

THE A3C CONNECTION

Academic Computing and Communications Center

Summer 2001



The ACCC Network Services Kit

Tech Tips



CONTENTS

- 1 The ACCC Network Services Kit
- 2 List of NSKit Applications
- 3 The Requirements for Dialing In
- 4 Accounts, Netids, Password Changes
- 5 The Basic Steps
- 7 Internet Access and the ACCC
- 8 Getting Help
- 10 Living with a Hostile Internet

The Network Services Kit (NSKit) is a collection of software that allows you to access email, participate in newsgroups, log in to UNIX machines at UIC and elsewhere, and to browse the World Wide Web. In short, it lets you make use of Internet resources, whether from home or office.

The price is right too — free if you download it from the UIC FTP site or \$15 if you buy the CD and printed documentation from a campus bookstore.

There's a new NSKit available now, Version 5.0. In addition to having the latest versions of the most important Internet software, it has two nifty new features and a potentially computer-saving one.

Web-based NSKit Upgrades

A neat feature of the new NSKit is that you will be able to upgrade applications in Version 5 of the NSKit on the Web. For more information, visit <http://www.uic.edu/depts/accc/>, click the purple **Software** button at the top of the page, and select **NSKit Version 5 Upgrades** on the "Available Software and Services" page.

Automatic Dialin Configuration for Windows 95, 98, and Me

While it's a lot easier to set up dialin connections for newer members of the Microsoft Windows operating system family than it used to be, it's not quite in the "it's a snap" class yet.

Until Version 5.0 of the NSKit, that is. The new NSKit has an automated script for Windows 95/98/Me that installs all necessary dialin components and creates a **Dial-up Networking** connection named **UIC-1** that connects to the

ACCC Dialin-9000 lines. Since Dialin-9000 automatically bounces to Dialin-2001 and Dialin-2002 if necessary, this **UIC-1** connection is all you need to use the Chicago new-style ACCC dialin lines.

There's a second Win 95/98/Me automated script that creates a connection named **Dialin-Express** that connects to the Chicago Dialin-Express phone lines. The NSKit documentation explains how to copy the **Dialin-Express** connection and re-configure it to connect to the other old-style dialin lines, Dialin-Rockford or Dialin-Peoria.

(Old-style dialin lines? New-style dialin lines? What's the difference? In addition to the new-style lines being faster — 56 Kbps vs. 28.8 Kbps or 33.6 Kbps — they're also easier to log in to. When using the old-style lines, you enter your UIC netid and password in a "terminal window" after your modem dials in; when using the new-style lines, you enter your netid and password before dialing. Want to know more? See "ACCC Dialin Services" at <http://www.accc.uic.edu/network/dialin/> or click the **Connect - Home** link in the "Quick Start" section of the ACCC home page.)

Norton AntiVirus

If the recent spate of Windows/Web/email viruses and worms (page 10) hasn't already scared you enough to install antivirus software on all your personal computers, both Windows and Macs, maybe it's because you've been lucky and haven't been inflicted with one yet. Don't depend on luck — install the NSKit's highly rated and easy to update Symantec Norton AntiVirus, NAV. There's an option to install NAV in the main menu of both the Windows and Mac Version 5 NSKit.

Run Norton AntiVirus's LiveUpdate by hand when you hear about a new virus or worm.

Our license agreement for Norton AntiVirus allows it to be installed on any computer belonging to any member of the UIC community, on campus or off.

Everyone should run antivirus software on all their computers, all the time.

After you install Norton AntiVirus, be sure to keep your virus protection up-to-date by running its Web **LiveUpdate** feature on a regular basis, say once a week, either by hand:

Windows: **Start**→**Programs**→**Norton AntiVirus**→**Norton AntiVirus Corporate Edition**→**LiveUpdate** button

Macs: **Macintosh HD**→**LiveUpdate** folder→**LiveUpdate**→**Update Everything Now** or automatically. For more information, see: <http://www.accc.uic.edu/software/antivirus/>

The NSKit Fine Print

NSKit software is available for Apple Macintosh personal computers and for personal computers running MS Windows that meet or exceed the NSKit machine and operating system requirements. (See "The Requirements" on page 3.)

The NSKit CD, which includes both the Windows and Mac NSKit, costs \$15.00 and may be purchased on the east side of campus at the UIC Bookstore, 118 CCC, and on the west side at the MicroStation West in the UIC Medical Bookstore, CIU.

If you're on-campus (including when you dial in on an ACCC dialin line), you can download the NSKit from the UIC FTP site. See the NSKit Web site, <http://www.accc.uic.edu/software/nskit/>, for instructions and links.

System Icons:



The Internet and the World Wide Web



Apple Macintosh



MS Windows



UNIX

Readership Icons:

Everyone



Novice



Expert

List of NSKit Applications

Core Applications & Plug-Ins	Win	Mac
Netscape Communicator	4.77	4.73
Eudora Pro Email	5.1R	5.0R
Host Explorer (Win) / Better Telnet (Mac)	6.2.01	2.0fc1
WS FTP (Win) / Fetch (Mac)	5.08	3.0.3
Adobe Acrobat Reader	5.01	5.0
RealPlayer media player	8 Basic	7.0
Apple QuickTime	5.02	4.12
MT-NewsWatcher (Mac only)	-	3.0

Optional & UofI-Online Components	Win	Mac*
✓ Norton AntiVirus	7.51	6.0.2
Asymetrix Toolbook II Neuron	8	-
MacroMedia Shockwave browser plug-in	8.5	8.0
MacroMedia Authorware browser plug-in	5.0f2	5.1f1
✓ Microsoft Internet Explorer	6.0	5.0
Windows Media Player	7.1	-
SoftArc FirstClass	5.5	5.5
✓ SSH Secure Shell (secure telnet)	2.3	-

✓ **Optional components we recommend that everyone install.** In addition to the core applications, we recommend that everyone install: **Norton AntiVirus**, **Microsoft Internet Explorer** (Windows only; IE is installed with the core applications when you use the Mac **Easy Install** option), and **SSH Secure Telnet** (Windows only.)

* **Except for Norton AntiVirus and FirstClass**, which have separate installers, all available components are automatically installed with the "Easy Install" option of the Mac NSKit. See: <http://www.accc.uic.edu/software/nskit/mac.html>

All users of ACCC services are expected to abide by the ACCC Acceptable Use Policy: <http://www.accc.uic.edu/policies/>

NSKit Version 5.0 Applications

The NSKit applications include:

Adobe Acrobat Reader: Acrobat Reader displays and allows you to print PDF (portable document format) files — a common way to view documents on the Internet.

Eudora: Eudora works with your email account, allowing you to manage your email on your personal computer without having to log in to your email account to do it. (Also Eudora is not Outlook, and therefore it isn't generally affected by Outlook viruses/worms; see page 10.)

FTP: Use File Transfer Protocol software such as WS FTP and Fetch to copy files between your computer and a remote computer. The remote computer may be your UNIX account, an FTP site such as [ftp.uic.edu](ftp://ftp.uic.edu), or any other location.

Web browsers: Browser software provides fast and easy graphical access to the Internet and the World Wide Web. **Netscape** is a core application; **MS Internet Explorer** is also offered as a recommended optional application.

Newsreaders: A newsreader is used to read and post to the over 5,000 NETNEWS/Usenet newsgroups. NETNEWS/Usenet gives you access to ClariNet, an electronic newspaper

which offers daily news, sports, weather, syndicated columns, AP wire service feature stories, and science and technological news. The MT-Newswatcher newsreader is included with the Macintosh NSKit; people using Windows can use the newsreader built into Netscape.

Telnet: Telnet allows you to access your accounts on remote shared computers such as the ACCC's tigger, icarus, or borg UNIX workstations. In addition to standard telnet applications, Host Explorer for Windows and Better Telnet for Macs, the Windows NSKit includes **SSH Secure Telnet**, a recommended optional application that allows you use your accounts on UNIX machines such as the ACCC's tigger, icarus, and borg *and* be sure that no one else can intercept your password or work. SSH was introduced in the April/May/June issue of the *A3C Connection*.

Various Media Players and Web Plug-ins:

RealPlayer and Apple QuickTime are core applications and a number of additional Web plug-ins are optional components, including Windows Media Player (Windows only).

Documentation: A printed booklet with comes with the NSKit, which includes instructions for installing the kit applications and for configuring your computer to connect to the Internet so you can use them. All the info in the printed booklet is also available online at:

<http://www.accc.uic.edu/software/nskit/>

The online version has several additions, including links to information about the NSKit applications. (See "The Basic Steps" on page 5.)

The Requirements for Dialing In

Tech Tips

Mac



1. A computer. The minimum requirements are:

Windows: Pentium or newer processor, 200 MHz or faster; Windows 95/98/Me/NT/2000; 32 MB or more RAM; 95 MB available disk space for NSKit applications.

Apple Macintosh: Mac OS 8 through 9, 32 MB of RAM (64 MB or more recommended), and 55 MB available disk space for NSKit applications. The Mac NSKit is not recommended for Mac OS X.

Need to upgrade your Mac OS? UIC Faculty and staff can contact the CSO about an upgrade or purchase; students should contact commercial vendors. If you can't upgrade your Mac to at least Mac OS 8.0, use the previous version of the NSKit, Version 4.3, available from <ftp://ftp.uic.edu>.

2. Connection hardware for your computer. Either: **a modem**, at least 28.8 Kbps, 33.6 or 56 Kbps is better; or **a network card**.

3. A connection to the Internet.

Connect from off campus, with modem and an ACCC dialin line:

There are two types of ACCC dialin lines. The principal difference between them is the point at which you enter your UIC netid and ACCC password to “authenticate” (definitively identify yourself) when connecting. When using the old-style lines, you enter your UIC netid and password in a “terminal window” after your modem dials in; when using the new-style lines, you enter your netid and password before dialing.

Please don't use the ACCC dialin lines when the computer you're connecting is on the UIC campus.

Except for Dialin-Express, which has a 30-minute connection time limit, all the ACCC dialin lines have off-campus telephone numbers and you will be charged by the minute on your campus phone bill if you dial in using them from on campus. These per-minute charges can really add up.

For more information on the ACCC dialin lines, see “ACCC Dialin Services,”

<http://www.accc.uic.edu/network/dialin/>, or click the **Connect - Home** link in the “Quick Start” list on the left side of the ACCC home page. “ACCC Dialin Services” gives the locations, phone numbers, and connection details for all the ACCC dialin lines. (All the new-style lines are in Chicago. In addition to Dialin-Express, which is on campus, there are old-style lines in Rockford and Peoria.)

Connect from off campus with a modem and a commercial dialin ISP (Internet Service Provider) or

Connect from off campus with network card and a commercial ISP cable modem or DSL connection:

Consider using a commercial ISP if you (1) live outside the UIC local calling area, (2) need to connect first time, every time, or (3) want a very fast connection. If any of these apply to you, see “Connecting from Home - Finding an ISP,” and in particular “Warning: When you connect through an commercial ISP, you are not ‘on the UIC campus’”: <http://www.accc.uic.edu/network/>

Connect from on campus with network card and a UIC-Net connection in an office or lab:

Contact your department's REACH member to arrange for a UIC-Net network connection. Don't know who your REACH representative is? There's a search form on the ACCC REACH Web site, <http://www.accc.uic.edu/reach/>, or call the CSO at (312)413-0003 and ask them.

Connect from on campus with network card and a Res-Net connection in a dorm:

Students in on-campus dorms, see the Res-Net page, <http://www.accc.uic.edu/lan/res-net/>, to apply for a personal Res-Net connection. You must open your ACCC account before you apply for a Res-Net connection. You can open your account and change your password online; see the “Accounts, Netids, and Password Changes” box.

Accounts, Netids, and Password Changes

You must have a valid ACCC account and password to use most ACCC services, including dialin access, the machines in the ACCC public personal computer labs, the campus Res-Net network, and your ACCC email account.

All members of the UIC community — students, faculty, and staff — are eligible for a free personal ACCC account. Need to open yours? Go to <http://www.accc.uic.edu/>, click the purple **Accounts** button, then select **Accounts - Get an Account**. Problems? Contact the CSO; see “Getting Help” on page 8.

Your “ACCC account” consists of two things: your *public* UIC netid which says who you are (it's even part of your email address), and your *private* ACCC password, which you use to definitively identify yourself as you.

Students are assigned netids of the form *jtesti1* (built from their names, in this hypothetical case, J. Testing, and a one- or two-digit number). If you're a faculty or staff member, you must choose your own netid and have your department's phonebook contact person register it for you. There's more information about UIC netids and a search form that you can use to look up your department's phonebook contact person in “Getting a UIC Netid,” <http://www.accc.uic.edu/accts/netids.html>.

Your Password Secures Your Account — Change It Early; Change It Often

Change your ACCC password as soon as you open your account and on a regular basis thereafter. (That will keep your password from expiring.) Never give your password to anyone else. Changing your password is a lot easier than you might think when you use the ACCC Web-based Password Changing Utility. Learn more by visiting <http://www.accc.uic.edu/>, clicking the **Accounts** button, and then selecting **Password Changing Utility**.

You can even use the Password Changing Utility to change your password when you've forgotten what it was, provided that you've planned ahead. Visit the Password Change Utility Web page to select a personal challenge/response phrase now, before you forget your password.

Connect from on campus with network card, a Cat-5 ethernet cable, and a UNAS-UIC (UIC Network Access Stations) station in Science and Engineering Laboratory or the Daley Library:

See the UNAS-Web page, <http://www.accc.uic.edu/lan/unas/>, for more information.

4. A UIC netid and a valid, active ACCC account and password.

You will use your netid and the password for your ACCC account to authenticate yourself when you:

- ✓ Log into your account(s) on tigger, icarus, or borg.
- ✓ Check your email on tigger, icarus, or mailserv.
- ✓ Connect to the Internet using an ACCC Dialin line, a UNAS-UIC station, or Res-Net in a dorm, or log in to a machine in an ACCC lab.
- ✓ Visit a UIC-or UoI-restricted Web site.

See “Accounts, Netids, and Password Changes” on page 4 for a description of student netids, instructions for faculty and staff on how to get a

netid, and instructions on how to open your ACCC account online and how to change your password.

Your ACCC password will expire regularly and should be changed as soon as you open your account and on a regular basis thereafter. The ACCC Password Changing Utility is a convenient way to change your password from the Web. Learn more by visiting <http://www.accc.uic.edu/>, clicking the **Accounts** button, then selecting **Password Changing Utility**.

You can even use the Password Changing Utility to change your password when you forget it, provided that you plan ahead. Visit the Password Changing Utility Web page to select a personal challenge/response phrase now, before you forget your password.

And finally,

5. Software to use with the Internet — the NSKit

The ACCC Network Services Kit — the NSKit — gives you the software you need to use the Internet.

The Basic Steps

Tech Tips



1. Get and Install the NSKit CD-ROM.

“The NSKit Fine Print” on page 2 explains how to purchase (\$15) or download (free, but you must be on campus) the NSKit.

There are NSKit installation instructions in the booklet that comes with the NSKit CD, which has both the Windows NSKit (for Windows 95, Windows 98, Windows Me, Windows NT, and Windows 2000) and the Mac NSKit (for Mac OS 8 through Mac OS 9). Installing the kit requires acceptance of the “Academic Computing and Communications Center Network Services Kit License Agreement.”

2. Configure Your Computer to Connect.

The printed NSKit booklet includes three sets of instructions explaining how to configure the built-in networking features of your Windows or Apple Macintosh computer to connect to the Internet, instructions for:

Windows 95/98/Me, for use with the new- and old-style ACCC dialin lines, and with on-campus UIC-Net connections.

Windows NT, for use with the new- and old-style ACCC dialin lines, and with on-campus UIC-Net connections.

Apple Macintosh Mac OS 8–Mac OS 9, for use with both types of ACCC dialin lines, and with on-campus UIC-Net connections.

For more info, including configuration instructions for additional operating systems, see

<http://www.accc.uic.edu/network/dialin/>
<http://www.accc.uic.edu/network/ethernet/>

If you’re connecting from a UIC dorm using Res-Net, see the Res-Net Web pages for configuration instructions, <http://www.accc.uic.edu/lan/res-net/>.

If you’re connecting from home using a commercial ISP, either dialin or cable/DSL, you can and should use the NSKit applications, but follow your ISP’s instructions to set up your Internet connection.

A PDF version of the NSKit booklet is available online at:
<http://www.accc.uic.edu/software/nskit/nskit.pdf>

3. Connect to the Internet.

Most likely, your computer will start your Internet connection automatically, particularly for always-on connections such as UIC-Net on campus or cable/DSL at home.

- ✓ **For UIC-Net**, opening your Internet connection is completely automated. Your UIC-Net connection will start up automatically when you turn your computer on.

Note: If you configure your computer to use both UIC-Net and a dialin connection, there's an additional step in the configuration process to tell it not to dial in when the network connection is present. That is discussed in the dialin (Windows) and UIC-Net (Macs) sections of the NSKit booklet.

- ✓ **For Res-Net and UNAS-UIC**, you have to open a Web browser and log in using your UIC netid and password to open a connection and then log in again as a period of time goes by without any Internet activity. See their Web pages for details:

<http://www.accc.uic.edu/lan/res-net/resconfig.html#5>

<http://www.accc.uic.edu/lan/unas/index.html#GettingConnected>

- ✓ **For dialin connections such as the ACCC dialin lines**, your computer will either automatically initiate the login procedure for a dialin connection when you open an Internet application or you can initiate the dialin connection by hand. The NSKit booklet and Web pages explain how and give instructions on how you authenticate using your UIC netid and password to use the ACCC dialin lines.

4. Use the NSKit Internet Applications.

The Internet applications in the NSKit are listed in a table on page 2. Links to introductory instructions on how to use them are available online in "The Basic Steps to Internet Access" page,

<http://www.accc.uic.edu/software/nskit/steps.html>.

In addition to these Web links, the ACCC's Instructional Technology Lab (ITL), gives seminars — often hands-on — on Web browsing, Web authoring, and using selected NSKit applications. For more information, including a schedule and online registration, go to the ACCC Seminars page, <http://www.accc.uic.edu/seminars/>.

5. If you dialed in to connect, disconnect when you're done.

- ✓ **If you connect using a dialin connection, disconnect when you're finished.** The dialin configuration instructions in both the NSKit booklet and the NSKit Web pages include instructions on how to disconnect.
- ✓ **If you connect using Res-Net**, you will be asked to reauthenticate after three hours of inactivity, and your connection will be closed if you fail to do so.
- ✓ **If you connect using Res-Net or UIC-Net**, you will automatically be disconnected when you shut down your computer.
- ✓ **If you connect using UNAS-UIC**, you will be disconnected after one hour of inactivity. If you want to stay connected, open a Web browser and sign-in again.

6. Regardless of how you connect, don't forget security.

These days there are two security items you cannot do without, regardless of how you connect to the Internet.

- ✓ **Good antivirus software**, such as the NSKit's Norton AntiVirus, NAV, **that you keep up-to-date.** To keep NAV up-to-date, run LiveUpdate on a regular basis, say once a week, and also whenever you hear about a new virus or worm.
- ✓ **A personal firewall** such as Zone Alarm from Zone Labs. A good personal firewall will not only block unauthorized access *to your personal computer from the Internet*, but will also block software (and viruses) on your computer from sending information out *from your personal computer to the Internet* without your permission.

That way, even if you do get an email worm and it attempts to send copies of itself — or, like SirCam (page 10), copies of random personal documents — to everyone you have ever sent email to and even some that you haven't, your personal firewall can block those messages from leaving your computer. (That is, of course, unless you do your email with Microsoft Outlook and it's an Outlook worm. That substantially diminishes your chances of being saved by a personal firewall.)

For more info on personal firewalls, see:

<http://www.accc.uic.edu/network/athome/homeseccurity.html#firewall>

Internet Access and the ACCC

Tech Tips

Mac



When it comes to providing Internet access, what the ACCC does is no different from what commercial Internet providers do. We provide the application software to use on the Internet — the Network Services Kit — and Internet access to use the NSKit applications with.

ACCC on-campus network connections: UIC-Net in campus offices and labs, Res-Net in campus dorm rooms, and a limited number of UNAS-UIC (UIC Network Access Stations) laptop plug-in stations in Science and Engineering Laboratory (SEL) and the Daley Library.

ACCC off-campus phone/modem connections: the ACCC dialin lines.

If you're connecting on campus, use a campus network connection.

Faculty and staff, contact your department's REACH member to arrange for a UIC-Net network connection. Don't know who that is? There's a search form on the ACCC REACH Web site, <http://www.accc.uic.edu/reach/>, or call the CSO at (312)413-0003 and they'll look it up for you.

You are not limited to a single ISP or connection type.

Even if you normally use a commercial ISP, dialin or cable/DSL, there might be times that you want to use an ACCC dialin line or to bring your home computer in to UIC and use it with a campus network. That's absolutely no problem. All you need is define a dial-up or network configuration for each connection method that you use.

The NSKit configuration pages specifically include instructions on how to set up a single personal computer for both dialin and network connections and how to specify the connection method you want to use as your default.

Also, you certainly can use NSKit applications when you connect using a commercial ISP; almost all of them will work without modification with any ISP. There are some consequences, however, as explained in "Warning: When you connect through an commercial ISP, you are not 'on the UIC campus'": <http://www.accc.uic.edu/network/notcampus.html>

In particular, if you connect to UIC using another ISP, you cannot use the ACCC's sending email SMTP servers and you will be asked to authenticate using Bluestem when you visit some university-restricted Web sites.

Students living in on-campus dorms, visit <http://www.accc.uic.edu/lan/res-net/> to apply for your personal Res-Net connection. You must open your ACCC account before you can apply for a Res-Net connection. See "Accounts, Netids, and Password Changes" on page 4.

Don't use the ACCC dialin lines when connecting from on the UIC campus.

Except for Dialin-Express, which has a 30-minute connection time limit, all the ACCC dialin lines' telephone numbers are off campus, and you will be charged by the minute on your campus phone bill if you dial in using them from on campus. Having your computer connected to the campus ethernet backbone is a much better, faster, and cheaper alternative.

If you're connecting from off campus, consider using the ACCC dialin service, but it might not be best for you.

Any member of the UIC community, student, faculty, or staff, can use the ACCC dialin services. There are no UIC charges involved. Even though the ACCC dialin lines are "free," there are three important reasons why you might not want to use them.

1. We continually monitor the ACCC lines and improve them as we can, but we can't guarantee one will always be available when you want it.
2. They are not always really free. When you're dialing in from reasonably far off campus, the per-minute telephone charge to connect to the ACCC dialin lines' (312)666 and (312)413 exchanges can add up very quickly.
3. You want or need a really fast home connection.

If either of the first two are issues for you, consider subscribing to a commercial Internet dialin service provider that has a "no busy signal" guarantee and local access telephone numbers that are convenient when you're at home and/or when you're traveling. If the third is your most important consideration, look into a home cable or DSL connection.

For more information on how to choose an ISP, see "Connecting at Home - Finding an ISP" at: <http://www.accc.uic.edu/network/isp.html>

Getting Help

The ACCC Beat



Can't get connected? Eudora broken? Lost a file on tigger? Here's how to get help.

Getting Help on Your Own

No matter what your problem is, chances are you're not the first person to have it. So you might want to look around a bit on your own before you contact us. For example, check the ACCC's online tutorials and other Web-based resources. Start at the:

ACCC home page, <http://www.accc.uic.edu/>, and, in particular, its search link (in the yellow area on the left of the ACCC home page) and the links on the **Help** page (click the purple **Help** button at the top of most ACCC Web pages).

Troubleshooting page, <http://www.uic.edu/htbin/accc/inform>, or click the **Troubleshooting** "Quick Start" link in the yellow area on the ACCC home page.

FAQs, <http://www.accc.uic.edu/home/faqs.html>, or the **List of FAQs** "Quick Start" link.

The frequently asked questions pages cover pretty much the same territory as the troubleshooting pages, but it's easier to browse through them when you're just looking for inspiration.

The alphabetical list of ACCC "core" Web pages, <http://www.accc.uic.edu/home/list.html>, or the **Alphabetic** "Document List" in the yellow area on the ACCC home page.

Your roommates, colleagues, and in particular your department's REACH representative are also good and quick resources. You might find that they've seen the problem you're having and know how to fix it. No matter how fast we could answer your question, getting the answer on your own or from your next-door neighbor is faster.

Getting Help from the CSO

When getting help on your own doesn't do it, the ACCC's Client Services Office — the CSO — is there to help. Here's how to get in touch with us:

Email or the AHEAD Web page: Send your question by email to consult@uic.edu or enter your question directly into ACCC AHEAD (ACCC HELP and Answer Database) via the AHEAD Web site: <http://consult.accc.uic.edu/>

Walk-in: East side: the Client Services Office, room 2267 SEL, 950 South Halsted. The CSO is open 9 a.m. until 5 p.m. weekdays, except Wednesday when it closes at 4 p.m. Walk-in hours are extended until 7 p.m. during the first two and last two weeks of the semester. West side: room 181 BGRC, 1940 West Taylor, from 9 a.m. until 5 p.m. weekdays, except Wednesday, when it closes at 3:30 p.m. There are also lab monitors in BSB, CCC, LIB, SSB, SRC, and SEL. The current schedules are on the Web: <http://www.accc.uic.edu/cso/> <http://www.accc.uic.edu/plabs/hours.html>

Telephone: (312) 413-0003; 9 a.m. to 7 p.m. weekdays, except from 4 p.m. to 5:30 p.m. on Wednesday. We have six incoming lines, but since each call might take five to ten minutes, if you call at a peak time you might find that our "consultants are currently busy." If you're put on hold, please stay on the line.

How should you contact the CSO?

AHEAD is best for most problems.

AHEAD lets you describe your problem in detail (see "You Can Help Us Help You" for a list of useful "details"), automatically keeps a record of all your questions and all our correspondence about it, and makes it easy to refer your question to an expert if necessary. We get a lot of email, so we probably won't answer your question right away, but we try to get back to you within 24 hours.

Using the AHEAD Web page is in some ways better than submitting a problem by email, because you'll know right away that your question has been submitted. And the AHEAD Web page allows you to check the status of your problem (or revisit previous AHEAD questions) any time you want, even if you don't have access to a working email system. That's really convenient when your problem is that you can't get to your email.

When you visit the AHEAD Web page, you'll be asked to login with Bluestem — that's to make sure that only you see your problems. To submit a question, click the **Report a Problem** link at the bottom of the page. After you fill in the required



fields (select **General** as the **Subject:** if you can't choose or if none of the others apply), describe your problem in the **Long problem description:** box, then click .

You'll return to the list of your open problems. Click your browser's **Refresh** icon and you'll see the problem you just opened included in your list.

Regardless of how you submit your problem, you'll receive an email response in a short while acknowledging that your message was received. It will be from **consult@uic.edu** and its subject will be: **[ProblemDB] nnnnn:** followed by the subject of the email message you sent or the text you entered in the **Short problem description:** field on the New Request Web page. The *nnnnn* is your "AHEAD problem ID." You will also receive an email message from AHEAD when we reply to your problem.

When writing us about an AHEAD problem, please use either use the AHEAD Web page (click on the the problem's **Description**) or use your email program's **Reply** function to send your reply back to AHEAD with **[ProblemDB] nnnnn:** in the subject. Your reply will then be automatically posted to your problem in AHEAD and will be emailed to everyone involved in handling it. Please don't open a new problem, send a new message to **consult@uic.edu**, or reply directly to a ACCC staff member.

Walk-in for account problems or to demonstrate your problem directly.

If you're having a problem with your account, we'll take a quick look at your photo ID, just to make sure we're fixing the right account for the right person.

You might also drop by to discuss a problem that you find difficult to explain (the consultants know the questions to ask to zero in on what your problem really is), to pick up a quick start handout, or when you're just in the neighborhood.

Phone in when you have a fast question that requires immediate assistance or to report a systemwide problem.

If you're phoning to report a systemwide problem, including problems with the UIC campus networks, dialin telephone connections, and printers, call Network Operations at (312) 413-8080; Operations is staffed 24 hours per day, 7 days a week. Otherwise, call the CSO at (312)413-0003 during its telephone hours.

You Can Help Us Help You

A major portion of the CSO's and our consultants' job is helping you troubleshoot the computer-related problems that you experience, whether you're on campus in your office or in our labs or you're connecting via an ACCC dialin line from home. Problems using a commercial connection should go to your ISP.

But please help us help you by being prepared.

First, please select the most appropriate contact method for your particular problem; usually that will be AHEAD, either:

by email to **consult@uic.edu** or
on the Web at **http://consult.accc.uic.edu/**

Next, please include as many details as you can when you describe your problem. Let's say, for example, that you're having trouble with Eudora.

Don't say: "Help, my email isn't working!" There's not much information there.

Better: "Eudora can't download my mail from tigger." This is better because it saves all of us from our first set of questions: "Where do you get your mail?" and "How do you read it?"

Better still: "I'm running WinMe with Eudora Pro 5.1, on campus with a UIC-Net ethernet connection. My POP server is tigger, and I repeatedly get the error message 'POP server busy.' I'm sure my password is correct, because I can telnet to tigger and log on. What's up?"

That's a lot more like it! Though you could mention whether it ever worked, and if it did, when it broke.

To Sum It Up

To sum it up and add a few more while we're at it, some useful details to include in your note are:

- ✓ What operating system you're using, and if it's UNIX, whether it is borg or icarus or tigger.
- ✓ How you're connecting to the Internet.
- ✓ What program you're using.
- ✓ What the exact error message is.
- ✓ What the conditions are when you get the error.

Don't worry about giving us info that we don't need; the more you tell us, the more likely we are to be able to answer your question or at least to figure out which ACCC group we should refer it to.

Comments are welcome; please send them to Margaret Bird, **mbird@uic.edu**

Email or AHEAD us, please, at:
consult@uic.edu
or
http://consult.accc.uic.edu/

One question per AHEAD problem; one problem per question.

For more about CSO services, see the CSO Web page: **http://www.accc.uic.edu/cso/**

Living with a Hostile Internet

News on the Net



This summer has been a really bad time for those of us who use the Internet for work or for pleasure.

July 17: SirCam

SirCam is a nasty Outlook worm that randomly picks an item from your hard drive and sends it, with a distressingly convincing wrapper, to everyone you know and also to email addresses it finds on the cached copies of Web pages you visited recently. It also has a destructive payload; it was designed to either empty or fill the C: drive on randomly selected machines. (A bug in its design made that unlikely to occur, but we won't be so lucky the next time.)

SirCam spread by email, but you didn't have to use Outlook or even to have opened an infected message to get it. It also spread by "open network shares" — creating copies of itself on all writable directories, including those accessed over a local area network. Thus a infected file shared on a network could spread SirCam to all machines on the network.

July 19 and August 4: Code Red I and II

Shortly after SirCam began infecting individual PCs, three worms appeared that attacked Microsoft Web servers and brought the Internet to a grinding halt.

The Code Red worms infected Microsoft Internet Information Server (IIS) Web servers running under Windows NT4 or Windows 2000, attacking two well-known vulnerabilities that already had published fixes. Many people whose machines were infected by the Code Reds didn't even realize they were running a Web server, and so they had no idea that they ought to have patched it. (But don't feel bad, even some of Microsoft's Web servers were infected by Code Red.)

September 18: Nimda

As bad as the Code Reds were, they didn't spread by email. Nimda, the next worm/virus, was much worse, both from an infection and Internet traffic point of view. "Nimda" is "admin" spelled backwards, which is quite appropriate, because it was a huge problem for system administrators everywhere.

Nimda is an equal-opportunity infector attacking machines running any Windows operating system and spreading four ways:

From an infected machine to arbitrarily selected Web servers. Like Code Red, Nimda scans the Internet looking for Web servers using Microsoft's Internet Information Server (IIS) and Personal Web Server (PWS) software and attempts to exploit a number of long-known server vulnerabilities or to use "backdoors" left by previous worms, including Code Red.

From infected Web servers to an individual's PC, by browsing infected Web sites. Yes, visiting the wrong Web site could infect your PC with Nimda. (But not if you have an up-to-date version of Norton AntiVirus, thanks to its File System Realtime Protection.)

From PC to PC via open network shares. Like SirCam, Nimda creates copies of itself on all writable directories (and also attaches itself to executable files), including shared files accessed over a local area network.

And the standard, via email. PCs can be infected when Outlook or another email program uses Internet Explorer to open an HTML-formatted message carrying the worm. (Just opening the message is enough, not an attachment.)

So Why Should You Care?

The SirCam filters on tigger and icarus rejected thousands of messages in their first few hours. (We stopped counting after that.) SirCam could and did send people's personal files all over the Internet.

Nimda was similarly widespread. On September 19, just one day after Nimda was first identified, we had to filter (refuse traffic to and from) half the subnets on the UIC campus just to keep the rest of our network going at a crawl. On September 21, there were still 300 individual machines on campus that were filtered due to Nimda.

The most annoying and regrettable thing about Code Red and Nimda is that Microsoft released fixes for the security holes they use before the worms appeared. The patches for the security holes that Code Red uses were released in July 2000 and June 2001. The patch for the IIS hole that Nimda uses was released in October 2000 — yes, almost a year before Nimda — and patch for the email

Read More About Nimda

For an interesting and not too difficult to read technical description of Nimda, including graphs of its effect on Internet traffic, see the SANS Institute (System Administration, Networking, and Security) incident.org's "NIMDA Worm/-Virus Report — Final" at: <http://www.incidents.org/react/nimda.pdf>

Use Windows? You may be running IIS.

If you are running Microsoft FrontPage or a similar program that is used to design Web pages, IIS may be installed on your computer.

MIME exploit it uses was released in March 2001. Nimda, at least, shouldn't have happened.

Nor should the vast majority of SirCam infections have occurred; Symantec released a virus definition for Norton AntiVirus that detected SirCam on July 17, the same day that SirCam was first detected. In spite of that, SirCam was still going strong at the beginning of September. (NAV is the antivirus software that anyone at UIC can use on any of their computers, even at home, at no cost, under a UIC site license; see "Norton AntiVirus" on page 1.)

What You as an Individual Can Do

A REACH representative put together these suggestions for people running Windows. Her department's subnet was one of the ones the ACCC filtered for Nimda; its major offender was not a "computer"; it was a Cisco switch with a vulnerable IIS Web interface. Who would have guessed?

"You may have heard of the Nimda worm which brought down [our department's] network (and many, many others) Tuesday morning. Ed Zawacki and other heroes at the ACCC work hard to protect us from such disasters, but without our help they can't keep the network free of threats. I am asking all of you who use Microsoft Windows to do the following:

"1) Run **LiveUpdate** in Norton Antivirus: Double click on the yellow shield in the lower right corner of your monitor and click on the **LiveUpdate** button. Make sure you have selected the option to update using files found on the Internet, then click the **Next** button. Click **Finish** when LiveUpdate completes the download and **Exit** to close the Norton AntiVirus window.

"2) Upgrade your version of Microsoft Internet Explorer. If you have Internet Explorer on your computer, please visit the Web site: <http://www.microsoft.com/windows/ie/downloads/ie6/download.asp> to upgrade to the latest version of Internet Explorer. [Or install IE 6 from the NSKit Version 5 CD.] Unpatched versions of IE up to IE 5.5 service pack 2 and any version earlier than 5.01 have bad security problems.

"3) Don't trust email attachments. [And don't use preview panes — you can get Nimda just by having an infected message opened in a preview pane.] If you don't need to open an attachment, don't. If you must open email attachments, make sure Norton AntiVirus is running on your computer and that you run **LiveUpdate** regularly.

"4) If you are using Microsoft Outlook to read your email, please try to switch to Eudora, Webmail, or any other email client. The worst of the recent viruses and worms have spread themselves through insecure Outlook email clients, using Outlook address books to find new hosts to infect." [Many people who know say Outlook is inherently insecure and would have to be rewritten from the ground up to have a semblance of security. It certainly is true that as soon as one Outlook security problem is fixed another one appears.]

What You as a "Sysadmin" Can Do

A fifth request, for everyone who owns a computer or computer-managed equipment of any sort: **Please consider all your software, computers, and computer-managed equipment from a security point of view.**

The almost universal point of view of all (Mac, Windows, and UNIX) operating system and software manufacturers is to turn everything on by default and to depend on the user to turn off what they don't need. That needs to change, but in the meantime you need to keep up your end of the bargain. And you also need to stay up-to-date with your operating system and the other software you run.

Sound overwhelming? It isn't. The FBI and the SANS Institute (see "Read More About Nimda" on page 10) have put together "SANS Resources — The Twenty Most Critical Internet Security Vulnerabilities, the Expert's Consensus," at <http://66.129.1.101/top20.htm>. That's the twenty most important of the hundreds of security vulnerabilities that have been identified; keep up-to-date with these twenty and you'll go a long way toward doing your part in keeping your machines, and the Internet, secure.

The list includes seven security problems that affect all types of systems (including running software that you don't need), six specific to Windows, and seven specific to various flavors of UNIX, including Linux and Solaris. It includes the security exploits that allowed Code Red and Nimda to spread so rapidly.

The SANS top twenty is a "living document" that will change as needed and includes instructions on how to fix the problems. Everything you'll need to secure your machines is there.

Comments are welcome; please send them to Ed Zawacki, security@uic.edu

*There are links
to additional
info in the
online version
of this article:*

<http://www.accc.uic.edu/newsletter/a dn32/hostile.html>

The A3C Connection

Academic Computing and Communications Center (MC 135)

Room 124 Benjamin Goldberg Research Center

1940 West Taylor Street

Chicago, Illinois 60612-7352

About The A3C Connection

The A3C Connection is published four times per year by the UIC Academic Computing and Communications Center, providing news and information about the use of computers, communications, and networking at UIC. It is edited by Judith Grobe Sachs with help from Bill Mayer and the UIC Office of Publications Services.

Distribution of the *A3C Connection* is free to UIC faculty, staff, and students, and to other universities and not-for-profit organizations. To subscribe, send us your name and address, UIC campus address if possible, including your department name and mail code. To cancel your subscription, send us your address label or a copy of all the information on it.

Contact us by electronic mail at connect@uic.edu; by telephone at the Client Service Office, (312) 413-0003; by US Mail at The A3C Connection, ACCC (MC 135), Room 124 Benjamin Goldberg Research Center, University of Illinois at Chicago, 1940 West Taylor Street, Chicago, Illinois 60612-7352; or by fax at (312) 996-6834.

We welcome any comments, suggestions, complaints, or requests you might have concerning the *A3C Connection*.

The Fine Print

The use of trade, firm, or corporation names in this publication is for the information and convenience of the reader. Such use does not constitute an official endorsement or approval by the University of Illinois of any product or service to the exclusion of others that may be suitable. Trade names that may appear in this publication include the following: Apple, the Apple logo, Mac, Mac logo, and Macintosh (registered trademarks of Apple Computer, Inc.); AIX and AIX/ESA (registered trademarks of IBM Corp.); UNIX (registered trademark of The Open Group); HP and HP-UX (registered trademarks of Hewlett-Packard Corporation); Sun, Solaris, and Java (registered trademarks of Sun Microsystems, Inc.); and Microsoft, Windows, Windows NT, and other Microsoft product names (trademarks or registered trademarks of Microsoft Corporation). All other product names mentioned herein are used for identification purposes only, and may be the trademarks or registered trademarks of their respective companies.

Permission is granted to reprint or adapt all or part of the *A3C Connection* for nonprofit use, provided that full acknowledgment of the source is given.