University of Oregon

COMPUTING NEWS

TWENTIETH ANNIVERSARY ISSUE! Winter 2005

Senior Systems Manager Bob Jones begins the process of assembling the new Darkwing cluster. The new Linux systems that comprise the cluster will speed email, web, and other network services. Story on page 4.

IN THIS ISSUE...

Campus Network Users Now Have More Control Over Stripped and Defanged Email

Bob Jones
Senior Systems Manager
Administrative Services/Computing Facilities

For some time now, UO systems administrators have been warding off computer viruses by automatically "defanging" or "stripping" incoming email traffic using a program called Procmail Email Sanitizer, or "PES."

PES typically either strips the message of suspicious email attachments, replacing it with a text attachment containing a warning, or renames the attachment to render it harmless (defanging).

Currently, we are delivering all stripped and defanged messages to their intended recipients, but as of March 1, stripped messages will no longer be delivered unless users explicitly request it.

Defanged messages will continue to be delivered unless users specify otherwise. Note, however, that many defanged messages are legitimate and contain nonmalicious attachments such as .ZIP files, and we would urge users not to choose to have them discarded unless they are *positive* that's what they really want to do.

You may specify the desired behavior for stripped and/or defanged messages by going to

https://password.uoregon.edu/husks/

UNIVERSITY OF OREGON

COMPUTING CENTER

TWENTIETH ANNIVERSARY ISSUE

COMPUTING NEWS
VOL. 20 #1

Computing News is published quarterly by the User Services and Network Applications staff of the Computing Center.

Contact: Joyce Winslow
jwins@uoregon.edu

Photography: Dave Ragsdale
dave@uoregon.edu

Joe St Sauver, Ph.D.
Director, User Services
and Network Applications
joe@uoregon.edu

Website:
http://cc.uoregon.edu/cnews/

Got Extras?

If your campus department receives surplus copies of *Computing News*, you may return them to the UO Computing Center for redistribution.

Large-format Scanner On the Way

The new scanner is the latest addition to the Architecture and Allied Arts Output Room, which caters to large-format printing needs on campus

Chris Jones
Director of AAA Computing Services
jonesey@uoregon.edu

The University of Oregon's Educational Technology Committee, Network Services, Telecom, and Facilities Services have partnered to purchase a large-format scanner for university use. The scanner will be available to the university community sometime in February 2005.

The new scanner, an Action Imaging Colortrac 4280, can scan documents up to 42 inches wide and half an inch thick. It will be housed at the School of Architecture and Allied Arts (A&AA) Output Room (280 Lawrence), where staff will be available to provide expert assistance to customers scanning large documents. The Output Room is also equipped with large-format color and black and white printers capable of producing signs, posters, banners, and blueprints.

To cover staffing and maintenance costs, customers will be charged a nominal fee to use the scanner.

To learn more about the specifications of the new scanner, visit the manufacturer's website at **http://www.action-imaging.com/colortrac.htm**

If you have questions about the large-format scanner or if you would like to use it once it arrives on campus, please contact Karl Owens, A&AA Output Room Manager (*karlo@uoregon.edu*). The Output Room is open Monday through Thursday from 9 A.M. to 10 P.M., on Fridays from 9 A.M. to 5 P.M., and on Saturdays from noon to 6 P.M.

Deb Carver Named Interim Associate VP for Information Services

Ron Renchler
Director, Library Communications
UO Libraries
ronr@darkwing.uoregon.edu

Deborah A. Carver, Philip H. Knight University Librarian, has been appointed interim associate vice president for information services at the UO, following Joanne Hugi's retirement.

The AVP for Information Services is the university's chief administrator for computing, networking, and telecommunication issues. Carver will serve in the position while a national search for a new AVP is conducted.

Carver has chaired or cochaired the university's Educational Technology Committee for three years. She also serves as the university's representative for the Northwest Academic Computing Council (NWACC).

Carver, who was named the Oregon Library Association's 1999 Librarian of the Year, has been a member of the UO faculty since 1990. She was appointed by the Oregon Senate to serve on the Interim Legislative Committee on Libraries and was a member of Oregon's Statewide Database Licensing Committee. She represented the state as an elected member of the American Library Association Council from 1998 to 2001. She was president of the Oregon Library Association in 1995-96 and served on its legislative committee and chaired its Vision 2010 Task Force.

Deborah Carver, University Librarian and Interim Associate VP for Information Services.

A 1973 magna cum laude graduate in political science from the University of Massachusetts, Amherst, Carver earned a master's degree in library science from the University of North Carolina, Chapel Hill, in 1976 and a master's degree in public administration from the University of Virginia, Charlottesville, in 1984.

Accessibility Web Tip: Use the 'Skip Navigation' Link

A simple anchor link can make your web pages far friendlier to people using screen readers. This link, called "skip navigation," jumps over navigation links and takes the reader directly to the main content of the page. This saves screen-reader users from having to listen to repetitive navigation links as they tab through each page of your site.

Depending upon your design preference, skip navigation links may be either visible or invisible. You'll find a detailed explanation of various approaches to using the skip link technique, with examples, at **http://jimthatcher.com/skipnav.htm**

For more general information on how to design universally accessible web sites, see "Web Accessibility for People with Disabilities" at **http://darkwing.uoregon.edu/~atl/web_acs.htm** If you have questions about designing your website to meet accessibility guidelines, please contact James Bailey, the UO's technology access adviser (*jbailey@uoregon.edu*, **541-346-1076**).

The New Darkwing: A Briefing

Systems staff take the first steps in a major reconfiguration of our vital campus server system: where we're headed and why…

Joe St Sauver, Ph.D.
Director, User Services and Network Applications
joe@uoregon.edu

Susan Hilton
Director, Administrative Services and Computing Facilities
hilton@uoregon.edu

This article is meant to serve as a briefing for members of the campus community who may be interested in learning more about the Computing Center's work in upgrading Darkwing. Let's begin by talking about "classic Darkwing."

Classic Darkwing

Darkwing is a server that's familiar to many UO faculty and staff, although if you're like many users, you may know it only as an email server. In reality, while Darkwing does deliver email for over 15,000 faculty, staff and graduate student accounts, it does quite a bit more, too:

- Darkwing accounts serve as the basis for faculty, staff, and graduate student authentication for a variety of campus resources, including such services as wireless access, dialin access, virtual private network (VPN) access, and the Blackboard teaching and learning system
- Darkwing hosts several hundred virtual web servers, including key web servers such as **www.uoregon.edu**, the university's primary website, and many others (for a list of all the virtual hosts served from Darkwing, see **http://virtual-www.uoregon.edu/**)

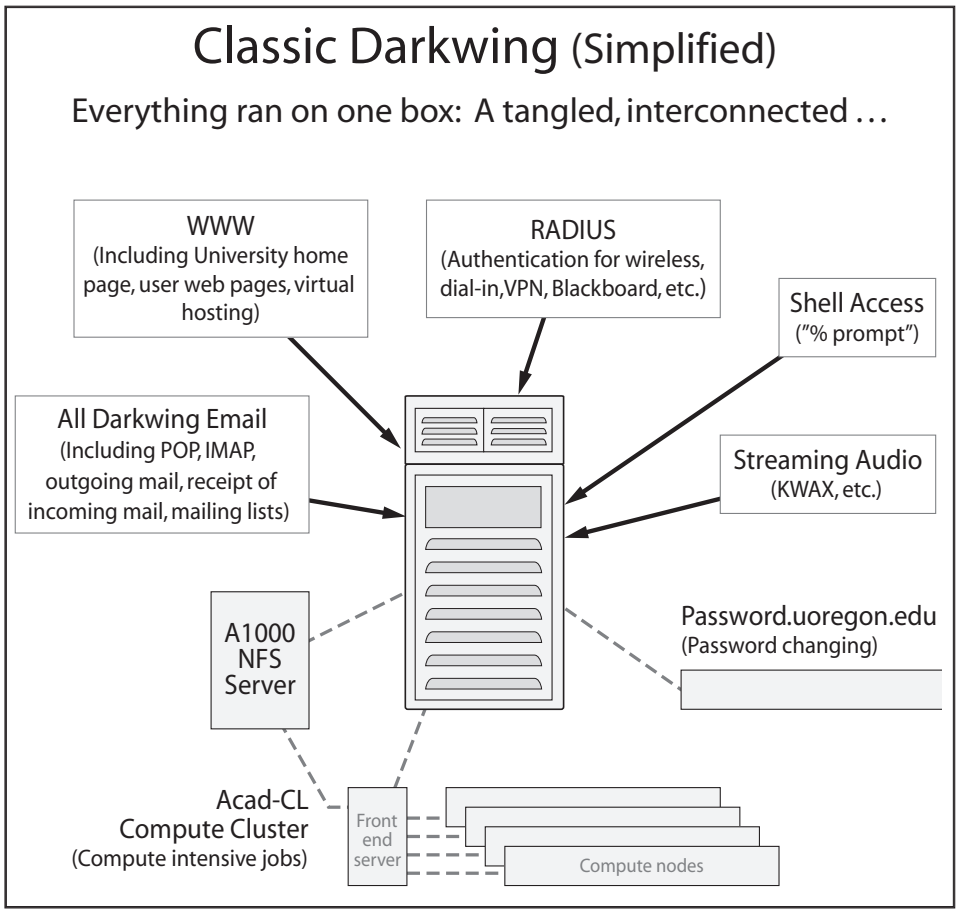


Fig. 1. The way we were… This chart shows the way Darkwing was configured before the upgrade began.

- Darkwing delivers streaming audio, via Real and Darwin Streaming Server, for KWAX and other high profile campus content providers
- Darkwing serves over 1300 majordomo-based email mailing lists
- Darkwing offers shell access for users who want to use pine, run statistical packages, compile and run their own programs, or otherwise work at the UNIX percent-sign **(%)** shell prompt
- Darkwing provides the boot environment and font server needed for X terminals such as those deployed in the basement corridors of McKenzie Hall and elsewhere on campus
- Darkwing acts as a print server for multiple campus print queues
- Darkwing also handles network backups of user files

(For a diagram of classic Darkwing functions, see Figure 1 above.)

That's a lot for a single six-year-old server to do. Not surprisingly, most noticeably beginning in 2004, Darkwing began to deliver unsatisfactory performance—in other words, "it got slow."

Monolithic Architecture

Moreover, having all those services on a single monolithic system also meant that if Darkwing did have problems, or if it were simply taken down for scheduled maintenance, the down time would affect many different activities, including mission critical production services such as faculty email or institutional web page delivery.

Running a single monolithic system also has implications for system replacement: if you were to replace a large monolithic system with an even larger monolithic system, you'd be investing in comparatively uncommon hardware with a premium price tag.

For example, Sun's top-of-the-line flagship E25K server starts at just over a million dollars (list price)[1] and it isn't very hard to configure an E25K in a way that would make it cost in excess of three million dollars, not including any significant disk storage. Even a more modest midrange Sun Fire E6900 with just 16 processors and 64GB of RAM has a list price of nearly $800,000 (again not including material disk space). In tight budgetary times, or at any time, that's a lot of money.

A final factor leading us away from monolithic systems is that we know from the commercial sector that it is easy to get to the point where no matter *how* much money you have, you can't buy a single system that's big enough to handle the aggregate load you may confront. For example, Google (at least as of March 2003) used over 15,000 commodity-class PCs [2] to meet the world's aggregate search engine requirements.

While we're nowhere near the size of Google, it's easy to see the writing on the wall: single monolithic servers don't scale well.

If We Don't Buy a Single Big Box, How Should We Split Up The Load Onto Multiple Smaller Boxes?

We thought about two approaches we could use to divide our load across multiple smaller servers:

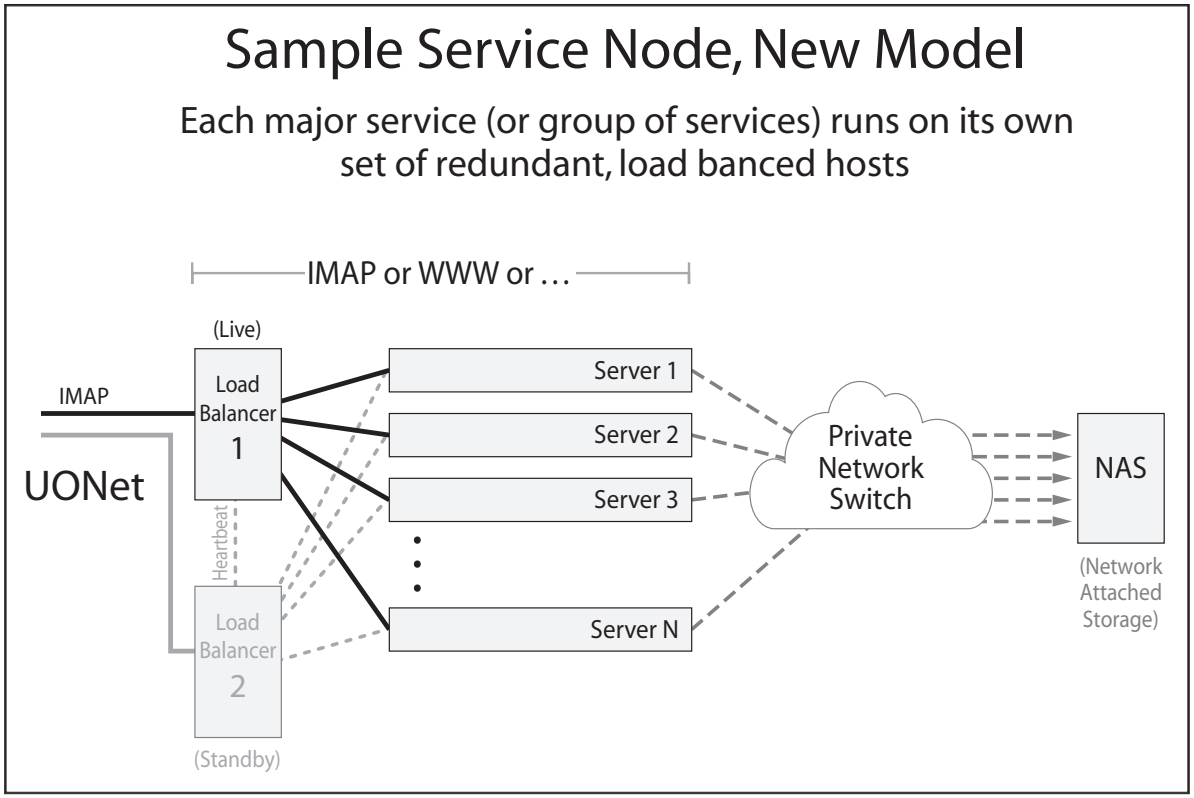
Model #1. We could divide things up by user. Taking that approach would involve:

- having each node running all services
- having some way to hash or "divvy up" users onto multiple nodes in a user-transparent way
- being willing to accept the fact that we might need to pay a substantial amount for any licensed product(s), if we needed to purchase and deploy those licensed products on each node
- recognizing that if we needed to add capacity, we would have to shuffle users around
- accepting the fact that it will be hard to evenly share load among nodes.

Model #2. Alternatively, we could divide the load by splitting things up according to service. Doing that sort of model means that:

- we can tailor nodes to the needs of particular services
- we can point traffic for a given service at a particular node via DNS
- we can limit the extent of licensed products we buy
- we can add capacity transparently by adding additional back-end nodes behind a load balancer.

Model # 2 is the model the UO has decided to pursue.



Server Building Blocks; Load Balancing

An inherent part of the new model is the use of commodity dual processor AMD Opteron-based 1U rackmount systems. Those dual processor Opteron boxes are the same sort of systems we've been using for a while for the current Academic Compute Intensive Cluster (e.g., the "acad-cl" nodes, see **http://acad-cl0.uoregon.edu/**), where they've proven themselves by delivering tremendous performance at a very reasonable price.[5] We're also looking at adding a less powerful (and less expensive) building block host to our architecture for situations where a dual Opteron, or even a single Opteron, would simply be overkill and unnecessary.

Two, three, or more building block servers, whether Opteron-based or something less powerful, would then sit behind a pair of load balancers (which are themselves simply building block servers, this time configured to run the LVS load balancing software).

Load balancers look at incoming connections along with backend server load, and then route incoming connections to a suitable server, either working round-robin style or by monitoring the load on each backend server and then sending connections to the currently most lightly loaded host.

Use of multiple load-balanced hosts in this fashion gives the university operational resilience by allowing one building block system to be taken out of service for maintenance or upgrades without users even noticing the change; the down side of this approach is that it increases server count (redundant servers are required) and it requires a way to share the load across the servers (e.g., it requires the use of load balancers).

Besides fixing the load problem and giving us critical operational resilience and a clean path for future growth, the new model also eliminates our reliance on expensive proprietary hardware and proprietary operating systems, while also allowing us to avoid the growing cost of maintaining aging hardware and setting the stage for enabling new services such as larger disk quotas.

Speaking of Disk Quotas, Storage Is Central

Even though Darkwing load manifested itself as general slowness, that slowness was really a function of limitations in the system's I/O (input/output) to disk storage as much as anything.

When you think about disk storage, you probably think about working within a comparatively limited disk quota, such as 100MB on classic Darkwing.

Emerging trends, such as large desktop drives (200-250 *gigabyte* desktop hard drives are routinely available now), and things such as Google's Gmail service (offering users 1000MB worth of free disk storage for email), meant that our traditional 100MB email quotas on Darkwing were really pretty antiquated. Meeting user expectations requires that we offer disk quotas that are basically an order of magnitude higher than current levels.

Simply buying more disk wouldn't be sufficient, however. At the same time you add disk space, you also need to increase the ability to do disk I/O operations (read operations, write operations, seek operations, etc.), and you also need to increase disk I/O throughput (the ability to shovel data over the wire from a server such as Darkwing to a network file server connected over the network).

It would do no good to increase the amount of disk space users would have if there wasn't increased capacity to read and write data to that disk space, and network capacity to move that data to/from the file server.

Our recent survey of Darkwing users[3], also identified the fact that users would like to be able to more easily restore accidentally damaged or unintentionally deleted files from backups, and the fact that users would also like to be able to get at their Darkwing files via a Microsoft Windows file system (e.g., "CIFS" or "Samba") rather than just via Darkwing's traditional UNIX-oriented NFS.

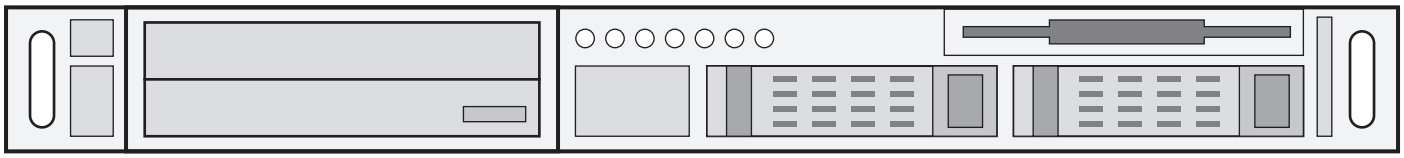
Still another factor was the desire to be well positioned to move to NFSv4 as soon as possible to minimize potential NFS-related security issues.[4]

Building Upon What We've Already Been Doing

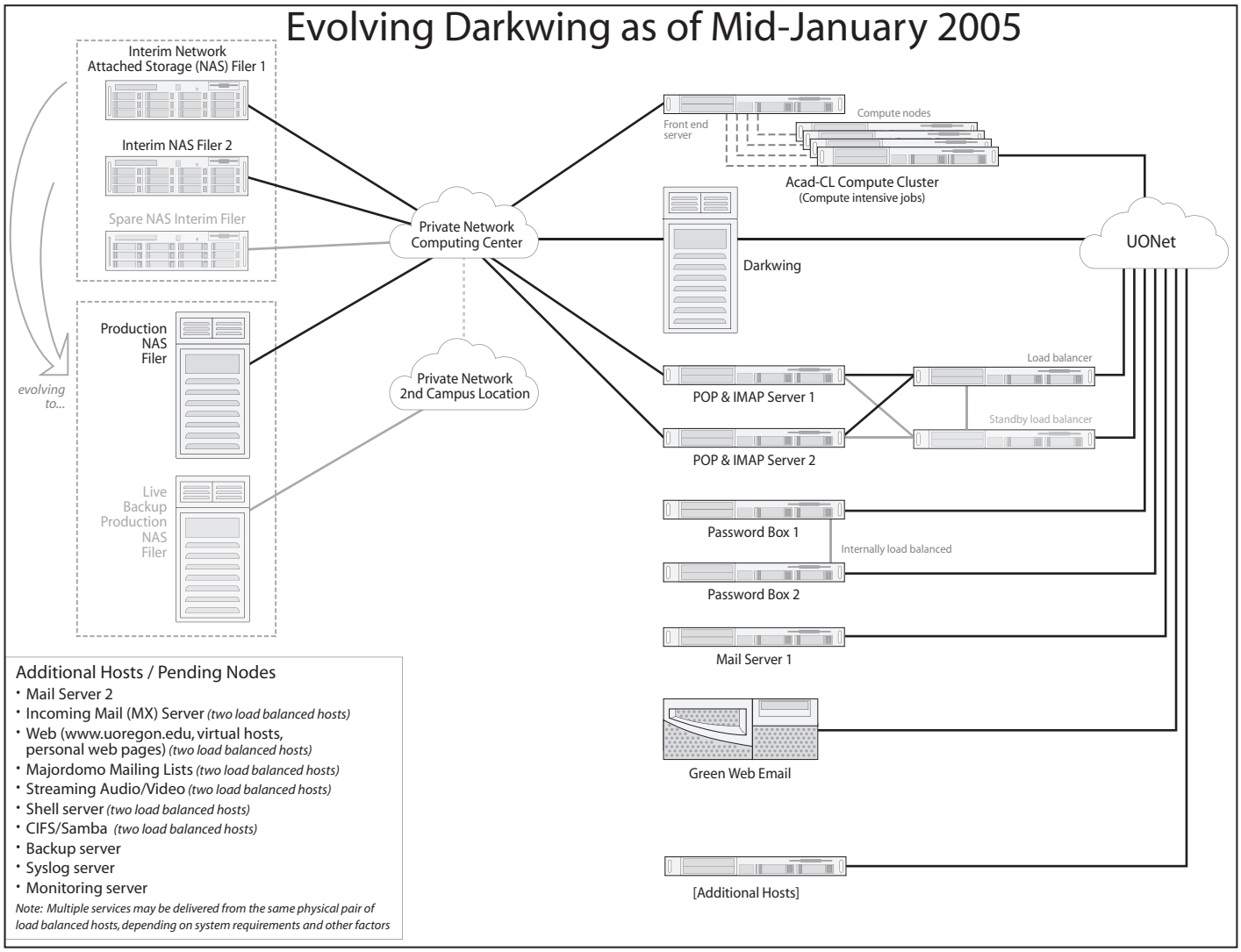
Over the last few years, the Computing Center has been actively experimenting with a variety of new technologies—technologies which have ended up shaping much of what we'll be doing in upgrading Darkwing.

We've already described the Opteron-based building blocks we'll be using; they are one example of a technology that's proven itself and moved from the lab into production.

Similarly, at least for now, Darkwing's disk storage is running on commodity serial ATA[6] disk network attached storage (NAS), storage which looks



Building block servers: *a DVD drive (left) and two hard drives. Any number of these server units may be mounted on racks and deployed as needed, providing a more flexible model for network service.*



much like the sort of disk storage proven in the storage of terabytes of data for the ANTC Route Views project.[7]

A third example of moving proven technologies from one project to another can be seen in the use of RedHat Linux-based load balancers[8] in front of multiple systems, as pioneered on campus by the Administrative Services group and the Systems Group in conjunction with deploying Internet Native Banner.

Transition Architecture

The Darkwing upgrade process has already begun, albeit on more of an expedited basis than we might have liked.

The first stage of that upgrade was the migration of user files from Darkwing's old, slow, and bottlenecked disks to new interim network attached storage (NAS) filers.[9]

The interim filers we're currently using do not offer the scalability and feature set we ultimately want, but its deployment is giving us the breathing room we need to complete procurement of the mirrored production filer that will be the core of the new Darkwing architecture. As we write this, the migration of Darkwing user files to the interim filer has been completed.

The next stage of the upgrade involved migration of POP and IMAP (email reading) services from classic Darkwing to a new load-balanced cluster of Opterons.

Moving user POP and IMAP activity to the new cluster requires contacting Darkwing POP and IMAP users, asking them to change their email programs so that instead of POPing or IMAPing against **darkwing.uoregon.edu**, they access POP as **pop.uoregon.edu** (or IMAP as **imap.uoregon.edu**).

At the same time we asked users to make that change, we also asked them to change their *outgoing* email server name from **darkwing.uoregon.edu** to **smtp.uoregon.edu**

At this time, the migration to the new **pop.uoregon.edu**, **imap.uoregon.edu** and **smtp.uoregon.edu** servers has also taken place.

We've also moved IMHO (the "green" web email client) off of classic Darkwing and onto its own server. Because users currently access that service by clicking on "Web Email" from the UO home page, or by visiting **http://email.uoregon.edu/** directly, we've been able to accomplish the migration of that service in a way that's transparent to users (except

for the fact that green web email is noticeably faster).

For an overview of Darkwing's current stage of development, see the *Evolving Darkwing* diagram at the top of the previous page.

The Production (Mirrored) Filers

Concurrently with the steps described above, we're also working on procuring a pair of production network attached storage (NAS) filers that will form the core of the new Darkwing. Because of the size of those filers (8TB, or 8000GB initially, scalable to just under 100TB or a tenth of a petabyte), and because the contents of those filers will be key to university operations, the contents of the filers will be "mirrored," or constantly synchronized, with one server located in the Computing Center and a second server located elsewhere on campus, connected over a private network consisting of multiple channel-bonded gigabit ethernet links supporting jumbo frames.[10]

That mirroring, along with traditional off-site tape backups, will ensure that even if the primary filer were to be destroyed by a catastrophic fire or other accident, the backup filer would still be available to provide access to your files.

Once deployed, the production filer will also offer users easier user-controlled restoration of damaged or accidentally deleted files, and eventually the ability to access files via CIFS/Samba. Once the production filer's in place, disk quotas should increase from 100MB to 250MB, and then, depending on utilization and other factors, upwards from there.

Deployment of the production filers will also be the key event that will allow us to finally decommission **oregon.uoregon.edu**, our legacy OpenVMS system, and with it, "black" web email ("green" web email will remain available, and we're also looking at a third generation web email client that will support a spell checker and address book, two features noticeably absent from the current green web email).

password.uoregon.edu

We've also recognized that our web-based password changing system, **http://password.uoregon.edu/** needed an upgrade.

For those who may not be familiar with **password.uoregon.edu**, that host provides the web-based interface for making password changes on Darkwing, Gladstone, and Oregon, while also allowing users to do things such as:

- check their disk usage via the web (**http://password.uoregon.edu/quota/**)
- set or disable mail forwarding (**http://password.uoregon.edu/forward/**)
- set their spam filtering preferences (**http://password.uoregon.edu/allowspam/**)
- set their viral husk disposition preferences (**http://password.uoregon.edu/husks/**)

Because most users rarely if ever access their Darkwing accounts via *ssh*, **password.uoregon.edu** provides an easy web-based interface for accomplishing tasks that would otherwise require *ssh* and arcane UNIX commands to accomplish.

The upgrade to **password.uoregon.edu** has been completed at this point, and that system now consists of a redundant load-balanced pair of systems that has far greater capacity than its predecessor.

Moving to a pair of systems for **password.uoregon.edu** means that down time for that host should now be a thing of the past, and we now have surge capacity to handle situations when many passwords need to be changed in a short time interval.

LDAP Authentication

Still another change that's underway is LDAP-based[11] authentication. Remember that one of the things that Darkwing currently does is to serve as an authentication system for faculty, staff, and graduate students so that the university can control access to resources such as the wireless network, dialin modems, the virtual private network (VPN), and the Blackboard teaching and learning system. Gladstone serves a similar authentication function for undergraduates.

When users supply their Darkwing username and password to access the UO's wireless network, or modems, or Blackboard, we have some confidence that two things are true:

1. They are who they claim to be and are somehow affiliated with the UO, and secondarily
2. They are *probably* UO faculty, UO staff, or a UO graduate student (although based simply on their ability to login to Darkwing, we don't know which of these they may be, and there's a chance that they might be an undergraduate, e.g., someone using a Darkwing student account specially created for a class)

Note that the second assertion is pretty weak. For example, if we had some service that could be provided *only* to staff members but not to faculty or graduate students, based on current Darkwing credentials it would be impossible for us to restrict that service to staff only.

Thinking about that, you start to understand the fact that authentication is only one leg of what's often called a three legged "**AAA**" stool. The three legs of that stool are:

- **A**uthentication ("I know **who** you are," often accomplished by using a username and secret password),
- **A**uthorization ("I know **what** you are/what you should be able to do in that role," e.g., I'm a faculty member, or an undergraduate student), and
- **A**ccess control ("I have the ability to control what you can access based on what you're authorized to do/see,"—for example, hypothetically one

might allow visitors to campus to access some databases but not others, or one might limit access to shared departmental printers to members of that department)

When the LDAP authentication project has been completed, Darkwing users will login just as they currently do, but behind the scenes the authentication process will be handled by the new LDAP server instead of directly by Darkwing.

Darkwing and Gladstone Consolidation

Another thing we want to mention is the eventual merger of Darkwing and Gladstone into a single unified system, with UO users—faculty, staff, graduate and undergraduate students alike—all using email addresses of the format *username@uoregon.edu*

While that project is still in the early planning stages, the process is greatly facilitated by the fact that we've always had a unified name space on Darkwing, Gladstone, and Oregon (the legacy OpenVMS cluster), partially in anticipation of the day when those systems might be consolidated. This means that if there are two accounts belonging to the same person, such as *jdoe@darkwing.uoregon.edu* and *jdoe@gladstone.uoregon.edu*, we don't need to figure out which of two account owners should be allowed to keep "their" username when merging Darkwing and Gladstone accounts.

The biggest question we're currently wrestling with when thinking about merging Darkwing and Gladstone is how to handle the possibility of two filesystems per user, with one tree of files from a user's Darkwing account and another tree of files from that same user's Gladstone account.

Our current thinking is that:

- users who have only a Darkwing account will see no difference; in a converged environment, their default directory will be their normal Darkwing default directory
- users who have only a Gladstone account will see no difference; in a converged environment, their default directory will be their normal Gladstone default directory
- users who have both a Darkwing and a Gladstone account will have their Darkwing directory as their default directory, and their Gladstone directory will live in a subdirectory (perhaps named "gladstone-files" or something similar)

As we work out these and other issues, we'll keep you posted. (Please note that it will be quite some time before we get to that merger project given all the other tasks which need to be handled first.)

Conclusion

We hope this information will help you understand a little about what's currently going on with respect to upgrading Darkwing. Although we've completed a lot of the work, we still have a lot more to do.

We know that you may have questions, so feel free to contact either of us (*joe@uoregon.edu* or *hilton@uoregon.edu)* with any questions or concerns you may have.

Notes:

[1] Sun Fire E25K Server
http://www.sun.com/servers/highend/sunfire_e25k/index.xml

[2] *Web Search for a Planet: The Google Cluster Architecture*
http://www.computer.org/micro/mi2003/m2022.pdf

[3] *Darkwing Faculty/Staff Survey Results: How You Voted*
http://cc.uoregon.edu/cnews/spring2004/dwsurvey.html

[4] *NFSv4 and NFS Security*
http://cc.uoregon.edu/cnews/summer2004/nfsv4.htm

[5] AMD Opteron Processor
http://www.amd.com/us-en/Processors/ProductInformation/0,,30_118_8825,00.html

[6] Serial ATA
http://www.serialata.org/

[7] Route Views Project
http://www.routeviews.org/

[8] *IP Load Balancing*
http://www.redhat.com/software/rha/cluster/piranha/

[9] See O'Reilly's "Using SANs and NAS"
http://www.oreilly.com/catalog/sansnas/

[10] *Practical Issues Associated with 9K MTUs*
http://darkwing.uoregon.edu/~joe/jumbos/jumbo-frames.ppt (or **.pdf**)

[11] An excellent LDAP reference is O'Reilly's "LDAP System Administration"
http://www.oreilly.com/catalog/ldapsa/index.html

UO Network's Transit Bandwidth Boosted

This fall, Network Services increased the UO network's transit bandwidth from 81 Mbs to 100 Mbs. Users should notice improved responsiveness when visiting Internet sites during the normally busy hours of 2 P.M. to 6 P.M.

For Optimum Network Performance, Reconfigure Your Email Settings

As explained on pages 4-9, we're making progress upgrading Darkwing, and much of the work is already done. As a result of the upgrade, if your email account is on Darkwing and if you use POP ((Post Office Protocol) or IMAP (Internet Message Access Protocol) email clients such as Outlook, Eudora, Pegasus, or Mac OS X Mail, you'll have to reconfigure your email settings.**

Here are the settings changes:

SERVICE	CURRENT	NEW
POP	darkwing.uoregon.edu	pop.uoregon.edu
IMAP	darkwing.uoregon.edu	imap.uoregon.edu
SMTP	darkwing.uoregon.edu	smtp.uoregon.edu* *If you're using an off-campus non-*uoregon.edu* SMTP server, ***don't*** change your SMTP server setting
ALL	gladstone.uoregon.edu	NO CHANGES

***Specific instructions for making the settings changes for your particular email program are available at* **http://micro.uoregon.edu/email/upgrade/** *If you're unfamiliar with the terms POP and IMAP and are unsure what type of email program you're using, see* **http://micro.uoregon.edu/email/popvsimap.html**

We recommend that you restart your email client software after making these settings changes. In addition, you may be prompted to accept a new SSL key. If this happens, don't be concerned; this prompt is a normal part of the process. (In case you're wondering why we chose a "global" settings name that currently applies only to Darkwing, the answer is that in the long-term the new settings will work for *all* Computing Center email accounts.)

'Black' Web Mail Being Phased Out for Darkwing and Gladstone

Joel Jaeggli
Advanced Academic User Support Specialist
joelja@uoregon.edu

The University of Oregon's first generation web email interface, commonly known as "black webmail" because of the color of its login screen, is being discontinued for Gladstone and Darkwing as of the end of winter term (March 21, 2005).

"Green web email," as accessed through the "WEB EMAIL" link from the UO Home page or via the link **http://email.uoregon.edu/** will continue to be available as the supported and recommended web email interface for Darkwing and Gladstone users.

Access to "Black Webmail" for Oregon users will continue until the Oregon-Darkwing user migration is completed later in the year.

The "black webmail" login screen.

What's the Problem with Free Demo Copies of NIS Firewalls?

If you allow your PC's built-in firewall to be disabled in favor of running a demo, you could run into trouble when the demo expires

Dan Albrich
Manager, Microcomputer Services
dalbrich@uoregon.edu

In recent months Microcomputer Services has been seeing a lot of new Dell computers that come with a demo copy of Norton Internet Security (NIS) installed by the vendor.

The problem with demo software in general is that it expires in 30 or 90 days and then asks you to pay to continue to use it. Because NIS is a firewall software product, it disables the built-in Windows firewall by default. In addition, it also disables the Security Center messages for Windows XP Service Pack 2 users. If people later become annoyed with NIS and disable it because it's blocking a network application they wish to use, or if they simply refuse to pay when the demo period expires, they will end up completely deprived of all firewall and security center protection.

Firewall protection is too important for the health of your PC to be ignored. Firewalls block all incoming unsolicited connections, and without a firewall, your PC will automatically run services that wait for connection from arbitrary Internet hosts. (Obviously, this is a bad idea when the current generation of computer viruses and worms can infect your PC the very *instant* you connect to the Internet!) And you needn't worry that enabling a firewall will bar you from accessing such favorite services as web and email: you'll still able to access whatever services you choose.

Microsoft spent a billion dollars developing Windows XP Service Pack 2 and its updated firewall product, and in our estimation it does a great job for the average user. Service Pack 2 blocks unsolicited incoming connections by default. If you try to use software that requires a firewall exception, XP SP2 prompts you for permission to make the change. This makes it easy for you to use the network applications you desire, even when exceptions to the firewall must be made to accommodate them. *(Note that **any** firewall exception presents a risk. However, it's always better to allow a few exceptions than to disable a firewall entirely.*)

A practical example of this is the Cisco IP/TV client. When the user runs it the first time, Windows asks the user if it is OK to make an exception to the firewall configuration to allow this program to run. If the user selects "allow," then the exception is made for them. It's important this process be uncomplicated. Prior to Service Pack 2 for Windows XP, most users would completely disable firewall protection any time it "got in their way."

NIS has some advanced settings, like the ability to block both inbound and outbound connections. If you're very computer savvy and want to create custom firewall rules, then it may be the right software for you. Other users who benefit from third-party firewall software are those running a Windows version prior to XP which by default lacks firewall protection. If you want to get a nice free-for-personal-use firewall package for an older version of Windows, see Zone Alarm at **http://zonelabs.com/**

Our Recommendation:

If you have Windows XP, disable NIS, then uninstall it. To disable NIS:

- Open NIS by double-clicking the icon on your desktop
- Select "Status & Settings…"
- Select "Security"
- Click on the "Turn Off" button

After disabling NIS, you can use the *Add/Remove Programs* control panel to finish the removal process. Then, open the *Firewall* control panel (*Start -> Control Panel ->Security Center -> Windows Firewall*) and make sure the "ON (Recommended)" setting is selected.

If you do not have a Security Center control panel, this means you lack Service Pack 2, which is an important update for XP. This update can be had free of charge. Please see **http://micro.uoregon.edu/security/windows/** for details.

A note about Internet Explorer. Because Microsoft Internet Explorer (IE) has become a well-known vector for many viruses and worms, NIS includes a popup blocker for Internet Explorer. Service Pack 2 also includes an updated IE with built-in popup blocking. Even if you are running NIS or Service Pack 2, however, it's still a good idea to consider using an alternate browser, such as Firefox, for general-purpose browsing. You'll find Firefox included on the 2004 Duckware CD, which is free to UO faculty, staff, and currently enrolled students. If you don't already have a copy, please go to the Microcomputer Services Help Desk in 151 McKenzie Hall.

Who's Who at the Computing Center

Meet Lois Johnson, the UO's "voice of Audix"

Joyce Winslow
jwins@uoregon.edu

Lois Johnson
Customer Service Supervisor
*Telecommunication Services**

Have you ever wondered about the voice that announces your UO voicemail and assists you through the various functions of Audix, the UO's automated phone system?

You need wonder no more. The voice belongs to Lois Johnson, the soft-spoken customer service manager at Telecommunications Services.

** Although now part of the Computing Center, Telecom Services operations are housed east of campus in the Rainier Building at 1244 Walnut Street.*

Lois is far more than just a soothing voice, however. She is one of the key staff people in programming, maintaining, and troubleshooting one of the most essential services on campus.

Having previously owned and operated a small answering service in Corvallis for six and a half years, Lois is no stranger to telecommunication services. But when the advent of answering machines began to put a dent in her business, and with four children to support, Lois found herself juggling as many as three part-time jobs to make ends meet. So it was a relief when a friend and former employee told her about a job opening at UO Telecom Services.

Lois' first job with Telecom Services was as a telephone operator/receptionist, but as her skills became evident to her employers she rapidly took on increasing responsibilities, culminating in the supervisory position she holds today.

Over the nearly 20 years she's worked on campus, Lois has mastered the nuts and bolts of UO telecommunications, performing all the behind-the-scenes functions that make Audix systems work seamlessly: programming phones and digital sets, setting up videoconferencing sessions and cell paging for campus users and troubleshooting the systems glitches that occasionally crop up, as well as overseeing her staff of eight customer service assistants. Because she has been Telecom's "Jill-of-all-trades" over the years, she is in a unique position as manager, being able to thoroughly instruct new hires and pinch-hit when people are absent.

Of all the jobs she's performed at Telecom, Lois considers her work as a systems analyst the most challenging—and rewarding—of her career. Without the benefit of prior programming training, Lois's initiation into the world of coding was a bracing sink-or-swim experience, and she is justifiably proud of her hard-won technical mastery.

Off the job, Lois enjoys a slower pace of life on her rural property in Sweet Home, which she shares with her husband Will and cat Hobo. An Oregon native who has spent her entire life in the Southern Willamette Valley, Lois enjoys the simple pleasures of country living—especially fishing. She and Will take off every chance they get to angle for trout, steelhead, and salmon in season.

? **HOW SAVVY ARE YOU?**

Take the Phishing IQ Test at

http://survey.mailfrontier.com/survey/quiztest.html

« cybercrime in the news »

Portland NASA Hacker Gets Six Months

Gregory Aaron Herns, a 21-year-old from Portland, Oregon, was sentenced to six months in jail for hacking the NASA network, causing systems crashes that took hours to fix. For details, see

http://www.theregister.co.uk/2004/12/20/nasa_cracker_jailed/

"ONLINE DRUGS: Easy to buy, tough to control"

What's behind the dangerous surge in unregulated Internet drug sales? The Cleveland *Plain Dealer's* December 19 article, "Come along on a ride to some unchecked virtual drugstores," describes one investigative reporter's experience trying to track unsolicited online prescription drug offers to their source. See

http://www.cleveland.com/news/plaindealer/index.ssf?base/news/110345384929970.xml

Local Child Porn Distributor Gets Hard Time

In October, 53-year-old Robert Earl Smith of Eugene was sentenced to more than 50 years in prison for producing and disseminating child pornography over the Internet. See **http://www.crime-research.org/news/06.10.2004/692/**

Teen Author of Blaster Virus Faces Jail

A Minnesota teenager who confessed to writing the Blaster.B variant of the Blaster virus is looking at a possible three-year jail sentence and a fine of $600,000. For details, see **http://news.zdnet.co.uk/internet/security/0,39020375,39185483,00.htm**

Online Credit Card Processor Hacked

In September, online credit card transactions being processed by Authorize.net, one of the nation's largest credit card processors, were disrupted by a series of major hack attacks. Tens of thousand of online merchants lost business as a result of the attacks, which are still under investigation. For details, see

http://news.zdnet.com/2100-1009_22-5378217.html
http://wired.com/news/infostructure/0,1377,65039,00.html

Brazil: Hackers' Paradise

Eight out of ten of the world's hackers currently operate out of Brazil, according to a recent electronic crime report released at an international crime-fighting conference in Brasilia. The report also noted that the overwhelming majority of such attacks targeted U.S. websites. See

http://www.falkland-malvinas.com/Detalle.asp?NUM=4251

Undercover Cops Nab 28 ID Thieves

In late October the U.S. Secret Service concluded a successful sting operation by arresting 28 identity thieves who were trading tips on fraud and forgery on the Internet. See

http://www.theregister.co.uk/2004/10/29/operation_firewall/

Hackers on University Campuses

George Mason University: The names, photos, and Social Security information of 30,000 faculty, staff, and students were stolen by hackers. The security breach was discovered on January 3. See

http://news.zdnet.com/2100-1009_22-5519592.html

University of Texas: In November a federal grand jury meted out a four-count indictment to a former University of Texas student who hacked his way into the university system and stole 37,000 Social Security numbers and other personal information belonging to faculty, staff, and students. See **http://www.msnbc.msn.com/id/6408290/**

Purdue University: In late October officials confirmed that Purdue's computer system had been penetrated by unauthorized intruders and urged all faculty, staff, and students to change their passwords as a precautionary measure. See

http://www.securityfocus.com/news/9786

Phishing News

Phishing scams steal $500 million from U.S. consumers. This fall the Ponemon Institute (**http://www.ponemon.org/**) reported a dramatic increase in the volume and frequency of spoofing and phishing incidents online. Among the more popular scams are emails purporting to be from well known businesses such as eBay and CitiBank. These bogus notices try to trick users into revealing their account details and passwords for use in identity theft crimes. See

http://www.theregister.co.uk/2004/09/29/phishing_survey/

Tsunami Relief Scam Crackdown Begins

The FBI has arrested a Pennsylvania spammer charged with soliciting donations for a bogus relief fund via the Internet. This is the first arrest in a nationwide crackdown on dozens of criminals seeking to profit from tragic headlines. For details, see

http://www.knoxstudio.com/shns/story.cfm?pk=TSUNAMI-SCAM-01-14-05&cat=AN

Ireland Battles Rogue Autodialers

To combat a surge in rogue autodialing scams, Ireland has blocked direct dialup Internet connections to 13 countries. Most of the blocked countries are in the South Pacific. See **http://www.theregister.co.uk/2004/09/22/ireland_rogue_dialler_crackdown/**

US Software Pirate Jailed

A Virginia court sentenced 33-year-old Kishan Singh to 18 months in prison after he was convicted of selling thousands of pirated software programs via a pay-for-access website. See

http://www.theregister.co.uk/2005/01/10/software_pirate_jailed

Try Using Selection Modifier Keys

These handy keyboard shortcuts can save you time and grief

Patrick Chinn
Distributed Network Computing Consultant
pchinn@uoregon.edu

We are all familiar with how to select an item on our computer: point to the object and click the mouse button. It's a technique we use frequently to read email messages: when new messages arrive, we select the message we want to read by pointing at the message and clicking the mouse.

But what happens when you have ten, 20, or 315 items to open, move, or delete? Trashing dozens of items one at a time is a recipe for exhaustion!

The solution is to use selection modifier keys. By pressing specific keys on the keyboard, we can tell the computer to do something different when we make our selection. These keys are called selection modifier keys.

Deleting Contiguous Items

Returning to our email example, let's say my business manager accidentally sends me 25 copies of the same budget spreadsheet via email. Of course I could delete the 24 unwanted messages individually by selecting each message and clicking the delete button. (That adds up to 48 total clicks!) But if I use a modifier key, I can delete those 24 messages with only *three* clicks (assuming the duplicate messages arrived all at once).

How do I do this? The secret is to use the SHIFT key. To delete a contiguous (neighboring or adjoining) set of messages, click on the first message in the set, hold down the SHIFT key, and click on the last message in the set. All 24 messages are then selected. To finish the operation, click the delete button, deleting all 24 messages at once.

Deleting Noncontiguous Items

Sometimes I receive lots of unwanted email, and those messages are scattered throughout my inbox. I could select a message and click "delete" for each item, but there's a faster way. To select noncontiguous items, I can hold down the COMMAND key (Mac OS) or CTRL key (Windows) and click to select each item. Now that I have selected all the junk messages in my mailbox, I need to click the delete button only once.

These modifier keys are useful in any program, such as email and Microsoft Excel, that presents information in the form of a list or table. But modifier keys can also be useful when working with items that are presented as icons or pictures. For instance, to select a set of files within a folder, click and drag to select files within the rectangular area. If you need to add a few more files to that selection, don't forget the COMMAND (or CTRL) key; hold the key and click on each file to add it to your selection.

Most programs that present data in the form of a list will support selection modifier keys. Web pages are often an exception to this rule, most notably webmail interfaces. Yahoo, Gmail, and the UO's own webmail interfaces all require the user to click innumerable check boxes to delete email en masse.

The 'Select All' Shortcut

Both Mac OS and Windows offer another selection-related shortcut: *select all*. To select all in Mac OS, press COMMAND+A; in Windows press CTRL+A. *Select all* will then select every item in the list, window, or page, depending on what program you are using.

In this article, I have focused solely on keyboard shortcuts that are related to selecting files or items. These shortcuts represent only a fraction of available keyboard controls.

For a complete list of Mac OS X keyboard shortcuts, see
http://docs.info.apple.com/article.html?artnum=75459

For a list of Windows XP keyboard shortcuts, see
http://support.microsoft.com/default.aspx?scid=kb;en-us;Q301583

New UO Design Guidelines in the Works…

UO web developers given green light to use Verdana, Arial fonts

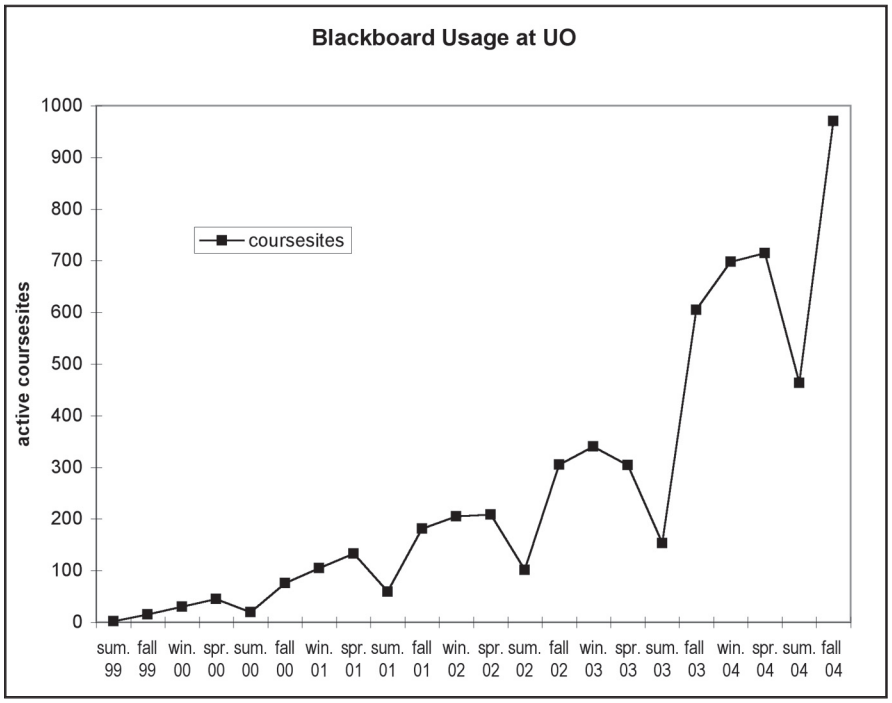
Creative Publishing (formerly University Publications) reports that it is permissible within the university's style standards to use Verdana and Arial fonts on UO web pages.

Creative Publishing is examining other online conventions and graphic practices with an eye toward creating a complete set of design guidelines for UO web pages. Please direct any comments or feedback along those lines to Guy Maynard, director of Creative Publishing, at *gmaynard@uoregon.edu*

UO Blackboard Use Grows: More Features Added

Ron Renchler
Director, Library Communications
UO Libraries
ronr@darkwing.uoregon.edu

Blackboard, the university's course management system, has seen steadily increasing use since its introduction in 1999. In fall 2004, Blackboard was used to manage more than 970 courses at the UO, and more than half of all student enrollments—about 53,000—were in a class where Blackboard was used. This fall, 18,000 students used Blackboard for at least one course. If the rapid growth in the use of Blackboard and the feedback received about its effectiveness are any indication, UO faculty and students have discovered that Blackboard is a very effective communications and management tool for their classes.



Blackboard use from summer 1999 through fall 2004.

For the UO Libraries, Blackboard has become "mission critical" in fulfilling some of the library's central goals: enriching the student learning experience and advancing access to resources for teaching and research. Blackboard training programs are now handled through the library's newly established Center for Educational Technologies (CET), where faculty can receive assistance with all aspects of Blackboard operations. CET is located in Room 19 on the ground floor of Knight Library. For more information, call **346-1942** from 9 A.M. to 6 P.M. Monday through Friday. Students can find out more about Blackboard by visiting the library Information Technology Centers (ITCs) or by calling **346-1935**.

Several upgrades to the Blackboard system have occurred in the past six months, and more are planned. Among the newest Blackboard features are:

• **Department sites.** Blackboard now allows academic units to set up a "coursesite" for departmental faculty. These sites have been useful in several academic departments as a place for communicating with faculty, particularly for sharing information about teaching. If a regular coursesite is the online extension of lectures, then a departmental coursesite might be an online extension of a faculty meeting. Typically, one faculty member in the department is designated as the "instructor" for the site, and all faculty and staff are automatically enrolled in the department's "course." Department coursesites are permanent; they aren't disabled from term to term as are coursesites for university classes.

• **Majors.** Similarly, "majors" coursesites can be set up for departments that offer an undergraduate major. These coursesites are handy for communicating with students whose major falls within a department. All students majoring in the field are automatically enrolled in the "course."

• **Gradebook upload to DuckWeb.** Faculty members can now upload their final grades from a Blackboard gradebook into a DuckWeb grade roster instead of having to enter them manually.

• **Blackboard "Application Pack I."** The "AP I" upgrade (installed this summer) includes a glossary tool that allows instructors to build a coursesite-wide list of specialized terms and definitions, improved support for mathematical notation in Blackboard content, and the ability for instructors to customize the list of courses they see on the *My UO* page (hiding old, no longer needed courses).

• **Blackboard "Application Pack II, Service Pack I."** Installed in November 2004, this upgrade includes many bug fixes and numerous added features, such as:

- continued on page 16

UO Blackboard, continued...

- **Improved support for the Firefox web browser**
- **Test and survey answer download:** Allows instructors to download detailed results of tests and surveys for statistical analysis or student performance tracking
- **Quick tool linking**: When instructors add material to a content page in the coursesite, they can now directly add a discussion board forum, a live chat, or any tool directly in any area of the course with a few clicks
- **ChalkBox support:** Allows the installation and management of ChalkBox titles, which are a new type of course cartridge accompanying specific textbooks that contains both content and interactive tools
- **SCORM and IMS players:** Allow the inclusion of SCORM 1.2, NLN, and IMS format learning objects within a Blackboard site, facilitating faculty collaboration with peers and use of best-quality content.

  To learn more about SCORM, see **http://www.academiccolab.org/projects/scorm.html**
- **Document Unpackager:** This new content type allows an instructor to upload a zip file containing folders and files to Blackboard, where it is unpackaged. Course content items are then created with the files attached. The directory structure within the zip file is translated into folders within Blackboard.
- **Advanced Group Management:** If you are an instructor who wants to use Blackboard groups to organize your course, check out the Advanced Group Management tool in the Control Panel. It makes management of groups and assignment of students to groups much easier.

• **Load Sharing.** Over winter break the Blackboard server architecture was substantially changed to better handle increased student usage. Instead of having a single Blackboard application server, several servers now share the load. This change should be invisible to users, but will result in better performance and reliability at peak usage times such as Dead Week.

For more information on any of these Blackboard features, contact JQ Johnson, Blackboard manager and director of the Center for Educational Technologies (**346-1746**, *jqj@darkwing.uoregon.edu*). To request set-up of a department or majors coursesite, email *courseinfo@blackboard.uoregon.edu* The Blackboard website is at **https://blackboard.uoregon.edu/**

Crackdowns on 419 Scammers Continue

Australia: An Australian judge sentenced the self-proclaimed ringleader of a major 419 scam operating out of Sydney to more than five years for scamming millions of dollars from victims worldwide. For details, see **http://www.wired.com/news/business/0,1367,65631,00.html** **http://www.theregister.co.uk/2004/11/08/aussie_419er_jailed/**

In another 419-related case in Melbourne, a 58-year-old financial planner faces the possibility of a stiff prison sentence for defrauding his clients of over $1 million. See **http://www.theregister.co.uk/2004/10/19/aussie_419_victim/**

The Netherlands: In an effort to quickly expel 419 scammers operating within its borders, the Netherlands is opting for deportation over prosecution as the method of choice. In a recent raid in October, Amsterdam police arrested 21 illegal immigrants from Nigeria and Sierra Leone who were running a 419 operation. See **http://www.theregister.co.uk/2004/10/08/419_scammers_deported/**

California: Two Pleasant Hill, California, residents have been arrested on suspicion of having swindled relatives and friends in a variation of the 419 scam. For details, see **http://www.contracostatimes.com/mld/cctimes/news/local/crime_courts/10520544.htm?1**

Federal Judge Refuses Guilty Plea in AOL Spam Case

Stating that it wasn't clear that the new federal anti-spam ("CAN-SPAM") law had been violated, a federal judge rejected the guilty plea of a former AOL software engineer accused of stealing millions of AOL clients' email addresses to sell to spammers. The sticking point for the judge was whether or not the "deception" requirement of the law had been met in this case. See **http://www.mercurynews.com/mld/mercurynews/business/technology/10468604.htm**

Ohio Anti-Spam Bill Passes

Ohio legislators recently passed a bill imposing criminal penalties on spammers who practice fraud and deception to entrap unsuspecting consumers. Modeled after the federal CAN-SPAM Act (**http://www.spamlaws.com/federal/108s877.html**) but with tougher penalties, the bill is expected to be signed into law by Governor Bob Taft. See **http://news.zdnet.com/2100-9588_22-5472453.html**

Sibling Spammers Convicted in Virginia

In November, a brother and sister were convicted under a Virginia anti-spam law for bombarding AOL subscribers with hundreds of thousands of junk emails. The first felony prosecution of Internet spam distributors by Virginia prosecutors, this conviction was preceded by a successful federal prosecution against Howard Carmack, the "Buffalo Spammer," who was sentenced to seven years in prison last May. See **http://www.theregister.co.uk/2004/11/04/sibling_spammers_convicted/**

Iowa ISP Wins $1 Billion in Anti-Spam Suit

CIS Internet Services, a small ISP serving Iowans in and around the town of Clinton, was awarded damages of $1 billion in a "John Doe" lawsuit against three spammers who jammed the network with as many as 10 million mass mailings a day. See **http://www.theregister.co.uk/2004/12/20/isp_wins_1bn_damages_from_spammers/**

Blogs Attacked by Comment Spam

Spammers are using automated scripts to bombard weblogs with comment spam, also known as link spam. As a result, web servers—especially those in shared hosting environments—have been seriously slowed, and some providers have disabled comments on the popular Movable Type (MT) blogging tool while MT publisher Six Apart works on software fixes. See **http://news.netcraft.com/archives/2004/12/17/hosts_disable_movable_type_as_comment_spam_slows_servers.html**

Major UK Spammer Racks Up More Criminal Charges

Peter Francis Clifford Macrae, who made the SpamHaus register list as one of the top spammers worldwide, has added blackmail, fraud, and criminal damage to his rap sheet of online scams. See **http://www.theregister.co.uk/2004/12/20/more_charges_for_uk_spammer/**

Microsoft Files Suit Against Tucson Spammer

On December 21, Microsoft Corporation filed its 88th lawsuit since beginning its agressive antispam war last year ("Microsoft Takes Stands Against Spam…" **http://www.washingtonpost.com/wp-dyn/articles/A41592-2004Sep22.html**). This latest suit claims a civil judgment of $7.4 million against a Tucson man who tried to promote his Internet business with a barrage of unsolicited emails). See **http://www.dailystar.com/dailystar/dailystar/55002.php**

Security Alerts…

— Microsoft Windows —

Test Confirms Unprotected PCs Can Be Hijacked almost Instantly

As soon as they connect to the Internet, unprotected PCs are toast. They can be hijacked immediately and grouped with other "zombie" PCs to perpetrate cybercrimes such as spamming, denial-of-service attacks, or identity theft.

This is the conclusion of independent security consultants Kevin Mitnick and Ryan Russell after two weeks of monitoring six "honeypot" computers set up to lure attackers. Operating systems tested included four varieties of Windows, Mac OSX, and Linspire.

The results of their study underscore the importance of using a firewall and keeping security patches up-to-date. See "Unprotected PCs can be hijacked in minutes" at **http://www.usatoday.com/money/industries/technology/2004-11-29-honeypot_x.htm**

Internet Explorer Still Extremely Vulnerable on Several Fronts

1. "Huge" Flaw in IE Opens the Door to Sophisticated Phishing Exploits:

In mid-December, a dangerous flaw was uncovered in Internet Explorer (IE) that makes even the latest and most secure version of the browser (XP S2) vulnerable to forging both the URL and SSL signature padlock at the bottom of the browser screen. This allows scammers to create very realistic malicious websites that pose as legitimate sites (a practice known as "spoofing") in order to trick users into divulging sensitive personal information that can be used in ID theft. For details, see **http://news.zdnet.co.uk/internet/security/0,39020375,39181466,00.htm**

2. Only Partial Fix for Latest IE 6.0 Bugs:

Extremely critical flaws in IE 6.0 reported by the Danish security watchdog Secunia remain only partially patched. Some of these vulnerabilities bypass the security in XP Service Pack 2. Details and recommended solutions are available at **http://secunia.com/advisories/12889/**

3. Cross-Site Scripting Flaw Found in IE:

The Greyhats Security Group recently uncovered a flaw in IE that could allow attackers to steal cookie-based authentication credentials. See **http://www.internetnews.com/security/article.php/3450131**

MS Issues Fix for XP S2 Firewall

Five months after announcing a critical hole in its built-in XP S2 firewall, Microsoft issued a fix. The patch is was released as part of Windows Update for September.See **http://support.microsoft.com/kb/886185** and **http://www.securityfocus.com/news/10152**

MS-04-028: Critical Jpeg Exploit

This critical vulnerability could allow attackers to run malicious code on a victim's machine when an embedded image file is opened in an email or downloaded from the web. The best protection is to be ***absolutely sure*** your Microsoft systems are fully patched with respect to Microsoft Security Bulletin MS04-028 (**http://www.microsoft.com/technet/security/bulletin/MS04-028.mspx**) It's also advisable to run the free SANS GDI system checker available at **http://isc.sans.org/gdiscan.php**

ASP.NET Vulnerability

Researchers recently discovered a simple coding bug in ASP.NET that could have caused serious problems in verifying authentication. For details, see Mark Burnett's December 20 article, "Security Holes that Run Deep" at **http://www.securityfocus.com/columnists/285**

Windows Virus Threat: W32/Bofra-A

The W32/Bofra-A worm, which spreads via email, web downloads, and chat rooms, has been circulating on campus recently. The infected vector typically contains a link to a site running on port 1639 or 1650, often with subject lines reading "Hi!", "Hey! (or HEY!)", "Confirmation", or [blank subject] and message texts such as "My name is Jane, I am from Miami, FL" or "PayPal has successfully charged $175 to your credit card." For more details, see **http://www.sophos.com/virusinfo/analyses/w32bofraa.html**

Phony Music, Video Files Harbor Adware, Pop-Ups

Downloading seemingly innocuous Windows Media files over peer-to-peer (P2P) networks such as Kazaa can invite a plague of pop-ups and adware, thanks to a loophole in licensing terms for Windows Media. Some of these files are merely annoying and can slow computer performace, but some are malicious and can allow attackers to hijack your PC. To learn more, go to **http://www.pcworld.com/news/article/0,aid,119016,00.asp**

Finding Microsoft Security Downloads

To search for patches for Microsoft products, go to the Microsoft Download page at **http://www.microsoft.com/downloads/search.aspx?displaylang=en&categoryid=7**

— Mac OS X —

Install Latest OS X Security Update

On December 2, Apple released a security update for OS X that fixes multiple vulnerabilities. These flaws are rated "highly critical" by security researchers at Secunia. For more details, see Secunia Advisory SA13362 (**http://secunia.com/advisories/13362/**) and *The Register*'s article, "Security bugs take a bite out of Apple" (**http://www.theregister.co.uk/2004/12/07/apple_vuln/**) To get the update, go to Apple's Service and Support Site at **http://www.apple.com/support/**

Scheduling Mac OS X software updates:

It's a good idea to take advantage of Mac OS X's automatic Software Update feature, which allows you to schedule regular checks for software updates. To activate this feature, go to the Apple menu and select "System Preferences." Then select "Software Update" click on "Update Software." Check the box labeled "Check for updates" and select the frequency ("Daily," "Weekly," or "Monthly") from the drop-down menu.

— Other Alerts —

Highly Critical Java Plugin Flaw Affects Windows, Linux

This vulnerability, which was publicized in late November, could allow execution of malicious code when a victim simply visits a booby-trapped web page. Users are advised to upgrade to the latest version of the Java plugin, which is available at **http://java.com/en/download/** If you don't know what version (if any) of Java is installed on your system, go to **http://www.java.com/en/download/help/testvm.jsp** If Java is already installed, you'll see a little Java "dancing Duke" character. If you don't have Java installed on your system, you need do nothing for this vulnerability.

'Patched' Versions of WinAmp (5.05 and 5.06) Fail to Plug Security Hole

Exploit code for America Online's WinAmp media player is circulating on the Internet and users are still vulnerable to attack, despite the vendor's assurances that its 5.05 and 5.06 updates fixed the problem. In the absence of a viable patch, users are advised to disassociate the playlist filename extensions **.cda** and **.m3u** from WinAmp. For details on this extremely critical vulnerability, see Secunia Advisory SA 13269 at **http://secunia.com/advisories/13269** and *PC World's* article "WinAmp Security Hole Deepens" at **http://www.pcworld.idg.com.au/index.php/id;1625490509;fp;2;fpid;1**

Malicious Program Masquerades as Lycos Europe Screensaver

A well-known Lycos Europe screensaver that was originally designed as an anti-spam tool has been appropriated by a malicious Trojan program. The Trojan is embedded in emails that purport to be from Lycos Europe, offering the screensaver for download. The Trojan has an embedded keystroke logger which can be used to steal personal information used in identity theft schemes. For details, see

http://www.ecommercetimes.com/story/security/trojan-lycos-anti-spam-38810.html

and

http://news.com.com/Trojan+poses+as+Lycos+Europe+screensaver/2100-7349_3-5481674.html

— Bogus Email Notices —

Beware Bogus 'RedHat Security' Notices

If you receive an email notice from "RedHat Security Team" urging you to download "patches" from a specified website, don't take the bait. These are not genuine RedHat websites and the patches are bogus. In actual fact, the patches are designed to compromise the security of your system, not improve it. Never click on or visit any website "spamvertised" by email.

Phony 'Antispam Corporation' Notices

We've had a number of inquiries from campus users regarding the "0fficial N0tification" they've received from "Antispam Corporation" that includes a link to various websites. This is yet another spammer, and you should *not* treat the message as credible. Don't click on the link or provide any information about your account.

Free Windows Beta Anti-Spyware Available

Check it out:

http://www.microsoft.com/athome/security/spyware/software/default.mspx

Spotlight on Browser Security

Internet Explorer leads list of vulnerable web browsers with extremely critical flaw

If you're a Windows user who routinely browses the Internet with Microsoft Internet Explorer (IE), you should be aware that the Danish security research firm Secunia is now warning that a months' old, still unpatched, IE vulnerability is even more dangerous than before.

Even if you have installed Microsoft's XP Service Pack 2, you are still vulnerable, and it appears that the patches released by Microsoft on January 11 do not include a remedy for IE.

Vulnerability test: Secunia has created a test for IE users to check their vulnerability. To take the test, go to **http://secunia.com/internet_explorer_command_execution_vulnerability_test/**

For more details on Secunia's report, see **http://www.informationweek.com/story/showArticle.jhtml?articleID=57700320**

Also see "Internet Explorer Still Vulnerable on Several Fronts" under *Security Alerts* on page 18.

All Major Browsers Affected by Pop-up Flaw that Facilitates Phishing Ploys

A "window injection" vulnerability common to almost all major browsers leaves the door open for phishing scammers to masquerade as legitimate businesses or institutions and glean sensitive ID information from visitors to pop-up sites. What makes this exploit particularly treacherous is that a perfectly legitimate pop-up window that's opened via a trusted website can later be hijacked by a malicious website, easily fooling the unwary user. For complete details, see **http://news.zdnet.com/2100-1009_22-5484315.html**

Check Your Vulnerability to Pop-up Phishing
Secunia has devised a simple test that can tell you if you're vulnerable to pop-up window phishing. To take the test, go to **http://secunia.com/multiple_browsers_window_injection _vulnerability_test/**

"Less Critical" Mozilla, Firefox Vulnerability Invites Phishing Scams

Hackers can easily "spoof," or mimic, the source URL address displayed in Mozilla's Download Dialog box. This flaw has been confirmed in Mozilla 1.7.3 for Linux, Mozilla 1.7.5 for Windows, and Mozilla Firefox 1.0, and may also be present in other versions.

No solution is currently available, but the vulnerability is slated to be fixed in future product updates. In the meantime, users are advised not to follow download links from untrusted websites. See **http://www.vnunet.com/news/1160352**

Critical New Flaw Discovered in Mozilla

In January, iSEC security researchers found a flaw in the way Mozilla handles Network News Transfer Protocol (NNTP). All versions prior to 1.7.5 are vulnerable to this flaw, which could allow an attacker to execute arbitrary code on a victim's machine.

To remedy this problem, upgrade to the latest version of Mozilla, which is available for downloading at **http://www.mozilla.org/products/mozilla1.x/**

For more details, see "Critical flaw plagues Mozilla," at **http://www.vnunet.com/news/1160400**

Update to Firefox 1.0 without Delay

Late last fall, some potentially nasty security holes were discovered in Firefox versions earlier than 1.0. The problems are assumed to affect all versions up to 0.9.

If you haven't yet upgraded to 1.0, you need to get up-to-date as soon as possible. You can download the update from the UO's public domain software site, *public*, by going to **ftp://public.uoregon.edu/software/Web/Firefox/Firefox_Setup_1.0.exe**
Or, to be guaranteed of the very latest upgrades, visit the Mozilla site at **http://mozilla.org/**

Automatic Updates: Unfortunately, the built-in "software update" in the 0.93 version of Firefox included on Duckware does not work. If you have already upgraded to version 1.0PR1 or newer, you can mouse over the arrow in the upper right of your browser (next to the Google search engine entry field) to check for new updates. Clicking on this icon will install any new update that's available. Or, if it's convenient, you may prefer to pick up the latest version of the Windows Security CD from the Help Desk in 151 McKenzie; this CD automatically checks your firefox browser version and helps you update it if necessary.

What's New in SAS Version 9?

The latest version of SAS includes some welcome additions…

Robin High
Statistical Programmer and Consultant
robinh@uoregon.edu

As you may know, thanks to our site license agreement, all University of Oregon students, faculty, and staff may install the statistical software package SAS on their personal computers at no cost. In recent years the PC version of SAS has become much more versatile, powerful, and convenient to run both small and large data analysis projects. The most recent and most advanced version of SAS, 9.1.3, is now available from the Computing Center documents room (175 McKenzie).

Most new SAS users should install Version 9. If you already have version 8.2 and decide to upgrade, you'll need to go through a completely new installation process, as described at **http://ssil.uoregon.edu/sas/** This site also contains registration and license renewal information.

Documentation

Online documentation for version 8.2 will continue to be available to UOnet users at **http://sas.uoregon.edu/sashtml/main.htm** Documentation for Version 9.1.3 is available in two formats from the SAS support website. The first website (**http://support.sas.com/onlinedoc/913/docMainpage.jsp**) is recommended for slower connection speeds. It allows you to search the table of contents for specific topics and select a link for further information.

A second website (requiring a high-speed connection and Adobe Acrobat Reader 6.0 or later) provides links to the contents of the SAS manuals in PDF format (**http://support.sas.com/documentation/onlinedoc/91pdf/index_913.html)** Although it's possible to download these manuals for viewing or printing, please note that the *entire* contents of each manual are placed into *one* PDF document. Some of these manuals are thousands of pages long (the STAT manual alone is over 5000 pages!) so print only the pages you need. Another alternative is to buy individual manuals by clicking the "purchase book" link next to each title on the site.

What's New in SAS 9?

You'll find a complete description of what's new in Version 9 at **http://support.sas.com/documentation/onlinedoc/91pdf/sasdoc_913/whatnew_8350.pdf** This document is 270 pages long, so once again, be judicious when printing.

Much of what you may already know about SAS has not changed. Since SAS is backward-compatible for the most part, the great majority of programs written for Version 8.2 (and earlier) will continue to work in 9.1.3 with few or no modifications. However, SAS has added many new features in its latest version, including functions for the DATA step, options for statistical programs, and specialized data analysis procedures not previously available. This article summarizes just a few of the most helpful tools SAS has added to its arsenal.

New Functions

New SAS functions include mathematical and statistical applications. In particular, these new functions enable you to work more effectively with date and character-string data:

```
DATA places;
LENGTH city $10 state $12 ;
FORMAT visit_date mmddyy10. ;
INPUT visit_date anydtdte10. city state;
location=CATX(", ",city,state); concatenate
DATALINES;
12/10/2004 Ashland Oregon
16JUL2004 Bertrand Nebraska
;

PROC PRINT DATA=places NOobs; RUN;
  city     state      visit_date    location
Ashland    Oregon      12/10/2004   Ashland, Oregon
Bertrand   Nebraska    07/16/2004   Bertrand, Nebraska
```

New functions for descriptive statistics allow you to identify the smallest, largest, or the range of data from a specified list of variables contained in the same row (observation). Like previously available functions which compute the mean or the number of missing values for a list of variables, the new MEDIAN function allows you to compute the median of a set of non-missing variables from each observation. Compare the behavior of the ORDINAL function with the new SMALLEST function in this example to see how they work with missing data.

```
DATA example;
INPUT a b c d e ;
MISSING b z;
min_r1 = ORDINAL(1,a,b,c,d,e);
min_row = SMALLEST(1,a,b,c,d,e);
mean_row = MEAN(a,b,c,d,e);
median_row = MEDIAN(a,b,c,d,e);
max_row = LARGEST(1,a,b,c,d,e);
nmiss_row = NMISS(a,b,c,d,e);
DATALINES;
3 2 z 4 5
13 12 34 34 35
9 . 5 3 1
2 5 99 z b
;

PROC PRINT DATA=example NOobs;
VAR min_r1 min_row median_row mean_row max_row
nmiss_row ;
RUN;
```

min_r1	min_row	mean_row	median_row	max_row	nmiss_row
Z	2	3.5	3.5000	5	1
12	12	34.0	25.6000	35	0
.	1	4.0	4.5000	9	1
B	2	5.0	35.3333	99	2

Study tip: Ron Cody's book *SAS Functions by Example*, which is available from the catalog at **http://www.sas.com/apps/pubscat/welcome.jsp**, is a comprehensive resource for descriptions and applications of SAS functions.

Longer Format Names

SAS formats allow you to enter descriptive labels for data stored as numbers or short alphabetic codes. In version 9, the maximum length for character format names has been extended to 31, and the maximum length for format names for numerical data is 32. This enables you to provide format names that are more descriptive.

```
PROC FORMAT;
VALUE  $gender_respondent  "F"="Female"
"M"="Male";
RUN;
PROC PRINT DATA=sashelp.class;
VAR name sex age height weight;
FORMAT sex $gender_respondent. ;
RUN;
```

PROC FORMAT now allows you to define multilabel formats for the same value. These formats may be written and applied with the procedures MEANS, SUMMARY, and TABULATE. They allow you to compute summary statistics for individual values or multiple ranges. You may read about this new feature at **http://support.sas.com/onlinedoc/912/getDoc/proc.hlp/a002473472.htm**

ODS for Statistical Graphics

The Output Delivery System (ODS), which first appeared in Version 8, places the results printed to the output file or to an output window directly into SAS datasets. Version 9 includes a new experimental extension of the ODS which automatically produces a variety of graphical outputs. The ODS for Statistical Graphics provides common displays, including scatter plots, histograms, box-and-whisker plots, and contour plots. Familiarity with ODS for tables is assumed since many ODS features, such as destination statements, apply to graphics. Among the approximately 30 procedures that support statistical graphics in Version 9.1.3 are CORR, ANOVA, GENMOD, GLM, LOGISTIC, MIXED, REG, ROBUSTREG, ARIMA, and AUTOREG.

You do not need to know how to apply the complex SAS/GRAPH commands since graphs from the procedures that support ODS graphics are produced separately. However, note that all data placed in any of these graphs can be retrieved with ODS and analyzed with SAS/GRAPH, giving you more control over their layout and format.

The ODS graphics capability remains 'experimental' since this software is not yet officially part of the SAS System. Although these experimental procedures have been extensively tested, they have not received the level of testing that SAS Institute requires for its software to be deemed 'production' level. You'll find a brief introduction to ODS and ODS graphics at **http://darkwing.uoregon.edu/~robinh/110_ods.txt** More information is available from SAS's support page at **http://support.sas.com/rnd/base/topics/statgraph/**

New Statistical Procedures

The following statistical procedures are new in SAS 9:

Robust Regression: The new ROBUSTREG procedure computes stable regression results in the presence of outliers by limiting their influence. Two of the most commonly employed methods found here are Huber's M estimation and LTS estimation.

Power and Sample Size Analysis: PROC POWER and PROC GLMPOWER procedures perform prospective power analyses and sample size computations for a variety of statistical models with the following goals:

- determine the sample size required to detect an effect size with specified power
- characterize the power of a study to detect a desired effect size for a given number of subjects
- assess the sensitivity of power or sample size calculations to other factors

Another new feature is the Power and Sample Size application, which brings power calculations into a windows interface. It also lists the SAS statements you can run with PROC POWER or GLMPOWER, allowing you to produce the same or similar analyses at a future time. These calculations can be saved to a dataset with the ODS, which can be graphed with the SAS GRAPH module. (Note that although it is part of SAS/STAT software, the Power and Sample Size application needs to be installed separately from the Mid Tier CD in the set of installation disks.)

New SURVEY Analysis Procedures

If your data are sampled from a population with a known finite size or collected with a sampling design, as is often the case with surveys, statistical procedures such as MEANS, FREQ, and REG will not calculate the estimates and their variances properly, especially if the sample data include a substantial proportion of subjects from the entire population. Analyses of survey data which do not consider the sample design and the population size may lead to incorrect statistical inferences.

SAS 9.1 introduces several new procedures for the analysis of survey data. Your data analyses will likely be improved with PROC SURVEYMEANS instead of PROC MEANS, PROC SURVEYREG instead of PROC REG, or PROC SURVEYLOGISTIC instead of PROC LOGISTIC.

To learn more about survey sampling procedures, see Chapter 10 of the SAS/STAT manual.

« sites worth seeing »

1. **Google scholar…** This new Google search tool enables specific searches for scholarly literature, including theses, books, abstracts, peer-reviewed papers, and technical reports: **http://scholar.google.com/**
2. **Internet Governance issues…**
   a. The latest proposals of the International Telecommunications Union (ITU) regarding Internet Governance, including management of Internet Protocol (IP) addresses: **http://www.itu.int/ITU-T/tsb-director/itut-wsis/files/zhao-netgov01.doc**
   b. The Number Resource Organization's response to ITU comments on managing IP addresses: **http://www.nro.net/documents/nro17.html**
3. **"WPA Cracking Proof of Concept Available"…** A new WPA proof-of-concept tool created by the authors of tinyPEAP demonstrates how Wi-Fi users who use short or dictionary-based passphrases are vulnerable to hacking. See **http://wifinetnews.com/archives/004428.html**
4. **"California considers open-source shift"…** New IT purchases by the state of California may shift to open-source software if a proposal from the California Performance Review Commission is adopted: **http://zdnet.com.com/2100-1104-5327581.html**
5. **Enabling VPN pass-through…** An instruction set from Actiontec for advanced network administrators: **http://www.qwest.com/internet/downloads/Actiontec_1520_VPN_Pass_through__IS_.pdf**
6. **UOnet modems usage monitor…** If you want to plan your dialin times to avoid heavy network traffic, you can track UOnet modem usage at: **http://netstat.uoregon.edu/netviewer/uo/UOnetModems.html**
7. **"How to Improve Your Modem Connectivity"…** Dan Albrich's article in the Summer 2004 *Computing News* offers some valuable tips for dialin users: **http://cc.uoregon.edu/cnews/summer2004/modemconnect.htm**
8. ***PHP iCalendar…*** If you need web-based, read-only access to Mac OS X's iCal-based calendars, you might want to investigate *PHP iCalendar*, the open-source PHP project that automatically parses iCal calendar files and creates a web front end. It offers views by the day, week, month or year, the ability to view one or more calendars at once, and easy calendar date navigation. It also offers printer-friendly views and RSS newsfeeds: **http://sourceforge.net/projects/phpicalendar/**
9. **Reviews of PDA phones…**
   Audiovox PPC-6600/PPC-6601/XV 6600 (HTC Harrier): **http://www.phonescoop.com/phones/phone.php?p=570**
   Verizon Wireless XV6600: **http://www.infosyncworld.com/news/n/5656.html**
   HTC Blue Angel: **http://www.theregister.co.uk/2004/11/18/review_htc_blue_angel/**
10. **CNet laptop reviews…** In addition to product reviews, CNet's site includes a notebook buying guide, information on notebook accessories, and a notebook users' forum: **http://reviews.cnet.com/Notebooks/2001-3121_7-0.html?tag=ont.note**
11. **"About Openfiler"…**Learn about this network storage management utility: **http://www.openfiler.org/about/**
12. **Directory Helpers (Freeware)…** Michael Rebar's handy tools for querying the UO or Qwest directories and exporting the information into contact management software: **http://darkwing.uoregon.edu/~mrebar/**
13. **Emergency first aid for your Windows PC…** Tips for fixing newer systems: **http://www.tomshardware.com/howto/20050112/index.html**

Think Spyware is Harmless? Think Again…

According to an article published on December 1 in the *VNU Network VNU Business Publications* (**http://www.vnunet.com/news/1159778**), two thirds of all PCs are infected with spyware.

This is the conclusion of information technology analyst firm International Data Corporation (IDC), whose report, "Worldwide Spyware Forecast and Analysis 2004-2008" is available at **http://www.idc.com/getdoc/jsp?containerId=32229**

Although not all spyware is malicious, it can have the ability to defeat firewall security, and at its worst it can track keystrokes, scan hard drives, and change system and registry settings.

Spyware is often bundled with legitimate programs, a fact about which even some relatively savvy users are dangerously blasé. See "Spyware on My Machine? So What?" at **http://www.wired.com/news/technology/0,1282,65906m00.html** and "Terminating Spyware with Extreme Prejudice" at **http://www.nytimes.com/2004/12/30/technology/circuits/30hard.html?8hpib**

COMPUTING CENTER GUIDE

UO Website
http://www.uoregon.edu/

Computing Center Website
http://cc.uoregon.edu/

Microcomputer Services
http://micro.uoregon.edu/

(151 McKenzie Hall)

- microcomputer technical support
- help with computing accounts, passwords
- scanning, CD burning, digital video
- help with damaged disks, files
- system software help
- Internet connections, file transfers
- public domain software, virus protection
- software repair (carry-in only, $80/hour, 1/2 hour minimum)

346-4412
microhelp@lists.uoregon.edu

Documents Room Library
http://darkwing.uoregon.edu/~docsrm/

(175 McKenzie Hall)
346-4406

Modem Number
Dialin modem number for UOnet, the campus network: **225-2200**

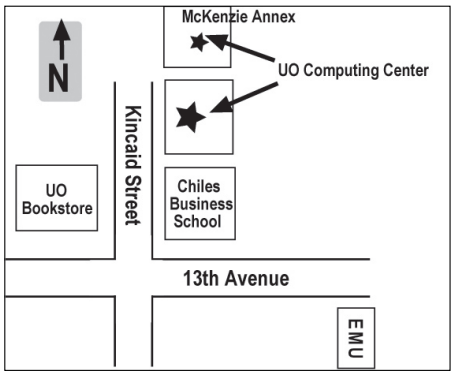
Large Systems Consulting
http://cc.uoregon.edu/unixvmsconsulting.html

(225-239 Computing Center)

- VMS, Unix
 (Gladstone, Darkwing, Oregon)
- email, multimedia delivery
- scientific and cgi programming
- web page development

346-1758
consult@darkwing.uoregon.edu
consult@gladstone.uoregon.edu

Statistics Consulting
Robin High
219 Computing Center
346-1718
robinh@uoregon.edu



Electronics Shop (151 McKenzie Hall)
http://cc.uoregon.edu/e_shop.html

Computer hardware repair, installation, and upgrades.
346-3548
hardwarehelp@oregon.uoregon.edu

Network Services
http://ns.uoregon.edu/

Provides central data communication and networking services to the UO community.
346-4395
nethelp@ns.uoregon.edu

Administrative Services
http://ccadmin.uoregon.edu/

Provides programming support for campus administrative computing, including BANNER, A/R, FIS, HRIS, and SIS. Call **346-1725**.

Computing Center Hours
Mon - Fri 7:30 A.M. - 5:00 P.M.

McKenzie Building Hours

Mon - Thu	7:30 A.M. - 11:30 P.M.
Friday	7:30 A.M. - 7:30 P.M.
Saturday	9 A.M. - 9:30 P.M.
Sunday	9 A.M. - 9:30 P.M.

- Note: These are *building* access hours; hours for individual facilities may vary.

UNIVERSITY OF OREGON
UO COMPUTING CENTER
1212 University of Oregon Eugene, OR 97403-1212