

TCP/IP Quick Guide

OSI MODEL

Layer 7: Application Layer

- Defines interface to user processes
- Provides standardized network services

Layer 6: Presentation Layer

- Specifies architecture-independent data transfer format
- Encodes and decodes data; Encrypts and decrypts data; Compresses and decompresses data

Layer 5: Session Layer

- Manages user sessions and dialogues
- Controls establishment and termination of logical links between users

Layer 4: Transport Layer

- Provides reliable and sequential end-to-end packet delivery
- Provides connectionless oriented packet delivery

Layer 3: Network Layer

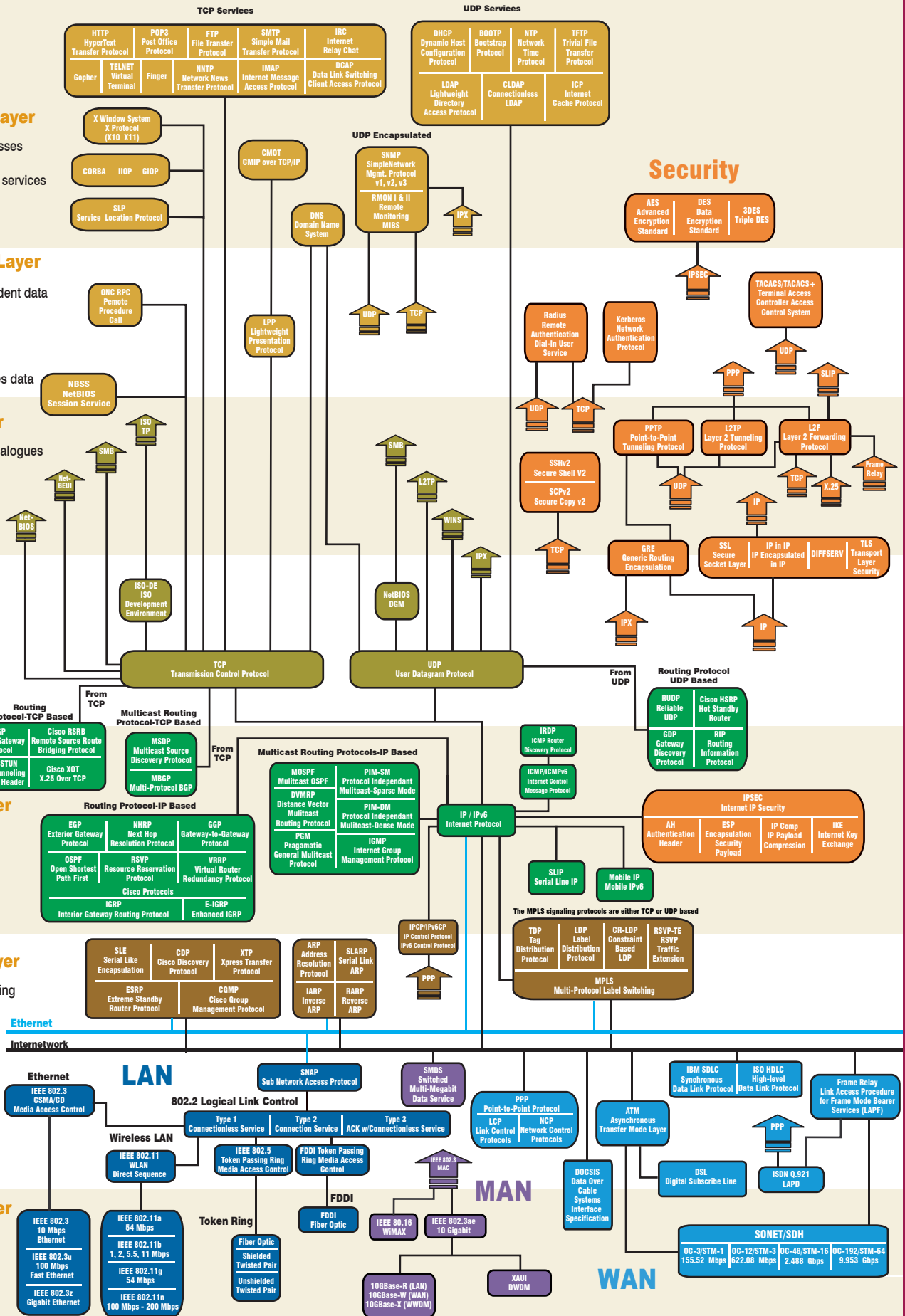
- Routes packets according to unique network addresses

Layer 2: Data Link Layer

- Defines procedures for operating the communication link
- Provides framing and sequencing

Layer 1: Physical Layer

- Defines physical means of sending data over network devices



IP: Internet Protocol

IPv4: Internet Protocol version 4

IPv4 is defined in IETF RFC 791.

IPv4 Packet Format

4	8	16	32bit	
Version	IHL	Type of service	Total length	
Identification		Flags	Fragment offset	
Time to live	Protocol	Header checksum		
Source address				
Destination address				
Option + Padding				
Data				

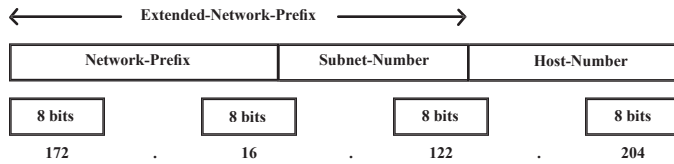
- Version – the version of IP (4 for IPv4).
- IP Header Length (IHL) – number of 32-bit words that points to the beginning of the data. It is between 5 (20bytes) to 15 (60 bytes).
- Type-of-Service – indicates the quality of service desired.

Type of service	Differentiated Services
Precedence (000 – 111)	000
D (1 = minimize delay)	0
T (1 = maximize throughput)	0
R (1 = maximize reliability)	0
C (1 = minimize cost)	1 = ENC capabl
x (reserved and set to 0)	1 = congestion experienced
- Total Length – the length of the entire IP packet in bytes. Maximum length is 65,535.
- Identification – an integer that identifies the current datagram.
- Flags – a 3-bit field of which the two low-order bits control fragmentation.

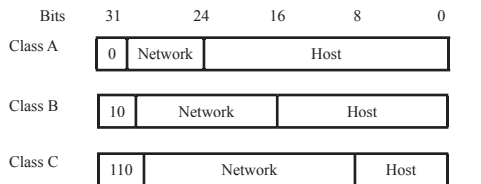
X (reserved and set to 0)	
D (1 = don't fragment)	
M (1 = more fragment)	
- Fragment Offset – indicates the position of the fragment's data relative to the beginning of the data in the original datagram.
- Time-to-Live – a counter that gradually decrements down to zero, at which point the datagram is discarded.
- Protocol - indicates which upper-layer protocol receives incoming packets after IP processing is complete. Some sample protocols:

1 ICMP	2 IGMP	6 TCP	9 IGRP
17 UDP	47 GRE	50 ESP	51 AH
57 SKIP	88 EIGRP	89 OSPF	115 L2TP
- Header Checksum – ensures IP header integrity.
- Source Address – 32 bits field specifies the sending node.

IPv4 Address Format



IPv4 Address Classes



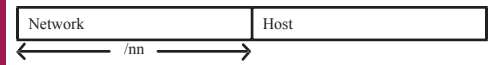
Address Class	# Network Bits	# Hosts Bits	Decimal Address Range	Number of Usable IP
Class A	8 bits	24 bits	1-126	16,777,216 (1 A)
Class B	16 bits	16 bits	128-191	1,048,544 (16 B)
Class C	24 bits	8 bits	192-223	65,534 (256 C)
Class D	Multicast		224 - 239	
Class E	Experimental		240 - 255	

- Destination Address – 32 bits field specifies the receiving node.
- Options – allows IP to support various options.

0 End of option list	1 No operation (PAD)
7 Record route	68 timestamp
131 Loose source route	137 Strict source route
- Data – contains upper-layer information.

CIDR

CIDR: Classless and Subnet Address Extensions and Supernetting



CIDR prefix length	Dotted Decimal Netmask	Number of Classfull Networks	Number of Usable IPs
/1	128.0.0.0	128 As	2,147,483,646
/2	192.0.0.0	64 As	1,073,741,822
/3	224.0.0.0	32 As	536,870,910
/4	240.0.0.0	16 As	268,435,454
/5	248.0.0.0	8 As	134,217,726
/6	252.0.0.0	4 As	67,108,862
/7	254.0.0.0	2 As	33,554,430
/8	255.0.0.0	1 A or 256 Bs	16,777,214
/9	255.128.0.0	128 Bs	8,388,606
/10	255.192.0.0	64 Bs	4,194,302
/11	255.224.0.0	32 Bs	2,097,150
/12	255.240.0.0	16 Bs	1,048,574
/13	255.248.0.0	8 Bs	524,286
/14	255.252.0.0	4 Bs	262,142
/15	255.254.0.0	2 Bs	131,070
/16	255.255.0.0	1 B or 256 Cs	65,534
/17	255.255.128.0	128 Cs	32,766
/18	255.255.192.0	64 Cs	16,382
/19	255.255.224.0	32 Cs	8,190
/20	255.255.240.0	16 Cs	4,094
/21	255.255.248.0	8 Cs	2,046
/22	255.255.252.0	4 Cs	1,022
/23	255.255.254.0	2 Cs	510
/24	255.255.255.0	1 C	254
/25	255.255.255.128	1/2 C	126
/26	255.255.255.192	1/4 C	62
/27	255.255.255.224	1/8 C	30
/28	255.255.255.240	1/16 C	14
/29	255.255.255.248	1/32 C	6
/30	255.255.255.252	1/64 C	2
/31	255.255.255.254	1/128 C	0
/32	255.255.255.255	1/256 C	0

IPv6: Internet Protocol version 6

IPv6 is defined in IETF RFC 1883 and RFC 2460.

IPv6 Packet Format

4	12	16	24	32 bit
Version	Traffic Class	Flow label		
Payload length		Next header type	Hop limit	
Source address (128 bits)				
Destination address (128 bits)				
Next header	Extension Header Information (optional and variable length)			
Data (Variable Length)				

- Version – Internet Protocol Version number (IPv6 is 6).
- Traffic class – enables a source to identify the desired delivery priority of the packets.
- Flow label – used by a source to label packets for special handling by the IPv6 router.
- Payload length – the length of the data portion of the packet.
- Next header – identifies the type of header immediately following the IPv6 header. It is similar to the “protocol” field in IPv4.
- Hop limit – specifies the maximum number of routers (hops) through which a packet can traverse before discarded.
- Source address – 128-bit address of the originator of the packet.
- Destination address – 128-bit address of the intended recipient of the packet.
- Extension Header Information – an optional field (not included in the basic header) with variable length.
 - Routing
 - Fragmentation
 - Authentication
 - Encapsulation
 - Hop-by-Hop Option
 - Destination Options

IPv6 Address Format



IPv6 Address Types

IPv6 address is classified in three types: Unicast, Multicast and Anycast.

Unicast Address: applied to one network interface.

The common global unicast address divisions:

Global Routing Prefix (N bits)	Subnet ID (64-N bits)	Interface ID (64 bits)
--------------------------------	-----------------------	------------------------

Link-local unicast address divisions:

111111010 (10 bits)	0x00...0 (54bits)	Interface ID (64 bits)
---------------------	-------------------	------------------------

Site-local unicast address divisions:

111111011 (10 bits)	0x0...0	Site Level Aggregation	Interface ID (64 bits)
---------------------	---------	------------------------	------------------------

(Interface ID is based on hardware MAC address.)

Multicast Address: applied for multiple network interfaces, and communication is conducted with all hosts with the same address.

0xFF (8 bits)	Flag (4 bits)	Scope (4 bits)	Group ID (112 bits)
---------------	---------------	----------------	---------------------

Anycast Address: applied for multiple network interfaces, but actual communication is conducted with one of them. It has the same format as the Unicast address.

IPv4-mapped IPv6 address:

0x00...0 (80 bits)	0xFFFFF (16 bits)	IPv4 Address (32 bits)
--------------------	-------------------	------------------------

IPv4-compatible IPv6 address:

0x00...0 (80 bits)	0x0000 (16 bits)	IPv4 Address (32 bits)
--------------------	------------------	------------------------

IPv4 vs. IPv6

Subjects	IPv4	IPv6	IPv6 Advantages
Address Space	4 Billion Addresses	3.4 x 10 ³⁸ addresses	79 Octillion times the IPv4 address space
Configuration	Manual or use DHCP	Universal Plug and Play (UPnP) with or without DHCP	Lower Operation Expenses and reduce error
Broadcast / Multicast	Uses both	No broadcast and has different forms of multicast	Better bandwidth efficiency
Anycast support	Not part of the original protocol	Explicit support of anycast	Allows new applications in mobility, data center
Routing efficiency	Need to process Option and Checksum fields by every router	No checksum; Extended header for options.	Improved support for extensions and options and better routing efficiency.
Network Configuration	Mostly manual and labor intensive	Facilitate the re-numbering of hosts and routers	Lower operation expenses and facilitate migration
QoS support	ToS using DIFFServ	Flow classes and flow labels	More Granular control of QoS
Security	Uses IPsec for Data packet protection	IPsec becomes the key technology to protect data and control packets	Unified framework for security and more secure computing environment
Mobility	Uses Mobile IPv4	Mobile IPv6 provides fast handover, better router optimization and hierarchical mobility	Better efficiency and scalability; Work with latest 3G mobile technologies and beyond.

TCP: Transmission Control Protocol

TCP is defined by IETF RFC 793.

TCP Header Format

16								32 bit							
Source port								Destination port							
Sequence number															
Acknowledgement number															
Offset	Rsvd	U	A	P	R	S	F	Window							
Checksum								Urgent pointer							
Option + Padding															
Data															

- Source port – Identifies points at which upper-layer source process receives TCP services.
- Destination port – Identifies points at which upper-layer Destination process receives TCP services.
- Sequence number – Specifies the number assigned to the first byte of data in the current message.
- Acknowledgment number – Contains the sequence number of the next byte of data the sender to receive.
- Offset – Indicates where the data begins.
- Reserved – Reserved for future use. Must be zero.
- Control bits (Flags) – Carry a variety of control information. The control bits may be:
 - U (URG) Urgent pointer field significant.
 - A (ACK) Acknowledgment field significant.
 - P (PSH) Push function.
 - R (RST) Reset the connection.
 - S (SYN) Synchronize sequence numbers.
 - F (FIN) No more data from sender.
- Window – Specifies the size of the sender's receive window.
- Checksum – Indicates whether the header was damaged in transit.
- Urgent Pointer – Points to the first urgent data byte in the packet.
- Option + Padding – Specifies various TCP options.
 - 0 End of Option List
 - 1 No operation (pad)
 - 2 Maximum segment size
 - 3 window scale
 - 4 Selective ACK ok
 - 8 Timestamp
- Data – contains upper-layer information.

UDP: User Datagram Protocol

UDP is defined by IETF RFC 768.

UDP Header Format

16		32 bit	
Source port		Destination port	
Length		Checksum	
Data			

- Source port – An optional field indicates the port of the sending process.
- Destination port – Identifies points at which upper-layer Destination process receives UDP services.
- Length – The length in octets of the user datagram, including the header and the data (Minimum is 8).
- Checksum -- Indicates whether the header was damaged in transit.
- Data – Contains upper-level information.

TCP/IP Utilities

ICMP

ICMP: Internet Message Control Protocol. ICMP for IPv4 is defined in IETF RFC 792 and ICMP for IPv6 is defined in IETF RFC 2463.

ICMP Header Format.

8		16		32 bit	
Type	Code	Checksum			
Identifier		Sequence number			
Address mask					

Type	Code
0 Echo Reply	0
3 Destination Unreachable	0 Net Unreachable 1 Host Unreachable 2 Protocol Unreachable 3 Port Unreachable 4 Fragmentation Needed & DF Set 5 Source Route Failed 6 Destination Network Unknown 7 Destination Host Unknown 8 Source Host Isolated 9 Network Administratively Prohibited 10 Host Administratively Prohibited 11 Network Unreachable for TOS 12 Host Unreachable for TOS 13 Communication Administratively Prohibited
4 Source Quench	0
5 Redirect	0 Redirect Datagram for the Network 1 Redirect Datagram for the Host 2 Redirect Datagram for the TOS & Network 3 Redirect Datagram for the TOS & Host
8 Echo	0
9 Router Advertisement	0
10 Router Selection	0
11 Time Exceeded	0 Time to Live exceeded in Transit 1 Fragment Reassembly Time Exceeded
12 Parameter Problem	0 Pointer indicates the error 1 Missing a Required Option 2 Bad Length
13 Timestamp	0
14 Timestamp Reply	0
15 Information Request	0
16 Information Reply	0
17 Address Mask Request	0
18 Address Mask Reply	0
30 Traceroute	0

TCPDUMP

tcpdump – dump traffic on a network

tcpdump [-aenStvx] [-c count] [-F file] [-i int] [-r file] [-s snaplen] [-w file] [-f filter_expression]

- a Convert network and broadcast addresses to names
 - c Exit after receiving count packets
 - F Filter expression in file
 - i Listen on interface
 - n Don't convert IP addresses to names
 - r Read packets from file
 - s Get snaplen bytes from each packet
 - t Don't print timestamp
 - v Verbose mode
 - w Write packets to file
 - x Display in hex
 - X Display in hex and ASCII
- filter_expression Selects which packets will be dumped.

PING

ping - send ICMP ECHO_REQUEST to network hosts

ping [-LRUbdnqrVaAB] [-c count] [-i interval] [-l preload] [-p pattern] [-s packetsize] [-t ttl] [-w deadline] [-F flowlabel] [-I interface] [-M hint] [-Q tos] [-S sndbuf] [-T timestamp option] [-W timeout] [hop ...] destination

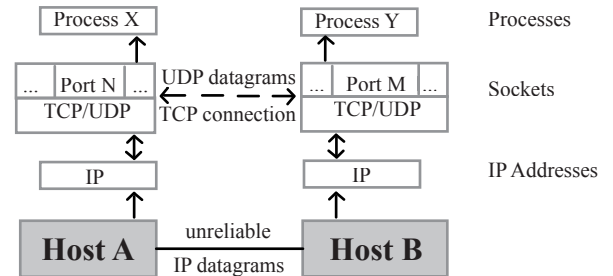
- a Audible ping.
- A Adaptive ping.
- b Allow ping to a broadcast address.
- B Do not allow ping to change source address.
- c count Stop after sending count ECHO_REQUEST packets.
- d Set the SO_DEBUG option on the socket being used.
- F flow label Allocate 20 bits flow label on echo request packets (Only ping6)
- f Flood ping.
- i interval Wait interval seconds between sending each packet.
- I interface address Set source address to specified interface address.
- l preload Sends [preload] packets not waiting for reply.
- L Suppress loopback of multicast packets.
- n Numeric output only.
- p pattern Specify (up to 16) "pad" bytes to fill out the out packet.
- Q tos Set Quality of Service-related bits in ICMP datagrams.
- q Quiet output.
- R Record route.
- r Bypass routing tables and send to a host on an attached interface.
- s packetsize Specify the number of data bytes to be sent.
- S sndbuf Set socket sndbuf.
- t ttl Set the IP Time to Live.
- T timestamp option Set special IP timestamp options
- M hint Select Path MTU Discovery strategy.
- U Print full user-to-user latency.
- v Verbose output.
- V Show version and exit.
- w deadline Specify a timeout (seconds) before ping exits.
- W timeout Time to wait for a response (seconds).

The Mostly Used TCP/UDP Port Numbers

Port No.	Protocol	Service Name	Aliases	Comment
1	TCP	tcpmux		TCP Port Service Multiplexer
2	TCP/UDP	compressnet		Management Utility
3	TCP/UDP	compressnet		Compression Process
7	TCP/UDP	echo		Echo
13	TCP/UDP	daytime		Daytime
19	TCP/UDP	chargen	ttyst source	Character generator
20	TCP	ftp-data		File Transfer
21	TCP	ftp		FTP Control
22	TCP	ssh		SSH remote login protocol
23	TCP	telnet		Telnet
25	TCP	smtp	mail	Simple Mail Transfer
37	TCP/UDP	Time		Time
39	UDP	RLP	resource	Resource Location Protocol
42	TCP/UDP	nameserver	name	Host Name Server
43	TCP	nicname	whois	Who Is
49	UDP	TACACS		TACACS: Login Host Protocol
53	TCP/UDP	domain	DNS	Domain Name Server
67	UDP	bootps	dhcps	Bootstrap Protocol Server
68	UDP	bootps	dhcpc	Bootstrap Protocol Client
69	UDP	TFTP		Trivial File Transfer Protocol
70	TCP	gopher		Gopher
79	TCP/UDP	finger		Finger
80	TCP/UDP	http	www, http	World Wide Web
88	TCP/UDP	kerberos	krb5	Kerberos
101	TCP	hostname	hostnames	NIC Host Name Server
102	TCP	iso-tsap		ISO-TSAP Class 0
107	TCP	rtelnet		Remote Telnet Service
110	TCP	pop3	postoffice	Post Office Protocol - Version 3
111	TCP/UDP	sunrpc	rpcbind portmap	SUN Remote Procedure Call
113	TCP	Auth	ident tap	Authentication Service
117	TCP	uucp-path		UUCP Path Service
118	TCP	sqlserv		SQL Services
119	TCP	nttp	usenet	Network News Transfer Protocol
123	UDP	ntp		Network Time Protocol
135	TCP/UDP	epmap	loc-srv	DCE endpoint resolution
137	TCP/UDP	netbios-ns	nbname	NETBIOS Name Service
138	UDP	netbios-dgm	nbdatagram	NETBIOS Datagram Service
139	TCP	netbios-ssn	nbssession	NETBIOS Session Service
143	TCP	imap	imap4	Internet Message Access Protocol
158	TCP	pcmail-srv	repository	PC Mail Server
161	UDP	snmp	snmp	SNMP
162	UDP	snmptrap	snmp-trap	SNMP TRAP
170	TCP	Print-srv		Network PostScript
179	TCP	BGP		Border Gateway Protocol
194	TCP	irc		Internet Relay Chat Protocol
213	UDP	ipx		IPX over IP
389	TCP	ldap		Lightweight Directory Access Protocol
401	TCP/UDP	UPS		Uninterruptible Power Supply
443	TCP/UDP	https	MCom	http protocol over TLS/SSL
445	TCP/UDP	CIFS		Microsoft-ds (CIFS)
464	TCP/UDP	kpasswd		Kerberos (v5)
500	UDP	isakmp	ike	Internet Key Exchange (IPSec)
513	TCP	login		Remote Login
513	UDP	who	whod	Database of who's logged on, average load
514	TCP	cmd	shell	Automatic Authentication
514	UDP	syslog		
515	TCP	printer	spooler	Listens for incoming connections
517	UDP	tals		Establishes TCP Connection

Port No.	Protocol	Service Name	Aliases	Comment
520	TCP	efs		Extended File Name Server
520	UDP	Routing	router routed	RIPv.1, RIPv.2
521	UDP	Routing	router routed	RIPng
525	UDP	Timed	timeserver	Timeserver
526	TCP	Tempo	newdate	Newdate
530	TCP/UDP	Courier	rpc	RPC
531	TCP	conference	chat	IRC Chat
532	TCP	netnews	readnews	Readnews
533	UDP	Netwall		For emergency broadcasts
540	TCP	Uucp	uucpd	Uucpd
543	TCP	Klogin		Kerberos login
544	TCP	Kshell	krcmd	Kerberos remote shell
550	UDP	new-rwho	new-who	New-who
554	UDP	rtsp		Real Time Stream Control Protocol
556	TCP	remotefs	rfs rfs_server	Rfs Server
560	UDP	rmonitor	rmonitord	Rmonitor
561	UDP	monitor		
636	TCP	Ldaps	sldap	LDAP over TLS/SSL
749	TCP/UDP	kerberos-adm		Kerberos administration
750	UDP	Kerberos-iv		Kerberos version IV
1080	TCP/UDP	socks		socks
1812	TCP	RADIUS		RADIUS
1813	TCP	RADIUS		RADIUS accounting

TCP/UDP Ports



Well Known Ports: from 0 through 1023
 Registered Ports: from 1024 through 49151
 Dynamic and/or Private Ports: from 49152 through 65535

Javvin

ISBN 0-9740945-4-4



Related Products:
 Network Communication Protocol Map
 Network Protocols Handbook
 Packet Analyzer

To order Javvin products:
 Javvin Technologies, Inc.
 13485 Old Oak Way
 Saratoga CA 95070 USA
www.javvin.com
help@javvin.com
 1-408-872-3881