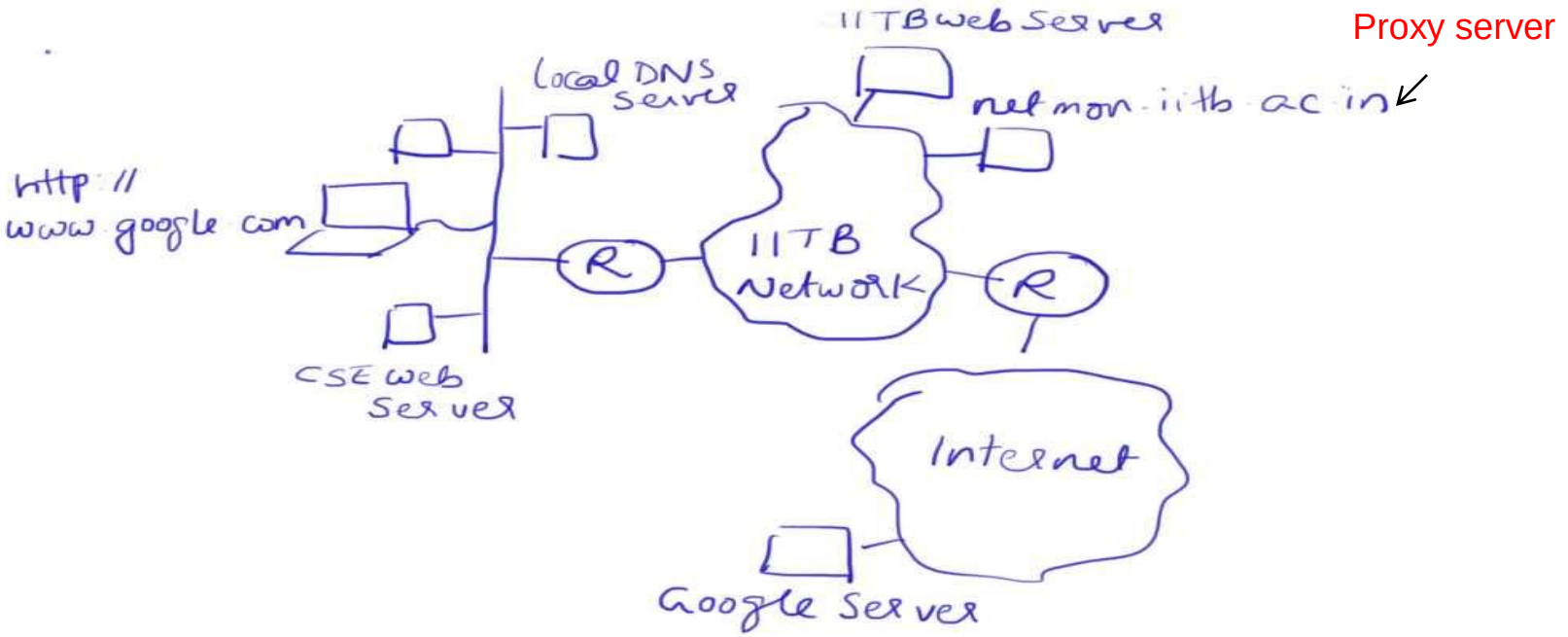
Computer Networks Lab

Overview

Kameswari Chebrolu

Getting you started



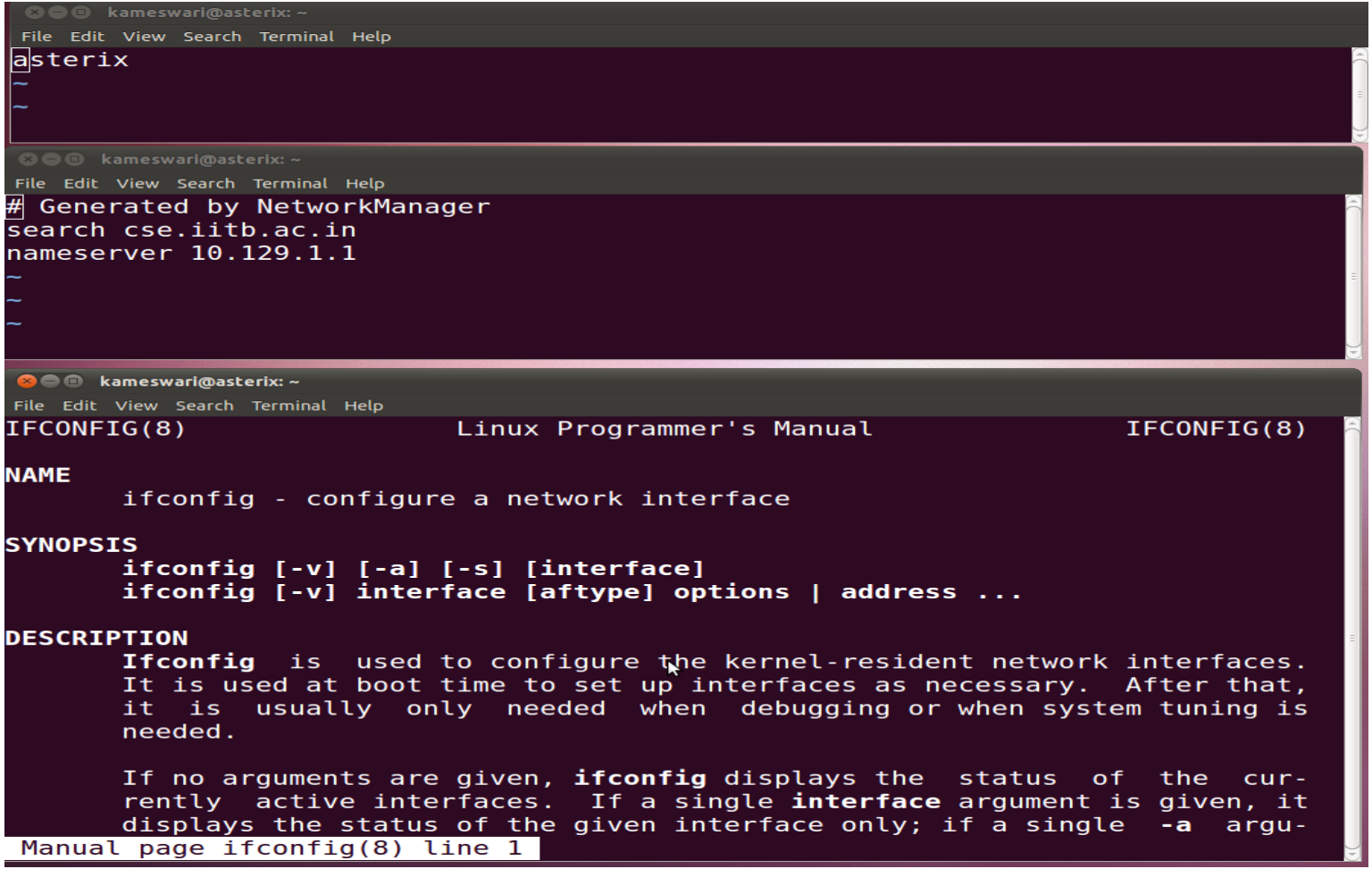
Proxy server

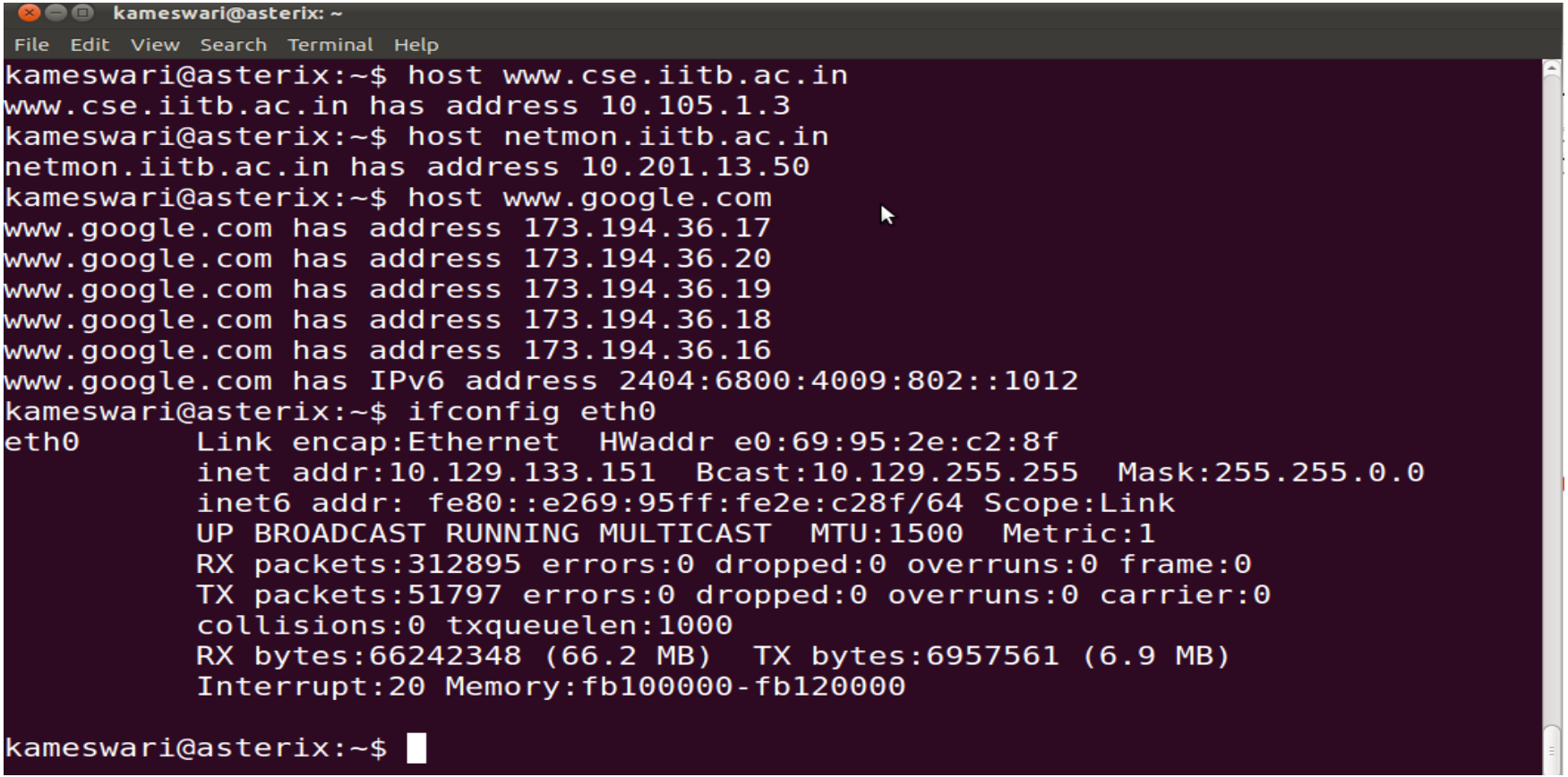
End-Hosts

- Host name
  - asterix.cse.iitb.ac.in, www.google.com
- IP address
  - Configurable, depends on location
- MAC address
  - Fixed
- DNS Server: Host name to IP address translation

Commands/Files

- /etc/hostname: specifies hostname
- Host (DNS service)
- /etc/resolv.conf: specifies the IP address of the local DNS server
- Ifconfig: provides network interface information
  - Can configure as well with root permission
- 'man' pages very helpful


kameswari@asterix: ~
File Edit View Search Terminal Help
asterix
~
~
kameswari@asterix: ~
File Edit View Search Terminal Help
Generated by NetworkManager
search cse.iitb.ac.in
nameserver 10.129.1.1
~
~
~
kameswari@asterix: ~
File Edit View Search Terminal Help
IFCONFIG(8) Linux Programmer's Manual IFCONFIG(8)
NAME
ifconfig - configure a network interface
SYNOPSIS
ifconfig [-v] [-a] [-s] [interface]
ifconfig [-v] interface [aftype] options | address ...
DESCRIPTION
Ifconfig is used to configure the kernel-resident network interfaces.
It is used at boot time to set up interfaces as necessary. After that,
it is usually only needed when debugging or when system tuning is
needed.
If no arguments are given, ifconfig displays the status of the cur-
rently active interfaces. If a single interface argument is given, it
displays the status of the given interface only; if a single -a argu-
Manual page ifconfig(8) line 1

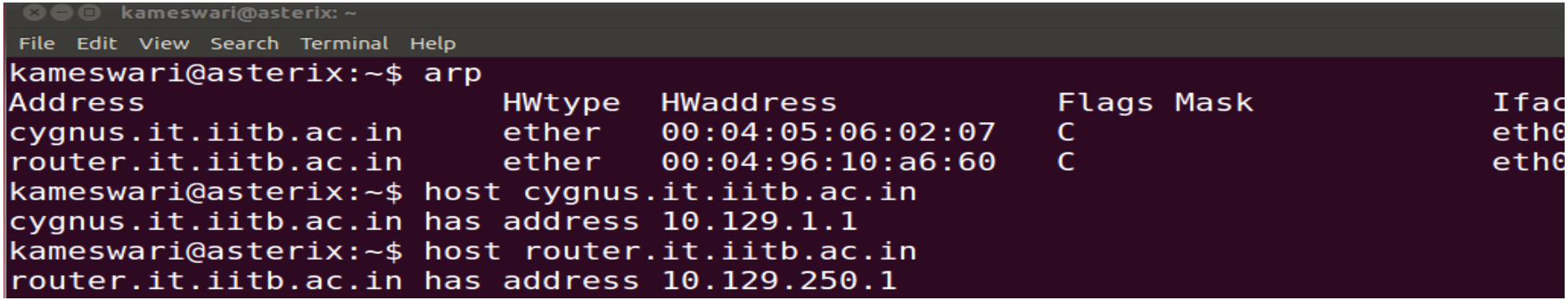

kameswari@asterix: ~
File Edit View Search Terminal Help
kameswari@asterix:~$ host www.cse.iitb.ac.in
www.cse.iitb.ac.in has address 10.105.1.3
kameswari@asterix:~$ host netmon.iitb.ac.in
netmon.iitb.ac.in has address 10.201.13.50
kameswari@asterix:~$ host www.google.com
www.google.com has address 173.194.36.17
www.google.com has address 173.194.36.20
www.google.com has address 173.194.36.19
www.google.com has address 173.194.36.18
www.google.com has address 173.194.36.16
www.google.com has IPv6 address 2404:6800:4009:802::1012
kameswari@asterix:~$ ifconfig eth0
eth0 Link encap:Ethernet HWaddr e0:69:95:2e:c2:8f
inet addr:10.129.133.151 Bcast:10.129.255.255 Mask:255.255.0.0
inet6 addr: fe80::e269:95ff:fe2e:c28f/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:312895 errors:0 dropped:0 overruns:0 frame:0
TX packets:51797 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:66242348 (66.2 MB) TX bytes:6957561 (6.9 MB)
Interrupt:20 Memory:fb100000-fb120000
kameswari@asterix:~$

Where are we?

- User clicked http://www.google.com
- Need to get Google web server's IP address
- Need to contact local DNS server whose IP address is in /etc/resolv.conf

How to contact DNS?

- Need its MAC address if within same LAN (next-hop neighbour, so need link address)
- ARP: provides IP address to MAC address translation

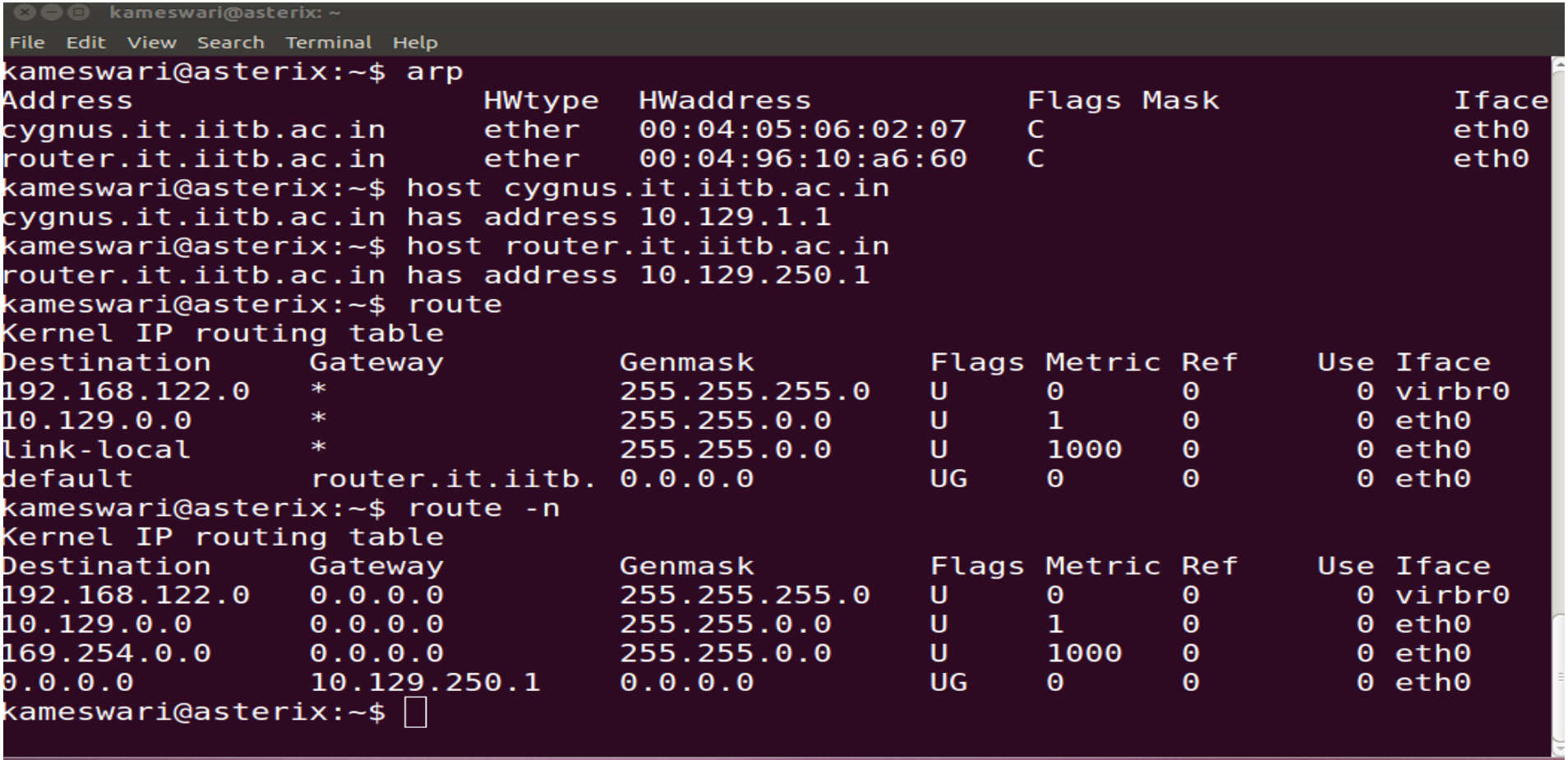

kameswari@asterix: ~
File Edit View Search Terminal Help
kameswari@asterix:~$ arp
Address HWtype HWaddress Flags Mask Ifac
cygnus.it.iitb.ac.in ether 00:04:05:06:02:07 C eth0
router.it.iitb.ac.in ether 00:04:96:10:a6:60 C eth0
kameswari@asterix:~$ host cygnus.it.iitb.ac.in
cygnus.it.iitb.ac.in has address 10.129.1.1
kameswari@asterix:~$ host router.it.iitb.ac.in
router.it.iitb.ac.in has address 10.129.250.1

Where are we?

- User clicked http://www.google.com
- Need Google web server's IP address
- So contacted local DNS server whose IP address is in /etc/resolv.conf
- Got the DNS server's MAC address through arp
- Sent packet(s) to DNS server asking for the IP address of Google server and got a reply.
- Assembled a http packet, which in turn triggers a TCP connection (TCP packet)
- Who to send this TCP packet to?

Who to send the TCP packet to?

- SRC IP: user's IP
- DST IP: Google's web server IP
- SRC MAC: user's mac
- DST MAC: ?
- Need next-hop router information
- Command: route
  - Default gateway is the next-hop router
  - Gateway at a host is configured during host's IP address configuration.
  - Its MAC address is stored in cache (can also be got via arp)

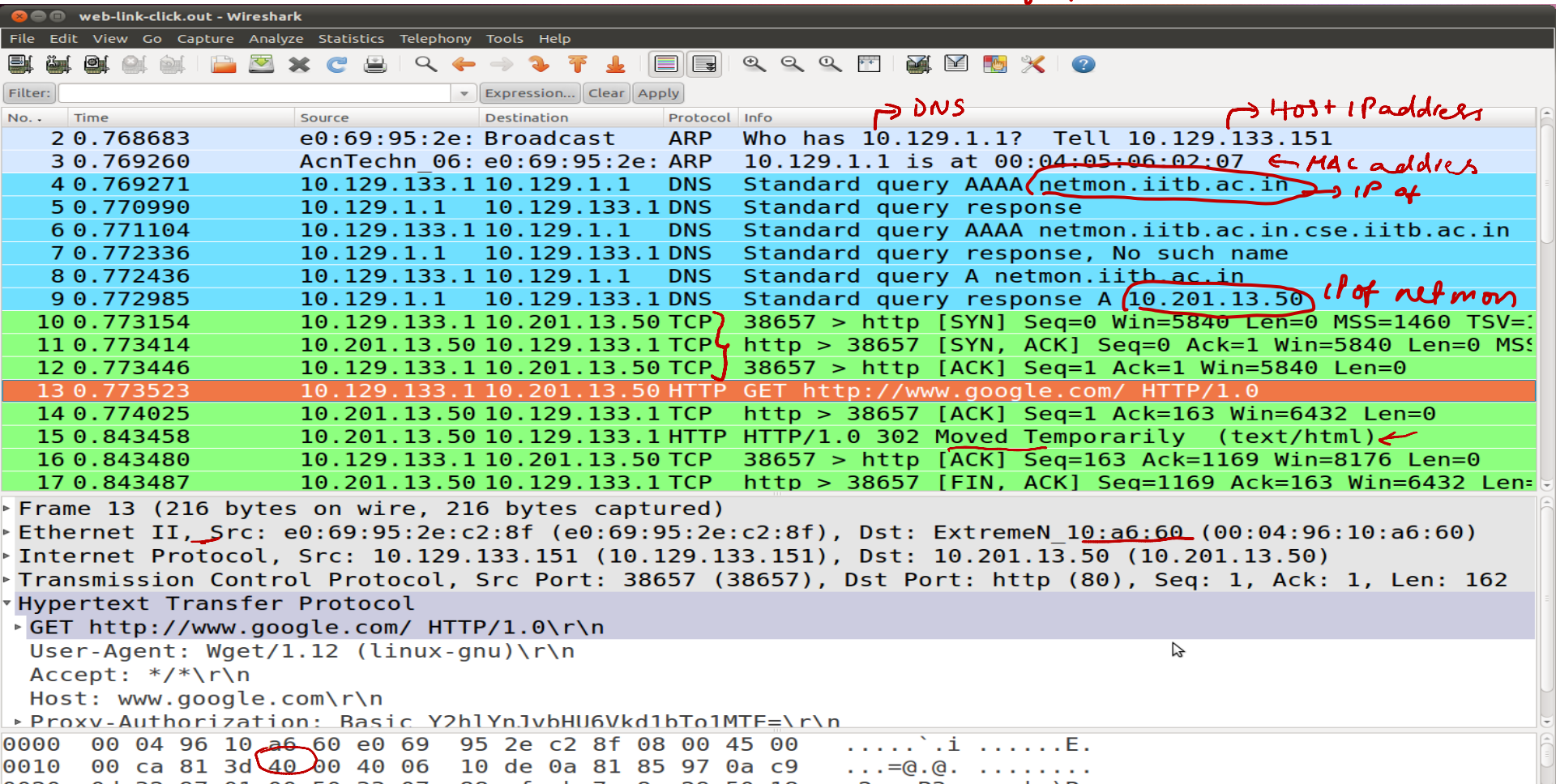

kameswari@asterix: ~
File Edit View Search Terminal Help
kameswari@asterix:~$ arp
Address HWtype HWaddress Flags Mask Iface
cygnus.it.iitb.ac.in ether 00:04:05:06:02:07 C eth0
router.it.iitb.ac.in ether 00:04:96:10:a6:60 C eth0
kameswari@asterix:~$ host cygnus.it.iitb.ac.in
cygnus.it.iitb.ac.in has address 10.129.1.1
kameswari@asterix:~$ host router.it.iitb.ac.in
router.it.iitb.ac.in has address 10.129.250.1
kameswari@asterix:~$ route
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
192.168.122.0 * 255.255.255.0 U 0 0 0 virbr0
10.129.0.0 * 255.255.0.0 U 1 0 0 eth0
link-local * 255.255.0.0 U 1000 0 0 eth0
default router.it.iitb. 0.0.0.0 UG 0 0 0 eth0
kameswari@asterix:~$ route -n
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
192.168.122.0 0.0.0.0 255.255.255.0 U 0 0 0 virbr0
10.129.0.0 0.0.0.0 255.255.0.0 U 1 0 0 eth0
169.254.0.0 0.0.0.0 255.255.0.0 U 1000 0 0 eth0
0.0.0.0 10.129.250.1 0.0.0.0 UG 0 0 0 eth0
kameswari@asterix:~$

Tracing

- Tcpdump, wireshark (very useful tools)
- Capture packets sent/received at a host
  - Many filtering options available
  - Tcpdump provides commandline interface, Wireshark provides GUI
  - Run tcpdump to capture trace and view the trace in wireshark (wireshark can capture too)

"wget"

http://www.google.com



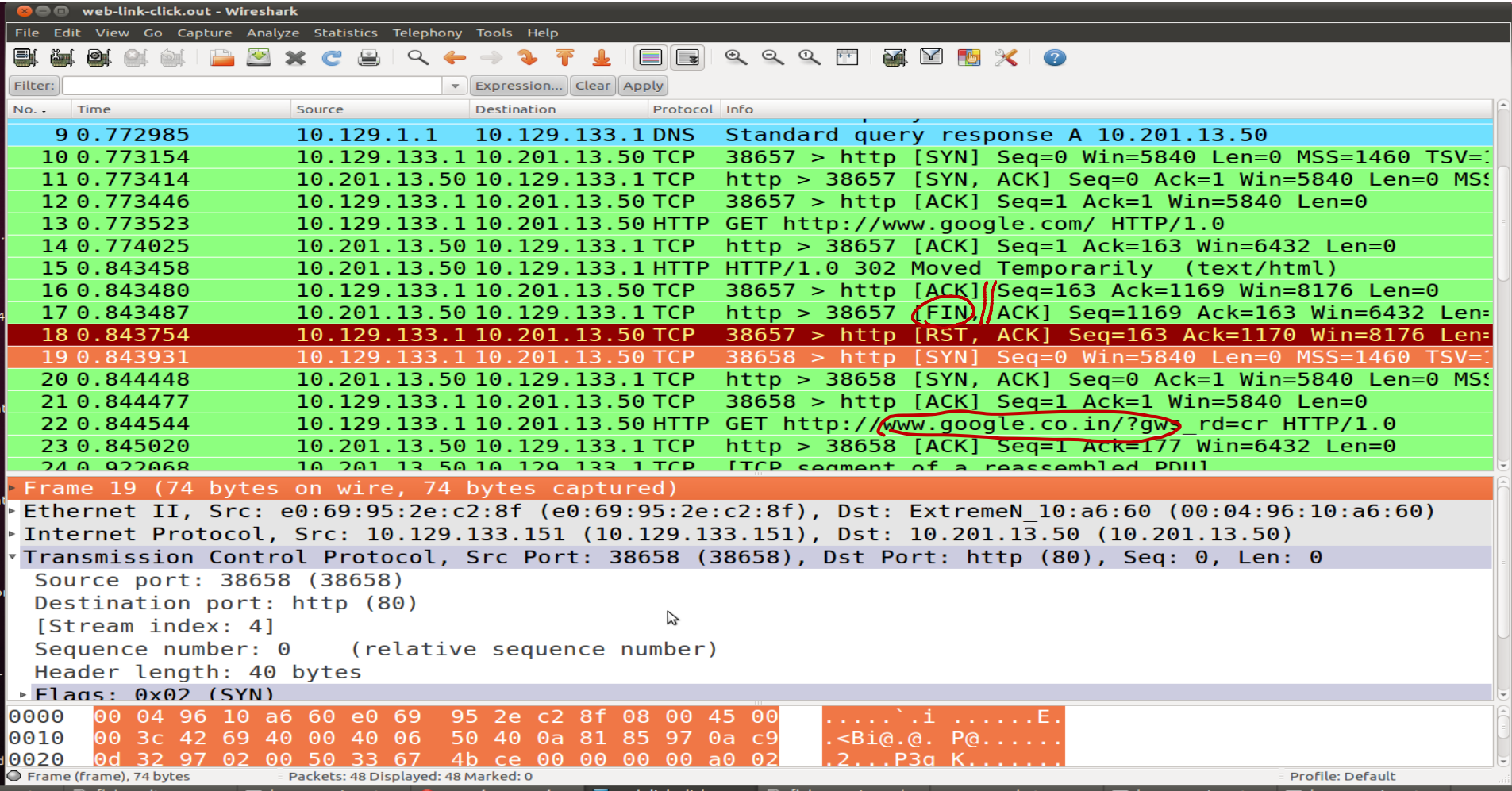
DNS

Host + IP address

MAC address

IP of

IP of netmon


web-link-click.out - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
9 0.772985 10.129.1.1 10.129.133.1 DNS Standard query response A 10.201.13.50
10 0.773154 10.129.133.1 10.201.13.50 TCP 38657 > http [SYN] Seq=0 Win=5840 Len=0 MSS=1460 TSV=
11 0.773414 10.201.13.50 10.129.133.1 TCP http > 38657 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MS
12 0.773446 10.129.133.1 10.201.13.50 TCP 38657 > http [ACK] Seq=1 Ack=1 Win=5840 Len=0
13 0.773523 10.129.133.1 10.201.13.50 HTTP GET http://www.google.com/ HTTP/1.0
14 0.774025 10.201.13.50 10.129.133.1 TCP http > 38657 [ACK] Seq=1 Ack=163 Win=6432 Len=0
15 0.843458 10.201.13.50 10.129.133.1 HTTP HTTP/1.0 302 Moved Temporarily (text/html)
16 0.843480 10.129.133.1 10.201.13.50 TCP 38657 > http [ACK] Seq=163 Ack=1169 Win=8176 Len=0
17 0.843487 10.201.13.50 10.129.133.1 TCP http > 38657 [FIN, ACK] Seq=1169 Ack=163 Win=6432 Len=
18 0.843754 10.129.133.1 10.201.13.50 TCP 38657 > http [RST, ACK] Seq=163 Ack=1170 Win=8176 Len=
19 0.843931 10.129.133.1 10.201.13.50 TCP 38658 > http [SYN] Seq=0 Win=5840 Len=0 MSS=1460 TSV=
20 0.844448 10.201.13.50 10.129.133.1 TCP http > 38658 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MS
21 0.844477 10.129.133.1 10.201.13.50 TCP 38658 > http [ACK] Seq=1 Ack=1 Win=5840 Len=0
22 0.844544 10.129.133.1 10.201.13.50 HTTP GET http://www.google.co.in/?gws_rd=cr HTTP/1.0
23 0.845020 10.201.13.50 10.129.133.1 TCP http > 38658 [ACK] Seq=1 Ack=177 Win=6432 Len=0
Frame 19 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: e0:69:95:2e:c2:8f (e0:69:95:2e:c2:8f), Dst: ExtremeN_10:a6:60 (00:04:96:10:a6:60)
Internet Protocol, Src: 10.129.133.151 (10.129.133.151), Dst: 10.201.13.50 (10.201.13.50)
Transmission Control Protocol, Src Port: 38658 (38658), Dst Port: http (80), Seq: 0, Len: 0
Source port: 38658 (38658)
Destination port: http (80)
[Stream index: 4]
Sequence number: 0 (relative sequence number)
Header length: 40 bytes
Flags: 0x02 (SYN)
0000 00 04 96 10 a6 60 e0 69 95 2e c2 8f 08 00 45 00
0010 00 3c 42 69 40 00 40 06 50 40 0a 81 85 97 0a c9
0020 0d 32 97 02 00 50 33 67 4b ce 00 00 00 00 a0 02
Frame (frame), 74 bytes
Packets: 48 Displayed: 48 Marked: 0
Profile: Default