OARtech
December 12, 2007

Introductions

Oarnet Updates
Slides are available at
http://www.osc.edu/networking/oartech/presentations.shtml

Paul Schopis

They are still working on ring 4 because AEP is working on the POP in Huntington, WV. The projected end date is now March 2008. Gigabit connections in POPs in Columbus, Cleveland, and Dayton have been turned on as well as others. See the slides for details.

OSC gateways are running with a 61% average load and 80% median load on transits that we purchase. The total peak utilization runs at about 5 Gbps, so OSC will be getting additional bandwidth from Level3. This gives OSC 8 Internet 1 (I1) gateways and it is getting to be difficult to manage the routing. They are looking at reducing the number of I1 gateways and at making the remaining gateways bigger. Their NewNet load has spiked at 2.2Gbps. Ring 1 will be fully 10G before the beginning of the year and new Juniper routers have been added.

They are leveraging portals within the state. In phase 0 of the implementation of the state portals, they are planning to gain efficiencies by using equipment currently in the state network. Operational plans for phase 1 are currently being written. The Merit interconnect should be up soon and will light at 10G. The port will be shared with NewNet. They are still working on the Pittsburg connection. The gear is here and the Youngstown side is done. They are waiting on the PSC side power and PSC is talking about moving the fiber connection to a new location.

NLR and I2
The NLR board rejected the proposals and the I2 board says they can't go any further with it. OSCnet was NLR member by proxy. However, the CIC CIO indicated that if the merger did not go through, they would pull from NLR which will affect OSCnet's current connections to NLR.

OSC is looking at some new management tools. They are looking at the ADVA Etherjack product to give them the capability to do loopback tests to devices both at the end site and at the central site. This will make the testing a little easier and help them to distinguish between a fiber cut and a power outage.

They are looking to standardize their descriptions using Network Description Language with XML capabilities. This would make the descriptions machine readable so graphing would be a little easier, allowing you to drill down in network diagrams. See examples in the slides.

What does the POP move in West Virginia mean for the southern Ohio area? This allows a better loop because right now the loop for that area has OC3 that would be over subscribed in the event of a fiber cut. There was some discussion about the ownership and possible changes to the building that contains the POP in the southern Ohio area.

Client Services
Ann Zimmerman

There were several site updates with several using the OPTEMAN service from ATT and others using Time Warner and OC-3. OSU is upgrading to 10G. See slides for the complete list.

The new collocation facility is up and running. They have installed 20 cabinets with 7 current clients and 2 more to in 2008. The emergency splash internet site is coming up with 2 demo sites. More information will be available at Osteer. For more costs and lists of the sites signed up see the slides.

OSC is Partnering with OCLC, LexisNexis and Chemical Abstracts to move the traffic to and from these sites to using intra-Ohio (IO) bandwidth. They are looking for other ways that would push the IO traffic with research.

State of Ohio Health Networking
Dennis Walsh
As OSC worked through the various state connections, they discovered a project for a State of Ohio Health care initiative. It came out of the FCC Rural Healthcare project with total grants for about $400M and Ohio was awarded 69 of the grants. These grants were for regional health networks. They affected Jackson and Gallia counties, Northeast Ohio in 23 counties, and Southern Ohio impacting 15 counties. See slides for details.

Do you know what they were planning to do with these nets? Dennis felt that the groups found it easier to define networks, then to define the data that goes on it. There are some problems with insurance for tele-medicine, and other administrative issues that have slowed the growth of the tele-medicine.

One of the groups called West Virginia Telehealth Alliance is planning on accessing I2 resources through Ohio. They have included Ohio in their project based on the ring 4 planning that has been occurring.

The FCC healthcare funding is based on different levels of connectivity (regional, state and national) and is causing a review of the Broadband Ohio Network for possibly cutting costs for last mile connections. OSC is also looking at the costs associated with providing I2/NLR connectivity to healthcare.

Why is this important to us? The FCC is very aware of the infrastructure being built and the potential of it interfacing with other entities. They are hoping that, with Broadband Ohio, the healthcare nets will benefit a larger group. Can they help in sustainability past the grant period to help with connecting other groups beyond healthcare?

Dennis will also include the slides from OSC's first meeting on the healthcare project on the OARtech web site. These projects will increase the networking that may be available in the affected areas. One of the major applications is transporting and reading MRIs and XRays.

The first meeting of the Ohio Broadband Council has occurred. How did that go? It was very interesting. You have state agencies and some vendors that are competitors on the council. This was an introductory meeting used to pass some bylaws and to get to know the players. Members to the Council are appointed by the Governor and are a very interesting mix.

Roundtable Discussion
What's the latest update on statistics on bandwidth? They just hired someone to have this as a primary duty.

Oberlin asked about providing NDT service in Ohio. OSCnet does not have one, but will be willing to put one in the collocation facility. Oberlin volunteered to make one available. The old Looking Glass tool is no longer available. Cal Frye did a demonstration of NDT. It does 2 things: it describes packet loss and duplex mismatch problems. They have several deployed on their campus for testing sites on their

campus. Because of services moving remotely, they are getting very concerned about bandwidth and performance across the external links. They have put test sites on either side of their packetshaper, firewalls, etc... The tool has helped in determining problems with edge equipment. Having one at the collocation facility would help in troubleshooting network issues.

Paul Schopis is aware of a package that allows work with firewalls to make video conferencing work better with the firewalls. There is some grant money that could be used for this to provide some of these boxes to campuses. Paul will publish the link with information on the equipment. If you are interested in participating let Paul know.

Why do people use a Packetshaper so much? Generally to control the bandwidth associated with P2P or dorm traffic, and to reduce the bandwidth and a costs associated with it. Oberlin is now using Packet Logic from Procera Networks (www.proceranetworks.com) and found it finds more P2P protocols than their Packetshaper. Some sites have changed their packet shaping so it doesn't look at protocol but instead puts limits per IP bandwidth usage.

Anyone using MARS? Only a couple of sites indicated they have it.

Would we be interested in hearing from Fireshark? The site that saw the product presentation indicated that it is probably more effective at the site level than at the ISP level. It looks at flow data to determine location of botnets, and other systems that might be causing network issues.

What are people using for collaboration? Chat? Several sites use Skype for language interactions. At another site they are using wikis. Is Illuminate through OLN available to OARnet members? Ann thought so, but would have to check and send us more information.

Is anyone doing VoIP? One site has implemented it with about 200 extensions.

Exchange 2007 - Did any sites upgrade due to hardware upgrades? There wasn't anyone else running 2007.

What are people doing about the iphones, and other mobile devices? Most campuses list the standard devices and the requirements the new devices must comply with before they can help customers with them.

Is anyone serious about outsourcing your email? Several sites are going live soon with Google or Microsoft. Some sites are still working through the legal issues with liability. Apparently the vendors are still making the school liable even though they are not running the servers. There was some discussion on how the outsourcing was occurring and why they are moving to this solution and how the authentication will occur.

What are people doing for identity management? The discussion centered on sites that have grown their own. Some do batch uploads; others are getting triggers from their admin systems. Some have it more automated than others.

Lunch

MailChannels
David Cawley
Slides are available at
http://www.osc.edu/networking/oartech/presentations.shtml

MailChannels is an anti-spam technology company based out of Vancouver BC.

History of email and spam
Email started out on a single host and then they added the @ symbol to the addressing in 1971. Up until the mid-seventies email was

primarily used by controlled audiences. In the early 80s, the standards were developed. In the late 80s, email became available to the public. In 2001, the SMTP protocol defined. The original forecast of problems with junk email was recognized in 1976.

SMTP was originally developed inherently insecure. Since it was originally standardized, they have added SMTP-Auth/TLS, and have added SPF records and sender-ID. These didn't stop spam because new technologies are not used over all servers. Also, often legitimate accounts or machines are hijacked and used for sending spam, so are allowed through.

The first spam was sent 1978 (DCE sent a message to advertise a conference). The name "spam" was coined in 1993. Early spam was primarily through open relays. RBLs took zero tolerance policies to force administrators to clean up their open relays. The Nigerian spam was born in 2000. Interestingly, this mail was sent via satellite though internet cafes. They started looking at the receipt IPs to help find the origination point. Before 2003, anti-spam and anti-virus writers worked independently. In 2003 the sobig virus emerged and is used to send spam. Since then, there has been much more synergy between the anti-virus and anti-spam vendors. Legislation was introduced in 2003. Spam is still around and it has changed. As more messages are sent by infected end hosts, it became more important to look at the content. The spammers have moved from text to html to image spam to animated images, flash, PDF, etc.... The problem for the anti-spam vendors is that it is becoming more and more computationally intensive to sense the spam. He predicts that soon we will see spam that is MP3, excel, P2P and botnets with command and control. The spammers will find the vulnerabilities and then plug the hole after exploiting the system to prevent other spammers from taking over the system.

Some statistics from the NY Times: 0.02% people click and buy from spam. This allows the spammer to earn a lot of money when a lot of spam that is sent. The spammer's response to filters is to increase the volume of the spam to keep their rate of return.

Traditional filtering includes MD5, Fuzzy Signatures, Bayesian, Header Regex, RBL's, URL Lists, and Grey Listing. The problems with these filters is that the spammers use obfuscation techniques and different formats for the messages (html, image, PDF, doc, xls, ole, MP3,...). Zombies and botnets get around the RBLs and blocking lists.

He showed a graph showing that spammers use IPs only once or twice then move on to another.

This vendor uses SMTP Multiplexing that sets up transparent SMTP proxy with connection pooling to insulate the MTA and avoid delay of legitimate mail. They support up to 10k simultaneous connections to prevent DoS. He showed a diagram that shows the SMTP Clients for the end user and spam source sends and receives messages through a traffic control system that sends/receives the traffic to the MTA.

Their product does traffic control by providing a QoS and scoring the connections by reputation by looking at traffic from honey pots and other sources of spam. They throttle the traffic from the unknown senders and fast track the legitimate senders.

Their traffic control product will reject the known bad mail, the good mail and the suspicious mail is sent to the MTA via different paths, allowing the throttling of suspicious messages. In the connect stage they can look for early talkers, whitelists, blacklists, RBLs, etc, at the HELO stage they can check DNS, in Mail From they look at SPF. They throttle the messages from the spammers by varying the TCP window size to add a configurable delay. When they throttle a connection they follow the RFP standards for throttle times so they do not

violate the standard wait times.

Traffic control can talk with many MTAs (Sendmail, Postfix, Exim, qmail, SunJSMS). It reduces the load the MTA has to deal with as it deals only with valid messages, not the spam.

How does this compare to the throttling done within the MTA software? The MTA throttling is done with the number of connections and denies across the board, not towards a specific host, or spammer. None of this would prevent zombies.

Asynchronous IO is event driven, non-blocking front end, and blocking back-ends. They use a multiplexed pool to allow them to service the messages based on events instead of serially, or as a time slot.

They also have passive OS fingerprinting (POF). This looks at the IP packet data to determine the operating system and then makes a decision to throttle the messages.

Spamming is driven by economics and what they can earn from the spam. The botnet operators need to make money. By slowing down the spam it will make them go away because they are not willing to wait for a slow connection.

Questions:
questions@mailchannels.com
+1-778-785-6143
www.mailchannels.com

Can you control on per source address? Yes.
They are building in an admin console to allow you control multiple traffic control instances.

Licensing model: The price is based on a per user model.

They do not have a per user ability to control the throttling.

Normally, this would be added to existing anti-spam solutions. It is put in front of the MTA to insolate it from the traffic.

Scott McCollum, Sinclair, won the iPod from MailChannel.

This product would be used only on external messages coming in, it would not be applied to messages going out. They have a partnership with Cloudmark for adding the content filtering.

Currently it runs on 32 bit platform, but they are currently working on 64-bit platform.

If you are interested in case studies or talk to references, or are interested in a demonstration, contact him.

They have several articles on the currently state of spam and anti-spam on their web site.

Meeting was adjourned.