               FYI on a Network Management Tool Catalog:
             Tools for Monitoring and Debugging TCP/IP Internets
                       and Interconnected Devices

Status of this Memo

Abstract

   The goal of this FYI memo is to provide an update to FYI 2, RFC 1147
   [1], which provided practical information to site administrators and
   network managers. New and/or updated tools are listed in this RFC.
   Additonal descriptions are welcome, and should be sent to: noctools-
   entries@merit.edu.

Introduction

   A static document cannot incorporate references to the latest tools
   nor recent revisions to the older catalog entries. To provide a more
   timely and responsive information source, the NOCtools catalog is
   available on-line via the Internet and Usenet.

       news   comp.networks.noctools
       ftp   wuarchive.wustl.edu:/doc/noctools

   Because of publication delays and other factors, some of the entries
   in this catalog may be out of date. The reader is urged to consult
   the on-line service to obtain the most up-to-date information.

   The index provided in this document reflects the current contents of
   the on-line documentation.

   The NOCtools2 Working Group of the Internet Engineering Task Force
   (IETF) has compiled this revised catalog. Future revisions will be
   incorporated into the on-line NOCtools catalog. The reader is
   encouraged to submit new or revised entries for (near-immediate)
   electronic publication.

The tools described in this catalog are in no way endorsed by the
IETF. For the most part, we have neither evaluated the tools in this
catalog, nor validated their descriptions. Most of the descriptions
of commercial tools have been provided by vendors. Caveat Emptor.

Acknowledgements

This catalog is the result of work on the part of the NOCTools2
Working Group of the User Services Area of the IETF. The following
individuals made especially notable contributions: Chris Myers,
Darren Kinley, Gary Malkin, Mohamed Ellozy, and Mike Patton.

Current Postings

The current contents of the NOCtools catalog may be retrieved via
anonymous FTP from wuarchive.wustl.edu. The entries are stored as
individual files in the directory /doc/noctools.

"No-Writeups" Appendix

This section contains references to tools which are known to exist,
but which have not been fully cataloged. If anyone wishes to author
an entry for one of these tools please contact us at:

        noctools-request@merit.edu

Keep in mind that if these or other tools are included in the future,
they will be available in the on-line version of the catalog.

Each mention is separated by a <form-feed> for improved readability.
If you intend to actually print-out this section of the catalog, then
you should probably strip-out the <ff>.

How to Submit/Update an Entry

     1) review the template included below to determine what
        information you will need to collect,
     2) review the keywords to see what your indexing options are,
     3) assemble (update) catalog entry to include results of
        1) and 2).
     4) Submit your entry using either of the following two methods:

        a) Post your submission to: comp.internet.noctools.submissions
        b) Email your submission to: noctools-entries@merit.edu

New entries will be circulated automatically upon reception. As time
permits, the NOCtools editors will review recent submissions and
incorporate them into the master indexes. Enquiries regarding the

status of a submission should be E-Mailed to:

                          noctools-request@merit.edu

Those submitting an entry to the catalog should insure that any E-mail addresses provided are correct and functional. Either the catalog editors or prospective users of your tool may wish to reach you.

TEMPLATE

   NAME
           <tool-name>

   KEYWORDS
           [<keyword-A1>[,<keyword-A2>[,...,<keyword-An>]]];
           [<keyword-B1>[,<keyword-B2>[,...,<keyword-Bn>]]];
           [<keyword-C1>[,<keyword-C2>[,...,<keyword-Cn>]]];
           [<keyword-D1>[,<keyword-D2>[,...,<keyword-Dn>]]];
           [<keyword-E1>[,<keyword-E2>[,...,<keyword-En>]]].

   ABSTRACT
           <summary of the tool>
           <summary of the tool>
           <summary of the tool>

   MECHANISM
           <high level technical details of how it works>
           <high level technical details of how it works>
           <high level technical details of how it works>

   CAVEATS
           <any warnings or cautions>
           <any warnings or cautions>
           <any warnings or cautions>

   BUGS
           <any warnings or cautions>
           <any warnings or cautions>
           <any warnings or cautions>

   LIMITATIONS
           <any warnings or cautions>
           <any warnings or cautions>
           <any warnings or cautions>

   HARDWARE REQUIRED
           <list any hardware requirements>
           <list any hardware requirements>
           <list any hardware requirements>

      SOFTWARE REQUIRED
              <list any software requirements>
              <list any software requirements>
              <list any software requirements>

      AVAILABILITY AND CONTACT POINT FOR INFORMATION ABOUT THIS TOOL
              <How to acquire the tool.>
              <Location/Contact Info to access/obtain tool>

      CONTACT POINT FOR CHANGES TO THIS CATALOG ENTRY
              <Contact info for person responsible for catalog entry>

      DATE OF MOST RECENT UPDATE TO THIS CATALOG ENTRY
              <YYMMDD>

Keywords

   This catalog uses "keywords" for terse characterizations of the
   tools. Keywords are abbreviated attributes of a tool or its use. To
   allow cross-comparison of tools, uniform keyword definitions have
   been developed, and are given below. Following the definitions,
   there is an index of catalog entries by keyword.

Keyword Definitions

   The keywords are always listed in a prefined order, sorted first by
   the general category into which they fall, and then alphabetically.
   The categories that have been defined for management tool keywords
   are:

                o   the general management area to which a tool
                      relates or a tool's functional role;

                o   the network resources or components that are
                      managed;

                o   the mechanisms or methods a tool uses to
                      perform its functions;

                o   the operating system and hardware environment
                      of a tool; and

                o   the characteristics of a tool as a hardware
                      product or software release.

The keywords used to describe the general management area or
functional role of a tool are:

Alarm
     a reporting/logging tool that can trigger on specific
     events within a network.

Analyzer
     a traffic monitor that reconstructs and interprets pro-
     tocol messages that span several packets.

Benchmark
     a tool used to evaluate the performance of network com-
     ponents.

Control
     a tool that can change the state or status of a remote
     network resource.

Debugger
     a tool that by generating arbitrary packets and moni-
     toring traffic, can drive a remote network component to
     various states and record its responses.

Generator
     a traffic generation tool.

Manager
     a distributed network management system or system com-
     ponent.

Map
     a tool that can discover and report a system's topology
     or configuration.

Reference
     a tool for documenting MIB structure or system confi-
     guration.

Routing
     a packet route discovery tool.

Security
     a tool for analyzing or reducing threats to security.

Status
     a tool that remotely tracks the status of network com-
     ponents.

Traffic
a tool that monitors packet flow.

The keywords used to identify the network resources or components
that a tool manages are:

Bridge
a tool for controlling or monitoring LAN bridges.

CHAOS
a tool for controlling or monitoring implementations of
the CHAOS protocol suite or network components that use
it.

DECnet
a tool for controlling or monitoring implementations of
the DECnet protocol suite or network components that
use it.

DNS
a Domain Name System debugging tool.

Ethernet
a tool for controlling or monitoring network components
on ethernet LANs.

FDDI
a tool for controlling or monitoring network components
on FDDI LANs or WANs.

IP
a tool for controlling or monitoring implementations of
the TCP/IP protocol suite or network components that
use it.

OSI
a tool for controlling or monitoring implementations of
the OSI protocol suite or network components that use
it.

NFS
a Network File System debugging tool.

Ring
a tool for controlling or monitoring network components
on Token Ring LANs.

SMTP
     an SMTP debugging tool.

Star
     a tool for controlling or monitoring network components
     on StarLANs.

The keywords used to describe a tool's mechanism are:

CMIS
     a network management system or component based on
     CMIS/CMIP, the Common Management Information System and
     Protocol.

Curses
     a tool that uses the "curses" tty interface package.

Eavesdrop
     a tool that silently monitors communications media
     (e.g., by putting an ethernet interface into "promiscu-
     ous" mode).

NMS
     the tool is a component of or queries a Network Manage-
     ment System.

Ping
     a tool that sends packet probes such as ICMP echo mes-
     sages; to help distinguish tools, we do not consider
     NMS queries or protocol spoofing (see below) as probes.

Proprietary
     a distributed tool that uses proprietary communications
     techniques to link its components.

RMON
     a tool which employs the RMON extensions to SNMP.

SNMP
     a network management system or component based on SNMP,
     the Simple Network Management Protocol.

Spoof
     a tool that tests operation of remote protocol modules
     by peer-level message exchange.

X
     a tool that uses X-Windows.

   The keywords used to describe a tool's operating environment are:

        DOS
             a tool that runs under MS-DOS.

        HP
             a tool that runs on Hewlett-Packard systems.

        Macintosh
             a tool that runs on Macintosh personal computers.

        OS/2
             a tool that runs under the OS/2 operating system.

        Standalone
             an integrated hardware/software tool that requires only
             a network interface for operation.
        Sun
             a tool that runs on Sun Microsystems platforms.
             (binary distribution built for use on a Sun.)

        UNIX
             a tool that runs under 4.xBSD UNIX or related OS.

        VMS
             a tool that runs under DEC's VMS operating system.

   The keywords used to describe a tool's characteristics as a hardware
   or software acquisition are:

        Free
             a tool is available at no charge, though other restric-
             tions may apply (tools that are part of an OS distribu-
             tion but not otherwise available are not listed as
             "free").

        Library
             a tool packaged with either an Application Programming
             Interface (API) or object-level subroutines that may be
             loaded with programs.

        Sourcelib
             a collection of source code (subroutines) upon which
             developers may construct other tools.

Tools Indexed by Keywords

   Following is an index of the most up-to-date catalog entries sorted
   by keyword, which is available via:

      news   comp.networks.noctools.tools
      ftp   wuarchive.wustl.edu:/doc/noctool

   This index can be used to locate the tools with a particular
   attribute: tools are listed under each keyword that characterizes
   them. The keywords and the subordinate lists of tools under them are
   in alphabetical order.

   Alarm

   CMIP Library
   Dual Manager
   Eagle
   EMANATE
   EtherMeter
   LanProbe
   LANWatch
   MONET
   NetMetrix Load Monitor
   NetMetrix Protocol Analyzer
   NETMON for Windows
   NETscout
   NOCOL
   SNMP Libraries and Utilities from Empire Technologies
   SNMP Libraries and Utilities from SNMP Research
   snmpd from Empire Technologies
   SpiderMonitor
   XNETMON from SNMP Research
   xnetmon from Wellfleet

   Analyzer

   LANVista
   LANWatch
   NetMetrix Protocol Analyzer
   NETscout
   PacketView
   Sniffer
   SpiderMonitor

Benchmark
----
hammer & anvil
iozone
LADDIS
LANVista
nhfsstone
SPIMS
spray
ttcp
XNETMON from SNMP Research

CMIS

CMIP library
Generic Managed System
MIB Browser

Control

CMIP Library
Dual Manager
Eagle
MIB Manager from Empire Technologies
MONET
NETMON for Windows
proxyd
SNMP Libraries and Utilities from Empire Technologies
SNMP Libraries and Utilities from SNMP Research
SNMP Packaged Agent System
snmpd from Empire Technologies
TokenVIEW
XNETMON from SNMP Research

Debugger

Ethernet Box II
LANVista
NetMetrix Traffic Generator
ping from UCB
SPIMS
XNETMON from SNMP Research

Generator
----
hammer & anvil
LADDIS
LANVista

        NetMetrix Traffic Generator
        nhfsstone
        ping
        ping from UCB
        Sniffer
        SpiderMonitor
        spray
        TTCP

        Manager

        Beholder
        CMIP Library
        CMU SNMP Distribution
        decaddrs by Wellfleet
        Dual Manager
        EMANATE
        Ethernet Box II
        getone by Wellfleet
        Interactive Network Map
        LanProbe
        LANVista
        MIB Manager from Empire Technologies
        MONET
        NetLabs CMOT Agent
        NetLabs SNMP Agent
        NETMON for Windows
        NETscout
        NNStat
        NOCOL
        OverVIEW
        SAS/CPE for Open Systems Software
        SNMP Development Kit
        SNMP Libraries and Utilities from Empire Technologies
        SNMP Libraries and Utilities from SNMP Research
        SNMP Packaged Agent System
        snmpd from Empire Technologies
        tokenview
        Tricklet
        Wollongong-Manager
        XNETMON from SNMP Research
        XNETMON from Wellfleet
        xnetperfmon

        Map
        ---
        decaddrs by Wellfleet
        Dual Manager

        etherhostprobe
        EtherMeter
        Interactive Network Map
        LanProbe
        NETMON for Windows
        Network Integrator I
        NPRV
        SNMP Libraries and Utilities from SNMP Research
        XNETMON by SNMP Research
        XNETMON by Wellfleet

        Reference

        EMANATE
        ethernet-codes
        HyperMIB
        MIB Manager from Empire Technologies
        XNETMON

        Routing
        ----
        arp
        decaddrs by Wellfleet
        etherhostprobe
        getone by Wellfleet
        hopcheck
        MONET
        net_monitor
        NETMON for Windows
        netstat
        NPRV
        ping from UCB
        query
        traceroute

        Security

        Computer Security Checklist
        Dual Manager
        Eagle
        EMANATE
        LAN Patrol
        SNMP Libraries and Utilities from SNMP Research
        XNETMON by SNMP Research
        xnetperfmon

```
Status
------
Beholder
CMIP Library
CMU SNMP
DiG
dnsstats
doc
Dual Manager
EMANATE
fping
getone by Wellfleet
host
Internet Rover
lamers
LanProbe
mconnect
MONET
net_monitor
Netlabs CMOT Agent
Netlabs SNMP Agent
NETscout
NNStat
NOCOL
NPRV
OverVIEW
ping
ping from UCB
proxyd from SNMP Research
SAS/CPE
SNMP Development Kit
SNMP Libraries and Utilities from Empire Technologies
SNMP Libraries and Utilities from SNMP Research
SNMP Packaged Agent System
PSI SNMP
snmpd from Empire Technologies
snmpd from SNMP Research
TokenVIEW
Tricklet
vrfy
XNETMON by SNMP Research
xnetmon by Wellfleet
xnetperfmon
xup
```

    Traffic
    ----
    etherfind
    EtherMeter
    Ethernet Box II
    EtherView
    getethers
    LAN Patrol
    LanProbe
    LANVista
    LANWatch
    ENTM
    MONET
    NetMetrix Load Monitor
    NetMetrix NFS Monitor
    NetMetrix Protocol Analyzer
    NetMetrix Traffic Generator
    NETMON by Mitre
    NETscout
    netwatch
    Network Integrator I
    nfswatch
    nhfsstone
    NNStat
    ositrace
    PacketView
    Sniffer
    SpiderMonitor
    spray
    tcpdump
    tcplogger
    trpt
    ttcp
    XNETMON by SNMP Research

    Bridge
    ------
    decaddrs by Wellfleet
    EMANATE
    MIB Manager from Empire Technologies
    MONET
    proxyd by SNMP Research
    SAS/CPE
    SNMP Libraries and Utilities from SNMP Research
    SNMP Packaged Agent System
    snmpd from SNMP Research
    XNETMON from SNMP Research

CHAOS

Interactive Network Map
LANWatch

DECnet
------
decaddrs by Wellfleet
LANVista
LANWatch
MONET
net_monitor
NetMetrix Protocol Analyzer
NETMON for Windows
NETscout
Sniffer
SNMP Libraries and Utilities from SNMP Research
SpiderMonitor
XNETMON from SNMP Research
xnetperfmon from SNMP Research

DNS

DiG
dnsstats
doc
lamers
LANWatch
NetMetrix Protocol Analyzer
NOCOL

Ethernet
----
arp
Beholder
Eagle
EMANATE
etherfind
etherhostprobe
EtherMeter
Ethernet Box II
ethernet-codes
EtherView
getethers
LAN Patrol
LanProbe
LANVista
LANWatch

ENTM
Interactive Network Map
MONET
NetMetrix Load Monitor
NetMetrix NFS Monitor
NetMetrix Protocol Analyzer
NetMetrix Traffic Generator
NETMON for Windows
NETscout
netwatch
Network Integrator I
nfswatch
NNStat
PacketView
proxyd from SNMP Research
SAS/CPE
Sniffer
SNMP Libraries and Utilities from SNMP Research
SNMP Packaged Agent System from SNMP Research
snmpd from SNMP Research
SpiderMonitor
tcpdump
XNETMON from SNMP Research
xnetperfmon from SNMP Research

FDDI

EMANATE
ethernet-codes
NetMetrix Load Monitor
NetMetrix NFS Monitor
NetMetrix Protocol Analyzer
NetMetrix Traffic Generator
nfswatch
SAS/CPE
SNMP Libraries and utilities from SNMP Research
SNMP Packaged Agent System from SNMP Research
snmpd from SNMP Research
XNETMON from SNMP Research

IP
--
arp
CMU SNMP
Dual Manager
Eagle
EMANATE
etherfind

```
etherhostprobe
EtherView
fping
getone from Wellfleet
hammer & anvil
hopcheck
Internet Rover
LanProbe
LANVista
LANWatch
ENTM
Interactive Network Map
MIB Manager from Empire Technologies
MONET
net_monitor
Netlabs CMOT Agent
Netlabs SNMP Agent
NetMetrix Load Monitor
NetMetrix Protocol Analyzer
NetMetrix Traffic Generator
NETMON by Mitre
NETMON for Windows
NETscout
netstat
netwatch
nfswatch
nhfsstone
NNStat
NOCOL
NPRV
OverVIEW
PacketView
ping
ping from UCB
proxyd from SNMP Research
query
SAS/CPE
SNMP Development Kit
SNMP Libraries and Utilities from SNMP Research
SNMP Packaged Agent System from SNMP Research
PSI SNMP
snmpd from Empire Technologies
snmpd from SNMP Research
PSI SNMP
SpiderMonitor
SPIMS
spray
tcpdump
```

        tcplogger
        traceroute
        trpt
        ttcp
        XNETMON from SNMP Research
        xnetmon from Wellfleet
        xnetperfmon from SNMP Research

        OSI

        CMIP Library
        Dual Manager
        EMANATE
        LANVista
        LANWatch
        Netlabs CMOT Agent
        NetMetrix Protocol Analyzer
        NETMON for Windows
        NETscout
        NOCOL
        ositrace
        proxyd from SNMP Research
        SAS/CPE
        Sniffer
        SNMP Libraries and Utilities from SNMP Research
        SNMP Packaged Agent System from SNMP Research
        snmpd from SNMP Research
        SpiderMonitor
        SPIMS
        XNETMON from SNMP Research
        xnetperfmon from SNMP Research

        NFS
        ---
        etherfind
        EtherView
        iozone
        LADDIS
        NetMetrix NFS Monitor
        NetMetrix Protocol Analyzer
        NETscout
        nfswatch
        nhfsstone
        Sniffer
        tcpdump

```
Ring
----
Eagle
EMANATE
Interactive Network Map
LANVista
LANWatch
NetMetrix Load Monitor
NetMetrix NFS Monitor
NetMetrix Protocol Analyzer
NetMetrix Traffic Generator
NETMON by Mitre
NETMON for Windows
NETscout
netwatch
PacketView
proxyd from SNMP Research
Sniffer
SNMP Libraries and Utilities from SNMP Research
SNMP Packaged Agent System from SNMP Research
snmpd from SNMP Research
TokenVIEW
XNETMON from SNMP Research
xnetperfmon from SNMP Research

SMTP
----
host
Internet Rover
LANWatch
mconnect
NetMetrix Protocol Analyzer
Sniffer
vrfy

Star
----
EMANATE
Interactive Network Map
LAN Patrol
LANWatch
NETMON for Windows
NETscout
proxyd from SNMP Research
Sniffer
SNMP Libraries and Utilities from SNMP Research
SNMP Packaged Agent System from SNMP Research
snmpd from SNMP Research
```

      XNETMON from SNMP Research
      xnetperfmon from SNMP Research

      Curses

      Eagle
      Internet Rover
      net_monitor
      nfswatch
      NOCOL
      PSI SNMP

      Eavesdrop
      ----
      etherfind
      Ethernet Box II
      EtherView
      LAN Patrol
      LANVista
      LANWatch
      ENTM
      NetMetrix Load Monitor
      NetMetrix NFS Monitor
      NetMetrix Protocol Analyzer
      NetNetrix Traffic Generator
      NETMON from Mitre
      NETscout
      netwatch
      nfswatch
      NNStat
      OSITRACE
      PacketView
      Sniffer
      SpiderMonitor
      tcplogger
      trpt

      NMS

      CMU SNMP
      decaddrs from Wellfleet
      Dual Manager
      EMANATE
      EtherMeter
      Ethernet Box II
      getone from Wellfleet
      Interactive Network Map
      MONET

    Netlabs CMOT Agent
    Netlabs SNMP Agent
    NETMON for Windows
    NETscout
    NNStat
    NOCOL
    OverVIEW
    proxyd from SNMP Research
    SNMP Development Kit
    SNMP Libraries and Utilities from SNMP Research
    SNMP Packaged Agent System from SNMP Research
    PSI SNMP
    snmpd from Empire Technologies
    snmpd from SNMP Research
    TokenVIEW
    XNETMON from SNMP Research
    xnetmon from Wellfleet
    xnetperfmon from SNMP Research

    Ping
    ----
    etherhostprobe
    fping
    getethers
    hopcheck
    Interactive Network Map
    Internet Rover
    LANWatch
    net_monitor
    NOCOL
    NPRV
    ping
    ping from UCB
    spray
    traceroute
    ttcp
    XNETMON from SNMP Research
    xup

    Proprietary

    Eagle
    EtherMeter
    Ethernet Box II
    LanProbe
    LANVista
    TokenVIEW

RMON

Beholder

SNMP

Beholder
CMU SNMP
decaddrs from Wellfleet
Dual Manager
EMANATE
getone from Wellfleet
Interactive Network Map
MIB Manager from Empire Technologies
MONET
Netlabs SNMP Agent
NetMetrix Load Monitor
NetMetrix NFS Monitor
NetMetrix Protocol Analyzer
NetMetrix Traffic Generator
NETMON for Windows
NETscout
NOCOL
OverVIEW
proxyd from SNMP Research
SNMP Development Kit
SNMP Libraries and utilities from SNMP Research
SNMP Packaged Agent System from SNMP Research
PSI SNMP
snmpd from Empire Technologies
snmpd from SNMP Research
Wollongong-Manager
XNETMON from SNMP Research
xnetmon from Wellfleet
xnetperfmon from SNMP Research

Spoof

DiG
doc
Internet Rover
host
LADDIS
mconnect
nhfsstone
NOCOL
query
SPIMS

    vrfy

    X
    -
    Dual Manager
    Interactive Network Map
    MIB Manager from Empire Technologies
    NetMetrix Load Monitor
    NetMetrix NFS Monitor
    NetMetrix Protocol Analyzer
    NetMetrix Traffic Generator
    SAS/CPE
    PSI SNMP
    XNETMON from SNMP Research
    xnetperfmon from SNMP Research
    xup

    DEC

    Wollongong-Manager

    DOS

    Computer Security Checklist
    Ethernet Box II
    hammer & anvil
    hopcheck
    iozone
    LAN Patrol
    LANVista
    netmon
    NETMON for Windows
    netwatch
    OverVIEW
    PacketView
    ping
    SAS/CPE
    SNMP Libraries and Utilities from SNMP Research
    SNMP Packaged Agent System from SNMP Research
    snmpd from SNMP Research
    TokenVIEW
    Wollongong-Manager
    xnetperfmon from SNMP Research

   HP
   --
   iozone
   SAS/CPE
   xup

   Macintosh

   HyperMIB

   OS/2

   Beholder
   Tricklet

   Standalone

   LANVista
   Sniffer
   SNMP Packaged Agent System from SNMP Research
   SpiderMonitor

   Sun

   Avatar SunSNMPD
   Wollongong Manager

   UNIX
   ----
   arp
   CMIP Library
   CMU SNMP
   decaddrs from Wellfleet
   DiG
   doc
   dnsstats
   Eagle
   etherfind
   etherhostprobe
   EtherView
   fping
   getethers
   getone from Wellfleet
   host
   Interactive Network Map
   Internet Rover
   iozone
   LADDIS

      lamers
      mconnect
      MIB Manager from Empire Technologies
      MONET
      net_monitor
      Dual Manager
      NetMetrix Load Monitor
      NetMetrix NFS Monitor
      NetMetrix Protocol Analyzer
      NetMetrix Traffic Generator
      NETMON from Mitre
      NETscout
      netstat
      Network Integrator I
      nfswatch
      nhfsstone
      NNStat
      NOCOL
      OSITRACE
      ping
      ping from UCB
      proxyd from SNMP Research
      query
      SAS/CPE
      SNMP Development Kit
      SNMP Libraries and Utilities from Empire Technologies
      SNMP Libraries and Utilities from SNMP Research
      SNMP Packaged Agent System from SNMP Research
      PSI SNMP
      snmpd from Empire Technologies
      snmpd from SNMP Research
      SPIMS
      spray
      tcpdump
      tcplogger
      traceroute
      Tricklet
      trpt
      ttcp
      vrfy
      XNETMON from SNMP Research
      xnetmon from Wellfleet
      xnetperfmon from SNMP Research

      VMS
      ---
      arp
      ENTM

       fping
       net_monitor
       netstat
       NPRV
       ping
       SNMP Libraries and Utilities from SNMP Research
       tcpdump
       traceroute
       ttcp
       xnetperfmon from SNMP Research

       Free
       ----
       arp
       Beholder
       CMIP Library
       CMU SNMP Distribution
       DiG
       dnsstats
       doc
       ENTM
       fping
       getethers
       hammer & anvil
       hopcheck
       host
       Interactive Network Map
       Internet Rover
       iozone
       lamers
       net_monitor
       netmon from Mitre
       netstat
       netwatch
       nfswatch
       nhfsstone
       NNStat
       NOCOL
       NPRV
       OSITRACE
       PING
       ping from UCB
       query
       SNMP Development Kit
       tcpdump
       tcplogger
       traceroute
       Tricklet

      trpt
      ttcp
      vrfy

      Library

      CMIP Library
      CMU SNMP
      Dual Manager
      NetMetrix Protocol Analyzer
      NetMetrix Traffic Generator
      proxyd from SNMP Research
      SAS/CPE

      Sourcelib

      Beholder
      CMIP Library
      CMU SNMP
      EMANATE
      HyperMIB
      Interactive Network Map
      Internet Rover
      LANWatch
      MIB Manager from Empire Technologies
      net_monitor
      NETMON for Windows
      NOCOL
      proxyd from SNMP Research
      SNMP Development Kit
      SNMP Libraries and Utilities from Empire Technologies
      SNMP Libraries and Utilities from SNMP Research
      SNMP Packaged Agent System from SNMP Research
      snmpd from SNMP Research
      SpiderMonitor
      Tricklet
      XNETMON from SNMP Research
      xnetperfmon from SNMP Research

Tool Descriptions

   This section is an updated collection of brief descriptions of tools
   for managing TCP/IP internets. These entries are in alphabetical
   order, by tool name.

   The entries all follow a standard format. Immediately after the NAME
   of a tool are its associated KEYWORDS. Keywords are terse
   descriptions of the purposes or attributes of a tool. A more

detailed description of a tool's purpose and characteristics is given
in the ABSTRACT section. The MECHANISM section describes how a tool
works. In CAVEATS, warnings about tool use are given. In BUGS,
known bugs or bug-report procedures are given. LIMITATIONS describes
the boundaries of a tool's capabilities. HARDWARE REQUIRED and
SOFTWARE REQUIRED relate the operational environment a tool needs.
Finally, in AVAILABILITY, pointers to vendors, online repositories,
or other sources for a tool are given.

Where tool names conflict, the vendor name is used as well. For
example, MITRE, and SNMP Research each submitted an updated
description of a tool called, "NETMON". These tools were
independently developed, are functionally different, and run in
different environments. MITRE's tool is listed as "NETMON_MITRE,"
and the tool from SNMP Research as "NETMON_WINDOWS_SNMP_RESEARCH".

Internet Tool Catalog   ARP

NAME
        arp

KEYWORDS
        routing; ethernet, IP;; UNIX, VMS; free.

ABSTRACT
        Arp displays and can modify the internet-to-ethernet
        address translations tables used by ARP, the address
        resolution protocol.

MECHANISM
        The arp program accesses operating system memory to
        read the ARP data structures.

CAVEATS
        None.

BUGS
        None known.

LIMITATIONS
        Only the super user can modify ARP entries.

HARDWARE REQUIRED
        No restrictions.

SOFTWARE REQUIRED
        BSD UNIX or related OS, or VMS.

AVAILABILITY AND CONTACT POINT FOR INFORMATION ABOUT THIS TOOL

        Available via anonymous FTP from uunet.uu.net, in
        directory bsd-sources/src/etc. Available with 4.xBSD
        UNIX and related operating systems. For VMS, available
        as part of TGV MultiNet IP software package, as well as
        Wollongong's WIN/TCP and Process Software Corporation's
        TCPware for VMS.

CONTACT POINT FOR CHANGES TO THIS CATALOG ENTRY
        This entry maintained by the NOCtools editors.
        Send email to noctools-request@merit.edu.

Internet Tool Catalog   AVATAR-SNMP-TOOLKIT

NAME
     SNMP Application Development Toolkit

KEYWORDS
     manager;;SNMP;;sourcelib.

ABSTRACT
     snmpapi is an api toolkit for developing SNMP
     applications and agents. The toolkit is simple and
     very fast that can be used for any type of
     application. It is very well suited for embedded
     systems such as bridges or routers. An example MIB II
     agent for Sun Sparcstations is provided. snmpapi is
     distributed in source form only.

MECHANISM
     snmpapi is a library of C functions.

CAVEATS
     None.

BUGS
     None known.

LIMITATIONS
     None.

HARDWARE REQUIRED
     No restrictions.

AVAILABILITY
     Available now. For more information, send e-mail to
     info@avatar.com.

Internet Tool Catalog   AVATAR-SUNSNMPD

NAME
     sunsnmpd

KEYWORDS
     manager;;snmp;sun;.

ABSTRACT
     sunsnmpd is a fully supported SNMP agent with MIB II
     support for Sun Sparscations running SunOS 4.1 or
     higher. sunsnmpd supports both SNMP GET and SET
     operations.

MECHANISM
     sundnmpd is a daemon process which starts up at boot
     time from the rc.local file. It uses /dev/kmem to access
     kernel structures.

CAVEATS
     None.

BUGS
     None known.

LIMITATIONS
     Must be started by a super user.

HARDWARE REQUIRED
     Sun Sparcstations.

AVAILABILITY
     Available now. Site licensing only. For more information,
     send e-mail to info@avatar.com.

Internet Tool Catalog   ChameLAN-100

NAME
        ChameLAN 100

KEYWORDS
        analyzer, benchmark, debugger, generator, map,
        reference, status, traffic; bridge, DECnet, ethernet,
        FDDI, IP, OSI, NFS, ring; eavesdrop, SNMP, X;
        standalone, UNIX.

ABSTRACT

        Tekelec's ChameLAN 100 is a portable diagnostic system
        for monitoring and simulation of FDDI, Ethernet and
        Token Ring networks -- simultaneously. Protocol
        analysis of multiple topologies, as well as mixed
        topoloies simultaneously, is a key feature of
        the product family. Tekelec's proprietary FDDI
        hardware guarantees complete real-time analysis of
        networks and network components at the full ring
        bandwidth of 125 Mbps. It passively connects to the
        network and captures 100 percent of the data, measures
        performance and isolates real-time problems.

        The simulation option offers full bandwidth load
        generation that allows you to create and simulate any
        network condition. It gives you the ability to inject
        errors and misformed frames. A set of
        confidence tests allow simple evaluation of new
        equipment. A ring map feature displays network
        topology and status of all nodes via the SMT
        process.

        Monitoring of FDDI, Ethernet and Token Ring allows the
        user to: view network status in real time; view
        network, node, or node pair statistics; capture
        frames; control capture using trigger and filter
        capabilities; view real-time statistics; view captured
        frames in decoded format; and view the last frame
        transmitted by each station.

        The following Real-Time Network Statistics of FDDI,
        Ethernet and Token Ring networks is displayed: frame
        rate, runts, byte rate, jabbers, CRC/align errors, and
        collisions.

        Product developers can use the ChameLAN 100 to observe

and control various events to help debug their FDDI,
Ethernet and Token Ring products. End users can
perform real-time monitoring to test and
diagnose problems that may occur when developing,
installing or managing FDDI, Ethernet and Token Ring
networks and network products. End users can use the
ChameLAN 100 to aid in the installation and
maintenance of Ethernet and Token Ring networks. To
isolate specific network trouble spots the ChameLAN
100 uses filtering and triggering techniques for data
capture. Higher level protocol decode includes
TCP/IP, OSI and DECnet protocol suites. Protocol
decode of IPX, SNMP, XTP, and AppleTalk are also
supported. Development of additional protocol decodes
is also under development. The ChameLAN 100 family
also offers a Protocol Management Development System
(PMDS) that enables users to develop custom protocol
decode suites.

The FDDI, Ethernet and Token Ring hardware interfaces
feature independent processing power. Real-time data
is monitored unobtrusively at full bandwidth without
affecting network activity. Real-time data may also
be saved to a 120MB or optional 200MB hard disk drive
for later analysis. FDDI data is captured at 125 megabits
per second (Mbps), Ethernet at 10 Mbps and Token Ring
at 4 or 16 Mbps.

MECHANISM
        This portable, standalone unit incorporates the power
        of UNIX, X-Windows and Motif. Its UNIX-based
        programming interface facilitates development of
        customized monitoring and simulation applications. The
        ChameLAN 100 may connect to the network at any
        location using standard equipment. Standard graphical
        Motif/X-Windows and TCP/IP allow remote control
        through Ethernet and 10Base T interfaces. Tekelec
        also offers a rackmounted model -- ChameLAN 100-X.
        Both models can be controlled via a Sun Workstation
        remotely.

CAVEATS
        none.

BUGS
        none known.

     LIMITATIONS
          none reported.

     HARDWARE REQUIRED
          None. The ChameLAN 100 is a self-contained unit, and
          includes its own interface cards. It installs
          into a network with standard interface
          connectors.

     SOFTWARE REQUIRED
          None.

     AVAILABILITY AND CONTACT POINT FOR INFORMATION ABOUT THIS TOOL
          The ChameLAN 100 product famil y is available
          commercially. For more information or a free demo,
          call or write:

          1.800.tek.elec
          Tekelec
          26580 West Agoura Road
          Calabasas, CA 91302
          Phone: 818.880.5656
          Fax: 818.880.6993

          The ChameLAN 100 is listed on the GSA schedule.

     CONTACT POINT FOR CHANGES TO THIS CATALOG ENTRY
          Todd Koch
          Public Relations Specialist
          818.880.7718
          Internet: todd.koch@tekelec.com

Internet Tool Catalog   CMU_SNMP

NAME
     The CMU SNMP Distribution

KEYWORDS
     manager, status; IP; NMS, SNMP; UNIX; free, sourcelib.

ABSTRACT
     The CMU SNMP Distribution includes source code for an
     SNMP agent, several SNMP client applications, an ASN.1
     library, and supporting documentation.

     The agent compiles into about 10 KB of 68000 code. The
     distribution includes a full agent that runs on a
     Kinetics FastPath2/3/4, and is built into the KIP
     appletalk/ethernet gateway. The machine independent
     portions of this agent also run on CMU's IBM PC/AT
     based router.

     The applications are designed to be useful in the real
     world. Information is collected and presented in a
     useful format and is suitable for everyday status
     monitoring. Input and output are interpreted
     symbolically. The tools can be used without
     referencing the RFCs.

MECHANISM
     SNMP.

CAVEATS
     None.

BUGS
     None reported. Send bug reports to
     sw0l+snmp@andrew.cmu.edu. ("sw0l" is "ess double-you
     zero ell.")

LIMITATIONS
     None reported.

HARDWARE REQUIRED
     The KIP gateway agent runs on a Kinetics FastPath2/3/4.
     Otherwise, no restrictions.

SOFTWARE REQUIRED
     The code was written with efficiency and portability in
     mind. The applications compile and run on the follow-

ing systems: IBM PC/RT running ACIS Release 3, Sun3/50
running SUNOS 3.5, and the DEC microVax running Ultrix
2.2. They are expected to run on any system with a
Berkeley socket interface.

AVAILABILITY
This distribution is copyrighted by CMU, but may be
used and sold without permission. Consult the copy-
right notices for further information. The distribu-
tion is available by anonymous FTP from the host
lancaster.andrew.cmu.edu (128.2.13.21) as the files
pub/cmu-snmp.9.tar, and pub/kip-snmp.9.tar. The former
includes the libraries and the applications, and the
latter is the KIP SNMP agent.

Please direct questions, comments, and bug reports to
sw0l+snmp@andrew.cmu.edu. ("sw0l" is "ess double-you
zero ell.") If you pick up this package, please send a
note to the above address, so that you may be notified
of future enhancements/changes and additions to the set
of applications (several are planned).

Internet Tool Catalog   COMPUTER-SECURITY-CHECKLIST

NAME
     Computer Security Checklist

KEYWORDS
     security; DOS.

ABSTRACT
     This program consists of 858 computer security ques-
     tions divided up in thirteen sections. The program
     presents the questions to the user and records their
     responses. After answering the questions in one of the
     thirteen sections, the user can generate a report from
     the questions and the user's answers. The thirteen
     sections are: telecommunications security, physical
     access security, personnel security, systems develop-
     ment security, security awareness and training prac-
     tices, organizational and management security, data and
     program security, processing and operations security,
     ergonomics and error prevention, environmental secu-
     rity, and backup and recovery security.

     The questions are weighted as to their importance, and
     the report generator can sort the questions by weight.
     This way the most important issues can be tackled
     first.

MECHANISM
     The questions are displayed on the screen and the user
     is prompted for a single keystroke reply. When the end
     of one of the thirteen sections is reached, the answers
     are written to a disk file. The question file and the
     answer file are merged to create the report file.

CAVEATS
     None.

BUGS
     None known.

LIMITATIONS
     None reported.

HARDWARE REQUIRED
     No restrictions.

SOFTWARE REQUIRED
     DOS operating system.

AVAILABILITY
     A commercial product available from:
          C.D., Ltd.
          P.O. Box 58363
          Seattle, WA 98138
          (206) 243-8700

Internet Tool Catalog   CMIP-LIBRARY

NAME
        CMIP Library

KEYWORDS
        manager; osi; cmis; unix; free, sourcelib.

ABSTRACT

        The CMIP Library implements the functionality of the
        Common Management Information Service/Protocol as in
        the full international standards (ISO 9595, ISO 9596)
        published in 1990. It is designed to work with the
        ISODE package and can act as a building block for the
        construction of CMIP-based agent and manager
        applications.

MECHANISM
        The CMIP library uses ISO ROS, ACSE and ASN.1
        presentation, as implemented in ISODE, to provide its
        service.

CAVEATS
        None.

BUGS
        None known.

LIMITATIONS
        None known.

HARDWARE REQUIRED
        Has been tested on SUN 3 and SUN 4 architectures.

SOFTWARE REQUIRED
        The ISODE protocol suite, BSD UNIX.

AVAILABILITY
        The CMIP library and related management tools built
        upon it, known as OSIMIS (OSI Management Information
        Service), are publicly available from University
        College London, England via FTP and FTAM. To obtain
        information regarding a copy send email to
        osimis-request@cs.ucl.ac.uk or call +44 71 380 7366.

Internet Tool Catalog   DECADDRS

NAME
     decaddrs, decaroute, decnroute, xnsroutes, bridgetab

KEYWORDS
     manager, map, routing; bridge, DECnet; NMS, SNMP; UNIX.

ABSTRACT
     These commands display private MIB information from
     Wellfleet systems. They retrieve and format for
     display values of one or several MIB variables from the
     Wellfleet Communications private enterprise MIB, using
     the SNMP (RFC1098). In particular these tools are used
     to examine the non-IP modules (DECnet, XNS, and Bridg-
     ing) of a Wellfleet system.

     Decaddrs displays the DECnet configuration of a
     Wellfleet system acting as a DECnet router, showing the
     static parameters associated with each DECnet inter-
     face. Decaroute and decnroute display the DECnet
     inter-area and intra-area routing tables (that is area
     routes and node routes). Xnsroutes displays routes
     known to a Wellfleet system acting as an XNS router.
     Bridgetab displays the bridge forwarding table with the
     disposition of traffic arriving from or directed to
     each station known to the Wellfleet bridge module. All
     these commands take an IP address as the argument and
     can specify an SNMP community for the retrieval. One
     SNMP query is performed for each row of the table.
     Note that the Wellfleet system must be operating as an
     IP router for the SNMP to be accessible.

MECHANISM
     Management information is exchanged by use of SNMP.

CAVEATS
     None.

BUGS
     None known.

LIMITATIONS
     None reported.

HARDWARE REQUIRED
     Distributed and supported for Sun 3 systems.

         SOFTWARE REQUIRED
              Distributed and supported for SunOS 3.5 and 4.x.

         AVAILABILITY
              Commercial product of:
                   Wellfleet Communications, Inc.
                   12 DeAngelo Drive
                   Bedford, MA 01730-2204
                   (617) 275-2400

Internet Tool Catalog   DIG

NAME
     DiG

KEYWORDS
     status; DNS; spoof; UNIX; free.

ABSTRACT
     DiG (domain information groper), is a command line tool
     which queries DNS servers in either an interactive or a
     batch mode. It was developed to be more
     convenient/flexible than nslookup for gathering perfor-
     mance data and testing DNS servers.

MECHANISM
     Dig is built on a slightly modified version of the bind
     resolver (release 4.8).

CAVEATS
     none.

BUGS
     None known.

LIMITATIONS
     None reported.

HARDWARE REQUIRED
     No restrictions.

SOFTWARE REQUIRED
     BSD UNIX.

AVAILABILITY
     DiG is available via anonymous FTP from venera.isi.edu
     in pub/dig.2.0.tar.Z.

Internet Tool Catalog   EMANATE_SNMP_RESEARCH

NAME
        EMANATE: Enhanced MANagement Agent Through Extensions
        from SNMP Research.

KEYWORDS
        alarm, control, manager, reference, security, status;
        bridge, Ethernet, FDDI, IP, OSI, ring, star;
        NMS, SNMP;
        sourcelib.

ABSTRACT
        The EMANATE system provides a run-time extensible SNMP
        agent that dynamically reconfigures an agent's MIB
        without having to recompile, relink, or restart the
        agent. An EMANATE capable SNMP agent can support zero,
        one, or many subagents and dynamically reconfigure to
        connect or disconnect those subagents' MIBs.

        The EMANATE system consists of several logically
        independent components and subsystems:

        o Master SNMP agent which contains an API to communicate
          with subagents.
        o Subagents which implement various MIBS.
        o Subagent Developer's Kit which contains tools to assist
          in the implementation of subagents.
        o EMANATE libraries which provide the API for the
          subagent.

MECHANISM
        A concise API allows a standard means of communication
        between the master and subagents. System dependent
        mechanisms are employed for transfer of information
        between the master and subagents.

CAVEATS
        None.

BUGS
        None known.

LIMITATIONS
        None reported.

HARDWARE REQUIRED
        Multiple platforms including PC's, workstations, hosts,
        and servers are supported. Contact SNMP Research for
        more details.

SOFTWARE REQUIRED
        C compiler.

AVAILABILITY AND CONTACT POINT FOR INFORMATION ABOUT THIS TOOL
        This is a commercial product available under license
        from:

        SNMP Research
        3001 Kimberlin Heights Road
        Knoxville, TN 37920-9716
        Attn: John Southwood, Sales and Marketing
        (615) 573-1434 (Voice) (615) 573-9197 (FAX)

CONTACT POINT FOR CHANGES TO THIS CATALOG ENTRY
        users@seymour1.cs.utk.edu

Internet Tool Catalog   ETHERFIND_SUN

NAME
     etherfind

KEYWORDS
     traffic; ethernet, IP, NFS; eavesdrop; UNIX.

ABSTRACT
     Etherfind examines the packets that traverse a network
     interface, and outputs a text file describing the
     traffic. In the file, a single line of text describes
     a single packet: it contains values such as protocol
     type, length, source, and destination. Etherfind can
     print out all packet traffic on the ethernet, or
     traffic for the local host. Further packet filtering
     can be done on the basis of protocol: IP, ARP, RARP,
     ICMP, UDP, ND, TCP, and filtering can also be done
     based on the source, destination addresses as well as
     TCP and UDP port numbers.

MECHANISM
     In usual operations, and by default, etherfind puts the
     interface in promiscuous mode. In 4.3BSD UNIX and
     related OSs, it uses a Network Interface Tap (NIT) to
     obtain a copy of traffic on an ethernet interface.

CAVEATS
     None.

BUGS
     None known.

LIMITATIONS
     Minimal protocol information is printed. Can only be
     run by the super user. The syntax is painful.

HARDWARE REQUIRED
     Ethernet.

SOFTWARE REQUIRED
     SunOS.

AVAILABILITY
     Executable included in Sun OS "Networking Tools and
     Programs" software installation option.

              Internet Tool Catalog   ETHERNET-CODES

         NAME
                 ethernet-codes

         KEYWORDS
                 reference;
                 ethernet, fddi;
                 ;
                 ;
                 ;

         ABSTRACT
                 Mike Patton of MIT LCS has compiled a very
                 comprehensive list of the IEEE numbers used on
                 Ethernet and FDDI (with some permutation).
                 This file contains collected information on the
                 various codes used on IEEE 802.3 and EtherNet.
                 There are three "pages": type codes, vendor
                 codes, and the uses of multicast (including
                 broadcast) addresses.

         MECHANISM
                 FTP the file and use it like a secret decoder ring.

         CAVEATS
                 Since this information is from collected wisdom,
                 there are certainly omissions.

         BUGS
                 Mike welcomes any further additions.
                 They can be sent to a special mailbox that he has set up:

                         MAP=EtherNet-codes@LCS.MIT.Edu

         LIMITATIONS
                 See caveats.

         HARDWARE REQUIRED
                 No restrictions.

         SOFTWARE REQUIRED
                 No restrictions.

         AVAILABILITY AND CONTACT POINT FOR INFORMATION ABOUT THIS TOOL
                 The file is stored as flat, non-compressed ASCII text.
                 It can be FTP'ed from:
                         ftp.lcs.mit.edu

                 Retreive the file:
                         /pub/map/EtherNet-codes

         To submit additions or obtain further assistance, send email to:
                     MAP=EtherNet-codes@LCS.MIT.Edu

         CONTACT POINT FOR CHANGES TO THIS CATALOG ENTRY
                 This entry maintained by the NOCtools editors.
                 Send email to noctools-request@merit.edu

Internet Tool Catalog   GENERIC-MANAGED-SYSTEM

NAME
        Generic Managed System

KEYWORDS
        manager; osi; cmis; unix; free, sourcelib

ABSTRACT
        The Generic Managed System (GMS) implements the
        functions that would be common to any OSI managed
        system. These include the parseing of CMIS requests,
        selection of managed objects according to the scoping
        and filtering rules, handling of notifications and
        event forwarding discriminators etc. The intention is
        that the implementors should use the GMS as a basis
        for their own managed object implementations. A
        support environment is provided to assist with this.

MECHANISM
        The GMS uses the UCL CMIP library plus a library of
        C++ objects representing common managed objects and
        attribute types.

CAVEATS
        The system is still experimental, is subject to change
        and is not yet well documented.

BUGS
        See above.

LIMITATIONS
        None known.

HARDWARE REQUIRED
        Has been tested on SUN 3 and SUN 4 architectures.

SOFTWARE REQUIRED
        The ISODE protocol suite, BSD UNIX, UCL CMIP Library,
        GNU C++ (g++).

AVAILABILITY
        The CMIP library and related management tools built
        upon it, known as OSIMIS (OSI Management Information
        Service), are publicly available from University
        College London, England via FTP and FTAM. To obtain
        information regarding a copy send email to
        osimis-request@cs.ucl.ac.uk or call +44 71 380 7366.

Internet Tool Catalog   GETETHERS

NAME
        getethers

KEYWORDS
        Traffic; Ethernet; Ping; UNIX; Free

ABSTRACT
        Getethers runs through all addresses on an ethernet
        segment (a.b.c.1 to a.b.c.254) and pings each address,
        and then determines the ethernet address for that
        host. It produces a list, in either plain ASCII, the
        file format for the Excelan Lanalyzer, or the file
        format for the Network General Sniffer, of
        hostname/ethernet address pairs for all hosts on the
        local nework. The plain ASCII list optionally
        includes the vendor name of the ethernet card in
        each system, to aid in the determination of the
        identity of unknown systems.

MECHANISM
        Getethers uses a raw IP socket to generate ICMP echo
        requests and receive ICMP echo replies, and then
        examines the kernel ARP table to determine the
        ethernet address of each responding system.

CAVEATS
        Assumes that the ethernet it is looking at is either
        a Class C IP network, or part of a Class B IP network
        that is subnetted with a netmask of 255.255.255.0.
        (This is easy to change, but it's compiled in.)

BUGS
        None known.

LIMITATIONS
        None.

HARDWARE REQUIRED
        Has been tested on Sun-3 and Sun-4 (SPARC) systems
        under SunOS 4.1.x, DEC VAXes under 4.3BSD.

SOFTWARE REQUIRED
        Runs under SunOS 4.x and 4.3BSD; should be easy to
        port to any other Berkeley-like system. Requires
        raw sockets and the ioctl calls to get at the ARP
        table.

        AVAILABILITY AND CONTACT POINT FOR INFORMATION ABOUT THIS TOOL
                Public domain, and freely distributable. Available
                via anonymous FTP from harbor.ecn.purdue.edu; also has
                been posted to comp.sources.unix. The current version
                is Version 1.4 from May 1992.

                Contact point:
                        Dave Curry
                        Purdue University
                        Engineering Computer Network
                        1285 Electrical Engineering Bldg.
                        West Lafayette, IN 47907-1285
                        davy@ecn.purdue.edu

        CONTACT POINT FOR CHANGES TO THIS CATALOG ENTRY
                        Dave Curry (see address above).

Internet Tool Catalog   GETONE_WELLFLEET

NAME
     getone, getmany, getroute, getarp, getaddr, getif,
     getid.

KEYWORDS
     manager, routing, status; IP; NMS, SNMP; UNIX.

ABSTRACT
     These commands retrieve and format for display values
     of one or several MIB variables (RFC1066) using the
     SNMP (RFC1098). Getone and getmany retrieve arbitrary
     MIB variables; getroute, getarp, getaddr, and getif
     retrieve and display tabular information (routing
     tables, ARP table, interface configuration, etc.), and
     getid retrieves and displays system name, identifica-
     tion and boot time.

     Getone <target> <mibvariable> retrieves and displays
     the value of the designated MIB variable from the
     specified target system. The SNMP community name to be
     used for the retrieval can also be specified. Getmany
     works similarly for groups of MIB variables rather than
     individual values. The name of each variable, its
     value and its data type is displayed. Getroute returns
     information from the ipRoutingTable MIB structure,
     displaying the retrieved information in an accessible
     format. Getarp behaves similarly for the address
     translation table; getaddr for the ipAddressTable; and
     getif displays information from the interfaces table,
     supplemented with information from the ipAddressTable.
     Getid displays the system name, identification, ipFor-
     warding state, and the boot time and date. All take a
     system name or IP address as an argument and can
     specify an SNMP community for the retrieval. One SNMP
     query is performed for each row of the table.

MECHANISM
     Queries SNMP agent(s).

CAVEATS
     None.

BUGS
     None known.

          LIMITATIONS
               None reported.

          HARDWARE REQUIRED
               Distributed and supported for Sun 3 systems.

          SOFTWARE REQUIRED
               Distributed and supported for SunOS 3.5 and 4.x.

          AVAILABILITY
               Commercial product of:
                    Wellfleet Communications, Inc.
                    12 DeAngelo Drive
                    Bedford, MA 01730-2204
                    (617) 275-2400

Internet Tool Catalog   HAMMER_ANVIL

NAME
     hammer & anvil

KEYWORDS
     benchmark, generator; IP; DOS; free.

ABSTRACT
     Hammer and Anvil are the benchmarking programs for IP
     routers. Using these tools, gateways have been tested
     for per-packet delay, router-generated traffic over-
     head, maximum sustained throughput, etc.

MECHANISM
     Tests are performed on a gateway in an isolated
     testbed. Hammer generates packets at controlled rates.
     It can set the length and interpacket interval of a
     packet stream. Anvil counts packet arrivals.

CAVEATS
     Hammer should not be run on a live network.

BUGS
     None reported.

LIMITATIONS
     Early versions of hammer could not produce inter-packet
     intervals shorter than 55 usec.

HARDWARE REQUIRED
     Hammer runs on a PC/AT or compatible, and anvil
     requires a PC or clone. Both use a Micom Interlan
     NI5210 for LAN interface.

SOFTWARE REQUIRED
     MS-DOS.

AVAILABILITY
     Hammer and anvil are copyrighted, though free. Copies
     are available from pub/eutil on husc6.harvard.edu.

Internet Tool Catalog   HOPCHECK

NAME
     hopcheck

KEYWORDS
     routing; IP; ping; DOS; free.

ABSTRACT
     Hopcheck is a tool that lists the gateways traversed by
     packets sent from the hopcheck-resident PC to a desti-
     nation. Hopcheck uses the same mechanism as traceroute
     but is for use on IBM PC compatibles that have ethernet
     connections. Hopcheck is part of a larger TCP/IP pack-
     age that is known as ka9q that is for use with packet
     radio. Ka9q can coexist on a PC with other TCP/IP
     packages such as FTP Inc's PC/TCP, but must be used
     independently of other packages. Ka9q was written by
     Phil Karn. Hopcheck was added by Katie Stevens,
     dkstevens@ucdavis.edu. Unlike traceroute, which
     requires a UNIX kernel mod, hopcheck will run on the
     standard, unmodified ka9q release.

MECHANISM
     See the description in traceroute.

CAVEATS
     See the description in traceroute.

BUGS
     None known.

HARDWARE REQUIRED
     IBM PC compatible with ethernet network interface card;
     ethernet card supported through FTP spec packet driver.

SOFTWARE REQUIRED
     DOS.

AVAILABILITY
     Free for radio amateurs and educational institutions;
     others should contact Phil Karn, karn@ka9q.bellcore.com.
     Available via anonymous FTP at ucdavis.edu, in the
     directory "dist/nethop".

Internet Tool Catalog   INTERNET_ROVER

NAME
     Internet Rover

KEYWORDS
     status; IP, SMTP; curses, ping, spoof; UNIX; free,
     sourcelib.

ABSTRACT
     Internet Rover is a prototype network monitor that uses
     multiple protocol "modules" to test network functional-
     ity. This package consists of two primary pieces of
     code: the data collector and the problem display.

     There is one data collector that performs a series of
     network tests, and maintains a list of problems with
     the network. There can be many display processes all
     displaying the current list of problems which is useful
     in a multi-operator NOC.

     The display task uses curses, allowing many terminal
     types to display the problem file either locally or
     from a remote site. Full source is provided. The data
     collector is easily configured and extensible. Contri-
     butions such as additional protocol modules, and shell
     script extensions are welcome.

MECHANISM
     A configuration file contains a list of nodes,
     addresses, NodeUp? protocol test (ping in most cases),
     and a list of further tests to be performed if the node
     is in fact up. Modules are included to test TELNET,
     FTP, and SMTP. If the configuration contains a test
     that isn't recognized, a generic test is assumed, and a
     filename is checked for existence. This way users can
     create scripts that create a file if there is a prob-
     lem, and the data collector simply checks the existence
     of that file to determine if there is problem.

CAVEATS
     None.

BUGS
     None known.

LIMITATIONS
     This tool does not yet have the capability to perform
     actions based on the result of the test. Rather, it is
     intended for a multi-operator environment, and simply
     displays a list of what is wrong with the net.

HARDWARE REQUIRED
     This software is known to run on Suns and IBM RTs.

SOFTWARE REQUIRED
     Curses, 4.xBSD UNIX socket programming libraries, BSD
     ping.

AVAILABILITY
     Full source available via anonymous FTP from merit.edu
     (35.1.1.42) in the ~ftp/pub/inetrover directory.
     Source and executables are public domain and can be
     freely distributed for non-commercial use. This pack-
     age is unsupported, but bug reports and fixes may be
     sent to: wbn@merit.edu.

Internet Tool Catalog   IOZONE

NAME
        iozone

KEYWORDS
        benchmark; nfs;; dos,hp,unix,vmx; free.

ABSTRACT
        Software to assess the sequential file I/O capability
        of a system. May be useful as reference to compare
        against results obtained when files are accessed via
        NFS, Andrew, etc.

MECHANISM
        This test writes a X MEGABYTE sequential file in Y
        byte chunks, then rewinds it and reads it back.
        [The size of the file should be big enough to factor
        out the effect of any disk cache.]. Finally,
        IOZONE deletes the temporary file. Options allow one to
        vary X and Y. In addition, 'auto test' runs IOZONE
        repeatedly using record sizes from 512 to 8192 bytes
        (adjustable), and file sizes from 1 to 16 megabytes
        (adjustable). It creates a table of results.

CAVEATS
        The file is written (filling any cache buffers), and
        then read. If the cache is >= X MB, then most if not
        all the reads will be satisfied from the cache.
        However, if it is less than or equal to
        .5X MB, then NONE of the reads will be satisfied from
        the cache. This is becase after the file is written,
        a .5X MB cache will contain the upper .5 MB of the
        test file, but we will start reading
        from the beginning of the file (data which is no
        longer in the cache).

        In order for this to be a fair test, the length of the
        test file must be AT LEAST 2X the amount of disk cache
        memory for your system. If not, you are really
        testing the speed at which your CPU
        can read blocks out of the cache (not a fair test).

BUGS
        none known at this time.

        LIMITATIONS
                IOZONE does not normally test the raw I/O speed of
                your disk or system-em. It tests the speed of
                sequential I/O to actual files.
                Therefore, this measurement factors in the efficiency
                of you machines file system, operating system, C
                compiler, and C runtime library. It produces a
                measurement which is the number of bytes
                per second that your system can read or write to a file.

        HARDWARE REQUIRED

                This program has been ported and tested on the
                following computer operating systems:

```
Vendor             Operating System    Notes on compiling IOzone
---------------------------------------------------------------------
Apollo             Domain/OS           no cc switches -- BSD domain
AT&T               UNIX System V R4
AT&T 6386WGS       AT&T UNIX 5.3.2     define SYSTYPE_SYSV
Generic AT&T       UNIX System V R3    may need cc -DSVR3
Convergent         Unisys/AT&T SVR3    cc -DCONVERGENT -o iozone iozone.c
Digital Equipment  ULTRIX V4.1
Digital Equipment  VAX/VMS V5.4        see below **
Digital Equipment  VAX/VMS (POSIX)
Hewlett-Packard    HP-UX 7.05
IBM                AIX Ver. 3 rel. 1
Interactive        UNIX System V R3
Microsoft          MS-DOS 3.3          tested Borland, Microsoft C
MIPS               RISCos 4.52
NeXt               NeXt OS 2.x
OSF                OSF/1
Portable!          POSIX 1003.1-1988   may need to define _POSIX_SOURCE
QNX                QNX 4.0
SCO                UNIX System V/386 3.2.2
SCO                XENIX 2.3
SCO                XENIX 3.2
Silicon Graphics   UNIX                cc -DSGI -o iozone iozone.c
Sony Microsystems  UNIX                same as MIPS
Sun Microsystems   SUNOS 4.1.1
Tandem Computers   GUARDIAN 90          1. call the source file IOZONEC
                                        2. C/IN IOZONEC/IOZONE;RUNNABLE
                                        3. RUN IOZONE
Tandem Computers   Non-Stop UX
```

** for VMS, define iozone as a foreign command via this DCL command:

        $IOZONE :== SYSDISK:[]IOZONE.EXE

          this lets you pass the command line arguments to IOZONE

     SOFTWARE REQUIRED
          OS as shown in the hardware listing above.

     AVAILABILITY AND CONTACT POINT FOR INFORMATION ABOUT THIS TOOL
          Author: Bill Norcott
                  1060 Hyde Avenue
                  San Jose, CA 95129
                  norcott_bill@tandem.com

          Availability:
                  This tool has been posted to comp.sources.misc.
                  It is available from the usual archive sites.
                  Program can be located using ARCHIE or other
                  servers.

     CONTACT POINT FOR CHANGES TO THIS CATALOG ENTRY
          This entry is maintained by the noctools editors.
          Send email to noctools-request@merit.edu.

Internet Tool Catalog   LADDIS

NAME
        LADDIS

KEYWORDS
        benchmark, generator;
        NFS;
        spoof;
        unix;
        free.

ABSTRACT

        "LADDIS: A Multi-Vendor and Vendor-Neutral SPEC NFS
        Benchmark", Bruce Nelson, LADDIS Group & Auspex Systems.

        Over the past 24 months, engineers from Legato,
        Auspex, Data General, DEC, Interphase, and Sun
        (LADDIS) met regularly to create the LADDIS NFS
        benchmark: an unbiased, standard, vendor-independent,
        scalable NFS performance test.

        The purpose of the LADDIS benchmark is to give users a
        credible and undisputed test of NFS performance, and
        to give vendors a publishable standard performance
        measure that customers can use for load planning,
        system configuration, and equipment buying decisions.
        Toward this end, the LADDIS benchmark is being adopted
        by SPEC (the System Performance Evaluation
        Cooperative, creators of SPECmarks) as the first
        member of SPEC's System-level File Server (SFS)
        benchmark suite."

        "In particular, we have had unexpected interest from
        some router vendors in using LADDIS to both rate and
        stress-test IP routers. This is because LADDIS can
        send back-to-back full-size packet trains, and because
        it can generate a 90%-Ethernet util on simulated
        "real" NFS workloads, just like routers encounter in
        the real world. But LADDIS is for local Ethernet or
        FDDI nets only, not WAN."

MECHANISM
        Generates NFS requests and measures responsiveness of
        the server.

CAVEATS
        "LADDIS is not released yet by SPEC, although a free
        beta version, quite stable, is available now as
        PRE-LADDIS. So you might want to put PRE-LADDIS in
        your listing, noting that full LADDIS
        availability from SPEC is expected by the end of 1992."

BUGS
        The licensee is requested to direct beta test comments
        via electronicmail to:
        "spec-preladdis-comments@riscee.pko.dec.com".

        This alias will forward all comments to the SPECSFS
        mailing list (which includes the LADDIS Group).

LIMITATIONS
        LADDIS is for local Ethernet or FDDI nets only, not
        WAN.

HARDWAE REQUIRED
        A host with LAN connectivity. Presumably, a host with
        enough horsepower to generate an adequate work load.

SOFTWARE REQUIRED
        LADDIS is a sophisticated Unix-based NFS traffic
        generator program.

AVAILABILITY AND CONTACT POINT FOR INFORMATION ABOUT THIS TOOL
        Date: Mon, 10 Feb 92 13:12:20 PST
        From: bnelson (Bruce Nelson)

        Dear Person:

        The SPEC PRE-LADDIS beta test process became
        operational on Monday, February 3, 1992. This email
        describes the process as announced during the LADDIS
        Group's presentation at UniForum '92 and
        also at Interop '91. The content of the beta test
        license and the license request process are consistent
        with the proposals approved by the SPEC Steering
        Committee at the January 1992 meeting in Milpitas,
        California.

        The SPEC PRE-LADDIS beta test will consist of one beta
        test version of PRE-LADDIS distributed ONLY by
        electronic mail. The SPEC PRE-LADDIS Beta test
        software is licensed by SPEC, not by the LADDIS
        Group.

                    To obtain the PRE-LADDIS Beta test software, an
                    individual must:

                    1. Request the SPEC PRE-LADDIS beta test License by
                        electronic mail to
                        "spec-preladdis-beta-test@riscee.pko.dec.com" with a
                        subject line of "Request SPEC PRE-LADDIS Beta Test
                        License".
                    2. Print a hardcopy of the license and sign.
                    3. Attach a cover letter written on the individual's
                        company letterhead requesting the PRE-LADDIS Beta
                        Test Kit.
                    4. U.S. Mail the signed license and cover letter to:
                            SPEC PRE-LADDIS Beta Test
                            c/o NCGA, 2722 Merrilee Drive, Suite 200
                            Fairfax, VA 22031

                    After completing these steps, the SPEC PRE-LADDIS beta
                    test kit will be emailed to the requestor from
                    riscee.pko.dec.com. The licensee is requested to
                    direct beta test comments via electronic mail
                    to "spec-preladdis-comments@riscee.pko.dec.com". This
                    alias will forward all comments to the SPECSFS mailing
                    list (which includes the
                    LADDIS Group).

                    Note that PRE-LADDIS is ONLY available through
                    electronic mail and ONLY through the process listed
                    above in steps 1-4. If you do not have internet email
                    available to you (which is unlikely if you are
                    receiving THIS email), you must arrange delivery of
                    PRE-LADDIS through some email-capable part of your
                    organization, not through LADDIS members like Auspex,
                    DEC, Sun, etc.

              CONTACT POINT FOR CHANGES TO THIS CATALOG ENTRY
                    This entry is maintained by the NOCtools editors.
                    Send E-mail to noctools-request@merit.edu.

Internet Tool Catalog   LAN_PATROL

NAME
     LAN Patrol

KEYWORDS
     security, traffic; ethernet, star; eavesdrop; DOS.

ABSTRACT
     LAN Patrol is a full-featured network analyzer that
     provides essential information for effective fault and
     performance management. It allows network managers to
     easily monitor user activity, find traffic overloads,
     plan for growth, test cable, uncover intruders, balance
     network services, and so on. LAN Patrol uses state of
     the art data collection techniques to monitor all
     activity on a network, giving an accurate picture of
     how it is performing.

     LAN Patrol's reports can be saved as ASCII files to
     disk, and imported into spreadsheet or database pro-
     grams for further analysis.

MECHANISM
     The LAN Patrol interface driver programs a standard
     interface card to capture all traffic on a network seg-
     ment. The driver operates from the background of a
     standard PC, maintaining statistics for each station on
     the network. The information can be viewed on the PC's
     screen, or as a user-defined report output either to
     file or printer.

CAVEATS
     None. Normal operation is completely passive, making
     LAN Patrol transparent to the network.

BUGS
     None known.

LIMITATIONS
     LAN Patrol can monitor up to 10,000 packets/sec on an
     AT class PC, and is limited to monitoring a maximum of
     1024 stations for intervals of up to 30 days.

     Because LAN Patrol operates at the physical level, it
     will only see traffic for the segment on which it is
     installed; it cannot see traffic across bridges.

HARDWARE REQUIRED
     Computer: IBM PC/XT/AT, PS/2 Model 30, or compatible.
     Requires 512K memory and a hard drive or double-sided
     disk drive.

     Display: Color or monochrome text. Color display
     allows color-coding of traffic information.

     Ethernet, StarLAN, LattisNet, or StarLAN 10 network
     interface card.

SOFTWARE REQUIRED
     PC DOS, MS-DOS version 3.1 or greater.

AVAILABILITY
     LAN Patrol many be purchased through network dealers,
     or directly from:
          Legend Software, Inc.
          Phone: (201) 227-8771
          FAX: (201) 906-1151

Internet Tool Catalog   LANVista

NAME
     LANVista

KEYWORDS
     analyzer, benchmark, debugger, generator, manager, traffic;
     DECnet, Ethernet, IP, OSI, Ring; Eavesdrop, Proprietary;
     DOS, Standalone.

ABSTRACT
     CXR/Digilog's LANVista family of protocol and statistical
     analyzers provide the tools to troubleshoot an Ethernet and
     Token Ring 4/16Mbps network. LANVista lets you capture
     frames to RAM and or disk, generate traffic for stress
     testing, test your network cable for fault isolation, and
     decode all 7 layers of many popular protocol stacks.
     LANVista's 100 family offers exceptional price/performance
     and a wide range of options. Combined with an
     integrated upgrade path to the fully distributed LANVista
     200 system, the 100 line provides a reasonably priced
     entry into LAN management and protocol analysis.

     All LANVista models are fully operable under Microsoft
     Windows. Under Windows, LANVista can be operated in
     the background, gathering data and alarms as other
     tasks are completed. Displayed data may easily be
     cut from LANVista and pasted into other Windows
     applications such as Excel, Lotus 1-2-3, Harvard
     Graphics, etc.

     The versatile LANVista family can also be remotely
     controlled through the use of PC Anywhere, Commute,
     Carbon Copy, or other PC remote control packages.
     This feature allows the use of "co-pilot" mode which
     enables an operator at the central site to guide and
     train a remote operator through network management or
     analysis tasks.

     All LANVista models provide features vital to effective
     network management and troubleshooting. Basic
     capabilities include: Network database, statistics
     based on the entire network and on a node basis, Token
     Ring functional address statistics, Bridged traffic
     statistics, Protocol statistics, logging of statistics
     to a printer or file of user definable alarms, Hardware
     Pre-Capture filtering, Post capture filtering, Playback of
     captured data, Traffic simulation and On-line context

sensitive Help.

Protocol Interpreters used for decoding network traffic
supported by LANVista include: TCP/IP, DECnet, Banyan
Vines, XNS/MS-Net, AppleTalk, IBM Token Ring, Novell,
3Com 3+ Open, SNMP and OSI.

MECHANISM
    LANVista is available in three forms. A kit version which
    consists of a plug-in PC card and Master software, a self
    contained unit that packages the kit version in a portable
    PC, and a Distributed system. The LANVista distributed
    system allows slave units placed anywhere in the world to
    be controlled from a single central location for
    centralized management of an enterprise network.
    LANVista's PC cards provides a physical interface to
    the LAN and frame preprocessing power. The Master
    software controls the PC card, and the display and
    processing of information gathered from the network.

CAVEATS
    Optimal performance of LANVista's master software is achieved
    with DOS 5.0 by utilizing RAMDRIVE.SYS, SMARTDRV.SYS and High
    memory.

BUGS
    None Known.

LIMITATIONS
    None Known.

HARDWARE REQUIRED
    IBM PC AT, 386, 486 or compatible.

SOFTWARE REQUIRED
    DOS

AVAILABILITY AND CONTACT POINT FOR INFORMATION ABOUT THIS TOOL
    LANVista is available worldwide. For information on a
    local sales representative contact:

        CXR/DIGILOG
        900 Business Center Drive
        Horsham, PA 19044
        Phone 1-800-DIGILOG
        FAX: 215-956-0108

    GSA schedule pricing is honored.

          CONTACT POINT FOR CHANGES TO THIS CATALOG ENTRY
             CXR/DIGILOG Help Desk 1-800-DIGILOG
             Send email to: lanvista@digilog.uucp

Internet Tool Catalog   LANPROBE

NAME
     LanProbe -- the HP 4990S LanProbe Distributed Analysis
     System.

KEYWORDS
     alarm, manager, map, status, traffic; ethernet; eaves-
     drop, NMS; proprietary.

ABSTRACT
     The LanProbe distributed monitoring system performs
     remote and local monitoring of ethernet LANs in a pro-
     tocol and vendor independent manner.

     LanProbe discovers each active node on a segment and
     displays it on a map with its adapter card vendor name,
     ethernet address, and IP address. Additional informa-
     tion about the nodes, such as equipment type and physi-
     cal location can be entered in to the data base by the
     user.

     When the NodeLocator option is used, data on the actual
     location of nodes is automatically entered and the map
     becomes an accurate representation of the physical lay-
     out of the segment. Thereafter when a new node is
     installed and becomes active, or when a node is moved
     or becomes inactive, the change is detected and shown
     on the map in real time. The system also provides the
     network manager with precise cable fault information
     displayed on the map.

     Traffic statistics are gathered and displayed and can
     be exported in (comma delimited) CSV format for further
     analysis. Alerts can be set on user defined thres-
     holds.

     Trace provides a remote protocol analyzer capability
     with decodes for common protocols.

     Significant events (like power failure, cable breaks,
     new node on network, broadcast IP source address seen,
     etc.) are tracked in a log that is uploaded to Pro-
     beView periodically.

     ProbeView generates reports that can be manipulated by
     MSDOS based word processors, spreadsheets, and DBMS.

MECHANISM
        The system consists of one or more LanProbe segment
        monitors and ProbeView software running under Microsoft
        Windows. The LanProbe segment monitor attaches to the
        end of an ethernet segment and monitors all traffic.
        Attachment can be direct to a thin or thick coax cable,
        or via an external transceiver to fiber optic or twist-
        ed pair cabling. Network data relating to the segment
        is transferred to a workstation running ProbeView via
        RS-232, ethernet, or a modem connection.

        ProbeView software, which runs on a PC/AT class works-
        tation, presents network information in graphical
        displays.

        The HP4992A NodeLocator option attaches to the opposite
        end of the cable from the HP4991A LanProbe segment mon-
        itor. It automatically locates the position of nodes
        on the ethernet networks using coaxial cabling schemes.

CAVEATS
        None.

BUGS
        None known.

LIMITATIONS
        None reported.

HARDWARE REQUIRED
        HP 4991A LanProbe segment monitor
        HP 4992A NodeLocator (for optional capabilities)
        80386 based PC capable of running MS-Windows

SOFTWARE REQUIRED
        HP 4990A ProbeView
        MSDOS 3.0 or higher and Microsoft Windows/286 2.1.

AVAILABILITY
        A commercial product available from:
            Hewlett-Packard Company
            P.O. Box 10301,
            Palo Alto, CA 94303-0890

Internet Tool Catalog   LANWATCH

NAME
     LANWatch

KEYWORDS
     alarm, analyzer, traffic; CHAOS, DECnet, DNS, ethernet,
     IP, OSI, ring, SMTP, star; eavesdrop; DOS; library,
     sourcelib.

ABSTRACT
     LANWatch 2.0 is an inexpensive, powerful and flexible
     network analyzer that runs under DOS on personal com-
     puters and requires no hardware modifications to either
     the host or the network. LANWatch is an invaluable
     tool for installing, troubleshooting, and monitoring
     local area networks, and for developing and debugging
     new protocols. Network managers using LANWatch can
     inspect network traffic patterns and packet errors to
     isolate performance problems and bottlenecks. Protocol
     developers can use LANWatch to inspect and verify
     proper protocol handling. Since LANWatch is a
     software-only package which installs easily in existing
     PCs, network technicians and field service engineers
     can carry LANWatch in their briefcase for convenient
     network analysis at remote sites.

     LANWatch has two operating modes: Display and Examine.
     In Display Mode, LANWatch traces network traffic by
     displaying captured packets in real time. Examine Mode
     allows you to scroll back through stored packets to
     inspect them in detail. To select a subset of packets
     for display, storage or retrieval, there is an exten-
     sive set of built-in filters. Using filters, LANWatch
     collects only packets of interest, saving the user from
     having to sort through all network traffic to isolate
     specific packets. The built-in filters include alarm,
     trigger, capture, load, save and search. They can be
     controlled separately to match on source or destination
     address, protocol, or packet contents at the hardware
     and transport layers. LANWatch also includes suffi-
     cient source code so users can modify the existing
     filters and parsers or add new ones.

     The LANWatch distribution includes executables and
     source for several post-processors: a TCP protocol
     analyzer, a node-by-node traffic analyzer and a dump
     file listing tool.

MECHANISM
     Uses many common PC network interfaces by placing them
     in promiscuous mode and capturing traffic.

CAVEATS
     Most PC network interfaces will not capture 100% of the
     traffic on a fully-loaded network (primarily missing
     back-to-back packets).

BUGS
     None known.

LIMITATIONS
     LANWatch can't analyze what it doesn't see (see
     Caveats).

HARDWARE REQUIRED
     LANWatch requires a PC or PS/2 with a supported network
     interface card.

SOFTWARE REQUIRED
     LANWatch runs in DOS. Modification of the supplied
     source code or creation of additional filters and
     parsers requires Microsoft C 5.1

AVAILABILITY
     LANWatch is commercially available from FTP Software,
     Incorporated, 26 Princess Street, Wakefield, MA, 01880
     (617 246-0900).

Internet Tool Catalog   LLL_ENTM

NAME
     ENTM -- Ethernet Traffic Monitor

KEYWORDS
     traffic; ethernet, IP; eavesdrop; VMS; free.

ABSTRACT
     ENTM is a screen-oriented utility that runs under
     VAX/VMS. It monitors local ethernet traffic and
     displays either a real time or cumulative, histogram
     showing a percent breakdown of traffic by ethernet pro-
     tocol type. The information in the display can be
     reported based on packet count or byte count. The per-
     cent of broadcast, multicast and approximate lost pack-
     ets is reported as well. The screen display is updated
     every three seconds. Additionally, a real time, slid-
     ing history window may be displayed showing ethernet
     traffic patterns for the last five minutes.

     ENTM can also report IP traffic statistics by packet
     count or byte count. The IP histograms reflect infor-
     mation collected at the TCP and UDP port level, includ-
     ing ICMP type/code combinations. Both the ethernet and
     IP histograms may be sorted by ASCII protocol/port name
     or by percent-value. All screen displays can be saved
     in a file for printing later.

MECHANISM
     This utility simply places the ethernet controller in
     promiscuous mode and monitors the local area network
     traffic. It preallocates 10 receive buffers and
     attempts to keep 22 reads pending on the ethernet dev-
     ice.

CAVEATS
     Placing the ethernet controller in promiscuous mode may
     severly slow down a VAX system. Depending on the speed
     of the VAX system and the amount of traffic on the lo-
     cal ethernet, a large amount of CPU time may be spent
     on the Interrupt Stack. Running this code on any pro-
     duction system during operational hours is discouraged.

BUGS
     Due to a bug in the VAX/VMS ethernet/802 device driver,
     IEEE 802 format packets may not always be detected. A
     simple test is performed to "guess" which packets are

in IEEE 802 format (DSAP equal to SSAP). Thus, some
DSAP/SSAP pairs may be reported as an ethernet type,
while   valid ethernet types may be reported as IEEE 802
packets.

In some hardware configurations, placing an ethernet
controller in promiscuous mode with automatic-restart
enabled will hang the controller. Our VAX 8650 hangs
running this code, while our uVAX IIs and uVAX IIIs do
not.

Please report any additional bugs to the author at:
     Allen Sturtevant
     National Magnetic Fusion Energy Computer Center
     Lawrence Livermore National Laboratory
     P.O. Box 808; L-561
     Livermore, CA 94550
     Phone : (415) 422-8266
     E-Mail: sturtevant@ccc.nmfecc.gov

LIMITATIONS
     The user is required to have PHY_IO, TMPMBX and NETMBX
     privileges. When activated, the program first checks
     that the user process as enough quotas remaining
     (BYTLM, BIOLM, ASTLM and PAGFLQUO) to successfully run
     the program without entering into an involuntary wait
     state. Some quotas require a fairly generous setting.

     The contents of IEEE 802 packets are not examined.
     Only the presence of IEEE 802 packets on the wire is
     reported.

     The count of lost packets is approximated. If, after
     each read completes on the ethernet device, the utility
     detects that it has no reads pending on that device,
     the lost packet counter is incremented by one.

     When the total number of bytes processed exceeds
     7fffffff hex, all counters are automatically reset to
     zero.

HARDWARE REQUIRED
     A DEC ethernet controller.

SOFTWARE REQUIRED
     VAX/VMS version V5.1+.

          AVAILABILITY
               For executables only, FTP to the ANONYMOUS account
               (password GUEST) on CCC.NMFECC.GOV and GET the follow-
               ing files:

               [ANONYMOUS.PROGRAMS.ENTM]ENTM.DOC   (ASCII text)
               [ANONYMOUS.PROGRAMS.ENTM]ENTM.EXE   (binary)
               [ANONYMOUS.PROGRAMS.ENTM]EN_TYPES.DAT (ASCII text)
               [ANONYMOUS.PROGRAMS.ENTM]IP_TYPES.DAT (ASCII text)

Internet Tool Catalog   Interactive Network Map

NAME
     map -- Interactive Network Map

KEYWORDS
     manager, map; CHAOS, ethernet, IP, ring, star; NMS,
     ping, SNMP, X; UNIX; free, sourcelib.

ABSTRACT
     Map draws a map of network connectivity and allows
     interactive examination of information about various
     components including whether hosts can be reached over
     the network.

     The program is supplied with complete source and is
     written in a modular fashion to make addition of dif-
     ferent protocols stacks, displays, or hardcopy devices
     relatively easy. This is one of the reasons why the
     initial version supports at least two of each. Contri-
     butions of additional drivers in any of these areas
     will be welcome as well as porting to additional plat-
     forms.

MECHANISM
     Net components are pinged by use of ICMP echo and,
     optionally, CHAOS status requests and SNMP "gets." The
     program initializes itself from static data stored in
     the file system and therefore does not need to access
     the network in order to get running (unless the static
     files are network mounted).

CAVEATS
     As of publication, the tool is in beta release.

BUGS
     Several minor nits, documented in distribution files.
     Bug discoveries should be reported by email to Bug-
     Map@LCS.MIT.Edu.

LIMITATIONS
     See distribution file for an indepth discussion of sys-
     tem capabilities and potential.

HARDWARE REQUIRED
     An X display is needed for interactive display of the
     map, non-graphical interaction is available in non-
     display mode. For hardcopy output a PostScript or Tek-

tronix 4692 printer is required.

SOFTWARE REQUIRED
    BSD UNIX or related OS. IP/ICMP is required;
    CHAOS/STATUS and SNMP can be used but are optional.
    X-Windows is required for interactive display of the
    map.

AVAILABILITY
    The program is Copyright MIT. It is available via
    anonymous FTP with a license making it free to use and
    distribute for non-commercial purposes. FTP to host
    FTP.LCS.MIT.Edu, directory nets. The complete
    distribution is in map.tar.Z and some short
    documentation files are there (as well as in the
    distribution). Of most interest are ReadMe and Intro.

    To be added to the email forum that discusses the
    software, or for other administrative details, send a
    request to: MAP-Request@LCS.MIT.Edu

Internet Tool Catalog   MCONNECT

NAME
     mconnect

KEYWORDS
     status; SMTP; spoof; UNIX.

ABSTRACT
     Mconnect allows an interactive session with a remote
     mailer. Mail delivery problems can be diagnosed by
     connecting to the remote mailer and issuing SMTP com-
     mands directly.

MECHANISM
     Opens a TCP connection to remote SMTP on port 25. Pro-
     vides local line buffering and editing, which is the
     distinction between mconnect and a TELNET to port 25.

CAVEATS
     None.

BUGS
     None known.

LIMITATIONS
     Mconnect is not a large improvement over using a TELNET
     connection to port 25.

HARDWARE REQUIRED
     No restrictions.

SOFTWARE REQUIRED
     BSD UNIX or related OS.

AVAILABILITY
     Available with 4.xBSD UNIX and related operating sys-
     tems.

Internet Tool Catalog   MIB-BROWSER

NAME
         MIB Browser

KEYWORDS
         manager; osi; cmis, x; unix; free, sourcelib.

ABSTRACT
         The MIB Browser is an X Windows HCI tool that allows
         you to "browse" through the objects in a Management
         Information Base (MIB). The browser is generic in that
         it can connect to a CMIS agent without having any
         prior knowledge of the structure of the MIB in the
         agent.

MECHANISM
         CMIP is used to transfer the values of attributes
         between the managed system and the browser.

CAVEATS
         None.

BUGS
         Unexpected termination of the agent can cause browser
         to crash (ISODE bug!).

HARDWARE REQUIRED
         Unix workstation, has been tested on SUN 3 and SUN 4
         architectures.

SOFTWARE REQUIRED
         The ISODE protocol suite, BSD UNIX, X Windows, GNU C++
         (g++), Interviews (2.6).

AVAILABILITY
         The CMIP library and related management tools built
         upon it, known as OSIMIS (OSI Management Information
         Service), are publicly available from University
         College London, England via FTP and FTAM. To obtain
         information regarding a copy send email to
         osimis-request@cs.ucl.ac.uk or call +44 71 380 7366.

        Internet Tool Catalog   MONET

     NAME
             MONET -- the Hughes LAN Systems SNMP Network Management
             Center (formerly the Hughes LAN Systems 9100) software
             product runs on a Sun SPARCStation hardware platform.

     KEYWORDS
             control, graphics, network topology,manager, routing,
             status, traffic; bridge, configuration, performance,
             alarm management, relational database, mib parser for
             RDBMS, intelligent hub management, DECnet, ethernet,
             IP; NMS, SNMP; UNIX.

     ABSTRACT
             Monet provides the capability to manage and control
             SNMP-based networking products from any vendor including
             those from Hughes LAN Systems.

             A comprehensive relational database manages the data and
             ensures easy access and control of resources throughout
             the network.

             Monet provides multivendor management through its
             advanced Mib master MIB parser that allows the parsing
             of enterprise MIBs (ASN.1 format per RFC1212) directly
             into the RDBMS for use by Monet's applications.

             Major features include:

             Remote access with X:
                  Use of the X/Motif user-interface, enabling remote
                  access to the all applications.

             Database Management
                  Stores and retrieves the information required to
                  administer and configure the network. It can be
                  used to:
                          - Store and recall configuration data for all
                            devices.
                          - Provide availability history for devices.
                          - Assign new internet addresses.
                          - Provide administrative information such as
                            physical location of devices, responsible
                            person, maintenance history, asset data,
                            hardware/software versions, etc.
                          - Full-function SQL interface.
                          - User-customizable RDBMS report generation.

Graphics and Network Mapping
     The Graphics module enables the user to view the
     nodes in the network as "dynamic" icons in
     heirarchical maps. The network is represented by
     these heirarchical maps. Though there is a
     library of device icons, cities and geographical
     maps included, the user has access to a
     graphics editor that allows customizing and the
     creation of new icons and maps.
     A Device's icon may be selected to:
          - Register/deregister the device,
          - Access the open alarms and acknowledge
            faults for the selected device,
          - Ping the device to determine accessibility,
          - Draw graphs of any of the device's numeric
            MIB objects, either the values as retrieved
            in real-time or the history values
            previously stored in the RDBMS by the
            Performance Manager,
          - Telnet to the device,
          - Customize the graphical dynamics (color,
            fill, rotation, etc.) of the device's icon
            by associating them to the values of the
            device's MIB objects.

Configuration Management
     - Retrieves configuration information from SNMP
       devices.
     - Stores device parameters in the RDBMS, with
       common sets of parameters used for multiple
       devices, or for multiple ports on a device,
       stored only once in the RDBMS.
     - Configures devices from the parameters stored in
       the RDBMS, including those relating to TCP/IP,
       DECnet and any other protocol/feature
       configurable via SNMP.
     - Polls devices to compare their current parameter
       values with those in the database and produce
       reports of the discrepancies.
     - Collect data about the state of the network.
     - Learn the parameters of the devices in the
       network and populate the database.

Performance Management
     - Displays local network traffic graphically, by
       packet size, protocol, network utilization,
       sources and destinations of packets, etc.
     - Provides for the scheduling of jobs to retrieve

                         MIB values of a device and store them in the RDBMS
                         for review or summary reporting at a later time.
                     - Allows high/low thresholds to be set on retrieved
                       values with alarms generated when thresholds are
                       exceeded.

               Fault Management
                     - Provides availability monitoring and indicates
                       potential problems.
                     - Creates alarms from received SNMP traps, and from
                       other internally-generated conditions,
                     - Records alarms in the alarm log in the RDBMS.
                     - Lists alarms for selected set of devices,
                       according to various filter conditions,
                     - Possible causes and suggested actions for the
                       alarms are listed.
                     - New alarms are indicated by a flashing icon and
                       optional audio alert.
                     - Visual indication of alarms bubbles up the network
                       map heirarchy.
                     - Cumulative reports can be produced.

               Utilities Function
                     - View and/or terminate current NMC processes,
                     - Access to database maintenance utilities.

        MECHANISM
               SNMP.

        CAVEATS
               None reported.

        BUGS
               None known.

        LIMITATIONS
               Maximum number of nodes that can be monitored is
               18,000. This can include Hosts, Terminal Servers, PCs,
               Routers, and Bridges.

        HARDWARE REQUIRED
               The host for the NMC software is a Sun 4 desktop works-
               tation. Recommended minimum hardware is the Sun IPX
               Color workstation, with a 1/4" SCSI tape drive.

        SOFTWARE REQUIRED
               MONET V5.0, which is provided on 1/4" tape format, runs on
               the Sun 4.1.1 Operating System.

          AVAILABILITY AND CONTACT POINT FOR INFORMATION ABOUT THIS TOOL
              A commercial product of:
                   Hughes LAN Systems Inc.
                   1225 Charleston Road
                   Mountain View, CA 94043
                   Phone: (415) 966-7300
                   Fax: (415) 960-3738
                   RCA Telex: 276572

          CONTACT POINT FOR CHANGES TO THIS CATALOG ENTRY
                   kishoret@msgate.hls.com
                   kzm@hls.com

Internet Tool Catalog   NET_MONITOR

NAME
     net_monitor

KEYWORDS
     routing, status; DECnet, IP; curses, ping; UNIX, VMS;
     free, sourcelib.

ABSTRACT
     Net_monitor uses ICMP echo (and DECnet reachability
     information on VAX/VMS) to monitor a network. The mon-
     itoring is very simplistic, but has proved useful. It
     periodically tests whether hosts are reachable and
     reports the results in a full-screen display. It
     groups hosts together in common sets. If all hosts in
     a set become unreachable, it makes a lot of racket with
     bells, since it assumes that this means that some com-
     mon piece of hardware that supports that set has
     failed. The periodicity of the tests, hosts to test,
     and groupings of hosts are controlled with a single
     configuration file.

     The idea for this program came from the PC/IP monitor
     facility, but is an entirely different program with
     different functionality.

MECHANISM
     Reachability is tested using ICMP echo facilities for
     TCP/IP hosts (and DECnet reachability information on
     VAX/VMS). A DECnet node is considered reachable if it
     appears in the list of hosts in a "show network" com-
     mand issued on a routing node.

CAVEATS
     This facility has been found to be most useful when run
     in a window on a workstation rather than on a terminal
     connected to a host. It could be useful if ported to a
     PC (looks easy using FTP Software's programming
     libraries), but this has not been done. Curses is very
     slow and cpu intensive on VMS, but the tool has been
     run in a window on a VAXstation 2000. Just don't try
     to run it on a terminal connected to a 11/750.

BUGS
     None known.

LIMITATIONS
     This tool is not meant to be a replacement for a more
     comprehensive network management facility such as is
     provided with SNMP.

HARDWARE REQUIRED
     A host with a network connection.

SOFTWARE REQUIRED
     Curses, 4.xBSD UNIX socket programming libraries (lim-
     ited set) and some flavor of TCP/IP that supports ICMP
     echo request (ping). It has been run on VAX/VMS run-
     ning WIN/TCP and several flavors of 4BSD UNIX (includ-
     ing SunOS 3.2, 4.0, and 4.3BSD). It could be ported to
     any platform that provides a BSD-style programming li-
     brary with an ICMP echo request facility and curses.

AVAILABILITY
     Requests should be sent to the author:

     Dale Smith
     Asst Dir of Network Services
     University of Oregon
     Computing Center
     Eugene, OR 97403-1211

     Internet: dsmith@oregon.uoregon.edu.
     BITNET: dsmith@oregon.bitnet
     UUCP: ...hp-pcd!uoregon!dsmith
     Voice: (503)686-4394

     With the source code, a makefile is provided for most
     any UNIX box and a VMS makefile compatible with the
     make distributed with PMDF. A VMS DCL command file is
     also provided, for use by those VMS sites without
     "make."

     The author will attempt to fix bugs, but no support is
     promised. The tool is copyrighted, but free (for now).

Internet Tool Catalog   NETLABS_CMOT_AGENT

NAME
     Netlabs CMOT Agent

KEYWORDS
     manager, status; IP, OSI; NMS.

ABSTRACT
     Netlabs' CMOT code debuted in Interop 89. The CMOT
     code comes with an Extensible MIB, which allows users
     to add new MIB variables. The code currently supports
     all the MIB variables in RFC 1095 via the data types in
     RFC 1065, as well as the emerging MIB-II, which is
     currently in experimental stage. The CMOT has been
     benchmarked at 100 Management Operations per Second
     (MOPS) for a 1-MIPS machine.

MECHANISM
     The Netlabs CMOT agent supports the control and moni-
     toring of network resources by use of CMOT message
     exchanges.

CAVEATS
     None.

BUGS
     None known.

LIMITATIONS
     None reported.

HARDWARE REQUIRED
     Portable to most hardware.

SOFTWARE REQUIRED
     Portable to most operating systems.

AVAILABILITY
     Commercially available from:
          Netlabs Inc
          11693 Chenault Street Ste 348
          Los Angeles CA 90049
          (213) 476-4070
          lam@netlabs.com (Anne Lam)

Internet Tool Catalog   NETLABS_DUAL_MANAGER

NAME
     Dual Manager

KEYWORDS
     alarm, control, manager, map, security, status; IP,
     OSI; NMS, SNMP, X; UNIX; library.

ABSTRACT
     Netlabs' Dual Manager provides management of TCP/IP
     networks using both SNMP and CMOT protoocls. Such
     management can be initiated either through the X-
     Windows user interface (both Motif and Openlook), or
     through OSI Network Management (CMIP) commands. The
     Dual Manager provides for configuration, fault, secu-
     rity and performance management. It provides extensive
     map management features, including scanned maps in the
     background. It provides simple mechanisms to extend
     the MIB and assign specific lists of objects to
     specific network elements, thereby providing for the
     management of all vendors' specific MIB extensions. It
     provides an optional relational DBMS for storing and
     retrieving MIB and alarm information. Finally, the
     Dual Manager is an open platform, in that it provides
     several Application Programming Interfaces (APIs) for
     users to extend the functionality of the Dual Manager.

     The Dual Manager is expected to work as a TCP/IP
     "branch manager" under DEC's EMA, AT&T's UNMA and other
     OSI-conformant enterprise management architectures.

MECHANISM
     The Netlabs Dual Manager supports the control and moni-
     toring of network resources by use of both CMOT and
     SNMP message exchanges.

CAVEATS
     None.

BUGS
     None known.

LIMITATIONS
     None reported.

HARDWARE REQUIRED
     Runs on Sun/3 and Sun/4s.

        SOFTWARE REQUIRED
              Available on System V or SCO Open Desktop environments.
              Uses X-Windows for the user interface.

        AVAILABILITY
              Commercially available from:
                    Netlabs Inc
                    11693 Chenault Street Ste 348
                    Los Angeles CA 90049
                    (213) 476-4070
                    lam@netlabs.com (Anne Lam)

Internet Tool Catalog   NETLABS_SNMP_AGENT

NAME
     Netlabs SNMP Agent.

KEYWORDS
     manager, status; IP; NMS, SNMP.

ABSTRACT
     Netlabs' SNMP code debuted in Interop 89, where it
     showed interoperation of the code with several imple-
     mentations on the show floor. The SNMP code comes with
     an Extensible MIB, which allows users to add new MIB
     variables. The code currently supports all the MIB
     variables in RFC 1066 via the data types in RFC 1065,
     as well as the emerging MIB-II, which is currently in
     experimental stage. The SNMP has been benchmarked at
     200 Management Operations per Second (MOPS) for a 1-
     MIPS machine.

MECHANISM
     The Netlabs SNMP agent supports the control and moni-
     toring of network resources by use of SNMP message
     exchanges.

CAVEATS
     None.

BUGS
     None known.

LIMITATIONS
     None reported.

HARDWARE REQUIRED
     Portable to most hardware.

SOFTWARE REQUIRED
     Portable to most operating systems.

AVAILABILITY
     Commercially available from:
          Netlabs Inc
          11693 Chenault Street Ste 348
          Los Angeles CA 90049
          (213) 476-4070
          lam@netlabs.com (Anne Lam)

Internet Tool Catalog   NetMetrix-Load-Monitor

NAME
        NetMetrix Load Monitor

KEYWORDS
        alarm,traffic; Ethernet, FDDI, IP, Ring; Eavesdrop,
        SNMP, X; UNIX;

ABSTRACT
        The NetMetrix Load Monitor is a distributed
        client-server monitoring tool for ethernet, token
        ring, and FDDI networks. A unique "dual" architecture
        provides compatibility with both RMON and X windows.
        RMON allows interoperability and an enterprise-wide
        view, while X windows enables much more powerful,
        intelligent applications at remote segments and saves
        network bandwidth.

        The Load Monitor provides extensive traffic
        statistics. It looks at load by time interval, source
        node, destination node, application, protocol or
        packet size. A powerful ZOOM feature allows extensive
        correlational analysis which is displayed in a wide
        variety of graphs and tables.

        You can answer questions such as: Which sources are
        generating most of the load on the network when it is
        most heavily loaded and where is this load going?
        Which source/destination pairs generate the most
        traffic over the day? Where should bridges and
        routers be located to optimally partition the network?
        How much load do applications, like the X Windows
        protocol, put on the network and who is generating that
        load when it is the greatest.

        A floating license allows easy access to the software
        tool anywhere you need it.

    MECHANISM
        NetMetrix turns the network interface into promiscuous
        mode to capture packets.

    CAVEATS
        none.

    BUGS
        none known.

        LIMITATIONS
                none.

        HARDWARE REQUIRED
                SPARC system

        SOFTWARE REQUIRED
                SunOS 4.0 or higher

        AVAILABILITY AND CONTACT POINT FOR INFORMATION ABOUT THIS TOOL
            NetMetrix is available from:
                        Sales Department
                        Metrix Network Systems, Inc.
                        One Tara Boulevard
                        Nashua, New Hampshire 03062
                        telephone: 603-888-7000
                        fax: 603-891-2796
                        email: info@metrix.com

        Government agencies please note that NetMetrix is on the GSA
        schedule.

        CONTACT POINT FOR CHANGES TO THIS CATALOG ENTRY
            Norma Shepperd
            Marketing Administrator
            603-888-7000
            norma@metrix.com

Internet Tool Catalog   NetMetrix-NFS-Monitor

NAME
     NetMetrix NFS Monitor

KEYWORDS
     traffic; Ethernet, FDDI, NFS, Ring; Eavesdrop, SNMP, X;
     UNIX

ABSTRACT
          The NetMetrix NFS Monitor is a distributed network
          monitoring tool which monitors and graphs NFS load,
          response time, retransmits, rejects and errors by
          server, client, NFS procedure, or time
          interval. Breakdown server activity by file system
          and client activity by user.

          A powerful ZOOM feature lets you correlate monitoring
          variables. You can see client/server relationships,
          compare server performance, evaluate NFS performance
          enhancement strategies.

          A floating license and the X Window protocol allows
          monitoring of remote ethernet, token ring and FDDI
          segments from a central enterprise-wide display.

MECHANISM
          NetMetrix turns the network interface into promiscuous
          mode to capture packets.

CAVEATS
          none.

BUGS
          none known.

LIMITATIONS
          none.

HARDWARE REQUIRED
          SPARC system

SOFTWARE REQUIRED
          SunOS 4.0 or higher

          AVAILABILITY AND CONTACT POINT FOR INFORMATION ABOUT THIS TOOL
               NetMetrix is available from:
                         Sales Department
                         Metrix Network Systems, Inc.
                         One Tara Boulevard
                         Nashua, New Hampshire 03062
                         telephone: 603-888-7000
                         fax: 603-891-2796
                         email: info@metrix.com

               Government agencies please note that NetMetrix is on
               the GSA schedule.

          CONTACT POINT FOR CHANGES TO THIS CATALOG ENTRY
               Norma Shepperd
               Marketing Administrator
               603-888-7000
               norma@metrix.com

Internet Tool Catalog   NetMetrix-Protocol-Analyzer

NAME
     NetMetrix Protocol Analyzer

KEYWORDS
     alarm, analyzer, traffic; DECnet, DNS, Ethernet, FDDI,
     IP, OSI, NFS, Ring, SMTP; Eavesdrop, SNMP, X; UNIX;
     Library

ABSTRACT
     The NetMetrix Protocol Analyzer is a distributed
     client-server monitoring tool for ethernet, token
     ring, and FDDI networks. A unique "dual" architecture
     provides compatibility with both RMON and
     X windows. RMON allows interoperability, while X
     windows enables much more powerful, intelligent
     applications at remote segments and saves network
     bandwidth.

     With the Protocol Analyzer, you can decode and display
     packets as they are being captured. Extensive filters
     let you sift through packets either before or after
     trace capture. The capture filter may be specified by
     source, destination between hosts, protocol, packet
     size, pattern match, or by a complete expression using
     an extensive filter expression language.

     Full 7-layer packet decodes are available for all
     major protocols including DECnet, Appletalk, Novell,
     XNS, SNA, BANYAN, OSI and TCP/IP. The decodes for the
     TCP/IP stack have all major protocols including NFS,
     YP, DNS, SNMP, OSPF, etc.

     Request and reply packets are matched. Packets can be
     displayed in summary, detail or hex, with multiple
     views to see packet dialogues side by side.

     A complete developers' kit is available for custom
     decodes.

     A floating license allows easy acess to the software
     tool anywhere you need it.

MECHANISM
     NetMetrix turns the network interface into promiscuous
     mode to capture packets.

        CAVEATS
                none.

        BUGS
                none known.

        LIMITATIONS
                none.

        HARDWARE REQUIRED
                SPARC system

        SOFTWARE REQUIRED
                 SunOS 4.0 or higher

        AVAILABILITY AND CONTACT POINT FOR INFORMATION ABOUT THIS TOOL
            NetMetrix is available from:
                    Sales Department
                    Metrix Network Systems, Inc.
                    One Tara Boulevard
                    Nashua, New Hampshire 03062
                    telephone: 603-888-7000
                    fax: 603-891-2796
                    email: info@metrix.com

            Government agencies please note that NetMetrix is on the
            GSA schedule.

        CONTACT POINT FOR CHANGES TO THIS CATALOG ENTRY
            Norma Shepperd
            Marketing Administrator
            603-888-7000
            norma@metrix.com

Internet Tool Catalog   NetMetrix-Traffic-Generator

NAME
        NetMetrix Traffic Generator

KEYWORDS
        Debugger, Generator, Traffic; Ethernet, FDDI, IP,
        Ring; Eavesdrop, SNMP, X; UNIX; Library

ABSTRACT
        The NetMetrix Traffic Generator is a distributed
        software tool which allows you to simulate network
        load or test packet dialogues between nodes on your
        ethernet, token ring, or FDDI segments. The Traffic
        Generator can also be used to test and validate
        management station alarms, routers, bridges, hubs, etc.

        An easy-to-use programming interface provides complete
        flexibility over variables such as bandwidth, packet
        sequence, and conditional responses.

        A floating license and the X Window System protocol
        allows testing of remote ethernet, token ring and FDDI
        segments from a central console.

MECHANISM
        NetMetrix turns the network interface into promiscuous
        mode to capture packets.

CAVEATS
        none.

BUGS
        none known.

LIMITATIONS
        none.

HARDWARE REQUIRED
        SPARC system

SOFTWARE REQUIRED
        SunOS 4.0 or higher

         AVAILABILITY AND CONTACT POINT FOR INFORMATION ABOUT THIS TOOL
            NetMetrix is available from:
                    Sales Department
                    Metrix Network Systems, Inc.
                    One Tara Boulevard
                    Nashua, New Hampshire 03062
                    telephone: 603-888-7000
                    fax: 603-891-2796
                    email: info@metrix.com

            Government agencies please note that NetMetrix is on
            the GSA schedule.

         CONTACT POINT FOR CHANGES TO THIS CATALOG ENTRY
            Norma Shepperd
            Marketing Administrator
            603-888-7000
            norma@metrix.com

Internet Tool Catalog   NETMON_MITRE

NAME
     NETMON and iptrace

KEYWORDS
     traffic; IP; eavesdrop; UNIX; free.

ABSTRACT
     NETMON is a facility to enable communication of net-
     working events from the BSD UNIX operating system to a
     user-level network monitoring or management program.
     Iptrace is a program interfacing to NETMON which logs
     TCP-IP traffic for performance measurement and gateway
     monitoring. It is easy to build other NETMON-based
     tools using iptrace as a model.

     NETMON resides in the 4.3BSD UNIX kernel. It is
     independent of hardware-specific code in UNIX. It is
     transparent to protocol and network type, having no
     internal assumptions about the network protocols being
     recorded. It is installed in BSD-like kernels by
     adding a standard function call (probe) to a few points
     in the input and output routines of the protocols to be
     logged.

     NETMON is analogous to Sun Microsystems' NIT, but the
     interface tap function is extended by recording more
     context information. Aside from the timestamp, the
     choice of information recorded is up to the installer
     of the probes. The NETMON probes added to the BSD IP
     code supplied with the distribution include as context:
     input and output queue lengths, identification of the
     network interface, and event codes labeling packet dis-
     cards. (The NETMON distribution is geared towards
     measuring the performance of BSD networking protocols
     in an IP gateway).

     NETMON is designed so that it can reside within the
     monitored system with minimal interference to the net-
     work processing. The estimated and measured overhead
     is around five percent of packet processing.

     The user-level tool "iptrace" is provided with NETMON.
     This program logs IP traffic, either at IP-level only,
     or as it passes through the network interface drivers
     as well. As a separate function, iptrace produces a
     host traffic matrix output. Its third type of output

is abbreviated sampling, in which only a pre-set number
of packets from each new host pair is logged. The
three output types are configured dynamically, in any
combination.

OSITRACE, another logging tool with a NETMON interface,
is available separately (and documented in a separate
entry in this catalog).

MECHANISM
Access to the information logged by NETMON is through a
UNIX special file, /dev/netmon. User reads are blocked
until the buffer reaches a configurable level of full-
ness.

Several other parameters of NETMON can be tuned at com-
pile time. A diagnostic program, netmonstat, is
included in the distribution.

CAVEATS
None.

BUGS
Bug reports and questions should be addressed to:
ie-tools@gateway.mitre.org
Requests to join this mailing list:
ie-tools-request@gateway.mitre.org
Questions and suggestions can also be directed to:
Allison Mankin (703)883-7907
mankin@gateway.mitre.org

LIMITATIONS
A NETMON interface for tcpdump and other UNIX protocol
analyzers is not included, but it is simple to write.
NETMON probes for a promiscuous ethernet interface are
similarly not included.

HARDWARE REQUIRED
No restrictions.

SOFTWARE REQUIRED
BSD UNIX-like network protocols or the ability to
install the BSD publicly available network protocols in
the system to be monitored.

        AVAILABILITY
            The NETMON distribution is available by anonymous FTP
            in pub/netmon.tar or pub/netmon.tar.Z from aelred-
            3.ie.org. A short user's and installation guide,
            NETMON.doc, is available in the same location. The
            NETMON distribution is provided "as is" and requires
            retention of a copyright text in code derived from it.
            It is copyrighted by the MITRE-Washington Networking
            Center.

Internet Tool Catalog   NETMON_WINDOWS_SNMP_RESEARCH

NAME

NETMON for Windows -- an SNMP-based network management
tool that runs under Microsoft Windows 3.0 from SNMP
Research.

KEYWORDS

alarm, control, manager, map, routing;
DECnet, Ethernet, IP, OSI, ring, star;
NMS, SNMP;
DOS;
sourcelib.

ABSTRACT

The NETMON application implements a powerful network
management station based on a low-cost DOS platform.
NETMON's network management tools for configuration,
performance, security, and fault management have been
used successfully with a wide assortment of wide- and
local-area-network topologies and medias. Multiprotocol
devices are supported including those using TCP/IP,
DECnet, and OSI protocols.

Some features of NETMON's network management tools include:

o Fault management tool displays a map of the network
  configuration with node and link state indicated
  in one of several colors to indicate current status;
o Configuration management tool may be used to edit the
  network management information base stored in the
  NMS to reflect changes occurring in the network;
o Graphs and tabular tools for use in fault and performance
  management;
o Mechanisms by which additional variables, such as vendor-
  specific variables, may be added;
o Alarms may be enabled to alert the operator of events
  occurring in the network;
o Events are logged to disk;
o Output data may be transferred via flat files for
  additional report generation by a variety of
  statistical packages.

The NETMON application comes complete with source code
including a powerful set of portable libraries for generating
and parsing SNMP messages.

MECHANISM
        The NETMON for Windows application is based on the
        Simple Network Management Protocol (SNMP). Polling is
        performed via the powerful SNMP get-next operator and
        the SNMP get operator. Trap directed polling is used
        to regulate the focus and intensity of the polling.

CAVEATS
        None.

BUGS
        None known.

LIMITATIONS
        None reported.

HARDWARE REQUIRED
        The minimum system is a IBM 386 computer, or
        compatible, with hard disk drive.

SOFTWARE REQUIRED
        DOS 5.0 or later, Windows 3.0 in 386 mode, and TCP/IP
        kernel software from FTP Software.

AVAILABILITY AND CONTACT POINT FOR INFORMATION ABOUT THIS TOOL
        This is a commercial product available under license
        from:
                SNMP Research
                3001 Kimberlin Heights Road
                Knoxville, TN 37920-9716
                Attn: John Southwood, Sales and Marketing
                (615) 573-1434 (Voice) (615) 573-9197 (FAX)

CONTACT POINT FOR CHANGES TO THIS CATALOG ENTRY
        users@seymour1.cs.utk.edu

        Internet Tool Catalog   NETscout

        NAME
                NETscout(tm)

        KEYWORDS
                Alarm, Analyzer, Manager, Status, Traffic;
                DECnet, Ethernet, IP, OSI, NFS, Ring, Star, Eavesdrop;
                NMS, SNMP;
                UNIX;

        ABSTRACT
                The NETscout family of distributed LAN Analyzer
                devices are intended to provide network users with a
                comprehensive capability to identify and isolate fault
                conditions in data communications networks.
                NETscout has the capability to collect wide ranging
                statistical data, to display selectively captured and
                fully decoded network traffic, to set user-defined
                alarm conditions, and to obtain real-time updates
                from all segments of a widely dispersed internetwork
                from a centralized SNMP-compatible network management
                console.

                The NETscout family is based on standards so that
                operation may be realized in heterogeneous networks
                which constitute a multi-protocol, multi-topology,
                multi-vendor environment. The fundamental standards
                upon which NETscout is based are the Simple Network
                Management Protocol (SNMP), which defines the protocol
                for all inter-communications between NETscout devices,
                and the Remote Monitoring Management Information Base
                (RMON-MIB), which defines the type of information
                which is to be gathered and made available to the
                user for each network segment.

                NETscout clients provide a full array of monitoring
                and analysis features including intelligent seven
                level decoding of all majorprotocol stacks:

                DOD including TCP/IP   XNS   Novell
                DECNET including LAT   ISO   APPLETALK
                IBM Token Ring   Vines   NETBIOS/SMB
                SNMP including RMON-MIB SUN-NFS   SMT

                NETscout agents support all nine groups of the
                RMON-MIB standard. NETscout agents can work with any
                SNMP-based network management system and currently

support Ethernet and Token Ring.

MECHANISM
The operation of the NETscout family is divided into
two distinct subcategories. The first is the "Client"
which is the user console from which operational
commands are issued and where all results and
diagnostic information are displayed. In a NETscout
topology it is feasible to have multiple clients
active simultaneously within a single network. The
second category is the "Agent", a hardware/software
device which is attached to a specific network
segment and which gathers statistical information for
that segment as well as providing a window into that
segment where network traffic may be observed and
gathered for more detailed user analysis. A
typical network will have multiple segments and
multiple agents up to the point of having one agent
for each logical network segment.

NETscout Model 9210 is a software package which, when
combined in a Sun SPARCstation in conjunction with
SunNet Manager running under Open Windows, implements
the NETscout client function. SunNet Manager provides
the background operational tools for client operation
while the NETscout software provides
application-specific functions related to RMON-MIB
support as well as all software necessary to
perform the protocol decode function.
SunNet Manager also implements a network map file
which includes a topographical display of the entire
network and is the mechanism for selecting
network elements to perform operations.

NETscout Model 9215 is a software package that
operates in conjunction with SunNet Manager and
implements the statistics monitoring function only.
That is, it does not include the protocol
decode function or the mechanism to retrieve actual
data from a remote agent. It does, however, include
complete statistics gathering and event and alarm
generation.

Frontier NETscout Models 9510 and 9515, and Model 9610
and 9615 are agent software packages that implement
selected network diagnostic functions when loaded into
a Sun SPARCstation (9510, 9515) or a SynOptics
LattisNet Hub (9610, 9615) respectively which is

connected to an Ethernet network segment
using conventional network interface hardware. Models
9510 and 9610 support all nine RMON-MIB groups
including "filters" and "packet capture" and thus
provide for complete protocol monitoring and decode
when used with a client
equipped with protocol decode software. Models 9515
an 9615 include support for seven RMON-MIB groups
which excludes "filters" and "data capture" and
therefore perform network monitoring only through
collection and presentation of network statistics,
events, and alarms. All models also support the MIB2
system and interface groups.

Frontier NETscout Models 9520 and 9525, and Model 9620
and 9625 are agent software packages that are
identical in function to their respective models
described above except that they are for use on
Token Ring segments.

CAVEATS
         The RMON-MIB standard for Token Ring applications has
         not yet beenformally released and is not approved.
         NETscout products correspond to the latest draft for
         Token Ring functions and will be updated as
         required to conform to the standard as it is approved.

BUGS
         None known.

LIMITATIONS
         None reported.

HARDWARE REQUIRED
         Sun SPARCstation or LattisNet Hub depending upon Model
         number.

SOFTWARE REQUIRED
         Sun OS 4.1.1 for client and agent, SunNet Manager for
         client.

AVAILABILITY AND CONTACT POINT FOR INFORMATION ABOUT THIS TOOL
        NETscout products are available commercially. For
        information regarding your local representative, contact:
                Frontier Software Development, Inc.
                1501 Main Street
                Tewksbury, MA 01876
                Phone: 508-851-8872
                Fax: 508-851-6956

    CONTACT POINT FOR CHANGES TO THIS CATALOG ENTRY
                Marketing
                Frontier Software

Internet Tool Catalog   NETSTAT

NAME
     netstat

KEYWORDS
     routing; IP; UNIX, VMS; free.

ABSTRACT
     Netstat is a program that accesses network related data
     structures within the kernel, then provides an ASCII
     format at the terminal. Netstat can provide reports on
     the routing table, TCP connections, TCP and UDP
     "listens", and protocol memory management.

MECHANISM
     Netstat accesses operating system memory to read the
     kernel routing tables.

CAVEATS
     Kernel data structures can change while netstat is run-
     ning.

BUGS
     None known.

LIMITATIONS
     None reported.

HARDWARE REQUIRED
     No restrictions.

SOFTWARE REQUIRED
     BSD UNIX or related OS, or VMS.

AVAILABILITY
     Available via anonymous FTP from uunet.uu.net, in
     directory bsd-sources/src/ucb. Available with 4.xBSD
     UNIX and related operating systems. For VMS, available
     as part of TGV MultiNet IP software package, as well as
     Wollongong's WIN/TCP.

Internet Tool Catalog   NETWORK_INTEGRATOR

NAME
     Network Integrator I

KEYWORDS
     map, traffic; ethernet; UNIX.

ABSTRACT
     This tool monitors traffic on network segments. All
     information is dumped to either a log file or, for
     real-time viewing, to a command tool window. Data is
     time-stamped according to date and time. Logging can
     continue for up to 24 hours.

     The tool is flexible in data collection and presenta-
     tion. Traffic filters can be specified according to
     header values of numerous protocols, including those
     used by Apple, DEC, Sun, HP, and Apollo. Bandwidth
     utilization can be monitored, as well as actual load
     and peak throughput. Additionally, the Network
     Integrator can analyze a network's topology, and record
     the location of all operational nodes on a network.

     Data can be displayed in six separate formats of bar
     graphs. In addition, there are several routines for
     producing statistical summaries of the data collected.

MECHANISM
     The tools work through RPC and XDR calls.

CAVEATS
     Although the tool adds only little traffic to a net-
     work, generation of statistics from captured files
     requires a significant portion of a workstation's CPU.

BUGS
     None known.

LIMITATIONS
     Must be root to run monitor. There does not seem to be
     a limit to the number of nodes, since it monitors by
     segments. The only major limitation is the amount of
     disk space that a user can commit to the log files.
     The size of the log files, however, can be controlled
     through the tool's parameters.

         HARDWARE REQUIRED
              Sun3 or Sun4.

         SOFTWARE REQUIRED
              4.0BSD UNIX or greater, or related OS.

         AVAILABILITY
              Copyrighted, commercially available from
              Network Integrators,
              (408) 927-0412.

Internet Tool Catalog   NFSwatch

NAME
        nfswatch

KEYWORDS
        Traffic; Ethernet, IP, NFS; Curses, Eavesdrop; UNIX;
        Free

ABSTRACT
        Nfswatch monitors all incoming ethernet traffic to an
        NFS file server and divides it into several
        categories. The number and percentage of packets
        received in each category is displayed on
        the screen in a continuously updated display.

        By default, nfswatch monitors all packets destined for
        the local host over a single network interface.
        Options are provided to specify the specific interface
        to be monitored, or all interfaces at once. NFS
        traffic to the local host, to a remote host, from a
        specific host, between two hosts, or all NFS traffic
        on the network may be monitored.

        Categories of packets monitored and counted include:
        ND Read, ND Write, NFS Read, NFS Write, NFS Mount,
        Yellow Pages (NIS), RPC Authorization, Other RPC, TCP,
        UDP, ICMP, RIP, ARP, RARP, Ethernet Broadcast, and
        Other.

        Packets are also tallied either by file system or file
        (specific files may be watched as an option), NFS
        procedure name (RPC call), or NFS client hostname.

        Facilities for taking "snapshots" of the screen, as
        well as saving data to a log file for later analysis
        (the analysis tool is included) are also available.

MECHANISM
        Nfswatch uses the Network Interface Tap, nit(4) under
        SunOS 4.x, and the Packet Filter, packetfilter(4),
        under Ultrix 4.x, to place the ethernet interface into
        promiscuous mode. It filters out NFS packets, and
        decodes the file handles in order to determine how to
        count the packet.

CAVEATS
        Because the NFS file handle is a non-standard (server
        private) piece of data, nfswatch must be modified to
        understand file handles used by various
        implementations. It currently knows
        about the SunOS 4.x and Ultrix file handle formats.

BUGS
        Does not monitor FDDI interfaces. (It should be a
        simple change, but neither author has access to a
        system with FDDI interfaces for testing.)

LIMITATIONS
        Up to 256 exported file systems and 256 individual
        files can be monitored at any time.

        Only NFS requests are counted; the NFS traffic
        generated by a server in response to those packets
        is not counted.

HARDWARE REQUIRED
        Any Ultrix system (VAX or DEC RISC hardware)

SOFTWARE REQUIRED
        Ultrix release 4.0 or later. For Ultrix 4.1, may
        require the patched "if_ln.o" kernel module, available
        from Digital's Customer Support Center.

AVAILABILITY AND CONTACT POINT FOR INFORMATION ABOUT THIS TOOL
        Copyrighted, but freely distributable. Available via
        anonymous FTP from harbor.ecn.purdue.edu,
        ftp.erg.sri.com, and gatekeeper.dec.com, as well as
        numerous other sites around the Internet. The current
        version is Version 3.0 from January 1991.

Contact points:

Dave Curry   Jeff Mogul
Purdue University   Digital Equipment Corp.
Engineering Computer Network   Western Research Laboratory
1285 Electrical Engineering Bldg.   100 Hamilton Avenue
West Lafayette, IN 47907-1285   Palo Alto, CA 94301
davy@ecn.purdue.edu   mogul@decwrl.dec.com

CONTACT POINT FOR CHANGES TO THIS CATALOG ENTRY
        Dave Curry (see address above).

Internet Tool Catalog   NHFSSTONE

NAME
     nhfsstone

KEYWORDS
     benchmark, generator; NFS; spoof; UNIX; free.

ABSTRACT
     Nhfsstone (pronounced n-f-s-stone, the "h" is silent)
     is an NFS benchmarking program. It is used on an NFS
     client to generate an artificial load with a particular
     mix of NFS operations. It reports the average response
     time of the server in milliseconds per call and the
     load in calls per second. The nhfsstone distribution
     includes a script, "nhfsnums" that converts test
     results into plot(5) format so that they can be graphed
     using graph(1) and other tools.

MECHANISM
     Nhfsstone is an NFS traffic generator. It adjusts its
     calling patterns based on the client's kernel NFS
     statistics and the elapsed time. Load can be generated
     over a given time or number of NFS calls.

CAVEATS
     Nhfsstone will compete for system resources with other
     applications.

BUGS
     None known.

LIMITATIONS
     None reported.

HARDWARE REQUIRED
     No restrictions.

SOFTWARE REQUIRED
     4.xBSD-based UNIX

AVAILABILITY
Available via anonymous FTP from bugs.cs.wisc.edu.
Alternatively, Legato Systems will provide the program
free of charge, if certain conditions are met. Send
name and both email and U.S. mail addresses to:
Legato Systems, Inc.
Nhfsstone
260 Sheridan Avenue
Palo Alto, California 94306

A mailing list is maintained for regular information
and bug fixes: nhfsstone@legato.com or
uunet!legato.com!nhfsstone. To join the list:
nhfsstone-request@legato.com or
uunet!legato.com!nhfsstone-request.

Internet Tool Catalog   NNSTAT

NAME
     NNStat

KEYWORDS
     manager, status, traffic; ethernet, IP; eavesdrop, NMS;
     UNIX; free.

ABSTRACT
     NNStat is a collection of programs that provides an
     internet statistic collecting capability. The NNStat
     strategy for statistic collection is to collect traffic
     statistics via a promiscuous ethernet tap on the local
     networks, versus instrumenting the gateways. If all
     traffic entering or leaving a network or set of net-
     works traverses a local ethernet, then by stationing a
     statistic gathering agent on each local network a pro-
     file of network traffic can be gathered. Statistical
     data is retrieved from the local agents by a global
     manager.

     A program called "statspy" performs the data gathering
     function. Essentially, statspy reads all packets on an
     ethernet interface and records all information of
     interest. Information of interest is gathered by exa-
     mining each packet and determining if the source or
     destination IP address is one that is being monitored,
     typically a gateway address. If so then the contents
     of the packet are examined to see if they match further
     criteria.

     A program called "collect" performs global data collec-
     tion. It periodically polls various statspy processes
     in the domain of interest to retrieve locally logged
     statistical data.

     The NNSTAT distribution comes with several sample awk
     programs which process the logged output of the collect
     program.

MECHANISM
     Local agents (statspy processes) collect raw traffic
     data via a promiscuous ethernet tap. Statistical, fil-
     tered or otherwise reduced data is retrieved from the
     local agents by a global manager (the "collect" pro-
     cess).

CAVEATS
     None.

BUGS
     Bug fixes, extensions, and other pointers are discussed
     in the electronic mail forum, bytecounters. To join,
     send a request to bytecounters-request@venera.isi.edu.
     Forum exchanges are archived in the file
     bytecounters/bytecounters.mail, available via anonymous
     FTP from venera.isi.edu.

LIMITATIONS
     NNStat presumes a topology of one or more long haul
     networks gatewayed to local ethernets.

     A kernel mod required to run with SunOS4. These mods
     are described in the bytecounters archive.

HARDWARE REQUIRED
     Ethernet interface. Sun 3, Sun 4 (SPARC), or PC RT
     workstation.

SOFTWARE REQUIRED
     Distribution is for BSD UNIX, could easily be adapted
     to any UNIX with promiscuous ethernet support.

AVAILABILITY
     Distribution is available via anonymous FTP from
     venera.isi.edu, in file pub/NNStat.tar.Z. Documenta-
     tion is in pub/NNStat.userdoc.ms.Z.

Internet Tool Catalog   NOCOL(8)

NAME
     nocol - network monitoring tools for an IP network

SYNOPSIS
     This is an overview of the NOCOL software.

DESCRIPTION
     NOCOL (Network Operations Center On-Line) is a
     collection of network monitoring programs that run on
     Unix systems. The software consists of a number of
     monitoring agents that poll various parameters from any
     system and put it in a format suitable for
     post-processing. The post-processors can be a display
     agent, an automated troubleshooting program, an
     event logging program, etc. Presently, monitors for
     tracking reachability, SNMP traps, data throughput
     rate, and nameservers have been developed and are in
     use. Addition of more monitoring agents is easy and
     they will be added as necessary. A display agent-
     nocol(1) using curses has already been developed. Work
     on an "intelligent" module is currently in progress for
     event logging and some automatic troubleshooting.

     All data collected by the monitoring agents follows a
     fixed (non-readable) format. Each data entry is termed
     an event in NOCOL, and each event has certain flags and
     severity associated with it. The display agent
     nocol(1), displays the output of these monitoring
     agents depending on the severity of the event. There
     can be multiple displays running simultanously and
     all process the same set of monitored data.

     There are four levels of severity associated with an
     event- CRITICAL, ERROR, WARNING and INFO. The severity
     level is controlled independently by the monitoring
     agents, and the decision to raise or set an event's
     severity to any level depends on the logic imbedded in
     the monitoring agent.

     As an example, for the pingmon(8) monitor, if a site is
     unreachable via ping, it would be assigned a severity
     of WARNING by pingmon, which would then elevate to
     CRITICAL if the site is still unreachable after some
     time. In the case of trapmon(8), an SNMP trap message
     of EGP neighbor lost would be directly assigned a
     severity level of CRITICAL, while an Warm Start trap is

assigned a severity of WARNING.

The display agent (and other data post-processors)
would use this event severity to decide whether to
display it (or troubleshoot/log it) depending on the
user selected display severity level.

The software is very flexible and allows enhancements
and development with a minimum amount of effort. The
display module processes all the files present in the
data directory, and displays them sequentially. This
allows new monitoring programs to simply start
generating data in the data directory and the display
module will automatically start displaying the new
data. The monitoring tools can be changed, and the only
element that has to remain common between all the
modules is the EVENT data structure.

CURRENT MODULES
     NOCOL presently consists of the following modules:

nocol
     which simply displays the data collected by the
     monitoring agents. It uses the curses screen
     management system to support a wide variety of terminal
     types. The criterion for displaying an event is:

     1. Severity level of the event is higher than the
        severity level set in the display.

     2. The display filter (if set) matches some string in
        the event line.

     The display can be in regular 80 column mode or in
     extended 132 column mode. Critical events are
     displayed in reverse video (if the terminal type
     supports it). Additional features like displaying
     informational messages in a part of the window,
     automatic resizing window sizes, operator
     acknowledgement via a bell when a new event goes
     critical are also available.

ippingmon
     which monitors the reachability of a site via "ICMP"
     ping packets (ICMP was preferred over SNMP for many
     obvious reasons). This program can use the default out-
     put from the system's ping program, but an accompanying
     program (multiping) can ping multiple IP sites at the

same time and is preferable for monitoring a large list
of sites. A site is marked unreachable if a certain
number of packets is lost, and the severity level is
increased each time that the site tests unreachable.

osipingmon
        which is similar to the ippingmon module but uses the
        OSI ping program instead. No multiple ping program for
        OSI sites has been developed at this time. The only
        requirement is that the system's ping program output
        match the typical BSD IP ping program's output.

nsmon
        which monitors the nameservers (named) on the list of
        specified hosts. It periodically sends an SOA query for
        the default domain and if the queried nameservers
        cannot resolve the query, then the site is elevated to
        CRITICAL status.

tpmon
        For monitoring the throughput (kbits per second) to a
        list of hosts. The program connects to the discard
        socket on the remote machine (using a STREAM socket)
        and sends large packets for a small amount of time to
        evaluate the effective throughput. It elevates a site
        to WARNING level if the throughput drops below a
        certain threshold (set in the configuration file).

trapmon
        Converts all SNMP traps into a format suitable for
        displaying using NOCOL. The severity of the various
        traps is preset (and can be changed during compilation
        time).

PLATFORM
        Any Unix system with the curses screen management library
        and IP (Internet Protocol) programming facility. It has been
        tested on Sun Sparc 4.1.1, Ultrix, and NeXT systems. Porting
        to other platforms might require minor adjustments depending
        on the vagaries of the different vendors (mostly in the
        include files).

AVAILABILITY
        NOCOL was developed at JvNCnet and has been in use for
        monitoring the JvNCnet wide area network since 1989.
        It is available via anonymous FTP from ftp.jvnc.net under
        pub/jvncnet-packages/nocol.tar.Z. The system running at

JvNCet can be viewed by logging into the host nocol.jvnc.net
with username nocol (an rlogin instead of telnet will handle
your X window terminal types better).
To be added to the NOCOL mailing list (for future updates
and bug fixes), send a message to nocol-users-
request@jvnc.net with your email address.

FUTURE DEVELOPMENTS

Possible future enhancements are:

1. Event logging.

2. Addition of an automated troubleshooting mechanism
   when a site severity level reaches a particular
   level.

3. SNMP monitors to watch the state of certain vari-
   ables (interface errors, packet rate, route state
   changes).

AUTHOR
     The software was developed at JvNCnet over a period of time.
     The overall design and initial development was done by Vikas
     Aggarwal and Sze-Ying Wuu. Additional development is being
     done and coordinated by Vikas Aggarwal (vikas@jvnc.net).
     Copyright 1992 JvNCnet. (See the file COPYRIGHT for full
     details)

SEE ALSO
     nocol(1) nocol(3) tpmon(8) tsmon(8) nsmon(8)

Internet Tool Catalog   NPRV

NAME
     NPRV -- IP Node/Protocol Reachability Verifier

KEYWORDS
     map, routing, status; IP; ping; VMS; free.

ABSTRACT
     NPRV is a full-screen, keypad-oriented utility that
     runs under VAX/VMS. It allows the user to quickly scan
     through a user-defined list of IP addresses (or domain
     names) and verify a node's reachability. The node's
     reachability is determined by performing an ICMP echo,
     UDP echo and a TCP echo at alternating three second
     intervals. The total number of packets sent and
     received are displayed, as well as the minimum, average
     and maximum round-trip times (in milliseconds) for each
     type of echo. Additionally, a "trace route" function
     is performed to determine the path from the local sys-
     tem to the remote host. Once all of the trace route
     information has filled the screen, a "snapshot" of the
     screen can be written to a text file. Upon exiting the
     utility, these text files can be used to generate a
     logical network map showing host and gateway intercon-
     nectivity.

MECHANISM
     The ICMP echo is performed by sending ICMP ECHO REQUEST
     packets. The UDP and TCP echoes are performed by con-
     necting to the UDP/TCP echo ports (port number 7). The
     trace route information is compiled by sending alter-
     nating ICMP ECHO REQUEST packets and UDP packets with
     very large destination UDP port numbers (in two
     passes). Each packet is initially sent with a TTL
     (time to live) of 1. This should cause an ICMP TIME
     EXCEEDED error to be generated by the first routing
     gateway. Then each packet is sent with a TTL of 2.
     This should cause an ICMP TIME EXCEEDED error to be
     generated by the second routing gateway. Then each
     packet is sent with a TTL of 3, and so on. This pro-
     cess continues until an ICMP ECHO REPLY or UDP PORT
     UNREACHABLE is received. This indicates that the
     remote host has been reached and that the trace route
     information is complete.

CAVEATS
     This utility sends one echo packet per second (ICMP,
     UDP or TCP), as well as sending out one trace route
     packet per second. If a transmitted trace route packet
     is returned in less than one second, another trace
     route packet is sent in 100 milliseconds. This could
     cause a significant amount of contention on the local
     network.

BUGS
     None known. Please report any discovered bugs to the
     author at:
          Allen Sturtevant
          National Magnetic Fusion Energy Computer Center
          Lawrence Livermore National Laboratory
          P.O. Box 808; L-561
          Livermore, CA 94550
          Phone : (415) 422-8266
          E-Mail: sturtevant@ccc.nmfecc.gov

LIMITATIONS
     The user is required to have SYSPRV privilege to per-
     form the ICMP Echo and trace route functions. The
     utility will still run with this privilege disabled,
     but only the UDP Echo and TCP Echo information will be
     displayed. This utility is written in C, but unfor-
     tunately it cannot be easily ported over to UNIX since
     many VMS system calls are used and all screen I/O is
     done using the VMS Screen Management Routines.

HARDWARE REQUIRED
     Any network interface supported by TGV Incorporated's
     MultiNet software.

SOFTWARE REQUIRED
     VAX/VMS V5.1+ and TGV Incorporated's MultiNet version
     2.0.

AVAILABILITY
     For executables only, FTP to the ANONYMOUS account
     (password GUEST) on CCC.NMFECC.GOV (128.55.128.30) and
     GET the following files:

     [ANONYMOUS.PROGRAMS.NPRV]NPRV.DOC   (ASCII text)
     [ANONYMOUS.PROGRAMS.NPRV]NPRV.EXE   (binary)
     [ANONYMOUS.PROGRAMS.NPRV]SAMPLE.IPA   (ASCII text)

Internet Tool Catalog   NSLOOKUP

NAME
        nslookup

KEYWORDS
        status; DNS, BIND; UNIX, VMS; free.

ABSTRACT
        Nslookup is an interactive program for querying
        Internet Domain Name System (DNS) servers. It is
        essentially a user-friendly front end to
        the BIND "resolver" library routines.

        This program is useful for converting a hostname
        into an IP address (and vice versa), determining
        the name servers for a domain , listing
        the contents of a domain, displaying any type of
        DNS record, such as MX, CNAME, SOA, etc.,
        diagnosing name server problems.

        By default, nslookup will query
        the default name server but you can specify a
        different server on the command line or from a
        configuration file. You can also specify
        different values for the options that control the
        resolver routines.

MECHANISM
        The program formats, sends and receives DNS
        (RFC 1034) queries.

CAVEATS
         None.

BUGS
        None known.

LIMITATIONS
        None known.

HARDWARE REQUIRED
        No restrictions.

SOFTWARE REQUIRED
        BSD UNIX or related OS, or VMS.

AVAILABILITY
          NSLookup is included in the BIND distribution.

          Available via anonymous FTP from uunet.uu.net,
          in directory /networking/ip/dns/bind. Available
          with 4.xBSD UNIX and related operating systems.
          For VMS, available as part of TGV MultiNet IP
          software package, as well as Wollongong's WIN/TCP.

Internet Tool Catalog   OSITRACE

NAME
     OSITRACE

KEYWORDS
     traffic; OSI; eavesdrop; UNIX; free.

ABSTRACT
     OSITRACE is a network performance tool that displays
     information about ISO TP4 connections. One line of
     output is displayed for each packet indicating the
     time, source, destination, length, packet type,
     sequence number, credit, and any optional parameters
     contained in the packet. Numerous options are avail-
     able to control the output of OSITRACE.

     To obtain packets to analyze, OSITRACE uses Sun
     Microsystems' Network Interface Tap (NIT) in SunOS 3.4,
     3.5, and 4.0.X. OSITRACE may also obtain data from the
     NETMON utility which is described as another tool
     entry.

     In Sun systems, OSITRACE may be easily installed: OSI
     kernel support is not needed, nor is any other form of
     OSI software support.

MECHANISM
     This tool has been designed in such a way that code to
     process different protocol suites may be easily added.
     As such, OSITRACE also has the ability to trace the DOD
     TCP protocols.

CAVEATS
     None.

BUGS
     Bug reports and questions should be addressed to: ie-
     tools@gateway.mitre.org

     Requests to join this mailing list: ie-tools-
     request@gateway.mitre.org

     Questions and suggestions can also be directed to: Greg
     Hollingsworth, gregh@gateway.mitre.org

LIMITATIONS
     None reported.

HARDWARE REQUIRED
     No restriction.

SOFTWARE REQUIRED
     SunOS 3.4, 3.5, or 4.0.X, or BSD UNIX-like network pro-
     tocols with NETMON installed.

AVAILABILITY
     OSITRACE is copyrighted by the MITRE-Washington Net-
     working Center, but freely distributed "as is." It re-
     quires retention of a copyright text in code derived
     from it. The distribution is available by anonymous
     FTP in pub/pdutrace.tar or pub/pdutrace.tar.Z from
     aelred-3.ie.org.

Internet Tool Catalog   OVERVIEW

NAME
     OverVIEW

KEYWORDS
     manager, status; IP; NMS, SNMP; DOS.

ABSTRACT
     Network and internet monitor; Performance monitor;
     Fully Graphic user interface; Event logging; TFTP boot
     server

MECHANISM
     OverVIEW uses SNMP to query routers, gateways and
     hosts. Also supports SGMP, PING and is committed to
     CMIP/CMOT. The SNMP queries allow dynamic determina-
     tion of configuration and state. Sets of related
     queries allows monitoring of congestion and faults.
     The hardware and software are sold as an integrated
     package.

CAVEATS
     None.

BUGS
     None known.

LIMITATIONS
     256 nodes, 256 nets

HARDWARE REQUIRED
     80286, 640K, EGA, mouse.

SOFTWARE REQUIRED
     MS-DOS, OverVIEW, Network kernel, Mouse driver, SNMP
     agents for monitored devices.

AVAILABILITY
     Fully supported product of Proteon, Inc. For more
     information, contact:
          Proteon, Inc.   Phone: (508) 898-2800
          2 Technology Drive   Fax: (508) 366-8901
          Westborough, MA 01581   Telex: 928124

Internet Tool Catalog   PING

NAME
     ping

KEYWORDS
     generator, status; IP; ping; DOS, UNIX, VMS; free.

ABSTRACT
     Ping is perhaps the most basic tool for internet
     management. It verifies that a remote IP implementa-
     tion and the intervening networks and interfaces are
     functional. It can be used to measure round trip
     delay. Numerous versions of the ping program exist.

MECHANISM
     Ping is based on the ICMP ECHO_REQUEST message.

CAVEATS
     If run repeatedly, ping could generate high system
     loads.

BUGS
     None known.

LIMITATIONS
     PC/TCP's ping is the only implementation known support
     both loose and strict source routing. Though some ping
     implementations support the ICMP "record route"
     feature, the usefulness of this option for debugging
     routes is limited by the fact that many gateways do not
     correctly implement it.

HARDWARE REQUIRED
     No restrictions.

SOFTWARE REQUIRED
     None.

AVAILABILITY
     Ping is widely included in TCP/IP distributions. Pub-
     lic domain versions of ping are available via anonymous
     FTP from uunet.uu.net, in directory bsd-
     sources/src/etc, and from venera.isi.edu, in directory
     pub.

Internet Tool Catalog   PROCESS-TCPWARE-SNMP

NAME
        SNMP agent

KEYWORDS
        alarm, manager, status, traffic; IP; SNMP; VMS;.

ABSTRACT
        The SNMP agent listens for and responds to network
        management requests sent from SNMP-conforming network
        management stations. The SNMP agent also sends SNMP
        traps, under specific conditions, to identified trap
        receivers. SNMP communities and generation of traps
        are fully configurable. The SNMP agent supports all
        MIB-II variables except the EGP group.

MECHANISM
        Network management variables are made available for
        inspection and/or alteration by means of the Simple
        Network Management Protocol (SNMP).

CAVEATS
        None.

BUGS
        No known bugs.

LIMITATIONS
        Does not yet provide the ability for sites to add
        extra MIB definitions.

HARDWARE REQUIRED
        Supported VAX processors.

SOFTWARE REQUIRED
        VMS V4 or later

AVAILABILITY
        The SNMP agent is included in TCPware for VMS, a
        commercial product available under license from:
                Process Software Corporation
                959 Concord Street
                Framingham, MA 01701
                +1 800 722 7770, +1 508 879 6994 (voice)
                +1 508 879-0042 (FAX)   TELEX 517891
                sales@process.com

Internet Tool Catalog   PROXYD

NAME
        proxyd -- SNMP proxy agent daemons from SNMP Research.

KEYWORDS
        control, management, status;
        bridge, Ethernet, IP, OSI, ring, star;
        NMS, SNMP;
        UNIX;
        library, sourcelib.

ABSTRACT
        SNMP proxy agents may be used to permit the monitoring
        and controlling of network elements which are otherwise
        not addressable using the SNMP management protocol
        (e.g., a network bridge that implements a proprietary
        management protocol). Similarly, SNMP proxy agents may
        be used to protect SNMP agents from redundant network
        management agents through the use of caches. Finally,
        SNMP proxy agents may be used to implement elaborate
        MIB access policies.

        The proxy agent daemon:

        - listens for SNMP queries and commands from logically
          remote network management stations,
        - translates and retransmits those as appropriate
          network management queries or cache lookups,
        - listens for and parses the responses,
        - translates the responses into SNMP responses, and
        - returns those responses as SNMP messages to the
          network management station that originated the
          transaction.

        The proxy agent daemon also emits SNMP traps to
        identified trap receivers. The proxy agent daemon is
        designed to make the addition of additional vendor-
        specific variables a straight-forward task. The proxy
        application comes complete with source code including a
        powerful set of portable libraries for generating and
        parsing SNMP messages and a set of command line utilities.

MECHANISM
        Network management variables are made available for
        inspection and/or alteration by means of the Simple
        Network Management Protocol (SNMP).

CAVEATS
        None.

BUGS
        None known.

LIMITATIONS
        This application is a template for proxy application
        writers.

        Only a few of the many LanBridge 100 variables are
        supported.

HARDWARE REQUIRED
        System from Sun Microsystems, Incorporated.

SOFTWARE REQUIRED
        Sun OS 3.5 or 4.x.

AVAILABILITY AND CONTACT POINT FOR INFORMATION ABOUT THIS TOOL
        This is a commercial product available under license
        from:
                SNMP Research
                3001 Kimberlin Heights Road
                Knoxville, TN 37920-9716
                Attn: John Southwood, Sales and Marketing
                (615) 573-1434 (Voice) (615) 573-9197 (FAX)

CONTACT POINT FOR CHANGES TO THIS CATALOG ENTRY
                users@seymour1.cs.utk.edu

Internet Tool Catalog   PROXYD_SNMP_RESEARCH

NAME
        proxyd -- SNMP proxy agent daemons from SNMP Research.

KEYWORDS
        control, management, status;
        bridge, Ethernet, IP, OSI, ring, star;
        NMS, SNMP;
        UNIX;
        library, sourcelib.

ABSTRACT
        SNMP proxy agents may be used to permit the monitoring
        and controlling of network elements which are otherwise
        not addressable using the SNMP management protocol
        (e.g., a network bridge that implements a proprietary
        management protocol). Similarly, SNMP proxy agents may
        be used to protect SNMP agents from redundant network
        management agents through the use of caches. Finally,
        SNMP proxy agents may be used to implement elaborate
        MIB access policies.

        The proxy agent daemon:

        - listens for SNMP queries and commands from logically
          remote network management stations,
        - translates and retransmits those as appropriate
          network management queries or cache lookups,
        - listens for and parses the responses,
        - translates the responses into SNMP responses, and
        - returns those responses as SNMP messages to the
          network management station that originated the
          transaction.

        The proxy agent daemon also emits SNMP traps to
        identified trap receivers. The proxy agent daemon is
        designed to make the addition of additional vendor-
        specific variables a straight-forward task. The proxy
        application comes complete with source code including a
        powerful set of portable libraries for generating and
        parsing SNMP messages and a set of command line utilities.

MECHANISM
        Network management variables are made available for
        inspection and/or alteration by means of the Simple
        Network Management Protocol (SNMP).

        CAVEATS
                None.

        BUGS
                None known.

        LIMITATIONS
                This application is a template for proxy application
                writers.

                Only a few of the many LanBridge 100 variables are
                supported.

        HARDWARE REQUIRED
                System from Sun Microsystems, Incorporated.

        SOFTWARE REQUIRED
                Sun OS 3.5 or 4.x.

        AVAILABILITY AND CONTACT POINT FOR INFORMATION ABOUT THIS TOOL
            This is a commercial product available under license
            from:
                SNMP Research
                3001 Kimberlin Heights Road
                Knoxville, TN 37920-9716
                Attn: John Southwood, Sales and Marketing
                (615) 573-1434 (Voice) (615) 573-9197 (FAX)

        CONTACT POINT FOR CHANGES TO THIS CATALOG ENTRY
                users@seymour1.cs.utk.edu

Internet Tool Catalog   QUERY

NAME
     query, ripquery

KEYWORDS
     routing; IP; spoof; UNIX; free.

ABSTRACT
     Query allows remote viewing of a gateway's routing
     tables.

MECHANISM
     Query formats and sends a RIP request or POLL command
     to a destination gateway.

CAVEATS
     Query is intended to be used a a tool for debugging
     gateways, not for network management. SNMP is the pre-
     ferred protocol for network management.

BUGS
     None known.

LIMITATIONS
     The polled gateway must run RIP.

HARDWARE REQUIRED
     No restriction.

SOFTWARE REQUIRED
     4.3BSD UNIX or related OS.

AVAILABILITY
     Available with routed and gated distributions.

     Routed may be obtained via anonymous FTP from
     uunet.uu.net, in file bsd-
     sources/src/network/routed.tar.Z.

     Gated may be obtained via anonymous FTP from
     devvax.tn.cornell.edu. Distribution files are in
     directory pub/gated.

Internet Tool Catalog   SAS-CPE

NAME
        SAS/CPE(tm) for Open Systems Software

KEYWORDS
        manager, status;
        bridge, ethernet, FDDI, IP, OSI, NFS;
        X;
        DOS, HP, UNIX;
        library.

ABSTRACT
SAS/CPE(tm) for Open Systems software is an integrated system designed
to facilitate the analysis and presentation of computer performance
and resource utilization data. SAS/CPE software features include:

    . Processing of raw computer and network performance data into
      detail-level SAS data sets.
    . Conversion and validation of logged data values to forms
      more useful for display and analysis (e.g., I/O counts
      are converted to I/O rates per second).
    . Numerous sample reports on performance data processed by
      SAS/CPE software.
    . Reduction of logged performance data into daily, weekly,
      monthly or yearly summarized values.
    . Menu-driven interface to the creation and management of multiple
      performance data bases.
    . Menu-driven report designing interface that allows users with no
      programming knowledge to create and manage custom reports from
      their performance data base. No SAS coding is needed for this
      interface.

MECHANISM
        SAS/CPE for Open Systems processes and reports data
        from SNMP and other proprietary monitoring protocols,
        as well as du and accounting.

CAVEATS
        The product is currently in alpha testing.

BUGS
        None known.

LIMITATIONS
        None reported.

HARDWARE REQUIRED
        HP, SUN or IBM Workstation

SOFTWARE REQUIRED
        The SAS(r) System Base Software, SAS/GRAPH Software and
        SAS/CPE for Open System Software

AVAILABILITY AND CONTACT POINT FOR INFORMATION ABOUT THIS TOOL
        SAS/CPE for Open Systems Software is available from:
            SAS Institute Inc.
            SAS Campus Drive
            Cary, NC 27513
            Phone 919-677-8000
            FAX 919-677-8123

CONTACT POINT FOR CHANGES TO THIS CATALOG ENTRY
        Send email to snodjs@mvs.sas.com.

Internet Tool Catalog   SNIFFER

NAME
     Sniffer

KEYWORDS
     analyzer, generator, traffic; DECnet, ethernet, IP,
     NFS, OSI, ring, SMTP, star; eavesdrop; standalone.

ABSTRACT
     The Network General Sniffer is a protocol analyzer for
     performing LAN diagnostics, monitoring, traffic genera-
     tion, and troubleshooting. The Sniffer protocol
     analyzer has the capability of capturing every packet
     on a network and of decoding all seven layers of the
     OSI protocol model. Capture frame selection is based
     on several different filters: protocol content at lower
     levels; node addresses; pattern matching (up to 8
     logically-related patterns of 32 bytes each); and des-
     tination class. Users may extend the protocol
     interpretation capability of the Sniffer by writing
     their own customized protocol interpreters and linking
     them to the Sniffer software.

     The Sniffer displays network traffic information and
     performance statistics in real time, in user-selectable
     formats. Numeric station addresses are translated to
     symbolic names or manufacturer ID names. Network
     activities measured include frames accepted, Kbytes
     accepted, and buffer use. Each network version has
     additional counters for activities specific to that
     network. Network activity is expressed as
     frames/second, Kbytes/second, or per cent of network
     bandwidth utilization.

     Data collection by the Sniffer may be output to printer
     or stored to disk in either print-file or spread-sheet
     format.

     Protocol suites understood by the Sniffer include:
     Banyan Vines, IBM Token-Ring, Novell Netware, XNS/MS-
     Net (3Com 3+), DECnet, TCP/IP (including SNMP and
     applications-layer protocols such as FTP, SMTP, and
     TELNET), X Windows (for X version 11), NFS, and several
     SUN proprietary protocols (including mount, pmap, RPC,
     and YP). Supported LANs include: ethernet, Token-ring
     (4Mb and 16Mb versions), ARCNET, StarLAN, IBM PC Net-
     work (Broadband), and Apple Localtalk Network.

MECHANISM
     The Sniffer is a self-contained, portable protocol
     analyzer that require only AC line power and connection
     to a network to operate. Normally passive (except when
     in Traffic Generator mode), it captures images of all
     or of selected frames in a working buffer, ready for
     immediate analysis and display.

     The Sniffer is a standalone device. Two platforms are
     available: one for use with single network topologies,
     the other for use with multi-network topologies. Both
     include Sniffer core software, a modified network
     interface card (or multiple cards), and optional proto-
     col interpreter suites.

     All Sniffer functions may be remotely controlled from a
     modem-connected PC. Output from the Sniffer can be
     imported to database or spreadsheet packages.

CAVEATS
     In normal use, the Sniffer is a passive device, and so
     will not adversely effect network performance. Perfor-
     mance degradation will be observed, of course, if the
     Sniffer is set to Traffic Generator mode and connected
     to an active network.

BUGS
     None known.

LIMITATIONS
     None reported.

HARDWARE REQUIRED
     None. The Sniffer is a self-contained unit, and
     includes its own interface card. It installs into a
     network as would any normal workstation.

SOFTWARE REQUIRED
     None.

         AVAILABILITY
             The Sniffer is available commercially. For information
             on your local representative, call or write:
                 Network General Corporation
                 4200 Bohannon Drive
                 Menlo Park, CA 94025
                 Phone: 415-688-2700
                 Fax: 415-321-0855

             For acquisition by government agencies, the Sniffer is
             included on the GSA schedule.

Internet Tool Catalog   SNMP_DEVELOPMENT_KIT

NAME
     The SNMP Development Kit

KEYWORDS
     manager, status; IP; NMS, SNMP; UNIX; free, sourcelib.

ABSTRACT
     The SNMP Development Kit comprises C Language source
     code for a programming library that facilitates access
     to the management services of the SNMP (RFC 1098).
     Sources are also included for a few simple client
     applications whose main purpose is to illustrate the
     use of the library. Example client applications query
     remote SNMP agents in a variety of modes, and generate
     or collect SNMP traps. Code for an example SNMP agent
     that supports a subset of the Internet MIB (RFC 1066)
     is also included.

MECHANISM
     The Development Kit facilitates development of SNMP-
     based management applications -- both clients and
     agents. Example applications execute SNMP management
     operations according to the values of command line
     arguments.

CAVEATS
     None.

BUGS
     Fixed in the next release.

LIMITATIONS
     None reported.

HARDWARE REQUIRED
     The SNMP library source code is highly portable and
     runs on a wide range of platforms.

SOFTWARE REQUIRED
     The SNMP library source code has almost no operating
     system dependencies and runs in a wide range of
     environments. Certain portions of the example SNMP
     agent code are specific to the 4.3BSD implementation of
     the UNIX system for the DEC MicroVAX.

AVAILABILITY
        The Development Kit is available via anonymous FTP from
        host allspice.lcs.mit.edu. The copyright for the
        Development Kit is held by the Massachusetts Institute
        of Technology, and the Kit is distributed without
        charge according to the terms set forth in its code and
        documentation. The distribution takes the form of a
        UNIX tar file.

        Bug reports, questions, suggestions, or complaints may
        be mailed electronically to snmp-dk@ptt.lcs.mit.edu,
        although no response in any form is guaranteed. Dis-
        tribution via UUCP mail may be arranged by contacting
        the same address. Requests for hard-copy documentation
        or copies of the distribution on magnetic media are
        never honored.

Internet Tool Catalog   SNMP_Libraries_SNMP_RESEARCH

NAME
          SNMP Libraries and Utilities from SNMP Research.

KEYWORDS
          alarm, control, manager, map, security, status;
          bridge, DECnet, Ethernet, FDDI, IP, OSI, ring, star;
          NMS, SNMP;
          DOS, UNIX, VMS;
          sourcelib.

ABSTRACT
          The SNMP Libraries and Utilities serve two purposes:

          1)   to act as building blocks for the construction of
                SNMP-based agent and manager applications; and

          2)   to act as network management tools for network
                fire fighting and report generation.

          The libraries perform ASN.1 parsing and generation tasks
          for both network management station applications and
          network management agent applications. These libraries
          hide the details of ASN.1 parsing and generation from
          application writers and make it unnecessary for them to
          be expert in these areas. The libraries are very robust
          with considerable error checking designed in. The
          several command line utilities include applications for
          retrieving one or many variables, retrieving tables, or
          effecting commands via the setting of remote network
          management variables.

MECHANISM
          The parsing is performed via recursive descent methods.
          Messages are passed via the Simple Network Management
          Protocol (SNMP).

CAVEATS
          None.

BUGS
          None known.

LIMITATIONS
          The monitored and managed nodes must implement the SNMP
          over UDP per RFC 1157 or must be reachable via a proxy
          agent.

    HARDWARE REQUIRED
            This software has been ported to numerous platforms
            including workstations, general-purpose timesharing
            systems, and embedded hardware in intelligent network
            devices such as repeaters, bridges, and routers.

    SOFTWARE REQUIRED
            C compiler, TCP/IP library.

    AVAILABILITY AND CONTACT POINT FOR INFORMATION ABOUT THIS TOOL
            This is a commercial product available under license
            from:
                    SNMP Research
                    3001 Kimberlin Heights Road
                    Knoxville, TN 37920-9716
                    Attn: John Southwood, Sales and Marketing
                    (615) 573-1434 (Voice) (615) 573-9197 (FAX)

    CONTACT POINT FOR CHANGES TO THIS CATALOG ENTRY
            users@seymour1.cs.utk.edu

Internet Tool Catalog   SNMP_PACKAGED_AGENT_SNMP_RESEARCH

NAME
        SNMP Packaged Agent System -- an SNMP host/gateway
        agent daemon including a complete protocol stack and
        runtime environment required to support an SNMP Agent
        from SNMP Research.

KEYWORDS
        control, manager, status;
        bridge, Ethernet, FDDI, IP, OSI, ring, star;
        NMS, SNMP;
        DOS, standalone, UNIX;
        sourcelib.

ABSTRACT
        The snmpd agent daemon listens for and responds to
        network management queries and commands from logically
        remote network management stations. The agent daemon
        also emits SNMP traps to identified trap receivers.
        The agent daemon is designed to make the addition of
        additional vendor-specific variables a
        straight-forward task. The snmpd application comes
        complete with source code including a powerful set of
        portable libraries for generating and parsing SNMP
        messages and a set of command line utilities.

        The Packaged Agent System is designed to aid the
        hardware manufacturer who is not experienced with the
        TCP/IP protocol suite. A lightweight, non-preemptive
        scheduler/tasking system for faster execution and less
        impact on slow CPUs is included in the package.
        Development environment is either MS DOS or UNIX.

MECHANISM
        Network management variables are made available for
        inspection and/or alteration by means of the Simple
        Network Management Protocol (SNMP).

CAVEATS
        None.

BUGS
        None known.

LIMITATIONS
        None reported.

HARDWARE REQUIRED
        The Motorola 68XXX and the Intel 8088 and X86
        platforms are fully supported. Other platforms can be
        supported. Contact SNMP Research for details.

        This software has been ported to numerous platforms
        including workstations, general-purpose timesharing
        systems, and embedded hardware in intelligent network
        devices such as repeaters, bridges, and routers.

SOFTWARE REQUIRED
        C compiler.

AVAILABILITY AND CONTACT POINT FOR INFORMATION ABOUT THIS TOOL
        This is a commercial product available under license
        from:
                SNMP Research
                3001 Kimberlin Heights Road
                Knoxville, TN 37920-9716
                Attn: John Southwood, Sales and Marketing
                (615) 573-1434 (Voice) (615) 573-9197 (FAX)

CONTACT POINT FOR CHANGES TO THIS CATALOG ENTRY
                users@seymour1.cs.utk.edu

Internet Tool Catalog   SNMPD_SNMP_RESEARCH

NAME
        snmpd -- an SNMP host/gateway agent daemon from SNMP
        Research.

KEYWORDS
        control, mananger, status;
        bridge, Ethernet, FDDI, IP, OSI, ring, star;
        NMS, SNMP;
        DOS, UNIX;
        sourcelib.

ABSTRACT
        The snmpd agent daemon listens for and responds to
        network management queries and commands from logically
        remote network management stations. The agent daemon
        also emits SNMP traps to identified trap receivers. The
        agent daemon is architected to make the addition of
        additional vendor-specific variables a straight-forward
        task. The snmpd application comes complete with source
        code including a powerful set of portable libraries for
        generating and parsing SNMP messages and a set of
        command line utilities.

MECHANISM
        Network management variables are made available for
        inspection and/or alteration by means of the Simple
        Network Management Protocol (SNMP).

CAVEATS
        None.

BUGS
        None known.

LIMITATIONS
        Only operating system variables available without
        source code modifications to the operating system and
        device device drivers are supported.

HARDWARE REQUIRED
        This software has been ported to numerous platforms
        including workstations, general-purpose timesharing
        systems, and embedded hardware in intelligent network
        devices such as repeaters, bridges, and routers.

SOFTWARE REQUIRED
        C compiler.

AVAILABILITY AND CONTACT POINT FOR INFORMATION ABOUT THIS TOOL
        This is a commercial product available under license
        from:
                SNMP Research
                3001 Kimberlin Heights Road
                Knoxville, TN 37920-9716
                Attn: John Southwood, Sales and Marketing
                (615) 573-1434 (Voice) (615) 573-9197 (FAX)

CONTACT POINT FOR CHANGES TO THIS CATALOG ENTRY
                users@seymour1.cs.utk.edu

Internet Tool Catalog   SPIDERMONITOR

NAME
     SpiderMonitor P220, K220 and
     SpiderAnalyzer P320, K320

KEYWORDS
     alarm, analyzer, generator, traffic; DECnet, ethernet,
     IP, OSI; eavesdrop; standalone; sourcelib.

ABSTRACT
     The SpiderMonitor and SpiderAnalyzer are protocol
     analyzers for performing ethernet LAN diagnostics, mon-
     itoring, traffic generation, and troubleshooting. The
     SpiderMonitor has the capability of capturing every
     packet on a network and of decoding the first four
     layers of the OSI protocol model. The SpiderAnalyzer
     has additional software for decoding higher protocol
     layers. Protocol suites understood: TCP/IP (including
     SNMP and applications-layer protocols), OSI, XNS, DEC-
     net and IPX. User-definable decodes can be written in
     'C' with the Microsoft version 5.0 'C' compiler. A
     decode guide is provided.

     The SpiderAnalyzer supports multiple simultaneous
     filters for capturing packets using predefined patterns
     and error states. Filter patterns can also trigger on
     NOT matching 1 or more filters, an alarm, or a speci-
     fied time.

     The SpiderAnalyzer can also employ TDR (Time Domain
     Reflectometry) to find media faults, open or short cir-
     cuits, or transceiver faults. It can transmit OSI,
     XNS, and Xerox link-level echo packets to user-
     specified stations, performs loop round tests.

     In traffic generation mode, the SpiderAnalyzer has the
     ability to generate packets at random intervals of ran-
     dom lengths or any combination of random or fixed
     interval or length, generation of packets with CRC
     errors, or packets that are too short, or packets that
     are too long.

     Output from the SpiderMonitor/Analyzer can be imported
     to database or spreadsheet packages.

MECHANISM
     The SpiderMonitor and Spider Analyzer are available as
     stand-alone, IBM PC compatible packages based upon a
     Compaq III portable system, or as a plug-in boards for
     any IBM XT/AT compatible machine. The model 220 (Spi-
     derMonitor) systems provide a functional base suited
     for most network management needs. The model 320 (Spi-
     derAnalyzer) systems provide extended functionality in
     the development mode and traffic generation mode as
     well more filtering capabilities than the 220 models.

CAVEATS
     Traffic generation will congest an operational ether-
     net.

BUGS
     None known.

LIMITATIONS
     Monitoring of up to 1024 stations and buffering of up
     to 1500 packets. The model 220 provides for 3 filters
     with a filter depth of 46 bytes. The model 320 pro-
     vides for 4 filters and a second level of filtering
     with a filter depth of 64 bytes.

HARDWARE REQUIRED
     PX20s are self contained, the KX20s require an IBM
     PC/XT-AT compatible machine with 5 megabytes of hard
     disk storage and the spare slot into which the board
     kit is plugged.

SOFTWARE REQUIRED
     None. The SpiderAnalyzer requires the Microsoft 'C'
     Compiler, Version 5.0 for writing user defined decodes.

AVAILABILITY
     The SpiderMonitor/Analyzer is available commercially.
     For information on your local representative, call or
     write:
          Spider Systems, Inc.
          12 New England Executive Park
          Burlington, MA 01803
          Telephone: 617-270-3510
          FAX: 617-270-9818

Internet Tool Catalog   SPIMS

NAME
         SPIMS -- the Swedish Institute of Computer Science
                  (SICS) Protocol Implementation Measurement
                  System tool.

KEYWORDS
         benchmark, debugger; IP, OSI; spoof; UNIX.

ABSTRACT
         SPIMS is used to measure the performance of protocol
         and "protocol-like" services including response time
         (two-way delay), throughput and the time to open and
         close connections. It has been used to:

         o   benchmark alternative protocol implementations,

         o   observe how performance varies when parameters in
                 specific implementations have been varied (i.e.,
                 to tune parameters).

         SPIMS currently has interfaces to the DoD Internet Pro-
         tocols: UDP, TCP, FTP, SunRPC, the OSI protocols from
         the ISODE 4.0 distribution package: FTAM, ROSE, ISO TP0
         and to Sunlink 5.2 ISO TP4 as well as Stanford's VMTP.
         Also available are a rudimentary set of benchmarks,
         stubs for new protocol interfaces and a user manual.

         For an example of the use of SPIMS to tune protocols,
         see:
                 Nordmark & Cheriton, "Experiences from VMTP: How
                 to achieve low response time," IFIP WG6.1/6.4:
                 Protocols for High-Speed Networks, May 1989,
                 Zurich. To be published.

         For an example of how SPIMS can be used to benchmark
         protocols, see:

                 Gunningberg, Bjorkman, Nordmark, Sjodin, Pink &
                 Stromqvist "Application Protocols and Performance
                 Benchmarks", IEEE Communications Magazine, June
                 1989, Vol. 27, No.6, pp 30-36.

                 Sjodin, Gunningberg, Nordmark, & Pink, "Towards
                 Protocol Benchmarks', IFIP WG6.1/6.4 Protocols
                 for High-Speed Networks, May 1989, Zurich, pp
                 57-67

MECHANISM
        SPIMS runs as user processes and uses a TCP connection
        for measurement set-up. Measurements take place
        between processes over the measured protocol. SPIMS
        generates messages and transfers them via the measured
        protocol service according to a user-supplied specifi-
        cation. SPIMS has a unique measurement specification
        language that is used to specify a measurement session.
        In the language there are constructs for different
        application types (e.g., bulk data transfer), for
        specifying frequency and sequence of messages, for dis-
        tribution over message sizes and for combining basic
        specifications. These specifications are independent
        of both protocols and protocol implementations and can
        be used for benchmarking. For more details on the
        internals of SPIMS, see:

        Nordmark & Gunningberg, "SPIMS: A Tool for Protocol
        Implementation Performance Measurements" Proc. of 13:th
        Conf. on Local Computer Networks, Minneapolis 1989, pp
        222-229.

CAVEATS
        None.

BUGS
        None known.

LIMITATIONS
        None reported.

HARDWARE REQUIRED
        No restrictions.

SOFTWARE REQUIRED
        SPIMS is implemented on UNIX, including SunOS 4.,
        4.3BSD UNIX, DN (UNIX System V, with extensions) and
        Ultrix 2.0/3.0. It requires a TCP connection for meas-
        urement set-up. No kernel modifications or any modifi-
        cations to measured protocols are required.

AVAILABILITY AND CONTACT POINT FOR INFORMATION ABOUT THIS TOOL
        SPIMS is not in the public domain and the software is
        covered by licenses. Use of the SPIMS software
        represents acceptance of the terms and conditions of
        the licenses.
        The licenses are enclosed in the distribution package.
        Licenses and SPIMS cover letter can also be obtained
        via an Internet FTP connection without getting the whole
        software. The retrieval procedure is identical to the
        below university distribution via FTP. The file to
        retrieve is pub/spims-dist/licenses.tar.Z

        There are two different distribution classes depending on
        requesting organization:

        1. Universities and non-profit organizations.

        To these organizations, SPIMS source code is distributed
        free of charge. There are two ways to get the software:

                1. FTP.
                If you have an Internet FTP connection, you
                can use anonymous FTP to sics.se
                [192.16.123.90], and retrieve the file
                pub/spims-dist/dist910304.tar.Z
                (this is a .6MB compressed tar image) in
                BINARY mode. Log in as user anonymous and at
                the password prompt, use your complete
                electronic mail address.

                2. On a Sun 1/4-inch cartridge tape.
                For mailing, a handling fee of US$150.00 will be
                charged. Submit a bank check with the request.
                Do not send tapes or envelopes.

        2. Commercial organizations.

        These organizations can chose between a license for
        commercial use, or a license for internal research
        only and no commercial use whatsoever.

                For internal research use only:

                The SPIMS source code is distributed for a one
                time fee of US$500.00. Organizations
                interested in the research prototype need to
                contact us via e-mail and briefly motivate why
                they qualify (non-commercial use) for the

                      research prototype.
                      They will thereafter get a permission to
                      obtain a copy from the same distribution
                      source as for universities.

                      Commercial use:

                      A commercial version of SPIMS will eventually
                      be distributed and supported by a commercial
                      partner. nIn the meantime we will distribute
                      the research prototype (source code) to
                      interested organizations without any guaranty
                      or support. Contact SICS for further
                      information.

              For more information about the research prototype
              distribution and about a commercial license, contact:

                      Swedish Institute of Computer Science
                      Att: Birgitta Klingenberg
                      P.O. Box 1263
                      S-164 28 Kista
                      SWEDEN

                      e-address: spims@sics.se
                      Phone: +46-8-7521500, Fax: +46-8-7517230

         CONTACT POINT FOR CHANGES TO THIS CATALOG ENTRY
                 Bengt Ahlgren
                 Swedish Institute of Computer Science
                 Box 1263
                 S-164 28 KISTA, SWEDEN

                 Email: bengta@sics.se
                 Tel: +46 8 752 1562 (direct)
                   or   +46 8 752 1500
                 Fax: +46 8 751 7230

Internet Tool Catalog   SPRAY_SUN

NAME
     spray

KEYWORDS
     benchmark, generator; IP; ping; UNIX.

ABSTRACT
     Spray is a traffic generation tool that generates RPC
     or UDP packets, or ICMP Echo Requests. The packets are
     sent to a remote procedure call application at the des-
     tination host. The count of received packets is
     retrieved from the remote application after a certain
     number of packets have been transmitted. The differ-
     ence in packets received versus packets sent represents
     (on a LAN) the packets that the destination host had to
     drop due to increasing queue length. A measure of
     throughput relative to system speed and network load
     can thus be obtained.

MECHANISM
     See above.

CAVEATS
     Spray can congest a network.

BUGS
     None known.

LIMITATIONS
     None reported.

HARDWARE REQUIRED
     No restrictions.

SOFTWARE REQUIRED
     SunOS

AVAILABILITY
     Supplied with SunOS.

Internet Tool Catalog   TCPDUMP

NAME
     tcpdump

KEYWORDS
     traffic; ethernet, IP, NFS; UNIX, VMS; free.

ABSTRACT
     Tcpdump can interpret and print headers for the follow-
     ing protocols: ethernet, IP, ICMP, TCP, UDP, NFS, ND,
     ARP/RARP, AppleTalk. Tcpdump has proven useful for
     examining and evaluating the retransmission and window
     management operations of TCP implementations.

MECHANISM
     Much like etherfind, tcpdump writes a log file of the
     frames traversing an ethernet interface. Each output
     line includes the time a packet is received, the type
     of packet, and various values from its header.

CAVEATS
     None.

BUGS
     None known.

LIMITATIONS
     Public domain version requires a kernel patch for
     SunOS. TCPware for VMS - currently interprets headers
     for IP, TCP, UDP, and ICMP only.

HARDWARE REQUIRED
     Any Ultrix system (VAX or DEC RISC hardware)

SOFTWARE REQUIRED
     Ultrix release 4.0 or later. For Ultrix 4.1, may
     require the patched "if_ln.o" kernel module, available
     from Digital's Customer Support Center.

AVAILABILITY
        Available, though subject to copyright restrictions,
        via anonymous FTP from ftp.ee.lbl.gov. The source and
        documentation for the tool is in compressed tar format,
        in file tcpdump.tar.Z. Also available from
        spam.itstd.sri.com, in directory pub. For VMS hosts
        with DEC ethernet controllers, available as part of TGV
        MultiNet IP software package and TCPware for VMS from
        Process Software Corporation.

Internet Tool Catalog   TCPLOGGER

NAME
     tcplogger

KEYWORDS
     traffic; IP; eavesdrop; UNIX; free.

ABSTRACT
     Tcplogger consists of modifications to the 4.3BSD UNIX
     source code, and a large library of post-processing
     software. Tcplogger records timestamped information
     from TCP and IP packets that are sent and received on a
     specified connection. For each TCP packet, information
     such as sequence number, acknowledgement sequence
     number, packet size, and header flags is recorded. For
     an IP packet, header length, packet length and TTL
     values are recorded. Customized use of the TCP option
     field allows the detection of lost or duplicate pack-
     ets.

MECHANISM
     Routines of 4.3BSD UNIX in the netinet directory have
     been modified to append information to a log in memory.
     The log is read continuously by a user process and
     written to a file. A TCP option has been added to
     start the logging of a connection. Lots of post-
     processing software has been written to analyze the
     data.

CAVEATS
     None.

BUGS
     None known.

LIMITATIONS
     To get a log at both ends of the connection, the modi-
     fied kernel should be run at both the hosts.

     All connections are logged in a single file, but
     software is provided to filter out the record of a sin-
     gle connection.

HARDWARE REQUIRED
     No restrictions.

        SOFTWARE REQUIRED
             4.3BSD UNIX (as modified for this tool).

        AVAILABILITY
             Free, although a 4.3BSD license is required. Contact
             Olafur Gudmundsson (ogud@cs.umd.edu).

Internet Tool Catalog   TOKENVIEW_PROTEON

NAME
     TokenVIEW

KEYWORDS
     control, manager, status; ring; NMS, proprietary; DOS.

ABSTRACT
     Network Management tool for 4/16 Mbit IEEE 802.5 Token
     Ring Networks. Monitors active nodes and ring errors.
     Maintains database of nodes, wire centers and their
     connections. Separate network management ring allows
     remote configuration of wire centers.

MECHANISM
     A separate network management ring used with Proteon
     Intelligent Wire Centers allows wire center configura-
     tion information to be read and modified from a single
     remote workstation. A log of network events used with
     a database contain nodes, wire centers and their con-
     nections, facilitates tracking and correction of net-
     work errors. Requires an "E" series PROM, sold with
     package.

CAVEATS
     Currently, only ISA bus cards support the required E
     series PROM.

BUGS
     None known.

LIMITATIONS
     256 nodes, 1 net.

HARDWARE REQUIRED
     512K RAM, CGA or better, hard disk, mouse supported.

SOFTWARE REQUIRED
     MS-DOS, optional mouse driver

AVAILABILITY
     Fully supported product of Proteon, Inc. Previously
     sold as Advanced Network Manager (ANM). For more in-
     formation, contact:
          Proteon, Inc.   Phone: (508) 898-2800
          2 Technology Drive   Fax: (508) 366-8901
          Westborough, MA 01581   Telex: 928124

Internet Tool Catalog   TRACEROUTE

NAME
     traceroute

KEYWORDS
     routing; IP; ping; UNIX, VMS; free.

ABSTRACT
     Traceroute is a tool that allows the route taken by
     packets from source to destination to be discovered.
     It can be used for situations where the IP record route
     option would fail, such as intermediate gateways dis-
     carding packets, routes that exceed the capacity of an
     datagram, or intermediate IP implementations that don't
     support record route. Round trip delays between the
     source and intermediate gateways are also reported
     allowing the determination of individual gateways con-
     tribution to end-to-end delay.

     Enhanced versions of traceroute have been developed
     that allow specification of loose source routes for
     datagrams. This allows one to investigate the return
     path from remote machines back to the local host.

MECHANISM
     Traceroute relies on the ICMP TIME_EXCEEDED error
     reporting mechanism. When an IP packet is received by
     an gateway with a time-to-live value of 0, an ICMP
     packet is sent to the host which generated the packet.
     By sending packets to a destination with a TTL of 0,
     the next hop can be identified as the source of the
     ICMP TIME EXCEEDED message. By incrementing the TTL
     field the subsequent hops can be identified. Each
     packet sent out is also time stamped. The time stamp
     is returned as part of the ICMP packet so a round trip
     delay can be calculated.

CAVEATS
     Some IP implementations forward packets with a TTL of
     0, thus escaping identification. Others use the TTL
     field in the arriving packet as the TTL for the ICMP
     error reply, which delays identification.

     Sending datagrams with the source route option will
     cause some gateways to crash. It is considered poor
     form to repeat this behavior.

BUGS
     None known.

LIMITATIONS
     Most versions of UNIX have errors in the raw IP code
     that require kernel mods for the standard version of
     traceroute to work. A version of traceroute exists
     that runs without kernel mods under SunOS 3.5 (see
     below), but it only operates over an ethernet inter-
     face.

HARDWARE REQUIRED
     No restrictions.

SOFTWARE REQUIRED
     BSD UNIX or related OS, or VMS.

AVAILABILITY
     Available by anonymous FTP from ftp.ee.lbl.gov, in file
     traceroute.tar.Z. It is also available from
     uc.msc.umn.edu.

     A version of traceroute that supports Loose Source
     Record Route, along with the source code of the
     required kernel modifications and a Makefile for
     installing them, is available via anonymous FTP from
     zerkalo.harvard.edu, in directory pub, file
     traceroute_pkg.tar.Z.

     A version of traceroute that runs under SunOS 3.5 and
     does NOT require kernel mods is available via anonymous
     FTP from dopey.cs.unc.edu, in file
     ~ftp/pub/traceroute.tar.Z.

     For VMS, traceroute is available as part of TGV Mul-
     tiNet IP software package.

Internet Tool Catalog   TRPT

NAME
     TRPT -- transliterate protocol trace

KEYWORDS
     traffic; IP; eavesdrop; UNIX; free.

ABSTRACT
     TRPT displays a trace of a TCP socket events. When no
     options are supplied, TRPT prints all the trace records
     found in a system, grouped according to TCP connection
     protocol control block (PCB).

     An example of TRPT output is:

     38241 ESTABLISHED:input
     [e0531003..e0531203)@6cc5b402(win=4000)<ACK> -> ESTA-
     BLISHED
     38241 ESTABLISHED:user RCVD -> ESTABLISHED
     38266 ESTABLISHED:output
     6cc5b402@e0531203(win=4000)<ACK> -> ESTABLISHED
     38331 ESTABLISHED:input
     [e0531203..e0531403)@6cc5b402(win=4000)<ACK,FIN,PUSH>
     -> CLOSE_WAIT
     38331 CLOSE_WAIT:output
     6cc5b402@e0531404(win=3dff)<ACK> -> CLOSE_WAIT
     38331 CLOSE_WAIT:user RCVD -> CLOSE_WAIT
     38343 LAST_ACK:output
     6cc5b402@e0531404(win=4000)<ACK,FIN> -> LAST_ACK
     38343 CLOSE_WAIT:user DISCONNECT -> LAST_ACK
     38343 LAST_ACK:user DETACH -> LAST_ACK

MECHANISM
     TRPT interrogates the buffer of TCP trace records that
     is created when a TCP socket is marked for debugging.

CAVEATS
     Prior to using TRPT, an analyst should take steps to
     isolate the problem connection and find the address of
     its protocol control blocks.

BUGS
     None reported.

LIMITATIONS
     A socket must have the debugging option set for TRPT to
     operate. Another problem is that the output format of
     TRPT is difficult.

HARDWARE REQUIRED
     No restrictions.

SOFTWARE REQUIRED
     BSD UNIX or related OS.

AVAILABILITY
     Included with BSD and SunOS distributions. Available
     via anonymous FTP from uunet.uu.net, in file bsd-
     sources/src/etc/trpt.tar.Z.

Internet Tool Catalog   TTCP

NAME
     TTCP

KEYWORDS
     benchmark, generator; IP; ping; UNIX, VMS; free.

ABSTRACT
     TTCP is a traffic generator that can be used for test-
     ing end-to-end throughput. It is good for evaluating
     TCP/IP implementations.

MECHANISM
     Cooperating processes are started on two hosts. The
     open a TCP connection and transfer a high volume of
     data. Delay and throughput are calculated.

CAVEATS
     Will greatly increase system load.

BUGS
     None known.

LIMITATIONS
     None reported.

HARDWARE REQUIRED
     No restrictions.

SOFTWARE REQUIRED
     BSD UNIX or related OS, or VMS.

AVAILABILITY
     Source for BSD UNIX is available via anonymous FTP from
     vgr.brl.mil, in file ftp/pub/ttcp.c, and from sgi.com,
     in file sgi/src/ttcp.c. A version of TTCP has also
     been submitted to the USENET news group
     comp.sources.unix. For VMS, ttcp.c is included in the
     MultiNet Programmer's Kit, a standard feature of TGV
     MultiNet IP software package.

Internet Tool Catalog   UNISYS-PARAMAX

NAME
        Paramax Network Security Server

KEYWORDS
        alarm, control, manager, security, status;
        ethernet, FDDI, IP; X; UNIX.

ABSTRACT
        The Paramax Network Security Server (NSS) is a
        security officer's tool for centralized security
        management of TCP/IP-based networks. The NSS provides
        capability for collection, on-line storage,
        maintenance, and correlation of audit data from hosts,
        workstations, servers, and network devices. Through
        the X window based user interface, a security officer
        can review and analyze this audit data at the NSS,
        select and request filtered portions of host audit
        data, and receive and analyze security alerts from
        across the network. The NSS supports centralized
        access control of network resources through its
        capability to create and update user and host access
        permissions data. The user access permissions data
        identifies network addresses that each user is
        permitted to access. The host access permissions data
        identifies network addresses between which
        communication is permitted. The NSS supports
        centralized management of user authentication data
        (user IDs and passwords) and other user data for use
        by hosts, workstations, and servers in the network.
        It generates pseudo-random pronounceable passwords for
        selection and assignment to users by the security officer.

        The NSS deadman timer locks the NSS screen or logs the
        security officer off the NSS after periods of
        inactivity. A biometric authentication device is
        optional for rigorous fingerprint authentication of
        users at the NSS, and logins to the NSS itself are
        permitted only at the console. The NSS currently
        provides centralized security management for a System High
        Network. It is being upgraded for a Compartmented Mode
        environment.

MECHANISM
    The NSS uses the Audit Information Transfer Protocol
    (AITP) for the transfer of security alerts and audit
    data. AITP is NOT proprietary, and the specification
    is available from the address listed below. Access to
    the NSS audit database is provided via the Structured
    Query Language (SQL).

CAVEATS
    None.

BUGS
    None known.

LIMITATIONS
    None reported.

HARDWARE REQUIRED
    Hardware required is a Sun 4 (SPARCStation) with a color
    monitor, at least 600 MB disk, and 150 MB 1/4"
    cartridge tape drive.

SOFTWARE REQUIRED
    SunOS Version 4.1.1 running the Sun OpenWindows X
    windowing environment and the SYBASE Relational Data
    Base Management System.

AVAILABILITY AND CONTACT POINT FOR INFORMATION ABOUT THIS TOOL
    Commercially available from:
        Paramax Systems Corporation
        5151 Camino Ruiz
        Camarillo, California 93011-6004
        805-987-6811
        Peter Vazzana

CONTACT POINT FOR CHANGES TO THIS CATALOG ENTRY
        Paramax Systems Corporation
        5151 Camino Ruiz
        Camarillo, California 93011-6004
        805-987-6811
        Nina Lewis <nina@cam.paramax.com>

Internet Tool Catalog   WOLLONGONG-MANAGER

NAME
        Management Station, Release 3.0

KEYWORDS
        manager; ; snmp, x; sun, dec, dos;.

ABSTRACT
        Management Station is a network management software
        product that supports SNMP. Release 3.0 implements a
        distributed network management architecture that helps
        solve the scalability and reliability limitations of
        using a single cpu for all SNMP management tasks.
        Additionally, there are many applications provided
        that are all user-configurable. The following
        applications and their functionality is listed below:

        General Info:

        X Windows, 11.4 based implemented with OSF/Motif 1.1.1
        toolkit. X Windows interface for all configuration
        files. Most applications have "verbose" mode for
        display of SNMP PDU traffic. On-line help and
        Reference manual pages. ANSI C compliant.

        Network Management Daemon:

        Responsible for device discovery, trap/alarm
        management and fault monitoring for the network map.
        Connection with other distributed daemons and any
        connected stations is accomplished with SNMP/TCP.
        Configured via Manager MIB; also incorporates SMUX MIB
        (RFC 1227). Sends any information to INGRES, Oracle
        or Sybase via an ESQL interface. User-defined actions
        include: send alarm to map; send info to flat file;
        execute ESQL command; call any UNIX system command;
        forward traps and filter user-defined alarms.
        User-defined alarms can use any boolean expression and
        MIB variable expressions can be combined with AND/OR
        statements.

        MIB Compiler

        ASN.1 MIB compiler with X Windows interface. Accepts
        RFC 1155 and 1212 format. Most vendor-specific MIBs
        and proposed Internet standard MIBs already included.

Network Map

Comprehensive network monitoring map with click and
drag interface, hiearchical and virtual views.
Toolkit and preferences applications, device
discovery. Uses /etc/hosts file, NIS or DNS for
device resolution. Background pixmapping capability,
user-definable menu bar, network manager and console
operator modes via UNIX group permissions. Multiple
map use without limitation.

MIB Form and MIB Form Editor

User-designed, X-based SNMP applications. Alias for
MIB variables and interprets returned values. GET
NEXT and SET capability. User-defined polling and
multi-device [agent] capability. Configured via X
interface.

MIB Chart and MIB Chart Editor

Choice of strip chart, packed strip chart or bar
graphs. User-specified polling interval, MIB
variable(s) or MIB expressions using arithmetic
operands. Plot actual value, delta or delta/interval.
Plot multiple MIB expressions from multiple agents
simultaneously. X Windows interface. Pause polling
and grid options.

MIB Tool

X Windows application for the general viewing and
'walking' of MIB trees. GET NEXT and SET options.
Window for viewing RFC 1212 MIB definitions. Command
line interface option.

Application Programming Interface

Complete set of APIs for developers to write SNMP
applications in character mode or X Windows.

MECHANISM
Management Station uses SNMP and ICMP Echo Request to
monitor and control SNMP Agents. Network management
daemon implements Wollongong's Manager MIB, SNMP over
TCP and the SMUX protocol.

CAVEATS
        none.

BUGS
        See Product Release Notice.

LIMITATIONS
        Limitations on number of management agents and network
        management daemons not known at this time.

HARDWARE REQUIRED
        Sun SPARC workstations and servers
        DEC DECstations and DECsystems
        Motorola MPC (Delta 8000 series)
        3/486 PC and PC-compatible

        16 MB RAM
        n20 MB free disk space for installation
        Color monitor strongly recommended

SOFTWARE REQUIRED
        SunOS 4.1-1 or greater & OpenWindows 2.0 or greater (SUN)
        X Windows, 11.4 or greater
        RISC ULTRIX 4.1 or greater (DEC)
        R32V2 (Motorola)
        Open Desktop 1.1 or greater (3/486)

        Provided on 1/4" cartridge, TK-50 or 3 1/2" diskettes,
        as appropriate, in cpio format.

AVAILABILITY
        A commercial product of:

         The Wollongong Group, Inc.
                1129 San Antonio Rd
                Palo Alto, CA. 94303
        ph.:   (800) 962 - 8649 (in California)
                (800) 872 - 8649 (outside California)
        fax: (415) 962 - 0286

Internet Tool Catalog   XNETDB

NAME
        Xnetdb

KEYWORDS
        database, manager, map, monitoring, status; IP; Ping,
        SNMP, Unix, X; free.

ABSTRACT
        Xnetdb is a network monitoring tool based on X Windows
        and SNMP which also has integrated database and
        statistic viewing capabilities. Xnetdb will determine
        and display the status of routers and circuits it has
        been told to monitor by querying the designated sites
        and displaying the result. It can also query the
        status of certain designated SNMP variables, such as a
        default route for an important router. Additionally,
        it also has integrated database functionality in that
        it can display additional information about a site or
        circuit such as the equipment at the site, the contact
        person(s) for the site, and other useful information.
        Finally it can gather designated statistical
        information about a circuit and display it on demand.

MECHANISM
        Xnetdb uses SNMP or ping to monitor things which its
        configured to monitor. It dynamically builds a
        network map on its display by querying entities and
        obtaining IP addresses and subnet masks. A
        configuration file tells xnetdb which IP hosts you
        want to monitor.

CAVEATS
        While "ping" can be used to monitor hosts, more useful
        results are obtained using SNMP.

BUGS
        Bugs and other assorted topics are discussed on the
        xnetdb mailing list. To join, send a note to
        "xnetdb-request@oar.net".

LIMITATIONS
        None.

HARDWARE REQUIRED
        No restrictions.

SOFTWARE REQUIRED
        Most any variety of UNIX plus X-Windows and/or
        OpenWindows.

AVAILABILITY
        Available via anonymous ftp from ftp.oar.net
        (currently 131.187.1.102) in the directory /pub/src.
        Special arrangements can be made for sites without
        direct IP access by sending a note to
        "xnetdb-request@oar.net". There are minimal licensing
        restrictions - these are detailed within the package.

Internet Tool Catalog   XNETMON_SNMP_RESEARCH

NAME
        XNETMON -- an X windows based SNMP network management
        station from SNMP Research.

KEYWORDS
        alarm, benchmark, control, debugger, manager, map,
        reference, security, status, traffic;
        bridge, DECnet, Ethernet, FDDI, IP, OSI, ring, star;
        NMS, Ping, SNMP, X;
        UNIX;
        Sourcelib.

ABSTRACT
        The XNETMON application implements a powerful network
        management station based on the X window system.
        XNETMON's network management tools for configuration,
        performance, security, and fault management have been
        used successfully with a wide assortment of wide- and
        local-area-network topologies and medias.
        Multiprotocol devices are supported
        including those using TCP/IP, DECnet, and OSI
        protocols.

Some features of XNETMON's network management tools include:

        o Fault management tool displays a map of the network
          configuration with node and link state indicated
          in one of several colors to indicate current status;
        o Configuration management tool may be used to edit the
          network management information base stored in the
          NMS to reflect changes occurring in the network;
        o Graphs and tabular tools for use in fault and performance
          management (e.g. XNETPERFMON);
        o Mechanisms by which additional variables, such as vendor-
          specific variables, may be added;
        o Alarms may be enabled to alert the operator of events
          occurring in the network;
        o Events are logged to disk;
        o Output data may be transferred via flat files for
          additional report generation by a variety of
          statistical packages.

        The XNETMON application comes complete with source
        code including a powerful set of portable libraries
        for generating and parsing SNMP messages.

MECHANISM
        XNETMON is based on the Simple Network Management
        Protocol (SNMP). Polling is performed via the
        powerful SNMP get-next operator and the SNMP get
        operator. Trap-directed polling is used to regulate
                focus and intensity of the polling.

CAVEATS
        None.

BUGS
        None known.

LIMITATIONS
        Monitored and managed nodes must implement the SNMP over
        UDP per RFC 1157 or must be reachable via a proxy agent.

HARDWARE REQUIRED
        X windows workstation with UDP socket library.
        Monochrome is acceptable, but color is far superior.

SOFTWARE REQUIRED
        X windows version 11 release 4 or later or MOTIF.

AVAILABILITY AND CONTACT POINT FOR INFORMATION ABOUT THIS TOOL
        This is a commercial product available under license
        from:
                SNMP Research
                3001 Kimberlin Heights Road
                Knoxville, TN 37920-9716
                Attn: John Southwood, Sales and Marketing
                (615) 573-1434 (Voice) (615) 573-9197 (FAX)

CONTACT POINT FOR CHANGES TO THIS CATALOG ENTRY
        users@seymour1.cs.utk.edu

Internet Tool Catalog   XNETMON_WELLFLEET

NAME
      xnetmon, xpmon

KEYWORDS
      alarm, manager, map, status; IP; NMS, SNMP; UNIX.

ABSTRACT
      Xnetmon and xpmon provide graphical representation of
      performance and status of SNMP-capable network ele-
      ments. Xnetmon presents a schematic network map
      representing the up/down status of network elements;
      xpmon draws a pen plot style graph of the change over
      time of any arbitrary MIB object (RFC1066). Both xnet-
      mon and xpmon use the SNMP (RFC1098) for retrieving
      status and performance data.

MECHANISM
      Xnetmon polls network elements for the status of their
      interfaces on a controllable polling interval. Pop-up
      windows displaying the values of any MIB variable are
      supported by separate polls. When SNMP traps are
      received from a network element, that element and all
      adjacent elements are immediately re-polled to update
      their status. The layout of the network map is stati-
      cally configured. Xpmon repeatedly polls (using SNMP)
      the designated network element for the value of the
      designated MIB variable on the user-specified interval.
      The change in the variable is then plotted on the strip
      chart. The strip chart regularly adjusts its scale to
      the current maximum value on the graph.

CAVEATS
      Polling intervals should be chosen with care so as not
      to affect system performance adversely.

BUGS
      None known.

LIMITATIONS
      None reported.

HARDWARE REQUIRED
      Distributed and supported for Sun-3 systems.

SOFTWARE REQUIRED
      SunOS 3.5 or 4.x; X11, release 2 or 3.

        AVAILABILITY
            Commercial product of:
                Wellfleet Communications, Inc.
                12 DeAngelo Drive
                Bedford, MA 01730-2204
                (617) 275-2400

Internet Tool Catalog   XNETPERFMON_SNMP_RESEARCH

NAME
        xnetperfmon -- a graphical network performance and
        fault management tool from SNMP Research.

KEYWORDS
        manager, security, status;
        DECnet, Ethernet, IP, OSI, ring, star;
        NMS, SNMP, X;
        DOS, UNIX, VMS;
        sourcelib.

ABSTRACT
        Xnetperfmon is a XNETMON tool used to produce plots of
        SNMP variables in graphical displays. The manager may
        easily customize the labels, step size, update interval,
        and variables to be plotted to produce graphs for fault
        and performance management. Scales automatically adjust
        whenever a point to be plotted would go off scale.

MECHANISM
        The xnetperfmon application communicates with remote
        agents or proxy agents via the Simple Network Management
        Protocol (SNMP).

CAVEATS
        All plots for a single invocation of xnetperfmon must be
        for variables provided by a single network management
        agent. However, multiple invocations of xnetperfmon may
        be active on a single display simultaneously or proxy
        agents may be used to summarize information at a common
        point.

BUGS
        None known.

LIMITATIONS
        None reported.

HARDWARE REQUIRED
        Systems supporting X windows.

SOFTWARE REQUIRED
        XNETMON from SNMP Research and X Version 11 release 4 or
        later (option MOTIF)

AVAILABILITY AND CONTACT POINT FOR INFORMATION ABOUT THIS TOOL
        This is a commercial product available under license
        from:

        SNMP Research
        3001 Kimberlin Heights Road
        Knoxville, TN 37920-9716
        Attn: John Southwood, Sales and Marketing
        (615) 573-1434 (Voice) (615) 573-9197 (FAX)

CONTACT POINT FOR CHANGES TO THIS CATALOG ENTRY
        users@seymour1.cs.utk.edu

Internet Tool Catalog   XUP_HP

     NAME
          xup

     KEYWORDS
          status; ping, X; HP.

     ABSTRACT
          Xup uses the X-Windows to display the status of an
          "interesting" set of hosts.

     MECHANISM
          Xup uses ping to determine host status.

     CAVEATS
          Polling for status increases network load.

     BUGS
          None known.

     LIMITATIONS
          None reported.

     HARDWARE REQUIRED
          Runs only on HP series 300 and 800 workstations.

     SOFTWARE REQUIRED
          Version 10 of X-Windows.

     AVAILABILITY
          A standard command for the HP 300 & 800 Workstations.

Appendix: "No-Writeups"

   This section contains references to tools which are known to exist,
   but which have not been fully cataloged. If anyone wishes to author
   an entry for one of these tools please contact: noctools-
   request@merit.edu.

   Each mention is separated by a <form-feed> for improved readability.
   If you intend to actually print-out this section of the catalog, then
   you should probably strip-out the <ff>.

tuecho.c

```
/*
 * Send / receive TCP or UDP echos in any of a number of bizzare ways.
 *
 *   Joel P. Bion, March 1990
 *   Copyright (c) 1990 cisco Systems. All rights reserved.
 *
 * This "tuecho" program is distributed in the hope that it will be
 * useful, but WITHOUT ANY WARRANTY; without even the implied warranty
 * of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.
 *
 * Prompts as:
 *   Host: -- host to send echos to -- can be name or a.b.c.d --
 *   Enter protocol (0 = UDP, 1 = TCP) [0]: -- UDP or TCP
 * Size of data portion (bytes) [100]: -- bytes in data, excluding
 * headers -- Number of bursts [5]: -- number of bursts of packets to
 * send -- Packets per burst [1]: -- packets per burst, all sent AT
 * ONCE -- Timeout (seconds) [2]: -- how long to wait for data
 * Pause interval (seconds) [0]: -- Pause interval between bursts of
 * frames
 *   Type of pattern (specify = 0, increment = 1) [1]:
 *           -- if 0 specified, allow you to specify a 16bit pattern
 *           -- as four hex digits (see below). If 1, will create a
 *           -- "incrementing", cycling pattern from 0x0000 -> 0xffff
 *           -- ->.
 *   Enter pattern (hex value) [abcd]:  -- if "0" specified above
 */
```

Availability:
        ftp.uu.net:/networking/cisco/tuecho.c
        ftp.cisco.com:tuecho.c

SPY   An NFS monitoring/tracing tool

Availability:
        A postscript file describing SPY is located on
        ftp.uu.net:/networking/ip/nfs/spy.ps.Z

NFSTRACE

   This is the rpcspy/nfstrace package.

   It is described in detail in the paper "NFS Tracing by Passive
   Network Monitoring", which appeared in the January, 1992 USENIX
   conference.

   You'll need either a DEC machine running ULTRIX (with the
   packetfilter installed in the kernel) or a Sun running SunOS 4.x
   (with NIT). Or you'll need to do a bit of hacking.

   The package differs slightly from the version in the paper:

   - The handle->name translation facility has been removed. It's
     just too fragile to include in the general release. If you need it,
     contact me directly and I'll be happy to mail you the code.

   - The output format is a wee-bit different.

   - The IBM-RT Enet filter version is also not included, since I seem to
     be the only person in the world running it. RTs are really too slow
     for this anyway.

   To configure the package, edit the makefile in the obvious (to me at
   least) way.

   Note that the not all versions of SunOS NIT have working versions of
   the packet timestamp mechanism. Try to set the -DSTAMPS option in
   the makefile, and if that doesn't work, take it out.

   If you are actually going to use this to gather traces, I'd like to
   hear from you! Please send email, and share your results/traces if
   your organization will allow it. I maintain a mailing list of users
   for updates, etc. Send me mail to be added to it.

   Happy tracing.
   Matt Blaze
   Department of Computer Science
   Princeton University
   35 Olden Street
   Princeton, NJ 08544
   mab@cs.princeton.edu
   609-258-3946

   Availability:
           ftp.uu.net:/networking/ip/nfs/nfstrace.shar (or check archie)

        LAMER

    # Lame delegation notifier
    # Author: Bryan Beecher
    # Last Modified: 6/25/92
    #
    # To make use of this software, you need to be running the
    # University of Michigan release of BIND 4.8.3, or any version
    # of named that supports the LAME_DELEGATION patches posted to
    # USENET. The U-M release is available via anonymous ftp from
    # terminator.cc.umich.edu:/unix/dns/bind4.8.3.tar.Z.
    #
    # You must also have a copy of query(1) and host(1). These
    # are also available via anonymous ftp in the aforementioned
    # place.
    # ---

    # ---
    # handle arguments
    # ---
    #   -d <day>
    #   This flag is used to append a dot-day suffix to the LOGFILE.
    #   Handy where log files are kept around for the last week
    #   and contain a day suffix.
    #
    #   -f <logfile>
    #   Change the LOGFILE value altogether.
    #
    #   -w
    #   Count up all of the DNS statistics for the whole week.
    #
    #   -v
    #   Be verbose.
    #
    #   -t
    #   Test mode. Do not send mail to the lame delegation
    #   hostmasters.

    Availability:
            ftp.uu.net:/networking/ip/dns/lamer.tar.Z (or check archie)

     HOST

     host - look up host names using domain server

SYNOPSIS
     host [-v] [-a] [-t querytype] [options] name [server]
     host [-v] [-a] [-t querytype] [options] -l domain [server]
     host [-v] [options] -H [-D] [-E] [-G] domain
     host [-v] [options] -C domain
     host [-v] [options] -A host

DESCRIPTION
     host looks for information about Internet hosts or domains.
     It gets this information from a set of interconnected
     servers that are spread across the world. By default, it
     simply converts between host names and Internet addresses.
     However, with the -t, -a and -v options, it can be used to
     find all of the information about hosts or domains that is
     maintained by the domain nameserver.

```
/*
 * Extensively modified by E. Wassenaar, Nikhef-H, <e07@nikhef.nl>
 *
 * The officially maintained source of this program is available
 * via anonymous ftp from machine 'ftp.nikhef.nl' [192.16.199.1]
 * in the directory '/pub/network' as 'host.tar.Z'
 *
 * Also available in this directory are patched versions of the
 * BIND 4.8.3 nameserver and resolver library which you may need
 * to fully exploit the features of this program, although they
 * are not mandatory. See the file 'README_FIRST' for details.
 *
 * You are kindly requested to report bugs and make suggestions
 * for improvements to the author at the given email address,
 * and to not re-distribute your own modifications to others.
 */
/*
 *                      New features
 *
 * - Major overhaul of the whole code.
 * - Very rigid error checking, with more verbose error messages.
 * - Zone listing section completely rewritten.
 * - It is now possible to do recursive listings into subdomains.
 * - Maintain resource record statistics during zone listings.
 * - Maintain count of hosts during zone listings.
 * - Exploit multiple server addresses if available.
 * - Option to exploit only primary server for zone transfers.
 * - Option to exclude info from names that do not reside in a domain.
```

```
 * - Implement timeout handling during connect and read.
 * - Write resource record output to optional logfile.
 * - Special MB tracing by recursively expanding MR and MG records.
 * - Special mode to check SOA records at each nameserver for domain.
 * - Special mode to check inverse mappings of host addresses.
 * - Code is extensively documented.
 */
```

PINGs

Many many versions of the PING program exist.
Each implementation has its own set of additional features.
Here are a few more PINGs that are worth taking a look at.

Version on ftp.cc.berkeley.edu:pub/ping:
        This version has duplicate packet detection, Record Route,
        ability to specify data pattern for packets, flood pinging, an
        interval option, Multicast support, etc.

Version on nikhefh.nikhef.nl:/pub/network/rping.tar.Z:
        'rping' is just like 'ping', but only a single probe packet
        is sent to test the reachability of a destination.
        As an option, the loose source routing facility is used
        to show the roundtrip route the packet has taken.
        Multiple addresses of remote hosts are tried until one
        responds. As an option, each of multiple addresses can be
        probed unconditionally.
        Contains a patch for making loose source routing work in
        case you have a SUN with an OMNINET ethernet controller.

VRFY

vrfy.tar.Z   (Version 921021)
        'vrfy' is a tool to verify email addresses and mailing lists.
        In its simplest form it takes an address "user@domain", figures
        out the MX hosts for "domain", and issues the SMTP command VRFY
        at the primary MX host (optionally all), or at "domain" itself
        if no MX hosts exist. Without "domain" it goes to "localhost".
        More complex capabilities are: recursively expanding forward
        files or mailing lists, and detecting mail forwarding loops.
        Full-blown RFC822 address specifications are understood.
        Syntax checking can be carried out either locally or remotely.
        Various options are provided to exploit alternative protocol
        suites if necessary, and to print many forms of verbose output.
        Obvious limitations exist, but on average it works pretty well.
        Needless to say you need internet (nameserver and SMTP) access.
        See the man page and the extensive documentation in the source
        for further details.

Please send comments and suggestions to Eric Wassenaar <e07@nikhef.nl>

If you want to receive notification of updates, please send an email
with the keyword "subscribe" in the subject or the body to the address
<net-dist-request@nikhef.nl>

available as: nikhefh.nikhef.nl:/pub/network/vrfy.tar.Z

XNETLOAD

NAME
     xnetload - ethernet load average display for X

SYNOPSIS
     xnetload[-toolkitoption ...] [-scale integer]
          [-update seconds] [-hl color] [-highlight color]
          [-jumpscroll pixels] [-label string] [-nolabel] host

DESCRIPTION
     The xnetload program displays a periodically updating histo-
     gram of the ethernet load average for the specified host.
     The resulting graph is scaled as 0% to 100%, where 0%
     corresponds to 0mbs and 100% corresponds to 10mbs. NOTE:
     The specified host must be running rpc.etherd.

This program has been run using X11R4 and X11R5, under the following
operating systems:

          SUNOS 4.1.0
          SUNOS 4.1.1
          ULTRIX V4.2
          IRIX 3.3.2

Assuming the Imake templates and Rules are in order and in the proper
place on your system, these programs should compile and link
straightforward by running the following sequence:

          xmkmf
          make

Then, as root, issue the following:

          make install
          make install.man

Then, on your host system, (or on any other system you can rlogin or rsh
into) start the etherd daemon with the following (must be root):

          /usr/etc/rpc.etherd le0 &

where le0 is the mnemonic for the primary ethernet interface.

To start the xnetload program, the following command line is suggested:

          ./xnetload -hl red host &

where "host" is the name of any reachable network node (including
LOCALHOST) that is running the etherd daemon. A small xload window
should appear on your local display with nine horizontal lines. The
label:
        "Ethernet Load %"
should appear in the upper left hand corner, just below any additional
title bars or other decorations provided by your window manager. If the
program comes up without the nine lines, or without the "Ethernet Load"
label, then either your resource file is not properly installed in the
appropriate app-defaults directory, or you may have picked up the wrong
xnetload image. Try re-running "make install" as root, or be sure to
include the "./" in front of the command name.

Good Luck!

The following changes have been made to this directory since R3:

        o Now use Athena StripChart widget.

        o Understands WM_DELETE_WINDOW.

        o 3-26-92 Modified from xload to xnetload by Roger Smith,
          Sterling Software at NASA-Ames Research Center,
          Mountain View, Calif. rsmith@proteus.arc.nasa.gov

Availability:
        ftp proteus.arc.nasa.gov:pub/XEnetload.tar.Z (or check archie)

NETTEST

     nettest, nettestd - Performs client and server functions for
     timing data throughput

     The nettest and nettestd commands invoke client and server
     programs that are used for timing data throughput of various
     methods of interprocess communication. For TCP and OSI con-
     nections, the nettest program establishes a connection with
     the nettestd program, and then it does count writes of size
     bytes, followed by count reads of size bytes. For UDP, the
     nettest program performs only writes; reads are not per-
     formed. The nettestd program, if used with UDP connections,
     reads the data packets and prints a message for each data
     packet it receives.   The number and size of the reads and
     writes may not correlate with the number and size of the
     actual data packets that are transferred; it depends on the
     protocol that is chosen. If you append an optional k (or K)
     to the size, count, or bufsize value, the number specified
     is multiplied by 1024.

   This source for nettest and nettestd are provided on an "as is"
   basis. Cray Research does not provide any support for this code
   (unless you are a customer who has purchased the UNICOS operating
   system).

   We will gladly take bug reports for nettest/nettestd. Suggested
   fixes are prefered to just bug reports. Changes to allow
   nettest/nettestd to run on other architectures are also welcomed. We
   will try to incorporate bugfixes and update the publicly available
   code, but we can make no guarantees.

   For copyright information, see the notice in each source file.

   Send bug-reports/fixes to:
        E-mail: dab@cray.com
        U.S. Mail: David Borman
                         Cray Research, Inc.
                         655F Lone Oak Drive
                         Eagan, MN 55121
   Notes:

   1) The -b option to nettestd has not been tested...
   2) The ISO code should work on a 4.4BSD system, but the
      gethostinfo() routine is specific to UNICOS...

   Availability:
          ftp sgi.com:/sgi/src/nettest

ETHERCK

etherck is a simple program that displays Sun ethernet statistics.
If you have a high percents of input errors that are due to "out of
buffers", then you can run the "iepatch" script to patch a kernel
that uses the Intel ethernet chip ("ie"). A back of the envelope
calculation shows that a .25% input error rate gives about a 10%
degradation of NFS performance if 8k packets are being used.

In our environment at Legato, patching the ie buffer allocation made
the input error rate drop more than 2 orders of magnitude. This was
after we had applied other networking fixes (e.g., using Prestoserve,
going from thin wire to twisted pair) and pushed a higher load on the
server.

Note that both etherck and iepatch must be run by root (or you can
make etherck setgid kmem).

Availability:
        send EMAIL to: request@legato.com
        with a Subject line: send unsupported etherck

The following is part of the 'help' file from the Legato Email
Server:

This message comes to you from the request server at Legato.COM,
request@Legato.COM. It received a message from you asking for help.

The request server is a mail-response program. That means that you
mail it a request, and it mails back the response.

The request server is a very dumb program. It does not have much
error checking. If you don't send it the commands that it
understands, it will just answer "I don't understand you".

The request server has 4 commands. Each command must be the first
word on a line. The request server reads your entire message before
it does anything, so you can have several different commands in a
single message. The request server treats the "Subject:" header line
just like any other line of the message. You can use any combination
of upper and lower case letters in the commands.

The request server's files are organized into a series of directories
and subdirectories. Each directory has an index, and each
subdirectory has an index. The top-level index gives you an overview
of what is in the subdirectories, and the index for each subdirectory
tells you what is in it.

The server has 4 commands:

"help" command: The command "help" or "send help" causes the server to
        send you the help file. You already know this, of course,
        because you are reading the help file. No other commands are
        honored in a message that asks for help (the server figures
        that you had better read the help message before you do
        anything else).

SEND a request to Legato to get the rest of the help file!

NETCK

netck is a shar file that contains the sources to build "netck", a
network checker that uses the rstat(3R) protocol to gather and print
statistics from machines on the network. netck is useful to help
understand what part of what machines are potential NFS bottlenecks.
To get this file, send email to the request server with the command
"send unsupported netck".

Availability:
        same as ETHERCK (send email To: request@legato.com; subject:
        HELP)

References

   [1] Stine, R., Editor, "FYI on a Network Management Tool Catalog:
       Tools for Monitoring and Debugging TCP/IP Internets and
       Interconnected Devices", FYI 2, RFC 1147, Sparta, Inc., April
       1990.

Security Considerations

   Security issues are not discussed in this memo.

Authors' Addresses

   Robert M. Enger
   Advanced Network and Services
   1875 Campus Commons Drive, Suite 220
   Reston, VA. 22091-1552

   Phone: 703-758-7722
   EMail: enger@reston.ans.net

   Joyce K. Reynolds
   Information Sciences Institute
   University of Southern California
   4676 Admiralty Way
   Marina del Rey, CA 90292

   Phone: (310) 822-1511
   Email: JKREY@ISI.EDU