OARtech meeting Minutes
August 13, 2003
Teresa Beamer

Meeting called to order by Ransel Yoho at 10:10

Introductions - What's new for your upcoming school year?

Clark State Community College - website update, Novell update, and pending funding a possible SANS project
University of Cincinnati - VoIP, construction, Blackboard update
OhioLink - Firewall updates have gone out, acceptable use policy is also available. Both documents are available on OhioLink's web site.
University of Toledo - constructing new dorm, adding wireless, upgrading from hubs to switches and other network upgrades
Sinclair Community College - Data center move to another building. Implementing wireless security, upgrading firewalls, and upgrading backbone to 10 Gb. Looking at policy based computing on the switches
Oberlin - SANS implementation, upgrading backbone to 10 Gb, new dorms, wireless
Lorain County Community College - upgrading cable plant, adding wireless
Columbus State Community College - using NETmail for email, driving a unified username/password project for blackboard, labs, new computer room move, new building, Blackboard 6 upgrade, migrating to new sans
University of Northwest Ohio - brought up exchange for email, discontinued Blackboard and using Angel, brought up LDAP authentication, implemented web sense (web filtering software)
NASA-Glen - new director coming in Oct 1, campus-wide wireless deployment using Blue socket, continuing to update the cable plant and doing some VoIP
Miami University - new VP for IT and developing a strategic plan, campus-wide wireless with Bluesocket, new SAN
DeVry - 802.11a and b campus-wide, 4 Linksys system on the a and b side and all were bad out of the box, complete website re-design, upgraded to windows XP at the desktop
Ohio Northern - Site license with Microsoft, wireless, construction on new buildings, add 300 beds in apartment style housing
Wright State - replaced mail server, selection of ERP package to replace administrative software selection between SCT or PeopleSoft, selected Sun1 product for mail (32,000 email accounts), upgrades core backbone, upgrading Cisco equipment throughout University
Denison - new buildings, wireless using Bluesocket, upgrading backbone equipment
Kenyon College - VPN concentrator, new website design using Ingeniux, their first non-unix web server, runs on a Windows server with Explorer with XML, developing a 2nd computer room on campus for additional space and disaster recovery, planning for new athletic facility

Notre Dame - IPv6, new IP range for students
Kent State - 2 new residence buildings with authenticated wireless using Bluesocket, new email (Sun1) and Campus Pipeline, changed all email accounts to new system and had password change on all, migrating backbone from ATM to gigabit Ethernet
University of Rio Grande - bring all desktops to XP, Webct upgrade, installed spam filtering seeing 75% spam discarding, dual gigabit links to all edge switches, put in port level security, moving from erp package to a home built using Student Space

OARnet update - Steve Gordon
Final proposal for grant has been sent out. Verbal approval has been received. University of Cincinnati's project also has a verbal approval. General proposal is to build a set of tools that can tell us what is happening as we move to the TFN. They are planning have a beacon server distributed around the state available for testing various protocols end-to-end to see where the problems might come up in a high bandwidth network. They hope to have extra equipment available for checkout and training on the tools. OARtech is the oversight group for the project. Will try to mesh the University of Cincinnati's project and this project to see where they can work together. The project is an 18-month project. They will be starting the process of buying the hardware as soon as possible.

Netflow Update - Patty Vendt
Wright State has finished their part of the code. They need to work on the web front end. Hope to have something to show at the next meeting. Notre Dame has been working with some front ends from other sites for looking at the netflow statistics and is working with Wright State to see whether it would work with this netflow project. They did find that putting the raw data into a database does not run well.

OARnet Network Monitoring
Mark Fullmer, maf@eng.oar.net

Customer requests for data include circuit states, tcp/ip header based statistics, top talkers, I2 vs internet, in state vs inter state, and diagnostic tools that are easy to use and accessible. Internal requests require that it be proactive, monitor all interfaces with as much automation as possible. Issues include the need for a well-documented network and workflow that is kept in synch with the equipment. It needs to be minimal work on the part of operations staff and operations staff shouldn't need to understand the details.

The workflow changes are use the router description field to encode information for all the circuits in tag=value form (e.g. oic=OARnet d=

texual description, t=type). Using this encoded information in the SNMP polling and the router configuration to generate database entries. Currently monitoring 4000 interfaces with 8 people working on this without much documentation to work from. They also changed the device naming convention to include the device type in the name to indicate the backbone link or customer equipment. This would allow better accuracy for DNS names.

New tools that they are using include StatsScout, Nagios, Router Proxy, Router Log Proxy, Flow-tools and IPERF:

StatScout is a fast SNMP poller with a web a based reporting tool. It runs on FreeBSD and commodity Intel based hardware. They negotiated for no cost software, but with a yearly maintenance based on port count. StatScout is partially deployed, waiting for a current license and hardware to run it on. Sites would use this to find your router and look at your statistics.

Nagios is a replacement for NOCOL and is a generic event based tool for monitoring. Using plugins for services such as ping, SMTP, etc... and has a web interface. Identified network problems require acknowledgements from staff and the software is open source with many plugins available. Nagios is used for monitoring services, on all the interfaces. They are finding that not all equipment is configured to handle the monitoring, so it is a labor intensive project to get everything to accept it. Runs on Linux BSD. Can be used to monitor disk space, IO, etc....

Router Proxy is a web proxy to router CLI interface that is password protected, rate limited, logged, and restricted to a subset of commands. Commercial client routers will not be accessible. Router Proxy allows you to do tests (e.g. traceroute) from the external device to devices in your network to find out where the problems are.

Router log proxy is a web proxy for reading router syslogs. Router Log Proxy allows you to access log information for your router.

Flow-tools is developing software for looking at network flows. They are starting to use flow collectors installed at the I2 schools. Netflow will have information available by flows for sites to determine how the network is being used. For data storage they are using Escalade raid controller from Treeware.

IPERF - beacon objects are used for end-to-end performance testing. The 6 TFN pops will have measurement servers with IPERF.

Did demos of interfaces currently testing. Not in production mode yet, but to give a feel for what is coming.

Third Frontier Network
Dennis Walsh

Fiber status - all fibers have been completed and tested except for one link that is waiting for a building to be finished.
Engineering has completed integrated construction in Toledo, Columbus, Youngstown, and AFS. There are pending projects in Akron, Cincinnati, Columbus, Dayton, Toledo, and Youngstown.
Lighting and Architecture committee unanimously approved physical and logical designs. Optical/IP based MPLS with fast reroute layer 3 protection (non-SONET based network) approved equipment Optical Cisco 15454, Router Cisco 12000 with Installation by SBC with OARnet assisting.
Pricing committee approved a pricing model for network with components including membership dues, connection fee, I1 fee, I2 fee, and a service fee.
Last Mile Committee did a completed review of the RFP. The RFP is on hold pending
OTA meeting and final mailing list. Expected to be release by 8/25/03. If you know of a vendor that should be on the list, please submit the contact information to Dennis. Have added all K-12 sites and will have an approved vendor list.
Implementation committee verified the key milestones for installation have been determined. Hope to move to new backbone by 1/2004 to reduce the lease backbone costs. Will move the backbone from ATM architecture to gigabit Ethernet architecture. Ohio Telecom Associated Meeting was held 7/31/03 to discuss open issues regarding TFN. Focus of TFN is on Research on Education and service. It is not competing with the telecos for services and they will have more opportunities to participate, improved communications.
Funding: obtained controlling board approval for purchase of equipment and transferred to OSU to make it available. Obtained School Net funding for their phase 1 last mile sites. Seeking grant funding for Central State, Wilberforce and Cedarville last mile. Also seeking $5M funding from PUCO for last mile costs.

Special projects - Congratulations to Ruth on her retirement.

Lunch

KarlNet
Doug Karl and Dave Hudak

Was involved early on with OSU and OARnet began working with wireless in the 90's. They were working with firewalls, but are now working with the longer distance outdoor wireless. Lucent used their technology as did

Avia, Apple, etc.... They've been incorporated for 10 years. They are in the ISM band 900 Mhz free band, in building, enterprise, and location of 802.11 sources (to find hotspots). Residential wireless is primarily out of Taiwan, but Karlnet is moving some in that market. Karlnet is totally employee owned with 35 employees.

Passed around several access points. Agere and Intercill are the primary radio chipset manufacturers. Agere is better quality control. The box radio if purchased in high quantity is about $50 an access point. Equipment shown includes: a tiny access point, a small blue saucer access point (all B only), a chipset for outdoor access port that you can plug in whatever radio you want, a small board where the PCI/MCA network card has been reduced to one chip, and a mini PCI card with a radio with A, B, and G from Atheros.

Are there drivers available for these? Agere does their own drivers, Intercill, and Atheros contract out their drivers.

800 MW radio board with amplifier: This is a home-plugged network that runs through electrical wire in your home. Worked great in home environment not as well in work environment with metal conduits.

Outdoor antennas need to be able to handle the outdoor environment conditions, and directs the radio signal in a specific direction. He showed an 802.11 radio antenna that was a square box that concentrates the signal so that it can go up to 5 miles. How tough is the alignment? If aiming at an omni, it is not too bad, if pointing at another directional then a little harder. Must be line of sight, can have trees and buildings in the way, but must be line of sight and will have some signal diminished. The whole system is less then $300 and can be plugged into powered Ethernet line. He talked about the outdoor antenna and how it works.

What's happening with A, B and G? You will not see any standalone A products. You are now seeing dual band solutions. Manufactured price for B radio is about $18, an A, B, and G radio is still in the $40 range. A requires more power, B can penetrate buildings better. Recommends that you do G if deploying now. Current market is selling "pre-G". When the spec is "good-enough" vendors will start deploying them under the draft. The different G breeds should work together, but most will probably work together with a software change. B is a subset of G. Does not see it going away but sees it working with the newer access points. A is 5 Ghz, B and G is 2.4 Ghz. Still sees B a little cheaper for the next couple of years. They do not see A taking over B, it is a 5 Ghz vs 2.4 Ghz question. Most of the consumer products are in the 2.4 Ghz range.

A lot of sites have buildings being designed that will have wireless. What

do we design for? Over design for more cells. As you will need more cells as you have more traffic.

One site liked A because it could have more adjacent channels and thus have a better chance of covering a classroom. It would improve the throughput. Of those that have done large lecture halls how many APs did you use? Some 3 B ABs, one used an A, B AP solution.

What about security? What do we need to be concerned about in roaming, etc?

Security definitions, 802.11 security, weak IV problem and Wi-Fi protected WPA security and 802.11i.

Security context between 2 entities should have authentication, integrity, and privacy (identity, detects altered packets, and prevents eavesdropping).

802.11 security is currently tied to association between the station and the AP in a session. Authentication is Open systems - all stations may associate, shared key, stations must know the secret. Integrity check fills in the frame but it not very secured. WEP is not very secure (lot of ways to crack it). When you are using 64 bit WEP it really only a 40 bit key. Some of the original IV algorithms use 0 as initial value and incremented by 1. WEP+ fixed the "Weak IV" issues. Can exhaust the key space in 5 hours.

We have to improve authentication, integrity and privacy to improve the security.

802.11i "MAC enhancement for wireless security" was to be compatible with earlier draft. 2 authentication algorithms: 802.1x and pre-shared key for small home single access point solution. 802.1x (not 802.11x) uses EAP for generic wrapper for authentication traffic, which has the impact that authentication is between laptop and server. The AP is pretty stupid, and allows and denies based on the EAP messages.

WPA uses Temporal Key Integrity Protocol (TKIP) has stronger privacy (but still uses exclusive OR as does WEP). But adds key rollover and has a stronger integrity algorithm (MICHAEL) with a separate integrity key. It has integrity counter measures that if it detects MIC failures then it will back off. Comment from the floor - sounds like a good place for a DOS attack.

Additions in 802.11i also have IBSS authentication and CCMP (Counter-Mode/CBC- MAC Protocol (privacy: AES-CCM (128 bit key) Integrity: CBC-MAC). You will probably see WPA products next summer.

MAC Radius, 802.1x or ACL authentication then apply the policies: Web,

Full, or deny access.

They have 4 major development projects - putting software on the small access point, maintaining the Karl bridge base currently in the apple and other APs that currently have their hardware and software, and software that can be loaded onto the most popular APs.

Minutes from June meeting were approved.

No new business

Meeting adjourned at 2:25.