Oartech Minutes

April 13, 2011

Introductions

OARnet/OARtech
Ann Zimmerman
(slides are available on OARtech site: http://www.oar.net/about/oartech/presentations.shtml)

The next OARtech will be 6/8/11 and we are looking for sites to have the meetings. There was a request for topics. If there are any vendors or topics you are interested in let Ann know. Suggestions that came up include log management, IPv6, and Firewalls.

Thanks to Sinclair for hosting.

John Conley was announced as the new Ohio Board of Regents CTO. It will probably be September before the steering committee will be filled. They don't foresee anything negative with the new governor.

Time Warner e-Lan Project – Bought 2G of bandwidth from Timewarner. This allows sites to use the e-Lan product. Mount Vernon Nazarene, Heidelberg/Maumee, OSU Remote campuses in Mansfield, Marion, Lima, Newark, Muskingum, Columbus College of Art and Design (new member) are using this product to connect. Since 2009 bandwidth usage has gone from 6Mb/s to 11.7. There are 6 new OARnet members.

Special Projects include collaboration efforts with OhioLink, OLN and eTech to consolidate and share resources and cloud computing. Remedy is migrating to "Service Now". Adding bandwidth and special projects with Kent State, U of Dayton, Stark State, Clark State/Wittenberg, OU Med Center (10G Upgrade), and U of Rio Grande and OMMC. OMMC is getting close to finishing the environmental assessment and will begin building soon.

A Review of services include commodity Internet, I2, Intra Ohio (now called OnNet), remote Campuses and Upgrades, Looking for Co-Location Services at U of Findlay and Northwest State Community College (3 racks). Probably a year from June those in the collocation site at KRC will have to move. OARnet also provides emergency web hosting, video conferencing (eTech) and VMware.

They held VMware Desktop regional meetings at Marion Technical College and OSU with Matrix Integration. Both were full and they had a waiting list. Having another with MCPC April 19 in Cincinnati, at Kingsgate Marriot and May 4 Cleveland in Plain Dealer Building. If you would like to host one of the meetings, Ann has vendors willing to do the presentations and demonstrations.

OARnet was conference participants at the following conferences: OHECC March 28-31 at Wright State with a Member meeting. They will probably combine these meetings in the future. The I2 member meeting will be April 18-21. Bowling Green and Cleveland state have both dropped out as full members. There has been a request that I2 look at their model due to the budget issues in today's financial climate. There will be a follow-up meeting in May. Educause Regional was March 14-16 in Chicago. There will be a Merit Member Meeting May 18-20 and the next OARnet Member Meeting will be June 2

How do you charge for a 2nd connection? There is no extra charge. Oarnet will, temporally, bump campuses up for a short time to allow the campus to see where their traffic peaks out.

What is the Timewarner e-Lan? It is similar to the Optiman from ATT. It has multiple size pipes at different cost. A 100Mb connection would be $650/month. It may be worth contacting them to see if you can convert current Timewarner services to their e-Lan service. The e-Lan is a mesh service where Timewarner provides the aggregation. Contact your sales representative for a listing of the pricing.

Is anyone working with VMware resellers for services that Oarnet should talk to help provide services/training? If so let TJ Sandor know. Is anyone doing Desktop projects? Eastern Gateway CC did a desktop presentation at OHECC. They had to do to a major expansion in a short time, and did it via VDI using VMware. Edison CC also is using VMware View. Columbus State is using it at their Delaware campus. U of Toledo has a 5k seat project. There are several others if you need to talk to a resource. OSU is doing collaboration with Columbus State on this.

OARnet Network and Technology Updates
Paul Schopis

Change in administration. The state is replacing the CTO (K-16 technology officer) with John Conley. They are moving faster than he has seen in the past for the new administration to put things into place. OARnet has the view that they should engage the new Chancellor and the new CTO in a conversation of how they can help them achieve their strategies.

OMMC technical Update- all are stuck on environmental assessments. They are running into Endangered Species, Indian Burial Grounds (affecting Horizon most), and Historic buildings.

Consolidated Network Architecture – Ohio Public Broadcasting HD TV has been rolled onto OARnet's IP service. The Radio Service is waiting MOU updates. They are redesigning the intra Partners network (BOR, OhioLink, OLN and eTech).

Network Operations – Oarnet is moving to an optical-mesh architecture implementation with full mesh lambda capability to replace the ring architecture. It has the capability of running longer distances. Ring 0 is complete; Ring 4 is underway now. The east side of the ring is complete and the issue regarding fiber dispersion has been resolved and is passing test traffic.

Shared Infrastructure – They are developing different service models and are current running a "Gold" model on a community cloud service. They are working on a Bronze and Silver service models. The Silver service is like an Amazon service, and for the Bronze they provide the provisioning, but you do the programming. They are also looking at a virtual computer lab. This is in the development phase and the first step will be a pilot program. After the proposal is done, there will be call for participation. This would allow access to lab resources from remote locations. The roots for this project come from the high performance computing space. The code is all open source and they will determine whether it can be a production service using open source, or whether they need to use a commercial product like VDI from VMware. There is a question about the tools available for managing large numbers of virtual systems.

Will there be different OS systems available in the Virtual Lab? Yes, they would like to allow you to use any OS you want. In the testing they would like to have multiple OS's tested.

CIO's are looking to see if you can consolidate resources and reap some savings.

Is VCL replacing what Prassad did in the past? Not necessarily. Would like to find where the best spot will be in cost and usability.

Developments in Cloud Computing – Distributed Management Task Force (DMTF). The biggest problem with cloud computing is that the various virtual systems don't interact well. VMware, Microsoft, and Citrix are working on an Open Virtual Format for interaction between the virtual systems. They would require an envelope that would contain the necessary information and all other stuff is extensible. This would provide all information down to the machine level. This summer IEEEE has announce new protocol, P2301, for OVF idea of moving things around dynamically and P2302 is the operational aspects of this such as Federations. An example of the need for this would have been when OhioLink's Distributed Repository Commons (DRC) project needed to be moved.

Designing and Implementing a Secure LAN strategy
Scott McCollum and Darnell Brown
(slides are available on OARtech site: http://www.oar.net/about/oartech/presentations.shtml)

They gave an overview of the institution: 26k students and 2k employees, 55 acre 20 buildings with 5 remote sites, 240 servers (80% virtual), 5,400 PCs and 80TB storage. The project they discussed was instituted to take care of infections before PCs connect into the network. It started back in 2004 when the first major infections cause problems on multiple campuses and they began looking and implementing network access control (NAC).

NAC definition: Authentication of user and/or device, restriction of traffic types, compliance verification with policy, quarantining non-compliance systems and remediation of the problems. There are many proprietary implementations. They were not interested in going through the proprietary path, but instead looked at the Trusted Computing Group's (TCG) TNC architecture which was formed to develop the standards.

Their approach: Identified the strategy and evaluated the existing capabilities of the network. They then identified the needs to fill in. The good includes a standard image, images built and maintained centrally, lab computers are locked down and the image is secure. They have automated account management and processes for creating exceptions. AD is the repository for all known-users and known-devices. The bad is the employees are local administrators of their computer and IT is unable to force the images. The ugly is the open jacks in public and unsecured spaces and the growing demand for wireless. They defined a strategy that includes 3 access levels with regard to users and devices. See slides for detailed definitions. He showed how their meshed routing core is connected to the switched edge. They used network authentication based on 802.1x.

A new PC connects to the network and has no connectivity until the OS connects to the switch with 802.1x. The switch authenticates to a radius server. The radius server checks with AD and a filter id is sent back with the policy for the port. This policy defines the access the new PC has.

They are using Enterasys to identify and enforce the traffic based on the policy. A user role is for known devices and a specific role is applied to prevent the system from masquerading as an unauthorized server. For example, they deny port 25, 80, 1434, and 67.   You are defined within a specific VLAN. The containment role prevents bilateral traffic on TCP and UDP ports 1023, 5554 and others that are used by viruses or Trojans. Another role would be a printer role that denies all traffic by default in a production VLAN, then they allow source port 161 (SNMP) and allow bilateral ports 23, 9100, and other specific printer ports for communication. The VoIP phone role uses Shortel and prioritizes the VoIP traffic and identifies the devices by MAC address, though they have looked at 802.1x authentication. They contain VoIP to a specific VLAN and prioritize MGCP, RTP, and FTP over non latency sensitive protocols. Other roles include Corporate User, Guest Access, projector, tartan card, unregistered, quarantine, and Macintosh computer. You can have up to 8 possible devices authenticated to a single port.

The timeline for implementation – They started in October 2004 by defining strategy, defined the AUP and did system installation in 2005. They did the NAC roll out in 2005-2007. The implementation took longer than expected because they found each platform and vendors did things differently. They went through a lot of pain to develop their system but they won several awards for their solution.

The issues that came up included: each of the components acts on it own; time and delays in the boot process and transition times; no central repository for status or actions; and building the skills in front line support. You don't want systems and network engineers troubleshooting all PC connection issues.

They added a NAC appliance from Enterasys to proxy the connections to the other necessary pieces of the solution. It provides a log and database of what is happening with each of the pieces in the connection process. Before the NAC appliance, Sinclair had to build their program. They wanted to leverage existing policy to enable the architecture. The NAC appliance gave the engineer a view of what status the port was in when connecting and provided end system monitoring. This allowed them to see how many systems were connected and in what state they were in. They can see the history of the connections for a system and can force a re-authentication or quarantine.   They can also lock a MAC down to a specific port.

How do customers know they've been quarantined? When you open up a web browser you are redirected to a web page indicating that the system has been quarantined.

The operator can do an evaluation of the port to determine why a port might/or might not authenticate and see what devices have been connected to the network. Their system will manage both wired and wireless connectivity.

They did a demonstration showing what an end user would see connecting to the network as well as what you would see at the management console. The unregistered status has a very limited guest access. After login the acceptable use policy is presented and they must accept it. If connected via a wired port, the system is not given any access off the registration network. It can download an agent, either a persistant or non-persistent agent from Enterasys to determine whether the system fits their access control rules. They modify the rules to define what rules would be applied to each roles.

For wireless configurations, they have Enterasys wireless and the traffic is tunneled back to controllers. You are required to authenticate to the network as well. They have several different wireless networks within their current strategy to be able to assign devices depending on their role. They have 4 wireless gateways to allow for redundant connections to the network. The benefit they get from using the Enterasys NAC appliance on an Enterasys based network is the granularity of the policies they can apply to the ports.

End users can choose which agent they want to use, the non-persistent or persistent. If they choose the non-persistent agent, they must have their system checked every 5 days.

The NAC appliance was just introduced to their network last November.

What about security devices? Their security network is a completely separate network that is not supported by the same group as the data network.

How do you deal with dynamic egress? These are devices that connect once and then don’t do anything. They needed determine how to deal with this issue. They currently set a default VLAN.

Meeting adjourned at 12:30