OARTech Notes for April 9, 1997

Galen called meeting to order at 10:00. Everybody introduced her- or him- self. Kingsley moved to accept last minutes from the last meeting. Seconded and approved. Upcoming June items are review of White paper and picking a volunteer for the new OARTech secretary.

SMTP and Novell (and others too)....

Most of us have grown up in shops with big systems. Now the desktop computer is dominating. What do we do to assure reliability and maintainability? David, Eric, Galen and Kingsley have had recent experiences with several popular packages. David has experience with SL Mail. To David, the office suite for UNIX is vi and ls :-). David got in touch with Jack DeWinter from Canada. Jack's package went commercial via Seattle Labs. Jack still maintains the code. SL Mail is a full SMTP server that runs under NT, WIN95 and legacy 16 bit systems. The NT version is $349. The program is also downloadable as a 30 day trial. Download from www.seattlelab.com. The basic requirements: an Intel box running NT, a registered DNS name, an MX host and an IP address.

How does it interface with a firewall? So far, this has not been a problem. It could be a problem if you don't have a static IP due to the behavior of the firewall or address allocation mechanism on the network. The system configures with a simple menu; the icon is placed in the startup group. The program offers full logging of all the transactions. User accounts, mailing lists and auto responders are added and maintained via the Windows GUI. The mailing list feature is very easy to set up. With the full version of the package, there are no limits on the number of accounts, aliases or lists, other than the capacity of the system. Aliases and users may be imported exported via text files. One feature that has not been implemented is a bulk remove via file or automatic expiration of inactive accounts. There are a wide variety of configurations controlling inbound and outbound message handing such as when and how to hand off to a smart host. Bandwidth can be managed by controlling the allowable number of simultaneous connections.

Logging is very configurable. POP3 is supported for retrieving mail. Q: Passwords are clear text? Yes, only when being imported or exported. The accounts must be managed from the system console. Q: Are the mailboxes encoded? No. Q: The number of recipients may be limited; does this prevent the server from being used as a spamming relay? I don't know, but the maximum size of a given letter may be limited. Q: Will an error message be bounced? Yes. Q: How are MIME attachments handled. This is really a mail client issue; the server doesn't care. Q: Can receipt from certain domains be blocked? Yes: by either domain or by IP. DeVry students use Eudora 1.44 set up on a floppy diskette downloaded from a Netware server. All the students mail and personalized copy of Eudora stay on that diskette.

Ipswitch is another package with similar capabilities, running on NT. Ipswitch was able to pull in 1800 accounts from an AS400. What's nice is that Ipswitch is that it may be managed on web port 8383. The price is $380 for the basic package, $100 additional for the web interface. A version that supports LDAP and a variety of other features is due out second quarter of 1997.

Galen on his project using IMS: This last semester, Galen was given the charge to set up access to student labs, set up a lot of accounts, etc. Galen, coming from a UNIX-oriented background found the idea of dealing with high volume pointing and clicking to be daunting. The applications distributed with NT are unacceptable because they require complex manual binary editing of the registry. He discovered IMS, which comes from Microsoft's European development lab. IMS has the advantage of being fee. Documentation and the binaries may be found at emwac.ed.ac.uk. IMS has the ability to automatically build the accounts automatically. There are limitations of IMS's flexibility for aliasing and forwarding in a pre-existing environment with multiple repositories. IMS has the ability to accept mail for multiple domains. Aliasing is done with text files similar to the style of UNIX. The service has to be started and stopped via the NT control panel whenever a change is made to the configuration. Galen feels that one of the biggest benefits is low administration overhead. He likes to keep most of the management focused on a UNIX system. If your needs are fewer, also consider a package named BLAT. Galen supports 1400 accounts on an NT machine with 64 megs, 200 MHz Pentium. IMS doesn't tax the system very much. Galen's server is handling all other student file services as well.

Q: Why use anything other than exchange? Exchange is really good at integrating with X.400 and similar systems. It is big and needs management, however.

CERT Advisories

CERT mailings: Recently, there have been several worrisome messages regarding the vulnerability of INND news servers and POP servers. OARNet has modified sendmail.cf to prevent the INN servers from mailing to anybody outside the local domain. The CERT advisory applies only to the University of Washington IMAP daemon. Be aware that much code is based on the U Wash implementation. Pat: had to stave off an assault; was in contact with Steve Romig. There is some desire to form a task force to develop policies, procedures and contacts. Contact pvendt@wright.edu if you are interested. Ohio State is forming a CERT First team. KSU was being mail-bombed from one of the regional campuses. A regional campus had a Cisco terminal server with a PPP security hole; the solution was to fix the hole. George is working on the legalities and issues pertaining to unsolicited junk mail. For instance, Sanford Wallace sells a junk mail service provider; he's currently at aegis.net. George has filed amicus briefs in several cases. The Compuserve case is still open. For the present, junk mail is being treated as common law trespass - if you've put the originator on notice that you don't want your system accessed by that party. Sendmail older than 8.8.5 is vulnerable use as an unwitting relay. Newer versions of sendmail offer rule sets to block exterior relaying and blocking of problem domains. There are several mailing lists dealing with abolishing spamming: spam-l@peach.ease.lsoft.com and spam-law@zorch.sf-bay.org. George would like to hear from universities with law departments savvy in communications law. Perhaps, the junk fax law may be adapted to email. Contact George at tigerwolf@tigerden.com. The Federal Trade Commission is soliciting comments through April 15th, 1997. Q: What makes you think you can stop this, if pornography can't be shut down. George feels this is a different issue because the junk mailer is intruding into your system, rather than you going out to the porn site. Q: How do people find out about spamming in a timely manner; i.e. how do you monitor the performance of the server? Contemplate also, web push services.

Groupwise

Patti on Groupwise: Patti Brewer is manager of the LAN Operating Systems group. They are an in-house implementation group that competes with VARs to provide turn-key solutions. In general they don't push Groupwise. They install an SMTP gateway for a department, then configure Groupwise. The calendaring program of Groupwise, however, is of particular interest. The old approach to scheduling a meeting was to use a shotgun approach. The desire is to develop a more savvy approach for electronic scheduling, conflict resolution and document distribution. The solution had to encompass PC/Win, Macintosh, legacy systems, UNIX and work-at-home. Patti's team decided to use the Universal In-box, but decided not to use the email part. The other issue is that they don't like using Netware machines for application serving; they'd rather use NT boxes. Groupwise does run on NT and falls under the Universal Licensing Agreement for about $12.75 per user. Contact Patti at brewer.57@osu.edu.

What is LDAP?

Todd Atchison from Ohio U: LDAP (Lightweight Directory Access Protocol) and X.500 are directory services. X.500 is a object storage tree. X.500 is accessed via DAP. DAP is complicated and difficult to manage. University of Michigan saw the benefits of X.500, but wanted to have something simpler; LDAP is the result. X.500 has a tree of objects growing from the US Standards Organization. It is indeed registered similar to the idea of registering a domain with the Internic. Most people are thinking of using LDAP as an electronic replacement for a phone book white pages. LDAP is a server based protocol accessed on a port via IP or UDP. The source code is available from University of Michigan. Netscape and others do indeed have commercial implementations. Using ldapd is an indication that you have

X.500. Slapd is an encapsulation mechanism that prevents one from having to deal with the complexities of the whole X.500 structure. University of Michigan thought well into the future by providing finger gateway, white pages gateway, and tool kits for developing other services. All mail to Ohio U goes through mail.mail500.ohiou.edu. The relay machine looks up in X.500 to determine how mail should be dispatched.

Access controls may or may not be a problem, depending on how your specific LDAP and X.500 interact. Access control is typically rule-based. Slapd runs without an X.500 back end. Because it is self-contained, access control is done through slapd. Beware of proprietary vendor implementations. Replication is an issue at a large site. A main server would be used to synchronize a number of LDAP servers used in departmental settings.

Ohio U is a DEC shop with a legacy VAX and a number of Alpha/UNIX machines. They use DEC X.500, DEC's web interface and a number of customized U of Michigan servers. They have about 50,000 entries in their X.500 server. The X.500 server is essentially an electronic realization of the hard copy phone book; it is based on authoritative records coming from payroll, admissions, etc. The system is automated; no direct user modification is allowed. The reasoning is the security issue of clear text passwords on the wire and problems of rebuilding the directory in the worst case disaster scenario. Currently, they use mostly DEC tools running on large UNIX Alphas.

What are the challenges?: The user resistance to change. There was the advantage that the old system was due for improvements. By careful planning, the system was ready and functional on time. There is a complex state driven machine that uses a variety of metrics to decide when an entry should be deleted. This is best implemented in C code. LDAP is a good vehicle for mail forwarding, but does require the user to be facile in sendmail configuration. Newer sendmails would probably be easier to customize than the DEC IDA distribution product.

Current issues:
    Naming: how are people going to be named in the database;
        they use X.400
    Recoverability: more difficult if you allow end-users to

manipulate records.
- User modification: edit a back-end with periodic database transfers into the tree.
- Listserver functionality.
- Add departments, guest accounts.
- Switch to Umich LDAPD and DCE, SSL integration: the benefit is single sign-on multiple services. Note that Microsoft has integrated DCE into ActiveX.

Future:

- Rapid evolution: results in some proprietary implementations (eg. H-P).
- Security (DCE) integration
- Attributes sets - setting own standards: fields are currently up to vendor/user.

Summary:

- Successful migration 5K to 50K entries.
- Reliable operation, but more complex.
- Excellent base for infrastructure.

Q: Is there an LDAP web page? Try looking at www.city.umich.edu. Note that Netscape hired a lot of people from umich. Q: Are the X.500 entries open. Yes; they're the same as the hard copy phone book. Q: I'm using the CSO name server tightly linked to mail, what do I do? LDAP has to make two sendmail invocations. Sufficient CPU horsepower is required.

Lunch Break

A very nice lunch of salad, pizza and soft drinks was provided courtesy of OARNet.

Galen also shared a letter from the Governor to Tony Yankus at Oplin, expressing concern over use of publicly funded equipment for accessing unsavory material at public libraries.

A sample sendmail.cf to shut down unauthorized mail forwarding was made available.

Featured speaker

Danny Lis of Skycorp: Skycorp contracted to provide dial-up services for Ohiolink patrons. Skycorp is also providing a similar service of per-user IP addresses for a project called Building Industry Platform. Skycorp decided to build their own platform with web access backed up with the Oracle database engine. Skycorp has developed secure web access services for several large clients.

The issue: how do I outsource dial-up access, but still maintain the IP address predictability and uniqueness as required by the Ohiolink data source providers. Skycorp provides a known subnet for the subscriber institutions. At the time the patron dials in, a Skycorp's server performs a query on the institution's Inopac library system database. The university provides a boolean value that determines whether the client should receive a non- privileged general IP or an authorized IP known by Ohiolink. The authentication is possible through terminal servers in a number of cities. Universities may either sub-let a class C IP block or choose to lease an IP block form Skycorp. Skycorp will negotiate with the member university for a POP installation in a given location. Upon dialing and connecting, the patron is presented a web page customized for the member institution.

Q: How much does it cost? Institutions have to negotiate individually. The price varies with the number of anticipated patrons. Typically, it should be below $20 per month per patron.

Skycorp does offer several value added features such as customized web pages and resume on line. The patrons are also allotted two to five megabytes of storage space on the Skycorp server. At UC, the students pay individually and are billed to a credit card monthly. Skycorp is willing to negotiate bulk purchases. 1-800 dial access is available and is billed separately per hour. Skycorp is willing to install a POP, but only after negotiation with an institution to guarantee a certain level of revenue stream.

Kevin

The Support Center at OARNet: Kevin reiterated the mission statement (see the web page for wording).

Support issues in order of frequency: Mail, Line, Routing, DNS, Equipment, News, Wrong Number, WWW, Software, Misc., User Config., Service Change, Training, Time Server, FTP

Support rate: Calls/month: about 325 OARnet, 75 OPLIN

Focus for Improvement: Teamwork, Training, Staffing, Facility, Telephone System, Separate OPLIN phone number, Dedicated OPLIN Specialists.

SOMACS Update

Ruth: Ameritech is making the 60 day installation deadline. The problem is that there are still a lot of troubles with provisioning and turn-up problems with lines not passing packets properly. There are now nine schools with a total of 56 lines outstanding. There is a backlog of schools asking for DS3 or OC3C circuits. Please allow at least several months lead time for Ameritech returning estimates. OARnet is working hard to recover any equipment that was loaned out during the installation phase. Suggestion: OARnet may want to consider sending out what equipment is currently showing in their inventory for the member schools. Some money is still available from the NSF for schools who want to install T1 circuits despite the fact NSF is emphasizing high performance networking.

Internet 2, etc.

Gene: A rather comprehensive package of network topology and load diagrams was passed around. Note that Ohio is centrally located relative to many asserts accessible through the Internet. Many upgrades to the backbone are planned for 1997. Cleveland

and Akron have recently been upgraded to ATM switches; they now terminate in the OET/Office Tower connections. Several additional switches are on order to complete a ring design. The design of the ring is planned to eliminate any single points of failure. Negotiations are under way with MCI for the OC3 connection. For instance there is only a single DS3 circuit available into Kentucky. The supplier that has the circuit wants $15,000 per month. Luckily, in state, MCI has more capacity available. Many 7000 routers are being replaced with 7500s. RSP2s are also being replaced. The current routing table has about 40,000 entries. Lately MCI and CICnet have experienced some problems related to running very new implementations of Cisco's flow switching code. The code will be required to achieve the next generation of routing; hopefully, it will be stable by the fall 1998. The concept of the Gigapop is being finalized; Gene feels it is quite do-able both in terms of cost and availability of lines. The ultimate role of Internet 2 is still being defined. Gene feels it will go pretty well beyond the original VbNS definition.

Pat Vendt points out that UFL is working with their equivalent of OARnet to get the NFS grants. Gene replied that the OCARNET is working under a similar model. The grant is for $350K for two years, and only covers connectivity; not capital equipment. Steve Gordon is the person who is coordinating the OCARNET and grant.

Ohiolink

Anita: The biggest think we'll be hearing in the next few months is the bringing on of full text journals. They are working with Elsevier, who has 1200 journals. The collection has been imaged and covers the last few years. The database could be larger than a terabyte in less than a year. 175 scientific journals will be added. Imaging software from UMI is being added. A number of sources in .PDF format will be made available. Ohiolink is considering moving to Columbus for easier access to bandwidth. There is staffing positions to be filled for a network engineer and a multimedia product developer. Both positions will be advertised shortly.

New Business

None. Moved to adjourn. Meeting closed at 14:20