Avaya Solution & Interoperability Test Lab

Application Notes for Real Soft Remote Admin, One Manage, and NetWatch SNMP Monitor with Avaya Interactive Response 1.2 - Issue 1.0

Abstract

These Application Notes describe the interoperability compliance testing of three different Real Soft software packages with Avaya Interactive Response (IR). Real Soft Remote Admin (Version 4.1.1) is a Windows-based GUI tool that provides remote administration capabilities for Avaya Interactive Response. Real Soft OneManage (Version 4.0) is a client-server package that provides a Windows-based GUI interface for deploying and managing IVR applications on multiple Avaya Interactive Responses. Real Soft NetWatch SNMP Monitor (Version 4.0) provides fault reporting, configuration, and monitoring capabilities for one or more Avaya Interactive Responses using the industry standard SNMP protocol.

The interoperability test included installation and testing of the three products in a simulated distributed call center environment. Configuration of a firewall in this test environment is also covered. Testing concluded that all three Real Soft products; Remote Admin, OneManage, and NetWatch SNMP Monitor successfully interoperate with Avaya Interactive Response 1.2. Information in these Application Notes has been obtained through compliance testing and additional technical discussions. Testing was conducted via the Developer*Connection* Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

Integration of Avaya Interactive Response with Real Soft Remote Admin, OneManage, and NetWatch SNMP Monitor mitigates the complexities of administering, managing, and monitoring multiple instances of Avaya Interactive Response. These solutions work when multiple Avaya Interactive Responses are in one large contact center, or even when they are disbursed over multiple, geographically distributed contact centers.

For Interoperability Compliance Testing, the configuration shown in **Figure 1** was used. This test configuration has two local Avaya Interactive Responses set up in a typical contact center environment where they are administered, managed, and monitored locally. This test configuration also has two remote Avaya Interactive Responses set up in a typical distributed contact center environment where there are two firewalls (with possible NATing) between the local and remote sites.

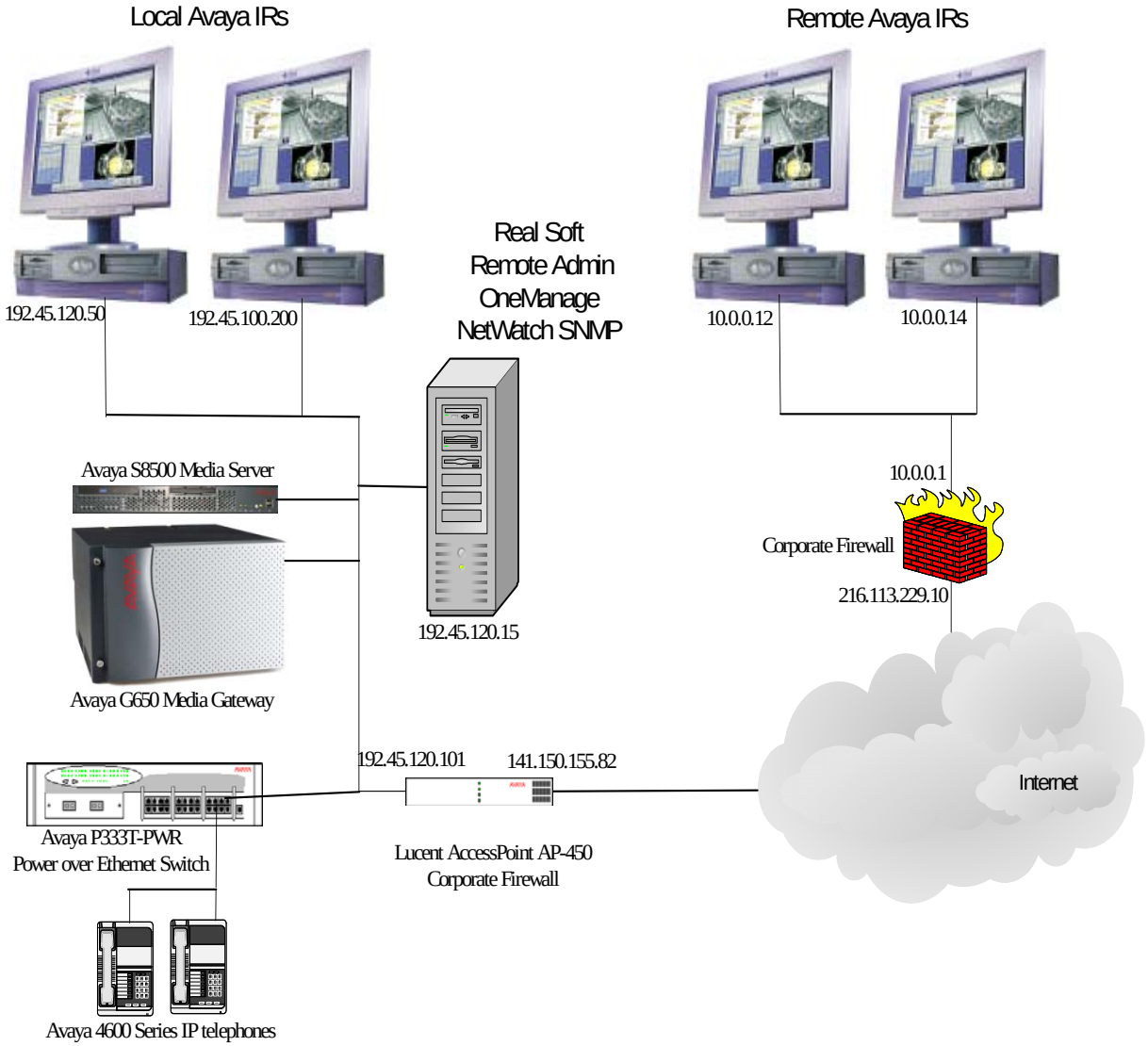


Figure 1: Test Configuration for Remote Admin with Avaya Interactive Response 1.2

In the test configuration, the two remote Avaya IRs resided at a remote corporate site behind a corporate firewall. The firewall allowed ping, SNMP, RSH, and TCP port 7000 traffic through. The two local Avaya IRs were located on two different class C subnets behind a Lucent AccessPoint 2.0 firewall. The Windows-based PC was configured on one of those two class C subnets. The major part of the network configuration was setting up the Lucent AccessPoint as a firewall to NAT the Windows-based PC and the primary OneManage IR. See **Appendix B** for the specifics on the configuration of this firewall.

To understand the test environment, it is necessary to follow the communication flows for each of the three Real Soft products. For Remote Admin, all communication is initiated by the Windows-based PC and goes between this PC and each Avaya IR. There is no communication between Avaya IRs, nor is there any traffic initiated by any of the Avaya IRs to the PC.

For NetWatch SNMP Monitor, SNMP traffic is initiated by the different Avaya IRs and goes between the Avaya IRs and the Windows-based PC loaded with the SNMP manager. Again, no NetWatch related traffic goes between the Avaya IRs.

For OneManage things are a little more complex. The Windows-based PC client initiates traffic to all of the Avaya IRs. In addition, the one primary Avaya IR initiates traffic to each of the secondary Avaya IRs. This means that in the test configuration where a local network using private IP address that contains a single local Windows-based PC hosting all three Real Soft programs along with a local primary Avaya IR (for OneManage), two different IP addresses must be NAT'ed to public IP addresses and passed by the firewall. (Note that in the test configuration all three Real Soft products were installed on the same Windows-based PC. Each product could have been installed on a different PC, as they do not interact with each other. However, doing so would have added the need for NATing these two additional PCs to two additional public IP addresses.)

2. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

Equipment	Software
Avaya Interactive Response 1.2 on SunFIRE 250.	R1.2
Avaya Interactive Response 1.2 on SunBlade 120	R1.2
Avaya S8500 Media Server with Avaya G650 Media Gateway	Communication Manager 2.1 (R012x.01.0.411.7)
Avaya P333T-PWR	3.12.1
Avaya 4600 Series IP telephones (4620IP & 4624IP)	1.8.1
Lucent AccessPoint AP450	V2.2.1 R2
Real Soft Remote Admin	4.1.1
Real Soft OneManage	4.0

Real Soft NetWatch SNMP Monitor	4.0

3. Installation

Remote Admin installs on both a Windows-based PC and the Solaris-based Avaya IR. OneManage has a client that installs on a Windows-based PC and a server that installs on the Solaris-based Avaya IR. NetWatch SNMP Monitor requires a third party SNMP manager that typically installs on a Windows-based PC along with the Real Soft server that installs on the Solaris-based Avaya IR. The third party SNMP manager used in the test configuration was SNMPc from Castle Rock (http://www.castlerock.com).

The minimum specifications for the Windows-based PC are:

- Pentium III-500mhz with 512 MB RAM, 10GB disk space, 48x CD-ROM drive, an Ethernet adapter, and a 15" VGA monitor.
- Windows XP, or 2000.

All three products can be installed on the same Windows-based PC.

3.1 Remote Admin

Installing and configuring Remote Admin for Avaya IR can be broken into four main parts: installing the software on Avaya IR, installing the software on the Windows-based PC, adding the Avaya IR machine names and IP addresses to the /etc/hosts file, and creating a new map file upon starting Remote Admin. After these four parts are complete, some sample commands can be issued to each Avaya IR to verify the program has been installed and configured correctly. These sample commands are covered in Section 5 of this document, Verification.

3.1.1 Installation on Avaya Interactive Response

#	Installation Procedure
1	The Avaya IR part of Remote Admin is distributed as a package to be installed via the Solaris **pkgadd** command. The distribution package file is called *RSIradm.pkg*. This file must first be made accessible to Avaya IR by either copying the file to Avaya IR via ftp, or by inserting the distribution CD-ROM into the Avaya IR CD-ROM drive.

2 After the *RSIradm.pkg* package file is on Avaya IR, the command:

pkgadd –d <device>RSIradm.pkg

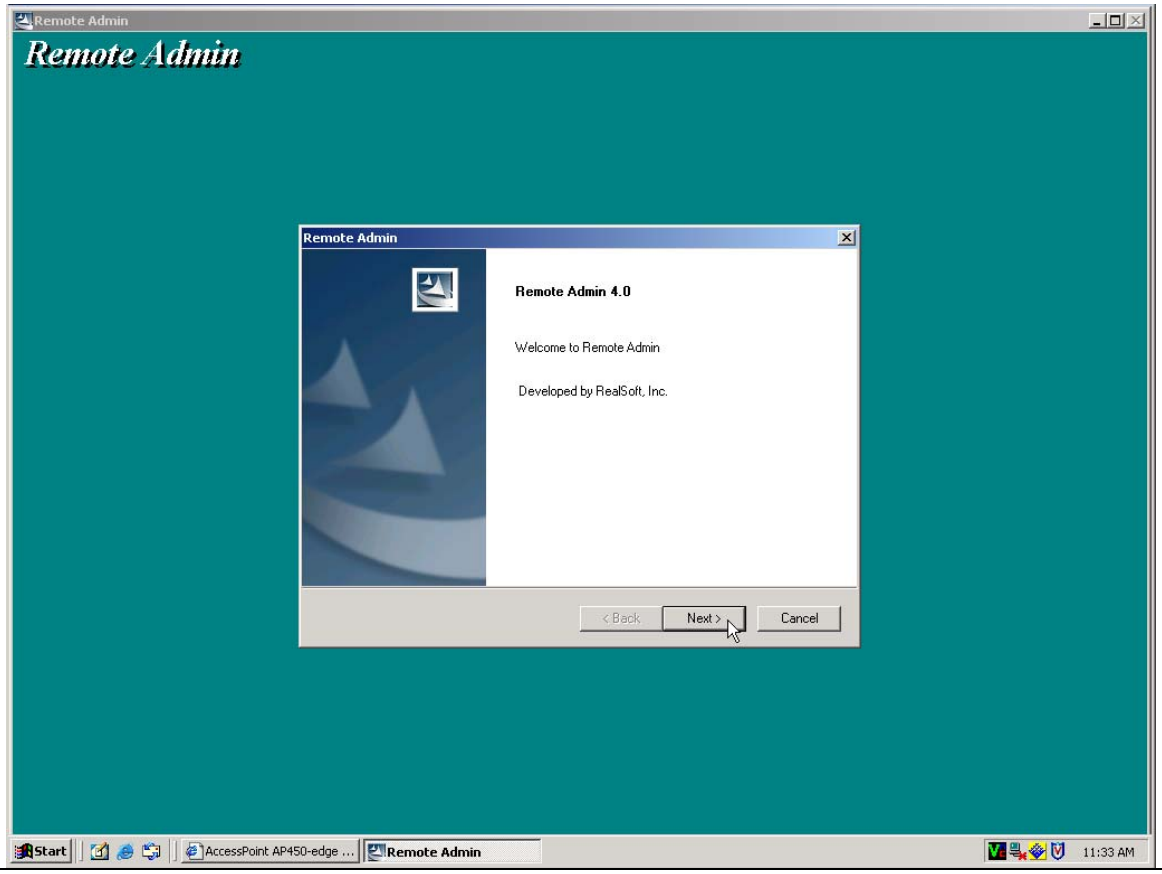
will install the package. **<device>** is either **/cdrom/cdrom/** for the CD-ROM drive, or the full path name of the directory where the *RSIradm.pkg* file was copied to by ftp.

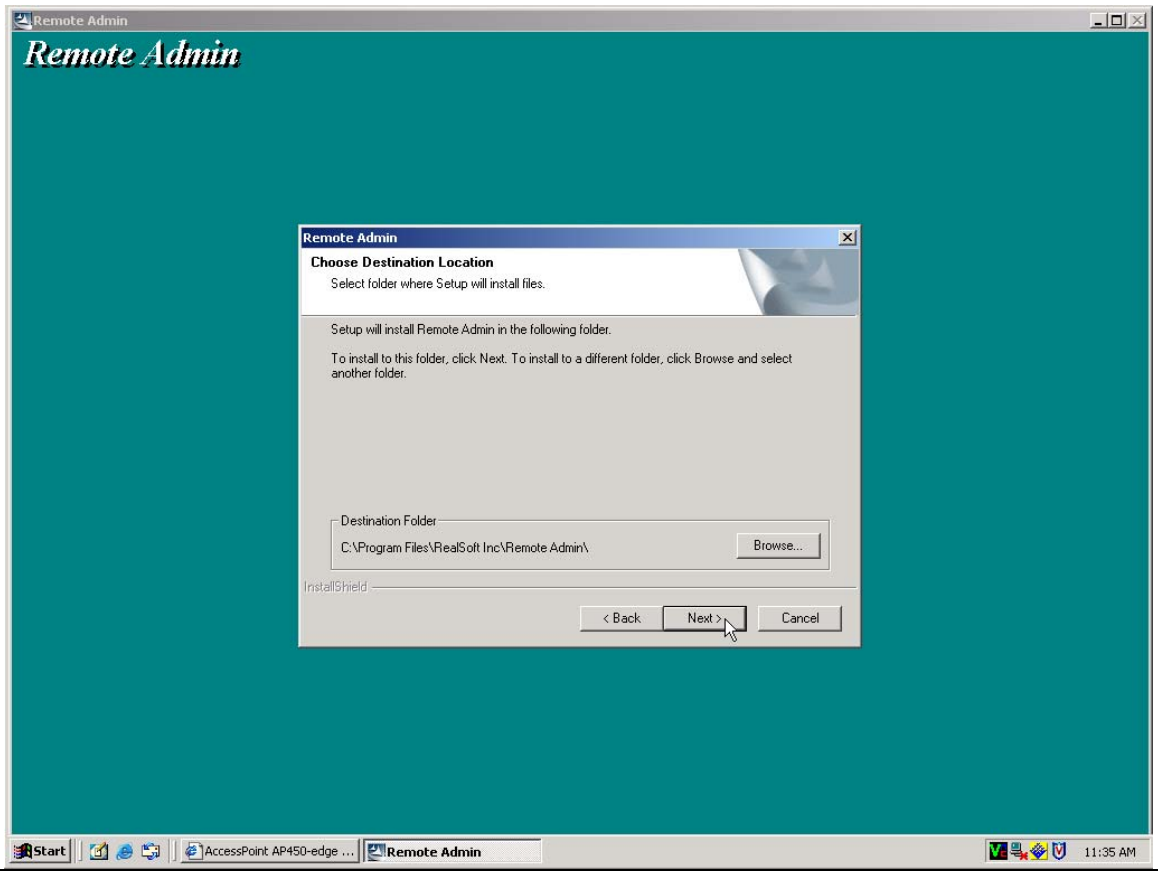
The **pkgadd** command will also run a post install script that completes the installation. A screen capture of the **pkgadd** command is shown below.

```
Realsoft - Remote Admin
(sparc) 4.1.6
Using (/opt/RSI) as the package base directory.
## Processing package information.
## Processing system information.
   4 package pathnames are already properly installed.
## Verifying disk space requirements.
## Checking for conflicts with packages already installed.
## Checking for setuid/setgid programs.

This package contains scripts which will be executed with super-user
permission during the process of installing this package.

Do you want to continue with the installation of (RSIradm) [y,n,?] y

Installing Realsoft - Remote Admin as (RSIradm)

## Executing preinstall script.
## Installing part 1 of 1.
/opt/RSI/cfg/nwoam.cfg
/opt/RSI/oam/NWOAMReinit
/opt/RSI/oam/NWOAMStart
/opt/RSI/oam/NWOAMStatus
/opt/RSI/oam/NWOAMStop
/opt/RSI/oam/NWOamAgent
/opt/RSI/oam/OAMLic
/opt/RSI/oam/bandr.res
/opt/RSI/oam/nwasaichan.sh
/opt/RSI/oam/nwasaidom.sh
/opt/RSI/oam/nwasaistat.sh
/opt/RSI/oam/nwasaiver.sh
/opt/RSI/oam/nwass
/opt/RSI/oam/nwbus.sh
/opt/RSI/oam/nwchansvc.sh
/opt/RSI/oam/nwcus1rpt.sh
/opt/RSI/oam/nwcus2rpt.sh
/opt/RSI/oam/nwcus3rpt.sh
/opt/RSI/oam/nwcus4rpt.sh
/opt/RSI/oam/nwcus5rpt.sh
/opt/RSI/oam/nwdb.sh
/opt/RSI/oam/nwdispsvc.sh
/opt/RSI/oam/nweqpoptcard.sh
/opt/RSI/oam/nwgetcmd.sh
/opt/RSI/oam/nwgetmsg.sh
/opt/RSI/oam/nwhlist.sh
/opt/RSI/oam/nwhost.sh
/opt/RSI/oam/nwmsg.sh
/opt/RSI/oam/nwmsgadm.sh
/opt/RSI/oam/nwnumsvc.sh
/opt/RSI/oam/nwoam.sh
/opt/RSI/oam/nwoamcmd.dat
/opt/RSI/oam/nwostart
/opt/RSI/oam/nwrenum.sh
/opt/RSI/oam/nwsdlc.sh
/opt/RSI/oam/nwspfunc.sh
/opt/RSI/oam/nwstream.sh
/opt/RSI/oam/nwtkr.sh
/opt/RSI/oam/nwvsstat.sh
/opt/RSI/oam/nwvstopimm.sh
/opt/RSI/oam/nwvxml.sh
/opt/RSI/oam/postinstall.sh
/opt/RSI/oam/preremove.sh
/usr/local/bin/nwoamenv
[ verifying class (none) ]
## Executing postinstall script.

Installation of (RSIradm) was successful.
devconir280(root)#
```

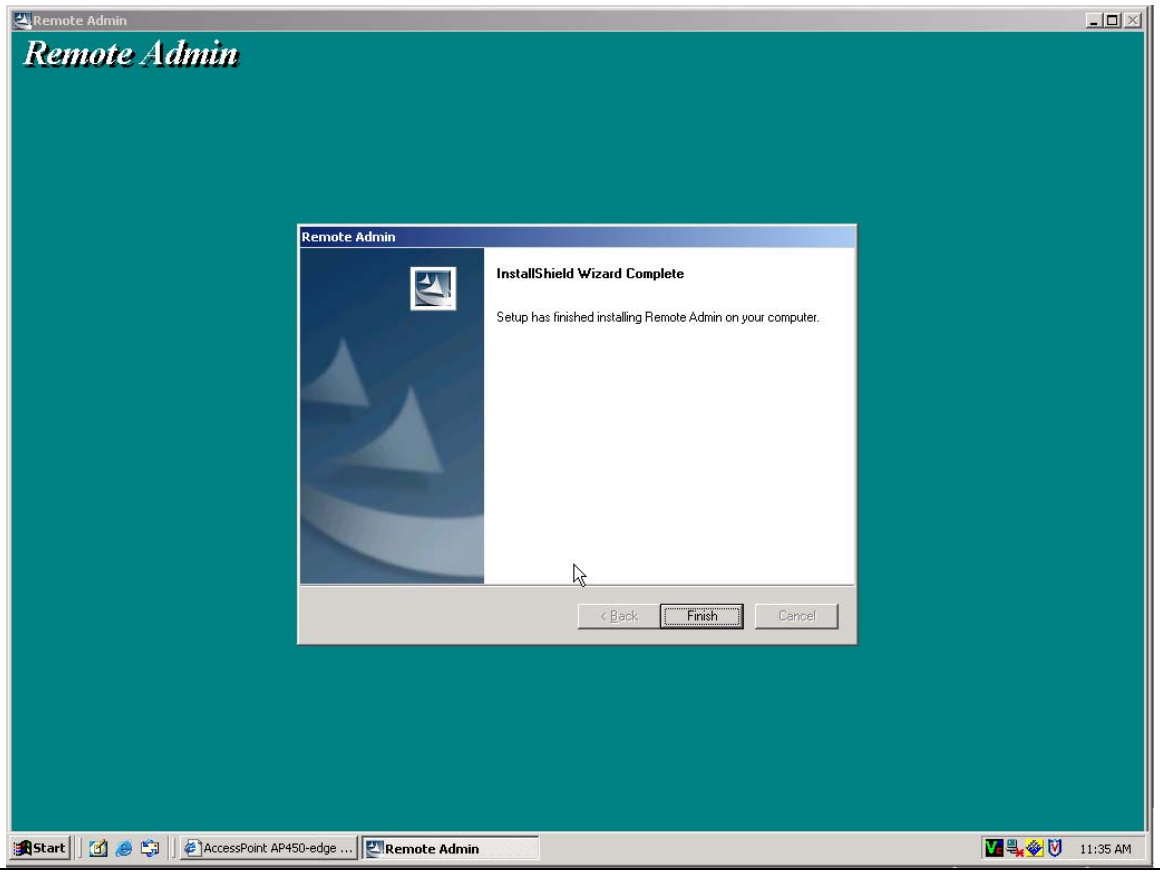
Refer to **Appendix A** for how to remove remote Admin from Avaya IR, if necessary.

3.1.2 Installation on Windows-based PC

#	Installation Procedure
1	The Windows-based PC portion of Remote Admin is distributed on a CD-ROM. Insert this CD-ROM in the CD-ROM drive of the Windows-based PC. If autorun is enabled, the setup program will start automatically. If not, browse to the CD-ROM drive, and select and run the setup.exe file.
2	A splash screen will appear for a few seconds, followed by the welcome screen shown below. Click on the **"Next"** button to continue. 

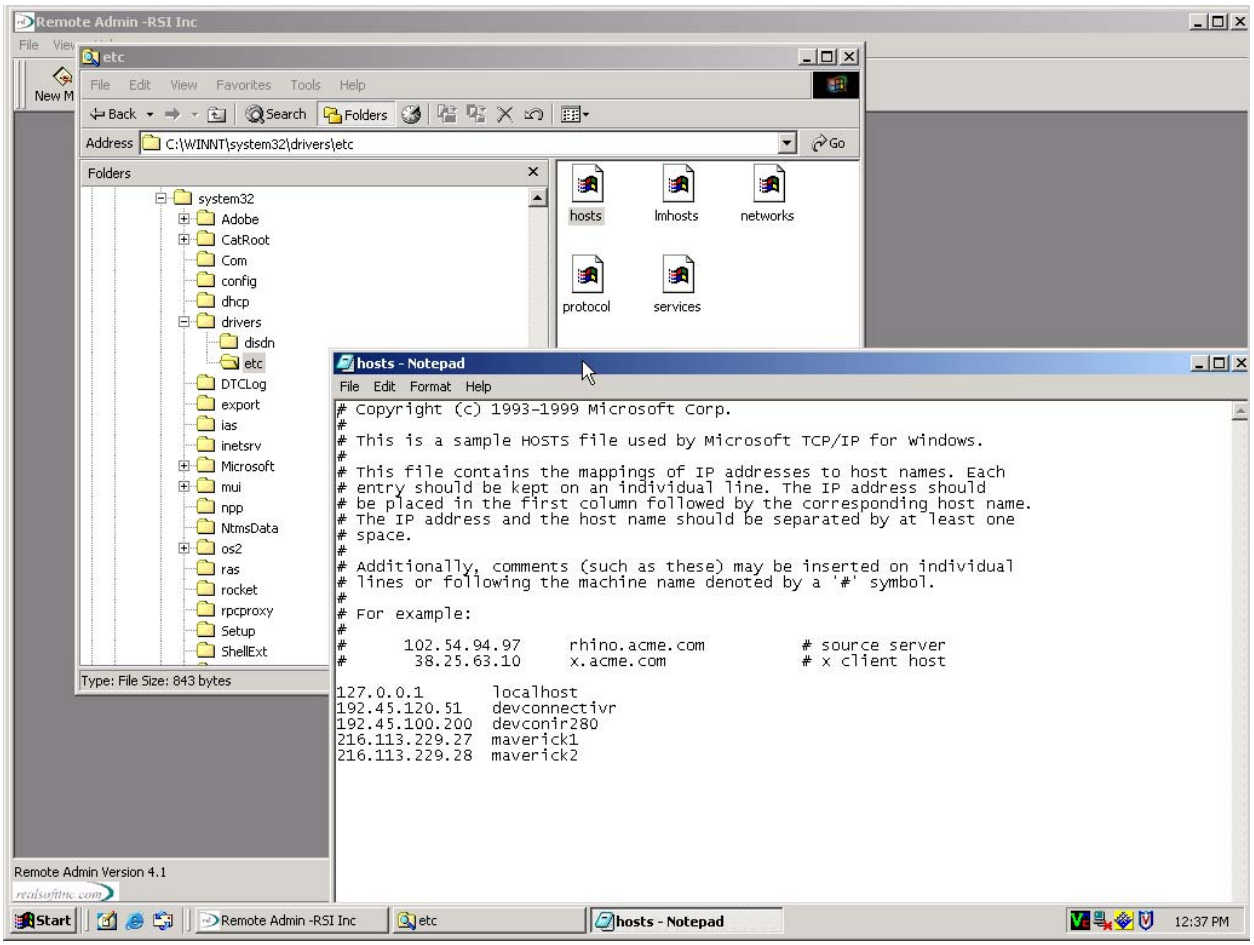
3	A destination screen as shown below will appear. Choose the destination folder for this installation. If the default folder is not acceptable, browse to the desired folder. Click on the **"Next"** button to perform the actual install. 

4	Progress screens will be displayed as files are copied and installed. Upon successful completion, a finish screen as shown below will appear. Click on the **"Finish"** button to complete the installation process.



3.1.3 Editing the /etc/hosts file

Remote Admin uses the /etc/hosts file for the IP addresses of the Avaya IRs it can administer. The /etc/hosts file is a plain text file containing a list of computer name and IP address pairs. This file is primarily used for address resolution on machines that either do not have DNS or WINS services available to them, or for lookups that are required before these services are started or available. In a Unix environment, the file's full path name is /etc/hosts. In a Windows environment, the full path name depends upon the version of Windows. For Windows 2000, the file is \WINNT\system32\drivers\etc\hosts. The file can be edited with Window's Notepad. Add a new line at the bottom of the file for each Avaya IR machine. Each line should start with a dotted quad IP address, followed by white space (spaces or tabs), and end with the machine name. In the screen shot below, the following four Avaya IRs were added: devconnectivr (192.45.120.51), devconivr280 (192.45.100.200), maverick1 (216.113.229.27), and maverick2 (216.113.229.28).



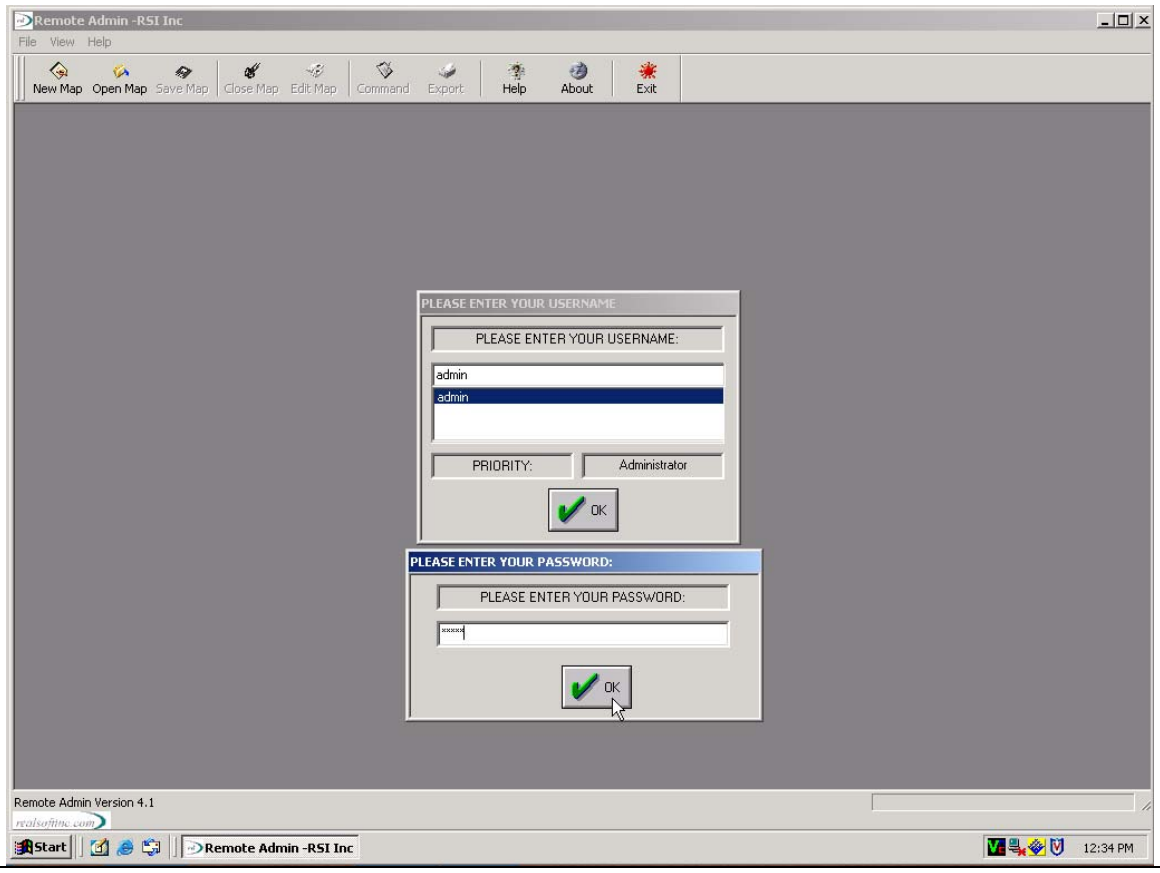
3.1.4 Creating a new map

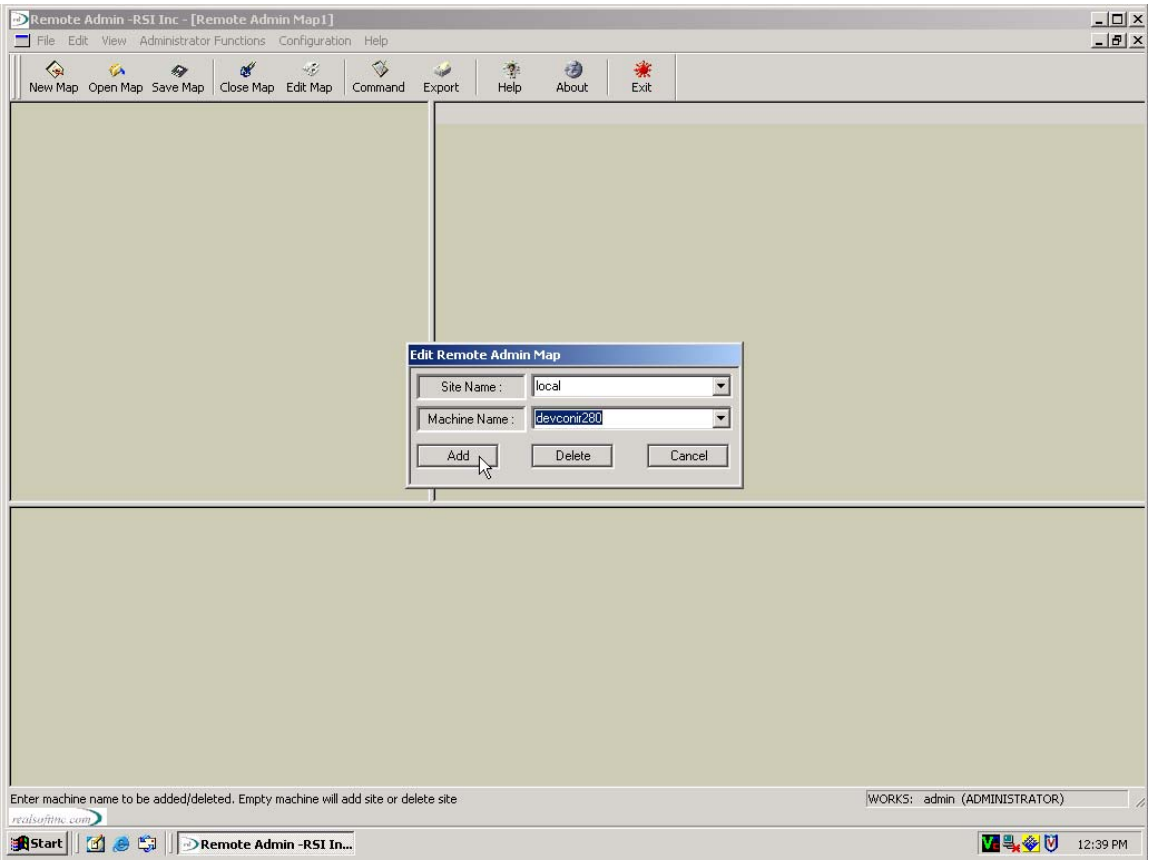
Once Remote Admin has been installed and the /etc/hosts file has been updated with the Avaya IR machine(s), a new map file can be created in Remote Admin. The map file provides a collapsible tree display of each Avaya IR that can be administered and monitored by Remote Admin.

The following steps were used to create a new map for the test configuration:

#	Creating a new map
1	Start the Remote Admin program by clicking through the following sequence: **Start->Programs->Remote Admin->Remote Admin**

2	A Real Soft splash screen will appear while the program is loading, followed by the authentication screen shown below. The default user name *Admin*. Enter a password and click on the **OK** button to continue.

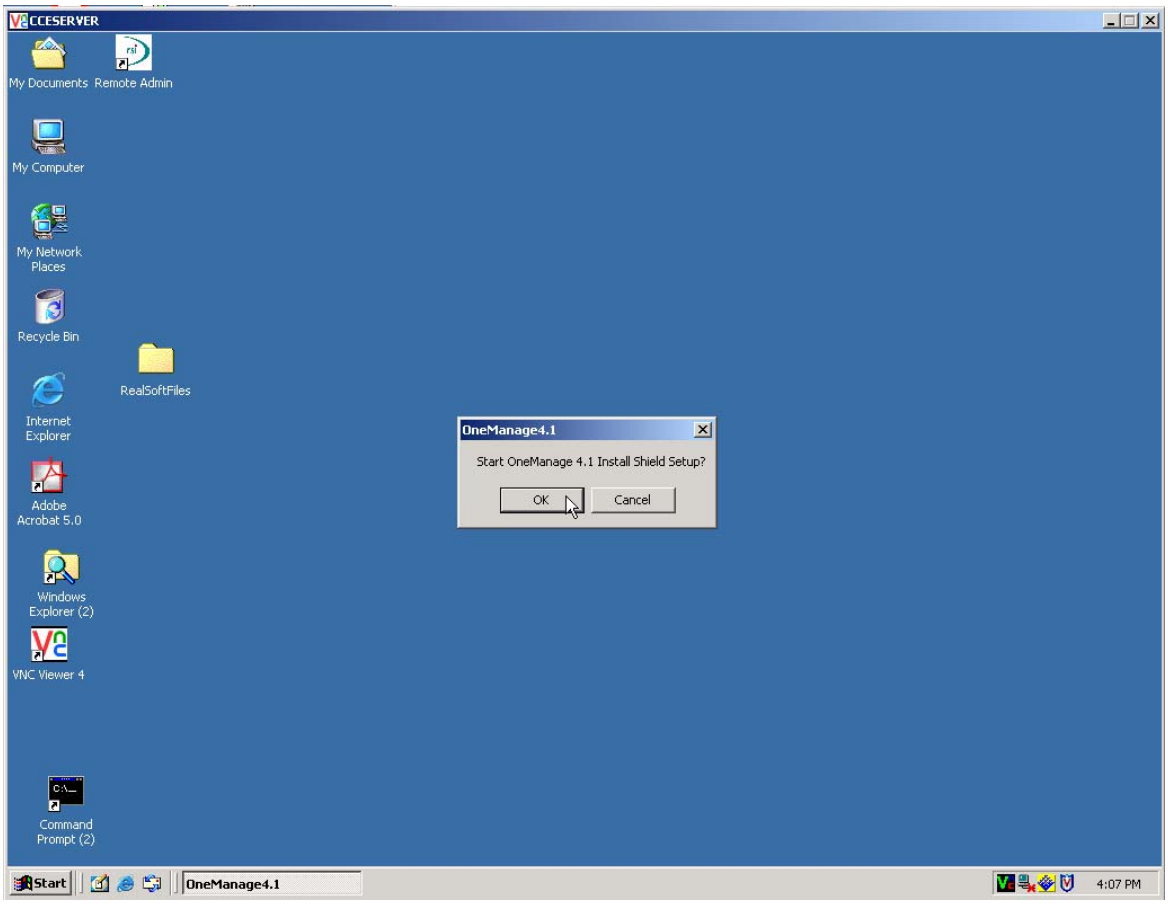


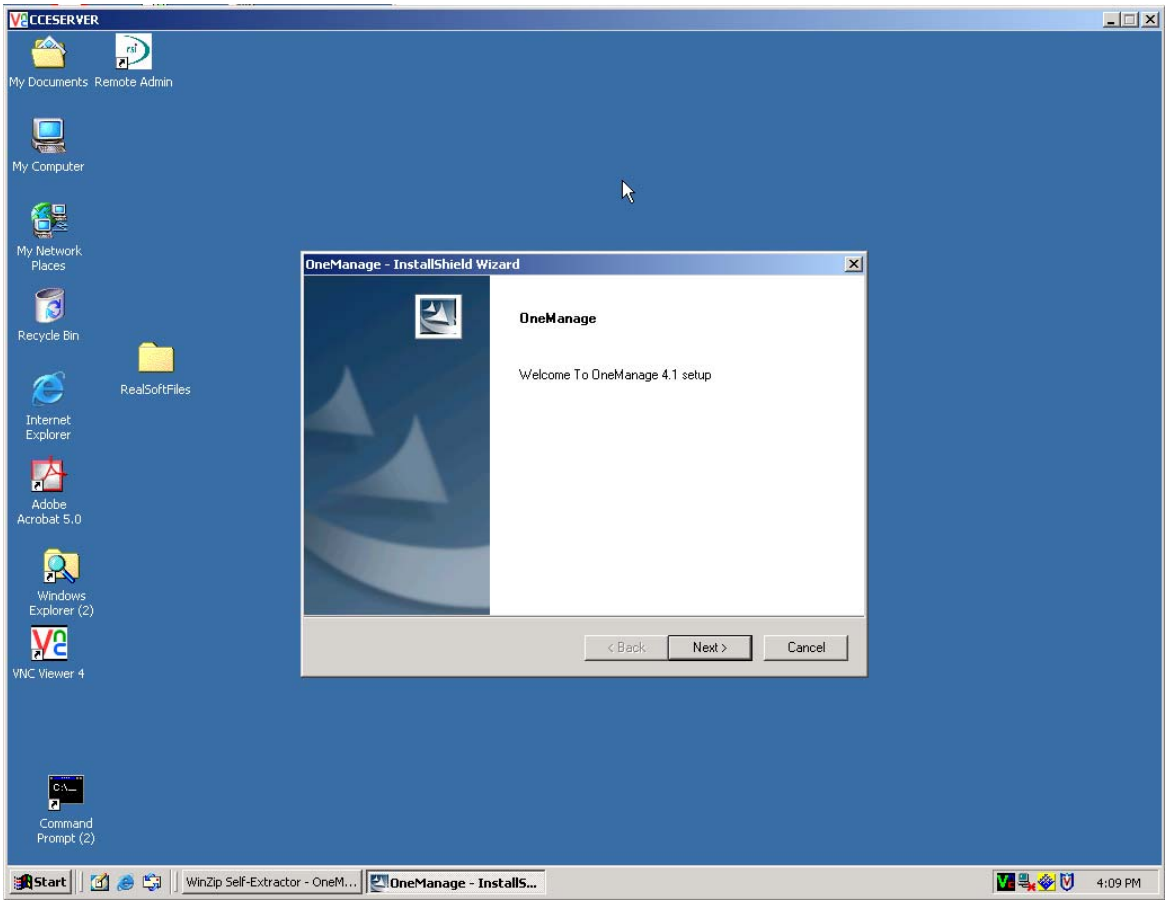
3	Upon completing the login screen, Remote Admin will display a main window that is empty. To proceed, click on the **New Map** link on the tool bar. The main window will be split into three sub panes. Click on the **Edit Map** link on the tool bar. An "Edit Remote Admin Map" window will open similar to the screen shot below. 
4	Enter a Site Name (in the test case, *local* was used) and choose an Avaya IR machine name from the pull down menu (the menu is populated with machine names from the /etc/hosts file updated in section 3.1.3. Click on the **Add** button to add this machine to the map. A new computer icon will appear in the upper left hand corner of the upper left pane. The icon will be labeled with the Site Name that was entered.

3.2 OneManage

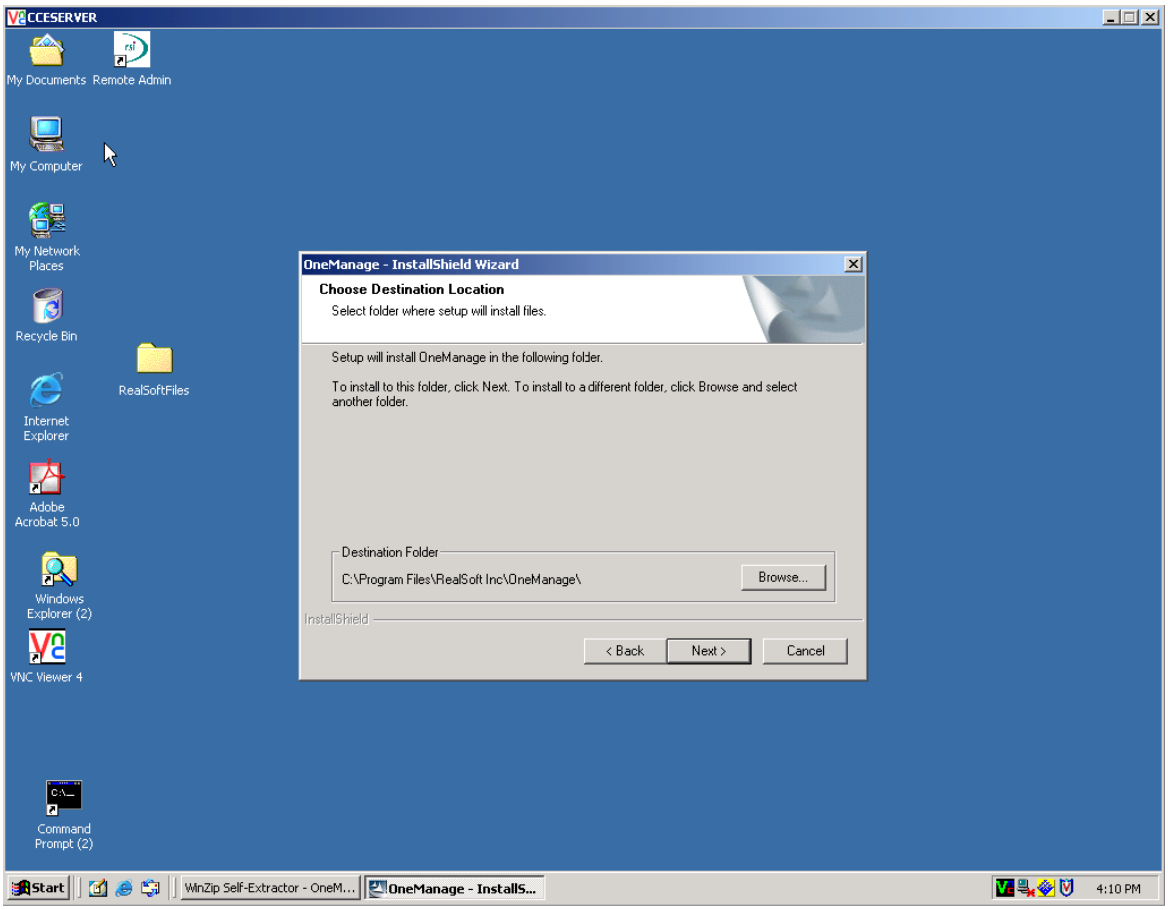
Installation of Real Soft One Manage can be broken into three parts; installation of the OneManage client on a Windows-based PC, installation of the One Manage server on Avaya IR, and adding the Avaya IR machine names and IP addresses to the /etc/hosts file. The One Manage program is distributed on two CD-ROMs, one for the client and one for the server.

3.2.1 Client

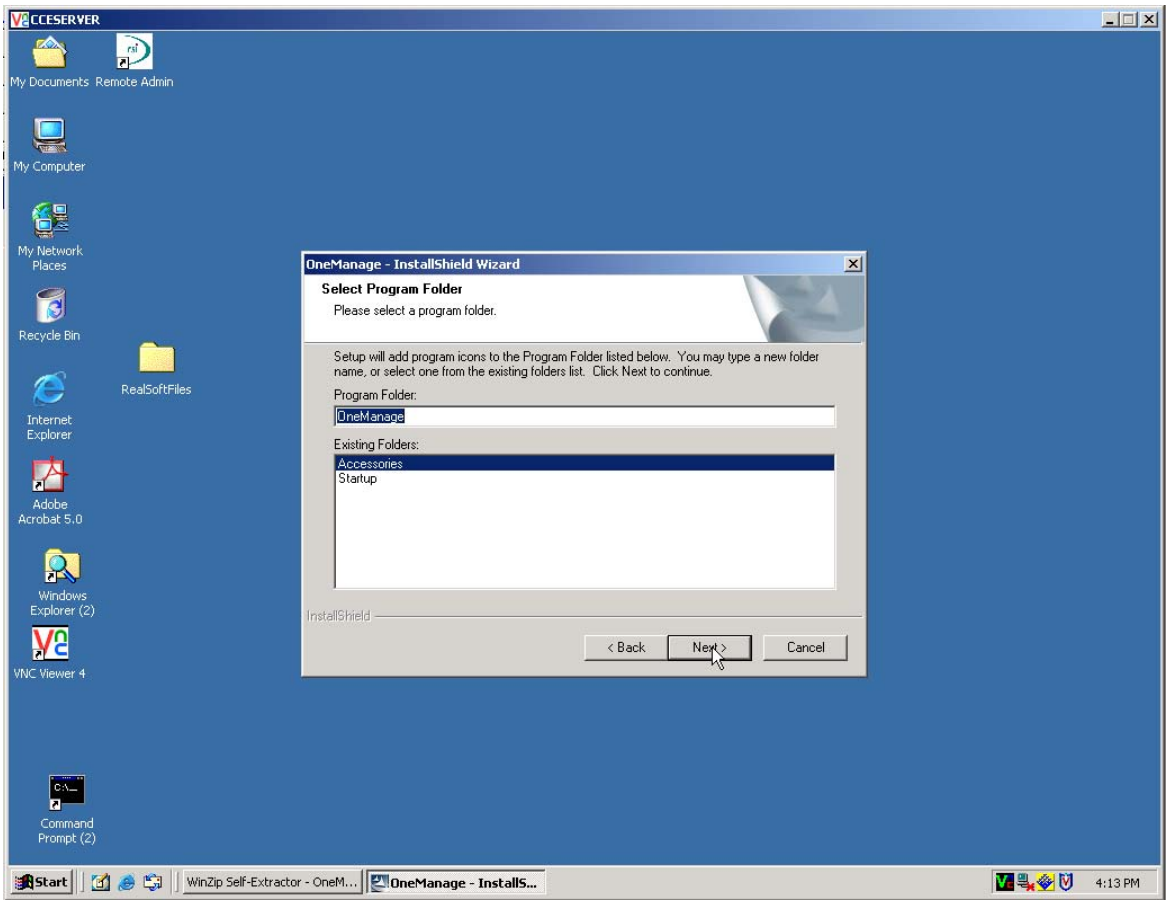
#	Installation Procedure
1	The One Manage client is distributed on a CD-ROM. Insert this CD-ROM in the CD-ROM drive of the Windows-based PC. If autorun is enabled, the setup program will start automatically. If not, browse to the CD-ROM drive, and select and run the setup.exe file.
2	A RSI splash screen will appear for a few seconds, followed by a small dialog box as shown below. Click on the **"OK"** button to continue. 

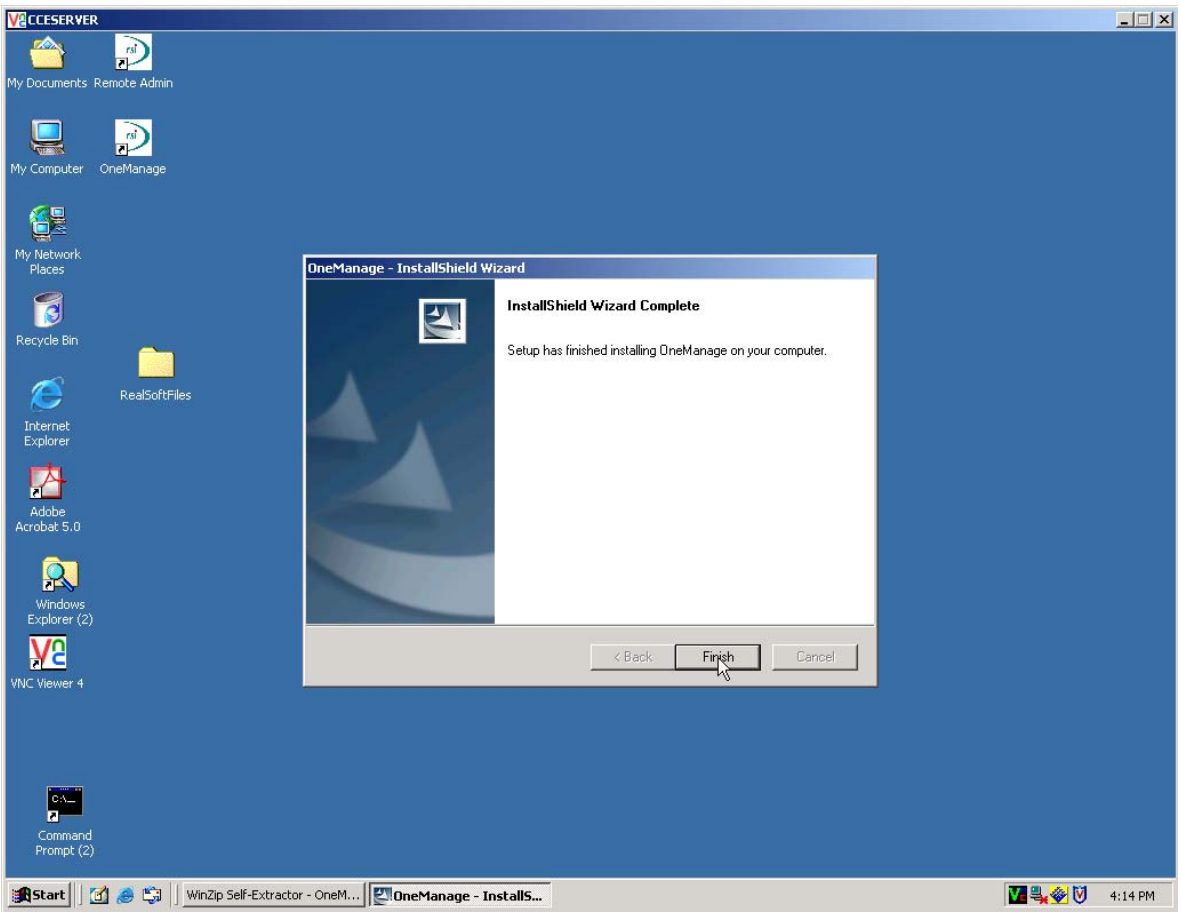
3	The One Manage InstallShield Wizard will appear. Click on the **"Next"** button to continue with the install. 

4	A destination screen as shown below will appear. Choose the destination folder for this installation. If the default folder is not acceptable, browse to the desired folder. Click on the **"Next"** button to continue the installation.



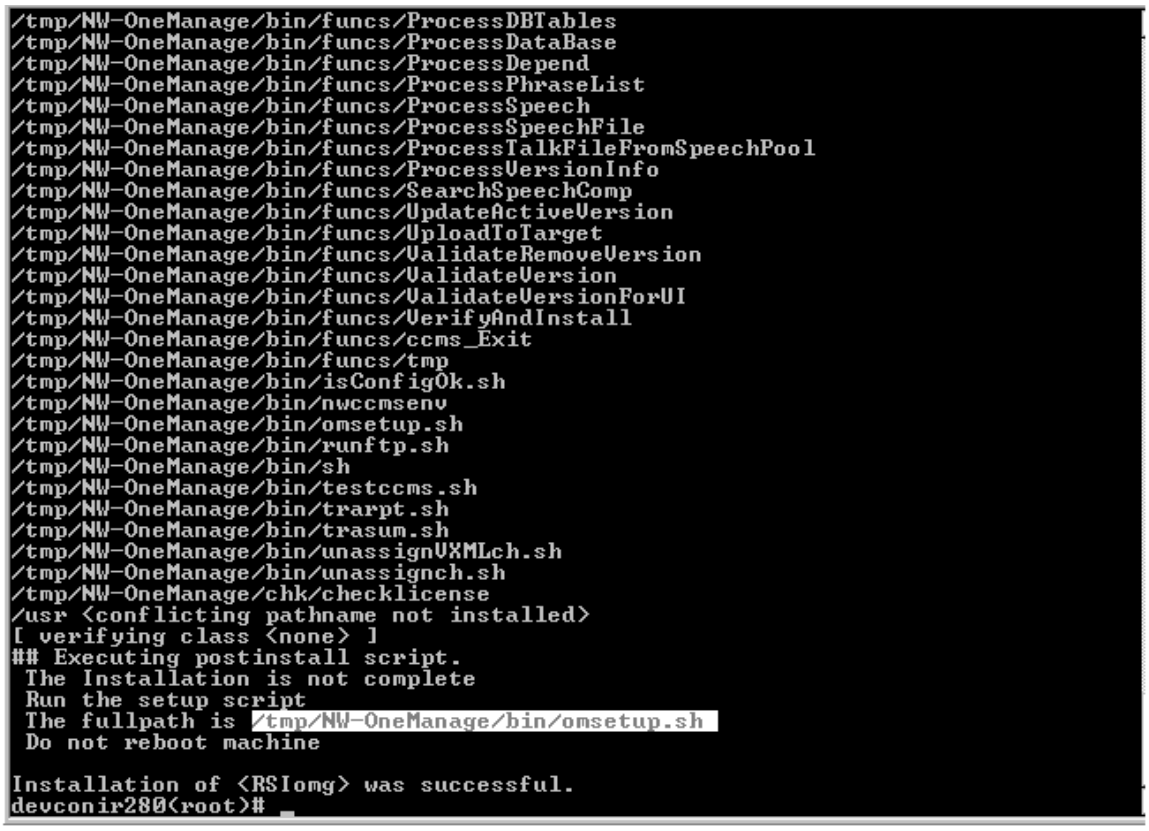
5	A Select Program Folder screen as shown below will appear. Choose the Program Folder for this installation. For the test configuration the default folder, *OneManage*, was used. Click on the **"Next"** button to start the actual install.



6	Progress screens will be displayed as files are copied and installed. Upon successful completion, a finish screen as shown below will appear. Click on the **"Finish"** button to complete the installation process. 

3.2.2 Server

#	Installation Procedure
1	The Avaya IR part of OneManage is distributed as a package to be installed via the Solaris **pkgadd** command. The distribution package file is called *RSIomg.pkg*. This file must first be made accessible to Avaya IR by either copying the file to Avaya IR via ftp, or by inserting the distribution CD-ROM into the Avaya IR CD-ROM drive.

2	After the *RSIomg.pkg* package file is on Avaya IR, the command: **pkgadd –d <device>RSIomg.pkg** will install the package. **<device>** is either **/cdrom/cdrom/** for the CD-ROM drive, or the full path name of the directory where the *RSIomg.pkg* file was copied to by ftp. There are a large number of files that are installed during the pkgadd command, the following screen shot shows a partial listing of them. 

3	Unlike the installation of Remote Admin, the **pkgadd** command for OneManage does not automatically run the post install script. For OneManage, the post install script requires license information and must be run manually. The command is **/tmp/NW-OneManage/bin/omsetup.sh** This command installs the product in the following directory **/voice1/onemanage** The license key is based on either the network IP address or the hostname of the Avaya IR, and should be obtained from Real Soft. devconir280(root)# /tmp/NW-OneManage/bin/omsetup.sh ********** Initial Setup for One Manage ********** Please enter the license key: =>NB041308513816313808 4738 6 blocks Please enter "rsi123" as the passwd for rsiomg login New password: Re-enter new password: passwd (SYSTEM): passwd successfully changed for rsiomg Please indicate the type of Avaya IR system 1. Primary 2. Secondary Please indicate your choice.[2]=>2 Make sure Avaya IR is loaded on this system This is your Secondary system for RSI OneManage Starting RSI OneManage Agent NWOneManageAgent has been started successfully. Thank you for choosing OneManage from Real Soft,Inc. devconir280(root)# _

4	The **pkginfo** tool can be used to verify the installation of the OneManage package on Avaya IR. The format is shown in the screen shot below.

```
devconir280(root)# pkginfo -l RSIomg
   PKGINST:  RSIomg
      NAME:  OneManage
  CATEGORY:  application
      ARCH:  sparc
   VERSION:  4.1
    VENDOR:  Real Soft Inc, 2540 Route 130 N, Suite #118, Cranbury NJ - 08512
      DESC:  OneManage Agent
    PSTAMP:  08/2004
  INSTDATE:  Sep 21 2004 14:15
   HOTLINE:  1-609-409-3636
     EMAIL:  support@realsoftinc.com
    STATUS:  completely installed
     FILES:      152 installed pathnames
                   5 shared pathnames
                  12 directories
                 140 executables
                1318 blocks used (approx)

devconir280(root)#
```

5	There is one final step to complete the installation of OneManage on Avaya IR. Different releases of Avaya IR are built on different releases of the Solaris operating system, which have different default enabled/disabled settings for some TCP and UDP services. The OneManage program requires that the TCP echo service is enabled for it to work. The file */etc/services* contains the default settings for the various network services on the Avaya IR box. In this file each service has its own line, and if the line for a particular service starts with a # (the pound or number sign), then that service is disabled. The line must not start with a pound sign for the service to be enabled. Edit this file with a text editor to ensure the entry for **echo** does not start with a pound sign as shown below.

```
# All rights reserved.
#
# Network services, Internet style
#
tcpmux          1/tcp
echo            7/tcp
echo            7/udp
#discard                9/tcp           sink null
#discard                9/udp           sink null
#systat         11/tcp          users
#daytime                13/tcp
#daytime                13/udp
#daytime                15/tcp
#chargen                19/tcp          ttytst source
#chargen                19/udp          ttytst source
ftp-data        20/tcp
ftp             21/tcp
telnet          23/tcp
#smtp           25/tcp          mail
"services" [Read only] 118 lines, 3914 characters
```

3.2.3 Editing the /etc/hosts file

Like Remote Admin, OneManage uses the /etc/hosts file for the IP addresses of the Avaya IRs it administers. However, unlike Remote Admin, the /etc/hosts file is the only source of Avaya IR IP addresses for OneManage. If an Avaya IR is not listed in the /etc/hosts file on the OneManage machine, OneManage will not be able to connect to it.

If OneManage is being installed on the same client PC as Remote Admin, then the /etc/hosts file has already been updated (refer to section 3.1.3). If OneManage is being installed on a different client PC, entries for each Avaya IR machine must be added to the /etc/hosts file. Follow the instructions in section 3.1.3 to accomplish this.

3.3 NetWatch SNMP Monitor

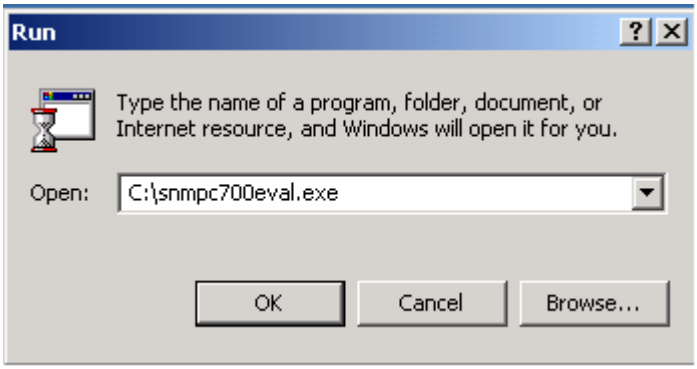
NetWatch SNMP Monitor is a server program that installs on the Solaris-based Avaya IR that communicates with a third party SNMP manager typically installed on a Windows-based PC. There are numerous third party SNMP managers available and Real Soft has tested their application with SNMP managers from Castle Rock, HP OpenView, and IBM Tivoli. For the test configuration, the third party SNMP manager used was SNMPc from Castle Rock (http://www.castlerock.com).

3.3.1 Client

The Castle Rock SNMPc manager is available as an evaluation download from their website mentioned above. The program is installed by running the downloaded .exe file

snmpc700eval.exe

The installation defaults will work for this application.



There are five .mib files that must be installed on the client PC for the SNMP manager to accept SNMP notifications from Avaya IRs. These five .mib files are distributed on the Real Soft NetWatch SNMP Monitor CD-ROM. Copy these files to the following directory:

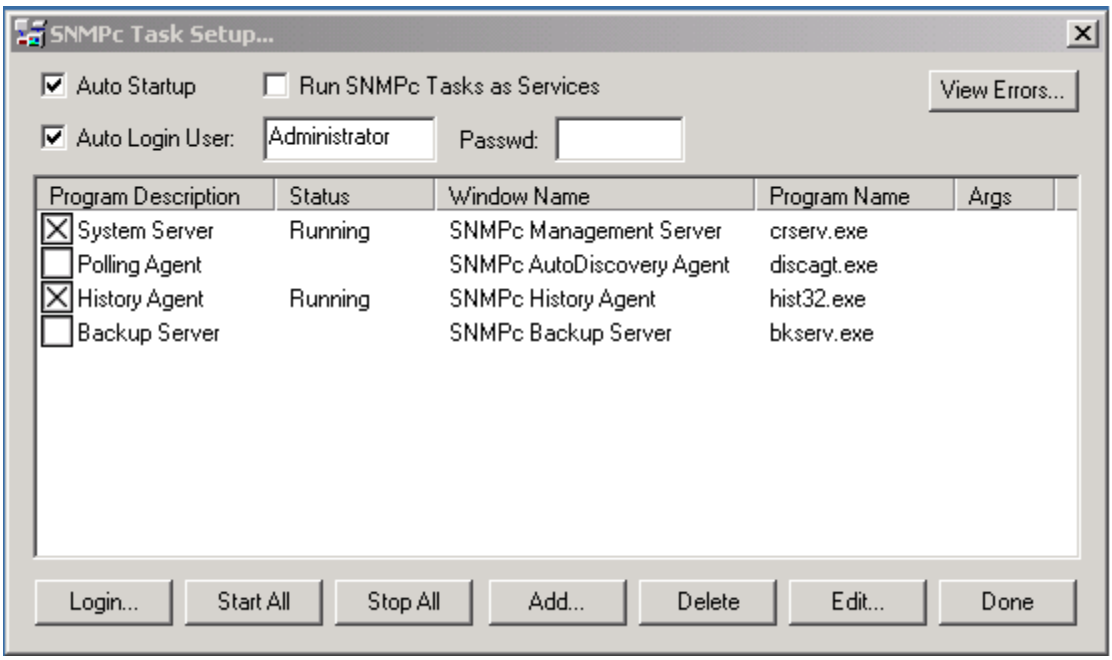
C:\Program Files\SNMPc Network Manager\mibfiles

The five .mib files are:

- host.mib
- NetWatch.mib
- netwatch-v3.mib

- nwnms.mib
- nwremote.mib

Once SNMPc has been installed, start two of its services using the SNMPc Task Setup program. Check the **System Server** and the **History Agent** boxes and then click on the **Add** button.



3.3.2 Server

#	Installation Procedure
1	The Avaya IR part of NetWatch SNMP Monitor is distributed as a package to be installed via the Solaris **pkgadd** command. The distribution package file is called *rsinwfms.pkg*. This file must first be made accessible to Avaya IR by either copying the file to Avaya IR via ftp, or by using a copy on a CD-ROM.

2 After the *RSInsfms.pkg* package file is on Avaya IR, the command:

pkgadd –d <device>RSInwfms.pkg

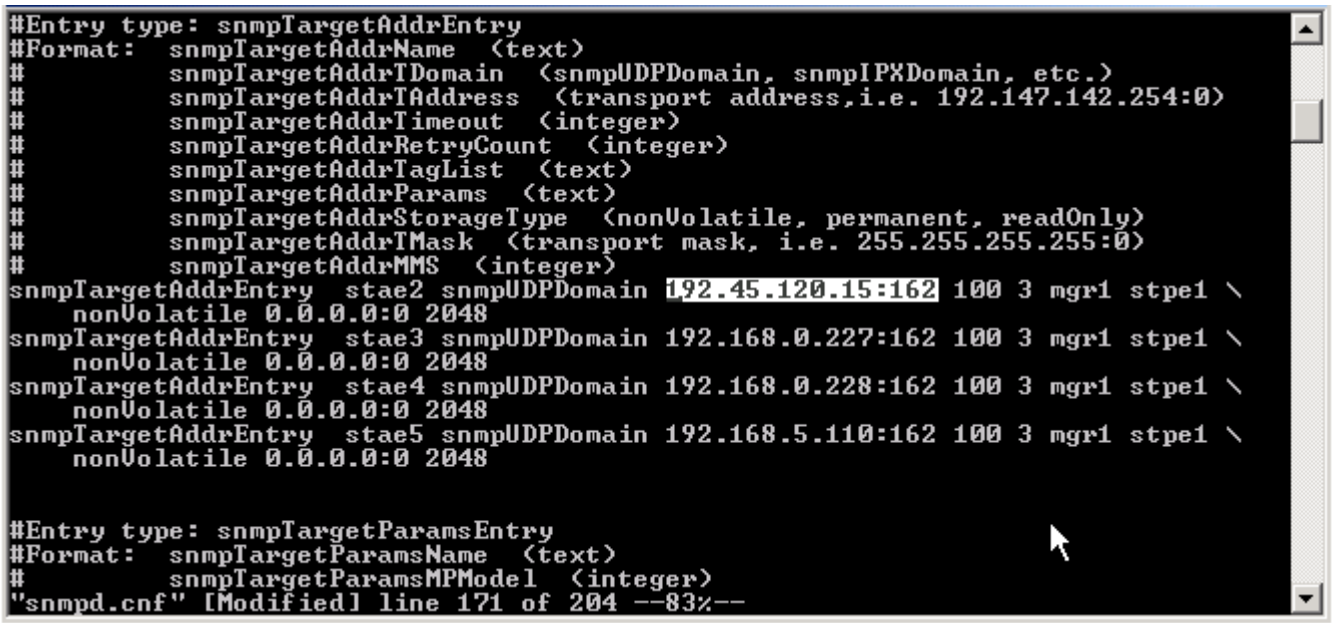
will install the package. **<device>** is either **/cdrom/cdrom/** for the CD-ROM drive, or the full path name of the directory where the *RSInwfms.pkg* file was copied to by ftp. During the install it is possible the following warning message may be generated:

The following files are already installed on the system….

Do you want to install these conflicting files [y,n,?,q]

Answer this question with **n** to not re-install the files and then enter a **y** to continue the installation. There are a large number of files that are installed during the **pkgadd** command; the following screen shot shows a partial listing of them.

```
devconir280(root)# pkgadd -d RSInwfms.pkg

The following packages are available:
  1  RSInwfms     Avaya IR 1.2 System - NetWatch SNMP Monitor
                  (sparc) 4.0.8

Select package(s) you wish to process (or 'all' to process
all packages). (default: all) [?,??,q]:

Processing package instance <RSInwfms> from </RSInwfms.pkg>

Avaya IR 1.2 System - NetWatch SNMP Monitor
(sparc) 4.0.8
----------------------------------------------------------------

        (C) Copyright 2003-2004 Real Soft, Inc.
        All rights reserved.

        Postal: Real Soft, Inc.
                2540 Route 130 North, Suite 118
                Cranbury, NJ  08512
                USA

           Tel: +1 609 409 3636
           Fax: +1 609 409 3637

        E-mail: support@realsoftinc.com"
           URL: http://www.realsoftinc.com/

----------------------------------------------------------------
Using </opt/RSI> as the package base directory.
## Processing package information.
## Processing system information.
   7 package pathnames are already properly installed.
## Verifying disk space requirements.
## Checking for conflicts with packages already installed.

The following files are already installed on the system and are being
used by another package:
  /usr/local <attribute change only>

* - conflict with a file which does not belong to any package.

Do you want to install these conflicting files [y,n,?,q] n

Do you want to continue with the installation of <RSInwfms> [y,n,?] y
## Checking for setuid/setgid programs.

This package contains scripts which will be executed with super-user
permission during the process of installing this package.

Do you want to continue with the installation of <RSInwfms> [y,n,?] y
## Processing package information.
## Processing system information.

Installing Avaya IR 1.2 System - NetWatch SNMP Monitor as <RSInwfms>

## Executing preinstall script.
## Installing part 1 of 1.
/opt/RSI/NW-FMS/.origcfg/NWMONmsg
/opt/RSI/NW-FMS/.origcfg/NWMONmsg.sh
/opt/RSI/NW-FMS/.origcfg/logNWMON.h
/opt/RSI/NW-FMS/.origcfg/nw.cfg
/opt/RSI/NW-FMS/.origcfg/nw_site.cfg
/opt/RSI/NW-FMS/.origcfg/nw_trap.cfg
/opt/RSI/NW-FMS/.origcfg/nwa.cfg
/opt/RSI/NW-FMS/.origcfg/nwa_beep.cfg
```

3	After the *RSInsfms.pkg* package has been installed on Avaya IR, the command: **pkgadd –d <device>RSInwfms_expires_x.x.x.pkg** will install the necessary license information. **<device>** is either **/cdrom/cdrom/** for the CD-ROM drive, or the full path name of the directory where the *RSInwfms_expires_x.x.x.pkg* file was copied to by ftp. This file is provided by Real Soft and is typically installed by a Real Soft technician. During the install it is possible the following warning message may be generated: *The following files are already installed on the system….* *Do you want to install these conflicting files [y,n,?,q]* Answer this question with **n** to not re-install the files and then enter a **y** to continue the installation.
4	Edit the following file with a text editor such as vi or emacs: **/opt/RSI/NW-FMS/cfg/snmp/snmpd.cnf** In the *snmpTargetAddrEntry* section, on approximately line #171, there is an entry that has default IP addresses for the SNMP management PC. Modify this IP address to reflect the address of the Windows-based PC that the SNMPc management program was installed. A copy of the relevant section of this file is shown below. Port number 162, which is the standard SNMP trap port, is used after a colon after the IP address. 

```
#Entry type: snmpTargetAddrEntry
#Format:  snmpTargetAddrName  (text)
#         snmpTargetAddrTDomain  (snmpUDPDomain, snmpIPXDomain, etc.)
#         snmpTargetAddrTAddress  (transport address,i.e. 192.147.142.254:0)
#         snmpTargetAddrTimeout  (integer)
#         snmpTargetAddrRetryCount  (integer)
#         snmpTargetAddrTagList  (text)
#         snmpTargetAddrParams  (text)
#         snmpTargetAddrStorageType  (nonVolatile, permanent, readOnly)
#         snmpTargetAddrTMask  (transport mask, i.e. 255.255.255.255:0)
#         snmpTargetAddrMMS  (integer)
snmpTargetAddrEntry  stae2 snmpUDPDomain 192.45.120.15:162 100 3 mgr1 stpe1 \
    nonVolatile 0.0.0.0:0 2048
snmpTargetAddrEntry  stae3 snmpUDPDomain 192.168.0.227:162 100 3 mgr1 stpe1 \
    nonVolatile 0.0.0.0:0 2048
snmpTargetAddrEntry  stae4 snmpUDPDomain 192.168.0.228:162 100 3 mgr1 stpe1 \
    nonVolatile 0.0.0.0:0 2048
snmpTargetAddrEntry  stae5 snmpUDPDomain 192.168.5.110:162 100 3 mgr1 stpe1 \
    nonVolatile 0.0.0.0:0 2048


#Entry type: snmpTargetParamsEntry
#Format:  snmpTargetParamsName  (text)
#         snmpTargetParamsMPModel  (integer)
"snmpd.cnf" [Modified] line 171 of 204 --83%--
```

5	The package is installed in the /opt/RSI/NW-FMS directory. In this install directory there is a subdirectory named bin. Change directory to this bin directory. Three script files are in this bin directory: **NWStatus** (prints the status of the numerous NetWatch agents) **NWStart** (starts the NetWatch agent processes running) **NWStop** (stops the NetWatch agent processes running) Run the **NWStatus** script to verify the NetWatch agents are currently not running. Run the **NWStart** script to start the NetWatch agents. A screen snapshot of these commands is given below.

```
devconir280(root)# pwd
/opt/RSI/NW-FMS
devconir280(root)# cd bin
devconir280(root)# ls
DisableMIB2.sh  NWSmon          hostagt         nwfs            nwps.sh
EnableMIB2.sh   NWStart         hwHandler.sh    nwfunc.sh       nwremoteagt
NWAgent         NWStatus        install.sh      nwhost          nwsstart
NWBBInfo        NWStop          ipcHandler.sh   nwhw            perfHandler.sh
NWBeep          NWTrap          netwatchagt     nwipc           postinstall.sh
NWCardInfo      beep.sh         nwastart        nwmqerr.sh      preremove.sh
NWChanInfo      beep_k.sh       nwchkmac.sh     nwmqok.sh       psHandler.sh
NWConfig        collectPerf.sh  nwclean.sh      nwmsg.sh        snmpdm
NWHmon          fsHandler.sh    nwcms.sh        nwnmsagt
NWLic           gen_sys_rpt.sh  nwemail.sh      nwperf
NWReinit        hostHandler.sh  nwfrs.sh        nwps
devconir280(root)# NWStatus
Checking status of NetWatch Agents
        NWAgent is not running.
        NWBeep is not running.
        snmpdm is not running.
        netwatchagt is not running.
        hostagt is not running.
        nwnmsagt is not running.
        nwremoteagt is not running.
devconir280(root)# pwd
/opt/RSI/NW-FMS/bin
devconir280(root)#
devconir280(root)# NWStart
Starting NetWatch Agents
        NWAgent has been started successfully.
        NWBeep has been started successfully.
        snmpdm has been started successfully....
        netwatchagt has been started successfully....
        hostagt has been started successfully....
        nwnmsagt has been started successfully....
        nwremoteagt has been started successfully....
devconir280(root)#
```

6	The **pkginfo** tool can be used to verify the installation of the NetWatch SNMP Monitor package on Avaya IR. The format is shown in the screen shot below.

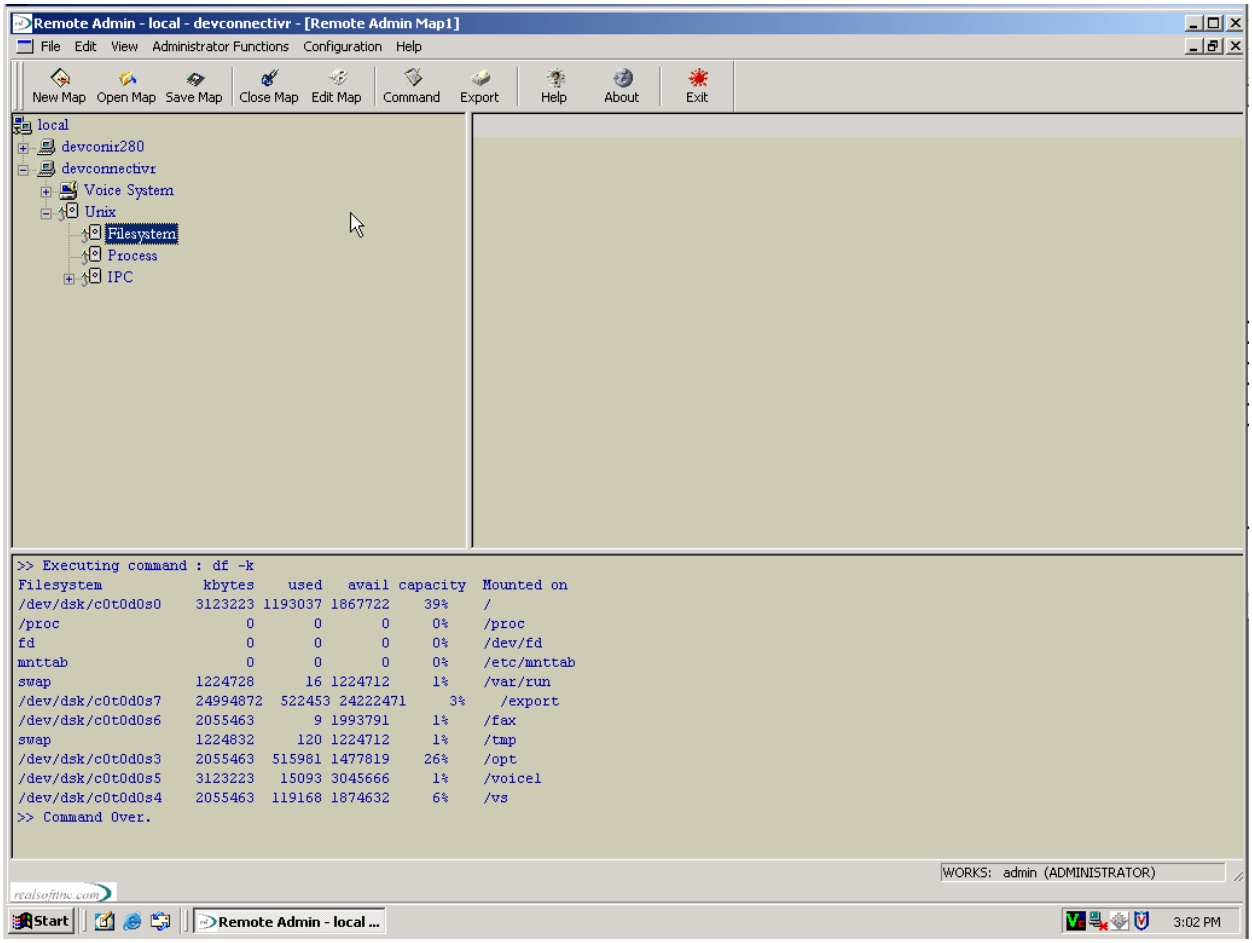
```
devconnectivr(root)# pkginfo -l RSInwfms
   PKGINST:  RSInwfms
      NAME:  Avaya IR 1.2 System - NetWatch SNMP Monitor
  CATEGORY:  application
      ARCH:  sparc
   VERSION:  4.0.8
   BASEDIR:  /opt/RSI
    VENDOR:  Real Soft, Inc., 2540 Route 130 North, Suite 118, Cranbury, NJ 0851
2, USA
    PSTAMP:  05/28/04
  INSTDATE:  Sep 20 2004 15:09
     EMAIL:  support@realsoftinc.com
    STATUS:  completely installed
     FILES:      135 installed pathnames
                   6 shared pathnames
                  23 directories
                  61 executables
               14074 blocks used (approx)

devconnectivr(root)#
```

4. Verification

4.1 Remote Admin

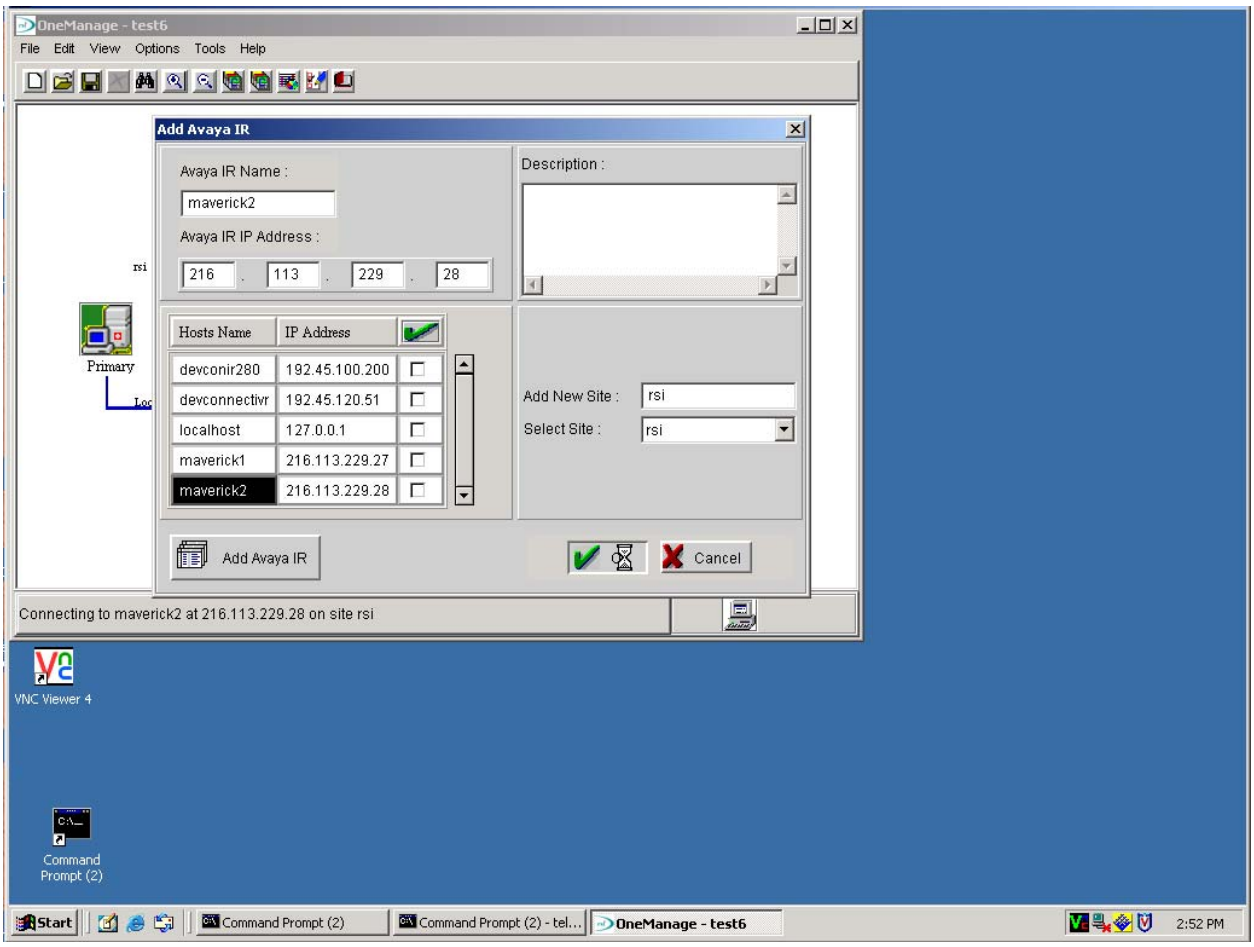
To verify Remote Admin has been correctly installed and configured on a Windows-based PC, the following procedure can be used to add an Avaya IR to the map and attempt to run any of the Unix commands.

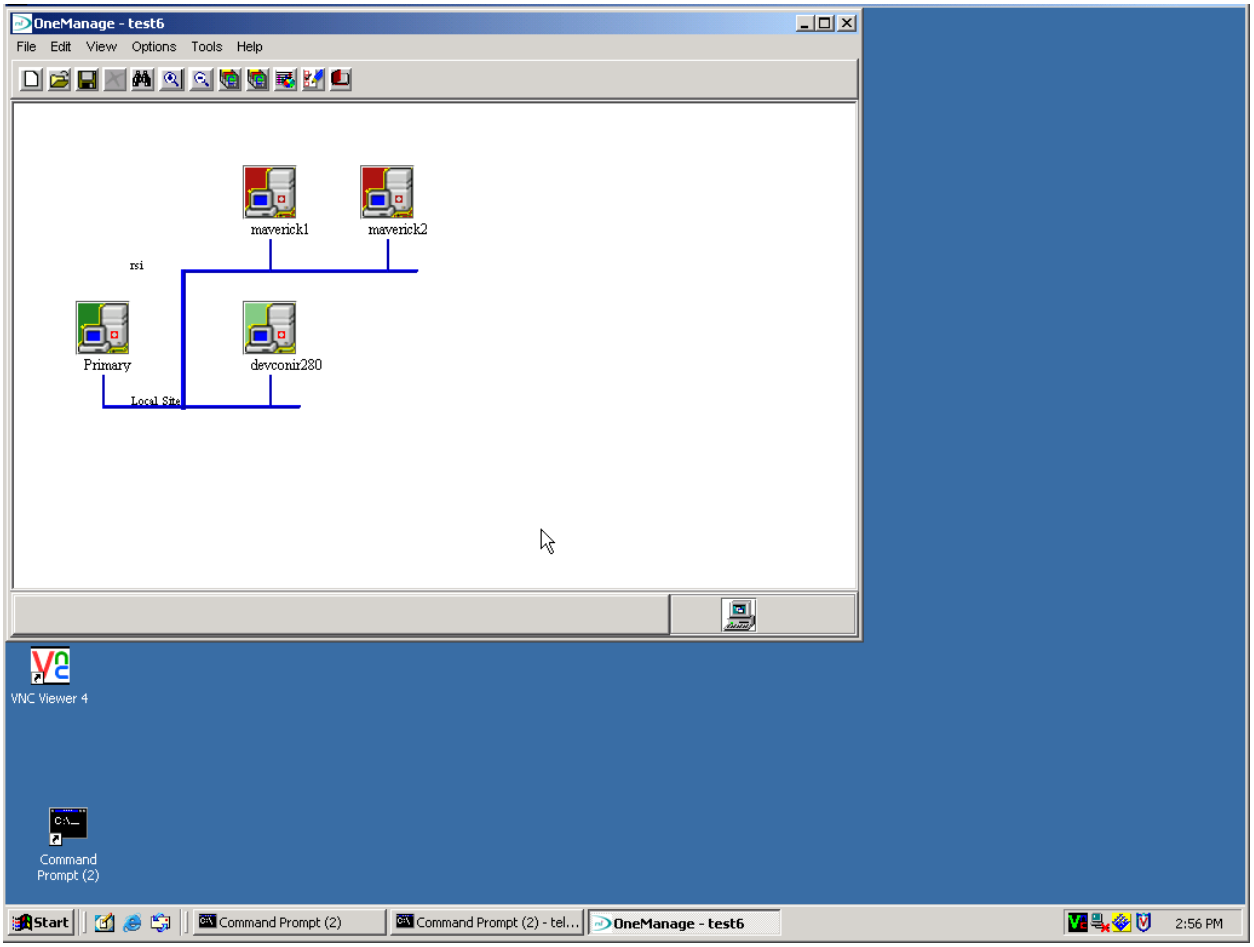
Click on the **Edit Map** button on the toolbar. Enter a name for the site, such as *local*. Choose one of the Avaya IRs from the pull down list (these are populated from the /etc/hosts file edited in Section 3.1.3). Click on the **Add** button to add the site and the machine to the upper left hand window. Now expand the tree in this upper left hand window by double clicking on the site name, and then double clicking on the machine name. Expand the **Unix** table to show the Unix commands. Click on the **Filesystems** tab to run the Unix command *df –k* on the remote Avaya IR. The results will be displayed in the bottom window as shown below.



4.2 OneManage

To verify OneManage is installed correctly installed on a Windows-based PC, start OneManage and attempt to add an Avaya IR to the managed window. Opening a new map file will display the **Add Avaya IR** window. Select an Avaya IR name and enter its IP address. Alternatively, an Avaya IR and its IP address can be selected from the list if the machine has an entry in the /etc/hosts file. Click on **Add Avaya IR** to complete the process. OneManage will attempt to establish a connection to this Avaya IR. This process can take a while, between one and two minutes is typical. If it succeeds an IR icon is added to the map with a green background. If it fails, the IR icon will be added with a red background.

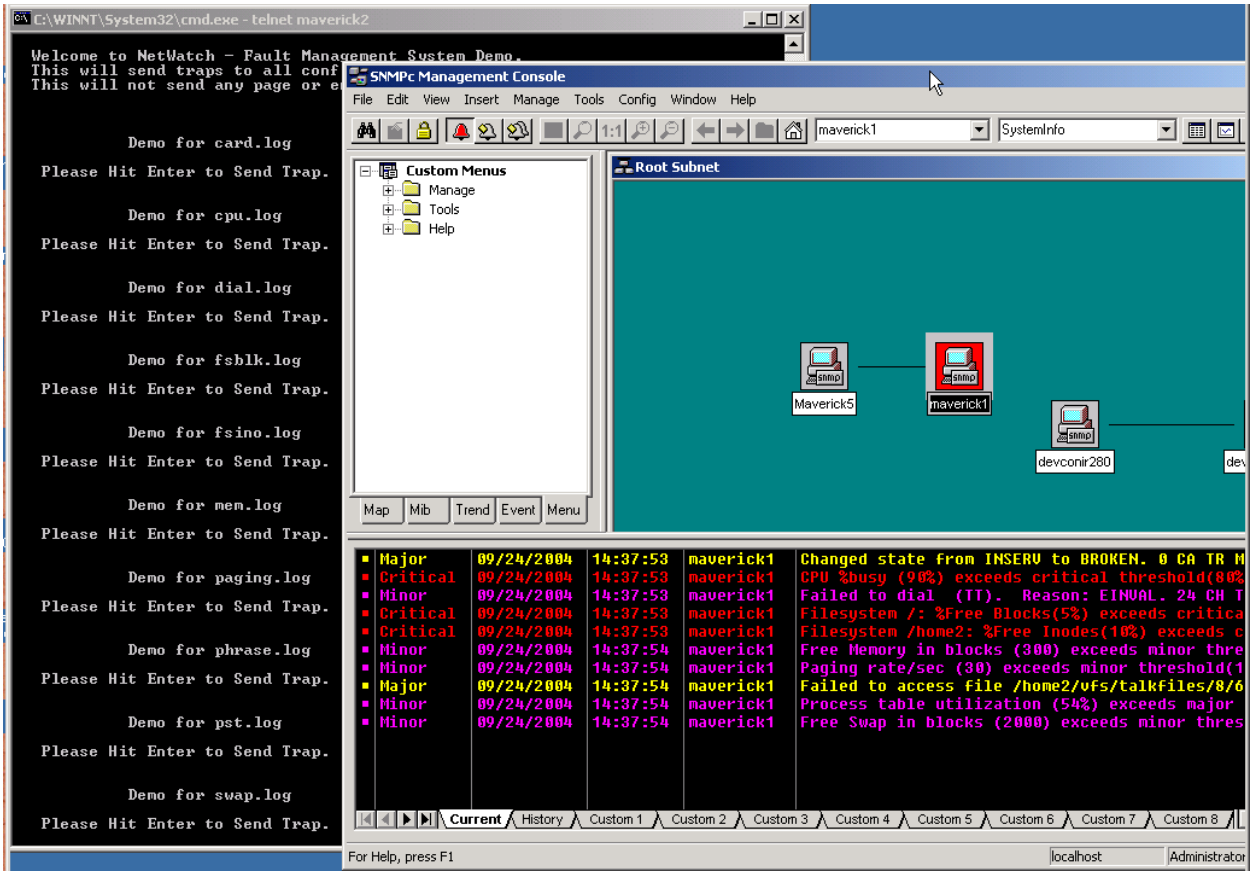




4.3 NetWatch SNMP Monitor

NetWatch is designed to capture and display SNMP traps generated by the Avaya IRs it is monitoring. When this program is installed on Avaya IR, a demo test script is installed with it. The demo test script is called *demo.sh* and is installed in the /opt/RSI/NW-FMS/demo/ directory. Running this test script will generate 10 different SNMP alarms, waiting for the user to enter a carriage return between each alarm generation. By running this demo test script, ten different SNMP alarms will be generated on Avaya IR. If NetWatch has been correctly installed and configured, these ten alarms should be displayed on the SNMPc management screen monitoring this Avaya IR.

The following screen snapshot shows this verification step in progess. The left and rear command window contains a telnet session to a remote Avaya IR on which the demo test script was just run. The right and front screen is the SNMPc console screen, which shows the ten SNMP alarms along with the red background around the Avaya IR icon in alarm.



5. Interoperability Compliance Testing

5.1 General test Approach

The scope of DevConnect Compliance Testing is to verify these Real Soft products operate properly with the Avaya IR system in a typical call center environment. Since the Real Soft product literature highlights the products' abilities to work with both local and remote Avaya IRs, the test environment was designed to simulate distributed call centers with multiple Avaya IRs. Two different locations, each with two Avaya IRs, local internal networks, and firewalls with NAT to the Internet were set up to simulate two geographically separate call centers. The three Real Soft products were installed on a Windows-based PC and used to administer, manage, and monitor both the local and remote Avaya IRs.

Real Soft Remote Admin allows users to perform the day-to-day administration of one or more Avaya IR systems through a user-friendly graphical interface. These administrative functions were tested on both the local and remote Avaya IRs.

Real Soft OneManage allows one Avaya IR (the primary IR) to act as a distribution point to deploy and manage IVR applications on one or more additional Avaya IRs (the secondary IRs). The ability to deploy, assign, and start an IVR application from a local primary Avaya IR to both another local secondary Avaya IR and to a remote secondary Avaya IR was tested.

Real Soft NetWatch SNMP Monitor allows one or more Avaya IRs (local and/or remote) to be monitored from a local SNMP management screen. The ability to monitor local and remote Avaya IRs from the SNMP management screen was tested.

5.2 Test Results

Real Soft Remote Admin- Version 4.1.1 successfully passed all interoperability compliance tests with Avaya IR 1.2.

Real Soft OneManage- Version 4.0 successfully passed all interoperability compliance tests with Avaya IR 1.2.

Real Soft NetWatch SNMP Monitor- Version 4.0 successfully passed all interoperability compliance tests with Avaya IR 1.2.

6. Support

Support for Real Soft products is available by:

- phone between 9:00 am and 5:30 pm(EST) at 732 – 735 - 0310.
- email at:

support@realsoft.com

Support for Avaya IR is available by contacting:

support@conversant.com

7. Conclusion

All three Real Soft products; Remote Admin, OneManage, and NetWatch SNMP Monitor successfully interoperate with Avaya IR.

Real Soft Remote Admin (Version 4.1.1), a Windows-based GUI tool, successfully interoperates with Avaya IR 1.2.

Real Soft OneManage (Version 4.0), a client-server package providing a Windows-based GUI interface, successfully interoperates with Avaya IR 1.2.

Real Soft NetWatch SNMP Monitor (Version 4.0), a monitoring tool that interfaces to a third party industry standard SNMP manager, successfully interoperates with Avaya IR 1.2.

8. Additional References

User manuals for Real Soft products are provided in electronic format on the product media (CD-ROM). Copies of these manuals are also available from the Real Soft website at:

- "User Manual: Remote Admin – Version 4.1 – Avaya IR 1.0/1.2", is available on Real Soft's website at:
  http://www.realsoftinc.com/pr_va_remoteadmin.html
- "User Manual: One Manage – Version 4.0 – Avaya IR 1.0/1.2", is available on Real Soft's website at:
  http://www.realsoftinc.com/pr_va_onemanage.html
- "User Manual: NetWatch SNMP Monitor – Version 4.0 – Avaya IR 1.0/1.2", is available on Real Soft's website at:
  http://www.realsoftinc.com/pr_va_metwatch.html

Appendix A: Uninstalling Programs.

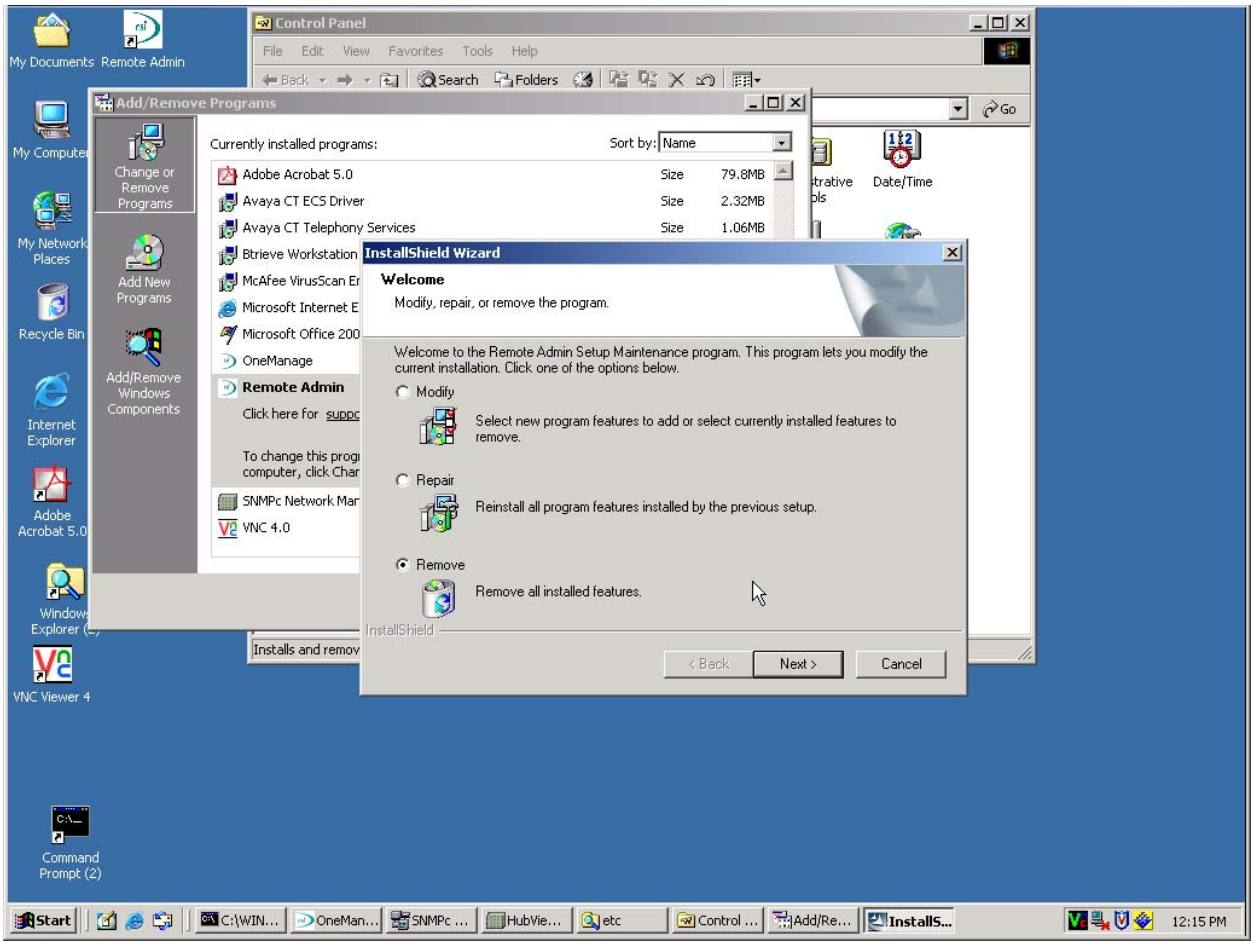
The Solaris package tool **pkgrm** can be used to uninstall Remote Admin from the Avaya IR, if necessary. The format of the command is:

Pkgrm RSIradm

This command will not only remove all of the files, but will also kill any running Remote Admin processes. A screen shot of the output of this command is found below.

```
The following package is currently installed:
   RSIradm          Realsoft - Remote Admin
                    (sparc) 4.1.6

Do you want to remove this package? y

## Removing installed package instance <RSIradm>

This package contains scripts which will be executed with super-user
permission during the process of removing this package.

Do you want to continue with the removal of this package [y,n,?,q] y
## Verifying package dependencies.
## Processing package information.
## Executing preremove script.
Stopping NetWatch OAM Agents
        Kill NWOamAgent process:  828
## Removing pathnames in class <none>
/usr/local/bin/nwoamenv
/usr/local/bin <shared pathname not removed>
/opt/RSI/oam/reports
/opt/RSI/oam/preremove.sh
/opt/RSI/oam/postinstall.sh
/opt/RSI/oam/nwvxml.sh
/opt/RSI/oam/nwvstopimm.sh
/opt/RSI/oam/nwvsstat.sh
/opt/RSI/oam/nwtkr.sh
/opt/RSI/oam/nwstream.sh
/opt/RSI/oam/nwspfunc.sh
/opt/RSI/oam/nwsdlc.sh
/opt/RSI/oam/nwrenum.sh
/opt/RSI/oam/nwostart
/opt/RSI/oam/nwoamcmd.dat
/opt/RSI/oam/nwoam.sh
/opt/RSI/oam/nwnumsvc.sh
/opt/RSI/oam/nwmsgadm.sh
/opt/RSI/oam/nwmsg.sh
/opt/RSI/oam/nwhost.sh
/opt/RSI/oam/nwhlist.sh
/opt/RSI/oam/nwgetmsg.sh
/opt/RSI/oam/nwgetcmd.sh
/opt/RSI/oam/nweqpoptcard.sh
/opt/RSI/oam/nwdispsvc.sh
/opt/RSI/oam/nwdb.sh
/opt/RSI/oam/nwcus5rpt.sh
/opt/RSI/oam/nwcus4rpt.sh
/opt/RSI/oam/nwcus3rpt.sh
/opt/RSI/oam/nwcus2rpt.sh
/opt/RSI/oam/nwcus1rpt.sh
/opt/RSI/oam/nwchansvc.sh
/opt/RSI/oam/nwbus.sh
/opt/RSI/oam/nwass
/opt/RSI/oam/nwasaiver.sh
/opt/RSI/oam/nwasaistat.sh
/opt/RSI/oam/nwasaidom.sh
/opt/RSI/oam/nwasaichan.sh
/opt/RSI/oam/log <non-empty directory not removed>
/opt/RSI/oam/bandr.res
/opt/RSI/oam/OAMLic
/opt/RSI/oam/NWOamAgent
/opt/RSI/oam/NWOAMStop
/opt/RSI/oam/NWOAMStatus
/opt/RSI/oam/NWOAMStart
/opt/RSI/oam/NWOAMReinit
/opt/RSI/oam <shared pathname not removed>
/opt/RSI/cfg/nwoam.cfg
/opt/RSI/cfg <shared pathname not removed>
## Updating system information.
```

Remote Admin can be uninstalled using the Windows **Add/Remove Programs** capability from **Settings->Control Panel**. Clicking on the Remote Admin entry under the list of programs will bring up an Install Wizard that allows Remote Admin to be modified, repaired, or removed. Selecting the **Remove** radio button and clicking on the **Next** button will remove Remote Admin from the PC. A screen shot of this process is shown below.



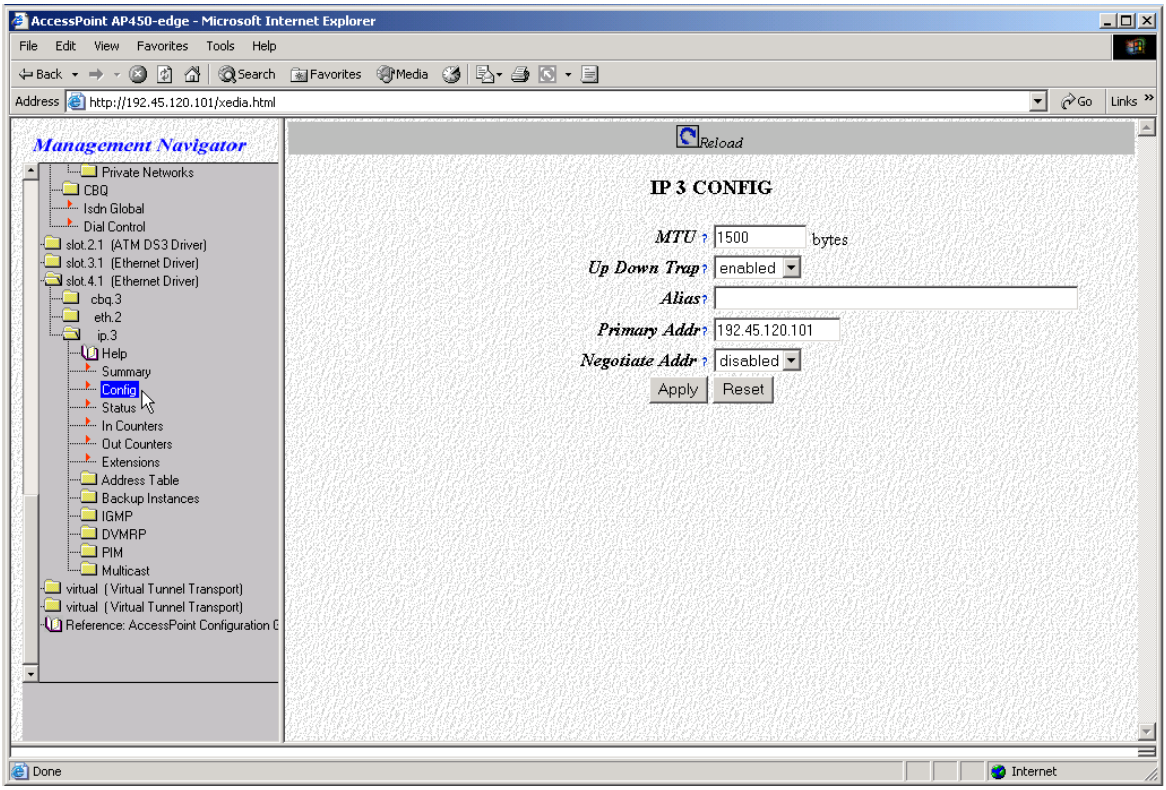
The Solaris package tool **pkgrm** can be used to remove NetWatch SNMP Monitor from the Avaya IR, if desired. The command format is:

pkgrm RSInwfms

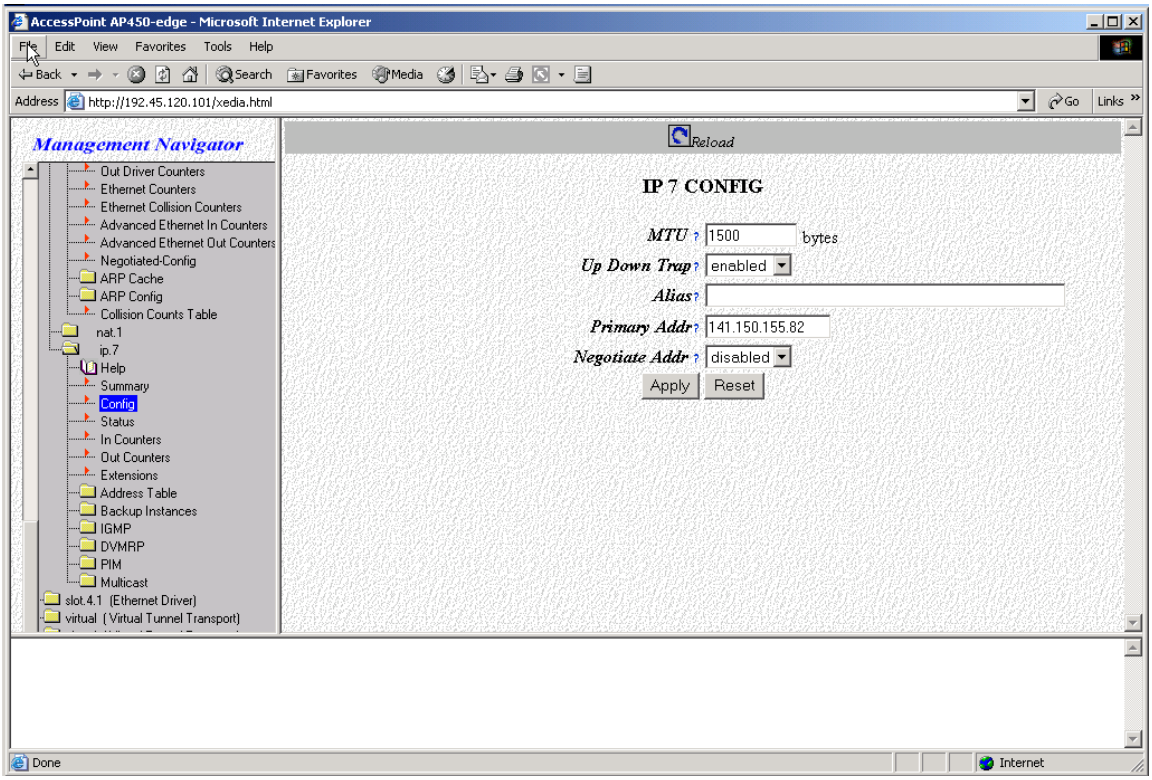
The output of this command is given below.

```
devconir280(root)# pkgrm RSInwfms

The following package is currently installed:
   RSInwfms         Avaya IR 1.2 System - NetWatch SNMP Monitor
                    (sparc) 4.0.8

Do you want to remove this package? y

## Removing installed package instance <RSInwfms>

This package contains scripts which will be executed with super-user
permission during the process of removing this package.

Do you want to continue with the removal of this package [y,n,?,q] y
## Verifying package dependencies.
## Processing package information.
## Executing preremove script.
Stopping NetWatch Agents
        Kill NWAgent process:  2689
        Kill NWBeep process:  2702
        Kill hostagt process:  2763
        Kill netwatchagt process:  2734
        Kill snmpdm process:  2721
        Kill nwnmsagt process:  2776
        Kill nwremoteagt process:  2789
## Removing pathnames in class <editfile>
## Removing pathnames in class <none>
/usr/local/bin/nwenv
/usr/local/bin <shared pathname not removed>
/usr/local <shared pathname not removed>
/opt/RSI/NW-FMS/sample/mypgm.sh
/opt/RSI/NW-FMS/sample/mypgm.c
/opt/RSI/NW-FMS/sample/makefile
/opt/RSI/NW-FMS/sample
/opt/RSI/NW-FMS/reports/trarpt
/opt/RSI/NW-FMS/reports/msgrpt <non-empty directory not removed>
/opt/RSI/NW-FMS/reports/custom4
/opt/RSI/NW-FMS/reports/custom3
/opt/RSI/NW-FMS/reports/custom2
/opt/RSI/NW-FMS/reports/custom1
/opt/RSI/NW-FMS/reports/cdsrpt
/opt/RSI/NW-FMS/reports/cddrpt
/opt/RSI/NW-FMS/reports/ccarpt
/opt/RSI/NW-FMS/reports <non-empty directory not removed>
/opt/RSI/NW-FMS/log <non-empty directory not removed>
/opt/RSI/NW-FMS/lib/libnwa.a
/opt/RSI/NW-FMS/lib
/opt/RSI/NW-FMS/include/nwxx_type.h
/opt/RSI/NW-FMS/include/nwxx_trap.h
/opt/RSI/NW-FMS/include/nwxx_proto.h
/opt/RSI/NW-FMS/include/nwxx_mesg.h
/opt/RSI/NW-FMS/include/nwxx_lic.h
/opt/RSI/NW-FMS/include/nwxx_hash.h
/opt/RSI/NW-FMS/include/nwxx_extn.h
/opt/RSI/NW-FMS/include/nwxx_eror.h
/opt/RSI/NW-FMS/include/nwxx_conf.h
/opt/RSI/NW-FMS/include/convsnmp.h
/opt/RSI/NW-FMS/include
/opt/RSI/NW-FMS/demo/timeout.sh
/opt/RSI/NW-FMS/demo/swap.log
/opt/RSI/NW-FMS/demo/pst.log
/opt/RSI/NW-FMS/demo/phrase.log
/opt/RSI/NW-FMS/demo/paging.log
/opt/RSI/NW-FMS/demo/mem.log
/opt/RSI/NW-FMS/demo/fsino.log
/opt/RSI/NW-FMS/demo/fsblk.log
```

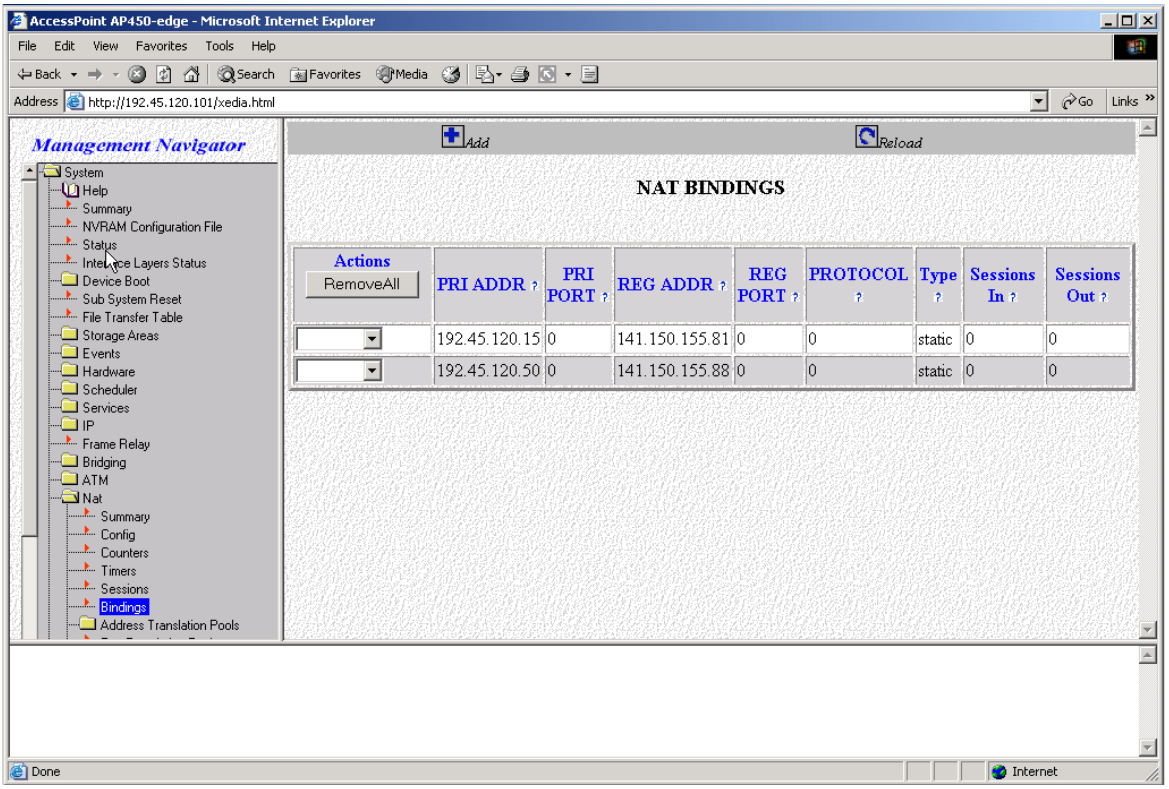
Appendix B: Firewall Configuration.

#	Configuration of AccessPoint
1	The Lucent AccessPoint can be configured by either a terminal connected to its serial port, or by a browser connected to its network port (assuming the IP address has already been configured).
2	In the test configuration, IP3 was configured to the Ethernet card in slot 4 and was assigned to the private internal network using IP address 192.45.120.101 as shown below. 

3	IP7 was configured to the Ethernet card in slot 3 and was assigned to the public external network using IP address 141.150.155.82, as shown below.



4	The NAT menu was used to bind the two internal private IP addresses to two external public IP addresses, as shown below.



Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya Solution & Interoperability Test Lab at interoplabnotes@list.avaya.com