Avaya™ ATM WAN Survivable Processor Manager

Release 1.1
Installation and Configuration

555-233-223
Issue 3
June 2002

Notice

Every effort was made to ensure that the information in this document was complete and accurate at the time of printing. However, information is subject to change.

Preventing Toll Fraud

"Toll fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there may be a risk of toll fraud associated with your system and that, if toll fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Fraud Intervention

If you suspect that you are being victimized by toll fraud and you need technical assistance or support, in the United States and Canada, call the Technical Service Center's Toll Fraud Intervention Hotline at 1-800-643-2353.

How to Get Help

For additional support telephone numbers, go to the Avaya Web site:
http://www.avaya.com/support/
If you are:

- Within the United States, click *Escalation Lists*, which includes escalation phone numbers within the USA.
- Outside the United States, click *Escalation Lists* then click *Global Escalation List*, which includes phone numbers for the regional Centers of Excellence.

Providing Telecommunications Security

Telecommunications security (of voice, data, and/or video communications) is the prevention of any type of intrusion to (that is, either unauthorized or malicious access to or use of) your company's telecommunications equipment by some party.

Your company's "telecommunications equipment" includes both this Avaya product and any other voice/data/video equipment that could be accessed via this Avaya product (that is, "networked equipment").

An "outside party" is anyone who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf. Whereas, a "malicious party" is anyone (including someone who may be otherwise authorized) who accesses your telecommunications equipment with either malicious or mischievous intent.

Such intrusions may be either to/through synchronous (time-multiplexed and/or circuit-based) or asynchronous (character-, message-, or packet-based) equipment or interfaces for reasons of:

- Utilization (of capabilities special to the accessed equipment)
- Theft (such as, of intellectual property, financial assets, or toll-facility access)
- Eavesdropping (privacy invasions to humans)
- Mischief (troubling, but apparently innocuous, tampering)
- Harm (such as harmful tampering, data loss or alteration, regardless of motive or intent)

Be aware that there may be a risk of unauthorized intrusions associated with your system and/or its networked equipment. Also realize that, if such an intrusion should occur, it could result in a variety of losses to your company (including but not limited to, human/data privacy, intellectual property, material assets, financial resources, labor costs, and/or legal costs).

Responsibility for Your Company's Telecommunications Security

The final responsibility for securing both this system and its networked equipment rests with you - Avaya's customer system administrator, your telecommunications peers, and your managers. Base the fulfillment of your responsibility on acquired knowledge and resources from a variety of sources including but not limited to:

- Installation documents
- System administration documents
- Security documents
- Hardware-/software-based security tools
- Shared information between you and your peers
- Telecommunications security experts

To prevent intrusions to your telecommunications equipment, you and your peers should carefully program and configure:

- Your Avaya-provided telecommunications systems and their interfaces
- Your Avaya-provided software applications, as well as their underlying hardware/software platforms and interfaces
- Any other equipment networked to your Avaya products.

Voice Over Internet Protcal (VoIP)

If the equipment supports Voice over Internet Protocol (VoIP) facilities, you may experience certain compromises in performance, reliability and security, even when the equipment performs as warranted. These compromises may become more acute if you fail to follow Avaya's recommendations for configuration, operation and use of the equipment. YOU ACKNOWLEDGE THAT YOU ARE AWARE OF THESE RISKS AND THAT YOU HAVE DETERMINED THEY ARE ACCEPTABLE FOR YOUR APPLICATION OF THE EQUIPMENT. YOU ALSO ACKNOWLEDGE THAT, UNLESS EXPRESSLY PROVIDED IN ANOTHER AGREEMENT, YOU ARE SOLELY RESPONSIBLE FOR (1) ENSURING THAT YOUR NETWORKS AND SYSTEMS ARE ADEQUATELY SECURED AGAINST UNAUTHORIZED INTRUSION AND (2) BACKING UP YOUR DATA AND FILES.

Standards Compliance

Avaya Inc. is not responsible for any radio or television interference caused by unauthorized modifications of this equipment or the substitution or attachment of connecting cables and equipment other than those specified by Avaya Inc. The correction of interference caused by such unauthorized modifications, substitution or attachment will be the responsibility of the user. Pursuant to Part 15 of the Federal Communications Commission (FCC) Rules, the user is cautioned that changes or modifications not expressly approved by Avaya Inc. could void the user's authority to operate this equipment.
The equipment described in this manual complies with standards of the following organizations and laws, as applicable:

- Australian Communications Agency (ACA)
- American National Standards Institute (ANSI)
- Canadian Standards Association (CSA)
- Committee for European Electrotechnical Standardization (CENELEC) – European Norms (EN's)
- Digital Private Network Signaling System (DPNSS)
- European Computer Manufacturers Association (ECMA)
- European Telecommunications Standards Institute (ETSI)
- FCC Rules Parts 15 and 68
- International Electrotechnical Commission (IEC)
- International Special Committee on Radio Interference (CISPR)
- International Telecommunications Union - Telephony (ITU-T)
- ISDN PBX Network Specification (IPNS)
- National ISDN-1
- National ISDN-2
- Underwriters Laboratories (UL)

Product Safety Standards

This product complies with and conforms to the following international Product Safety standards as applicable:

Safety of Information Technology Equipment, IEC 60950, 3rd Edition including all relevant national deviations as listed in Compliance with IEC for Electrical Equipment (IECEE) CB-96A.

Safety of Laser products, equipment classification and requirements:

- IEC 60825-1, 1.1 Edition
- Safety of Information Technology Equipment, CAN/CSA-C22.2 No. 60950-00 / UL 60950, 3rd Edition
- Safety Requirements for Customer Equipment, ACA Technical Standard (TS) 001 - 1997
- One or more of the following Mexican national standards, as applicable: NOM 001 SCFI 1993, NOM SCFI 016 1993, NOM 019 SCFI 1998

Electromagnetic Compatibility (EMC) Standards

This product complies with and conforms to the following international EMC standards and all relevant national deviations:

Limits and Methods of Measurement of Radio Interference of Information Technology Equipment, CISPR 22:1997 and EN55022:1998.

Information Technology Equipment – Immunity Characteristics – Limits and Methods of Measurement, CISPR 24:1997 and EN55024:1998, including:

- Electrostatic Discharge (ESD) IEC 61000-4-2
- Radiated Immunity IEC 61000-4-3
- Electrical Fast Transient IEC 61000-4-4
- Lightning Effects IEC 61000-4-5
- Conducted Immunity IEC 61000-4-6
- Mains Frequency Magnetic Field IEC 61000-4-8
- Voltage Dips and Variations IEC 61000-4-11
- Powerline Harmonics IEC 61000-3-2
- Voltage Fluctuations and Flicker IEC 61000-3-3

Federal Communications Commission Statement

Part 15:

Note: This equipment 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 own expense.

Part 68: Answer-Supervision Signaling. Allowing this equipment to be operated in a manner that does not provide proper answer-supervision signaling is in violation of Part 68 rules. This equipment returns answer-supervision signals to the public switched network when:

- answered by the called station,
- answered by the attendant, or
- routed to a recorded announcement that can be administered by the customer premises equipment (CPE) user.

This equipment returns answer-supervision signals on all direct inward dialed (DID) calls forwarded back to the public switched telephone network. Permissible exceptions are:

- A call is unanswered.
- A busy tone is received.
- A reorder tone is received.

Avaya attests that this registered equipment is capable of providing users access to interstate providers of operator services through the use of access codes. Modification of this equipment by call aggregators to block access dialing codes is a violation of the Telephone Operator Consumers Act of 1990.

This equipment complies with Part 68 of the FCC Rules. On the rear of this equipment is a label that contains, among other information, the FCC registration number and ringer equivalence number (REN) for this equipment. If requested, this information must be provided to the telephone company.

The REN is used to determine the quantity of devices which may be connected to the telephone line. Excessive RENs on the telephone line may result in devices not ringing in response to an incoming call. In most, but not all areas, the sum of RENs should not exceed 5.0. To be certain of the number of devices that may be connected to a line, as determined by the total RENs, contact the local telephone company.

REN is not required for some types of analog or digital facilities.

Means of Connection

Connection of this equipment to the telephone network is shown in the following table.

Manufacturer's Port Identifier	**FIC Code**	**SOC/REN/ A.S. Code**	**Network Jacks**
Off/On premises station	OL13C	9.0F	RJ2GX, RJ21X, RJ11C
DID trunk	02RV2-T	0.0B	RJ2GX, RJ21X
CO trunk	02GS2	0.3A	RJ21X
CO trunk	02LS2	0.3A	RJ21X
Tie trunk	TL31M	9.0F	RJ2GX
Basic Rate Interface	02IS5	6.0F, 6.0Y	RJ49C
1.544 digital interface	04DU9-BN, 1KN, 1SN	6.0F	RJ48C, RJ48M
120A2 channel service unit	04DU9-DN	6.0Y	RJ48C

If the terminal equipment (for example, the MultiVantage™ Solution equipment) causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. But if advance notice is not practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.

The telephone company may make changes in its facilities, equipment, operations or procedures that could affect the operation of the equipment. If this happens, the telephone company will provide advance notice in order for you to make necessary modifications to maintain uninterrupted service.

If trouble is experienced with this equipment, for repair or warranty information, please contact the Technical Service Center at 1-800-242-2121 or contact your local Avaya representative. If the equipment is causing harm to the telephone network, the telephone company may request that you disconnect the equipment until the problem is resolved.

It is recommended that repairs be performed by Avaya certified technicians.
The equipment cannot be used on public coin phone service provided by the telephone company. Connection to party line service is subject to state tariffs. Contact the state public utility commission, public service commission or corporation commission for information.
This equipment, if it uses a telephone receiver, is hearing aid compatible.

Canadian Department of Communications (DOC) Interference Information

This Class A digital apparatus complies with Canadian ICES-003.
Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

This digital apparatus does not exceed Class A limits for radio noise emission set out in the radio interference regulation of the Canadian Department of Communications.

Le Présent Appareil Nomérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils manicures de la class A préscrites dans le reglement sur le brouillage radioélectrique édicté par le ministére des Communications du Canada.

This equipment meets the applicable Industry Canada Terminal Equipment Technical Specifications. This is confirmed by the registration number. The abbreviation, IC, before the registration number signifies that registration was performed based on a Declaration of Conformity indicating that Industry Canada technical specifications were met. It does not imply that Industry Canada approved the equipment.

DECLARATIONS OF CONFORMITY

United States FCC Part 68 Supplier's Declaration of Conformity (SDoC)

Avaya Inc. in the United States of America hereby certifies that the equipment described in this document and bearing a TIA TSB-168 label identification number complies with the FCC's Rules and Regulations 47 CFR Part 68, and the Administrative Council on Terminal Attachments (ACTA) adopted technical criteria.
Avaya further asserts that Avaya handset-equipped terminal equipment described in this document complies with Paragraph 68.316 of the FCC Rules and Regulations defining Hearing Aid Compatibility and is deemed compatible with hearing aids.
Copies of SDoCs signed by the Responsible Party in the U. S. can be obtained by contacting your local sales representative and are available on the following Web site:
http://support.avaya.com/elmodocs2/DoC/SDoC/index.jhtml/
All MultiVantage™ system products are compliant with FCC Part 68, but many have been registered with the FCC before the SDoC process was available. A list of all Avaya registered products may be found at:
http://www.part68.org/
by conducting a search using "Avaya" as manufacturer.

European Union Declarations of Conformity

CE

Avaya Inc. declares that the equipment specified in this document bearing the "CE" (*Conformité Europeénne*) mark conforms to the European Union Radio and Telecommunications Terminal Equipment Directive (1999/5/EC), including the Electromagnetic Compatibility Directive (89/336/EEC) and Low Voltage Directive (73/23/EEC). This equipment has been certified to meet CTR3 Basic Rate Interface (BRI) and CTR4 Primary Rate Interface (PRI) and subsets thereof in CTR12 and CTR13, as applicable.

Copies of these Declarations of Conformity (DoCs) signed by the Vice President of MultiVantage™ Solutions research and development, Avaya Inc., can be obtained by contacting your local sales representative and are available on the following Web site:
http://support.avaya.com/elmodocs2/DoC/IDoC/index.jhtml/

Japan

This is a Class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may occur, in which case, the user may be required to take corrective actions.

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Network Connections

Digital Connections - The equipment described in this document can be connected to the network digital interfaces throughout the European Union.
Analogue Connections - The equipment described in this document can be connected to the network analogue interfaces throughout the following member states:

Belgium	Germany	Luxembourg
Netherlands	Spain	United Kingdom

LASER Product

The equipment described in this document may contain Class 1 LASER Device(s) if single-mode fiber-optic cable is connected to a remote expansion port network (EPN). The LASER devices operate within the following parameters:

- Maximum power output –5 dBm to -8 dBm
- Center Wavelength 1310 nm to 1360 nm
- CLASS 1 LASER PRODUCT IEC 60825-1: 1998

Use of controls or adjustments or performance of procedures other than those specified herein may result in hazardous radiation exposure. Contact your Avaya representative for more laser product information.

To order copies of this and other documents:

Call: Avaya Publications Center
Voice 1.800.457.1235 or 1.410.568.3680
FAX 1.800.457.1764 or 1.410.891.0207
Write: Globalware Solutions
200 Ward Hill Avenue
Haverhill, MA 01835 USA
Attention: Avaya Account Management
E-mail: totalware@gwsmail.com

Table of Contents

1 Welcome

Purpose

This book explains how to install and configure Avaya™ ATM WAN Spare Processor Manager, how to test the installation, and how to troubleshoot it.

Prerequisites

Installing ASP Manager requires familiarity with data networking concepts, knowledge of your company's data network, and proficiency with Windows.

Intended Audience

We wrote this book for PC Administrators who are responsible for installing this software.

Conventions Used in This Book

In this book, we use the following typographical conventions:

- We use bold type for emphasis and for any information that you should type; for example: **save translation**.
- We use Courier font for any information that the computer screen displays; for example: `login`.
- We use arrows to indicate options that you should select on cascading menus; for example: "Select File>Open" means choose the "Open" option from the "File" menu.
- We use the term "main server" to mean DEFINITY Server R.

Additional Resources

You may find the following additional resources helpful.

For help using ASP Manager, look in the online help. For more detailed information on ATM WSPs, see *ATM Installation, Upgrades, and Administration Using Avaya MultiVantage™ Solutions,* 555-233-124.

For help with complex administration tasks, use the *Administrator's Guide for Avaya MultiVantage™ Software*, 555-233-506, which explains system features and interactions in detail.

Tell Us What You Think!

Let us know how this book measured up to your expectations. Your opinions are crucial to helping us meet your needs! Please complete and return the comment card at the front of this book. Optionally, send us your comments by mail, fax, or e-mail, as follows:

Mail:	Avaya Inc. ASP Manager Documentation Team B3-H25 1300 W. 120th Ave. Westminster, CO 80234-2726 USA
Fax:	ASP Manager Documentation Team + 1 303 538 1741
E-mail:	document@avaya.com

How to Get This Book on the Web

To view or download the latest version of this book, perform the steps listed next.

1. Install your internet browser.

   Most computers are sold with browsers already installed.

2. Get access to the Internet.

   If you do not already have access to the Internet, contact your local Internet Service Provider (ISP).

3. Set up your browser preferences.

   Refer to the documentation that came with your browser.

4. Install Adobe Acrobat Reader with Search, version 3.0 or later.

   This is available on your DNA CD-ROM or from: http://www.adobe.com.

5. Access www.avayadocs.com

6. Search for *Avaya™ ATM WAN Spare Processor Manager Installation and Configuration*, 555-233-223.

   To get other books on the web, repeat these steps, and then search for the publication of interest.

How to Order More Copies

To order this book, call or write us and request the following publication:

Order:	Document Number:	555-233-223
	Issue:	Issue 3
	Date:	June 2002
Call:	Avaya Publications Center	USA
	Voice:	1 800 457 1235
	Fax:	1 800 457 1764
	For callers that cannot access US 1-800 numbers, dial:	
	Voice:	+1 410 568 3680
	Fax:	+1 410 891 0207
Write:	Globalware Solutions 200 Ward Hill Avenue Haverhill, MA 01835 USA	

2 Overview

Avaya™ ATM WAN Spare Processor Manager is a client-server application that allows you to upload translations from Avaya MultiVantage™ software on a "main" server and download them to multiple WAN spare processors (WSPs) simultaneously, according to a schedule you specify. This chapter explains roughly how the application works, explains security considerations, and summarizes the installation process.

The Upload and Download Process

ASP Manager copies translations from MultiVantage software on the "main" server to its WSPs as follows.

Uploading Translations from the Main Server

When ASP Manager copies translations from a main server to its WSPs, it first makes a connection with the main server over an Ethernet LAN or WAN, via the C-LAN board on the main server. It logs in to the main server using an "administration" login ID and password that has already been set up on the main server and specified in ASP Manager. It issues the save translations command, and if the command is successful, ASP Manager logs off and disconnects. It then reconnects using the "upload/download" login, and issues the **upload translations** command. (If the **save translations** command fails, ASP Manager will proceed with the second command only if you have specified that ASP Manager should do so.) The translations from the main server are uploaded to ASP Manager, and then ASP Manager disconnects. ASP Manager logs the success or failure of the upload in its log, which you can view from the ASP Manager user interface. If the translations were uploaded successfully, ASP Manager keeps a copy before downloading the translations to the WSPs.

Modifying Translations for the WSPs

ASP Manager does not download an exact copy of the translations to the WSPs. If it did, it would overwrite critical connectivity information that allows the WSP to communicate with other systems. Instead, after uploading translations from the main server, ASP Manager makes some minor adjustments to the translations; for example, changing IP address, port, and node name information, as appropriate, to work on the given WSP.

Downloading Translations to the WSPs

Once ASP Manager has uploaded translations from the main server, it issues the **status atm wsp** command on the main server. If the WAN Processor Role field contains a value of "pending", no WSP data is available and ASP Manager logs an error. If the WAN Processor Role field contains any other value, ASP Manager can then display the name, number, and link status of each WSP in the network.

ASP Manager then connects and logs in to each WSP, using login IDs and passwords that have previously been set up on the WSPs and specified in ASP Manager. ASP Manager issues the **status atm wsp** command on each WSP. If the WAN Processor Role field contains a value of "spare" and the State field contains a value of "standby," then ASP Manager issues the **save translations removable-media** command, and then the **download translations** command. If the WAN Processor Role and the State fields contain any other values, then ASP Manager aborts the save translations and the download and logs an error. After ASP Manager downloads translations successfully, it does one of two things: for anything prior to DEFINITY ECS Release 10 systems, it issues a **reset system 4 disk** command; for DEFINITY ECS Release 10 and later systems, it issues a **reset system 3 disk preserve-license** command. These commands reboot the WSP in a forced-standby mode. This terminates the connection between the WSP and ASP Manager.

Several minutes later, ASP Manager attempts to reconnect to the rebooted WSP. If it fails, it tries again in another several minutes. If it fails again, it logs an error in its status log. If it succeeds, ASP Manager modifies the translations. Precisely how depends on whether or not the main server has the "critical reliability" feature enabled.

If the main server has critical reliability enabled, ASP Manager issues the **status pnc** command to determine whether A-pnc or B-pnc is active. If B-pnc is active, ASP Manager issues the command **reset pnc interchange override** and waits for two minutes. A-pnc must be active before ASP Manager can issue the command **busyout pnc-standby,** which occurs next. If that step is successful, ASP Manager issues the command **change system duplication,** and sets both SPE dup and PNC dup to 'n'. If that is successful, ASP Manager issues the command **busy atm pnc 1,** and if that is successful ASP Manager issues the command **remove atm pnc1.** Next, ASP Manager issues the command **list config all** to determine the physical location of the ATM interface circuit packs. This returns two locations. Then, ASP Manager issues the command **change system maintenance,** changing the value of the field called WSP to 'SPARE,' entering the ATM interface circuit pack locations determined with the **list config all** command, entering the WSP number, and entering the takeover time. Next, ASP Manager issues the **change system duplication** command, and changes the value of the field called PNC dup back to 'y'. Finally, ASP Manager issues the commands **save trans active** and either **reset system 4 disk** or **reset system 3 disk preserve-license,** depending on the release number of the systems.

For systems without critical reliability, ASP Manager issues the **busyout atm pnc 1** command; it issues the **remove atm pnc 1** command; and then **busyout atm pnc 2** and **remove atm pnc 2** (if applicable). Then, it issues a **list configuration all** command to retrieve the ATM interface location. This location is required for the next change system parameters command. This returns one location. Then, ASP Manager makes the following changes on the **change system-parameters maintenance** form of the WSP: it enters "spare" in the WAN Processor Role field; it enters the previously determined location of the ATM-EI board in the A-PNC Board Location field; it enters the WSP number (gathered from the main server) in the WSP Number field; and it enters the number of minutes (gathered from the ASP Manager user) after which the WSP will take over in the event of a main server failure in the WSP Takeover Time field. Finally, ASP Manager issues the commands **save trans active** and either **reset system 4 disk** or **reset system 3 disk preserve-license,** depending on the release number of the systems.

Scheduling Uploads/Downloads

ASP Manager lets you specify when you want to copy translations. You can copy them immediately or schedule the copy to occur once, daily, or weekly.

Limited Administration of WSPs

ASP Manager lets you set the number of minutes after which a WSP will take over in the event of a main server failure. All other WSP administration commands are accessible only from a System Administration Terminal (SAT) or system administration application, such as Avaya MultiVantage™ Configuration Manager (MCM) or Avaya Site Administration.

Security

ASP Manager has no login and password protection. Unauthorized use of ASP Manager is prevented only through the login and password required by Windows, and the logins and passwords required by the MultiVantage software on the main servers and WSPs. Once ASP Manager has been installed and configured, it stores the login IDs and passwords of the main server and its WSPs on the ASP Manager server, which means from that point forward, only your Windows security prevents unauthorized users from gaining access to these devices. However, all that an unauthorized user could do with ASP Manager is copy translations from the main server to its WSPs. Using ASP Manager, users cannot manually modify translations between uploading them from the server and downloading them to the WSP, which means that using ASP Manager, users have no way to introduce errors or sabotage the WSP translations.

If you have a service agreement with Avaya, or if you want Avaya support during ASP Manager's warranty period, you must install a copy of pcAnywhere on the ASP Manager computers that you want Avaya to support. For the required version number of pcAnywhere, see "Understanding System Requirements'' on page 19. If used incorrectly, pcAnywhere can be a security risk. It is your responsibility to protect your network from unauthorized use. Before installing pcAnywhere, see the guidelines in "Understanding pcAnywhere Security" on page 36.

Installation Checklist

The installation will follow a process like the one listed below.

1. **Connect ASP Manager computers to the main server(s) and WSPs.**

   We recommend that PC administrators or telephone technicians perform the following steps.

   a. Connect ASP Manager computers, and the main server and WSPs that it supports, to a LAN or WAN, following the instructions in "Connecting the Hardware" (page 21).

2. **Prepare the main server(s) and WSPs for ASP Manager.**

   We recommend that an Avaya technician perform the following tasks.

   a. Install main PPN, ATM-PNC, and WSPs, if you have not already.

   For instructions on installing main PPNs and WSPs, visit http://made-easy.avaya.com and click the MCC link to view *Installation for MCC Made Easy*. For instructions on installing ATM-PNC, refer to *ATM Installation, Upgrades, and Administration Using MultiVantage Solutions*.

   b. Install, administer, and test C-LAN boards on all main servers and WSPs that ASP Manager will support, if you have not already.

   c. Set up asynchronous links, if you have not already.

   d. If you will be using Access Security Gateway (ASG) on a main server or WSP that ASP Manager supports, and if it is not already enabled, then contact Avaya to have this feature enabled (page 25).

   e. Have Avaya enable the "`System Management Data Transfer Only?`" customer option for each main server and WSP that ASP Manager supports, if it is not already enabled ((page 25)).

   f. Create an "Upload/Download" login and "Administration" login for each main server and WSP that ASP Manager supports, if these do not already exist (page 27).

3. **Prepare computers for ASP Manager.**

   a. Upgrade existing computers (if necessary) to meet the hardware and software requirements specified on page 19.

   b. Ensure TCP/IP connectivity between the ASP Manager server and all ASP Manager clients.

   c. Ensure TCP/IP connectivity between the ASP Manager server, the "main" server, and all of its WSPs.

   Make sure they can ping each other. Troubleshoot problems with the LAN/WAN administrator.

   d. Set the PC's time (page 41).

4. **Give Avaya access to your system.**

   This step applies if you have a maintenance support agreement with Avaya, or if you want Avaya to be able to support you during ASP Manager's warranty period. We recommend that PC administrators perform the following tasks.

   a. Install modems and pcAnywhere on all computers that you want Avaya to be able to access to support ASP Manager.

   b. Provide Avaya's Technical Service Center (TSC) the phone number or IP address to access ASP Manager computers.

5. **Install ASP Manager.**

   We recommend that PC administrators perform the following tasks.

   a. Install ASP Manager client and server software (page 37).

   b. Reboot.

6. **Configure ASP Manager.**

   We recommend that PC administrators perform the following tasks.

   a. Specify the "main" server connection information (page 42).

   b. Specify the WSP connection information (page 44).

7. **Test the Installation.**

   We recommend that PC administrators perform the following tasks.

   a. Test connections to devices (page 47).

   b. Have ASP Manager copy translations from the "main" server to the associated WSPs and examine the Status Log for errors.

8. **Troubleshoot, if appropriate.**

   We recommend that PC administrators and network administrators collaborate to perform the following tasks.

   a. Troubleshoot hardware connections.

   b. Troubleshoot software connections (page 48).

   c. Troubleshoot uploading/downloading.

Getting Help with the Installation

If you are located within the United States and require assistance installing ASP Manager, contact your local Avaya representative for options and details. Please allow a 4-week lead time to ensure that your requested due date can be met.

If you are located outside the United States and require assistance installing ASP Manager, contact your Avaya local representative or dealer. Please allow a 4-week lead time to ensure that your requested due date can be met.

3 Understanding System Requirements

PC Requirements

Any computer you use to run the ASP Manager client or server software should meet the following requirements:

Parameter	Client	Server
Operating System	Windows 98, 2000, or Windows NT (SP 4 or later)	Windows 2000
Processor	Intel Pentium II 250 MHz	Intel Pentium III 450 MHz
Other Software	antivirus software	antivirus software, Java Runtime Environment
RAM	64 MB	128 MB
Available Disk Space	10 MB*	100 MB, plus 15 MB for each main switch or WSP*
CD-ROM Drive	Yes	Yes
Network Type	Ethernet	Ethernet

*** Note:** *If client and server software are on the same computer, add these space requirements together.

In addition, ASP Manager computers must be on the same LAN or WAN as the main switch(es) and WSPs that ASP Manager will support. If you want to use ASP Manager's E-mail notification feature, then the ASP Manager server must have access to the SMTP mail server that would be sending the notification E-mail.

IP addresses on the ASP Manager client and server computers can be static or DHCP. If you are using DHCP, you must refer to the ASP Manager server by host name.

ASP Manager can run on the same computer with Avaya Site Administration and pcAnywhere 9.0.

Enabling Avaya Remote Services

If you have a maintenance agreement with Avaya for support of ASP Manager, you are required to install a modem and a copy of Symantec's pcAnywhere on the computers that you want Avaya to be able to access. pcAnywhere enables Avaya personnel to remotely troubleshoot and correct problems on your system.

Before installing pcAnywhere, please read the pcAnywhere security guidelines on page 36, and visit the following web site for the latest pcAnywhere security information:
http://www.symantec.com/pcanywhere/index.html

Main Server and WSP Requirements

ASP Manager supports only Release 9.1 or greater of DEFINITY ECS systems. In addition, your "main" server and WSPs must meet the following requirements:

1. A C-LAN board must be installed, asynchronous links must be configured, and the board and configuration must be tested and fully functioning, both on the main server(s) and each of the WSPs that ASP Manager will support.

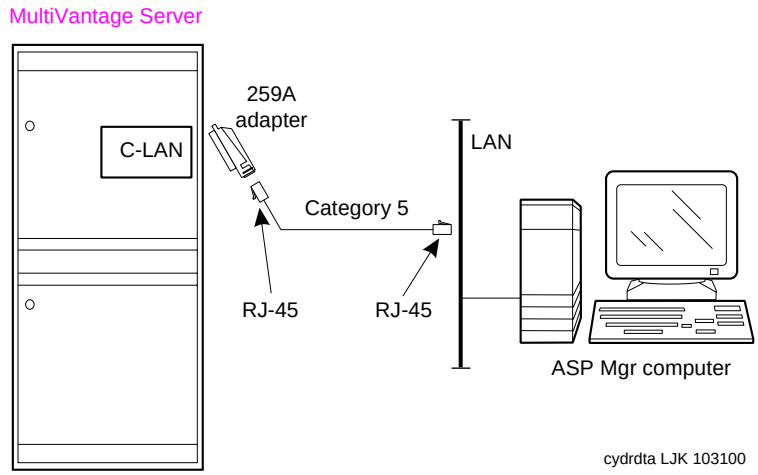
2. The main server(s) and the WSPs that you want to work with ASP Manager must all be on the same LAN or WAN, and that must be the same LAN or WAN that supports all of the ASP Manager computers.

4 Connecting the Hardware

To function properly, Avaya™ ATM WAN Spare Processor Manager must be connected to your Avaya MultiVantage™ software servers and ATM WSPs via a C-LAN board. Figure 1 illustrates one way to connect your ASP Manager computers to your main servers and WSPs.

Connecting via CLAN Board

Figure 1. Connecting main servers and WSPs via Network



1. Connect the equipment as shown in Figure 1.

5 Preparing Servers and WSPs for ASP Manager

Before you can use Avaya™ ATM WAN Spare Processor Manager to copy translations to WSPs, the following activities must happen. A number of these activities require you to call Avaya. To avoid calling repeatedly, read all of the sections first, and then determine what activities you need Avaya to perform.

Overview

1. Install the main server and MultiVantage software, if you have not already.

   For instructions on installing main PPNs, visit http://made-easy.avaya.com and click the MCC link to view *Installation for MCC Made Easy.*

2. Install the ATM-PNC, if you have not already.

   Refer to "Installing a DEFINITY Server ATM-PNC" on page 3-1 in *ATM Installation, Upgrades, and Administration Using MultiVantage Solutions,* 555-233-124, Issue 4.

3. Install the WSPs, if you have not already.

   Refer to "Installing a WAN Spare Processor" on page 3-36 in *ATM Installation, Upgrades, and Administration Using MultiVantage Solutions,* 555-233-124, Issue 4. In addition:

   a. On the WSP, if there are only two carriers installed, make sure that the second carrier is a 'C' carrier. Chances are the PPN has duplicated SPEs, which makes the 01B carrier a processor carrier. WSPs have single processors. Once the WSPs have a copy of the PPN's translations loaded and running, SPE dup will be turned off. Therefore, in order to make use of the second carrier, it should have the 'C' p-plug connected to it on the backplane.

   b. If the WSP has 3 carriers, you can either make the second carrier a 'C' carrier (as in Step 3a, above) or you can leave the second carrier as a 'B' carrier, and simply not put any circuit packs in it. Instead, place your C-LAN circuit pack in the 'C' carrier.

4. Verify that the WSP configuration matches the main PPN configuration.

   Refer to Figure 3-11 in ATM Instal*lation, Upgrades, and Administration Using MultiVantage Solutions*., 555-233-124, Issue 4.

5. Administer the WSPs on the main server.

   Refer to "Administration" on page 3-42 in *ATM Installation, Upgrades, and Administration Using MultiVantage Solutions*., 555-233-124, Issue 4.

6. Install the C-LAN circuit pack.

   Refer to "Installing and Administering a C-LAN Circuit Pack" on page 3-49 in *ATM Installation, Upgrades, and Administration Using MultiVantage™ Solutions*, 555-233-124, Issue 4. In addition:

   a. Make sure that the C-LAN circuit pack that ASP Manager uses to connect to the PPN is in cabinet 01, preferably in the 01C or 01D carrier.

   b. Do not put the C-LAN circuit pack in the B carrier on any of the WSPs.

   c. Make sure the node names of the C-LAN circuit packs are the same for all of the C-LAN circuit packs on both the PPN and all WSPs. Use the `change node-names ip` command.

   d. Do not attempt to enter the node names of the WSPs' C-LAN circuit packs in the Node Names screen of the PPN. (It is not possible, even if you perform Step c, above.)

7. Test C-LAN connectivity to the LAN.

   Refer to "Testing the external connection to the LAN" on page 3-54 in *ATM Installation, Upgrades, and Administration Using MultiVantage Solutions*, 555-233-124, Issue 4. In addition:

   a. Make sure you have C-LAN SAT access to the PPN and each WSP.

   b. The PC that will be running the ASP Manager server should also be able to access each of these C-LAN circuit packs.

c. If necessary, for troubleshooting purposes, you can install a copy of Avaya Site Administration on the PC that will be running the ASP Manager server.

8. If you want to use Access Security Gateway (ASG), have Avaya enable it on your servers and/or WSPs. (page 25)

9. Have Avaya turn on the `System Management Data Transfer Only?` customer option on each server and WSP that you plan to use with ASP Manager. (page 27)

10. On each main server and WSP, create a login that ASP Manager can use to upload or download translations, or use existing logins that have these permissions. If you create new logins for this purpose, have Avaya enable them. (page 27)

11. On each main server and WSP, create a login that ASP Manager can use for all other administration, or use existing logins that have this permission. If you create new logins for this purpose, have Avaya enable them. (page 30)

After you complete the above preparations, you can install and configure ASP Manager, as described in the next chapter. (page 41)

Enabling ASG on Your Main Servers

ASG is an optional security feature that prevents unauthorized persons from accessing the MultiVantage software on your servers and WSPs. To determine if the ASG feature is enabled on your server or WSP, complete the following steps:

1. Log in to the MultiVantage software on your server or WSP.

2. Type **display system-parameters customer-options** and press Enter.

If the `Access Security Gateway` field has a value of **y**, then your server has the ASG feature.

If your system does not have the ASG feature enabled, and you want it, you can order it by completing the following steps:

1. Call Avaya (see numbers below).

2. Give Avaya your Installation Location (IL) number.

3. Request that Avaya turn on the ASG customer option.

If you are calling from the United States...	Dial...
CT, DC, DE, FL, GA, MA, ME, NC, NH, NJ, NY, PA, RI, SC, VA, VT, WV	1-800-632-0900
AL, AR, IA, IL, IN, KS, KY, LA, MI, MN, MO, MS, ND, NE, OH, SD, TN, WI	1-800-572-0036
OK, TX	1-800-527-6889
AK, AZ, CA, CO, HI, ID, MT, NM, NV, OR, UT, WA, WY	1-800-829-8888

If you are calling from outside the United States, contact your Avaya representative or dealer.

Enabling MultiVantage Software to Work with ASP Manager

The MultiVantage software on your server or WSP will not work with ASP Manager until Avaya turns on the DNA customer option on that system.

To determine whether your system has the `System Management Data Transfer Only?` customer option turned on, complete the following steps:

1. Log in to the MultiVantage software on the "main" server or WSP.
2. Type **display system-parameters customer-options** and press Enter.

   If the `System Management Data Transfer Only?` field has a value of **y**, then the option is enabled, and your server will work with ASP Manager.

If this option is not enabled, you can enable it as follows:

1. Call Avaya (see numbers above).
2. Give Avaya your Installation Location (IL) number.
3. Request that Avaya turn on the `System Management Data Transfer Only?` customer option.

Creating the Upload/Download Login

On each "main" server and WSP that you will be using with ASP Manager, there must be a login that ASP Manager can use to upload translations (from the "main" server to the ASP Manager server), or download translations (from the ASP Manager server to the WSPs). MultiVantage software allows only one login with this permission.

Do you need to create this login?

Any login that has permissions to issue the **upload, download translations,** and **logoff** commands will work. If an appropriate login already exists on the main server and WSPs, then go to "Creating the Administrative Login'' on page 30.

If you need to create this login

The following procedure creates a login that, for security purposes, can only issue the **upload, download translations,** and **logoff** commands. To create the login, complete the following steps:

*** Note:** To perform this task, you must have permissions in the MultiVantage software to add and change logins.

1. Log in to the MultiVantage software.
2. At the command line, enter **add login** <**name**>

   Where <name> is the word you want to use as the login.
3. Enter your password.
4. Verify that the `Login Type:` field is set to **customer**.
5. Verify that the `Service Level:` field is set to **non-super-user**.
6. In the `Login's password:` field, enter the password that you want to associate with the login.
7. In the `Reenter Login's password:` field, enter the password again.
8. If you want this login to use ASG, then in the `Access Security Gateway?` field, enter a **y** and complete the fields on page 2 of the form (described in the following table).

   If you do not see this field, your server does not have the ASG feature enabled. To enable it, see "Enabling ASG on Your Main Servers" on page 25.

Field	Description
Blocked	Enter **y** to temporarily disable the login ID from accessing this system through ASG.
System Generated Secret Key?	To use ASG, either you or the MultiVantage software on this system must generate a Secret Key, which you must enter on this server and in ASP Manager when you are configuring it. Enter a **y** to have the MultiVantage software on this server generate the Secret Key.

Field	Description
Secret Key	**If you want to create your own Secret Key, enter it in this field. Be sure to note the Secret Key; you will need it to configure ASP Manager and/or any response generation devices.** **The Secret Key must conform to the following requirements:** It must be 20 digits long. Each digit must be between 0 (zero) and 7, inclusive. The last number must be 0 (zero). The next-to-last number must be 0 (zero), 2, 4, or 6.
Expiration Date	To disable this login after a certain date, enter the date in this field. If you enter a value in the Number of Sessions field, then the login will be disabled based on whichever criteria is satisfied first.
Number of Sessions	Enter the number of times this login ID can be used to access this system (between 1 and 999). If you enter a value in the Expiration Date field, then the login will be disabled based on whichever criteria is satisfied first.
Restrict Days of Week	Enter **y** to restrict this login from accessing this system on the specified day of the week.
Restrict From Time and Restrict To Time	Enter the time interval during which this login ID is blocked from accessing this system.

9. Press Enter to submit the form.

10. Call Avaya. (page 25)

11. Give Avaya your Installation Location (IL) number.

12. Give Avaya the login name you just added, and request that they enable the `System Management Data Transfer Only?` field on the first page of the Change Permissions form for your MultiVantage software.

*** Note:** Only Avaya can set the `System Management Data Transfer Only?` field to **y**. ASP Manager will not work with your server until this is enabled.

Creating the Administrative Login

ASP Manager needs a login that it can use to issue all of the commands described in "Downloading Translations to the WSPs" and “Limited Administration of WSPs’’ on page 14. The ASP Manager administrative login is what ASP Manager uses to make changes to the translations in your MultiVantage software. ASP Manager cannot make changes to the translations if you do not create this login.

Do you need to create this login?

Any login will work that has permissions to issue the commands **status atm wsp, reset system 4 disk (for DEFINITY ECS Release 9 systems), reset system 3 disk preserve-license (for DEFINITY ECS Release 10 and higher systems), list config all, busyout atm pnc 1, remove atm pnc 1, save translations,** and **logoff**. If an appropriate login already exists on the main server and WSPs, then skip the remainder of this section.

If you need to create this login

To create the administrative login, you must have permissions in the MultiVantage software to add and change logins.

1. Access the MultiVantage System Administration screens.
2. At the command line, enter **add login *<name>***

   Where <*name*> is the word you want to use as the login. If your location uses DNA, do *not* reuse DNA logins for this purpose.
3. Enter your password.
4. Verify that the `Login Type:` field is set to **customer**.
5. Verify that the `Service Level:` field is set to **super-user**.
6. In the `Login’s password:` field, enter the password that you want to associate with the administrative login.
7. In the `Reenter Login’s password:` field, enter the password again.

8. If you want this login to use ASG, then in the `Access Security Gateway?` field, enter a **y** and complete the fields on page 2 of the form.

   If you do not see this field, your server does not have the ASG feature enabled. To enable it, see "Enabling ASG on Your Main Servers'' on page 25.

Field	Description
Blocked	Enter **y** to temporarily disable the login ID from accessing the server through ASG.
System Generated Secret Key?	To use ASG, either you or the MultiVantage software on this server must generate a Secret Key, which you must enter on the server and in ASP Manager when you are configuring it. Enter a **y** to have the MultiVantage software on this server generate the Secret Key.
Secret Key	**If you want to create your own Secret Key, enter it in this field. Be sure to note the Secret Key; you will need it to configure ASP Manager and/or any response generation devices.** **The Secret Key must conform to the following requirements:** It must be 20 digits long. Each digit must be between 0 (zero) and 7, inclusive. The last number must be 0 (zero). The next-to-last number must be 0 (zero), 2, 4, or 6.
Expiration Date	To disable this login after a certain date, enter the date in this field. If you enter a value in the Number of Sessions field, then the login will be disabled based on whichever criteria is satisfied first.
Number of Sessions	Enter the number of times this login ID can be used to access the MultiVantage software on this server or WSP (between 1 and 999). If you enter a value in the Expiration Date field, then the login will be disabled based on whichever criteria is satisfied first.

Field	Description
Restrict Days of Week	Enter **y** to restrict this login from accessing the MultiVantage software on this server or WSP on the specified day of the week.
Restrict From Time and Restrict To Time	Enter the time interval during which this login ID is blocked from accessing the MultiVantage software on this server or WSP.

9. Press Enter to submit the form.

10. At the command line, enter **change permissions <*name*>.**

    Where <*name*> is the word you used as the login in Step 2. The system displays the Command Permission Categories form.

11. Set the fields to **y** to enable ASP Manager to perform the listed activity.

    Use the table below to decide which of the fields to set to **y**.

    The fields listed in the following table are for a basic configuration. Your MultiVantage software may display more than the following fields. For help setting those fields, refer to the *Administrator's Guide for Avaya MultiVantage™ Software*, 555-233-502.

If this field is set to Y...	Then...
Display Admin and Maint Data?	Setting this field to **y** allows ASP Manager to issue **status atm wsp** and **display circuit pack** commands. **The login you use for ASP Manager administration must have this field set to y for ASP Manager to work.**
System Measurements?	Since this field applies only to vs/si systems, and C-LAN boards are not available for vs/si systems, this field is irrelevant for ASP Manager purposes.
System Mgmt Data Transfer Only?	**Only Avaya can set this field. You should have them set it to y only for your ASP Manager Upload/Download login.**

If this field is set to Y...	Then...
Administer Stations?	ASP Manager can issue add, change, duplicate, or remove commands for stations, data modules, and associated features, such as abbreviated dialing, vectors, and routing tables. You do not need to set this field to **y** for ASP Manager to work.
Administer Trunks?	ASP Manager can issue commands to administer AAR/ARS, trunk groups, remote access, and route patterns. You do not need to set this field to **y** for ASP Manager to work.
Administer Features?	Setting this field to **y** allows ASP Manager to issue **remove atm pnc** and **save translations** commands. **The login you use for ASP Manager administration must have this field set to y for ASP Manager to work.**
Administer Permissions?	ASP Manager can issue commands to administer logins and command permissions. You do not need to set this field to **y** for ASP Manager to work.
Restricted Objects?	You can specify any objects that you want ASP Manager not to be able to access, like stations, trunks, or hunt groups. You do not need to set this field to **y** for ASP Manager to work.
Maintain System	Setting this field to **y** allows ASP Manager to issue **reset system 3 preserve-license** and **busyout atm pnc** commands. **The login you use for ASP Manager administration must have this field set to y for ASP Manager to work.**

12. Press Enter.
13. Call Avaya. (page 25)
14. Give Avaya your Installation Location (IL) number.
15. Give Avaya the login name you just added, and request that they enable the `Maintain System` field on the Change Permissions form for the MultiVantage software on this system.

*** Note:** Only Avaya can set the Maintain System field to y. ASP Manager will not work with your server until this is enabled.

6 Installing ASP Manager

Installation Prerequisites

Before you install Avaya™ ATM WAN Spare Processor Manager, be sure that the computers you plan to install it on meet the hardware requirements listed in “Understanding System Requirements’’ on page 19.

ASP Manager requires a functioning LAN or loop-back host to operate. The instructions in this section assume that your LAN is fully operational and that all ASP Manager computers can ping each other. In addition, to install ASP Manager, you must have a Windows login with Administrator privileges.

If your company has a support agreement with Avaya, then you need to install a modem and a copy of Symantec’s pcAnywhere on all computers that will host ASP Manager software. pcAnywhere enables Avaya service personnel to remotely troubleshoot and correct problems on your system. For the required version number of pcAnywhere, see “Understanding System Requirements’’ on page 19. Once pcAnywhere is installed, contact Avaya’s Technical Service Center (TSC) (from the US: 1 800 242 2121; from outside the US, contact your Avaya representative or dealer.) Then give them the phone numbers or IP addresses they should use to access your ASP Manager computers.

Finally, if you want to use ASP Manager’s E-mail notification feature, then the ASP Manager server computer must have access to the SMTP mail server that would be sending the E-mail.

Understanding pcAnywhere Security

Before you install a copy of Symantec's pcAnywhere on any of your computers, read this section.

You are responsible for the security of your data network and for preventing unauthorized individuals from accessing it. Therefore, exercise caution when using pcAnywhere. Having it installed does not pose a security risk; it must be up and running, and be configured to receive calls, before a remote user can enter the system. In addition, pcAnywhere offers a number of security features.

Follow these guidelines to protect PCs with pcAnywhere installed:

1. Unplug the modem from the phone jack when pcAnywhere is not in use.
2. Only run pcAnywhere when necessary.
3. Do NOT publish the phone number for the modem that people use to access the computer.
4. Change your password after Avaya personnel leave your site and after Avaya personnel terminate a remote service session.
5. Configure the following pcAnywhere security options:
   - Require login names for callers.
   - Make passwords case sensitive.
   - Log all failed connection attempts.
   - Set a maximum number of login attempts per call.
   - Allow time to enter the complete login.
   - Disconnect if inactive.
6. Configure pcAnywhere to log remote-call and online sessions.

For more information on pcAnywhere, including acquisition and security, visit the following web site:
http://www.symantec.com/pcanywhere/index.html

Installing ASP Manager

To install ASP Manager, you must use a Windows login that has Administrator privileges. Then, complete the following steps:

1. Shut down all applications running on the computer.
2. Insert the Avaya VisAbility Management Suite: Network Management Windows Server CD into the CD drive.

   Wait a moment for the CD browser window to appear automatically.
3. Click Install Network Management Products.

   The installation program extracts the necessary files.
4. At the Welcome window, click **Next.**
5. Specify the folder where you want to install the management suite and click **Next.**
6. Click the plus sign icon next to ATM WAN Survivable Processor Manager.

   The installation program displays the ASP Manager client and server options.
7. Put a check mark by the ASP Manager components you want to install and click Next.

   — Client: This can be installed on one or more computers. It is installed on the server computer automatically when you install the server software.

   — Server: This must be installed on a single computer only.

   If you plan to install both client and server, click server. This installs both.
8. Verify the information in the "Check Setup Information" screen and click Next.

   Click Back to correct any information, and click Next when you are ready to install the selected applications. The installation program copies the necessary files to your hard drive.
9. Read the license agreement and if you accept the terms and conditions, click **Yes.**

10. Specify the computer on which to install the ASP Manager server software.

    You can type the computer name or the fully-qualified domain name (FQDN). The FQDN is the host name followed by the IP domain name. For example: `dnapc1.department.company.com.`
    If you do not know the IP address, you can find it as follows: choose **Start>Settings>Control Panel,** double-click **Network**, click the **Protocols** tab, select **TCP/IP,** click the **Properties** button, and then click the **IP address** tab.

*** Note:** Note the information you enter here; you will need it when you install the client.

11. Specify the number of the port through which the ASP Manager server software will communicate with the ASP Manager clients and other devices, and click **Next.**

    ASP Manager installs the appropriate software.

12. If you selected Client in Step 7, enter the computer name or FQDN, and the port number, of the ASP Manager server computer.

    You recorded this information when you installed the ASP Manager server software.

13. Restart the computer by selecting "Yes, I want to restart my computer now."

    When the computer restarts, the ASP Manager server software will start automatically. When the client is first started, it displays the first screen that must be completed to configure ASP Manager. See "Specifying the Main Server" on page 42.

14. Click **OK.**

    You can now install the ASP Manager client on other computers in your network, using the same process.

Shutting Down ASP Manager

Before you uninstall ASP Manager, you must shut down ASP Manager. To do so, you must have access to the ASP Manager server PC. To shut down ASP Manager, complete the following steps:

1. Exit the client if it is open by choosing File>Exit.
2. Open an MS-DOS window.

   Most likely, you can access this from the Windows Start menu, by choosing Start>Programs, MS-DOS Command Prompt.
3. At the prompt, type **net stop "WSP Background Processes"**
4. Wait a minute for the ASP Manager server to shut down.

   The MS-DOS window will display a message that the services are stopping.

ASP Manager will not notify users when it has shut down, but users *will* receive an error to this effect if they attempt to perform an action that requires the ASP Manager server. The ASP Manager server software will automatically start again after you reboot the ASP Manager server.

Starting ASP Manager

Starting the ASP Manager Server

Once ASP Manager server software has been installed, the ASP Manager server software starts automatically each time you restart the computer it is installed on, and it runs continuously unless you stop it manually. If you have stopped it manually and you want to restart it without restarting your computer, complete the following steps:

1. Open an MS-DOS window.

   Most likely, you can access this from the Windows Start menu, by choosing Start>Programs, MS-DOS Command Prompt.
2. At the prompt, type **net start "WSP Background Processes"**
3. Wait a minute for the ASP Manager server to start.

   The MS-DOS window will display a message that the services were started successfully.

Starting the ASP Manager Client

To start the client, choose **Start>Programs>Avaya>ATM WAN Survivable Processor Manager.** If you installed ASP Manager under a different Program Group name, select that instead.

Uninstalling ASP Manager

To remove ASP Manager from a computer, you must have Windows Administrator privileges.

1. If the ASP Manager client is running on this computer, close it.
2. From the Windows Start menu, select **Settings>Control Panel.**
3. Double-click **Add/Remove Programs.**
4. On the **Install/Uninstall** tab, highlight ASP Manager and click the **Add/Remove** button.
5. Confirm that you want to remove the selected application.

   If the selected application uses software components that are also used by another application, the system displays the Remove Shared File? dialog box. If you know that the shared file is not being used by any other application, you can delete it by clicking **Yes** or **Yes to All.**
6. Click **OK.**

7 Configuring ASP Manager

To configure Avaya™ ATM WAN Spare Processor Manager, you will perform the following main steps. The rest of this chapter explain these steps in detail.

1. Set the PC's time.
2. Start ASP Manager. (page 40)
3. Specify the "main" server in the WSP network.
4. Provide connection and login information about each WSP.
5. (Optional) Specify E-mail notification information.

Setting the PC's Time

After ASP Manager is installed, when people use it to schedule downloads to occur from a "main" server to its WSPs, ASP Manager will execute the download according to the date and time that the user specifies. However, this date and time is the date and time at the PC where the ASP Manager server software is installed. For this reason, it is highly advantageous for the ASP Manager server PC to have the correct date and time set in the operating system.

To do so, complete the following steps:

1. Choose **Start>Settings>Control Panel** on your Windows PC.
2. In the Control Panel, double-click **Date/Time.**
3. Specify the date, time, and time zone using the dialog box.
4. Specify whether to automatically adjust for daylight savings time.
5. Click **OK.**

Specifying the Main Server

The first time you start ASP Manager, it will ask you to specify the "main" server. To do so, complete the following steps:

1. Enter the server name.
2. Enter the server's IP Address.

   To determine the server's IP address, you can ask your LAN/WAN administrator, or you can gather this information from the server itself, as follows:

   a. Log in to the MultiVantage software on that server using your favorite system administration tool.

   b. Type **display ip-interface** and press Enter.

   c. Look for the C-LAN board and note the value in the `Node Name` field.

   d. Then type **list node-name** and press Enter.

   e. Look for the Node Name you noted from the previous screen.

      Next to it will be the IP Address for that C-LAN board.

3. Enter the number of the IP Network port on this server's C-LAN board that ASP Manager should use to communicate with this server.

   This is a IP Network port number (for example, 5000), not a "switch" port address. To determine the IP Network port, you can ask your LAN/WAN administrator, or you can gather this information from the MultiVantage software itself, as follows:

   a. Log in to the MultiVantage software on this server using your favorite system administration tool.

   b. Type **display ip-interfaces** and press Enter.

   c. Look for the C-LAN board and note the value in the `Node Name` field.

   d. Then type **display ip-services** and press Enter.

   e. In the `Local Node` field, look for the Node Name you noted from the previous screen.

      Next to it, in the `Local Port` field, will be the IP Network port for that C-LAN board.

4. Check or clear the "Continue if save translation fails?" check box.

   Before copying translations, ASP Manager issues the **save translations** command on the main server. If you check this box, ASP Manager will copy the translations even if the **save translations** command fails on the "main" server. If you leave this box empty, ASP Manager will abort the copy if the **save translations** command fails.

5. In the Upload/Download area, and in the Administration area, specify the login IDs and passwords of the Upload/Download and Administration logins that you created (on page 27 and page 30) for the main server.

6. Check or clear the **Use ASG** check box.

   ASG is an optional security feature in your MultiVantage software. To determine if ASG is enabled on the main server, see page 25. If you set up the logins on your main server to use ASG, check this box. Otherwise, leave it empty.

7. Click **Test Connectivity.**

   Clicking this button tests the connection between the ASP Manager server and the main server, for both the Upload/Download login and the Administration login. If you encounter any error messages, see "Troubleshooting'' on page 48. If there are no errors with connectivity, ASP Manager will display the name, number, and link status of each WSP in the network, in the "Administration" tab of the main ASP Manager window. ASP Manager got this information from the main server (assuming that someone has already entered this information in the main server as part of Step 5 on page 24).

8. Click **OK.**

   This saves the information that you entered in this dialog box.

Specifying WSP Information

To finish configuring ASP Manager, you must supply login and password information about each WSP, as follows:

1. Double-click a WSP from the list on the "Administration" tab.

   ASP Manager displays the WSP Properties dialog box. The name of the WSP is displayed.

2. Enter the IP address, port, login IDs, passwords, and ASG information for this WSP, in the same way you did for the main server.

3. Specify the WSP Take Over Time.

   This is the amount of time you want this WSP to wait in the event of a failure on the "main" server, before the WSP comes up as the main processor.

4. Click **Test Connectivity.**

   This tests the connection between the ASP Manager server and the selected WSP, for both the Upload/Download login and the Administration login. If you encounter any error messages, see "Troubleshooting'' on page 48.

5. Click **OK.**

Setting Up E-mail Notification

Release 1.1 introduces an E-mail notification feature. To set up this feature, complete the following steps:

1. Choose Tools>Email Notification Configuration.
2. Specify the IP address of the (SMTP) E-mail server that ASP Manager can send messages to.
3. Specify whether or not this E-mail server requires authentication, and if it does, enter the login name and password that ASP Manager should use to send messages.
4. Specify under which conditions ASP Manager should send messages.
5. Specify the E-mail address where ASP Manager should send messages.
6. To do so, click Add, enter the E-mail address, and click OK. Repeat to add more.
7. Click OK.

Using ASP Manager

Refer to ASP Manager's embedded online help for instructions on how to use the product.

8 Testing the Installation

To test that you have correctly installed and configured all the components of Avaya™ ATM WAN Spare Processor Manager, complete the following sections.

Testing Connections

To test ASP Manager's connections to supported devices, complete the following steps:

1. Start ASP Manager (page 39).
2. Select a server on ASP Manager's main screen.
3. Choose **Tools>Validate.**

   ASP Manager attempts to connect to the main server, and if it is able to log in, it issues the **status atm wsp** command. If the WAN Processor Role field contains any value other than "pending," then ASP Manager can display the name, number, and link status of each WSP in the network.

Troubleshooting

In the table below, find the symptoms in the left column and follow the instructions in the right.

Message		Possible Causes and Solutions
Attempt to remove non-existing or un-writable file <translations file name>.	<1>	After ASP Manager uploads translations from a main server, it makes a copy for each WSP and then, before it downloads the copy to each WSP, it modifies the translations slightly so they will work on the WSP. This message can occur when ASP Manager attempts to rename the uploaded translations, if: • there was an error in uploading the translations and, in fact, no upload file really exists on the ASP Manager server. • there was an error in the file system that either a) prevented the upload file from being written to the ASP Manager server hard drive, or b) prevented the upload file from being copied and renamed to the WSP file name. • you or someone else changed your permissions after the ASP Manager server software was installed and configured. • whoever set up the directory on the ASP Manager server where the translations are uploaded didn't share the directory with you.
Cannot replace file <new translation file name>		See <1>.
Error reading schedule type <type> starting schedule now	<2>	You should never receive this message. This error would appear if ASP Manager is running a job that has a scheduling option that is no longer supported by ASP Manager. For example, if today's release supports "Run Now," "Run Once," "Run Daily," and "Run Weekly," and a subsequent release supports only 3 options, then you might see this message. In that case, you can simply click the Schedule tab and either alter the schedule or leave it as is and click Submit. By resubmitting the job, you will clear the error.

Message		Possible Causes and Solutions
Failed opening connection to <server> with <connection state>.	<3>	ASP Manager may encounter problems connecting to a server or WSP for any of the following reasons:· • the IP address, Network Port Number, default Gateway, or Subnet Mask in ASP Manager no longer matches what has been administered in the server or WSP, or on the LAN/WAN. • the login ID and password (and possibly ASG Secret Key) in ASP Manager no longer matches what has been administered in the main server or WSP.· • a physical connection has been severed. • the main server or WSP is down. • the part of the ASP Manager software that establishes a connection with a main server or WSP is experiencing problems.
Failed to create connection object for <system> <exception description>.	<4>	This message can occur if ASP Manager experiences difficulty building a connection file it uses to make a connection with the named device. Contact Technical Support, tell them what you were doing when the error occurred, and give them the exception description.

Message		Possible Causes and Solutions
Failed to retrieve ATM PNC board location from <WSP> <exception description>. Failed to run atmwsp command on <system> <exception description>. Failed to run busyout atm pnc command on <WSP> <exception description>. Failed to run remove atm pnc command on <WSP> <exception description>. Failed to run reset system 3 command on <server> <exception description>. Failed to run save translation command on <server> <exception description> Failed to set system parameters for <WSP> <exception description>	<5>	All of these are errors indicate that ASP Manager was unable to issue a command on the listed server or WSP. Information in the exception description may give a clue. Possible reasons include: • Someone upgraded the MultiVantage software but didn't upgrade ASP Manager, or vice versa (post Release 9) • There are problems with physical connectivity. • Someone entered the wrong connection information in ASP Manager or on the server or WSP (IP Address, Port, Subnet Mask, Gateway, login ID, password, or ASG Secret Key). • Someone changed the connection information in ASP Manager but not on the server or WSP, or vice versa. • There are problems with the permissions assigned to the ASP Manager login ID(s) that you created on the given server or WSP. You can either troubleshoot the problem yourself using the information provided in the exception description, or contact Technical Support and give the exception description to them.
File <translations file name> does not exist or is un-writable.See <1>		See <1>.
No network <network file path> or modem <file path + system> connection file(s) exist.	<6>	ASP Manager creates the network connection file when you install ASP Manager. Users cannot configure or modify this file. You should never receive this message. If you do, the recommended process is to reinstall the ASP Manager server software. If that doesn't work, call Technical Support and give them the exception description.
The connection definition file <definition file> does not exist.	<7>	ASP Manager creates the connection definition file when you install ASP Manager. Users cannot configure or modify this file. You should never receive this message. If you do, the recommended process is to reinstall the ASP Manager server software. If that doesn't work, call Technical Support.

Message		Possible Causes and Solutions
The WSP returned an unknown Link Status <state>.	<8>	This message is purely informational. ASP Manager can upload and download translations regardless of what the value in the Link Status field.
Schedule for <main server> submitted.	<9>	This message appears when you click the Submit button on the Schedule tab of ASP Manager's main screen. It simply confirms that ASP Manager has received the change you specified. It does NOT mean that the job is starting. Rather, the job will start when you specified for it to start.
Scheduled task failed while: uploading translations. Scheduled task failed while: verifying WSP list – this message indicates a fatal condition which occurred during the upload translations step. Scheduled task failed while: uploading translations: Save translations failed for <main server>. <main server> set to stop task if translations save failed.	<10>	All of these errors indicate that ASP Manager was unable to copy translations from the main server to the ASP Manager server. The only difference between them is when in the upload process the error was detected. Contact Technical Support.
Scheduled task pending. Start time is: <date> -	<11>	This message appears if you change a schedule, or when a schedule completes and it is set to run periodically.
Scheduled task started.	<12>	This message appears immediately before ASP Manager begins copying translations from the main server to the ASP Manager server. This message will stay in the history log until the history log fills and begins to overwrite the first entries.

Message		Possible Causes and Solutions
Translations download processing for <WSP> has failed. <exception description>	<13>	This indicates that ASP Manager was unable to copy translations from the ASP Manager server to the given WSP. Information in the exception description may give a clue. Possible reasons for the failure include:· • Problems with physical connectivity • Incorrect or changed connectivity information (IP Address, Port, Subnet Mask, Gateway, login ID, password, or ASG Secret Key) • Problems with the permissions assigned to the ASP Manager login ID(s) on the given server or WSP. You can either troubleshoot the problem yourself using the information provided in the exception description, or call Technical Support.
Translations upload processing for <main server> has failed. <exception description>		See <10>.
Upload of translation from <main server> has failed.		See <10>.
Updated schedule not started due to currently active schedule.	<14>	This error means that ASP Manager is already in the process of copying translations from a main server to WSPs. Reschedule the job in question to start after the current job is complete.
Updated WSP list from <server> received.	<15>	Each time you start the ASP Manager client, each time you choose Tools>Validate, and each time ASP Manager starts to upload translations, ASP Manager automatically contacts the main server and verifies that ASP Manager's list of WSPs is still accurate. When the MultiVantage software returns the updated list of WSPs, ASP Manager displays this informational message.

Index