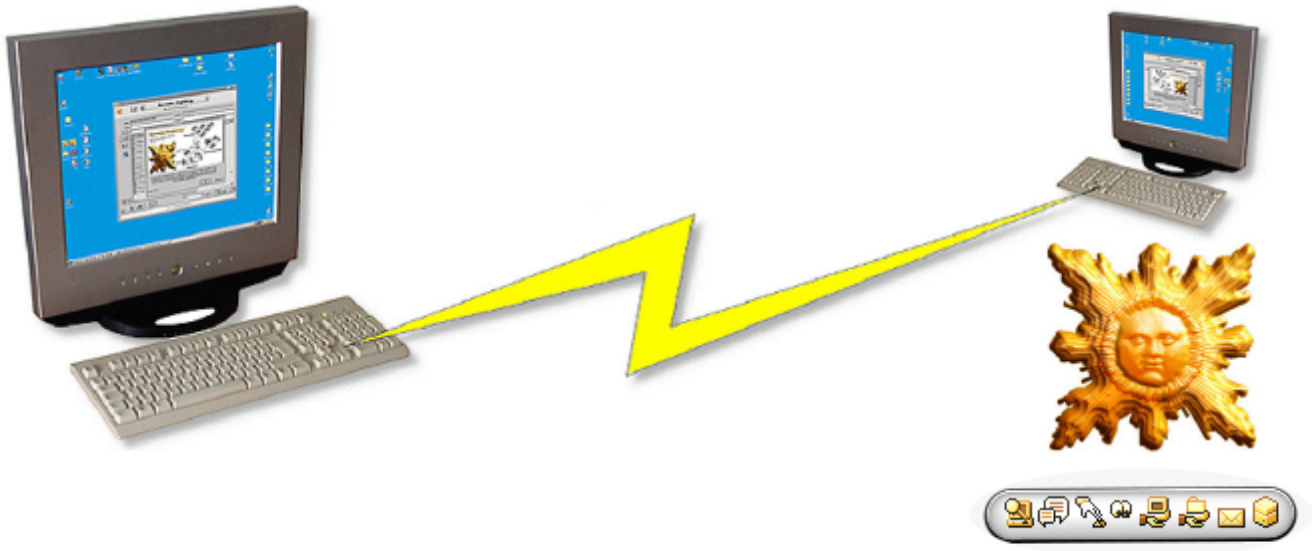
Remote-Anything

Version 4.3.3 for Windows (95, 98, Me, NT4, 2000 and XP)

Reference Manual



Copyright Notice

Warnings

Product specifications and the contents of this document are subject to change without notice. This document has been prepared with our utmost effort. However, if there are any queries or errors please contact eric.sanders@twd-industries.com. This document may not be copied, translated or transcribed in any form in part or in entirety without TWD Industries’ written permission.

Trademarks

Remote-Anything™, RA™, RA Gate™, RA Directory Server™ and RA DS™, are trademarks of TWD Industries SAS. Other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Table of Contents

System Specifications (minimum requirements)

- A PC or compatible, 386, 486, Pentium or higher
- 2 MB of free RAM or more (1MB for the Windows stack, plus twice the size of the video buffer)
- Windows 95, 98, Millennium, NT4 (SP3), 2000 or XP. *Master* and *Slave* can be used on all those Windows versions (even if they are mixed: a Win95 *Master* with a WinNT *Slave*)
- A VGA compatible Video Adapter or higher (supports resolutions up to 18000x16000 in 32-Bit)
- A Hard-Disk with 700 KB of free space for a *Master* PC (100 KB of free space for a *Slave* PC)
- A Mouse and a Keyboard
- A Network Adapter or a Modem or a Cable (null-modem or parallel) to link *Master* and *Slave*
- The TCP/IP protocol installed and working on *Master* and *Slave* PCs
- Winsock 2.0 (available since April 1996). Windows 95 users will have to download the Microsoft patch, W95ws2setup.exe (963 KB) from:
  http://www.microsoft.com/windows95/downloads/contents/WUAdminTools/S_WUNetworkingTools/W95Sockets2/Default.asp

Note: Optimal performances are achieved with appropriate hardware: among critical parts, a Network Adapter may double or triple the effective bandwidth -if the manufacturer is properly chosen. Some Windows Registry settings can also boost your connections (see the FAQ). Also, while RA supports any kind of resolution and color depth, keep in mind that you will get the best performances with a 16-Bit video mode (this is due to the way Windows works).

Please read the latest FAQ on http://www.remote-anything.com to learn more about performance hints and issues, TCP/IP installation, common problems, error messages, etc.

Product Overview

Remote-Anything (RA) is the most efficient solution to administrate or control computers via a LAN, a WAN, a Dial-Up connection (modem to modem), a serial or parallel cable, or via the Internet… and its volume pricing scheme allows organizations to install RA on all their PCs.

Whether you have to administrate thousands of PCs or you want to provide user assistance, training, maintenance services, or check service quality, RA is your best ally: even with a small support staff you can offer best-of-breed user services at an affordable cost!

- RA value grows with the time. In fact, instead of having an obsolete product after a new version is shipped, users of RA enjoy free updates the first year which they can download from the TWD Industries' web site.

Key Strengths

RA is radically different from the competition *by design, implementation and sales model*:

[*] available in a future version

- Instant Delivery: a 79*KB footprint* allows to request *and receive* support *instantly*! This allows for '*Deployment on Demand*' and reduced costs.

- Zero-Configuration: other products need days before you can use them. RA consists of *one unique 79KB file*. Double-click it and it's installed, configured, and operational!

- Firewall/Router Traversal (with the DS): Find any PC user by his name in the world! The DS allows you to locate, monitor and keep record of the usage of billions of PCs on a WAN. Centralize credentials, SOS Calls and logs!

- Ultra-Fast File-Transfer: the intelligent compression technology allows to transfer files at incredible speeds -just like if you had ten times more bandwidth!

- Text and Voice* Chat discuss as if you were on the phone! *Our technology requires a*

small bandwidth (only 2400 bps) while the competition typically uses 20 times more!

- Cross-Platform: Linux* / Mac* / Windows (95, 98, ME, NT4, 2000 and XP). Using any mix of the operating systems mentioned above. RA is written in portable C++ code.

- Real Support: We offer *free technical support* to registered and non-registered users and *free licenses* to those who find a new bug (we use to fix the problem in hours)!

- Free Updates: *You're not a customer for just one transaction. You're a customer for life*. As People can count on free updates, clients reward us with valuable feedback.

- Customer-Driven: RA is continually evolving because of the feedback of our clients. As a result, RA matches *all* their real-world needs better than any other product.

Note: RA is unique in the fact that *the same product* matches the needs of both the occasional mobile worker *as well as* the network administrator of a 20,000+ PC WAN.

More than 75% of our customers order more licenses after a first purchase because they believe in our ability to offer the reliability, consistency, and service they require.

Why pay more than needed to get deceptive service and obsolete products?
Purchase RA!

Installing Remote-Anything

RA consists of two single files (no DLLs, no dependencies):

Master.exe	**636 KB**	install it on the network administrator's PC
Slave.exe	**79 KB**	install it on all the PCs you need to access remotely

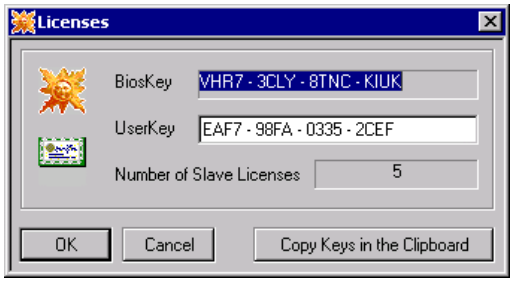
A *Master* and a *Slave* must be installed on -at least- two different machines. *Master* is used to remotely control the *Slave* workstation. *Slave* is a Windows Service and will automatically start at boot time before Windows (this allows you to log in remotely). *Master* and *Slave* can be installed *on the same PC* to control remote PCs -and to be controlled.

RA only supports PCs connected to **TCP/IP** networks (see how to install and configure TCP/IP in the **FAQ**). RA can also be used with **modem-to-modem connections**.

Installing a *Master*

To install a *Master*, you just have to copy *Master.exe* on the hard-disk of a PC, in the directory of your choice (the Windows Desktop is a good place).

The first time you run the *Master* you have to type in the supplied registration *UserKey*. If you do not have a *UserKey* you can type 'trial' to run *Master* in demo version (in this case, you will only be able to access *Slaves* with the password 'trial' and the port number '4000').



NT/2000: If you have installed and registered Master under a given user account then later you may be unable to use Master from another account. That's because you don't have the appropriate rights to access the Master options stored in the registry. To fix this problem, log in as Administrator, run Regedt32.exe, find the HKey_Local_Machine/Software/TWD key and then edit the permissions for all the keys and sub keys setting everyone supposed to use

Master to 'Full Control'. This way, the Registry key is available to any user logging in -which is what you need.

A *UserKey* to secure your *Master*

If one copies your registered *Master* or steals your hard-disk, he will not be able to access the *Slaves* installed on your network. As the BiosKey is based on the MAC address of the NIC, if you move *Master* to another PC, it will work in demo mode only (and will not be able to use passwords different from 'trial' and ports different from '4000').

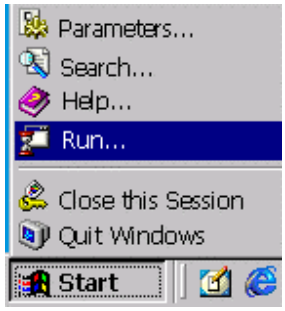
Installing a *Slave*

Installing a *Slave* on a single PC

Copy *Slave.exe* wherever you want on the hard-disk of the PC, and then double-click it. *Slave* is now running as a Windows Service (it will start automatically at boot time) and is ready to accept a connection from the *Master* with the default password: trial on the default port number: 4000 (during the installation, *Slave* will set the -default or personalized- bound options in the Registry: HKEY_Local_Machine/Software/TWD/Remote-Anything).

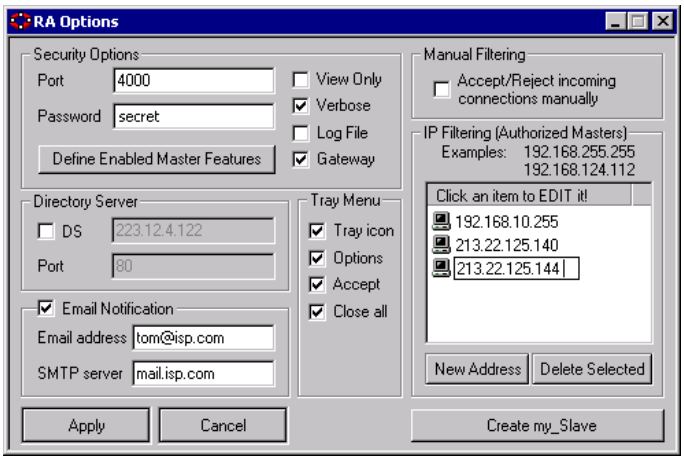
Registered users can use a personalized password. To display the *Slave* Options dialog:

Click on the Tray Icon in the Task Bar **OR** Type in '*Slave* -o trial' in the 'Run' dialog:



Slave options are described later in this Manual in the 'Security Options' Chapter.

Note that some of the default *Slave* options can be changed: you can bind options to a *Slave* so it will install your options when you run *Slave* on a PC for the first time.



Deploying a personalized *Slave*

Just copy a personalized *Slave* on every computer and run it: it is installed and configured! (See the 'Security Options' Chapter later in this Manual to make a personalized *Slave*)

You can send this personalized *Slave* by email, or let End Users download it from your web site: all they will have to do is just run it (a simple double click on the *Slave* icon) and you will be able to access their computer with your password and port number!

If you wish later to add *Slaves* to your network, you will only need a new *UserKey* from TWD Industries. After the new *UserKey* is updated in the *Master*, licenses are ready to use.

Remote Installation on a NT Server

You can reach a remote Server via TCP/IP but RA is not installed and you need to remote control this Server. There is a solution if you have the Administrator account of the distant PC! Open a DOS box and type the following commands:

NET USE \\192.168.112.24	**(type the IP of the remote PC)**
\IPC$ /user:administrator password	**(type your password)**
COPY "C:\Slave.exe" "\\192.168.112.24\C$\WinNT	**(or C$\Windows)**
NETSVC \\192.168.112.24 schedule /start	**(run scheduler)**
NET TIME \\192.168.112.24	**(get the PC time: 9:58)**

AT \\192.168.112.24 10:00 "C:\Slave.exe" **(run Slave.exe)**

That's it! RA is running on the remote PC so you can access it with Master! You can also use the following commands:

REGINI -m \\192.168.112.24 ra.reg **(install Registry settings)**
SHUTDOWN \\192.168.112.24 /R /Y /C /T:0 **(reboot the remote PC)**

Deploying RA with a NT Script

Here is a NT script sample to install a personalized Slave.exe file as a service on a remote computer. Under NT, the user running this script must have Admin privileges. To execute this script on networked PCs, you can use the NT logon script.

```
net use T: \\server1\d
copy "T:\Programs\RA\Slave.exe" "C:\WinNT\Slave.exe"
C:\WinNT\Slave.exe
net use T: /delete
```

This script performs the following operations to install a Slave:

1. Create a logical drive T: mapped to \\server1\d
2. Copy the Slave.exe file from the server to the Windows folder of the PC
3. Install Slave.exe as a Windows Service on the PC
4. Delete the T: logical drive

You will need to change the paths of this example to match the real paths of your systems. Note that you can install a Master with the same script (replacing Slave.exe by Master.exe).

Using *Master* and *Slave*

RA is extremely optimized and allows you to remotely use any Windows program or to watch a video playing on a distant computer. RA's powerful compression algorithm saves the bandwidth of your network and on-the-fly encryption protects your data. Do not worry about having to keep and maintain a list of IP addresses: RA detects and lists for you the PCs you can reach on your network. All you have to do is to choose one!

Using *Slave*

Slave Command Line Syntax

To get the following help dialog type in:

C:\Windows> *Slave* -h [return]

All the options are described in the 'Security Options' chapter.

⇨ *Slave*.exe can be run from the command line or with a double-click. If *Slave* is not installed yet then it will store the options in the Registry (HKEY_Local_Machine / Software / TWD / Remote-Anything), will register as a Windows Service (so it will start automatically at boot time), and will start within a few seconds so you can establish a connection from a *Master* PC. If *Slave* is already installed, it will simply run.

Using *Slave* in the context of a given user (Application V.S. Service)

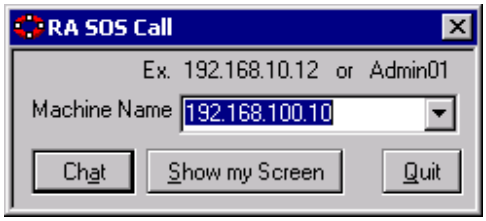
NEW If you run Slave.exe as a simple Application (instead of as a Service) then Slave.exe is running in the context of a given user (instead of 'System'). With Terminal Server, you can monitor the desktop of a given user just by running Slave.exe from the 'startup group'. To activate the Application Mode, simply add the string value "sApp. Mode = 1" in the Windows Registry (HKey_Local_Machine/Software/TWD/Remote-Anything).

Note: Automatic installation and update features, as well as the system login (Ctrl-Alt-Del) and the NT Event Log, are not available in the Application mode.

Displaying the *Slave* Tray Menu & IP Address

You can access the *Slave* **Options** by clicking the ***Slave* Tray Icon**. The Tray Menu allows you to **'Close All (established) Connections'**. If you uncheck '**Accept Connections**' this will block all incoming connections. The '**About…'** item will display the ***Slave* version** and the **Slave IP Address**.

'**Send an SOS…**' displays the connection dialog box:



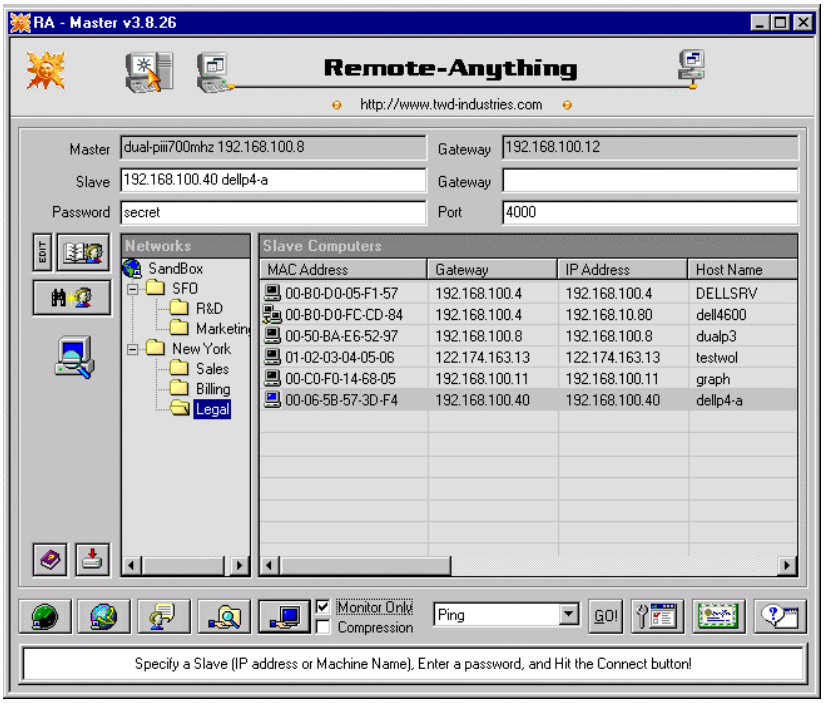
It allows a *Slave* User to **call a *Master*** (Text Chat) or directly to send its screen to a specified *Master*.

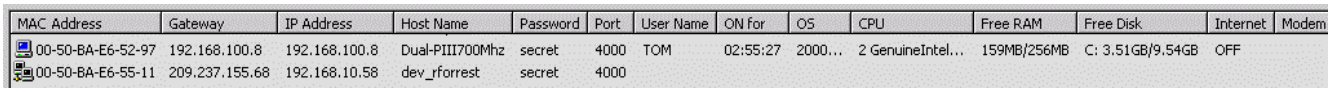
Using *Master*

Once *Masters* and *Slaves* are installed, a *Master* can access remotely any *Slave* PC.

The Connection Dialog

The button detects *Slaves* installed on a LAN. Click on it and you will see new IP addresses (209.237.155.62 for example) and information about *Slaves*: Mac address, Gateway address, Password, Port, User Name, working time, OS, CPU type, Total / Free RAM, Total / Free Disk space, Internet Connection Status and Modem type.



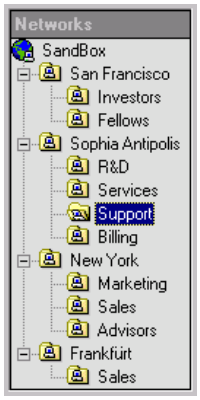


MAC Address	Gateway	IP Address	Host Name	Password	Port	User Name	ON for	OS	CPU	Free RAM	Free Disk	Internet	Modem
00-50-BA-E6-52-97	192.168.100.8	192.168.100.8	Dual-PIII700Mhz	secret	4000	TOM	02:55:27	2000...	2 GenuineIntel...	159MB/256MB	C: 3.51GB/9.54GB	OFF	
00-50-BA-E6-55-11	209.237.155.68	192.168.10.58	dev_rforrest	secret	4000								

You can resize each column to a null size if you want to hide one or more columns.

➪ The MAC (Medium Access Control) address is listed to avoid duplicate entries (we can recognize a PC even if its IP address has changed). It is also necessary for the Wake on LAN feature. The MAC address is found automatically during a RA connection or by the auto-detection and the 'Get Hardware Information' features. You can also enter it manually in the Address Book ('WinIPcfg.exe' and 'IPconfig.exe /all' on the Slave PC allow to retrieve it).

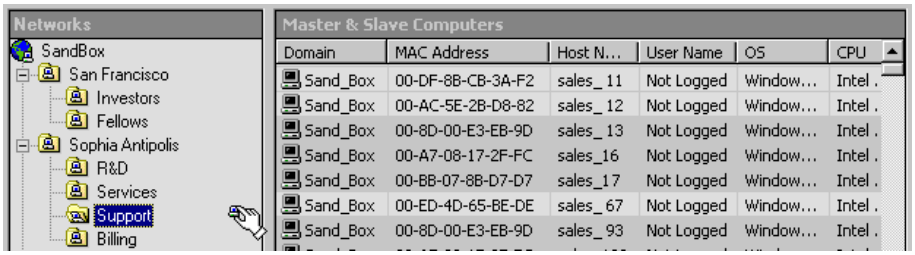
How to arrange PCs in Network Folders



If you need to work with a lot of PCs then you may find it more convenient to organize your PCs in 'Networks'. There is no obligation for you to use several Networks to split your list of PCs -this may just be more convenient.

The default **'SandBox'** Network is provided to collect PCs that do not (yet) belong to a user-defined Network. It will be useful to indicate new PCs when new Slaves will be installed in the future.

➪ To edit a Network name just click on one item of the tree. Press the [INS] key to create a Network. Press the [ENTER] key to save a record (or the [ESC] key to cancel changes). Press the [DEL] key to delete a network.



In order to associate PCs with a Network, just drag & drop PCs from the Computer List to the Networks Tree.

Note: You can move PCs from one Network to another Network at any time but it is far easier to deploy your Master and Slaves by Networks and wait that they are listed. Then, you can drag & drop them in just one step in the appropriate Network and deploy RA on

another Network, drag & drop them in a new Network folder, and so on...

Establishing a Connection

In order to establish a connection with a *Slave*, you have to specify a *Slave* **IP address** (or DNS name) and a **Password** in the Connection dialog (if you do not provide a port number, Master will use its default port number).

Click on the  Button (the password is 'trial' if you are in demo mode) to establish a connection with a *Slave*. You can also double-click a *Slave* in the list. The '**Monitor Only**' and '**Compression**' checkboxes allow you to override the *Master* options (see *Master* options later in this Chapter).

You will see the following window while the *Master* is attempting to establish the connection with the distant computer. If it fails, an error message will tell you why.

Note: A *Master* can establish more than 100 *simultaneous* connections to different *Slaves*. A *Slave* can be controlled/monitored by more than 100 different *Masters* at the same time.

How to find the IP address of a Slave PC

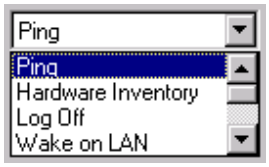
Even when you have defined a fixed local IP address for your PC on a LAN, each time you get connected to the Internet, your ISP is allocating a new routable IP address which will be used via the Internet. If a Master wants to connect to a Slave via the Internet, it needs the Slave routable (or 'public') IP address, not the Slave local (or 'private') IP address.

The most powerful way to detect Masters and Slaves is to use the TWD Directory Server (see http://www.twd-industries.com/en/downloads.htm). But to find a Slave IP address, you can use a 'fake' domain name (see http://www.dns2go.com), or the RA Port Scanner, ICQ, Yahoo Messenger, the IRC, a phone call, a fax, or the embedded Slave IP address email notification. Read the 'Slave security Options' chapter to learn how to setup a Slave in order to be notified the Slave IP address by email.

Displaying Online Help

The first of the  buttons gives access to the RA online Manual (or run Acrobat Reader to display the PDF Manual if it is stored in the *Master* directory) while the second button opens a 'save as' dialog to save on disk the *Slave* list as an ASCII text file.

Unconnected Features (Ping, Wake on LAN, etc.)



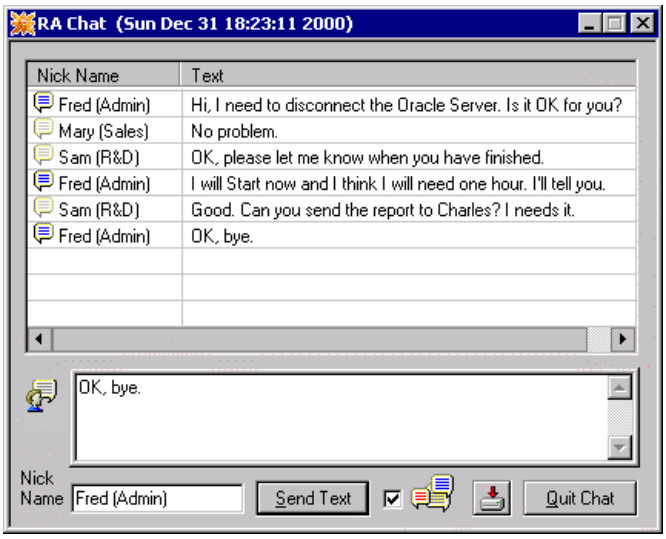
➪ The **Ping** command is in a combo box with some other commands like: **Hardware Inventory, Log Off**, **Wake on LAN**, **Shut Down, Reboot**, **Lock Up** and **Uninstall**. You can apply those commands to ***one or several selected Slaves*** from the *Slave* List with a single mouse click (if the *Slave* has been configured to accept these commands).

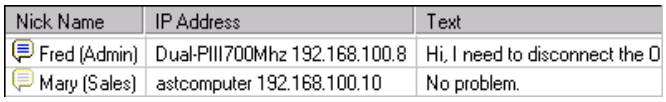
For example, you can select a few *Slave*s, try to shut them down, wait a bit, and then use Ping to check if they are all powered down (a blue PC icon will show PCs still ON).

Text Chat and Conference

The  button opens a dialog box to start a Chat session with the selected *Slave* User(s). You can change your **Nick Name** and enable or disable on-the-fly the **Conference Mode**. In the normal mode, the answers you receive from *Slave* Users will not be visible to all other *Slave* Users. The Conference Mode will broadcast every *Slave* User answer so all of them will know what was written (they will not *only* see your text).

- The Conference Mode is only available when you establish a session with more than one *Slave*. The '**Save to Disk**' button allows you to save the Chat text in a Text File. To send your text, you can press **Alt+S** or click the '**Send Text**' button (the text is encrypted when transmitted).
- There is an extra column (reduced by default) that you can enlarge to find one's IP address. To show it, just put the mouse cursor between the two columns and drag it to the right.

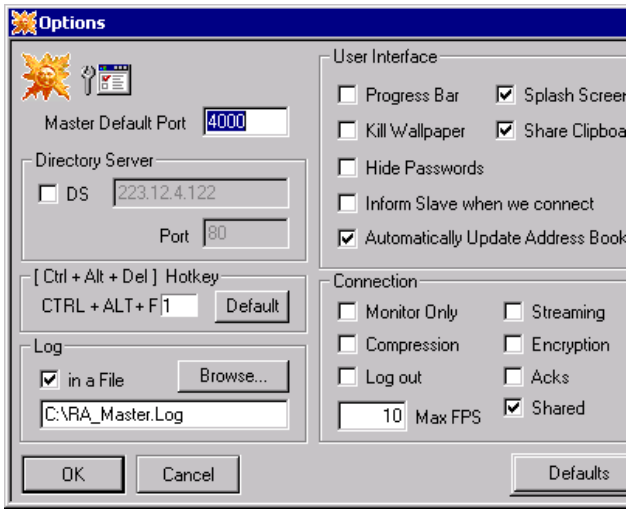




- The  button opens the File Browser to transfer files between the selected *Slave* PC and your PC (the File Browser is described later in this document).
- The  button allows you to check which TCP ports are listening on one or several remote PC(s). With this tool you can find other PCs using RA but you can also detect all the other TCP/IP programs used on a remote PC (like a web server). This port scanner is extremely fast: it tested 2000 ports per second on a LAN with a powerful PC.
- The  button traces the route used to reach the specified PC, listing the routers that relay the connection between the Master PC and the specified PC. This allows you to identify the connection point that slows down your RA connection for example.

- ***Master* Options**

- ⇨ The  button opens a dialog box which allows you to change the base ***port number*** used by the *Master*. If you change it, do not forget to change it also for *Slaves* (see 'Security Options').



  Enable or disable:
- **Progress Bar** show transferred data
- **Hide Passwords** hidden in the main dialog
- **Share Clipboard** *Master* ✍ *Slave*
- **Splash Screen** show/hide, quiet mode
- **Inform *Slave* when we connect** *Slave* will be notified of *Master* connections by a dialog box
- **Kill Wallpaper** remove the Wallpaper so we save time and bandwidth
- **Automatically Update Address Book** disable it if you use a Router or a DNS name to reach a Slave: when enabled, RA will always try to update the Address Book with the Slave IP address
- **Monitor Only** this mode disables the mouse and the keyboard, the Master can view only
- **Streaming** speedup slow connections by segmenting updates in smaller packets
- **Compression** speedup slow connections, saving bandwidth at the expense of the CPU load
- **Data Encryption** secures transmissions by making data unreadable
- **Acks** can boost a modem connection. Never set it on a LAN, it uses CPU and bandwidth
- **Shared** uncheck this option to be the only Master at a time to establish a connection with a Slave
- **Log out when disconnect** log off from Win9x, NT and 2000 and start the screen saver on Win9x
- **Max FPS**: that's the number of screen updates (frames) per second you want the *Slave* to send to the *Master*. The greatest the best for speed but also the most demanding for the *Slave* CPU. If you are using a slow connection (Internet or dial-up) then set a value of 1-2 because the bandwidth you have will not allow you to get more. On *fast* networks, you can use 10 or 15 (up to 100)
- **Log** in a file: all operations will be logged. Useful in case of severe security requirements or to isolate or debug a problem
- **Ctrl+Alt+Del** (Hotkey) allows you to select the key that will allow you to initiate a remote Logon
- **DS** This option is used only when you have purchased the Directory Server.

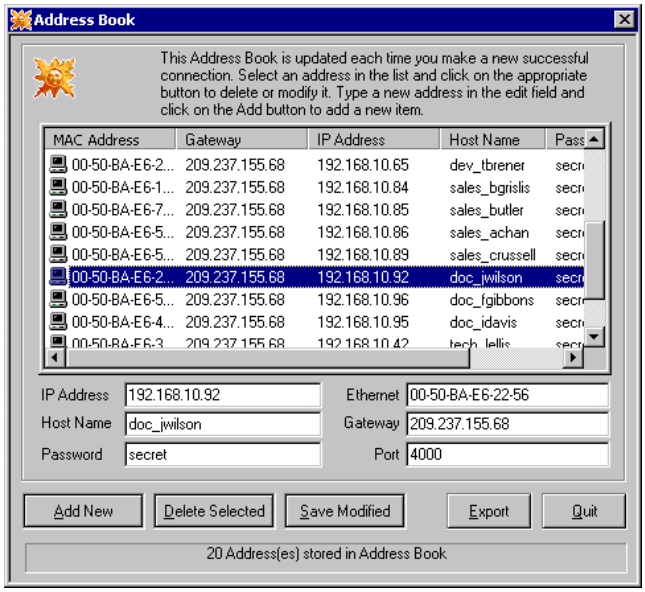
Address Book

Clicking  will display all the PCs you have established a connection with (they are stored in the Address Book).

The **EDIT** button opens a dialog box which allows to add, delete, or modify entries, as shown on the picture.

After a connection is established, a new entry is automatically stored in the Address Book.

You can quickly fill this Address Book by testing *Slaves* after their installation.



➪ You can **import** an Address Book from a *Master* PC to another *Master* PC with a *.reg file. To do that, **export** the Address Book from the first *Master* PC, copy the resulting *.reg file on the second *Master* PC and just run the *.reg file (or double click it).

Slave Auto Detection

The Broadcast button  sends an information request over the network to detect active *Slaves*. Detected PCs, if any, are displayed (with a blue PC icon) in the *Slave*s List. This is very useful for finding *Slave*s the first times, when addresses are not yet stored in the Address Book. With it you can check which PCs are running and available on the network at a given time and retrieve the 'Hardware Information' described above.

If you do not see a PC while you know that this PC is available, click two or three times on the auto-detection button. The PC you are looking for may be too busy to answer immediately or may be too far from you (the answer of the distant PC may take a few seconds to come back to you). If the Slave auto-detection does not work for you because you have blocking UDP broadcast packets (see the **FAQ** for more about this), then you can use **Ping** or **Hardware Inventory** from the combo box to check if a PC is available.

Connection Shortcuts or Batch File Transfers! (RA Command line arguments)

➪ To establish a connection directly from an icon on your Desktop just create a shortcut with the following information:

Master.exe [SlaveGate] <Slave> <Password> [Port Number]

([SlaveGate] and <Slave> can be an IP address or a DNS name)

Example: C:\Windows\Desktop\Master.exe 192.168.10.2 trial

Master can be called by another program or by a script.

- Master can transfer files when invoked from the command line.
  The syntax is:
  ([ ] denote an optional parameter while < > specify a mandatory parameter)

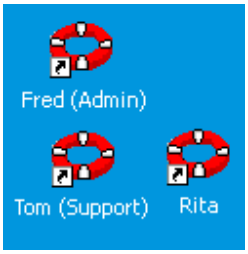
  Master -getfile <SourceFile> <DestPATH> [Gateway] <SlavePC> <Pwd> <Port>
  Master -sndfile <SourceFile> <DestPATH> [Gateway] <SlavePC> <Pwd> <Port>

  Example with a Slave Gateway:
  Master -getfile c:\file1.txt c:\folder1 10.1.1.12 10.1.10.2 secret 4000
  Master -sndfile c:\file2.txt c:\folder2 10.1.1.12 10.1.10.2 secret 4000

  Example without a Slave Gateway:
  Master -getfile c:\file1.txt c:\folder1 10.1.10.2 secret 4000
  Master -sndfile c:\file2.txt c:\folder2 10.1.10.2 secret 4000

  Master can be called by another program or by a script.

➪ ***Slave*.exe** can also be called from the command line to show its screen to a *Master* (the *Master* has to be running at this time):



Slave.exe -n <Master>

(<Master> can be an IP address or a DNS name)

Example: C:\Windows\Slave.exe -n 192.168.12.16

Note: < > indicate a required parameter while [ ] indicate an optional parameter.

☞ Once connected, you can see a window showing the screen of the distant PC:

If this is not the case, consult the FAQ for a checklist of common issues and pitfalls.

SPEED: How to get MORE Frames Per Second

To save CPU and bandwidth, RA does not transmit data if *nothing* changes on the Slave screen. To get the maximum speed available at a given time, just move the mouse cursor on the area of interest. RA will transmit the screen updates as fast as possible until the mouse stops moving. This trick is more efficient if the '**Active Window Updates**' option (explained later in this chapter) is selected.

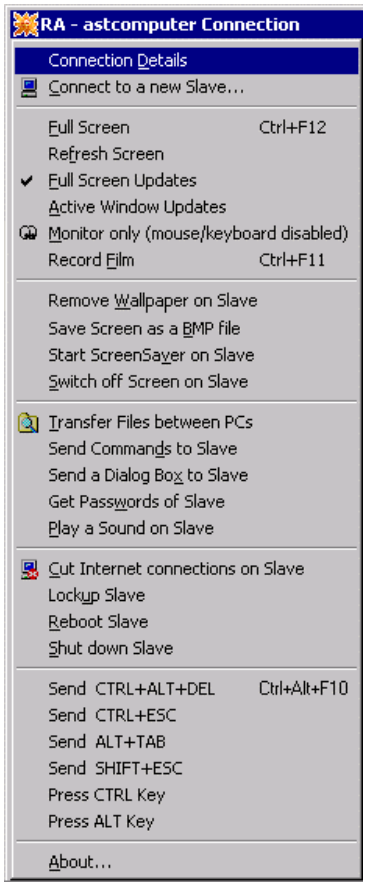
Example: if you select a sub-menu, move the mouse cursor *where the menu will be displayed*, this will bring it faster. If you open a new dialog, don't wait for it: move the mouse where it will come. If you watch a video, move the mouse over the video to get more speed.

Note: To speedup **DOS applications** start Explorer, select the file Windows_default.pif (yes,

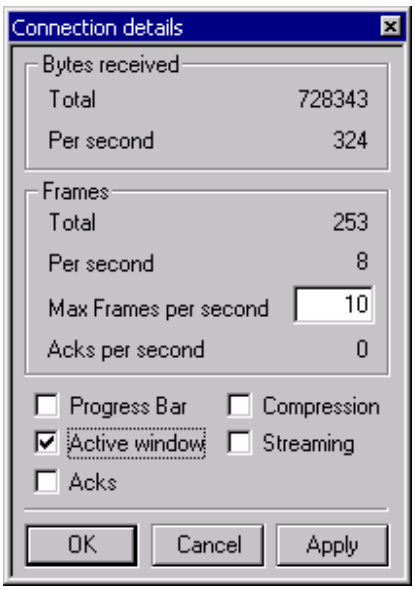
that is an underline), right mouse click, select “Properties”, select the “Misc” Tab, move the slider under “Idle Sensitivity” to the right (High), and apply the change. This same procedure would apply if you had created a unique PIF for the DOS application.

Master Menu Features

Once connected, the *Master* menu can be displayed by clicking the Title Bar with the right mouse button or by clicking the icon (see the image below) with the left mouse button:



Connection details opens a dialog box with real-time information about the current connection:



Tune the settings *while you are connected*, and reduce the CPU load (as low as 1-3%) playing with the settings to find the best possible refresh rate. **Compression**, **Streaming** and **Active Window** will speedup a modem connection but slow down a LAN connection (**Active Window** will only refresh the current window so if you need to refresh the full-screen just click on the place you want to be updated).

If you want to reduce the impact of a connection on a *Slave* CPU, reduce the **number of Frames** per second (and also disable **Acks**, **Encryption**, **Compression** and **Streaming**).

- **Connect to a new *Slave*** displays the Connection dialog which allows you to open a new window on another distant PC (thus you can intervene on more than one computer at the same time).
- **Full screen** switches the Full Screen mode and the windowed mode (and vice-versa). To toggle the Full Screen mode and the windowed mode, you can also use the **Ctrl+F12** hotkey.
- **Refresh screen** sends a request to the *Slave* to update the distant screen on the *Master*.
- **Full screen Updates** (default mode) scans and updates the full screen.
- **Active Window Updates** only updates the foreground window. This mode is faster than the Full screen Updates mode and requires less CPU resources of the *Slave* PC but does not redraw the

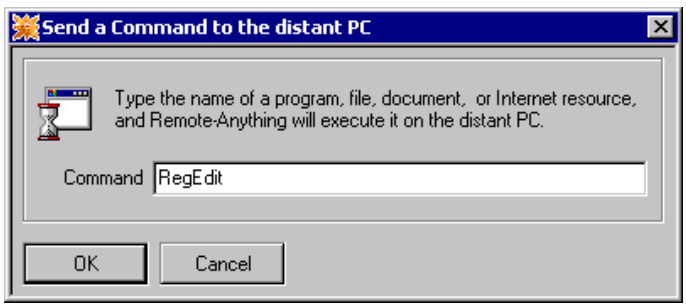
full screen; some operations like window moves may leave unwanted remainders. To erase them, you just have to click one time on the desktop window (it forces a full-screen refresh). This mode is especially useful to watch *real time* windowed video. It is also useful when you want to do something accurately with the mouse cursor, like drawing, because the mouse is more responsive. The smaller the Active Window, the best the results will be.

- **Monitor only** switches the visualization mode (mouse and keyboard inactive) and the active mode (where mouse moves and keystrokes are transmitted to the distant PC).
- **Create movie** creates a file called "[machinename][width]x[height](film#).FLM" in the Master's folder to record all that has been displayed on a Slave screen. Replay this file with the 'RA Session Player' (Player.exe). Check the 'Compression' Master option to make smaller (compressed) movie files. Use the **Ctrl+F11** hotkey to start/stop recording.
- **Remove wallpaper on *Slave*** removes the wallpaper from the distant desktop. It speeds up transmissions since there is less information to process.
- **Save Screen as a BMP file** opens a 'save as' dialog box which allows to save a copy of the distant screen as a bitmap on a disk.
- **Start Screen Saver on *Slave*** *immediately* runs a screen saver. This is really handy when you want to block the access to a PC after you have finished working remotely on it. In this case, you have to use a password-protected screen saver. NOTE: the screen saver may be immediately disabled if you are moving the mouse to select this option (use the keyboard or switch to 'Monitor Only' before selecting this menu option).
- **Switch off Screen of *Slave*** *immediately* powers off the screen (Windows 9x only). This option will really prevent everybody from working on the PC since it is not possible to see the screen contents. NOTE: This option will act like a screen saver if the display is NOT able to power off, in this case this option may be immediately disabled if you are moving the mouse to select it (use the keyboard or switch to 'Monitor Only' before selecting this menu option).
- **Transfer Files between PCs** displays an Explorer-like window with local and distant file systems and allows drag & drop to send and receive files (rename, delete them, etc.).
- **Send Commands to *Slave*** displays a dialog box which allows you to run programs, to open documents, to send e-mail, or to surf on the Internet with the distant PC. This is an equivalent of the 'Run' option of the Windows' Start menu.
- **Send a Dialog Box to *Slave*** allows to send a dialog box (with a title, a text, and an icon) to the distant PC.

- **Get Passwords of *Slave*** retrieves the passwords cached by Windows on the distant PC. Here is the screen saver password, if any, and those defined by Microsoft applications like Frontpage, but also network shares, dial up connections, FTP and HTTP authentication, etc. (Windows 9x only).
- **Play a Sound on *Slave*** plays a WAV sound on the distant PC (this is the default sound: 'ding', if you did not change it).
- **Cut Internet connections on *Slave*** stops immediately every active connection on the distant PC (HTTP, FTP, Email, etc.).
- **Lockup *Slave*** blocks the mouse and the keyboard on the distant PC until you select this option again to unlock inputs.
- **Reboot *Slave*** forces all applications to quit and reboots the distant PC. You will be able to reconnect to this PC once Microsoft Windows has restarted.
- **Shut Down *Slave*** forces all applications to quit and switches off the distant PC (the PC will power-off if the power supply implements this feature).
- **Send Ctrl+Alt+Del, Send Ctrl+Esc, Send Alt+Tab, Send Shift+Esc** sends complex keystrokes to the distant PC that would be interpreted by the local computer if typed at the *Master* keyboard.
- **Ctrl Key, Alt Key** will keep 'pressed' these control keys on the distant PC. You will have to deselect those options to 'release' the chosen control keys.
- **About…** displays a dialog box where the product version number of your copy can be found.

Sending Commands

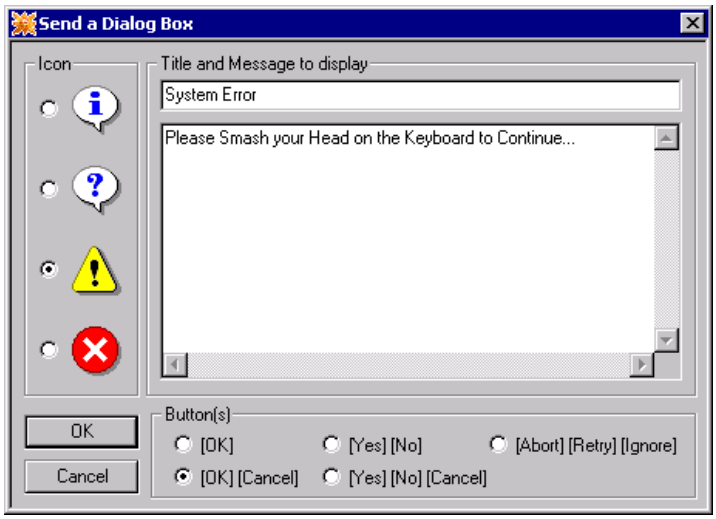
The **Send Commands to distant PC** option opens a dialog box which allows to run programs without knowing where they are located, to open documents without knowing which program is associated with, etc.
It is faster than a DOS box or than the Explorer since you do not have to look for what you want. Note that this is NOT a DOS prompt equivalent (del c:\autoexec.bat will not work).



Try: C:\Windows, image.bmp, Letter.doc, readme.txt, mailto:bgates@microsoft.com, SysEdit, RegEdit, etc.

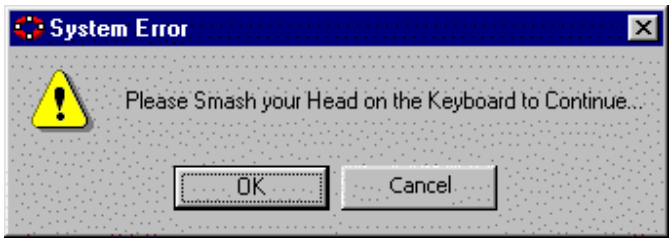
Sending a Dialog Box

The **Send a Dialog Box on distant PC** option opens a dialog box which allows you to create a message box you want to send to the distant PC.



Choose an icon if you want one and type the title and text of your message. The dialog box will be displayed immediately on the distant PC and will stay there until someone clicks on the 'OK' button.

This is an alternative way to communicate in the company… and the only one which grants you that the addressee will get it as soon as he uses his PC. We will enhance it by collecting answers in the DS database.



Getting System Passwords

The **Get Passwords of distant PC** option gets all the passwords cached by Windows: passwords for the screen saver, for applications like Microsoft FrontPage, for Internet and network connections. Get the screen saver password of a PC… and access it even if the user is on holidays!

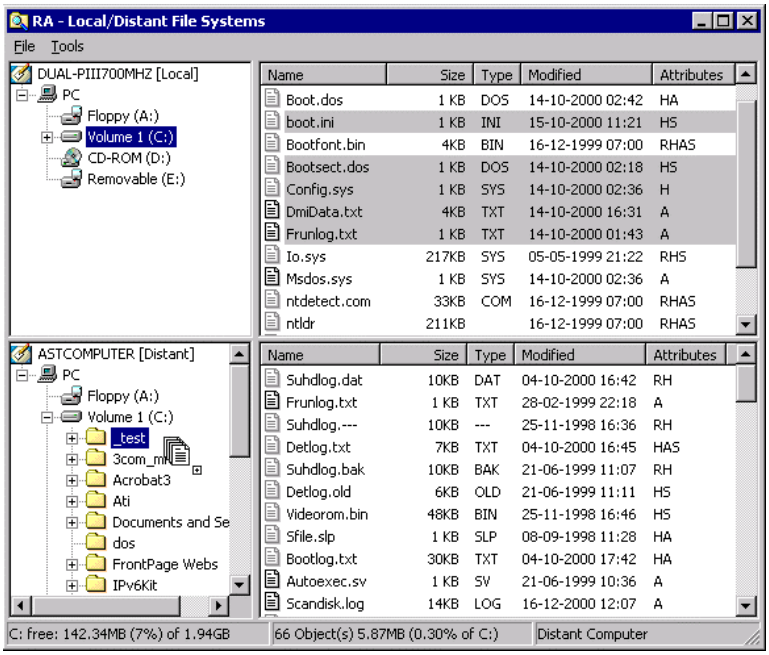
Note: This feature is not accessible with Windows 2000.

File Transfer

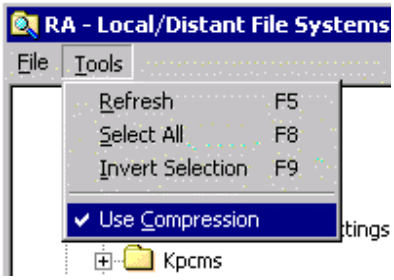
The **Transfer Files between PCs** option gives you a two paned window which allows you to copy files from one PC to another, using **Drag & Drop**, just as you could with Windows Explorer.

Those transfers are made without disturbing the *Slave* End User and without the need for an active Windows Session or shared disks.

To **create a new folder** press the **[Ins]** key or use the menu. To **rename a file or a directory**, just click on its name to edit it or press the **[F2]** key.

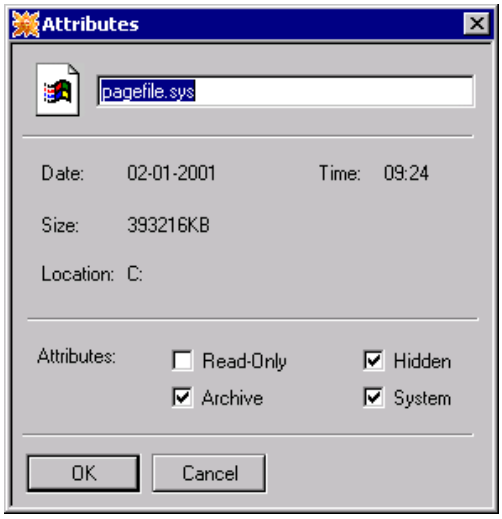


NEW The File Browser has a new '**Use Compression**' option to speedup file transfer. Enabling compression can lead to transfer 99% LESS data over the wire depending on the nature of the file you transmit (text files will compress better than *.zip files). This option is so efficient that we enabled it by default (it may give a boost of performances on any kind of connection).



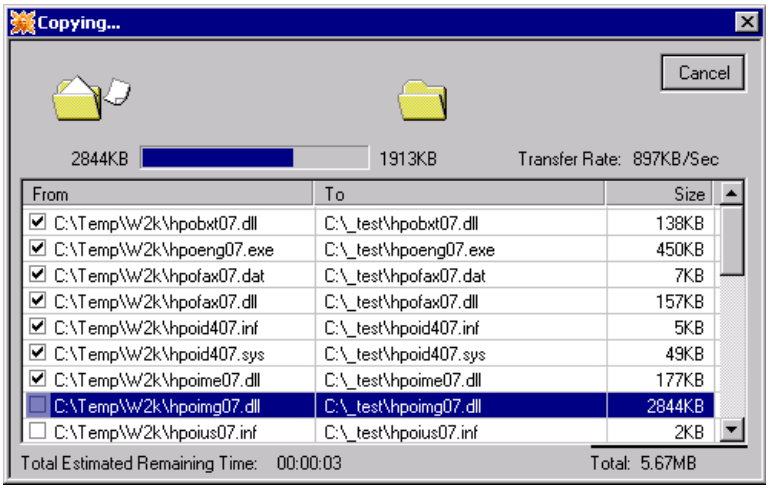
- The **[F5]** key **updates the file list having the focus** (click it to make sure it has the focus and then press F5). The File Browser allows to **rename folders** and to **edit the file attributes**. Also, the **position and size** of the **window and** the **columns** are saved after each session.

If you hit the **ENTER** key while a file is selected, then you will see the **Attributes** dialog which allows you to rename a file or to change its attributes. Note that you can rename a file simply by clicking on its name in the File List.

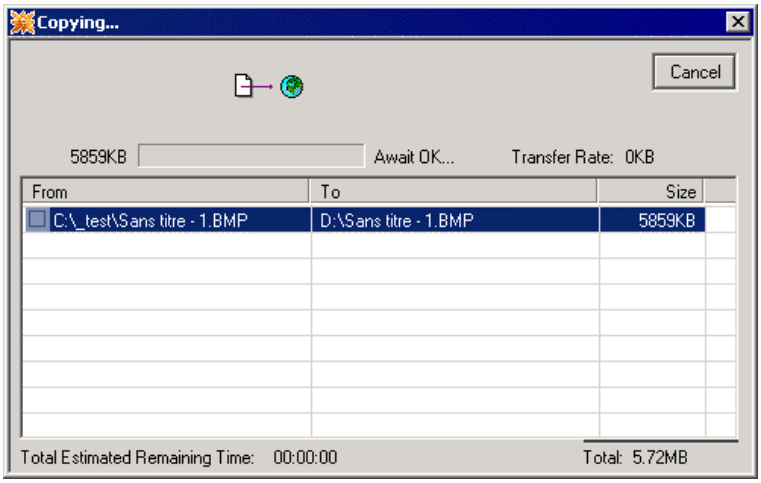


While displaying the file browser, you are still able to see what the distant user is doing. It allows you to check or update the distant system without disturbing the distant user and without being obliged to physically go to the distant PC.

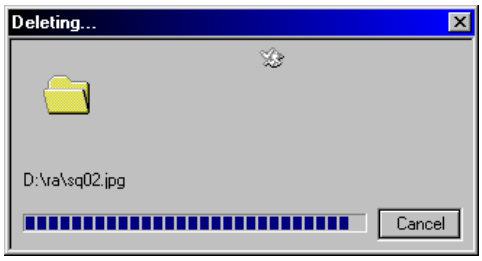
- The **file copy** dialog details the copy status: you have the **transfer rate**, **current status for each file**, the **total number of bytes to copy** and the **total estimated remaining time**. The copy is synchronized: if you hit the '**CANCEL**' button while a copy is in progress, the process will be interrupted immediately.



NEW After each file has been sent to a Slave, Master is waiting for a confirmation from the Slave PC that the file has been saved on a disk without error. If you are using the compression option, *it can take longer to receive this confirmation than to make the copy itself!* That's because the Slave PC may have to dump on disk several MB of data while a few KB only have been transferred.



This dialog box is displayed during file deletion. As file deletion is an extremely fast process, it may be difficult to stop it and almost impossible to stop it where you want it to stop.



To transfer files quickly, you can minimize the window of the distant screen (see below) to put it at the bottom of the screen, on the Task Bar. If you do this, as the *Master* will not actively request *Slave* updates of the distant screen, you will benefit from all the available bandwidth during file transfers.

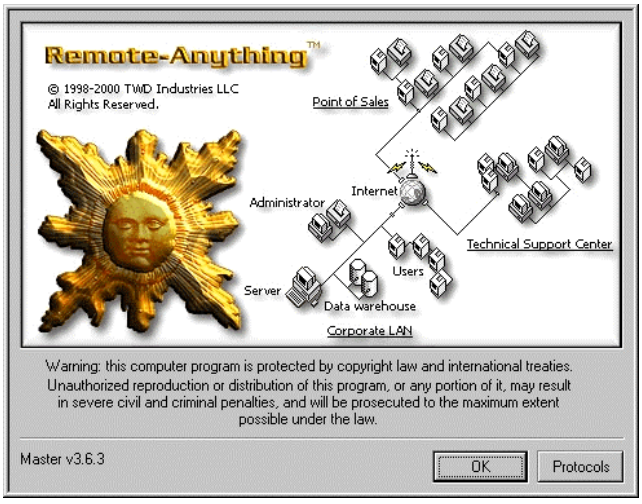
If you minimize the distant PC window into the Task Bar, the *Master* will stop sending requests to the *Slave* but will keep the connection open. This allows to keep a connection active while not using network and CPU resources of both distant and local PCs. When you want to use again the *Master*, click on Remote-Anything in the Task Bar (see the image below). You can 'freeze' several connections this way at the same time.

If the distant user modifies the structure of a disk (deleting a directory or adding new files for example), RA will automatically update the modified objects in the file browser when you select one of them (you can also use the [F5] key to refresh a file list).

Checking installed protocols

The **About** menu option displays a dialog with the product version number. To get free upgrades of our products, come often on our web site to check for new versions.

The **Protocols** button will allow you to check which protocols are installed on the *Master* PC.



Remote-Anything Security Options

Why modify the default Options?

Once RA is installed, and even *before* installing it, you can have very good reasons to think about modifying -at least- the default **password** (trial) and default **port number** (4000):

- If you are using the 'trial' password, every demo user can access and control your *Slaves*
- Changing passwords from time to time enhances the security of your systems
- Employees who know passwords may have left the company or moved to another department
- Different passwords may give access to different resources in the company (R&D, Sales, etc.)
- You have 65535 possible ports, choose yours! (Find reserved port numbers in the **FAQ**)

RA uses 36 characters encrypted Passwords (and never sends them over the wire) while Windows NT uses 14 characters Passwords (which are sent over the wire for authentication and can be compromised by a packet sniffer) so RA is much safer than NT itself.

➪ RA has many options which increase the security of your system. Some of them, like **IP Address Filtering** or **Manual Filtering** may be mandatory in a situation where security is an issue. But you can do more: you can **disable *Master* features** (like 'Get Passwords' or 'File Browser') to protect *Slaves* from *Masters*.

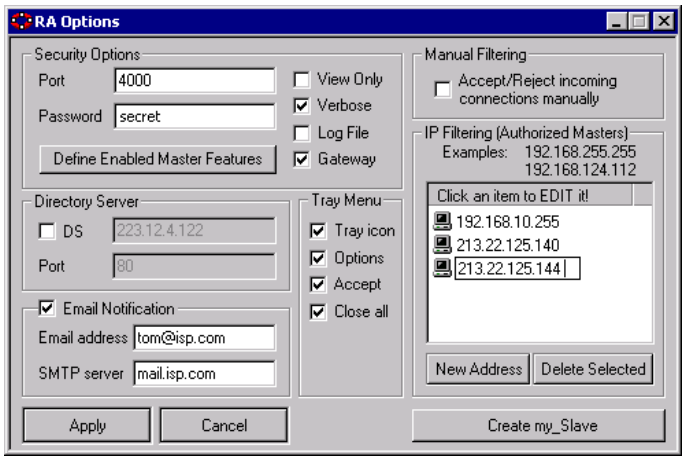
Slave Options

You can access the *Slave* **Options** by clicking the ***Slave* Tray Icon**.
You can also invoke the Option dialog from the **DOS command line**:

Slave -o <your_password> (or 'trial' if you are using a demo).

Note: When you change the port number of a *Slave*, ALWAYS stop and restart the *Slave* Service ('*Slave*.exe -s <password>' to stop it and then run *Slave*.exe again).

Note: The comma and space characters cannot be used in passwords.



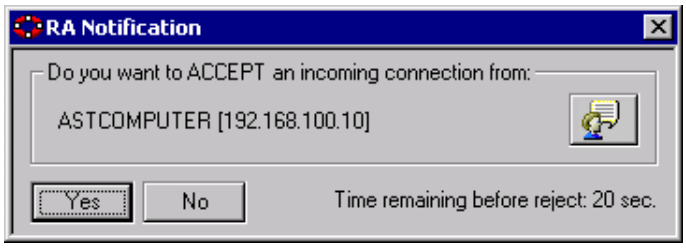
- **View Only** disables or enables the *Master*'s keyboard and Mouse.
- **Verbose** displays messages (Dialogs for Win9x and Event Log for NT/2000/XP).
- **Log File** enables/disables the *Slave* Log File.
- **Gateway** enables/disables the *Slave* Gateway.
- **Tray icon** shows/hides the *Slave* icon in the Task Bar.
- **Options** enables/disables the 'Options...' item in the Tray Menu.
- **Accept** enables/disables the 'Accept Connections' item in the Tray Menu.
- **Close All** enables/disables the 'Close All Connections' item in the Tray Menu.

'**Apply**' saves your modification in the Registry while '**Cancel**' only closes the dialog.

You can enable **IP Address Filtering** to prevent someone from using your *Slave(s)*. *This will allow only* authorized *Masters* to have access to the *Slave* machines. This list can contain IP addresses (like 192.168.28.162) or masks (like 223.48.255.255). You can also edit this list in the registry: "HKey_Local_Machine\Software\TWD\Remote-Anything\Allowed IP Addresses".

To define such a configuration for multiple PCs, you just have to define the same Registry value (a simple *.reg file exported from the Windows RegEdit.exe tool can do this).

You can **Accept or Reject Manually** incoming *Master* connections. If you select this checkbox, then all incoming *Master* connections will display this dialog box before being able to access the *Slave* PC.



This dialog box will stay flashing and beeping (with the Windows default Windows sound) for 30 seconds and will reject the connection if nobody accepts the connection (or if someone rejects the connection before the 30 seconds).

➪ Using the Chat button, a Slave user can start a Chat session with *Master before getting connected*. This allows the user to ask why the Master needs to take control of his PC.

Binding personalized Options in *Slave.exe*

You can **Bind** a **password** and a **port number** and some options (like 'Hide Tray Icon') into the ***Slave.exe*** file. Once personalized, you will only have to run *Slave.exe* on a PC to have the *Slave* service being installed, configured (with *your* default options) and running!

➪ There are two ways to make a personalized *Slave*: from the *Slave* Options dialog and from the command line (DOS prompt).

Note: When you run a personalized *Slave*, bound options will be activated ONLY IF this PC does not already have a *Slave* password installed in the Registry.

If you want to update the existing Registry options with the new *Slave*.exe options, you have to delete *first* the HKey_Local_Machine/Software/TWD/Remote-Anything Key

OR

You have to run *Slave* like this: '*Slave* -r' (update Registry contents with *Slave* new options)

Making a personalized *Slave* from the *Slave* Options dialog

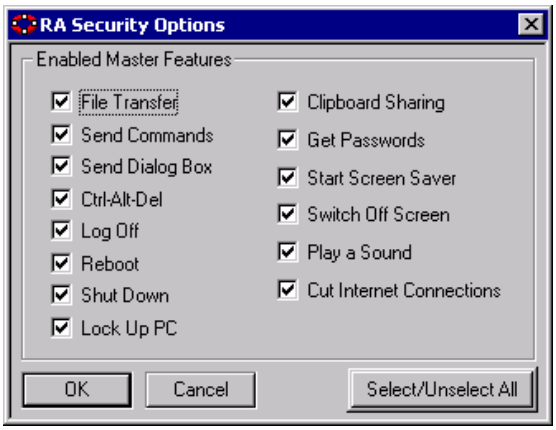
This way to make a personalized *Slave* allows to modify all the options of *Slave* (while the command line method allows only to define a password, a port number and email notification parameters).

➪ When you press the '**Create my_*Slave*.exe**' button, all the options currently selected in the *Slave* Options dialog box will be stored in the 'my_*Slave*.exe' file (with the exception of the 'Authorized *Master* IP Addresses' List).

You can also define precisely what features a *Master* will be able to use on the *Slave*. This is very handy to **restrict rights of *Master* users** who only need the remote access but not need the File Transfer for example. When you disable a *Master* feature for a *Slave*, this feature will not be displayed in the *Master* menu when the *Master* is connected to this *Slave*.

You can disable critical *Master* features like: Clipboard Sharing, Lock up PC, Get Passwords, Reboot, Shut Down and more:

Note: Those changes will take effect only for the *Slave* bound with the new options. Changing the checkbox states of an already installed *Slave* will not change the rights. To change the rights of an already installed *Slave*, make a personalized my_*Slave*.exe and update the old *Slave* (copy it on the *Slave* PC and then run it, it will replace the old *Slave* program during the next boot). Those options stay in the Slave.exe file (they are not stored in the Windows Registry).



Setting a Supervisor Password

With a 'Supervisor Password' you can use all the *Master* features of a restricted *Slave*. This feature will also allow to access the *Slave* PC even if the *Slave* password is changed. This feature is very useful for an administrator who spreads thousands of *Slaves* over different departments: each department may want to define a different password for confidentiality (changing the existing *Slave* password). The administrator will still be able to access the *Slaves*. To use this feature, you only have to **bind a 'supervisor password'** in the *Slave*.exe file. The syntax (at the DOS prompt) is:

***Slave* -a <supervisor_password>**

Example: C:\Windows> *Slave* -a pharaon

This command creates a my_*Slave*.exe file with the supervisor password in the current folder.

Note: Once bound into *Slave*.exe, a supervisor password cannot be changed. To define a new supervisor password, you have to work with an original *Slave*.exe file.

Making a personalized *Slave* from the command line

The syntax is: *Slave*.exe -c <Password> <Port_Number> [Smtp_Server] [Email_Address]
(where parameters between <> are mandatory and parameters between [ ] are optional)

- <Password> the password you want to define for the *Slave*
- <Port_Number> the port number you want to use with the *Slave*
- [Smtp_Server] your SMTP Mail Server for outgoing mail (example: mail.yourISP.com)
- [Email_Address] the address where you want *Slave* to notify you when it is connected to the Internet (the notification email will list all the *Slave* IP addresses)

The -c command will create a personalized copy of ***Slave.exe*** called ***my_Slave.exe***. Copy it on the PC(s) you want to remotely access. Running the file ***my_Slave.exe*** will install *Slave* with the options you defined.

Slave IP address e-mail Notification

If you enable '**Email Notification**', then you will **be notified when the *Slave* is connected to the Internet**: *Slave*s will send you the email below when they are connected to the Internet (whether it is a dialup 'direct' access or an access via a Proxy on a LAN).

IP Address: 192.168.1.10, 209.237.155.134
User Name: TOM
PC Name: sales_treed
PC active for: 00 hour(s) 35 minute(s) 08 second(s)

Note: Email notification MAY NOT work IF:

- you are not using the SMTP server which comes with your e-mail address. Example: SMTP server: 'mail.my_isp.com' and e-mail: 'me@domain.com' (you should use 'me@my_isp.com' instead)

- the SMTP server you are using does not belong to the ISP (Internet Service Provider) of the *Master* PC.

This limitation may apply because most ISPs reject entrant e-mail from unknown IP addresses (addresses they do not allocate themselves) to avoid SPAM.

Step by step instructions to Make a personalized *Slave*

We have seen many users experiencing problems when trying to create a personalized Slave file. Those problems come from one only reason: the fact that a file loaded in memory cannot be overwritten on disk. It may look obvious but many of us forget this when it matters.

In this example, we will create a personalized Slave where *ALL* the Slave options will be changed (*Slave* options, *Master* options and Supervisor Password) so you can use this example to make your own personalized Slave (it is assumed that Slave is installed and running in C:\Windows on this PC; optional steps are colored in blue).

1) Open the 'Slave Options' dialog box
2) Set the settings you want to be the defaults of your new Slave.exe file

- Disable Master Features -

3) Click the [Define Enabled Master features] button
4) Select the Master options you want to disable in the 'RA Security options' dialog box
5) Click [OK] to close this dialog and come back to the 'Slave Options' dialog box
6) Click the [Create my_Slave.exe] button, it creates (or overwrites) C:\Windows\my_Slave.exe
7) Copy C:\Windows\my_Slave.exe to C:\Slave.exe (eventually overwriting an old C:\Slave.exe file)

- Supervisor Password -

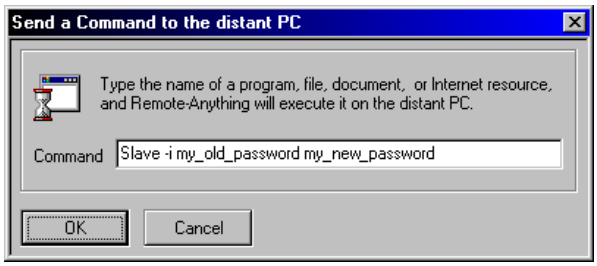
8) Open a DOS box under Windows and type 'CD..' to go to the C:\ root directory
9) Then type: 'Slave -a superPWD' (it creates or overwrites C:\my_Slave.exe)
10) Type: 'del Slave.exe' to delete Slave.exe
11) Type: 'ren my_Slave.exe Slave.exe' to rename my_Slave.exe to Slave.exe
12) Type 'exit' to close the DOS box

You can now copy and run this personalized *Slave.exe* file on a PC to install a *Slave* with the options of your choice. For example, without dialog boxes for error messages ('Verbose' off) and without the Tray Icon and the ability to change the Slave Options ('Set Options' off).

Remotely Modifying Options of a *Slave*

Modifying the Password

It may be done with the *Master* '**Send Commands to distant PC**' menu option or from a DOS prompt. The commands to use are identical in both cases:

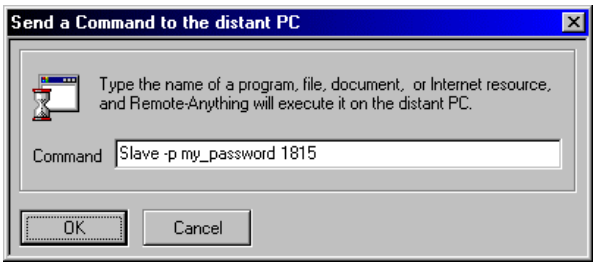


Note: The space character cannot be used in passwords.

Once done, RA will use the new password for each new connection. The old password has been replaced in the Windows Registry of the *Slave*.

Modifying the Port Number

When you change the port number of a *Slave*, ALWAYS Stop and restart the *Slave* Service ('*Slave*.exe -s <password>' to stop it and then run *Slave*.exe again) otherwise you will not be able to run the File Browser from the *Master* (alternatively, a simple reboot will do the job).



If you need to remotely modify other *Slave* options, you will need to do it through a remote-control session or by installing a new my_*Slave*.exe file on the PC(s) with the -r switch (*'Slave -r'* will update any Registry contents with the options bound in Slave.exe).

Modifying the options in the Registry

Slave options are stored in the Registry. You can modify them remotely by using:

- a remote control session and interacting with the *Slave* Options Dialog box
- a Windows remote registry session: (to access the Registry of remote PCs you have to enable the Windows Remote-Registry service on the *Slave* PCs)

[HKEY_LOCAL_MACHINE\SOFTWARE\TWD\Remote-Anything]
"16-Bit" {set it to "0" to disable the 16-bit video modes}
"BiosKey"="VHR7 - 3CLY - XXXX - XXXX"
"UserKey"="EAF7 - 98FA - XXXX - XXXX"
"Port"="4000"
"EMailAddress"=""
"EMailServer"=""
"NotifyIPAddress"="0"
"View Only"="0"
"Verbose"="1"
"Log File"="1"
"Filter Manually"="0"
"Allowed IP Addresses"="255.255.255.255 "
"Password"=hex:04,c4,1a,0a… {ENCRYPTED, cannot be changed manually}
"Allow Options"="1"
"Tray Icon"="1"
"Accept Connections"="1"
"Close All"="1"
"sDS"="213.45.12.55" {can be a DNS name: "domain.com"}
"sDS (use)"="1"
"sDS Port"="80"

[HKEY_LOCAL_MACHINE\SOFTWARE\TWD\Remote-Anything\MRU]
"order"="ACB"
"A"="192.168.100.10"
"B"="192.168.100.8"
"C"="192.168.100.11"

Updating Remote-Anything

TWD Industries offers free updates of RA (check http://www.remote-anything.com from time to time to get the latest version). So, updating RA must be easy to do and reliable. We especially worked on a way to circumvent the Windows limitations that prevent files loaded in memory from being deleted (or overwritten) on disks.

Updating a *Master*

You just have to replace the file ***Master.exe*** where it is stored (for example, on the Windows Desktop: C:\Windows\Desktop*Master*.exe).

Updating a *Slave*

On a local PC

The following procedure is useful especially if you do not want to reboot the *Slave* PC.

STOP the *Slave* program (from a DOS prompt: '*Slave* -s <password>'), and then copy the new ***Slave.exe*** file over the old *Slave*.exe file (usually it is located in the C:\Windows directory). Then run *Slave* just by double-clicking it. There is NO need to restart Windows.

Remotely with a *Master*

NEW Master v3.6.6 and greater can automatically update Slaves (see later in this chapter).

The old method still works in case of need:
Run a *Master* to transfer the new ***Slave.exe*** on the C:\ folder of the PC you want to update and then run the new Slave.exe (specify the full path: C*Slave*.exe to avoid to run the old *Slave* in C:\Windows instead of the new in C:\). The old version will be replaced during the next boot (and will use the existing Registry options unless you use the -r switch: 'Slave -r').

Note:

You have to use the old *Master* to remotely replace the old *Slave* with the new *Slave* (in order to keep using the same version for *Master* and *Slave*).

If no existing *Slave* can be found, the new *Slave* will simply install itself and will copy the new *Slave* options in the Registry.

➪ You can even update RA by e-mail if the computers are too distributed to be accessed directly. That's the kind of thing that you cannot afford to do with other remote-control products which size is in the tens of MB range.

Remotely with a NT Script

➪ Here is a NT script sample to update a Slave file on a remote computer. Under NT, the user running this script must have admin privileges. To execute this script on networked PCs, you can use the NT logon script.

```
net use T: \\server1\d
copy "T:\Programs\RA\Slave.exe" "C:\Slave.exe"
C:\Slave.exe          (use the '-r' switch to force new options)
net use T: /delete
```

This script performs the following operations to update a Slave:

1. Create a logical drive T: mapped to \\server1\d
2. Copy the new Slave.exe file from the server to the C:\ root directory of the PC
3. Run Slave.exe to update the running Slave.exe Windows service
4. Delete the T: logical drive

You will need to change the paths of this example to match the real paths of your systems.

Automatic Update

It is possible to automatically update remotely all your *Masters* and all your *Slaves* without even having to reboot the Slave PCs. Master and the Directory Server (DS) do this and much

more (Please read the '**Directory Server**' Manual for more details about the DS).

NEW When a Master (v3.6.6 or greater) establishes a connection (remote-control or file-transfer) to a Slave (v3.6.6 or greater) then, if Master and Slave do not share the same version number, Master will allow you to remotely update Slave with a simple mouse click (as Slave is only 70KB, this will take 6 seconds on a 56Kbps link). You will not have to reboot the Slave PC, you will just have to restart your connection with the Slave.

Note: You have to copy the latest *Slave.exe* file in the *Master* folder to have *Master* remotely replace the old *Slave* with the new *Slave*. *Master* will compare the file version with all the *Slaves* it talks with and will appropriately update them if needed.

Uninstalling Remote-Anything

The RA uninstall procedure has been designed to be as simple as possible. As some customers wanted to spread thousands of *Slaves* on their corporate network, we focussed on a way to circumvent the Windows limitations which prevent files that are loaded in memory from being deleted from disks.

Uninstalling a *Master*

Just delete the file ***Master.exe*** from your hard disk (there are no DLLs and no dependencies). You may also want to delete the Master Registry entry (which contains the address book): HKey_Local_Machine/Software/TWD.

Uninstalling a *Slave*

There are two different ways to uninstall ***Slave.exe***:

Using Uninstall_*Slave*.exe

Download ***Uninstall_Slave.exe*** from:
http://www.remote-anything.com/archives/uninstall_*Slave*.zip

Decompress ***Uninstall_Slave.zip*** to ***Uninstall_Slave.exe*** and run it on every PC from where you want to uninstall a *Slave*. This can be done by e-mail with an attachment. Users will only have to double-click on the ***Uninstall_Slave.exe*** icon to remove the *Slave* from their system (and clean the Registry).

Remotely with a NT Script

Here is a NT script sample to uninstall a Slave file on a remote computer. Under NT, the user running this script must have admin privileges. To execute this script on networked PCs, you can use the NT logon script.

```
net use T: \\server1\d
```

copy "T:\Programs\RA\Uninstall_Slave.exe" "C:\uSlave.exe"

C:\uSlave.exe

net use T: /delete

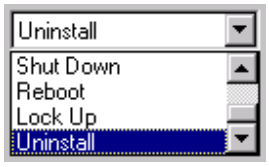
This script performs the following operations to uninstall a Slave:

1. Create a logical drive T: mapped to \\server1\d
2. Copy the Uninstall_Slave.exe file from the server to the C:\ root directory of the PC
3. Run uSlave.exe to uninstall the Slave.exe Windows service
4. Delete the T: logical drive

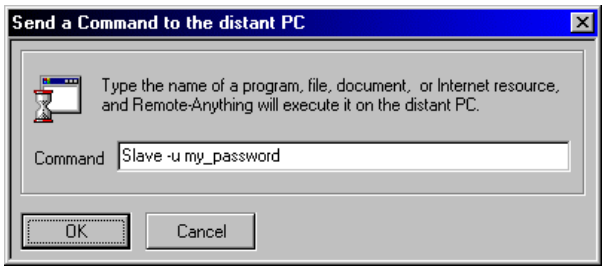
You will need to change the paths of this example to match the real paths of your systems.

Remotely with a *Master*

You can uninstall multiple *Slaves* from a *Master* in just one mouse click!



➪ Select a group of *Slaves* from the list of available PCs in the RA connection dialog box. Then select the 'Uninstall' item of the combo box and click the 'GO!' Button.



➪ Alternatively, to uninstall ONE *Slave* you can use the '**Send Commands to distant PC**' option and type the following command as shown here (replacing 'my_password' by your password).

➪ You can apply the same command from a DOS box:

Those procedures remove RA and the related Registry entries after Windows is restarted.

Dial Up connections (modem to modem)

➪ You can use RA to call directly another PC –without an Internet connection.

Windows NT4 and Windows 98 come with the *Dial-up Networking Server* (Windows 95 includes it in the Plus! Pack). Install it on the *Slave* PC (Control Panel, Add/Remove Programs, Windows Setup) and follow the instructions below:

1) On the *Slave* PC, configure the *Dial-up Networking Server* to allow incoming connections:

- Click on the Start Menu / Programs / Accessories / Communications / Remote-Access (or Network and Dial-up Connections)
- Click on the '*Connections*' pull-down Menu
- Click on the '*Dial-up Networking Server*' (or '*Remote Access Server*') Menu item
- You have to allow the access (and eventually define a password). Then, click the 'OK' button
- The *Slave* PC is ready now to accept incoming dial-up calls (there is an icon in the Task Bar).

2) On the *Master* PC, you have now to make a call using Dial-up Networking:

- Click on the Start Menu / Programs / Accessories / Communications / Remote-Access (or Network and Dial-up Connections)
- Click on the '*New Connection*' Icon
- Name it, select the modem to use, enter the *Slave* Phone number and click the '*Finish*' button
- To use your new connection just double click on its icon (it will directly Dial Up the *Slave* PC)
- Now run the *Master* and type in the *Slave* IP address (usually this address is 192.168.55.1)
- Enter the *Slave* password and port number and hit the '*Connect*' button

You should be connected to your *Slave* PC after a few seconds (a typical full screen refresh of 1024x768 pixels is transmitted in 40KB. That's a delay of 2.5 seconds with a 128K ISDN connection and 6.7 seconds with a 56K modem). Further screen changes only transmit changes, leading to nearly real-time updates.

RA Port Numbers, Routers, Firewalls and Proxies

Routers, Firewalls and Proxies are subject to a lot of confusion, because this is a complex area which involves knowledge of multiple components. To help you in this matter, TWD Industries provides the following information but we cannot help you to configure your own router or firewall -you will have to ask assistance from the corresponding vendor if this documentation does not answer your questions.

RA port numbers

When you have installed RA you may have to take care of other applications like Firewalls (or Proxies) which need to be configured in order to allow access to the ports that RA uses. Usually, as Firewalls are only blocking *incoming* connections it is only a question of opening (and routing) the following -entrant- port numbers:

- Port 4000: TCP, *Slave* Remote-Control Session (Master is using a random source port)
- Port 3999: TCP, *Slave* File Browser Session (Master is using a random source port)
- Port 3997: TCP, *Master* Daemon (SOS Calls)
- Port 3998: UDP, Reserved for future use (Voice over IP)
- Port 3997: UDP, *Master* Daemon (Chat, HW info, etc.)
- Port 3996: UDP, *Slave* Daemon (Chat, HW info, etc.)

If you modify the default port number, you have to do it for both *Master* and *Slave* programs. If this port number is 5000 (instead of 4000) then RA will use the following ports:

- Port 5000: TCP, *Slave* Remote-Control Session (Master is using a random source port)
- Port 4999: TCP, *Slave* File Browser Session (Master is using a random source port)
- Port 4997: TCP, *Master* Daemon (SOS Calls)
- Port 4998: UDP, Reserved for future use (Voice over IP)
- Port 4997: UDP, *Master* Daemon (Chat, HW info, etc.)
- Port 4996: UDP, *Slave* Daemon (Chat, HW info, etc.)

Is opening port numbers in your Firewall a security issue?

To establish a connection with a server application (like an email server, a web server or Slave.exe) you need to open a given port in your firewall and a machine must be listening for that port number. If the firewall has no open port, this means that no connection can be established because the Firewall will block them (this is its purpose). This surely offers the best possible security but a network which cannot to establish connections is of limited use.

Specialists agree on the fact that opening a port number is a security issue but if you ask why, they also usually experience difficulties to explain it.

Open ports are possible security holes **IF** the server application (email server, web server, RA Slave) has security breaches. For example, it is now recognized that having Microsoft Internet Server (IIS) behind your Firewall is dangerous because each month a new IIS security issue is found and pirates can use IIS to gain control of the machine that hosts it. Pirates will access the PCs of your LAN via IIS' trusted ports and the Firewall will not block the intruders.

After all those years and hundreds of thousand of Slaves installed in banks and international companies we have never received reports of a security breach. In fact, Windows is much more dangerous than Slave from this point of view because Windows has open ports which may be used to compromise the security of your network while nobody has ever done this with *Slave*.

Note: If you still do not feel comfortable with the idea of opening ports then the DS is the solution: with a DS, Masters and Slaves are not listening to any port so they no longer need you to open ports in routers or firewalls.

Using NAT to reach 'hidden' *Slaves* on a LAN (with a Router, a Proxy or a Firewall)

PCs on a LAN have private IP addresses that cannot be routed over the Internet. This is why you are using a router or a proxy which is directly connected to the Internet. To reach those 'hidden' PCs from *outside* the LAN you have to use NAT (Network Address Translation) to route incoming *Master* connections to the appropriate *Slave* PCs.

With NAT it is possible to share a single registered (routable) IP address between multiple local computers and connect them all at the same time. The outside world is unaware of this division and thinks that only one computer (or router) is connected.
Here is an example of a NAT table:

Router Port: 5000	**(the port used to access this PC by using 'port mapping')**
Destination IP: 192.168.10.4	**(the PC to be reached on the LAN)**
Destination Port: 4000	**(the port of the destination PC)**

Type: TCP		**(select TCP or UDP as appropriate for this port)**
Direction: Incoming		**(the Router will route only from outside the LAN)**

Master would use the following information to establish a connection with this *Slave* PC:

Slave Gate:		**(do not type in something here)**
Slave:	**223.18.12.9**	**(the public IP address of the Router)**
Password:	**secret**	**(your password)**
Port:	**5000**	**(the port number used to do 'port mapping')**

Because RA is using several port numbers, you have to create the same NAT table for each RA port if you want to use all the features (but it's possible to just use the two first TCP ports):

- Port 4000: TCP, *Slave* Remote-Control Session (Master is using a random source port)
- Port 3999: TCP, *Slave* File Browser Session (Master is using a random source port)
- Port 3997: TCP, *Master* Daemon
- (Slave SOS Calls are using a random source port)
- Port 3998: UDP, Reserved for future use (Voice over IP)
- Port 3997: UDP, *Master* Daemon (Chat, HW info, etc.)
- Port 3996: UDP, *Slave* Daemon (Chat, HW info, etc.)

In your NAT table the IP address of your Router will be used to access all the hidden Slaves of your LAN. As a result, you have to use different port numbers to access different PCs:

Slave PC #1: 192.168.10.2 (mapped to base port 8000)

Router IP address: 168.70.90.110 port 8000 => Slave IP address: 192.168.10.2 on port 4000
Router IP address: 168.70.90.110 port 7999 => Slave IP address: 192.168.10.2 on port 3999
Router IP address: 168.70.90.110 port 7998 => Slave IP address: 192.168.10.2 on port 3998
Router IP address: 168.70.90.110 port 7997 => Slave IP address: 192.168.10.2 on port 3997
Router IP address: 168.70.90.110 port 7996 => Slave IP address: 192.168.10.2 on port 3996

Slave PC #2: 192.168.10.4 (mapped to base port 7995)

Router IP address: 168.70.90.110 port 7995 => Slave IP address: 192.168.10.4 on port 4000
Router IP address: 168.70.90.110 port 7994 => Slave IP address: 192.168.10.4 on port 3999
Router IP address: 168.70.90.110 port 7993 => Slave IP address: 192.168.10.4 on port 3998
Router IP address: 168.70.90.110 port 7992 => Slave IP address: 192.168.10.4 on port 3997
Router IP address: 168.70.90.110 port 7991 => Slave IP address: 192.168.10.4 on port 3996
Etc.

Note: There is an easier way to do that (without doing NAT for all Slaves). Just define a single

NAT entry for one unique Slave with the Gateway option enabled. Then, you will be able to access all the other Slaves of the LAN via this Gate:

```
          Internet                LAN                          LAN
Master ======= Firewall ---------- Slave1 (Gateway) ----------Slave2...
               213.12.12.12        192.168.10.12                192.168.10.10
```

From Master, you will have to provide the following information to establish a connection to Slave1 (the Gateway):

Slave : 213.12.12.12
Port : 8000 / the port used to do NAT (it may also be 4000)
Password: <your password>

From Master, you will have to provide the following information to establish a connection to Slave2:

Slave	**: 192.168.10.12**	(the private IP address of the Slave PC to reach)
Port	**: 8000 / the port used to do NAT**	(the port number used to do NAT; may also be 4000)
Gateway	**: 213.12.12.12**	(the public IP address of the Router)
Password:	**<your password>**	(type here your password or 'trial' for the demo)

This example assumes that the unique NAT entry is:

213.12.12.12: 8000 => 192.168.10.10: 4000

All incoming connections will use this Slave Gateway to access all other 'hidden' PCs on the LAN. This will save you a lot of time (since the NAT table has one unique entry).

Here are a few things to consider when using RA with NAT:

- The NAT table must map to the address of the Slave PC, for this reason the Slave address should be a static private IP address unless you can dynamically update the NAT table.
- RA Masters will have to know the external IP address of the host's NAT server. If the NAT server connects to the Internet using Dial-up Networking, that address is dynamically assigned by an Internet Service Provider and will probably be different with each dial-up. Therefore, remote Masters connecting in will have to somehow be given that address each time.

Using well-known ports to reach *Slaves* behind a Firewall

Well-known ports belong to standard services. For example, HTTP uses port 80. Well-known port numbers range from 1 to 1023. Well-known ports are generally odd-numbers because early servers used an odd/even pair of ports for duplex operations. Most servers require only a single port but some others, like FTP (20 and 21), use two ports.

High ports range from 1024 to 65535 and can be used by any user-developed application like RA. High ports are also used by client applications only for as long as they need. Clients do not need assigned well-known ports because they initiate a connection with a server which uses a known port. A connection just requires that the combination of protocol, IP address and port number is unique.

Your firewall has only well-known ports opened (see the table below) and you cannot change this. How can you use RA? Here is a list of ports that you may be able to use:

A (much) longer list is available from: http://www.iana.org/assignments/port-numbers

Well-known Port	Service
7 / TCP	Echo
11 / TCP	Systat
18 / TCP / UDP	Message Sent Protocol
19 / TCP / UDP	Character generator
20 / TCP / UDP	FTP (Data)
21 / TCP / UDP	FTP (Control)
22 / TCP / UDP	SSH
23 / TCP / UDP	Telnet
25 / TCP / UDP	SMTP
42 / TCP	Host Name Server
43 / TCP	Who Is
49 / UDP	Tacacs
53 / TCP/UDP	DNS (zone/ lookup)
66 / TCP	Oracle-SQLnet
69 / UDP	TFTP
79 / TCP	Finger
80 / TCP	HTTP
81 / TCP	HTTP spare port

88 / TCP/UDP	Kerberos
109 / TCP	POP2
110 / TCP	POP3
111 / TCP	Sun RPC
118 / TCP	SLQ Server
119 / TCP	NNTP
135 / TCP	RPC/DCE Endpoint Mapper
137 / UDP	NetBIOS Name Service
138 / UDP	NetBIOS Datagram Service
139 / TCP	NetBIOS Session Service
143 / TCP	IMAP
161 / UDP	SNMP
162 / UDP	SNMP-Trap
179 / TCP	BGP
256 / TCP	SNMP-Checkpoint
389 / TCP/UDP	LDAP
396 / TCP	Netware-IP
407 / TCP	Timbuktu
443 / TCP	HTTPS (SSL/TLS)
445 / TCP/UDP	Microsoft SMB/CIFS
464 / TCP/UDP	Kerberos password
500 / UDP	IKE, IPSec
513 / TCP/UDP	rLogin / rWho
514 / TCP/UDP	rShell / SysLog
515 / TCP/UDP	Printer
520 / UDP	Router
524 / TCP	Netware-NCP
593 / TCP	HTTP RPC Endpoint Mapper
636 / TCP	LDAP over SSL/TLS
799 / TCP	Computer Associates / Remotelypossible
1080 / TCP	Socks
High Port	**Service**
1313 / TCP	BMC-Patrol-DB
1352 / TCP	Lotus Notes
1433 / TCP	Microsoft SLQ
1494 / TCP	Citrix
1498 / TCP	Sybase SQL-anywhere
1524 / TCP	Ingres-lock
1525 / TCP	Oracle-srv
1527 / TCP	Oracle-tli
1723 / TCP	Pptp
1745 / TCP	Winsock-proxy

2000 / TCP	CA remotely-anywhere
2001 / TCP	Cisco-mgmt
2049 / TCP	NFS
2301 / TCP	Compaq-web
2447 / TCP	OpenView
2501 / TCP	Tivoli Remote-Control
2502 / TCP	Tivoli Remote-Control / file transfer
2503 / TCP	Tivoli Remote-Control / chat
2511 / TCP / UDP	MetaStorm
2512 / TCP / UDP	Citrix – IMA
2513 / TCP / UDP	Citrix – Admin
2998 / TCP	RealSecure
3268 / TCP	Microsoft Active-Directory Global catalog
3269 / TCP	Microsoft Active-Directory Global catalog / SSL
3300 / TCP	BMC-Patrol-agent
3306 / TCP	MySQL
3351 / TCP	SSQL
3389 / TCP	Windows Terminal Server
4001 / TCP	Cisco-mgmt
4045 / TCP	NFS-lockd
5631 / TCP	Symantec - PCanywhere (data)
5632 / TCP	Symantec - PCanywhere (stat)
5800 / TCP	VNC
6000 / TCP	X-Windows
6001 / TCP	Cisco-mgmt
6549 / TCP	APC
6667 / TCP	IRC
8000 / TCP	Web
8001 / TCP	Web
8002 / TCP	Web
8080 / TCP	Web
9001 / TCP	Cisco-xremote
32771 / TCP	RPC-Solaris
32780 / TCP	SNMP-Solaris
43188 / TCP	ReachOut
65301 / TCP	Symantec - PCanywhere-def

- If your Firewall has *two contiguous TCP ports* (x and x-1, say 22 and 21) in its list of opened ports, then you can use the remote-control (port x) and file-transfer (port x-1) features (you can also use two opened UDP ports for the UDP RA features: Chat, Hardware info, etc.) as described below:

Example:

Your Firewall NAT table will have two entries for each PC:

Router IP address: 168.70.90.110 port x => Slave IP address: 192.168.10.4 on port x

Router IP address: 168.70.90.110 port x-1=> Slave IP address: 192.168.10.4 on port x-1

- But if you cannot find two contiguous port numbers, do the following: one port for remote-control (on port x, like 43) and the other for file-transfer (on port y, like 79).

Example:

Your Firewall NAT table will have two entries for each PC:

Router IP address: 168.70.90.110 **port x** => Slave IP address: 192.168.10.4 on **port x**

Router IP address: 168.70.90.110 **port y** => Slave IP address: 192.168.10.4 on **port x-1**

The Source and Destination ports

When a TCP/IP connection is cut a timeout (TIME_WAIT and CLOSE_WAIT) happens. As the connection status is not completely 'closed', one cannot establish a new connection on the *same source and destination ports* with the *same source and destination IP addresses* during the timeout delay (a period of time ranging from 30 seconds to 5 minutes). This delay allows the system to make sure that no data is lost on both sides.

To avoid this issue, Master (the client), like many client applications (Telnet, FTP, HTTP), is using a *random source port* to establish a connection with a Slave (the server).

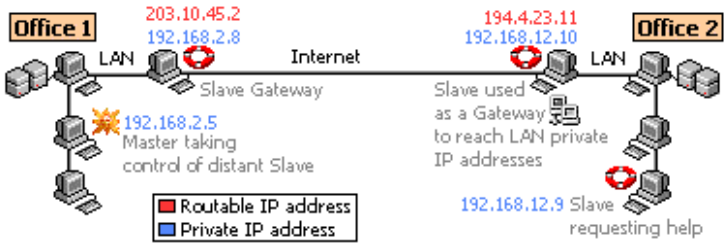
Some firewalls will require that the connection is using *identical source and destination ports*. As a direct consequence, RA will not be able to be used on well-known ports (like explained in the last paragraph) with those Firewalls. You will be obliged to open a set of port numbers in your Firewall for RA.

Using the *Slave* integrated *Gateway* to reach 'hidden' *Slaves* on a LAN

⇨ If the Slave PC is on a remote LAN and, on the Slave LAN, the device directly connected to the Internet is a PC instead of a Router, to reach hidden *Slaves,* you can use **Slave.exe** which has an **integrated Gateway** able to route up to 128 *concurrent* connections. This proxy works for RA only (this is not a general proxy able to route common protocols like HTTP, FTP,

POP3, SMTP, etc.).

To establish a connection from a *Master* to a *Slave* located on a remote LAN you do not have to use Network Address Translation (NAT) or a third-party proxy.



You simply have to install a *Slave* on the PC of the distant LAN which is directly connected to the Internet. This PC has two IP addresses: one is private (like 192.168.12.10 which is LAN-based and cannot be routed on the Internet) and the other is assigned by your ISP (like 194.4.23.11, an IP address which can be accessed from anywhere on the Internet).

To access a *Slave* in [Office 2] from a Master in [Office 1] use the following settings:

Slave Gate:	**194.4.23.11**	**(Office 2: IP address of the Slave Gateway to enter the Slave LAN)**
Slave:	**192.168.12.9**	**(Slave LAN-based private IP address)**
Password:	**secret**	**(your password)**
Port:	**4000**	**(your port number)**

The Slave Gate will route the connections to the hidden Slave on [Office 2] LAN. It will also route unconnected requests (like Ping, Hardware Inventory, Log Off, Wake on LAN, etc.).

Note: *Master*, *Slave Gateway* and *Slave* must use the same port number

Client / Server Security: secrets and lies

The Secrets

It is a temptation for a software publisher to use recognized encryption algorithms (like those of the AES selection) in order to offer a 'bullet-proof' security for their products. This strategy usually impresses the masses. Unfortunately, without a proper implementation, this is like hiding the key of your safety-box under the carpet of your living-room. You may have the most expensive vault, if one has the key he will open it like a vulgar toilets door.

Some preeminent remote-control products *do not use encryption* -or the kind of encryption that only stops your grandmother. Among them, Computer Associates (Remotely Possible 4.0 and Control IT 4.5) which passwords can be found in… seconds.

Symantec, the auto-proclaimed "security expert", is stating that PCanywhere is the *#1 remote-control package in sales*. We doubt that Symantec clients know that each time they use PCanywhere anybody can get their password: the second IP packet *sent over the wire* after the authentication process contains the user name and password (each string starts with a '06' byte followed by the number of characters and the 'encrypted' string itself)! This encryption scheme, *the default when you install the product,* is so sloppy that 10 lines of BASIC can break it in less than a second:

```
1. PRINT "Enter the PCanywhere string to decrypt (username or password, in hex bytes): "
2. INPUT code$
3. length = LEN(code$) / 2
4. nb = VAL("&h") + LEFT$(code$, 2)) XOR &HAB
5. plaintext$ = CHR$(nb)
6. FOR count = 1 to length - 1
7. nb = (VAL(&h" + MID$(code$, count*2+1, 2)) XOR VAL("&h" + MID$(code$, (count-1)*2+1, 2)) XOR (count-1) OR &H40
8. plaintext$ = plaintext$ + CHR$(nb)
9. NEXT
10. PRINT "The secret word is:"; plaintext$
```

Companies who trust Symantec may wonder why such a backdoor exists *since version 2.0* in all the versions of PCanywhere. If they don't, we do. BTW, the second encryption scheme was coded by a recognized security expert: Microsoft. Good luck to Symantec clients.

Some other remote-control products claim to offer 'top-notch' security by using a strong algorithm. And they name it in their manuals. First, that's one secret that the pirate will not have to uncover. Second, as the pirate knows which algorithm is used, he will just have to scan the code of this product to find *when this algorithm is used*, and, furthermore, *where he can get the keys*.

In addition, as applications programmers are rarely encryption experts, they usually do not understand the concept of '*weak keys*' when they implement random keys.

The Lies

Some applications use a ***fixed key*** (you know, the one hidden under the carpet). And it will not take long to a motivated pirate to find it in the code of the application. Keys should be automatically changed -each time they are used- (they are called *session keys*) to make sure that the potential opponent will not have the physical time to break them.

Using a 128-bit or 1024-bit encryption key makes no technical difference because the weak point is the fact that *the key is stored in the PC* -like the code using it. And it is much easier (and faster) to find *where* the key is rather than trying to guess *what* the key is…

Other applications generate ***random keys***… without wondering if they are good for cryptography. Some weak keys can simply break the security of the best algorithm. Also, most 'random generators' follow a logic that computers can perfectly reproduce so this remains 'random' for the human eye only.

And you have the rest: those who *think they know how to do it right*. They follow a good method: using ***hashed keys*** for authentication… but their implementation is a total disaster: one famous example is the Microsoft Windows NT Lan-Manager hashing method used for NT passwords; a 'security' that allows any password to be cracked in hours with a $1,000 PC.

> This security breach comes from two points: the hashing algorithm is known so brute force attacks can be conducted without the cost involved by reverse-engineering and the key is segmented in two sub-keys, making it much faster to break the whole key.

This NT/2000 vulnerability is so well known that recognized security experts (J. Scambray

from Ernst & Young, S. McClure from Foundstone) recommend that remote-control users *DO NOT* use NT passwords with remote-control tools! It is OK to have a sloppy lock for your bathroom but this is not a reason to use the same lock for your main entry door: you can trust people in your house, but you should not trust total strangers!

Security and RA

RA does not use the same keys, or the same algorithms when there is something to hide:

- the encrypted 36 characters **Slave password** is stored in the Slave registry and never transmitted over the wire. It is used by the Master as a key to encrypt a bunch of random bytes that have to be validated by the Slave to grant access to incoming Master connections
- if you are using the DS, then Slaves verify the incoming Master credentials in the DS database: a Master PC must be allowed to be used and a Master User must be authorized to access this Slave PC (with a DS, Slave passwords are no longer used for authentication).
- the **Chat messages** and **shared clipboard text** are encrypted when transmitted
- the **hardware information**, **transferred files** and **screen updates** are encrypted
- incoming connections can be filtered manually or by IP address
- Slave can disable Master features (prevent file transfer or keyboard/mouse input, etc.)

Keys are checked before being used. And when it is necessary to negotiate *session keys* (keys that are different for each transaction) authentication is done prior to key exchange to make sure that we are not risking to divulge the new key to a potential malicious opponent. What about sniffers? On the top of all this, the streams are always encrypted!

No security -or lock- in the world is bullet-proof. That's why banks have alarms. The only purpose of a security system is to make sure that the cost (in terms of time, money and risks) involved to break the security scheme is orders of magnitude higher than the value of the information we try to protect.

➪ It is much easier to break the security of Windows than to break the security of RA. So, if you were an intruder, which target would you choose to penetrate a system?…

TWD's Directory Server

Version 2.11.18 for Windows (95,98,ME,NT4,2000 and XP)

The Directory Server (DS)

What is the Directory Server?

If you manage tens (hundreds of thousands) of PCs then you need a way to:

- Administrate groups of Masters and Slaves from one centralized location
- Allow a Master to find a Slave by user name / host name / MAC-address / IP-address
- Allow Slave users to send SOS Calls that will be processed by the first available Master

The DS implements ***load-balancing*** and ***redundancy*** so it is a scalable solution for a LAN or WAN of an unlimited number of PCs (up to 18,446,744,073,709,551,616 PCs): if you are out of processing power, *the only thing you have to do is to add a new DS!*

- Dynamic IP addresses, routers and firewalls are supported (for Masters, Slaves and all DS'!)
- Masters no longer need a UserKey (you can move your Masters at will, without downtime)
- Masters and Slaves updates are performed automatically (without even rebooting PCs)
- Master Users need credentials to access a list of Slave PCs (from any authorized Master PC)
- The DS maintains a database of all your Users, Master and Slave PCs (and stores changes)

What are the benefits of the DS?

- Router/Firewall Traversal (zero-configuration: it is not necessary to open ports, or to use NAT)
- Higher Security (as Masters and Slaves no longer listen to any port no one can connect to them)
- Network Management (Administration, Application Deployment, Maintenance, etc.)
- Network Security (Audits, Alerts, Monitoring, PC Usage History, Statistics, etc.)
- Directory Server (Remote-Control, Voice over IP & Personal Voice answering Machine, etc.)
- Help Desk (Chat, Remote-Control, Client & Problem Tracking, SOS Ticket, etc.)
- LAN / WAN Browser (Search Persons, Files or Plain Text over thousands of distributed PCs)
- Power Management (Wake Up, Reboot or Power Down a group of PCs with one mouse click)
- Fail-Safe Architecture (Redundancy, Load Balancing, Load Monitoring, etc.)

➪ If you need more information about the DS, please read the DS Manual available from: http://www.twd-industries.com/en/downloads.htm.

Technical Support

TWD Industries provides free Technical Support to registered users the first year and to users testing the product:

- Email: support@twd-industries.com
- Telephone: (Hours: 9:00 AM to 6:00 PM, Greenwich Meridian Time+1)
  - Voice +33 (0)492 940 510
  - Fax +33 (0)492 940 512

Please read the latest FAQ on http://www.remote-anything.com to solve common issues.

Users reporting a new bug or suggesting a new feature really useful for other users will get a free license (even if they are already registered users) and a corrected version within a few days. At TWD Industries, we care about customers and their feedback allows us to make a better product. See http://www.remote-anything.com/en/testimonials.htm.

Program Updates

New versions of RA are free for registered users, just download the last version from:
http://www.remote-anything.com/en/news.htm
RA is constantly evolving and so is your investment with TWD Industries.

Note: TWD Industries develops, markets and supports Remote-Anything (RA), the Directory Server (DS) and the Voice over IP (VoIP) Phone and Answering Machine.
Since TWD Industries DOES NOT WORK WITH SOFTWARE RETAILERS, RESELLERS or DISTRIBUTORS then there is no other company in the world allowed to sell TWD Industries' products.
If someone sells licenses for TWD products, then that's fraud. Help us to create and maintain affordable quality software by purchasing legitimate licenses.

Small Glossary of the Network Terminology used in this Manual

Networking is a complex subject and many experienced computer users feel confused about some words they simply do not understand. So, here is a small introduction to networks that is intended to make you feel more comfortable with those barbarian terms.

LAN (Local Area Network): a private network of several PCs.

WAN (Wide Area Network): several interconnected LANs via leased lines or the Internet.

IP (Internet Protocol): this is a protocol (a language) used by computers and devices like routers, printers, etc. to communicate over a network. This is also the protocol used by the Internet. TCP/IP is declined in two transport protocols: TCP and UDP.

TCP (Transport Control Protocol): this is a connection-oriented protocol which involves two computers for an exchange of information (see it as a phone call: you dial to call someone, talk from both sides and then hang up). TCP is reliable since it checks that the packets it sends are received by the other end. RA is using TCP for 'remote-control' and 'file-transfer' sessions.

UDP (User Datagram Protocol): this is an unconnected protocol (see it as bottle you throw in a river: it may reach your friend located below but it may be lost). UDP is not reliable but is faster than TCP since it uses far less resources. RA is using UDP for the 'Chat', 'Wake-on-LAN' or 'Get Hardware Information' features.

IP address (Internet Protocol address): this is a 4-byte logical address (an address that can be defined by the user) used to reach another machine (or 'node') over the Internet or on a LAN (see it as the phone number you use to dial to talk to your mother). Some IP addresses are reserved:

- if it ends with zero(s): 137.50.4.0 or 137.50.0.0, then it specifies a network
- if it ends with 255: 13.4.2.255 or 13.4.255.255, then it defines a broadcast address (or a mask)
- if it starts with 127: 127.50.10.121 or equals 0.0.0.0, then it specifies the local machine
- if it starts with 0: 0.68.10.11 or 0.0.10.11, then it defines an address on the current network
- 255.255.255.255 is a 'limited broadcast' used on a LAN, it will be blocked by routers

Example of a valid IP address that can be assigned to a computer: 192.168.124.12

Public or routable IP address: this is an IP address that everybody can use on the Internet. Some of these addresses have been assigned to geographical regions:

- 194.0.0.0 – 195.255.255.255, Europe
- 198.0.0.0 – 199.255.255.255, North America
- 200.0.0.0 – 201.255.255.255, Central and South America
- 202.0.0.0 – 203.255.255.255, Pacific Area

Example of a valid public IP address: 213.18.124.12

Private or non-routable IP address: this is an IP address that can be ONLY used on a private LAN. As specified in the RFC 1597 issued in March 1994, the following IP addresses can be used for private networks:

- 10.0.0.0 – 10.255.255.255, allowing 1 network of 16,777,214 IP addresses
- 172.16.0.0 – 172.31.255.255, allowing 16 networks of 65,534 IP addresses each
- 192.168.0.0 – 192.168.255.255, allowing 256 networks of 254 IP addresses each

Example of a valid private IP address: 192.168.124.12

NAT (Network Address Translation): NAT is used to translate a private IP address to a public IP address. Example: a Master user can reach a Slave PC located on a private LAN via a router connected to the Internet doing NAT (see it as a phone center dispatching customer's incoming calls to the internal lines of a corporate building).

NIC (Network Interface Card): a network adapter (usually for Ethernet or Token Ring) that allows you to connect your computer to a local LAN.

MAC (Media Access Control): a 6-byte physical address (i.e. an address burned into the silicon of your hardware) which allows computers to translate (with the ARP protocol) a logical address like an IP address into something related to a physical device like a computer. The MAC address is supposed to be unique: the first 3 bytes are the manufacturers identifier and the rest is used to define 2^(3*8) = 16,777,216 unique cards for each manufacturer. Example: 00-50-BF-12-D4-98

License Agreement

The software described in this document is provided with a License Agreement and may not be used without acceptance of the terms of this License. This software is licensed, not sold. The fee you pay entitles you to use the software, not to own it. The software is copyrighted material and TWD Industries SAS owns the exclusive distribution rights of this software.
This is a legal agreement between you, the end user, and TWD Industries SAS, a French company.

GRANT OF LICENSE – This TWD License Agreement permits you to use one copy of the TWD Industries software product acquired with this License on any single computer, provided the software is in use on only one computer at any time. If you have multiple Licenses for the software then at any time you may have as many copies of the software in use as you have Licenses. The software is "in use" on a computer when it is loaded into the temporary memory (i.e. RAM) or installed into the permanent memory (e.g. hard disk, CD ROM, or other storage device) of that computer, except that a copy installed on a network server for the sole purpose of distribution to other computers is not "in use". If the anticipated number of users of the software will exceed the number of applicable Licenses, then you must have a reasonable mechanism or process in place to assure that the number of persons using the software concurrently does not exceed the number of Licenses.

COPYRIGHT - The software is owned by TWD Industries or its suppliers and is protected by United States copyright laws, international treaty provisions, and all other applicable national laws. Therefore, you must treat the software like any other copyrighted material (e.g. a book or musical recording) except that if the software is not copy protected you may either make one copy of the software solely for backup or archival purposes, or transfer the software to a single hard disk provided you keep the original solely for backup or archival purposes. You may not copy the Product manual(s) or technical and commercial written materials accompanying the software.

OTHER RESTRICTIONS – You may not rent or lease the software, but you may transfer your rights under this TWD Industries License Agreement on a permanent basis provided that you transfer all copies of the software and all written materials, and the recipient agrees to the terms of this agreement. You may not reverse engineer, decompile or disassemble the software. Any transfer must include the most recent update and all prior versions.

LIMITED WARRANTY – TWD Industries warrants for a period of 60 days from the date of receipt that the software will perform substantially in accordance with the accompanying Product Manual(s); and any TWD Industries supplied hardware accompanying the software will be free from defects in materials and workmanship under normal use and service for a period of one year from the date of receipt. Any implied warranties on the software and hardware are limited to 60 days and one (1) year, respectively.

CUSTOMER REMEDIES – TWD Industries' entire liability and your exclusive remedy shall be, at TWD Industries' option, either return of the price paid or repair or replacement of the software or hardware that does not meet TWD Industries' Limited Warranty and which is returned to TWD Industries with a copy of your receipt. This Limited Warranty is void if failure of the software or hardware resulted from accident, abuse, or misapplication. Any replacement software will be warranted for the remainder of the original warranty period or 30 days, whichever is longer.
NO OTHER WARRANTIES – TWD INDUSTRIES DISCLAIMS ALL OTHER WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WITH RESPECT TO THE SOFTWARE, THE ACCOMPANYING PRODUCT MANUAL(S) AND WRITTEN MATERIALS, AND ANY ACCOMPANYING HARDWARE. THIS LIMITED WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS.

NO LIABILITY FOR CONSEQUENTIAL DAMAGES – IN NO EVENT SHALL TWD INDUSTRIES or its suppliers be liable for any other damages whatsoever (including, without limitation, damages for loss of business profits, business interruption, loss of business information, or other pecuniary loss) arising out of the use of or inability to use this TWD industries product, even if TWD industries has been advised of the possibility of such damages. In any case, TWD industries entire liability under any provision of this agreement shall be limited to the amount actually paid by you for the software.
U.S. Export Controls: You agree that you will not export or re-export these products to any country, person, entity or end user subject to U.S.A. export restrictions. Restricted countries currently include, but are not necessarily limited to Cuba, Iran, Iraq, Libya, North Korea, Syria, and the Federal Republic of Yugoslavia (Serbia and Montenegro, U.N. Protected Areas and areas of Republic of Bosnia and Herzegovina under the control of Bosnian Serb forces). You warrant and represent that neither the U.S.A. Bureau of Export Administration nor any other federal agency has suspended, revoked or denied your export privileges.

This Agreement is governed by the French laws and the competent Tribunal is Antibes, France. Should you have any question concerning this Agreement, or if you desire to contact TWD Industries for any reason, please mail to: info@twd-industries.com.