OARtech minutes
12-Feb-2003
Taken by Teresa Beamer

Meeting started at 10:00 by Tim Gruenhagen

Attendees:
Antioch University - Bruce Friend
Case Western Reserve University - Eric Chan
Cedarville University - Gabe Custer
Central State University - Showkat Choudhury
Clark State Community College - Steve Jaworski
Columbus State - Jim Buncan
Columbus State Community College - Chris Scanlan, Shane Stewart, Jim Webb
Denison University - Terri Beamer
DeVry University - Dave Leitch
Kent State University - Jim Li
Lorain County Community College - Norm Lease
Miami University - Tim Gruenhagen, Joe Simpson
NASA Glenn - Dean Harter, Dave Pleva
NEOUCOM - Bill Mayhew
OARnet - Christopher Cook, Ruth Crites, Aaron Lafferty, Linda Roos, Paul Schopis, Al Stutz, Gene Wallis
Ohio DAS - Michael Yerian
Ohio Northern University - Bob Beer
Ohio State University - Brian Moeller
OhioLink - Anita Cook
Otterbein College - Jeff Kasson
Sinclair Community College - Steve Hurley
UA - Debra Keller
University of Cincinnati - Diana Noelcke, Tom Ridgeway
University of Dayton - Ronnie Wagers
University of Findlay - Mike Pifner
University of Rio Grande - Tim Bramhall, Kingsley Meyer, Mike Snider
Wright State University - Shane DeWalt, Patty Vendt
Xavier University - Mike Bowling

Minutes approved.

Introduction - Attendees are to mention their current projects.

Miami University - IDS, developing procedures to deal with the problems illuminated by the IDS. Using Red Siren $2000/mo and feel it's worth it. One sensor was brought up and within an hour they found an attack on the engineering department.

NEOUCOM - Wireless

Denison University - We are preparing to go into new buildings.

Wright State - They are working on single sign on, and upgrading their core with Cisco 4000, and 3550s.

Case Western has been setting up an Alliance for the members to purchase Cisco equipment through. They setup the discounts and have made them available to OARnet sites.

DeVry - Major renovation on all of their networks moved from Nortel to Cisco. Setting up a remote classroom.

Rio Grande - They are finishing up a network install from last spring. They got hit with Slammer.

Case Western - Continuing to upgrade gigabit network on campus. Continuing to deploy wireless.

Cedarville U - Wireless, NetWare VPN server, replacing core this summer. Looking at Cisco and Extreme networks equipment.

Antioch - Integrate 3 campus networks into 1 network.

Columbus State Community College - They are bringing their email system in-house and will put logins in their labs.

Kent State - Hit with Slammer, 12 machines were hit. Didn't have access to routers when the worm was active. Very interested in the Packeteer presentation. They have rigid caps on their residential net, even though not hitting the caps the student traffic seems to run at a crawl.

Comment: when you setup a control on the Packeteer on one class, it can affect other classes.

Baldwin-Wallace - Looking at Cisco's long-range Ethernet to implement in their stadium.

Lorain County Community College - They're upgrading the cable plant, wireless input, but found a Trojan that was effecting their network equipment.

University of Cincinnati - They are bringing up the research center on the metro ring. They have brought several sites up on the ring. Also looking at unified voice mail system, looking to take email to one platform.

University of Finley - Bringing 2 new buildings up next summer, and bringing up new firewall. They are using Iplanet, and doing an active directory migration.

Xavier - Admin systems replaced with SCT Banner and will be moving off VMS. Slammer did not affect them. They have wireless using leap with mac filtering.

University of Akron - Brought 2 new buildings on-line and going to a 10-gig backbone.

The White Paper is on Debbie Keller's web page - she will give the URL and show what is there later in the meeting.

OARnet
Academic Services - Chris Cook - OARtech website
There has been some interest in moving the OARtech website to the OARnet website. Is this what you want? There was some discussion that there is nothing on the site that is proprietary. There was a motion, seconded, and passed. Chris will coordinate with Ransel to make the move.

ITEC - Linda Roos, Paul Schopis, Steve Gordon
Al has asked Steve to take ITEC after Pankaj's left. He will work with OSC and remote collaboration, and distributed computing with other universities. All the projects they are currently working on will continue (Netflow, and others). He sees lots of opportunies with ITEC and I2 that can benefit Ohio. ITEC is the testing site with I2 for operational issues and also with Abilene. OARnet provides the staff for the testing.

Beacon 1.1 is released, 1.2 is to be released in March. It was designed so the end user should be able to download and run it.

Is there any movement to get a test response site/network measurement sites within OARnet for the OARnet sites? Working toward this, but not setup yet. They see Iperf as a good test tool, as it can test UDP and TCP. Problem could affect TCP and not effect UDP. There are other tools; he will send a message to the list with the info. End-to-End QoS? You can do QoS, but end-to-end is not available yet. Unless you have OARnet controlling into your domain, you can't get end-to-end QoS.

Dark Fiber Project - Al Stutz
There is lots of interest in getting the cart before the horse. Remember that we are in
Phase 1: the backbone. The money will be saved at this phase to pay for the fiber.
Phase 2 is bringing in the 4-year state funded and research universities and where it makes sense, other institutions.
Phase 3 is bringing in remaining institutions.

CERN is alive, Cincinnati Education and Research Network - used the same lighting gear that is being considered for the Dark Fiber project.

They are looking at other names for the Dark Fiber project in case there are state funding problems with TFN. They have already paid $2M+ and the contracts are signed. Specifications for the network interconnect builds are being finalized. Spectrum is getting bids and will review them with OARnet. Until they get the bids, they don't have a good schedule. They expect the bids to be < $1M.

Architecture, Lighting, Engineering committee (ALE) are developing best practices document without consideration for costs.

Pricing Committee is developing a model for charging without consideration for cost. Costs will then be mapped out. They would like the model to include the foundations of the expenses and plan them out so they can then determine the costs for the services. They are getting some interest for private lambdas on the network.

Implementation committee is discussing the planning and implementation strategies including segment test strategies.

Partnerships
Schoolnet has made a firm verbal commitment to participate. MOU is currently being drafted. They are willing to co-build the OARnet legs. This may create a need for a new advisory/oversight group. They have been having some discussion with Schoolnet, IUC- CIO's and Osteer, etc....

We need your help! Anytime you talk about the network emphasize that we are building the worlds most robust network for research and education. We are willing to come to your campus and talk about the new network with your campus community. They want to do things that push the fringe of networking.

The Governor is supporting the plans. His science advisor is participating. We hope to be briefing DAS soon and will have a rollout to media in mid-April.

How are the communities learning about the project? They have been keeping the information quiet until after the contracts were signed. This should be better after the April rollout. Most communities are finding this out via the education organizations.

Gene Wallis
OARnet has some more expensive contracts that are phasing out, and bringing up connections via the quilt contracts. (e.g. taking down Sprint links and bringing up Level 3 and Cable & Wireless which are part of the Quilt consortium). This brings down the costs of the links. As part of the new network, they will be looking at re-locating some of the pop sites. Because of this there will be a transition phase that will have to occur. They will

try to keep us aware of what it happening.

What kind of time frames? Hopefully as of this week they hope to have all contracts for additional connections done. Next step will be to get the quotes in and the plans for the integration pieces for the new network. One of these is the primary long haul fiber site for Columbus as well as the 2 fiber rings in Columbus, to OSU and other locations. Also they are concerned with the pop locations in Cincinnati and an integration ring to connect Williams and AEP fiber. Cleveland will be connected via the AFS ring that is currently being built. Integration costs will be well within the budget. They will need to build interconnects between existing and new sites. These will be planned in parallel with the equipment specifications.   Looking at September for really seeing active links.

How far on fiber do you have to go before you have to have regeneration? About 50-70 miles.

Looking to bring up the Cincinnati ring and the Cleveland ring first. They are bringing it with SONET as the base, so that they have some protection, and redundancy in the first cut. Then they will transition to GigE.

What about School Net, what model will they use? Gene wasn't sure. But the move can be done in pieces.

Tom Ridgeway, H.323 committee
This committee grew out of the problems with firewalls and video conferencing. There was some testing with firewalls. The lower powered firewalls do mangle the packets. The higher-powered firewalls can participate much better. There is a problem they found with the PIX firewalls in passing smart flow packets. Problems weren't so much the firewall at the high end, but port problems. They also found Ridgeway systems software that can help in dealing with the protocol issues on firewalls, and NAT.   They will write up a summary. OARtech would also like to have a best practices document.

Anita Cook, Ohio Link
The video notice has been sent out. They are expecting you to use the free version of Real. They will start putting the videos up in April. Ohio Link is responsible for digitizing the videos. They are looking for institutions that are willing to help them with the digitizing.

Has their been any testing with caching? Not been given permission to do the caching. They are still working with the vendor to get the caching issues worked out. They have no idea how much they will be used.

Lunch.

Debbie Keller - White Paper
A new and improved version is available the website:
http://gozips.uakron.edu/~keller/whitepaper
She will email it to the OARtech list. The section that says "contributed by ...." no one has signed up for that topic. "Planned by" sections have been assigned to the person indicated. Feel free to let Debbie know if you are willing to do a section. The policy sections needs to be done by Osteer members.

Net Flow - Patti Vendt
The committee met Jan 16. They setup the goals of the project and did an overview. Some decisions were made on some report options. Mark suggested they go with 25 reports. 6 combo reports with information from each of the participating schools were decided on: protocol, source prefix, source tag, type of service, and ASN. Reports will be available much the same as the current statistics reports. They also looked at what is currently available from OARnet statistics. They hope OARnet would look at this preliminary information to see what it would take to look at an alternative statistical model. The question was asked who would be interested in having OARnet look at an alternative - 17 indicated yes. They plan to have the pilot in place by the end of April.

Security subcommittee will have their first meeting at end of March. If you are interested in participating on this subcommittee, let Patti or someone at OARnet know.

Packeteer Inc., Sean Applegate
There is a certified training partner in Dayton. This new trainer is Mike Solomon with Stratecache. There are only 4 certified trainers in the US as the trainers go through a pretty strenuous program to become trainers.

There are 5 partition strategies that can be used:

Flat auto-discovered.
Flat with Logical Folders is popular on some educational sites.
Divide and Conquer by subnet/address ranges is also popular in education.
  However, you have to have a strong enough box to do this.
Per user limiting the dynamic sub-partitions. The deeper the dynamic
  partitions the harder the box has to work. The per-user limit has had some
  problems and is very dependent on the version of code you were using. It
  doesn't work real well in the over subscription model. They don't have many
  universities using this method, but some ISPs.
System limits. Checks the limits of the box to set the number of partitions available.

They can't do bandwidth limiting on dynamic hosts.

Kazaa they block the upload traffic and it makes a big difference on the bandwidth.

Classifications
OSI Layer 2,3, & 4 are immediate and are very efficient and fast. Layers 5-7 do not classify immediately and require more processing power as it takes more then one packet to classify. You will see some of these get reclassified as time goes on. If you have flows that don't go away, the state table needs to timeout the flows.

If you see a lot of things falling in the default bucket, it may mean the box is too busy. Two main OSI layer 5-7 processes - appness and magic, these use roughly 50% of the memory. If the device is busy it will classify to the best of its ability, but it may be more coarse level classifications (e.g. NIMDA, Code Red may be seen as http). If the box is too busy then look at the high-water mark on the memory usage for a classification and see if TCP allocations fail. Set an event on your box that notifies you when you have a lot of traffic coming in without return traffic. See TCP Server ignore in the TCP Server percentage metrics as these go up it may indicate a DoS attack.

Useful commands:
Traffic flow
Tr flow -a (show all flow data)
Tr flow -c class (show info for class)
Tr flow -o (summary information)
Tr flow -V service (looks for a particular service type)

Tr h f 192.168.123.161
Walks through the tree to see what this IP is doing.

Tr h r /inbound /default
Show traffic history recent for class to find the top talkers. Basically looks at the last 10 flows.

Hostdb info
-sf sort by flow per minutes in descending order
-sr sort hosts by current rate in descending order
-n # give number switch to specify the number of hosts to display
ex: hostdb info sortrate -n 35

New Features
Packetlog is used to log packets. It can add, remove, set on/off, set limit, and show status. The log is in tcpdump format in 9.258/pktlog directory. The buffer size depends on the Packetshaper model.

sapplegate@packeteer.com

Kazaa 2.0

Uses UDP 1214 for Queries. So it is best to use a discard policy. Uses multiple flows for each download, which means more flows per host. Uses dynamic or user assigned ports and http for some transport.

They rewrote the patterns/headers for OSI layer 7 packets. They break out uploads, downloads, and queries. You can use the traffic reclassify command to build a list of super node flow comparisons. Goes through the data every 15 minutes to reclassify the data for the layer 7 patterns. You can eliminate the tons of flows by discarding uploads for Kazaa.

The 9.256/log directory has logs that can show you why a shaper crashes.

The most efficient matching tree is the one auto discovered. Fewer classes get faster performance. The tree sorts from the top down and by branch. It skips over the children classes if the parent isn't matched. Every flow is compared to each exception class. If you have a lot of exceptions, then you add a lot of overhead. The most current version is 5.30.

Optimizing your tree. Turn off auto-discovery and eliminate unneeded port classes, and unneeded exception classes or folders. Rollup multiple host classes into fewer classes using host lists, this will save some of the classification time. Leverage the parent/child tree structure for application classes go from general to progressively more specific rules.) Try not to break out classifications and keep them within their parent classes.

Next Version
Super Chief is the next feature release. It has been in beta test since November/December. It has application traffic acceleration, improved security: SSL/SSH management sessions, SSL is signed by Packeteer. Support for a redundant or more complex environment. It can connect 2 Packetshapers to talk so they can work together (I1, I2 issues) and allows backup, and restore of line data. It can schedule functions. Partitions are added that you can set as % of the link size rather than a fixed number. Pie graphs of class and children will be available. You can create custom interface portal for others to look at a selection of reports.

With Redundancy as an objective, they have re-architected the direct standby options to have fail over to work better. I1/I2 sites can have 2 Packetshapers with a redundant path between both Packetshapers.

Showed some example of hot standby configurations.

Access-Link Monitoring - polls the interfaces to understand the differences of the interface usages and is Packetwise 6.0. It polls the router for interface status and access link utilization and provides access link mirroring.

2 modes of operations - basic mode automatically adjust the in/out bound partition sizes based on the link state.

The scheduling has been put in the web page. It has day option and no longer needs the startup.cmd file. You can set time ranges, for maintenance windows. You can have the results of procedures emailed to an address.

Uploading or downloading files from the Packetshaper for common operations no longer has to be done via ftp. It can be done via http for configuration files, crash files, logs, etc.... You can create a web interface screen that simplifies repetitive tasks to allow other users to do common tasks. You can do any command with variables that can be entered by the users. It basically uses XML.

New protocols - http tunneling will be discovered as will new VoIP technologies such as SIP, MGCP and MEGACO.

There will be the ability to setup partitions by %.

New shaping status on graphs to indicate if shaping is on or off. New variables have been included to provide better visibility into the load on partitions relative to the configured sizes. This helps with late-drops (too much high priority traffic for all the traffic get through) and scheduled-drops (too much traffic for partition size).

Recommends that you use the report-portal to build your reports.

There is a new Netele 2 plug in available from support.

If you have a class, but no policy, then it is probably a candidate for clearing it out, unless you want a measurement.

Packeteer is looking at Net Flow for possible additions.

Possible Topics for April meeting: IDS or Wireless

Meeting adjourned.