Subject: OARtech October Minutes

OARtech meeting
October 9, 2002
Minutes by Teresa Beamer and Bill Mayhew

Meeting started at approximately 10:00 in 3rd floor conference room of OARnet building, North Star Road, Upper Arlington. Tim Gruenhagen, chairperson.

Attendees:
Air Force Institute of Technology - Tim Fox
Ashland University - Simeon Ananou
Case Western Reserve University - Eric Chan
Cedarville University - Gabe Custer, Alan McCain
Clark State Community College - Hugh Evans, Steve Jaworski, Romy Lu
Cleveland State University - Rodney Ehlert
Columbus State - Jim Buncan
Denison University - Terri Beamer
Dept. of Admin Services - Mike Yerian
Heidelberg College - Kurt Huenemann
Kent State - Lyod Park
Lorain County Community College - Norm Lease
Miami University - Tim Gruenhagen, Joe Simpson
NEOUCOM - Bill Mayhew
OARnet - Gene Bassin, Christopher Cook, Megan Crabb, Bob Dixon, Arif Khan, Aaron Lafferty, Brian Moeller, Linda Roos, Paul Schopis, Pankaj Shah, Al Stutz, Gene Wallis
Oberlin College - Art Ripley
Ohio Board of Regents - David Barber
Ohio Northern University - Bob Beer
Ohio State University - Gabe Moulton
Sinclair Community College - Steve Hurley
Terra Community College - Tim Kincaid, Kathy Minton
University of Akron - Randy Woodling
University of Cincinnati - Dave Dessauer, Perry Morgan
University of Dayton - Darryl Egbert
University of Findlay - Mike Pifner
University of Rio Grande - Tim Bramhall, Kingsley Meyer
University of Toledo - John Heiden
Wright State University - Patty Vendt
Xavier University - Gordon Suggs

Introductions - Some people are reporting sever Packet Shaper problems following release of Kaaza II on September 25th. Question of the day: What are you using to manage Internet bandwidth? Have you had any new problems this school year, e.g. Kazaa version 2?

Miami's solution was to ban Kaaza traffic completely. Gnutella has increased since banning Kaaza.

Kent reports that they are getting several new border routers and two new Packet Shapers to improve service to the residence halls.

Wright State has added bandwidth, but the dorms are still taking up lots of bandwidth. They are moving to a 100% Novell IP network. They are considering capping bandwidth and not allowing bursting. They are upgrading technology for their Netflow logs.

Ohio Northern has stayed with 9-megabit service on 6 T1s, now delivered on DS3. They have not noticed the Kaaza problem. They are on version 5.22 of the operating system. Kaaza still needs port 1214 for control; if that is blocked the back end can't harm the rest of the network protocols.

Cincinnati uses a segmentation design to prevent dorm traffic from overwhelming the campus portion of the network.

University of Rio Grande does use Packet Shaper. They haven't noticed any major problems, but have seen some slow downs. They want to investigate more. They are also looking at picking a new ERP system. They are short staff and looking to change vendors to move off the AS500.

U of Cincinnati is looking at IP6, Multicast, and at Packet Shaper. Also looking at a regional fiber loop between schools in Cincinnati area. They are also doing more with Netflow.

Cleveland State University is using Packeteer. They use a bit rate partition for dorms, rather than trying to filter by protocol. They have 90 Cisco access points and plan on installing 200 more. They are moving to Peoplesoft version 8. They are looking at VoIP applications. The access points use LEAP and Cisco ACS server.

Denison is using Packet Shaper. They're noticing an increase in http traffic. Students are required to register servers. (Comment, if the traffic goes away with a reboot then is KAZAA.)

University of Akron is waiting to get money to purchase a Packet Shaper. They block port 1214 because they were having a lot of problems with mal-ware coming in Kaaza payloads. They are looking on having a very tight use policy. They are installing a 10-gigabit backbone.

Lorain County Community College is not shaping traffic as they don't have residential students so haven't seen a problem. They are working on PC replacements and network upgrades.

AFIT have not had any problems with network bandwidth issues. They use VPN for external access.

Terra Community College is non-resident, so they don't have many problems with Kaaza. They have blocked port 1214 with a firewall. They register all MAC addresses any service that goes on the network must see the computing department.

Columbus State Community College uses a Packet Shaper and is currently updating their networks.

University of Findley uses a Packet Shaper and a firewall. They are migrating to Iplanet with Solaris from HP.

Clark State Community College is working on a big VoIP project. They have completed the analysis phase and selected the vendor. They still have to work on 911 service and their dial plan. They have Packet Shaper and are discarding Kazaa packets. They moved from an Alpha to Solaris for administrative computing.

Miami University is putting in a VPN service. They are going to be installing content sensitive switches. They are a Novell shop, but are heavily dependent on LDAP from Iplanet. They couldn't scale the Novell LDAP (Comment - Wright State is having the same problems). They have found there are problem with Novell NFAP working with Macintosh and Apple has acknowledge this is a problem.

University of Toledo is working on Novell server consolidation with Novell clustering. They are using NDS with LDAP for authentication. They do use Packet Shapers for bandwidth management. They are re-engineering their perimeter to provide high availability.

Baldwin-Wallace College is working with video conferencing to work through their Packet Shaper. They are using a RadVision IP to ISDN converter. They

just became an I2 member. They would be interested in talking to anyone using Sflow.

Heidelberg College has recently upgraded their administrative system to version 5 SCT. They have a Packet Shaper and began experiencing problems when they upgraded to version 5.2.3. They currently use a 3-1/2 year replacement cycle for PCs. They switched from hand made computers from DMI to using IBM supplied.

Case Western uses a Packet Shaper 6500 with version 5.2.2. They have been having problems with Kazaa version 2 since the beginning of the school year resulting in up to 36 megabit/second peak rates. They are planning to increase to 45 megabits. They are also working on traffic separation techniques to separate I1 and I2 traffic with the Packet Shaper dealing with both. They are still working on a 10-Gigabit network with 6509 and 6513 in the backbone and GigE to the desktop. They ran into problems with Eudora sending large attachments with Netgear GA10 gigabit cards. There is a problem in the NDIS.SYS file from Microsoft that Netgear needs to rewrite the driver to fix. The latest beta driver set from Netgear seems to have fixed the problem. For the Internet 2 meeting, Case in conjunction with the Cleveland Institute of Music is working on an arts performance with USC across the network that will require a 250-megabit video stream. Miami is working on separating I1 and I2 traffic. Their solution has been to set up two separate channels. They have separate router interfaces and separate Packet Shapers since Packet Shaper doesn't have a way to manage multiple streams. They have to run BGP and had to set up ASN numbers for the networks.

OARnet Updates
Linda Roos
SEGP and I2 has 3 new members: Cedarville, Malone College, and Cleveland Institute of Art.

Gene Wallis
Bandwidth use is growing daily. The Abilene connection will be upgraded from OC12 to OC48. The Quilt is consortium of regional networks that has setup aggregate buying contracts with various vendors to get better rates on large quantity Internet capacity. OARnet, a member of the Quilt, currently uses 2 of the vendors: Qwest, and Cable and Wireless. OARnet will be renegotiating the contract with Cable and Wireless to up the capacity on an OC12 to 180mb. They still have connections with Genuity and Sprint that will expire in the next year. They will be looking at the quilt vendors for replacements to these contracts. They are looking at Level 3 in the Cleveland area as they have a fiber ring in that area.

Are you seeing any congestion? OARnet is upgrading links, as they are needed, but not redoing a lot of them unless necessary due to the dark fiber project coming up.

Paul Schopis
Firewall and H.323 Testing

They have tested Checkpoint on a Sun E250 single CPU 400MHz, with a quad Ethernet (qfe) 10/100 card, Solaris 2.6, and Checkpoint 4.1 service pack 4 as well as a Packet Shaper. RFC2524 has information about searching allow/deny lists. The Checkpoint firewall had problems when the mix reached 80% allow, 20% deny. The Packeteer worked very well. It can filter at line speed. It shapes TCP well, but shapes UDP in only one direction: out bound. You can try to use exclusion with Packeteer to pick up the inbound UDP in a separate class, but you still might run into trouble as UDP vies with other traffic in that class. The only other solution is 2 packeteers back to back.

He will be posting the information on the web.

Patty mentioned that Checkpoint has completely re-done their software and it addresses H.323 specifically. Bottom line is that so far the firewalls tested created performance problems with passing H.323. Wright State is willing to provide the resources for testing with the new version of Checkpoint.

What conclusions can we draw from this? Is there a packet forwarding problem? Except for the Packeteer, yes. You need to have a big enough firewall to handle the traffic. What management do we need to do to fix the H.323 problems? We need to look at the management issues as well as the boxes.

Patty Vendt
White Paper
New format has divided the paper into topics with a document body that contains a couple of paragraphs for issues, best practices, etc.... A signup list for volunteers to write the drafts was passed around. Patty will be contacting people. Goal is get the technical topics covered and will be talking with Osteer for the others. She will post the new format to the list again. Please contact patty@wright.edu if you want to volunteer to write a section.

Bob Dixon
Transportable Satellite System

ADEC is the primary user of the Tachyon Satellite Network that is optimized for IP with guaranteed speeds. OARnet provides NOC services for ADEC. The transportable satellite project was developed for ADEC, which currently has 50 fixed satellite sites now and plan to have 90 in a year. The goal is to provide high-speed access for all purposes, be inexpensive to build, operate with off the shelf parts and be transportable to any location. The applications include distance learning in under connected locations, demonstrations and evaluation for fixed satellite installations, provide field instructions, provide service for special events, and access in disasters. Typically, once the system is set up, it can run for days without modification.

The subsystems can get its power via an extension cord, batteries via UPS (8 hours), and gasoline (24 hours) . It can be setup in 15 minutes once at the location. Aiming is done with the PC. They hope to provide overlays for matching the satellite signatures. The equipment is weatherproof and mounted on shock absorbers in temperature-controlled cabinets. It has long-range wireless that can reach up to 20 miles, and wall penetrating wireless that can go through non-metal walls. It can do local wireless within 1000 feet or local Ethernet cable at 200 feet or they can connect it to an existing LAN in a building. It supports all types of Internet access. The cost of the trailer is in the ballpark of $40,000- 50,000 for education. An ADEC member could get it in under NSF funding.

The mobile units transmit to the San Diego center; the traffic is routed back over I2. The guaranteed downlinks are 1.5 megabits and uplinks are 512 kilobits. The trailer with equipment will be available for viewing over the lunch hour. Please refer to the handout for additional technical information.

Bob did a demonstration using his PC. Attendees were encouraged to go down and look at the trailer.

Lunch

Dark Fiber project
Al Stutz

Russ Pitzer requested Al Stutz become acting director while OSC searches for Doug's replacement. This year OARnet is also looking at some service cuts. ENS security audit service, firewall service and video editing have been eliminated under advisement of the executive committee. These services were

to be run on a cost recovery basis, but weren't breaking even. It was felt they were further than some services from the core mission of OARnet. The staff on the firewall has been transferred to OSU and will be supported from there.

OARnet also made some organizational changes in light of Ruth's announced retirement. Linda Roos is stepping into Ruth's position. OARnet will then fill the I2 coordinator's position.

Dark Fiber
Is this real? Yes. They are due to sign the contract on the 1300 miles of fiber soon. The timing for the Ohio Board is to it passed by the first of the year. The first phase of the project is building the backbone. The first phase does not actually focus on how the clients will connect, but just connecting the existing POPs to replace the old backbone.

David Barber - contracts
The governor announced, "the Third Frontier Network." TFN is going to be spending $150 million per year for high technology communications. The Dark Fiber Project is part of the over-all TFN vision. The contracts are with 3 vendors.

Gene Wallis - Transitions
Fiber is not all from the same vendors. Using a consolidation of fiber from various vendors. Phase 1 is to bring the backbone up. Phase 2 is to bring in the major universities. They will be looking at the various metro fiber ring projects to see how they can fit in to the overall requests, so if anyone knows of fiber in their area that might be available for use in this project let Gene know. Phase 3 will bring in the rest of the universities.

Who carries the contracts? For phase 1 OARnet will have the contract. For the later phases, it will vary with the location, as it will depend on what has been established in the various areas. The ultimate goal is for every school to have a dedicated fiber, not a telco leased circuit, connection to the backbone. Gene is hoping that by October 2003, he can announce OARnet is running the fiber backbone. It is anticipated that the cut-over to the new backbone will be able to be done in a way that does not incur a substantial cost to the members when/if POPs change locations. Cincinnati and Akron are two areas where fiber from two different vendors has to be interconnected. Money has been funded for the two networks to run in parallel for a time.

Gene showed a map with approximate fiber paths for phase 1. There are 2 major vendors shown on the map. Basically split via north and south of the state.

The third vendor, Spectrum, brings to the table the coordination between the vendors providing the fiber. OARnet expects the cut over and build will last for at least the next 2 years. If your institution is on the fiber paths you may be included earlier in the implementation than others. OARnet is also looking at separating the I1 and I2 networks using wavelengths.

OARnet will be talking about the loops and where they will connect and there will be extra committees created to help manage the project at the October 15th Dark fiber meeting. Questions can be sent to al@oar.net or to gene at wallis@oar.net.

There was some talk about the so-called, "National 'Light' Rail Project." The NLRP would only supply non-commodity Internet teragrid connectivity. It would cost about $1 million to join and $800 thousand per year. The board of regents decided forthcoming funding from NSF to support supercomputing centers is more appropriate.

In high performance computing, OSC will be receiving 300 Itanium processors for its supercomputing node. Once built it will be listed as one of the top super computers in the world.

Tim recommended that technical representatives contact your CIO's to know how the fiber project will affect you. If you know of any fiber in your area that may be usable, let OARnet know.

Break

Flow-tools Tutorial
Mark Fullmer
maf@oar.net

Network flows allow you trace packets to see the source and destinations of those packets. You can use the logs to find out who attackers are and the other hosts that have been compromised. You can find what users are running services, or scanning. You can look at your hosts by service so you can find out who is using odd protocols. You can look at your traffic by department. You can also track network-based viruses back to the hosts and find what hosts on your campus have been infected.

Flows have common attributes, creation and expiration policies, counters, routing information, and can be unidirectional or bi-directional. An application flow looks past the headers to classify the packets by their contents. This allows you to aggregate flows or to get a flow of flows.

The keys available define the flows. The type and number of keys can determine the number of flows. The application flow will look down in the packet to allow you to look at the content. You can aggregate flows to get a total measure (e.g. aggregate diff application flows for one set of source/destination). By using flows you can reduce the amount of data you have process to understand the traffic. (e.g. you can analyze 452 octets with 1 flow).

Flow collection can be done with a passive monitor, router, other existing network devices or you can mirror traffic. Passive requires a probe with mirrored traffic. The router collection does not require a probe, but it requires a collector to store the data. You must have one passive monitor for each LAN segment; however, they usually can look at more variables. A router is only going to see traffic that goes through the router and is limited to the packet header information; it cannot do application data.

Cisco's implementation is called NetFlow. Which supports unidirectional flows, Ipv4 unicast and multicast, and aggregated and unaggregated flows. The flows are exported via UDP and are supported in both IOS and CatIOS platforms. The catalyst flows are not as good as the IOS implementation as it contains more bugs. There are currently several versions of NetFlow. Different versions can give you different information. V9 is in development. The typical version used is V5. V8 is aggregated V5 flows. A NetFlow packet has a common header with a sequence number, version specific data where n records of the data type are exported and the n is determined by the size of the flow. The 5500 uses version 7 flows.

Cisco IOS configuration is placed on the input interface. You define the version, and the IP address for the collector. Optionally, you can set the timeout, configuration flow table size, and the sample rate.

Some sample IOS commands:
Show ip flow export Shows you the information on the flows currently seen.
Show ip ca fl Shows the flow caches before the flow is exported to the collector.

Some sample CatIOS configuration commands:
Set mls flow full
Set mls nde version 7
Set mls nde 10.0.0.10 9110
Set mls agingtime 32
Show mls
Show mls stat entry

What kind of impact does the flow collection have? Depends on the type of flows. There are some DOS attacks that can cause some problems. On a 5500 run 12.1 with CEF. You don't want to switch the flows. The 6500 with supervisor on it was similar to the 5500. The hardware flow cache in the original 6500 is too small and can be filled up. In later models it becomes an accounting function, but it has some bugs in that it reduces the information that you can get. The 6500 versions are not up to date with the router versions. They are working on fixing it. On the CatIOS on 6500 Sup2/MSFC2 the NetFlow implementation does not fill in the important field like input/output interface. On router implementation, it can create flows; even if the user is spoofing traffic and the packet does not go anywhere. Juniper configurations are more complete and less buggy.

Flow-tools are written in C, designed to be fast and scales to large implementations. It is a collection of programs to collect and process Cisco NetFlow compatible flows. It can expire older flow files and allow pre-filtering, and pre-tagging. It provides instrumentation for flows/sec, packets/sec and dropped packets. It has a server for TCP based flow clients and a privacy mask option to remove host bits from the flows. You can tell if you drop the flows as the flows have a sequence number. Below is a list of some of the Flow-tool programs.

Flow-capture - Collects NetFlow export packets and stores to disk.
Flow-fanout - Replicates netflow udp from one source ot many destinations.
Flow-expire - removes old flow files based on the dataset size or number of files.

Abilene's flow configuration was shown. It currently has 4 collectors that then go to a single collector. The new design will have a collector at each of the pops. NetFlow is UDP, so you want the collector connected directly to the router to minimize packet loss. An undersized collector will drop flows.

Flow-print - show an example of the output of the flow
Flow-cat - concatenate flow files
Flow-merge - merges data from multiple collectors.
Flow-filter - old version - allows filtering on the protocol port field
Flow-nfilter - new version - allows filtering on any defined fields.
Flow-split - splits flow files into smaller files.
Flow-tag - tag your flows to allow splits (e.g. tag with department then split the flow information by department)
Flow-header - displays the meta information in the flow file
Flow-stat - generates reports from flow files, with on flow report with one

data path
Flow-report - replacement of flow-stat, can do multiple reports per data pass. Currently about 70 reports defined.

Several sample reports from Abilene were shown. Why can't Oarnet provide this information to the campuses? You would need to get funding approved for the reports to be done. See your Osteer representative.

Flow-dscan - DoS detection/network scanning tool
Flow-gen - to generate flows for debugging
Flow-send - takes the flow captures and sends them in Cisco format
Flow-receive - like flow capture, but does not manage disk space. Used for debugging.
Flow-import - import flows from other formats to flow-tools.
Flow-export - export flow-tools to other formats. Currently working on mySQL format.
Flow-xlate - translates flows between different versions, all the functionality has been built into flow-report.

Flow-tools is still in development. They are trying to output flow-reports to SQL for billing or long term trend analysis.

Include references from last slide.
Flow-tools: http://www.splintered.net/sw/flow-tools
Abilene Netflow page: http://www.itec.oar.net/abilene-netflow
Simon Leinen's FloMA Pointers & Software Page: http://www.switch.cf/tf-tant/floma/software.html
IETF standards efforts: http://ipfix.doit.wisc.edu

What about the Cisco provided tools? They're not very good and he doesn't know anyone who uses them.

Is this doable for the I2 schools? It is very doable. You would have to come up with a list of what you want to have done. There are some privacy issues that need to be considered. The infrastructure for this on the I2 schools is in place. Cost would be the server and staff time to deal with the scripts.

Would it be useful sites to see these stats? We'd find out how much is being used, what it is being used for, and could find the hosts that are doing the I2. Would like to see the type of reports that might be applicable to I1 traffic. A report like this showing what your traffic is like can be used to make OARnet a unique provider for their educational customers. It would also allow you see common problems across the institutions.

Patty will draft a proposal to request NetFlow data reports be provided for I2 school sites to be sent to Osteer. If you have ideas for reports that you would like to see send information to patty at patty@wright.edu

Minutes from the last meeting were approved.

If you have information for the web page send them to Ransel at Ransel@kent.edu.

Meeting adjourned.