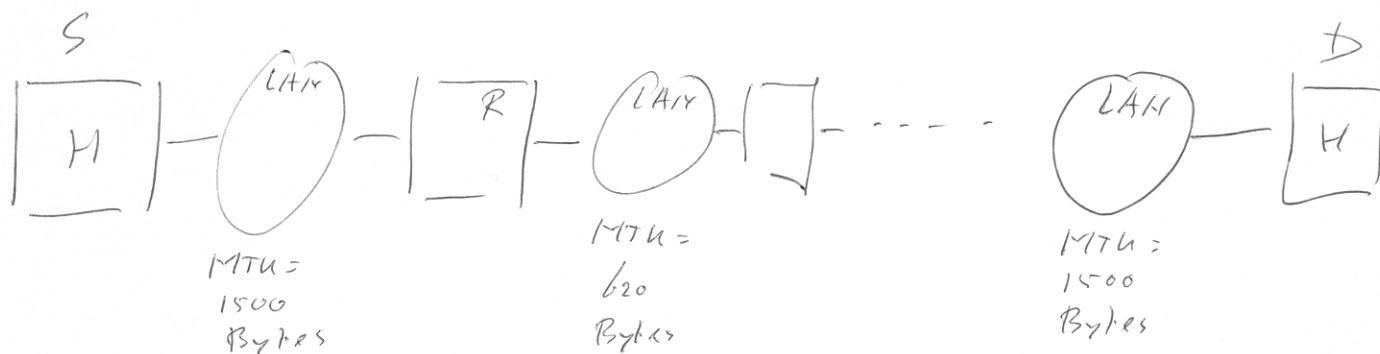


Every LAN has an MTU
Maximum Transfer Unit,
ethernet: 1500 Bytes.



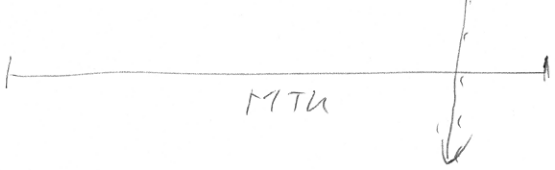
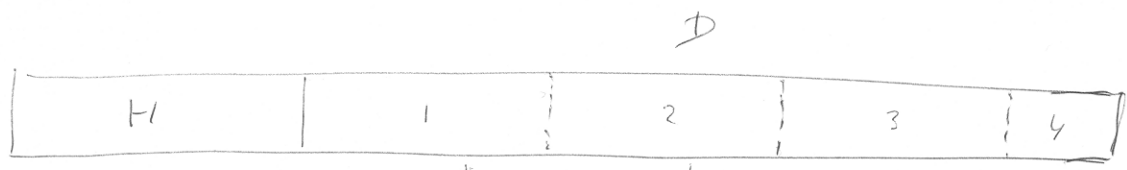
Host S (Source) may send an IP packet of 1500 Bytes (or almost 1500 Bytes); does not fit in later LAN;

Fragmentation

↓ $D=1$ ("do not fragment bit is set");

do not fragment.
drop. Send message.

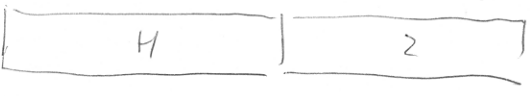
(ICMP) (!)



Fr. 1



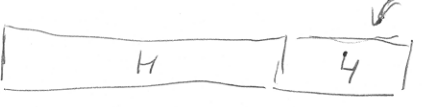
Fr. 2



Fr. 3



Fr. 4



Headers: ^{Largely} "mostly copied". But:

Total length: Recomputed.

TTL: TTL as always

Checksum: Recomputed as always.

Options: depends.

Some only in first fragment.

Some in all fragments.
(later).

Do not Fragment flag: No issue.

The More bit:

M=0 : This is the last (incl. only) bit.

M=1 : There is more to come.

Fragmentation Offset:

The number of data bytes in preceding fragments.

In units of $\delta = 2^3$ Bytes.

Why units of 8 ?

Fragmentation Offset field is 13 bits.

$$2^{13} = 8192. \quad \text{Start here} \quad 2^{13} \times 2^3 = 2^{16} = 65536 \quad \text{Start here} \quad 02/13/2004. \quad \text{Start here} \quad 02/17/2004.$$

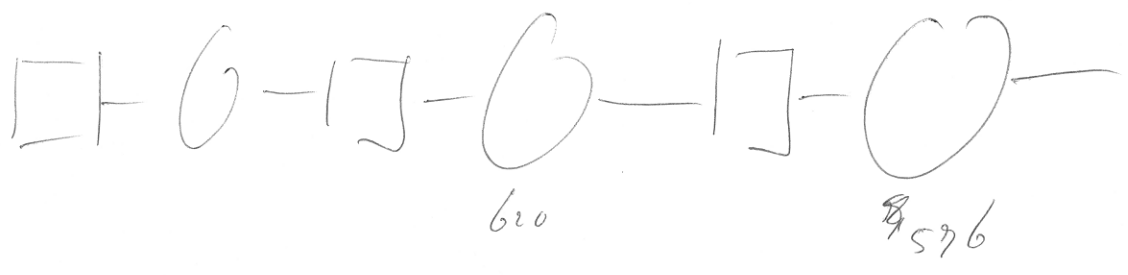
All but the last fragment have a number of data bytes that is a multiple of 8.

Hence : Length of fragment likely to be less than MTU !

(if "greedy" : $MTU - 9 \leq TL \leq MTU$)
for non-last fragment.

Re-assembly: in final destination.
not intermediate routers.

Fragment can be further fragmented



A fragment with $M=1$:

all pieces get $M=1$.

A fragment with $M=0$ ("last")

all but last get $M=1$

last gets $M=0$.

Different fragments of one packet may take different routes!

(Forwarding Tables are dynamic).

ICMP

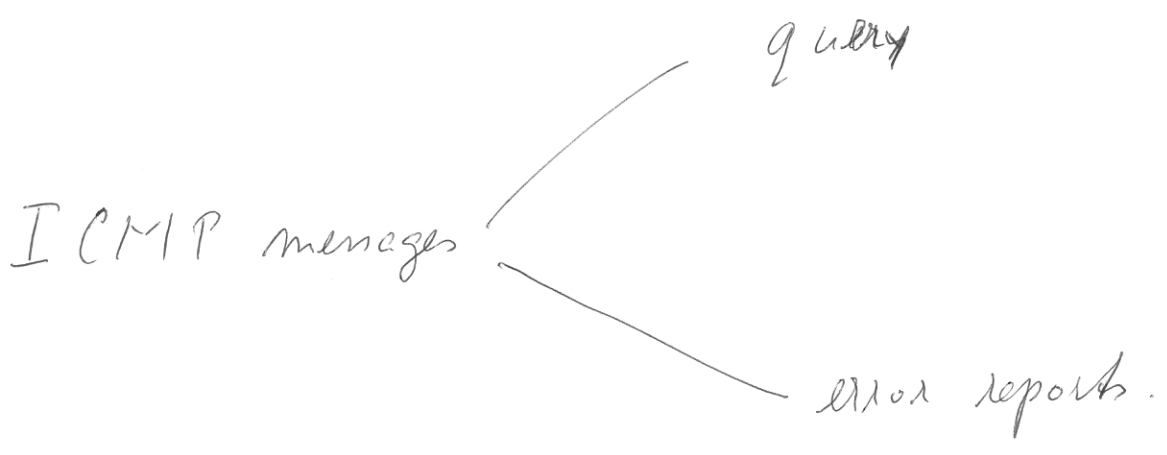
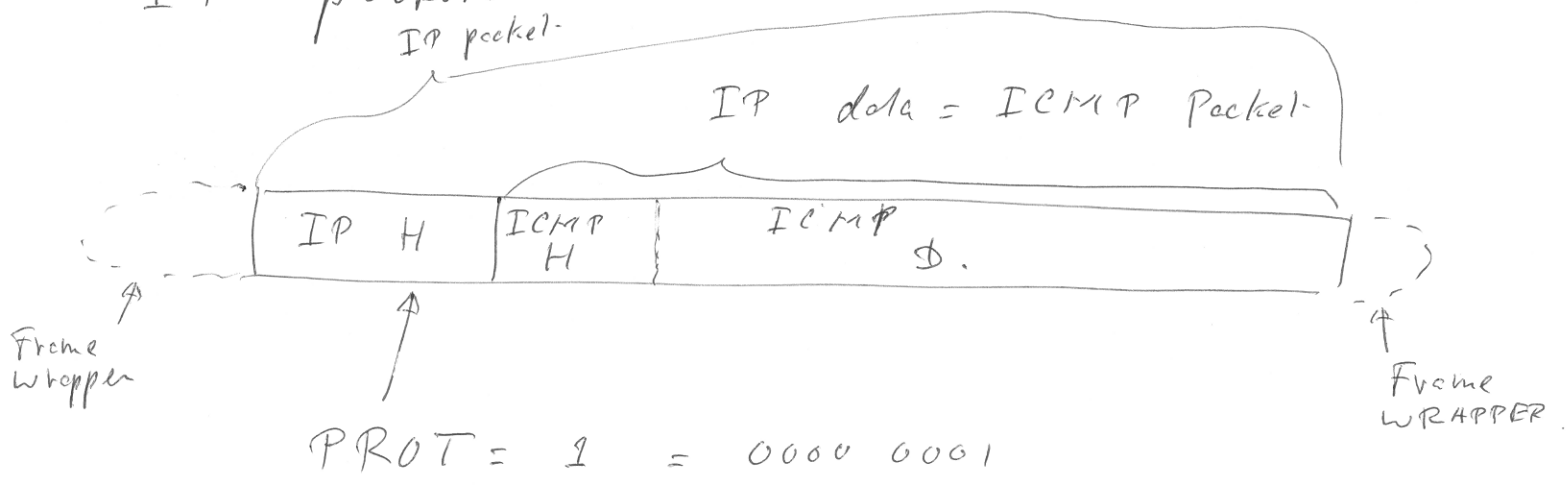
Internet Control Message Protocol.

Examples:

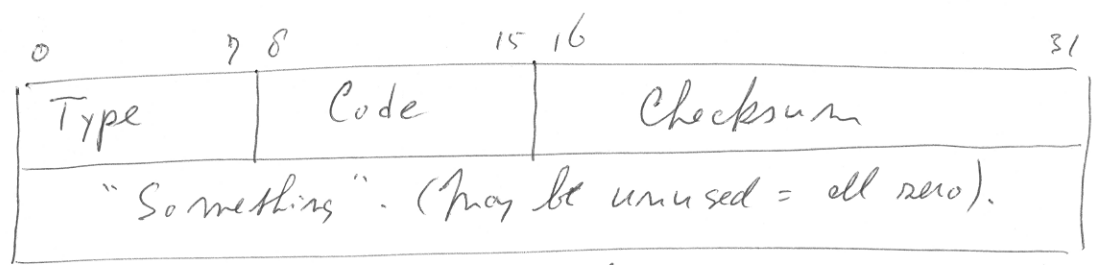
- (1) Router receives packet that is too large for the next hop (MTU), and DF bit is set: drop packet and send ICMP message to source.
 - (2) Router receives packet and ~~to~~ does not find a matching route in forwarding table, and does not have default route: drop packet and send ICMP message to source.
- etc.

ICMP messages are carried inside

IP packets:
IP packet-



ICMP Header:

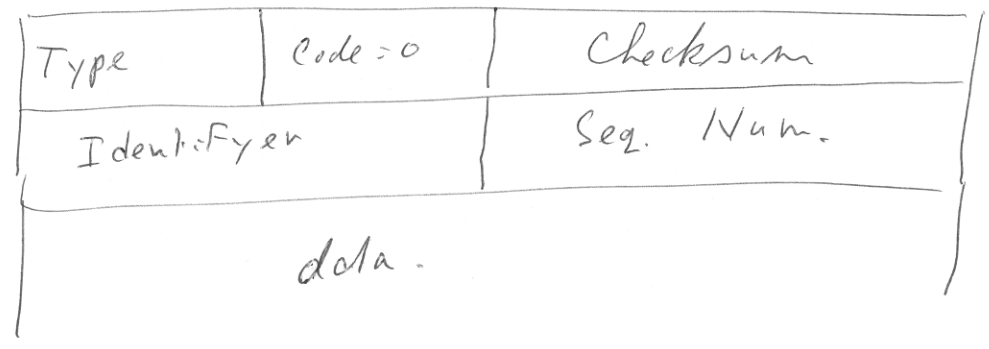


(plus possibly ICMP data).
Checksum: whole ICMP packet.

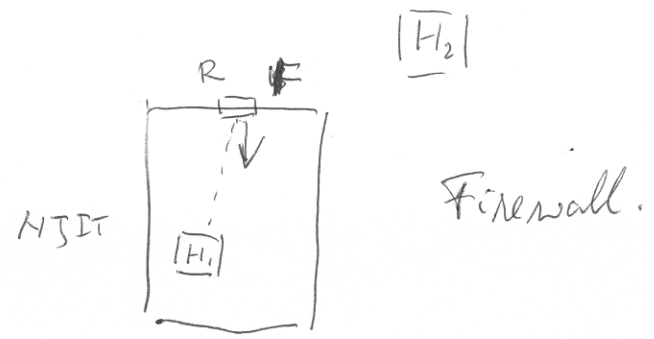
ICMP Echo Request
("Return this to me")

ICMP Echo Response

Type: 8 for request, 0 for response.



Echo Request / Reply are the basis for
Ping.



Ping.

Ping arrangements are slightly different from OS to OS.

typical

```
>: ping <name>
    <name> is alive.
```

(<name>: either domain name or IP address)

```
>: ping -s <name>
```

Result: a sequence of ping packets for each the round trip time is given.

end with control-C :

```
gives # packets transmitted
      #      received
      packet loss
```

min / avg / max Round Trip Time.

There are options to set:

data bytes per ping packet.

packets to be sent,

Time between packets (default = 1 sec). (don't charge this!)
etc.

do

>: man ping.

Homework : (do not hand in).

① Log on to aFs x.
ping aFs y (x ≠ y)

play with ping.
(round trip time in msec. accurate).

② Log on to laFite or mouton.

(Linux computers in my lab:
Remote logon only!)

lafite.njit.edu.

From lafite or montou:

ping aFsx.

play with ping.

round trip times are given in μ sec accurate.

Send me Email if you can not log on to
lafite or montou

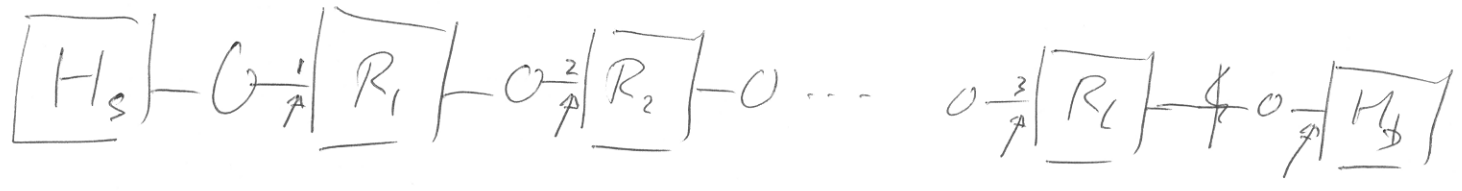
ICMP error messages.

If a packet causes a problem at end must be dropped, when possible an ICMP error message is sent:

Typical Format

Type	Code	Checksum
Something (possibly unused = zero)		
Data = IP header of offending packet, plus the first 64 bits of IP data		

ICMP Time exceeded is the basis for
Trace route.



H_s sends a sequence of packets, all destination address H_d .

with TTL = 1,

TTL = 2

etc. (default: 3 of each).

TTL=1: ICMP Time exceeded from R_1
(address 1)

TTL=2: ICMP Time exceeded from R_2
(address 2)

etc.

So you find the route from H_s to H_d .

with Round Trip Times.

Traceroute: default sends UDP (later)
 option send ICMP echo Request. ~~default~~
 (in some OSs: default?)

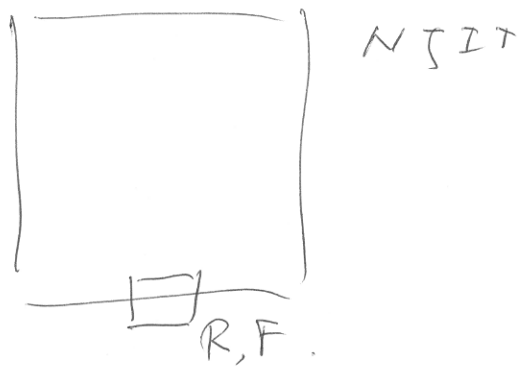
Trace route:

Log on to ofsx. do
"mon traceroute".
play with traceroute.

Try Traceroute to
same net.,
different one

Log on to ~~ats~~ lafide, to Mountain.
do "mon traceroute".
play with traceroute.

Problem with NJIT firewall.



Router,
Firewall.

The Firewall does not let ICMP packets
through!
(Defense against DoS attack).

Ping, Traceroute do not work between
inside & outside.

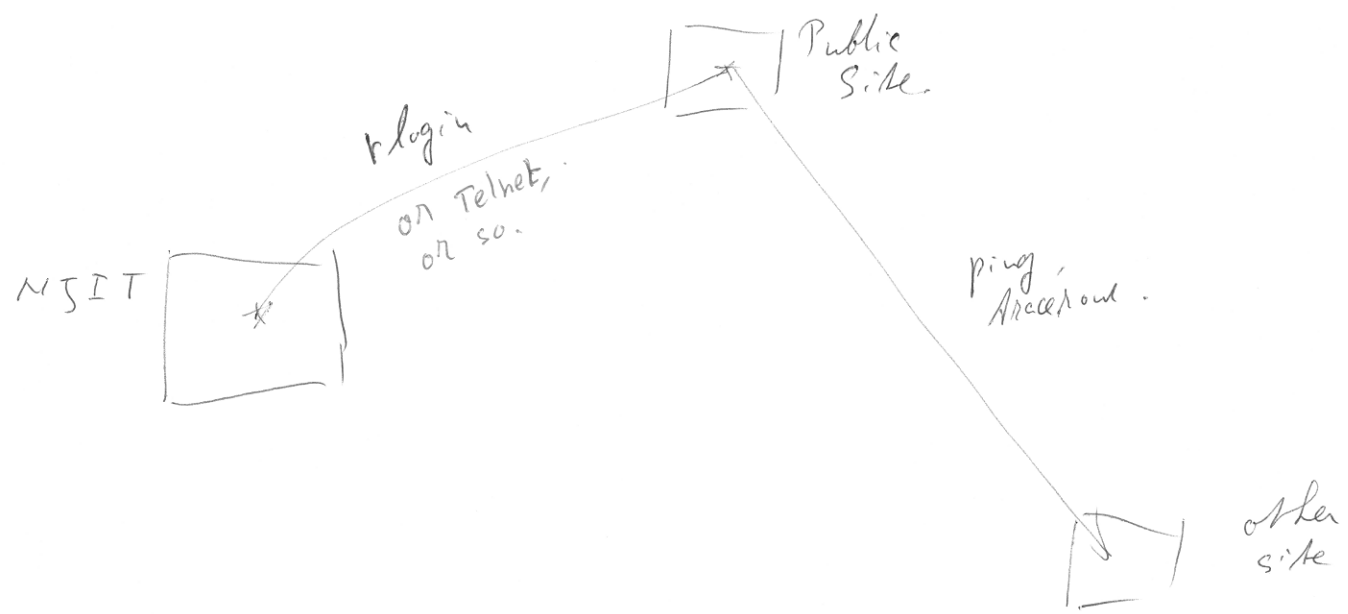
Go

Homework:

Go to Google.

Search for ping,
traceroute.

You will find "~~publ~~" "public"
ping, traceroute sites.



traceroute;
only routers on the way from
public site to other site.

List of Types,
Codes,

~~Forman~~
Forouzan pp 228-229,
etc.

Cornel p. 133, p 135

Query	ICMP Type	Error Reporting Message
Echo Request	8	Destination Unreachable
Echo Reply	0	3
Timestamp Request	13	Source Quench
Timestamp Reply	14	4
Address Mask Request	17	Time Exceeded
Address Mask Reply	18	11
Router Solicitation	10	Parameter Problem
Router Advertisement	9	12
		Redirection
		5

Such an ICMP error message is
sent for "~~everything~~ going wrong"
anything

But not for an ICMP error message
going wrong. (Obvious!).

It is sent for IP datagram,
ICMP query.

not for ICMP error message.

ICMP messages.

Echo Req, Reply (did).

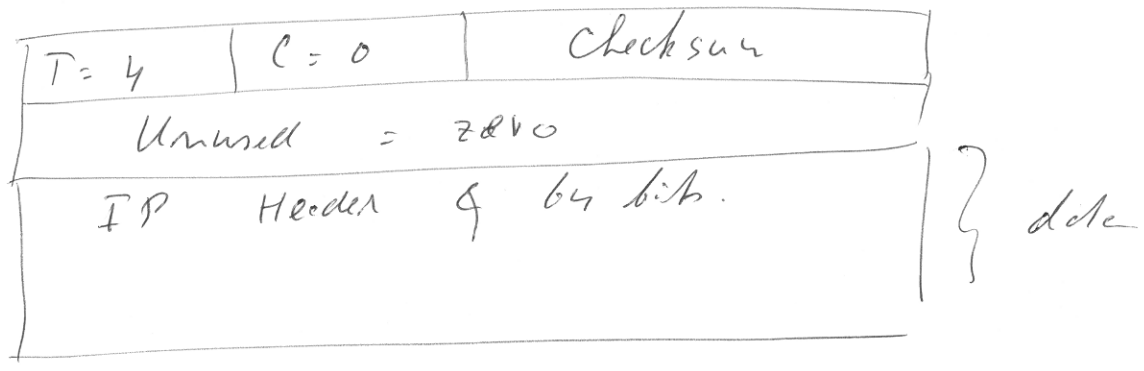
Cover p 134
Forouzan p 239

Destination unreachable (did)

Cover p 134.
Forouzan p 230 etc

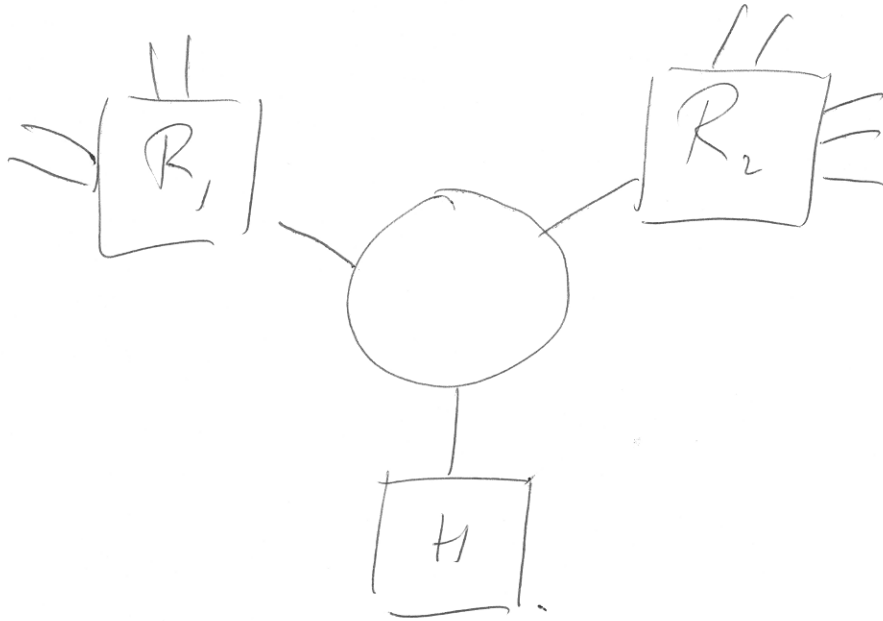
Source Quench.

Cover p. 136 etc.
Forouzan p 233



NO "compulsory" reduction in flow!

Redirect.



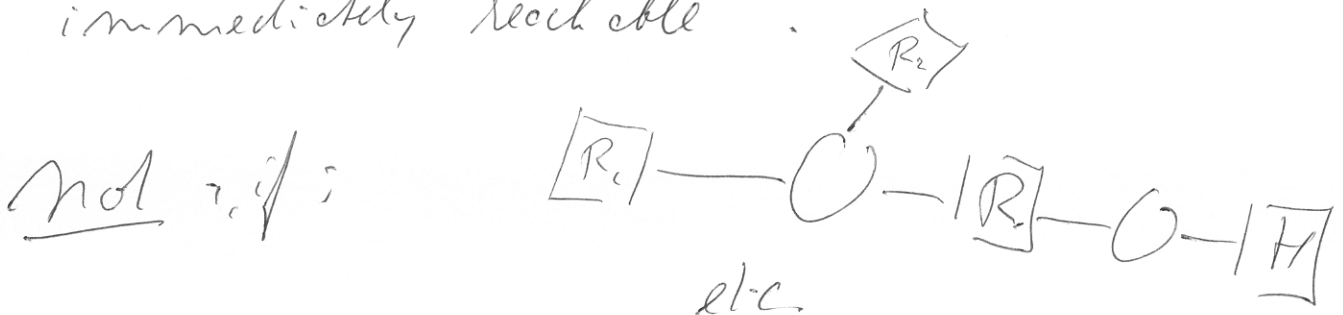
Host sends IP packet to some address.
Forwards to R_1 .

R_1 "knows" R_2 is more appropriate.

(1) Forwards packet to R_2
("nice guy")

(2) Sends Redirect to H.

Redirect is sent only if source is "immediately reachable".



Redirect:

T=S	C=...	Checksum
Router IP address ("better R").		

Code: complicated. don't worry. { Code: 0 Net/Speck
1 Host Sp.
2 Net, ToS
3 Host, ToS.

Time exceeded: Comer p. 139.

do need! Forouzan p 234

Para

Parameter Problem

Forouza p 235

$T=12$	$C = \begin{cases} 0 \\ 1 \end{cases}$	
PTR	Unused = zero	
Interms H + 64 bits		

PTR: pointer to start of offending field.

Obtaining a subnet mask:
Comer p 142

Forouzan p 241

Router discovery
Comer p 143

Forouzan p 242-

Router Solicitation
Comer p 144

Forouzan p 242

All three: read yourself.

(Ends ch. 9) (Forouzan Ch-9)
(Comer Ch. 9)

Delay (Without congestion).



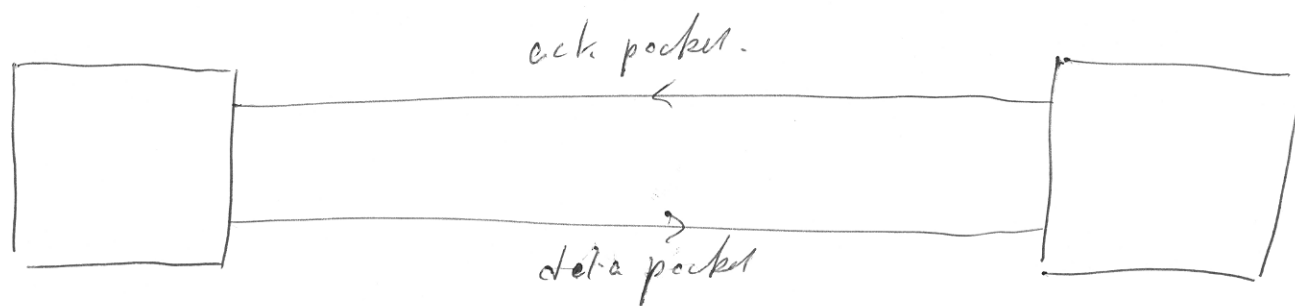
Propagation Delay : P_d (sec., or msec)

Bandwidth ~~P_b~~ d_r (bits/sec) or

Packet size P_S (bits).

$$\text{Delay} : \frac{P_S}{d_r} + P_d$$

|



Packet sizes : PS_d , PS_a

Prop. delay : P_d

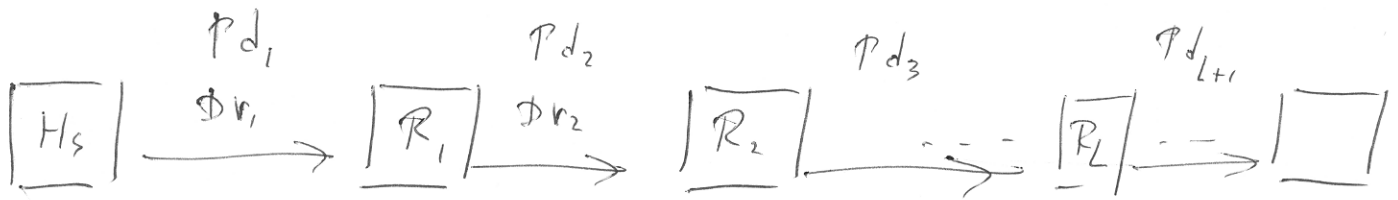
data rate : Φ_r .

Round Trip Time =

$$\left(\frac{PS_d}{\Phi_r} + P_d \right) + \left(\frac{PS_a}{\Phi_r} + P_d \right)$$

In case of ping

$$PS_d = PS_a.$$



Packet size: PS .

Delay: (one way)

$$\left(\frac{PS}{B_{v_1}} + P_{d_1} \right) + \left(\frac{PS}{B_{v_2}} + P_{d_2} \right) + \dots + \left(\frac{PS}{B_{v_{L+1}}} + P_{d_{L+1}} \right) =$$

$$= PS * \left(\frac{1}{B_{v_1}} + \frac{1}{B_{v_2}} + \dots + \frac{1}{B_{v_{L+1}}} \right)$$

$$+ P_{d_1} + P_{d_2} + \dots + P_{d_{L+1}}.$$

we do the experiment over and over again, varying only PS :

$$\text{Delay} = PS * C_1 + C_2.$$

Assumes: "Store and Forward"
no cut-through.

Ping (again).

90

on my workstation:

ping -s <name> 100 10
(different on different OSs) ←
causes 10 Ping packets, each 100 Bytes

Ping data.

Response:

108 bytes From <name> --- icmp_seq = 0 time = ...
1
2
↑
(?)

100 Bytes Ping data
with 8 Bytes ICMP header;

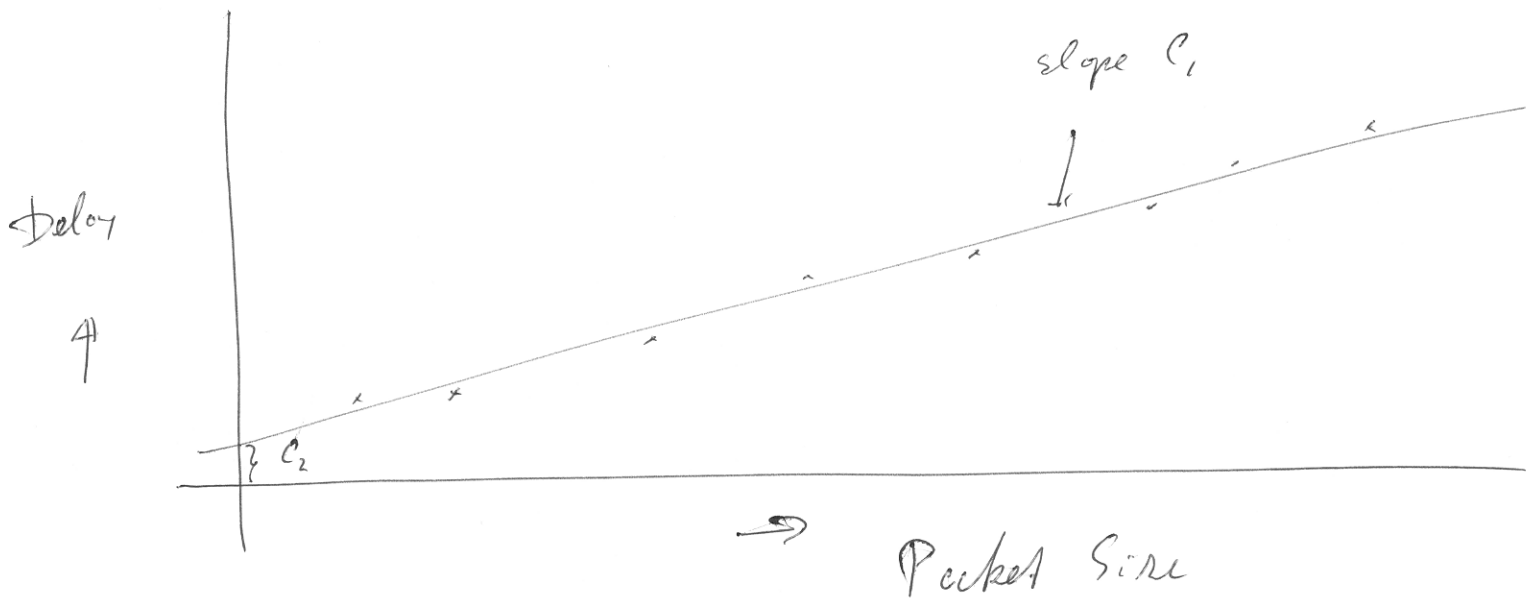
108 Bytes IP data

with IP header;

Packet size is 128 Bytes.

with ethernet header: framesize = ...

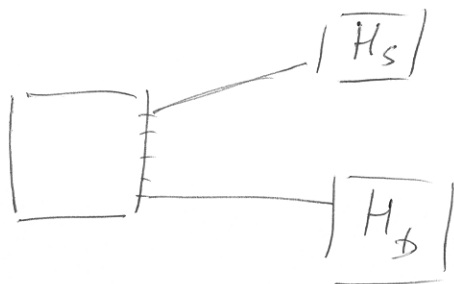
$$\text{Delay} = C_1 * (\text{Packet size}) + C_2$$



C_2 : Propagation delay.
and Software delay.
(and congestion).

$\frac{L}{C_1} = \text{If one hop:}$
 $\frac{L}{C_1} = \Delta t$

Problem with ethernet switches.



Ethernet Switch
does store and forward.

Log on to left, moulton.

Are they on the same VLAN?

Use ping to determine:

What is the date of that VLAN?

Is there an ethernet switch in between them?

Do you ping:

The command is different on linux.

// Same for other networks.

Also between networks.

// Ping: primarily for
 "is alive"
 "distance" (small packets).

The difference between "query" and "error report" is important. (somewhat). Why?

When an IP packet comes to a router and the router can not route the packet,

it :

(1) drops the packet.

(2) Send ICMP message to source.

ICMP error report

" Destination Unreachable,

with as data :

The IP header of the offending packet, plus 8 Bytes (64 bits) of the IP data. (if there)

(Usually: that is the first 8 Bytes of TCP Header or UDP header).

Cornet p 135.

Forouzan p 231

Many Codes:

- 0 : D. Network Unreachable
 - 6 : D. Network Unknown
 - 1 : D. Host Unreachable
 - 7 : D. Host unknown.
 - 4 : Fragmentation Required, DF=1.
- etc.

) difference?