

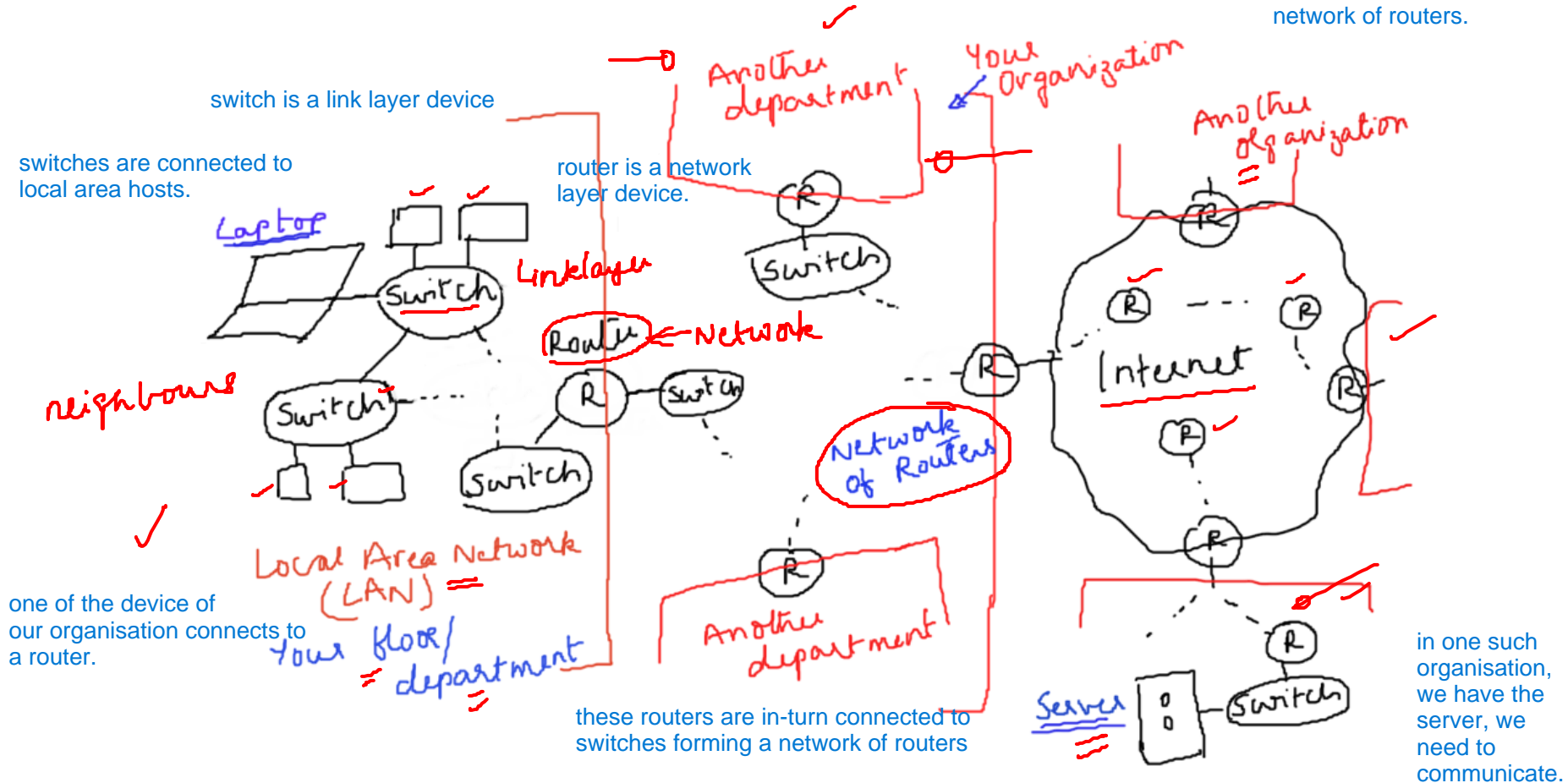
Tool Set-1: Action at a Host (Computer Networks Lab)

Kameswari Chebrolu

High Level Picture

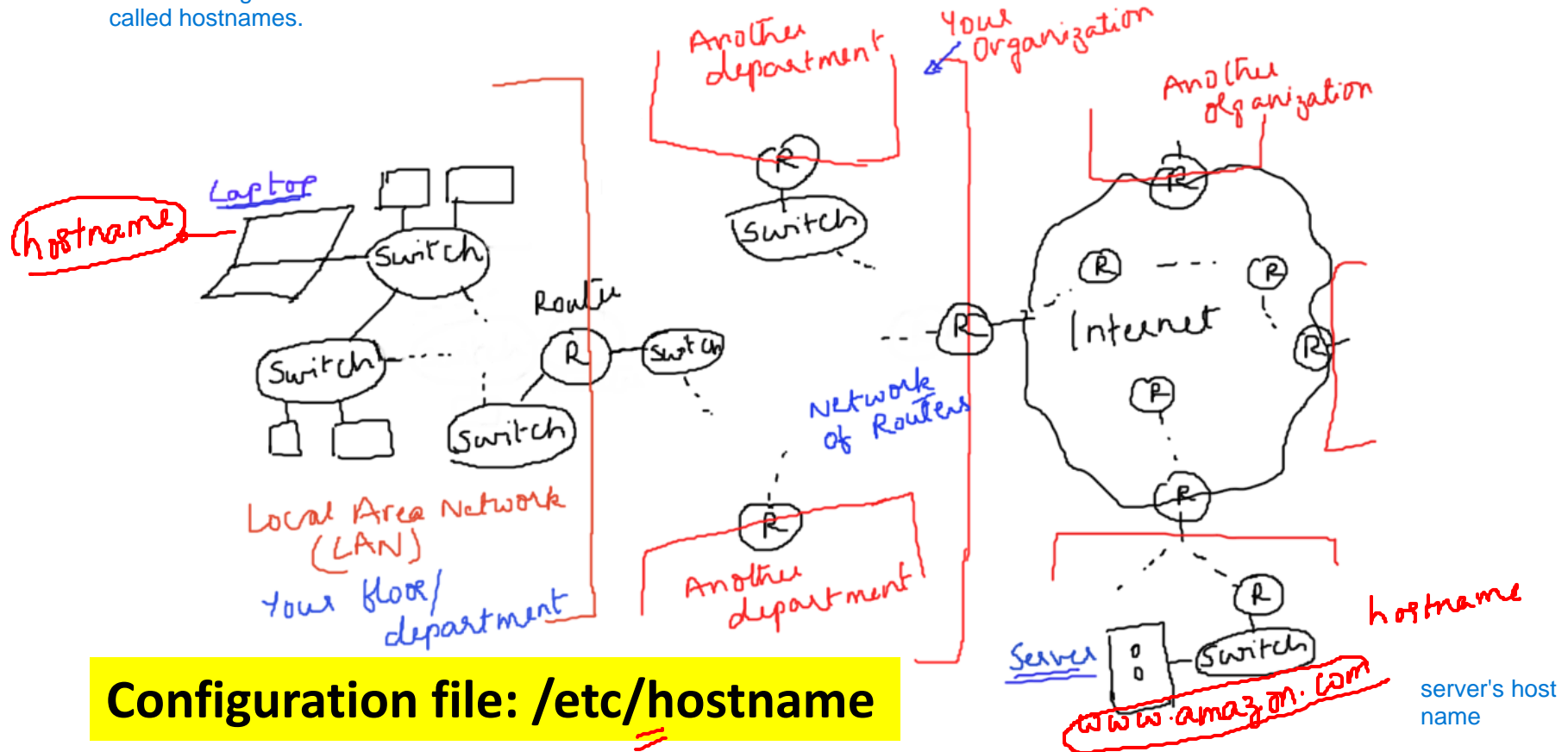
organisation = combination of departments

one special router connects our organisation to the internet..which itself is a network of routers.



Know thy machine!

machines ...given names
called hostnames.



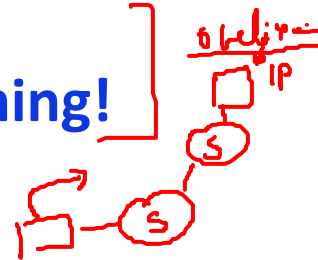
which server to contact? we need ip addr correspond to hostname...routers deal with ip addresses only.

browser is a piece of code.
it needs to figure out.. which server to
contact entered an url.

Application Layer:

u can enter the hostname <--> ip
adresss in the /etc/hosts file , then if
u want to send packets to that ip, ur
machine will look that file and figure
out

**Will cover application
development as part
of socket
programming!**



- You enter URL in browser *software*
 - e.g. <https://www.amazon.in/>
- Which server to contact?
 - Server hostname to IP address (DNS service)

- Command: host amd Configuration file: /etc/hosts

u need to deliver the packet to correct application on sever, so u need port.

- What port is the server listening on?

- Configuration File: /etc/services

fixed

web	- 80
ssh	- 22

rather than using a Server like DNS, we use
fixed ports. found in that file of server/

Also local host 127.0.0.1 is not the REAL ip. it is used for machine to adress to itself. its same n all machines.

Application Layer

application layer data.

sample-trace-iitb-website.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
108	6.627559	10.129.158.65	10.102.1.111	HTTP	386	GET / HTTP/1.1
155	10.264488	10.102.1.111	10.129.158.65	HTTP	181	HTTP/1.1 200 OK (text/html)
211	10.311757	10.129.158.65	10.102.1.111	HTTP	381	GET /modules/system/system.base.css?q08lbg HTTP/1.1
218	10.312291	10.102.1.111	10.129.158.65	HTTP	1471	HTTP/1.1 200 OK (text/css)
224	10.313428	10.129.158.65	10.102.1.111	HTTP	382	GET /modules/system/system.menus.css?q08lbg HTTP/1.1
227	10.313959	10.102.1.111	10.129.158.65	HTTP	998	HTTP/1.1 200 OK (text/css)
229	10.315648	10.129.158.65	10.102.1.111	HTTP	385	GET /modules/system/system.messages.css?q08lbg HTTP/1.1
230	10.316039	10.102.1.111	10.129.158.65	HTTP	1383	HTTP/1.1 200 OK (text/css)
231	10.316405	10.129.158.65	10.102.1.111	HTTP	382	GET /modules/system/system.theme.css?q08lbg HTTP/1.1

> Frame 108: 386 bytes on wire (3088 bits), 386 bytes captured (3088 bits) on interface 0

> Ethernet II, Src: Giga-Byt_8f:55:63 (1c:1b:0d:8f:55:63), Dst: Cisco_1a:75:b7 (84:b8:02:1a:75:b7)

> Internet Protocol Version 4, Src: 10.129.158.65, Dst: 10.102.1.111

> Transmission Control Protocol, Src Port: 57397, Dst Port: 80, Seq: 1, Ack: 1, Len: 332

HyperText Transfer Protocol

> GET / HTTP/1.1\r\n

Host: www.iitb.ac.in\r\n

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:71.0) Gecko/20100101 Firefox/71.0\r\n

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n

Accept-Language: en-US,en;q=0.5\r\n

Accept-Encoding: gzip, deflate\r\n

DNT: 1\r\n

Connection: keep-alive\r\n

Upgrade-Insecure-Requests: 1\r\n

\r\n

[Full request URI: http://www.iitb.ac.in/]

[HTTP request 1/5]

[Response in frame: 155]

[Next request in frame: 211]

0050 20 14 0c 3d 00 00 47 45 34 20 21 20 48 34 34 30 /1.1..Ho st: www.
0040 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 77 77 77 2e iitb.ac. in-User
0050 69 69 74 62 2e 61 63 2e 69 6e 0d 0a 55 73 65 72 -Agent: Mozilla/
0060 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 5.0 (win dows NT
0070 35 2e 30 20 28 57 69 6e 64 6f 77 73 20 4e 54 20 10.0; Wi n64; x64
0080 31 30 2e 30 3b 20 57 69 6e 36 34 3b 20 78 36 34 ; rv:71. 0) Gecko
0090 3b 20 72 76 3a 37 31 2e 30 29 20 47 65 63 6b 6f /2010010 1 Firefo
00a0 2f 32 30 31 30 30 31 30 31 20 46 69 72 65 66 6f x/71.0... Accept:
00b0 78 2f 37 31 2e 30 0d 0a 41 63 63 65 70 74 3a 20 text/htm l,applic
00c0 74 65 78 74 2f 68 74 6d 6c 2c 61 70 70 6c 69 63 ation/xh tml+xml,
00d0 61 74 69 6f 6e 2f 78 68 74 6d 6c 2b 78 6d 6c 2c applicat ion/xml,
00e0 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 6d 6c 3b application/xml;
00f0 71 3d 30 2e 39 2c 2a 2f 2a 3b 71 3d 30 2e 38 0d q=0.9,*/* ;q=0.8
0100 0a 41 63 63 65 70 74 2d 4c 61 6e 67 75 61 67 65 :Accept- Language
0110 3a 20 65 6e 2d 55 53 2c 65 6e 3b 71 3d 30 2e 35 : en-US, en;q=0.5

Hypertext Transfer Protocol (http), 332 bytes

Packets: 2892 · Displayed: 210 (7.3%)

Profile: Default

TCP

0	4	10	16	31				
Source Port ✓				Destination Port ✓				
Sequence Number								
Acknowledgment								
Hdr Len	0	U	A	P	R	S	F	Advertised Window
Checksum								Urgent Pointer
Options (Variable)								
Data								



http Expression...

No.	Time	Source	Destination	Protocol	Length	Info
108	6.627559	10.129.158.65	10.102.1.111	HTTP	386	GET / HTTP/1.1
155	10.264488	10.102.1.111	10.129.158.65	HTTP	181	HTTP/1.1 200 OK (text/html)
211	10.311757	10.129.158.65	10.102.1.111	HTTP	381	GET /modules/system/system.base.css?q081bg HTTP/1.1
218	10.312291	10.102.1.111	10.129.158.65	HTTP	1471	HTTP/1.1 200 OK (text/css)
224	10.313428	10.129.158.65	10.102.1.111	HTTP	382	GET /modules/system/system.menus.css?q081bg HTTP/1.1
227	10.313959	10.102.1.111	10.129.158.65	HTTP	998	HTTP/1.1 200 OK (text/css)
229	10.315648	10.129.158.65	10.102.1.111	HTTP	385	GET /modules/system/system.messages.css?q081bg HTTP/1.1
230	10.316039	10.102.1.111	10.129.158.65	HTTP	1383	HTTP/1.1 200 OK (text/css)
231	10.316405	10.129.158.65	10.102.1.111	HTTP	382	GET /modules/system/system.theme.css?q081bg HTTP/1.1

- > Frame 108: 386 bytes on wire (3088 bits), 386 bytes captured (3088 bits) on interface 0
- > Ethernet II, Src: Giga-Byt_8f:55:63 (1c:1b:0d:8f:55:63), Dst: Cisco_1a:75:bf (84:b8:02:1a:75:bf)
- > Internet Protocol Version 4, Src: 10.129.158.65, Dst: 10.102.1.111
- > Transmission Control Protocol, Src Port: 57397, Dst Port: 80, Seq: 1, Ack: 1, Len: 332

Source Port: 57397

Destination Port: 80

[Stream index: 7]

[TCP Segment Len: 332]

Sequence number: 1 (relative sequence number)

[Next sequence number: 333 (relative sequence number)]

Acknowledgment number: 1 (relative ack number)

0101 = Header Length: 20 bytes (5)

> Flags: 0x018 (PSH, ACK)

Window size value: 8212

[Calculated window size: 2102272]

[Window size scaling factor: 256]

Checksum: 0xdc5d [unverified]

[Checksum Status: Unverified]

Urgent pointer: 0

> [SEQ/ACK analysis]

> [Timestamps]

TCP payload (332 bytes)

> Hypertext Transfer Protocol

http
etc/service

the kernel can use any random unused source port.

socket

Network Layer

TCP

IPv4 header

IPv4

- Source IP
 - Command: **ip addr**

- Destination IP

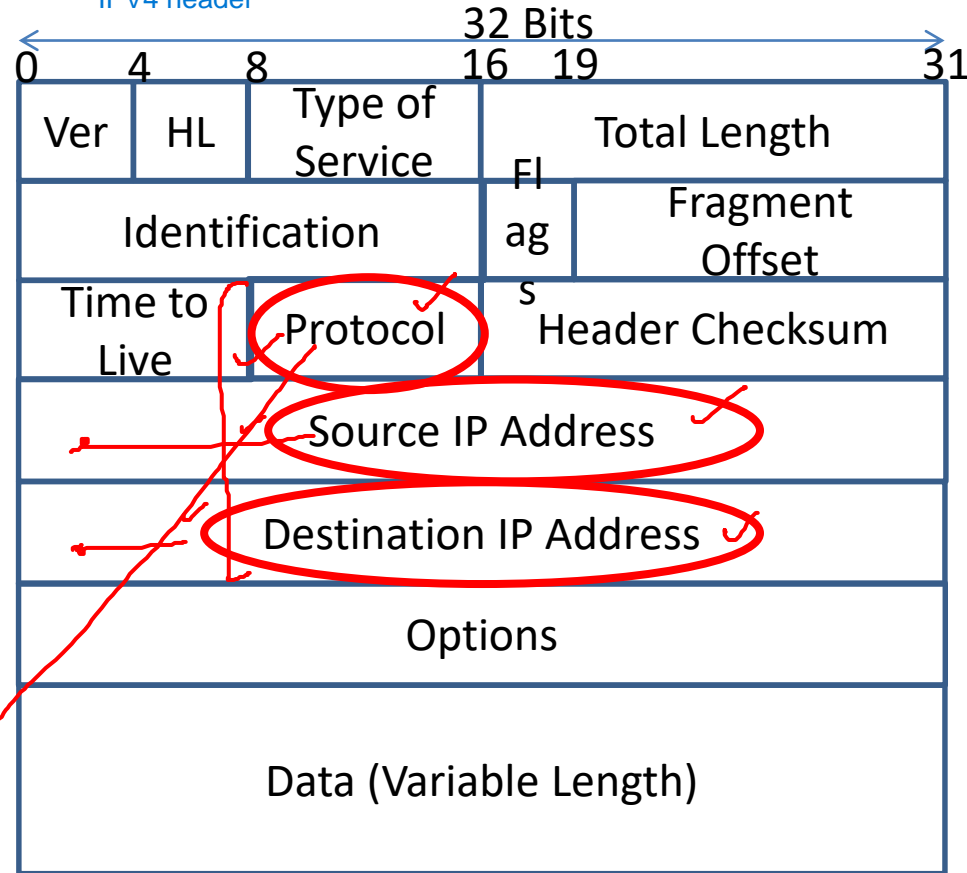
– Saw earlier

(Command: **Host**)

- Protocol

- Configuration File:
/etc/protocols

Transport



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

lo.	Time	Source	Destination	Protocol	Length	Info
108	6.627559	10.129.158.65	10.102.1.111	HTTP	386	GET / HTTP/1.1
155	10.264488	10.102.1.111	10.129.158.65	HTTP	181	HTTP/1.1 200 OK (text/html)
211	10.311757	10.129.158.65	10.102.1.111	HTTP	381	GET /modules/system/system.base.css?q081bg HTTP/1.1
218	10.312291	10.102.1.111	10.129.158.65	HTTP	1471	HTTP/1.1 200 OK (text/css)
224	10.313428	10.129.158.65	10.102.1.111	HTTP	382	GET /modules/system/system.menus.css?q081bg HTTP/1.1
227	10.313959	10.102.1.111	10.129.158.65	HTTP	998	HTTP/1.1 200 OK (text/css)
229	10.315648	10.129.158.65	10.102.1.111	HTTP	385	GET /modules/system/system.messages.css?q081bg HTTP/1.1
230	10.316039	10.102.1.111	10.129.158.65	HTTP	1383	HTTP/1.1 200 OK (text/css)
231	10.316405	10.129.158.65	10.102.1.111	HTTP	382	GET /modules/system/system.theme.css?q081bg HTTP/1.1

> Frame 108: 386 bytes on wire (3088 bits), 386 bytes captured (3088 bits) on interface 0

> Ethernet II, Src: Giga-Byt_8f:55:05 (1c:1b:0d:8f:55:63), Dst: Cisco_1a:75:bf (84:b8:02:1a:75:bf)

> Internet Protocol Version 4, Src: 10.129.158.65, Dst: 10.102.1.111

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 372

Identification: 0xed92 (60818)

> Flags: 0x4000, Don't fragment

...0 0000 0000 0000 = Fragment offset: 0

Time to live: 128

Protocol: TCP (6)

Header checksum: 0x575a [validation disabled]

[Header checksum status: Unverified]

Source: 10.129.158.65

Destination: 10.102.1.111

> Transmission Control Protocol, Src Port: 57397, Dst Port: 80, Seq: 1, Ack: 1, Len: 332

> Hypertext Transfer Protocol

```

0000 84 b8 02 1a 75 bf 1c 1b 0d 8f 55 63 08 00 45 00  ....u... ..Uc..E.
0010 01 74 ed 92 40 00 80 06 57 5a 0a 81 9e 41 0a 66  .t..@... WZ...A.f
0020 01 6f e0 35 00 50 ef 48 29 0d 44 75 1e 6a 50 18  .c.5.P.H ).Du.jP.
0030 20 14 dc 5d 00 00 47 45 54 20 2f 20 48 54 54 50  . .]..GE T / HTTP

```

NETWORK LAYER INFO

command

ip addr.

better command

ifconfig

~we can see
many interfaces.

main interface
en01

also lo
interface...loop
back. sending
packets to other
process in same
machine

IP addr - Network layer

MAC addr

src

network interface embed

Link Layer

here we use MAC addresses



- Source MAC Address ✓
– **Command: ip addr** (previous: ifconfig)
- Destination MAC address? (need to use ARP service)

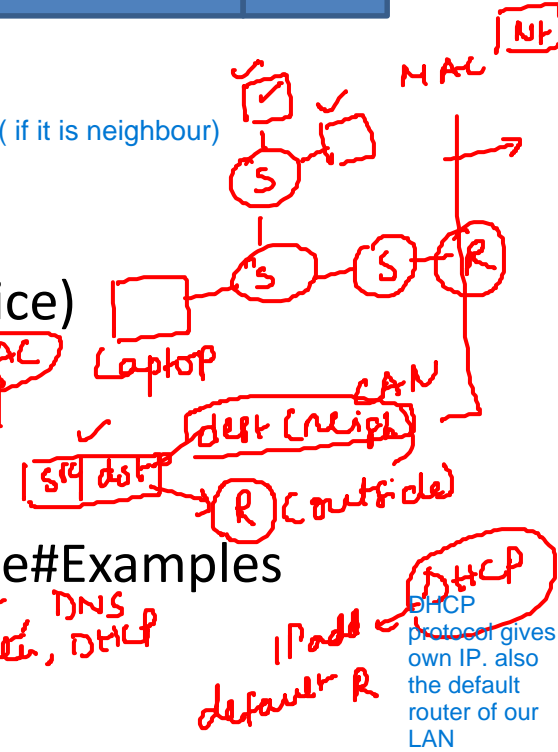
dest MAC: MAC address of host(if it is neighbour)
else it is MAC addr of Router.

- **Command: `ip route`** (previous: `route`)

Command: ip neigh (previous: arp)

– **Command: arping ip-addr**

- Type: See <https://en.wikipedia.org/wiki/EtherType#Examples>



ARP protocol
gives MAC for a given ip.

if neigh , gives the MAC given ip address available in the arp cache of our machine. if the trequired ip is not available then use 3rd command, it populates the cache and finds out.

sample-trace-iitb-website.pcapng

ip route gives ip addr of the LAN router.
ip neigh gives MAC<--> ip mapping stored.

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help



http Expression...

No.	Time	Source	Destination	Protocol	Length	Info
108	6.627559	10.129.158.65	10.102.1.111	HTTP	386	GET / HTTP/1.1
155	10.264488	10.102.1.111	10.129.158.65	HTTP	181	HTTP/1.1 200 OK (text/html)
211	10.311757	10.129.158.65	10.102.1.111	HTTP	381	GET /modules/system/system.base.css?q081bg HTTP/1.1
218	10.312291	10.102.1.111	10.129.158.65	HTTP	1471	HTTP/1.1 200 OK (text/css)
224	10.313428	10.129.158.65	10.102.1.111	HTTP	382	GET /modules/system/system.menus.css?q081bg HTTP/1.1
227	10.313959	10.102.1.111	10.129.158.65	HTTP	998	HTTP/1.1 200 OK (text/css)
229	10.315648	10.129.158.65	10.102.1.111	HTTP	385	GET /modules/system/system.messages.css?q081bg HTTP/1.1
230	10.316039	10.102.1.111	10.129.158.65	HTTP	1383	HTTP/1.1 200 OK (text/css)
231	10.316405	10.129.158.65	10.102.1.111	HTTP	382	GET /modules/system/system.theme.css?q081bg HTTP/1.1

> Frame 108: 386 bytes on wire (3088 bits), 386 bytes captured (3088 bits) on interface 0

> Ethernet II, Src: Giga-Byt_8f:55:63 (1c:1b:0d:8f:55:63), Dst: Cisco_1a:75:bf (84:b8:02:1a:75:bf)

> Destination: Cisco_1a:75:bf (84:b8:02:1a:75:bf)

> Source: Giga-Byt_8f:55:63 (1c:1b:0d:8f:55:63)

Type: IPv4 (0x0800)

Static

IPv4
IPv6
ARP

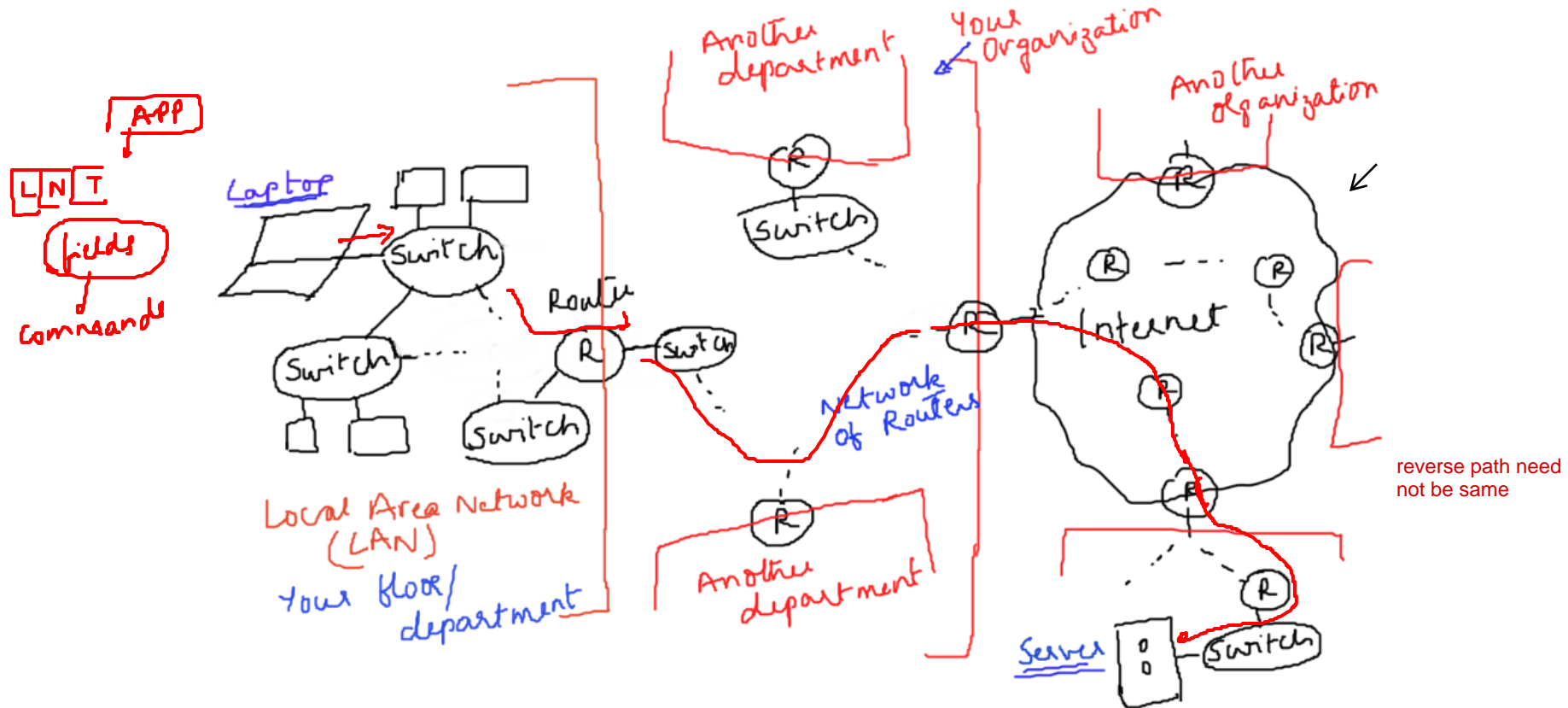
> Internet Protocol Version 4, Src: 10.129.158.65, Dst: 10.102.1.111

> Transmission Control Protocol, Src Port: 57397, Dst Port: 80, Seq: 1, Ack: 1, Len: 332

> Hypertext Transfer Protocol

```
0000 84 b8 02 1a 75 bf 1c 1b 0d 8f 55 63 08 00 45 00 .....u...Uc..E.
0010 01 74 ed 92 40 00 80 06 57 5a 0a 81 9e 41 0a 66 .t..@...WZ...A.f
0020 01 6f e0 35 00 50 ef 48 29 0d 44 75 1e 6a 50 18 .o.5.P.H).Du.jP.
```

Journey of this packet



Summary

Concepts: Layering; Encapsulation/De-capsulation via Headers; Demultiplexing; Addressing ✓

Type, Protocol, Port

IP
MAC

- Host: /etc/hostname
- Application Layer: /etc/services, /etc/hosts and host
- Transport Layer: /etc/services
- Network Layer: ip addr; host; /etc/protocols
- Link Layer: ip addr; ip route; ip neigh; arping

References

- “man” pages of commands
 - Example: “man host”; “man ip”
- IP command cheat sheet
(https://access.redhat.com/sites/default/files/attachments/rh_ip_command_cheatsheet_1214_jcs_print.pdf)