10 Das Transmission Control Protocol (TCP)

Christian Zahler

Das TCP-Protokoll ist ein **zuverlässiges**, **verbindungsorientiertes**, **paketvermitteltes Transportprotokoll** in Computernetzwerken. Es ist Teil der Internetprotokollfamilie, der Grundlage des Internets.

Entwickelt wurde TCP von Robert E. Kahn und Vinton G. Cerf. Ihre Forschungsarbeit, die sie im Jahre 1973 begannen, dauerte mehrere Jahre. Die erste Standardisierung von TCP erfolgte deshalb erst im Jahre 1981 als RFC 793. Danach gab es viele Erweiterungen, die bis heute in neuen RFCs, einer Reihe von technischen und organisatorischen Dokumenten zum Internet, spezifiziert werden.

Im Unterschied zum verbindungslosen UDP *(User Datagram Protocol)* stellt TCP einen virtuellen Kanal zwischen zwei Endpunkten einer Netzwerkverbindung (Sockets) her. Auf diesem Kanal können in beide Richtungen Daten übertragen werden. TCP setzt in den meisten Fällen auf das IP (*Internet-Protocol*) auf, weshalb häufig (und oft nicht ganz korrekt) auch vom „TCP/IP-Protokoll“ die Rede ist. Es ist in **Schicht 4** des OSI-Referenzmodells angesiedelt.

Aufgaben:

- garantiert den sicheren Transport von Daten im Netz
- gewährleistet, dass kein Datenpaket verlorengeht und dass alle Pakete in der richtigen Reihenfolge ankommen

10.1 TCP-Header

Natürlich fügt auch das TCP-Protokoll spezielle Daten hinzu – wieder in Form eines Headers – der wie folgt aufgebaut ist: **(Bild un Text rechts oben)**

10.2 TCP-Ports

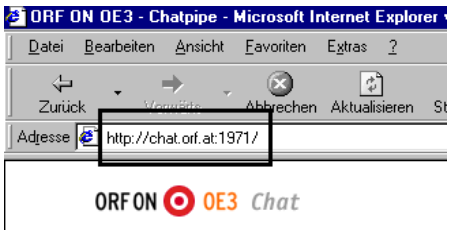
Auf TCP/IP basieren viele verschiedene Dienste wie FTP, Mail, News, DNS, etc. Um nun diese Dienste innerhalb der Protokollfamilie TCP/IP voneinander abzugrenzen, werden diese Dienste den sogenannten Ports zugewiesen. Ein Port ist nichts anderes als eine zusätzliche Kennung, die durch das TCP-Protokoll übertragen wird. Derzeit sind rund 65.536 Ports definiert, welche sich auf verschiedene Bereiche aufteilen (festgelegt in **RFC 1340** (Request for Comment, „Bitte um Kommentar“, de facto eine „Internet-Norm“).

Well known Ports	0 1023
Registered Ports	1024 49151
Dynamic and/or private Ports	49152 65535

Sender-Port		Empfänger-Port	
Sequenznummer			
Quittungsnummer			
Datenabstand	Reserviert	Flags	Fenstergröße
Prüfsumme		Urgent-Zeiger	
Optionen		Füllzeichen	

Im Verzeichnis `C:\Windows\System32\etc` (Linux: `/etc`) befindet sich eine Datei mit dem Namen `SERVICES`, in der die Portnummern für bekannte Dienste gemäß IANA abgelegt sind **(siehe Seiten am Ende des Artikels)**.

Wenn nötig, ist die Portnummer auch anzugeben (mit einem Doppelpunkt nach der eigentlichen Adresse). Ein Beispiel ist der bekannte Ö3-Chat:



Die Syntax in der URL-Zeile lautet allgemein:

```
Servertyp://
servername.domain.tld:portnumber
```

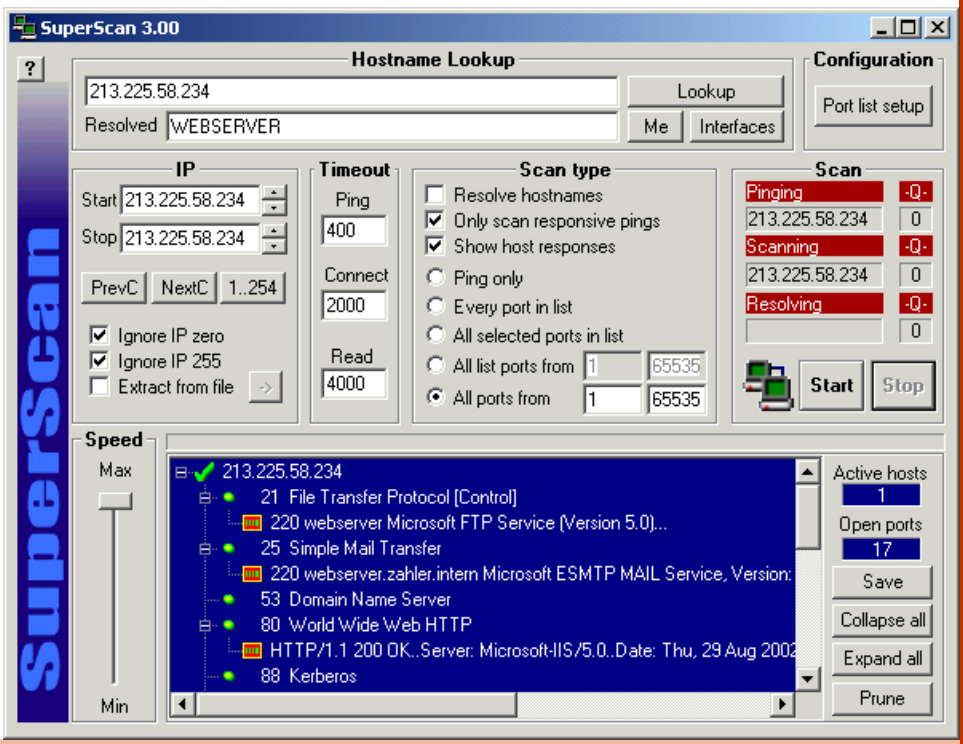
Die IP-Adresse gemeinsam mit der Portnummer (diese Kombination wird auch als **„Socket“** bezeichnet) gestattet die eindeutige Identifikation eines Dienstes, der auf einem PC läuft. So hätte also der WWW-Dienst auf einem Server mit der IP 203.225.56.204 mit der TCP-Anschlussnummer 80 die komplette Identifikation 203.225.56.204:80.

- Sender/Empfänger-Port (je 16 B): Endpunkte der Verbindung
- Sequenz-/Quittungsnummer (32 B): Synchronisation der Daten
- Datenabstand (4 B): Länge des Headers in 32 B
- Flags (6 B): Aktionen (Aufbau, Ende, ...)
- Fenstergröße (16 B): Größe des verfügbaren Empfängerbuffers (bei 0 Stop des Senders)
- Prüfsumme (16 B): Korrektheit des Headers
- Urgent-Zeiger (16 B): zur Verarbeitung von wichtigen Daten
- Optionen (24 B), Füllzeichen (6 B)

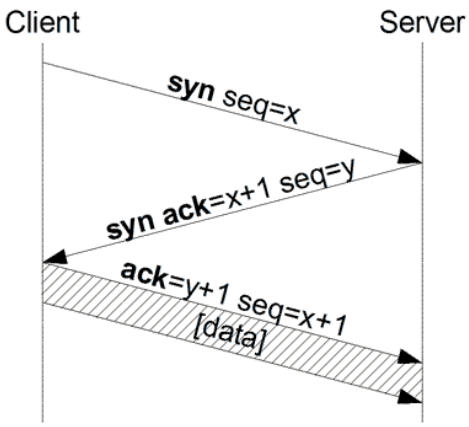
Die genaue Kenntnis der TCP-Ports ist vor allem auch wichtig, um die Sicherheit eines Netzwerkes zu gewährleisten. Mit sogenannten **„Port-Scannern“** ist es leicht möglich, herauszufinden, welche TCP-Ports auf einem Rechner oder Router freigegeben sind. Dies wiederum ermöglicht Hackern den unerwünschten Zugriff auf Firmennetze.

Beispiel für einen Port-Scanner: **„Superscan“ (Bild unten)**.

Download von Superscan zum Beispiel unter http://www.foundstone.com/



10.3 Aufbau von TCP-Verbindungen

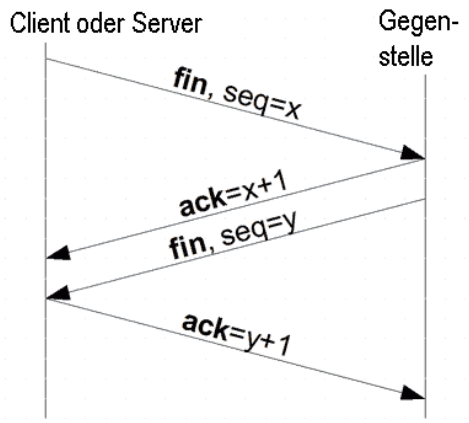


Beim Aufbau einer TCP-Verbindung kommt der so genannte **Drei-Wege-Handshake** zum Einsatz. Der Rechner, der die Verbindung aufbauen will, sendet dem anderen ein SYN-Paket (von engl. *synchronize*) mit einer Sequenznummer x. Die Sequenznummern sind dabei für die Sicherstellung einer vollständigen Übertragung in der richtigen Reihenfolge und ohne Duplikate wichtig. Es handelt sich also um ein Paket, dessen SYN-Bit im Paketkopf gesetzt ist (siehe TCP-Header). Die Start-Sequenznummer ist eine beliebige Zahl, deren Generierung von der jeweiligen TCP-Implementierung abhängig ist. Sie sollte jedoch möglichst zufällig sein, um Sicherheitsrisiken zu vermeiden.

Die Gegenstelle **(siehe Skizze)** empfängt das Paket. Ist der Port geschlossen, antwortet sie mit einem TCP-RST um zu signalisieren, dass keine Verbindung aufgebaut werden kann. Ist der Port geöffnet, sendet sie in einem eigenen SYN-Paket im Gegenzug ihre Start-Sequenznummer y (die ebenfalls beliebig und unabhängig von der Start-Sequenznummer der Gegenstelle ist). Zugleich bestätigt sie den Erhalt des ersten SYN-Pakets, indem sie die Sequenznummer x um eins erhöht und im ACK-Teil (von engl. *acknowledgment* = Bestätigung) des Headers zurückschickt.

Der Client bestätigt zuletzt den Erhalt des SYN/ACK-Pakets durch das Senden eines eigenen ACK-Pakets mit der Sequenznummer y+1. Dieser Vorgang wird auch als „*Forward Acknowledgement*" bezeichnet. Außerdem sendet der Client den Wert x+1 aus Sicherheitsgründen ebenso zurück. Dieses ACK-Segment erhält der Server, das ACK-Segment ist durch das gesetzte ACK-Flag gekennzeichnet. Die Verbindung ist damit aufgebaut.

10.4 Verbindungsabbau



Der geregelte Verbindungsabbau erfolgt ähnlich. Statt des SYN-Bits kommt das FIN-Bit (von engl. *finish* = Ende, Abschluss) zum Einsatz, welches anzeigt, dass keine Daten mehr vom Sender kommen. Der Erhalt des Pakets wird wiederum mittels ACK bestätigt. Der Empfänger des FIN-Pakets sendet zuletzt seinerseits ein FIN-Paket, das ihm ebenfalls bestätigt wird.

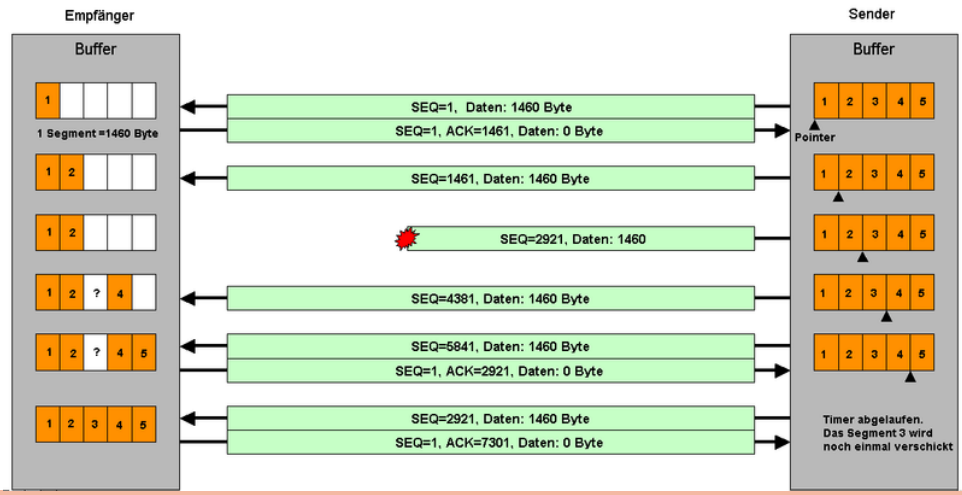
Obwohl eigentlich vier Wege genutzt werden, handelt es sich beim Verbindungsabbau auch um einen Drei-Wege-Handshake, da die ACK- und FIN-Operationen vom Server zum Client als ein Weg gewertet werden.

Zudem ist ein verkürztes Verfahren möglich, bei dem FIN und ACK genau wie beim Verbindungsaufbau im selben Paket untergebracht werden. Die *maximum segment lifetime* (MSL) ist die maximale Zeit, die ein Segment im Netzwerk verbringen kann, bevor es verworfen wird. Nach dem Senden des letzten ACKs wechselt der Client in einen zwei MSL andauernden Wartezustand (*Waitstate*), in dem alle verspäteten Segmente verworfen werden. Dadurch wird sichergestellt, dass keine verspäteten Segmente als Teil einer neuen Verbindung fehlinterpretiert werden. Außerdem wird eine korrekte Verbindungsterminierung sichergestellt. Geht ACK y+1 verloren, läuft beim Server der Timer ab, und das LAST_ACK Segment wird erneut übertragen.

10.5 Beispiel für eine TCP-Datenübertragung

Der Sender schickt sein erstes TCP-Segment mit einer Sequenznummer SEQ=1 (variiert) und einer Nutzdatenlänge von 1460 Byte an den Empfänger. Der Empfänger bestätigt es mit einem TCP-Header ohne Daten mit ACK=1461 und fordert damit das zweite TCP -Segment ab dem Byte Nummer 1461 beim Sender an. Dieser schickt es dann mit einem TCP-Segment und SEQ=1461 an den Empfänger. Dieser bestätigt es wieder mit einem ACK=2921 und so weiter. Der Empfänger braucht nicht jedes TCP-Segment zu bestätigen, wenn diese zusammenhängend sind. Empfängt er die TCP-Segmente 1–5, so braucht er nur das letzte TCP-Segment zu bestätigen. Fehlt zum Beispiel das TCP-Segment 3, weil es verloren gegangen ist, so kann er nur die 1 und die 2 bestätigen, 4 und 5 jedoch noch nicht. Da der Sender keine Bestätigung für die 3 bekommt, läuft sein Timer ab, und er verschickt die 3 noch einmal. Kommt die 3 beim Empfänger an, so bestätigt er alle fünf TCP-Segmente. Der Sender startet für jedes TCP-Segment, welches er auf die Reise schickt, einen Timer (RTT).

Ablauf einer TCP-Datenübertragung (Quelle: Wikipedia)



```
# Copyright (c) 1993-2004 Microsoft Corp.
#
# This file contains port numbers for well-known services defined by IANA
#
# Format:
#
# <service name>  <port number>/<protocol>  [aliases...]   [#<comment>]
#

echo                7/tcp
echo                7/udp
discard             9/tcp    sink null
discard             9/udp    sink null
systat             11/tcp    users                #Active users
systat             11/udp    users                #Active users
daytime            13/tcp
daytime            13/udp
qotd               17/tcp    quote                #Quote of the day
qotd               17/udp    quote                #Quote of the day
chargen            19/tcp    ttytst source        #Character generator
chargen            19/udp    ttytst source        #Character generator
ftp-data           20/tcp                         #FTP, data
ftp                21/tcp                         #FTP. control
ssh                22/tcp                         #SSH Remote Login Protocol
telnet             23/tcp
smtp               25/tcp    mail                 #Simple Mail Transfer Protocol
time               37/tcp    timserver
time               37/udp    timserver
rlp                39/udp    resource             #Resource Location Protocol
nameserver         42/tcp    name                 #Host Name Server
nameserver         42/udp    name                 #Host Name Server
nicname            43/tcp    whois
domain             53/tcp                         #Domain Name Server
domain             53/udp                         #Domain Name Server
bootps             67/udp    dhcps                #Bootstrap Protocol Server
bootpc             68/udp    dhcpc                #Bootstrap Protocol Client
tftp               69/udp                         #Trivial File Transfer
gopher             70/tcp
finger             79/tcp
http               80/tcp    www www-http         #World Wide Web
hosts2-ns          81/tcp                         #HOSTS2 Name Server
hosts2-ns          81/udp                         #HOSTS2 Name Server
kerberos           88/tcp    krb5 kerberos-sec    #Kerberos
kerberos           88/udp    krb5 kerberos-sec    #Kerberos
hostname          101/tcp    hostnames            #NIC Host Name Server
iso-tsap          102/tcp                         #ISO-TSAP Class 0
rtelnet           107/tcp                         #Remote Telnet Service
pop2              109/tcp    postoffice           #Post Office Protocol - Version 2
pop3              110/tcp                         #Post Office Protocol - Version 3
sunrpc            111/tcp    rpcbind portmap      #SUN Remote Procedure Call
sunrpc            111/udp    rpcbind portmap      #SUN Remote Procedure Call
auth              113/tcp    ident tap            #Identification Protocol
uucp-path         117/tcp
sqlserv           118/tcp                         #SQL Services
nntp              119/tcp    usenet               #Network News Transfer Protocol
ntp               123/udp                         #Network Time Protocol
epmap             135/tcp    loc-srv              #DCE endpoint resolution
epmap             135/udp    loc-srv              #DCE endpoint resolution
netbios-ns        137/tcp    nbname               #NETBIOS Name Service
netbios-ns        137/udp    nbname               #NETBIOS Name Service
netbios-dgm       138/udp    nbdatagram           #NETBIOS Datagram Service
netbios-ssn       139/tcp    nbsession            #NETBIOS Session Service
imap              143/tcp    imap4                #Internet Message Access Protocol
sql-net           150/tcp
sqlsrv            156/tcp
pcmail-srv        158/tcp                         #PCMail Server
snmp              161/udp                         #SNMP
snmptrap          162/udp    snmp-trap            #SNMP trap
print-srv         170/tcp                         #Network PostScript
bgp               179/tcp                         #Border Gateway Protocol
irc               194/tcp                         #Internet Relay Chat Protocol
ipx               213/udp                         #IPX over IP
rtsps             322/tcp
rtsps             322/udp
mftp              349/tcp
mftp              349/udp
ldap              389/tcp                         #Lightweight Directory Access Protocol
https             443/tcp    MCom                 #HTTP over TLS/SSL
https             443/udp    MCom                 #HTTP over TLS/SSL
microsoft-ds      445/tcp
microsoft-ds      445/udp
kpasswd           464/tcp                         # Kerberos (v5)
kpasswd           464/udp                         # Kerberos (v5)
isakmp            500/udp    ike                  #Internet Key Exchange
crs               507/tcp                         #Content Replication System
crs               507/udp                         #Content Replication System
exec              512/tcp                         #Remote Process Execution
biff              512/udp    comsat
login             513/tcp                         #Remote Login
who               513/udp    whod
cmd               514/tcp    shell
syslog            514/udp
printer           515/tcp    spooler
talk              517/udp
```

```
ntalk           518/udp
efs             520/tcp                         #Extended File Name Server
router          520/udp    route routed
ulp             522/tcp
ulp             522/udp
timed           525/udp    timeserver
tempo           526/tcp    newdate
irc-serv        529/tcp
irc-serv        529/udp
courier         530/tcp    rpc
conference      531/tcp    chat
netnews         532/tcp    readnews
netwall         533/udp                         #For emergency broadcasts
uucp            540/tcp    uucpd
klogin          543/tcp                         #Kerberos login
kshell          544/tcp    krcmd                #Kerberos remote shell
dhcpv6-client   546/tcp                         #DHCPv6 Client
dhcpv6-client   546/udp                         #DHCPv6 Client
dhcpv6-server   547/tcp                         #DHCPv6 Server
dhcpv6-server   547/udp                         #DHCPv6 Server
afpovertcp      548/tcp                         #AFP over TCP
afpovertcp      548/udp                         #AFP over TCP
new-rwho        550/udp    new-who
rtsp            554/tcp                         #Real Time Stream Control Protocol
rtsp            554/udp                         #Real Time Stream Control Protocol
remotefs        556/tcp    rfs rfs_server
rmonitor        560/udp    rmonitord
monitor         561/udp
nntps           563/tcp    snntp                #NNTP over TLS/SSL
nntps           563/udp    snntp                #NNTP over TLS/SSL
whoami          565/tcp
whoami          565/udp
ms-shuttle      568/tcp                         #Microsoft shuttle
ms-shuttle      568/udp                         #Microsoft shuttle
ms-rome         569/tcp                         #Microsoft rome
ms-rome         569/udp                         #Microsoft rome
http-rpc-epmap  593/tcp                         #HTTP RPC Ep Map
http-rpc-epmap  593/udp                         #HTTP RPC Ep Map
hmmp-ind        612/tcp                         #HMMP Indication
hmmp-ind        612/udp                         #HMMP Indication
hmmp-op         613/tcp                         #HMMP Operation
hmmp-op         613/udp                         #HMMP Operation
ldaps           636/tcp    sldap                #LDAP over TLS/SSL
doom            666/tcp                         #Doom Id Software
doom            666/udp                         #Doom Id Software
msexch-routing  691/tcp                         #MS Exchange Routing
msexch-routing  691/udp                         #MS Exchange Routing
kerberos-adm    749/tcp                         #Kerberos administration
kerberos-adm    749/udp                         #Kerberos administration
kerberos-iv     750/udp                         #Kerberos version IV
mdbs_daemon     800/tcp
mdbs_daemon     800/udp
ftps-data       989/tcp                         #FTP data, over TLS/SSL
ftps            990/tcp                         #FTP control, over TLS/SSL
telnets         992/tcp                         #Telnet protocol over TLS/SSL
imaps           993/tcp                         #IMAP4 protocol over TLS/SSL
ircs            994/tcp                         #IRC protocol over TLS/SSL
pop3s           995/tcp    spop3                #pop3 protocol over TLS/SSL (was spop3)
pop3s           995/udp    spop3                #pop3 protocol over TLS/SSL (was spop3)
kpop           1109/tcp                         #Kerberos POP
nfsd-status    1110/tcp                         #Cluster status info
nfsd-keepalive 1110/udp                         #Client status info
nfa            1155/tcp                         #Network File Access
nfa            1155/udp                         #Network File Access
activesync     1034/tcp                         #ActiveSync Notifications
phone          1167/udp                         #Conference calling
opsmgr         1270/tcp                         #Microsoft Operations Manager
opsmgr         1270/udp                         #Microsoft Operations Manager
ms-sql-s       1433/tcp                         #Microsoft-SQL-Server
ms-sql-s       1433/udp                         #Microsoft-SQL-Server
ms-sql-m       1434/tcp                         #Microsoft-SQL-Monitor
ms-sql-m       1434/udp                         #Microsoft-SQL-Monitor
ms-sna-server  1477/tcp
ms-sna-server  1477/udp
ms-sna-base    1478/tcp
ms-sna-base    1478/udp
wins           1512/tcp                         #Microsoft Windows Internet Name Service
wins           1512/udp                         #Microsoft Windows Internet Name Service
ingreslock     1524/tcp    ingres
stt            1607/tcp
stt            1607/udp
l2tp           1701/udp                         #Layer Two Tunneling Protocol
pptconference  1711/tcp
pptconference  1711/udp
pptp           1723/tcp                         #Point-to-point tunnelling protocol
msiccp         1731/tcp
msiccp         1731/udp
remote-winsock 1745/tcp
remote-winsock 1745/udp
ms-streaming   1755/tcp
ms-streaming   1755/udp
msmq           1801/tcp                         #Microsoft Message Queue
msmq           1801/udp                         #Microsoft Message Queue
radius         1812/udp                         #RADIUS authentication protocol
```

```
radacct          1813/udp                    #RADIUS accounting protocol
msnp             1863/tcp
msnp             1863/udp
ssdp             1900/tcp
ssdp             1900/udp
close-combat     1944/tcp
close-combat     1944/udp
nfsd             2049/udp    nfs             #NFS server
knetd            2053/tcp                    #Kerberos de-multiplexor
mzap             2106/tcp                    #Multicast-Scope Zone Announcement Protocol
mzap             2106/udp                    #Multicast-Scope Zone Announcement Protocol
qwave            2177/tcp                    #QWAVE
qwave            2177/udp                    #QWAVE Experiment Port
directplay       2234/tcp                    #DirectPlay
directplay       2234/udp                    #DirectPlay
ms-olap3         2382/tcp                    #Microsoft OLAP 3
ms-olap3         2382/udp                    #Microsoft OLAP 3
ms-olap4         2383/tcp                    #Microsoft OLAP 4
ms-olap4         2383/udp                    #Microsoft OLAP 4
ms-olap1         2393/tcp                    #Microsoft OLAP 1
ms-olap1         2393/udp                    #Microsoft OLAP 1
ms-olap2         2394/tcp                    #Microsoft OLAP 2
ms-olap2         2394/udp                    #Microsoft OLAP 2
ms-theater       2460/tcp
ms-theater       2460/udp
wlbs             2504/tcp                    #Microsoft Windows Load Balancing Server
wlbs             2504/udp                    #Microsoft Windows Load Balancing Server
ms-v-worlds      2525/tcp                    #Microsoft V-Worlds
ms-v-worlds      2525/udp                    #Microsoft V-Worlds
sms-rcinfo       2701/tcp                    #SMS RCINFO
sms-rcinfo       2701/udp                    #SMS RCINFO
sms-xfer         2702/tcp                    #SMS XFER
sms-xfer         2702/udp                    #SMS XFER
sms-chat         2703/tcp                    #SMS CHAT
sms-chat         2703/udp                    #SMS CHAT
sms-remctrl      2704/tcp                    #SMS REMCTRL
sms-remctrl      2704/udp                    #SMS REMCTRL
msolap-ptp2      2725/tcp                    #MSOLAP PTP2
msolap-ptp2      2725/udp                    #MSOLAP PTP2
icslap           2869/tcp
icslap           2869/udp
cifs             3020/tcp
cifs             3020/udp
xbox             3074/tcp                    #Microsoft Xbox game port
xbox             3074/udp                    #Microsoft Xbox game port
ms-dotnetster    3126/tcp                    #Microsoft .NET ster port
ms-dotnetster    3126/udp                    #Microsoft .NET ster port
ms-rule-engine   3132/tcp                    #Microsoft Business Rule Engine Update Service
ms-rule-engine   3132/udp                    #Microsoft Business Rule Engine Update Service
msft-gc          3268/tcp                    #Microsoft Global Catalog
msft-gc          3268/udp                    #Microsoft Global Catalog
msft-gc-ssl      3269/tcp                    #Microsoft Global Catalog with LDAP/SSL
msft-gc-ssl      3269/udp                    #Microsoft Global Catalog with LDAP/SSL
ms-cluster-net   3343/tcp                    #Microsoft Cluster Net
ms-cluster-net   3343/udp                    #Microsoft Cluster Net
ms-wbt-server    3389/tcp                    #MS WBT Server
ms-wbt-server    3389/udp                    #MS WBT Server
ms-la            3535/tcp                    #Microsoft Class Server
ms-la            3535/udp                    #Microsoft Class Server
pnrp-port        3540/tcp                    #PNRP User Port
pnrp-port        3540/udp                    #PNRP User Port
teredo           3544/tcp                    #Teredo Port
teredo           3544/udp                    #Teredo Port
p2pgroup         3587/tcp                    #Peer to Peer Grouping
p2pgroup         3587/udp                    #Peer to Peer Grouping
upnp-discovery   3702/tcp                    #UPNP v2 Discovery
dvcprov-port     3776/tcp                    #Device Provisioning Port
dvcprov-port     3776/udp                    #Device Provisioning Port
msfw-control     3847/tcp                    #Microsoft Firewall Control
msdts1           3882/tcp                    #DTS Service Port
sdp-portmapper   3935/tcp                    #SDP Port Mapper Protocol
sdp-portmapper   3935/udp                    #SDP Port Mapper Protocol
net-device       4350/tcp                    #Net Device
net-device       4350/udp                    #Net Device
ipsec-msft       4500/tcp                    #Microsoft IPsec NAT-T
ipsec-msft       4500/udp                    #Microsoft IPsec NAT-T
llmnr            5355/tcp                    #LLMNR
llmnr            5355/udp                    #LLMNR
rrac             5678/tcp                    #Remote Replication Agent Connection
rrac             5678/udp                    #Remote Replication Agent Connection
dccm             5679/tcp                    #Direct Cable Connect Manager
dccm             5679/udp                    #Direct Cable Connect Manager
ms-licensing     5720/tcp                    #Microsoft Licensing
ms-licensing     5720/udp                    #Microsoft Licensing
directplay8      6073/tcp                    #DirectPlay8
directplay8      6073/udp                    #DirectPlay8
man              9535/tcp                    #Remote Man Server
rasadv           9753/tcp
rasadv           9753/udp
imip-channels   11320/tcp                    #IMIP Channels Port
imip-channels   11320/udp                    #IMIP Channels Port
directplaysrvr  47624/tcp                    #Direct Play Server
directplaysrvr  47624/udp                    #Direct Play Server
```