**Creo Inc.**
**A subsidiary of Kodak**
3700 Gilmore Way
Burnaby, B.C., Canada
V5G 4M1
Tel: 1.604.451.2700
Fax: 1.604.437.9891

**Request support:**
ecentral.creo.com

www.creo.com

**Internal:** 731-00616A-EN Rev A
**Release date:** 16 August 2005

Procedure

# Enabling Telnet on Mac OS X

## Understanding inetd

Many common UNIX® internet services (such as FTP, telnet, rlogin, POP, finger) on Mac OS® X are launched by the *inetd* daemon.

**Important note:** Only the server component of these UNIX services is referred to in this document, and it is not implied that you can use outgoing client-side services.

The UNIX internet systems are not constantly used, and the systems are only activated when necessary. Instead of running a separate process for each service, *inetd* monitors the port associated with each service. Then when *inetd* detects that a remote system is trying to connect to a service, it activates the relevant service and connects to the remote service. *inetd* is controlled by the **/etc/inetd.conf** file. A sample portion of the **/etc/inetd.conf** file is shown below:

```
#ftp      stream  tcp     nowait  root    /usr/libexec/tcpd          ftpd -l
#login    stream  tcp     nowait  root    /usr/libexec/rlogind       rlogind
#nntp     stream  tcp     nowait  usenet  /usr/libexec/nntpd         nntpd
#ntalk    dgram   udp     wait    root    /usr/libexec/ntalkd        ntalkd
#shell    stream  tcp     nowait  root    /usr/libexec/rshd          rshd
telnet    stream  tcp     nowait  root    /usr/libexec/telnetd       telnetd
#telnet   stream  tcp     nowait  root    /usr/libexec/tcpd          telnetd
```

## Activating the Telnet service

To activate the Telnet service, perform one of the following actions:

- Enable **Remote login** in the Services tab of the Sharing Preferences
- Uncomment the Telnet process line in the **etc/inetd.conf** file.

After changing the *inetd* configuration, you need to restart the Mac OS X workstation.

## The /etc/hosts.allow file

**Note:** The **/etc/hosts.allow** file does not exist by default. However, if it does, you need to edit it as detailed below.

The *tcpd access control* language contains several options. The most common usages are provided below, which are sample lines from a fictional **host allow** file.

```
ALL : localhost : allow
telnetd : .goodguys.com, 192.168.17.24 : allow
ftpd : mybuddy.good.com, 192.168.39., 10.162.23.0/255.255.255.0 : allow
ALL : ALL : deny
```

The basic format of a line in the **hosts.allow** file is as follows:

daemon_list : client_list : option : option ...

where:
**daemon_list** is a list of daemons to which the options refer to. For clarity, you can usually list only one daemon per line unless using a wildcard, such as ALL.
**client_list** is a list of clients to which the allow/deny options refer to.

**The client_list can have one of the following formats:**

- **Explicit hostname** can be either a fully-qualified domain name (e.g. foo.somewhere.com) or a local hostname specified in NetInfo.
- **Explicit IP Address** is self-explanatory—the IP addresses that you want to allow or deny.
- **Pattern-matched hostname or IP Address** by adding a leading or trailing "." to a hostname or IP address, you can match anything within a domain or network.

  For example, if you list ".stepwise.com", then any machine with a DNS name inside the stepwise.com domain will match. If you list "192.168.33.", then any machine with an IP address whose first three fields are "192.168.33" will match.
- **Net/mask pair**—it is not crucial to understand the inner workings of IP addressing. Basically, a host address matches if "net" matches the bitwise *and* the host address and "mask". The end result is similar to a pattern-matched IP address, except that matched addresses can cross the octet boundaries in IP addresses—for example, the net/mask pair "10.168.23.0/255.255.254.0" matches any host IP address in the range of 10.168.23.0 to 10.168.24.255.

## Handling Logging Denied Connections

Using the *syslog* facility, you can log attempted and failed logins.
The **/etc/syslog.conf** file contains the following lines:

*# The authpriv log file should be restricted access; these*

*# messages shouldn't go to terminals or publically-readable files.*

*authpriv.*;remoteauth.* /var/log/secure.log*

By adding the following line to the file, you can log all remote activity on your system:

**.info /var/log/allmessages*

**Notes:**

- Restart the Mac OS X system after changing the **/etc/syslog.conf** file.
- You should never use tabs in the **/etc/syslog.conf** file; only spaces are allowed.

**About Kodak Graphic Communications Group (GCG)**

The leading provider of graphic communications solutions worldwide, Kodak's Graphic Communications Group (GCG) offers image capture systems; professional color, copydot, and high-speed document scanning systems; inkjet printing and proofing systems; workflow and color management software; thermal imaging devices for film, plates, and proofs; high-quality proofing media, printing plates, and recording film; on-demand color and black-and-white printing systems; data storage products; and professional services. Creo joined the GCG in June 2005, when it became a wholly owned subsidiary of Kodak. With corporate headquarters located in Rochester, N.Y., Kodak (NYSE: EK) had sales of $13.5 billion in 2004 and is committed to a digitally oriented growth strategy.

© 2005 Kodak. The Creo product names mentioned in this document are trademarks or service marks of Creo Inc., a subsidiary of Kodak, and may be registered in certain jurisdictions. Other company and brand, product, and service names are for identification purposes only and may be trademarks or registered trademarks of their respective holders. Data subject to change without notice.