

INTERNETWORKING MISC

CS 130

Creative Software Architectures
for Collaborative Projects

Prof. Donald J. Patterson

Content adapted from Essentials of Software
Engineering 3rd edition by Tsui, Karam, Bernal
Jones and Bartlett Learning



TOOLS SHOWN TODAY

MTR

- A network diagnostic tool
- example “`sudo mtr -t www.djp3.net`”

My traceroute [v0.86]							
Codex-Perductum.local (0.0.0.0)				Wed Sep 7 10:07:19 2016			
Keys: Help Display mode Restart statistics Order of fields quit							
Host	Packets			Pings			
	Loss%	Snt	Last	Avg	Best	Wrst	StDev
1. 10.45.63.254	0.0%	8	0.8	0.8	0.6	1.0	0.0
2. KHCore-KHDist.westmont.edu	0.0%	8	0.9	0.8	0.7	0.9	0.0
3. PA-FW.westmont.edu	0.0%	8	1.3	1.2	0.9	1.5	0.0
4. ip176-11.outside.westmont.edu	0.0%	8	1.8	1.5	1.3	1.8	0.0
5. wsip-174-78-247-41.sd.sd.cox.net	0.0%	8	6.7	6.1	5.5	6.7	0.0
6. ip68-4-11-200.oc.oc.cox.net	0.0%	8	6.5	6.8	5.5	14.1	2.9
7. ashbbprj02-ae2.0.rd.as.cox.net	0.0%	7	78.9	79.0	78.4	79.7	0.0
8. aggr501a-94-core9.iad3.rackspace.net	0.0%	7	79.9	79.6	79.2	80.1	0.0
9. ???							
10. corea-dcpel.iad3.rackspace.net	0.0%	7	79.8	79.8	79.5	80.3	0.0
11. corea-core7.iad3.rackspace.net	0.0%	7	80.5	80.1	79.3	80.9	0.0
12. core7-aggr403a-8.iad3.rackspace.net	0.0%	7	79.9	79.6	79.3	80.0	0.0
13. 104.239.160.189	0.0%	7	79.5	79.5	79.1	80.1	0.0

TOOLS SHOWN TODAY

MTR

- “combines the functionality of the **traceroute** and **ping** programs in a single network diagnostic tool.
- As mtr starts, it investigates the network connection between the host mtr runs on and HOSTNAME by sending packets with purposely low TTLs. It continues to send packets with low TTL, noting the response time of the intervening routers. This allows mtr to print the response percentage and response times of the internet route to HOSTNAME. A sudden increase in packet loss or response time is often an indication of a bad (or simply overloaded) link.
- The results are usually reported as round-trip-response times in milliseconds and the percentage of packetloss.”



TOOLS SHOWN TODAY

DIG

- A DNS lookup utility
- “dig +trace www.djp3.net”

```
; <<>> DiG 9.8.3-P1 <<>> +trace www.djp3.net
;; global options: +cmd
.                262510  IN      NS      b.root-servers.net.
.                262510  IN      NS      g.root-servers.net.
.                262510  IN      NS      m.root-servers.net.
.                262510  IN      NS      i.root-servers.net.
.                262510  IN      NS      a.root-servers.net.
.                262510  IN      NS      j.root-servers.net.
.                262510  IN      NS      k.root-servers.net.
.                262510  IN      NS      d.root-servers.net.
.                262510  IN      NS      l.root-servers.net.
.                262510  IN      NS      h.root-servers.net.
.                262510  IN      NS      c.root-servers.net.
.                262510  IN      NS      f.root-servers.net.
.                262510  IN      NS      e.root-servers.net.
;; Received 508 bytes from 10.50.10.4#53(10.50.10.4) in 61 ms

net.             172800  IN      NS      e.gtld-servers.net.
net.             172800  IN      NS      g.gtld-servers.net.
net.             172800  IN      NS      k.gtld-servers.net.
net.             172800  IN      NS      i.gtld-servers.net.
net.             172800  IN      NS      c.gtld-servers.net.
net.             172800  IN      NS      l.gtld-servers.net.
net.             172800  IN      NS      a.gtld-servers.net.
net.             172800  IN      NS      h.gtld-servers.net.
net.             172800  IN      NS      m.gtld-servers.net.
net.             172800  IN      NS      j.gtld-servers.net.
net.             172800  IN      NS      f.gtld-servers.net.
net.             172800  IN      NS      d.gtld-servers.net.
net.             172800  IN      NS      b.gtld-servers.net.
;; Received 499 bytes from 192.5.5.241#53(192.5.5.241) in 109 ms

djp3.net.        172800  IN      NS      ns3.hover.com.
djp3.net.        172800  IN      NS      ns1.hover.com.
djp3.net.        172800  IN      NS      ns2.hover.com.
;; Received 141 bytes from 192.43.172.30#53(192.43.172.30) in 65 ms

www.djp3.net.    900      IN      A        104.239.160.189
;; Received 46 bytes from 64.98.148.13#53(64.98.148.13) in 73 ms
```

TOOLS SHOWN TODAY

DIG

- “dig (domain information groper) is a flexible tool for interrogating DNS name servers. It performs DNS lookups and displays the answers that are returned from the name server(s) that were queried. Most DNS administrators use dig to troubleshoot DNS problems because of its flexibility, ease of use and clarity of output. Other lookup tools tend to have less functionality than dig.”



TOOLS SHOWN TODAY

HOST

- A DNS lookup utility

```
[504]djp3@Codex-Perductum: ~  
$ host www.westmont.edu  
www.westmont.edu has address 10.50.10.130  
[505]djp3@Codex-Perductum: ~  
$ host 10.50.10.130  
130.10.50.10.in-addr.arpa domain name pointer www.westmont.edu.
```



TOOLS SHOWN TODAY

HOST

- “host is a simple utility for performing DNS lookups. It is normally used to convert names to IP addresses and vice versa. When no arguments or options are given, host prints a short summary of its command line arguments and options.”



TOOLS SHOWN TODAY

WIRESHARK

- “Interactively dump and analyze network traffic”
- “Wireshark is the world's foremost network protocol analyzer. It lets you see what's happening on your network at a microscopic level. It is the de facto (and often de jure) standard across many industries and educational institutions.”
- <https://www.wireshark.org/>
 - recommend install with package manager like brew



tcp.stream eq 10

No.	Time	Source	Destination	Protocol	Length	Info
118	9.962200	10.45.10.231	104.239.160.189	TCP	78	62937 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=141509014 TSecr=0 SACK...
218	10.041006	104.239.160.189	10.45.10.231	TCP	66	80 → 62937 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=512
223	10.041045	10.45.10.231	104.239.160.189	TCP	54	62937 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
331	11.517950	10.45.10.231	104.239.160.189	HTTP	951	GET / HTTP/1.1
332	11.597515	104.239.160.189	10.45.10.231	TCP	60	80 → 62937 [ACK] Seq=1 Ack=898 Win=31232 Len=0
336	13.941513	104.239.160.189	10.45.10.231	TCP	1514	[TCP segment of a reassembled PDU]
337	13.941565	104.239.160.189	10.45.10.231	TCP	1514	[TCP segment of a reassembled PDU]
338	13.941673	10.45.10.231	104.239.160.189	TCP	54	62937 → 80 [ACK] Seq=898 Ack=2921 Win=259200 Len=0
339	13.941690	104.239.160.189	10.45.10.231	TCP	1514	[TCP segment of a reassembled PDU]
340	13.941714	10.45.10.231	104.239.160.189	TCP	54	[TCP Window Update] 62937 → 80 [ACK] Seq=898 Ack=2921 Win=262144 Len=0
341	13.941846	104.239.160.189	10.45.10.231	TCP	1514	[TCP segment of a reassembled PDU]
342	13.941934	104.239.160.189	10.45.10.231	TCP	1514	[TCP segment of a reassembled PDU]
343	13.941936	10.45.10.231	104.239.160.189	TCP	54	62937 → 80 [ACK] Seq=898 Ack=5841 Win=259200 Len=0
344	13.942099	104.239.160.189	10.45.10.231	TCP	1514	[TCP segment of a reassembled PDU]
345	13.942142	104.239.160.189	10.45.10.231	TCP	1514	[TCP segment of a reassembled PDU]
346	13.942194	10.45.10.231	104.239.160.189	TCP	54	62937 → 80 [ACK] Seq=898 Ack=8761 Win=256288 Len=0
347	13.942280	104.239.160.189	10.45.10.231	TCP	1514	[TCP segment of a reassembled PDU]
348	13.942344	10.45.10.231	104.239.160.189	TCP	54	62937 → 80 [ACK] Seq=898 Ack=11681 Win=253376 Len=0
349	13.942396	104.239.160.189	10.45.10.231	TCP	1514	[TCP segment of a reassembled PDU]
350	13.943506	104.239.160.189	10.45.10.231	TCP	1514	[TCP segment of a reassembled PDU]
351	13.943592	10.45.10.231	104.239.160.189	TCP	54	62937 → 80 [ACK] Seq=898 Ack=14601 Win=250464 Len=0
352	13.946538	10.45.10.231	104.239.160.189	TCP	54	[TCP Window Update] 62937 → 80 [ACK] Seq=898 Ack=14601 Win=262144 Len=0
353	14.034440	104.239.160.189	10.45.10.231	TCP	1514	[TCP segment of a reassembled PDU]
354	14.034539	104.239.160.189	10.45.10.231	TCP	1514	[TCP segment of a reassembled PDU]
355	14.034586	10.45.10.231	104.239.160.189	TCP	54	62937 → 80 [ACK] Seq=898 Ack=17521 Win=260672 Len=0
356	14.034662	104.239.160.189	10.45.10.231	TCP	1514	[TCP segment of a reassembled PDU]
357	14.034737	10.45.10.231	104.239.160.189	TCP	54	62937 → 80 [ACK] Seq=898 Ack=18981 Win=262144 Len=0
358	14.034781	104.239.160.189	10.45.10.231	TCP	1514	[TCP segment of a reassembled PDU]
359	14.034925	104.239.160.189	10.45.10.231	TCP	1514	[TCP segment of a reassembled PDU]
360	14.034958	10.45.10.231	104.239.160.189	TCP	54	62937 → 80 [ACK] Seq=898 Ack=21901 Win=260672 Len=0
361	14.035031	104.239.160.189	10.45.10.231	TCP	1514	[TCP segment of a reassembled PDU]
362	14.035108	10.45.10.231	104.239.160.189	TCP	54	62937 → 80 [ACK] Seq=898 Ack=23361 Win=262144 Len=0
363	14.035150	104.239.160.189	10.45.10.231	TCP	1514	[TCP segment of a reassembled PDU]
364	14.035295	104.239.160.189	10.45.10.231	TCP	1514	[TCP segment of a reassembled PDU]
365	14.035326	10.45.10.231	104.239.160.189	TCP	54	62937 → 80 [ACK] Seq=898 Ack=26281 Win=260672 Len=0
366	14.035401	104.239.160.189	10.45.10.231	TCP	1514	[TCP segment of a reassembled PDU]
367	14.035478	10.45.10.231	104.239.160.189	TCP	54	62937 → 80 [ACK] Seq=898 Ack=27741 Win=262144 Len=0
368	14.035523	104.239.160.189	10.45.10.231	TCP	1514	[TCP segment of a reassembled PDU]
369	14.035663	104.239.160.189	10.45.10.231	TCP	1514	[TCP segment of a reassembled PDU]
370	14.035696	10.45.10.231	104.239.160.189	TCP	54	62937 → 80 [ACK] Seq=898 Ack=30661 Win=260672 Len=0
371	14.035771	104.239.160.189	10.45.10.231	TCP	1514	[TCP segment of a reassembled PDU]
372	14.035836	10.45.10.231	104.239.160.189	TCP	54	62937 → 80 [ACK] Seq=898 Ack=32121 Win=262144 Len=0
373	14.035883	104.239.160.189	10.45.10.231	TCP	1514	[TCP segment of a reassembled PDU]
374	14.036033	104.239.160.189	10.45.10.231	TCP	1514	[TCP segment of a reassembled PDU]
375	14.036068	10.45.10.231	104.239.160.189	TCP	54	62937 → 80 [ACK] Seq=898 Ack=35041 Win=260672 Len=0
376	14.036092	104.239.160.189	10.45.10.231	HTTP	1039	HTTP/1.1 200 OK (text/html)
377	14.036121	10.45.10.231	104.239.160.189	TCP	54	62937 → 80 [ACK] Seq=898 Ack=36026 Win=259680 Len=0
433	15.137128	10.45.10.231	104.239.160.189	HTTP	1228	GET /wp-admin/admin.php?page=stats&noheader&proxy&chart=admin-bar-hours-scale HTTP...
473	15.216966	104.239.160.189	10.45.10.231	TCP	60	80 → 62937 [ACK] Seq=36026 Ack=2072 Win=33792 Len=0
676	17.794851	104.239.160.189	10.45.10.231	HTTP	701	HTTP/1.1 200 OK (PNG)
677	17.794989	10.45.10.231	104.239.160.189	TCP	54	62937 → 80 [ACK] Seq=2072 Ack=36673 Win=261472 Len=0
783	37.793925	104.239.160.189	10.45.10.231	TCP	60	80 → 62937 [FIN, ACK] Seq=36673 Ack=2072 Win=33792 Len=0
784	37.794071	10.45.10.231	104.239.160.189	TCP	54	62937 → 80 [ACK] Seq=2072 Ack=36674 Win=262144 Len=0
817	41.654644	10.45.10.231	104.239.160.189	TCP	54	62937 → 80 [FIN, ACK] Seq=2072 Ack=36674 Win=262144 Len=0
871	41.733236	104.239.160.189	10.45.10.231	TCP	60	80 → 62937 [ACK] Seq=36674 Ack=2073 Win=33792 Len=0

▶ Frame 118: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface 0
 ▶ Ethernet II, Src: Apple_3b:2a:1a (c8:2a:14:3b:2a:1a), Dst: CiscoInc_97:cf:7f (00:26:0b:97:cf:7f)
 ▼ Internet Protocol Version 4, Src: 10.45.10.231, Dst: 104.239.160.189

- 0100 = Version: 4
- 0101 = Header Length: 20 bytes (5)
- ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 - Total Length: 64
 - Identification: 0x1214 (4628)
- ▶ Flags: 0x02 (Don't Fragment)
 - Fragment offset: 0
 - Time to live: 64
 - Protocol: TCP (6)
- ▶ Header checksum: 0x0000 [validation disabled]
 - Source: 10.45.10.231
 - Destination: 104.239.160.189
 - [Source GeoIP: Unknown]
 - [Destination GeoIP: Unknown]

 ▼ Transmission Control Protocol, Src Port: 62937 (62937), Dst Port: 80 (80), Seq: 0, Len: 0

- Source Port: 62937
- Destination Port: 80

wireshark_pcapng_en0_20160907101618_0e8Xhm Packets: 1375 · Displayed: 55 (4.0%) Profile: Default

This is the complete network traffic exchange for loading www.djp3.net in Chrome, down to the individual bits that were sent across the Ethernet



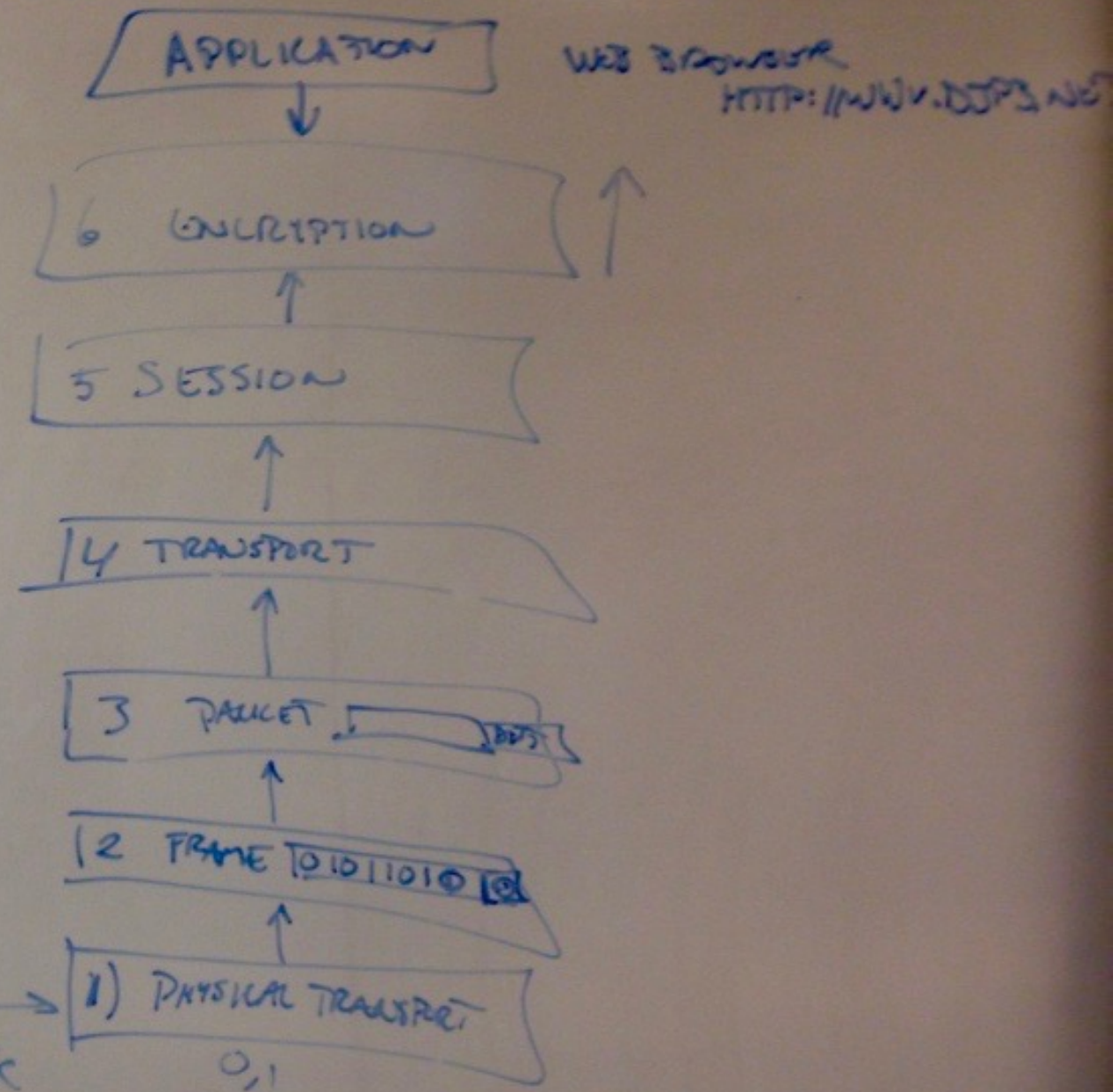
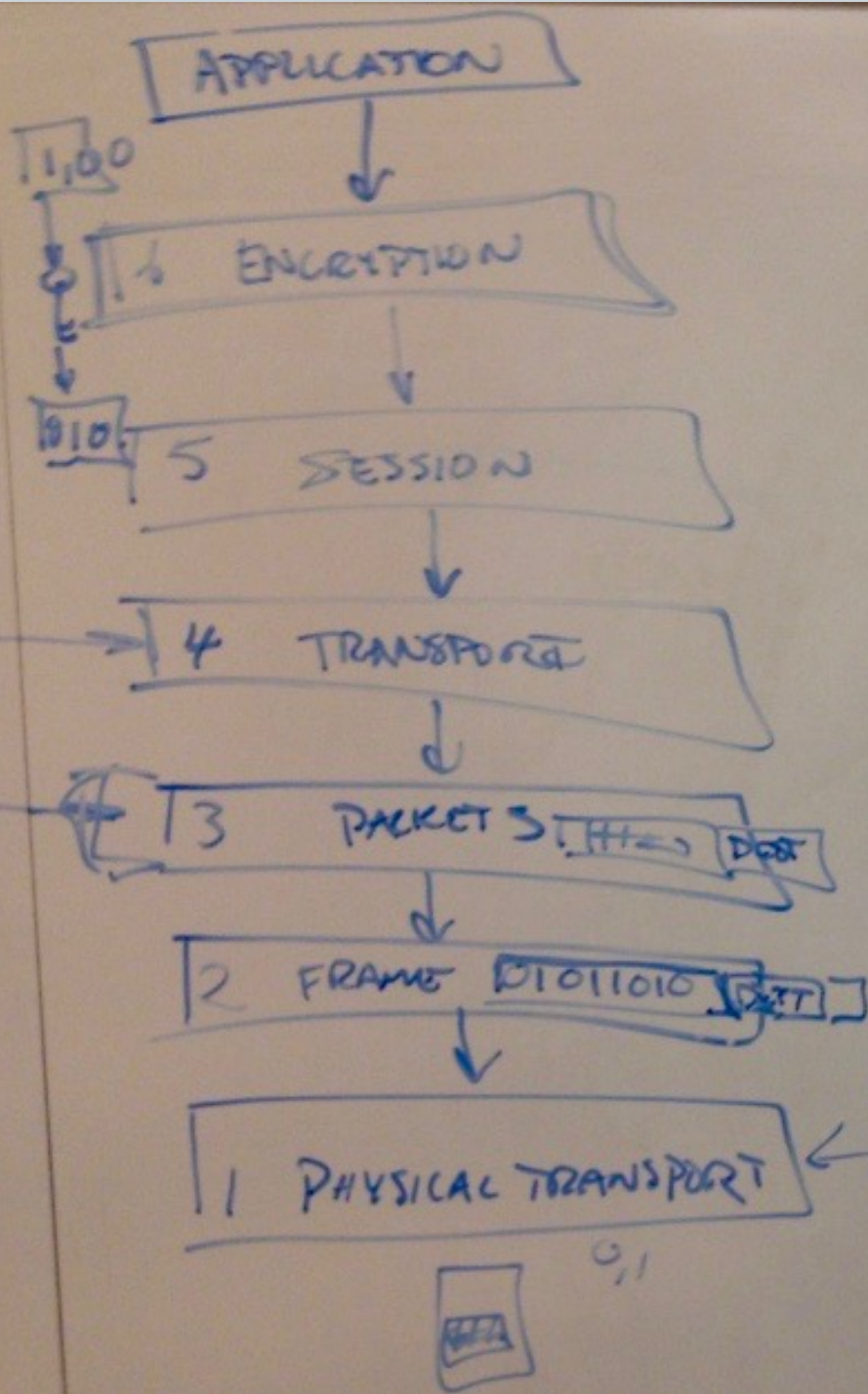
TOOLS SHOWN TODAY

WIRESHARK

- “Wireshark is the world's foremost network protocol analyzer. It lets you see what's happening on your network at a microscopic level. It is the de facto (and often de jure) standard across many industries and educational institutions.”



OSI MODEL OF THE NETWORK



Fiber optic Light over glass

Wired Ethernet Elec over copper

WiFi RF over Air

Modem Elec over copper



NETWORKING DETAILS

IPv4

192.68.1.40

IPv4

32bit, 32bit, 32bit, 32bit

0-255.

www.cnn.com:80

:80 HTTP

A — B

A — B

A — C — D — E — B

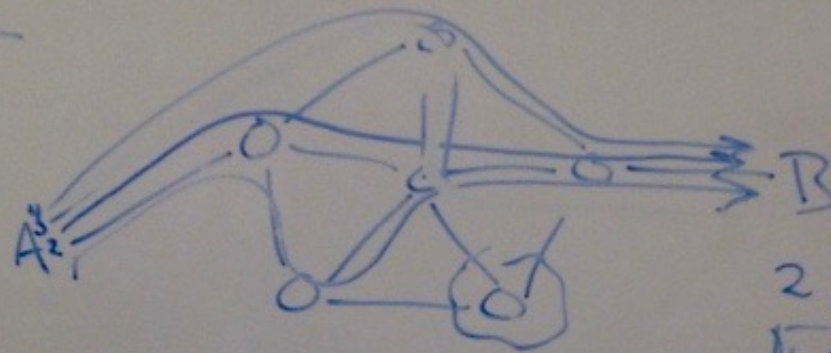
IPv6

HHHH:HHHH:HHHH:HHHH

0-F

0-15

F0B1:5572:131A:DD00



2 x 14

1 2 x 4

3

1 2 3 4

TCP/IP

UDP





WESTMONT **INSPIRED**
— COMPUTING LAB —