©Copyright 1994 AT&T and Lumeta Corporation. All Rights Reserved.
Notice: For personal use only. These materials may not be reproduced or distributed in any form
or by any means except that they may be downloaded from this source and printed for personal use.

Appendix B

TCP and UDP Ports

B.1 Fixed Ports

An abbreviated table of TCP and UDP ports is given here, as well as our recommendations for which ones should be blocked by a packet filter. In some cases, you will be referred to a more detailed discussion.

Recall that (1) we do not think that packet filters are, in general, secure by themselves, and that (2) we don't think you should just block known trouble areas.

Any of these services can be used to see if a host is alive; if you block ICMP `Echo` (*ping*), block all of these services.

Port	Protocol	Name	Description
1	TCP	tcpmux	The TCP port multiplexer. Not very common. Cannot accept some, reject others (Sec. 3.3.5).
7	UDP, TCP	echo	An echo server; useful for seeing if a machine is alive. A higher level equivalent of ICMP `Echo` (*ping*).
9	UDP, TCP	discard	The `/dev/null` of the Internet. Harmless.
11	TCP	systat	Occasionally (but rarely) connected to *netstat*, *w*, or *ps*. If you do that sort of thing—and you shouldn't—block this.
13	UDP, TCP	daytime	The time of day, in human-readable form. Harmless.
15	TCP	netstat	See *systat*.

Port	Protocol	Name	Description
19	UDP, TCP	chargen	A character stream generator. Some people like reading that sort of thing, and it won't upset your system if they do.
20	TCP	ftp-data	Data channel for FTP. Hard to filter (Secs. 2.6.2, 3.3.2).
21	TCP	ftp	FTP control channel. Allow in only to your FTP server, if any (Secs. 2.6.2, 3.3.2).
23	TCP	telnet	*Telnet*. Permit only to your login gateway (Sec. 2.4.2).
25	TCP	smtp	Mail. Allow only to your incoming mail gateways, and make sure those aren't running *sendmail* (Sec. 2.4.1).
37	UDP, TCP	time	The time of day, in machine-readable form. Before blocking it (and there's no reason to), remember that ICMP can provide the same data.
43	TCP	whois	Allow in if you run a sanitized *whois* server; otherwise block (Sec. 2.4.4).
53	UDP, TCP	domain	Block TCP except from secondary servers. If you want to hide your DNS information, see Section 3.3.4; otherwise, allow (Sec. 2.3).
67	UDP	bootp	Block; it gives out too much information.
69	UDP	tftp	Block (Sec. 2.6.1).
70	TCP	gopher	Dangerous but useful. Be careful if you allow it (Sec. 2.8.1).
79	TCP	finger	Allow in only if you run a sanitized *finger* server, and only to it; block to all other destinations (Sec. 2.4.4).
80	TCP	http	Also known as WWW. Dangerous but useful. Be careful if you allow it (Sec. 2.8.1).
87	TCP	link	Rarely used, except by hackers. A lovely port for an alarm.
88	UDP	kerberos	The official Kerberos port. If you allow people to log in to your site, whether directly or via interrealm authentication, you have to open up this port; otherwise, block it (Sec. 13.2). Do the same for 750, the original Kerberos port. Block 749 and 751, the current and original Kerberos password changing ports. The ports used for Kerberos-protected services are probably safe, though.

Port	Protocol	Name	Description
95	TCP	supdup	Rarely used except by hackers. Another lovely port for an alarm.
109	TCP	pop-2	Unless folks need to read their mail from outside, block it.
110	TCP	pop-3	Ditto.
111	UDP, TCP	sunrpc	Block, but remember that attackers can scan your port number space anyway (Sec. 2.5.1).
113	TCP	auth	Generally safe. If you block it, don't send an ICMP rejection (Sec. 7.3).
119	TCP	nntp	If you allow it in, use source and destination address filters (Sec. 2.8.2).
123	UDP	ntp	Safe if you use NTP's own access controls (Sec. 2.4.3).
144	TCP	NeWS	A window system. Block as you would X11.
161	UDP	snmp	Block.
162	UDP	snmp-trap	Block, unless you monitor routers outside of your net.
177	UDP	xdmcp	For X11 logins. Block, of course.
512	TCP	exec	Block. It could be useful with a variant *rcp*; as is, the only thing that has ever used it is the Internet worm. Besides, it doesn't do any logging.
513	TCP	login	*Shudder.* Block (Sec. 2.7).
514	TCP	shell	*Double shudder.* It doesn't do any logging, either. Block (Sec. 2.7).
515	TCP	printer	There have been reports of problems, and there's rarely a good reason for outsiders to use your printers. Block.
512	UDP	biff	Block; it's a buggy, dangerous service.
513	UDP	who	You shouldn't get anything legitimate on this port; block it.
514	UDP	syslog	Apart from security holes (and there are some), if this is open, your logs can be attacked. Block (Sec. 6.2).
517	UDP	talk	Block; the actual protocol involves a conversation between random TCP ports.
518	UDP	ntalk	Ditto.
520	UDP	route	Block; don't allow outsiders to play games with your routing tables (Sec. 2.2).
540	TCP	uucp	Historically a dangerous service, and mostly obsolete on the Internet. Block.

Port	Protocol	Name	Description
1025	TCP	listener	The usual port for the System V Release 3 listener. An amazingly bad choice; if you have such machines, either change the listener port (it's a local option), or be sure to block incoming calls only to this port; you're sure to have outgoing calls using it.
2000	TCP	openwin	Like X11. Block.
2049	UDP	nfs	Block, and don't think twice.
2766	TCP	listen	The System V listener. Like *tcpmux*, but with more services. Block.
6000–6xxx	TCP	x11	Block the entire range of X11 ports (Secs. 2.9, 3.3.3).
6667	TCP	IRC	Block. Internet Relay Chat may or may not be a security risk *per se* (although there are a few dangerous options in IRC clients), but some channels, at least, attract the sort of network people who send out ICMP `Destination Unreachable` messages.

B.2 MBone Usage

Some old multicast implementations use fixed port numbers. These are bound to specific multicast addresses. By convention, certain ports and addresses are used for multicasts of IETF meetings and other network-related meetings.

Service	Address	Port	Use
sd	224.2.127.255	9876	
vat	224.2.0.1	3456	data
		3457	"session" info
nv	224.2.1.1	4444	
ivs	224.8.8.8	2232	video
		2233	audio
		2234	control
IETF chan 1 audio (GSM)	224.0.1.10	4100	
		4101	
IETF chan 2 audio (GSM)	224.0.1.13	4130	
		4131	
IETF chan 1 audio (PCM)	224.0.1.11	4110	
		4111	
IETF chan 2 audio (PCM)	224.0.1.14	4140	
		4141	
IETF chan 1 video	224.0.1.12	4444	
IETF chan 2 video	224.0.1.15	4444	