OARtech
October 10, 2007

Introductions

If anyone has suggestions on topics for meetings, please let Mike Pinson know.

Academic Services Update
TJ Sandors
Slides are available at
http://www.osc.edu/networking/oartech/presentations.shtml.

OSU is reviewing a 10 Gb connection. Sites getting or have put in upgrades: Ashland, Zane State, Northwest State CC, Marion Technical College, Ohio Northern, Baldwin-Wallace, John Carroll, Lake Erie, Kent State, Walsh, OAI, NASA Glen, Lorain CC, Notre Dame, Lakeland, Clark State CC, Jefferson CC, Southern State CC, and Sinclair CC. Marietta and Washington State CC is collaborating and upgrading to DS3. University of Rio Grande is working with the surrounding county to bring broadband to that area.

The new Co-location facility is now available. For $2500 you get cabinet, 100Mb bandwidth, key, power, etc... with a monthly fee of $500. The cabinets are sold as an entire cabinet. They do not sell partial cabinets. Any outside vendor must have an OSU representative with them to access the cabinets.

The remaining 7 T1 schools are upgrading to broadband. There are currently 7 schools that are using the Ruckus download services.

Remember - your feedback matters! Let us know if you have any questions or issues.

What is the difference between an "Ethernet" solution vs "Fiber"? The Ethernet solutions will depend on the vendors that the sites may contract with: Optiman, Time Warner Cable, etc... are not fiber solutions, but they are Ethernet.

What kind of packet shaping does OSU use? They don't "shape" the traffic, but they police it. With policing they allow some bursting above your limit, but keep it around the contracted limit. 2 ways to do in intra-Ohio: one is a hard limit (because of packet shapers), and the other is burstable. What is used is dependant on what the site wants. If you have questions, they can run counters to look at what might be happening.

A site has changed to another shaper. Can you get intra-Ohio traffic tagged so you know what to do with routing protocols? Just request it through support. They can tag the intra-Ohio bandwidth if you need it.

Dennis Walsh
(See slides for details)
Broadband connections: 85 member universities to OSCnet, 41 universities connected at OC3 to 1gig or higher and 44 universities connected at varying speeds up to 45 Mbps. The last mile really makes a difference in what you can take advantage of. Ohio Aerospace Institute (OAI) with NASA Glenn have 1 Gig connections. OSCnet is building links to various communities: Dublin, Central Ohio Research Network (CORN), Tuscarawaras, and One Community in northeast Ohio. OSC has national collaborations with I2/Abilene, MERIT, and Pittsburgh Supercomputing Center. Plans in 2007-8 include upgrading remaining T1 sites, connecting several community rings and health care facilities.

After having built the network, they have extra capacity, and are looking to use it to help the whole state of Ohio. The Governor has established the Ohio Broadband Council to direct a unified, statewide broadband development effort that includes OSCnet as well as the state network to try and bring down the cost of networking throughout the state. The council is composed with co-chairs (OSC director, and OIT director) with participation from various different groups in the state. OIT will manage the last mile to all state executive agencies. OSC will manage the backbone, academic K-20 and research.

Beginning steps of funding from the state is $4 million from OIT and $20 million from the Third Frontier fund.

OSCnet Engineering
Tony Eller
(See slides for details)

They expect the equipment for closing of ring 4 to ship early December and will see work completed by late January and early February. They are adding Gigabit portals at the POPs with the state that will be turned up in October in Dayton, Cleveland, Toledo, Cincinnati, Columbus, Akron, and Youngstown. Majority are going into the POPs in Qwest locations.

Current gateways are running at 75% with total utilization approaching 3 Gbps. They have increased the bandwidth to Time Warner Telco. The NewNet peering connection is ~600 Mbps. They will be increasing links between Columbus and Cleveland, Columbus and Dayton, and Columbus and Cincinnati to10 Gig in the future. 2 routers have been added.

All K-12 ITC sites that are using some form of sonnet are moving to Ethernet by the end of the year. They are leveraging portals within the state. Phase 0 implementation has the state router connections at layer 2. The Merit interconnect fiber splice will occur at the end of October and will be lit with 10 GigE and shared with NewNet. They are connecting Pittsburgh and Youngtown with 10Gig.

The NewNet connection is up and running, but they are still working through some issues with the commodity peering service which is an issue within NewNet.

Router Memory Issue

There is a limited amount of memory on line cards in older 7200 routers in the network. Those cards can run out of memory as the number of routes increases. The only affects a limited number of older 7200s in the network. Basically, the older equipment has already been moved out of the network because Oarnet saw this limit a while ago. If you are using a 6500 MSFC2, and you use full routes, you may see this limit.

The original presenter cancelled so Mark is doing the presentations.

Two Factor Authentication Using HOTP
Mark Fullmer
Slides are available at
http://www.osc.edu/networking/oartech/presentations.shtml

They implemented a standard using smart cards and smart card readers to allow authenticated access to network equipment using one time passwords. One Time Passwords (OTP) are passwords that can be using only once and are generated by for a login session. A common implementation is SKey and SecurID. There is also SKey software to allow you to generate the passwords on your PC or you can print out a generated list to carry with you.

S/Key is a forty bit key one time password. It is not very practical for non-technical users, but is okay for the technical user.

Why OTP's? Given the opportunity, people will choose easy passwords and many accesses are not encrypted. Staffs have a lot of passwords to remember; when one password doesn't work you try another and it's common to use the same username for multiple systems. If someone sees an insecure telnet connection it is unencrypted and they can see you accessing another system that may be secure. They may try the

username and/or password they saw on the secured system. OTP stops this type of compromise because the passwords are only good once. It does not stop hijacked unencrypted unauthenticated sessions. If the device you're logging in from has been rooted, then your session can be hijacked.

Barrier to OTP deployment
While S/Key is free, it is not for the non tech savvy user. Secure-ID or other vendors with proprietary solutions cost money and can increase with each user; thus can get expensive. There are lower cost bundles, but in general it can get costly.

Requirements for OTP
The cost per user is low and it is available in small quantities (e.g. one person). It needed to be useable by non tech savvy staff. The vendors want to sell lots of quantities. They didn't want to have the implementation to be OS specific and didn't want to maintain drivers. They wanted an open source solution.

Their solution was: Smart card + reader + HOTP + small library + pam module. Smart card and readers were issued to users. The PAM module runs on a login server. He showed several samples of smart card balance readers that are used in Europe for Ecards. Another they tried was the Spyrus PAR II.

Half the software is running in the smart cards and half in the readers. The smart card is run through the reader to send an ID. Some cards are real simple, some have full java. What is in and running on the card are vendor specific.

They use a BasicCard: a ZC 3.9 type microcontroller based card with 256 bytes of RAM and 8k EEPROM. The IDE allows you to program it in a BASIC like language with a crypto library.

HOTP is an Internet draft detailing how to generate an OTP based on HMAC. HOTP(K,C) = Truncate (HMAC-SHA-1(K,C)). Every time you use the cards the counter increases. When you log into the server, the server also increases that count. HMAC is an MD5 checksum with a key. It requires a shared key on the smart card and on the server. It also requires a loosely synchronized shared count. Computing passwords is always forward within a window. This solution uses a Berkley database as the underlying database. If you enter the pin wrong after 10 attempts the card will lock itself out.

Getting Started:
Get a ZC3.9 smart card, balance reader, and a pc/sc compatible

interface, or just get the BasicCard development kit for $80. Smart card - $3.10/user, Balance Readers $12.35/user or Spyrun PARII $60. The PC interface is $10-50. Download the HOTP software. If using the Spyrus reader download the HOTP firmware. (This does requires a special cable)

Program the keys in the smart card with hotpt.exe, and configure pam to use pam_otp.so. Try to login then use the smart card and balance reader or Syprus reader to generate the challenge response.

This is open source. The full implementation can be found at http://www.splintered.net/sw/otp. They also have a plug-in module for OpenVPN.

OSCnet currently has about 40 users using this. They use Trampoline BSD servers at redundant locations with HOTP required on all logins only on in-band access to equipment. The VPN deployment is for other services that do not easily support SSH.

Contact
Mark Fullmer
maf@splintered.net
http://www.splintered.net/sw/otp

How well does this scale? The first day it there was a lot of complaining, but it just has become a part of your process. A lot of times it's only done at the beginning of the day. This works for a small number of people. They don't want to make bad choices for passwords, or have a central location that may get isolated in the event of a network problem.

If we wanted to use this in a small scale, would you be willing to help us with it? Sure. It is all open source, but he has not publicized it.

Anyone have Vista on campus that they are happy with?

Vista machines on campus - UNOH have about 3 labs with Vista. They have a remote management agent on the system to enforce when students can use them by the instructor.

One site had problems with clean access on Vista.

Are there any topics that people are interested and having? Any vendors? Enterasys has some interesting things in their offerings. One site has retired their packet shaper and are now using Packet

Logic. They feel it does a better job of identifying traffic, especially p2p. This unit is made by Procera. It is big in the ISP market in Europe and they are moving into Education. Procera Networks.com.

Denison is investigating devices to help looking at logs and flow data to find problems as they develop on the network. They have tried the Q1Radar product and will be trying the Xangati product. The main issue they saw with the Q1Radar product is it seemed to constantly need to be tuned.

Lunch

APCON
Andrew Roberson
North Central Regional Manager

Physical Layer Switch Solutions
APCON sells physical layer switches for Layer1. They were established in 1993 and are based out of Portland OR and are privately held. They design, build the switches and software in house.

A physical layer switch (PLS) is an OEO (optical, electrical, optical) layer 1 switch, electrical layer. The switch is protocol independent. It does not read packets, filter/drop packets, or buffer data. The equipment passes all the packets and doesn't modify any of the packets. It is device agnostic. It does not care what is plugged into it. It is non-blocking, any to any connection at wire speed. The equipment could be thought of as an intelligent patch panel. You can make changes to infrastructure without touching the cables. It does not do any auto-sensing. You can do conversions of MM to SM or Copper G to Fiber G using the PLS as the converter instead of having to purchase an adapter.

The PLS chassis is generally 32-64 port, but they are available in any number of ports. All PLS should be able to handle the same data rates.

Manual cable changes can have physical problems with patch cables. PLS allows you to make cable changes from the console port. Can save on capital equipment expenses, operation, etc.... They make it easier to share analyzer tools or other appliances across multiple physical connections. It allows the creation of lab environments without having to purchase multiple test equipment, and allows multiple use of single piece of equipment.

He showed pictures having buildings back to a physical switch and

mapping those devices to sniffers on the fly within the software. In the test lab it allows the reconfiguration of the test topologies through software without changing the wiring. It also allows electronically moving the test equipment around the network without physically moving it. Allows the sharing of devices and/or user groups with a shared device pool (tape devices, etc).

With the physical layer switch you can test cable break failovers by turning off a port (it turns off the port completely). You can send traffic from a single traffic generator to multiple locations. Allows remote access to the PLS. You can replicate span data to multiple devices.

He showed an example of using PLS for building a redundant network.

PLS should be able to handle any device to do a one to one, one to many, many to one, or many to many relationship between devices. It can be from/to any type of network - tdm, frame, sonnet, enet, etc...

The concept is for PLS to make network monitoring, using devices to make life easier for the network staff by allowing you to map any device to any device from a console.

The vendor showed a physical box and did a demonstration.

A PLS shouldn't care what kind of cable is plugged in (straight through, cross over, etc). Because this device is at the electrical layer, you can make the change in the software. This is a "patch panel" with intelligence and secure remote access.

Embedded secure GUI allows you to access the box via a web GUI. Or can use scripting directly to a CLI. The cable connections are already predefined so you can just test by running different scripts. There is also a way of clicking on icons to represent the devices and then draw a line between those icons to establish a connection between the devices.

They have built into their software that you cannot connect two spanning ports to each other. They have the ability to import and export configurations to the switch. They have 3 different ways to look at the network and create the connections. You must set each port to the same data rate but can use different media. They don't support data conversion so you can't take like a TDM to Ethernet. But you could take 100Mb copper to 100Mb MM fiber.

Do you have RJ21 connections? Not currently, but can take that back

for an enhancement request.

You can setup presets for setting up regular test environments. They also have multiple layer authentication (admin, advanced operator, operator, guest), with authentication to an internal database or to a radius server. They are able to do TACACS. You set up zones based on organization or devices to subset the ports.

You can lock ports to a particular configuration to make sure that a test environment does not get disconnected in the middle of a test.

Most common chassis is the 4 blade chassis. $30k
Blades are about $10K so the single blade box is about $10K.

Contact information:
Andrew Robertson
Sales Manager, North Central Region
drewr@apcon.com

Meeting was adjourned at 2:30pm.
