From: Teresa Beamer <BEAMER@DENISON.EDU>
Subject: Minutes from December 12, 2001 OARtech meeting
To: OARTECH@LISTS.OAR.NET

OARtech Minutes 12/12/2001

Introductions
AFIT - Paul Bergeron, Tim Fox, James Reynolds
Anitoch University - Bruce Friend
Ashland University - Simeon Ananou, Brad Frederici
Bowling Green State University - Mike Smith
Case Western Reserve University - Eric Chan
Cedarville University - Alan McCain
Clark State Community College - Hugh Evans, Jim Gossett, Steve Hurley
Denison University - Teresa Beamer, Marshall Chris
DeVry Institute of Technology - Dave Leitch
Edison Community College - Jeff Collett, Harry Lawhorn, Bert Waldrop
Heidelberg University - Kurt Huenemann, Sean Joyce
Kent State University - Ransel Yoho
Lakeland Community College - David Levine
Lorain County Community College - Steve Clutter
Miami University - Tim Gruenhagen
Mount Union College - K. John, Tina
Mount Vernon - Tim Myatt
NASA Glenn Research Center - Dave Pleva
NEOUCOM - Bill Mayhew
OARnet - Christopher Cook, Ruth Crites, Fred Crowner, Doug Gale, Weiping Mandrawa, Bill Miller, Linda Roos, Jodi Santini, Paul Schopis
Ohio Dominican College - Arron King
Ohio Northern University - Bob Beer
Ohio University - Marina Bykova, Curt Flood, Royce Holiday, Brandon Saunders
Otterbein College - Jeff Kasson
Owens Community College - Bill Bowser, Marty Stroud
Packeteer - Sean Applegate, Mike Driscoll
Sinclair Community College - Roslyn Taylor
Southern State Community College - Dennis Grifford, Josh Montgomery, Bob Snellman
Univeristy of Akron - Tom Bordonaro, Debbie Keller, Randy Woodling
University of Dayton - Tim Harrington, Ronnie Wagers
University of Findland - Mike Pifer
University of Rio Grande - Kingsley Meyer, Michael Snider, Mike Snider
University of Toledo - John Heiden
Wright State University - Shane Dawalt, Larry Fox, John Pearson, Patricia Vendt

Xavier University - Mike Bowling, Carl Dichaus, Gordon Suggs

Minutes were approved.

Question posed to the group: How many sites are getting the NetPD notifications? A show of hands indicates about 7 sites. These are notifications are notice of copyright violations. Rio Grande actually disconnected user until the end of the quarter. Others have sporadic response, no response, some responded to all. This afternoon we'll be talking about how schools are responding to these problems.

Ruth Crites
Pick up copies of the Memorandum of Understanding and the Annual Report. The Memorandum of Understanding is your contract with OARnet.

Linda Roos
2 new SEGPs - Hiram, and?
There will be certification classes in January for using the H323 and use of video conferencing bridge.
What I2 initiatives are available to the SEGPs? Middleware I2 initiative is open to SEGP participation.

Albert School
Middleware initiative - Albert has been doing some work on secure video conferencing. He had a meeting with 12 people from around the world at NC-CH to see what the different players in the video industry would be willing to put into their products. This is kind of a niche area of middleware. Also, middleware authentication services are being worked on, specifically with public key infrastructures. He has built a test infrastructure working with PKI certificates. It is past the demo stage, but is interested in getting people to do testing. He has been working on putting credentials into a smart card. He would be interested in working with anyone that is also working on this technology to test for interoperability. He would be willing to come out and help people setup up and consult about their infrastructure.

Gene Wallis via conference call
There was a handout on "Standard Practices for Network Management". Network Management can affect the quality of the bandwidth available. These are basic suggestions for keeping the "scrap" packets off the net. Thus helping to prevent the DOS attacks. Some attacks to some sites in the past have been as high as 80Mb. This isn't really bandwidth management, but does affect the bandwidth or can cause disruption to the network. There are local policies affecting bandwidth usage as well as legal aspects.

What do schools feel OARnet can do now to affect the bandwidth? Many of the things must be done at the users site on the end servers. The only way OARnet can affect servers is to run the servers - which may or may not be feasible. Other things that OARnet can do are to provide access to resources to help the sites see their use of the net, to provide more information to the sites themselves.

A comment on the handout - the client router is the router at the client site that provides the connection to OARnet. The border router is the OARnet router that terminates a transit carrier's connection.

Where is the router for the gigaman project going to be placed? This has not been determined.

What other services do we want OARnet to provide? OARnet is looking for input from the clients as to value added services that clients would like to see. They have been looking at remote testing sites that would allow clients testing from and possibly for H.323 testing sites. This would allow sites to check out response time issues, routing issues, etc.... Ohio University is doing this by putting a machine in OARnet central site and it is a very valuable service. This gives testing from OARnet back to the client sites.

Can you give us an update on ipv6 and how it will affect us? Ask Paul about this.

On the common carrier legal issues, does that apply to port specific traffic - is it considered editing/publishing data? However if you open the packet and made a determination based on the content in the packet, then you would be in publishing, editing arena. Could you have a packet shaping or bandwidth control device? You are only a publisher if you look at the data payload, looking at headers does not fall into that category. One of the things to think about is the possibility of coming up with something common or broader types of services that OARnet can provide.

Paul Schopis
Weather Map Project
Specifications - used ifxTable from RFC2233 that allows them to provide 64 bit counters. They used Perl 6.6.0, Net-SNMP, Ploticus, Immunix, Apache.

See http://monitor.oar.net;8080. If you go to this address you get a menu, select the weather map option and you can see a state map. If you click on the link you can see the statistics for that day. The current version of the

software is considered beta. You are able to query for historical data. The map is color coded, based on the traffic. The links shown are between the main pops. They allow you to see the data as graphs, as processed data, and as raw data. This service is available now, but it is beta. So if there are problems, please let them know. Feel free to turn this over to your NOC to use. Please look at the site and give them suggestions.

What about protocol breakdowns? That is not part of this project, but is part of the netflow project. Is there value to see the critical points? They need to look at cost versus the value it can provide. The netflow project goal is looking at the control of traffic between various government sites. The question is can they with verify that the use and the routing policies are working properly.

IPV6 status
Any requests for IPV6 connectivity should be directed through Linda. Abilene is getting ready to crank up their V6 DNS server.

Jodi Santini
Remedy Web project
To main page and select the Remedy web project under the support links. This can be used by site NOCs, but they will need the most current java applet and IE55, as it is somewhat quirky with Netscape. You log in using your client number and stats web password. Then you can view open tickets as well as view all tickets for last 30 days. They will only provide the login information via the listed contacts for sites.

Comment from the floor - what about sending the password to a predetermined address for a site with a password query via a button? Everything is running on a secure server, and they try to provide security as best they can. If the group would like passwords to be emailed to a predetermined address instead of or in addition to the phone contacts, they can provide that.

Patty Vendt
In February we are looking to have the FBI and some of the their security people in to talk about incidence response.

Clifford Collins.
Web Sensors project - Detecting CyberTerrorism
The slides for this presentation are available on the ENSS web site: www.enss.net

Cyberterriorists are terrorist groups, sympathizers, anti-US groups, and

thrill seekers. They deface electronic info, use DOS attacks, attack critical infrastructure and/or corrupt critical data.

Http://Defaced.aldas.de - catalog of defacements that have been reported.

They are more likely to attack during specific events, both political and military. Past statistics show activity does go up in response to specific events.

First install the GPL open SSL package on an independent server, then generate a known good checksum for the top-level web site. Initially they run a cron job on an hourly basis to execute the script. It compares the current checksum with the stored checksum and will send out an alert that the page has been changed.

Their current effort is to develop a web based service for monitoring the web pages and servers. They provide multiple notifications, update check sums, vary the polling frequency, allow stock and custom notices, and log the changes using an XML based configuration. They are using an SSL web server that receives the configuration file from the web sensor daemon that polls the various web servers and can send email to the user's mail. They are writing this in perl.

This is a work in project, and will be free when it's functional and will be open to suggestions, and contributions.

Humblenet
The lab is open, fully operational, and it can be accessed remotely. They haven't had too much requests for access, so they are still determining how to make it available. They can provide testing for firewalls, PKI, smartcards, etc.... Contact Clifford Collins if you are interested and to get access.

Doug Gale
Dark Fiber project
The project has been dropped. Mission Communications was not able to raise enough funding. They did not go bankrupt, but just closed the doors on this project. The project is history.

What does the future hold? Right now the most likely is with Williams Communications where they have extra fiber that they have indicated they may be willing to sell. OARnet would have to purchase 2 rings minimum. They are meeting with folks from other states to determine how they might be able to share the costs. The other vendors are not near as attractive. They have a

couple of good alternatives and a couple of long shots to look at. The good news is it would provide a good starting traffic and provide bandwidth in the high bandwidth corridor. However, it does not address the local loop issues. It's not what we were hoping for, but it is better than nothing.

Is there anything happening at the state level? They are working with the state on this initiative and other's that may come up. He doesn't see DS3 postage stamp rates occurring. They are looking at wireless options, as well as dark fiber solutions to local loop issue.

What about the AEP fiber project? They are using some fiber from AEP to connect to OU. AEP is now a part of another company and they are having problem continuing contacts with AEP as they move to a larger company America Fiber Network. However, they have some fiber in corridors that it is not available by other means and so would like to continue to pursue that option.

Lunch

Packeteer Discussion
Format - Sites will talk about how they are using it. Then Shawn Applegate, a systems engineer from Packeteer, will answer questions.

Miami - Tim Gruenhagen
Been using Packeteer for 2.5 years. They are pushing the envelope on what the packetshaper will carry. They discovered Napster before they new what it was. They had already limited the traffic when the big use hit. Their traffic classification has been evolving. It requires constant tweaking, and support. When packetshaper technology came up, the technical people don't make the policy. A policy committee defines the policy. They give general priority based on generic classifications. They have carved the residence halls as a separate traffic class. The only application actually blocked is the Napster directories. Other low priority applications are given a low priority or low bandwidth. They don't do a lot in conjunction with the firewall. Limits are more on class of service. Currently, they have 60Mb to the Internet.

Rio Grande - Micheal Snider
New to Packeteer - only had it on campus for 2 weeks. Only thing they have done so far is to implement policies that were already stated in their resnet policies. Bandwidth is back down to where it was 2 years ago. They are blocking the peer-to-peer apps. Made a major change in his network. Resnet has 200 users. Before shaping traffic both T1s were full.

Denison - Chris Marshall

1700 student registered for using the network. Geared originally toward stopping off-campus traffic. All peer-to-peer from off-campus goes into a 600k tunnel. Half the T1s can use outgoing peer-to-peer, but only at a lower priority than other traffic. We have Acamai /Ibeam web caches are an issue.

Cincinnati
Packeteer 1.5 years
14000 students, 3 T1s
Created a separate partition for entertainment such as peer-to-peer, games and instant messenger traffic. Starting to max out with standard web traffic. They will begin to move a partition for Resnet as they increase their network Internet links. When they maxed out the packetshaper, they find some strange things happening but it has made life much more livable.

Case Western
OC3 to I2, 36M to I1, 3-4000 students
Packetshaper 6500, install 1 year ago
Before it was installed their lines were constantly maxed out. They hooked it up right out of the box and found it useful for identifying traffic. They have configured the Packetshaper by classifying by subnet instead of by application. They want to find the top talkers, and not restrict by application. They do define a group with Napster, and Kazah and only allow 5Mb outbound traffic. From their student subnets, they found ftp servers, and other server that use the higher number ports are taking up the traffic. They are now restricting, and capping traffic by IP address. How are you assigning IP addresses? They use DHCP. They use dynamic partitions. Each student subnet is 2000 addresses, but the Packetshaper is limited to 1024 dynamic partitions.

Shane, Wright State
DS3, 21Mb I1, 3000 students
The Packetshaper was in place when they had about 600 in Resnet. The Packetshaper had worked great for controlling the Napster type traffic. The reporting features are great for finding out what is there. He would like to see a limit on the number of connections through the packet shaper. They are seeing lots of HTTP traffic as well. He thinks that some of the http traffic is something other than web surfing.

University of Dayton
24Mb
They found that users are sharing full-length movies and have been talking to the top talkers. They have 2 Packetshapers: An Internet Packetshaper and a firewall Packetshaper. This controls the number of connections to the

firewall. They initially used service classifications and lately have been going after the top talkers. They have started restricting outbound file sharing traffic but found that affects the inbound file sharing traffic. They spends 2-3 hours a day doing maintenance.

It seems that there is an unusually high usage of http on several campuses. If you connect via http to Kazah on a specific port 1214 then all that peer-to-peer looks like http to the Packetshaper. You might want to use a mime type streaming classification.

Sean Applegate, Packeteer

About 380 - 390 schools are using Packetshapers. He knows about some schools using other products - e.g. netflow, etc.... If you use rate shaping, the Packetshaper can work well with netflow using committed access rates.

The Packeteer theory - all applications are not treated equally. Some applications are mission critical such as email, web surfing, and streaming video. The Packetshaper can tell you what you are spending your money on.

Version 5.2 will be released this week. Their products include Packetshaper, AppVantage, AppCelera, PolicyCenter (management station). The Packetshaper is based on PSOS and classifies 350+ Apps at OSI Layers 2-7.

Hint: To get more history at the command line go to http://url_of_packetshaper/cli.htm

Ohio has higher Ed users than any other state. Use Randolph Macon College as an example site. They automatically classify 350+ apps at OSI layers 2-7: peer-to-peer applications include aimster, audoio, galaxy, cutemx, directconnect, gnutella, hotline, imesh, kazaa/morpheus, napster, and scour.

To implement good policy use a four-step process: classify, analyze, control, and report.

The ways to classify traffic include: 1. Check by inbound/outbound; 2. Protocol family; 3. Service; 4. Inside/outside server; 5. port; 6. proxy; 7. IP address, mac address; 8. Subnet mask; 9. URL. He went through talking about how you want to setup the above-mentioned classifications so you can find out what kind of traffic you have. Then you look at what the top talkers/listeners via traffic discovery. The classification tree is sorted from the top down.

After you have classified your traffic, you need to analyze your traffic to find out what is being retransmitted, and see how effective your usage is. Check your top ten protocols that are doing transmitting. You can see top ten users, Response time summaries, (he likes the normalized network delay), transaction delay time shows where the bottlenecks might be.

Control - How do I control the traffic? You can set the policy by rate, priority, never-admit, ignore, and discard. Rates allow you to allocate guaranteed bandwidth specific classes. The default priority is 3. The never admit policy is used to block things like Nimda. Rate policies get evaluated first at their priories. It uses a proactive rate control to speed up the latency sensitive flows and smoothes out the TCP transfers. Queues will delay packets and can lose traffic as the queue fills up. They can rate shape UDP traffic, but it is not as good as TCP.

Partitions create a virtual pipe to aggregate traffic and to limit traffic classes or to protect traffic. Dynamic partitions will automatically setup and take down partitions based on the active users. He has seen generally outbound peer-to-peer is given about half the pipe, while inbound peer-to- peer is given a lot less.

There is time of day rate shaping, but it is only available via the CLI interface:
Schedule <time range> <cmd> | <-f cmd file>
Use schedule show to see scheduled items.
Use schedule delete # to remove scheduled items.
The schedule commands are stored in ram only so you must create a startup.cmd that is executed when the box reboots. When rebooting use "run startup.cmd".

Reporting
You can use CSV, SNMP, XML and plugins for third party products for importing data from the Packetshaper. The event reporter can notify you via email or SNMP trap to warn you about poor performance in case of DoS attacks. It notifies you when an event occurs. This is setup via command line. You can create your own events or use their pre-defined events. These settings are stored in the ASCII configuration file.

Tools available: http;//support.packeteer.com
Includes a boiler plate reporting portal
majordomo@lists.stanford.edu body subscribe packeteer-edu
archive http://www.stanford.edu/group/networking/netlists

sapplegate@packeteer.com

Showed an example of reporting scripts.

Meeting adjourned. Next meeting in February.