

Linux Networking: nc

-- network cat

David Morgan

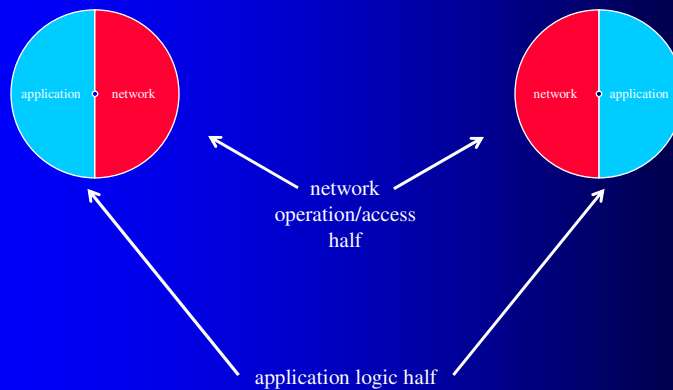
© David Morgan 2006-2018

Client and server programs

-- each contain 2 halves

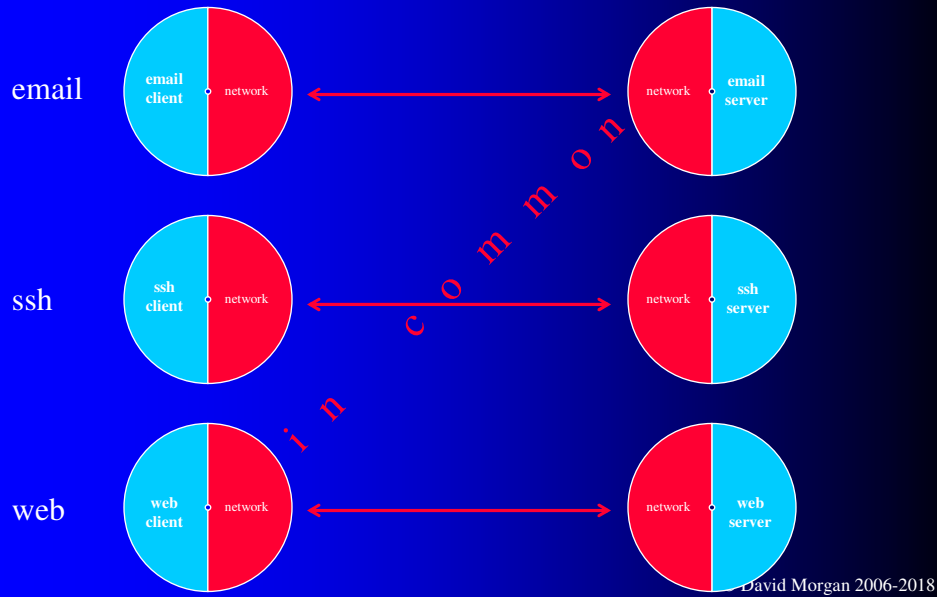
a client program

matching server program

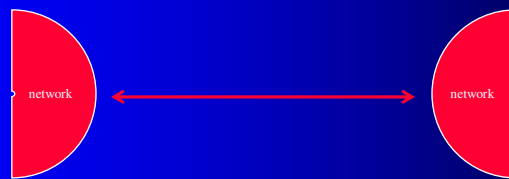


© David Morgan 2006-2018

Examples



Two copies of netcat

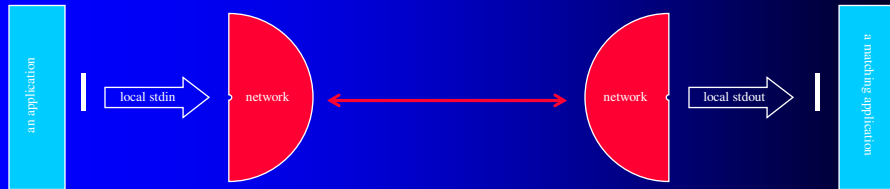


the network mechanism that clients and servers use,
stand-alone and generic

no application logic

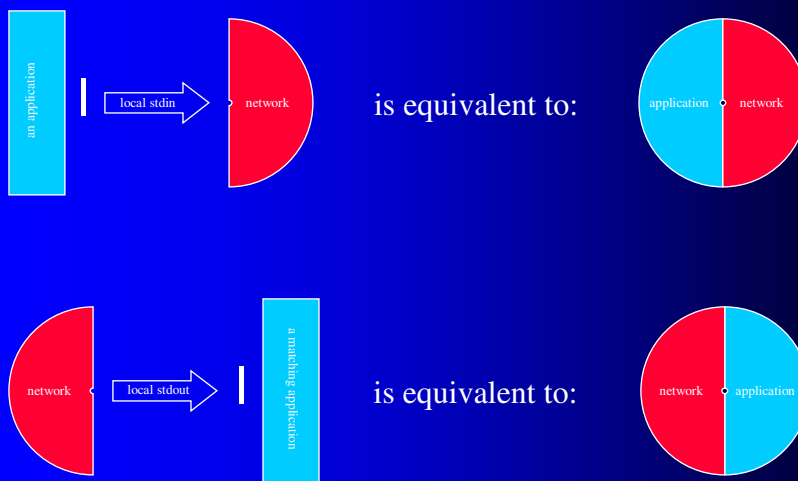
© David Morgan 2006-2018

Marry them to (non-network) applications



© David Morgan 2006-2018

Equivalency



© David Morgan 2006-2018

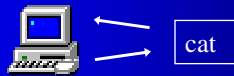
cat command – input-to-output

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

© David Morgan 2006-2018

cat – input and output

Local

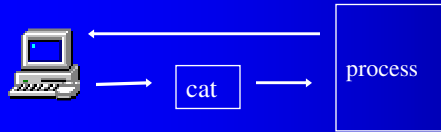


```
Tera Term - 192.168.3.2 VT
File Edit Setup Control Window Help
[root@rh root]# cat
hello how are you?
hello how are you?
[root@rh root]#
[root@rh root]#
[root@rh root]#
[root@rh root]# cat
hello how are you?
hello how are you?
...and a second line this time.
...and a second line this time.
[root@rh root]#
```

© David Morgan 2006-2018

cat and pipes – input and output

Local



Input to cat becomes input to process.

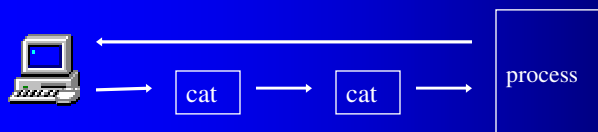
Output from process becomes pipeline's output.

```
Tera Term - 192.168.3.2 VT
File Edit Setup Control Window Help
[root@rh root]# cat | sort
jan
feb
mar
apr
may
jun
apr
feb
jan
jun
mar
may
[root@rh root]#
```

© David Morgan 2006-2018

cat and pipes – extended

Local



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

Output from process becomes pipeline's output.

```
Tera Term - 192.168.3.2 VT
File Edit Setup Control Window Help
[root@rh root]# cat | cat | sort
jan
feb
mar
apr
may
jun
jul
apr
feb
jan
jul
jun
mar
may
[root@rh root]#
```

© David Morgan 2006-2018

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)

© David Morgan 2006-2018

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

© David Morgan 2006-2018

source-to-destination mapping

If it comes from:

Then it goes to:

netcat's stdin



a socket write

a socket read



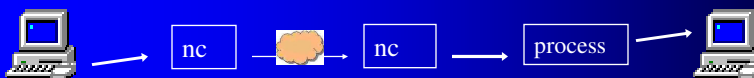
netcat's stdout

© David Morgan 2006-2018

nc – input and output

Local

Remote



```
Tera Term - 192.168.3.2 VT
File Edit Setup Control Window Help
[root@rh root]# nc 192.168.3.19 5600
jan
feb
mar
apr
may
jun
jul
[root@rh root]#

Tera Term - 192.168.3.19 VT
File Edit Setup Control Window Help
[root@U1 htntl]# nc -l -p 5600 | sort
apr
feb
jan
jul
jun
mar
may
[root@U1 htntl]#
```

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

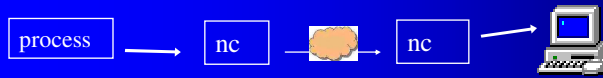
Output from process on remote machine, is the output there.

© David Morgan 2006-2018

nc – local file on remote screen

Local

Remote



```
Tera Term - 192.168.3.2 VT
File Edit Setup Control Window Help
[root@rh root]# cat testfile
-----
this is
a test
file
=====
[root@rh root]# cat testfile | nc 192.168.3.19 5600
[root@rh root]#
```

```
Tera Term - 192.168.3.19 VT
File Edit Setup Control Window Help
[root@U1 html]# nc -l -p 5600
-----
this is
a test
file
=====
[root@U1 html]#
```

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.

© David Morgan 2006-2018

local file to remote disk - poor man's ftp

Local

Remote



```
Tera Term - 192.168.3.2 VT
File Edit Setup Control Window Help
[root@rh root]# cat testfile | nc 192.168.3.19 5600
[root@rh root]#
```

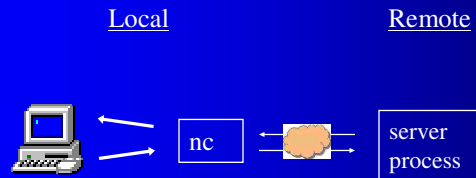
```
Tera Term - 192.168.3.19 VT
File Edit Setup Control Window Help
[root@U1 html]# nc -l -p 5600 > testfile
[root@U1 html]#
[root@U1 html]# cat testfile
-----
this is
a test
file
=====
[root@U1 html]#
```

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.

© David Morgan 2006-2018

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.

© David Morgan 2006-2018

nc –interaction w/sample server

```
Tera Term - 192.168.3.2 VT
File Edit Setup Control Window Help
[root@rh root]# nc 192.168.3.19 3344
W
X[root@rh root]#

Tera Term - 192.168.3.19 VT
File Edit Setup Control Window Help
[root@U1 root]# cat server3.c | grep port
server_address.sin_port = htons(3344);
[root@U1 root]#
[root@U1 root]# ./server3
server waiting
server waiting
```

© David Morgan 2006-2018

nc – server interaction w/apache

```
Tera Term - 192.168.3.2 VT
File Edit Setup Control Window Help
[root@rh root]# nc 192.168.3.19 80
GET /index.html HTTP/1.0

HTTP/1.1 200 OK
Date: Tue, 10 May 2005 07:35:07 GMT
Server: Apache/2.0.40 (Red Hat Linux)
Last-Modified: Tue, 10 May 2005 07:34:46 GMT
ETag: "80c73-49-9730b180"
Accept-Ranges: bytes
Content-Length: 73
Connection: close
Content-Type: text/html; charset=ISO-8859-1

<HTML> <BODY>
<H4>This is /var/www/html/index.html</H4>
</BODY> </HTML>

[root@rh root]#

Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://192.168.3.19/
Latest Headlines
http://192.168.3.19/ NPR: Sub Base on List...
This is /var/www/html/index.html
```

© David Morgan 2006-2018

telnet – interaction w/apache

```
Tera Term - 192.168.3.2 VT
File Edit Setup Control Window Help
[root@rh root]# telnet 192.168.3.19 80
Trying 192.168.3.19...
Connected to 192.168.3.19.
Escape character is '^I'.
GET /index.html HTTP/1.0

HTTP/1.1 200 OK
Date: Tue, 10 May 2005 07:42:40 GMT
Server: Apache/2.0.40 (Red Hat Linux)
Last-Modified: Tue, 10 May 2005 07:34:46 GMT
ETag: "80c73-49-9730b180"
Accept-Ranges: bytes
Content-Length: 73
Connection: close
Content-Type: text/html; charset=ISO-8859-1

<HTML> <BODY>
<H4>This is /var/www/html/index.html</H4>
</BODY> </HTML>

Connection closed by foreign host.
[root@rh root]#

Tera Term - 192.168.3.19 VT
File Edit Setup Control Window Help
[root@U1 html]# cat /var/www/html/index.html
<HTML> <BODY>
<H4>This is /var/www/html/index.html</H4>
</BODY> </HTML>

[root@U1 html]#
```

© David Morgan 2006-2018

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/>