ETHLOAD 1.01

USER'S GUIDE

A simple public domain

Ethernet load/problems analyzer

and events tracer

E. Vyncke

vyncke@csl.sni.be

1. Introduction.

ETHLOAD is a public domain software running on any MS-DOS PC with an Ethernet controller.

Currently, ETHLOAD supports the following drivers:
- Digital Equipment Corp. DLL specification;
- Microsoft 3Com NDIS (Network Driver Interface Specification);
- packet driver as issued from PC/TCP or Clarkson University;
- Novell ODI (Open Datalink Interface) iff the driver supports promiscuous mode.

The purpose of ETHLOAD is threefold:
- display very simply non accurate numbers about the Ethernet load (number of frames/sec, bits/sec, ...);
- display important parameters, events and loads for the DECnet protocol;
- display important parameters, events and loads for the TCP/IP protocols suite.

ETHLOAD allows you to:
- check simply the load of your Ethernet (with error rate, interframe gap,...);
- check which host is sending most of frames;
- see which host is sending to wich host;
- see what kind of protocols are in use in your Ethernet;
- ...

In a TCP/IP network, ETHLOAD allows you to:
- see ARP table contents;
- see which host is sending (un)resolved ARP probes;
- see the IP host which is sending most of the IP, UDP or TCP packets;
- see what kind of protocols are in used (either TCP or UDP);
- see which is the mostly used telnet/rlogin server (or client);
- see some characteristics of IP hosts (fragments size, MTU, IP retransmission,...);
- see important TCP events: start/stop of connections,...
- see other important events relevant to BOOTP, SMTP, TFTP, ...

In a DECnet network, ETHLOAD allows you to:
- see which node are sending/receiving most of DECnet packets;
- see all Connect Initiate packets (including object number, ...) ;
- see returned packets;
- ...

*** * ***

*** ***

*****

2. Acknowledgments.

2.1. Original copyright.

This software is based on the very first version of ETHLOAD I have developped while I was working in a company called Network Research Belgium. This version was already in the public domain thanks to the management of this company.

Here follows the copyright included in the source files of about 30% of the current version of ETHLOAD.

/* This software and documentation can be copied, used, modified freely as long as:
- the source contains this text
- this software, documentation is provided free of charge (but for the cost of media: paper, CD-ROM, ...).
Network Research Belgium and the individuals who have written this software DO NOT ASSUME any responsabilities in respect to the use, (un)expected side -effects of this program.
The software and documentation is provided as it is. No maintenance will be given.
Anyway, we would be pleased to hear of any use of these softwares by email, fax or phone:

bert@nrb.be
fax: +32.41.48.11.70

phone: +32.41.40.72.11 ask for a BERT member.
Suggestions, modifications are always welcome.
These softwares have been developped by a special team called BERT in a company called Network Research Belgium located in Herstal, Belgium, Europe .
This team includes:

Eric Vyncke, vyncke@nrb.be now vyncke@csl.sni.be
Frederic Blondiau, blondiau@nrb.be
Michel Ghys, now mghys@cisco.com
Marie-Christine Timmermans, timmermans@nrb.be
Jean Hotterbeex, now working in Trasys with no email
Manu Khronis, khronis@nrb.be
Vincent Keunen, keunen@nrb.be

*/

2.2. Current copyright and disclaimer.

Right now, all software developments is made home and tested after working hours in my current company: Siemens Nixdorf. So, here follows the usual disclaimer: Siemens Nixdorf is by no means responsible for any good or bad effects of this program.

Both Siemens Nixdorf and the author do not support this software.

2.3. Support.

Anyway, you can get some support from the author since he wants to promote this software... You can reach the author through email: vyncke@csl.sni.be[1] or by post mail:

Eric Vyncke
Rue Nolden, 25
B-4432 Alleur
Belgium.

If you are happy with ETHLOAD, my little son, Pierre, would appreciate to receive any postcard!

2.4. Distribution channel.

I have no access to internet, so I cannot place ETHLOAD on anonymous FTP server, if you run such a server I will appreciate that you reserved some place for ETHLOAD...

2.5. Thanks to testers.

I would like to thank anyone of you about his/her comments.

I thank especially:

Michel Dalle, michel@d92.cb.sni.be

* * *
* *
*

1email in Belgium is not free :-(So that's my employeer which pays any email. If any site in Belgium or BITnet is whishing to start-up a distribution list for ETHLOAD, I would really appreciate ;-)

AB-00-03-00-00-00	DEC: Local Area Transport -LAT-
FF-FF-FF-FF-FF-FF	Broadcast
CF-00-00-01-00-00	Loopback Assistance
00-00-00-00-00-00	Null Address

3. Configuration files.

In order to run in basic mode (i.e. without translation of addresses into names,...) ETHLOAD does not require any configuration file. The configurations are required only if you want to achieve good printings: host name instead of addresses, ...

All configuration files are in the same format:
- plain ASCII files, i.e. lines ended by CR/LF;
- any line beginning with a ';' or a '#' is considered as a comment;
- empty lines are ignored;
- other lines must begin with a token generally numeric, called the key, then a serie of space or TAB characters, followed by another token, called the value. The value token is ended by the CR/LF end of line.

Most of these files are the MS-DOS image of the well known TCP/IP files for Unix: /etc/hosts, /etc/ethers, /etc/protocols, ... The simplest way to use them is to FTP them from your Unix box.

If you are using TCP/IP you should FTP /etc/hosts of a Unix host and perhaps add some MAC addresses to the ETHERS file.

If you are using DECnet, you probably don't need to modify any of these files.

If you are using another protocol, you will probably need to modify ETHERS file together with TYPES and/or SAPS.

All these optional files must be located in the current directory of the current drive.

ETHERS

This file contains the mapping between MAC Ethernet addresses into host names.

The key token is the Ethernet MAC address in the format HH-HH-HH-HH-HH-HH where HH is a pair of hexadecimal digits.

The value token is any character string representing the name of this host.

Part of ETHERS file:

```
139.21.20.18    d012s509.ap.mchp.sni.de d012s509
139.21.18.140   d012s322.ap.mchp.sni.de d012s322
139.21.22.206   d012s712 rm400ap
139.21.24.1     cisco.ap.mchp.sni.de
139.24.16.44    baumann
```

Remark: ETHLOAD is smart enough to recognize a DECnet node and display the DECnet address of any MAC address.

Remark 2: ETHLOAD is also listening for ARP requests and replies, so it can display the IP address of any MAC address.

Remark 3: ETHLOAD as it is (i.e. without ETHERS) cannot even display correctly well known address as the null address or even the broadcast address.

Remark 4: you should add your own MAC addresses only if you are not using DECnet or TCP/IP, moreover, you should add these addresses at the end of ETHERS file and keep the original contents of ETHERS.

HOSTS

This file contains the mapping between IP address and host names.

The key token is an IP address in the format ddd.ddd.ddd.ddd where ddd is up to three decimal digits.

The value token is any character string representing the name of this host.

Part of HOSTS file:

The best way to initiate this file is to get a /etc/hosts from a Unix machine (or the stdout of the **ypcat hosts.byaddr** if you are running NIS[1]).

PROTOCOL

This file contains the mapping between IP protocols and protocol names.

The key token is a decimal number up to 255.

The value token is any character string representing the name of the protocol.

One again, the best way to initiate this file is to get /etc/protocols from a Unix machine or using the PROTOCOL file you may have receive with ETHLOAD. The first solution

1Also known previously by Yellow Pages

0	ip
1	icmp
3	ggp, gateway-gateway protocol
6	tcp
8	egp, exterior gateway protocol
12	pup
17	udp
20	hmp, host monitoring protocol
22	xns-idp
27	rdp, reliable datagram protocol

is probably not useful since /etc/protocols are always nearly the same.

The shipped PROTOCOL file contains:

SAPS

This file contains the mapping between IEEE 802.2 LLC SAP and SAP names.

The key token is two hexadecimal digits.

The value token is the name representing the Service Access Point.

Part of a sample SAPS file:

80	3Com XNS
8E	Proway-LAN
AA	TCP/IP-SNAP (Ethernet type in LLC)
BC	Banyan VINES
E0	Novell NetWare
F0	IBM NetBIOS

Remark: ETHLOAD has a built-in knowledge of SNAP.

WKS.TCP (resp. WKS.UDP)

This file contains the mapping of TCP (resp. UDP) well-known services ports.

The key token is a decimal number up to 65535 which is the port number assigned to the service.

Part of a sample WKS.TCP file:

79	finger
21	ftp
101	hostnames
256	informix
1524	ingreslock

This file together with WKS.UDP contains all the information of the usual /etc/services Unix file but in a slighty different format.

Since the file /etc/services is always the same on all Unix machine, you may probably use the files provided with ETHLOAD.

```
0600-0600 XNS Cisco
0800-0800 IP
0806-0806 ARP Address Translation
0BAD-0BAD Banyan
1000-1000 DOS Sytek
1001-100F IEEE 802.1 Internetwork
```

TYPES

This file contains the mapping of the DIX Ethernet packet type into names.

The key token is 4 hexadecimal digits.

Part of a sample TYPES file:

VENDORS

This file contains the mapping between the IEEE vendor codes and the vendor names. The IEEE vendor code is representing the most significant three bytes of the MAC address of any adapter built by this manufacturer.

The key token is 3 bytes represented each by two hexadecimal digits, each byte is separated by a dash.

Part of a sample VENDORS file:

*** * ***
*** ***
*****

4. Set-up of datalink drivers.

ETHLOAD as already said is currently running as it is on the top of four different datalink drivers. ETHLOAD automatically configures itself to use the first driver found. It tries in the following order:

- Digital Equipment DLL;
- Microsoft 3Com NDIS version 2.0.1 or higher[1];
- PC/TCP packet driver;
- Novell ODI.

Some of these datalink drivers allow for simultaneous execution of ETHLOAD and of you usual protocol stack: NDIS and ODI. All other drivers prevent the execution of your usual protocol stack, it means that you will abort all current connections to any servers.

Some of these datalink drivers do not require a PC reboot after running them: DLL, NDIS version 2.0 or higher, packet driver and ODI.

Finally, only one kind of drivers namely ODI allows for the identification of faulty frame by their source or destination addresses.

In conclusion, if your Ethernet hardware has a ODI driver with promiscuous mode support, it is better to use ODI.

A final remark, packet driver does not differenciate between the various kind of errors in its statistics. So, you should use any other driver if possible.

4.1. Digital Equipment DLL.

If DLL.EXE (or DEPCADLL.EXE) is already loaded, you have nothing to do before starting ETHLOAD by the ETHLOAD command.

Note: in order to go promiscuous, DLL requires that ETHLOAD shutdown ALL connections: LAT, DECnet, ... After using ETHLOAD you probably will have to reset the whole DECnet protocol stack (so reboot your PC).

4.2. Microsoft 3Com NDIS v 1.0.1.

Before running ETHLOAD for the first time, you must modify your PROTOCOL.INI (usually located as C:\LANMAN\PROTOCOL.INI see your C:\CONFIG.SYS file and the DEVICE=..PROTMAN... /I:<path>).

1The version 1.0.1 is also supported, but with several restrictions (see further)...

```
[ETHLOAD]
        drivername = ETHLOAD$
        bindings = MYMAC
```

You must add the following lines in your PROTOCOL.INI (anywhere in the file but after a section):

where MYMAC is the name of the MAC module you want to use.

These modifications do not modify the usual behaviour of your PC, so you may leave these lines in your PROTOCOL.INI file even if you don't use ETHLOAD.

After you have made these changes, you must reboot your PC.

After this reboot, when you want to use ETHLOAD you must issue the ETHLOAD command to the MS-DOS prompt.

By the way, the Protocol Manager directory (containing NETBIND.EXE, ...) should be in the PATH of MS-DOS.

Remark 1: in PROTOCOL.INI the case of the left part of '=' does not matter, but uppercase characters must be used on the right part as indicated in the examples above.

Remark 2: as you are using a version of Protocol Manager older than version 2.0.1 [1], ETHLOAD will display some warnings and you have to pay special attention to the following points:

- don't run NETBIND.EXE before ETHLOAD (so look out in your AUTOEXEC.BAT for automatic running of NETBIND.EXE)
- reboot your PC after running ETHLOAD since Protocol Manager cannot be reset in a correct state
- some statistics are missing.

4.3. Microsoft 3Com NDIS v2.0.1 or higher.

Before running ETHLOAD for the first time, you must modify your PROTOCOL.INI (usually located as C:\LANMAN\PROTOCOL.INI see your C:\CONFIG.SYS file and the DEVICE=..PROTMAN... /I:<path>).

You must add the following lines in your PROTOCOL.INI (anywhere, after a section):

where MYMAC is the name of the MAC module you want to use.

1You can check the version by looking at the banner displayed when Protocol Manager is loaded from CONFIG.SYS. Also, if the Protocol Manager directory is missing the PROTMAN.EXE file, you can bet you have a old 1.0 version.

```
[PROTOCOL MANAGER]
    devicename = PROTMAN$
    dynamic = YES
    bindstatus = YES
    priority = ETHLOAD
```

You also have to modify the [PROTOCOL MANAGER] entry to add a dynamic line. But first try without this modification before modifying further your PROTOCOL.INI file.

These modifications do not modify the usual behaviour of your PC, so you may leave these lines in your PROTOCOL.INI file even if you don't use ETHLOAD[1].

After you have made these changes, you must reboot your PC.

After this reboot, when you want to use ETHLOAD you must issue the ETHLOAD command to the MS-DOS prompt.

By the way, the Protocol Manager directory (containing NETBIND, ...) should be in the PATH of MS-DOS.

Remark 1: in PROTOCOL.INI the case of the left part of '=' does not matter, but uppercase characters must be used on the right part as indicated in the examples above.

Remark 2: the use of ETHLOAD is not disruptive for your favorite protocol stacks, so you don't have top reboot your PC.

4.4. Packet driver.

Packet drivers exist for nearly all known Ethernet adapters.

You have to use a software interrupt between 0x60 and 0x7F in order to let ETHLOAD run.

ETHLOAD will use the first packet driver found while checking from interrupt 0x60 up to 0x7F.

The use of ETHLOAD is not disruptive to your other network application which will continue to run at very bad efficiency...

To start ETHLOAD, just issue the ETHLOAD command to the MS-DOS prompt.

1But for the bindstatus=YES, which increase the resident part of the Protocol Manager, thus, reducing the available base memory. If you are concerned with base memory, you may instead use bindstatus=NO, then ETHLOAD won't be able to display some informations about Protocol Manager but wil anyway work as usual.

Remark: nearly all packet drivers are in the public domain and can be found in numerous anonymous FTP server including SIMTEL20.ARMY.MIL. For BITnet users, they can also be fetched through TRICKLE server.

4.5. Novell ODI.

The first thing to note is that only very few ODI drivers supports the promiscuous mode which is needed for ETHLOAD. Novell has a list of those drivers since the promiscuous mode is also needed by Novell LANanalyzer product.

To use ETHLOAD, you just have to load the ODI driver (preceeded as usual by LSL.COM) and having a correct C:\NET.CFG. If you can run any other ODI application (Novell LAN Workplace for DOS, Siemens Nixdorf LAN 1, ...), you should be able to run ETHLOAD as it is.

The use of ETHLOAD is not disruptive to your other network application which will continue to run at very bad efficiency...

To start ETHLOAD, just issue the ETHLOAD command to the MS-DOS prompt.

*** * ***
*** ***
*****

5. The different screens of ETHLOAD

5.1. Introduction

5.1.1. Screen layout

The different screens displayed by ETHLOAD have all the same design:

- the top line is just a copyright notice + version identification + percentage of dropped frames due to internal buffer shortage (either in ETHLOAD or in data link driver or even in Ethernet controller);
- in the top right corner a character is flipping from '+' to '-' as frames are received;
- the second line is a summary of all commands available for this screen;
- the bottom line displays the first bytes of the last received frame:
  * six bytes of MAC destination address ;
  * six bytes of MAC source address ;
  * two byte(s) for either DIX packet type or for IEEE 802.3 frame length;
  * a few bytes of data.

All screens are refreshed every five seconds to reflect the current statistics or table contents.

5.1.2. Commands.

You can enter a single character command. This command will be acted upon only before the screen refresh, i.e., you can issue only one command every five seconds... [1] The case of the character is ignored.

Two commands are always recognized:

- '**Z**' or '**0**': for resetting all statistics of ETHLOAD to zero and clearing all tables. Note that all statistics are cleared and not only the ones currently displayed;
- '**X**' or **<ESC>**: for leaving the current screen and getting back to the previous menu.

On some screens a large table is displayed: ARP table, ... As these tables are larger than the 23 lines of display available, you have to use the **PgUp** and **PgDn** key to scroll between the different pages.

5.1.3. Data display.

1This very long delay has be chosen to give the most of CPU power to packet analysis.

Three common display are often used:

- top of sorted table display;
- raw table display;
- history of events display.

The ***'top display'*** consists of a title beginning with 'Top of...' and displays the contents of an internal table sorted from the highest frequency down to the lowest frequency. An example of such a display is the display of MAC Transmitter.

Each line of a ***'top display'*** consists of:

- percentage (e.g. the percentage of Ethernet frames transmitted by the displayed Ethernet node in respect to the total number of Ethernet frames);
- display of the node (e.g. Ethernet MAC address with perhaps the corresponding host name of DECnet address);
- a bar graph for visual representation (resolution 2.5%).

The ***'raw table display'*** is just the display of a non sorted internal table. An example is the display of the ARP table.

Each line of a ***'raw table display'*** consists of two values (e.g. the Ethernet MAC address associated with an IP address).

The ***'event history'*** is used to display a chronological log of events (e.g. the list of ICMP requests).

Each line of an ***'event history'*** consists of:

- a time stamp in the form hh:mm:ss.hh;
- a description of the event.

5.1.4. Accuracy

A final remark must be done on the accuracy of the figures:

- some packets are lost, so the load is always higher than indicated if you are using a slow Ethernet controller or a non efficicient driver;
- ETHLOAD relies on the MS-DOS timer which has a resolution of about 50 msec, moreover if the network load is high and you have a powerless CPU some timer ticks can be missed;
- for the busiest and current 5 seconds, the figures are actually computed by relying on the C sleep function which is definitively inaccurrate...

To summarize, ETHLOAD give reliable figure on a medium loaded Ethernet (10% ?) and on a correct CPU 80386dx 25 MHz. In all other case, ETHLOAD can only indicate that your Ethernet is probably heavily loaded and you will have to buy an expensive LAN analyzer!

5.2. MAC Level screen

The MAC level screen can be divided into two parts:
- three statistics summaries: last five seconds, busiest five seconds, cumulative;
- VU-meter of the peak and current load.

5.2.1. MAC Summary

Important figures are displayed for three important samples:
- the last five seconds;
- the busiest five seconds, i.e. the five seconds period when the Ethernet load was the highest ;
- the cumulative since the start of ETHLOAD or the last reset.

For all these samples, the following figures are displayed:
- total number of Ethernet frames: the mean interframe gap is also displayed if available;
- total number of bytes of data: i.e. MAC header + MAC data (the FCS and preamble is not taken into account) and the load of Ethernet in % of the 10 Mbps bandwidth of Ethernet;
- the number of frames containing errors + rate of error per second.

If the datalink driver supports error differentitation (namely all but packet driver), the kind of error is also indicated:
- CRC error (cabling problem ?);
- too long packet (babbling transceiver or controller);
- too short packet (garbage of collision).

If you are using the ODI datalink driver, by using the 'E' command you have access to the MAC source address of faulty Ethernet frames.

5.2.2. MAC VU-meter

The VU-meter is at the bottom of the screen and is graduated in Mbps.

The '>' is the peak marker, i.e. the highest load on five seconds since ETHLOAD has been started or reset.

The bar is the last five seconds marker.

The color of the peak marker and of the bar is changing in respect to the load:
- green under 1 Mbps;
- yellow under 5 Mbps;
- red over 5 Mbps.

5.2.3. MAC Commands

The MAC level screen has three main commands:
- '**X**' to exit ETHLOAD and get back to MS-DOS ;
- '**D**' to go to the DECnet screens ;
- '**I**' to go to the TCP/IP screens.

5.3. TCP/IP screens

to be added

5.4. DECnet screens

to be added