Packet Filtering characteristics for various protocols

Protocols Index:

Packet Filtering characteristics for various protocols

Dir.: In = Incoming traffic into Internal network
Out = Outgoing traffic to External network
SA: Source Address, Ext = External address; Int = Internal address
DA: Destination Address, Ext = External address; Int = Internal address
PROT: Protocol in use
SP: Source Port
DP: Destination Port
ACK Set: a: UDP does not have an equivalent for ACK
b: (YES) TCP ACK bit will be set on all packets, EXCEPT THE FIRST PACKET!
First packet without ACK bit set signals: REQUEST TO ESTABLISH A CONNECTION

Remote Procedure Calls (RPC)

Dir.	SA	DA	PROT	SP	DP	ACK Set	Notes
In	Ext	Int	UDP	>1023	135	a	Request, external client to internal MS/DCE RPC Location server
Out	Int	Ext	UDP	135	>1023	a	Response, internal MS/DCE location server to external client
Out	Int	Ext	UDP	>1023	135	a	Request, internal client to external MS/DCE RPC Location server
In	Ext	Int	UDP	135	>1023	a	Response, external MS/DCE location server to internal client
In	Ext	Int	TCP	>1023	135	b	Request, external client to internal MS/DCE RPC Location server
Out	Int	Ext	TCP	135	>1023	YES	Response, internal MS/DCE location server to external client
Out	Int	Ext	TCP	>1023	135	b	Request, internal client to external MS/DCE RPC Location server
In	Ext	Int	TCP	135	>1023	YES	Response, external MS/DCE location server to internal client
In	Ext	Int	UDP	>1023	135	a	Request, external client to internal MS/DCE RPC server
Out	Int	Ext	UDP	135	>1023	a	Response, internal MS/DCE server to external client
Out	Int	Ext	UDP	>1023	135	a	Request, internal client to external MS/DCE RPC server
In	Ext	Int	UDP	135	>1023	a	Response, external MS/DCE server to internal client
In	Ext	Int	TCP	>1023	135	b	Request, external client to internal MS/DCE RPC server
Out	Int	Ext	TCP	135	>1023	YES	Response, internal MS/DCE server to external client
Out	Int	Ext	TCP	>1023	135	b	Request, internal client to external MS/DCE RPC server
In	Ext	Int	TCP	135	>1023	YES	Response, external MS/DCE server to internal client

a: UDP does not have an equivalent for ACK
b: (YES) TCP ACK bit will be set on all packets, EXCEPT THE FIRST PACKET!
First packet without ACK bit set signals: REQUEST TO ESTABLISH A CONNECTION

NetBIOS over TCP/IP (NetBT)

Dir.	SA	DA	PROT	SP	DP	ACK Set	Notes
In	Ext	Int	UDP	>1023	138	a	Request, external client to internal NetBT datagram server
Out	Int	Ext	UDP	138	>1023	a	Response, internal NetBT datagram server to external client
Out	Int	Ext	UDP	>1023	138	a	Request, internal client to external NetBT datagram server
In	Ext	Int	UDP	138	>1023	a	Response, external NetBT datagram server to internal client
In	Ext	Int	TCP	>1023	138	b	Request, external client to internal NetBT datagram server
Out	Int	Ext	TCP	138	>1023	YES	Response, internal NetBT datagram server to external client
Out	Int	Ext	TCP	>1023	138	b	Request, internal client to external NetBT datagram server
In	Ext	Int	TCP	138	>1023	YES	Response, external NetBT datagram server to internal client

a: UDP does not have an equivalent for ACK
b: (YES) TCP ACK bit will be set on all packets, EXCEPT THE FIRST PACKET!
First packet without ACK bit set signals: REQUEST TO ESTABLISH A CONNECTION

Note: TCP port 138 and UDP port 139 are also registered for use by NetBT but are not actually used.!

Server Message Block (SMB)
Common Internet File System (CIFS)

Dir.	SA	DA	PROT	SP	DP	ACK Set	Notes
In	Ext	Int	TCP	>1023	139, 445	a	Incoming SMB/TCP connection, client to server
Out	Int	Ext	TCP	139, 445	>1023	YES	Incoming SMB/TCP connection, server to client
In	Ext	Int	UDP	>1023	138, 445	b	Incoming SMB/UDP connection, client to server
Out	Int	Ext	UDP	138, 445	>1023	b	Incoming SMB/TCP connection, server to client
Out	Int	Ext	TCP	>1023	139, 445	a	Outgoing SMB/TCP connection, client to server
In	Ext	Int	TCP	139, 445	>1023	YES	Outgoing SMB/TCP connection, server to client
Out	Int	Ext	UDP	>1023	138, 445	b	Outgoing SMB/UDP connection, client to server
In	Ext	Int	UDP	138, 445	>1023	b	Outgoing SMB/UDP connection, server to client

a: UDP does not have an equivalent for ACK

b: (YES) TCP ACK bit will be set on all packets, EXCEPT THE FIRST PACKET!
First packet without ACK bit set signals: REQUEST TO ESTABLISH A CONNECTION

IP Security (IPsec)

Dir.	SA	DA	PROT	SP	DP	Notes
In	Ext	Int	AH	a	a	Incoming AH, client to server
Out	Int	Ext	AH	a	a	Incoming AH, server to client
In	Ext	Int	ESP	a	a	Incoming ESP, client to server
Out	Int	Ext	ESP	a	a	Incoming ESP, server to client
In	Ext	Int	UDP	500	500	Incoming ISAKMP request
Out	Int	Ext	UDP	500	500	ISAKMP response
Out	Int	Ext	AH	a	a	Outgoing AH, client to server
In	Ext	Int	AH	a	a	Outgoing AH, server to client
Out	Int	Ext	ESP	a	a	Outgoing ESP, client to server
In	Ext	Int	ESP	a	a	Outgoing ESP, server to client
Out	Int	Ext	UDP	500	500	Outgoing ISAKMP request
In	Ext	Int	UDP	500	500	ISAKMP response

a: AH and ESP do not have source or destination ports

Point-To-Point-Tunneling Protocol (PPTP)

Dir.	SA	DA	PROT	SP	DP	ACK Set	Notes
In	Ext	Int	GRE	a	a	b	Tunnel data, external client to internal server
Out	Int	Ext	GRE	a	a	b	Tunnel reply, internal server to external client
In	Ext	Int	TCP	>1023	1723	c	Setup request, external client to internal server
Out	Int	Ext	TCP	1723	>1023	YES	Setup response, internal server to external client
Out	Int	Ext	GRE	a	a	b	Tunnel data, internal client to external server
In	Ext	Int	GRE	a	a	b	Tunnel reply, external server to internal client
Out	Int	Ext	TCP	>1023	1723	c	Setup request, internal client to external server
In	Ext	Int	TCP	1723	>1023	YES	Setup response, external server to internal client

a: GRE does not have ports. GRE does have protocol types, and PPTP is protocol type hexadecimal 880B.

b: GRE does not have an equivalent for ACK

c: (YES) TCP ACK bit will be set on all packets, EXCEPT THE FIRST PACKET!
First packet without ACK bit set signals: REQUEST TO ESTABLISH A CONNECTION

Layer 2 Transport Protocol (L2TP)

Dir.	SA	DA	PROT	SP	DP	ACK Set	Notes
In	Ext	Int	UDP	>1023	1701		External client to internal server
Out	Int	Ext	UDP	1701 (a)	>1023		Response, internal server to external client
Out	Int	Ext	UDP	>1023	1701		Internal client to external server
In	Ext	Int	UDP	1701 (a)	>1023		Response, external server to internal client

a: The standard does not require L2TP servers to return packets from port 1701; they must receive packets at 1701 but may send them from any port. Many servers will send packets from 1701 to simplify interactions with network address translation and dynamic packet filtering.

HyperText Transport Protocol (HTTP)

Dir.	SA	DA	PROT	SP	DP		Notes
In	Ext	Int	TCP	>1023	80 (a)	b	Request, external client to internal server
Out	Int	Ext	TCP	80 (a)	>1023	YES	Response, internal server to external client
Out	Int	Ext	TCP	>1023	80 (a)	b	Request, internal client to external server
In	Ext	Int	TCP	80 (a)	>1023	YES	Response, external server to internal client

a: 80 is the standard port number for HTTP servers, but some servers run on different port numbers.

b: (YES) TCP ACK bit will be set on all packets, EXCEPT THE FIRST PACKET! First packet without ACK bit set signals: REQUEST TO ESTABLISH A CONNECTION

HTTPS and Secure HTTP (a)

Dir.	SA	DA	PROT	SP	DP		Notes
In	Ext	Int	TCP	>1023	443	b	Request, external client to internal server
Out	Int	Ext	TCP	443	>1023	YES	Response, internal server to external client
Out	Int	Ext	TCP	>1023	443	b	Request, internal client to external server
In	Ext	Int	TCP	443	>1023	YES	Response, external server to internal client

a: Secure HTTP is designed to operate over port 80 and uses shttp:// in the URL, as opposed to https:// for HTTPS.

b: (YES) TCP ACK bit will be set on all packets, EXCEPT THE FIRST PACKET! First packet without ACK bit set signals: REQUEST TO ESTABLISH A CONNECTION

Internet Cache Protocol (ICP)

Dir.	SA	DA	PROT	SP	DP		Notes
In	Ext	Int	UDP	>1023	3130 (a)	b	ICP request or response, external cache to internal cache
Out	Int	Ext	UDP	3130 (a)	>1023	b	ICP request or response, internal cache to external cache
In	Ext	Int	TCP	>1023	3128 (c)	d	HTTP request, external cache to internal cache
Out	Int	Ext	TCP	3128 (c)	>1023	YES	HTTP response, internal cache to external cache
Out	Int	Ext	TCP	>1023	3128 (c)	d	HTTP request, internal cache to external cache
In	Ext	Int	TCP	3128 (c)	>1023	YES	HTTP response, external cache to internal cache

a: 3130 is the standard port number for ICP, but some servers run on different port numbers.
b: UDP does not have an equivalent for ACK
c: 3128 is the standard port number for intercache HTTP servers, but some servers run on different port numbers.
d: (YES) TCP ACK bit will be set on all packets, EXCEPT THE FIRST PACKET!
First packet without ACK bit set signals: REQUEST TO ESTABLISH A CONNECTION

Gopher

Dir.	SA	DA	PROT	SP	DP		Notes
In	Ext	Int	TCP	>1023	70 (a)	b	Request, external client to internal server
Out	Int	Ext	TCP	70 (a)	>1023	YES	Response, internal server to external client
Out	Int	Ext	TCP	>1023	70 (a)	b	Request, internal client to external server
In	Ext	Int	TCP	70 (a)	>1023	YES	Response, external server to internal client

a: 70 is the standard port number for Gopher servers, but some servers run on different port numbers.
b: (YES) TCP ACK bit will be set on all packets, EXCEPT THE FIRST PACKET!
First packet without ACK bit set signals: REQUEST TO ESTABLISH A CONNECTION

WAIS

Dir.	SA	DA	PROT	SP	DP		Notes
In	Ext	Int	TCP	>1023	210 (a)	b	Request, external client to internal server
Out	Int	Ext	TCP	210 (a)	>1023	YES	Response, internal server to external client
Out	Int	Ext	TCP	>1023	210 (a)	b	Request, internal client to external server
In	Ext	Int	TCP	210 (a)	>1023	YES	Response, external server to internal client

a: 210 is the standard port number for WAIS servers, but some servers run on different port numbers.
b: (YES) TCP ACK bit will be set on all packets, EXCEPT THE FIRST PACKET!
First packet without ACK bit set signals: REQUEST TO ESTABLISH A CONNECTION

Simple Mail Transfer Protocol (SMTP)

Dir.	SA	DA	PROT	SP	DP		Notes
In	Ext	Int	TCP	>1023	25	a	Incoming mail, sender to recipient
Out	Int	Ext	TCP	25	>1023	YES	Incoming mail, recipient to sender
Out	Int	Ext	TCP	>1023	25	a	Outgoing mail, sender to recipient
In	Ext	Int	TCP	25	>1023	YES	Outgoing mail, recipient to sender

a: (YES) TCP ACK bit will be set on all packets, EXCEPT THE FIRST PACKET!
First packet without ACK bit set signals: REQUEST TO ESTABLISH A CONNECTION

Lotus Notes

Dir.	SA	DA	PROT	SP	DP		Notes
In	Ext	Int	TCP	>1023	1352	a	Incoming Notes connection, client to server
Out	Int	Ext	TCP	1352	>1023	YES	Incoming Notes connection, server to client
Out	Int	Ext	TCP	>1023	1352	a	Outgoing Notes connection, client to server
In	Ext	Int	TCP	1352	>1023	YES	Outgoing Notes connection, server to client

a: (YES) TCP ACK bit will be set on all packets, EXCEPT THE FIRST PACKET!
First packet without ACK bit set signals: REQUEST TO ESTABLISH A CONNECTION

Post Office Protocol (POP2/ POP3)

Dir.	SA	DA	PROT	SP	DP	ACK Set	Notes
In	Ext	Int	TCP	>1023	110, 109 (a)	b	Incoming POP connection, client to server
Out	Int	Ext	TCP	110, 109 (a)	>1023	YES	Incoming POP connection, server to client
In	Ext	Int	TCP	>1023	995	b	Incoming POP over SSL connection, client to server
Out	Int	Ext	TCP	995	>1023	YES	Incoming POP over SSL connection, server to client
Out	Int	Ext	TCP	>1023	110, 109 (a)	b	Outgoing POP connection, client to server
In	Ext	Int	TCP	110, 109 (a)	>1023	YES	Outgoing POP connection, server to client
Out	Int	Ext	TCP	>1023	995	b	Outgoing POP over SSL connection, client to server
In	Ext	Int	TCP	995	>1023	YES	Outgoing POP over SSL connection, server to client

a: Modern POP (POP3) servers use port 10; older POP2 servers use port 109.
b: (YES) TCP ACK bit will be set on all packets, EXCEPT THE FIRST PACKET!
First packet without ACK bit set signals: REQUEST TO ESTABLISH A CONNECTION

Internet Message Access Protocol (IMAP)

Dir.	SA	DA	PROT	SP	DP	ACK Set	Notes
In	Ext	Int	TCP	>1023	143	b	Incoming IMAP connection, client to server
Out	Int	Ext	TCP	143	>1023	YES	Incoming IMAP connection, server to client
In	Ext	Int	TCP	>1023	993, 585 (a)	b	Incoming IMAP over SSL connection, client to server
Out	Int	Ext	TCP	993, 585 (a)	>1023	YES	Incoming IMAP over SSL connection, server to client
Out	Int	Ext	TCP	>1023	143	b	Outgoing IMAP connection, client to server
In	Ext	Int	TCP	143	>1023	YES	Outgoing IMAP connection, server to client
Out	Int	Ext	TCP	>1023	993, 585 (a)	b	Outgoing IMAP over SSL connection, client to server
In	Ext	Int	TCP	993, 585 (a)	>1023	YES	Outgoing IMAP over SSL connection, server to client

a: 993 is the current standard, but some older implementations use 585.
b: (YES) TCP ACK bit will be set on all packets, EXCEPT THE FIRST PACKET!
First packet without ACK bit set signals: REQUEST TO ESTABLISH A CONNECTION

Network News Transfer Protocol (NNTP)

Dir.	SA	DA	PROT	SP	DP	ACK Set	Notes
In	Ext	Int	TCP	>1023	119	a	Incoming news
Out	Int	Ext	TCP	119	>1023	YES	Incoming news responses
Out	Int	Ext	TCP	>1023	119	a	Outgoing news, or internal client contacting external server
In	Ext	Int	TCP	119	>1023	YES	Outgoing news responses, or external server responding to internal client

a: (YES) TCP ACK bit will be set on all packets, EXCEPT THE FIRST PACKET!
First packet without ACK bit set signals: REQUEST TO ESTABLISH A CONNECTION

File Transfer Protocol (FTP)

Dir.	SA	DA	PROT	SP	DP	ACK Set	Notes
In	Ext	Int	TCP	>1023	21	a	Incoming FTP request
Out	Int	Ext	TCP	21	>1023	YES	Response to incoming request
Out	Int	Ext	TCP	20	>1023	a	Data channel creation for incoming FTP request, normal mode
In	Ext	Int	TCP	>1023	20	YES	Data channel responses for incoming FTP request, normal mode
In	Ext	Int	TCP	>1023	>1023	a	Data channel creation for incoming FTP request, passive mode
Out	Int	Ext	TCP	>1023	>1023	YES	Data channel responses for incoming FTP request, passive mode
Out	Int	Ext	TCP	>1023	21	a	Outgoing FTP request
In	Ext	Int	TCP	21	>1023	YES	Response to outgoing request
In	Ext	Int	TCP	20	>1023	a	Data channel creation for outgoing FTP request, normal mode
Out	Int	Ext	TCP	>1023	20	YES	Data channel responses for outgoing FTP request, normal mode
Out	Int	Ext	TCP	>1023	>1023	a	Data channel creation for outgoing FTP request, passive mode
In	Ext	Int	TCP	>1023	>1023	YES	Data channel responses for outgoing FTP request, passive mode

a: (YES) TCP ACK bit will be set on all packets, EXCEPT THE FIRST PACKET!
First packet without ACK bit set signals: REQUEST TO ESTABLISH A CONNECTION

Trivial File Transfer Protocol (TFTP)

Dir.	SA	DA	PROT	SP	DP	ACK Set	Notes
In	Ext	Int	UDP	>1023	69	a	Incoming TFTP request (first packet from client)
Out	Int	Ext	UDP	>1023	>1023	a	Response to incoming request
In	Ext	Int	UDP	>1023	>1023	a	Subsequent packets from client
Out	Int	Ext	UDP	>1023	69	a	Outgoing TFTP request (first packet from client)
In	Ext	Int	UDP	>1023	>1023	a	Response to outgoing request
Out	Int	Ext	UDP	>1023	>1023	a	Subsequent packets from client

a: UDP does not have an equivalent for ACK

Terminal Access (Telnet)

Dir.	SA	DA	PROT	SP	DP		Notes
In	Ext	Int	TCP	>1023	23	a	Incoming session, client to server
Out	Int	Ext	TCP	23	>1023	YES	Incoming session, server to client
Out	Int	Ext	TCP	>1023	23	a	Outgoing session, client to server
In	Ext	Int	TCP	23	>1023	YES	Outgoing session, server to client

a: (YES) TCP ACK bit will be set on all packets, EXCEPT THE FIRST PACKET!
First packet without ACK bit set signals: REQUEST TO ESTABLISH A CONNECTION

MS Terminal Server Remote Desktop Protocol (RDP)

Dir.	SA	DA	PROT	SP	DP		Notes
In	Ext	Int	TCP	>1023	3389	a	Incoming RDP connection, external client to internal server
Out	Int	Ext	TCP	3389	>1023	YES	Incoming RDP connection, internal server to external client
Out	Int	Ext	TCP	>1023	3389	a	Outgoing RDP connection, internal client to external server
In	Ext	Int	TCP	3389	>1023	YES	Outgoing RDP connection, external server to internal client

a: (YES) TCP ACK bit will be set on all packets, EXCEPT THE FIRST PACKET!
First packet without ACK bit set signals: REQUEST TO ESTABLISH A CONNECTION

Internet Relay Chat (IRC)

Dir.	SA	DA	PROT	SP	DP	ACK Set	Notes
In	Ext	Int	TCP	>1023	6667 (a)	b	External client or server contacting internal server
Out	Int	Ext	TCP	6667 (a)	>1023	YES	Internal server answering
Out	Int	Ext	TCP	>1023	>1023	b	DCC connection requested by external client; internal client answering invitation from external client
In	Ext	Int	TCP	>1023	>1023	YES	DCC connection from external client
Out	Int	Ext	TCP	>1023	6667 (a)	b	Internal client or server contacting external server
In	Ext	Int	TCP	6667 (a)	>1023	YES	External server answering
In	Ext	Int	TCP	>1023	>1023	b	DCC connection requested by internal client; external client answering invitation from internal client
Out	Int	Ext	TCP	>1023	>1023	YES	DCC connection from internal client

a: Although 6667 is the most commonly used port for IRC, some servers use other port numbers.
b: (YES) TCP ACK bit will be set on all packets, EXCEPT THE FIRST PACKET!
First packet without ACK bit set signals: REQUEST TO ESTABLISH A CONNECTION

ICQ

Dir.	SA	DA	PROT	SP	DP	ACK Set	Notes
Out	Int	Mirabilis	UDP	>1023	4000	b	Internal client to server
In	Mirabilis	Int	UDP	4000	>1023	b	Server to internal client
Out	Int	Mirabilis	TCP	>1023 (a)	>1023	c	Internal client sending messages via server
In	Mirabilis	Int	TCP	>1023	>1023 (a)	YES	Server sending messages to internal client
Out	Int	Ext	TCP	>1023 (a)	>1023	c	Internal client sending messages direct to external client
In	Ext	Int	TCP	>1023	>1023 (a)	YES	External client replying to internal client
In	Ext	Int	TCP	>1023	>1023 (a)	c	External client sending messages direct to internal client
Out	Int	Ext	TCP	>1023 (a)	>1023	YES	Internal client replying to external client

a: The port range used for this purpose can be configured on the client.

b: UDP does not have an equivalent for ACK

c: (YES) TCP ACK bit will be set on all packets, EXCEPT THE FIRST PACKET!
First packet without ACK bit set signals: REQUEST TO ESTABLISH A CONNECTION

Multimedia Protocol H.323

Dir.	SA	DA	PROT	SP	DP	ACK Set	Notes
In	Ext	Int	TCP	>1023	1720	b	External caller contacting internal callee
Out	Int	Ext	TCP	1720	>1023	YES	Internal callee responding to external caller
Out	Int	Ext	TCP	>1023	1720	b	Internal caller contacting external callee
In	Ext	Int	TCP	1720	>1023	YES	External callee responding to internal caller
Out	Int	Ext	TCP	>1023	>1023	b	Call control for data going internal to external
In	Ext	Int	TCP	>1023	>1023	YES	Responses to call control for data going internal to external
In	Ext	Int	TCP	>1023	>1023	b	Call control for data going external to internal
Out	Int	Ext	TCP	>1023	>1023	YES	Responses to call control for data going external to internal
Out	Int	Ext	UDP	>1023	>1023	a	Data going internal to external
In	Ext	Int	UDP	>1023	>1023	a	Data going external to internal

a: UDP does not have an equivalent for ACK

b: (YES) TCP ACK bit will be set on all packets, EXCEPT THE FIRST PACKET!
First packet without ACK bit set signals: REQUEST TO ESTABLISH A CONNECTION

NetMeeting

Dir.	SA	DA	PROT	SP	DP	ACK Set	Notes
In	Ext	Int	TCP	>1023	1731	a	External caller contacting internal callee, audio control
Out	Int	Ext	TCP	1731	>1023	YES	Internal callee responding to external caller, audio control
In	Ext	Int	TCP	>1023	389	a	External client to internal ILS server
Out	Int	Ext	TCP	389	>1023	YES	Responses from internal ILS server
In	Ext	Int	TCP	>1023	522	a	External client to internal ILS server
Out	Int	Ext	TCP	522	>1023	YES	Responses from internal ILS server
Out	Int	Ext	TCP	>1023	1731	a	Internal caller contacting external callee, audio control
In	Ext	Int	TCP	1731	>1023	YES	External callee responding to internal caller, audio control
Out	Int	Ext	TCP	>1023	389	a	Internal client to external ILS server
In	Ext	Int	TCP	389	>1023	YES	Responses from external ILS server
Out	Int	Ext	TCP	>1023	522	a	Internal client to external ILS server
In	Ext	Int	TCP	522	>1023	YES	Responses from external ILS server

a: (YES) TCP ACK bit will be set on all packets, EXCEPT THE FIRST PACKET!
First packet without ACK bit set signals: REQUEST TO ESTABLISH A CONNECTION

Domain Name System (DNS)

Dir.	SA	DA	PROT	SP	DP	ACK Set	Notes
In	Ext	Int	TCP	>1023	53	a	Query via TCP, external client to internal server
Out	Int	Ext	TCP	53	>1023	YES	Response via TCP, internal server to external client
Out	Int	Ext	UDP	>1023	53	b	Query via UDP, internal client to external server
In	Ext	Int	UDP	53	>1023	b	Response via UDP, external server to internal client
Out	Int	Ext	TCP	>1023	53	c	Query via TCP, internal client to external server
In	Ext	Int	TCP	53	>1023	YES	Response via TCP, external server to internal client
In	Ext	Int	UDP	53	53	b	Query or response between two servers (a) via UDP
Out	Int	Ext	UDP	53	53	b	Query or response between two servers (a) via UDP
In	Ext	Int	TCP	>1023	53	c	Query or zone transfer requested from external server to internal server via TCP
Out	Int	Ext	TCP	53	>1023	YES	Response (including zone transfer response) from internal server to external server via TCP
Out	Int	Ext	TCP	>1023	53	c	Query or zone transfer requested from internal server to external server via TCP
In	Ext	Int	TCP	53	>1023	YES	Response (including zone transfer response) from external server to internal server via TCP

a: Not all servers use 53 as a source port for UDP; some will use a port above 1023, like other clients.

b: UDP does not have an equivalent for ACK

c: (YES) TCP ACK bit will be set on all packets, EXCEPT THE FIRST PACKET!
First packet without ACK bit set signals: REQUEST TO ESTABLISH A CONNECTION

NetBT Name Service
(Windows Internet Name Service - WINS)

Dir.	SA	DA	PROT	SP	DP	ACK Set	Notes
In	Ext	Broadcast	UDP	137, >1023	137	a	Incoming NetBT name service request via UDP, client to server
In	Ext	Int	UDP	137, >1023	137	a	Incoming WINS query via UDP, client to server
Out	Int	Ext	UDP	137	137, >1023	a	Answer to incoming UDP query, server to client
In	Ext	Int	TCP	137, >1023	137	b	Incoming query via TCP, client to server
Out	Int	Ext	TCP	137	137, >1023	YES	Answer to incoming TCP query, server to client
Out	Int	Broadcast	UDP	137, >1023	137	a	Outgoing NetBT name service query via UDP
Out	Int	Ext	UDP	137, >1023	137	a	Outgoing WINS query via UDP
In	Ext	Int	UDP	137	137, >1023	a	Answer to outgoing UDP query
Out	Int	Ext	TCP	137, >1023	137	b	Outgoing query via TCP, client to server
In	Ext	Int	TCP	137	137, >1023	YES	Answer to outgoing TCP query, server to client
Out	Int	Ext	TCP	>1023	42	b	WINS server replication request from internal server to external server
In	Ext	Int	TCP	42	>1023	YES	WINS server replication reply
In	Ext	Int	TCP	>1023	42	b	WINS server replication request from external server to internal server
Out	Int	Ext	TCP	42	>1023	YES	WINS server replication reply

a: UDP does not have an equivalent for ACK

b: (YES) TCP ACK bit will be set on all packets, EXCEPT THE FIRST PACKET!
First packet without ACK bit set signals: REQUEST TO ESTABLISH A CONNECTION

Lightweight Directory Access Protocol (LDAP)

Dir.	SA	DA	PROT	SP	DP	ACK Set	Notes
In	Ext	Int	TCP	>1023	389 (a)	b	Query, external LDAP client to internal server
Out	Int	Ext	TCP	389 (a)	>1023	YES	Response, internal server to external LDAP client
In	Ext	Int	TCP	>1023	636 (c)	b	Query, external LDAPS client to internal server
Out	Int	Ext	TCP	636 (c)	>1023	YES	Response, internal server to external LDAPS client
Out	Int	Ext	TCP	>1023	389 (a)	b	Query, internal LDAP client to external server
In	Ext	Int	TCP	389 (a)	>1023	YES	Response, external server to internal LDAP client
Out	Int	Ext	TCP	>1023	636 (c)	b	Query, internal LDAPS client to external server
In	Ext	Int	TCP	636 (c)	>1023	YES	Response, external server to internal LDAPS client

a: 3268 for Active Directory service Global Catalog
b: (YES) TCP ACK bit will be set on all packets, EXCEPT THE FIRST PACKET!
First packet without ACK bit set signals: REQUEST TO ESTABLISH A CONNECTION
c: 3269 for Active Directory service Global Catalog

Kerberos V5

Dir.	SA	DA	PROT	SP	DP	ACK Set	Notes
In	Ext	Int	UDP	>1023	88	a	Request to internal KDC (Key Distribution Center)
Out	Int	Ext	UDP	88	>1023	a	Response from internal KDC (Key Distribution Center)
Out	Int	Ext	UDP	>1023	88	a	Request to external KDC (Key Distribution Center)
In	Ext	Int	UDP	88	>1023	a	Response from external KDC (Key Distribution Center)
In	Ext	Int	TCP	>1023	88	b	Over-length request to internal KDC (Key Distribution Center)
Out	Int	Ext	TCP	88	>1023	YES	Over-length response from internal KDC (Key Distribution Center)
Out	Int	Ext	TCP	>1023	88	b	Over-length request to external KDC (Key Distribution Center)
In	Ext	Int	TCP	88	>1023	YES	Over-length response from external KDC (Key Distribution Center)

a: UDP does not have an equivalent for ACK
b: (YES) TCP ACK bit will be set on all packets, EXCEPT THE FIRST PACKET!
First packet without ACK bit set signals: REQUEST TO ESTABLISH A CONNECTION

Remote Authentication Dial-in User Service (RADIUS)

Dir.	SA	DA	PROT	SP	DP	ACK Set	Notes
In	Ext	Int	UDP	>1023	1812 (a)	b	Authentication query, external client to internal RADIUS server
Out	Int	Ext	UDP	1812 (a)	>1023	b	Authentication response, internal RADIUS server to external client
In	Ext	Int	UDP	>1023	1813 (c)	b	Authentication notification, external client to internal RADIUS server
Out	Int	Ext	UDP	1813 (c)	>1023	b	Authentication response, internal RADIUS server to external client
Out	Int	Ext	UDP	>1023	1812 (a)	b	Authentication query, internal client to external RADIUS server
In	Ext	Int	UDP	1812 (a)	>1023	b	Authentication response, external RADIUS server to internal client
Out	Int	Ext	UDP	>1023	1813 (c)	b	Authentication notification, internal client to external RADIUS server
In	Ext	Int	UDP	1813 (c)	>1023	b	Authentication response, external RADIUS server to internal client

a: Early implementations may use 1645
b: UDP does not have an equivalent for ACK
c: Early implementations may use 1646

Simple Network Management Protocol (SNMP)

Dir.	SA	DA	PROT	SP	DP	ACK Set	Notes
In	Ext	Int	UDP	>1023	161	a	Query from external management station to internal SNMP device
Out	Int	Ext	UDP	161	>1023	a	Response from internal SNMP device to external management station
Out	Int	Ext	UDP	>1023	161	a	Query from internal management station to external SNMP device
In	Ext	Int	UDP	161	>1023	a	Response from external SNMP device to internal management station
In	Ext	Int	UDP	>1023	162	a	Trap from external SNMP device to internal management station
Out	Int	Ext	UDP	162	>1023	a	Trap from internal SNMP device to external management station

a: UDP does not have an equivalent for ACK

Routing Information Protocol (RIP)

Dir.	SA	DA	PROT	SP	DP	ACK Set	Notes
In	Ext	Int	UDP	>1023	520	a	Request, external client to internal server
Out	Int	Ext	UDP	520	>1023	a	Response, internal server to external client
Out	Int	Ext	UDP	>1023	520	a	Request, internal client to external server
In	Ext	Int	UDP	520	>1023	a	Response, external server to internal client
In	Ext	Broadcast	UDP	520	520	a	Update, external server to internal servers
Out	Int	Broadcast	UDP	520	520	a	Update, internal server to external servers

a: UDP does not have an equivalent for ACK

Open Shortest Path First (OSPF)

Dir.	SA	DA	PROT(a)	Packet Type (b)	Notes
In	Ext	224.0.0.5	89	1	Router hello, announcing its existence and neighbors
Out	Int Router	224.0.0.5	89	1	Internal router hello, announcing its existence and neighbors
In	Ext	Int Router	89	2	External router database description, giving an external router's link state database
Out	Int Router	Ext	89	2	Internal router database description
In	Ext	Int Router	89	3	External router link state request, asking for information about a particular link
Out	Int Router	Ext	89	4	Internal router link state update for a particular link in response to a request
Out	Int Router	Ext	89	3	Internal router link state request
In	Ext	Int Router	89	4	External router link state update
In	Ext	224.0.0.5	89	4	External router link state update, flooding all link states, from a designated router
Out	Int Router	224.0.0.6	89	5	Internal router link state acknowledgement response from a nondesignated router
In	Ext	224.0.0.6	89	4	External router link state update, from a nondesignated router
Out	Int Router	224.0.0.5	89	5	Internal router link state acknowledgement response from a designated router
Out	Int Router	224.0.0.5	89	4	Internal router link state update from a designated router
In	Ext	224.0.0.6	89	5	External router link state acknowledgement from a nondesignated router
Out	Int Router	224.0.0.6	89	4	Internal router link state update, from a nondesignated router
In	Ext	224.0.0.5	89	5	External router link state acknowledgement from a designated router

a: OSPF is layered directly on IP, not TCP or UDP.UDP does not have an equivalent for ACK

b: OSPF does not have source and destination ports, but messages are distinguished by type.

Internet Group Management Protocol (IGMP)

SA	DA	PROT	Packet Type	Notes
Router	224.0.0.1	2 (IGMP)	0x11	Host membership query
Host	Multicast (a)	2 (IGMP)	0x12	Version 1 host membership report
Host	Multicast (a)	2 (IGMP)	0x16	Version 2 host membership report
Host	224.0.0.1	2 (IGMP)	0x17	Leave group

a: This multicast will be addressed to the multicast group that it is reporting about.

Router Discovery / ICMP Router Discovery Protocol (IRDP)

Dir.	SA	DA	PROT	Message Type (b)	Notes
In	Ext	Broadcast,	ICMP	10	Incoming router solicitation
		224.0.0.2	ICMP		
Out	Int	Ext,	ICMP	9	Outgoing router announcement
		Broadcast,	ICMP		
		224.0.0.1	ICMP		
Out	Int	Broadcast,	ICMP	10	Outgoing router solicitation
		224.0.0.2	ICMP		
In	Ext	Int,	ICMP	9	Incoming router advertisement
		Broadcast,	ICMP		
		224.0.0.1	ICMP		

a: ICMP messages do not have source or destination port numbers;
they have a single ICMP message type field instead. ICMP has no ACK equivalent.

Dynamic Host Configuration Protocol (DHCP) and BootP

Dir.	SA	DA	PROT	SP	DP	Notes
In	Ext (a)	Broadcast	UDP	68	67	External client request to internal server
Out	Int	Ext (b)	UDP	67	68	Internal server positive response to external client
Out	Int	Broadcast	UDP	67	68	Internal server negative response to external DHCP client
In	Ext (b)	Broadcast	UDP	68	67	External client accepting DHCP offer
Out	Int	Ext (b)	UDP	67	68	Internal server acknowledging DHCP lease
Out	Int (a)	Broadcast	UDP	68	67	Internal client request to external server
In	Ext	Int (b)	UDP	67	68	External server positive response to internal client
In	Ext	Broadcast	UDP	67	68	External server negative response to internal DHCP client
Out	Int (b)	Broadcast	UDP	68	67	Internal client accepting DHCP offer
In	Ext	Int (b)	UDP	67	68	External server acknowledging DHCP lease

a: This address need not be a valid address; the destination machine is assumed not to be fully configured and the delivered packet will actually be based on lower-level data, not on the apparent destination address. The lower-level data may have a broadcast or unicast address depending on client capabilities.

b: This is now the valid, agreed-upon address.

ICMP Message Types

Msg. type	Description	Permit/Deny
0	Echo reply (reply to ping)	
3	Destination unreachable. May indicate host unreachable, network unreachable, port unreachable, or other	
4	Source quench (somebody telling destination: "slow down; you're talking too fast")	Should usually be allowed in both directions
5	Redirect (somebody telling destination to change a route); is supposed to be ignored by your systems unless it comes from a directly connected router. In particular, make sure the routers that are part of your firewall ignore it.	Should usually be blocked inbound. Definitely block to routers that are part of your firewall.
8	Echo request (generated by ping)	
9	Router announcement (used by router discovery)	Should be blocked in both directions.
10	Router selection (used by router discovery)	Should be blocked in both directions.
11	Time to live exceeded (packet appears to be looping)	Should usually be allowed in both directions
12	Parameter problem (problem with a packet header)	Should usually be allowed in both directions

Ping

Dir.	SA	DA	PROT	Message Type (b)	Notes
In	Ext	Int	ICMP	8	Incoming ping
Out	Int	Ext	ICMP	0	Response to incoming ping
Out	Int	Ext	ICMP	8	Outgoing ping
In	Ext	Int	ICMP	0	Response to outgoing ping

a: ICMP messages do not have source or destination port numbers; they have a single ICMP message type field instead. ICMP has no ACK equivalent.

Tracert

Dir.	SA	DA	PROT	SP(a)	DP(a)	Msg Type (b)	Notes
Out	Int	Ext	UDP	b	b	a	Outgoing UDP tracert probe
Out	Int	Ext	ICMP	a	a	8	Outgoing ICMP tracert probe
In	Ext	Int	ICMP	a	a	0	ICMP echo response (answering probe)
In	Ext	Int	ICMP	a	a	11	Incoming "time to live exceeded"
In	Ext	Int	ICMP	a	a	3	Incoming "destination unreachable"
In	Ext	Int	UDP	b	b	a	Incoming UDP tracert probe
In	Ext	Int	ICMP	a	a	8	Incoming ICMP tracert probe
Out	Int	Ext	ICMP	a	a	0	ICMP echo response (answering probe)
Out	Int	Ext	ICMP	a	a	11	Outgoing "time to live exceeded"
Out	Int	Ext	ICMP	a	a	3	Outgoing "destination unreachable"

a: UDP packets have source and destination ports; ICMP packets have only message type fields. UDP or ICMP have no equivalent for ACK.

b: tracert probe packet UDP source/destination ports vary by implementation, invocation, and/or command-line argument.
They are generally >32768, but that's about the only generalization you can make about them.
Specific implementations (particularly in routers and on non-Unix platforms) may vary.
Destination ports, in particular, are usually in the range 33434 through 33523.
Why this is the case is somewhat complicated, and you should read the comments in the Unix tracert source code if you are perversely curious.

Network Time Protocol (NTP)

Dir.	SA	DA	PROT	SP	DP	Notes
In	Ext	Int	UDP	>1023	123	Query, external client to internal server
Out	Int	Ext	UDP	123	>1023	Response, internal server to external client
Out	Int	Ext	UDP	>1023	123	Query, internal client to external server
In	Ext	Int	UDP	123	>1023	Response, external server to internal client
In	Ext	Int	UDP	123	123	Query or response between two servers
Out	Int	Ext	UDP	123	123	Query or response between two servers
In	Ext	Int	UDP	123	123	Multicast query or response from an external server
Out	Int	Ext	UDP	123	123	Multicast query or response from an internal server