



USER MANUAL

ATCS SERVER (ASERVER) DATA MANAGEMENT SOFTWARE

FEBRUARY 2007 (REVISED AUGUST 2014)

**DOCUMENT NO. COM-00-02-10
VERSION A.1**

Siemens Industry, Inc. Rail Automation
9568 Archibald Ave., Suite 100,
Rancho Cucamonga, California 91730
1-800-793-SAFE

Copyright © 2007 - 2014 Siemens Industry, Inc.
All rights reserved

PRINTED IN U.S.A.

PROPRIETARY INFORMATION

Siemens Industry, Inc. has a proprietary interest in the information contained herein and, in some instances, has patent rights in the systems and components described. It is requested that you distribute this information only to those responsible people within your organization who have an official interest.

This document or the information disclosed herein, shall not be reproduced or transferred to other documents or used or disclosed for manufacturing or for any other purpose except as specifically authorized in writing by **Siemens Industry, Inc.**

TRANSLATIONS

The manuals and product information of Siemens Industry, Inc. are intended to be produced and read in English. Any translation of the manuals and product information are unofficial and can be imprecise and inaccurate in whole or in part. Siemens Industry, Inc. does not warrant the accuracy, reliability, or timeliness of any information contained in any translation of manual or product information from its original official released version in English and shall not be liable for any losses caused by such reliance on the accuracy, reliability, or timeliness of such information. Any person or entity that relies on translated information does so at his or her own risk.

WARRANTY INFORMATION

Siemens Industry, Inc. warranty policy is as stated in the current Terms and Conditions of Sale document. Warranty adjustments will not be allowed for products or components which have been subjected to abuse, alteration, improper handling or installation, or which have not been operated in accordance with Seller's instructions. Alteration or removal of any serial number or identification mark voids the warranty.

SALES AND SERVICE LOCATIONS

Technical assistance and sales information on **Siemens Industry, Inc.** products may be obtained at the following locations:

SIEMENS INDUSTRY, INC. RAIL AUTOMATION
2400 NELSON MILLER PARKWAY
LOUISVILLE, KENTUCKY 40223
TELEPHONE: (502) 618-8800
FAX: (502) 618-8810
SALES & SERVICE: (800) 626-2710
WEB SITE: <http://www.rail-automation.com/>

SIEMENS INDUSTRY, INC. RAIL AUTOMATION
939 S. MAIN STREET
MARION, KENTUCKY 42064
TELEPHONE: (270) 918-7800
CUSTOMER SERVICE: (800) 626-2710
TECHNICAL SUPPORT: (800) 793-7233
FAX: (270) 918-7830

FCC RULES COMPLIANCE

The equipment covered in this manual has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his/her own expense.

DISCLAIMER

ASERVER AND WCCMAINT ARE DIAGNOSTIC TOOLS DESIGNED FOR NETWORK MANAGEMENT AND TROUBLESHOOTING. IT IS POSSIBLE TO RESET OR MISCONFIGURE REMOTE UNITS IN SUCH A WAY THAT CODELINE (CTC) TRAFFIC IS DISRUPTED. THE PURPOSE OF THIS DOCUMENT IS TO ACQUAINT THE END USER WITH THE FULL RANGE OF CAPABILITIES OF THESE TOOLS; AND THEIR USE MUST BE COMBINED WITH SPECIFIC KNOWLEDGE OF THE USER'S SIGNALING SYSTEM TO ENSURE UNINTERRUPTED SERVICE. ANY DIAGNOSTIC PROCEDURES THAT COULD DISRUPT SERVICE ARE CLEARLY MARKED AND SAFETRAN ASSUMES NO RESPONSIBILITY FOR ANY MISUSE OF THESE TOOLS, ACCIDENTAL OR OTHERWISE.

DOCUMENT HISTORY

Version	Release Date	Sections Changed	Details of Change
1.0	7-23-02		Preliminary released. Based on raw input from M. Knoblock. Inserted in Technical Information project loop on 6-6-02 awaiting available writer.
A	Feb 2007	All	Updated version from M. Knoblock for ver 5.0 sfw and higher.
A.1	Aug 2014		Convert to Siemens branding

TABLE OF CONTENTS

<u>Section</u>	<u>Title</u>	<u>Page</u>
	PROPRIETARY INFORMATION.....	II
	TRANSLATIONS.....	II
	WARRANTY INFORMATION	II
	FCC RULES COMPLIANCE.....	II
	DISCLAIMER.....	III
	DOCUMENT HISTORY	IV
	TABLE OF CONTENTS.....	V
	LIST OF ILLUSTRATIONS.....	VIII
	LIST OF TABLES.....	IX
	GLOSSARY	XI
1.0	INTRODUCTION.....	1-1
1.1	HARDWARE/SYSTEM REQUIREMENTS.....	1-3
1.2	SOFTWARE VERSIONS.....	1-3
1.3	SUPPORTING APPLICATIONS	1-4
	1.3.1 SECURITY.....	1-4
	1.3.2 WINDOWS APPLICATION LOG SUPPORT	1-4
	1.3.3 SYSTEM PERSONALITY	1-4
	1.3.4 NMS SERVICES MANAGER.....	1-5
	1.3.5 NMS SERVICES.....	1-5
2.0	INSTALLATION	2-1
2.1	RUN SETUP (REQUIRED).....	2-2
2.2	INSTALL SERVICES MANAGER (OPTIONAL).....	2-3
2.3	INSTALL SERVICES (OPTIONAL).....	2-4
2.4	INSTALL PERSONALITY MODULE	2-4
2.5	RELOCATE FILES (REQUIRED)	2-4
2.6	DATABASE SETUP (REQUIRED)	2-4
	2.6.1 MICROSOFT ACCESS:.....	2-5
	2.6.2 SQL SERVER:.....	2-5
2.7	DATA SOURCES (REQUIRED).....	2-5
	2.7.1 DATA LINK FILE METHOD.....	2-6
	2.7.2 ODBC METHOD	2-10
2.8	EDIT SAFETRAN.INI (REQUIRED)	2-12
	2.8.1 DATA SOURCES.....	2-12
	2.8.2 RAILROAD NUMBERS	2-13

2.8.3	FILE PATHS.....	2-14
2.8.4	SECURITY.....	2-14
2.9	SETUP WINDOWS LOGGING (OPTIONAL).....	2-15
2.10	CONVERT INI FILES TO MS_ACCESS (OPTIONAL):.....	2-17
2.11	RUN ASERVER FOR THE FIRST TIME:.....	2-17
3.0	CONFIGURATION	3-1
3.1	INTRODUCTION	3-1
3.1.1	RAILROADS.....	3-3
3.1.2	SUBNET IP ADDRESSES.....	3-3
3.1.3	DATABASE / FILE PATHS.....	3-5
3.1.4	SUBSYSTEMS	3-6
3.1.5	SECURITY.....	3-8
3.1.6	TCP SOCKETS.....	3-10
3.1.7	CRITICAL ALERTS	3-11
3.2	ASERVER CONFIGURATION OPTIONS LISTING	3-13
4.0	OPERATION.....	4-1
4.1	INTRODUCTION	4-1
4.2	THE ASERVER CONSOLE.....	4-2
4.3	MAIN MENU.....	4-8
4.3.1	FILE SUBMENU	4-8
4.3.1.1	FILE: Configure.....	4-8
4.3.1.2	FILE: Enable Tracing.....	4-8
4.3.1.3	FILE: Exit.....	4-8
4.3.2	VIEW SUBMENU.....	4-8
4.3.2.1	VIEW: Event Log.....	4-9
4.3.2.2	VIEW: Tracing.....	4-11
4.3.2.3	VIEW: Routing.....	4-14
4.3.2.4	VIEW: Errors.....	4-16
4.3.2.5	VIEW: IPxref.....	4-16
4.3.2.6	VIEW: Refresh.....	4-17
4.3.2.7	VIEW: WCMs.....	4-17
4.3.2.8	VIEW: WCCs.....	4-17
4.3.3	SERVICES SUBMENU	4-18
4.3.3.1	SERVICES: Manager.....	4-18
4.3.4	AUX SUBMENU	4-19
4.3.4.1	AUX: Send Time.....	4-19
4.3.4.2	AUX: Enable L2 Segments.....	4-19
4.3.4.3	AUX: Slow Broadcast.....	4-19
4.3.4.4	AUX: Node Dump.....	4-19

4.3.4.5	AUX: Route Dump.....	4-19
4.3.4.6	AUX: Config/Exec Tracking.....	4-20
4.3.4.7	AUX: Track DB Cache.....	4-20
4.3.4.8	AUX: Dump DB Cache.....	4-20
4.3.4.9	AUX: Field Alarms To Socket.....	4-20
4.3.5	HELP SUBMENU	4-20
4.3.5.1	HELP: Version.....	4-21
4.4	DIAGNOSTIC MODES	4-23
4.4.1	EXCLUSIVE MODE.....	4-23
4.4.2	CO-RESIDENT OCG MODE.....	4-25
5.0	SECURITY	5-1
5.1	INTRODUCTION	5-1
5.2	INITIAL SETUP	5-2
5.2.1	ENABLE SECURE MODE	5-2
5.2.2	SHUT DOWN AND RESTART	5-3
5.2.3	START USER MANAGER.....	5-4
5.3	THE USER MANAGER.....	5-5
5.3.1	SECURITY PERMISSION BIT DESCRIPTIONS.....	5-7
5.3.2	PASSWORD OPTIONS	5-8
5.3.3	CREATING A NEW USER.....	5-9
5.3.4	ASSIGNING PERMISSIONS TO A USER.....	5-9
5.3.5	CHANGING USER PASSWORD	5-10
5.3.6	SAVING CHANGES	5-10
5.4	ADDITIONAL SECURITY FEATURES	5-11
5.4.1	NODE DISPLAY	5-11
5.5	MENU FUNCTIONS.....	5-12
5.5.1	LAUNCH USER MANAGER.....	5-12
5.5.2	LOCK/UNLOCK CONSOLE	5-12
5.5.3	SEND CLIENT MESSAGE.....	5-13
 APPENDIX A – ADVANCED TRAIN CONTROL SYSTEM		A-1
 APPENDIX B – ATCS SPECIFICATION 250 RAILROAD CODE LIST		B-1
 APPENDIX C – DATA SOURCE SETUP FOR SQL SERVER		C-1
 APPENDIX D – WCC AND OCG SUBNETTING		D-1
 APPENDIX E – SERVER CONTENTION HANDLING.....		E-1
 APPENDIX F – WCM SUBSYSTEMS.....		F-1
 APPENDIX G – SNMP ALARM SERVICE (Applicable to CSX systems only)		G-1

LIST OF ILLUSTRATIONS

<u>Figure No.</u>	<u>Title</u>	<u>Page</u>
Figure 1-1.	ASERVER Process Interconnection	1-1
Figure 1-2.	ASERVER Physical Connectivity	1-2
Figure 2-1.	Data Link Properties Dialog Box	2-6
Figure 2-2.	Data Link Properties Dialog Box – Provider Tab	2-7
Figure 2-3.	Data Link Properties Dialog Box – Connection Tab	2-8
Figure 2-4.	Database Browse Window	2-8
Figure 2-5.	Data Link Dialog Box Showing Selected Database	2-9
Figure 2-6.	ODBC Data Source Window	2-10
Figure 2-7.	Create New Data Source Selection Window	2-10
Figure 2-8.	ODBC Microsoft Access Setup Window	2-11
Figure 2-9.	Select Database Dialog Box	2-11
Figure 2-10.	Event Viewer Window	2-15
Figure 2-11.	Event Properties Window With DLL Registration	2-16
Figure 2-12.	Event Properties Window Without DLL Registration	2-16
Figure 2-13.	The ASERVER Console	2-18
Figure 2-14.	ASERVER Error Display	2-19
Figure 3-1.	ASERVER Configuration Menu Selection	3-2
Figure 3-2.	Online Configuration Form – Railroads Tab	3-2
Figure 3-3.	Online Configuration – Subnet IP Tab	3-3
Figure 3-4.	Online Configuration – Database/Paths Tab	3-5
Figure 3-5.	Online Configuration – Subsystems Tab	3-6
Figure 3-6.	Screen Displays From WCCMAINT.EXE	3-7
Figure 3-7.	Online Configuration – Security Tab	3-8
Figure 3-8.	Online Configuration – Security Features	3-9
Figure 3-9.	Online Configuration – TCP Sockets	3-10
Figure 3-10.	Online Configuration – Alerts Tab	3-11
Figure 3-11.	Alert Text Display Window	3-12
Figure 4-1.	ASERVER Console (Upper)	4-2
Figure 4-2.	ASERVER Console (Lower)	4-4
Figure 4-3.	ASERVER Menu Bar – File Submenu	4-8
Figure 4-4.	ASERVER Menu Bar – File Submenu	4-8
Figure 4-5.	Event Log Window	4-9
Figure 4-6.	Event Log Window Filtered To Show Alarms Only	4-10
Figure 4-7.	The Trace Window	4-11
Figure 4-8.	Full Trace Warning Message	4-13
Figure 4-9.	ASERVER Routing Table Window	4-14
Figure 4-10.	Route List Sorted By Route Number	4-15
Figure 4-11.	ASERVER Errors Window	4-16

Figure 4-12. IP Cross Reference Table Window..... 4-16

Figure 4-13. WCM List Window..... 4-17

Figure 4-14. WCC List Window..... 4-17

Figure 4-15. Services Submenu..... 4-18

Figure 4-16. Services Manager Window..... 4-18

Figure 4-17. Aux Submenu..... 4-19

Figure 4-18. Help Submenu..... 4-20

Figure 4-19. ASERVER Version Window..... 4-21

Figure 4-20. Extended Help Window..... 4-21

Figure 4-21. View Submenu Showing “IP Includes” Menu Option..... 4-23

Figure 4-22. The IP Includes List Window..... 4-24

Figure 4-23. ASERVER Showing Proxy Mode Status In The Title Bar..... 4-25

Figure 5-1. ASERVER Configuration Window – Security Tab.....5-3

Figure 5-2. ASERVER After Restart – Showing New Security Menu Option.....5-3

Figure 5-3. The Security Submenu.....5-4

Figure 5-4. The User Manager Login Window.....5-4

Figure 5-5. The User Manager Window.....5-5

Figure 5-6. WccMaint Overview Window Showing WCC Tabs.....5-6

Figure 5-7. WccMaint Overview Window Showing OCG Cluster Tabs.....5-6

Figure 5-8. User Manager Window Showing User Account Locked Out.....5-8

Figure 5-9. Changing User Password..... 5-10

Figure 5-10. Workstation Node Security Popup Menu..... 5-11

Figure 5-11. Send Message Dialog Box..... 5-12

Figure 5-12. Security Submenu..... 5-12

Figure 5-13. Console Unlock Verification Screen..... 5-13

Figure 5-14. WCCM Client Messaging Dialog Box..... 5-13

LIST OF TABLES

<u>Table No.</u>	<u>Title</u>	<u>Page</u>
Table 1-1.	Anticipated ATCS Network Size.....	1-3
Table 3-1.	Configuration Options – Category: General.....	3-13
Table 3-2.	Configuration Options – Category: Logging.....	3-14
Table 3-3.	Configuration Options – Category: Network.....	3-15
Table 3-4.	Configuration Options – Category: Alarms.....	3-17
Table 3-5.	Configuration Options – Category: Database.....	3-18
Table 3-6.	Configuration Options – Category: OCG/WccMaint.....	3-19
Table 3-7.	Configuration Options – Category: Security.....	3-19
Table 3-8.	Configuration Options – Category: Diagnostics.....	3-20

NOTES, CAUTIONS, AND WARNINGS

Throughout this manual, notes, cautions, and warnings may be used to direct the reader's attention to specific information. Use of the three terms is defined as follows:

NOTE

Generally used to highlight certain information relating to the topic under discussion.

CAUTION

APPEARS IN UPPERCASE TYPE AND REFERS TO PROPER PROCEDURES OR PRACTICES WHICH IF NOT STRICTLY OBSERVED, COULD RESULT IN A POTENTIALLY HAZARDOUS SITUATION AND/OR POSSIBLE DAMAGE TO THE EQUIPMENT. CAUTIONS TAKE PRECEDENCE OVER NOTES AND ALL OTHER INFORMATION, EXCEPT WARNINGS.

WARNING

HIGHLIGHTED IN BOLD, UPPERCASE TYPE AND INDICATES A POTENTIALLY HAZARDOUS SITUATION WHICH, IF NOT AVOIDED, COULD RESULT IN DEATH OR SERIOUS INJURY. WARNINGS ALWAYS TAKE PRECEDENCE OVER NOTES, CAUTIONS, AND ALL OTHER INFORMATION.

If there any questions, contact Safetran Applications Engineering.

GLOSSARY

AEI Equipment:	<u>Automatic Equipment Identification</u> - AEI sites are installed along the track to read and report the train consist information.
ARES:	<u>Advanced Railroad Electronics System</u> - Created by Rockwell International as an alternative to AAR ATCS.
ASERVER:	A software application designed by Safetran Systems to centrally organize and distribute all network management traffic in ATCS networks.
ATCS:	<u>Advanced Train Control System</u> - A set of standards compiled by the AAR for controlling all aspects of train operation.
BCP:	<u>Base Communications Package</u> - Defined by the ATCS specifications as the transmitter / receiver base station and associated processors to handle communications between mobile and central office equipment.
CADS:	A legacy serial-based CTC system in use at CSX Corp.
CC:	<u>Cluster Controller</u> - An ATCS ground network node responsible for the control of BCP's.
Congestion:	<u>Congestion mode</u> for a WCC is a condition that results from a system traffic overload, usually caused by very high inbound message traffic under ducting conditions. While in congestion mode, the WCC enforces restrictions on outbound traffic to mitigate the overload and help restore the system to normal.
CPC:	<u>Central Protocol Converter</u> - Modular component of Safetran's R/Link™ Radio Control System that converts CTC code line control and indication message data to ATCS-compatible data.
CRC:	<u>Cyclical Redundancy Check</u> - The CRC on a data packet is normally calculated and appended to the data so that the receiver can verify that no data was lost or corrupted during transit.
CTC:	<u>Central Traffic Control System</u>
DTE device:	<u>Data Terminal Device</u> - A device that originates or consumes data.

GLOSSARY - *continued*

Ducting:	A temporary RF condition that results in unusual coverage patterns for bases and groups, typically over very large distances. This condition is a natural phenomenon that is caused by a combination of atmospheric and weather conditions.
FEP:	<u>Front End Processor</u> - An ATCS ground network node responsible for providing network access to ground host and terminal users.
GTC:	<u>Ground Terminal Computer</u> -
HDLC:	<u>High-level Data Link Control</u> - A serial protocol for exchanging synchronous information.
HUB:	A logical process in ATCS that interfaces to base stations and distributes code line traffic to and from any number of LCTs. Also referred to as FEPHUB.
IP:	See TCP/IP
LAN:	<u>Local Area Network</u> – A collection of devices, usually PCs or workstations, that are interconnected for the purpose of sharing data, typically on an Ethernet communications platform.
LCT:	<u>Line Control Task</u> - A logical process in ATCS that controls a collection of bases and groups and interfaces them to a CTC office. Commonly referred to as a code line.
LSB:	<u>Least Significant Bit</u> of a binary number (having the lowest numerical weight).
MCP/WCP:	<u>Mobile/Wayside Communications Package</u> - The radio and associated processor used by mobile and wayside ATCS compatible equipment to communicate to the central office.
MSB:	<u>Most Significant Bit</u> of a binary number (having the greatest numerical weight)
NGD:	<u>Next Generation Dispatch</u> – An IP-based CTC system designed by Union Switch & Signal currently implemented by CSX Corp.

GLOSSARY - *continued*

- OCG: Office Communications Gateway – A software application that performs the functions of WCCs (controlling HUB and LCT functions). OCG was conceived as an alternative to using WCC hardware where no serial (RS-232) communications is involved (all communications are Ethernet-based).
- OSI: Open System Interconnection - A reference model created by the International Standards Organization (ISO) as a framework for networking communications architecture. The model divides network communications design and implementation into seven layers as follows: (1)(bottom layer) Physical, (2) Data Link, (3) Network, (4) Transport, (5) Session, (6) Presentation, (7) Application.
- RSSI: Received Signal Strength Indication – see SSI.
- Squitter: A squitter is a specific message in ATCS or ARES that broadcasts the identity of the sender. It is used in several different contexts, including XID and BCP tag messages.
- SSI: Signal Strength Indicator - A measure of the relative strength of an incoming RF signal when it was received by a BCP.
- TCP/IP: Transmission Control Protocol / Internet Protocol - The Internet protocol used to connect a world-wide inter-network of universities, research laboratories, military installations, organizations, and corporations. The TCP/IP includes standards for how computers communicate and conventions for connecting network and routing traffic.
- UDP: User Datagram Protocol - A transport protocol used primarily for the transmission of network management information. Not as reliable as TCP.
- WCC/FPD: Wayside Communications Controller/Field Protocol Device – Safetran assembly A53401 (9-port model) or A53430 (12-port model) is a lan-based general purpose platform capable of many communications and codeline functions including front-end processing (FEP), cluster control (CC), and centralized protocol conversion (CPC) in a variety of railroad signal, communications, and network environments. Commonly referred to as a packet switch, WCC, FPD, or RFPD depending on local use and function.

GLOSSARY - *continued*

- WCCMAINT: Abbreviated form of WCC Maintenance, Safetran's windows-based utility for maintaining and troubleshooting ATCS networks. Used strictly in conjunction with Aserver.
- WCE: WCC-Extended – This is a logical extension of WCC hardware (assembly number A53401 or A53430) that has a unique configuration that allows it to support multiple codelines on one serial port. This implementation is CTC system specific. Contact Safetran for advice on whether this configuration is appropriate for a given CTC system.
- WCM: Wayside Communications Manager – Safetran assembly A53477, commonly referred to as a 6-port packet switch, which is primarily used as an Ethernet-to-ATCS interface in a field application where the communications transport to the office is IP-based instead of the more traditional RF-based transport.

SECTION 1

INTRODUCTION

1.0 INTRODUCTION

Safetran’s ATCS Server (ASERVER.EXE) is a standalone executable program that manages statistical and diagnostic traffic in an ATCS (Automatic Train Control System) environment. Its primary function is to route NMS (Network Management System) data packets between endpoints in a LAN-based WCC/OCG network. Endpoints include WCCs (Wayside Cluster Controllers, also WCC/FPD), Office Communications Gateway (OCG) applications, PC workstations running Safetran’s WCC maintenance/diagnostic utility (WCCMAINT.EXE), ATCS-aware hardware devices, and software services that interface to external databases and processes.

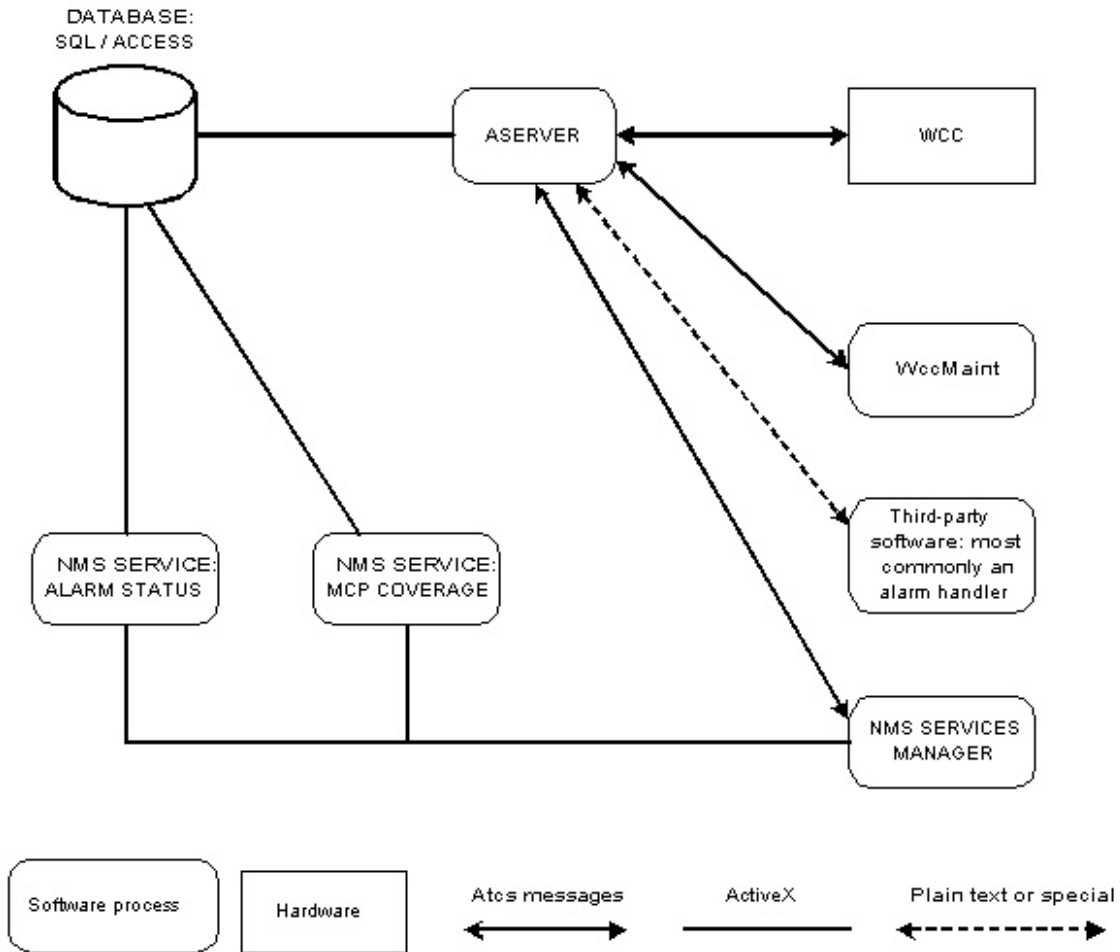
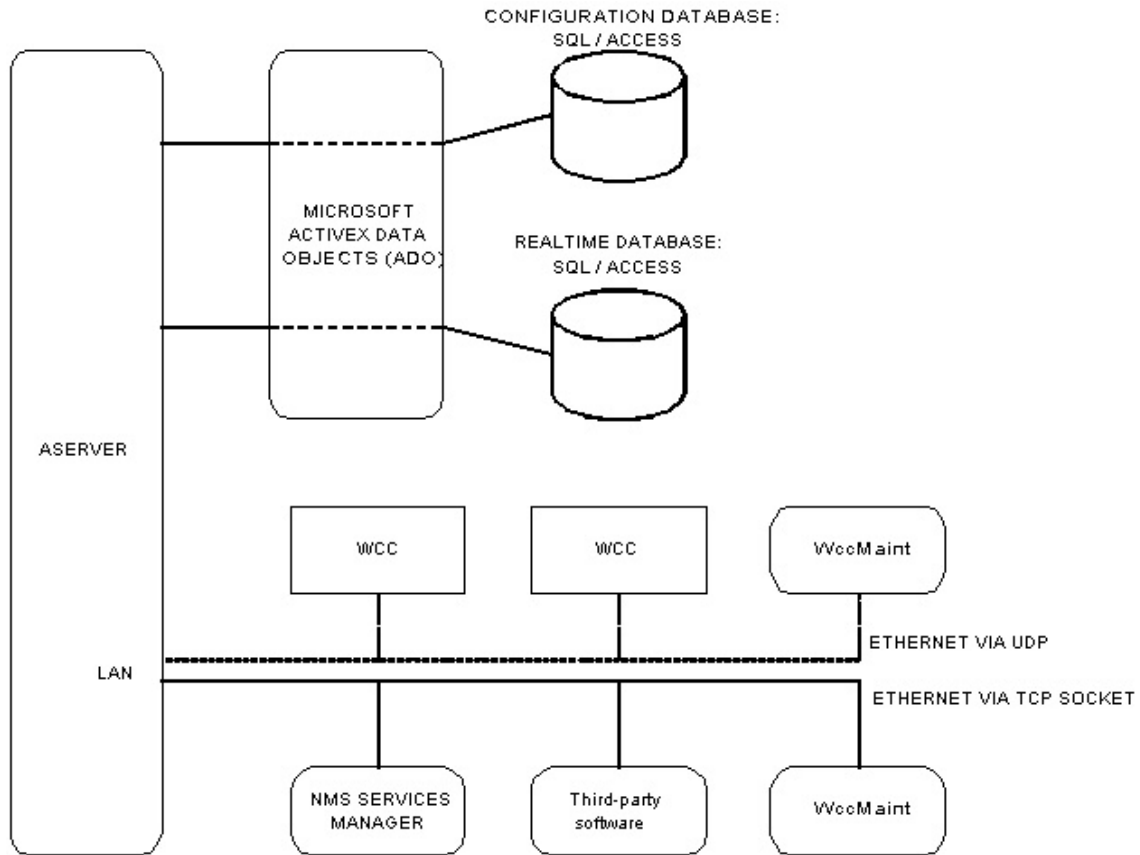


Figure 1-1. ASERVER Process Interconnection

Aserver is the core of a suite of Safetran software packages that process statistical data, alarms, and diagnostic information from WCC/OCGs so that WccMaint users can monitor, manage, test and troubleshoot their ATCS networks from a single program interface. Aserver is the sole interface between WCC/OCGs (and by extension, the ATCS field network) and any process that needs to communicate with them. Aserver physical connectivity is shown in Figure 1-2.



Notes:

1. Connection to database via ADO or ODBC is usually an internal machine interface; if DB is located on another machine on LAN, connection is via Ethernet (ODBC not shown)
2. Services manager is usually run on same machine but this is not a requirement. The connection is to the Aserver TCP server socket.
3. WccMaint may connect to Aserver via UDP or TCP connection as required.

Figure 1-2. ASERVER Physical Connectivity

1.1 HARDWARE/SYSTEM REQUIREMENTS

ASERVER 5.0 and above is supported on Windows 2000, Windows 2000 Server, Windows 2000 Advanced Server, Windows Server 2003 and Windows XP platforms. At the time of this writing, Aserver under Windows Vista has been beta tested but not officially released for support. For optimum performance, hardware requirements for Aserver depend on the anticipated size of the ATCS network; see Table 1-1 below. For larger systems, SQL Server is the preferred database platform for scalability reasons. It is not recommended that Aserver and SQL Server run on the same physical hardware. A typical configuration database is 5-10 Mb; real-time data can exceed 100 Mb.

Table 1-1. Anticipated ATCS Network Size

System Size:	Small (<30 nodes)	Medium (30-100 nodes)	Large (> 100 nodes)
Memory:	512 Mb	1Gb	2Gb
Hardware:	Workstation	Hi-end ws or entry server	Server class
Hard Drive:	10 Gb	20-40 Gb	80 Gb

NOTE

A node is any ATCS endpoint, typically either a WCC (packet switch), OCG, or a WccMaint client workstation.

Aserver maintains 2 databases, one for static configuration data, and one for realtime data. Supported database types are Microsoft Access 2000 and Microsoft SQL Server; the choice of this software and its installation is the responsibility of the customer. Because Aserver interfaces to these databases via ActiveX or ODBC (Open DataBase Connectivity), these data access components must be installed on the Aserver machine as well. Microsoft Data Access Components (MDAC) 2.5 or later is required.

Note that, if the system is originally installed using an Access database, it can be later scaled up to SQL Server with a simple configuration change in Aserver.

1.2 SOFTWARE VERSIONS

Each release of ASERVER.EXE has a version number associated with it. The format of this version number is :

`<Major version>.<Minor version>.<Release>.<Build>`

In its current release, Aserver's major version is 5. The minor version number changes with a significant feature added to Aserver, and usually involves a corresponding change in WccMaint; major and minor version numbers should always match for AServer and WccMaint to ensure feature compatibility.

The release number is incremented each time Aserver is released for distribution to customers, typically for enhancements, feature additions, or bug fixes. The build number is used internally to track incremental software changes.

This documentation refers to Aserver software version 5.2.3.3 and later, although most of the material will apply to any version after 5.1.x.x.

1.3 SUPPORTING APPLICATIONS

Several DLLs support server-related functions. These DLLs are installed by the Aserver setup program and are placed in the Windows system folder (C:\WINDOWS or C:\WINNT) by default

1.3.1 Security

ASRVSEC.DLL provides security features for NMS and is used to restrict WccMaint functionality depending on permissions set for the individual user. For instance, WccMaint users who have 'database' permissions are allowed to modify group and base names. The current version of ASRVSEC.DLL is 4.1.0.101. Security for NMS is discussed in Section 5.

1.3.2 Windows Application Log Support

SAFETRANASERVER.DLL is a resource DLL that supports logging to the Windows Application log (Control Panel -> Administrative Tools -> Event Viewer). Critical errors, exception traps, AServer startup/shutdown, and other critical events are logged to the system event log. Setting up this DLL provides string resource information to the event viewer that creates meaningful log entries. This DLL is NOT enabled automatically by AServer setup; see Section 2 for setting up this module.

1.3.3 System Personality

Personality DLL modules are customer-specific and control NMS features that are licensed to individual customers. NMS services (SNMP Agent, RF Coverage History, etc) and maximum allowed logins are controlled by the personality module. WccMaint uses the same DLL to enable customer-specific features within WccMaint as well. Aserver and WccMaint are fully functional without any personality modules registered; they are only required to enable customer-specific enhancements.

Personality modules are named in the format NMSP_CUSTNAME.DLL and are not included in the AServer setup CD; they are sent from the factory direct to customers as required. Contact Safetran Technical Support for more information about the release of these modules.

1.3.4 NMS Services Manager

The Services Manager is an Activex EXE that manages all NMS Services from a single interface. It is a separate application from Aserver and has its own setup program. The Aserver setup DOES NOT install the Services Manager, but it does install the files necessary to run the Services Manager setup. See Section 2 for details on Services Manager setup.

1.3.5 NMS Services

NMS Services are Activex EXEs that use Aserver to interface to the ATCS network to perform auxiliary functions. For example, the SNMP Agent Service receives text alarms from Aserver, OCG and WAMS Status Manager, converts these alarms to SNMP traps and forwards them to an SNMP Enterprise Manager.

NMS Services are customized for each user's requirements and are purchased separately, and as such they are not included in the Aserver setup CD. Contact Safetran Sales and Marketing for more information about custom services.

This page intentionally left blank.

SECTION 2

INSTALLATION

2.0 INSTALLATION

A complete installation of ASERVER involves the following steps, some of which are optional:

1. Program files installation (**run SETUP.EXE**).
2. Install Services Manager.
3. Install any Safetran services, if included.
4. Install personality module, if supplied.
5. Relocate files as required.
6. Set up databases as required.
7. Create data sources for Aserver's access to the data files.
8. Edit SAFETRAN.INI.
9. Setup windows logging.
10. Convert older INI files into Access databases (if necessary).
11. First Aserver run.

QUICK START

If the following conditions apply:

- ACCESS databases will be used in their default locations OR
- No database is required
- You will not use any NMS services
- You will not run in secure mode

You may use the following quick setup procedure:

1. Run SETUP.EXE (2.1)
2. Edit C:\Program Files\Safetran Systems\Atcs Server\SAFETRAN.INI:
 - a) If using database, add any railroads used (2.8.2).
 - b) If not using any database, uncomment the **NoDatabase=true** line.
3. Move SAFETRAN.INI to the windows system folder.
4. ASERVER is ready to run.

If you are not sure about any of the above conditions, or the database defaults are not suitable, please run the full setup procedure, starting with 2.1

2.1 RUN SETUP (REQUIRED)

Run SETUP.EXE from the installation CD to extract all system files and create the necessary directories. This will install the following files:

Folder C:\Program Files\Safetran Systems\ATCS server:

File	Function
Aserver.exe	Main server executable
WccMaint.exe	NMS maintenance utility
Safetran.ini	Default INI file. This must be moved to the Windows system folder (step 2.5)
Read.txt	Text file containing release notes
W53401.exe	WCC diagnostic utility
W53401.hlp	Help file for W53401

Folder C:\Program Files\Safetran Systems \ATCS server\data\:

Subfolder	File	Function
Access2000	Nmscfg.mdb	Blank configuration database
Access2000	Nmsrt.mdb	Blank realtime database
Access2000	Nmscfg.udl	Blank datalink file for configuration database
Access2000	Nmsrt.udl	Blank datalink file for realtime database
SQL Server	Nms_cfg_v6.sql	Script for configuration database creation
SQL Server	Nms_rt_v6.sql	Script for realtime database creation
SQL Server	Application_types.txt	Support file for script
SQL Server	Atcs_railroad_numbers.txt	Support file for script
SQL Server	Device_types.txt	Support file for script
SQL Server	Equipment_types.txt	Support file for script

Folder C:\Program Files\Safetran Systems \ATCS server\temp\:

Subfolder	File	Function
ServicesManager	SETUP.EXE	Setup for Services Manager
ServicesManager	NSManager.cab	Setup support
ServicesManager	Setup.lst	Setup support
MDAC/Jet4.0	Jet40Sp3_comp.exe	Microsoft JET data access installation
MDAC/mdac2.5	Mdac_typ.exe	Data access components version 2.5
MDAC/mdac2.5	Mdac_typ.exe	Data access components version 2.5

Folder C: \WINDOWS\SYSTEM32 or

Folder C: \WINNT\SYSTEM32 (Windows 2000):

File	Function
Vclx50.bpl	Borland runtime libraries
Inet50.bpl	
Inetdb50.bpl	
Nmfast50.bpl	
Vcl50.bpl	
Vcldb50.bpl	
Vclbde50.bpl	

Folder C: \WINDOWS or

Folder C: \WINNT (Windows 2000):

File	Function
Wccconfig.dll	WCC configuration editor
Bocgconfig.dll	OCG configuration editor (BNSF)
Cocgconfig.dll	OCG configuration editor (CSX)
Asrvsec.dll	Aserver security module
Nmsp_dflt.dll	Default personality module
Safetranaserver.dll	Windows event log support module

2.2 INSTALL SERVICES MANAGER (OPTIONAL)

The Safetran Services Manager is a single interface for Aserver to access any existing or future services (see Figure 1-1). It is an ActiveX EXE that must be registered on the system before any services may be used. If no NMS services are to be used, this step may be skipped.

To install, run SETUP.EXE in the folder

C:\Program Files\Safetran Systems\ATCS server\temp\ServicesManager

Follow the prompts to complete this installation. In most cases it is acceptable to use all the defaults offered by the setup program. When complete, the Services Manager is installed and registered, and no reboot is required.

Note that there are no configuration options for the Services Manager. If the Services Manager is not installed, Aserver will note this as a warning and continue to run without it.

2.3 INSTALL SERVICES (OPTIONAL)

An NMS service is an ActiveX EXE that performs a specific function in relation to Aserver/WccMaint networks. For instance, the Alarm Status service maintains the current state of any ATCS alarms received on the system in the realtime database. Contact Safetran for details on available services. The procedure for installing a service is described in Appendix G. Note that, if services are to be used, the Services Manager must be installed as described in paragraph 2.2.

2.4 INSTALL PERSONALITY MODULE

Custom personality DLL modules are shipped separately from the Aserver installation CD. For Aserver, the primary function of the personality module is to allow NMS services to run. Aserver will be fully functional without a personality module, but it will log an error on startup. The default NMSP_DFLT.DLL is shipped with Aserver Setup to satisfy the personality requirement, but no services are enabled. If NMS services are used (SNMP Agent, Alarm Service, etc), the appropriate customer DLL must be placed in the Windows system folder.

2.5 RELOCATE FILES (REQUIRED)

The following step is **required**:

SAFETRAN.INI must be located in the Windows system folder. For Windows 2000, this is **C:\WINNT**; otherwise it is **C:\WINDOWS**. The SETUP program places a default SAFETRAN.INI file in the **Program Files** folder path in order not to overwrite an existing INI file. If Aserver is being re-installed, nothing needs to be done (the existing INI file will be used); otherwise, move the default SAFETRAN.INI to the system folder.

The following steps are **optional**:

ASERVER.EXE or WCCMAINT.EXE may be placed in any desired folder, but any shortcuts established by the setup program must be updated to point to the new locations.

Access database files may be placed in any desired folder, and it is recommended that the corresponding UDL files be located in the same folder. If database files are moved, they must be moved before the UDL files are configured in the next step.

2.6 DATABASE SETUP (REQUIRED)

If no databases are to be used (for instance, when Aserver is used in a test environment or for interfacing a field crossing network to WAMS), Aserver database handling may be turned off. The effect of NOT using a database is that, for WccMaint clients, field devices (ATCS groups and bases) cannot have names associated with them, and always appear as generic blue icons.

In general, if WccMaint is not to be used, or WAMS is the primary user interface to the field network, an Aserver database is not needed (WAMS maintains its own database). If this is the case, please skip to step 2.8.

2.6.1 Microsoft Access:

Aserver setup creates 2 databases: NMS_CFG.MDB and NMS_RT.MDB, the configuration and realtime Access databases, respectively. These databases are unpopulated except for tables that contain static data such as AAR Railroad descriptions, equipment type lists, etc. They are created as Access 2000 databases, which will not be recognized by older versions of Access. Earlier versions of Access are not supported.

If databases are to be located in a folder other than the defaults established by the setup program, move them now and proceed to step 2.7.

2.6.2 SQL Server:

If MS SQL Server is to be used, it must be installed on the target machine before proceeding with step 2.7. Running SQL Server on the same machine as Aserver is not recommended except for very small or development systems.

From SQL Enterprise Manager, create a blank database named NMS_CFG, and another blank database named NMS_RT. These are the configuration and realtime databases, respectively. Once they are created, run the associated scripts (nms_cfg_v6.sql or nms_rt_v6.sql) into each database. Scripts are located in

`C:\Program Files\Safetran Systems \ATCS server\data\SQL Server`

2.7 DATA SOURCES (REQUIRED)

Note: if no databases are used, skip to step 2.8.

Aserver requires either an ODBC DSN (Data Source Name) or a datalink (UDL extension) file to interface the database to its internal DB drivers. This DSN or UDLfile serves as a 'pointer' to the external data, and one is required for each database. The datalink file method is preferred because this is an ActiveX interface, which is faster and uses less system overhead.

NOTE

Both databases must be interfaced via the same method; that is, if the configuration database uses ODBC, the realtime database must use ODBC as well.

NOTE

There are slight differences in setting up data sources for SQL Server. Skip this section and see Appendix B for details if SQL Server is used.

For data link files (**preferred method**), proceed to step 2.7.1. If this method fails, proceed to step 2.7.2.

2.7.1 DATA LINK FILE Method

1. Using Windows Explorer, locate the blank UDL file NMS_CFG.UDL that was created by with the Aserver installation CD:

C:\Program Files\Safetran Systems\ATCS server\data\Access2000\nms_cfg.udl

2. Double-click the file to open the Data Link file Properties dialog:

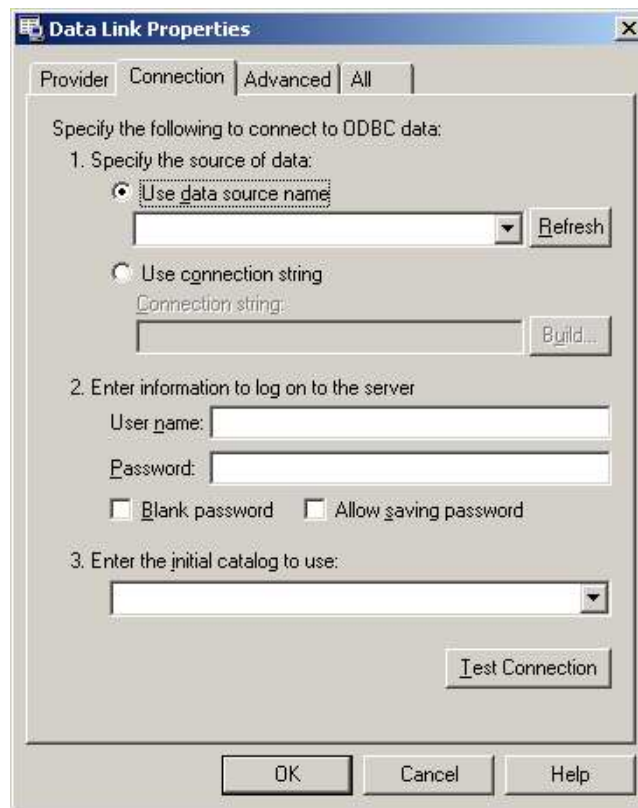


Figure 2-1. Data Link Properties Dialog Box

NOTE

If this dialog does not appear, you must use ODBC. Proceed to step 2.7.2.

3. Click on the 'Provider' tab and select the line with 'Microsoft Jet' (this may be a version other than 4.0 as shown) :

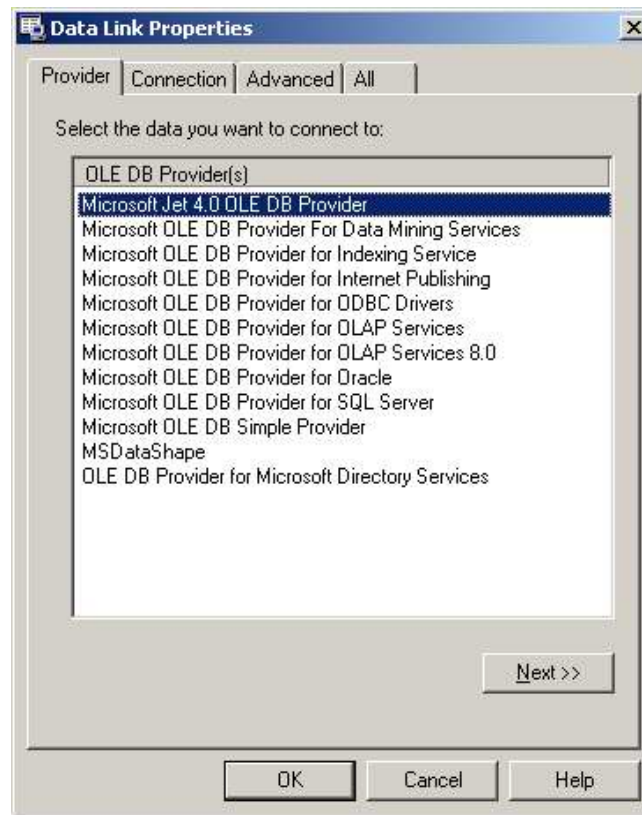


Figure 2-2. Data Link Properties Dialog Box – Provider Tab

4. Click 'Next'. The Connection tab will display:

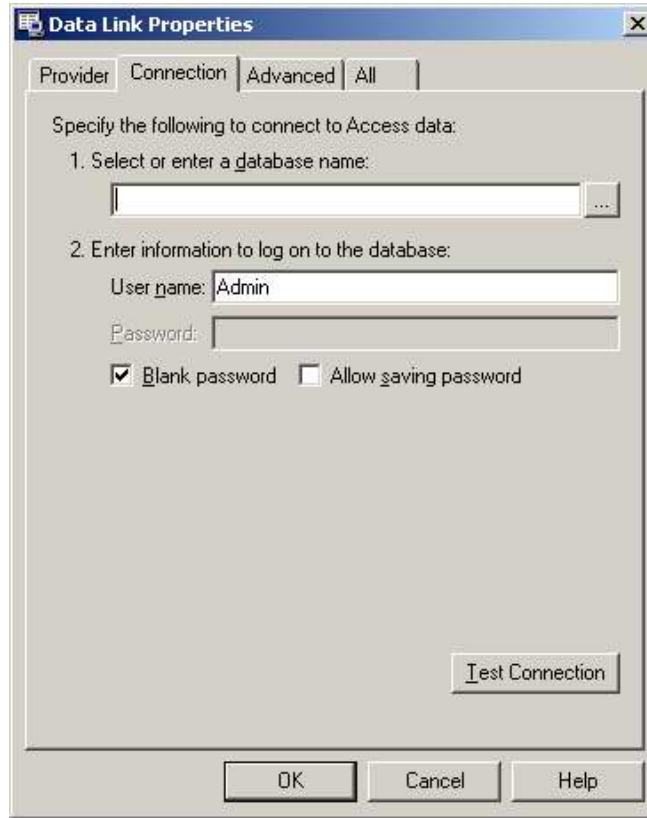


Figure 2-3. Data Link Properties Dialog Box – Connection Tab

5. Click the dotted box to the right of the database name field to browse for the database:

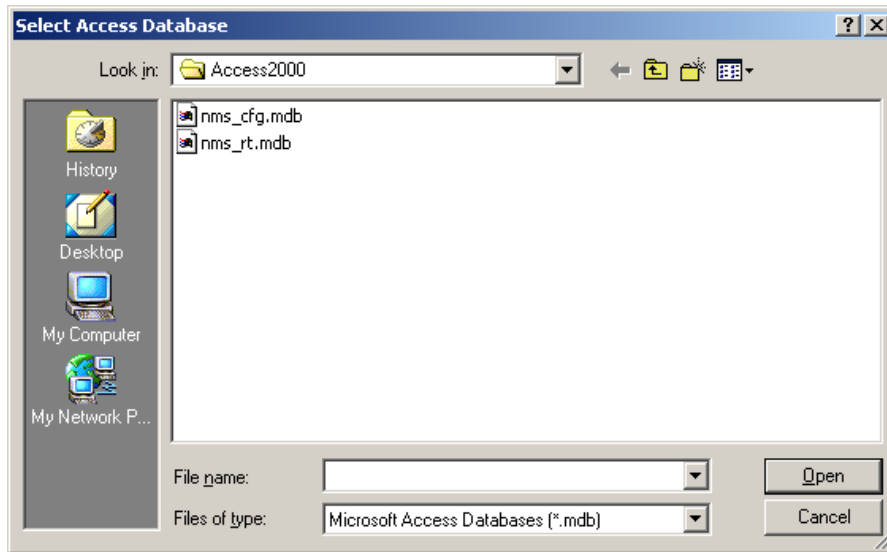


Figure 2-4. Database Browse Window

6. Locate and highlight the NMS_CFG.MDB database and click 'Open'. The Connection tab will re-appear with the database path in the edit window.

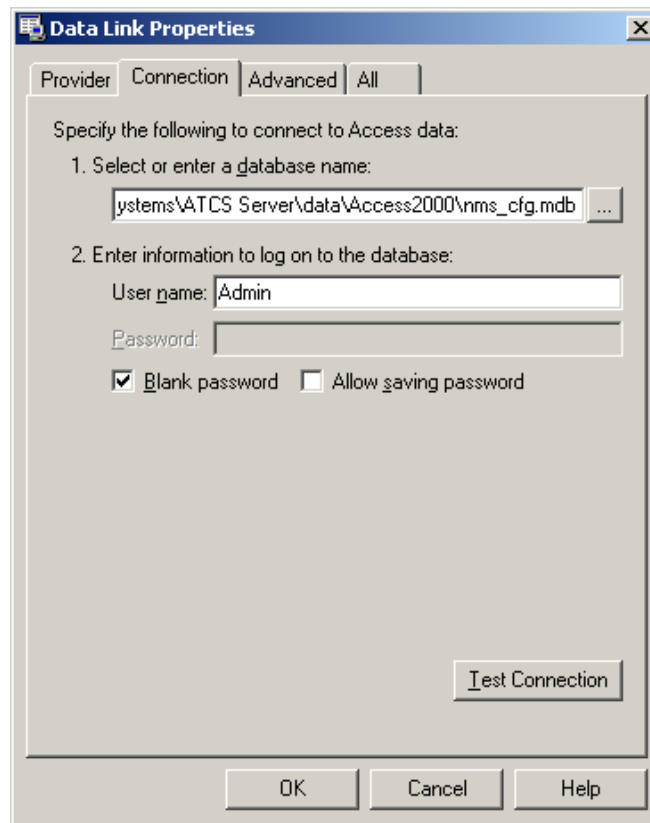


Figure 2-5. Data Link Dialog Box Showing Selected Database

7. Click the 'Test Connection' button. The system will verify the datalink and should display a message box that says "Test Connection Succeeded". If this does not appear, verify that you have selected the correct database file and repeat the test. If the error persists, you may have an incompatible version of either Microsoft database components or MDB files, and ODBC will have to be used instead of datalink files.
8. Datalink file creation is complete – proceed to step 2.8. If this process has failed for any reason, you may try the ODBC method in step 2.7.2.

2.7.2 ODBC Method

1. Login as Administrator or User with Administrator rights.
2. Open the Control Panel (Start > Settings > Control Panel).
3. Open Administrative Tools.
4. Open Data Sources (ODBC).

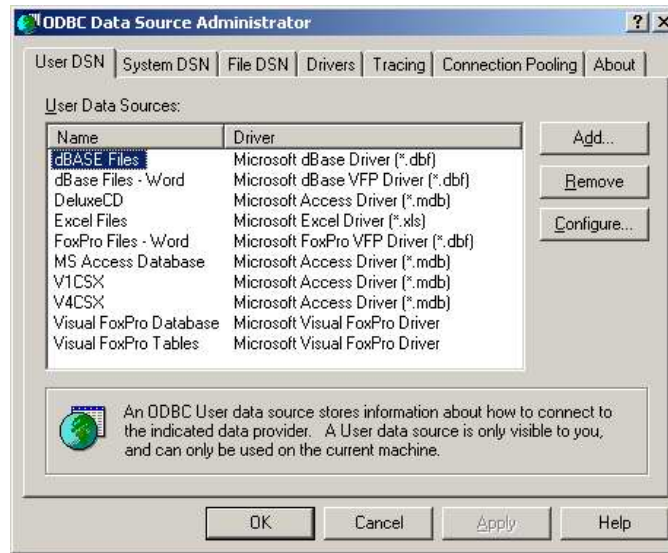


Figure 2-6. ODBC Data Source Window

5. Click on the 'System DSN' tab, then click 'Add...'. The 'Create New Data Source' dialog will appear, as shown in Figure 2-6.



Figure 2-7. Create New Data Source Selection Window

- Highlight 'Microsoft Access Driver (*.mdb)' and click 'Finish'. The 'ODBC Microsoft Access Setup' window will appear (Figure 2-8).

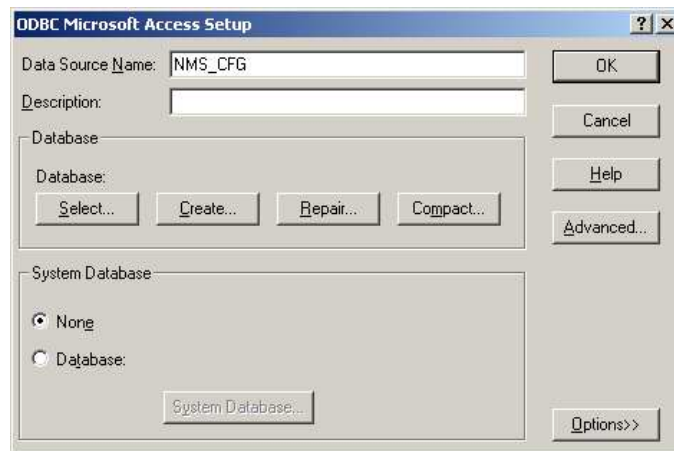


Figure 2-8. ODBC Microsoft Access Setup Window

- Type 'NMS_CFG' in the 'Data Source Name' field, as shown in Figure 2-8.
- Click the 'Select' button in the 'Database' group box. The 'Select Database' dialog box will appear (Figure 2-9).

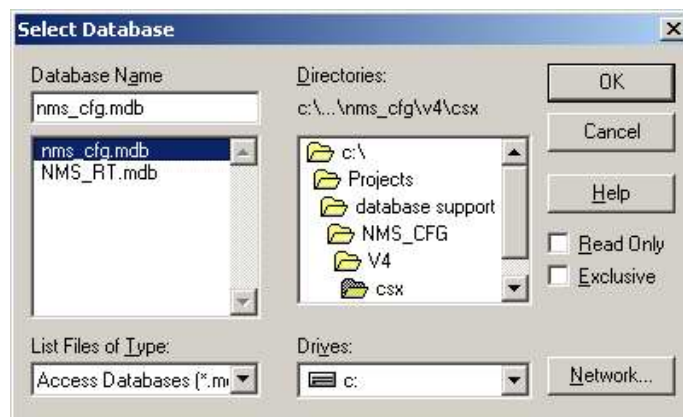


Figure 2-9. Select Database Dialog Box

- Browse the folders on the right to select the directory where the database file NMS_CFG.MDB is located, then highlight the database file in the file list. Click OK. The ODBC DSN has now been created; click OK on all dialogs to exit ODBC setup.
- Repeat this procedure to create an ODBC DSN for the realtime database. Name this DSN 'NMS_RT' in step 7 and select NMS_RT.MDB in step 8.
- ODBC setup is complete – proceed to 2.8.

2.8 EDIT SAFETRAN.INI (REQUIRED)

Both Aserver and WccMaint use SAFETRAN.INI to set up internal program values and modify run-time behavior. Using Windows Explorer, locate and double-click Safetran.INI (c:\windows or c:\winnt). This will open the file in Notepad. Scroll to the [Aserver] section and create the entries described below. Be sure to type the entries exactly as shown, with no spaces (the item keyword – to the left of the equals sign – is case sensitive).

This section describes a minimal setup for SAFETRAN.INI that will enable Aserver to start up for the first time. If Aserver's security features are to be used, it is suggested that the INI file be re-edited for this or any other configuration options **after** the installation has been successfully completed. All configurable parameters are fully described in the Section 3, 'Configuration'.

Note: INI files use a **comment** (semicolon) character in the first column of a line to denote that the line is to be ignored. This is useful for inserting comments in a file or to leave options ready to be enabled by removing the comment character ('**uncommenting**' the line).

SAFETRAN.INI is defaulted for minimal setup, and only needs to be edited for database functions and, if databases are to be used, at least one railroad. If databases have been configured with all the installation defaults, all that needs to be done is to uncomment the appropriate lines in the INI file.

Database Options:

Aserver may be run with or without any databases. If Aserver is used as a gateway to office applications only (for instance, a SEAR-II field network to WAMS), no database is required. If Aserver is used in a full ATCS environment (e.g., using WccMaint) a database is required for equipment lists, group/base names, etc.

If no database is to be used, uncomment the line **NoDatabase=true** and proceed to step 2.8.2.

If using the default (ACCESS) databases in their default locations, proceed to step 2.8.2.

If the ACCESS databases are to be placed in another location or SQL Server is to be used, proceed to step 2.8.1.

2.8.1 Data Sources

1. Configuration database pointer: This is Aserver's interface to NMS_CFG.MDB.

If ODBC is used, enter the line:

ODBCDSN=NMS_CFG

This assumes you have created an ODBC source named NMS_CFG. If another name was used, replace 'NMS_CFG' with the DSN name.

NOTE

Because of hard coded defaults in some of NMS Services, it is best to name the DSNs NMS_CFG and NMS_RT as shown above.

If datalink (UDL) files are used, enter the line:

UDLFILE=C:\SAFETRAN\NMS_CFG.UDL

NOTE

Be sure to enter the correct full path to the datalink file you created in the 'Data Sources' section above. Mistyping the path is the single most common problem in first-time Aserver setups.

2. Realtime database pointer: Aserver's interface to NMS_RT.MDB.

For ODBC the entry is:

ODBCDSN_RT=NMS_RT

If using datalink files, the entry is:

UDLFILE_RT=C:\SAFETRAN\NMS_RT.UDL

2.8.2 Railroad Numbers

NOTE

If no database is used, proceed to step 2.8.3.

Aserver needs railroad numbers (designated by ATCS Spec 250 - see Appendix A) to initialize the database. You must include a line in SAFETRAN.INI for each railroad number you intend to use, for example:

Railroad1=22
Railroad2=76

INSTALLATION

Up to 10 railroads may be entered with the format shown above, ie 'Railroad<n>=<RR>' where <n> is a sequential number starting at 1 and <RR> is the AAR railroad number.

If this step is omitted and there are no railroads in the database, ASERVER and WCCMAINT will still operate, but you will not be able to associate names with RF bases and MCP groups on the WCCMAINT line displays.

NOTE

The railroad number is part of the address assigned to all ATCS entities. Refer to Appendix B for a list of railroad numbers. Contact Safetran if there is any doubt as to the correct numbers to use for this purpose.

2.8.3 File Paths

If Aserver is run on a machine where C: is not a valid drive letter, or if a specific directory must be used for any files Aserver may need to create, the following line must appear in SAFETRAN.INI:

SupportPath=<path>

Where <path> is the full path, including drive letter, where Aserver will be able to store dynamic system files for logging and caching. See Section 4, 'Operation' for details about logging and support files.

2.8.4 Security

Security is defaulted to OFF for installation.

See Section 3, 'Configuration', to set up security for Aserver and WccMaint clients after successful installation.

Save the changes you have made to SAFETRAN.INI and exit Notepad.

2.9 SETUP WINDOWS LOGGING (OPTIONAL)

Aserver sends certain critical and informational messages to the Windows Application log. SAFETRANASERVER.DLL is a resource file that Windows uses to interpret and display the messages logged in this way. In order to use SAFETRANASERVER.DLL, it must be entered in the Windows registry.

SETUP provides several registry key files that automatically register the DLL for the Event Viewer:

SAFETRANASERVER_2003.REG
SAFETRANASERVER_WIN2000.REG
SAFETRANASERVER_XP.REG

These files are located in:

C:\Program Files\Safetran Systems\ATCS server\temp

Double-click on the REG file appropriate to the operating system used. You will be prompted to enter the data into the registry; click YES to confirm. Once this registration is complete, the Windows Event Viewer will correctly display log information from Aserver.

To view the Windows Application log, click **Start->Settings->Control Panel-> Administrative Tools**, then select **'Event Viewer'**: The Event Viewer Window appears as shown in Figure 2-10

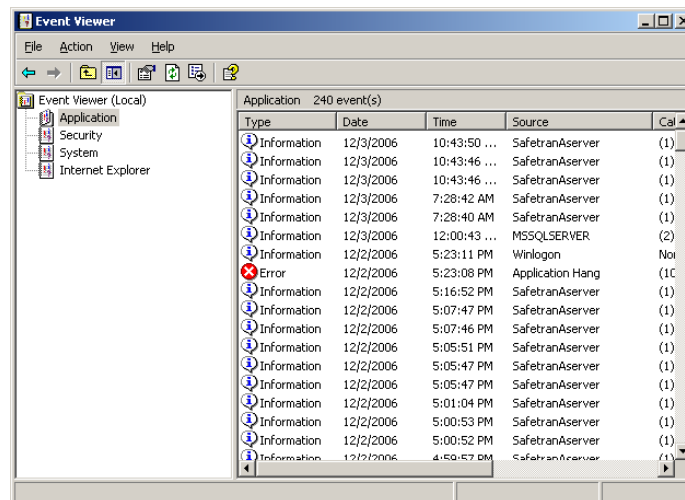


Figure 2-10. Event Viewer Window

Double-click on **Application** in the left pane to view events in the Application log.

INSTALLATION

To view details of a single log entry, double-click on the entry: An Event Properties window appears as shown in Figure 2-11.

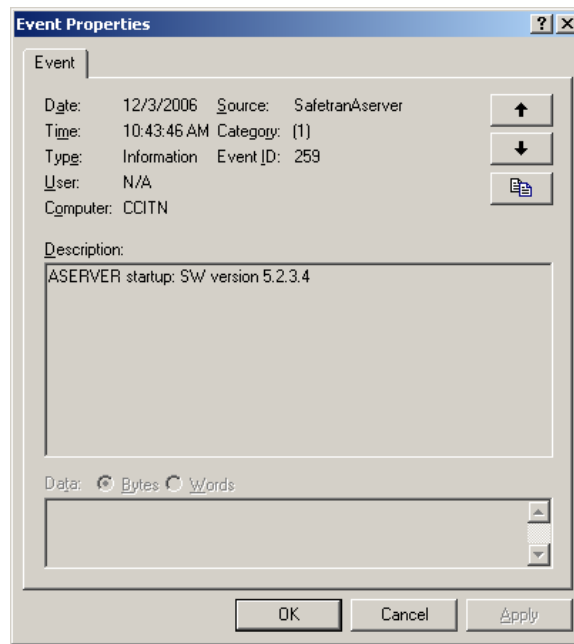


Figure 2-11. Event Properties Window With DLL Registration

Without the DLL registration, this event would display as shown in Figure 2-12.

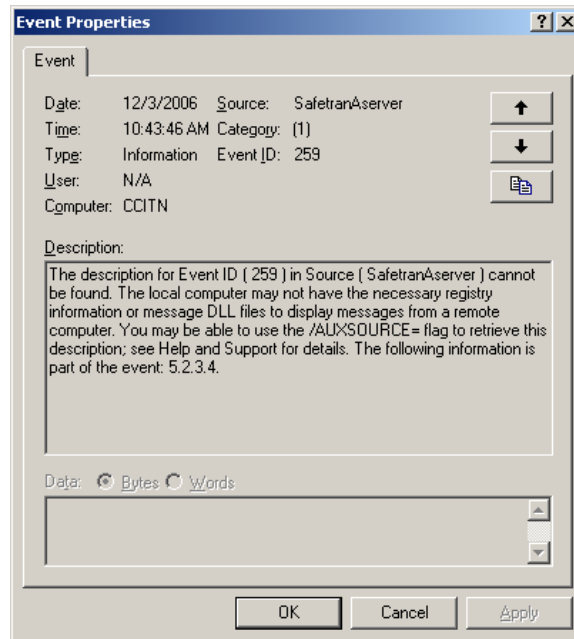


Figure 2-12. Event Properties Window Without DLL Registration

2.10 CONVERT INI FILES TO MS_ACCESS (OPTIONAL):

Older versions of Aserver (3.3x) used flat text files to store base names, group names, equipment types, and other runtime data. These flat files had an INI extension and the number of files varied depending on the size of the network and other factors.

Aserver 4.0 and later versions do not read these data files, and are shipped with a blank database. Therefore, for systems that have been in operation for any length of time before upgrading to Aserver 5.x, any site-specific information contained in the INI files will not be utilized. For smaller installations, the site data may be re-entered via the WccMaint line display screen as before, and the database will be populated as this data is entered. This may not be practical or desirable for larger systems, however, and there are conversion utilities that may be used to transfer INI file information into the configuration database as a final step in Aserver installation. Contact Safetran for assistance with INI file conversions.

2.11 RUN ASERVER FOR THE FIRST TIME:

Double-click on the Aserver icon on the desktop to launch it. Aserver will perform its initialization process:

- Reads SAFETRAN.INI for runtime options
- Opens log file (Aserverlog.txt)
- Opens TCP socket as server for client applications and Services Manager
- Creates udp sockets for communications with WCCs and OCG devices
- Opens connections to configuration and realtime databases
- Adds railroad numbers to the database (first run only)
- Creates cache files for bases and groups

When initialization is complete, the Aserver console will display the status of all connections to external devices and processes, as well as internal status and certain statistics (see Figure 2-13 below). WCC nodes and WccMaint sessions may not appear until network configuration requirements are satisfied.

Figure 2-13 represents a typical console display after Aserver initialization:

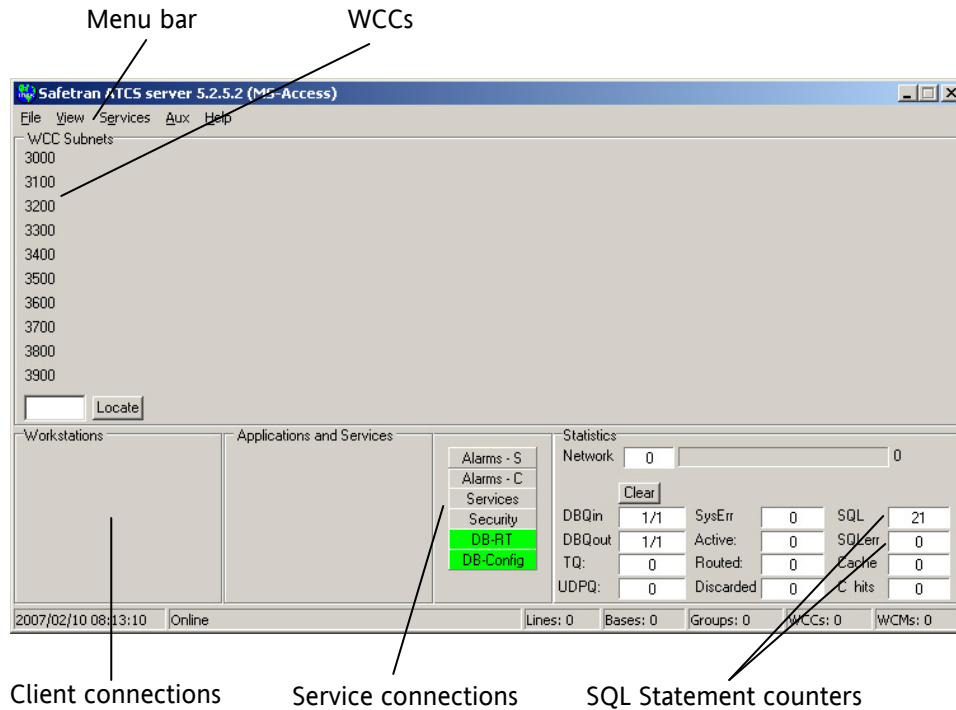


Figure 2-13. The ASERVER Console

Aserver has started and initialized the database properly, as indicated by the green status bars (DB-RT, DB-Config). The SQL counter indicates that several queries have been executed with no errors.

The 'Services' bar will be green if at least one NMS service has been started by the Service Manager (note that the Service Manager itself will not display a connection of its own). Services also appear as a node in the 'Applications and Services' panel.

WCCs and client connections will not appear unless Aserver and client devices are configured with the correct network parameters. See Section 3, 'Configuration' for details.

If Aserver encounters any problems during startup, it will open an error form and display the error(s) as shown in Figure 2-14.

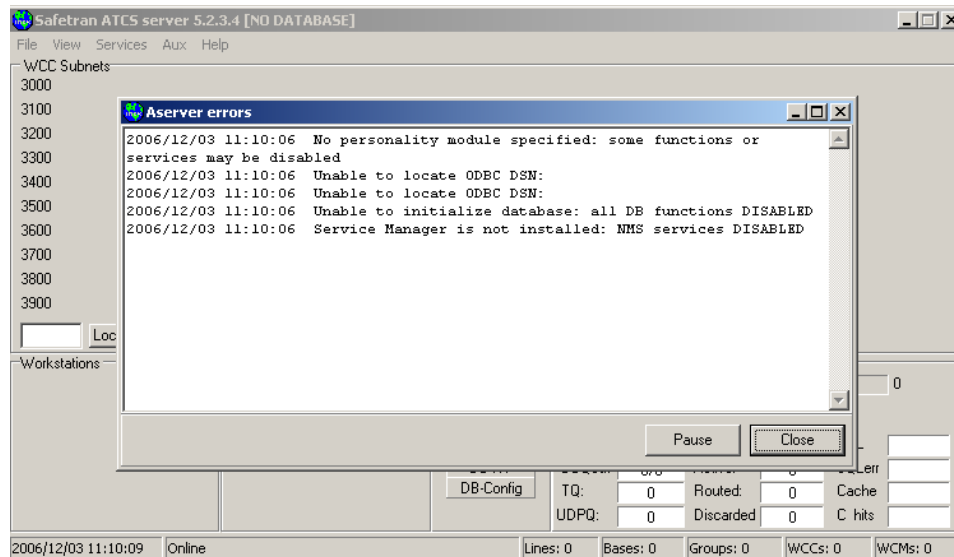


Figure 2-14. ASERVER Error Display

NOTE

If Aserver encounters a setup problem, it will disable the appropriate function and continue. In the case above, the database was not properly setup, and Aserver defaulted to NoDatabase mode. Also, NMS Services were disabled because the Services Manager was not installed. The user may either correct the setup errors and restart the server or close the error window and let the server continue.

This completes the initial installation of Aserver. Further configuration is most easily completed using the online configuration screens available from the Aserver console.

See Section 3 to complete Aserver configuration.

For a complete description of the console and the operator interface, refer to Section 4, 'Operation'.

This page intentionally left blank.

SECTION 3

CONFIGURATION

3.0 CONFIGURATION

3.1 INTRODUCTION

Configurable features in Aserver are grouped into the following categories:

- Railroads
- Subnet IP addresses
- Database and File Paths
- SubSystems (WccMaint tabs)
- TCP socket parameters
- Security
- Critical Alerts

These categories correspond to tabs on the online configuration screen shown below. Configuration options can be changed by editing SAFETRAN.INI or by using the online configuration screen in Aserver. The exceptions to this are noted below. When options are changed online, they are written to SAFETRAN.INI when the form is closed. However, Aserver only reads the INI file on startup, so most changes do not take effect until Aserver is restarted (WCC subnet changes are immediate). In general, once initial setup and installation is complete, configuration changes are more easily done online. Table 3-1 through Table 3-8 at the end of this section summarize all configuration options.

INI file entries for Aserver are below the [Aserver] header in SAFETRAN.INI. Each configuration line consists of a key and a value. For example, in the line:

InitialKB=Unlocked

the key is 'InitialKB'. Keys are case sensitive and values are not, so in the above example the value could also be typed as 'unlocked' or 'UNLOCKED' but 'InitialKB' must be entered exactly as shown.

CONFIGURATION

To view or change options, start Aserver, then click on File, then Configure on the Menu bar (Figure 3-1) to display the Online Configuration form (Figure 3-2).

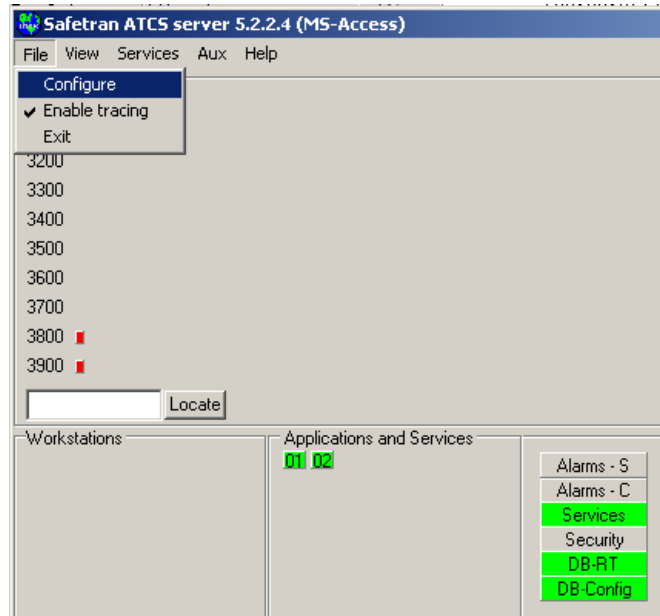


Figure 3-1. ASERVER Configuration Menu Selection

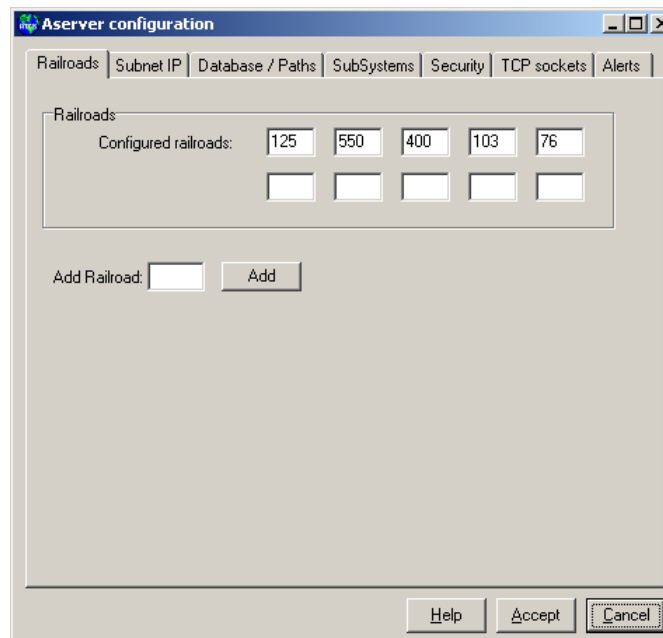


Figure 3-2. Online Configuration Form – Railroads Tab

Configuration options for each category may be edited by clicking each respective tab.

When the **Accept** button is clicked, configuration data on this form is saved to SAFETRAN.INI. If data has changed, a message box will remind the user that changes will not take effect until Aserver is restarted.

3.1.1 Railroads

The Railroads tab (Figure 3-2) will display the railroad numbers listed in SAFETRAN.INI. New railroad numbers may be added on this form as required. Railroad numbers updated with the **Add** button are added to the database as well.

3.1.2 Subnet IP Addresses

To configure Aserver to recognize a particular WCC/OCG, the IP or subnet address of the WCC/OCG must be in the subnet list shown in Figure 3-3 (see Appendix D for a discussion of subnetting and visibility in ATCS networks).

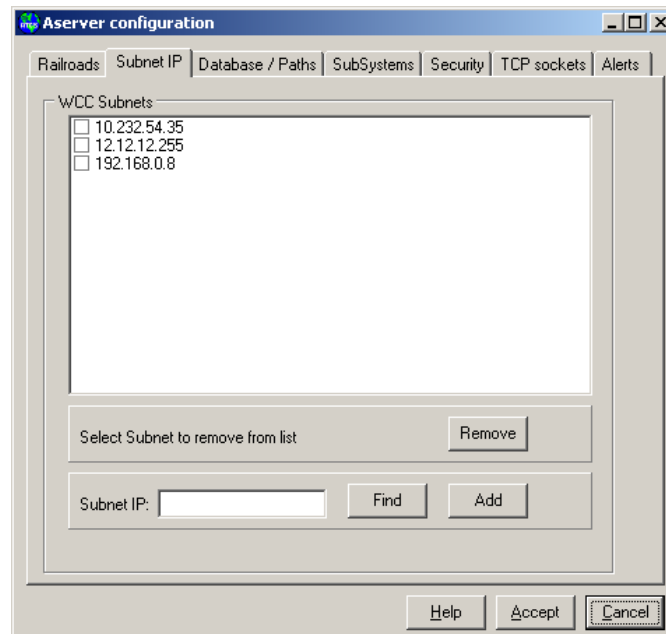


Figure 3-3. Online Configuration – Subnet IP Tab

The purpose of this subnet list is to establish and maintain connectivity between office devices (WCC, OCG or WCM) and Aserver for diagnostics. Every 10 seconds, Aserver will send an INT_RTE_UPDATE message to every checked IP address in this list. Newly started office devices will use this message to establish a connection for diagnostic traffic to and from Aserver.

CONFIGURATION

To add subnets, type the IP address into the 'Subnet IP' edit box, then click 'Add'. Repeat this process for all subnets; each address will appear in the 'WCC Subnets' list box. Check each subnet to activate it. When the subnet list is very large, the **Find** button may be used to locate a particular subnet.

NOTE

Subnets become active as soon as they are checked; it is not necessary to save the form first.

NOTE

Although the individual IP address of each WCC/OCG may be separately entered and checked here, it is more efficient to address all WCC/OCGs on a subnet with a single entry – see Appendix D. Aserver defaults to a limit of 32 in this table (more specifically, Aserver will only use the first 32 entries in the list). If more subnets are needed, there is an INI switch to set the number of allowed entries (see the end of this section for INI options).

It is not recommended to edit SAFETRAN.INI for subnet management. The INI entries created by the online tool are:

```
SubnetIP_X=150.50.175.255 ; subnet entry #N
SubnetActive_X=1         ; 1=checked (in use), 0=unchecked
```

3.1.3 Database / File Paths

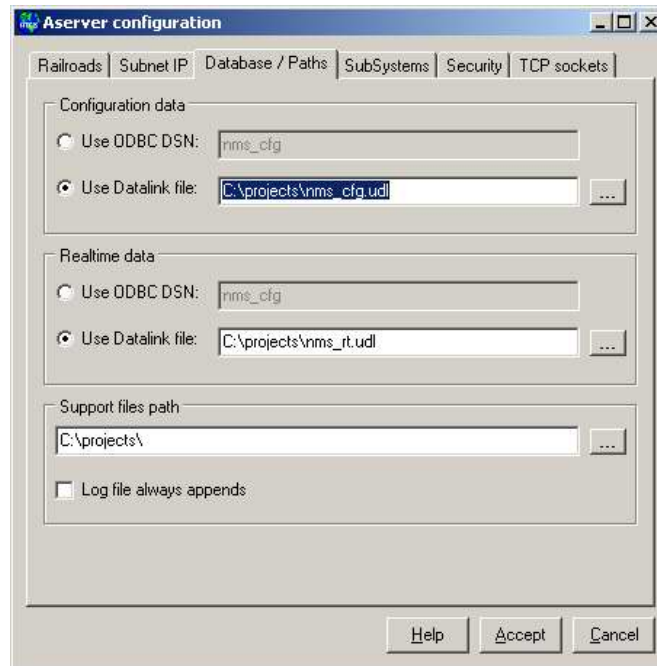


Figure 3-4. Online Configuration – Database/Paths Tab

As explained in Section 2, ODBC and Microsoft Datalink File (ADO) data access is supported. If both are available, datalink files are preferred because they directly access ActiveX without intermediate drivers, and therefore provide a faster and more efficient interface.

Configuration And Realtime Data

Data sources names, paths and types can be entered directly into SAFETRAN.INI or done online; typically they are entered into the INI file during initial installation and not changed thereafter. However, if changes are required, the online form is a more convenient means than editing SAFETRAN.INI.

Support Path

Aserver maintains a time-stamped event log that records startup events, non-fatal runtime errors, database errors, and security events. This event log is kept, along with diagnostic dump and temporary cache files, in a support files directory that can be set to any desired path or network directory. If no support path is specified in SAFETRAN.INI, Aserver attempts to create 'C:\safetran\' and use it for the default support files path.

The support files path may be changed at any time. If this path is changed, a new event log (`aserver_log_yyyymmdd.txt`) will be created in the new support directory. Check the 'Log file always appends' box if Aserver should append to the log file rather than overwriting it on startup. The equivalent lines in SAFETRAN.INI are:

```
SupportPath=C:\anypath\  
AppendLog=TRUE
```

3.1.4 SubSystems

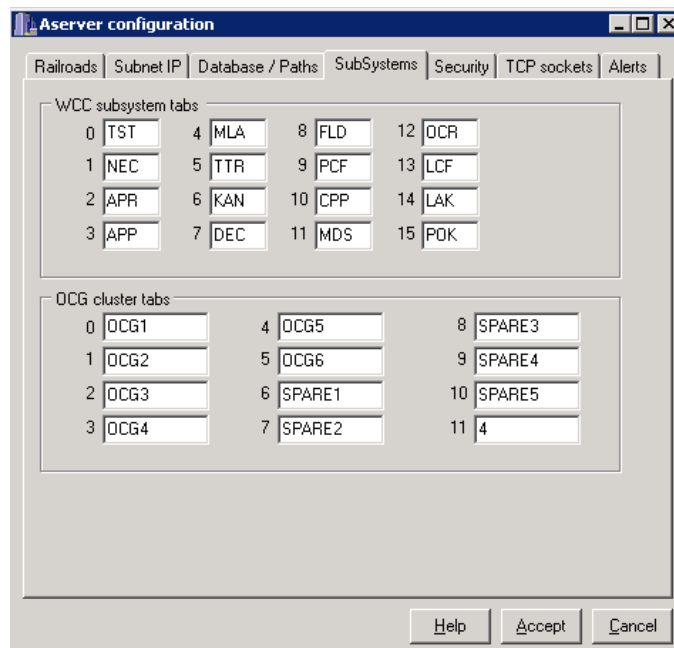


Figure 3-5. Online Configuration – Subsystems Tab

Subsystem tabs, or mnemonics, are the titles of the 16 subsystem tabs appearing on the WccMaint WCC overview screen, and the titles of the 12 OCG cluster tabs. These tabs divide an ATCS network into logical subsystems for easier management. The mnemonics shown above will result in the WccMaint displays shown below. Changes to tab mnemonics must be saved in Aserver before new WccMaint clients will see the new titles (see Figure 3-6).

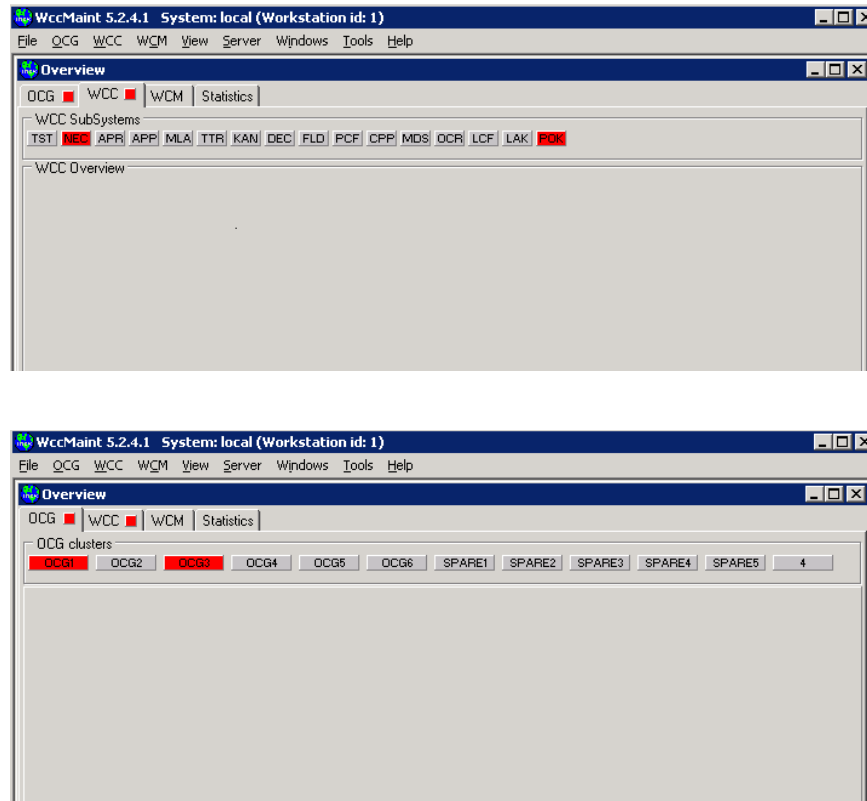


Figure 3-6. Screen Displays From WCCMAINT.EXE

The corresponding lines in SAFETRAN.INI to create these tab mnemonics are:

```

RegionID_0=TST
RegionID_1=NEC
.
.
OCGID_0=OCG1
OCGID_1=OCG2

```

3.1.5 Security

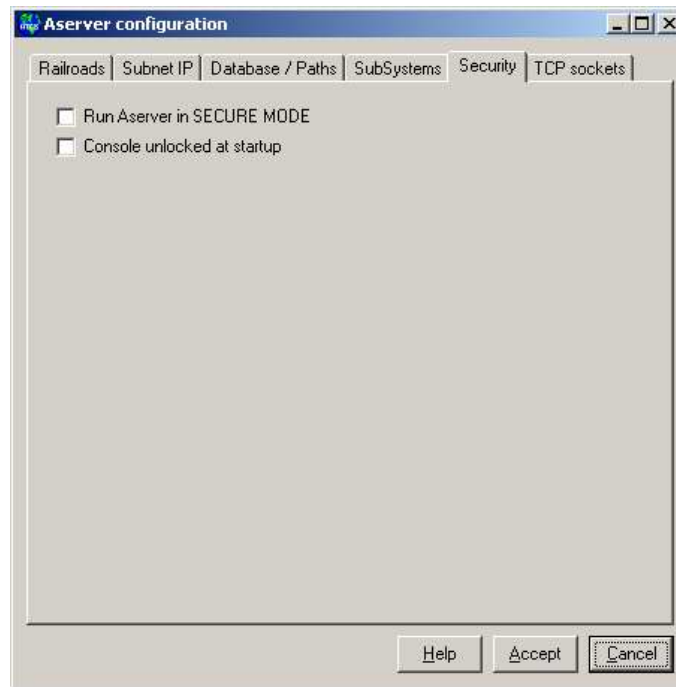


Figure 3-7. Online Configuration – Security Tab

Initially, SECURE MODE is disabled to facilitate installation. If the system is to use Aserver's security features, SECURE MODE must be enabled by checking the appropriate checkbox on this tab. The equivalent line in SAFETRAN.INI is:

SecureMode=TRUE

Setting this flag to FALSE will disable security. Checking the 'Console unlocked at startup' checkbox will set the initial state of the Aserver console (the user interface) to unlocked at the next startup. When the console is unlocked, all security-related menu items and functions on the user interface are enabled. The equivalent line in SAFETRAN.INI is:

InitialKB=Unlocked

If SECURE MODE is enabled and the form is saved, when Aserver restarts, the Security tab now displays all security options (Figure 3-8).

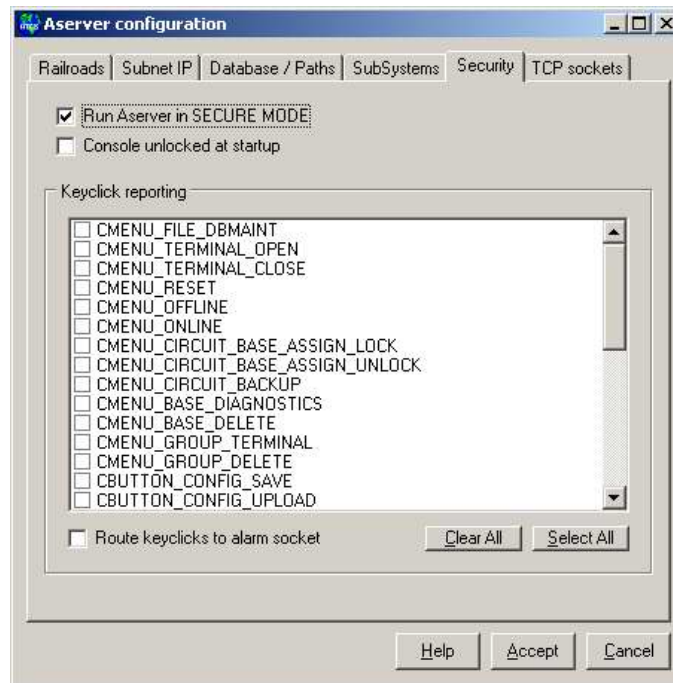


Figure 3-8. Online Configuration – Security Features

The keyclick reporting checklist box is a complete list of keystrokes that may be monitored on each WccMaint client session that logs in under security. For instance, if the Administrator wishes to record any attempts by any WccMaint clients to reset a WCC from its context menu, the CMENU_RESET checkbox is checked. Any subsequent resets will then result in an Aserver log entry similar to:

```
2002/06/03 19:35:08 Node 2 click: CMENU_RESET device: 3000
```

Checking the box 'Route keyclicks to alarm socket' will enable the option of sending the above text message to an established alarm TCP socket connection. Once this form is saved, any new keystroke checks will apply only to newly logged-in users.

NOTE

There are no SAFETRAN.INI equivalent entries for keystroke processing.

See Section 5 for a complete discussion of Aserver's security features.

3.1.6 TCP Sockets

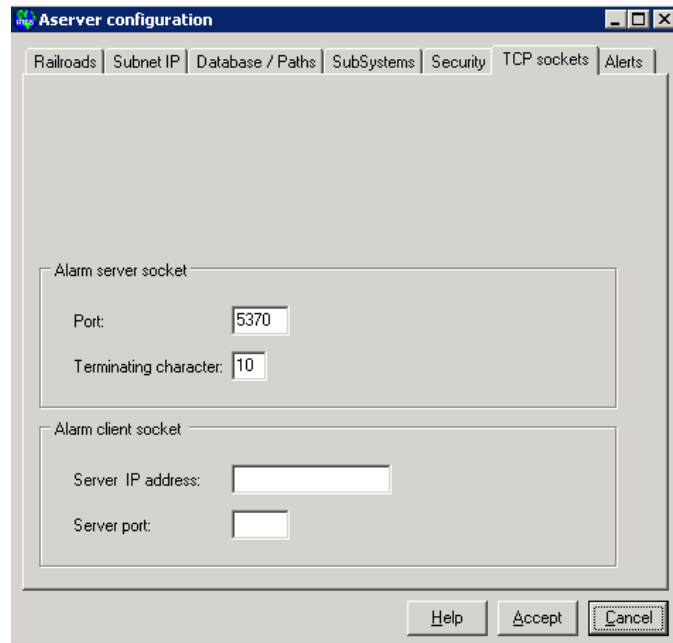


Figure 3-9. Online Configuration – TCP Sockets

Use this screen to configure auxiliary TCP connections maintained by Aserver.

Alarm Server Socket

If a port is specified in this section, Aserver will open a TCP server socket on the given port and wait for a client connection. When a client connects to this socket, Aserver will route text alarm messages from networked WCCs to the client.

The ‘Terminating character’ is an ASCII character appended to the text that is sent to the socket; this is normally used as a delimiting character for the alarm server. The termination character is treated as a decimal value; e.g. for a linefeed character (hex 0A) enter the number 10.

The SAFETRAN.INI lines equivalent to this option are:

```
AlarmServerPort=5370
AlarmTerminator=10
```

Alarm Client Socket

Aserver can be configured to open a client connection to an external server, typically a third-party alarm server. To activate this interface, enter the server IP address and port number in the appropriate edit boxes. If these fields contain legitimate values, Aserver will attempt to open the socket as a client; once a connection is established, Aserver will route text alarm messages from networked WCCs to this socket.

The SAFETRAN.INI lines equivalent to this option are:

```
AlarmClientAddress=  
AlarmClientPort=0
```

3.1.7 Critical Alerts

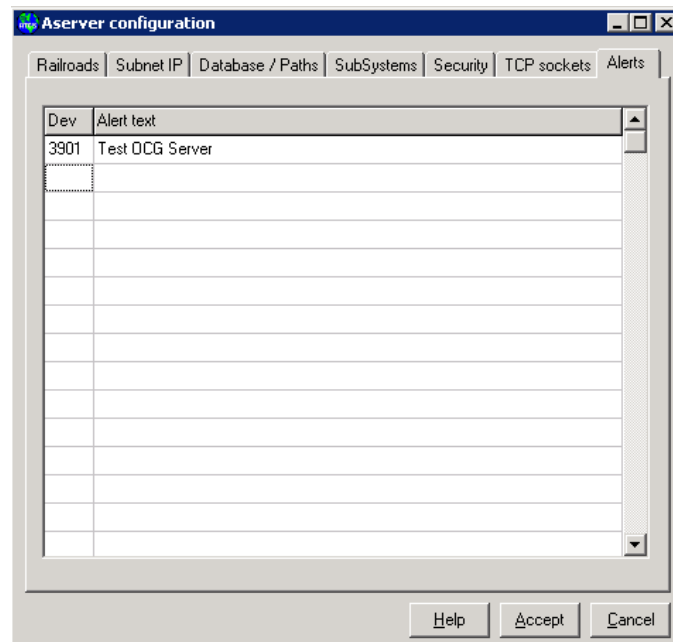


Figure 3-10. Online Configuration – Alerts Tab

Critical alerts are high-urgency messages sent from Aserver to all WccMaint clients. They are generated in Aserver when an OCG or WCC that is designated as ‘critical’ goes offline. A device is considered offline if it has not contacted Aserver in approximately 1 minute. Note that if a critical OCG is shut down, it will take Aserver 50-60 seconds to become aware of the loss of this OCG and send the appropriate alert.. In the example above, OCG 3901 is designated as critical so that WccMaint clients are alerted should it go offline.

CONFIGURATION

Enter device numbers and the desired alert text as shown in Figure 3-10. Up to 100 devices may be designated as critical. When the **Accept** button is clicked, the alerts are activated without having to restart Aserver.

The alert text is sent to each connected client and displayed in red, on top of all other forms as shown in Figure 3-11.

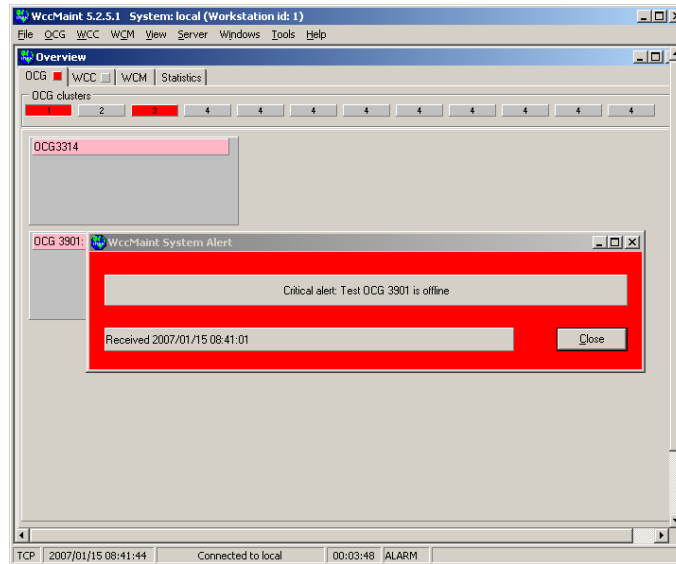


Figure 3-11. Alert Text Display Window

3.2 ASERVER CONFIGURATION OPTIONS LISTING

Table 3-1. Configuration Options – Category: General

INI SWITCH	INPUT VALUES	FUNCTION	NOTES	DEFAULT	UI EDIT
ShutdownWarning	True/False	Flag: if true, user must acknowledge warning dialog before Aserver will shut down		TRUE	No
Pmodule	String	Opens personality module	Enter module name only. (no DLL extension)	nmsp_dflt	No
ContentionEnable	True/False	Enables contention mode	Refer to Appendix E	FALSE	No
ContentionClusterIpIgnore	Valid IP address	Exempts cluster virtual IP address from contention rules	Refer to Appendix E	None	No
OnContention	SHUTDOWN or WARNING	Modifies contention behavior	If superior server is found, this server will either shut down or display a warning. Refer to Appendix E.	SHUTDOWN	No
NoServiceManagerWarning	True/False	Bypasses error message generated on startup when Services Manager is not found		FALSE	No

Table 3-2. Configuration Options – Category: Logging

INI SWITCH	INPUT VALUES	FUNCTION	NOTES	DEFAULT	UI EDIT
SupportPath	Pathspec string	Folder specification for event log	Aserver_log_date.txt event file closes and reopens a new file every day at midnight	C:\safetran	Yes
AppendLog	True/False	Flag: if true, old log file is not overwritten when Aserver is restarted (new events are appended).		TRUE	Yes
LogProxyActivity	True/False	Flag: if true, all messages over TCP link to co-resident OCG are traced.	For co-resident OCG operation only. Events are logged to error log.	FALSE	No
CE_TRACK	True/False	Flag: if true, configuration or executive uploads are noted in event log		FALSE	No
TrackStatus	True/False	Flag: if true, diagnostic display of message tab/label/command appears on status bar	Factory testing only	FALSE	No
EventLogDisable	True/False	Flag: if true, local event log display does not scroll events in realtime. Does not affect logging to the event file.		FALSE	No
TraceLogDisable	True/False	Flag: if true, trace log does not scroll any trace data.		FALSE	No
SqlLogging	True/False	Flag: if true, SQL queries are logged to event file in realtime.		FALSE	No
InitialTrace	Legal IP address	Allows setting up a traced IP address at startup. If set to a valid IP address, the trace window opens when Aserver starts.		None	No

Table 3-2. Configuration Options – Category: Logging - concluded

INI SWITCH	INPUT VALUES	FUNCTION	NOTES	DEFAULT	UI EDIT
TracingEnabled	True/False	Enables/disables the 'Tracing' menuitem in the View menu	Ensures that tracing can be disabled as a power-up default		No
CacheDump	True/False	Enables/disables the tracking (logging) of database cache creation and updates		FALSE	No
CacheDumpFile	Pathspec string	Cache file name		C:\cachedump.p.txt	No
ErrorLogging	True/False	Controls logging of system errors	ErrorLog_20050103.txt	TRUE	No

Table 3-3. Configuration Options – Category: Network

INI SWITCH	INPUT VALUES	FUNCTION	NOTES	DEFAULT	UI EDIT
HandleUdpPAT	True/False	Enables UDP port address translation handling	Needed for some network transports (e.g., cellular)	FALSE	No
SubnetIP_1... SubnetIP_32	Valid IP subnet address	Target subnet for Aserver NMS route broadcast	It is recommended to let the Aserver UI manage these subnets – do not edit directly.	None	Yes
SubnetActive_1 ... SubnetActive_32	True/False	Flag: if true, broadcast will be sent to this address at ClusterTime intervals			
WccDropout	Integer	Timeout value (seconds) for a WCC		150	No
WcmL2RetryTime	Integer	UDP retry interval (seconds) for WCMs	WCCs are hardcoded to 5 seconds	5	No
WcmDropout	Integer	Timeout value (seconds) for a WCM		150	No
WccNode1 ... WccNode10	Integer between 2-98	Exempts NN from WCM classification	See Appendix F	None	No
ClusterTime	Integer between 10 - 240	Time (seconds) between cluster broadcasts.		10	No

Table 3-3. Configuration Options – Category: Network - concluded

INI SWITCH	INPUT VALUES	FUNCTION	NOTES	DEFAULT	UI EDIT
ExclusiveMode	True/False	Flag: if true, Aserver will send/receive UDP packets only to specific IP addresses.	'Legal' IP addresses for Aserver must be explicitly listed. See IPX_1	FALSE	No
IPX_1 ... IPX_50	Valid IP address	IP addresses to be used in exclusive mode.	These switches are in a separate section of safetran.ini: [Aserver IPX].	None	No
NoWcmFilter	True/False	If true, broadcasts from WCMs are not filtered by individual WccMaint range settings.	This effectively makes all WCMs look like WCCs to WccMaint clients.	FALSE	No
MaxSubnets	Integer	Sets the maximum number of broadcast subnets allowed.	Under most circumstances the number of broadcasts should be kept to a minimum; static memory is allocated to store subnets.	16	No
LocalUdpPort	Integer	Sets local (rx) UDP port to use for WCC network.	Used in conjunction with RemoteUdpPort	5361	No
RemoteUdpPort	Integer	Sets remote (tx) UDP port to use for WCC network.	Used in conjunction with LocalUdpPort	5361	No

Table 3-4. Configuration Options – Category: Alarms

INI SWITCH	INPUT VALUES	FUNCTION	NOTES	DEFAULT	UI EDIT
FieldAlarmsToAlarmSocket	True/False	Sends ATCS field alarms to external alarm handler		FALSE	No
HandleRealtimeAlarms	True/False	Flag: if true, Aserver processes the request from WccMaint for a realtime alarm summary		TRUE	No
AlarmServerPort	Integer	TCP port for Aserver to open when it is configured as the Server end of the alarm socket		5370	Yes
AlarmTerminator	Integer	Terminating character (as a decimal integer) appended to every string sent to the alarm socket		10 (CR)	Yes
AlarmClientAddress	Legal IP address	When Aserver is the client end of the alarm socket, this is the address of the server		None	Yes
AlarmClientPort	Integer	When Aserver is the client end of the alarm socket, this is the TCP port to use		None	Yes
AlarmMaxLength	Integer	Truncate strings sent to external alarm server to this length		80	No
RtAlarmLogging	True/False	Controls logging (not handling) of ATCS alarms from the field network	Rtalarms_20050213.txt	FALSE	No

Table 3-5. Configuration Options – Category: Database

INI SWITCH	INPUT VALUES	FUNCTION	NOTES	DEFAULT	UI EDIT
Railroad_1 ... Railroad_10	Integer	Railroad numbers for database	Refer to Appendix B for a list of approved RR numbers	None	Yes
UseDefaultDatabase	True/False	Aserver connects to the blank default ACCESS databases provided on install.	Refer to Installation section	TRUE	No
UseDbServer	True/False	If true, redirects route 9004 destination messages to a standalone DB server.	Reserved for future use.	FALSE	No
NoDatabase	True/False	If true, Aserver runs without any database functions. All other (routing) functions are normal.	This is a common setting for SEAR/WAMS only installations.	FALSE	No
UDLFILE	Pathspec string	Full path/filename of datalink file with connection data for configuration data (NMS_CFG)		None	Yes
RT_UDLFILE	Pathspec String	Full path/filename of datalink file with connection data for realtime data (NMS_RT)		None	Yes
ODBCDSN	String	Name of ODBC data source used for configuration data (NMS_CFG)		None	Yes
RT_ODBCDSN	String	Name of ODBC data source used for realtime data (NMS_RT)		None	Yes

Table 3-6. Configuration Options – Category: OCG/WccMaint

INI SWITCH	INPUT VALUES	FUNCTION	NOTES	DEFAULT	UI EDIT
RegionID_1 ... RegionID_16	String	Sets tab names for WCC clusters in WccMaint	Max chars is 3. Input will be truncated if necessary		Yes
Ocgld_1 ... Ocgld_12	String	Sets tab names for OCG clusters in WccMaint	Max chars is 8. Input will be truncated if necessary		Yes
OcgProxy	True/False	Flag: if true, Aserver opens TCP socket 5383 and expects a connection to OCG on this socket	For co-resident OCG operation only.	FALSE	No
WcmMin	Integer	Lower node in WCM range for WccMaint	Allows setting default range for all WccMaint users	0	No
WcmMax	Integer	Higher node WCM range for WccMaint		0	No
CriticalAlert1... CriticalAlert100	Integer between 3000-3999	Device number of packet switch / OCG that is monitored for critical failure	These switches are in a separate section of safetran.ini: [AserverAlerts]. Direct edits are not recommended.	None	Yes
CriticalAlertText1... CriticalAlertText100	String	Text displayed for offline condition of monitored device			

Table 3-7. Configuration Options – Category: Security

INI SWITCH	INPUT VALUES	FUNCTION	NOTES	DEFAULT	UI EDIT
SecureMode	True/False	Enables secure mode.	Secure mode requires logins and passwords from WccMaint users.	FALSE	Yes
ConsoleLock	True/False	Enables/disables security-related functions of the UI. Has no effect if Secure Mode is not enabled		FALSE	Yes

Table 3-8. Configuration Options – Category: Diagnostics

CAUTION

THESE PARAMETERS CAN AFFECT SERVER OPERATION.

INI SWITCH	INPUT VALUES	FUNCTION	NOTES	DEFAULT	UI EDIT
ShowUdpStatus	True/False	Diagnostic flag	Factory use only	FALSE	No
No5370	True/False	Flag: if true, disables alarm socket functionality, client or server (whichever is enabled)	Diagnostic tests only	FALSE	No
No5371	True/False	Flag: if true, disables socket for communications with WCT application	Diagnostic tests only . WCT is used for dialup SEAR-II applications	FALSE	No
No5380	True/False	Flag: if true, disables socket used with NMS services	Diagnostic tests only	FALSE	No
No5381	True/False	Flag: if true, disables socket used by WAMS Status Manager	Diagnostic tests only	FALSE	No
No5382	True/False	Flag reserved for future use	Diagnostic tests only	FALSE	No
No5390	True/False	Flag: if true, communications with WccMaint clients is disabled	Diagnostic tests only	FALSE	No
No5361	True/False	Flag: if true, disables UDP connectivity with WCC network	Diagnostic tests only	FALSE	No
No2000	True/False	Flag: if true, disables UDP connectivity with legacy GEONODE applications	Diagnostic tests only	FALSE	No
No68	True/False	Flag: if true, DHCP monitoring is disabled	Diagnostic tests only. Disables remote WCM bootstrap function	FALSE	No

SECTION 4

OPERATION

4.0 OPERATION

4.1 INTRODUCTION

Aserver is primarily a packet router and, therefore, does not require significant operator intervention to function normally. Once the configuration has been completed and Aserver put into operation, it will run indefinitely with no periodic or recommended maintenance.

A Graphical User Interface (GUI) is included to provide the operator with visual indications of the status of the ATCS network in terms of system management-oriented traffic. Statistics are available to monitor network conditions and troubleshoot connection and traffic problems. The Aserver console (GUI) is not intended as a troubleshooting tool for code systems; the WCC Maintenance utility (WccMaint.EXE) is better suited for this purpose. Certain console functions (ie, logging and tracing) are included for tracking non-critical problems, but in general, particularly on a busy system, these troubleshooting tools are more appropriate to WccMaint. The majority of this section deals with interpreting the status information on the main form and navigating its menus.

There are some administrative functions in Aserver that have to do with system security. These are fully described in Section 5, 'Security'.

4.2 THE ASERVER CONSOLE

The primary user interface for Aserver is the user console, a single overview form with indicators and statistics that reflect the status of the diagnostic network. This section explains the statistics and controls on the console.

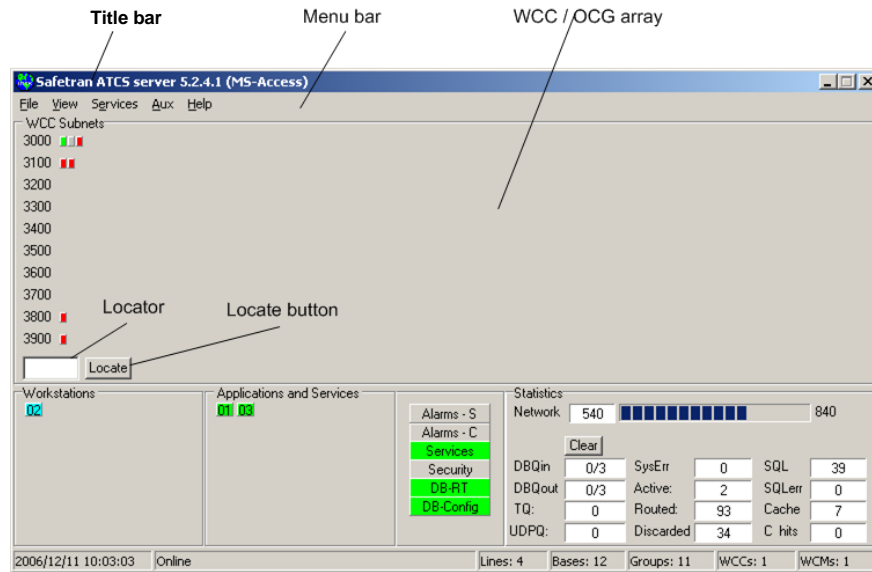


Figure 4-1. ASERVER Console (Upper)

Menu Bar:

The menu bar is used to access all available secondary forms. Services and User manager interfaces are accessed via the menu bar. The menu system is fully described in paragraph 4.3.

Title Bar:

The Title bar summarizes the current Aserver configuration. Program title, database type (Access or SQL Server) and if enabled, security mode and console condition are displayed in the Title bar.

WCC/OCG Array:

The WCC/OCG array is a 10-row by 100-column grid of panel icons that represent WCCs or OCGs that are visible to Aserver. In Figure 4-1, 7 WCCs are displayed in various states.

NOTE

For illustrative and descriptive purposes, the terms WCC and OCG are used interchangeably in this document. Aserver does not differentiate between WCCs and OCGs on the panel display.

A device address for a WCC is the device (DDDD) portion of its ATCS address (device address ranges for WCCs are currently restricted to 3000-3999 – see Appendix F). As the grid display is too compact to display device numbers directly, any WCC's device number may be viewed by hovering the mouse over its panel icon. The device number will appear momentarily as a Windows hint box. In normal operation, all WCCs will be green and the grid functions as a health overview for connected units. If a WCC should lose contact with Aserver, its panel icon will turn red. The hover feature may be used to determine which WCC has failed.

When a WCC establishes a connection with Aserver, a green panel is created for it and a keep-alive timer is established for the WCC. The timer is refreshed every time a region or WCC update message is received from the WCC, which sends the updates at least once per minute. Because WCCs are connected via UDP, which is a connectionless, non-guaranteed communications protocol, some packets may be lost on busy networks. The WCC timer will expire if 150 seconds pass without any status updates from the WCC. When this occurs, the panel will turn red and an alarm message will be generated and sent to any configured alarm sockets. When the WCC re-establishes connection, the panel turns green and a recovery message is sent to the alarm sockets (if enabled).

On startup, Aserver scans the database for WCCs that are in the database and classified as in-service. It then creates a yellow icon for each of these WCCs, which turn green when contact with the WCC is established. If the WCC is not heard from in 150 seconds, the panel icon turns red.

A gray panel icon indicates a WCC that is sending packets to Aserver, but is not properly initializing communications. This indicates that the unit is misconfigured or has incorrect firmware loaded.

Locator / Locator Button:

Because the WCC subnet array has no visible numbers associated with the panel icons, a locator function has been added to the display. To locate a particular WCC, type its device number (3005, for example) into the locator field and click the locator button. If the desired WCC is online, its panel icon will flash. Click the locator button a second time to stop the flashing.

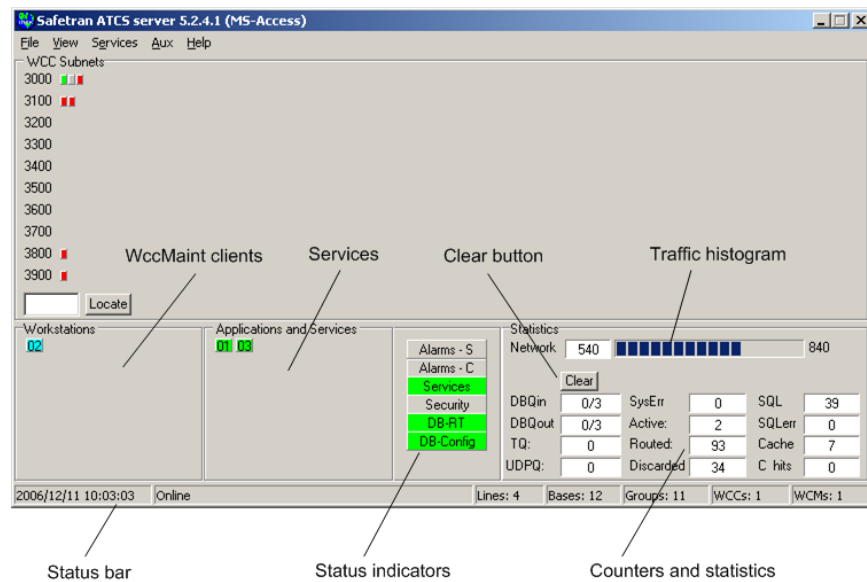


Figure 4-2. ASERVER Console (Lower)

WccMaint Clients:

This area is a 4-row by 16-column grid of panel icons that represent WccMaint client nodes currently connected to Aserver. Node numbers are arbitrary and are assigned to the WccMaint client node when it connects. The node numbers are displayed on the panel icons, and unlike the WCC subnet array, this array is automatically sorted.

Services:

This area contains icons that represent NMS services or third-party applications that are nodes currently connected to Aserver.

NOTE

The term 'node' in Aserver context means any session or process that creates and maintains a client relationship with Aserver. Typically, this is either a WccMaint session or a client service (the Alarm Status Service, for example). A node is a logical endpoint in the ATCS network, so Aserver maintains one or more routes for any connected node, and therefore is able to route messages to and from these nodes. This is why the Services Manager is not a node to Aserver and is not represented in the array – it never sends or receives messages as an endpoint.

Colors are used to differentiate between node types and their status. A green node is a service connected through the Services Manager (these are always TCP socket connections). Cyan denotes a WccMaint client connected via TCP socket. Under secure mode, a white node is a WccMaint client that has contacted Aserver but has not yet logged in. As always, red signifies that the node is no longer connected: it has timed out (UDP) or the socket has been disconnected (TCP).

The Workstation node array also has hover hint features for the icon panels. When the mouse is hovered over a node, the hint displays the node number, the type of connection and its IP address. For instance, hovering over a service node panel will display the hint text:

N1: TCP-SRVC at 127.0.0.1

This signifies that Node 1 is a TCP-connected service originating at IP address 127.0.0.1. If a WccMaint client node is hovered, the hint text will display, for example:

N2: TCP-WCCM at 150.50.143.25

This means Node 5 is a TCP-connected WccMaint client at the given IP address.

Hints for WccMaint clients are different under secure mode. See Section 5 for details.

Status Bar:

The status bar is a partitioned panel that displays text messages that reflect system status. From the left, the panels display:

- Current time
- Status or error messages
- Total number of ATCS codelines in the database
- Number of bases in the database
- Number of groups in the database
- Number of nodes currently connected. This is the total number of nodes: workstations, services and WCCs.
- Number of nodes classified as WCMs. To Aserver, WCMs are functionally the same as WCCs or OCGs (in that they are considered ATCS office devices with type 2 addresses), but are not represented in the WCC/OCG array. Treatment of WCMs, and their addressing and restrictions, are explained in Appendix F.

Status Indicators:

This section presents a visual display of optional connections to Aserver; ie those that are neither WccMaint clients nor WCCs:

- **Alarms-S** : If Green, Aserver has opened a server socket for an external alarm client and the client has connected. If red, the client had connected but the connection was lost or terminated. If gray, either the socket is available but no client has connected or this feature is not configured.
- **Alarms-C** : This panel refers to Aserver's client connection to an external alarm server. It turns yellow when a connection is made or when alarm text is sent to the server. It turns green when text is received from the server. If the connection is lost or closed, the panel turns red. Gray signifies that this feature is not configured.
- **Services**: Green indicates that one or more services are currently connected through Services Manager. Note that Services Manager itself will not set this panel green. If any service terminates its connection, the panel will turn red. Gray indicates that no services are installed or running.
- **Security**: This panel will be green if secure mode is active; otherwise it is gray.
- **DB-RT**: This panel is green as long as the connection to the realtime database is active. Red indicates loss of connection to the database. This panel is never gray once Aserver initialization is complete.
- **DB-Config**: This panel is green as long as the connection to the configuration database is active. Red indicates loss of connection. This panel is never gray once Aserver initialization is complete. NOTE: the database connections are managed in a separate thread from Aserver's main thread. This panel or the DB-RT panel may turn red if the thread stops executing, which would indicate a program fault or fatal database error.

Packet Statistics:

These panels are counters that display various internal statistics. All count are referenced to Aserver startup or the last time the 'Clear' button was clicked.

- **DBQin, DBQout**: All database functions are handled in a separate program (database) thread, and messages to and from this thread must be queued. Messages from the main Aserver thread to the database thread go to the DBQin stack. After the database thread has processed the message, if a return message must be sent to the network, this message is placed in the DBQout stack to return to the main Aserver thread. This panel is therefore a rough gauge of the depth of both queues, and indirectly an indication of how busy the database thread is. Each value is represented as the number of messages currently in the queue with the highest number of messages the queue has ever held. A display of 0/3, for example, indicates the queue is currently empty, but has had as many as 3 messages queued.

- **TQ:** This is used for factory diagnostics only.
- **UDPQ:** This is the number of UDP datagrams sent to UDP clients that are stored pending an acknowledgement from the destination host. This is an indirect indicator of how busy/responsive the network is. This number should always be very low; around 0-4 for average sized networks..
- **Active:** Number of active nodes; same as status panel nodes count.
- **Routed:** This is the total number of packets routed by Aserver.
- **Discarded:** This is a count of all packets that cannot be routed, usually because the destination route in the message does not exist in Aserver's route list.
- **SQL:** Total number of SQL queries executed against both databases.
- **SQLerr:** When the execution of a SQL query results in a database error, this count is incremented. This could be due to a syntax error, duplicate record found, a sequence error, or incorrect database versions. SQL errors are always logged in the event log. This count should be zero; always report any SQL errors to Safetran support.
- **Cache:** Total number of cache requests. See note on caching below.
- **C hits:** Total number of cache requests that were successful. This number should be very close to the cache count above.
- **Network:** This is a count of all packets received from all nodes. It is reset every 60 seconds, so this functions as a packets-per-minute indicator of network traffic. This value is graphically displayed in the traffic histogram.

Clear Button:

Clicking this button clears the above stats windows. This event is logged.

Traffic Histogram:

A visual display of the total packets received by Aserver from all nodes in one minute. This is the same as the Network statistic above.

NOTE

When Aserver initializes, it retrieves basic data (names, states, equipment types, etc) for all bases and groups in the database. This data is cached internally and is used to buffer requests from WccMaint clients for routine line display data. In this way the database is not queried constantly for the same data. In general, cache counts should always far exceed SQL statements, and cache hits should be nearly the same as cache counts. The cache hit percentage (cache hits / cache count) should be above 90%.

4.3 MAIN MENU

4.3.1 FILE Submenu

Clicking on 'File' on the menu bar will display the File Submenu as shown in Figure 4-3:

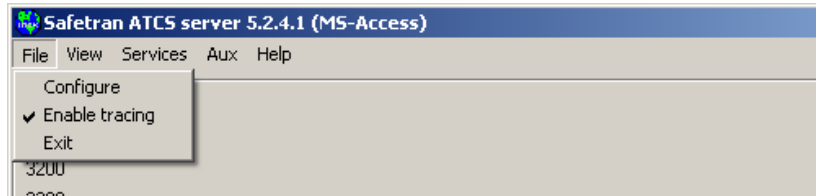


Figure 4-3. ASERVER Menu Bar – File Submenu

4.3.1.1 FILE: Configure

Click 'Configure' to display the online configuration screen. For full details on configuring Aserver with this online tool, see Section 3 .

4.3.1.2 FILE: Enable Tracing

This is a checkbox-style menu item that enables the menu item for tracing (under the **View** section below). This is meant as a safeguard against accidentally clicking the **Trace** function, which is a feature that can have adverse effects on the system. See comments under **tracing** below.

4.3.1.3 FILE: Exit

This is the preferred method of shutting down Aserver; all cache files will be flushed and allocated memory released, then any services will be shut down in an orderly way.

4.3.2 VIEW Submenu

Click 'View' on the File menu to display the View submenu:

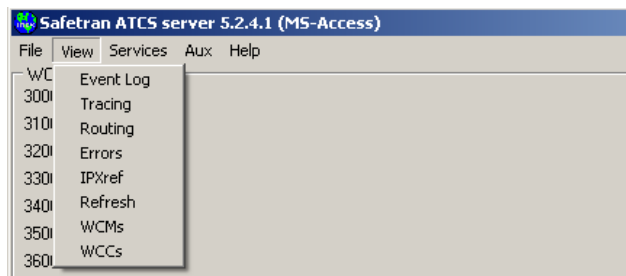


Figure 4-4. ASERVER Menu Bar – File Submenu

4.3.2.1 VIEW: Event Log

Aserver maintains the event log on the configured hard drive. When 'Event Log' is clicked, a copy of the event file is made and read into a window for display:

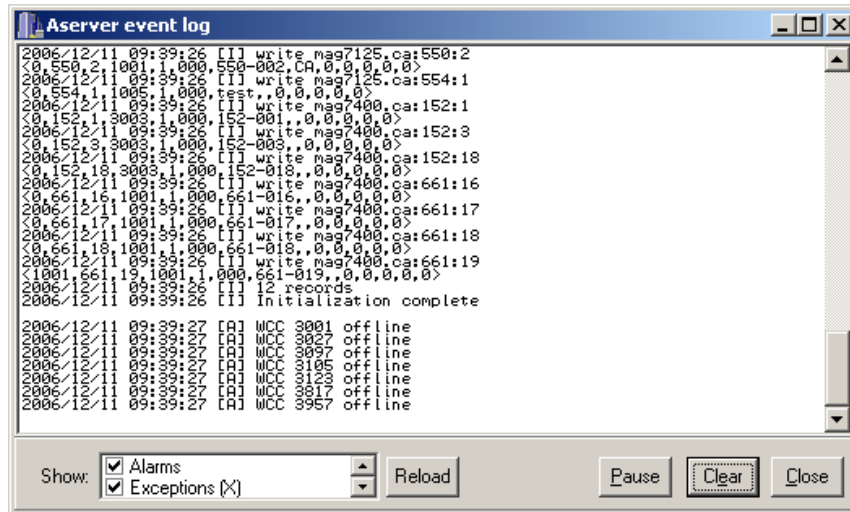


Figure 4-5. Event Log Window

The first 20-25 lines in the event log are informational messages generated when Aserver is initializing. Most log entries pertain to database startup. The checkbox list at the bottom of this form allows the user to enable or disable logging of the following events:

- Alarms (A): Aserver-generated WCC alarms
- Exceptions (X): Program failures or traps, typically Access Violations
- Information (I): Non-critical log events
- Warnings (W): Potential problems, typically with UDP connections
- Field alarms (F): ATCS alarms received from bases/groups
- System errors (E): Internal events not caught by the exception mechanism
- DB errors (Q): Errors generated by the database driver (typically syntax errors)
- DB queries (S): SQL queries executed
- DHCP events (D): BOOTP messages between WCMs and WccMaint clients (see Appendix F)
- Security keyclicks (C): Critical WccMaint user clicks/keystrokes logged
- Security login events (L): Login/logout events
- Debug messages (Z): Factory debugging messages

The following events are checked by default: Alarms, Exceptions, Information, Warnings, System errors, and DB errors.

Another feature of the event log is that the checkboxes can be used to filter the log display. Note that every line in the log is preceded by an identifier character (A for alarms, for example). The log can be filtered based on these identifiers. For example, the log shown above can be filtered to display only Alarms. Uncheck all checkboxes except for **Alarms**, and click **Reload**.

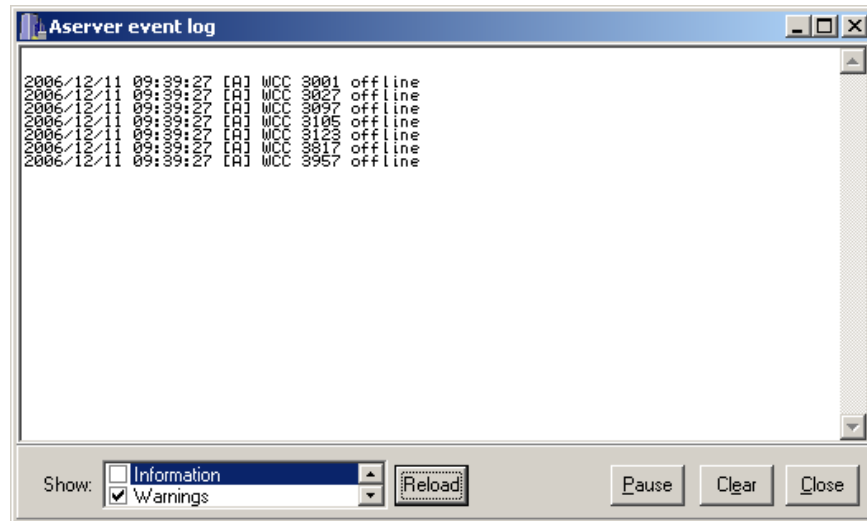


Figure 4-6. Event Log Window Filtered To Show Alarms Only

The event log display is now filtered for alarms only.

Pause Button:

Log messages will not scroll into the window if this button is clicked. Any messages missed are not recoverable in the current window, but they are logged to the hard disk file. The event log window can be closed and re-opened to view missed messages if desired. To resume logging to the window, click the button again (the button label will change to 'Resume' if the display is paused).

Clear Button:

Clicking this button will clear the display window. The contents of the log file itself are not affected.

Close Button:

Clicking this button closes the log window.

4.3.2.2 VIEW: Tracing

Clicking this menu item displays the trace window as shown in Figure 4-7.

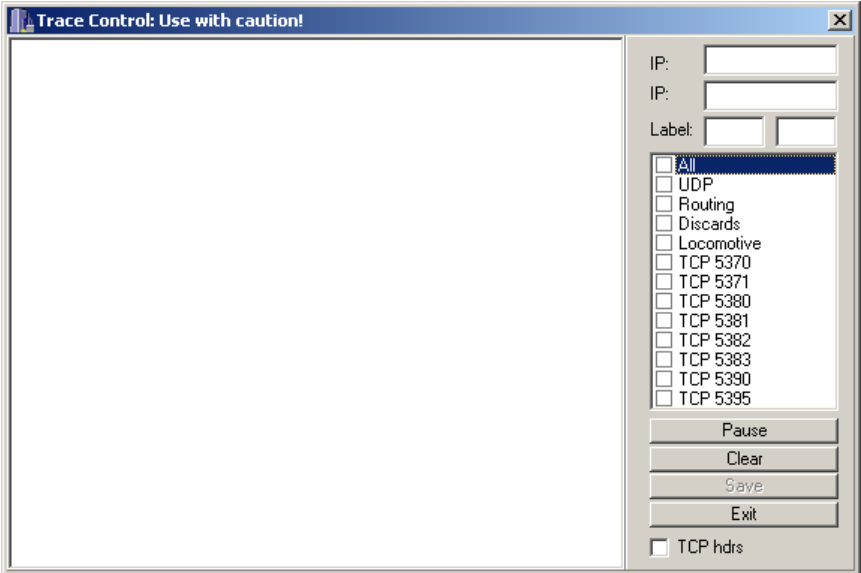


Figure 4-7. The Trace Window

Tracing is a troubleshooting method that displays the contents of any message in or out of Aserver. Most messages are full ATCS messages, but low-level packets including route broadcasts and Layer 2 connection messages are also traceable.

WARNING

AS THE TITLE BAR INDICATES, TRACING IS EXTREMELY PROCESSOR-INTENSIVE AND SHOULD BE USED JUDICIOUSLY. ASERVER OPERATION CAN BE DISRUPTED AND POSSIBLY DISABLED IF VERBOSE TRACING IS ENABLED ON A BUSY NETWORK. BECAUSE ASERVER SEES ALL NMS TRAFFIC ON THE NETWORK, MESSAGE TRACING IS A TOOL THAT IS MUCH EASIER AND SAFER TO USE FROM A WCCMAINT SESSION. USE THIS TOOL ONLY WHEN ABSOLUTELY NECESSARY.

The correct way to trace messages in Aserver is to use filters to trace only selected messages. The following filters are available:

OPERATION

IP:

Two IP addresses may be traced; only messages to or from IPs matching those in the IP window will be traced.

Label:

Enter the hex value of an ATCS message label in this edit box to selectively display only messages that contain that label. For instance, entering 04E0 in this box will trace all WCC status messages (WCC_LOCAL_STATUS_REPLY).

Level:

The level of tracing may be set by checking the appropriate check box in this control. Available levels are:

- All: every message in and out of Aserver will be traced when this box is checked. See note below.
- UDP: All UDP traffic is traced (all WCC/OCG traffic).
- Routing: UDP routing messages (INT_RTE_REQUEST, INT_RTE_UPDATE) are traced.
- Discards: Discarded (unroutable) messages are traced.
- Locomotive: type 1 traffic (to/from locomotive devices) traced
- TCP 5370: Alarm socket data
- TCP 5371: WCT socket data
- TCP 5380: NMS Services socket data
- TCP 5381: WAMS Status Manager
- TCP 5382: Aux ATCS socket (third-party applications)
- TCP 5383: Coresident OCG
- TCP 5390: WccMaint clients
- TCP 5395: Crossing alarms from WAMS Status Manager

To set up tracing, first enter any IP or label filters, then select the level of the data stream that will pass through the filters. Multiple streams (TCP sockets) may be selected. Filters are not applied to Routing, Discard, or Locomotive streams (these are traced regardless of filter settings).

As an example, to trace a specific message passed from an OCG to a WccMaint client, enter the IP address of the WccMaint client and of the OCG, enter the message label, then select TCP 5390 (WccMaint) and UDP (OCG).

NOTE

When **All** or **UDP** is checked, and no other filters (IP, label) have been entered, this potentially harmful trace is prompted for confirmation as shown in Figure 4-8.

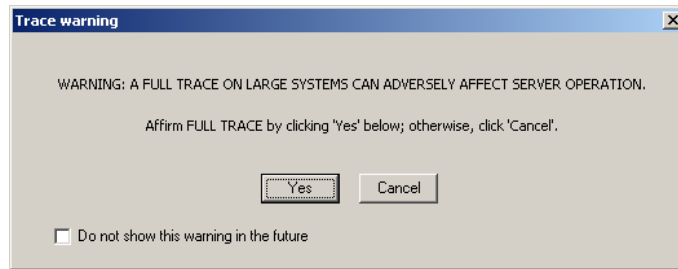


Figure 4-8. Full Trace Warning Message

Pause Button:

Clicking this button will stop the display from scrolling as new data arrives (incoming data is not lost).

Clear Button:

Clicking this button will clear the display.

Save Button:

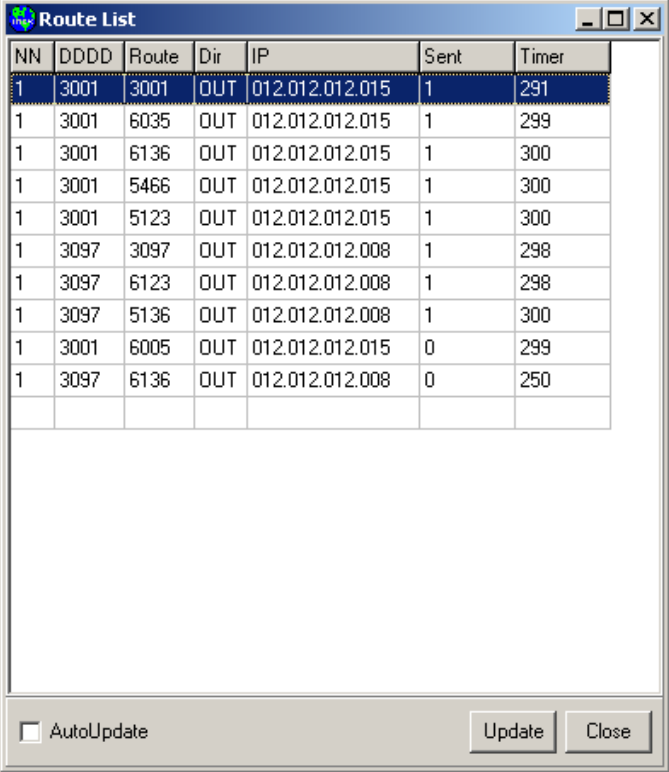
Click this button to save the entire contents of the window, including any text that has scrolled out of view, to a file.

Exit Button:

Click this button to close this window. NOTE: all tracing will be stopped when the window is closed. The user is prompted to save any unsaved trace data before the form is closed.

4.3.2.3 VIEW: Routing

Clicking this menu item to display the Aserver Routing Table.



The screenshot shows a window titled "Route List" with a table of routing information. The table has seven columns: NN, DDDD, Route, Dir, IP, Sent, and Timer. The data is as follows:

NN	DDDD	Route	Dir	IP	Sent	Timer
1	3001	3001	OUT	012.012.012.015	1	291
1	3001	6035	OUT	012.012.012.015	1	299
1	3001	6136	OUT	012.012.012.015	1	300
1	3001	5466	OUT	012.012.012.015	1	300
1	3001	5123	OUT	012.012.012.015	1	300
1	3097	3097	OUT	012.012.012.008	1	298
1	3097	6123	OUT	012.012.012.008	1	298
1	3097	5136	OUT	012.012.012.008	1	300
1	3001	6005	OUT	012.012.012.015	0	299
1	3097	6136	OUT	012.012.012.008	0	250

At the bottom of the window, there is a checkbox labeled "AutoUpdate" which is unchecked, and two buttons labeled "Update" and "Close".

Figure 4-9. ASERVER Routing Table Window

The route list displays all routes registered for each node, including the route direction, count of packets sent to this route, IP address, and the route timer. Aserver routes are dynamic, so that they will be created on demand and expire if not refreshed in 5 minutes.

The display may be sorted by clicking the header of the desired column. For example, the display below shown in Figure 4-10 has been sorted by Route.

NN	DDDD	Route	Dir	IP	Sent	Timer
1	3001	3001	OUT	012.012.012.015	1	291
1	3097	3097	OUT	012.012.012.008	1	298
1	3001	5123	OUT	012.012.012.015	1	300
1	3097	5136	OUT	012.012.012.008	1	300
1	3001	5466	OUT	012.012.012.015	1	300
1	3001	6005	OUT	012.012.012.015	0	299
1	3001	6035	OUT	012.012.012.015	1	299
1	3097	6123	OUT	012.012.012.008	1	298
1	3097	6136	OUT	012.012.012.008	0	250
1	3001	6136	OUT	012.012.012.015	1	300

AutoUpdate Update Close

Figure 4-10. Route List Sorted By Route Number

AutoUpdate Checkbox:

If this box is checked, it is equivalent to clicking the 'Update' button once per second. This display does not update by default because slow diagnostic connections have a problem keeping up with changing displays.

Update Button:

Click this button to refresh the display (check for new/expired routes and update the timers).

4.3.2.4 VIEW: Errors

When this menu item is clicked, the Error form is displayed.

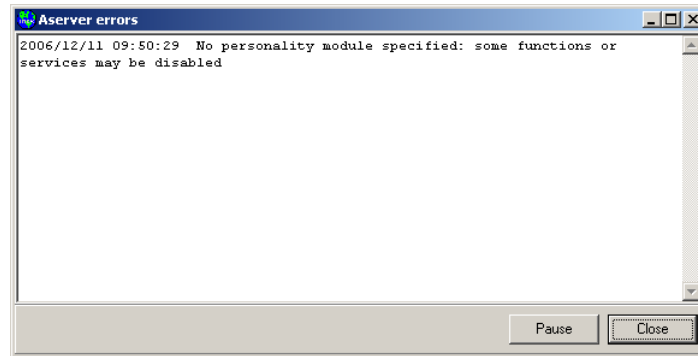


Figure 4-11. ASERVER Errors Window

This form contains any error messages posted by Aserver during startup and normal operation. If errors occur during startup (as shown above), this form will display automatically.

4.3.2.5 VIEW: IPxref

Clicking this menu item will display the IP Cross Reference Table (Figure 4-12).

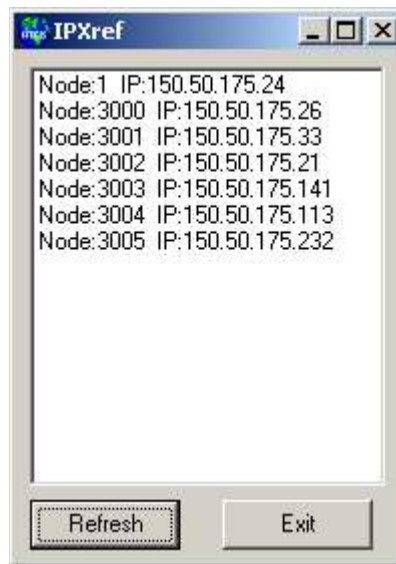


Figure 4-12. IP Cross Reference Table Window

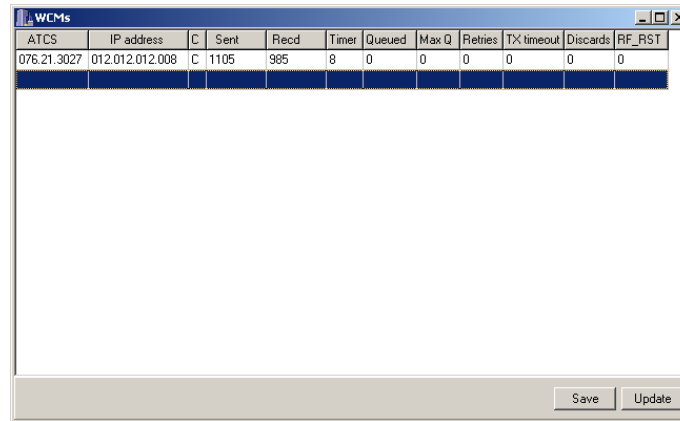
This table identifies registered nodes in terms of their respective IP addresses.

4.3.2.6 VIEW: Refresh

Clicking this menu item will refresh the node display; any icons for WCCs that are gray will be deleted.

4.3.2.7 VIEW: WCMs

Clicking this menu item will open the WCM List Window as shown in Figure 4-13.



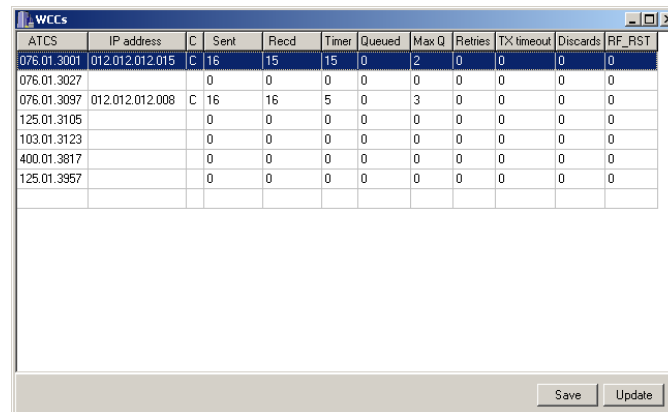
ATCS	IP address	C	Sent	Recd	Timer	Queued	Max Q	Retries	TX timeout	Discards	RF_RST
076.01.3027	012.012.012.008	C	1105	985	8	0	0	0	0	0	0

Figure 4-13. WCM List Window

All registered WCM devices on the network are displayed in this grid, with ATCS address, IP address, and UDP packet statistics. This display may be sorted by ATCS or IP address by clicking on the appropriate column header.

4.3.2.8 VIEW: WCCs

Clicking this menu item will open the WCC List Window as shown in Figure 4-14.



ATCS	IP address	C	Sent	Recd	Timer	Queued	Max Q	Retries	TX timeout	Discards	RF_RST
076.01.3001	012.012.012.015	C	16	15	15	0	2	0	0	0	0
076.01.3027			0	0	0	0	0	0	0	0	0
076.01.3097	012.012.012.008	C	16	16	5	0	3	0	0	0	0
125.01.3105			0	0	0	0	0	0	0	0	0
103.01.3123			0	0	0	0	0	0	0	0	0
400.01.3817			0	0	0	0	0	0	0	0	0
125.01.3957			0	0	0	0	0	0	0	0	0

Figure 4-14. WCC List Window

All known WCC/OCG devices on the network are displayed in this grid, with ATCS address, IP address, and UDP packet statistics. This display may be sorted by ATCS or IP address by clicking on the appropriate column header.

4.3.3 SERVICES Submenu

Click 'Services' on the File menu to display the Services submenu.

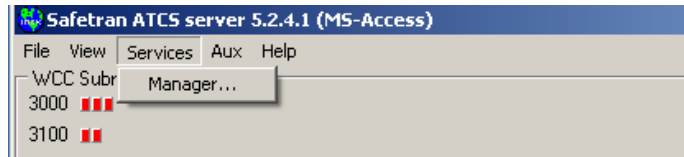


Figure 4-15. Services Submenu

4.3.3.1 SERVICES: Manager

Click 'Manager' to display the Services Manager user interface (Figure 4-16).

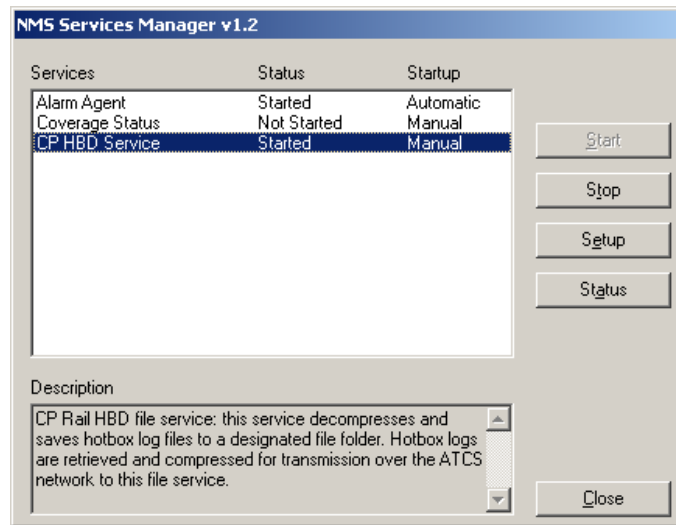


Figure 4-16. Services Manager Window

The NMS Services Manager is the common interface for all TCP-based services provided by Safetran. The Services Manager is the 'gateway' to the ATCS network via Aserver for these services.

All Service Manager functions (Start/Stop/Setup/Status) pertain to individual services. There is no configuration or setup required for Services Manager itself.

Contact Safetran for more information about available TCP services.

4.3.4 AUX Submenu

Click 'AUX' on the File menu to display the AUX Submenu (Figure 4-17).

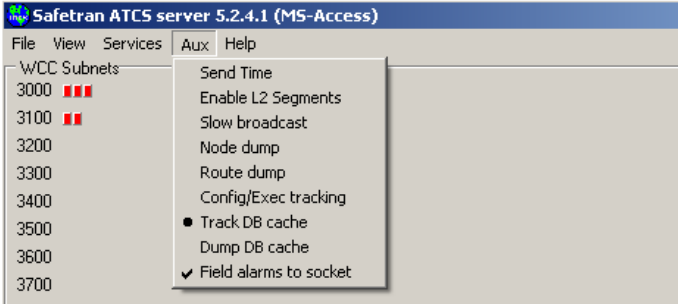


Figure 4-17. Aux Submenu

4.3.4.1 AUX: Send Time

Click 'Send Time' to send a TIME_MESSAGE (label 0xD702) as a broadcast to all online type 2 devices (WCCs, OCGs, WCMs). This message contains the current time/date on the machine that is hosting Aserver. In this way, a single time source is propagated throughout the ATCS network. Aserver automatically sends a time message to a WCC/OCG/WCM when it first connects and every 12 hours thereafter.

4.3.4.2 AUX: Enable L2 Segments

This menu item is deprecated and will be removed from future releases.

4.3.4.3 AUX: Slow Broadcast

This is an on/off option that will set Aserver's cluster broadcast time to 240 seconds instead of the standard 10 seconds. This is generally only used when another server is running in exclusive mode and needs to 'steal' WCCs from an active server. See paragraph 4.4.

4.3.4.4 AUX: Node Dump

Clicking this function will create a text file listing all nodes and their statistics to a file named VNODES.DMP. This file is used for diagnostics only.

4.3.4.5 AUX: Route Dump

Clicking this function will create a text file listing all NMS routes with statistics to a file named ROUTES.DMP. This file is used for diagnostics only.

4.3.4.6 AUX: Config/Exec Tracking

Clicking this function will set a flag in Aserver that forces a log entry every time a WccMaint client uploads either a configuration or executive software to a WCC (packet switch). OCG uploads are not included. The log line is of this format:

```
EXEC tag 25842 (1/32) to 76.1.3401 at 10.14.55.11 from 2.000.00.2014 at 10.15.1.14
```

This means message number 25842 (this is an internal tag), which was part 1 of 32 (multipart message), was sent to WCC 76.1.3401 from workstation 14. The IP addresses are included as well.

Note that this mode is redundant in systems running in secure mode. The intent of this flag is to document uploads in systems that do not implement security.

4.3.4.7 AUX: Track DB Cache

Setting this flag creates log entries that track changes to the database cache. This is typically only used temporarily for diagnostic purposes.

4.3.4.8 AUX: Dump DB Cache

Clicking this function creates a text file image of the current state of the database cache. This function is typically only used for diagnostic purposes.

4.3.4.9 AUX: Field Alarms To Socket

Setting this flag forces a log entry that records any ATCS alarm that has come in from the ATCS field network. The text is also sent to the alarm socket, if configured.

4.3.5 HELP Submenu

Click 'Help' on the File menu to display the Help submenu:



Figure 4-18. Help Submenu

4.3.5.1 HELP: Version

Click 'Version' to display Aserver version information (Figure 4-19).

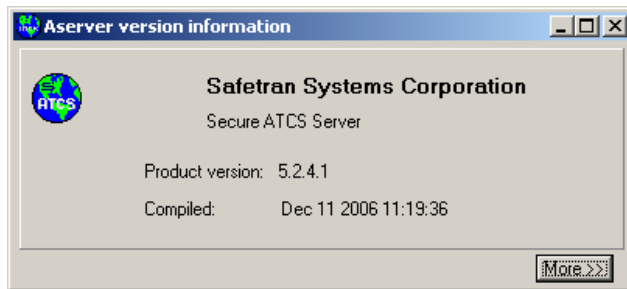


Figure 4-19. ASERVER Version Window

Extended diagnostic information is available on the extended form. Click 'More' to view extended help (Figure 4-20).

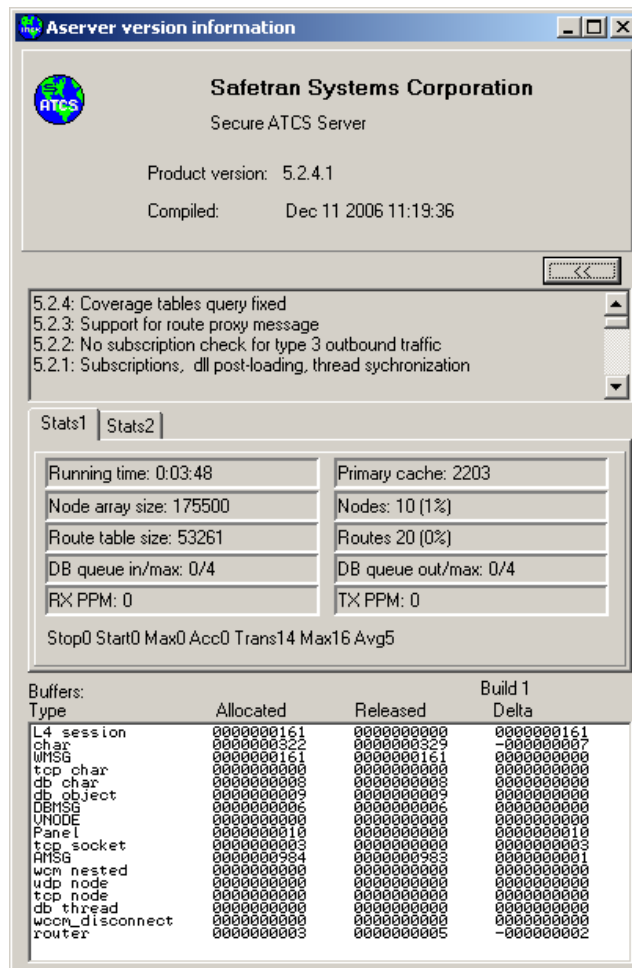


Figure 4-20. Extended Help Window

The scrollable text box contains a running list of updates to Aserver. Usually there are one or two updates per release.

OPERATION

Most of the diagnostic information on this form is of no interest during normal operation. In case of a software problem, however, these statistics may be helpful in determining its cause (contact Safetran support for assistance).

- Running time – The elapsed time Aserver has been running since the last restart.
- Primary Cache – The amount of system memory (heap space) allocated for database caching.
- Node array size – The amount of stack space allocated for internal node tables.
- Nodes – Number of nodes in use and percentage of available nodes used.
- Route table size – The amount of stack space allocated for the routing table.
- Routes – Current number of routes and percentage of total available.
- DB Queue in/max – Number of messages currently waiting to be processed by the database thread, and the maximum value attained.
- DB Queue out/max – Number of messages currently waiting to be routed from the database thread, and the maximum value attained.
- Buffers – Total number of unreleased buffers allocated for general use.
- Messages – Total number of unreleased buffers allocated for ATCS message handling.

4.4 DIAGNOSTIC MODES

4.4.1 Exclusive Mode

CAUTION

THIS IS AN 'EXPERT LEVEL' FUNCTION THAT CAN DISRUPT NORMAL ASERVER OPERATION AND IS INTENDED FOR EXPERIENCED USERS ONLY. USE ONLY WITH CAUTION.

Running Aserver in exclusive mode is a way to restrict the network traffic that it responds to. In this way, it can selectively 'pick' only certain WCC devices that it wants to work with. It can also be used to split WCC systems, with some using one server for the NMS route, others using a different server for NMS.

Setting up a server to use exclusive mode is done by entering the following line in SAFETRAN.INI:

```
[Aserver]
ExclusiveMode=true
```

Once Aserver is started in exclusive mode (this mode is announced on the Title bar), it will ignore all UDP traffic from any source IP addresses that are not in its include list.

To manage exclusive IP addresses, click View from the main menu (Figure 4-21).

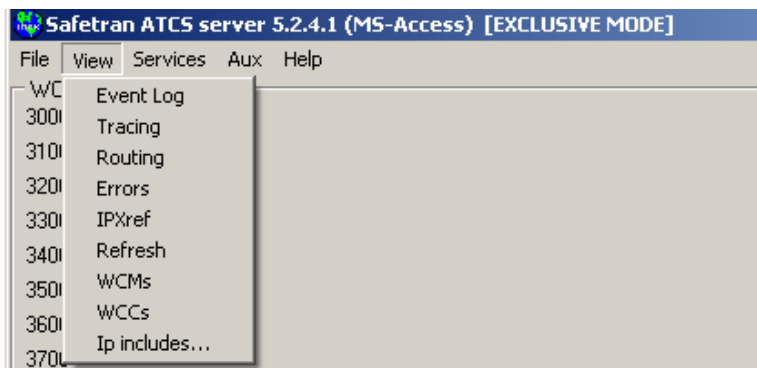


Figure 4-21. View Submenu Showing “IP Includes” Menu Option

Note that the **IP Includes** menu item is only visible when Aserver is running in exclusive mode.

OPERATION

Click “IP Includes...” to open the include list:

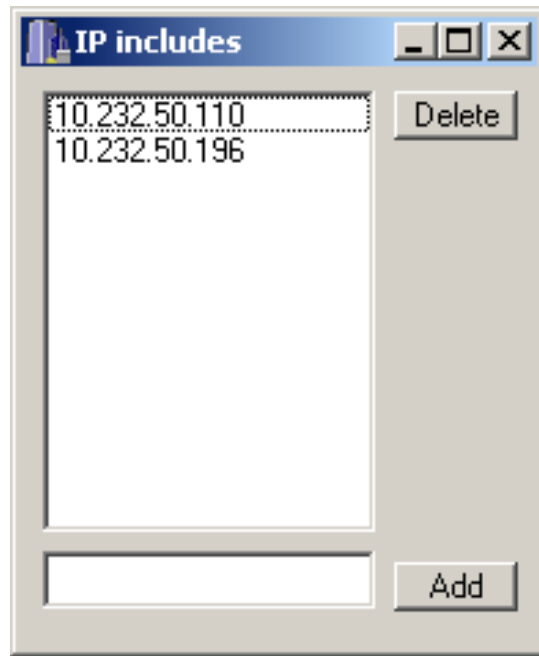


Figure 4-22. The IP Includes List Window

Add or delete exclusive IP addresses as needed.

If exclusive mode is used to start a new server instance and ‘steal’ one or more WCCs from an existing server, it may be necessary to put the original server in Slow Broadcast mode. This allows the test server to refresh the NMS route on the target WCCs more frequently than the original server, and allows the test server to retain these devices.

4.4.2 Co-Resident OCG Mode

Because OCG and Aserver use the same UDP port (typically 5361) to communicate with each other and with the rest of the ATCS network, it is ordinarily not possible to run both of these applications on the same machine, because Windows can only bind one interface to any given UDP port. This is the same reason that two instances of Aserver cannot run on one machine.

In some cases it may be necessary to run both applications together, and for this reason Aserver co-resident OCG mode was developed.

A special TCP port was created for this purpose, and if both applications are properly configured, they will use the TCP port to communicate between each other, and communications from OCG to the UDP network are proxied by Aserver. This means that UDP traffic intended for OCG is intercepted by Aserver, prepended with a special header, and passed on to the co-resident OCG.

Configure Aserver for this mode by editing SAFETRAN.INI:

```
[Aserver]
OcgProxy=true
```

OCG must be prepared to run in this mode by editing OCG.INI:

```
[ProgramOptions]
AserverProxy=true
```

Restart both applications. Aserver will display proxy mode status in the Title bar:

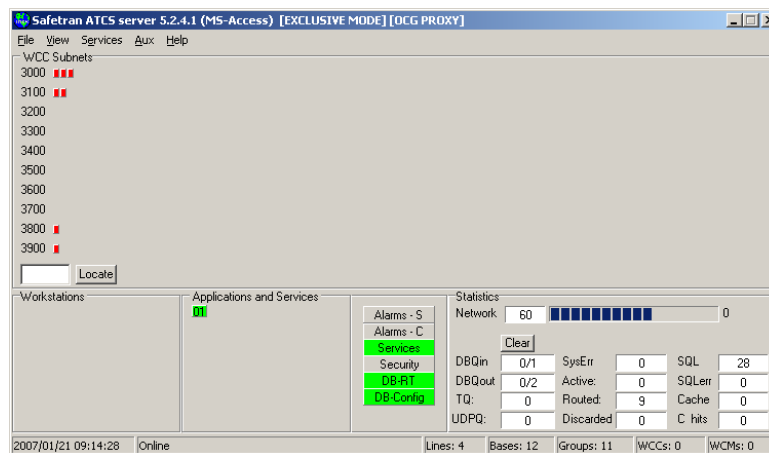


Figure 4-23. ASERVER Showing Proxy Mode Status In The Title Bar

This page intentionally left blank.

SECTION 5

SECURITY

5.0 SECURITY

5.1 INTRODUCTION

All Aserver installations now provide optional system security. Previous network management systems allowed anonymous access to the network to anyone with the appropriate client software and network connectivity. Aserver system security has been developed in order to:

- Keep unauthorized users off the network management system
- Set up permission classes for all critical WccMaint functions
- Establish classes of users with different permissions
- Maintain a log of user logins and logoffs
- Track critical (possibly service-affecting) keystrokes from WccMaint users
- Protect the aserver console from unauthorized access or inadvertent shutdown
- Provide a centralized means of sending administrative messages to WccMaint users
- Enable the Aserver administrator to force the logout of any unauthorized user

When secure mode is enabled, all WccMaint users are prompted to log into the system when WccMaint connects to the server. If the username and password is accepted, the WccMaint overview is displayed as usual. Depending on the security level of the user, certain functions will be unavailable. For instance, if the user does not have permission to reset a WCC, the popup menu for a WCC will have the 'Reset' menu item disabled. Additionally, any button on any form that results in a WCC reset will be disabled. Under security, the Aserver administrator has complete control over the capabilities of WccMaint clients.

Aserver security is a proprietary user security system that is not related to Windows security. Maintenance of user data is somewhat more straightforward than administering many levels of Windows user groups.

Permissions under security are grouped into 8 levels. Each level is represented by a bit in a security word that is linked to each user. Permissions bits are designated using the first letter of its description (V for View, etc) and are therefore referred to as V,R,C,E,D,S,O,and A bits. The permissions bits are:

- View – User is allowed full access to all displays, but any controls that would change anything on the network are disabled. For example, a user with View permissions can download and edit a configuration from a WCC, but the configuration can not be saved or uploaded back to the WCC.
- Reset – User is allowed to reset a WCC. Note that, because opening a terminal window allows the user to type ‘RESET’ commands to the WCC, terminal windows are also restricted for users without Reset permission.
- Configure – User is allowed to change (upload) WCC configurations.
- Executive software – User is allowed to load A,B,C,D and IP executive software.
- Database access – User is allowed to change database records. This permission is required if the user is to assign names/states to new bases and groups.
- Standby switching – Allows user to toggle ‘Online / Offline’ WCC status
- Operate Aserver – User has permission to operate the Aserver console. This includes opening the trace window, configuring Aserver, and shutting the program down.
- Administer Aserver – User has permission to open and run the User Manager.

All security functions are encapsulated in ASRVSEC.DLL. The latest release of the security module is 4.1.0.101. This file should be located in the Windows system folder, which is the default location used by the Aserver setup program.

5.2 INITIAL SETUP

Once Aserver has been installed and initially configured, security may be turned on. This involves turning secure mode on, restarting Aserver, and establishing user accounts with the User Manager. Follow the procedure below to set up security:

5.2.1 Enable Secure Mode

From the Aserver console, click File, then Configure on the Menu bar to open the configuration form. Select the ‘Security’ tab as shown in Figure 5-1.

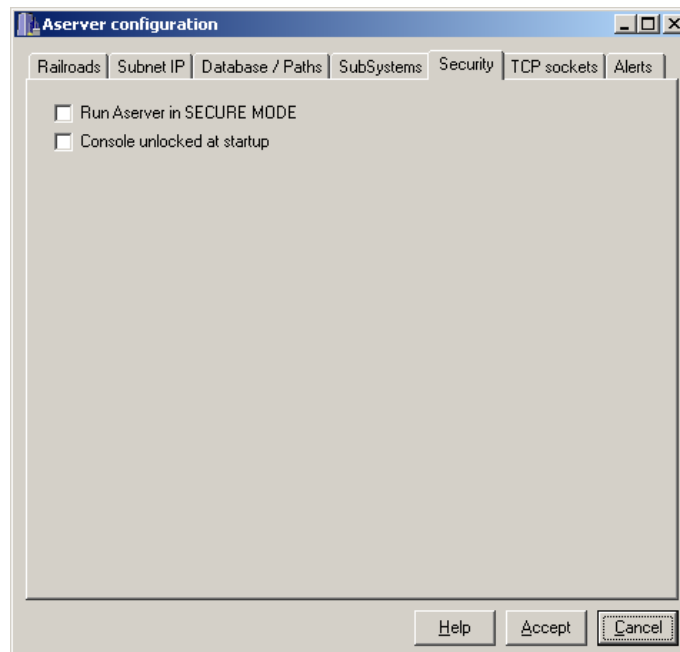


Figure 5-1. ASERVER Configuration Window – Security Tab

Check both the ‘Run Aserver in SECURE MODE’ and ‘Console unlocked at startup’ check boxes, then click ‘Accept’ . Before the form closes, a popup will appear stating that changes will not be effective until Aserver is restarted. Click OK to close both forms.

5.2.2 Shut Down And Restart

Select File, then Exit from the Menu bar to shut down Aserver. Double-click the Aserver icon on the desktop to restart; when Aserver is finished initializing, there will now be a ‘Security’ menu option on the menu bar as shown in Figure 5-2.

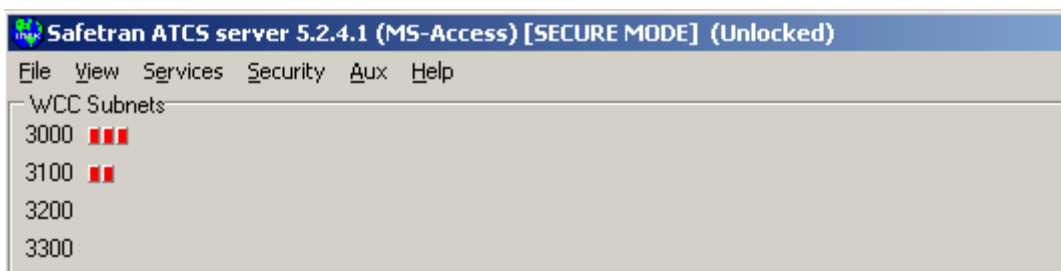


Figure 5-2. ASERVER After Restart – Showing New Security Menu Option

5.2.3 Start User Manager

Click 'Security' on the menu bar to drop down the security submenu:

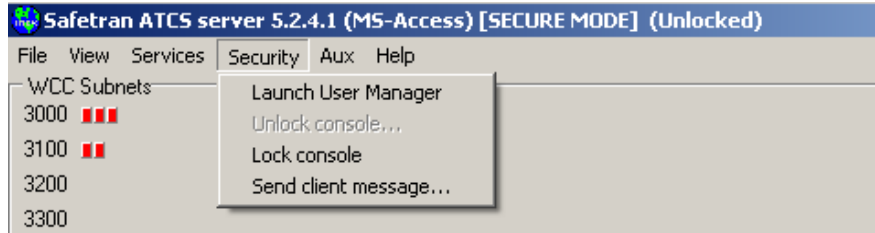


Figure 5-3. The Security Submenu

Click 'Launch User Manager'. The User Manager login will appear:

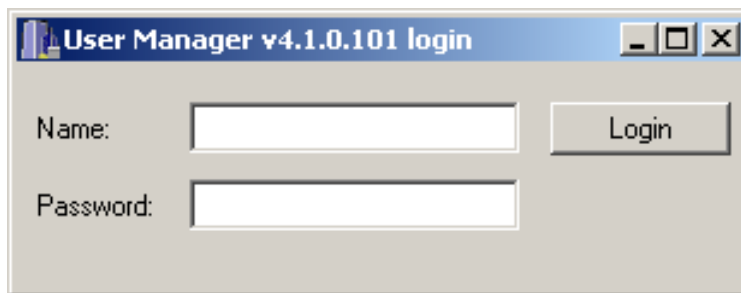


Figure 5-4. The User Manager Login Window

Enter 'Admin' in the Name edit box and 'password' in the Password edit box, then click 'Login' to launch the User Manager.

5.3 THE USER MANAGER

There are 2 default accounts created by the Security DLL (ASRVSEC.DLL) when it is first run:

- 'Admin', password = 'password', with full permissions
- 'Guest', no password required, with View permission only

The first time User Manager is run, it is HIGHLY recommended that the administrator change the Admin password and create a personal account with full permissions. The default accounts cannot be deleted, and the 'Guest' account password cannot be changed (any password is accepted for this account).

If it happens that the Admin password is changed and the password is then forgotten, there is no way to run the User Manager. The only way to recover security is to delete certain Windows registry keys, after which the security module will re-create the registry with the default accounts – but ALL user data will have been lost. Contact Safetran Technical Support about editing the registry should this occur.

The User Manager form is displayed as shown in Figure 5-5.

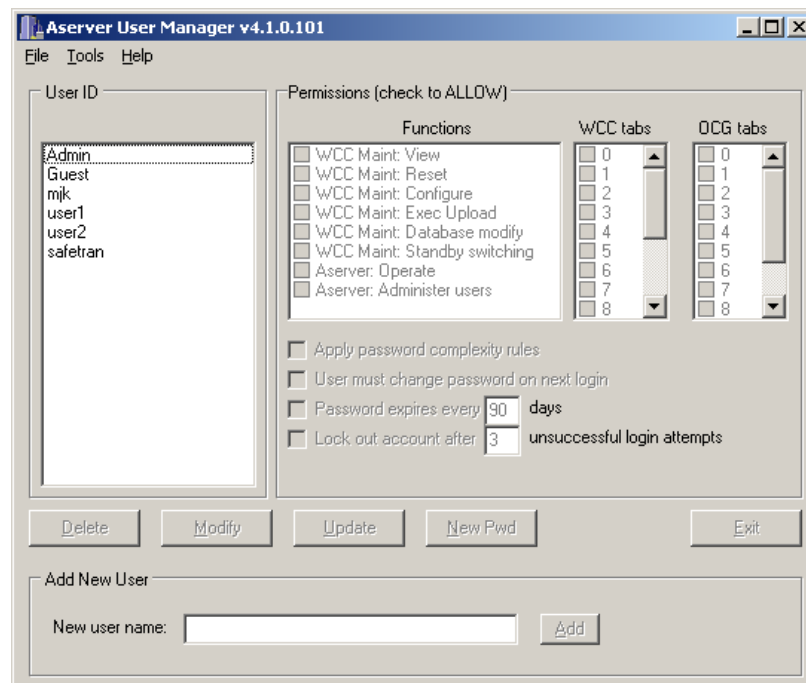


Figure 5-5. The User Manager Window

Referring to Figure 5-5, the User Manager interface has the following features:

User ID List:

This is the list of all users on the system. The illustration shows several accounts that were created in addition to the default users.

Permissions List:

There are three checkbox lists in this panel.

Functions are the permission bits referred to above.

WCC Tabs refers to the 16 WCC SubSystem tabs on the WccMaint overview (Figure 5-6).

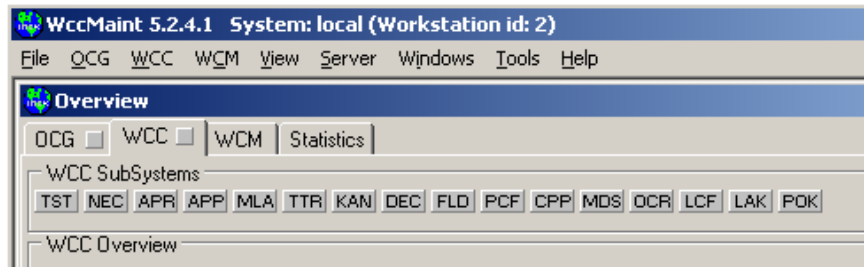


Figure 5-6. WccMaint Overview Window Showing WCC Tabs

OCG Tabs refers to the 12 OCG cluster tabs on the WccMaint overview (Figure 5-7).

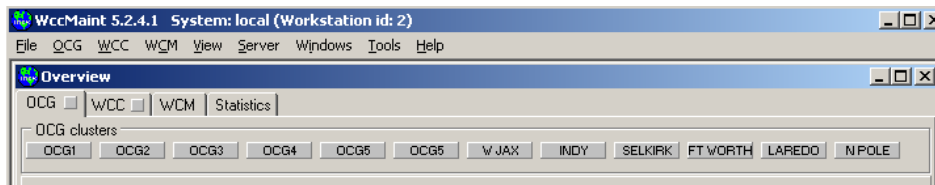


Figure 5-7. WccMaint Overview Window Showing OCG Cluster Tabs

Function Buttons:

As a user is selected in the user ID list, the appropriate function buttons for this user will be enabled. For instance, if 'Admin' is selected, the 'Delete' button remains disabled.

Add New User Box:

New users are created here; the process is described below.

5.3.1 Security Permission Bit Descriptions

Individual permissions bits are described below. More detail is provided in the WccMaint Operations Manual.

View:

This is the default permission granted to every user, and is the only permission granted the Guest user. All displays are available for viewing, but no changes can be made anywhere on the system

Reset:

Allows the user to reset a packet switch from its context menu. Because a WCC terminal allows typing of commands including RESET, this permission is also required to open a WCC terminal session.

Configure:

Allows the user to upload modified configuration data to a WCC or OCG. Downloading and editing are permitted, but saving modified configurations is denied.

This bit is also used to allow the user to modify RF coverage assignments for groups, and to lock or unlock RF coverage.

Exec Upload:

Allows the user to upload executive software to a WCC. This does not apply to OCG.

Database Modify:

Allows the user to assign names to bases and groups, and to enter records for office equipment (WCC and OCG panels) and office applications (codeline regions). Also allows the use of the DB Maintenance tool.

Standby Switching:

Allows the user to change the online/offline state of WCCs, OCGs, and LCTs or HUBs running on OCGs.

WCC/OCG Tabs:

Each checked tab represents a corresponding cluster tab on WccMaint where this user's permissions apply. Put another way, any tab NOT checked here forces the user to have Guest-only privileges on that tab. This is a way to segment territories, and give users full rights on his own tab(s) but not allow changes on others.

5.3.2 Password Options

There are four checkboxes in the Permissions area that pertain to password options.

Complexity Requirement:

If this box is checked, simple passwords (e.g., 'cat') are not allowed. Passwords conforming to this rule must be at least 6 characters long and have at least one alpha and at least one numeric character.

Change On Next Login:

Requires the user to change his/her password the next time a session is logged in. This option is set for all newly created users, which default to a password of **'password'**.

Password Expiration:

Passwords may be set to expire any interval from 1-90 days. When the password interval has expired, the user is prompted for a new password.

Lock Out:

This options locks out the account if the user attempts a login with an invalid password (see Figure 5-8). Thresholds are from 1-6 consecutive failed logins. Terminating and restarting WccMaint does not reset this counter. When an account is locked out, the User Manager must be used to restore it:

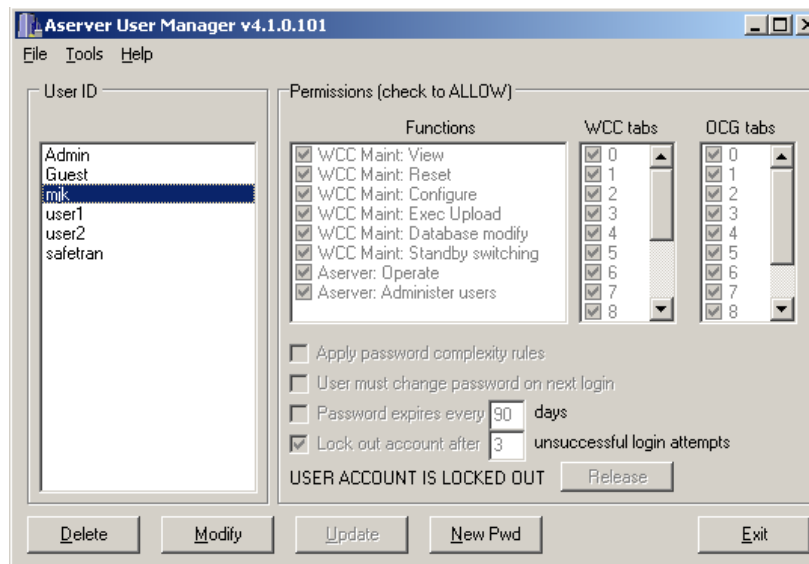


Figure 5-8. User Manager Window Showing User Account Locked Out

To reactivate the account, select the user, click **Modify**, then **Release**. Account reactivation is immediate.

The User Manager was designed to be very intuitive. As users are selected in the user list box, the associated permissions are displayed in the Permissions panel (the checkboxes are read-only unless the user is being updated). Common tasks are described below.

5.3.3 Creating A New User

1. Type the new username in the 'New user name' edit box.
2. Click 'Add'. The new user name is created and placed in the user list. When a new user is created, it is given '**password**' as a password. It is intended that a WccMaint user change his or her own password (this is done from WccMaint). User passwords are private; the User Manager cannot display them. If a user forgets the password, it may be changed (see below) , then the user can change it again.

5.3.4 Assigning Permissions To A User

1. Select the user from the user list..
2. Click 'Modify'. The Functions and SubSystems list boxes will become enabled.
3. Check the desired permissions for this user (Functions).
4. Check the SubSystems checkbox corresponding to WccMaint SubSystem tabs that the user will have any permissions applied to. SubSystems that are not checked will mask off the user's permissions for that SubSystem only. For example, if a user is given all permission bits but only SubSystem 1 is checked, then the user only has full permissions on WCCs that are on the first SubSystem tab. On all other tabs, the user is considered a Guest.
5. When all permissions are assigned, click 'Update'.

5.3.5 Changing User Password

1. Select the user from the user list.
2. Click 'New Pwd' to display the extended form:

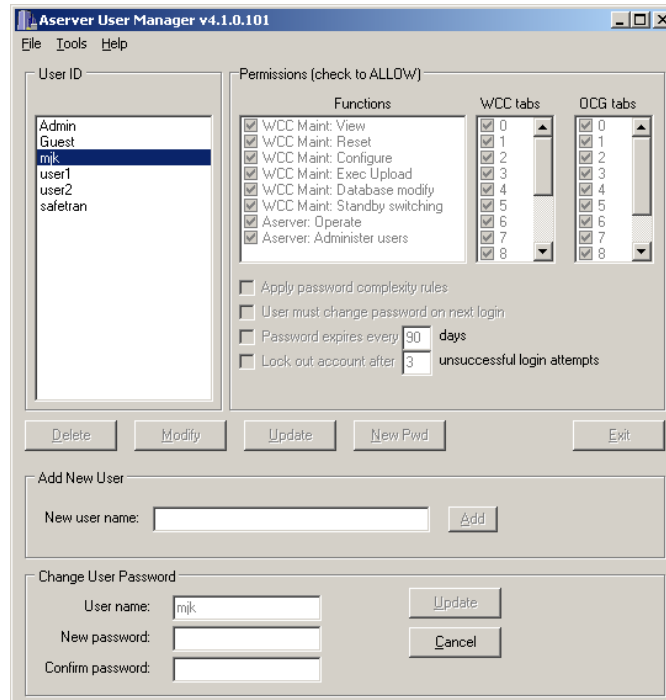


Figure 5-9. Changing User Password

3. Enter the new password in both 'New' and 'Confirm' edit boxes.
4. Click 'Update'.

5.3.6 Saving Changes

All settings are updated immediately as edits are made. Click **Exit** to close the User Manager.

5.4 ADDITIONAL SECURITY FEATURES

5.4.1 Node Display

In the Workstation Nodes display, the popup functions are slightly different under security. When a WccMaint client node is hovered, the hint text displays only the logged-in username. When this node is right-clicked, a menu pops up:

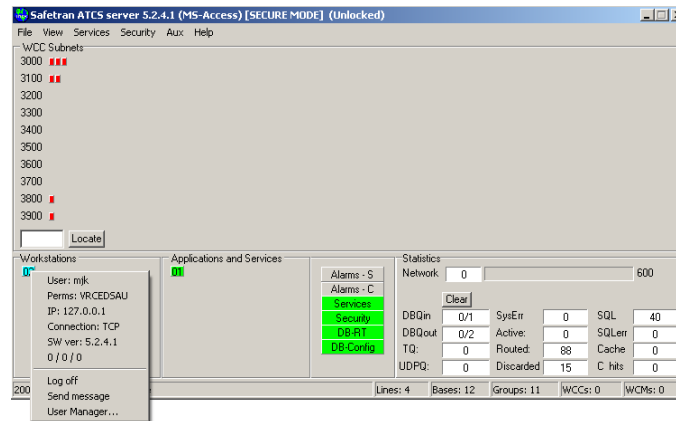


Figure 5-10. Workstation Node Security Popup Menu

This menu displays information about the user, including name, permissions (these are noted as abbreviations – see paragraph 5.1), the user IP address, type of connection, and the software version of WccMaint the user is running. The number graphic (0/0/0) is a diagnostic summary of TCP packet counters for this client. The numbers are:

of TCP packets stored / # of TCP packets retrieved / # of messages queued

Queueing and storage of TCP packets is a rare event indicating either very busy networks or a WccMaint client running over a slow connection or VPN link. These numbers should always be 0/0/0.

The lower half of the menu displays command functions. Clicking ‘Log off’ will force the user off the system. The WccMaint screen will display a popup message telling the user he has been logged off the system. Click ‘Send Message’ to send an Administrative message to the user. This message form will appear:

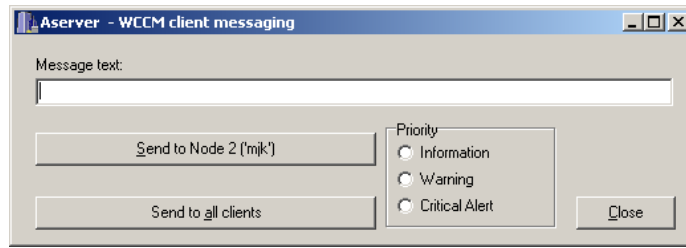


Figure 5-11. Send Message Dialog Box

A message typed into the 'Message text' edit box will be sent to the focused node, or to all WccMaint clients depending on which transmit button is clicked. Priority levels are reserved for future use – at this time all messages are sent as **critical alerts**.

The User Manager may also be launched from this popup menu.

5.5 MENU FUNCTIONS

When the 'Security' menu item is clicked, the security submenu appears:

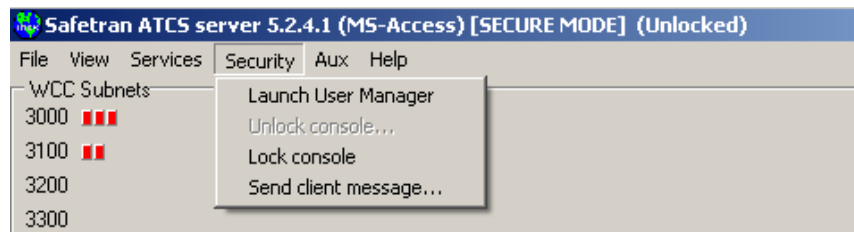


Figure 5-12. Security Submenu

5.5.1 Launch User Manager

See paragraph 5.3 for User Manager functions.

5.5.2 Lock/Unlock Console

For full security, the Aserver console should be locked when unattended. Locking disables any critical controls or menu items, and prevents shutdown of Aserver. To lock the console, simply click 'Lock console'. The Title bar will reflect the locking status of the console. Aserver Operator or Administrator permission is required to unlock the console, so that when 'Unlock console' is clicked, a verification screen is displayed as shown in Figure 5-13.

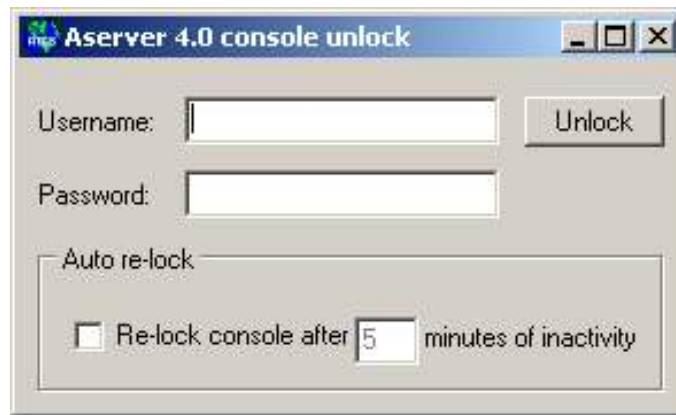


Figure 5-13. Console Unlock Verification Screen

Enter username and password in the appropriate edit boxes and click 'Unlock' to complete the console unlock procedure.

If the 'Re-lock console' checkbox is checked before 'Unlock' is clicked, the console will automatically revert to a locked condition after the time period displayed. In this way, if the operator is called away, the unattended console will protect itself.

5.5.3 Send Client Message

This function opens the client message form for broadcast to all clients:

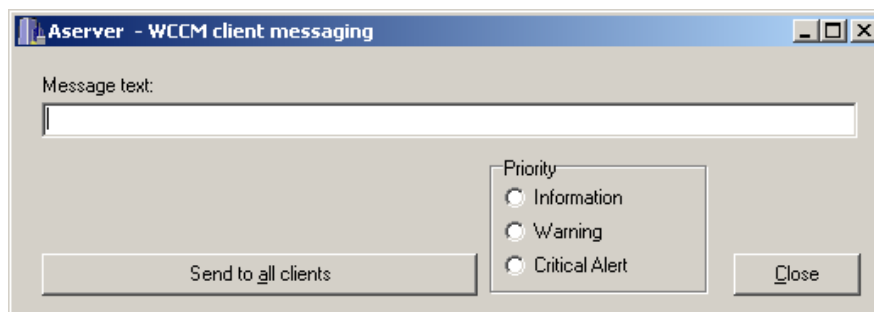


Figure 5-14. WCCM Client Messaging Dialog Box

Enter message text and click **Send to all clients** to broadcast the message.

This page intentionally left blank.

APPENDIX A

ADVANCED TRAIN CONTROL SYSTEM

A.0 OVERVIEW

The Advanced Train Control System (ATCS) standardizes the message formats and addressing scheme used by all railroads for train control applications. The system operates by sending and receiving standard datagrams (using a standard addressing scheme) between the various ATCS compatible signaling and operating equipment. Addresses are provided for wayside equipment, central office equipment, on-board equipment, base stations, maintenance equipment, railcars, and anything else found in a railroad environment. These messages convey operating instructions and status information such as track-and-time permits, codeline controls and indications, hot-box data, etc.

A typical ATCS network is shown in Figure A-1. Centralized Train Control (CTC) office equipment communicates with the onboard and wayside equipment via Base Communication Packages (BCPs), controlled by Cluster Controllers (CCs). Network Management System (NMS) office equipment monitors the dynamic performance of the network. Field radios are a mixture of Wayside Communication Packages (WCPs) and Spread-Spectrum Radios (SSRs). All communications use ATCS datagrams or packets.

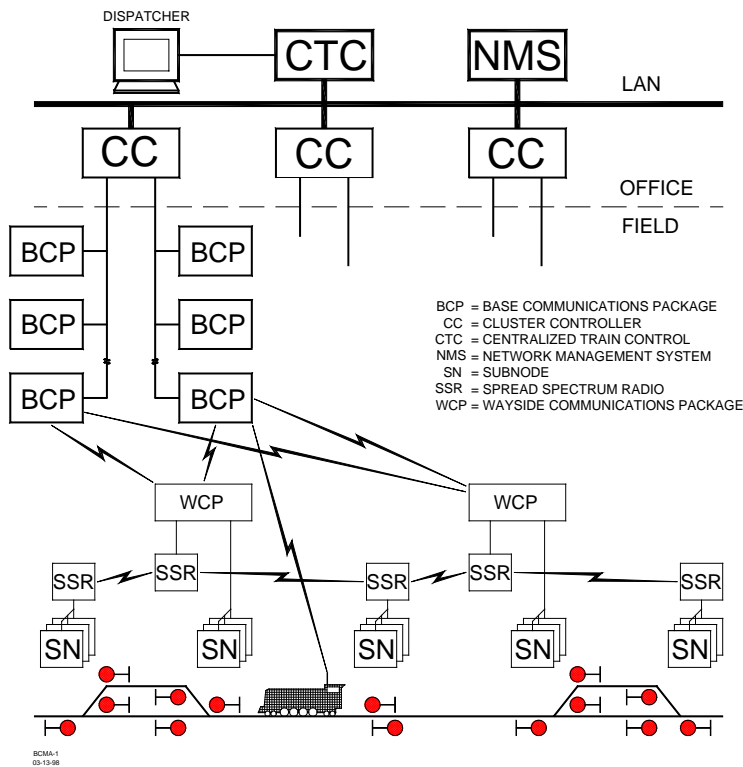


Figure A-1. Typical ATCS Network

A.1 ATCS ADDRESSING

Each ATCS datagram carries with it a destination address (i.e., the address of the equipment it is destined for), and a source address (i.e., the equipment that generated it). These addresses are constructed with slight differences for the various uses. For example, on-board equipment will have a Type 1 (locomotive) address while wayside equipment will have a Type 7 (wayside) address.

A number of the various types of addresses used are described in the following paragraphs. For further information concerning ATCS addressing, refer to the following specifications:

ATCS Specification 200 (March 1993) - ATCS Protocols

ATCS Specification 250 (March 1993) - ATCS Message Formats

ATCS Specification 700 (March 1993) - CPC Specification

ATCS Specification 157 (March 1993) - CPC Operation

R/Link ATCS Radio Code Line System Application Logic Generation Guide (Safetran Document No. C-00-94-06)

A.1.1 Locomotive Addresses (Type 1)

Each locomotive address consists of twelve digits in the following format: **1.RRR.VVVVVV.DD**

where:

- 1 = Locomotive address type
- RRR = Railroad number (see Appendix D)
- VVVVVV = Locomotive number
- DD = Device on board locomotive (e.g., Engineers display)

A.1.2 Office Equipment Addresses (Type 2)

Each office equipment address consists of ten digits in the following format: **2.RRR.NN.DDDD**

where:

- 2 = Office equipment address type
- RRR = Railroad number (see Appendix D)
- NN = Unit in the office (e.g., CTC computer, A53401 Packet Switch, etc.)
- DDDD = Application in the office (e.g., maintenance alarm monitoring)

A.1.3 Base Station Address (Type 3)

Each address consists of ten digits in the following format: **3.RRR.NN.DDDD**

where:

- 3 = Wire line address type
- RRR = Railroad number (see Appendix D)
- NN = Node number (railroad defined)
- DDDD = Base device number (railroad defined)

The ATCS specification recommends that the BCP node number be the same as the node number of the CC (A47620) to which it is connected. The device number is user defined, and can be set to any convenient value.

A.1.4 Wayside Equipment (Type 5)

The type 5 wayside address was used on earlier ATCS systems and is the default addressing scheme for Advanced Railroad Electronic System (ARES) wayside equipment. Although the ARES network differs slightly from the ATCS specification, for purposes of this discussion, the two can be considered identical systems.

Each address consists of ten digits in the following format: **5.RRR.NN.LL.GG**

where:

- 5 = Wayside address type
- RRR = Railroad number (see Appendix D)
- NN = Node or routing region number
- LL = Code-line number
- GG = Group or location number

This addressing scheme does not have the ability to address multiple devices at each location. The node number typically follows the node number of the CC controlling the base stations for the location.

A.1.5 Wayside Equipment (Type 7)

This is the default ATCS wayside addressing scheme.

Each address consists of fourteen digits in the following format: **7.RRR.LLL.GGG.SS.DD**

where:

7	=	Wayside address type
RRR	=	Railroad number (see Appendix D)
LLL	=	Code-line or region number
GGG	=	Group or location number
SS	=	Equipment or subnode at location
DD	=	Device controlled by this equipment

The LLL fields are normally assigned by each railroad according to internal conventions, and may represent a region, district, code line, or other area designation that shows it is part of the railroad.

The GGG field must be coordinated between the CTC equipment and field equipment configuration.

For the SS field, two subnode numbers are always pre-assigned at each location. The wayside-to-office communications device is defined as number 01, and number 02 is reserved for the wayside-to-wayside communications system. Any additional equipment (e.g., the R/Link™ I/O modules), will therefore have subnode numbers starting with 03.

Device numbers (DD field) are allocated in sequence beginning at 01. Each piece of field equipment has at least one internal device, but it may have more depending on the equipment.

Examples of full ATCS addresses for a wayside code system would be as follows:

For CP Rail, code line 8, control point 1: 7.105.008.001.03.02.

For the MCP radio at the same location : 7.105.008.001.01.01.

A.1.6 Other Address Types

Other address types are defined in ATCS for future applications. Please refer to the appropriate ATCS specifications for full details.

A.2 ATCS MESSAGE FORMATS

The major fields in an ATCS message are shown in Figure A-2.



Figure A-2. Major Fields Of An ATCS Message

The **Destination** field is the address of the recipient equipment. For example, if this is an indication message coming from a wayside code unit, the destination address will be the CTC dispatching equipment (2.RRR.NN.DDDD).

The **Source** field is the sender's address (e.g., 7.RRR.LLL.GGG.SS.DD).

The number in the message number (**M#**) field is allocated by the sender in a sequential fashion so that the recipient can detect duplicate, missing, or out of order messages.

The **Label** field describes the type of data carried by the message. Many different labels have been defined in ATCS Specification 250. Additional labels are defined by suppliers to perform custom functions.

The **Data** field carries the particular data required for the type of message defined by the **Label** field.

A.3 ATCS RADIO NETWORK – LAYER 1

The ATCS radio network consists of pairs of UHF channels. These channels are as follows:

<u>Channel Number</u>	<u>Base to Mobile Frequency</u>	<u>Mobile to Base Frequency</u>
1	935.8875	896.8875
2	935.9375	896.9375
3	935.9875	896.9875
4	936.8875	897.8875
5	936.9375	897.9375
6	936.9875	897.9875

NOTE

Transmission on the channels is baseline FSK. the deviation of the carrier to a higher frequency is interpreted as a logical 0 and to a lower frequency as a logical 1. The bit rate is 4800 bits per second. Nominal channel separation is 12.5kHz.

This page intentionally left blank.

APPENDIX B

ATCS SPECIFICATION 250 RAILROAD CODE LIST

B.0 RAILROAD CODE LISTING

The following chart lists the codes assigned to all carriers in accordance with ATCS Specification No. 250 and includes the railway carrier name along with the alphabetical and numerical codes assigned to each. In the event a discrepancy exists between the information in the following list and the current AAR specification, the AAR specification shall prevail.

APPENDIX B - ATCS SPECIFICATION 250 RAILROAD CODE LIST

ID	Company Name	RR Mark	ATCS
001	Aberdeen And Rockfish Railroad Company	AR	009
002	Akron & Barberton Belt Railroad Company	ABB	002
003	Alabama & Florida Railway Co	AF(LR)	917
004	Alameda Belt Line	ABL	014
005	Alameda Corridor Transportation Authority	ACTA	015
006	Alaska Hydro-Train	AHT	039
007	Alaska Railroad Corporation	ARR	005
008	Alexander Railroad Company	ARC	049
009	Algiers Winslow And Western Railway Company	AWW	004
010	Algoma Central Railroad Inc	AC	008
011	Allegheny & Eastern Railroad Inc	ALY	532
012	Alley Railroad Company		664
013	Almanor Railroad Company	AL	046
014	Alton & Southern Railway Company	ALS	032
015	Amador Central Railraod Company	AMC	019
016	Andalusia & Concecuh Railroad Company	ACRC	173
017	Angelina & Neches River Railroad Company	ANR	035
018	Anthracite Railway Inc	ATRW	176
019	Apache Railway Company	APA	011
020	Apalachicola Northern Railroad Company	AN	012
021	Appanoose County Community Railroad Inc	APNC	226
022	Arcade And Attica Railroad Corporation	ARA	013
023	Arkansas And Missouri Railroad Co	AM	906
024	Arkansas Louisiana & Mississippi (Missouri) Railro	ALM	016
025	ARTC		047
026	Ashley, Drew & Northern Railway Company	AND	020
027	Ashtabula Carson & Jefferson Railroad	ACJR	235
028	Atchison, Topeka And Santa Fe Railway Company Ats	ATSF	022
029	Atcs Shared Network	ATCS	340
030	Atcs Testing & Field Evaluation	ATCR	050
031	Atcs Testing & Field Evaluation	ATCT	620
032	Atlantic & Western Railway, L P	ATW	025
033	Austin Railroad	AUNW	924
034	Austin, Todd And Ladd Railroad Company	ATLT	514
035	Baltimore And Annapolis Railroad Company	BLA	053
036	Bangor & Aroostook Railroad Company	BAR	056
037	Bath And Hammospport Railroad Company	BH	079
038	Batten Kill Railroad Inc	BKRR	086
039	Bauxite & Northern Railway Company	BXN	084
040	Bay Colony Railroad Corporation	BCLR	082
041	Bayside Railway Co		021
042	BC HYDRO RAIL	BCE	072
043	BC RAIL LTD	BCOL	997
044	Beaufort And Morehead Railroad Company	BMH	068
045	Beech Mountain Railroad Company	BEEM	060
046	Belfast And Moosehead Lake Railroad Company	BML	087
047	Belt Railway Company Of Chicago	BRC	083
048	Belton Railroad Company	BRR	207
049	Berlin Mills Railway	BMS	073
050	Bessemer And Lake Erie Railroad Company	BLE	061

ID	CompanyName	RR Mark	ATCS
051	Birmingham Southern Rr Co	BS	065
052	Black River & Western Corporation	BRW	066
053	Bloomer Line, The	BLOL	223
054	Blue Mountain And Reading Railroad	BMRG	256
055	Border Pacific Railroad Co	BOP	225
056	Boston And Maine Corporation	BM	069
057	Brandon Corporation	BRAN	081
058	Brandywine Valley Railroad Company	BVRY	067
059	Broken Hill Proprietary Co.		042
060	Brownsville And Rio Grande International Rr	BRG	170
061	Buffalo Southern Railroad Inc	BSOR	085
062	Burlington Junction Railway	BJRY	383
063	Burlington Northern (Manitoba) Ltd	BNML	457
064	Burlington Northern Railroad Company	BN	076
065	Burlington Northern Santa Fe	BNSF	777
066	C&J Railroad Investment Company	CJRR	565
067	Cadillac And Lake City Railway Co	CLK	093
068	Cadiz Railroad Company	CAD	092
069	Cairo Terminal	CTML	162
070	California Western	CWR	100
071	CALTRAIN	CALTRAIN	708
072	Camas Prairie Railnet Inc	CSP	952
073	Cambria And Indiana Railroad Company	CI	101
074	Canada And Gulf Terminal Railway Company, The	CGT	116
075	Canadian National Railways	CN	103
076	Caney Fork And Western Rr	CFWR	187
077	Canton Railroad Company	CTN	097
078	Cape Fear Railways Inc	CF	099
079	Carolina Rail Services Inc	CRIJ	988
080	Carrollton Railroad	CARR	113
081	Carthage Knightstown & Shirley Railroad	CKSI	396
082	Cedar Rapids & Iowa City Railway Company	CIC	111
083	Cedar Valley	CVAR	313
084	Central California Traction Company	CCT	112
085	Central Indiana & Western Railroad Co Inc	CEIW	949
086	Central Michigan Railway Co	CMGN	472
087	Central Montana Rail Inc	CM	374
088	Central New York Railroad Corporation	CNYK	151
089	Central Vermont Railway	CV	120
090	Central Western Railway Corp	CWRL	527
091	Charles City Rail Lines	CCRY	967
092	Chattahoochee Industrial Railroad	CIRR	222
093	Chattahoochee Valley	CHV	124
094	Chelatchie Praire Railraod	CCPR	155
095	Chesapeake And Ohio Railway Company	CO	125
096	Chesapeake Western	CHW	179
097	Chestnut Ridge Railway Company	CHR	117
098	Chicago And Northwestern	CNW	131
099	Chicago And West Pullman	CWP	172
100	Chicago And Western Indiana	CWI	132

APPENDIX B - ATCS SPECIFICATION 250 RAILROAD CODE LIST

ID	CompanyName	RR Mark	ATCS
101	Chicago Central & Pacific Railroad Co	CC	569
102	Chicago Heights Terminal Transfer Railroad Company	CHTT	139
103	Chicago Illinois Midland	CIM	130
104	Chicago Short Line Railway Company	CSL	147
105	Chicago Southshore & South Bend Railroad	CSS	168
106	Cimarron Valley Railroad, L C	CVR	378
107	City Of Columbia	CT	090
108	City Of Prineville Railway	COP	166
109	Claremont Concord Railroad Corporation	CCRR	188
110	Clarendon And Pittsford Railroad Company, The	CLP	169
111	Cliffaide Railroad Company	CLIF	181
112	Colonels Island Railroad Co	CISD	164
113	Colorado & Wyoming Rwy Co	CW	158
114	Colorado Springs & Eastern	CSE	319
115	Columbia & Cowlitz Railway Company	CLC	163
116	Columbia & Silver Creek Railroad Company	CLSL	165
117	Columbus And Greenville Railway	CAGY	177
118	Conemaugh & Black Lick Railroad Company	CBL	215
119	Connecticut Central	CCCL	416
120	Connecticut Department of Transportation	CDOT	007
121	Consolidated Rail Corporation	CR	190
122	Cooperstown And Charlotte Valley Rwy	CACV	114
123	Copper Basin Railway Inc	CBRY	909
124	Corinth And Counce	CCR	201
125	Corman	RJCR	970
126	Cotton Belt (St. Louis Southwestern Rwy Company)	SSW	694
127	CP RAIL SYSTEM	CP	105
128	Crab Orchard & Egyptian Railroad	COER	089
129	CSXT	CSXT	171
130	Curtin Milburn	CMER	180
131	Cuyahoga Valley Railway Company, The	CUVA	186
132	D & I Railroad Company	DAIR	211
133	Dakota Minnesota & Eastern Railroad Corp	DME	912
134	Dakota Rail Inc	DAKR	221
135	Dakota Southern Railway Company	DSRC	526
136	Dansville And Mount Morris Railroad Company, The	DMM	220
137	Dardanelle & Russellville Railroad Company,	DR	191
138	Davenport Rock Island And North Western Railway Co	DRI	192
139	Delaware & Hudson Railway Company Inc	DH	195
140	Delaware Coast Line Rr Co	DCLR	214
141	Delta Valley & Southern Railway Company	DVS	193
142	Denver Union Terminal Ry Co.	DUT	288
143	Dequeen And Eastern Railroad Company,	DQE	200
144	Des Moines Union	DMU	202
145	Detroit And Mackinac	DM	204
146	Dominion And Atlantic	DA	209
147	Doniphan Kensett & Searcy Railway	DKS	210
148	DRGW	DRGW	197
149	Duluth & Northeastern Railroad Company,	DNE	212
150	Duluth Missabe And Iron Range Railway Company	DMIR	213

ID	CompanyName	RR Mark	ATCS
151	Duluth Winnipeg And Pacific Railway Company	DWP	216
152	Dunn-Erwin Railway Corporation	DER	219
153	East Camden & Highland Rr Co	EACH	242
154	East Cooper And Berkeley Railroad Company	ECBR	229
155	East Erie Commercial Railroad	EEC	040
156	East Jersey Railroad And Terminal Company	EJR	245
157	East St. Louis Junction Rr	ESLJ	233
158	East Tennessee Railway, L P	ETRY	257
159	Eastern Shore Railroad Inc	ESHR	251
160	Edgmoor & Manetta	EM	232
161	El Dorado And Wesson Railway Company	EDW	247
162	Elgin Joliet & Eastern Railway Company	EJE	238
163	Escanaba And Lake Superior Railroad Company	ELS	241
164	Esquimalt And Nanaimo	EN	246
165	Essex Terminal Railway Company The	ETL	228
166	Eureka Southern	EUKA	368
167	Everett Railroad	EV	231
168	Falls Creek	FCRK	267
169	Farmrail Corporation	FMRC	280
170	FCA - Ferrovía Centro - Atlantica SA	??	029
171	Ferdinand & Huntingburg	FRDN	273
172	Ferrocarril De Chihuahua Al Pacifico,	CHP	284
173	Ferrocarriles Nacionales De Mexico	NDM	266
174	Ferrocarriles Nacionales De Mexico	SBC	283
175	Ferrocarriles Nacionales De Mexico -	FCP	738
176	Ferrocarriles Unidos Del Sureste, S.A.	SE	281
177	Florida Central Railroad Co	FCEN	986
178	Florida East Coast Railway Company	FEC	263
179	Florida Midland Railroad Co Inc	FMID	507
180	Fonda, Johnstown And Gloversville	FJG	264
181	Fordyce And Princeton Railroad Co	FP	265
182	Fore River	CRY	908
183	Fort Smith And Van Buren	FSVB	279
184	Fort Worth & Western Railroad	FWWR	277
185	Galveston Railroad L P	GVSR	567
186	Galveston Warves	GWF	303
187	Galveston, Houston And Henderson	GHH	293
188	Garden City Western Railway Company, The	GCW	287
189	Genesee And Wyoming Railroad Company	GNWR	320
190	Georgetown Railroad Company	GRR	302
191	Gettysburg Railway	GBRY	294
192	Gloster Southern Railroad Company	GLSR	916
193	GO TRANSIT	GOT	954
194	Goderich - Exeter Railway Company	??	027
195	Golden Triangle Railroad	GTRA	295
196	Grafton And Upton Railroad Company	GU	323
197	Grainbelt Corporation	GNBC	443
198	Grand River	GRNR	322
199	Grand Trunk Western Railroad Incorporated	GTW	308
200	Graysonia, Nashville And Western	GNA	307

APPENDIX B - ATCS SPECIFICATION 250 RAILROAD CODE LIST

ID	CompanyName	RR Mark	ATCS
201	Great River Railroad	GTR	271
202	Great Southwestern	GSWR	305
203	Great Western Railway Company, The	GWR	311
204	Green Bay And Western	GBW	312
205	Green Hills Rural Development	GHRD	980
206	Green Mountain Railroad Corporation	GMRC	314
207	Gulf And Mississippi	GMSR	392
208	Hammersley Iron (Australia)		041
209	Hampton & Branchville Railroad Company	HB	330
210	Hartford And Slocomb Railroad Company	HS	366
211	Hartwell Railway Company	HRT	334
212	Helena Southwestern Railroad Company	HSW	331
213	High Point Thomasville & Denton Railroad Company	HPTD	366
214	Hillsboro And North Eastern Railway	HLNE	338
215	Hillsdale County Railway Company, Inc.	HCRC	326
216	Hillside (Australia)		018
217	Hollis & Eastern R R Co	HE	328
218	Houston Belt & Terminal Railway Company	HBT	342
219	Huntsville & Madison County Railroad Authority	HMCR	391
220	Huron And Eastern Railway Company Inc	HESR	890
221	Hutchinson And Northern Railway Company, The	HN	332
222	Illinois Central Railroad Company	IC	360
223	Indian Creek Railroad Company	ICRK	380
224	Indiana & Ohio Rail Corp.	INOH	344
225	Indiana Hi-Rail Corporation	IHRC	352
226	Indiana Rail Road Corporation	INRD	780
227	Indianapolis Union Railway	IU	363
228	Indonesia (Indonesian State Railways)		093
229	International Bridge And Terminal Company, The	IBT	358
230	Interstate Railroad Company	SOU	381
231	Iowa Interstate Railroad Ltd	IAIS	316
232	Iowa Northern Railroad	IANR	341
233	Iowa Southern Railroad Company	ISR	272
234	Iowa Traction Railroad Company	IATR	994
235	ITS - Highway Advanced Transportation Controller		051
236	ITS - Non-ATCS Railroad		052
237	Jefferson Warrior Railroad Co Inc	JEFW	254
238	Kankakee Beaverville And Southern Railroad Company	KBSR	399
239	Kansas And Missouri Railway	KM	414
240	Kansas City Southern Railway Company	KCS	400
241	Kansas City Terminal Railway Company	KCT	401
242	Kentucky And Tennessee Railway	KT	405
243	Keokuk Junction Railway	KJRY	365
244	Kiamichi Railroad Company Llc	KRR	424
245	Knox & Kane Railroad Company	KKRR	376
246	Kwt Railway Inc	KWT	996
247	Kyle Railroad Company	KYLE	377
248	Lake Erie & Northern	LEN	421
249	Lake Erie, Franklin & Clarion Railroad Company	LEF	423
250	Lake Superior & Ishpeming Railroad Company	LSI	425

ID	CompanyName	RR Mark	ATCS
251	Lake Terminal Railroad Company, The	LT	404
252	Lamoille Valley Railroad Company	LVRC	452
253	Lancaster And Chester Railway Company	LC	426
254	Landisville Railroad Inc (Formerly Amherst Industr	AMHR	071
255	Laurinburg And Southern Railroad Company	LRS	427
256	Levin-Richmond Terminal Corporation	PRT	606
257	Lewis & Clark Railway Co	LINC	355
258	Little Rock & Western Railway, L P	LRWN	485
259	Little Rock Port Railroad	LRPA	435
260	Livonia, Avon & Lakeville Railroad Corporation	LAL	398
261	Logansport & Eel River Short-Line Co Inc	LER	304
262	Long Island Railroad Company	LIRR	436
263	Longview, Portland & Northerm Railway Company	LPN	450
264	Los Angeles Junction Railway Company	LAJ	428
265	Louisana & Arkansas Railway Company	LA	441
266	Louisiana & Delta Railroad Inc	LDRR	972
267	Louisiana And North West Railroad Company, The	LNW	442
268	Louisville And Wadley Railway Company	LW	451
269	Louisville New Albany & Corydon Railroad	LNAL	446
270	Lowville And Beaver River Railroad Company, The	LBR	447
271	Ludington & Northern Railway	LUN	430
272	Madison Railroad (A Div Of City Of Madison Port Au	CMPA	144
273	Magma Arizona Railroad Company	MAA	463
274	Mahoning Valley Railway Company, The	MVRY	504
275	Maine Central Railroad Company	MEC	456
276	Manufacturers Junction Railway Company	MJ	459
277	Manufacturers Railway Company	MRS	460
278	Marinette, Tomahawk & Western Railroad	MTW	520
279	Maryland And Delaware Railroad Company	MDDE	454
280	Maryland And Pennsylvania Railroad Company	MPA	463
281	Maryland Midland Railway Inc	MMID	495
282	Maryland Rail Commuter	MARC	003
283	Massachusetts Bay Transportation Authority	MBTA	006
284	Massachusetts Central Railroad Corporation	MCER	461
285	Massena Terminal Railroad Company, The	MSTR	471
286	Mccloud Railway Company	MCR	466
287	Mckeesport Connecting Railroad Company	MKC	583
288	Meridian & Bigbee Railroad Company	MBRR	462
289	Metra		892
290	Mexican Pacific Railroad Company, Inc.	MDP	285
291	Mg Rail Inc	MGRI	388
292	Michigan-Wisconsin Transportation Company	MWTT	512
293	Mid Atlantic Railroad Co., Inc.	MRR	877
294	Middletown & Hummelstown Railroad Company	MIDH	479
295	Middletown & New Jersey Railway Company Inc	MNRR	475
296	Midland Terminal Co, The	MDLR	385
297	Midlouisiana Rail Corporation	MDR	919
298	Midsouth Corporation	MSRC	905
299	Milwaukee Road	MILW	140
300	Minnesota Commercial Railway Co	MNNR	973

APPENDIX B - ATCS SPECIFICATION 250 RAILROAD CODE LIST

ID	CompanyName	RR Mark	ATCS
301	Minnesota Dakota & Western Railway Company	MDW	610
302	Mississippi & Skuna Valley Railroad Company	MSV	503
303	Mississippi Delta Railroad	MSDR	786
304	Mississippi Export Railroad Company	MSE	506
305	Mississippi Railway Cooperative Inc	MSRW	502
306	Missouri Pacific Railroad Company	MP	494
307	Missouri-Kansas-Texas Railroad Co.	MKT	490
308	Mobile & Gulf Railroad Company	MG	483
309	Modesto And Empire Traction Company	MET	524
310	Monongahela Connecting Rr Co.	MCRR	498
311	Monongahela Railway Company	MGA	497
312	Montana Rail Link Inc	MRL	671
313	Morristown & Erie Railway Inc	ME	511
314	Moscow, Camden & San Augustine Railroad	MCSA	548
315	MRS Logistics of South America	??	028
316	Muncie And Western Railroad Company	MWR	464
317	N D C Railroad Company	NDCR	902
318	N J Transit Rail Operations (Commuter Carrier)	NJTR	574
319	Napa Valley Railroad Co	NVRR	402
320	Nash County Railroad Corp	NCYR	776
321	Nashville And Eastern Railroad Corp	NERR	934
322	National Railroad Passenger Corporation	AMTRAK	891
323	National Railways Of Mexico (Ferrocarriles Naciona	NDM	286
324	New Hampshire Northcoast Corp	NHN	787
325	New Hope & Ivyland Rail Road	NHRR	585
326	New York & Lake Erie Railroad	NYLE	545
327	New York Cross Harbor Railroad Terminal Corp	NYCH	573
328	New York Susquehanna And Western Railway Corp	NYSW	546
329	Nicolet Badger Northern Railroad Inc	NBNR	476
330	Nittany & Bald Eagle Railroad Co	NBER	249
331	Norfolk & Portsmouth Belt Line Railroad Company	NPB	549
332	Norfolk And Western Railway Company	NW	550
333	Norfolk Southern	NS	555
334	North Carolina & Virginia Railroad Co Inc	NCVA	531
335	North Shore Railroad Co	NSHR	248
336	North Stratford Railroad Corporation	NSCR	570
337	Northwestern Oklahoma Railroad Company	NOKL	591
338	Northwestern Pacific Railroad Company	NWP	559
339	Oakland Terminal Railroad Company	OTR	586
340	Octoraro Railway, Inc.	OCTR	587
341	Ogden Union Railway And Depot Company, The	OURD	956
342	Ohi-Rail Corporation	OHIC	579
343	Oil Creek & Titusville Lines	OCTL	948
344	Okanagan Valley Railway Company	OKAN	945
345	Oklahoma Central Railroad Co	OCR	270
346	Oklahoma, Kansas And Texas Railroad	OKKT	593
347	Old Augusta Railroad Company	OAR	578
348	Omaha Lincoln And Beatrice Railway Company	OLB	598
349	Ontario Central Railroad Corporation	ONCT	589
350	Ontario Midland Railroad Corporation	OMID	588

ID	CompanyName	RR Mark	ATCS
351	Ontario Northland Railway (Ontario Northland Trans	ONT	754
352	Oregon & Northwestern Railroad Co.	ONW	596
353	Oregon Pacific & Eastern Railway Company	OPE	597
354	Oregon, California & Eastern Railway	OCE	603
355	Ottertail Valley Railroad Co Inc	OTVR	983
356	Ottumwa Terminal Railroad Co	OTT	276
357	Paducah & Illinois Railroad Company	PI	614
358	Paducah & Louisville Railroad	PAL	907
359	Panther Valley Railroad Corporation	PVAL	575
360	Patapsco & Back Rivers Railroad Company	PBR	609
361	Pearl River Valley Railroad Company	PRV	636
362	Pecos Valley Southern Railway Company, The	PVS	644
363	Pee Dee River Railroad Corp	PDRR	010
364	Peninsula Terminal Company	PT	643
365	Peoria And Pekin Union Railway Company	PPU	645
366	Philadelphia Belt Line Railroad Company, The	PBL	608
367	Philadelphia Bethlehem And New England Railroad Co	PBNE	659
368	Pickens Railway Company	PICK	624
369	Pioneer And Fayette Railroad Company	PF	630
370	Pioneer Valley Railroad Company	PVRR	611
371	Pittsburg & Shawmut Railroad Inc	PSR	627
372	Pittsburgh Chartiers & Youghiogheny Railway Compan	PCY	629
373	Pittsburgh, Allegheny & Mckees Rocks Rr Co	PAM	607
374	Plymouth Short Line Ltd	PSLL	566
375	Pocono Northeast Railway, Inc.	PNER	618
376	Point Comfort & Northern Railway Company	PCN	651
377	Port Bienville Railroad	PBVR	677
378	Port Of Tillamook Bay Railroad	POTB	637
379	Port Royal Railroad	PRYL	393
380	Portland Terminal Company	PTM	619
381	Portland Traction Company	PRTD	632
382	Prescott And Northwestern Railroad Company	PNW	634
383	Providence And Worcester Railroad Company	PW	631
384	Quebec Central Railway Company	QC	658
385	Queensland Rail (Australia)		036
386	Quincy Railroad Company	QRR	656
387	Rac (Railway Association Of Canada)		033
388	Rarus Railway Company	RARW	516
389	Red River Valley & Western Railroad Co	RRVW	321
390	Renfe (National Railways Of Spain)		119
391	River Terminal Railway Company, The	RT	665
392	Robe (Australia)		044
393	Roberval And Saguenay Railway Company, The	RS	669
394	Rochester & Southern Railroad Inc	RSR	941
395	Rockdale Sandow & Southern Railroad Company	RSS	675
396	Rocky Mountain Railcar And Railroad Inc	RMRR	915
397	Roscoe Snyder & Pacific Railway Company	RSP	673
398	Sabine River & Northern Railroad Company	SRN	678
399	Saint Lawrence Railroad	SLAW	705
400	Saint Marys Railroad Company	SM	682

APPENDIX B - ATCS SPECIFICATION 250 RAILROAD CODE LIST

ID	CompanyName	RR Mark	ATCS
401	Salt Lake Garfield And Western Railway Company	SLGW	690
402	San Diego & Imperial Valley Railroad Co Inc	SDIY	315
403	San Luis Central Railroad Company	SLC	696
404	San Manuel Arizona Railroad Company	SMA	794
405	Sand Springs Railway Company	SS	707
406	Sandersville Railroad Company	SAN	691
407	Santa Maria Valley Railroad Company	SMV	741
408	Savannah State Docks Railroad Company	SSDK	679
409	Sequatchie Valley Railroad Inc	SQVR	910
410	Shore Fast Line Railroad Company Sflr 2	SFLR	255
411	Sierra Railroad Company	SERA	716
412	Singapore (Singapore)		076
413	Sisseton Southern Railway Co	SSOR	440
414	Somerset Railroad Corporation	SOM	772
415	SOO Line Rail Company	SOO	030
416	South Branch Valley Rail Road	SBVR	732
417	South Brooklyn Railway Company	SBK	718
418	South Buffalo Railway Company	SB	719
419	South Carolina Central Railroad Co Inc	SCRF	582
420	South Central Tennessee Railroad Corporation	SCTR	672
421	Southeast Kansas Railroad Company	SEKR	944
422	Southeastern Penn Transp Authority	SEPTA	024
423	Southern Indiana Railway Inc	SIND	720
424	Southern New Jersey Light Rail Transit	??	026
425	Southern Pacific Transportation Company	SP	721
426	Southern Railway Company	SOU	724
427	Southern San Luis Valley Railroad Company	SSLV	706
428	St Maries River Railroad Company	STMA	698
429	STA		048
430	Staten Island Railway Corporation	SIRY	389
431	Steelton & Highspire Railroad Company	SH	799
432	Stewartstown Railroad Co	STRT	729
433	Stockton Terminal And Eastern Railroad	STE	739
434	Strasburg Railroad Company	SRC	686
435	Strouds Creek And Muddlety Railroad	SCM	687
436	Sunset Railway Company	SUN	734
437	Tacoma Muncipal Belt Line Railway	TMBL	759
438	Tasrail		119
439	Tennessee Railway Company	SCM	767
440	Tennessee, Alabama And Georgia Railway	SOU	755
441	Tennken Railroad Company Inc	TKEN	745
442	Terminal Railroad Association Of St Louis	TRRA	757
443	Terminal Railway Alabama State Docks	TASD	758
444	Texas & Northern	TN	795
445	Texas Central Railroad Company	TEXC	750
446	Texas City Terminal Railway Company	TCT	761
447	Texas Mexican Railway Company, The	TM	762
448	Texas North Western Railway Company	TXNW	747
449	Texas South-Eastern Railroad Company	TSE	765
450	Texas, Oklahoma & Eastern Railroad Company	TOE	764

ID	CompanyName	RR Mark	ATCS
451	Thailand (Thai State Railways)		102
452	Tippecanoe Railroad Company	TIPP	753
453	Tonawanda Island Railroad Inc	TIRL	743
454	Towanda And Monroeton Shippers Lifeline, Inc.	TMSS	752
455	Transkentucky Transportation Railroad Co Inc	TTIS	773
456	Tranz Rail (Tasmania)		057
457	Trintity Railway Express		751
458	Trona Railway Company	TRC	779
459	TTCI Test Unit 1	TTCI	884
460	TTCI Test Unit 2	TTCI	885
461	TTCI Test Unit 3	TTCI	886
462	TTCI Test Unit 4	TTCI	887
463	TTCI Test Unit 5	TTCI	888
464	TTCI Test Unit 6	TTCI	889
465	Tucson, Cornelia & Gila Bend Railroad Company	TCG	783
466	Tulsa-Sapulpa Union Railway Company L L C	TSU	709
467	Turtle Creek Industrial Railroad Inc	TCKR	744
468	Tuscola And Saginaw Bay Railway Company Inc	TSBY	770
469	Union Pacific Railroad Company	UP	802
470	Union Railroad Company	URR	803
471	Union Railroad Of Oregon	UO	800
472	United South Eastern Railways Company	SE	281
473	Unity Railways Company	UNI	806
474	Upper Merion And Plymouth Railroad Company	UMP	808
475	Utah Railway Company	UTAH	811
476	Valdosta Southern Railroad	VSO	816
477	Vandalla Railroad Company	VRRC	781
478	Ventura County Railway Company	VCY	821
479	Vermont Railway Inc	VTR	817
480	Via Rail Canada Inc	VIA	818
481	Victrack (Australia)		017
482	Virginia Railway Express	VRE	023
483	Visalla Electric Railroad Company	VE	824
484	Walking Horse & Eastern Railroad Co Inc	WHOE	390
485	Warren & Saline River Railroad Company	WSR	832
486	Washington Central Railroad Company, Inc. Wcrc	WCRC	943
487	Washington County Railroad Corporation	WACR	812
488	Washington Terminal	WATC	849
489	Waterloo Railway Company	WLO	835
490	Wctu Railway Company	WCTR	844
491	Weatherford Mineral Wells & Northwestern	WMWN	837
492	West Jersey Short Line, Inc.	WJSL	387
493	West Shore Railroad Corp	WTSE	882
494	West Tennessee Railroad Corp	WTNN	258
495	West Virginia Northern Railroad	WVN	866
496	Western Railroad Company	WRRC	838
497	Westrail (Australia)		038
498	White Pass & Yukon	WPY	845
499	Willamette Valley Railway Company, Inc	WVR	863
500	Wilmington Terminal Railroad Inc	WTRY	981

ID	CompanyName	RR Mark	ATCS
501	Winchester And Western Railroad Company	WW	850
502	Winifrede Railroad Company	WNFR	852
503	Winston-Salem Southbound Railway Company (Csx Tran	WSS	854
504	Wisconsin & Calumet Railroad	WICT	382
505	Wisconsin & Southern Railroad Company	WSOR	879
506	Wisconsin Central Limited	WC	260
507	Yancey Railroad Company	YAN	876
508	Youngstown & Austintown Railroad Co	YARR	372
509	Youngstown & Southern Railway Company	YS	875
510	Yreka Western Railroad Company	YW	873
511	UK ATCS Testing and Field Evaluations	????	974
512	Network Rail - London North Eastern - UK	????	975
513	Network Rail - London North Western - UK	????	976
514	Network Rail - Scotland - UK	????	977
515	Network Rail - South East - UK	????	978
516	Network Rail - Western - UK	????	979

APPENDIX C

DATA SOURCE SETUP FOR SQL SERVER

C.0 SQL DATA SOURCE SETUP

NOTE

As a prerequisite to setting up the SQL Server data source, SQL Server must be installed and the configuration and realtime databases must be created (nms_cfg and nms_rt, respectively). Contact Safetran for assistance in setting up the SQL Server and running the scripts required to create the blank databases. It is assumed that the system SQL administrator will complete the process outlined in this Appendix.

SQL Server data sources are created as follows:

For ODBC:

1. Login as Administrator or user with administrator rights.
2. Open the Control Panel (Start -> Settings -> Control Panel)
3. Open the ODBC Administrator as follows:
 - click 'Administrative Tools'
 - click 'Data Sources (ODBC)'

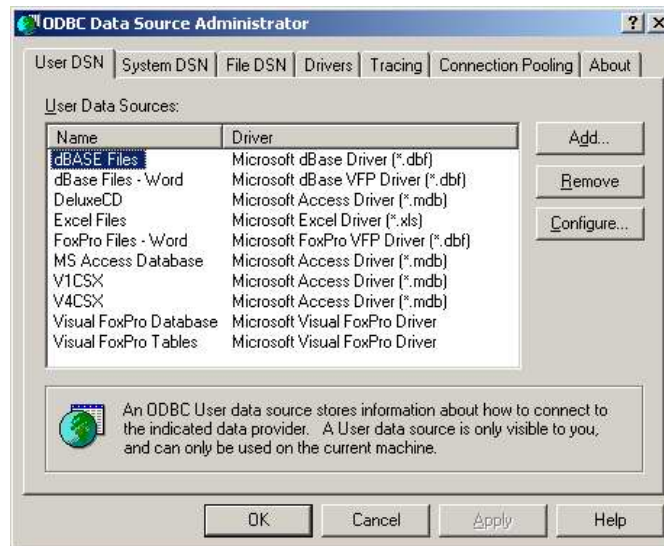


Figure C-1. ODBC Data Source Administrator Window

4. Click on the 'System DSN' tab, then click 'Add...'. The 'Create New Data Source' dialog will appear as shown in Figure C-2.
5. Highlight 'SQL Server' and click 'Finish' :

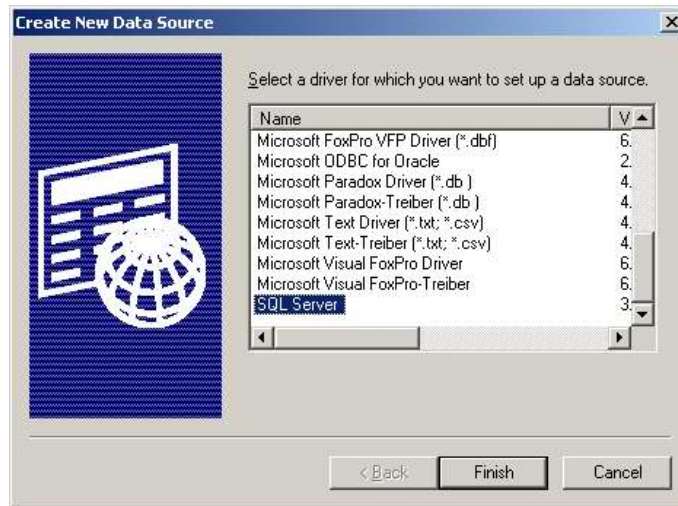


Figure C-2. New Data Source Selection Window

6. The 'Create New Data Source to SQL Server' dialog box opens:

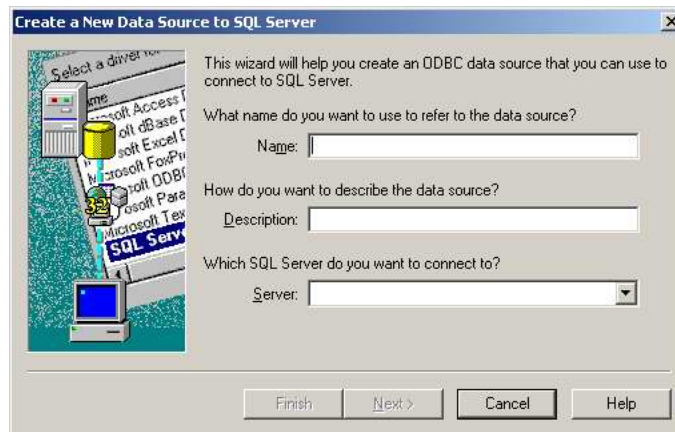


Figure C-3. Create New Data Source To SQL Server Dialog Box

7. In the 'Name' field, type 'NMS_CFG' (for configuration datasource) or 'NMS_RT' (for realtime datasource), then select the server from the dropdown list in the Server field:

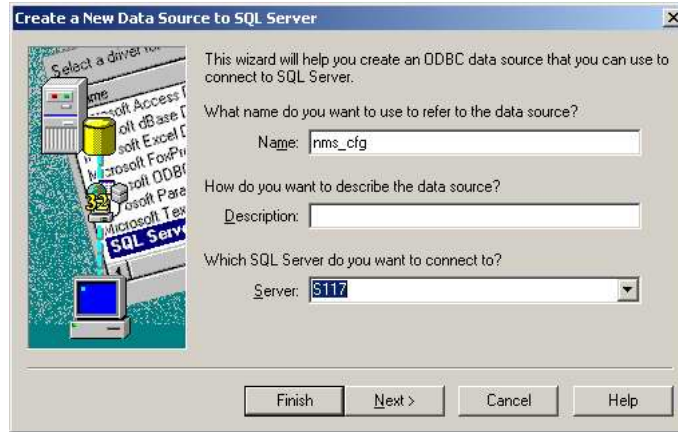


Figure C-4. New Data Source Name And Server

8. Click 'Next' and fill in the fields in the next dialog box as shown below:

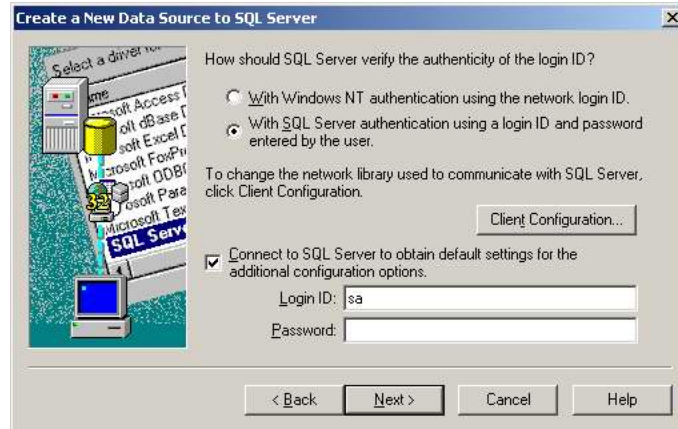


Figure C-5. Login Authenticity Verification Dialog Box

9. Click the 'Client Configuration...' button.

- In the 'Network Libraries' selections, click the 'TCP/IP' radio button as shown below, then click 'OK' to return to the New Data Source form.

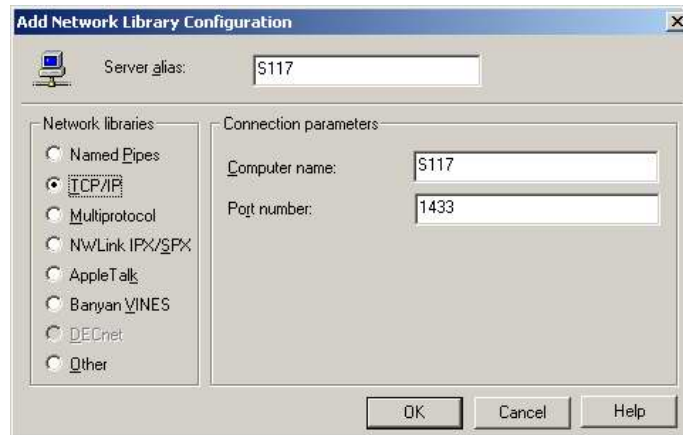


Figure C-6. Network Library Configuration Window

- Check the 'Change the default database to:' checkbox and select 'nms_cfg' for configuration database or 'nms_rt' for realtime database from the drop-down selection menu, then click 'Next'.

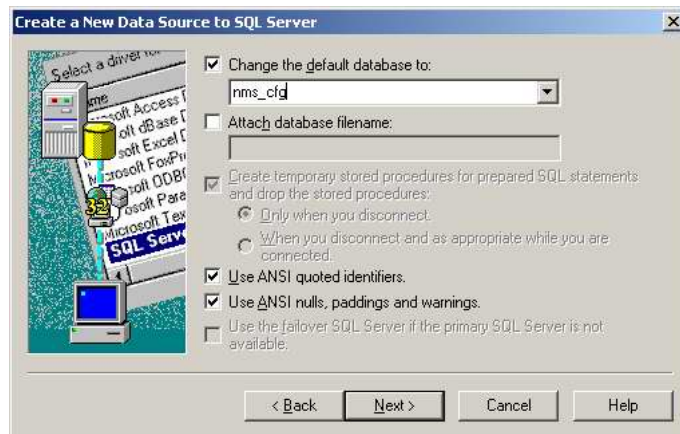


Figure C-7. Default Database Selection Window

12. Click 'Finish':

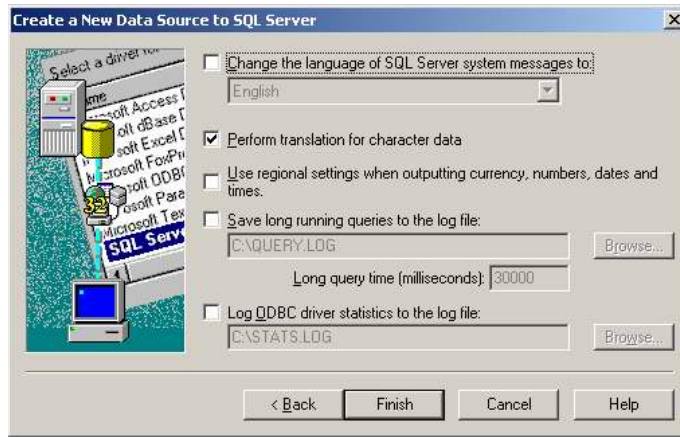


Figure C-8. Finishing the Data Source Setup

13. Click the 'Test Data Source...' button to verify the data source configuration, then click 'OK'. Repeat this procedure for the realtime data source, then click 'OK' on the Administrator form to exit.

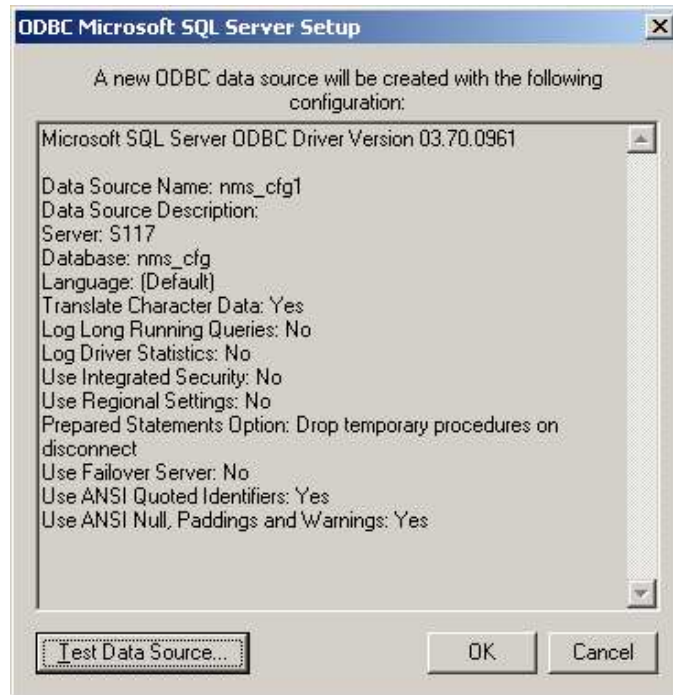


Figure C-9. New Data Source Configuration Verification

For DATALINK file:

1. Using Windows Explorer, locate the blank datalink file `NMS_CFG.UDL` that was shipped with the Aserver 5 installation CD.
2. Double-click on `NMS_CFG.UDL` to open the Datalink file Properties dialog box:

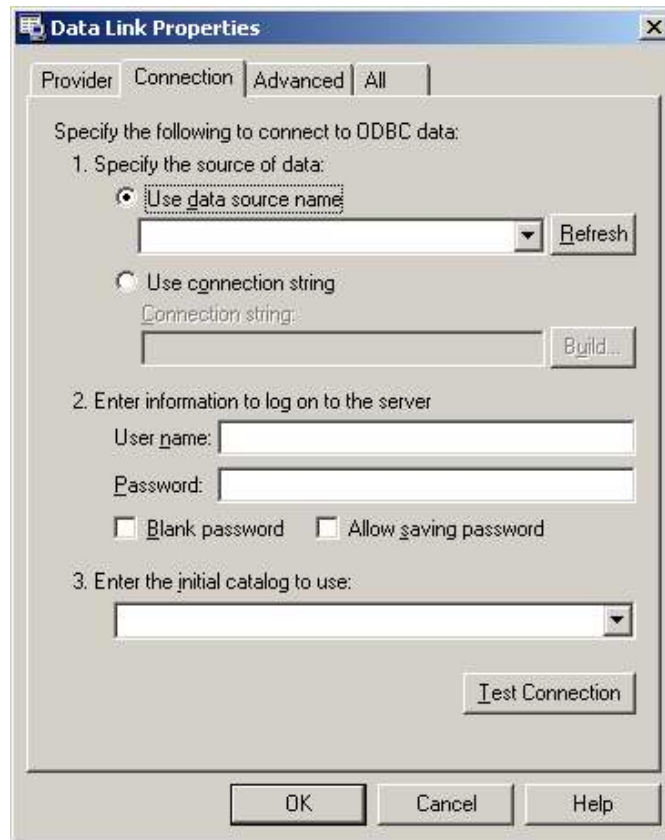


Figure C-10. Data Link Properties Dialog Box

3. Click on the 'Provider' tab and select 'Microsoft OLE DB Provider for SQL Server' as shown in Figure C-11.

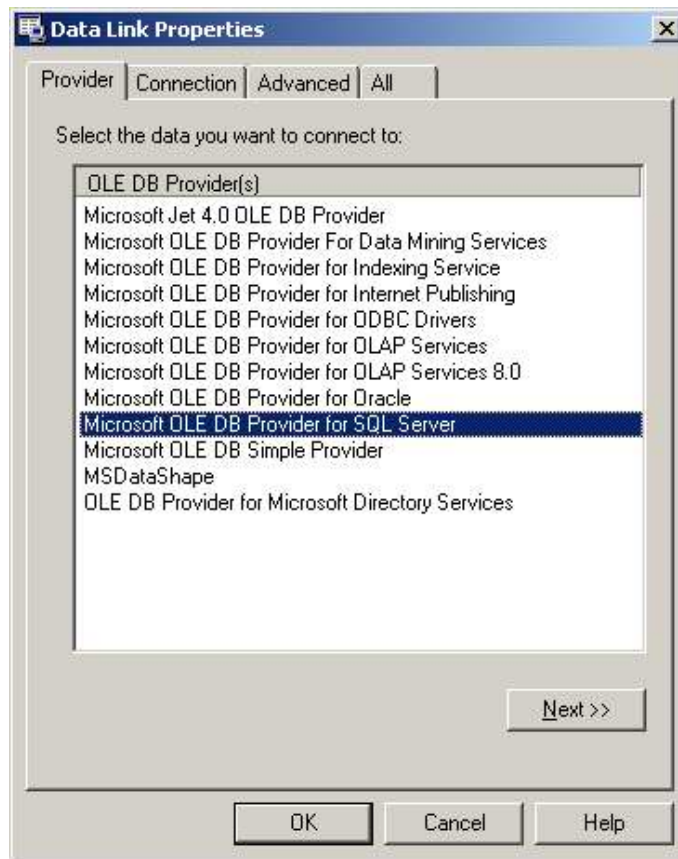


Figure C-11. Data Link Properties – Provider Tab

4. Click the 'Next' button.

5. When the Connection tab displays, fill in the fields as shown in Figure C-12 for the configuration database datalink (using correct Server name). No other fields are required.
6. Click the 'Test Connection' button to verify connection to the SQL Server, then click 'OK' to close.

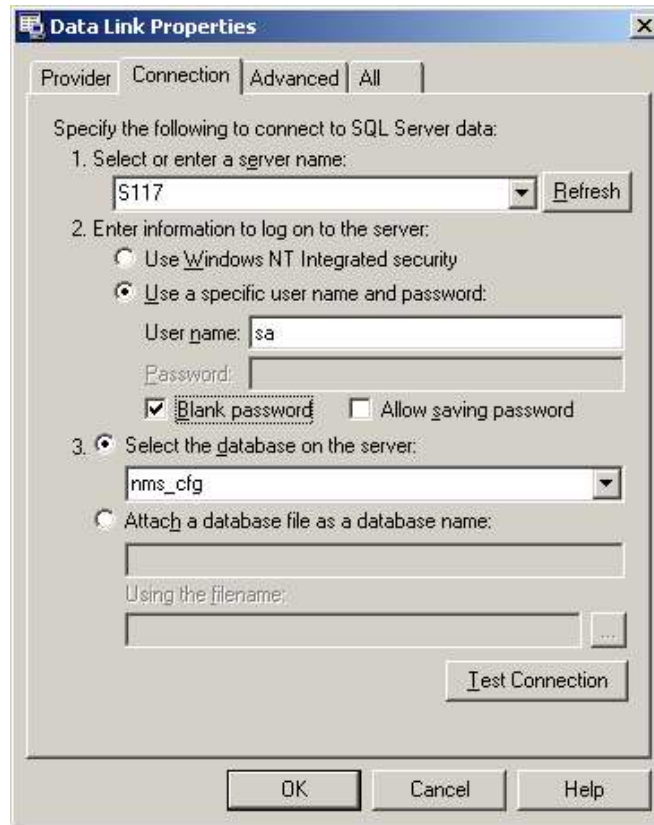


Figure C-12. Data Link Properties – Connection Tab

7. Repeat this procedure for the realtime datalink with the following exceptions:
 - Step 2: double-click on 'NMS_RT.UDL' to open its properties.
 - Step 4: select the 'nms_rt' database on the server.

This completes the procedure for setting up SQL Server data sources.

APPENDIX D

WCC AND OCG SUBNETTING

D.0 OVERVIEW

All office devices in an ATCS network that need to share routing information and code system traffic must establish a logical connection to each other (clustering). The most common communications path for this purpose is via Ethernet LAN, and clustering is accomplished by broadcasting small UDP packets to establish links between devices. It is also possible to cluster WCC/OCGs using synchronous serial links if LAN/WAN connectivity is not available. In addition, any WCC/OCGs that are to be centrally managed must be visible to ASERVER via LAN/WAN using UDP. This Appendix addresses the requirements for WCC/OCGs to establish and maintain a connection with ASERVER, and cluster relationships with other WCC/OCGs.

D.1 ROUTE DISCOVERY

Aserver and WCC/OCGs 'discover' each other by means of two special low-level messages: the route request and the route update (INT_RTE_REQUEST and INT_RTE_UPDATE). Aserver is permanently assigned a special route number (9999) designated as NMS; this is the route to which all WCC/OCG devices send broadcast (diagnostic) traffic. By default, all WCC/OCG devices attempt to resolve the 9999 route, and this may be done by simply waiting for an INT_RTE_UPDATE message from Aserver, after which the server's unicast IP address is known. If no route announcements from Aserver are received, these office devices will transmit a route request to their configured UDP broadcast address. When Aserver receives this packet, it responds with a route update, and the link is established.

In wide area networks, office devices and Aserver may be on different LAN segments, or on different router subnets. For NMS visibility, Aserver and the individual WCC/OCGs must be configured in such a way that the UDP route request/route update mechanism is supported.

For WCC/OCGs and ASERVER to communicate with each other over LAN/WAN, IP addressing and routing rules apply. To illustrate this several scenarios will be examined.

Where WCCs are referenced in the following diagrams, OCGs may be substituted.

D.1.1 Scenario 1: ASERVER and WCCs on same LAN segment

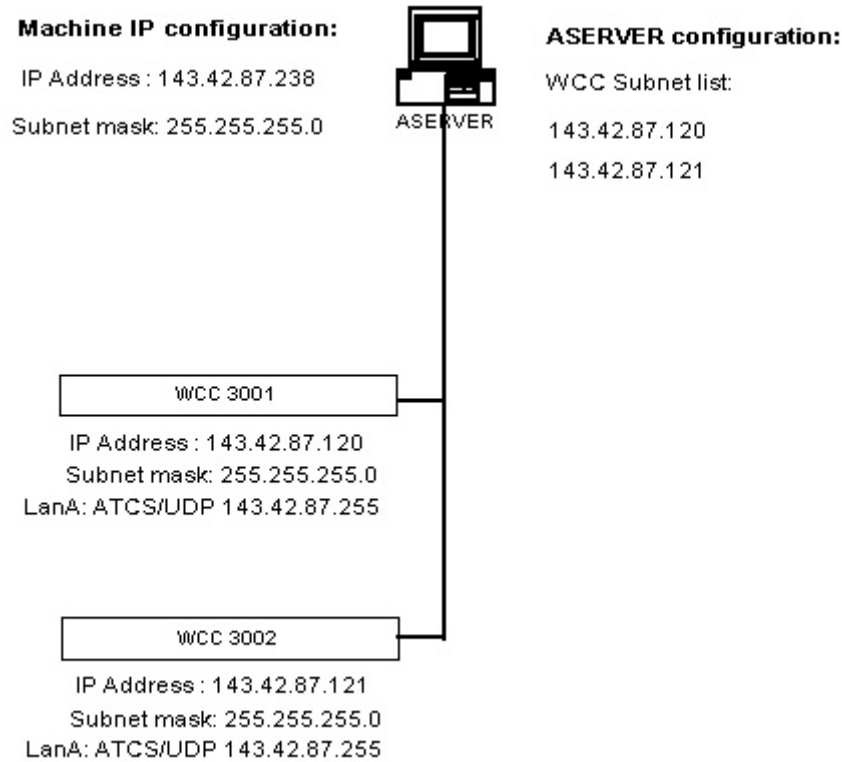


Figure D-1. WCCs On A Single Segment

Referring to Figure D-1, the basic configuration for a small WCC network is shown. The machine running ASERVER is on LAN segment 143.42.87.xxx, as is each WCC. The subnet masks for all devices is the same, so they all reside on the same subnet.

D.2 ASERVER LINKS

For the ASERVER connection process to begin, ASERVER must have a configured set of WCC subnets to broadcast its presense to. As shown, ASERVER will send a route announcement to each of the subnets in its list: 143.42.87.120, then 143.42.87.121. When a WCC hears this broadcast from ASERVER, it uses the source IP address from the broadcast to reply to ASERVER and establish the connection. When this process is complete, ASERVER will display a green panel icon for the new WCC node.

D.3 WCC CLUSTERING

The WCCs are shown with Lan A configured for ATCS/UDP, with an IP address of 143.42.87.255. The IP address associated with Lan A (or B,C,D) is the address to which the WCC will broadcast route announcements for clustering purposes. These route broadcasts are heard by other WCCs and are used to establish cluster relationships on the subnet. Once a cluster connection has been established between 2 WCCs, they are able to establish secondary routes to and from field locations, thereby 'sharing' control and indication traffic.

D.4 SUBNET ADDRESSES

Note that the WCCs are broadcasting to a subnet address, not a discrete IP address. In this way they are announcing their presence to ANY devices on the subnet. Subnet addressing is the most efficient way to manage small ATCS networks.

CALCULATING A SUBNET ADDRESS

- | | |
|--------------------------------------------------------|-----------------|
| 1. Start with the local IP address: | 143.042.087.102 |
| 2. AND this value with the subnet mask: | 255.255.255.000 |
| 3. The result: | 143.042.087.000 |
| 4. Is ORed with the 1's complement of the subnet mask: | 000.000.000.255 |
| 5. To obtain the subnet address: | 143.042.087.255 |

D.5 ASERVER WCC SUBNETS:

As more WCCs are added to the network, it becomes cumbersome to list each discrete WCC in the ASERVER subnet list as shown above. It is more efficient to enter the subnet address in the subnet list, as shown in Figure D-2 below.

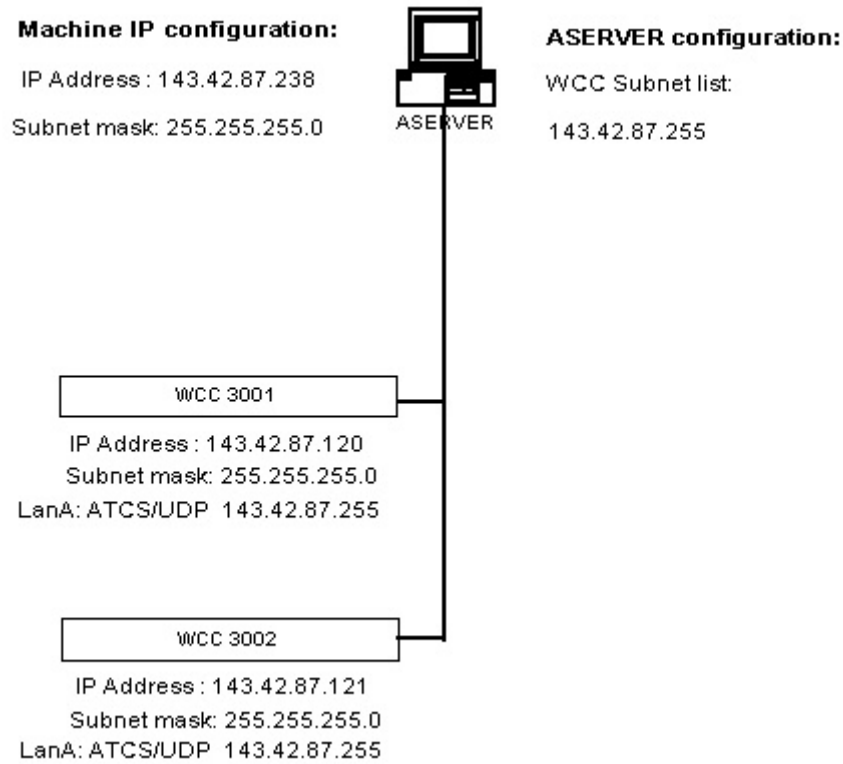


Figure D-2. ASERVER Using Subnet Addressing For WCC Subnets

D.5.1 Scenario 2: WCCs on different subnets with local clustering

When WCCs are distributed over a wide-area network (WAN), different subnets are connected via routers. Figure D-3 shows such a WAN configuration where ASERVER sees all WCCs on the network.

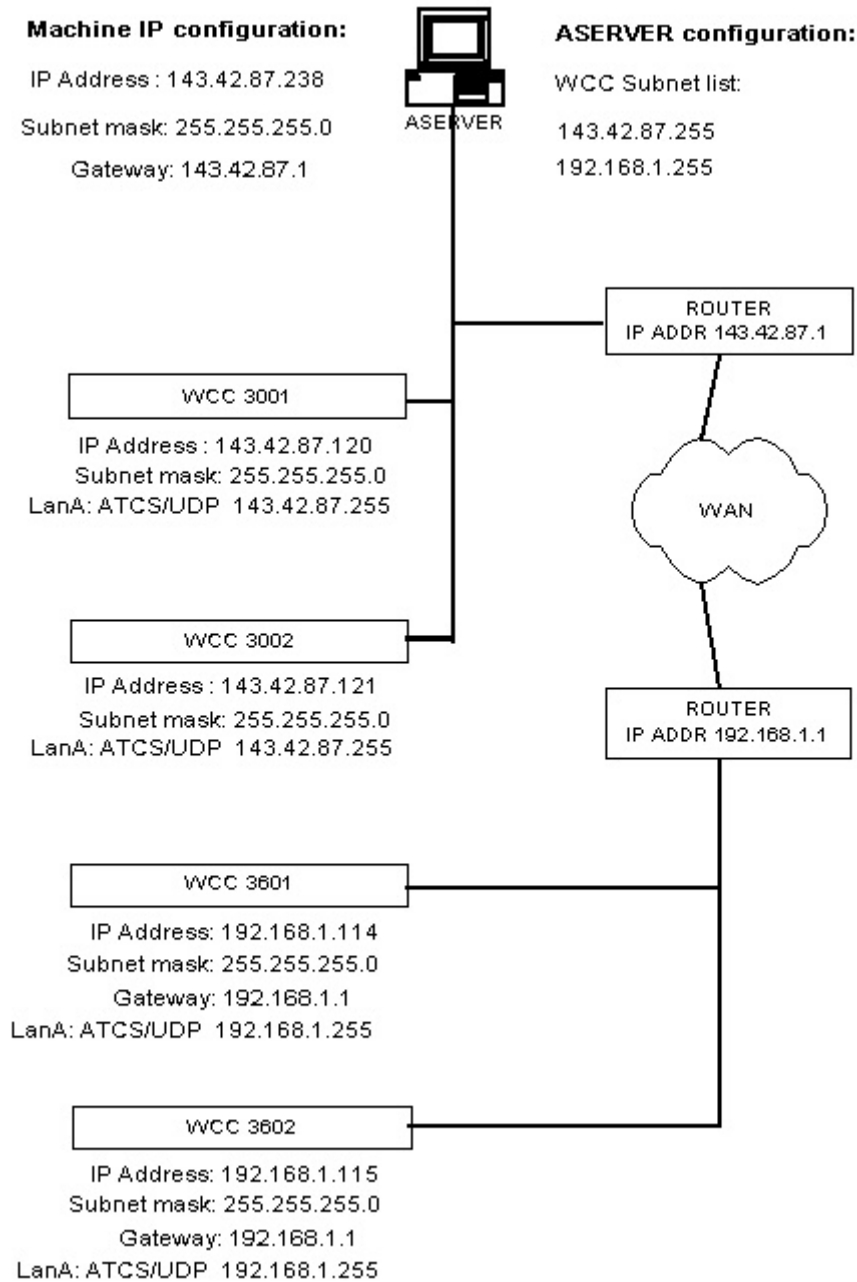


Figure D-3. WCCs In A WAN Configuration

Referring to Figure D-3, several differences are apparent between this configuration and the simple LAN described earlier.

1. ASERVER now has an additional WCC subnet in its list: 192.168.1.255. This makes all WCCs on the 192.168.1.xxx subnet visible to ASERVER.
2. WCCs 3601 and 3602 have Gateways configured (the router address, 192.168.1.1) . This enables the WCCs to send traffic to ASERVER on the 143.42.87.xxx subnet.
3. WCCs 3601 and 3602 are configured to cluster with each other, as seen by their LanA address of 192.168.1.255.
4. In the same way, WCCs 3001 and 3002 cluster to each other using 143.42.87.255 for a LanA address.
5. WCCs 3001 and 3002 are not configured to use a Gateway. This is because they only need to send traffic to each other and to ASERVER; that is, they never need to send traffic off their own subnet.

In this scenario, WCC clustering is confined to each subnet. For example, if WCC 3601 receives indications from an MCP that belongs to a code line controlled by WCC 3002, the system design prevents this indication from being handed off to WCC 3002. Sharing can only take place within individual subnets.

For a WCC to cluster with WCCs on a different subnet, as well as WCCs on its own subnet, multicasting must be used.

D.5.2 Scenario 3: WCCs on different (WAN) subnets with global clustering

When it is imperative that WCCs be able to cluster to WCCs on a different subnet while still clustering on their home subnet, multicasting must be used. This is illustrated in Figure D-4.

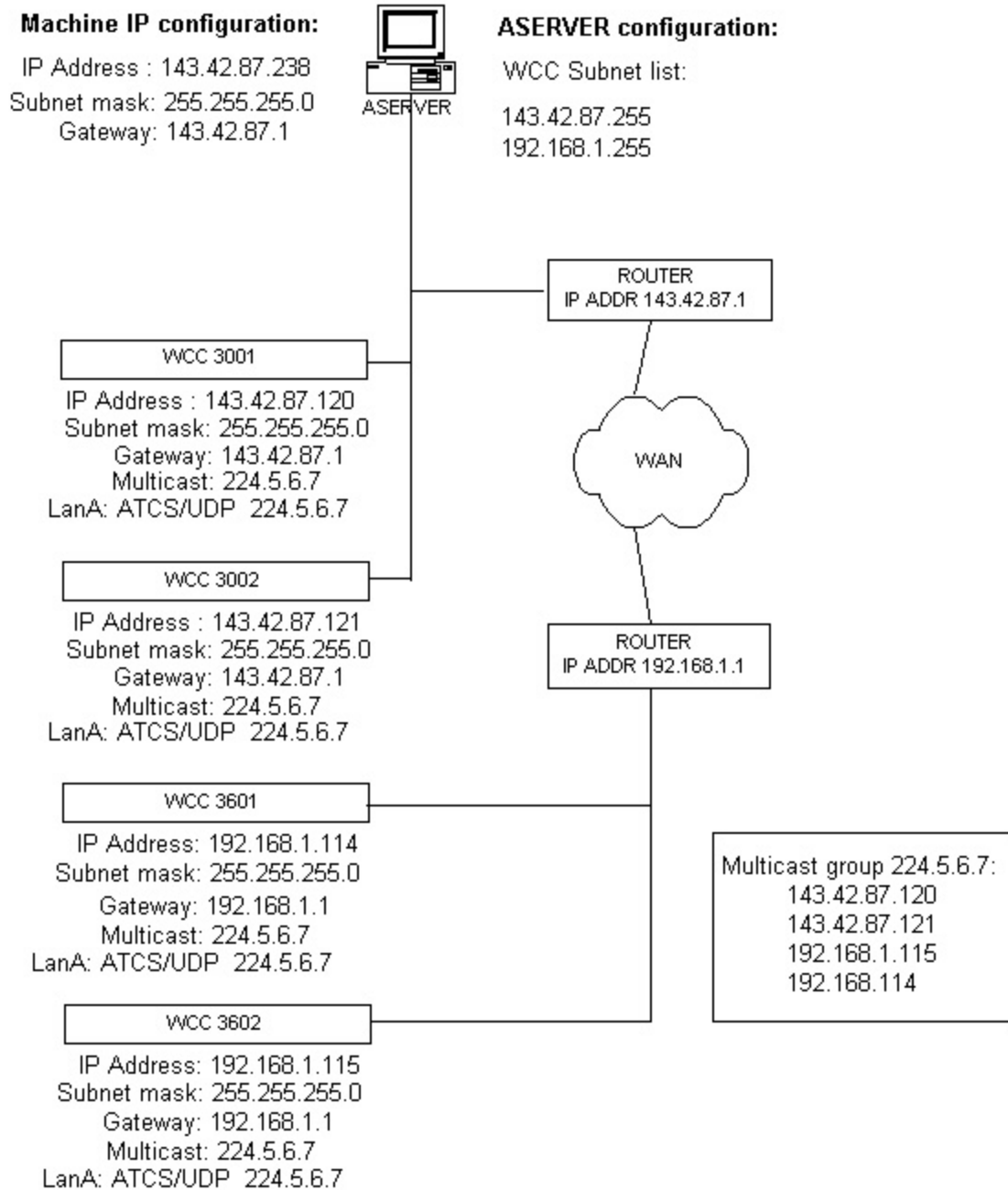


Figure D-4. WAN Configuration With Multicasting

Referring to Figure D-4, the difference between this configuration and the one in Figure D-3 is that ALL WCCs are able to cluster with each other, so that any WCC might 'borrow' a BCP (base station) on any other WCC in the network if needed.

NOTE: Network routers must be configured to support multicasting; in many large networks multicasting is not allowed by default. The use of multicasting is regulated by network administrators. For the purpose of this discussion, it is assumed that there are no multicasting restrictions on the network.

The following changes have been added to the sample network diagram configuration to support multicasting:

1. A multicast group with the IP address 224.5.6.7 has been established with 4 members – each of the 4 WCCs
2. Each WCC is now configured to belong to the multicast group. This allows the WCC to join the group and RECEIVE traffic sent to the multicast address. Each WCC continues to send and receive traffic on its own subnet as before.
3. Each WCC now uses the multicast address for LanA. This means the WCC will send broadcast traffic to the multicast address to establish clustering.
4. Each WCC is now configured for a Gateway address. Once remote clustering is established with multicasting, messages between clustered WCCs on different subnets is Unicast (specifically addressed with source and destination IP addresses).

It is important to note that multicasting is used for route establishment only. Any ATCS messages between WCCs are unicast. For example, in the above network, WCC 3002 broadcasts its routes to the multicast address every 10 seconds. WCC 3601 receives these broadcasts, and as a result, knows the IP address of WCC 3002. When an indication from a group on a codeline controlled by WCC 3002 is received on a base connected to WCC 3601, WCC 3601 sends the indication to WCC 3002 as a unicast ATCS message

APPENDIX E

SERVER CONTENTION HANDLING

E.0 INTRODUCTION

This Appendix deals with Aserver's facility for handling duplicate server instances on the same network. If, for example, a second instance of Aserver is launched on the same subnet as the original server, WccMaint clients will experience problems with system diagnostics. While the launching of a duplicate instance of Aserver on the **same** workstation is programatically inhibited, there is nothing to prevent inadvertent launching of a competing server on another workstation.

E.1 BACKGROUND

ATCS components (WCCs, OCGs etc) routinely send diagnostic information over the network, either as a broadcast or as a response to query messages from WccMaint clients. Aserver is the focal point for all such NMS traffic, responsible for maintaining client connections and providing the gateway for office applications to reach field ATCS devices.

All UDP-connected ATCS devices need a way to locate Aserver on startup and to maintain this route to the server for all inbound NMS traffic. WCCs and OCGs, as well as field WCMs, use UDP as a network transport, so they will attempt to locate the NMS (Aserver) route on startup as a default.

A WCC learns the NMS route when it receives a RTE_UPDATE message announcing ownership of the NMS (9999) route. Aserver can be configured to periodically broadcast this message to inform new devices of the network path to the server. In addition, Aserver will respond to a RTE_REQUEST message that specifically requests the NMS route. In fact, all office devices will begin sending these RTE_REQUEST messages for route 9999 on startup.

If an office device has an established link to the NMS route, and it receives a RTE_UPDATE message for route 9999 from another source (i.e., another instance of Aserver), it will immediately replace the IP address of the established link with the source IP address of the RTE_UPDATE message. All subsequent NMS traffic will be sent to this IP address.

In the case of two Aservers running simultaneously, assuming equal network visibility, both will presumably send RTE_UPDATE messages to office devices, causing these WCCs and OCGs to continuously toggle their NMS routes from one server to another. While this condition does not affect code line traffic, it will seriously disrupt diagnostics from a WccMaint point of view.

To avoid this condition of having two simultaneous (conflicting) servers running, Aserver uses this same RTE_REQUEST/RTE_UPDATE mechanism to determine if there is a competing Aserver on the same subnet.

E.1.1 Aserver Version

The contention resolution feature was introduced in Aserver version 5.1.140.4.

E.2 MULTIPLE INTERFACE HANDLING

When the Aserver machine is multi-homed, there will be more than one IP address identified with the server. For example, if the machine has more than one network interface card (NIC), each will have its own IP address. If Aserver is running in a Windows Cluster machine configuration, the machine is assigned a second (virtual) IP address for cluster operation. For contention to work as intended, competing servers must be detected on any interface from which Aserver receives traffic.

When Aserver starts up, it interrogates each network interface for all assigned IP addresses. These addresses are maintained in a list along with their subnet masks and their calculated subnet addresses.

The route request and contention messages (described below) are sent to ALL detected interfaces, and any responses are arbitrated to determine the superior server.

E.3 CONTENTION OPERATION

E.3.1 Startup

On startup, Aserver begins sending a RTE_REQUEST message for route 9999 to its local subnet. This requested is repeated continuously at 40-second intervals. Barring network problems, any other server running on the same subnet will respond with a RTE_UPDATE message. All versions of Aserver, including older versions, will respond to this RTE_REQUEST.

E.3.2 Discovery

If another server is detected, it is logged in the event log. Aserver maintains a list of up to 5 competing servers for handling. When a RTE_UPDATE is received for route 9999, a **contention message** is sent to the originating server.

E.3.3 Arbitration

A special **contention message** is used to resolve conflicts between servers. This message consists primarily of uptime information, and conflict resolution is based on simple seniority. If a contention message is received, its handling is based on the version of Aserver and how it is configured to respond.

E.3.4 Resolution

Obviously, older versions of Aserver do not handle the contention message. If a conflicting Aserver is an older version, the primary (newer) server will, after the 4th consecutive contention message is ignored, log the conflicting server and send critical alerts informing all WccMaint clients that a possible conflict exists.

For newer versions of Aserver, if a contention message is received, server uptimes are compared. If the uptime in the contention message is greater than the local uptime, the local server will shut down as a default. Instead of shutting down, the local server may also be configured to remain running with a local message box declaring the conflict. WccMaint clients connected to any server will receive critical alerts declaring the conflict.

Contention resolution is enabled by default and may be completely disabled if desired.

The route request process always continues to run, even after a competing server has been found. Once contact with a conflicting server has been lost, the primary server waits 5 minutes before dropping the conflicting server from its server list. During this time, any WccMaint client that connects will receive the critical alert declaring a possible conflict.

Any messages sent or received relating to server contention are logged in the event log.

E.4 CONTROLLING CONTENTION OPERATION

The use of contention and the actions associated with contention are controlled with entries in SAFETRAN.INI as follows:

[Aserver]

ContentionEnable = false

This switch will disable sending or reacting to contention messages. ContentionEnable defaults to TRUE.

OnContention = Warning

This switch instructs the server to remain running with a warning message displayed if a superior instance is detected. This option defaults to SHUTDOWN. Under the default, if a superior Aserver instance is detected, the local server shuts down.

ContentionClusterIpIgnore = 10.5.6.55

This switch instructs the server to ignore any contention messages coming from this IP address. This is used to enable contention in Windows Cluster environments where a server has both a real and virtual IP address on the cluster. If this option is not used in a Cluster environment, Aserver will detect its own virtual IP as a competing server. This option has no default value.

This page intentionally left blank.

APPENDIX F

WCM SUBSYSTEMS

F.0 INTRODUCTION

This appendix discusses ATCS addressing considerations for WCMs and the changes in broadcast traffic handling and routing rules for ASERVER that relates to them. The changes described in this appendix are the primary differences between ASERVER versions 4 and 5.

F.1 BACKGROUND

ASERVER was originally designed to route NMS traffic between office controllers (WCCs) and WccMaint clients. Routing was based on either the WCC device (3xxx) number or the HUB/LCT (6xxx,5xxx) region controlled by the WCC. For example, a WccMaint request for configuration data from a WCC was sent to the WCC's ATCS address (2.RRR.01.3901), and ASERVER would attempt to route the message to any 3901 route in its local routing tables. In the same way, a request for group status would be sent to an LCT (2.RRR.13.5515) and ASERVER would look for 5515 in the route table.

F.2 INTRODUCTION OF WCMS

When WCMs (Wayside Communications Manager) were introduced, they represented a new paradigm for NMS – a device that shared functionality both with existing office devices (WCCs) and field devices (MCPs). To accommodate this dual functionality, WCMs were given attributes that would allow two different ATCS addresses to apply to the unit – a type 2 address for the office end and a type 7 address for the field end.

Because WCMs are IP devices, they are able to cluster directly into existing WCC office networks using their type 2 address.

F.3 ATCS NUMBERING CONVENTIONS

The numbering convention that applies to type 2 addresses in Safetran NMS networks is that all type 2 devices must have a device number in the range 3000-3999. The problem that the introduction of WCMs created is that on any given system, thousands of WCMs could potentially be deployed. Since there was by definition only room for 1000 type 2 devices on a system, ASERVER expanded its routing rules for office devices to include the node (NN) portion of the ATCS address. At the same time, the guidelines for type 2 ATCS addressing for Safetran NMS systems were updated.

Under the new rules, ‘true’ office devices (WCCs and OCGs) still have the device number requirement of being between 3000 and 3999. In addition, the NODE number for these devices is now required to be either 01 or 99 (node 00 is not defined). WCM type 2 addresses have the same device number rules, but they must have node numbers between 2 and 98.

This effectively created 99 subsystems of type 2 devices, based on node numbers. Since nodes 1 and 99 are reserved, there remain 97 node numbers available for WCMs. This also created an opportunity to subdivide large WCM networks in a logical way. For example, all WCM installations on a certain railroad division can be given the same node number, and all WCMs on another division given a different node number. In this way, large WCM groupings can be displayed by territory on WccMaint. Most of the rule changes for WCMs resulted from efforts to control the display of such large numbers of similar devices in WccMaint.

F.4 WCM DISPLAY IN WCCMAINT

For a WCC to appear on WccMaint, it must send periodic status messages to Aserver that are in turn broadcast to all WccMaint clients. When WccMaint receives a WCC_LOCAL_STATUS_REPLY (0x04E0) message, it creates the large WCC panel and displays it on the tab specified in the message. When it receives a region status message for this WCC, it creates the region (HUB/LCT) panel and places it within the larger WCC panel.

It was determined that WCMs should not normally appear in WccMaint as WCCs do, because their potentially large numbers would exceed the display capacity of the forms in WccMaint. Instead, when ASERVER receives a broadcast message from a WCM, it blocks the message from passing through to WccMaint. All such broadcasts from WCMs are blocked unless the WccMaint client specifically requests traffic from a range of WCM nodes. ASERVER then records the node range for that client, and when broadcasts arrive, they are selectively sent only to WccMaint clients that have interest in them.

F.5 ASERVER ROUTING RULES

Because the NN portion of the type 2 address is now significant, ASERVER must now route outbound traffic to type 2 devices based on BOTH the NN and DDDD portion of its ATCS address. For example, there may be a WCM with address 2.125.32.3004, another with 2.125.21.3004, and an OCG with 2.125.01.3004. A message intended for the OCG is now properly routed by ASERVER because it looks for a match for both the node and device address of the OCG (01.3004) in its route table.

F.6 SUMMARY

- WCC and OCG devices must be configured with either node 1 or node 99 as the NN portion of their ATCS address. The original restriction of DDDD as 3000-3999 remains.

WCC address = 2.RRR.NN.DDDD = 2.125.01.3800

- WCM devices must have NN numbers between 2 and 98, with DDDD between 3000-3999.

WCM address = 2.RRR.NN.DDDD = 2.125.32.3800

- ASERVER blocks periodic broadcasts from WCM devices unless a specific WccMaint client has requested them.

ASERVER now routes outbound messages based on the destination ATCS address, using both the NN and DDDD portions for defining and locating routes.

This page intentionally left blank.

APPENDIX G

SNMP ALARM SERVICE

NOTICE

THIS APPENDIX IS APPLICABLE TO CSX
ENTERPRISE MANAGEMENT SYSTEMS ONLY!

G.0 BACKGROUND

An NMS service is an Activex EXE that 'plugs in' to Aserver via a TCP socket, and performs some continuous background function based on ATCS messages to and from the field network.

Typical services perform tasks such as managing ATCS field alarms, requesting and storing group coverage data from packet switches, handling dial backup, etc.

An SNMP interface service was created to instantiate an SNMP gateway to an enterprise management system and send traps to the system when alarms occur on the ATCS network. This service has been built specifically for the CSX SMART system, but may be modified in the future to support SNMP managers on other railroads.

Because the WAMS Status Manager and all packet switches/OCGs interface directly to Aserver, the service approach was taken in order to take advantage of the commonality of Aserver, allowing other alarms to be sent to SMARTS besides crossing alarms.

The message flow for a crossing alarm is as follows: A SEAR-II reports an alarm to Status Manager, who then forwards the alarm over a TCP socket to Aserver. Status Manager must be configured to handle the alarm in this way, similar to the existing Digicon and Megasys protocol drivers (a new protocol driver for SM has been created and is being distributed separately). When Aserver receives the alarm from Status Manager, it wrappers it in an ATCS message and sends it to the SNMP service, which converts it to an SNMP trap for forwarding to the network manager. When SMARTS receives the trap, it is displayed appropriately on the alarm monitor screen in the control center.

The advantage here is that Aserver can independently send SNMP traps for other events, such as OCG critical alerts or alarms from the field code network. This feature is planned but not implemented at this time.

To enable SNMP handling, there is an updated Aserver.EXE, a setup program that creates the SNMP service (NMSServiceAlarmServer.EXE) , and a new protocol (WAMSASCIIProtocol.DLL) for Status Manager. Installing Aserver, the SNMP service and the new protocol driver is explained in this document.

G.1 INSTALLING THE SERVICE

There are 3 install files for the SNMP service:

```
NMSSERVICEALARMAGENT.CAB  
SETUP.EXE  
SETUP.LST
```

Place these 3 files in a temporary directory and run `SETUP.EXE`. Follow the prompts and accept all defaults. If asked to keep any files, answer ‘Yes’. This setup program will install and register the service so that the NMS Services Manager will locate it.

The current version of the SNMP agent service is 1.1.0.

Configuring and monitoring the SNMP service is done through the Services Manager, which is run from the Aserver UI as shown below.

G.2 ASERVER VERSION

The earliest release of `Aserver.exe` that supports the SNMP agent is 5.1.140.2. This version opens the TCP socket to Status Manager for crossing alarms. `Aserver` needs no configuration changes to accommodate the SNMP service.

G.3 NMS SERVICES MANAGER VERSION

The latest release of the Services Manager is 1.2.

G.4 INSTALLING WAMSASCIIPROTOCOL

Installing the protocol driver involves copying the distributed file to the appropriate directory and manually registering it with Windows, as follows:

- Copy the `WAMSASCIIProtocol.DLL` to the following directory:

```
C:\Program Files\Common Files\WAMS\Protocols
```

- Using a DOS window, select the above directory as the current one and enter the following command:

```
>regsvr32 WAMSASCIIProtocol.dll.
```


G.5 CONFIGURING THE SNMP SERVICE

Open the Services Manager from the Aserver main menu (Figure G-1).

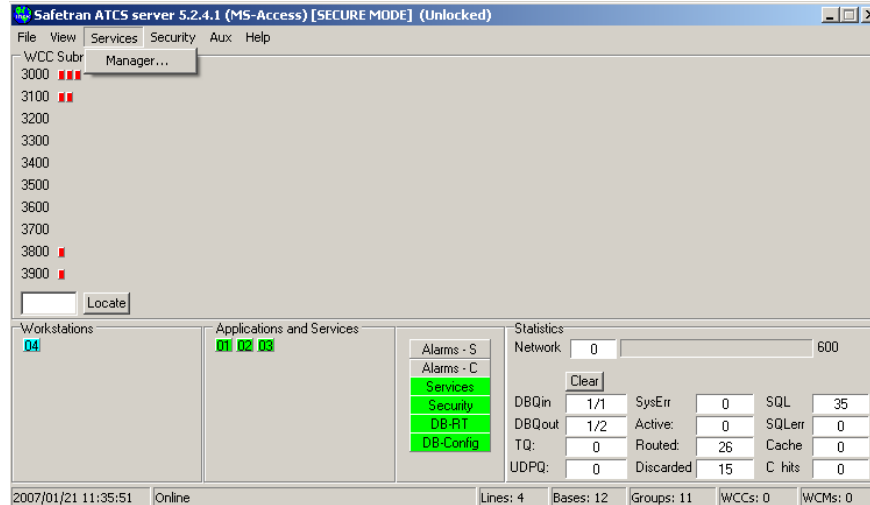


Figure G-1. Selecting The Aserver Services Manager

The Services Manager will list all services found. Highlight the ‘Alarm Agent’ service as shown in Figure G-2 and click **Setup**.

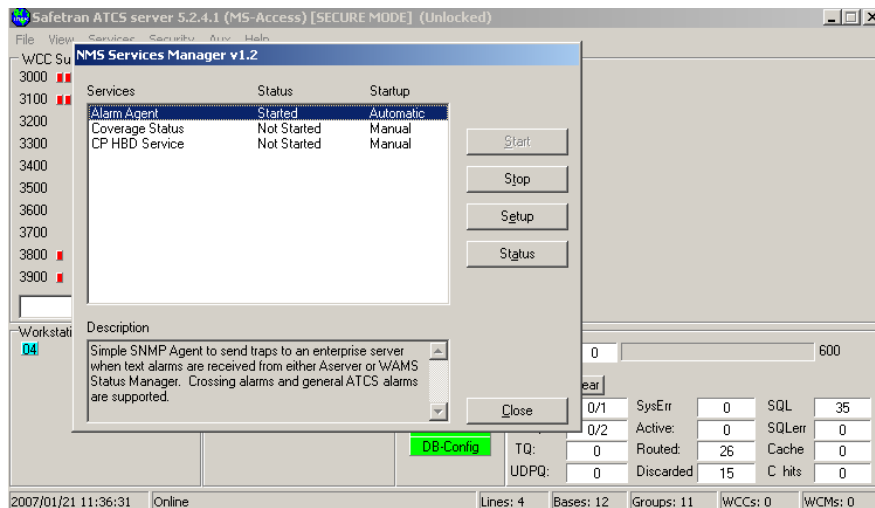


Figure G-2. Selecting The Alarm Agent Service

On the **General** tab, click **Automatic** so the service will start automatically (Figure G-3).

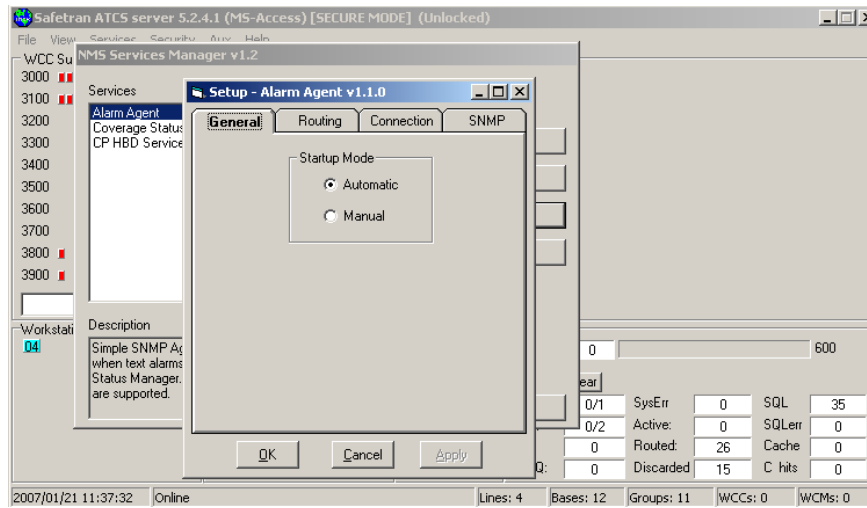


Figure G-3. Setting Automatic Startup

The **Routing** tab options may be left defaulted, as shown in Figure G-4.

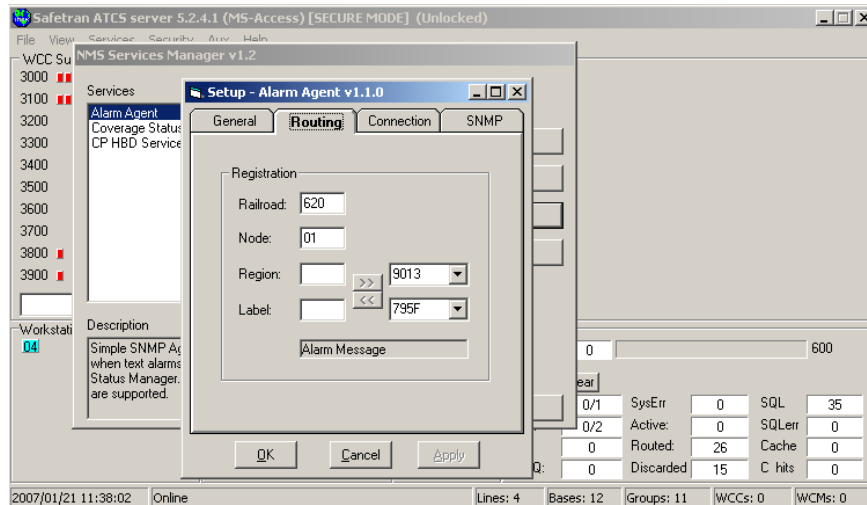


Figure G-4 Routing Tab Default Configuration

On the **Connection** tab, enter the Aserver IP address (loopback address shown in Figure G-5 is correct also) . Other settings should remain defaulted as shown.

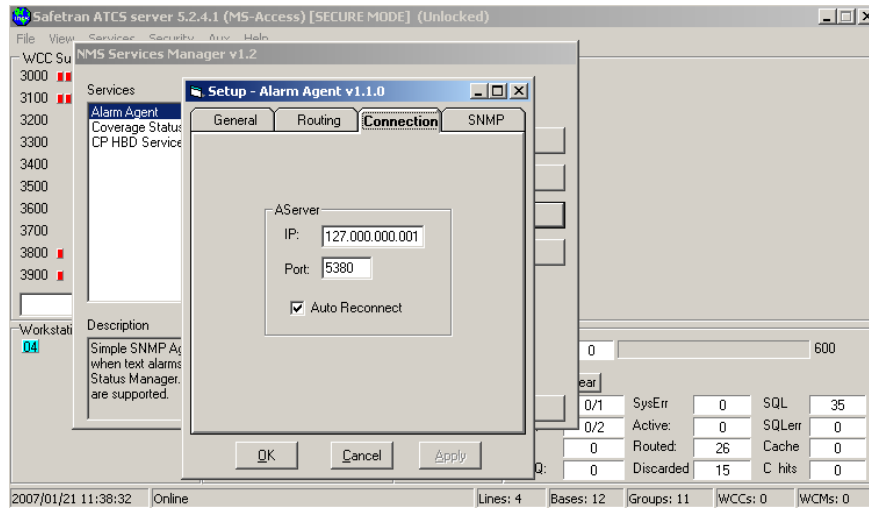


Figure G-5. Connection Tab Configuration

On the **SNMP** tab, enter the SMARTS server IP address. The Enterprise ID is hardcoded. Refer to Figure G-6 for example.

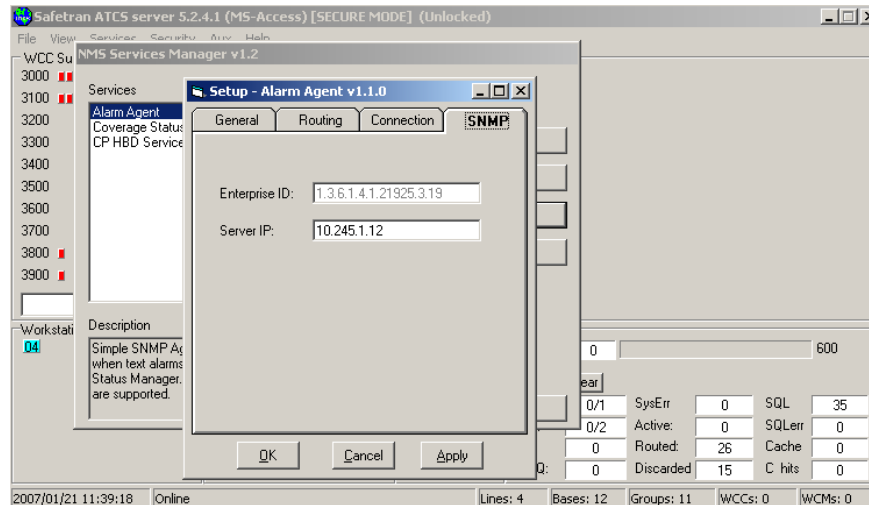


Figure G-6. SNMP Tab Configuration

Click **Apply** to save any changes and **OK** to exit the SNMP service setup.

On the Services Manager screen (above), if the service is not shown to be running, you can click **Start** to start the service. Alarms will be routed from Aserver to the service after the service 'registers' itself to Aserver, which should take 5-10 seconds.

G.6 CHECKING SNMP SERVICE STATUS

From the Status Manager, select the Alarm Agent service and click **Status**:

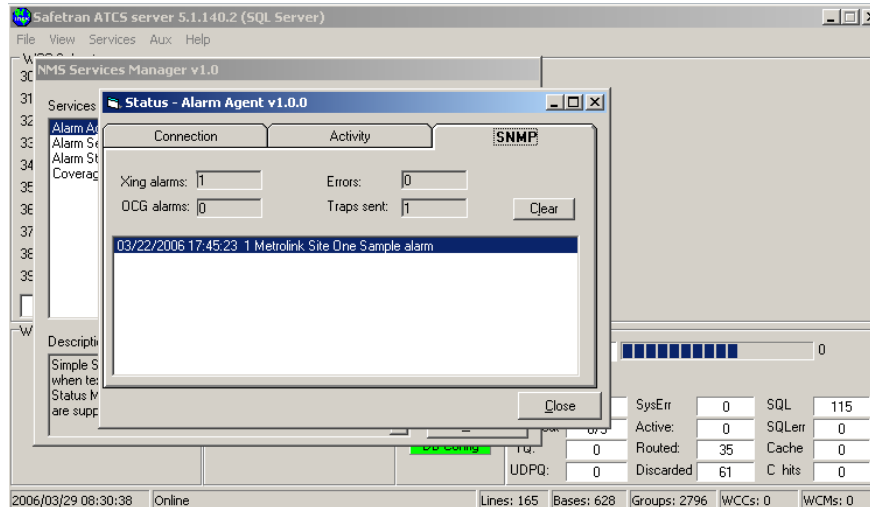


Figure G-7. Checking Alarm Agent Service Status

Status Descriptions:

Xing alarms is the count of alarms received from Status Manager.

Traps sent is the number of properly formatted traps sent to SMARTS. These two counts should be the same.

Errors is a count of message received from Aserver that could not be interpreted and were discarded.

OCG alarms is a count of alarms from the ATCS network received from Aserver. These are reserved for future use and are not currently implemented.

G.7 CONFIGURING THE WAMSASCIIPROTOCOL DRIVER

In Status Manager, select Router from the Connections menu. This will display the Alarm Socket Driver window as shown in Figure G-8.

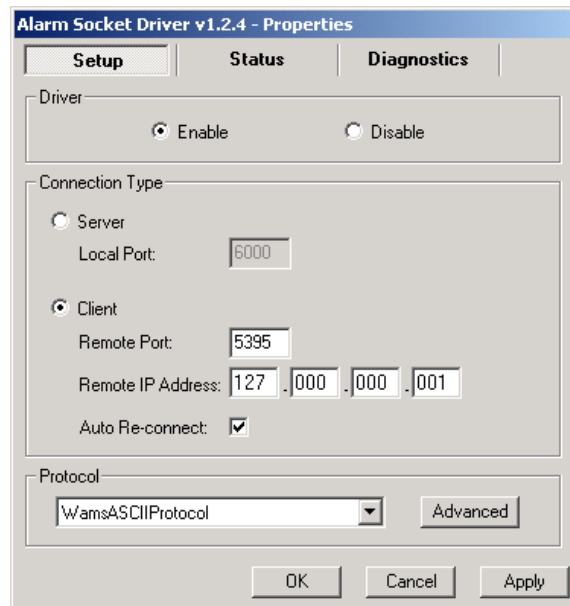


Figure G-8. Alarm Socket Driver Window

Select the **Enable** radio button to enable the alarm router driver.

Select the **Client** radio button to configure the driver for a TCP session.

Enter 5395 in the **Remote Port** field to communicate with AServer.

Enter 127.000.000.001 in the **Remote IP Address** field if AServer and Status Manager are running in the same PC. If that is not the case, enter the IP Address of the PC where AServer is running.

Select (check) the **Auto Re-connect** checkbox so the driver will automatically reconnect with AServer in the event of disconnection.

Select `WamsASCIIProtocol` from the **Protocol** field drop-down list.

Click the **Apply** or **OK** button.

To verify that the driver is connected with AServer, select the **Status** tab (Figure G-9).

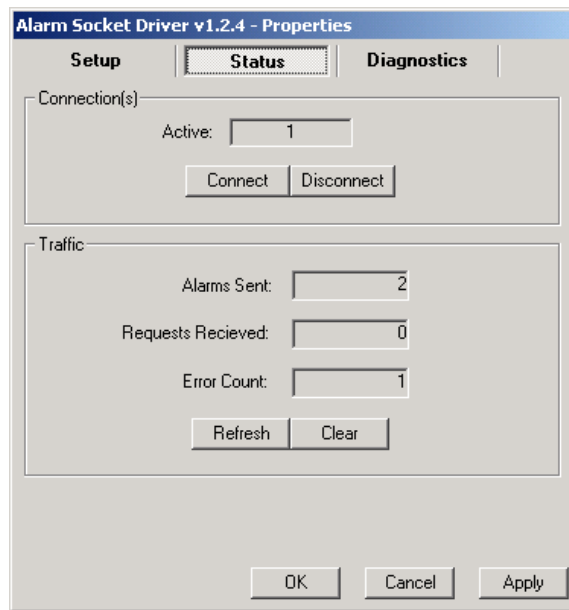


Figure G-9. Alarm Socket Status Window

This window should show an Active Connection greater than 0.

In addition, the Router Status indicator in Status Manager’s status bar should indicate the status of the connection:



Figure G-10. Status Manager Status Bar

Status Bar - Color Codes:

- Gray – Driver disabled
- Yellow – Driver attempting to connect with AServer
- Green – Driver connected with AServer
- Red – Driver has lost or not established a connection with AServer