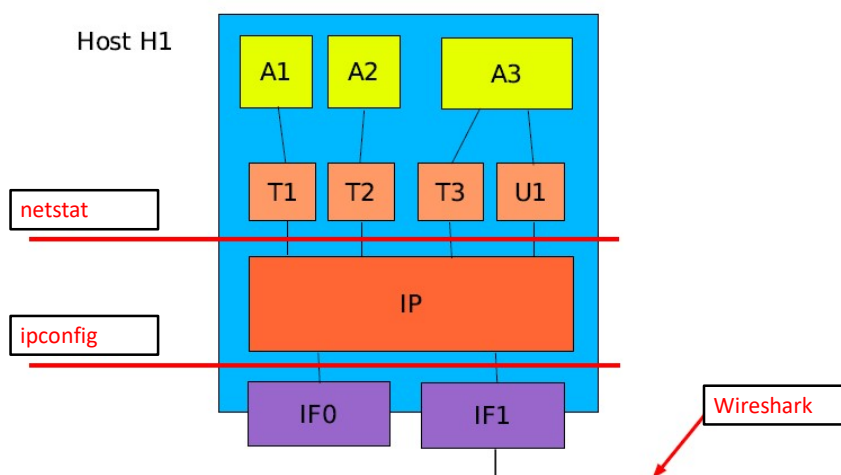


Tools of the Trade

- `ipconfig`
 - See local interfaces (links)
- `netstat`
 - See local connections
- Wireshark
 - Examine local packets
- `telnet/ssh`
 - Connect to a host
- `ping`
 - Check connectivity to a host
- `tracert`
 - Obtain route (set of routers) to a host

Tools: netstat, ipconfig, wireshark



Ipconfig shows local interfaces

```

C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Corey>ipconfig /all

Windows IP Configuration

Host Name . . . . . : beatyou
Primary Dns Suffix . . . . . :
Node Type . . . . . : Unknown
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : ma.dl.cox.net

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : ma.dl.cox.net
    Description . . . . . : VIA Rhine II Fast Ethernet Adapter
    Physical Address. . . . . : 00-50-2C-A5-F5-73
    Dhcp Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    IP Address. . . . . : 192.168.1.30
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.2
    DHCP Server . . . . . : 192.168.1.2
    DNS Servers . . . . . : 68.1.208.30
                           68.109.202.25
                           68.1.18.25
    Lease Obtained. . . . . : Monday, November 07, 2005 1:20:59 AM
  
```

Netstat shows local connections

```

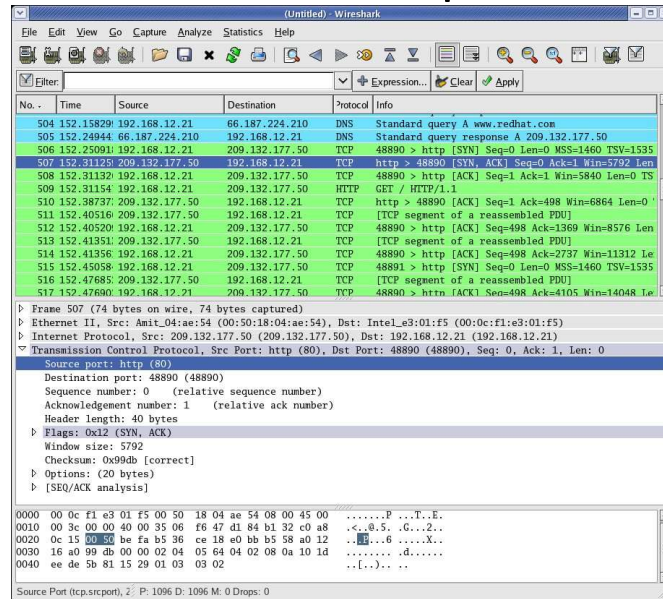
C:\Documents and Settings\Administrator>netstat -a -n -o

Active Connections

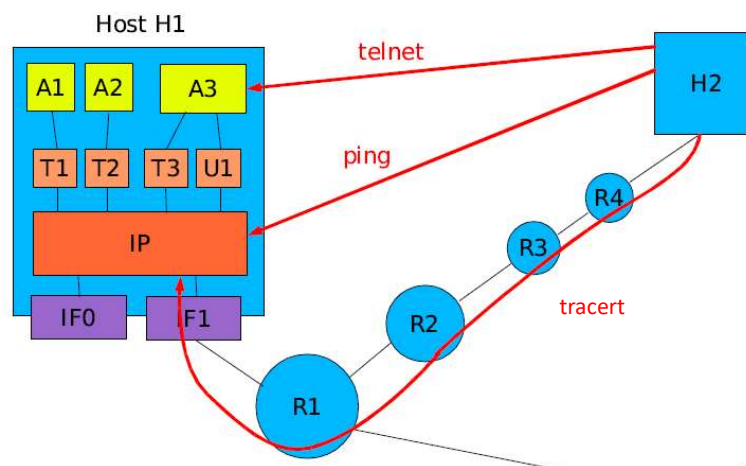
Proto Local Address Foreign Address State PID
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING 828
TCP 0.0.0.0:445 0.0.0.0:0 LISTENING 4
TCP 10.1.1.2:139 0.0.0.0:0 LISTENING 4
TCP 10.1.1.2:1278 219.64.34.26:1533 ESTABLISHED 2944
TCP 10.1.1.2:1669 72.246.103.49:80 TIME_WAIT 0
TCP 10.1.1.2:1670 72.246.103.49:80 TIME_WAIT 0
TCP 10.1.1.2:1672 64.86.142.27:80 TIME_WAIT 0
TCP 10.1.1.2:1674 64.86.142.27:80 TIME_WAIT 0
TCP 10.1.1.2:1717 72.246.103.48:80 TIME_WAIT 0
TCP 10.1.1.2:1765 66.90.104.15:80 TIME_WAIT 0
TCP 10.1.1.2:1780 64.191.203.30:80 TIME_WAIT 0
TCP 10.1.1.2:1816 72.14.221.91:80 TIME_WAIT 0
TCP 10.1.1.2:1824 72.14.221.91:80 TIME_WAIT 0
  
```

Process Name	Process ID	Protocol	Local Port	Local Port...	Local Address	Remote Address
BrComet.exe	2844	UDP	1720		0.0.0.0	
explorer.exe	644	UDP	2446		127.0.0.1	
lsass.exe	1520	UDP	500		0.0.0.0	
lsass.exe	1520	UDP	4500		0.0.0.0	
mcsasvc.exe	1740	TCP	6646		0.0.0.0	
mcsasvc.exe	1740	UDP	6646		99.240.214.105	
mDNSRespond...	404	TCP	5354		127.0.0.1	
mDNSRespond...	404	UDP	5353		99.240.214.105	
mDNSRespond...	404	UDP	1025		0.0.0.0	
MwlSvc.exe	1008	TCP	6636		0.0.0.0	
MwlSvc.exe	1008	UDP	6636		99.240.214.105	
svchost.exe	1776	TCP	135		0.0.0.0	
svchost.exe	532	TCP	2869		0.0.0.0	
svchost.exe	1972	UDP	1114		127.0.0.1	

Wireshark shows packet info



Tools: telnet, ping, tracert



Ping to google.com

```

Administrator: Command Prompt
Pinging vServer.virtualbox.local [192.168.100.1] with 32 bytes of data:
Reply from 192.168.100.1: bytes=32 time<1ms TTL=128
Reply from 192.168.100.1: bytes=32 time<1ms TTL=128
Reply from 192.168.100.1: bytes=32 time<1ms TTL=128
Reply from 192.168.100.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.100.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Administrator.VIRTUALBOX>ping google.com

Pinging google.com [209.85.169.103] with 32 bytes of data:
Reply from 209.85.169.103: bytes=32 time=78ms TTL=51
Reply from 209.85.169.103: bytes=32 time=61ms TTL=51
Reply from 209.85.169.103: bytes=32 time=189ms TTL=51
Reply from 209.85.169.103: bytes=32 time=56ms TTL=51

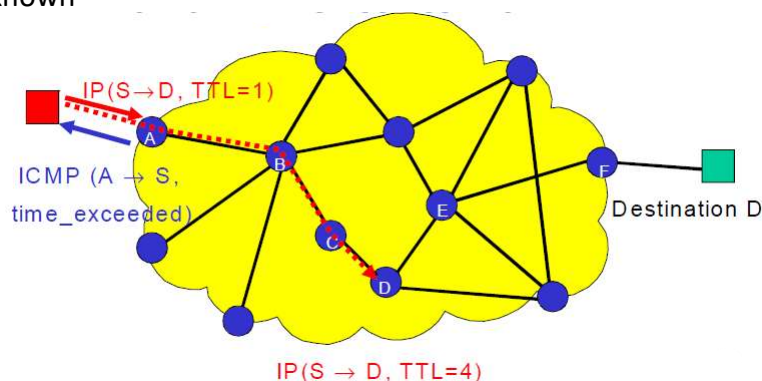
Ping statistics for 209.85.169.103:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 56ms, Maximum = 189ms, Average = 96ms

C:\Users\Administrator.VIRTUALBOX>

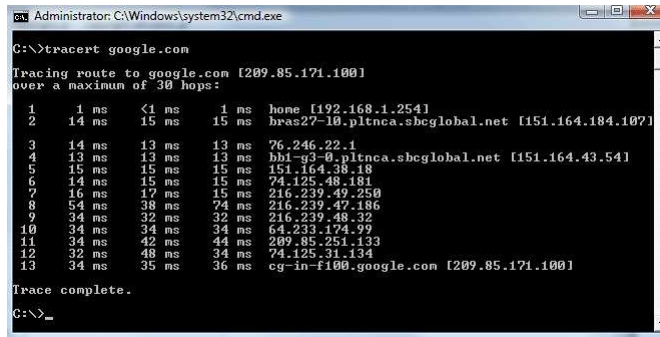
```

Tracert

- In IP, no explicit way to determine route from source to destination
- Tracert: trick intermediate routers into making themselves known

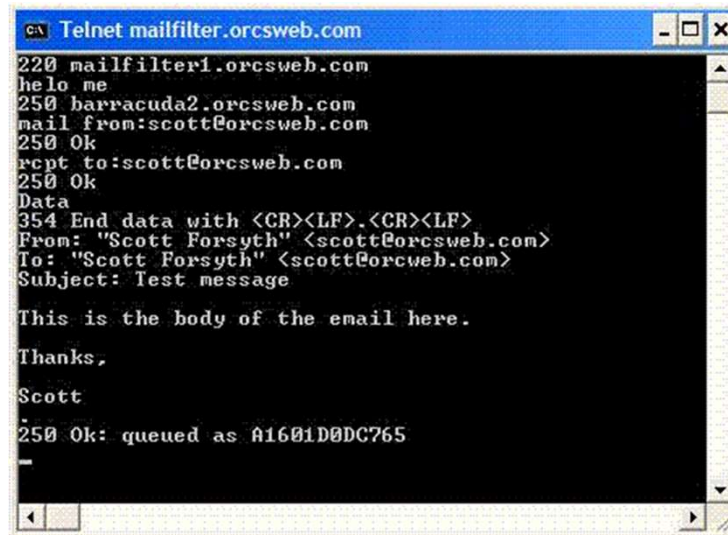


Tracert google.com



```
Administrator: C:\Windows\system32\cmd.exe
C:\>tracert google.com
Tracing route to google.com [209.85.171.100]
over a maximum of 30 hops:
  0  1 ms  <1 ms  1 ms  hone [192.168.1.254]
  1  14 ms  15 ms  15 ms  bras27-10.pltnca.sbcglobal.net [151.164.184.107]
  2  14 ms  13 ms  13 ms  76.246.22.1
  3  13 ms  13 ms  13 ms  bbl-g3-0.pltnca.sbcglobal.net [151.164.43.54]
  4  15 ms  15 ms  15 ms  151.164.38.18
  5  14 ms  15 ms  15 ms  74.125.48.181
  6  16 ms  17 ms  15 ms  216.239.49.250
  7  54 ms  38 ms  74 ms  216.239.47.186
  8  34 ms  32 ms  32 ms  216.239.48.32
  9  34 ms  34 ms  34 ms  64.233.174.99
 10  34 ms  42 ms  44 ms  209.85.251.133
 11  32 ms  48 ms  34 ms  74.125.31.134
 12  34 ms  35 ms  36 ms  cg-in-f100.google.com [209.85.171.100]
Trace complete.
C:\>
```

Telnet to mail server



```
Telnet mailfilter1.orcsweb.com
220 mailfilter1.orcsweb.com
helo me
250 barracuda2.orcsweb.com
mail from:scott@orcsweb.com
250 Ok
rcpt to:scott@orcsweb.com
250 Ok
Data
354 End data with <CR><LF>.<CR><LF>
From: "Scott Forsyth" <scott@orcsweb.com>
To: "Scott Forsyth" <scott@orcweb.com>
Subject: Test message

This is the body of the email here.

Thanks,

Scott
250 Ok: queued as A1601D0DC765
```