news@ftp

The FTP Software® Newsletter

Volume III, Number 3 October 1990

Inside…

Item	Page
Masthead	2
New Version of LANWatch	3
SNMP Tools for DOS	3
PC/TCP for OS/2 Description	4
“Oral Traditions” RFC	6

New Release of PC/TCP® for DOS™

by Bruce Campbell

FTP Software is pleased to announce the release of version 2.05 of PC/TCP for DOS. This version, which will begin shipping on October 22, includes many important improvements, including: print redirection, new mail features, a redesigned Telnet program, and an SNMP Agent. A new version of Inter-Drive® which features file locking will be available at the same time. A new version of NetBIOS, which has a number of technical improvements, will also be ready for shipment.

Those users who have the **ebanyan** kernel and a Banyan VINES™ 4.0 server will be pleased to learn that the bug which caused problems transferring files to and from the server has been found. Until a corrected version of the VINES software is available, users who have PC/TCP version 2.04 or earlier will need to upgrade to version 2.05, which does not provoke the problem.

Most interesting to many users will be an add-on program which is under development; it will allow PC/TCP to use the multitasking power of Windows 3.0 Enhanced Mode. It will be available as an addition to PC/TCP later this year.

Print Redirection

Many users of DOS programs want to be able to generate print-outs from within an application. FTP Software’s new print redirection facility will capture output sent to a printer port and spool it to a file. A hot key will then send the print file to a network printer without exiting the application. You can also choose to print from the DOS prompt after you exit the application.

The print redirector is capable of using any one of a number of protocols to get the file to a print server. PC-NFS, Lpr, and the Novell NetWare™ print facility are among the supported methods of printing across networks. This means that in most cases, existing systems will need no additional software to work with the new print redirection programs.

New Mail Support

To simplify reading, writing, sending, and receiving electronic mail, FTP Software has added a visual mail reader, named **vmail,** to PC/TCP for DOS. With **vmail**, users can connect to a mail server and execute all of their mail actions as a batch process. New mail is downloaded to the PC, where it can be read, answered, saved, and deleted offline. Notes that were composed offline are uploaded to the mail server for sending. Complete mail services are provided, and only a few moments of server time are required.

At the PC, facilities are provided for reading, forwarding, composing, and replying to messages. Any DOS text editor can be used for writing mail; an initial screen displays all

continued...

news@ftp

Volume III, Number 3 ¥ October 1990

Published by FTP Software, Inc.
Editor: Nancy Connor

Communications pertaining to this newsletter should be directed to:

news@ftp
FTP Software, Inc.
26 Princess Street
Wakefield, MA 01880-3004
Phone: (617) 246-0900
FAX: (617) 246-0901
Electronic mail: news@ftp.com

FTP Software welcomes suggestions and contributions from readers. Submissions for the next issue of the newsletter must be received no later than August 30, 1990.

continued from page 1

message headers for a quick look at your mail; you can select a particular message with the cursor; single letter commands are used to access a wide range of features, from forwarding mail to searching for a string within a message.

Telnet

We have made a number of improvements to the Telnet program which is included with PC/TCP. You can select one of 10 separate simultaneous IBM® 3270 and DEC® VT®220 sessions. The Telnet program will determine whether it is trying to connect to a UNIX™ or an IBM host and negotiate the appropriate terminal type. Screen savers and hot-key programs are also supported, via an escape character which tells the program to pass characters through to DOS.

SNMP Agent

An RFC-compliant SNMP Agent will be included with release 2.05. This means that any PC running the PC/TCP SNMP agent will answer SNMP requests from network management stations.

New features in InterDrive

To prevent multiple users from simultaneously modifying the same file, FTP Software has added file locking to InterDrive, its NFS™ client implementation. This feature provides advisory file locking with NFS servers which have the correct implementation of **lockd**. Suppose for example, that a person starts a spreadsheet program which implements the DOS file locking commands, and then starts to use a file on an InterDrive remote mounted disk. If the NFS server has a working **lockd**, lock-aware applications can avoid problems caused by two or more users unknowingly manipulating the same file at the same time.

Windows 3.0 Compatibility

We are working on an add-on program that will let PC/TCP use the power of Windows 3.0 enhanced mode. It will be ready for beta in sometime in the fourth quarter. We will probably release the product in the same way as we released printer redirection a no-charge mailing of a disk and later integration into the base PC/TCP product.

This add-on program will provide support for the PC/TCP kernel for Windows 3.0 386 enhanced mode, so that the kernel will handle calls from applications in different windows. For example, you will be able to open separate Telnet sessions in multiple windows, and, at the same time, use FTP to transfer files in another window. In addition, we will provide development environment support for our native mode (system call) interface. Please note that we will not have Windows-based applications; we have not rewritten any applications to use the mouse and icons.

The program is a VxD virtual driver. It works by handling the INT 61 calls coming from PC/TCP applications running in separate windows and passing them to the kernel. It will support multiple simultaneous sessions and applications, up to the number the kernel is started with. The kernel will run in real mode, and must be started before Windows. Data will have to be copied or remapped, and there will be a performance impact which is hard to estimate, but will probably make the kernel less than 25% slower. The asynchronous handler will be supported. This is used by the kernel to post a windows message to one of our applications when it has received a frame for the window. The kernel will use its present buffering scheme in this version.

Version 2.01 of LANWatch Released

by James VanBokkelen

The new drivers we re adding to version 2.01 are LW-110, for the Packet Driver, and LW-126 for the Ungermann-Bass PS/2 NIC interface (also sold as the IBM Micro Channel™ Baseband Adapter and AT&T Micro Channel Adapter). The Packet Driver version of LANWatch won t work with packet drivers that don t support the extended functions, because we need to set the interface into promiscuous mode, and because LANWatch exercises a few different aspects of the Packet Driver specification than the PC/TCP kernel.

New features include more information in many of the error messages and status indications on the bottom of the display, as well as parsing of SNMP Trap packets and Server Message Block file-sharing protocols.

Some of the more routine changes include parsing for a few new manufacturer codes, and some driver changes which will let you enlarge your MAC and IP name tables, and use MAC and IP names when specifying filters.

Bug fixes that we ve made include properly handling VGA systems with two displays attached (LANWatch currently uses only one, but it used to refuse to work at all), and fixing driver problems related to getting network errors under conditions of extreme load.

Release of SNMP Tools for DOS

by Bruce Campbell

We have just released a set of RFC-compliant SNMP tools which can be used by a technically knowledgeable person to perform network management functions. They implement the complete Simple Network Management Protocol (Get, Next, Set, and Trap) functions as defined in RFC 1098 and can get any MIB data which is compliant with RFC 1065, Structure of Management Information. We also wrote additional applications for monitoring hosts, and displaying and collecting operations data.

The RFC-defined SNMP functions are implemented in a command-line user interface with features that make them easier to use. Requests use symbolic SNMP variable descriptors, not the confusing ASN.1 dot notation; responses show symbolic descriptor, data type, and value, as well as the dot notation. To save retyping, multiple requests may be made from a given host at one time and second requests are made automatically if the first one fails. Helpful messages are generated when a host is not available or other errors occur. If a bad packet is returned, the -d option will parse the packet to aid debugging.

The basic functions implemented are:

¥ **get**, which asks an SNMP agent for the value of one or more MIB variables and displays the response.

¥ **next1**, which is similar to **get**, except that it requests the next SNMP variable in the tree under the variable specified on the command line.

continued

¥ **nextx**, which asks for the rest of the subtree under the variable specified.

¥ **sett**, which modifies, or set s, an SNMP variable. This can be used for anything from restarting a host to changing an IP address. Any variable which a manufacturer makes available to the set option can be modified.

¥ **trapd**, which captures SNMP traps and displays them in real time. The complete set of traps are recognized, including: ColdStart, WarmStart, LinkDown, LinkUp, AuthenticationFailure, EgpNeighborLoss, and EnterpriseSpecific.

We created the following network management features to enhance the functionality of the basic SNMP calls:

¥ **stat** prints a formatted display of the IP, TCP, UDP, EGP, ICMP, AT, Interface, and System MIB-1 subtrees. All subtrees can also be displayed with a single argument.

¥ **mon** monitors the response of hosts to pings and SNMP requests. Thus, even hosts without SNMP agents can be monitored. **mon** sends **ping** requests and SNMP requests, at a user defined interval, to up to 80 hosts in a standard hosts file. All of the hosts are displayed onscreen in a specific color (or shade) showing whether they are responding to **ping** requests, responding to SNMP requests, or not responding at all. Status changes are announced with a tone. This is especially useful for network managers who monitor a large number of hosts.

¥ **dog** is a watchdog program which queries a list of hosts for the values of specified variables at a user defined interval. Data is displayed as delta values and running averages to make it more informative. In addition to displaying data, maximum and minimum thresholds can be specified for each variable to generate alarms. **dog** will send mail detailing alarms, so a user is notified of problems immediately. Data can also be dumped to *.err* and *.log* files which are designed for post-processing analysis of data. One of the uses for such post-processing might be to load the information into a database for later retrieval and manipulation.

¥ **graph** is used to generate color bar graphs of one or more SNMP variables. A good use of graph is to show percentage of use for an interface. Autoscaling options ensure that all data is clearly displayed. Up to four graphs can be displayed at a time.

Because SNMP Tools uses the PC/TCP kernel, it will operate on Ethernet, Starlan, 802.5, and Token Ring networks. Over 60 different network interface cards are supported, making it possible to use practically any interface card on the market. SNMP Tools will run on IBM PC®s, AT®s, PS/2®s, or compatibles, including laptops, so a site can usually install SNMP Tools without buying any new hardware.

The libraries for the SNMP Tools will be included in the Development Kit available for version 2.05 of PC/TCP for DOS, which will be shipping in mid-November. Written in Microsoft C 5.1, the libraries can be used to develop custom SNMP applications. One possible use for the libraries might be to take the calls, which are robust and well tested, and build a friendly user interface.

The Past, Present, and Future of PC/TCP for OS/2

by Bill Rust

On April 2, 1990, FTP Software began shipping Version 1.0 of PC/TCP for OS/2. This article covers three areas: where the OS/2 product came from, what it is and how it differs from our DOS product, and what we intend to do with it. Obviously, our plans are subject to change, but this information may be useful as a statement of what we think is important.

Product Origins

PC/TCP for OS/2 product is a port of the BSD 4.3 networking software. As you might be aware, there have only been about half a dozen independent TCP/IP development projects, with two being particularly noteworthy: the Berkeley UNIX project and the M.I.T. DOS project. Our DOS product is based on the M.I.T. work; in fact one of our founders, John Romkey, did much of the development work while a student at M.I.T. Our OS/2 product is based on the Berkeley UNIX project.

Currently, we are maintaining expertise with both protocol stacks. This allows us to understand and integrate changes to either stack. It also allows for our technical support staff to have access to knowledge about the standard Berkeley networking software, to make their support load easier.

Differences between PC/TCP for DOS and PC/TCP for OS/2

While similar in functionality to the DOS product, some changes exist, which result from differences that arise from the different lineage of the two. For example, the OS/2 **ping** program keeps pinging until the user stops it, whereas the DOS **ping** program does not, unless the -t option is specified on the command line.

A second big difference is that the OS/2 product is NDIS based. This means that instead of the twenty part numbers (one for each card) of the DOS product, there is only one part number (the DOS product has something similar with the packet driver kernel). The card vendor supplies the actual device driver that is associated with the protocol stack (in our case, PC/TCP) using the Protocol Manager. This ensures that the people most familiar with the hardware are the people writing the software that runs it. It also simplifies our production process and means that a customer can order our product and not worry about getting the wrong version.

The third big difference has to do with the nature of OS/2. OS/2 is multi-tasking, which means that more than one program can be loaded and active at one time, without the problems that DOS has with TSRs. Further, the 640K limit of DOS is gone. To take advantage of this, PC/TCP for OS/2 supplies several server programs. These server programs include **ftpd**, **telnetd**, and several others. Now, the FTP server (**ftpd**) can be run in the background while the user runs whatever other programs he or she wants.

Finally, a low performance router is included in the package. While we really don t recommend using it (in general routers should be dedicated machines, not machines used for other tasks), there are a couple of situations where **routed** is useful. If two subnets need to be tied together to provide mail exchange or Telnet access, then **routed** might be a reasonable way to go.

We also started shipping a Development Kit for the product in June of this year. Currently, it offers 4.3BSD sockets in both small and large memory models as the interface to the kernel.

The Future

FTP Software intends to make many enhancements to PC/TCP for OS/2. Obviously this list is subject to change without notice and no guarantee is made as to when or in what order these additions will be made.

We will be adding **sendmail**, an SMTP server, which allows an independent network of PCs to exchange mail. Currently, all mail exchanged between PCs has to go through a UNIX-based mail server.

Kerberos, an encryption scheme for data traveling over the physical media (Ethernet, Token Ring, Starlan, etc.), will be added to the FTP, Telnet, and other applications. We will also be converting some of the applications to the Presentation Manager™ environment.

Our grand unified Telnet application, which includes VT220 and IBM 3270 emulation in one executable, will be ported from DOS. We will also add an equivalent to the INT14 Telnet interface used by DOS which will allow third party terminal emulators to access the net.

BIND, the Berkeley Internet Name Daemon, will be added to provide name resolution service on a PC-only network. Both server and client implementations of NFS will be added to allow mounting of remote disk drives. NETBIOS will also be added to allow document and application sharing.

A future release of the Development Kit will have several new libraries *telnet.lib*, *ftp.lib*, and *snmp.lib* will be developed, as well as a *glue.lib* to aid in porting DOS applications to OS/2.

These are the highlights of what FTP intends to do PC/TCP for OS/2 over the next year or so. There may be some things that have been omitted from this list, but we feel that OS/2 will be important enough to devote a fair amount of resources to its development. Comments and questions about the product are very welcome.

International VAR List

FTP Software Sells its products directly to end users in the United States. Sales to end users in other countries are made through OEMs and Value Added Resellers (VARs). They have signed agreements with FTP Software to dis-tribute up-to-date software and provide quality support. Here is a list of our international VARs.

Australia

Datacraft Manufacturing Pty. Ltd, Victoria
Tel: (61) 3 727 9111

MM Data Networks, Pymble NSW
Tel: (61) 2 488 8799

Network Solutions Pty. Ltd., Chatswood NSW
Tel: (61) 2 415 0500

Austria

Open Systems, Wein
Tel: (43) 1 513 91 62

Schoeller Electronics, Wien
Tel: (43) 222 842 631

Belgium

Belgian Net Builders, Opwijk
Tel: (32) 52 350 712

Comsol n.v., Brussels
Tel: (32) 2 425 1146

Koning En Hartman, Brussels
Tel: (32) 2 672 26 07

IMX, Zaventem
Tel: (32) 2 725 49 50

Positronika N.V./S.A., Aalst-Erembodegem
Tel: (32) 53 650 411

Canada

Allan Crawford & Associates, Mississauga, ON
Tel: (416) 890-2010, Fax: (416) 890-1959

Choreo Systems Ottawa, ON
Tel: (613) 238-1050, Fax: (613) 238-4453

Kanatek Technologies Kanata, ON
Tel: (613) 591-1482, Fax: (613) 591-1488

Columbia

Software Abierto, Bogota
Tel: (571) 212 9512, Fax: (571) 257 7681

Denmark

Cinet Denmark A/S, Herlev
Tel: (45) 2 94 73 77

Danadata A/S, Arhus
Tel: (45) 86 18 28 44, Fax: (45) 86 18 28 92

Macrocom, Kobenhavn
Tel: (45) 35 82 50 60, Fax: (45) 31 85 30 90

Finland

Lab Hi-Tech oy, Helsinki
Tel: (358) 0672497, Fax: (358) 06927724

Mikrolog, Espoo
Tel: (358) 0804611, Fax: (358) 08036617

Nordic Data Comm Espoo
Tel: (358) 08036033, Fax: (358) 08038614

Santa Monica, Espoo
Tel: (358) 08042544, Fax: (358) 08042606

Technical Systems, Helsinki
Tel: (358) 06926360, Fax: (358) 0679750

France

Top Log International, Suresnes
Tel: (33) 142042118, Fax: (33) 147729183

Germany

DNS GMBH, Olching
Tel: (49) 8142 18048, Fax: (49) 8142 3890

Raffel, Ratingen
Tel: (49) 21 02 45 0226, Fax: (49) 21 02 45 0245

Stemmer, Puchheim
Tel: (49) 89 809020, Fax: (49) 89 8090216

Telemation, Kronberg
Tel: (49) 6173 70900, Fax: (49) 6173 68788

Zellner, Munich
Tel: (49) 89 834 3086, Fax: (49) 89 834 2651

Singapore

NETBAND Technology
Tel: (65) 2748266, Fax: (65) 2782211

Iceland

Tolvusalan HF, Reykjavik
Tel: (354) 1 84779, Fax: (354) 1 687495

India

Priya Electronics, San Jose, Ca. USA
Tel: (408) 9541866, Fax: (408) 9548336

Israel

Bynet Data Communications, Tel-Aviv
Tel: (972) 3494511, Fax: (972) 35447990

Mitan Computers, Givataim
Tel: (972) 3324519, Fax: (972) 35795111

Italy

Fibronica, Milan
Tel: (39) 233403892, Fax: (39) 23083781

Optilan Systems Sesto, San Giovanni
Tel: (39) 226222317, Fax: (39) 226222313

Japan

Allied Telesis, K.K., Tokyo
Tel: 81 3 443 5640, Fax: 81 3 443 2443

Korea

Interlink, Seoul
Tel: (82) 22782053 or 2054, Fax: (82) 22782055

KCOM, Seoul
Tel: (82) 25630456, Fax: (82) 25630457

Malaysia

Berita Information Services, Kuala Lumpur
Tel: (60) 32741166, Fax: (60) 32741305

Mexico

Computadoras Micron Irapuato, Gto.
Tel: (52) 46251677

The Netherlands

Geveke Electronics, Amsterdam
Tel: (31) 20 5861411, Fax: (31) 20 5861568

Interay, Friesland
Tel: (31) 5116 4052, Fax: (31) 5116 4720

Vosko, Waddinxveen
Tel: (31) 1828 10666, Fax: (31) 1828 16755

New Zealand

MM Data Networks, Auckland
Tel: (64) 9772760, Fax: (64) 93022454

Norway

Cinet A/S, Oslo
Tel: (47) 2371075, Fax: (47) 2385818

Cosmotronic, Rud
Tel: (47) 2138120, Fax: (47) 2138980

Portugal

Topis International, Queluz de Baixo
Fax: (351) 1956405

Puerto Rico

Velez Computer System, San Juan
Tel: (809) 7235145, Fax: (809) 7210062

Singapore

Netband Technology Pte Ltd
Tel: (65) 2782211, Fax: (65) 2748266

Spain

ATD Sistemas, S.A., Madrid
Tel: (34) 12344000, Fax: (34) 15347663

Diode Espana, Madrid

Sweden

Edvina/Systprog, Solna
Tel: (46) 87356190, Fax: (46) 87354024

Heath Comm, Sundbyberg
Tel: (46) 87579700, Fax: (46) 87332330

Lundin Datasystem, Lund
Tel: (46) 46320090, Fax: (46) 46320091

Microfront, Vaxjo
Tel: (46) 47081065, Fax: (46) 47082356

TPM Produkter, Kista
Tel: (46) 87039555, Fax: (46) 87520901

Switzerland

Adcomp Ltd., Zurich
Tel: (41) 1 741 41 11, Fax: (41) 1 741 45 20

Softway, San Francisco, Ca.
Tel: (41) 53974666, Fax: (41) 53974677

W. Stolz AG, Baden-Dattwil
Tel: (41) 56 84 90 00, Fax: (41) 56 83 19 63

Taiwan, Republic of China

Longshine Electronics, Taipei
Tel: (886) 23634958, Fax: (886) 23626810

Nippon Data Systems, Taipei
Tel: (886) 25033223, Fax: (886) 27350670

United Kingdom

Unipalm, Cambridge
Tel: (011) 44954211797, Fax: (011) 44954211244

Yugoslavia

Mikrohit, Slovena
Fax: (35) 88036617

Network Working Group
Request for Comments: 1173

J. Van Bokkelen
FTP Software, Inc.
August 1990

Responsibilities of Host and Network Managers
A Summary of the Oral Tradition of the Internet

Status of this Memo

This informational RFC describes the conventions to be followed by those in charge of networks and hosts in the Internet. It is a summary of the oral tradition of the Internet on this subject. [RFC Editor s note: This memo is a contribution by the author of his view of these conventions. It is expected that this RFC will provide a basis for the development of official policies in the future.] These conventions may be supplemented or amended by the policies of specific local and regional components of the Internet. This RFC does not specify a standard, or a policy of the IAB. Distribution of this memo is unlimited.

Table of Contents

Status of this Memo 1
1. Basic Responsibilities 1
2. Responsibilities of Network Managers 2
3. Responsibilities of Host System Managers 2
4. Postmaster@foo.bar.baz 3
5. Problems and Resolutions 3
6. The Illusion of Security 4
7. Summary 5
8. Security Considerations 5
9. Author’s Address 5

1. Basic Responsibilities

The Internet is a co-operative endeavor, and its usefulness depends on reasonable behavior from every user, host and router in the Internet. It follows that people in charge of the components of the Internet MUST be aware of their responsibilities and attentive to local conditions. Furthermore, they MUST be accessible via both Internet mail and telephone, and responsive to problem reports and diagnostic initiatives from other participants.

Even local problems as simple and transient as system crashes or power failures may have widespread effects elsewhere in the net. Problems which require co-operation between two or more responsible individuals to diagnose and correct are relatively common. Likewise, the tools, access and experience needed for efficient analysis may not all exist at a single site.

This communal approach to Internet management and maintenance is dictated by the present decentralized organizational structure. The structure, in turn, exists because it is inexpensive and responsive to diverse local needs. Furthermore, for the near term, it is our only choice; I don’t see any prospect of either the government or private enterprise building a monolithic, centralized, ubiquitous Ma Datagram network provider in this century.

2. Responsibilities of Network Managers

One or more individuals are responsible for every IP net or subnet which is connected to the Internet. Their names, phone numbers and postal addresses MUST be supplied to the Internet NIC (or to the local or regional transit network s NIC) prior to the network s initial connection to the Internet, and updates and corrections MUST be provided in a timely manner for as long as the net remains connected.

In order to adequately deal with problems that may arise, a network manager must have either:

A. System management access privileges on every host and router connected to the local network, or:

B. The authority and access to either power off, reboot, physically disconnect or disable forwarding IP datagrams from any individual host system that may be misbehaving.

For all networks, a network manager capable of exercising this level of control MUST be accessible via telephone 8 hours a day, 5 days a week. For nets carrying transit traffic, a network manager SHOULD be accessible via telephone 24 hours a day.

3. Responsibilities of Host System Managers

One or more individuals must be responsible for every host connected to the Internet. This person MUST have the authority, access and tools necessary to configure, operate and control access to the system. For important timesharing hosts, primary domain name servers and mail relays or gateways, responsible individual(s) SHOULD be accessible via telephone 24 hours a day, 7 days a week.

For less important timesharing hosts or single-user PCs or workstations, the responsible individual(s) MUST be prepared for the possibility that their network manager may have to intervene in their absence, should the resolution of an Internet problem require it.

4. Postmaster@foo.bar.baz

Every Internet host that handles mail beyond the local network MUST maintain a mailbox named postmaster . In general, this should not simply forward mail elsewhere, but instead be read by a system maintainer logged in to the machine. This mailbox SHOULD be read at least 5 days a week, and arrangements MUST be made to handle incoming mail in the event of the absence of the normal maintainer.

A machine s postmaster is the normal point of contact for problems related to mail delivery. Because most traffic on the long-haul segments of the Internet is in the form of mail messages, a local problem can have significant effects elsewhere in the Internet. Some problems may be system-wide, such as disk or file system full, or mailer or domain name server hung, crashed or confused. Others may be specific to a particular user or mailing list (incorrect aliasing or forwarding, quota exceeded, etc.).

In either case, the maintainer of a remote machine will normally send mail about delivery problems to postmaster . Also, postmaster is normally specified in the reply-to: field of automatically generated mail error messages (unable to deliver due to nonexistent user name, unable to forward, malformed header, etc.). If this mailbox isn t read in a timely manner, significant quantities of mail may be lost or returned to its senders.

5. Problems and Resolutions

Advances in network management tools may eventually make it possible for a network maintainer to detect and address most problems before they affect users, but for the present, day-to-day users of networking services represent the front line. No responsible individual should allow their dumb-question filter to become too restrictive; reports of the form I haven t gotten any mumblefrotz mail for a week... or I could get there this morning, but not now... should always get timely attention.

There are three basic classes of problems that may have network-wide scope: User-related, host-related and network-related.

A. User-related problems can range from bouncing mail or uncivilized behavior on mailing lists to more serious issues like violation of privacy, break-in attempts or vandalism.

B. Host-related problems may include mis-configured software, obsolete or buggy software and security holes.

C. Network-related problems are most frequently related to routing: incorrect connectivity advertisements, routing loops and black holes can all have major impacts. Mechanisms are usually in place for handling failure of routers or links, but problems short of outright failure can also have severe effects.

Each class of problem has its own characteristics. User-related problems can usually be solved by education, but system managers should be aware of applicable federal and state law as well. Privacy violations or cracking attempts have always been grounds for pulling a user s account, but now they can also result in prosecution. Host-related problems are usually resolvable by reconfiguration or upgrading the software, but sometimes the manufacturer needs to be made aware of a bug, or jawboned into doing something about it; bugs that can t be fixed may be serious enough to require partial or total denial of service to the offending system. Similar levels of escalation exist for network-related problems, with the solution of last resort being ostracism of the offending net.

6. The Illusion of Security

Every host and network manager MUST be aware that the Internet as presently constituted is NOT secure. At the protocol level, much more effort has been put into interoperability, reliability and convenience than has been devoted to security, although this is changing. Recent events have made software developers and vendors more sensitive to security, in both configuration and the underlying implementation, but it remains to be demonstrated how much long-term effect this will have. Meanwhile, the existing system survives through the co-operation of all responsible individuals.

Security is subjective; one site might view as idle curiosity what another would see as a hostile probe. Since ultimately the existence of the Internet depends on its usefulness to all members of the community, it is important for managers to be willing to accept and act on other sites security issues, warning or denying access to offending users. The offended site, in turn, must be reasonable in its demands (someone who set off an alarm while idly seeing if the sendmail DEBUG hole was closed on a sensitive host probably should be warned, rather than prosecuted).

Because Internet security issues may require that local management people either get in touch with any of their users, or deny an offending individual or group access to other sites, it is necessary that mechanisms exist to allow this. Accordingly, Internet sites SHOULD NOT have general use accounts, or open (without password) terminal servers that can access the rest of the Internet.

In turn, the sensitive sites MUST be aware that it is impossible in the long term to deny Internet access to crackers, disgruntled former employees, unscrupulous competitors or agents of other countries. Getting an offender flushed is at best a stop-gap, providing a breathing space of a day or an hour while the security holes under attack are closed. It follows that each host s manager is ultimately responsible for its security; the more sensitive the application or data, the more intimate the manager must be with the host s operating system and network software and their foibles.

7. Summary

The heart of the Internet is the unique community of interest encompassing its users, operators, maintainers and suppliers. Awareness and acceptance of the shared interest in a usable Internet is vital to its survival and growth. The simple conventions presented here should be supplemented by common sense as necessary to achieve that end.

8. Security Considerations

Security issues are discussed in Sections 5 and 6.

9. Author’s Address

James B. VanBokkelen
FTP Software Inc.
26 Princess St.
Wakefield, MA 01880

Phone: 617-246-0900

EMail: jbvb@ftp.com