June 14 OARtech meeting

Meeting opened 10:10am
Introductions around the room

David Barber Ohio Joint program handed out the Video Conferencing Directory Services Survey to coordinate video conferencing sites in the state of Ohio. There is technical contact information and site location information. E-mail information to david@ohiolink.edu

Somacs line turnaround has been reduced from 60 days to 30 days although OARnet has not had any experience

Gene Wallis' update included problems related to Qwest. Master Service Agreement with ADP with pipes to Qwest and the State Building which will move the pop to OC-48. This year OARnet plans to implement an OC-3 to Dayton to Indianpolis to Chicago NAP for bandwidth on the order of 60-70Mb. 50-55 networks are peering in Chicago such as NREN, Big10, StarTap. Now are running OC-3 to Sprint, QWEST, and in process of removing DS-3 to cable and wireless with OC-12 and that looks like it will work out well. Pittsburgh link is scheduled for next week (week of June 20) and then the link to Washington D.C. ADP is to put in an OC-3 to Chillicothe to Portsmouth to Athens. ADP tends to be in places where other carriers don't go like Ohio NorthWest and SouthEast.

Demonstrated smart board technology. Writing, multiple colors, erase with fingers or eraser, print, multiple pages ($3K) and it comes in multiple sizes, site provides PC and works like a PC, with PC applications. Ruth will place detail on the OARnet website. It can also be used for a display of a videoconference.

Looking at a device from Accord that is a large MCU for H323 video. OARnet would like to introduce a central MCU site for H.323 video so anyone can get into video at less cost. The Accord looks scalable and reasonable to operate. Under evaluation now, OARnet engineers have found some problems and are working with the vendor to correct. One of the problems has to do with setting all of the sites with the same end speed or speed matching. It is going to be one of the most valuable features. It will allow gateway between H.323, H.321 (ATM), and the H.320 (ISDN).

ITEC is one of two I2 research centers - North Carolina has the pre-production testing and second operational center. OARnet applied to the state TAF (task action fund) for 1.5 million. Posting for a Sr. Network Engineer and an OC-48 fiber link from Columbus to Dayton to IN to set up a testbed to review new technologies. IN is where the I2 NOC is located. There is a certain portion of the money that is possibly available for projects.

Clifford Collins (ccollins@oar.net) joined OARnet April 1 to provide network security services to customers of OARnet; scanning systems, analytical assessments, data mining and incident analysis both pro and post active. The service is based on a request from OSTEER, it is fee-based, and Clifford hopes to hire two additional staff before the end of summer.

Site Security Audit
On and off site inventory
Vulnerabilities
Telephone vulnerabilities
Analysis of the results
Presentation

The explanation of why we do network security audits - there are many reasons but an audit helps to justify expenditures.

Deliverables:
1-hour presentation at exec level
Written executive summary
Separate technical assessment with cost
CD-ROM copy of all documents

Cliff provided a description of the technical report content using ISS model and the problem resolution information. The cost of the should be under $10K depending on the size of network. Currently ISS software is very expensive. OSU's prior $30K license is now $240, a normal Class B is $80K.

Future expectations include education and training, security resources web sites, certificate authority and PKI, incident response support, site licensing of security software, and broadening the firewall offering.

Ruth introduced Gene Bassin, OARnet Engineer

OhioLINK update. Anita Cook

1.
NASA images web site up by July, the beta site is
dmc-test.ohiolink.edu/mrsid/ls7 The images divide the state into nine sections, click, select date. There is cloud insurance, 30% cloud cover and OhioLINK does not buy the date. She showed Columbus with locators
on the right to tell you the location you are viewing and it is zoomable.

2.
Asked about security of the images - on Good Morning America, Microsoft bought the Russian spy images and has them available on a website or ftp raw files (1/2G per file). Sanborn maps (insurance maps) are located at dmc-test.ohiolink.edu/mrsid/sanborn. The maps have been available since 850-1970. The production site should be available in Fall.

3.
Electronic dissertations and theses
Caution concerning the blockage of services due to firewalls, proxy services, and changes to IP addresses

Member Security update: Mowgli Assor

www.net.ohio-state.edu/security/talks/updates/20000614.shtm

Current viruses - palm devices are now vulnerable. Recommend not executing anything immediately.
Ftp servers for unauthorized storage especially warez services.
Cisco TACTACS+
IBM Lotus Domino 5.0.1
Gdm 2.x
Cart32 2.5a, 3.0
Kerberos 4.x, 5.x
Qualcomm Qpopper 2.53

Trends at OSU
Anonymous FTP servers for warez storage
Use of Gnutella and similar applications increasing
Continued port 53 (DNS) probes

OARtech website update: Rancel Yoho, Kent State

Oartech.oar.net Change White Paper to Document Center

Election of Terri Beamer of Dension University, beamer@dension.edu for vice-chairperson. Sinclair closed election with a motion for unanimous vote. Bill Mayhew seconded.

Bill Mayhew update of Neucom rootstown (named after a man named Root) updated to a second T1 small compact campus with touching buildings. 3M Volition terminations connector that looks like cat5 and contains 2 fibers easy to use and install. Used air (gas) blown fiber. Vendor was Clover bought by Ameritech. www.3m.com/volition disappointment with gigabit ethernet less than 30%, usually 12MB (100Mb) /sec - good card is Asante Alcatel card repackaged 3Com work in Linux but not with NT ($800)

Integrated Voice, Video, and Data Network Technologies Mark Fulmer, OSU/OARnet

Mark Fulmer (OSU):

On Digital Video

Digital video incorporates transmission of video and audio data across ISDN, ATM, and IP. More common implementations utilize MPEG1 codec with a cost of around $1K. Newer implementations are using an MPEG2 codec with a cost of $7K to $10K. Both are implemented using a single card having the codec engine in hardware. MPEG2 is DVD quality, but requires a good deal of bandwidth to satisfy video needs. An MPEG1 codec can be supported on a simple 166 MHz Pentium class system.

On IP Telephony

An IP phone can be plugged into a network jack. IP phones use DHCP to glean an address for the network. The phone then contacts a call manager system on the network to register itself with the call routing system on the call manager. From then on, the call manager can route calls to the IP phone. By using DHCP, the phone can maintain its telephone number wherever it is connected; i.e., it can be moved from room to room and still have the same phone number. This is a problem with 911 locator service. This is addressed below.

IP phones require power to operate. Older installations require an external power supply. This implementation is not economical because a UPS is required for each phone in the case of a power outage. There are

proprietary solutions that send power over the unused pairs of a 10X Base-T link to the phone. A standard is currently in a working group that will provide DC power through the UTP pairs used for data transmission thus freeing the unused wires of a 10X Base-T link. A single UPS located in the closet where the network switch (with phone power support) is installed will provide backup power for all IP phones connected to the network switch. [Personal Note: One problem with this solution though is that network switches generally consume a decent amount of power. Adding IP phones to the list of consumables exacerbates the power utilization problem requiring a larger UPS for greater run-time. This in turn results in a large expenditure for UPSs across the entire campus to keep network switches running in the event of a power failure for emergency phone services.]

Switches that provide power to IP phones are IP-phone-aware. This means that the switch will generate a packet that is sent to the call manager (in addition to the registration request from the IP phone). The packet indicates the port and chassis on which the IP phone is connected. By having an up-to-date database of ports in all closets, it is "easy" to track the location of phone in this manner. This presupposes that a port database exists for the campus; the database is updated each time a patch cable is added, removed, or moved to a different port; and that one can obtain the call manager information. If this can be done then one can cross-reference the chassis/port information from the call manager to the database for a physical user room number. Doing so allows 911-locator service to be provided. OSU has painstakingly inventoried all ports in the dorms and have created a database that identifies each chassis/port to a given room location. All AMCs generate an update to the database to maintain port definitions.

The bandwidth of raw IP phone traffic is around 64 kbps, but with compression the rate drops to near 10 kbps. There is no reason that IP phones must be connected to switches. Standalone IP phones can work on repeated nets as experienced by OSU. In uncompressed state, IP phones use around 64 kbps, but with compression IP phones require around 10 kbps of network bandwidth.

IP phones need not be separate desktop devices; software on a PC and a microphone can also be used as an IP phone. Call management is the same as a standalone IP phone. Voice mail, in this case, is easy to implement as an E-mail attachment. Also, a Web-based directory service can be used for number lookup and call initiation. However, 911-locator service may not be immediately available since the network switching equipment views the

connection as a PC rather than a specialized IP phone device.

There was discussion of QoS, IP Multicasting, and etc. Essentially "How does it work?" which can be gleaned from any good Cisco book or Cisco documentation from CCO. One important distinction between Traffic Policing and Traffic Shaping was mentioned. Traffic Policing is Committed Access Rate (CAR) A.K.A. bandwidth limiting. When implementing traffic policing, a policy tells the router to drop packets exceeding the maximum bandwidth. With Traffic Shaping, a policy tells the router to shape traffic to a particular maximum bandwidth. Traffic Shaping queues traffic to conform to the specified bit rate. However, queues are not unbounded and thus Traffic Shaping may behave like Traffic Policing in that when a queue becomes full, packets will be dropped. It is said that Traffic Shaping includes Policing.

QoS for video/audio streams can be implemented using packet classification. Classification is performed using a queuing methodology or priority bits in the IP packet header. Affected packets are defined by using ACLs and route maps. The affected packets are then either placed into a queue or their IP packet header priority bits are re-written. Packets with set priority bits are handled by upstream routers. A particularly nasty problem with this implementation is that people move, IP addresses change, and ultimately a large amount of modifications to the route maps or ACLs are needed for moving or changing IP phones.

QoS can be implemented in various ways using Cisco routers with RSVP, RED and WRED. RSVP is a reservation protocol that is utilized by clients wanting access to video/audio streams. It works well, but all join information is maintained on the routers thus cutting into the router9s available memory. In this way, RSVP doesn9t scale all that well for large networks.

RED and WRED are based on a "Random Early Detection" algorithm that randomly drops packets from flows. In this case, a flow can be considered an audio/video stream. By randomly dropping packets a TCP connection will self-throttle due to its window size property which is constantly negotiated during transmission. Self-throttling implies automatic rate limiting. The "random" part of this scheme bypasses the problem of "global synchronization". Global synchronization occurs when a number of flows concurrently self-throttle due to excessive packet drops (window size is exceeded). With the reduced window size, the bit rate of each flow is also reduced thus freeing up more bandwidth. Each flow then notices that no packets are being dropped and thus begins to ramp up its window size. As the window size increases, the utilized bandwidth of each flow increases until the defined link maximum bandwidth is exceeded. RED drops the packets of all flows contributing to the excessive bandwidth. Each

flow sees the dropped packets causing their window sizes to be reduced again. This synchronization of the flows by cycling their window sizes and hence their bandwidth requirements is known as global synchronization. By randomly dropping packets over several flows, global synchronization is avoided.

WRED (Weighted RED) works in the same way, but allows weights to be placed on different flow types or flows originating from certain sources or to certain destinations. A flow that has a small weight is more probable to have random packets dropped to allocation more bandwidth for those flows with a high weighting. Simply put, a highly weighted flow is more important. This gives more important flows privileged bandwidth while steeling bandwidth of less important flows.

On ResNet

OSU uses Statscout (http://www.statscout.com) to monitor their ResNet connections. Monitoring occurs through in-band SNMP requests to over 500 network switches at one minute intervals. Input/output packets and error statistics are obtained for each port. The result is stored in a database on the system having Statscout installed. A Web interface allows statistical information to be displayed from the Statscout server. Information such as port errors, packet count, and utilization in and out can be displayed for all ports on a given network switch. It is also possible to show the Top number of ports in utilization, bit rate, or errors. Port descriptions can be absorbed by Statscout and displayed on the Web interface to show the physical room where the port is connected. Packed SNMP requests are used to reduce network traffic to and from network devices.

Statscout is a FreeBSD-only program, but is free to EDU sites. OSU is currently monitoring 15,000+ ports across over 500 switches using a Pentium II-450 MHz PC with 256 Megs of ECC RAM, a 2950UW SCSI controller, 1-4 GB hard drive and 2-9 GB SCSI-2 hard drives.
The two 9 GB drives are striped to a 18 GB virtual disk.

Patricia Vendt, Network Services