Introducing InetD

InetD is a super server that lets you enable and disable various daemon services through a single application. It determines the network services to which your PC responds when a client makes an incoming network request.

Instead of running separate server applications for each service, InetD conserves workstation resources by monitoring connection attempts in the background and starting the appropriate daemon when it receives a network request. You can enable or disable daemons to accommodate your local requirements. For example, you can use FTPd to distribute corporate files from a server. Clients would connect to the server and use FTP to download the files. The InetD daemon is based on asynchronous notification. It uses no CPU time and only a small amount of memory when waiting for incoming requests.

Note: With Windows NT, if you create a TelnetAccess or FTPAccess groups in the user administration program, the NT user must be a member of these groups to access the machine using Telnet or FTP. No security check is performed if the group does not exist, and access is allowed for every NT user account.

In Windows 98/Me environments, InetD runs automatically when placed in the Startup folder. In Windows NT/2000/XP/Server 2003 environments, InetD is installed as a service.

Note: The InetD daemon is installed in the Control Panel during Setup.

InetD handles both TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) servers. »

Related Topics

Maintaining System Security

Maintaining System Security

Users that connect to your drives and directories using the InetD services are restricted to file access based on the permission you assign.

Security for Windows 98/Me

With Windows 98/Me, you assign permissions using the InetD Admin application. InetD Admin is an administration tool designed to control access to your files and resources.

When remote users on the network try to log onto your PC via the InetD server programs, InetD Admin screens them and determines the level of access. To allow anonymous FTP access to your PC via the FTP daemon, you must set up an anonymous user account in InetD Admin.

Security for Windows NT/2000/XP/Server 2003

Windows NT/2000/XP/Server 2003 supports NTFS, FAT, and HPFS file systems. Of these, only NTFS provides access control at the file and directory level.

NTFS

Users that link NTFS drives and directories by means of the InetD services are restricted to file access according to Windows NT/2000/XP/Server 2003 permissions.

If you have enabled FTPd and/or Telnetd, also consider:

For FTP, if you create an FTPAccess group in the user administration program, the Windows NT/2000/XP/Server 2003 user must be a member to access the machine using FTP. No check is performed if the group does not exist; access is then allowed for every Windows NT/2000/XP/Server 2003 user account.

For Telnet, if you create a TelnetAccess group in the user administration program, the Windows NT/2000/XP/Server 2003 user must be a member of the group to successfully access the machine using Telnet. No check is performed if the group does not exist; access is then allowed for every Windows NT/2000/XP/Server 2003 user account.

FAT and HPFS

FAT and HPFS drives do not allow you to set user-access rights, setting the drive to write access allows all users to write to it. Granting all users write-access could leave your drive vulnerable.

If you have FAT or HPFS local disk drives, consider the following when determining whether to allow remote users to have access to your local machine using FTP or Telnet.

FTP—The FTP daemon (FTPd) lets you set read and write permissions to restrict users access to FAT and HPFS volumes. If you do not want users to have access to FAT or HPFS drives, do not include them in the -r, -w, or -rw parameters. If you do want users to have access to these drives, exercise caution when setting parameters.

Telnet—The server application, Telnetd, cannot restrict incoming users to a particular local disk drive. If you have a FAT or HPFS drive on your machine, and you enable Telnet access over the network, incoming users have unrestricted access to that drive. This means they could potentially delete all files.

There are two solutions to this problem:

- Use only NTFS file systems on your computer.
- If you have FAT or HPFS disk volumes, do not enable Telnet access over the network.

Related Topics

Setting File Security in an NTFS File System

Granting Anonymous FTP Access

Setting File Security in an NTFS File System

To set NTFS file security:

1. Select one or more files in My Computer.
2. On the File menu, click Properties. The Properties dialog box opens.
3. Click the Sharing tab.
4. Click Permissions. The Access Through Share Permissions dialog box opens.
5. Specify the appropriate security options. See your Windows NT/2000/XP/Server 2003 documentation for details on setting file security.

Enabling and Disabling Services

You can enable and disable daemon services in the InetD Configuration dialog box. Configuration information is stored in the file `inetd.ini`.

- To enable a service, select the service in the InetD Service list and click Enable.
- To disable a service, select the service in the InetD Service list and click Disable.
- To save changes made to InetD configuration, click Save.

Configuring Services

To configure a Network service:

1. In the InetD Configuration dialog box, select the service that you want to configure and click Configure. The Daemon Configuration dialog box opens.
2. Verify that the Daemon Name box contains the name of the selected service and that the Program Filename box contains the name of the file for the service.
3. In the Optional Parameters box, type any optional parameters associated with the selected service. For more information, see Default Services.
4. In the Port box, type a port number between 0 and 65535 to uniquely identify the service.
5. Select the protocol required for the server: either TCP or UDP. If you selected TCP, type the maximum number of servers that can be used for the service in the Maximum Servers box.
6. Click OK.
7. To save changes made to InetD configuration, click Save.

Adding Services

Any of the existing servers can be configured to run on any port, or added to run on more than one port at a time.

To add a service:

1. In the InetD Configuration dialog box, click Add. The Daemon Configuration dialog box opens.
2. In the Daemon Name box, type the name of the service you want to add.
3. In the Program Filename box, type the file name of the service.
4. In the Optional Parameters box, type any optional parameters associated with the service.
5. In the Port box, type a port number between 0 and 65535 to uniquely identify the service.
6. Select the protocol required for the server: either TCP or UDP. If you selected TCP, type the maximum number of servers that can be used for the service in the Maximum Servers box.
7. Click OK.
8. To save changes made to InetD configuration, click Save.

Related Topics

Deleting Services

Default Services

Deleting Services

Use the Delete button in the InetD Configuration dialog box to remove any or all of the services from the list of available InetD services.

To remove a service:

1. Select the service you want to remove and click Delete.
2. To save changes made to InetD configuration, click Save.

    Note: To reload all network services back into the Setup menu, click Reload. To reload the original default settings, click Defaults.

Related Topics

Adding Services

Default Services

Reloading Updated Configuration Information

After making changes to the InetD configuration, such as enabling or disabling a service, you can load the updated configuration without exiting your configuration session.

To reload the InetD configuration file, click Reload in the InetD Configuration dialog box. The system loads the new InetD configuration information.

Logging Server Activity

Windows NT/2000/XP/Server 2003

You can send all server start and stop messages to the Windows NT/2000/XP/Server 2003 Event Viewer Log file.

To enable logging, select the Connection Logging check box in the InetD Configuration dialog box.

Windows 98/Me

You can record all server start and stop messages in a log file.

To enable logging, select the Connection Logging check box in the InetD Configuration dialog box. InetD stores messages in the `inetd.log` file in the following directory:

```
system\Hummingbird\Connectivity\version\InetD\ine
```

where *version* is the version number of your Hummingbird product.

Granting Anonymous FTP Access

All users, including anonymous users, must provide a password.

Windows NT/2000/XP/Server 2003

To grant anonymous FTP access to your PC through the FTPd daemon, add an anonymous user using your operating system’s User Manager. Then add the anonymous user to the FTPAccess group.

Note: With Windows NT/2000/XP/Server 2003, if you create a TelnetAccess or FTPAccess groups in the user administration program, the Windows NT/2000/XP/Server 2003 user must be a member of these groups to access the machine using Telnet or FTP. No security check is performed if the group does not exist, and access is allowed for every Windows NT/2000/XP/Server 2003 user account.

Windows 98

To grant anonymous FTP access rights to users connecting to your PC through the FTPd daemon, you must add an anonymous FTP user to your password file. After this account is set up, any user can access your PC by typing the user name anonymous, and any password. You can add an anonymous FTP user using InetD Admin. For more information, see the InetD Admin Help.

Default Services

The following daemon services are provided.

TCP Services

Bootpd—Enables client workstations using BOOTP (Bootstrap Protocol) to request their configuration information.

Fingerd—Lets a remote user query the state of your current configuration.

FTPd (File Transfer Protocol Daemon)—Enables users to transfer files between other computers and your own.

Lpd—Lets other workstations send print files directly to your PC printer, or to a network print queue on the PC.

Telnetd—Lets Telnet clients make connections to your PC.

Xstartd—A local X client starter daemon that enables users to access X clients on your PC.

UDP Services

TFTPd—Lets users transfer files to and from your PC using the TFTP protocol.

Timed—A time server that other workstations can use to synchronize their current date and time.

TFTPd

TFTPd lets you use your PC as a TFTP (Trivial File Transfer Protocol) server. The TFTP server lets users transfer files to and from your PC. Any TFTP client program can use the TFTP server, including the DOS TFTP client.

Warning! TFTP does not require a user name and password.

One of the major applications for TFTP is to allow diskless workstations or PCs with Boot PROMs to retrieve boot images from a Windows NT/98/Me/2000/XP workstation in conjunction with the bootpdw server. To reduce any potential security issues, we suggest creating a directory specifically for boot image files and making only that directory available to TFTP clients using the -r option.

Optional Parameters

`-r`*`directory`* Specify a read directory for clients. For example, `-rc:\bootptab`

`-w`*`directory`* Specify a write directory for clients. For example, `-wc:\hcltcp`

`-o or –O` Allow clients to overwrite existing files.

TFTPd has an inactive timeout feature that you can use to ensure that TFTPd closes a connection after a period of client inactivity.

To specify a timeout limit:

1. Create a file named `tftpd.ini`.
2. Type the following in the file:

   ```
   [Inactive]
   TimeOut=n
   ```

   where *n* is the maximum number of seconds of inactivity after which TFTPd closes a connection. The minimum timeout is 10 seconds.

3. Save the file in the following directory:

   `system\HUMMINGBIRD\Connectivity\version\InetD`

   where *`version`* is the version number of your Hummingbird product.

Timed

Timed is a time server that other workstations can use to synchronize to the current date and time. When a machine sends a time request to your PC, Timed returns the current time. This is the time value since Jan 1st 1970 GMT.

You can set up workstations with the `hcltime` or `hctime32` program to synchronize the date and time across the network.

Bootpd

BOOTPd lets client workstations using Bootstrap Protocol request their configuration information. If a client machine is configured for BOOTP, a BOOTP request is broadcast over the network each time the machine starts.

The BOOTP request contains the MAC (Media Access Control) address of the machine (physical hardware address). When Bootpd is enabled, it responds to requests if the client’s MAC address is found in the `boottab` configuration file. »

Requirements

- You must enable Bootpd in InetD on at least one machine in the network. It is best to enable Bootpd on several machines so that if one machine fails to respond, the configuration information is available on other machines on the network.
- You must create a configuration file, `bootptab`, in the `system\HUMMINGBIRD\Connectivity\`*`version`*`\InetD` directory, where *`version`* is the version number of your Hummingbird product. You must use the same file on all machines running BOOTP.

Comparison to RARP

The Reverse Address Resolution Protocol (RARP), also lets a client determine its IP address when the MAC (Media Access Control) address is known. The difference between RARP and BOOTP is that RARP is a hardware, link-level protocol instead of an IP/UDP protocol. This means that RARP can be implemented only on local hosts on the same subnet.

Related Topics

BOOTPTAB Configuration File

BOOTPD.LOG File

Fingerd

Fingerd enables remote users to query the state of your current configuration. If the remote user requests a long listing, Fingerd also displays the contents of the `plan.hcl` and `project.hcl` files located in the following directory:

```
system\HUMMINGBIRD\Connectivity\version\InetD
```

where *`version`* is the version number of your Hummingbird product.

The Plan file typically contains information about how to contact you (phone number, address, e-mail and so on), while the Project file typically contains your function or current project.

FTPd (File Transfer Protocol Daemon)

FTPd handles incoming requests to transfer files between other computers and your own. Many Internet nodes contain files that are generally available through anonymous FTP.

When an FTP transfer is requested, the program checks for a user ID and password, and the user’s access rights on the various server drives before forwarding the request to FTPd. FTP requires the services of the TCP protocol to move files. Do not select UDP in the Daemon Configuration dialog box for this service.

You can create an FTP configuration file that lets you set the timeout period and the banner display. »

You can also set the following parameters in the Optional Parameters box of the Daemon Configuration dialog box.

Optional Parameters

For Windows 98/Me

Use the following syntax to specify the password files to be used to validate access:

```
- p password_file
```

where *`password_file`* is the full path and file name of the password file you are using. By default, the password file is called `password.hcl` in the system directory:

```
system\HUMMINGBIRD\Connectivity\version\InetD
```

where *`version`* is the version number of your Hummingbird product.

To create a password file, use InetD Admin. InetD Admin provides access to the password database that controls access to your PC from external users through passwords and user names. For more information, see the InetD Admin Help.

Windows NT/2000/XP/Server 2003

The following optional parameters are available for FTPd:

Parameter	Description
`-rdrives`	Limits FTP users to only read access on the listed drives
`-wdrives`	Limits FTP users to only write access on the listed drives
`-rwdrives`	Limits FTP users to read/write access on the listed drives

The format for specifying drives is as follows:

`-rwd:\` (limits FTP users to read/write access on the listed drive)

Related Topics

Maintaining System Security

Granting Anonymous FTP Access

Lpd

LPD (Line Printer Daemon) lets other workstations send print files directly to your PC printer, or to a network print queue on your PC. No print options are directly configurable under InetD, but if you want to allow users to print host files to your PC printer, you must define your default printer. See your Windows documentation for information about setting up the default printer.

Depending upon the remote host you want to print from, you may need to define an entry for the printer in the /ETC/PRINTCAP file on the remote host, or create a printer queue with the appropriate host administration tools.

To configure the LPD program to use an existing printer, you must configure the remote host to send print jobs to a queue. The PRINTCAP file on the remote host links the local queue name (to which the local PC sends print requests) to the remote queue name (where the files are actually printed).

For example, a user sends a print job to the queue hpjohn. The printer is actually called hplaser and it is connected to a remote machine named john. The remote host might have a PRINTCAP entry that links these two queue names, like this:

```
HPJOHN|printer:\
:in:ttl:rp=dos-hplaser:ih=JOHN
```

On the remote system the queue names for the PC are defined in the form xxx-*printer-name* or xxx-*printer-name*, where xxx can be DOS, DOSFF, UNIX, UNIXFF, or TEXT.

DOS	If xxx is DOS, the file is printed without modification.
UNIX	If xxx is UNIX, linefeeds are converted to carriage returns and linefeeds.
Ends in FF	If xxx ends in FF, a form feed is appended to the job if one is not already present.
TEXT	If xxx is TEXT, the output is rendered. This is usually used for printing text files directly to PostScript printers.

Note: Some systems have a limit on the number of characters in the remote queue name. Thus, if `UNIXFF-printer-name` is too long, use shortened prefixes (`D`, `DF`, `U`, `UF`, and `T`). Also, some systems do not allow a dash character in the remote queue name. For these systems, use an underscore character instead.

Telnetd

Telnetd is a Telnet server that lets Telnet clients make connections to your PC. Users can connect using the Hummingbird Telnet client, a graphical VT100/320 terminal emulator application, or any VT100 Telnet client.

If you are using NTFS in a Windows NT/2000/XP/Server 2003 environment, the user must have an account on the Windows system, and have appropriate permissions in the Windows security system. Users are restricted to the protection and access rights specified by the system administrator for each of the Windows machines, drives, directories, and files.

If the user administration program has the group TelnetAccess, the user must be a member to successfully access your workstation. No check is performed if the group does not exist—access is then allowed for every user account.

Optional Parameters (Windows 98/Me)

The following optional parameter is available for Telnetd:

```
- p password_file
```

where *password_file* is the full path and file name of the password file you are using. Use the specified password file to validate access. By default, the password file is called password.hcl, located in the following directory:

```
system\HUMMINGBIRD\Connectivity\version\InetD
```

where *version* is the version number of your Hummingbird product. The password file is empty until you modify it with InetD Admin.

Related Topics

Maintaining System Security

Xstartd

Xstartd is the local X client starter daemon. When Xstartd is enabled, other users can access X clients on your PC. They can connect to your PC and start X clients by using their Xstart application and the REXEC or RSH connection methods.

RSH is available only for Windows 98/Me. You cannot use the RSH protocol with Windows NT/2000/XP/Server 2003.

REXEC

When using the REXEC protocol, Xstartd verifies the user name and password to ensure that access has been granted to the remote user.

Windows 98/Me

Xstartd uses InetD Admin to verify user names and passwords. For REXEC, -p password_file specifies the password file to be used to validate access. By default, the password file is password.hcl, located in the following directory:

```
system\HUMMINGBIRD\Connectivity\version\InetD
```

where *version* is the version number of your Hummingbird product.

In Windows NT/2000/XP/Server 2003

User names and passwords are verified by the operating system itself. The user name used must belong to someone who uses that PC or to a fully qualified domain user who is permitted to login to that PC.

RSH

RSH is available on Windows 98/Me only. The rhosts file determines which hosts are allowed to connect to the PC and is located in the following directory:

```
system\HUMMINGBIRD\Connectivity\version\InetD
```

where *version* is the version number of your Hummingbird product.

The rhosts file consists of one or more lines in the following format:

```
hostname username
```

where *hostname* represents a host name from which RSH is allowed, and *username* represents the user ID of a user on the host, hostname, who is allowed to RSH to your PC.

You must put a space between the `hostname` and `username` parameters.

To include a comment in the file, begin the comment line with the number or pound sign (#).

You can use the plus character (+) in the hostname or username fields to represent any host and any user. For example:

To allow any user from sparc to RSH to your PC, specify:

```
sparc +
```

To allow all users with the user ID of John Smith on any host to RSH to your PC, specify:

```
+ JohnSmith
```

To allow any user on any host to RSH to your PC, specify:

```
+ +
```

To allow John Smith from host sparc to RSH to your PC, specify:

```
sparc JohnSmith
```

Note: You must put a space between the *`hostname`* and *`username`* parameters.

BOOTPD.LOG File

All BOOTP requests and responses are recorded in the `bootpd.log` file in the default `InetDHome` directory. Requests are time and date stamped to provide a chronological record of BOOTP events on the network. A sample segment from a `bootpd.log` file is as follows:

```
info(6) version 3.2

info(6): reading “c:\hcltcp\bootptab”

info(6): read 38 entries (38 hosts) from
“c:\hcltcp\bootptab”

info(6): recvd pkt from IP addr 0.0.0.0 AT Tue
Aug 16 08:14:44 2002

info(6): request from Ethernet address
00:60:8C:E8:CE:55

info(6): found 185.75.64.10 (pete)

info(6): vendor magic field is 99.130.83.99

info(6): sending reply(with RFC1048 options)

info(6): setarp 185.75.64.10 - 00:60:8C:E8:CE:55

info(6): recvd pkt from IP addr 0.0.0.0 AT Tue
Aug 16 08:16:32 2002

info(6): request from Ethernet address
00:60:8C:E8:CE:77
```

```
info(6): ound 185.75.64.12 (bobg)

info(6): vendor magic field is 99.130.83.99

info(6): sending reply (with RFC1048 options)

info(6): setarp 185.75.64.12 - 00:60:8C:E8:CE:77

info(6): recvd pkt from IP addr 0.0.0.0 AT Tue
Aug 16 08:17:57 2002

info(6): request from Ethernet address
00:60:8C:E8:CE:99

info(6): found 185.75.64.14 (roger)

info(6): vendor magic field is 99.130.83.99

info(6): sending reply (with RFC1048 options)

info(6): setarp 185.75.64.14 - 00:60:8C:E8:CE:99
```

You can include more detail in the log by inserting the `-`*d* option in the configuration for `bootpdw`. Up to four `-`*d* options (separated by spaces) can be inserted for increasing levels of detail. Enter the `-`*d* option(s) in the Optional Parameters box of the BOOTPD Daemon Configuration dialog box.

Related Topic

Configuring Services

BOOTPTAB Configuration File

The BOOTPTAB file is an ASCII file that matches the client machine MAC address (physical hardware address) with other configuration information. The configuration information in the BOOTPTAB file can vary from simply the IP address for each machine, to a complete set of configuration information such as default gateway, Domain Name Server, subnet mask, and Time Server.

Entry format

All entries must be in the format:

```
xx=value
```

where *xx* is a two-letter designation for a parameter. The *value* is either a number or text entry depending upon the nature of the parameter.

Configuration Information

The configuration information can appear in several forms as illustrated by the examples below.

IP address only »

Multiple parameters »

Multiple parameters with a common parameter block »

The parameter definitions are listed below.

bf	Boot File	mw	Minimum Wait
bs	Boot Size	nt	NTP Time Server
da	Authentication Server	ra	Reply Address
df	Dump File	rl	RLP Server
dl	DHCP Lease	rp	Root Path
dn	Domain Name	sa	Boot Server
ds	Domain Name Server	sm	Subnet Mask
ef	Extension File	sw	Swap Server
gw	Gateway	tc	Common Configuration Block
ha	Hardware Address	td	TFTP Directory
hd	Home Directory	to	Time Offset
hn	Send Hostname	ts	Time Server
ht	Network Type	vm	Vendor Magic
ip	IP Address	yd	NIS Domain
lg	Log Server	ys	NIS Server
lp	Printer Server		

General Accessibility

Hummingbird products are accessible to all users. Wherever possible, our software adheres to Microsoft Windows interface standards and contains a comprehensive set of accessibility features.

Access Keys All menus have associated access keys (mnemonics) that let you use the keyboard, rather than a mouse, to navigate the user interface (UI). These access keys appear as underlined letters in the names of most UI items. (If this is not the case, press Alt to reveal them.) To open any menu, press Alt and then press the key that corresponds with the underlined letter in the menu name. For example, to access the File menu in any Hummingbird application, press Alt+F.

Once you have opened a menu, you can access an item on the menu by pressing the underlined letter in the menu item name, or you can use the arrow keys to navigate the menu list.

Keyboard Shortcuts Some often-used menu options also have shortcut (accelerator) keys. The shortcut key for an item appears beside it on the menu.

Directional Arrows Use the directional arrows on the keyboard to navigate through menu items or to scroll vertically and horizontally. You can also use the directional arrows to navigate through multiple options. For example, if you have a series of radio buttons, you can use the arrow keys to navigate the possible selections.

Tab Key Sequence To navigate through a dialog box, press the Tab key. Selected items appear with a dotted border. You can also press Shift+Tab to go back to a previous selection within the dialog box.

Spacebar Press the Spacebar to select or clear check boxes, or to select buttons in a dialog box.

Esc Press the Esc key to close a dialog box without implementing any new settings.

Enter Press the Enter key to select the highlighted item or to close a dialog box and apply the new settings. You can also press the Enter key to close all About boxes.

ToolTips ToolTips appear for all functional icons. This feature lets users use Screen Reviewers to make interface information available through synthesized speech or through a refreshable Braille display.

Microsoft Accessibility Options

Microsoft Windows environments contain accessibility options that let you change how you interact with the software. These options can add sound, increase the magnification, and create sticky keys.

To enable/disable Accessibility options:

1. In Control Panel, double-click Accessibility Options.
2. In the Accessibility Options dialog box, select or clear the option check boxes on the various tabs as required, and click Apply.
3. Click OK.

If you installed the Microsoft Accessibility components for your Windows system, you can find additional accessibility tools under Accessibility on the Start menu.

Technical Support

You can contact the Hummingbird Technical Support department Monday to Friday between 8:00 a.m. and 8:00 p.m. Eastern Time.

Hummingbird Ltd. **1 Sparks Avenue, Toronto, Ontario, Canada M2H 2W1**		
	Canada and the USA	International
Technical Support:	1-800-486-0095	+1-416-496-2200
General Enquiry:	1-877-FLY-HUMM	+1-416-496-2200
Main:	+1-416-496-2200	
Fax:	+1-416-496-2207	
E-mail:	support@hummingbird.com	
FTP:	ftp.hummingbird.com	
Web Support:	support.hummingbird.com/customer	
Web Site:	www.hummingbird.com	