SAPTrack Version 2.0

By Justin A. Jones (jjones@realtech.com)

INTRODUCTION

SAPTrack is a network analysis utility that provides continuous monitoring of Novell SAP (Service Advertisement Protocol) and RIP (Routing Information Protocol) broadcasts, with the following features:

- Identifies all advertised services and networks.

- SAP and RIP broadcast packets decoded, analyzed, and displayed in real time.

- Quick identification of warning and alarm conditions by color code.

- Fast and friendly text-based windowing user interface.

- Sorting of statistics tables by hop count, address, service name, service type, and other fields.

- Does not rely on file server binderies - all information and statistics are collected directly from broadcasts.

- Completely passive - *SAPTrack does not transmit packets and does not effect the network*.

SAPTrack was developed to trouble shoot a problem with disappearing services and routes on a large internetwork. It is a useful tool for network administrators, engineers, and programmers. Use it to monitor, debug, and better understand your network.

You are free to copy and distribute SAPTrack v1.0 by any means you can think of.

NEW FEATURES IN SAPTrack 2.0

- *Multiple Packet Receive Buffers* - Minimize the chance of dropping packets on slow workstations multiple listening Event Control Blocks (ECBs) are posted.

- Statistics Capture - The contents of the SAP and RIP Statistics Windows can be saved to disk at any time. This is handy for documenting the state of the network.

- Packet Logging - All SAP and RIP packets can now be logged to disk in real time.

- Differentiation of RIP Broadcasts - The RIP Statistics Window now filters out broadcasts generated by workstations logging in, and etc. This information is identified in the RIP Packet Window

UNDERSTANDING SAPs and RIPs

Novell file servers, print servers, and other network resources normally advertise their presence every 60 seconds via a SAP broadcast packet. The packet contains the name and address of the service, as well as the number of router hops between the service and the current network.

Novell file servers and routers keep track of all known services and periodically advertise them to other networks. On a NetWare 386 File Server, the information is maintained in the bindery. It can be viewed by typing "DISPLAY SERVERS" at the console. It can also be inspected on Cisco Systems router by entering the command "SHOW NOVELL SERVERS" at the console.

As servers and routers learn about services on one segment they will advertise them on the other segments they are directly attached to. A service advertised on any segment of an internetwork will eventually be advertised by all servers and routers across the internetwork.

RIP broadcasts also occur in 60 second intervals and propagate though an internetwork in the same fashion. There purpose is to advertise network addresses. Routing tables are built from the broadcasts.

Every time a SAP or RIP is forwarded by a router the hop count is incremented by 1. Services are only forwarded a maximum of 15 hops. A hop count of 16 serves a special purpose. It is used to "unadvertise" a service or network that has become unavailable. A NetWare 386 file server will unadvertise services and routes when the "RESET ROUTER" command is given at he console, after which it will re-learn them.

Type "TRACK ON" at a NetWare console to view the view SAP and RIP packets received and transmitted by the file server. Note that a NetWare servers will transmit one SAP for each frame type.

USING SAPTrack

SAPTrack consists of a single executable. The only requirement is for IPX to be loaded (IPX.COM or IPXODI.EXE). Neither SPX or NETX is necessary, but it is a good idea to have a mouse driver loaded. There are no command line parameters - just type "SAPTRACK" and go. The interface is very intuitive and all options are available from the pull down menus.

When SAPTrack starts, the statistics windows are open. Updating the packet and log windows steal mucho CPU cycles, so keeping them open on a slow machine or very busy network may result in packets being dropped. It is therefore recommended that these windows remain closed when not being viewed.

Statistics Window

The SAP and RIP statistics windows are open when the application starts. One entry appears in each table for each service and each network. The tables are updated every time a SAP or RIP broadcast is received, even when the window is closed. Following is an explanation of the various columns in the statistics window:

COUNT - Indicates the position of the entry in the table.

AGE - Indicates how many seconds have passed since a service or network has been advertised. Stable entries are green, but turn yellow when the age passes 65 seconds, and red after 125 seconds. Unadvertised services will turn gray.

INT - The time interval, in seconds, between the previous two updates received.

TYPE - Indicates the service type. Values between 0000h and 8000h are reserved. The following well-known types have been defined by Novell:

Wild	FFFFh
Unknown	0000h
Print queue	0003h
NetWare Server	0004h
Job Server	0005h
Print Server	0007h
Archive Server	0009h
Remote Bridge Server	0024h
Advertising Print Server	0047h

HOPS - The number of router hops away the service or network is.

INTERNETWORK ADDRESS - The service address.

NAME - The service name.

TICKS - The number of clock ticks away the network is.

Log Window

The log windows displays SAP and RIP advertisements as they arrive. The newest arrival are added at the end. The logs scrolls upward when maximum number of entries is reached. Entries with hop counts greater than 15 are automatically grayed.

Packet Window

The packet windows displays the contents of the most recent SAP and RIP packets. Notice that each packet contains multiple entries.

ABOUT REALTECH

RealTech Systems Corporation is a systems integrator providing LAN, WAN, and Internet integration solutions. For information call 212.695.7100 for information or send e-mail to info@realtech.com.

DISCLAIMER