Release Notes

NetRecon™

Version 2.0

As a general pattern, AXENT Technologies releases versions of NetRecon in the following order: Beta, Early Shipment Program (ESP) and General Availability (GA).

Additional copies of this document or of other AXENT Technologies publications may be ordered from your authorized distributor or directly from

AXENT Technologies, Inc.
796 East Utah Valley Drive, Suite 200
American Fork, Utah 84003
Phone: (801)224-5306 Fax: (801)227-3791
World Wide Web: http://www.axent.com

For Technical Support: **Fax:** **(801)227-3788**
Internet: **net_supp@axent.com**

For Licensing Issues: **Fax:** **(801)227-3745**
Internet: **license@axent.com**

Trademarks

Document Revised: September 1998

Contents

System Requirements 5
Enhancements & New Features (2.0) 5
- Changed Objectives 5
- Improved Memory Handling and Performance 6
- Improved Reports 6
- New Vulnerabilities 6

Enhancements & New Features (1.1) 11
- Changed Scan What Dialog Box 11
- Source IDs 12
- New Vulnerabilities 12
- Objective Filter 14
- Entering a License Key 14
- Demo Mode 15
- Changed Progress Indicator 15
- Changed Set Scan Duration Dialog Box 15
- Scan Menu 15

Installation Information 15
Upgrade Information 16
Frequently Asked Questions 17
Solutions 20
Obtaining a License Key and Serial Number 21
- From AXENT Via the Web 21
- From AXENT in a Box 22
- From a Reseller or Bundled with a Computer 22
- Requesting a License Key 22
- License Options 22

NetRecon Maintenance 23

Receive Support from Your Reseller 23
Receive Support from AXENT 24

Release
Notes

System Requirements

Minimum system requirements to run NetRecon:

- Operating System: Windows NT 4 (Workstation or Server) with Service Pack 1 or greater
- Memory: 32 MB
- Disk Space: 12 MB

Enhancements & New Features

New in NetRecon 2.0

Changed Objectives

The NetRecon objectives list has been changed to accommodate certain types of scans. For example, all objectives related to identifying network resources (including verifying existence and determining names, addresses, aliases, types, etc.) have now been consolidated into one objective called “Identify network resources.” This makes it easier to perform a scan geared simply towards discovery and network mapping. Similarly, all objectives related to discovering network services have been consolidated

under the objective “Discover TCP / IP services.” That objective is a quick way to perform a port scan on a group of network resources.

Improved Memory Handling and Performance

The NetRecon scan engine has been optimized for greater performance and now uses less memory. The performance and memory use improvements apply especially to large scans (scanning hundreds or even thousands of network resources).

Note, however, that scans (and in particular, large scans) are memory, CPU, and network traffic intensive. For best results, run larger scans on machines that can be dedicated to NetRecon for the duration of the scan. This is never an absolute requirement; NetRecon is designed to run at the same time as other applications. Doing so, however, may significantly reduce the performance of NetRecon and any other applications run at the same time on the same machine. Additionally, while the latest version uses significantly less memory, memory may still occasionally be an issue when performing very large scans. In these cases, you should increase the amount of RAM (for best performance) or virtual memory in the system where NetRecon is installed.

Improved Reports

Several report options have been changed or added. Previously, you could choose to include a section listing vulnerabilities by network resource and another section that listed network resources by vulnerability. For each of these sections, you can now also choose to show only summary information or detailed lists or both. An option has also been added to the detailed vulnerability listing that permits inclusion of system types (which includes operating system information, server types, etc.) and aliases (such as the IP address along with the NT system name, and vice versa). The type and alias information makes it easier to identify particular network resources.

New Vulnerabilities

Approximately 100 vulnerabilities were added since version 1.1, bringing the total vulnerability count to over 250. Some notable additions include:

New NetWare Vulnerabilities

Example:

level1-1 (remote admin access) attack possible

As the name implies, this requires a signature level of 1 on both the server and client. This attack gives the user the ability to set an arbitrary object to have rights equivalent to the Admin account.

Note: This vulnerability is detected based on version information, and may not apply if you have already reconfigured your NetWare server.

Finger Service Vulnerabilities and Exploits

Example:

finger service allows remote command execution as root via filter

A malicious finger query can be used to execute arbitrary commands as root. No system accounts or authentication are required.

Vulnerabilities Reported Since 1.1 Was Released

SSH 1.x protocol allows insertion of data into stream

Due to a fundamental problem in the SSH 1.x protocol, versions 1.2.23 and earlier of Free SSH, as well as versions 1.3.4 and earlier of F-Secure SSH allow attackers to insert data into the encrypted SSH stream without a key. Vulnerable servers can be made to execute commands or otherwise compromise the session. Vulnerable clients allow misinformation to be displayed to the user.

New Vulnerabilities in NetRecon 2.0

Following is a complete list of vulnerabilities added since NetRecon 1.1. For descriptions of these vulnerabilities, along with suggested solutions, open the file *vulnlist.htm* (located in the NetRecon program directory) into any browser or, from within NetRecon, choose View, Vulnerability descriptions.

BACKDOOR (stealth back door program) can be installed
Bindas (authentication using password hash) attack possible
bindery susceptible to lasthope (NLM) attack
bindery susceptible to NW_Hack (client side EXE) attack
bnews service enabled
Burn (malformed packet logging) attack possible
busboy service enabled
common backdoor port is open
conference service enabled
console buffer overrun can ABEND server
courier service enabled
csnet-ns service enabled
dictionary service enabled
efs service enabled
eklogin service enabled
erlogin service enabled
Exim 1.62 and earlier allow shell users root access
finger service allows null redirects
finger service allows recursive null redirects
finger service allows remote command execution as root via filter
finger service allows remote command execution via filter
finger service lists all users
finger service lists all users who have ever logged in
finger service lists users currently logged in
finger service lists users who have never logged in
finger service recursively redirects queries
finger service redirects queries
GameOver (remote admin access) attack possible
garcon service enabled
gateway service enabled
Havoc (malformed packet) denial of service possible
hostnames service enabled

http service enabled
identified intruder tripwire or service wrapper
identified possible backdoor
iso-tsap service enabled
kerberos service enabled
kerberos_master service enabled
Kill (malformed packet flood) denial of service possible
klogin service enabled
knetd service enabled
kpop service enabled
krb_prop service enabled
kshell service enabled
level1-1 (remote admin access) attack possible
level3-1 (remote admin access) attack possible
link service enabled
login names obtained via finger
LOGOUT can be disabled
maitrd service enabled
malformed NCP call can ABEND server
man service enabled
mantst service enabled
mtb service enabled
mtp service enabled
name service enabled
nameserver service enabled
NDSas (authentication using password hash) attack possible
netnews service enabled
netstat service enabled
NetWare 4.x susceptible to IPX hijacking
network resource identified
new user password initialization is not encrypted
NeWS service enabled

nntp service enabled
open TCP port discovered
OpenVMS loginout allows unauthorized access
poker service enabled
pop service enabled
pop2 service enabled
pop3 service enabled
print-srv service enabled
qmaster service enabled
qpopper 2.41 buffer overflows allow remote root access
queue service enabled
remotefs service enabled
remp service enabled
rje service enabled
rmt service enabled
Sendmail allows information obscuring via long HELO/EHLO
sftp service enabled
SLmail 2.6 overflow allows code execution
SLmailNT 3.0 overflow allows code execution
SOCKS proxy identified
Solaris rpcbind high port is open
SSH 1.x protocol allows insertion of data into stream
sunrpc service enabled
supdup service enabled
supervisor password can be reset with console access
syscon does not encrypt password changes
systat service enabled
tcprepo service enabled
tempo service enabled
uucp-path service enabled
vmnet service enabled

vmnet0 service enabled

VNC service enabled

w service enabled

whois service enabled

Wild pad (wildcard signature) attack possible

Win32 Apache allows retrieval of files outside document trees

Win32 Apache allows some file restrictions to be bypassed

WinGate pop3 proxy overflow denial of service

WinGate telnet proxy buffer overflow

x400 service enabled

x400-snd service enabled

Yang (malformed broadcast packet) attack possible

New in NetRecon 1.1

Changed Scan What Dialog Box

The Scan What dialog box now has a Discover button that you can click to have NetRecon build a list of network resources to scan. When you click Discover, NetRecon does a preliminary search for network resources, creates a list, and inserts the list into the Scan What text box. You should always examine this list carefully to ensure that it contains only network resources you have permission to scan.

You can now specify a range of IP addresses that includes more than one traditional Class C network. NetRecon 1.0 permitted only IP address ranges in which the last address octet was changed (i.e. 127.0.0.1-127.0.0.154). In NetRecon 1.1, you can specify any block of addresses you want, even if that block crosses multiple Class C networks (i.e. 127.0.0.1-127.0.2.25).

The Scan What text box is now a drop target, so you can drag and drop text files containing lists of network resources you want to scan. In other words, you can save a list of network resources to a text file, then drag the icon for that file into the Scan What text box to insert the contents of the file. Note that this feature works only when you drag and drop text files.

Source IDs

The Source ID feature lets you see how NetRecon discovered particular vulnerabilities. This feature can help security administrators find not only particular vulnerabilities, but to see the path an attacker might take in finding out about a network and then exploiting particular weaknesses in the network's security configuration. Many seemingly innocuous security weaknesses can result in attackers being able to find much more serious problems.

As NetRecon scans a network, it gathers large amounts of information, which is stored in records. Each record is assigned an ID by NetRecon. When a vulnerability is discovered, NetRecon takes note of which record or records were used to find that particular vulnerability, and stores this information in a field called "Source IDs." Source IDs are shown in the Source ID column in the Data Table.

Note: Source IDs are references to records that contain data used to discover vulnerabilities. Since NetRecon shows only records that contain vulnerabilities, some source records may not be visible as you scroll through the Data Table pane. To see all the records generated during a scan (thereby ensuring that all source records are visible), have NetRecon display all records by using the All Records command in the View menu.

The Source ID feature demonstrates the power of NetRecon's Ultrascan technology. Since NetRecon can run many objectives simultaneously and selectively feed data gathered back to objectives, it can scan a network much as a human being would, exploiting one vulnerability to discover another, and so on. The Source ID features shows this ability to discover a vulnerability path, rather than simply individual vulnerabilities.

New Vulnerabilities

Approximately 50 new vulnerabilities were added for version 1.1. For example, if NetRecon locates any web servers, it now checks for CGI vulnerabilities, including the ability to execute several vulnerable CGI applications (such as the well known phf cgi problem), the ability to execute a perl interpreter (due to a misconfiguration of the web server), and the ability to execute a shell using CGI (also a misconfiguration problem). NetRecon also

now attempts to exploit some weaknesses in older versions of Windows to get usernames, network resource names, and passwords.

Here are several of the more notable vulnerabilities added:

accessed parent of shared directory

NetRecon was able to access the parent directory of a shared directory.

Also known as the "dot dot bug" (/..), this vulnerability permits an attacker to gain access to the directory structure above a shared directory. A number of operating system versions are vulnerable to this bug. For example, NetRecon attempts to exploit this vulnerability in earlier versions of Windows 95 to gain access to .PWL files, which it can use to discover user names, passwords, and network resource names.

HTTP allows execution of phf CGI

NetRecon has discovered a network resource that permits execution of a CGI program named phf that is susceptible to unauthorized command execution attacks.

Some versions of this white pages directory service program pass unchecked newline characters to the Unix shell.

Vulnerable versions included those shipped with NCSA 1.5a and earlier and Apache 1.0.5 and earlier.

HTTP allows execution of test-cgi CGI

NetRecon has discovered a network resource that permits execution of a CGI program named test-cgi that may be susceptible to unauthorized file inventory attacks.

Some versions of the test-cgi CGI application can be used to inventory directories. Knowing the contents of the cgi-bin directory, for example, can help attackers plan attacks on particular CGI scripts and applications.

Apache 1.2b2 is known to be vulnerable, and other versions may be vulnerable. Many servers include test-cgi.

password obtained via .PWL file

NetRecon exploits other Windows 95 vulnerabilities to try to gain file access to network resources running Windows, then looks for .PWL files. These files are used to store passwords when Windows connects to shares.

If NetRecon can obtain a .PWL file, it has already obtained a user name (since the user name is the first part of the .PWL file), and there is a chance that it can obtain one or more passwords, since older versions of Windows used a weak encryption scheme.

Objective Filter

Since many objectives rely on information gathered from other objectives to complete their assigned task, running one objective often causes NetRecon to automatically run one or more other objectives. In version 1.0, running a single objective often resulted in a wide range of vulnerabilities being reported by NetRecon, some of which weren't directly related to the objective run.

Starting with version 1.1, NetRecon now limits vulnerabilities reported to those directly related to the objective run. This limit applies to the records shown in the Data Table pane, the number of vulnerabilities shown in the Graph pane, and the vulnerabilities listed in NetRecon reports.

Filtering vulnerabilities reported based on the objective run lets security administrators hunt for particular types of problems with much greater accuracy, since they don't have to analyze as much data to see what NetRecon discovered.

Entering a License Key

If no license key has been specified when the program is run, a dialog box appears to indicate than no license key has been specified, and permitting the user to enter a new license key. Alternatively, a user can choose not to specify a license key and run NetRecon in Demo Mode. Existing license key information

can be viewed by choosing Administration, Enter License Key from within NetRecon; new license key information can be specified by clicking the New License button in this dialog box.

For information about obtaining a license key, see *Obtaining a License Key and Serial Number* later in these release notes.

Demo Mode

If no license key has been specified when the program is run, a dialog box appears to indicate than no license key has been specified, and permitting the user to enter a new license key. Alternatively, a user can choose not to specify a license key and run NetRecon in Demo Mode. Existing license key information can be viewed by choosing Administration, Enter License Key from within NetRecon; new license key information can be specified by clicking the New License button in this dialog box.

Changed Progress Indicator

In NetRecon 1.0, the progress indicator in the status bar showed records added to the Data Table. In NetRecon 1.1, the progress indicator now shows approximately how much of the total scan time has elapsed. The total scan time is set using the Set Scan Duration dialog box when a scan is begun.

Changed Set Scan Duration Dialog Box

"Indefinitely" has now been removed as an option in the drop-down list in the Set Scan Duration dialog box. This option was removed to ensure that all scans are of limited length (see *How long does it take to run NetRecon?* in the *Frequently Asked Questions* section later in these release notes).

Scan Menu

NetRecon now has a Scan pull-down menu in the main window. The Start Scan and Stop Scan menu options in the Scan menu start and stop scans, exactly like the Start and Stop buttons in the Tool Bar.

Installation Information

During installation, NetRecon sometimes tries to install files that already exist and are open. Since open files cannot be deleted and replaced, the installation program tells you to restart your computer after the installation is complete. If you receive a notification to restart your machine, it's very important that you do so before using NetRecon; otherwise, NetRecon may not run properly.

Upgrade Information

If you are upgrading from NetRecon version 1.0, please note the following issue:

1.0 File Compatibility

NetRecon data files (.nrd files) saved from NetRecon 1.0 can be retrieved into NetRecon 2.0, but with some serious limitations. Some vulnerabilities found in NetRecon 1.0 have been removed, some have been replaced by others, and some remain the same but have had their names changed. In those cases, NetRecon will retrieve the records that contain obsolete vulnerabilities, but will not correctly assign their risk value (instead they are assigned a value of 99). If you retrieve a 1.0 file and then generate a report, the links to obsolete or changed vulnerability descriptions will not work.

Since the Source ID feature did not exist in NetRecon 1.0 (see the *Enhancements and New Features* section earlier in these release notes), NetRecon 1.0 data files do not contain a Source ID field, and therefore do not support that feature.

If you have NetRecon 1.0 data files and wish to keep them and analyze them further, you may want to keep both NetRecon 1.0 and NetRecon 2.0 on your system. By default, NetRecon 2.0 is installed into a different folder from 1.0, easily allowing you to retain both programs. For best results, NetRecon 1.0 files should be opened and analyzed using version 1.0.

1.1 File Compatibility

NetRecon data files (.nrd files) saved from NetRecon 1.1 are fully compatible with NetRecon 2.0. A small number of vulnerabilities have been changed or obsoleted, but even in those cases, the risk values are still assigned correctly and all vulnerability description links in reports still work.

Frequently Asked Questions

How long does it take to run NetRecon?

When you run an objective, you are prompted for how long you want to run NetRecon. Some objectives could take hours or even days to complete (such as password cracking), and new resources could become available at any time, so deciding how long to run a scan is primarily a matter of how thorough a scan you want to perform. Running a longer scan simulates a more concentrated and thorough attack on a network, while running a short scan simulates a more cursory effort. Since no network is ever entirely secure, NetRecon can help you determine how much effort is required to penetrate your network, and weigh this against the importance of the data you want to protect.

You can get an idea of how much of a scan has been completed by looking at the objective Statistics dialog box. To open this dialog box, right-click any objective and choose Statistics from the Quick menu. This dialog box shows record statistics about all running objectives. The Sent column shows you how many records have already been processed for each objective. The Waiting column

shows you how many records are yet to be processed by each objective. Comparing the records already processed and the records yet to be processed, in combination with knowing how long the scan has already been going, can give you an idea of how much longer it will take for NetRecon to process the remaining records (though this can only provide an estimate, since it's always possible for new network resources to be discovered, which means that more records are added to the Waiting queue). The record processing speed can vary significantly, depending on such factors as the processor speed on the machine where you run NetRecon, the amount of memory that machine has, the speed and size of the network(s) you're scanning, and so forth.

Why do I get different results when I run NetRecon on the same network?

Networks typically contain many resources, only some of which may be available at any one time. NetRecon scans for all the network resources it can find, but there are a number of reasons why some resources may not be discovered during the period of the scan. Because of the interdependent nature of NetRecon objectives, finding one new network resource during a scan could lead to the discovery of many new network resources and vulnerabilities.

Does NetRecon perform denial of service attacks?

NetRecon detects the potential for denial of service attacks, but it does not actually perform such attacks. NetRecon does use some network bandwidth, and in some cases may slow portions of a network while it is being run. If your network is small, or relies on low capacity routers, it is probably best to perform long, intensive scans during off-peak hours.

Could an attacker use NetRecon to crack my network?

NetRecon has a number of safeguards built in to it to protect against its use as an attacking tool. For example, when NetRecon scans a network, it leaves evidence of itself and the system from which it was run.

Why do other applications on the same machine run slowly while NetRecon is running?

NetRecon is a CPU and memory intensive program, particularly when conducting large scans (hundreds or thousands of network resources). For best results, do not run other applications at the same time you run NetRecon. Doing so will decrease NetRecon's performance, and the performance of any other applications you run.

Why do my mapped drives get disconnected after I run NetRecon?

In order to perform certain kinds of scans, NetRecon must first temporarily disable your network connections (such as mapped network drives). Under most circumstances, this won't create any problems, since most network applications are designed to reconnect automatically when the network connection is needed again. In a few cases (mostly older network applications), you may experience some problems, in which case you simply need to restart that network applications so it can make a new connection.

Is it possible to accidentally scan someone else's network?

Yes. When you specify networks and network resources to scan, you could type incorrect information and inadvertently scan network resources you didn't intend to scan. If you have NetRecon search for networks to scan, NetRecon could find a network outside your control. You should take extra precautions

to avoid scanning other people's networks without authorization (see the warning below), including networks within your organization but administered by someone else.

Scanning a network without authorization could have severe results, including criminal prosecution and / or civil litigation.

Solutions

The following problems were addressed in this release of NetRecon:

- Under some circumstances, NetRecon could not determine if a network resource was running NetWare, which prevented it from obtaining revision information.
- Under rare circumstances, the portcom and netbios modules would exit with an access violation during a scan.
- Unusual circumstances caused NetRecon to exit with an access violation. Usually these were combinations of key strokes, but sometimes this happened without user intervention.
- NetRecon sometimes ran out of memory, particularly when performing very large scans (thousands of network resources). While the latest version uses significantly less memory (see *Improved Memory Handling and Performance* under *Enhancements and New Features* earlier in this document), memory may still occasionally be an issue when performing very large scans. In these cases, you

should increase the amount of RAM (for best performance) or virtual memory in the system where NetRecon is installed.

- Under rare circumstances, the TCPScan module would exit with an access violation. The module was not correctly handling a case where large amounts of data were received from a port connection.
- Under rare circumstances, the YPFind module would exit with an access violation. The module was not handling correctly a case where unusually large NIS records were received.
- Under some circumstances, when scanning by IP address, NetRecon wouldn't produce as many vulnerabilitites as when scanning by name.

Obtaining a License Key and Serial Number

There are a number of ways you could receive your license key, license type, and serial number, depending on where you purchased NetRecon or requested an evaluation copy.

From AXENT Via the Web

If you purchased NetRecon or requested an evaluation copy from an authorized representative of AXENT Technologies via the web, you also received the serial number via the web immediately after registering for the product and chose a licence type at that time. You should have received a license key from AXENT shortly thereafter in an e-mail. If you did not, see *Requesting a License Key* later in this section.

From AXENT in a Box

If you purchased NetRecon or requested an evaluation copy from an authorized representative of AXENT Technologies and received NetRecon in a box, the box contains a License Certificate that includes the serial number and license type and may include a license key. If it did not come with a license key, follow the instructions on that certificate to receive your license key.

From a Reseller or Bundled with a Computer

If you purchased NetRecon from a software reseller or it came bundled with a computer you purchased, NetRecon comes with a License Certificate that includes the serial number, license type, and instructions for obtaining a license key via the web. Follow the instruction on that certificate to receive your license key.

Requesting a License Key

Unless you purchased NetRecon from a reseller or it came bundled with a computer (in which case you should follow the instructions on the License Certificate), you can request a NetRecon license key in any of the following ways:

E-mail: license@axent.com

Web: http://www.axent.com/support/techsup/license.htm

License Options

NetRecon offers four license options:

Evaluation License

An Evaluation license lets you scan an unlimited number of network resources from one system. Each scan is limited to five minutes, and the evaluation license expires in seven days.

Limited License

A Limited license lets you scan up to 254 network resources from one system.

Unlimited License

An Unlimited license lets you scan an unlimited number of network resources from one system.

Consultant License

A consultant license is similar to an Unlimited license, except that it lets you install and use NetRecon on more than one machine for limited periods. It is designed for consultants, who work a different sites temporarily.

NetRecon Maintenance

There are several options available for obtaining technical support for NetRecon.

- Reseller Supplied Support
- 1-Year Standard Maintenance from AXENT
- 1-Year Priority Maintenance from AXENT
- Pay-per-Incident Support from AXENT

Receive Support from Your Reseller

Contact the reseller who sold you NetRecon for their maintenance offerings.

If the reseller does not provide support, then use the below AXENT direct support information.

Receive Support from AXENT

To purchase a maintenance contract, contact AXENT in one of the following ways (depending on your location). Note that a purchase order is required before AXENT can issue you a maintenance contract.

United States

Voice: (301) 258-2620 x536

Fax: (301) 670-3587, Attn: Deena Kouyeas

E-mail: dkouyeas@axent.com

Surface mail:

AXENT Technologies, Inc.

ATTN: Deena Kouyeas

2400 Research Blvd., Suite 200

Rockville, MD 20850-3243

Europe

General Inquiries:

Voice:+44-1372-729655

Fax:+44-1372-749965

Surface mail address for both support and general:

AXENT Technologies Ltd.
Apex House
4a-10 West Street
Epsom
Surrey
KT18 7RG
United Kingdom

1-Year Standard Maintenance

NetRecon customers can purchase a NetRecon Maintenance Package for the first year and then renew yearly for the life of the product.

The Standard Maintenance package allows NetRecon customers to receive regular technical telephone support, maintenance releases, tune-up packs, online web support, and e-mail support directly from AXENT. Support hours are weekdays, other than U.S. legal holidays, 6am-6pm U.S. Mountain Time.

When you contact AXENT Technical Support, you must provide your NetRecon serial number, version number, the passcode found on your NetRecon license certificate, and the Software Maintenance and Support Key.

You can contact AXENT Technical Support in any of the following ways:

United States

(Includes North and South America)

Voice: (801) 227-3700

Fax: (801) 227-3788

E-mail: net_supp@axent.com

Web: http://www.axent.com/support2/incident.htm

Europe

(Includes UK, Europe, Middle East, and South Africa)

Voice:+44-1372-729655

Fax:+44-1372-749965

1-Year Priority Maintenance

NetRecon customers can purchase a NetRecon Maintenance Package for the first year and then renew yearly for the life of the product.

The Priority Maintenance contract is the same as the 1-Year Standard Maintenance package, except that it offers support 365 days a year, 7 days a week, 24 hours a day. This extended service is available at an additional charge to the 1-Year Standard Maintenance contract. Customers outside the United States can purchase a Priority Maintenance contract, but must call the United States Technical Support team for after hours support.

After AXENT's finance department or the customer account representative clears the customer's Priority contract, a pager number is issued to the customer for contacting AXENT Technical Support outside of regular support hours. Pages are answered within 30 minutes. During regular support hours, you can contact AXENT Technical Support in any of the ways described in the Standard Maintenance package section earlier in this document.

Pay-Per-Incident Maintenance

Pay-per-incident support is available for customers who do not purchase a Standard or Priority Maintenance package. Customers who use pay-per-incident support will receive their first call for free. Each subsequent call is billed through a credit card on a per-incident basis. Unlike Standard and Priority maintenance, pay-per-incident support does not include free NetRecon upgrades and tune-up packs. Priority Maintenance is currently only available in the United States.

You can contact AXENT Technical Support in any of the ways described in the Standard Maintenance package section earlier in this document.