**OARtech**
**June 13, 2007**

Introductions

OSCnet Updates
Paul Schopis
The IRUs for closing ring 4 are in Capital Review. This is one of the several levels of approval and vetting that orders for OSC have to go through. The total process takes 4 to 6 months before the PO is generated. All the optical gear is in hand.

The New Philadelphia POP is up.

They are using I2 commodity peering service and have seen around 600Mpbs usage. They are also looking at leveraging a 10 GigE service from Level 3. This would allow OSCnet to buy burstable service to add "insurance" for failures or large bursts.

The Time Warner Telecom link is now in place at 625 Mbps.

K-12 ITC sites are still coming up on OSCnet. All but 2 are now connected. They are still TDM based but are moving to an Ethernet based network.

Level 3 and Buckeye finally agreed to terms. The original plan was to light a connection to MERIT with multiple 1 GigE lambdas and then migrate to 10Gbps. But they will probably go right to the 10 GigE.

The Pittsburgh connection is under way and the 1st optical unit has been installed in Youngtown. They are currently waiting for fiber to go into the rack.

I2 and NLR
The NewNet connection is now fully operational. We are using their peering service. It is not clear when or if the merger between the 2 organizations will be completed and that may effect fees. Council elections will be held soon with some local folks having been nominated for council positions.

Dennis Walsh
The Ohio state government is looking at OSCnet and wants to form a partnership to take advantage of the infrastructure that is already in place. They want to move SOMACs to Ethernet to reduce costs. The initial plan is to extend from a central office with an Opt-E-Man Network (first vendor to offer this is AT&T) and will allow OSC to aggregate the traffic in the central office. Then they can take a bigger pipe to connect to OSCnet. The total cost of the connection would be about $1300 comparable to today's T1 cost of $2800. It aggregates the traffic to OSCnet via a Gig line and may be paid for by the state. The plan is currently

being rolled out in the 6 major cities. These lines are mileage insensitive, so local schools may be able to take advantage of these connections. Currently the state is working with ATT, but is also looking at Time Warner and other providers to extend the service to the entire state.

What does this do for schools that paid significant $ for the last mile? You may be able to get a connection in addition to current connections, but it is up to the vendor as to whether they are actually ready in an area.

Do the local entities know who to purchase their internet service from? Yes, they will have their own state NOC for trouble calls.

The Opt-E-man service is best focused on creating local network in the local areas. Some schools may be connected both via Opt-E-man and Gig-E-man services.

There are some questions whether in some areas the vendors understand what is available or whether they are willing to use existing lines.
There is permission from OSC to help out the local schools and then traffic can be routed to the appropriate state networks. There was on-going discussion about using Time Warner. This may be the time for us to talk to vendors about aggregation of state traffic (local government, schools, etc) so that there can be an investment of equipment.

Ann Zimmerman
Disaster Recovery
Per OSTEER they are investigating offering a service to host a front splash page with a message in the event your school's services become unreachable. They are looking at selling rack space with power for co-location of servers for disaster recovery. They are working with an IPTV service for broadcasting events.

Ruckus now has their co-location in place on OSCnet. OSC is interested in feedback from sites that are using Ruckus. Feedback in the room was generally positive.

Bandwidth quotes have been sent out (June 1st) so OSC can get a sense of the bandwidth increases that will be requested. Sites OSC has not heard back from by July 1 will receive follow-up calls from their client services representative.

Today lunch will be at Camille's. OSC is looking for input for what to do in the future for lunches. The general consensus is that staying together here at the meeting site was preferable to going off-site for lunch. Julie will send out some options with the cost. We can let her know what we want.

What are sites doing about disk encryption? OSU doesn't have a written policy, but is riding on Bowling Greens' PGP pricing with the key escrow service run by

OIT. They don't expect to have it up and running until September, or October. They have not figured out a distribution service (PGP whole disk encryption) but they have the licenses. Some sites are finding that higher quantities of licenses can make the purchasing of the licenses less expensive. OSU is also looking at other devices and ways of solving the issues. (TPM, Low Jack - what are these?) Kent looked at whole disk encryption, but saw problems with it and key escrow. They are looking at Safe Boot. There are also sites using TruCrypt. One of the issues OSU is working on is vetting the people that need to have their keys replaced. Currently they think it will require a customer to physically come to the helpdesk with an id. They are looking at distributed key management with the possibility of allowing the various departments to vet their own people. OSU's current solution for Macintosh's is File Vault that operates at the home directory level. They are also looking at encrypted file images. But in both cases, there are problems with training the end users. There is information on OSU's site for using the existing hooks in the operating systems.
(http://safecomputing.osu.edu)

How many are looking at system virtualization? A show of hands indicated 4 or 5 sites. Some sites are using it in a test production environment using the free VMware. For anything that uses raid or high computation, they use hardware. But for the smaller services that don't need special hardware, they could be virtualized using the free VMware server. One school put campus DNS and DHCP for a short time on a virtual server, due to some fried equipment, and they were surprised at how well it worked. Cincinnati State has a full deployment with the paid VMware. They went from over 90 servers to 40 servers. It lets you maximize the "stupid" systems that need a box by themselves.

Is anyone working with Voice over IP? 4 or 5 schools are looking at it. A couple of smaller schools are running production VoIP. Some schools are looking at VoIP to leverage the Gig-E-Man links that they could use between regional campuses. One site is doing with the wireless as well. Products mentioned are Cisco and Shortel. Asterix is used for very small implementations or tests.

Is anyone using full campus VPN? A couple of schools are using it or have announced it. OSU has seen a case of someone jumping on the VPN to try and break other systems. Be very aware of the security implications and keep an eye on it.

Is anyone using Cisco Secure Desktop? No responses. Doesn't seem anyone is using it. There was some discussion on Cisco's security products.

Is anyone using MARS or others of this type of products? A few sites indicated they were using these types of products.

Lunch was off site, but not everyone went to the suggested restaurant. We had a much smaller attendance after lunch.

Xangati
Debby Goldman
Slides are available on the OARtech web site
(http://www.osc.edu/networking/oartech/presentations.shtml)

Xangati uses the same technology as NetZentry, but is focused on rapid problem identification.

The networks and applications have gotten much more complicated. The endpoints are very much interconnected and sometimes this makes it hard to see the source of a problem.

Users are usually the first to respond and complain about a symptom (intranet is slow, application is sluggish, service timing out, etc....). Users are the ones affected and we have to play catch up and the symptoms can cause you to follow the wrong path to a solution. Because finding the source of a problem is hard, 58% of the time a problem goes unresolved.

There are 2 stages to correct a problem. First is to identify the problem, the second is correct the problem. Xangati can identify the problem and alert you hopefully before things have snowballed. The product knows the endpoint's perspective of the network.

2 classes of symptoms:
Hyperactivity and performance - overloaded storage service, unusual access, overuse of Skype, unauthorized video streaming, broadcast storm, etc...
Hypoactivity and performance - lethargic intranet service, application performance, internet down, router interface down, DNS server down, email server down, other service down, unauthorized server....

The product is an appliance (a 2U box) and presents IT with the unique perspective of the application behavior of every endpoint, and application delivery infrastructure that builds the network. The RPI is fueled by precision profiling of the endpoints and applications. All this is to reduce the time to identify the cause of a problem.

The device uses a non-intrusive connection. There are no probes, no software agents, and is just an appliance. It receives flow information from the routers and switches to analyze the network. It uses the flows from the main aggregation points to monitor and understand the information and uses auto-discovery of endpoints, topology, applications, etc... to understand the network. It maps user identities through DNS and LDAP lookups and can characterize the endpoint with the LDAP queries to understand who the user is. The profiling looks at various variables such as bitrates, packet rate, affinity to the endpoint, application, area, time, etc.... You need to do the profiling to be able point out the broken points.

Profiling gets a list of endpoints, and symptoms. Correlating is looking at the profiles to analyze the symptoms and identify the core problems. It takes flows from several different pieces of equipment and then creates a uniform flow, and then has 4 engines to look at the flows: a mapping and topology engine, a profiling engine, an alerting engine and a monitoring engine. Each engine then fills 2 databases (mapping and topology, and profiling) and outputs the information to the management interface.

The vendor worked through some samples. The dashboard shows a list of the ids and identifies the abnormalities such as "very low volume interactions with endpoints" or "excess bitrates". These are abnormal as outside of the normal traffic for that endpoint. You can click down to see the detail such as incoming or outgoing traffic and the type of traffic (e.g. file transfers, etc). The profiling determines what is "normal" for that endpoint, and then looks for activity that may be different from that "normal" profile.

Notification can be done via email, or syslog based information. So, you can have regular parsing of the syslog. Can you set thresholds? You can set the length of abnormality or set severity notification.

How long do you build the profiles? They talk to the customers to come up with a natural period to set the profiling span to the period you want. They do allow use a small amount of ongoing traffic to learn on to determine normal changes in endpoint use.

How many education environments are you in now? They have product in production in one and are testing in a couple others.

For larger deployments they would have sensors closer to the flow data (not a full appliance) and have this come back to a central appliance.
They look for the natural aggregation points that see most of the traffic. They review the network topology and determine the aggregation points. They point the flows to the appliance, name the
DNS servers, etc... what are the important locations, what id is important, etc... then put the box in discovery mode and it collects data about each of the endpoints, and ids the points.

This tool looks at the symptoms and allows you to drill down to find common areas of problems. Data is stored in mysql databases and can be downloaded. The reporting client is java based.

Cost is $35k to $100k depending on the size of the network.

Next meeting is 2nd Wednesday on August.

Meeting was adjourned.