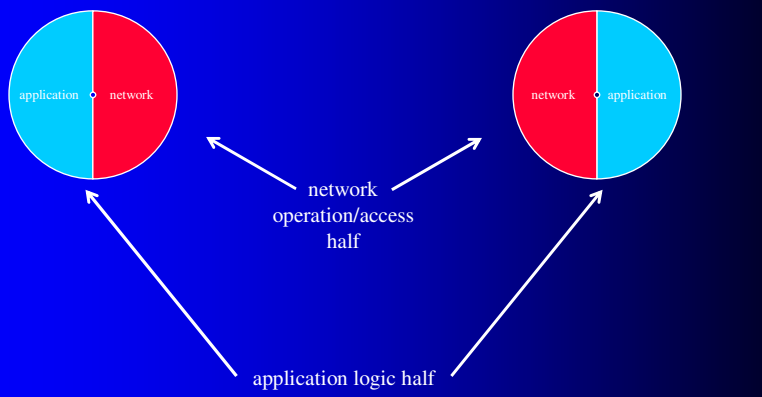
Linux Networking: nc
-- network cat

David Morgan

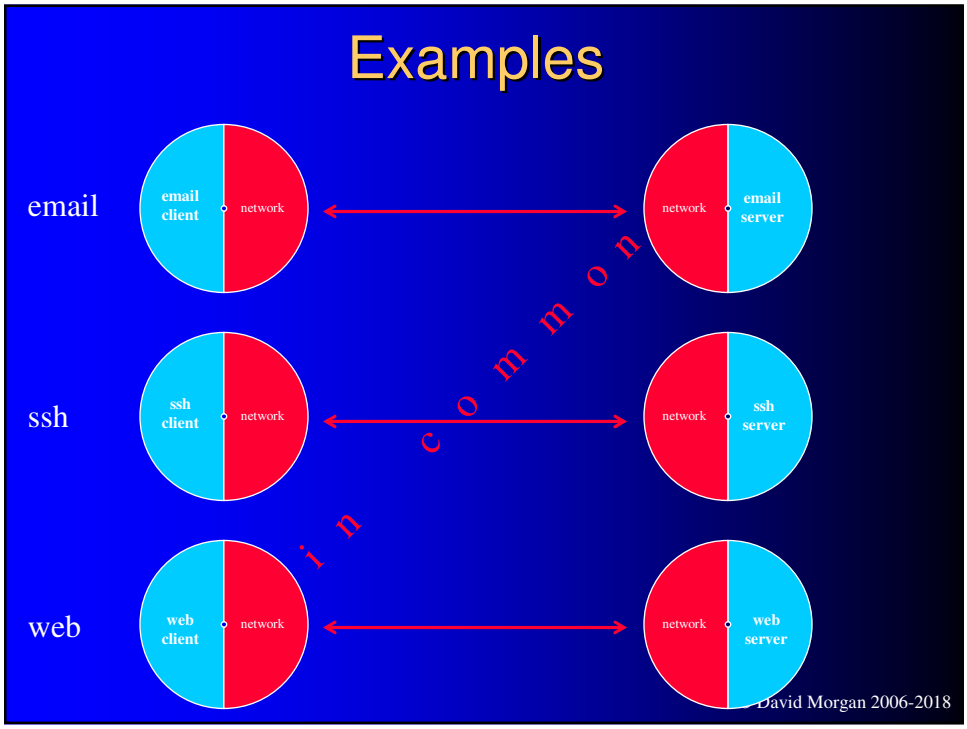
Client and server programs
-- each contain 2 halves

a client program

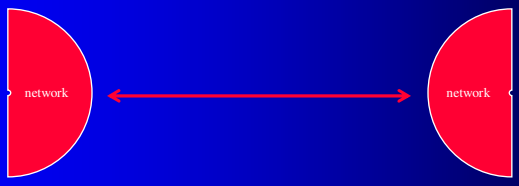
matching server program



Examples



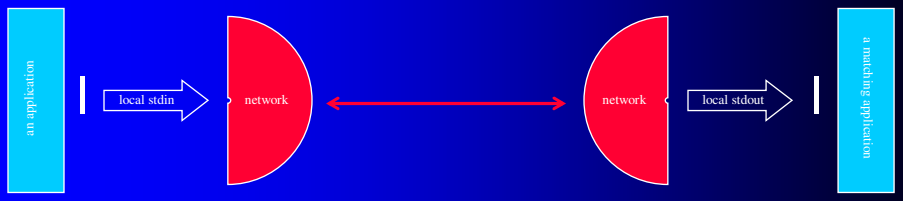
Two copies of netcat



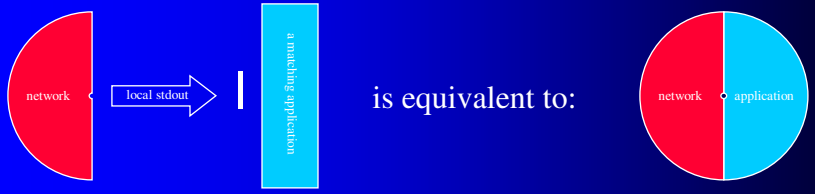
the network mechanism that clients and servers use,
stand-alone and generic

no application logic

Marry them to (non-network) applications



Equivalency

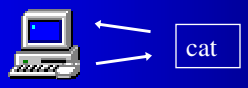


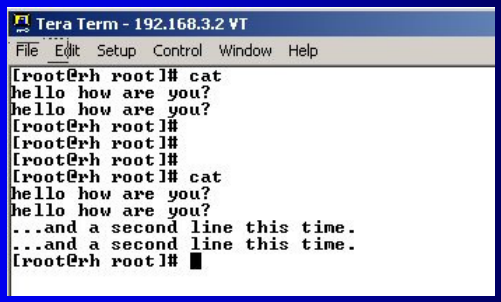
cat command – input-to-output

- best known as the file dumper
- but only if you give it a file, special case
- general case, copies standard input to standard output

cat – input and output

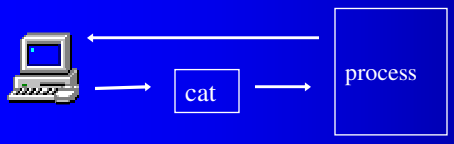
Local





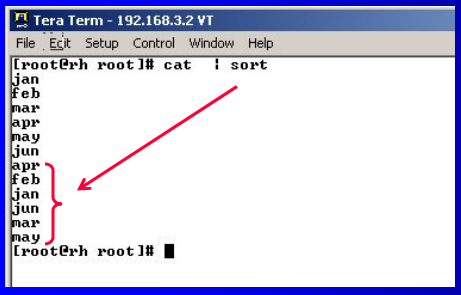
cat and pipes – input and output

Local



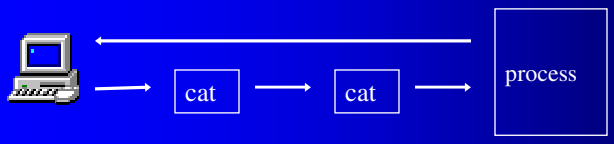
Input to cat becomes input to process.

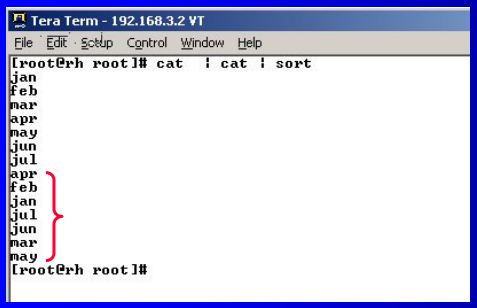
Output from process becomes pipeline's output.



cat and pipes – extended

Local





Input to cat becomes input to cat, becomes input to process.

Output from process becomes pipeline's output.

net cat (nc) command

- network version of cat
- puts output of one to input of other ***trans-net***

Client

step 2:

nc 192.168.3.19 5600

"run as a client, send any input to port 5600 at 192.168.3.19"

Server

(192.168.3.19)

step 1:

nc –l –p 5600*

"run as a service, listen on port 5600"

* or "nc –p 5600" (depending which nc version)

Possible sources/destinations

where nc could get from and put to

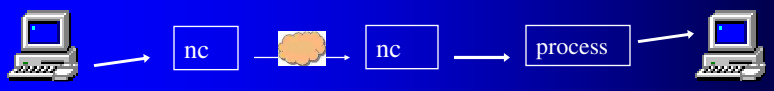
	input/source	output/destination
local	netcat's stdin	netcat's stdout
network	socket reads	socket writes

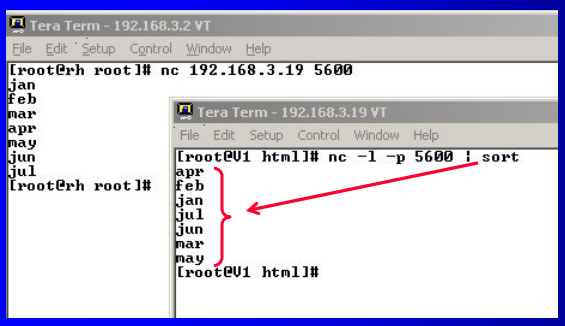
source-to-destination mapping

If it comes from:		Then it goes to:
netcat's stdin	→	a socket write
a socket read	→	netcat's stdout

nc – input and output

Local Remote



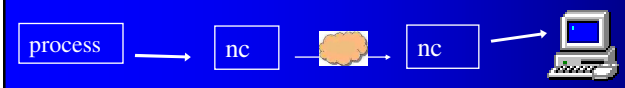


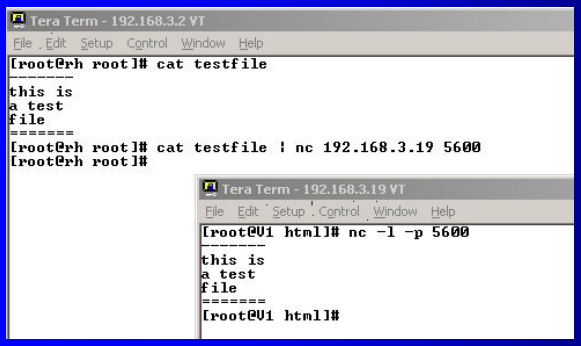
Input to nc on local machine, transferred to remote side, becomes input to process.

Output from process on remote machine, is the output there.

nc – local file on remote screen

Local Remote



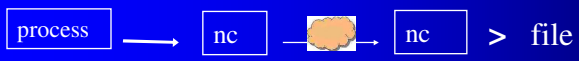


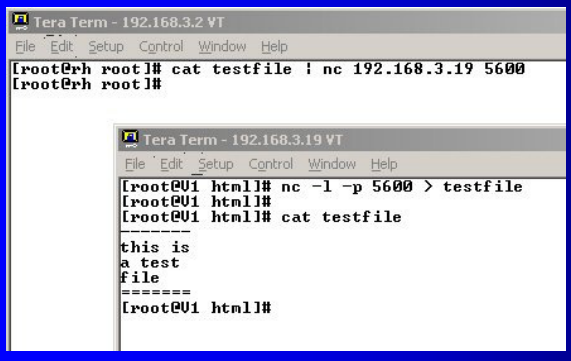
Input to nc on local machine, transferred to remote side, becomes network input to nc on remote machine.

Output from nc on remote machine, is the output there.

local file to remote disk - poor man's ftp

Local Remote

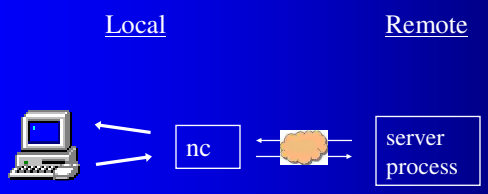




Input to nc on local machine, transferred to remote side, becomes network input to nc on remote machine.

Output from nc on remote machine, is deposited in a file there.

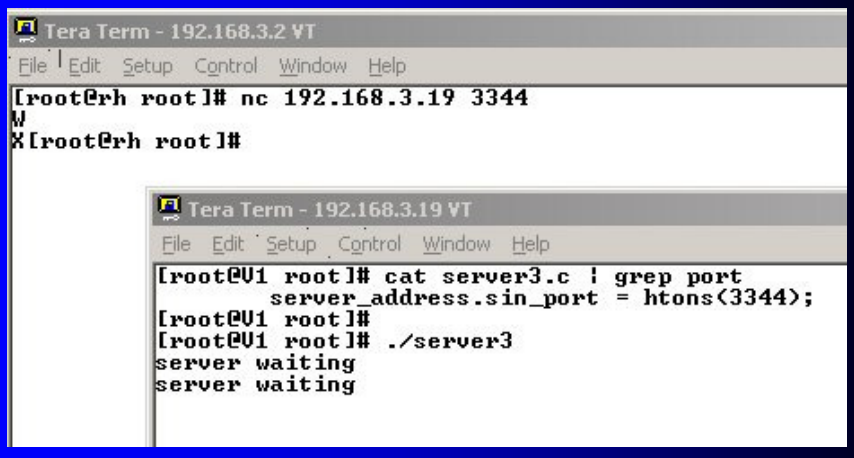
nc – server interaction



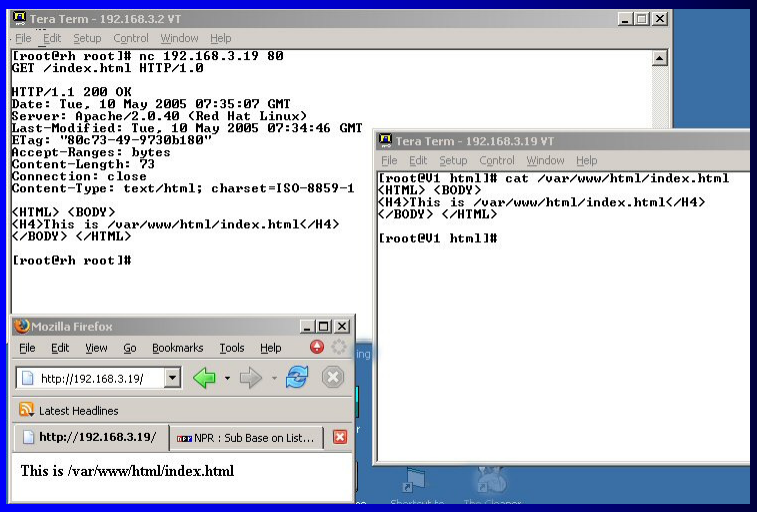
Input to nc on local machine, transferred to remote side, becomes network input to server process.

Network output from server process, transferred to local side, becomes output from nc.

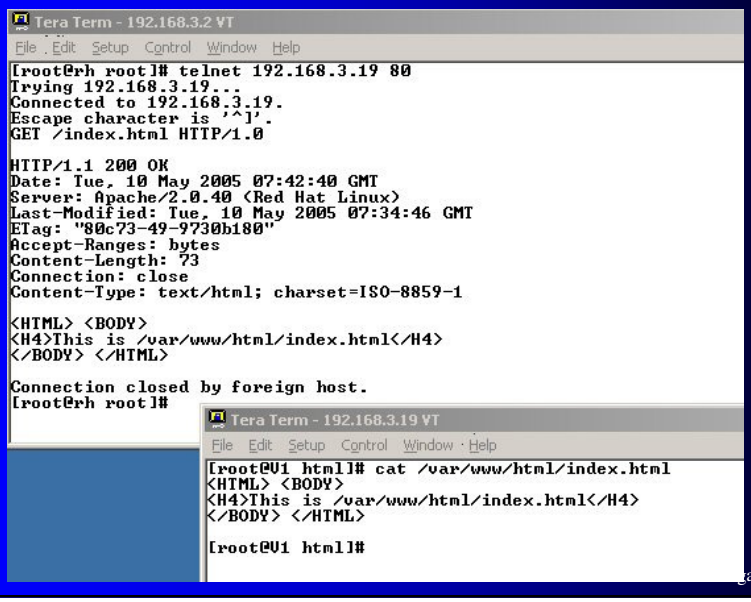
nc –interaction w/sample server



nc – server interaction w/apache



telnet – interaction w/apache



Multiple versions

- Original (by Hobbit)
- BSD (Fedora 4)
  - nc-1.78-2.i386.rpm
  - http://www.openbsd.org/cgi-bin/cvsweb/src/usr.bin/nc/
- GNU netcat
  - netcat-0.7.1-1.i386.rpm
  - http://netcat.sourceforge.net/