure and modify settings for the Sybase data and backup servers within the GCCS environment, such as total Sybase memory, number of CPUs, number of user connections, and number of database devices.
 - (6). **SYBADM**, Sybase Administration provides utilities for the maintenance and configuration of the Sybase server and data. Currently, these utilities include Alternate View Backup/Restore, Server ID, Auditing and an icon to launch Sybase Central (COTS).
 - c. Database segments are installed on the ISDS, which create their respective databases. There are typically six (6) databases loaded on intel:
 - (1). **CTDS (Common Track Data Store)** Data storage for GCCS-M parsed message data and TMS track data. The CTDS contains parsed message data from United States Message Text Format (USMTF) intelligence messages, and also stores TMS Track data. The datastore is not replicated and must be backed up. System administrators should determine the frequency of the backups. The databases can be backed up weekly under normal operations and daily during critical operations.

- (2). **EPL (ELINT Parameters List Database)** Contains observed parameter data useful for determining most operating ranges. Includes information on ELINT (electronic intelligence) notations, function codes, and associated platforms.
- (3). **GMIDB (General Military Intelligence Database)** creates four databases that contain order of battle, facilities, and unit data GMI- Primary Intelligence Data. Provides data on equipment, facilities, and units. Includes data from the MEPED database, which contains characteristics and performance data for Platforms, Weapons, and Electronics.
- (4). **IMDB (Image Management Database)** Provides structures for information about intelligence imagery, such as data on the type and location of imagery. IMDB provides data links to the imagery stored by the imagery server, which can be used for tactical analysis. The IMDB contains information about intelligence imagery by storing data on the type and location of imagery. IMDB provides data links to the imagery stored by the Imagery Transformation Services (ITS) that can be used for tactical analysis applications. IMDB is not replicated and must be backed up. System administrators should determine the frequency of the backups. The databases can be backed up weekly under normal operations and daily during critical operations.
- (5). **NERF (Navy Emitter Reference File)** Stores data for platforms, emitters, and related equipment. Contains Electronic Warfare (EW) Data consisting of Order of Battle (OB), Non-Hostile, and Hostile Threat Parameters. Worldwide in scope and consists of Order of Battle (OB), friendly, non-hostile, and hostile treat parametric data. Contains radar parametric data about military and commercial emitters including U.S. non-communications emitters.
- (6). **ISHOPD (Intelligence Shop Database)** Contains structures to hold persistent I³ business objects supporting Intelligence Shop Middle-Tier (ISHOPM) services. Provides data structures to support run-time creation and storage of I³ business objects such as Named Area of Interests (NAIs) and

Intelligence folders. The ISHOPD segment contains structures to hold persistent Integrated Imagery and Intelligence (I3) business objects supporting the Intelligence Shop Middle-Tier (ISHOPM) services. The ISHOPD database provides data structures to support run-time creation and storage of I3 business objects such as Named Areas of Interests (NAIs) and intelligence folders. ISHOPD is not replicated and must be backed up. System administrators should determine the frequency of the backups. The databases can be backed up weekly under normal operations and daily during critical operations.

2. Intelligence Client Segments (Client Tier)

- a. The **Standard Int On-site Present Sys (SINOPS)** is a client segment for the on-site indexing and delivery of GCCS documentation. This segment sends document requests to the MEDULA documentation server, using a web browser as its display mechanism. Upon install, SINOPS retrieves all COE applications segments (any COE segments that contain documentation to be stored on the MEDULA server) so that the documentation is “checked in” by SINOPS into MEDULA’s documentation database.
- b. The **BEA Client-Side JAR File (BEAJAR)** segment supports BEA WebLogic Server clients and WebLogic Workshop run-time clients.
- c. The **Intelligence Shop Interfaces (ISHOPI)** segment provides the Application Program Interfaces (APIs) that allow applications to access the Intelligence Shop Middle-Tier (ISHOPM) services, such as the Intelligence Shared Data Server (ISDS), Data Access Layer (DAL) and Order Of Battle (OOB) Folder Maintenance.
- d. The **Intelligence Shop Client-Tier (ISHOPC)** segment is designed to assist with force projection, strike planning, and intelligence/threat analysis. ISHOPC provides the capability to geographically display general military intelligence. It provides point-and-click access to national/tactical intelligence reports and associated imagery/video and provides the capability to view, update, and disseminate tactical intelligence.
- e. The **Intelligence Shop Office (ISHOPO)** for Windows 2000 segment provides the following features:

- Fully integrated with Microsoft Excel and other Office applications.
 - A companion product to the Intelligence Shop Client-Tier (ISHOPC) segment.
 - Point and click interface to facilities, units, equipment, persons, related documents, imagery, tracks, and messages from various data sources.
 - Display of imagery/video associated with related-intelligence.
 - Message Parsing Segment
- f. The **Intelligence Shop Message Parser (ISHOPP)** segment provides tactical message parsing capability for use in Intel data maintenance functions. Messages are parsed and associated with existing data in CTDS and GMI, and stored in CTDS. ISHOPP provides the ability to process incoming messages from any one of five United States Message Text Format (USMTF) message types (IIR, MISREP, OBREP, RECCEXREP, and SPIREP).
3. ISDS Database Administration Tasks
- a. Creating the Intelligence Groups
 - b. If the user is not in one of the following groups, they will only have access to the Analyst Workshop Welcome page. The user is given three attempts to enter a valid password before being locked out of the application server. It will be a half-hour before they can login again.

Group assigned to login account	Features Allowed
IntelligenceConsumer	Most Analyst Workshop Welcome page features: Sign-in Link; Sign-Out Link; Search on all tabs; all features under My Intel Shop , including the Customize View feature, the Search tab, the Collection Status and Graphic INTSUM (including Generate Overlay) features on the Produce tab, Patterns/Trends on the Analyze tab, and Export on Disseminate tab. Also any links to view a saved Folder (may be displayed under What's New).

Group assigned to login account	Features Allowed
IntelligenceProducer	Features of IntelligenceConsumer plus New Candidate to Target List (CTL) on Produce tab. Can also create, edit, and delete intelligence records/associations (Data Maintenance Tab only), access the browse hierarchy and browse relationships features on the Maintain tab, create a New CTL on the Produce tab and insert documents, aliases, and remarks via the OOB Reports.
IntelligenceSupervisor	Features of IntelligenceProducer plus Send To COP and Nominate on the Disseminate tab.
IntelligenceAdministrator	Features of IntelligenceConsumer plus the Administration link.

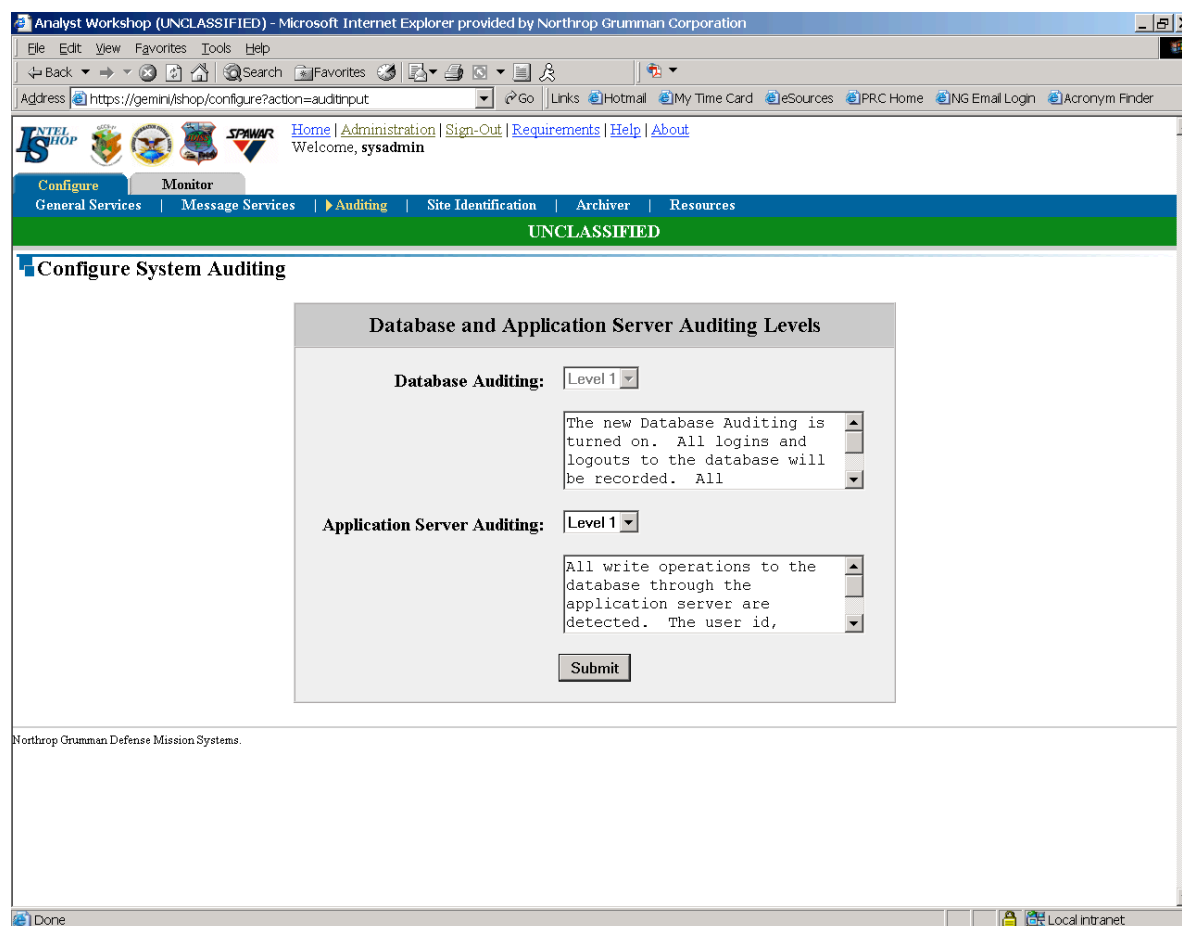
- c. There are specific features associated with each group.

Group assigned to login account	Features Allowed
No group assignment	Home Link, Requirements Link, Help Link, About Link, Survey Link, ISHOP, DISA, JDISS and Spawar Image Links on Welcome tab, Resources on Welcome and Search tabs, Collection Status on Produce tab, Links to any OOB Card/Report (may be displayed under What's New).

Group assigned to login account	Features Allowed
IntelligenceConsumer	Features of everyone plus Sign-in Link, Sign-Out Link, Search on all tabs, all features under My Intel Shop and Search tabs, Patterns/Trends on Analyze tab, Graphic INTSUM on Produce tab, Export on Disseminate tab. Also any links to view a saved Folder (may be displayed under What's New).
IntelligenceProducer	Features of IntelligenceConsumer plus New Candidate to Target List (CTL) on Produce tab. Can also create/modify local records/associations (Data Maintenance Tab only) and insert documents, aliases, and remarks via the OOB Reports.
IntelligenceSupervisor	Features of IntelligenceProducer plus Send To COP and Nominate on the Disseminate tab.
IntelligenceAdministrator	Features of IntelligenceConsumer plus the Configure link

4. The Intelligence Shared Data Server (ISDS) databases should be backed up on a regular basis. The backups can be used to recover from a disaster or a corrupt database. A database disaster can be caused by various conditions, such as a hard drive failure, and can cause the entire ISDS or a specific database to be unusable. During backup operations, the operational state of the GCCS-M system can continue as normal (users may continue to use the system), but should be scheduled during slower times for performance reasons.
 - a. Replication Mode - Normal database backups are not required when in replication mode. National and Local/Alternate view records are replicated to multiple servers. Therefore, daily or weekly backups are not necessary. The system administrator

- would contact the assigned replication administrator to reload the database if the database server or an MIDB database becomes inoperable and requires reloading.
 - b. Non-Replication Mode - Systems not participating in replication must be backed up. System administrators must determine the frequency of the backups. The databases can be backed up weekly under normal operations and daily during critical operations.
5. Database Auditing. As the system and/or database administrator, you can enable Sybase database auditing. Sybase Auditing permits the creation of a log file that records all user connections to the database server (which also includes the **sa** account).
- a. To enable Database Server and Application Server Auditing:
 - (1). Log in as **sysadmin**.
 - (2). Open the browser and in the URL box, enter: **https://appserver/ishop** The Analyst Workshop home page appears.
 - (3). Click Sign-In, log in as sysadmin, and enter the Password.
 - (4). Select the Administration link.
 - (5). Select the Configure tab.
 - (6). Click the Auditing tab. The Configure System Auditing page is displayed.



- (7). Select the Database Auditing level from the corresponding drop-down list. The corresponding description is displayed in the associated read-only text box. See the table below for a list of auditing options and descriptions.

Auditing Type	Option	Description
Database Server	Level 0	Auditing is turned off.
Database Server	Level 1	Database Auditing is turned on. All logins and logouts to the database will be recorded. All transactions of users with the sa_role or sso_role will be recorded.

- (8). Select the application server auditing level from the corresponding drop-down list (Level 1 is the default). The corresponding description is displayed in the

associated read-only text box. See the table below for a list of auditing options and their descriptions.

Auditing Type	Option	Description
Application Server	Level 1	(Default) All write operations to the database through the application server are detected. The user id, system date-time and the surrogate key (SK) of the affected records are recorded.
Application Server	Level 2	All read and write operations to the database through the application server are detected. The user id, system date-time and the surrogate key (SK) of the affected records are recorded.
Application Server	Level 3	All Structured Query Language (SQL) statements are detected. The user id, system date-time and the surrogate key (SK) of the affected records are recorded.

- (9). Click the **Submit** button to save the changes to the auditing levels. The system displays *The audit configuration was successfully saved*. Click **Continue**.

6. Configuring Access Services

- a. You must configure the servers on the network for the Intelligence Analyst Workshop and Intelligence Analyst Web Workshop to recognize them. This is done via the web application. To configure Intelligence Shop Web:
 - (1). Open the browser and in the URL box, enter:
https://appserver/ishop
 - (2). Click **Configure** (top right). Click **Sign In** (top right) and sign in as **sysadmin**.

Configure Services

Enter an IP address or hostname for each server.

Documentation Server:

Local Imagery Server:

Theater Imagery Server:

Mail Server:

Note: Hostnames must be defined in the DNS (Domain Name Services).

- (3). Enter the machine name or IP address of each server in the appropriate text box:
- (4). In the Documentation Server text box do not change the default.
- (5). In the Local Imagery Server text box enter: ITS_HOST.
- (6). In the Theater Imagery Server text box enter: <machine name of Image Product Library> (in most cases)
- (7). In the Mail Server text box enter: <machine name of mail server>, either for AMHS (GCCS-M) or Exchange (GCCS-I3). Click Submit.

7. Server Identifier

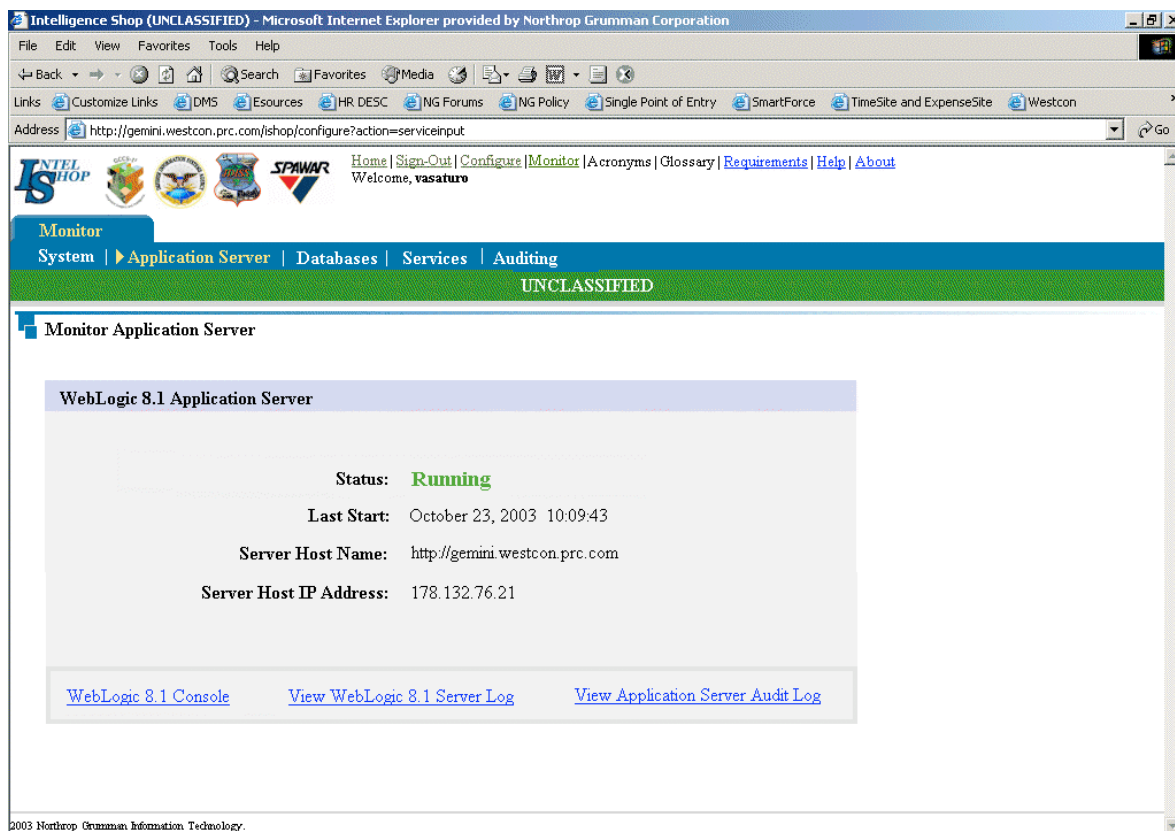
- a. When accessing Intelligence Shop - Web, you can configure Server Identifiers, which are used to assign unique identification numbers, called Site Codes, for the ISDS at every site. With Site Codes attached to each ISDS, users querying the GMI database with intelligence applications such as Intelligence Shop and can identify where the data originated when displayed in their reports. Furthermore, data from a specific site's server can be prioritized so that local data (you can also think of it as the most current data) from that site can be marked "best" for retrieval in database queries. When two or more records match from query, if one is marked with a priority only that one is returned.

- b. To identify Server:
 - (1). Log in as sysadmin.
 - (2). Open the browser and in the URL box, enter: https://appserver/ishop The Intelligence Shop home page appears.
 - (3). Click Configure (top right).
 - (4). Click Sign In (top right) and sign in as sysadmin. The Server Identifier window appears

- (5). In the Site Identification and Prioritization window, go to the pull-down menu under Site Name and scroll through the server list. Select the Site Code and Server Name that corresponds to your server. This list is intended to be comprehensive and cover all sites.
- (6). The server you selected at the top of the Site Identification and Prioritization box. Notice that the current server is always priority number 1. This means that when querying the local data, data from your site is given priority over data from other sites, assuming that the data is similar. Changes are automatically saved when you close the window.

8. Monitor System

- a. The Monitor System page shows the status of the Tactical Message Processor and the Sybase Database Server as well as the percent free space value for every system database.
- b. If the percent free space value drops below 20%, the cell background color becomes red to indicate that administrator action should be taken to extend the database.
- c. Select the **Application Server** option on the **Monitor** screen. The Monitor Application Server page displays. This page provides a link to the COTS application server console, the COTS application server audit log and the ISHOP application server audit log.
- d. Select the Databases option on the Monitor screen. There are three sections on the Monitor Databases page. The Sybase Server section shows the status of the database server and the date and time, it was last started.
- e. There are three sections on the Monitor Services page. The Tactical Message Processor section shows the status of the message processor and the date and time the last message was processed. The Track Archiver section shows the status of the track archiver and the date and time the last track was processed. The Profiles and Notifications section shows the name of each profile for each system user and the number of pending alerts for each profile. If necessary, this section will have horizontal and vertical scrolling.



Intelligence Shop (UNCLASSIFIED) - Microsoft Internet Explorer provided by Northrop Grumman Corporation

File Edit View Favorites Tools Help

Back Forward Stop Search Favorites Media

Links Customize Links DMS Esources HR DESC NG Forums NG Policy Single Point of Entry SmartForce TimeSite and ExpenseSite Westcon

Address http://gemini.westcon.prc.com/ishop/configure?action=serviceinput Go

INTEL SHOP SPAWAR Home Sign-Out Configure Monitor Acronyms Glossary Requirements Help About

Welcome, vasature

Monitor

System | Application Server | Databases | Services | Auditing

UNCLASSIFIED

Monitor Databases

Sybase Server

Current status of the Sybase server.

State: Running

Start Time: October 23, 2003 11:09:12

[View Sybase Error Log](#)

Sybase Replication

Current status of two-way replication.

State: Running

Start Time: October 23, 2003 11:09:12

[More Details](#)

Databases				
Name	Space Allocated	Space Used	Space Free	Percent Free
CTDS	500 MB	400 MB	100 MB	20 %
GMI	12000 MB	8000 MB	4000 MB	33%
IMDB	800 MB	400 MB	400 MB	50%
ISHOPD	300 MB	200 MB	100 MB	33%
SUPPORT	200 MB	150 MB	50 MB	25%

WARNING: Databases with low free space can cause server problems. Refer to the System Administrator Manual to take corrective action.

2003 Northrop Grumman Information Technology.

THIS PAGE INTENTIONALLY LEFT BLANK

INFORMATION SHEET 4-1-3

WEBLOGIC CONSOLE ADMINISTRATION

A. **Introduction**

This Information Sheet will provide the trainee with information about the accessing the Weblogic Console and maintaining all deployed web applications.

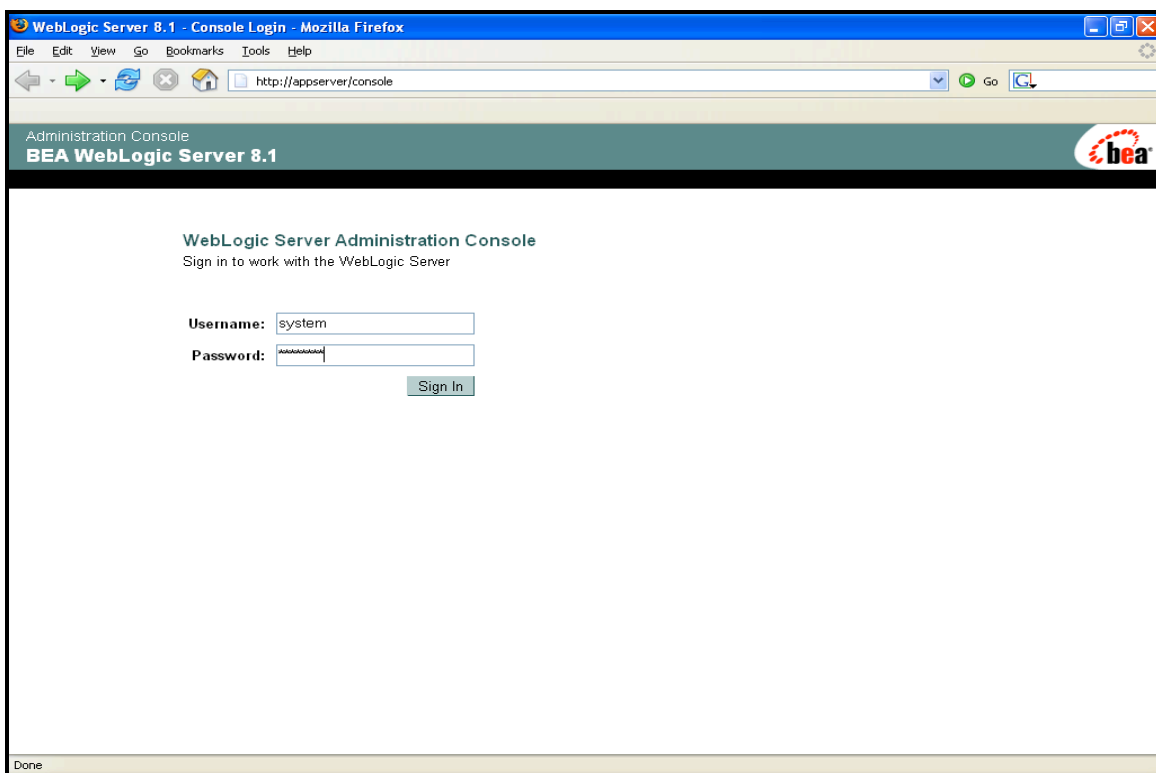
B. **References**

Online Embedded documentation

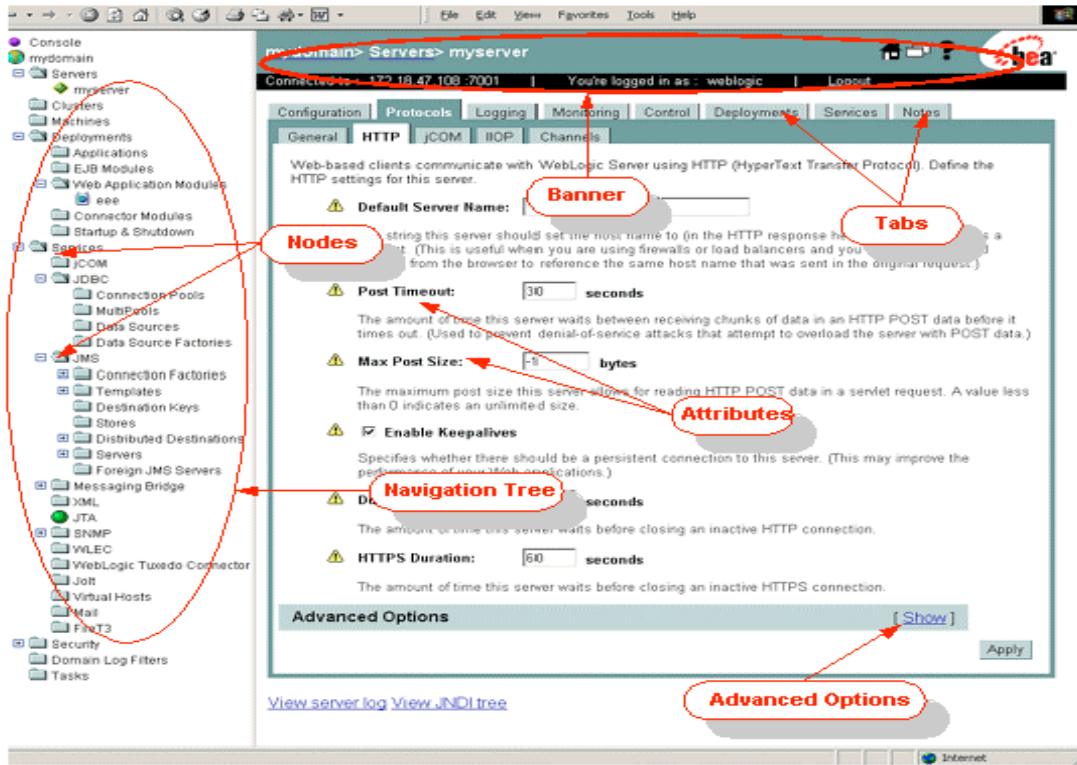
C. **Information**

1. The System Administration Console is a Web browser-based, graphical user interface you use to manage a WebLogic Server domain. One instance of WebLogic Server in each domain is configured as an Administration Server. The Administration Server provides a central point for managing a WebLogic Server domain. All other WebLogic Server instances in a domain are called Managed Servers. In a domain with only a single WebLogic Server instance, that server functions both as Administration Server and Managed Server. The Administration Server hosts the Administration Console, which is a Web Application accessible from any supported Web browser with network access to the Administration Server.
2. The System Administration Console is used to:
 - a. Configure, start, and stop WebLogic Server Instances
 - b. Configure WebLogic Server Clusters
 - c. Configure WebLogic Server Services, such as database connectivity (JDBC), and messaging (JMS).
 - d. Configure security parameters, including managing users, groups, and roles.
 - e. Configure and Deploy your applications.
 - f. Monitor server and application performance.
 - g. View server and domain log files.
 - h. View application deployment descriptors.

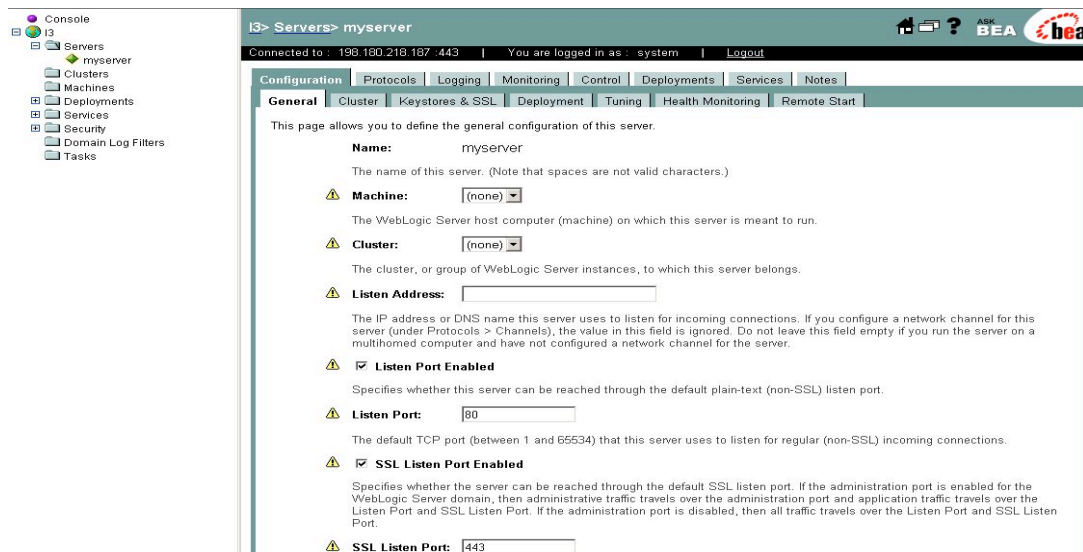
- i. Edit selected runtime application deployment descriptor elements.
3. The WebLogic Server Administration Console allows users to edit configurations or to perform other operations based on the default global security role they are granted. If this security role does not permit editing of configuration data, for example, the data is displayed in the Administration Console but is not editable. If the user attempts to perform a control operation that is not permitted, such as starting or stopping servers, the Administration Console displays an Access Denied error.
4. Accessing the console
 - a. Using a web browser with updated java applet support navigate to <http://appserver/console>
 - b. This will bring up log in and password option



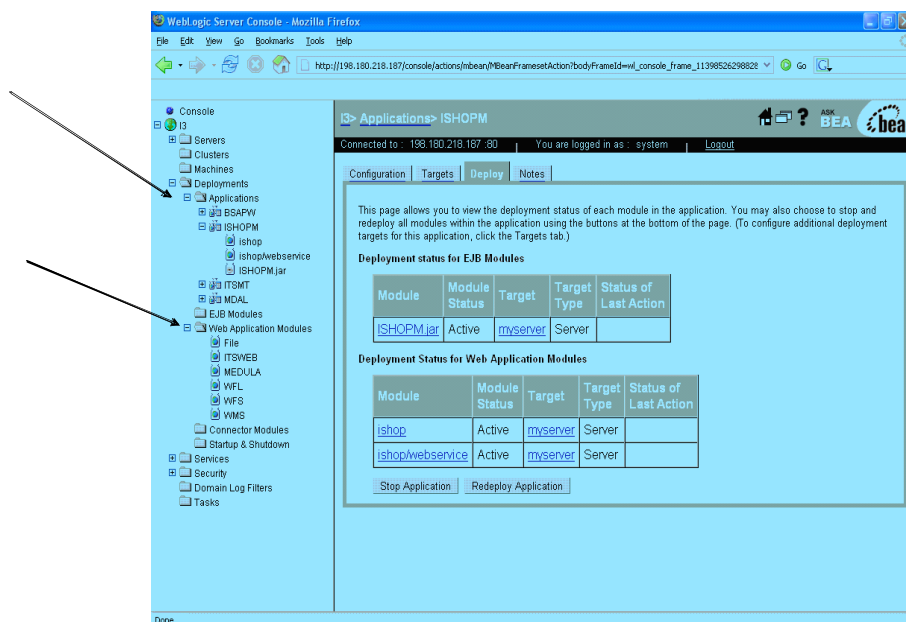
- c. By default the console user name is system, and password is provided during SOVT of system.



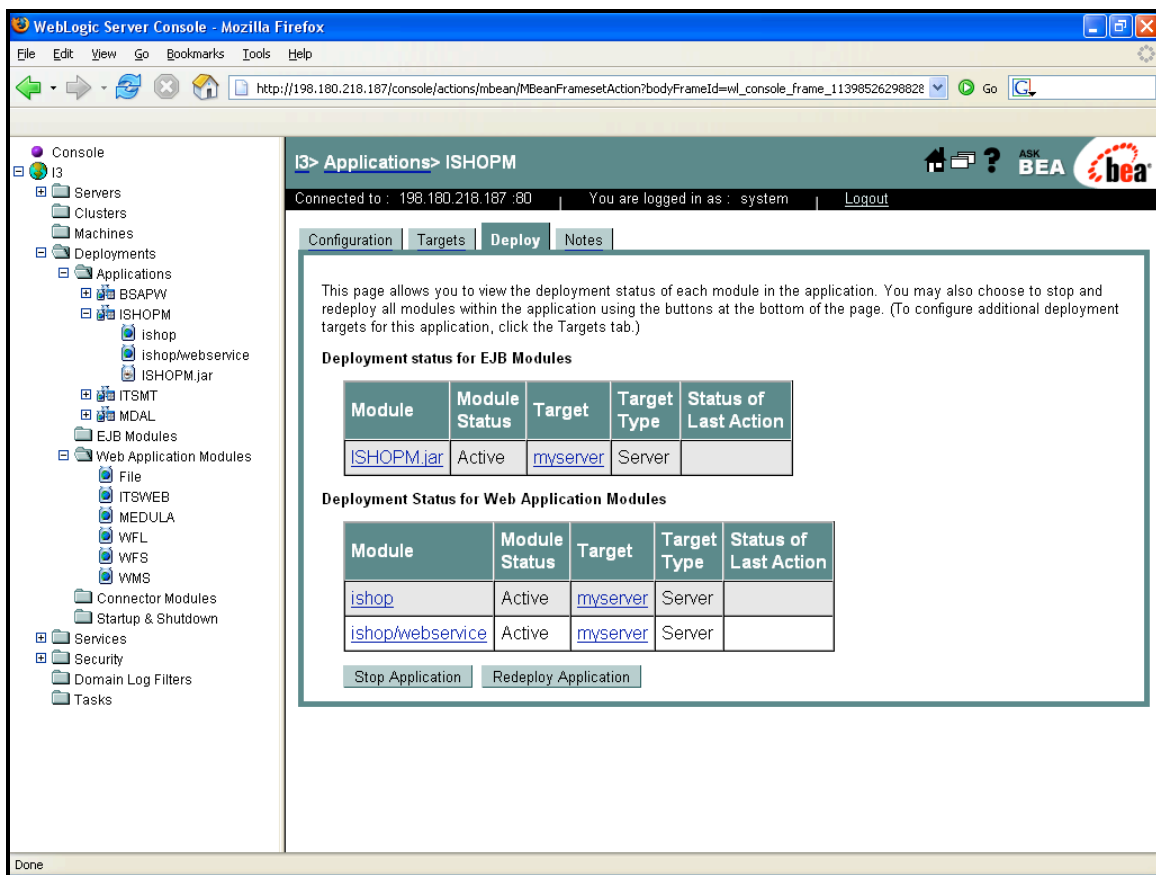
- d. The left panel in the Administration Console contains a navigation tree that is used to navigate to the console pages to manage the domain. By selecting (left-clicking) a *node* in the tree, you can access console pages related to the node, which are displayed in the right panel of the console. If a node in the tree is preceded by a plus sign, you can click on the plus sign to expand the tree to access additional resources.



- e. Through use of this console an administrator can check the current configuration of the appserver to include deployments, authentication, access, data stores.
 - f. Web Applications are typically packaged in an Enterprise Archive (EAR) file with an .ear extension, or can exist in exploded .ear format. An EAR file contains all JAR, WAR, and RAR component archive files for an application and deployment descriptor that describes the bundled components. The META-INF/application.xml deployment descriptor contains an entry for each Web and EJB component, and additional entries to describe security roles and application resources such as databases.
 - g. The Administration Console can be used to deploy an EAR file on the WebLogic Server if it is not already configured.
5. Checking deployment of applications and redeploying
- a. To check the deployment of applications simply navigate through the left pane tree to the deployments line item. This will show a list of current deployments on this web server.
 - b. Extending this subject will reveal 2 topics of interest; Applications, and Web Application Modules.



- c. By selecting an application (ISHOPM for example) and choosing the deployment tab, the status of the application should show ACTIVE, indicating this application is deployed or INACTIVE meaning it is not online.
- d. If this application is not ACTIVE then by clicking the Deploy button the application will change status from INACTIVE to IN Progress. When the process is complete ACTIVE will show and the user should be able to connect to the application via the web browser.

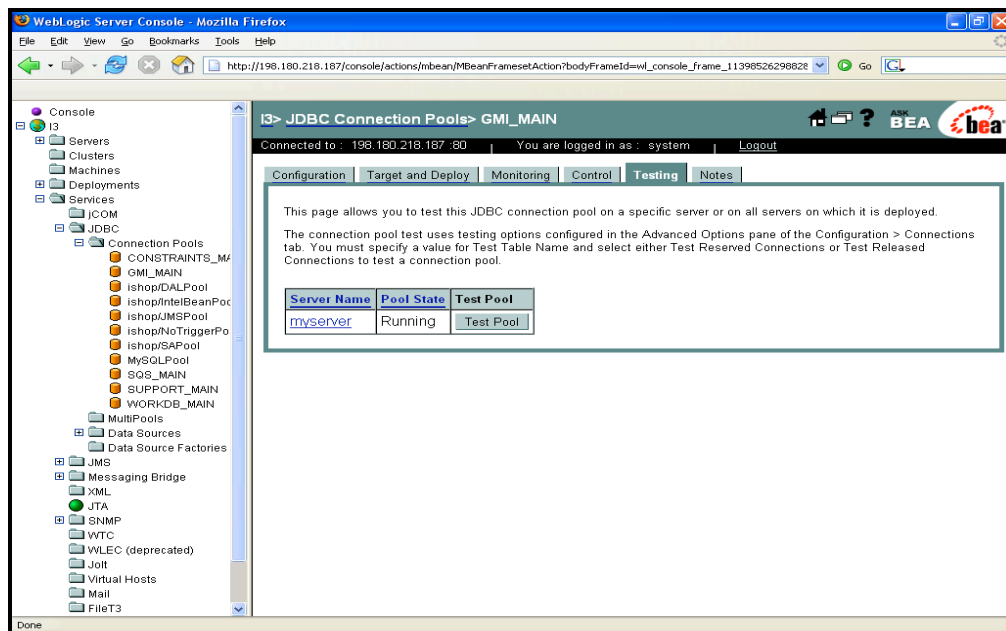
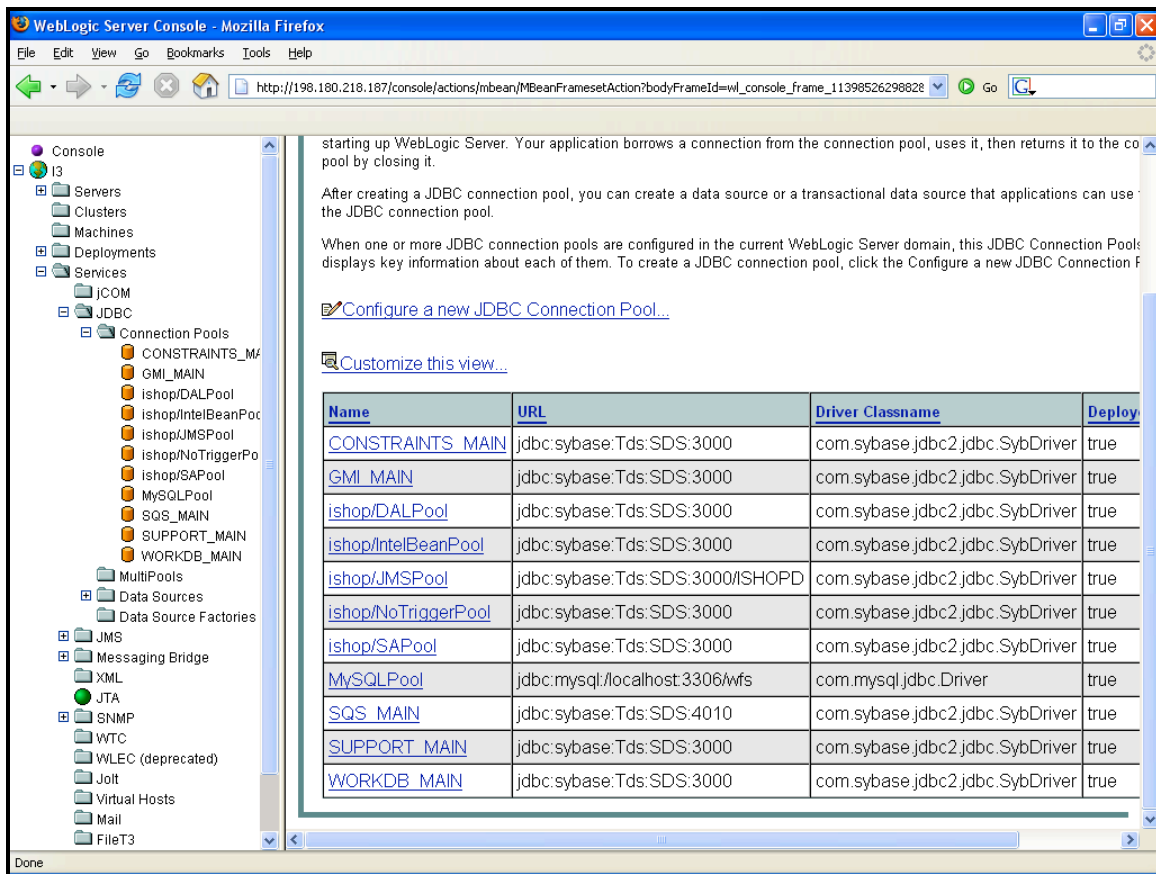


6. Redeploying Web Applications

- a. Redeploy ISHOPM
- b. On the WebLogic Server Console tab, from the Console list, select I3>Deployments (don't expand this list). In the I3>Deployment Order window, click Deploy New Application. In the Location area, click Application. In the Location area, browse to /h/ISHOPM/bin select ISHOPM.ear. Click Continue. On the Review your choices and deploy page, in the Name area, verify ISHOPM is entered and click Deploy.

The page dynamically updates and once the file is deployed, from the File menu, select Quit.

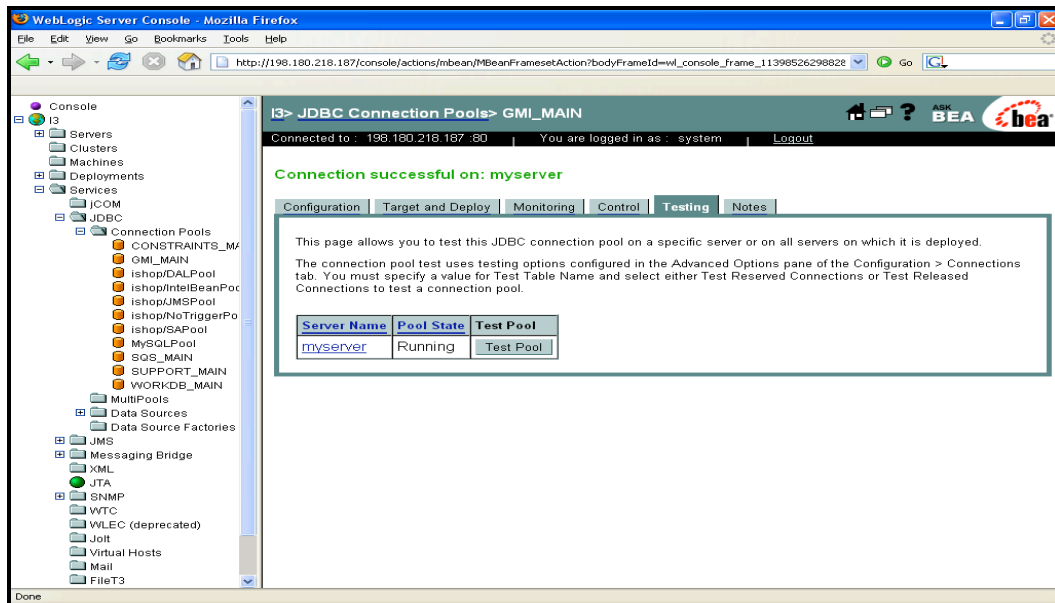
- c. To redeploy webcop
 - d. In the WebLogic Server Console – Mozilla window, on the WebLogic Server Console tab, from the Console list, select I3>Deployments>Web Application Modules (don't expand this list). In the I3>Web Applications areas, on the Configuration tab, click Deploy a new Web Application Module... In the Deploy a Web Application Module area, at the Location: appserver/h/data/local/I3CMT/ I3 prompt, click the h link. In the Deploy a Web Application Module area, at the Location: appserver/h prompt, select WEBCOP. In the Deploy a Web Application Module area, at the Location: appserver/h/WEBCOP prompt, select bin. In the Deploy a Web Application Module area, at the Location: appserver/h/WEBCOP/bin prompt, select webcop.war. Click Target Module. If the Security Warning window appears, click Continue. Click Deploy. If the Security Warning window appears, click Continue.
7. Checking data store user and password to actual SQL user and password
- a. Inside the tree structure on the left pane there is the Services Subject.
 - b. Extending this shows one topic of interest to the system administrator: JDBC. The JDBC Connection Pools are the connection to the SQL databases for Intel.
 - c. Each connection is user specific. This user is a replica of the actual user in the SQL database. These users and passwords have to match. To check connectivity click on a database connection (ie GMI_MAIN) from here click Testing Tab.
 - d. Then select test Pool. If the return is success, then your connection is established.



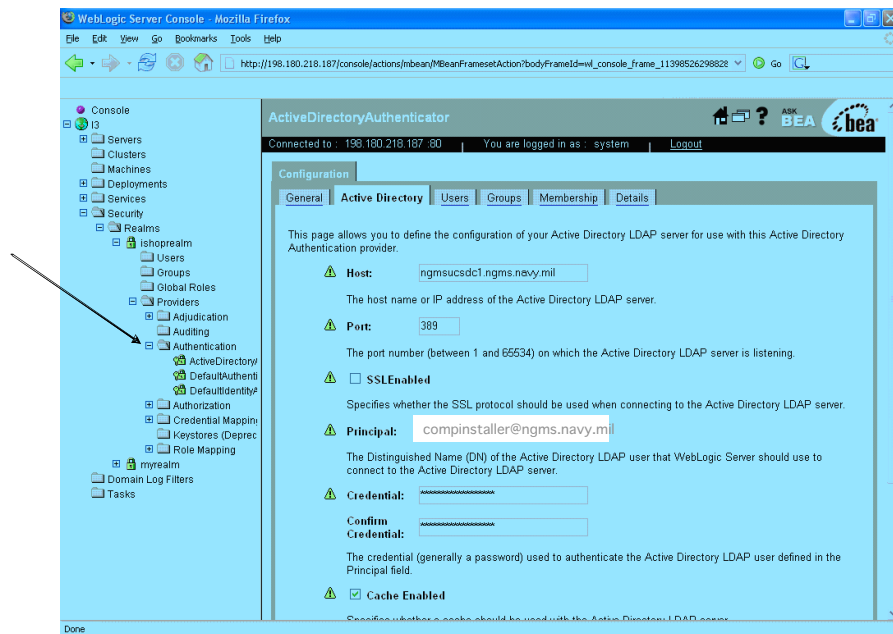
e. If a failure is received, check the Intel server for the possible errors:

- The Intel server was rebooted after the web server.

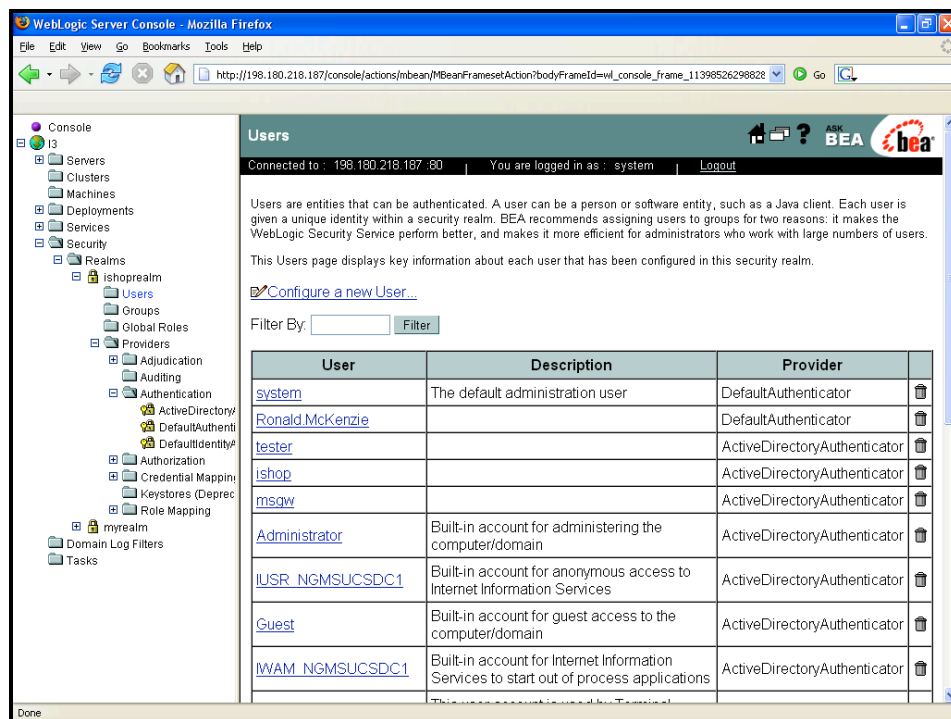
- The Intel server is not reachable
- The SQL database has different credentials for this user/database than specified in the appserver console.



8. Checking LDAP connection, Authentication and users/groups
 - a. Navigating down the left pane to the Security subject, expand further into this topic to see the current users and groups under the ishoprealm. A key object in this subject is the user responsible for the LDAP (lightweight Directory Access Protocol) connection that provides user and groups from the Active Directory domain. This is typically set during the I3CMT configuration module of the Load Plan.
 - b. Navigate to Realms, ishoprealm, providers, authentication. Inside this topic is a topic called ActiveDirectoryAuthentication. Selecting this will show the user and credentials (password) used to connect to the server specified on the same page.

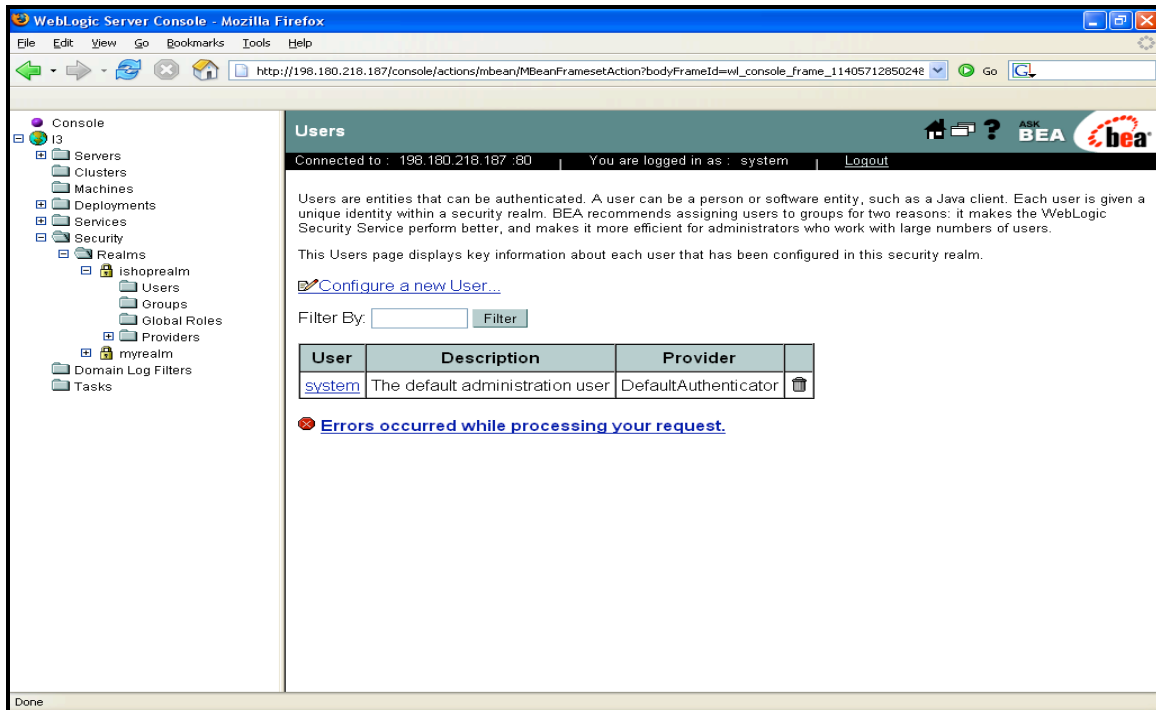


- c. Also, directly under the ishop realm are 2 topics (users and groups) these are the users and groups provided by the connection above.



- d. This is important to note, because if this user's password is changed on the active Directory side, it must be changed in the credentials, or when you look at the users and groups you will see an empty window, a red X and errors.

- e. This connection must be available to provide access to all GCCS-M Web Applications.



9. WebLogic Log Files

- a. The following WebLogic log files can be used for troubleshooting purposes. Other log files are available and it is important to note that the WebLogic Web Server can take a few minutes to start-up completely after a reboot.
(h/data/local/I3CMT/I3/logs/weblogic.log and wl-domain.log).
- b. The Administration Console can be used to view the log file for any server in the domain, regardless of whether the server is located on a remote computer for which you might not have login privileges.
- c. In addition, the Administration Console's log file viewer provides filtering tools that you can use to limit the set of messages that it displays.
- d. To view a server's log messages from the Administration Console: In the left pane of the Administration Console, expand the Servers folder and right-click the server whose log you want to view.

INFORMATION SHEET 4-4-4

IMAGE TRANSFORMATION SERVICES (ITS)

A. **Introduction**

This Information Sheet will provide the trainee with information about the ITS services provided by the intel machine and ITS related segments.

B. **References**

System Administrator's Manual (SAM) for the Documentation, Application, Database Server, and Intelligence segments

C. **Information**

1. ITS Admin Utilities
 - a. The user interface to administer the ITS Server is provided by the ITS Admin utilities of the ITS Client segment.
 - b. Set up the initial configuration of the ITS Server after the ITS Server segment is installed and before the ITS Server is used operationally.
 - c. Maintain the ITS Server and perform configuration adjustments after the ITS server is operational by adhering to procedures in the SAM.
2. ITS Client
 - a. The ITS Client segment provides a standardized set of software libraries which can be used by imagery applications to access the ITS Server for retrieval and storage of imagery.
 - b. The ITS Client libraries include tools for data entry, catalog query/selection, remote server queries, and data retrieval.
3. ITS and ISDS Segment Descriptions
 - a. Video Ingestor
 - (1). The Video Ingestor (VI) segment provides conversion of analog streams of motion imagery into digital streams of data.
 - (2). Supports MPEG 1 and MPEG 2.

- (3). Analyst settable encoding parameters. Parses telemetry from analog video stream.
- b. Universal Data Import/Export (UDIE)
- (1). This segment provides standardized imagery import and export services as well as provides a user interface for the ITS imagery transformations The mission of UDIE is to provide standardized imagery import and export services as well as provide a user interface for the ITS imagery transformation utilities.
 - (2). UDIE provides an application which allows imagery on the ITS server to be converted between various DoD and commercial formats, to be scaled, to be rotated, and to be exported to a variety of managed media. UDIE also allows the import of imagery from a variety of magnetic media into the ITS server. UDIE capabilities include:
 - Converting between the following formats: NITF, VITec, Sun Raster, XWD, TGA, TIFF, GIF, JPEG, and Flat Image.
 - Importing multiple images from tape or disk into the ITS server.
 - Exporting selected images from the ITS server, while converting to a user defined format, to tape or disk
 - Supported video formats are MPEG1 and MPEG2.
- c. Automated Image Import Module (AIIM)
- (1). This segment provides tools for users that allow them to easily populate the *ITS Server Catalog* with products and information about products that are available through other servers and are located on the local LAN
 - (2). Interface to schedule queries against various imagery archives including ITS, IPL, and 5D for data entry, catalog query/selection and data retrieval.
 - (3). Automated image and video imports from LAN resources.
 - (4). Netscape plug-in/helper application to preview (non-native) and save imagery and video products to ITS
 - (5). Utility on Windows to allow users to drag and drop digital products on an ITS Drop Target Icon and have them automatically cataloged in *ITS*

- d. Analyst Workshop (ISHOP C) – Supports Intel Workflow (Identify Threat, Focus/Organize, Maintain Threat, Produce, Disseminate) Analyst Workshop Java Component: Platform independent Java Application, built on middle tier foundation, tightly coupled with ICSF, geared towards Intel Analyst.
- e. Analyst Web Workshop(ISHOPM): Web based Intel applications, built on middle tier foundation, geared toward Intel Consumer, smaller footprint than Java Application
- f. Intelligence Shop Office (ISHOPO): MS Excel Plug-in geared towards the Intel Analyst who is more comfortable working in an MS Office environment.
- g. STRMGR (Stream Manager), Win2K PC & Solaris 8
 - (1). The purpose of the Stream Manager (STRMGR) segment is to receive TCPIP video and telemetry streams from the NT Video Ingestor workstation. The STRMGR software then, based upon configuration, will convert the TCPIP streams to UDP streams and will either multicast the streams across the LAN to all workstations, or will simply perform an internal UDP stream for the workstation where STRMGR is installed. If the Alerts segments are installed, STRMGR will also generate an alert to the Alerts Server, which will be used by the NOTIF segment.
- h. NOTIF (Notification Services), Win2K PC & Solaris 8
 - (1). This segment is to notify and alert users to the arrival of requested data. This software works in conjunction with the ALERTS Server (ALTSRV) software. The NOTIF segment uses the Alerts Client (ALTCLT) to receive streaming video alerts generated by Stream Manager. NOTIF provides the following specific abilities:
 - Launch applications based upon data arrival, such as JIVE to view the streaming video, or IMGR TelemetryCatcher to plot the video telemetry on the system chart
 - Popup visual screens with text messages upon data arrival
 - Play configurable audio alerts upon data arrival.
 - Provide per-user configuration of actions to be taken when streaming video alerts are received or cancelled.
- i. NITFS (National Imagery Transmission Format Services), Win2K PC & Solaris 8

- (1). The mission of the NITF Services is to supply a standardized set of software libraries used by imagery applications to process NITF formatted imagery files. The NITF Services libraries include tools to parse an NITF file into its components, as well as to assemble a valid NITF file from individual components. Tools are also provided to access, edit, create and delete each component of an NITF file. The NITF Services libraries provide the following functions to imagery applications through APIs:
 - Provide NITF 2.0, 2.1, and NSIF (Compliance Level 6) file format read/write capability for imagery applications.
 - Unpack NITF files into component elements (image, symbol, label, text).
 - Provide NITF image data decompression services.
 - Provide access (select, edit, add, and delete) to each element of an NITF file.
 - Provide NITF image data compression services.
 - Pack the component elements into a valid NITF file.
- j. ITS Client (Image Transformation Services), Win2K PC & Solaris 8
 - (1). The mission of the ITS Client is to supply a standardized set of software libraries which can be used by imagery applications to access the ITS Server for retrieval and storage of imagery. The ITS Client libraries include tools for data entry, catalog query/selection, remote server queries, and data retrieval. The ITS Client provides the following:
 - Client application interface to the ITS Server for data entry, catalog query/selection, data retrieval, and remote server queries.
 - Software library for integration with client applications.
 - Point and click query specifications.
 - Client runtime customization of the query window.
- k. IMX (Imagery Transformation Services), Win2K PC & Solaris 8
 - (1). The mission of the Image Transform Utilities (IMX) segment is to provide image data transformations (rotations and scaling), and image data format translations.
- l. ITSSVR (Image Transformation Services Server), Win2K PC & Solaris 8

- (1). The mission of the ITS Server is to provide cataloging, linking, management, selective archiving, and retrieval of digital imagery and related products. The ITS Server is scaleable software application which uses standard distributed processing techniques to provide client applications access to digital imagery. The ITS Server handles client application requests for data entry, catalog query/selection, and data retrieval.
 - (2). The ITS Server provides data integration with GCCS by maintaining the imagery catalog within the Intelligence Shared Data Server (ISDS), creating links between imagery and other intelligence data, and providing seamless access to an IPL (Image Product Library). The ITS Server provides the following functions:
 - Execute ITS Client application requests.
 - Brokers ITS Client application requests for data from an IPL.
 - Provides local imagery data management.
 - Provides a local cache for imagery pulled from an IPL.
 - Creates links between the Imagery and MIDB.
- m. JIVE (Java Image and Video Exploitation), Win2K PC & Solaris 8
- (1). The mission of Java Image Video Exploitation (JIVE) is to provide a GOTS image and video viewing and exploitation application for all imagery users. JIVE provides the ability to display, manipulate, and annotate any image cataloged by the ITS Server.
 - (2). JIVE also includes the capability to view MPEG-1 and MPEG-2 video clips. JIVE can play streaming video and telemetry and generating MPEG-1 video clips from these video streams. Video clips that are generated with JIVE can then be selectively stored to the ITS Server. This version of JIVE supports viewing of NITF, GIF and JPEG image file formats and MPEG-1 and MPEG-2 video clips.
- n. AIIM (Automated Image Import Module), Win2K PC & Solaris 8
- (1). The Automated Image Import Module (AIIM) segment consists of several applications and services designed to provide a means for automatically importing imagery from local and remote file systems into the ITS Server and

to provide management of the ITS Server search profiles and standing queries. Specifically, the segment provides an automated ability to import imagery from various sources, such as the GBS/JBS broadcast, into the ITS Server, to maintain a log of the received data and to optionally notify the user when new data is received.

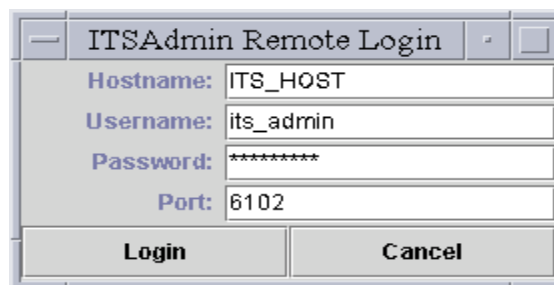
- (2). AIIM also provides the ability to configure and manage the retrieval of imagery from remote servers such as IPL by providing set-up tools for the ITS Server data search profiles and standing queries.
- (3). The AIIM software also provides a seamless method for importing imagery to the ITS Server when running Netscape (WEBBr) to download imagery. The image import module recognizes the following image formats: NITF 1.1, NITF 2.0, GIF, JPEG, TIFF, Sun Raster, Vitec, and XWD. All NITF imagery imported will be parsed and AIIM will update the Imagery Database (IMDB).

o. Imagery Database (IMDB)

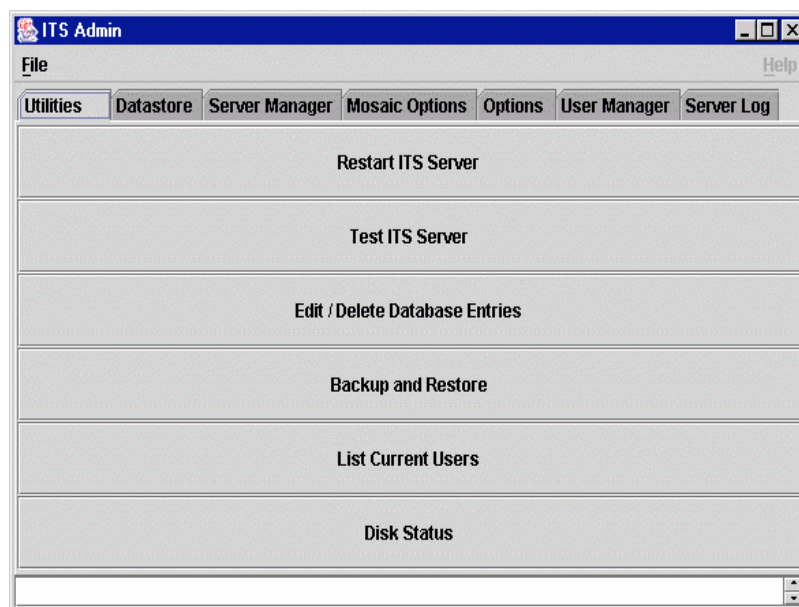
- (1). The mission of Image Manager is to provide an application for accessing imagery from the Common Operational Picture (COP) and for merging imagery into the COP. Image Manager provides the ability to query the ITS Server and display metadata for the subset of imagery specified by conditions set in the ITS Query Window (the functionality available to any client using the ITS Query Window).
- (2). In addition, the user may rubberband an area of interest on the COP and retrieve imagery metadata based on the geographic coordinates of this area. Footprints of the specified subset of imagery are plotted on the COP (and may be hidden via the COP's filtering capabilities). The user may select any number of images from the ITS QueryWindow results table to retrieve the actual imagery data from the ITS Server and display it in the COP. The imagery displayed in the COP may be selectively hidden using COP filtering functions or may be removed from the COP (to free up memory). Once Image Manager merges an image with the COP, a variety of COP information (such as tracks, MIDB symbols, etc.) can be plotted over the imagery

p. ITSWEB (ITSWeb Interface) Solaris 8

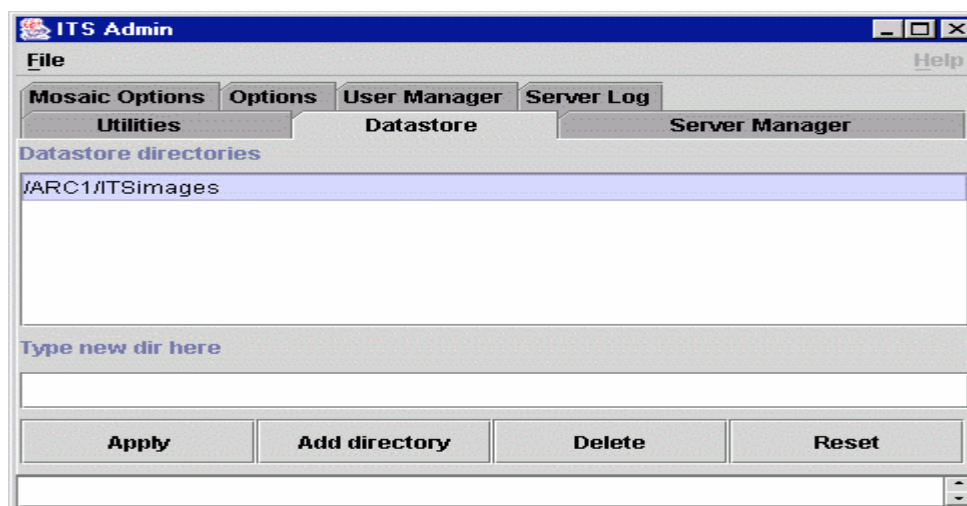
- (1). The mission of ITSWeb is to provide access to the ITS Server via a Web browser interface. ITSWeb provides the CGI interface that allows archiving, cataloging, and retrieval of digital products and related data using an Internet browser (Netscape or Internet Explorer) for pulling and pushing images to and/or from ITS Server.
 - (2). Requesting the appropriate URL generates the user interface for retrieving or storing imagery data. Additional functions provided by ITSWEB include image format transformations and image scaling.
4. Use ITS Admin to Configure the ITS Server datastore directories
- a. Login with an operator account that has the IntelligenceAdministrator group assigned to it and go into the Applications folder, DII APPS folder, then the ITS folder.
 - b. Start ITS ADMIN by selecting (double clicking) the ITS ADMIN icon in the ITS folder.
 - c. The following is the ITS Admin login window:



- (1). Login with an ITS Admin privileged account to display the following ITS Admin window.
- (2). The Operating System account used to access ITS Admin must have the **IntelligenceAdministrator** Group assigned, otherwise ITS Admin will not launch.
- (3). By default the Utilities tab is selected.



- (4). Select the Datastore Tab and select the default storage directory (/h/data/local/ITSSVR/data/images) and select the Delete button to remove the default ITS datastore directory that comes with a fresh load.
- (5). Under Type new dir here enter the correct ITS Server datastore directory path (for example: /ARC1/ITSimages or /home2/ITSimages or /farm1/ITSimages) and select the Add directory button.



- (6). Do this step for each disk/partition/directory that the ITS Server will use for data storage.

- (7). Select the Apply button once all directories have been added and you will be prompted to restart the ITS Server before the changes will take affect. Select Yes to restart the server.
 - (8). This will update the /h/data/local/ITSSVR/data/config/datastorefile with each disk/directory. The following text is an example of what might be in the ITSSVR datastorefile. This file can be manually edited using vi in an xterm, but will not take affect until the ITS Server is restarted
5. Use APM Client to Create an Administrator Account for ITS Admin
 - a. Login as secman and Launch APM Client. (Applications → Application Manager → DII_APPS → SecAdm → APMClient)
 - b. Click on the Accounts tab. Click on File → New Account
 - c. In the Login field, enter a login name. (for example: its_admin)
 - d. Enter the Password and Password Confirm. (prompted to change at first login)
 - e. Enter the Full Name of the user.
 - f. Set Template to None.
 - g. Set Shell to /bin/csh.
 - h. Set Home server to EACH HOST.
 - i. Set Manage as to Local.
 - j. Set the Default Group to Users
 - k. Click on the Groups tab and assign the following groups to the user: Intelligence Administrator, IMTK, SINOPS, and others as needed
 - l. Click on the Profiles tab and assign the desired profile (profile name may vary per site)
 - m. Click on the Hosts tab and assign the appropriate host(s).
 - n. Click on Submit.

THIS PAGE INTENTIONALLY LEFT BLANK