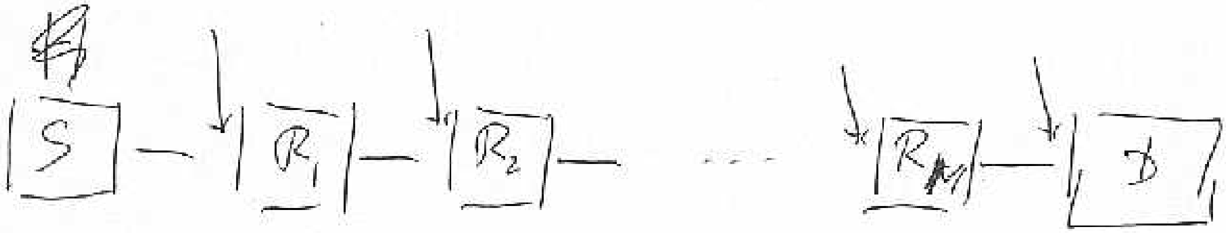


PA = 4.

On leaving S:

dest address: R_1, left

first option addr: R_2, left.

⋮

last option addr: D, "left"

} 2, 3, …, M, "D" — M addresses. $K \geq M$. ($K = M$?).

R_1: put R_2, left in *dest*.
put R_1, right (outgoing) into first

} address PA points at.

in general:

R_i: put R_{i+1}, *left* in dest.
put R_i, *righ* (outgoing) in address pointed at

} address pointed at.

PA += 4

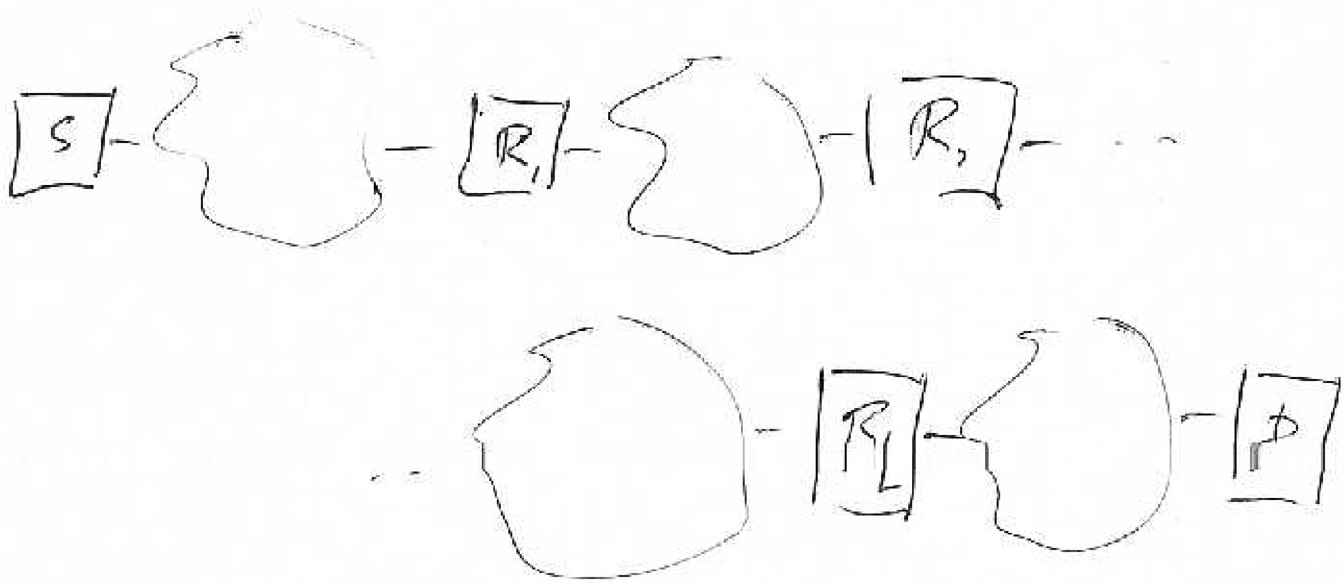
Loose Source Route

Copy = 1

Class = 00 1000 0011

Number = 3

☆ Only specific routers must be visited, in specific order, but gaps allowed



In $R_1, \ldots, R_L$: "same rotation as in strict source route".

But no requirement that "next" is reachable in one step.

Time Stamp option.
Comer p. 112

IP Time stamp option

Comer p 112

Code	Length	PTR	Oflow	Flags
first IP address				
first time stamp				

Flags:
- 0 Timestamps only
- 1 Time stamps & IP address
- 3 IP addresses ~~pre~~ specified by source! (~~change~~ do it only if you find "your" IP address)

Time:

<u>Date</u>, and time in msec. since last midnight GMT.

or: any convention you have agreed on.

Oflow: # of routers that could not provide timestamp because "PTR beyond options"

Back to addressing.
Comer, ch. 10.

Old (classfull) addressing scheme led to

(1) Inefficient use of address space
(2) Large Routing Tables in Routers.
which led to lots of traffic between routers.

(3) Administrative overhead.

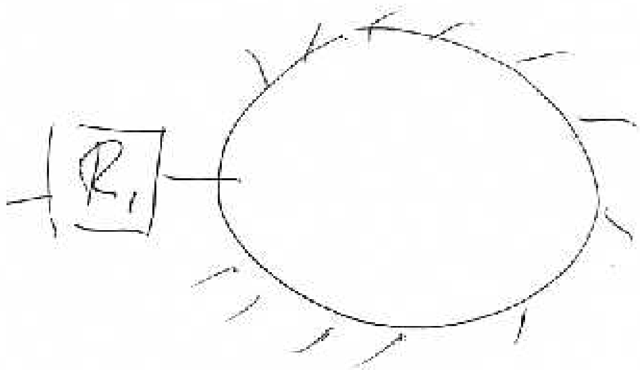
~~(address sp~~
Comer: with CIDR etc:
address space OK until 2019?
I doubt it.
Maybe with NAT?

Within a company, Univ, ...,
you can do whatever you want,
as long as the outside world does not need
to know.

Methods:

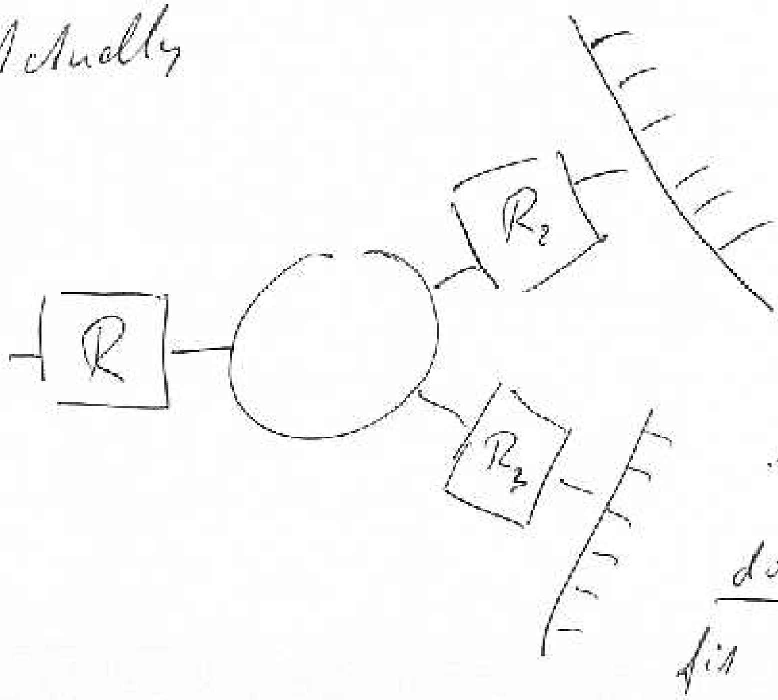
1. Transparent Routers.

From outside you think:



LAN with thousands (hundreds of thousands?) hosts.

Actually



"Nobody" (outside "Network") knows about R_2, R_3, ...

In this case "subnetwork boundaries" do not have to fit in with CIDR, masks, etc. Need not even be contiguous!

Transparent Routers.

But usually ~~you~~ they did / do something "CIDR-like".

Convention:
(Assume class A)

10. p. u. i

p ↑ denotes "router" (transparent)

i ↑ host.

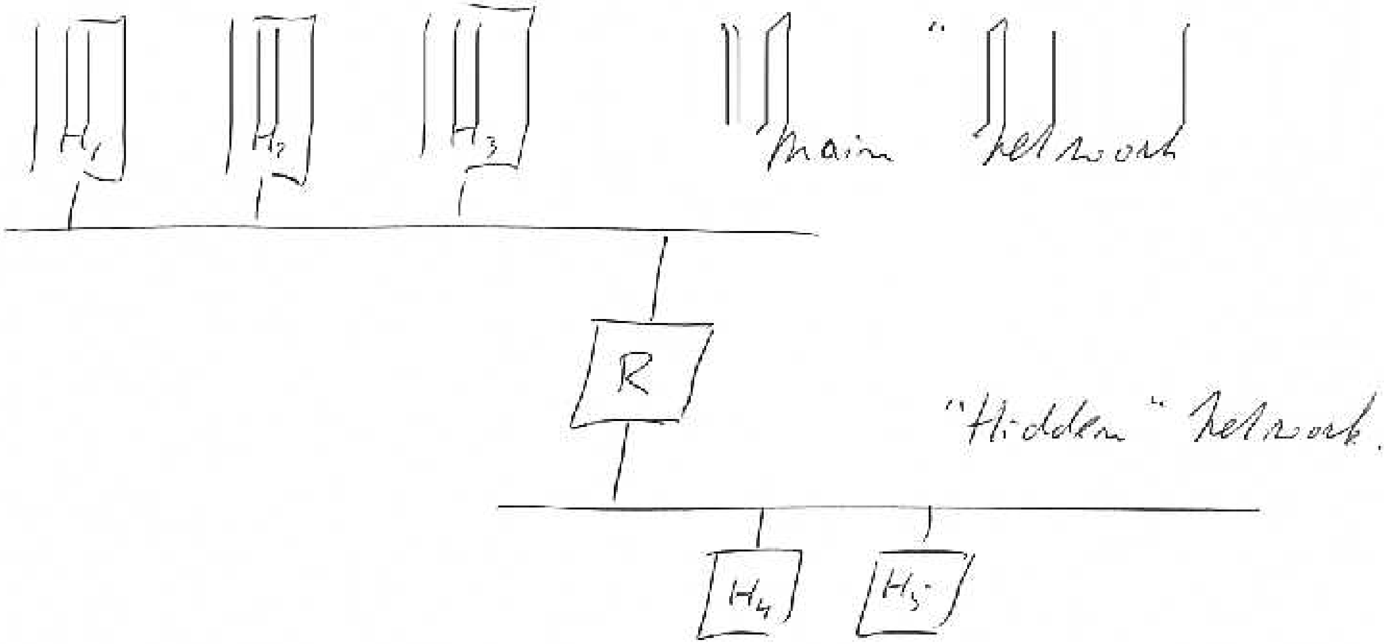
u: unused.

The network needs a <u>large</u> address space.

To make this work you <u>also</u> need something like
proxy-ARP.

ARP Hack,

2. Proxy ARP. Promiscuous ARP.



H_1, H_2, H_3, H_4, H_5 <u>think</u> they are on the same "LAN".

But they are not.

If (e.g.) H_1 sends an ARP Request for (e.g.) H_4:

R responds with its own physical address. (the one "toward" H_1).

R: must know the whole layout!

Problem: H_1 might find out that H_4 and H_5 "advertise" the same physical address.

(Proxy ARP).

Problem: must use ARP.

---

(3). Subnet Addressing

Idea: take class B address space, divide it up into "Subnets".

Network	local

Internet	physical subnet	Host.

"Basically" same as CIDR.
(in my opinion. tjo).

All masks are contiguous! (Comer p 150).
I will not ask about Comer section 10.10
(Read once, then not again).

Comer says that when using subnetting, all subnets must have the same length mask.

NJIT does not do it that way.
Who is right.
(I vote for NJIT)

Every Host must know its subnet mask!

Broadcast: to subnet.

Anonymous Point-to-Point links: later

---

(4) Supernetting.
Classless Addressing.
Done before. CIDR.

Did not mention: ROADS.
Running Out of Address Space

(Network Address, Count) not used.

x.y.z.u/c $0 \leq c \leq 32$.

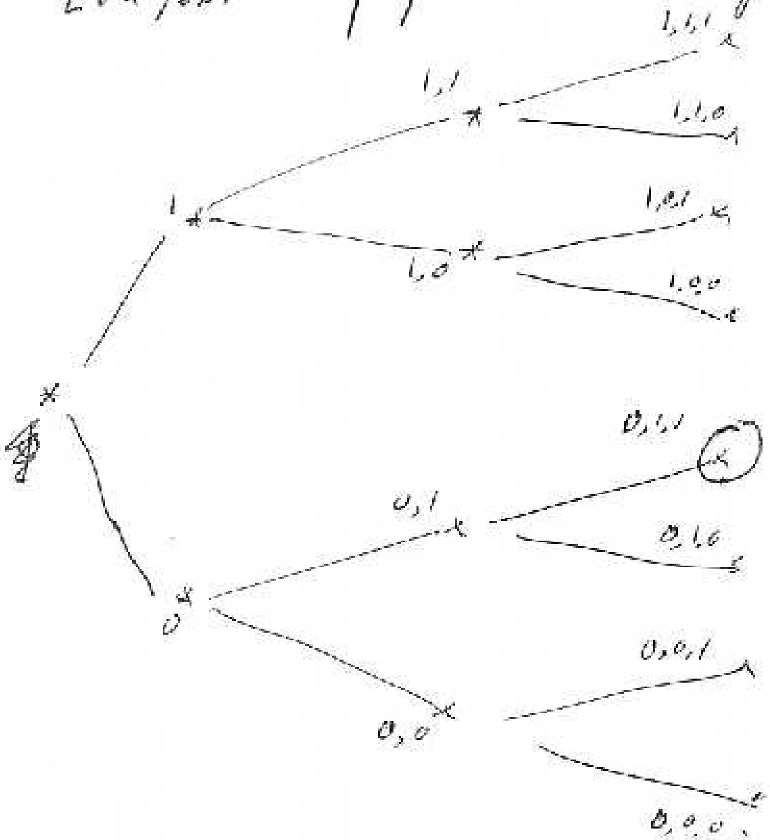
The binary representation of x.y.z.u must have at least (32-c) zeros at the end.

CIDR: soln

addresses no longer self-identifying.

// Skip section 10.23.1 in book.

Longest prefix routing.



(*) : a prefix of length 3.

96.0.0.0/3.

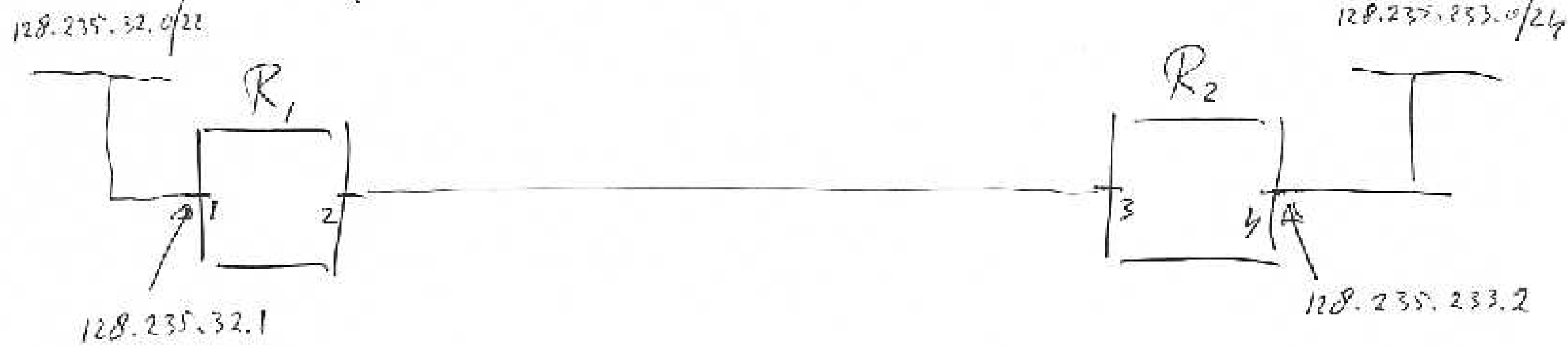
An <u>entry</u> in a forwarding table is a <u>prefix</u> to a set of addresses.

(A prefix of length k is a prefix to $\sim 2^{(32-k)}$ addresses.

(not all of which ~~are~~ can be host addresses)).

5. Anonymous Point to Point links.

(Anonymous Point to Point Networks).
(Unnumbered Network).



The link from "port 2" to "port 3" does not need physical addresses, does not need IP addresses.

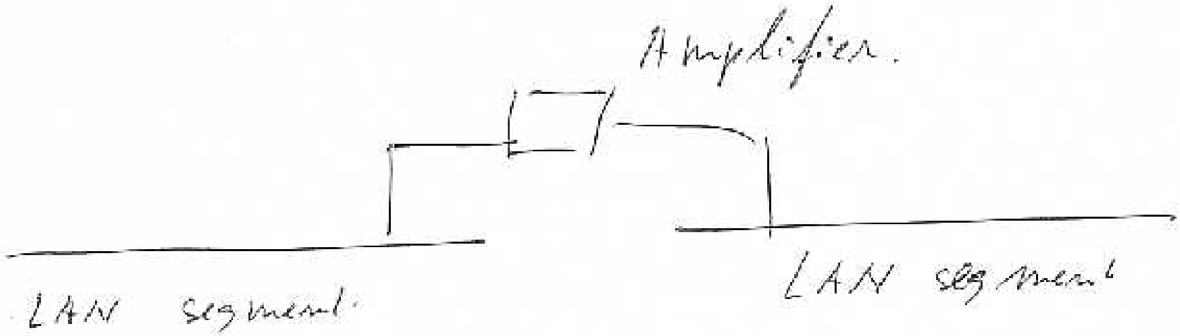
R1, in its forwarding table, uses "one of the other IP addresses" of R2. e.g. 128.235.233.2

In R1:

Mask	Netw.	Action	Interface.	Next address
255.255.253.0	128.235.32.0	DD	1	
255.255.255.0	128.235.233.0	Forw	2	128.235.233.2

(Saves some addresses).

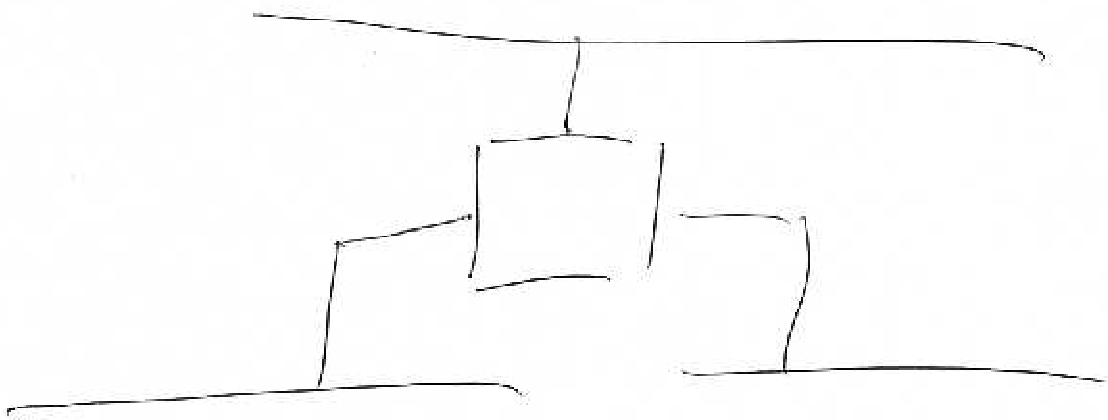
Repeaters,
Hubs
Bridges } From the time of coaxial cable.
Switches
Layer 3 Switches. } since.



Amplifier: amplifies everything
including noise.
including collisions.
enables collision between
"RHS" and "LHS".

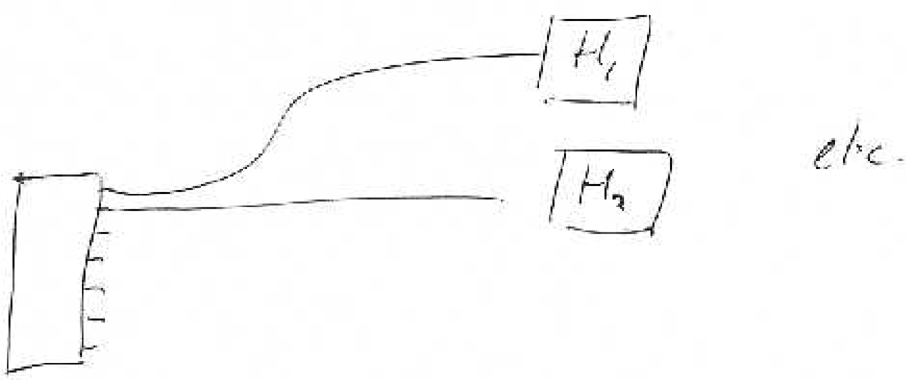
Hub: generic name..
could be anything

Bridge: Usually denotes
"Learning Bridge"



Learns which side ~~that~~ hosts
(physical addresses) are.

Ethernet Switch.



Category 5 cable.

This also "learns".

Layer 3 switch.

"Ethernet switch that understands IP addresses".

With VLAN Capability.

VLAN: Virtual LAN.

You can divide the customers into (up to 8?) Virtual LANs.

The Layer 3 Switch emulates Router Behavior:

~~decr~~ decreases TTL between VLANs, not inside one VLAN, etc..

This is the set-up in NJIT.

Don't know details.

VLANs can be defined as on the basis of:

Port number on Switch.

Physical Address of computer

IP address of computer ←

Combinations

The routers in NJIT do even more. including:

1. "Label Switching":
The First packet of a Flow is "software switched": takes more time.
Then a path is set up.
Later packets go Faster.

2. Cut-through.
"Switching", "Routing" occurs as soon as the header is in. Before rest of packet is in. Then packet Flows through, no need to store whole packet First.

more abstractly:

Router R:

Take address pointed at.
move it to dest. addr.
Take own outgoing address.
move it to address pointed at.

PAr += 4

If PAr > L: just route.

<u>Strict</u> source route:
(as long as PAr < L):
next address <u>must</u> be reachable in one hop.