

# TCP/IP Applications



# Objectives

- Describe common Transport layer protocols
- Explain the power of port numbers
- Define common TCP/IP applications such as HTTP, HTTPS, Telnet, e-mail (SMTP, POP3, and IMAP4), and FTP

# Overview

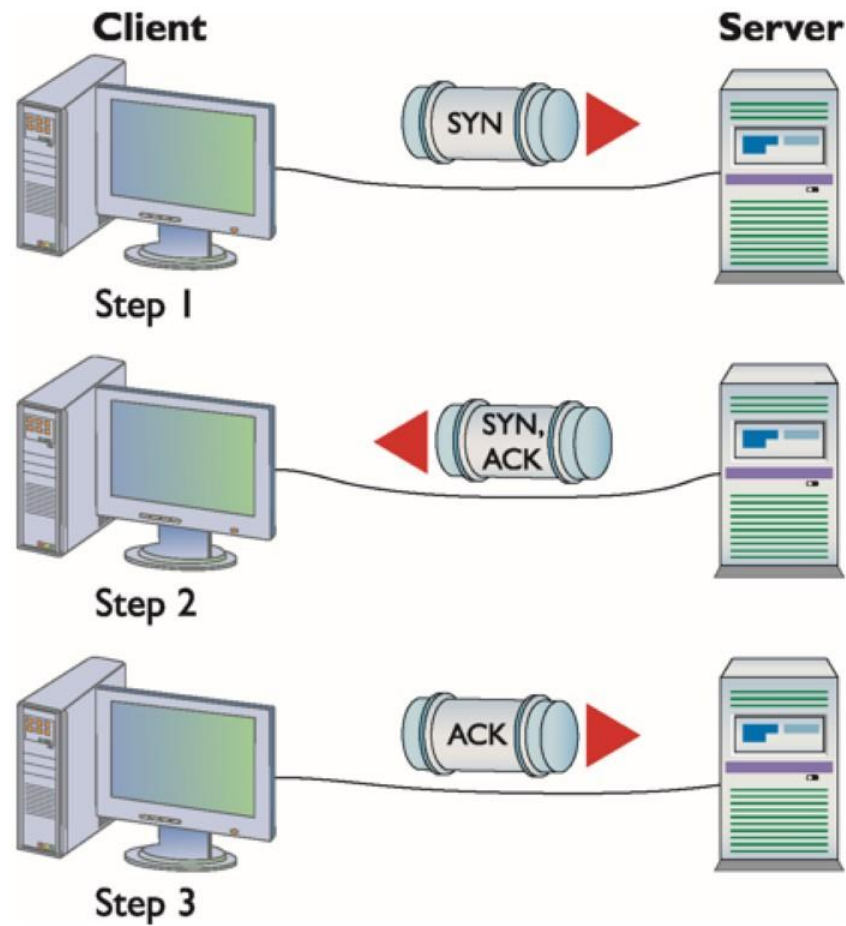
# **Three Parts to this Area**

- **Transport Layer Protocols**
- **The Power of Port Numbers**
- **Common TCP/IP Applications**

# Transport Layer Protocols

# How People Communicate

- **Connection-oriented**
  - Acknowledgement between two people beginning conversation
  - The conversation
  - Close of conversation



**Figure 9.1** A connection-oriented session starting

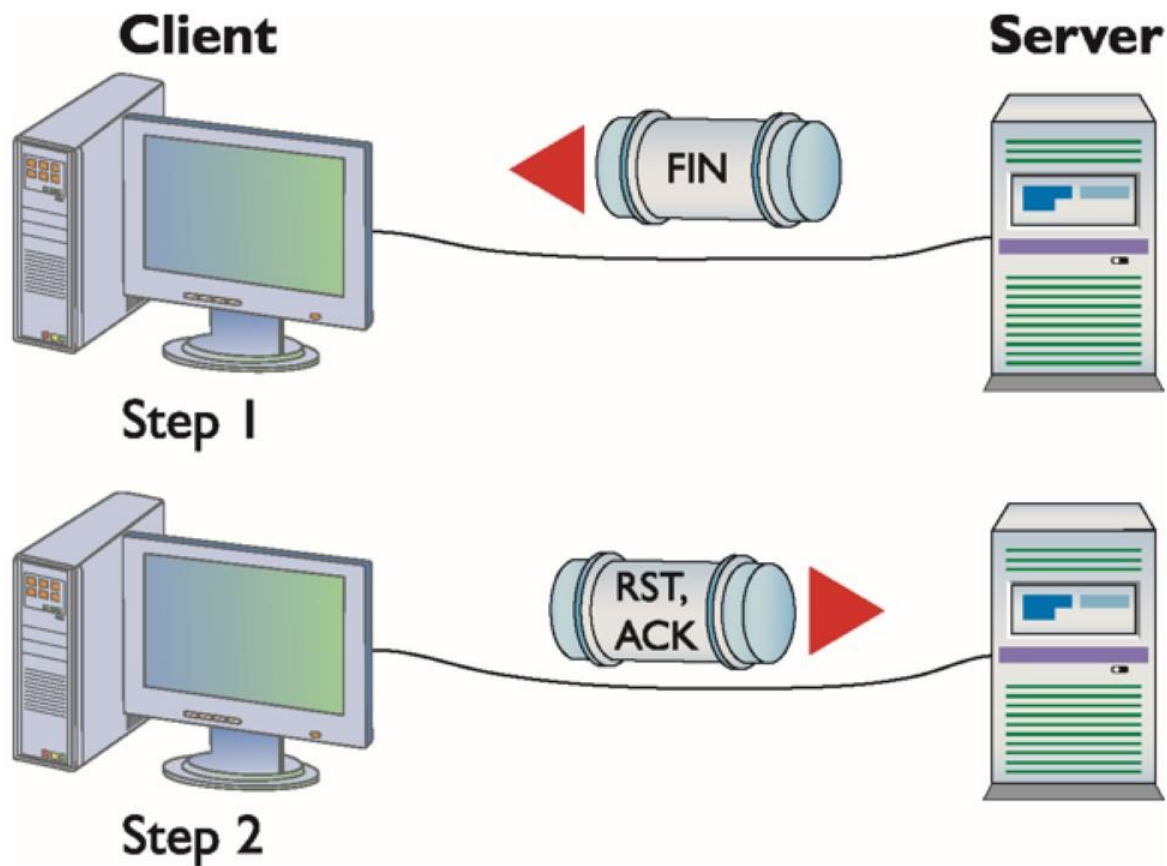
- **Connectionless**

- No opening acknowledge
- Short message shouted across a room
- No closing

- **Session**

- Any single communication between computers
- All session must begin and eventually end





**Figure 9.2** A connection-oriented session ending

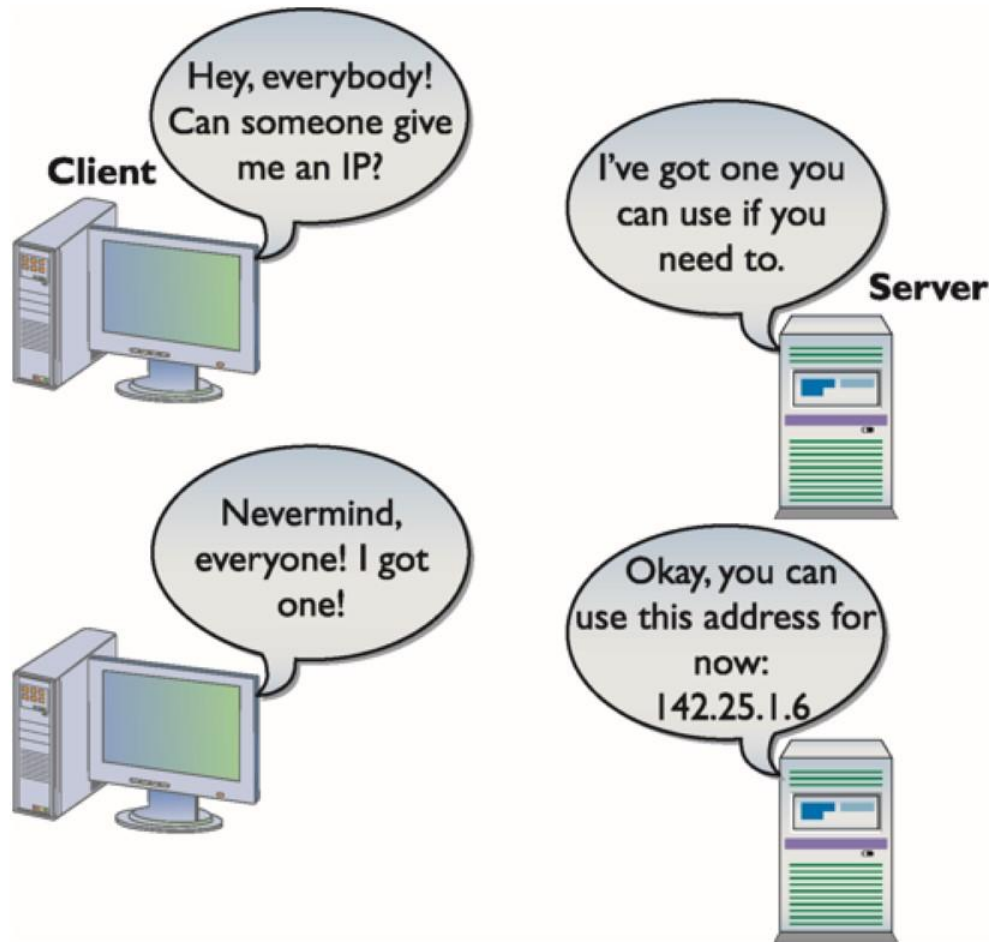
- **Transmission Control Protocol (TCP)**
  - In charge of connection-oriented communication
  - Most common type of TCP/IP session

- **Connection-oriented session**
  - Browser sends an ACK packet
  - Server responds with a SYN, ACK packet
  - Client sends an ACK, requests Web page
  - Server sends Web page and a FIN packet
  - Client responds with RST, ACK

- **User Datagram Protocol (UDP)**
  - Used by very few applications
  - Requires much less overhead than TCP
  - No start, no acknowledgement, no end

- **DHCP uses UDP**

- Client broadcasts discovery packet
- Server responds with DHCP offer (sent directly to MAC address)
- Client sends DHCP request directly to server MAC address
- Server sends DHCP acknowledgement with IP configuration
- Client responds with DHCP lease



**Figure 9.3** DHCP steps

- **Trivial File Transfer Protocol (TFTP)**
  - Uses UDP
  - Transfers files between computers
  - Does not have any data protection
  - Never use it over the Internet

- **Internet Control Message Protocol (ICMP)**
  - For connectionless communications that never need more than a single packet
  - Handles maintenance issues like disconnect (host unreachable)
  - Applications use ICMP to send status information to the other end of a session



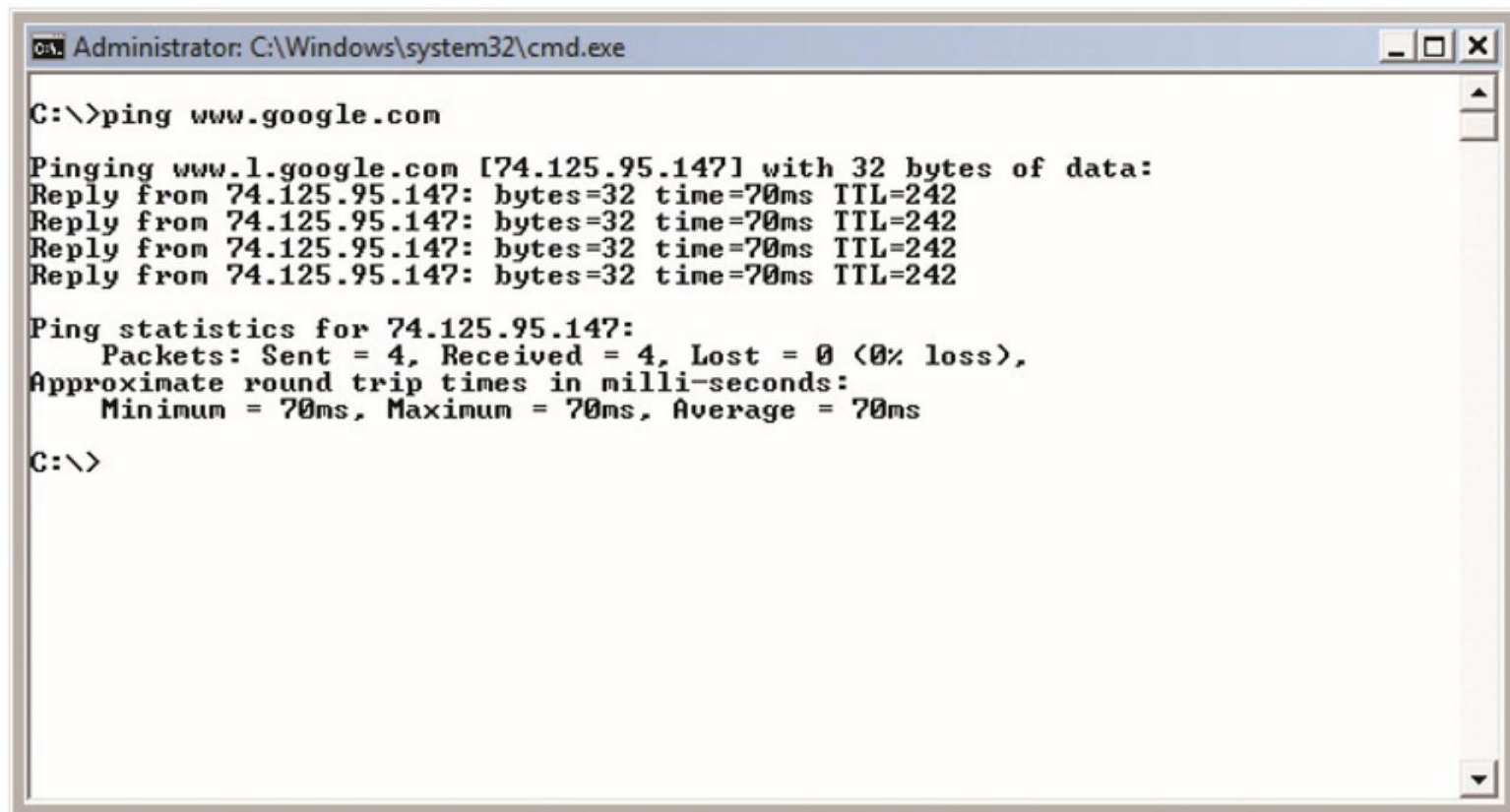
- **PING**

- **Sends a single ICMP packet**

- Echo request

- To an IP address

- **All computers (unless blocked by a firewall) respond with echo reply**

A screenshot of a Windows command prompt window. The title bar reads "Administrator: C:\Windows\system32\cmd.exe". The command prompt shows the user entering "ping www.google.com". The output displays four successful replies from IP address 74.125.95.147, each with 32 bytes of data, a response time of 70ms, and a TTL of 242. Below the replies, the ping statistics are shown: 4 packets sent, 4 received, 0% loss, and round trip times of 70ms minimum, maximum, and average. The prompt ends with "C:\>".

```
Administrator: C:\Windows\system32\cmd.exe
C:\>ping www.google.com

Pinging www.l.google.com [74.125.95.147] with 32 bytes of data:
Reply from 74.125.95.147: bytes=32 time=70ms TTL=242
Reply from 74.125.95.147: bytes=32 time=70ms TTL=242
Reply from 74.125.95.147: bytes=32 time=70ms TTL=242
Reply from 74.125.95.147: bytes=32 time=70ms TTL=242

Ping statistics for 74.125.95.147:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 70ms, Maximum = 70ms, Average = 70ms

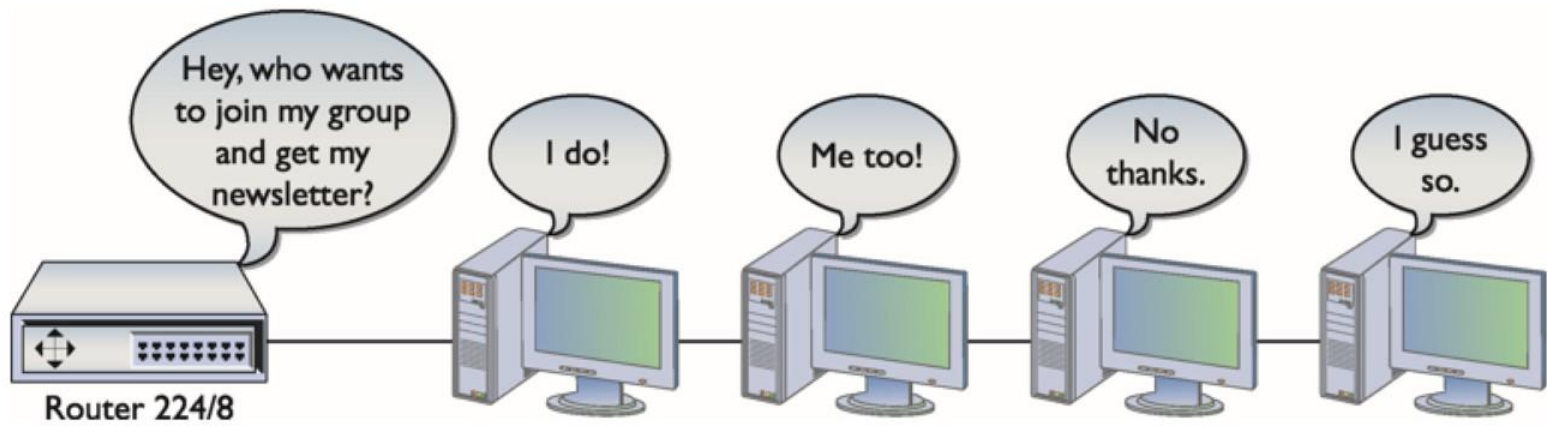
C:\>
```

**Figure 9.4 PING in action**

- **Internet Group Management Protocol (IGMP)**
  - Used for multicasts
  - Routers use to determine a “group” membership
  - Class D IP addresses with network ID 224/8

- **More about multicast**

- Does not assign IP addresses to hosts
- A multicast is assigned a certain 224/8 address
- Those who wish to receive this multicast must join the IGMP group
- Upstream router will send multicasts



**Figure 9.5 IGMP in action**

- **More about multicast**

- Does not assign IP addresses to hosts
- A multicast is assigned a certain 224/8 address
- Those who wish to receive this multicast must join the IGMP group
- Upstream router will send multicasts

# Transport Layer Protocols

- **Port numbers**

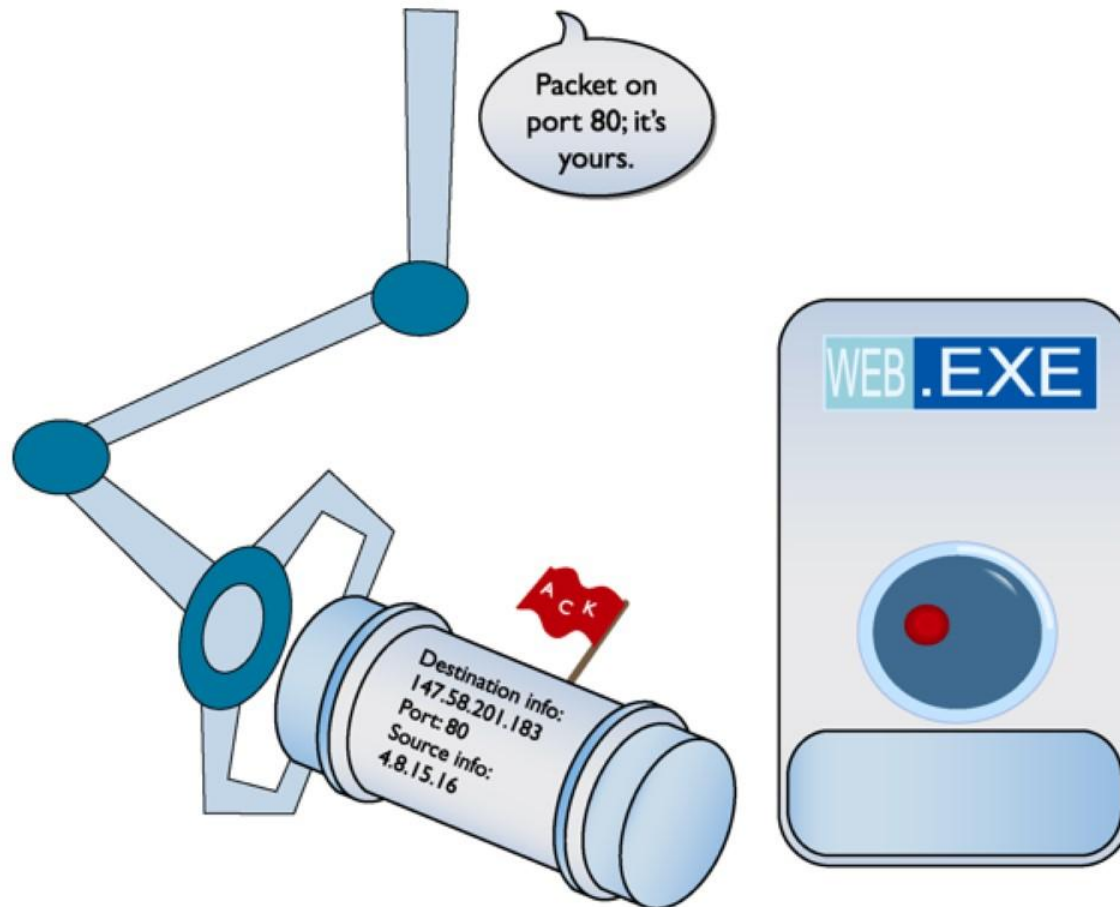
- Memorize common port numbers
- Every TCP/IP app requires a server and a client
- Defined port number for popular (well-known) TCP/IP applications



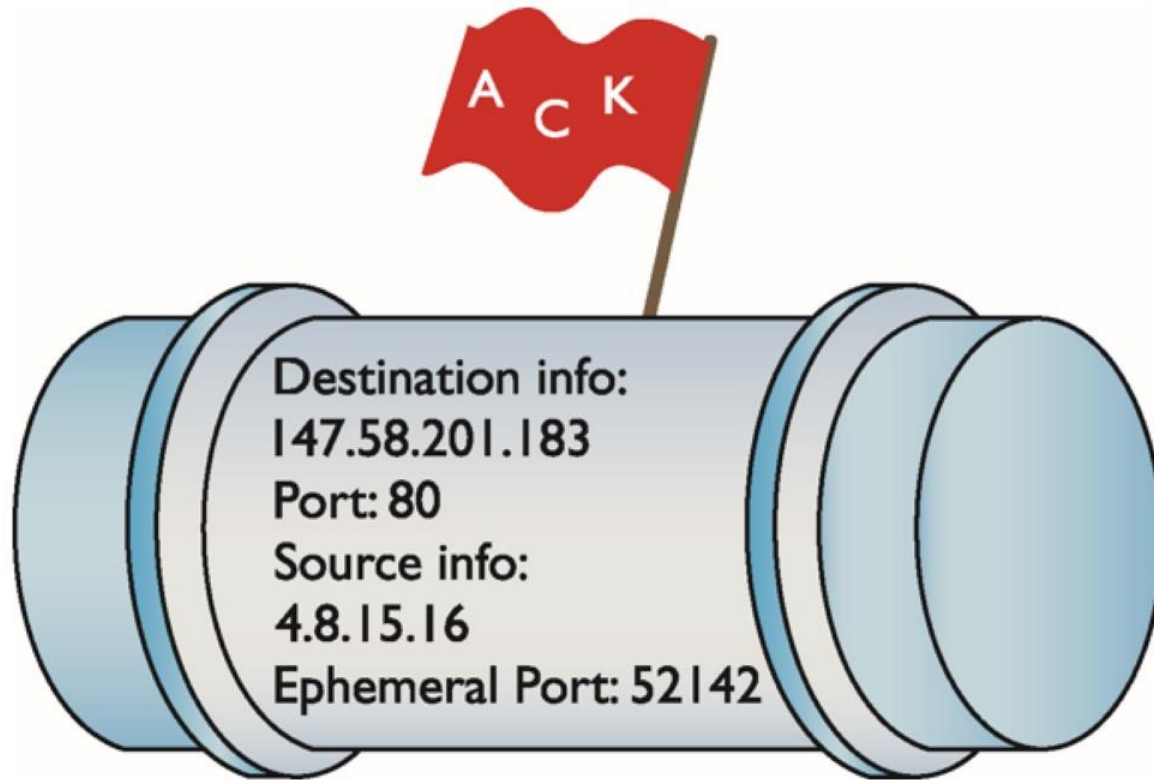
- **By the (port) numbers**
  - 16-bit values (0 to 65,535)
  - **Well-known port numbers (0-1023)** for specific TCP/IP applications
  - Web servers use port number 80
  - Web client sends HTTP ACT to server (port 80)
  - Server replies using ephemeral port



**Figure 9.6** HTTP ACK packet



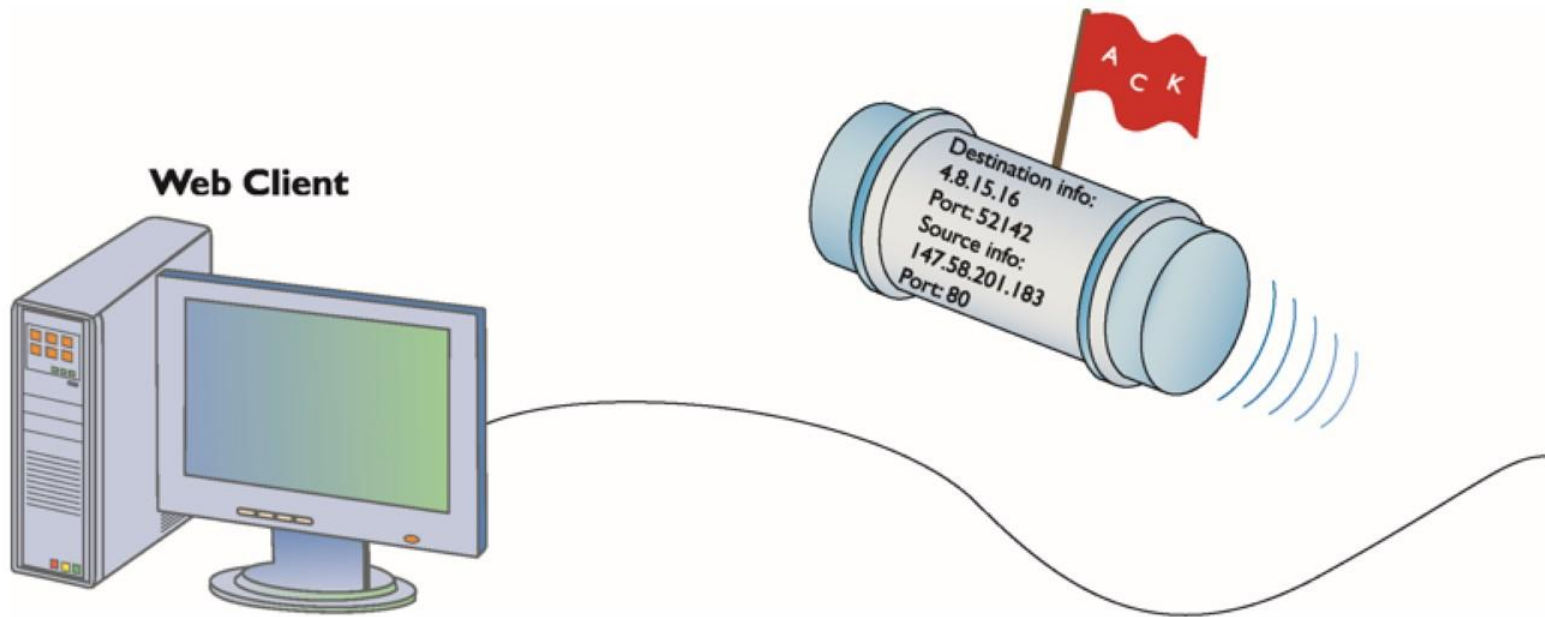
**Figure 9.7** Dealing with the incoming packet



**Figure 9.8** A more complete IP packet

- **Ephemeral ports**

- Pseudo-randomly generated by Web client
- **Ephemeral port numbers 1024-5000**
- **Dynamic or private port numbers 49152-65535**
- IANA recommends using only 49152-65535



**Figure 9.9** Returning the packet

- **Registered ports**

- 1024-49151

- Less-common TCP/IP applications register their ports with IANA

- Most operating systems avoid registered port numbers and use dynamic/private ports

- **Summary of port numbers**

- **0-1023**                      **well-known ports**
- **1024-49151**                **registered ports**
- **49152-65535**               **dynamic or private ports**



- **Using ports in a session**

- **Both computers keep track of status**

- Status info held in RAM
    - **Socket** or **endpoint** is one side's session information
    - **Socket pairs** or **endpoints** refer to data each computer stores about the connection
    - Session or **connection** refers to a connection in general

- **Endpoint information**

- Source and destination for one session

- Many simultaneous sessions

- Use `netstat -n` to see sessions

- Usually shows many connections

- TCPView for Windows: dynamic

- Net Activity Viewer for Linux



**Figure 9.10 Two open windows**

Protocol	Local Address	Remote Address	State
TCP	192.168.4.49:139	0.0.0.0	LISTENING
TCP	192.168.4.49:49202	192.168.4.10:445	ESTABLISHED
TCP	192.168.4.49:49388	66.163.181.173:5050	ESTABLISHED
TCP	192.168.4.49:49389	209.85.163.125:5222	ESTABLISHED
TCP	192.168.4.49:49390	209.85.163.125:5222	ESTABLISHED
TCP	192.168.4.49:49393	64.12.28.180:5190	ESTABLISHED
TCP	192.168.4.49:49394	207.46.107.108:1863	ESTABLISHED
TCP	192.168.4.49:49396	205.188.248.161:5190	ESTABLISHED
TCP	192.168.4.49:50991	192.168.4.9:445	ESTABLISHED
TCP	192.168.4.49:51238	206.71.145.10:8004	ESTABLISHED
TCP	192.168.80.1:139	0.0.0.0	LISTENING
TCP	192.168.136.1:139	0.0.0.0	LISTENING
TCP	192.168.4.49:51270	216.34.181.46:80	ESTABLISHED
TCP	192.168.4.49:51271	216.34.181.46:80	ESTABLISHED
TCP	192.168.4.49:51272	216.34.181.46:80	ESTABLISHED
TCP	192.168.4.49:51273	216.34.181.46:80	ESTABLISHED
TCP	192.168.4.49:51274	216.34.181.46:80	ESTABLISHED
TCP	192.168.4.49:51276	216.34.181.46:80	ESTABLISHED
TCP	192.168.4.49:51277	216.34.181.46:80	ESTABLISHED
UDP	0.0.0.0:123	**	
UDP	0.0.0.0:500	**	
UDP	0.0.0.0:3702	**	
UDP	0.0.0.0:3702	**	
UDP	0.0.0.0:4500	**	
UDP	0.0.0.0:5355	**	
UDP	0.0.0.0:53475	**	
UDP	0.0.0.0:53885	**	
UDP	0.0.0.0:53887	**	
UDP	0.0.0.0:65513	**	
UDP	127.0.0.1:1900	**	
UDP	127.0.0.1:53869	**	
UDP	127.0.0.1:53870	**	
UDP	127.0.0.1:53880	**	
UDP	127.0.0.1:53882	**	
UDP	127.0.0.1:53897	**	
UDP	127.0.0.1:53898	**	
UDP	127.0.0.1:55068	**	
UDP	127.0.0.1:55069	**	
UDP	127.0.0.1:57388	**	

**Figure 9.11 TCPView in action**

Protocol	Local Port	State	Remote Address	Remote Port	Remote Host	Pid	Program	
tcp	901	swat	LISTEN	*	*	.		
tcp	27015	LISTEN	*	*	.	6133	srcds_i486	
tcp	3306	mysql	LISTEN	*	*	.		
tcp	139	netbios-ssn	LISTEN	*	*	.		
tcp	10000	webmin	LISTEN	*	*	.		
tcp	80	www	LISTEN	*	*	.		
tcp	22	ssh	LISTEN	*	*	.		
tcp	631	ipp	LISTEN	*	*	.		
tcp	445	microsoft-ds	LISTEN	*	*	.		
tcp	58694	ESTABLISHED	91.189.94.9	80	www	avocado.canonical.com	8485	firefox
tcp	42787	CLOSED	91.189.90.19	80	www	yangmei.canonical.com	8485	firefox
tcp	38186	CLOSED	91.189.90.19	443	https	yangmei.canonical.com	8485	firefox
tcp	38191	CLOSED	91.189.90.19	443	https	yangmei.canonical.com	8485	firefox
tcp	38189	CLOSED	91.189.90.19	443	https	yangmei.canonical.com	8485	firefox
tcp	38192	CLOSED	91.189.90.19	443	https	yangmei.canonical.com	8485	firefox
tcp	38188	CLOSED	91.189.90.19	443	https	yangmei.canonical.com	8485	firefox
tcp	43699	CLOSED	209.85.225.97	443	https	iy-in-f97.google.com	8485	firefox
tcp	38190	CLOSED	91.189.90.19	443	https	yangmei.canonical.com	8485	firefox
tcp6	5900	LISTEN	*	*	.	7066	vino-server	
tcp6	22	ssh	LISTEN	*	*	.		
udp	27015		*	*	.	6133	srcds_i486	
udp	137	netbios-ns	*	*	.			
udp	137	netbios-ns	*	*	.			
udp	138	netbios-dgm	*	*	.			
udp	138	netbios-dam	*	*	.			

Established: 1/23 Sent: 23 KB +645 B/s Received: 91 KB +315 B/s

**Figure 9.12 Net Activity Viewer**

- **Connection Status**

- State changes continually
- **Listening port or open port**
- ESTABLISHED ports are active, working endpoint pairs
- CLOSE\_WAIT indicates that a client is making a graceful closure
- TIME\_WAIT indicates a lost connection

- **Detecting local program in a connection**
  - `Netstat -ano` will show local process ID (PID) for each connection

**Figure 9.13** Process Explorer

Process	PID	CPU	Description	Company Name
taskeng.exe	2016		Task Scheduler Engine	Microsoft Corporation
nlsvc.exe	2044		NetLimiter 2 service	Locktime Software
svchost.exe	2076		Host Process for Windows S...	Microsoft Corporation
nessusd.exe	2132		nessusd.exe	Tenable Network Security
LVPicSrv.exe	2156		Logitech LVPicSrv Module	Logitech Inc.
vmount2.exe	2216		virtual disk mount service	VMware, Inc.
vmnat.exe	2260		VMware NAT Service	VMware, Inc.
svchost.exe	2324		Host Process for Windows S...	Microsoft Corporation
SearchIndexer.exe	2360		Microsoft Windows Search I...	Microsoft Corporation
vmware-authd.exe	2404	0.78	VMware Authorization Service	VMware, Inc.
vmnetdhcp.exe	2484		VMware VMnet DHCP service	VMware, Inc.
svchost.exe	2840		Host Process for Windows S...	Microsoft Corporation
pcosystray.exe	3116		PowerChute System Tray Po...	American Power Conversio...
soffice.exe	3184		OpenOffice.org 2.3	OpenOffice.org
taskeng.exe	3188		Task Scheduler Engine	Microsoft Corporation
dm.exe	3376		Desktop Window Manager	Microsoft Corporation
explorer.exe	3460		Windows Explorer	Microsoft Corporation
MSASCui.exe	3536		Windows Defender User Inte...	Microsoft Corporation
juched.exe	3556		Java(TM) Platform SE binar...	Sun Microsystems, Inc.
wmdc.exe	3572		Windows Mobile Device Cen...	Microsoft Corporation
vmware-tray.exe	3580		VMware Tray Process	VMware, Inc.
hqtray.exe	3588		VMware Host Network Acce...	VMware, Inc.
CTHELPER.EXE	3660		DHelper Application	Creative Technology Ltd
IAAnotif.exe	3676		Event Monitor User Notificati...	Intel Corporation
MDM.exe	3792		Catalyst Control Center: Moni...	Advanced Micro Devices I...
iTunesHelper.exe	3800		iTunesHelper Module	Apple Inc.
ig.exe	3924			Grunding
PodService.exe	4172		PodService Module	Apple Inc.
CCC.exe	4320		Catalyst Control Centre: Host...	ATI Technologies Inc.
wuauclt.exe	4992		Windows Update Automatic ...	Microsoft Corporation
LVCComSer.exe	5368		Logitech Video CDM Service	Logitech Inc.
GoogleUpdate.exe	14324		Google Installer	Google Inc.
WUDFHost.exe	9892		Windows Driver Foundation ...	Microsoft Corporation
AppleMobileDeviceService.exe	100156		Apple Mobile Device Service	Apple Inc.
WINWORD.EXE	102028		Microsoft Word for Windows	Microsoft Corporation
taskmgr.exe	105244		Windows Task Manager	Microsoft Corporation
xnview.exe	109760		XnView for Windows	XnView, http://www.xnview...
Tcpview.exe	110876	14.78	TCPView	Sysinternals
ShareEnum.exe	110976			
SearchProtocolHost.exe	111112		Microsoft Windows Search P...	Microsoft Corporation
vmware-vmx.exe	111304		VMware Workstation/VMX	VMware, Inc.
SearchFilterHost.exe	111328		Microsoft Windows Search F...	Microsoft Corporation
vmware.exe	111468		VMware Workstation	VMware, Inc.
cmd.exe	111656		Windows Command Processor	Microsoft Corporation
procexp.exe	111988	0.78	Sysinternals Process Explorer	Sysinternals - www.sysinter...
firefox.exe	112092		Firefox	Mozilla Corporation

CPU Usage: 16.33% Commit Charge: 33.68% Processes: 82



- **Determining Good vs. Bad**

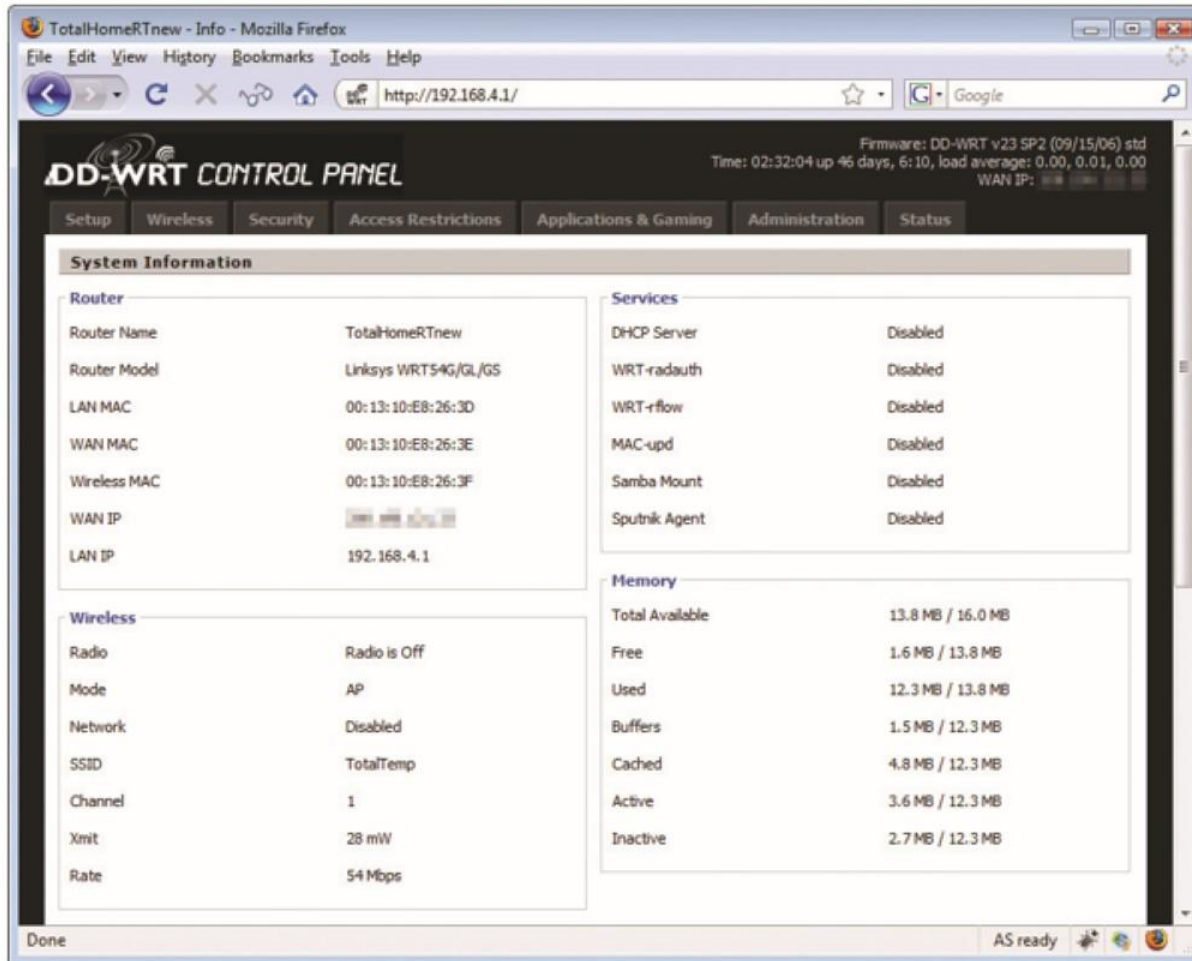
- Memorize a bunch of common ports
- Learn how to use NETSTAT
- Learn the ports that normally run on your operating system
- Research processes you don't recognize
- Get rid of bad processes

# **Common TCP/IP Applications**

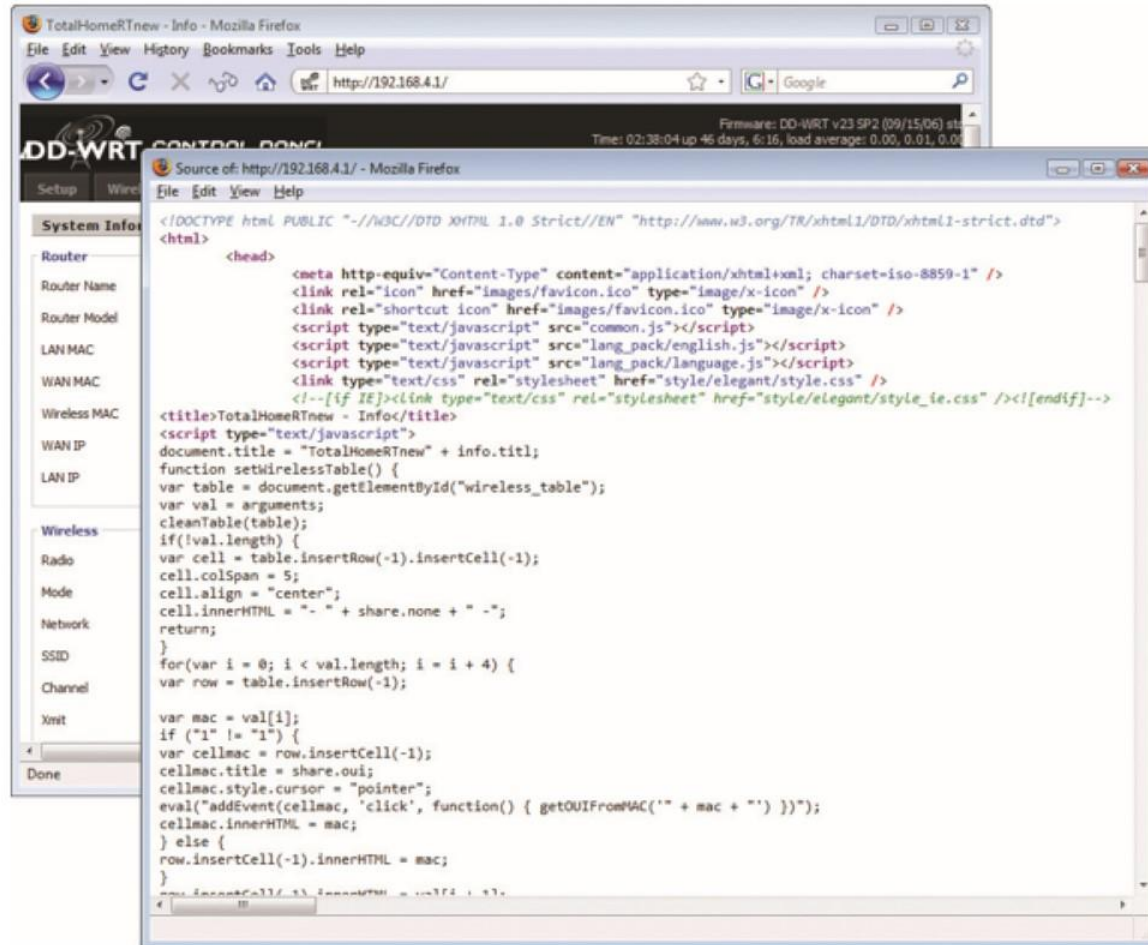
- **Web Servers**

- Store HTML documents

- XHTML is an updated HTML with XML syntax



**Figure 9.14** My router's Web page



**Figure 9.15** XHTML source code

- **Web browsers (client side)**

- Request HTML pages from Web servers
- Enter address into browser
- All browsers have a default Web page
- Web sites use text addresses using DNS

- **HTTP**

- Stands for **Hypertext Transport Protocol**
- Underlying protocol of the Web
- Uses port 80 to transmit Web page data
- **http://** at beginning of Web server address

- **HTTP weakness**

- Relays commands without reference to any commands the user previously executed
- Difficult to design complex and interactive Web pages
- Other technologies enhance HTTP
  - JavaScript/AJAX
  - Server-side scripting
  - Adobe Flash
  - Cookies



- **Publishing Web pages**

- **Web server will “host” a HTML document**

- **You can self-host**

- Install Web server software

- Acquire a public IP address

- Time-consuming and challenging

- **Host through your ISP**

- **Use a Web hosting service company**

- **Free Web hosting (nothing is free)**

- **Web Servers and Web Clients**
  - Web server serves up Web pages
  - Listens on port 80
  - Fetches and sends requested HTML pages
  - To create a Web server
    - Install Web server software
    - Connect computer to the Web

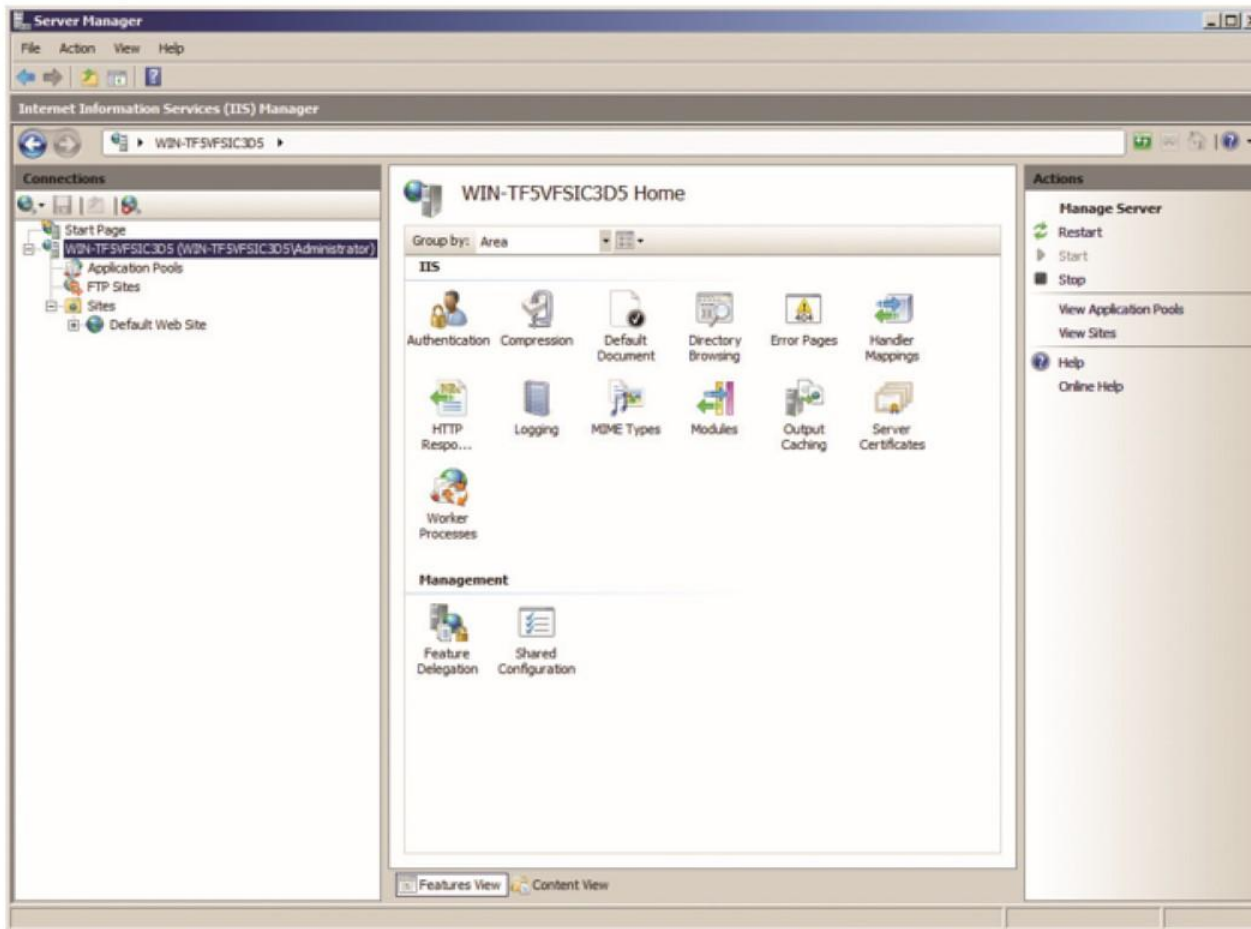
- **Web Server Software**

- **Microsoft Internet Information Services (IIS)**

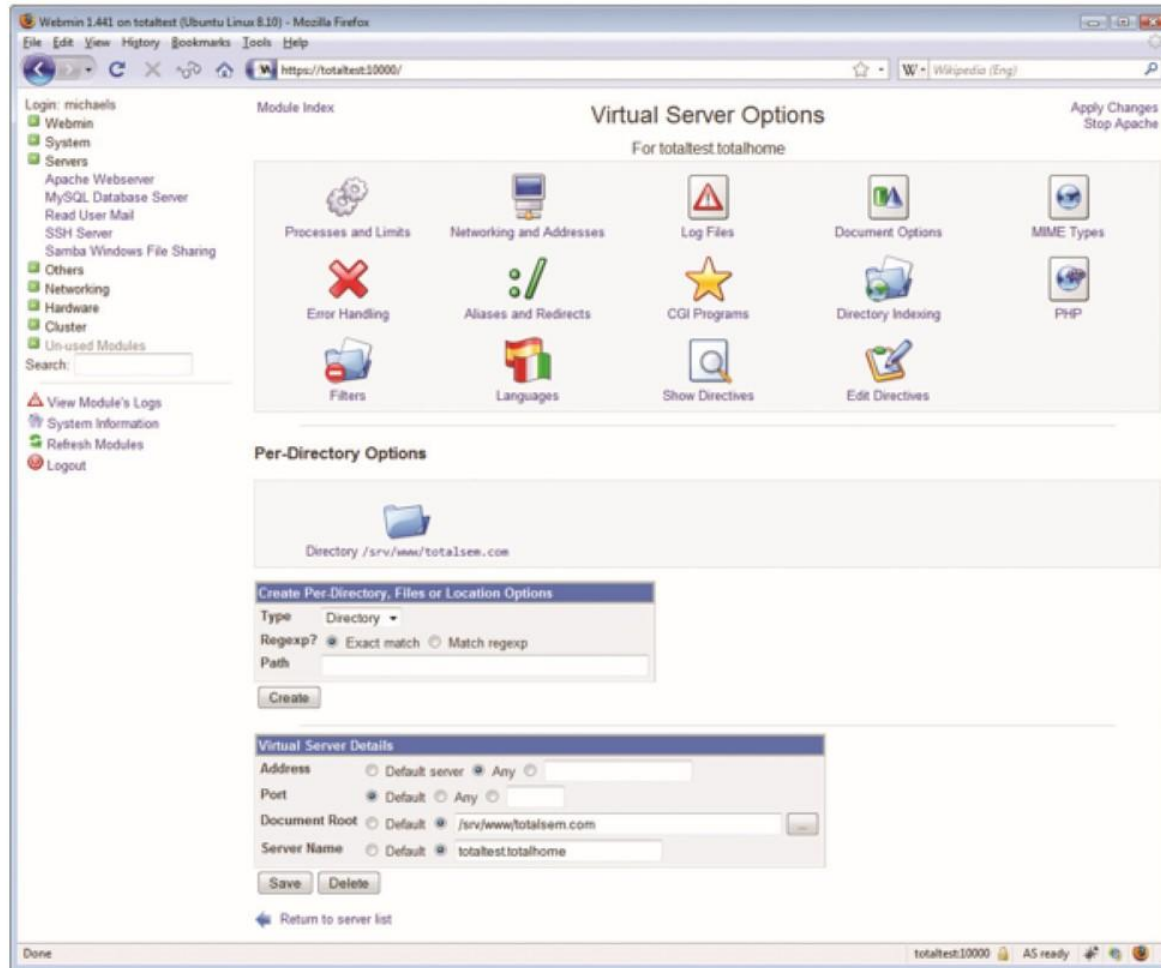
- 20-connection limit on non-server versions of Windows
    - Only run IIS on Server versions of Windows

- **Apache Server runs on UNIX/Linux/Windows**

- On over 50% of Internet Web servers
    - Free
    - Non-GUI
    - Web administrators use an add-on GUI (Webmin)



**Figure 9.16 IIS in action**



**Figure 9.17** Webmin Apache module

- **Web Client Software (browsers)**

- Request and display Web pages

- Many have multiple functions

- Most popular

- MS Internet Explorer (IE)

- Mozilla Firefox

- Apple Safari

- Opera

- Google Chrome

- **Secure Sockets Layer and HTTPS**
  - **HTTP not secure**
  - **Requirements for secure Internet apps**
    - Authentication
    - Encryption
    - Nonrepudiation
  - **SSL and HTTPS offer security**

- **Secure Sockets Layer (SSL)**

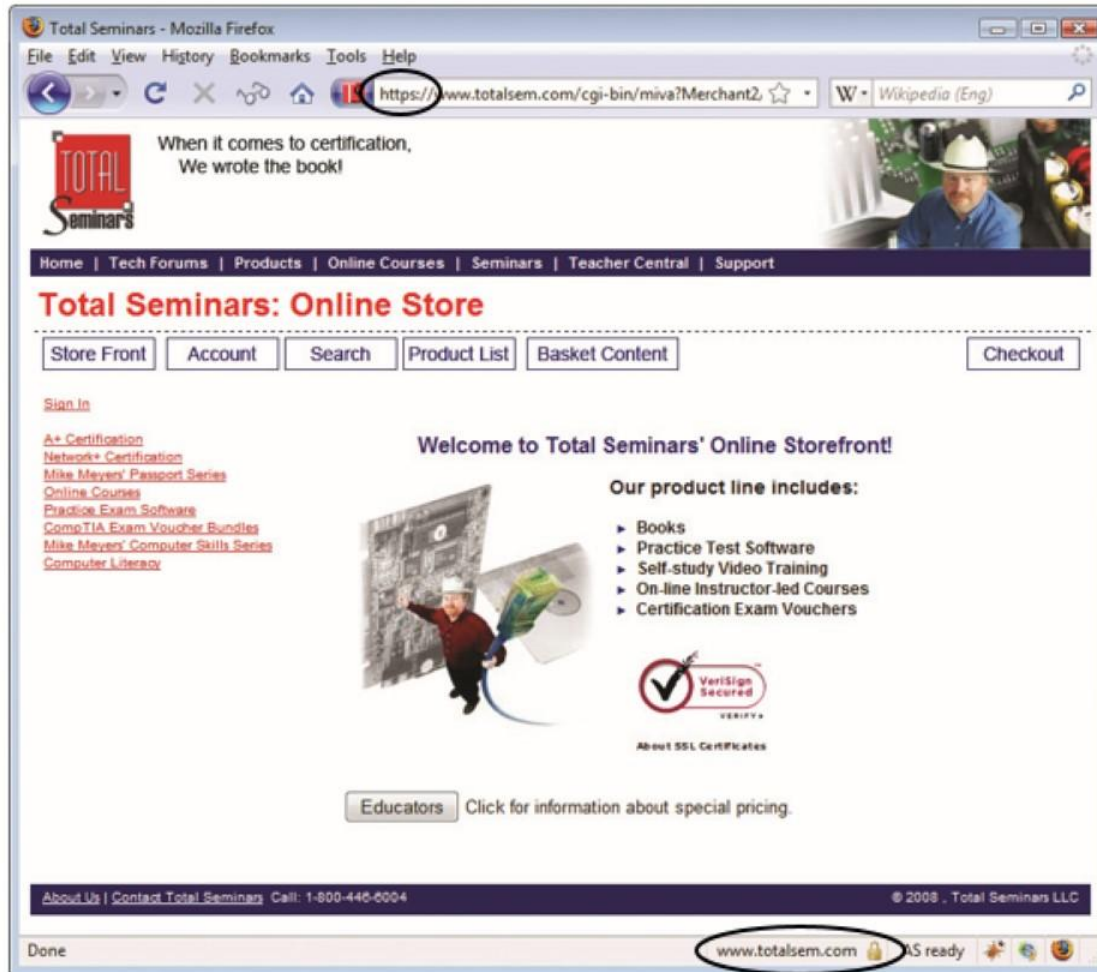
- Netscape-developed protocol
- Encrypts data with a public key
- Sends encrypted data over an SSL connection
- Data decrypted on receiving end with private key
- Supported by Web browsers and servers
- Many Web sites use SSL for confidential data
- Look for HTTPS or small lock in browser



- **HTTP over SSL**

- Uses TCP port 443

- Being replaced by Transport Layer Security (TLS)



**Figure 9.18 Secure Web Page**

- **Telnet**

- First networks were dumb terminals connected to more than one mainframe
- Run commands as if sitting at the mainframe
- Still exists as a way to connect remotely
- Uses port 23
- Used to administer servers
- Requires log on with user name and password

```

Telnet 192.168.4.85
Ubuntu 8.04.1
UMubuntu login: vmuser
Password:
Last login: Mon Nov 10 11:30:01 CST 2008 from michael.s.totalhome on pts/1
Linux UMubuntu 2.6.24-19-generic #1 SMP Fri Jul 11 23:41:49 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
vmuser@UMubuntu:~$ _
```

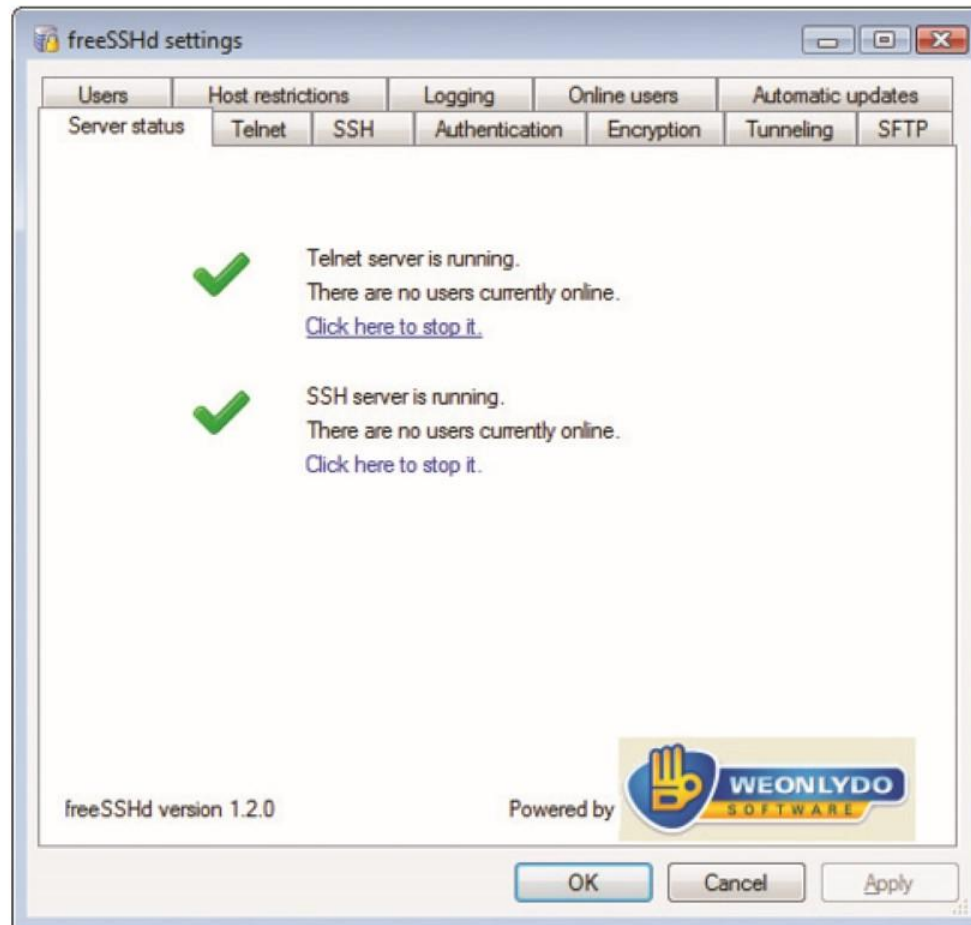
**Figure 9.20** Telnet client

- **Telnet (cont.)**

- Has no form of encryption
- Rarely used on the Internet
- Replaced by **Secure Shell (SSH)**, which has encryption
- Telnet still used on trusted networks
- Most routers support Telnet (often turned off for security)

- **Telnet (cont.)**

- Most OSs have built-in Telnet clients and servers
- Most servers allow access using Telnet
- Third-party clients and servers have more features



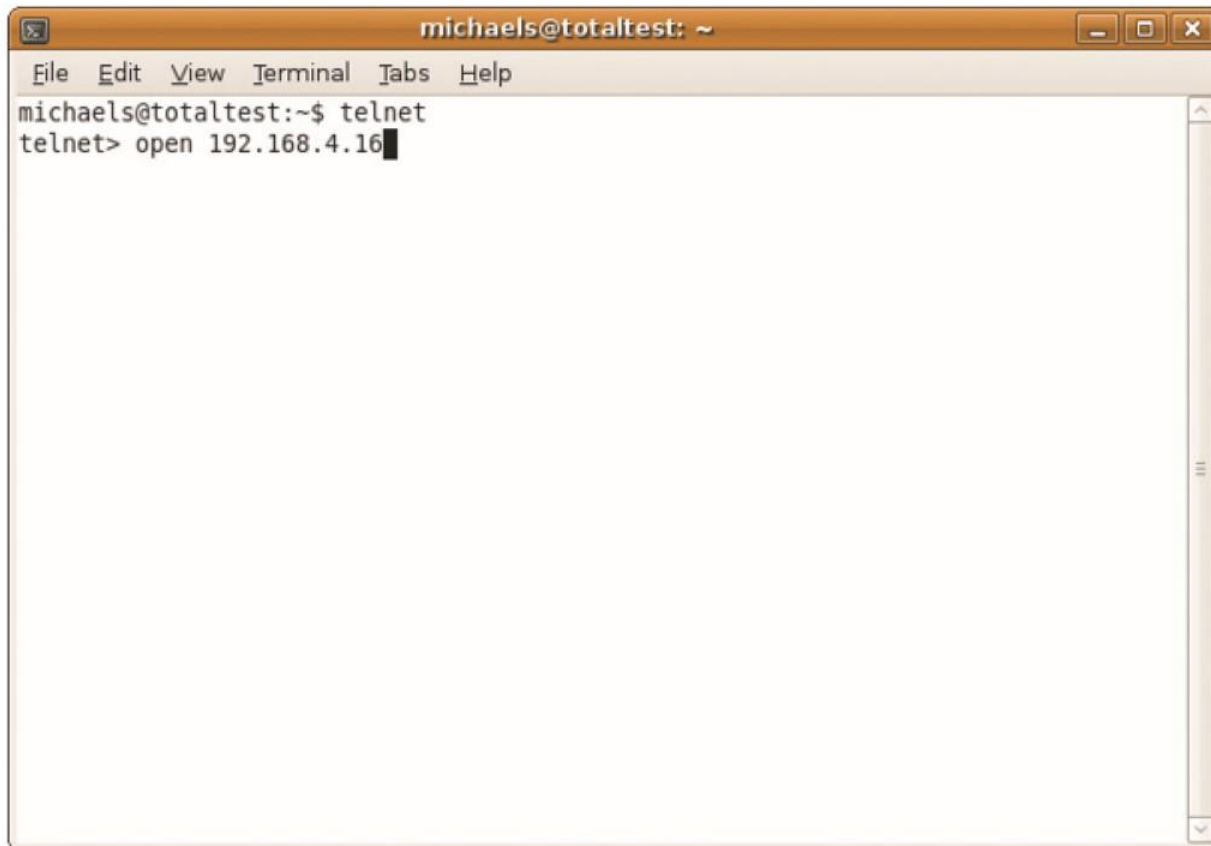
**Figure 9.21 freeSSHd**

- **Telnet (cont.)**

- **Configuring a Telnet client**

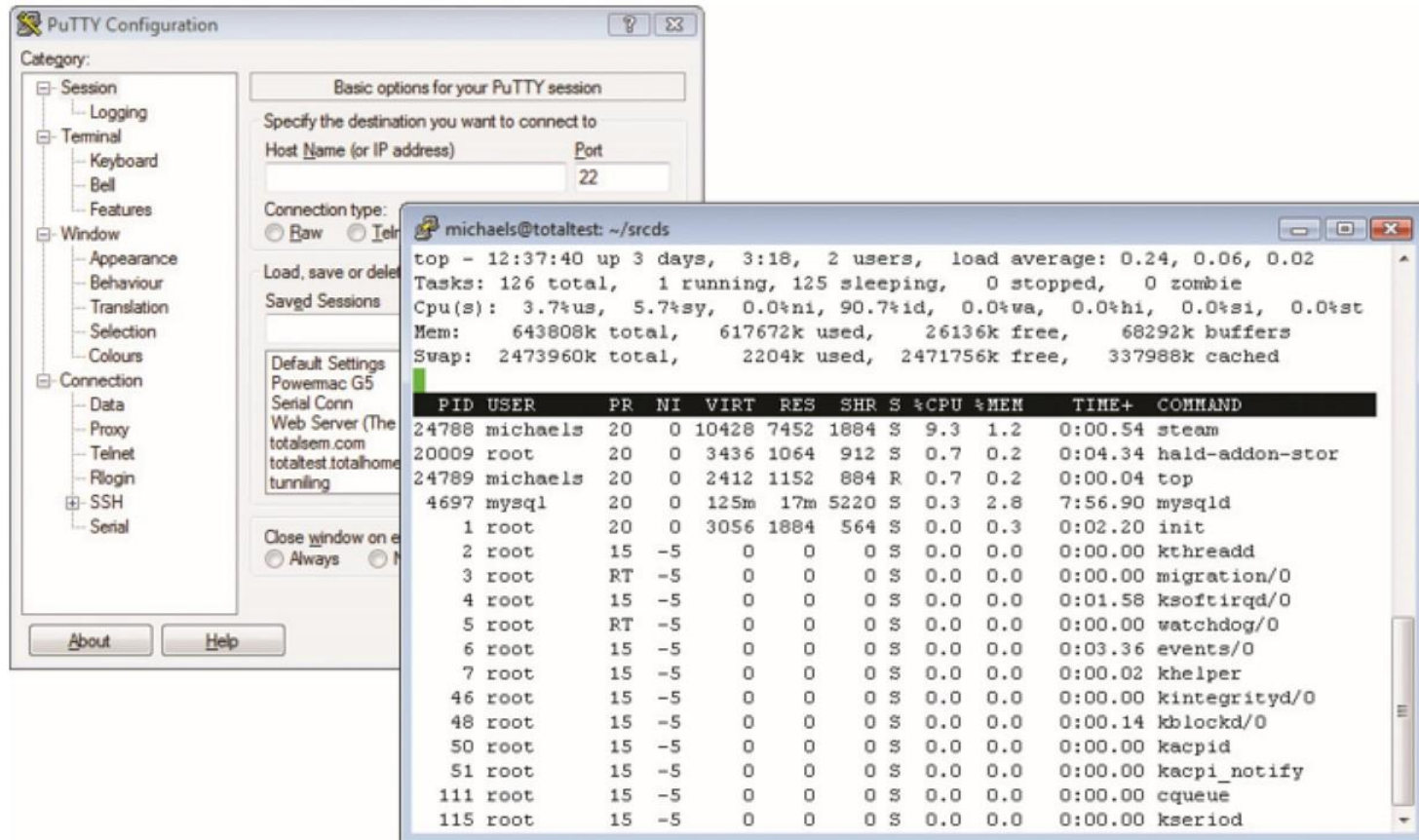
- Host name (name or IP address)
    - User login name
    - Password



A terminal window titled "michaels@totaltest: ~" with a menu bar containing "File", "Edit", "View", "Terminal", "Tabs", and "Help". The terminal content shows the user running "telnet" and then "telnet> open 192.168.4.16".

```
michaels@totaltest: ~  
File Edit View Terminal Tabs Help  
michaels@totaltest:~$ telnet  
telnet> open 192.168.4.16
```

**Figure 9.22** Ubuntu Telnet



**Figure 9.23 PuTTY**

- **Rlogin, RSH, and RCP**

- **Old UNIX remote programs**

- **Remote access and control of servers**

- **No encryption**

- **Do not use across the Internet**

- Rlogin – interactive, automatic login, TCP port 513

- RSH – non-interactive, sends a single command to server, use in scripts, TCP port 514

- RCP – copy files, use in scripts, shares TCP port 514 with RSH

- **SSH and the Death of Telnet**

- Has replaced Telnet

- Encrypts data

- Creates a terminal connection to remote host

- TCP port 22

- **Electronic mail (e-mail)**

- Major contributor to Internet revolution
- Streamlined junk mail industry
- Provides quick way for people to communicate
- Sends messages and attachments
- Normally offered free by ISPs
- Most e-mail clients have simple text editors

- **Electronic mail (e-mail)**

- Messages stored on e-mail server
- Most e-mail clients notify you when new message arrives or automatically download
- You manage messages (forward, delete, etc.)
- Most clients delete downloaded messages
- E-mail programs use application-level protocols

- **Simple Mail Transfer Protocol (SMTP)**
  - Used by clients to send e-mail
  - TCP port 25

- **Post Office Protocol version 3 (POP3)**
  - Clients use to retrieve e-mail from SMTP servers
  - TCP port 110
  - Used by most e-mail clients



- **Internet Message Access Protocol version 4 (IMAP4)**

- **Alternative to POP#**

- **Retrieves e-mail from an e-mail server**

- **TCP port 143**

- **Supports features not supported by POP3**

- Search messages by keyword

- Select messages before download

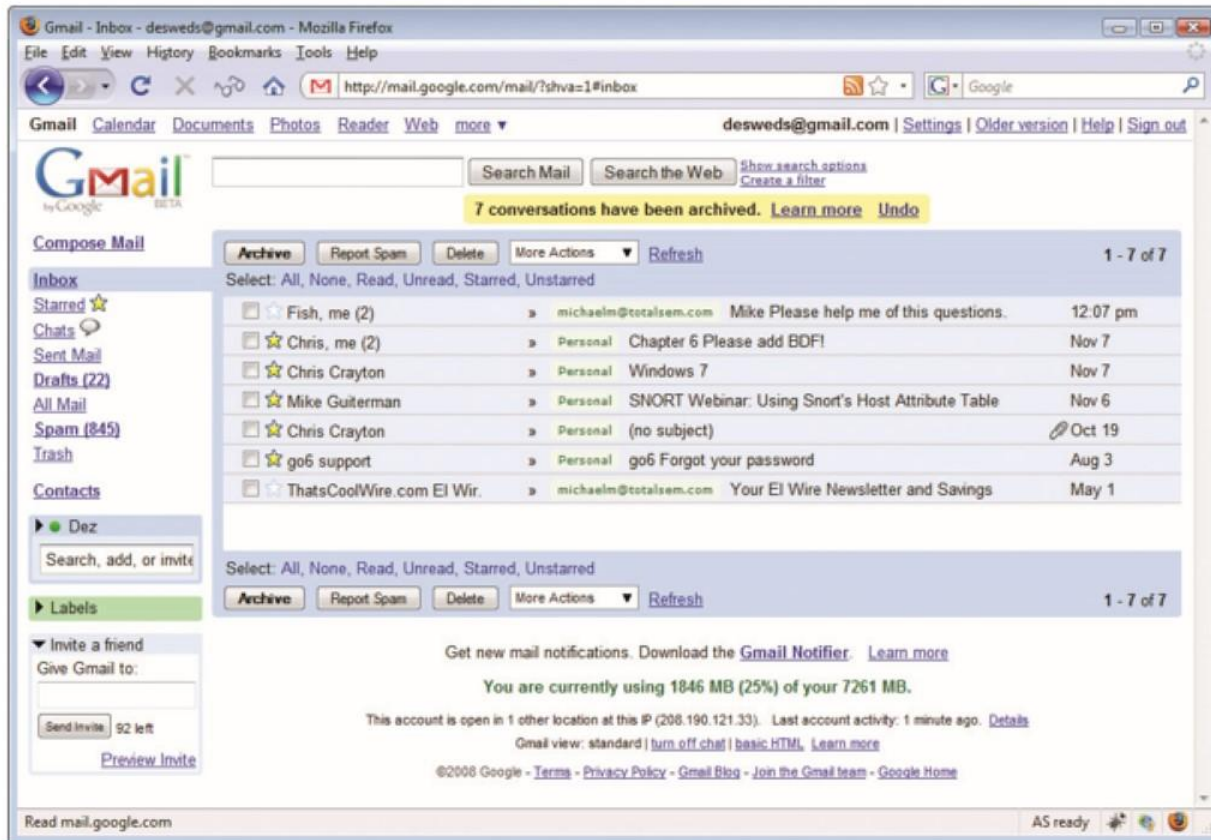
- Supports folders on IMAP4 servers

- **Alternatives to SMTP, POP3, and IMAP4**

- **Web-based e-mail**

- Access your e-mail from anywhere
    - Free
    - Handy for throw-away accounts
    - Do not confuse with Web-based e-mail services provided by traditional SMTP/POP/IMAP accounts

- **Proprietary solutions**



**Figure 9.24 Gmail in action**

- **E-mail Server software**

- **E-mail server market fragmented**

- **Sendmail for UNIX/Linux is leader (SMTP only)**

- No GUI interface

- Third-part interfaces (Webmin)

- Controls about 20% of e-mail servers

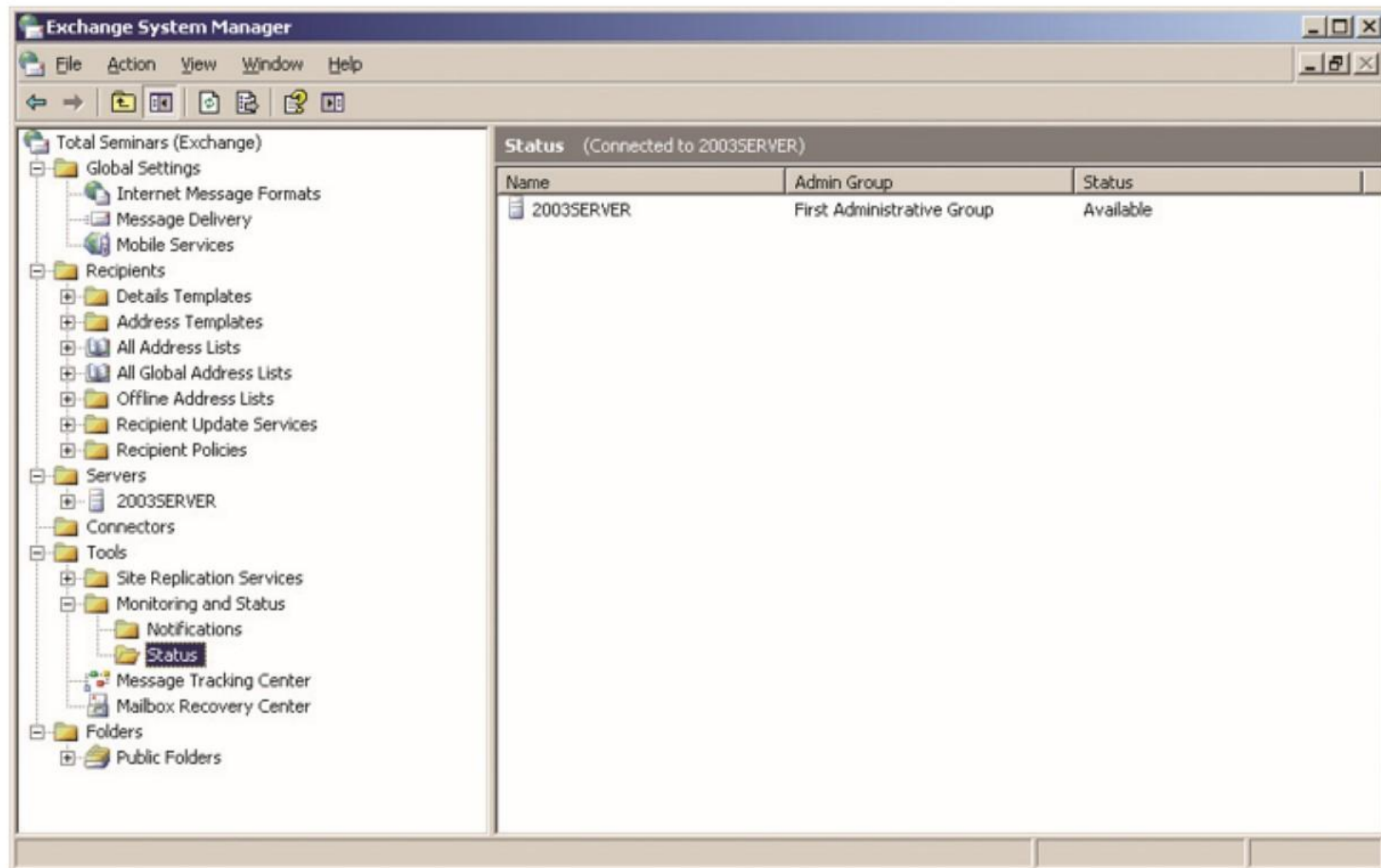
- Must use a POP3 or IMAP server program to support e-mail clients

- **Eudora's Qpopper sends mail to POP3 e-mail clients**



**Figure 9.25** Webmin with the sendmail module

- **E-mail Server software (cont.)**
  - MS Exchange Server (both SMTP and POP3)
  - **Mailboxes** are holding areas on server for each user's messages
  - Server arranges incoming messages
  - Server returns messages with unknown recipient
  - Difficult to manage

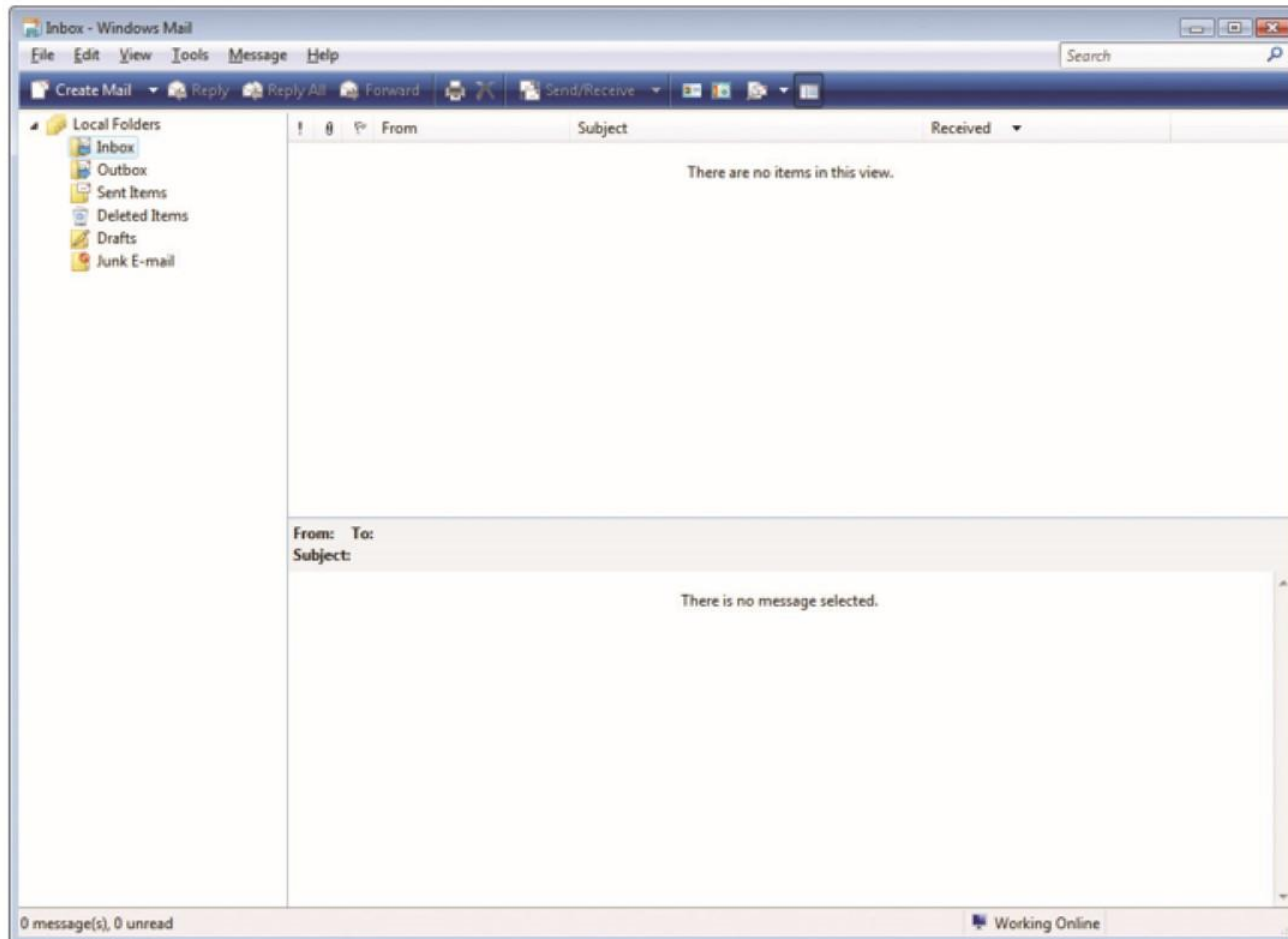


**Figure 9.26** Microsoft Exchange Server

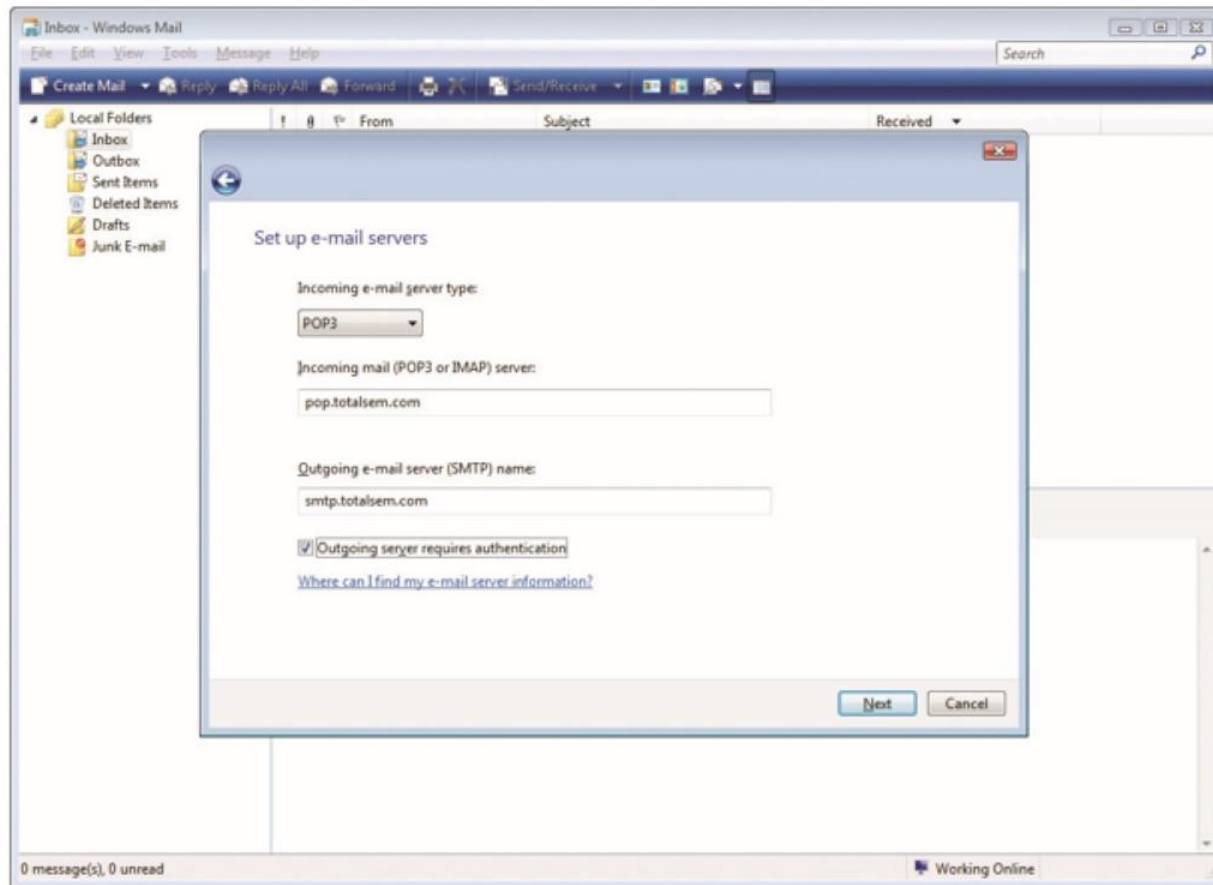
- **E-mail Client Software**

- Enables you to send, receive, and organize
- Communicates with SMTP server to send
- Communicates with IMAP or POP3 server to download messages
- **Hundreds of e-mail client programs**
  - Microsoft Windows Mail
  - Microsoft Outlook
  - Mozilla Thunderbird
  - Qualcomm Eudora





**Figure 9.27** Windows Mail



**Figure 9.28** Entering server information in Windows Mail

- **Configuring E-mail Client Software**
  - Obtain server's address and your mailbox user name and password
  - Enter POP3 or IMAP4 server's IP address
  - Enter user name and password

- **File Transfer Protocol (FTP)**

- Original Internet file transfer protocol
- Faster and more reliable than HTTP
- Includes security and data integrity
- TCP ports 20 and 21
- Anonymous or secured sites
- Some are both

- **FTP Servers**

- **Store files**
- **Accept incoming connections**
- **Verify user names and passwords**
- **Transfer files**
- **Easy to set up an FTP server**
- **UNIX/Linux have built-in FTP servers**
- **Third-party servers better**

- **FTP Clients**

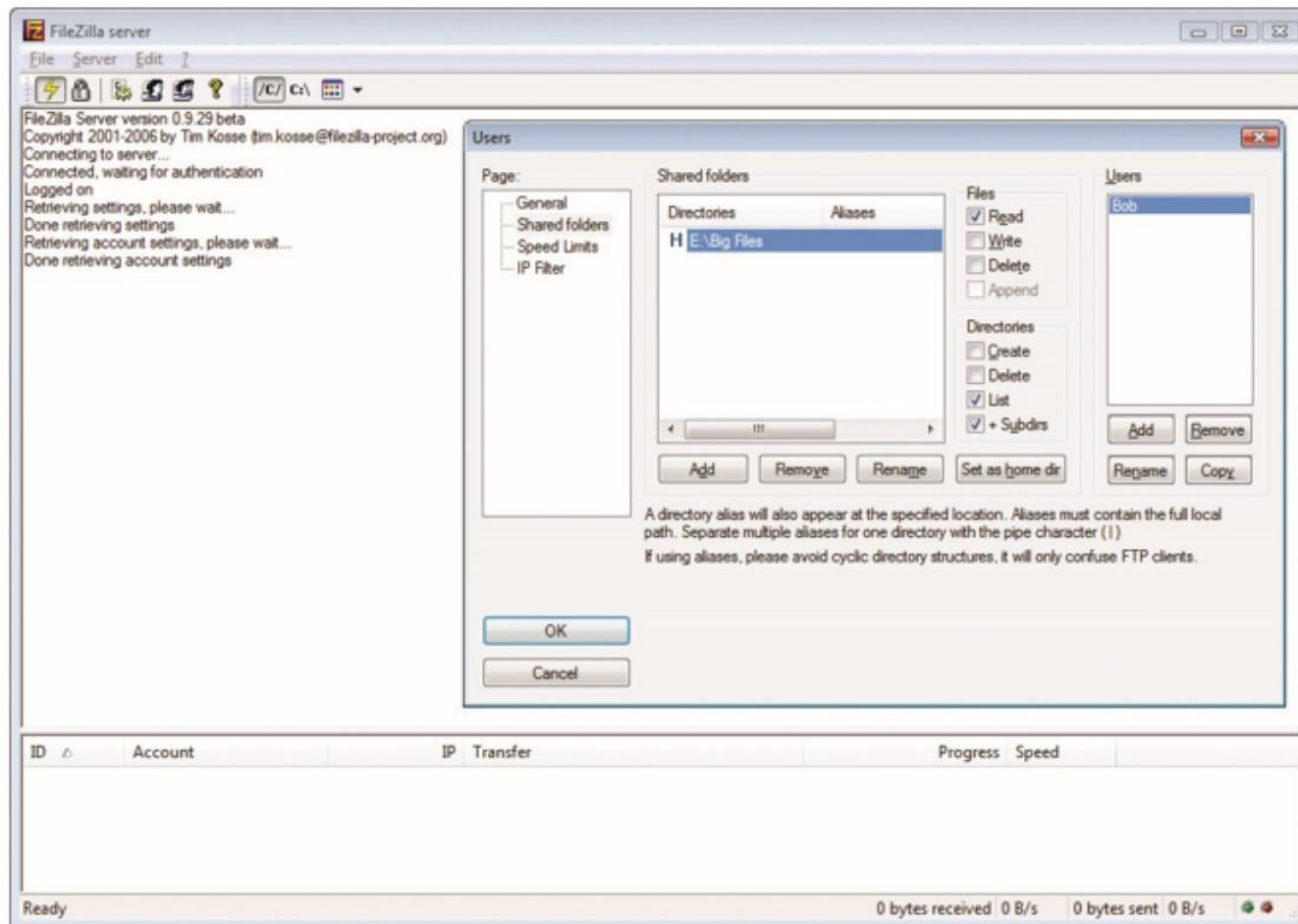
- **Access FTP servers many ways**

- Web site
    - Command line
    - FTP client applications

- **Most Web browsers support FTP, but lack features**

- **Dedicated FTP clients work best**

- FileZilla client
    - Mozilla FireFTP add-on to Firefox



**Figure 9.29 FileZilla Server**

- **Passive vs. Active FTP**

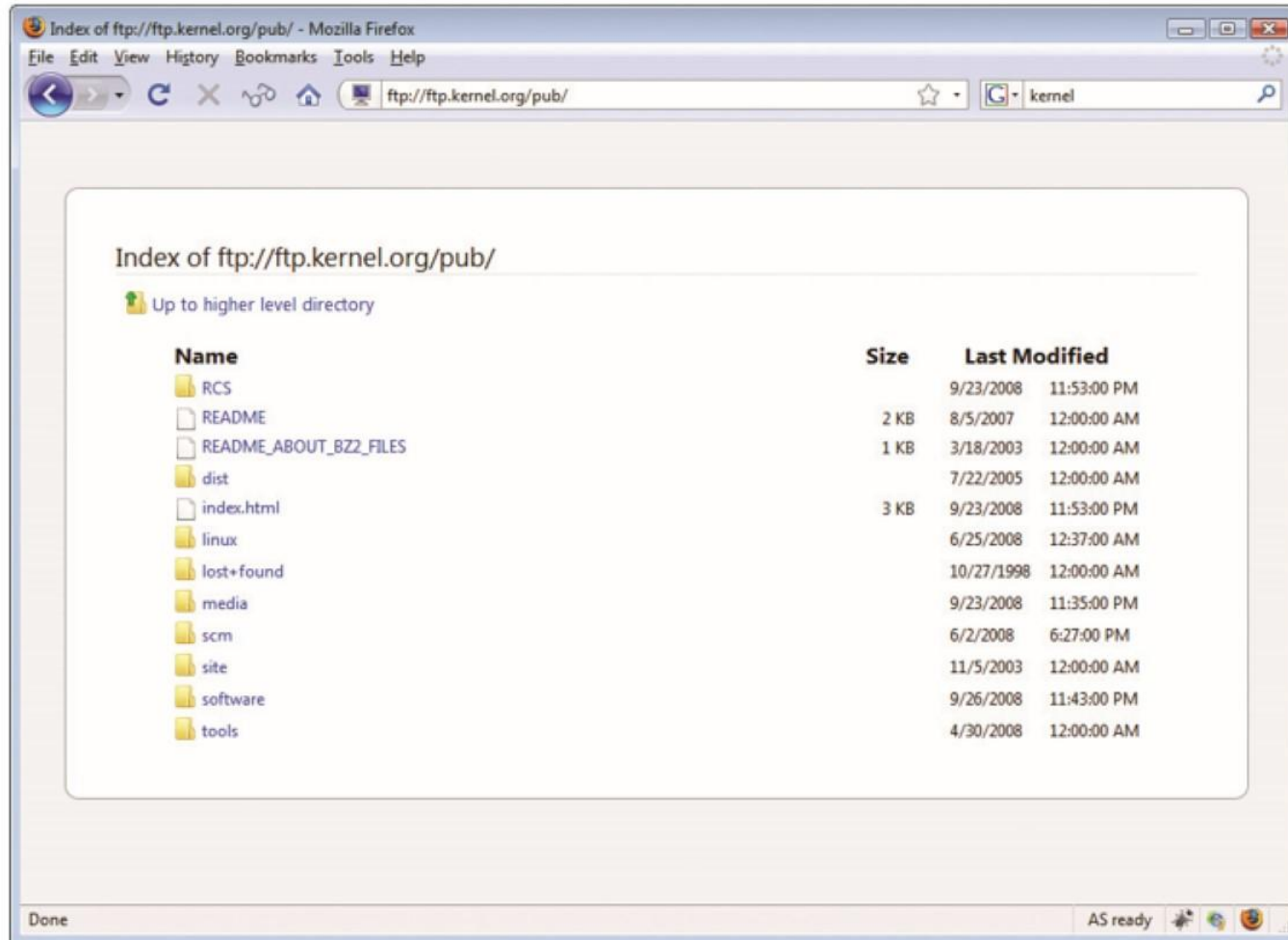
- **Traditional FTP uses active process**

- Clients send FTP request on TCP port 21
    - Server responds on an ephemeral destination port with TCP port 20 as the source port

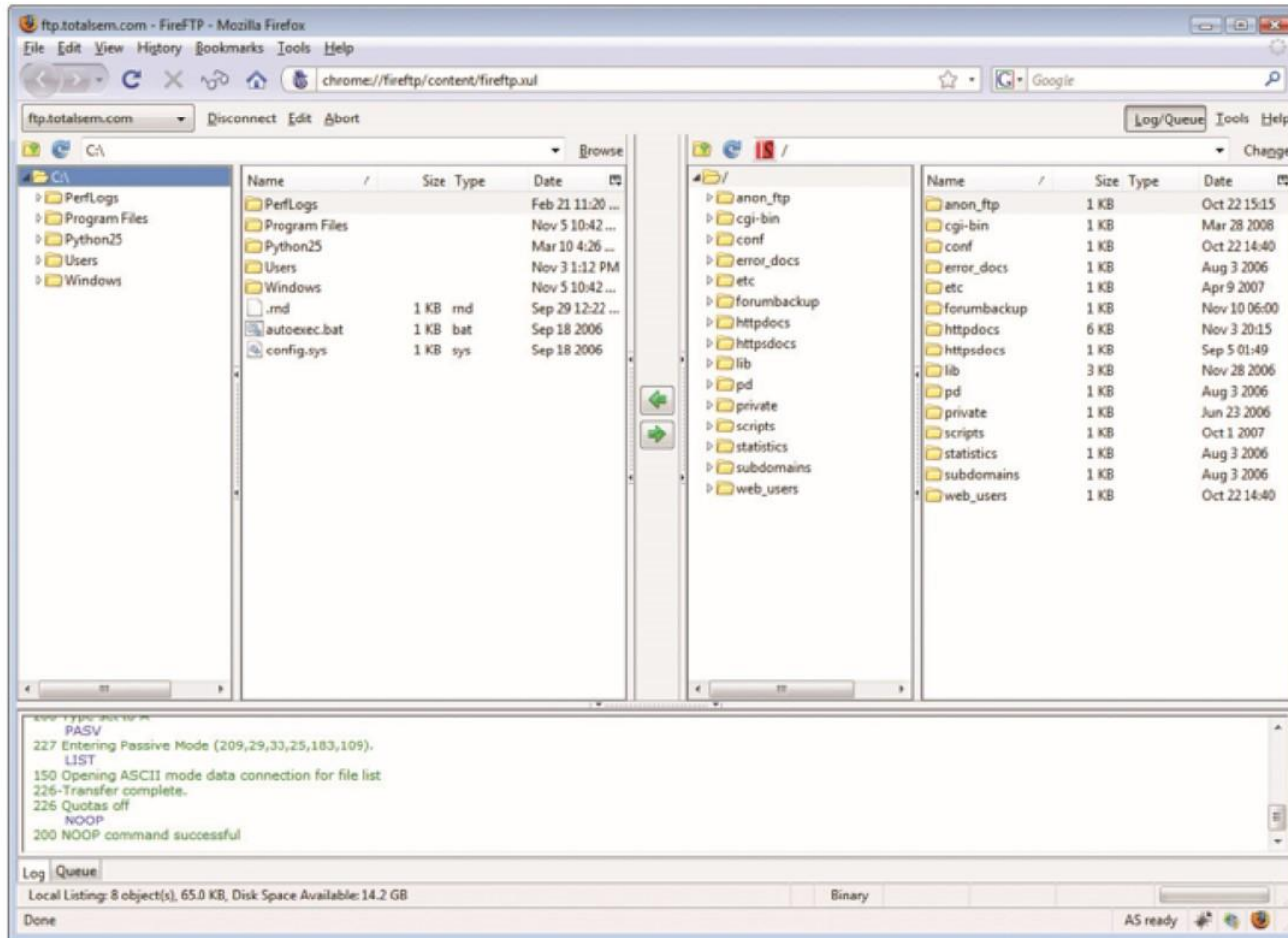
- **Passive FTP server doesn't use port 20**

- Works with NAT
    - Client must support passive FTP





**Figure 9.30** FTP in Web browser



**Figure 9.31** Author's FireFTP hard at work

## Internet Application Port Usage

Application	TCP/UDP	Port	Notes
HTTP	TCP	80	The Web
HTTPS	TCP	443	The Web, securely
Telnet	TCP	23	Terminal emulation
SSH	TCP	22	Secure terminal emulation
SMTP	TCP	25	Sending e-mail
POP3	TCP	110	E-mail delivery
IMAP4	TCP	143	E-mail delivery
FTP	TCP	20/21	File transfer
TFTP	UDP	69	File transfer