Network Monitoring
Originated by William L. Fanning on Mon, 02 May 2011

Originated by Bill Fanning on Mon, 02 May 2011

All,

Can anyone make a recommendation on network analyzer software and hardware (TAP or port mirroring switch)?

I want to get a look at both our HiSeasNet and FBB traffic as it leave/comes aboard the ship. First, I want to see who/what is the bandwidth hog (if we have one...) and would also like to troubleshoot some mail issues.

I have looked at Wireshark and Capsa from Colasoft. Both are free but I would appreciate any suggestions before I commit time and energy into the learning curve.

Thanks,
Bill

William L. Fanning
R/V Endeavor Technical Services
URI Graduate School of Oceanography
Narragansett, RI 02882

Reply From: Geoff Davis on Mon, 2 May 2011

Hi Bill,

I tend to use wireshark for low-level protocol debugging, because it runs on pretty much any UNIX-like system as well as windows.

Regarding finding bandwidth hogs - you might want to take a look at NTOP (ntop.org). NTOP is good for trying to find bandwidth hogs and can tell you who is talking to who, both on your local network and local to remote connections.

Geoff Davis
Scripps Institution of Oceanography

Reply from: Steve Foley on Mon, 2 May 2011

I have been using nfcapd/nfsen to capture and analyze netflow streams from routers. NFSen seems to be a little touchy to get working quite right for web based analysis, but the nfcapd stuff that it builds on seems pretty solid and has some scriptable tools for simple analysis of top ten talkers and what not.

-Steve

Reply from Robbie Laird on Mon, 02 May 2011

Hi

I would second ntop, it works really well. It allows one to see which ip address it using all the bandwidth and which address ashore it's going to.
Like the guy who was running the Carbonite software, (full backup to off site), on his computer and did not know it. The one problem with this is that we
(administrators) end up looking at who is going to which sites. While I'm confident that this is perfectly legal, since we all own our systems, it might be a surprise to the users. On the other hand, it's something that overly trusting users should be more aware of, since we are not the only point in the chain where this can be done.

Robbie

Robbie Laird
WHOI/SSSG

Reply from John Haverlack on Mon, 2 May 2011

Hi William,

I might recommend http://www.network-weathermap.com/?vs=0.941 though I've never personally set it up. I believe it can poll SNMP data from Cisco (and probably other) switches and routers for traffic data.

The University of Alaska system uses it to generate the following interactive traffic map:
http://weathermap.sw.alaska.edu/wan.html

I think they also integrate MRTG with the weather map to show graphs of data use over time. Again I'm not sure on the details.

Another application that may provide what you are looking for is CACTI. http://www.cacti.net/ I've had some success with Cacti in the past as a data collection tool.

The trick in any case will be configuring the data sources to mine the data resolution that you are looking for.

For that you could use a dual NIC linux box to filter traffic from the internal to external networks and collect per IP data on packet sizes using TCP dump. Linux can be set up as a bridging firewall such that the traffic does not even see the firewall as network hop because neither NIC on the Linux Firewall has an IP. To IP traffic this firewall is transparent. This is possible, but would require considerable setup.

I hope this helps.

Regards
--
John Haverlack
IT Manager, School of Fisheries and Ocean Sciences
University of Alaska Fairbanks
Fairbanks, Alaska 99775-7220