OARtech Minutes
October 12, 2005

Meeting started at 10:05

Introductions

Oarnet updates
Paul Schopis

Backbone upgrades on ring 0 (ROADMs were added. These are a combination between mux terminal and OADM) and added 10 GigE capability. They upgraded ring 2 with transponders at Newark, Canton and Youngstown. New PoPs were added in Canton, Newark, and Springfield. These were regen sites that have been upgraded to full PoPs. Recent schools add MVNU (Time Warner - it was noted that TW had an outage and had to be notified by OARnet of the outage as they were not monitoring the connection), Youngstown (Access Fiber), Marietta (SBC-OC3), Central State, Cedarville, Wittenberg, and several other were using SBC GigE.
Schools in the queue: Denison, Kent State, and NEOCOM. All of the old BB is retired. Only circuits remaining are those necessary for redundancy.

Partners for TFN are SchoolNet and OEB. These have merged to form Etech. The PoP builds are under way and the middle mile issues are being sorted out.

Issues on the backbone have mostly been related to software revisions and hardware support and some issues with CTM software support. Cisco has promised that they will fix the software problems, but OARnet is building a lab to test the equipment and software themselves.

There seems to be some confusion on the subscription policies. There are 3 models: Strict - completely locked down; loose-One category is locked and 2 can oversubscribe (Because of the way the routing works over subscription works best between I1 and Intra-Ohio); and Very loose - all categories can over subscribe and only applies for T1 lines. It is under provisioned for offered loads and there could be performance degradation. These models really only apply to full I2 members. SEGPs are purchasing a set amount of I2 so they cannot burst. They have looked at the model to have Intro-Ohio and I2 to run on the same vlan but it is harder to do. Caps can be adjusted for special events to allow higher bursts when needed.

What is the current setup between loose and strict? The default configuration is to use loose configurations. Ashland and Kent have experienced strange issues with moving large files. It gives large flow, then trickle and then a large burst, another trickle, etc... They brought a packet capture so OARnet will look into the problem. They are not seeing the TCP window adjusting. It seems to be only with OhioLink.

OARnet will look to see if there are a lot of drops on the line. Ashland should open a call with OARnet support.

There is a committee from Osteer to look at the subscription policies to better define what is needed. Currently with SEGPs, you buy a membership and you get 1 Mb, then buy it in 6Mb increments, but they are looking at changing the model to a per Mb pricing. They will be looking at the current tier pricing model.
There is a TFN event at Shawnee State tomorrow from 4:30 - 6:30. At the EDUCAUSE level, they are some looking at the COLEA ruling from the FCC. The ruling had to do with wiring tapping on voice but is being interpreted on data networks as well. There are some questions as to how it applies to the data network and what type of equipment will be needed. There will be a speaker at the IHETs that will be speaking on the COLEA ruling. Linda will send the information to the list.

There are up to 34 sites that have upgraded their last mile since the backbone was put into place.

Network Security - Patricia Vendt
MPLS Overview - Paul Schopis

Slides can be found on the OARtech web site.

OARnet uses MPLS in the network today. They are one of 2 regional networks that use it in production. MPLS is a label that is inserted into the packet with label, Class of Service (CoS), S label to indicate the bottom of the stack, and TTL. The packet routes along a "Label Switched Path", with values ranging from 0 to 1,048,575. The 0-15 range is for special defined packets:

0 - IPv4 Explicit Null label
1 - Router Alert Label
2 - Ipv6 Explicit Null label
3 - Implicit Null label

Choosing the next hop can be thought of as a composition of 2 functions. The first partitions the entire set of possible packets to a "Forwarding Equivalence Classes" (FECs). The second maps each FEC to a next hop. MPLS forwarding can be done by switches which are capable of doing label lookup and replacement, but are not capable of analyzing the network. The FEC is assigned when it enters the network and so can be used to determine the path of the packet. The information for where the packet came from is carried in the packet so you can make routing decisions based on that information. You don't have to worry about source routing. It also allows you to setup performance criteria for QoS issues.

OARnet did some early testing with MPLS for Abilene. The problem you are trying to correct by using MPLS: Goal was to create an Abilene Premium Service. They

needed to create "Virtual Wire" with a predictable bandwidth and be able to determine what packet was eligible to use the service. They used it to have admission control and dedicated bandwidth for specific types of traffic. They can pre-map tunnels and reserve bandwidth for special purposes. This gave OARnet experience with MPLS before the TFN project.

In the old network they used ATM pvcs to separate the I1 and I2 traffic. The Board of Regents wanted to be able to provide all the I2 services to any Ohio school connected to the TFN. To have jumbo frames, IPv6, and Multicast are available across the network if requested. The new architecture uses the MPLS labels to segment the traffic. I2 packets are tagged. If the packet is not tagged, then the packet follows the traditional routing paths. Paul showed several slides showing the relationships between the pop equipment and the customer premise equipment. OARnet is the only provider using logical routers.
The MPLS equipment must be able to do an MPLS ping and traceroute so they could see all the hops within the cloud. The reason the IntraOhio and I1 traffic can "slosh" is because both types of traffic go to the same piece of equipment.

Last week Level 3 and Cogent stopped peering last week was sink holing the traffic. So there were problems with customers getting to I1 sites. The situation lasted about 1 day. The 2 companies are having a disagreement.

Patty Vendt
There are enough sites in Ohio participating with RenISaC so you shouldn't have any problem being vetted. Darknet is useful and sites have been receiving reports.

What are sites doing to identify infected machines and what are you doing for remediation? How did your fall quarter go and would you what you did again?

Ashland - Good back to school. Remediation previously, put policy based rate limits on the students' lines in a per port basis. They are doing clean access, but not enforcing it, only notifying the users about problems. They settled on Clean access because was they were looking at Perfigo and NAC and
now these are now the same product. Clean access as has been really smooth. They don't seem to have a performance problem, but see the clean access system with a large load. Do you have users using the client? They are using the windows client. They de-register people once a week to force them to go through the cleaning. They are watching for the Macintosh client. They did find some load issues when all 2000 students were trying to hit the box at the same time.

Rio Grande - They are running Netreg to register and scan the systems. Wireless is going well. Best startup they ever had.

Kent - They have a "pseudo" site license for Perfigo (purchased before the merger). They are able to do high availability in front of all the resnets.

This fall was the best resnet connection they have ever had. They are doing a phased in approach. Their peak this year has been 5400 users. They did not see the load issue that Ashland had, but they have separated out the traffic.
They use Bluesocket for authenticate wireless. They do not do remediate wireless. They are starting up guest access to the network, but only with well known ports.

Heidelberg - Cisco's Clean Access was installed this summer. They required the agent and anti-virus software and all the window fixes. Mac clients and Linux would just authenticate. Their smoothest startup they've ever had. Not doing it to faculty and staff or wireless. They are thinking about authenticating wireless to it. The nice thing is they can see the exact fixes that are needed and thus can help the users over the phone.

Antioch - They are looking at Clean Access. Their helpdesk people have been looking at the tools that are available to help them. They are running 802.1x on their wireless.

Washington State - They don't have a residential campus, so they just provide limited access to their students when they are on campus.

Bowling Green - Very smooth start of year. Clean Access was installed last spring. They did not implement it for fall due to political issues, but haven't had any problems. They are still planning to do implement Clean Access. Wireless authenticates to Bluesocket, they are talking about adding Clean Access to their wireless users.

University of Cincinnati - They are using clean access in the dorms and force all students through it. For wireless, they are doing mac authentication. They still got lots of calls, but because of update problems. They rolled out Audible Magic to block copyrighted material.

Denison University - They use Bradford Manager and force all students through it when they register their machine using a registration system similar to Netreg.
Denison does scan the faculty/staff machines but we don't quarantine them.
They use blue socket to authenticate the wireless.

Oberlin - They feel that students are coming to campus with cleaner systems because they are being trained to startup the automatic updates, virus protection, etc.... They have Clean Access on the student resnet for reporting, but not enforcing. If you have the DNS server on the untrusted side of the network you can cause major problems. They do not require client.
They are migrating wireless to airspace on the untrusted side of the clean access server and forcing all wireless through the clean access. They rate limit guest access to plain TCP only. They require system registration to do IRC.

Wright State - They have guest accounts issued from the library for anyone with government issued IDs that are functional for a limited amount of time. They had someone come through to push for full functionally because it is a state institution. It was determined that state institutions can limit access to the resources as long as it is across the board. They are currently looking at Bradford Manager, and have looked at Clean Access. They have a lot of port blocking implemented and the helpdesk is able to look at the firewall logs to determine if user has cleaned their machine. They have a remediate web site to allow users to scan their machine for issues.

Lunch as the discussion continues.

Marietta - They have Clean Access, but were not ready to implement it this fall. They will be implementing it on an out of band solution. They use Cisco ACS on wireless, but it is not fully implemented. They hope to have the Clean Access on wireless in the future. They are using Audible Magic. This works well with MP3s, but not very good on anything else. This year, they have increased the priority on the gaming in the Packetshaper because gaming doesn't really use the bandwidth that was feared. Tests with Clean Access have been good. They will implement it slowly and will be forcing the client. They firewall their dorms. They have not seen a lot of virus problems this year.
Feel students are coming to campus with better equipment.

Xavier - Using Clean Access this fall requiring the agent. They implemented a building at a time. Wireless using leap with Cisco, but it requires the Helpdesk to touch the laptops. Probably the best year they have had.

Kenyon - all residential goes through Clean Access both wired and wireless. Last year did not require the client, but this year they did. On the non-resnet side they use Bluesocket to control access, and do provide some limited guest access. They are not requiring VPN on Bluesocket side.

Case Western - Looking at Clean Access, but don't have it. They do have a quarantine network. They are using a reactive approach where if they recognize someone scanning the network they would be put in the quarantine network. When users are quarantined, helpdesk is notified and they contact the student to get their system fixed. Wireless network is completely open. It provides access throughout the circle area with a cap of 5MB. For faculty/staff/student they request that a VPN client be used for wireless access. Fall move-in was very smooth. Use Samantec site license to do anti-virus across campus.

NetZentry
Network Anomaly Detection and Mitigation Peter Long Peter@netzentry.com

Founded in July 2003, first product shipped in 2004 and located in Palo Alto CA.

and funded by venture capital. They offer network security solutions that uniquely utilize a scalable and collaborative approach to instantly detect and precisely track anomalous traffic to mitigate the effects.

You get anomalous traffic that floods the networks including external internal DDOS attacks and zero day worms. Current security solutions are often incapable of stopping such unknown attacks. They may be able to detect the bad traffic, but since there is no signature then they can't help.

You can find where the attacks are coming from to mitigate the attack closer to the source rather than at the victim. When humans must get involve it extends the time of coordinating the mitigation of the attack. Their product helps to automate the detection, tracking and mitigation of the attack. Their Flood Guard solution detects the attack and then tracks the traffic and backs closer to the source, then applies mitigation, be it ACLs or some other type of block.

They determine an attack by comparing current traffic to a baseline. They then move back to the edge to track the traffic to the specific link. They mitigate the attack on the specific links. They can have multiple detection domains to perform the detection, tracking and mitigation domains. They can do these steps to internal systems as well as external so if an attack is originating from your site it can mitigate it as well. Can also be used to mitigate an inside worm attack.

They look at their product as another weapon in the arsenal. Components include detection, tracking, mitigation and management. All components can be set sideline, except the mitigation which is set sideline or inline. Response can occur in milliseconds. They look at netflow, cflow, and gigabit packet capture (for small environments). They look for traffic anomalies versus signatures to detect an attack. They build baselines on the items that are important and look at the normal traffic patterns. The anomalous behavior is identified relative to the established traffic patterns. It can detect multiple attacks.

They follow the data back via the links to find the attack source. Since attacks are often spoofed the source IP info is not valid. Mitigation uses dynamic filtering and does it per protection domain and per link. Once the attack traffic stops the filtering is removed. They can also sideline the traffic so that it is fed to another box scrubbed and then reinjected to the network.
They also provide reporting that will show the density of traffic by source.
You also have historical data that you can look at. Reports can also be email, or sent to a syslog server.

They showed a live demo with several protection domains. Showed a live "outside in" attack and historical data to see an "inside out" attack. You can go back up to 4 weeks to look at historical data.

How long is the training period for the determining the baseline? Could be one or 2 days, but it depends on your traffic flow.

With sideline mitigation the tracker is communicating with the ingress routers, when an attack is detected, there is a reroute request via BGP to the switch to reroute the attack traffic to the sideline equipment where the ACLs are applied and the traffic then injected back into the network via tunneling or even in a simple network with default routes. When the attack is over, another reroute request is sent to send the traffic back to the normal routes.

This can be implemented with one or two boxes. It runs on a fairly standard PC box. They also provide a hardware based product. More information can be found on the web site http://www.netzentry.com. The preferred solution is to purchase as an appliance, then provide netflow or packet capture to the device to get going. They do have an evaluation program.

REN-ISAC
They work out of the Abilene Network operations center. They have a service called the Darknet. If you want to get a report of systems on your campus that may be infected and is hitting the Darknet. You can go to http://ren-isac.net/ sign up and to get the daily hit list report and be sent a list of IPs hitting the Darknet. If you become a member by filling out the registration and have 2 member support the registration, you can join the Darknet. Ransel will send some slides to the Oartech list on this service.

New Business
Do have any way to have a directory of the Oartech members? In the past you were to send a request to oartech@domain.edu then it would go to the Oartech representative. Some sites have more than one person that attends the meetings and would rather see the inquiries go to the Oartech list or to the oartech address so that a directory does not have to be maintained.

Minutes from the last meeting were approved.

Adjourned at 2:15pm