New User Information

Structural Biology IT

Welcome!

This guide is intended to provide you with enough information to quickly bring you up to speed on the networking and computer environment here in the Structural Biology group.

We are here to help you; please let us know if we can assist you in any way. Our contact information and areas of responsibility are listed below.

Structural Biology IT
http://structure.bio.purdue.edu/support

<table>
<thead>
<tr>
<th>Name</th>
<th>Contact Information</th>
</tr>
</thead>
</table>
| Pia Mikeal | UNIX workstations, Web development  
Hockmeyer 117, 496-6781, pmikeal@purdue.edu |
| Steve Wilson | UNIX servers, networks, SBIT management  
Hockmeyer 115, 496-1946, stevew@purdue.edu |

Biological Sciences IT
http://www.biology.purdue.edu/resources/computer_services.htm

<table>
<thead>
<tr>
<th>Name</th>
<th>Contact Information</th>
</tr>
</thead>
</table>
| Bio-IT Services | Windows and MAC PCs, departmental servers  
Lilly B-137 |
| Bruce Fuller | Network and workstation hardware  
Lilly B-137, 494-8175, bfuller@purdue.edu |

Printing
http://structure.bio.purdue.edu/support/docs/printers

We have several shared printers in Hockmeyer available for your use. The following table lists the names of the shared printers and their characteristics:

<table>
<thead>
<tr>
<th>Printer Name</th>
<th>Location</th>
<th>Model</th>
<th>Duplexer?</th>
</tr>
</thead>
<tbody>
<tr>
<td>hock-hp4600-color</td>
<td>218</td>
<td>HP Color LaserJet 4600dtn</td>
<td>yes</td>
</tr>
<tr>
<td>hock-hp8150-1</td>
<td>118</td>
<td>HP LaserJet 8150dtn</td>
<td>yes</td>
</tr>
<tr>
<td>hock-hp8150-2</td>
<td>218</td>
<td>HP LaserJet 8150dtn</td>
<td>yes</td>
</tr>
<tr>
<td>hock-hp8150-3</td>
<td>318</td>
<td>HP LaserJet 8150dtn</td>
<td>yes</td>
</tr>
</tbody>
</table>

The URL to use when adding one of these printers to a Windows computer is:
http://printers.bio.purdue.edu:631/printers/

where printer_name is replaced with the name of one of the printers from the table above.

Backups and Data Recovery

The UNIX workstations are backed up each evening to a disk-based backup server. Backups are kept for 30 days. If you delete a file or directory by accident, we can restore it for you usually within a few minutes to an hour, depending upon the amount of data that needs to be recovered.

Please note that there are some areas that are not backed up by our backup server. These are called “scratch” areas and will be clearly labeled as scratch. If the scratch area is named after the lab's PI (e.g., /bio/rossmann-scratch2) then it is backed up locally, either on the same workstation or on another workstation in the same lab. If the scratch area is named after the
workstation (e.g., /bio/corgi2-­scratch) then it is not backed up. All other areas (i.e., non-­scratch) are backed up to the central backup server.

**Software**

http://structure.bio.purdue.edu/support/software

We strive to maintain current versions of both general-­purpose and scientific applications on our workstations. Many of the applications may be found under the directory /apps while other software may be located in /usr/bin, /usr/local/bin or other directories. Some labs have a special directory containing software that is installed and maintained by the lab. These are found in a directory under /usr/local. For example, the Rossmann lab has a directory named /usr/local/rossmann where their applications are located.

Although they may be free for academic use, many specialized applications require that they be cited in any published work that made use of the application as part of the paper’s research.

If you need a particular software package or a specific version of an application installed, please contact Pia Mikeal and she’ll do what he can to get it installed for you.

**Shared Network Storage**

_NFS_

All our UNIX workstations are interconnected at the filesystem level through NFS (Network File System). This means that you should be able to see the data areas on other workstations from your own as if they were mounted locally. In fact, your home directory may not even be located on the same computer that you login on. When you attempt to access a remote filesystem, your workstation will automatically mount it for you. These remote mount points are located under the directory /bio and include the computer name as well as the partition number (if it’s not the first partition). For example, if you want to list the contents of the second data partition on a computer named vermont you would type the following at a shell command prompt:

```
ls /bio/vermont2
```

Please note, though, that listing the contents of /bio will only show currently mounted remote filesystems, not all available remote filesystems.

**Miscellany**

- The UNIX computers should be left running, even when not in use. Much of our automated administration (including backups) takes place at night and needs the computers to be accessible over the network.
- It should be a rare event that a workstation require rebooting. If one of the SBIT staff is available, please check with them to see if they can correct the situation without rebooting. If you must reboot the computer, do so by executing an appropriate reboot command. _Only as a last resort (e.g., the computer is completely “frozen”) should you reboot the computer using the power or reset buttons since this could cause filesystem corruption._

**Security**

Most people don’t give much thought to computer security. But unfortunately, the days of an open and trusted computing environment are long past. At every level we must be vigilant to protect our computer and network security. You, as a user, are an important link in the protection of our IT resources and it is your responsibility to follow the University’s IT security policies (see http://www.purdue.edu/policies/pages/information_technology/info_tech.html).

Do not leave your computer for any period of time without first logging out or locking the desktop with a password-­protected screensaver. Also, be sure to lock the door to your work area when you leave if no one else is present. Computers
and other equipment have been stolen from unlocked areas. And, if given physical access to a computer, a hacker can easily break into it.

You may access our workstations from outside of the Biology networks through the SSH suite of programs (i.e., ssh, sftp, and scp). These programs encrypt your password and all other data before sending it across the Internet to the remote computer. You must use an SSH client that supports SSH protocol 2 or higher and you need to change the port from its default (22) to 2200.

The Biology networks are protected by firewalls from other Purdue networks and the public Internet. Virtually all outbound traffic is unrestricted but uninitiated inbound traffic is blocked at the firewall except for specifically permitted traffic (e.g., SSH access).

Peer-to-peer (P2P) file-sharing networks are usually large security risks, highly consumptive of network bandwidth and frequently used to illegally share copyrighted material. Some common examples of P2P networks include KaZaA, BitTorrent, Gnutella and eDonkey. For these reasons, we don't permit participation in a P2P network while connected to our Biology networks.

Questions???

Be sure to let us know if you have any questions. You may also want to check the information available from the Structure Group web site: http://structure.bio.purdue.edu. And if you have any suggestions for how we can improve the content of this document, we would like to hear them.

Thanks!