8.1.3 Common Ports

Network ports are logical connections, provided by the TCP or UDP protocols at the Transport layer, to be used by protocols in the upper layers of the OSI model. The TCP/IP protocol stack uses port numbers to determine what protocol incoming traffic should be directed to. Some characteristics of ports are listed below:

- Ports allow a single host with a single IP address to run network services. Each port number identifies a distinct service.
- Each host can have over 65,000 ports per IP address.
- Port use is regulated by the Internet Corporation for Assigned Names and Numbers (ICANN).

ICANN specifies the following three categories for ports:

- *Well known* ports range from 0 to 1023 and are assigned to common protocols and services.
- *Registered* ports range from 1024 to 49151 and are assigned by ICANN to a specific service.
- *Dynamic* (also called *private* or *high*) ports range from 49152 to 65535 and can be used by any service on an ad hoc basis. Ports are assigned when a session is established, and ports are released when the session ends.

The following table lists the well-known ports that correspond to common Internet services:

Port(s)	Service
20 TCP and UDP 21 TCP and UDP	File Transfer Protocol (FTP)
22 TCP and UDP	Secure Shell (SSH)
23 TCP	Telnet
25 TCP and UDP	Simple Mail Transfer Protocol (SMTP)
53 TCP and UDP	Domain Name Server (DNS)
67 TCP and UDP 68 TCP and UDP	Dynamic Host Configuration Protocol (DHCP)
69 TCP and UDP	Trivial File Transfer Protocol (TFTP)
80 TCP and UDP	Hypertext Transfer Protocol (HTTP)
110 TCP	Post Office Protocol (POP3)
119 TCP	Network News Transport Protocol (NNTP)
123 TCP and UDP	Network Time Protocol (NTP)
137 TCP and UDP 138 TCP and UDP 139 TCP and UDP	NetBIOS Name Service NetBIOS Datagram Service NetBIOS Session Service
143 TCP	Internet Message Access Protocol (IMAP4)
161 UDP 162 TCP and UDP	Simple Network Management Protocol (SNMP)
389 TCP and UDP	Lightweight Directory Access Protocol (LDAP)
443 TCP and UDP	HTTP over Secure Sockets Layer (HTTPS)
445 TCP	Microsoft Server Message Block (SMB) File Sharing
1720 TCP	H.323 Call Signaling
2427 UDP	Cisco Media Gateway Control Protocol (MGCP)
3389 TCP and UDP	Remote Desktop Protocol (RDP)
5004 TCP and UDP	Real-time Transport Protocol (RTP) Data

5005 TCP and UDP	Real-time Transport Protocol (RTP) Control
5060 TCP and UDP 5061 TCP	Session Initiation Protocol (SIP) Session Initiation Protocol (SIP) over TLS

To protect a server, ensure that only the necessary ports are open. For example, if the server is being used only for email, then shut down ports that correspond to FTP, DNS, HTTP, etc.