Purpose of Subnet

— Better management of IP space, Better policy enforcement etc
— Typically at organization level

Purpose of Route Aggregation/Supernet

— Reduce no of entries at routers
— Typically at higher level routers.

Default route - present typically only in lower level gateways/routers

⟹ **IP Header:-**

→ Data Connectness to be done by higher level protocol

⟹ Header to protect to send the packet to correct destination and prevent other issues.

⟹ **IHL:-** specified in 4 bytes words

⟹ Why 4? ⟹ Memory alignment

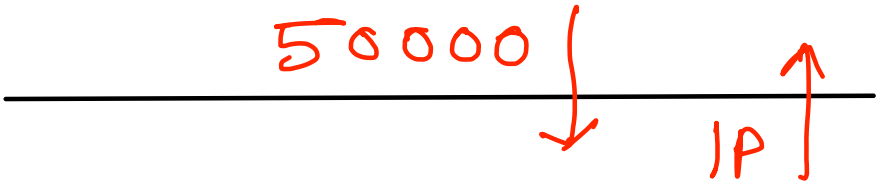
TOS Field largely ignored:-

① Appl can set it arbitarily
② Increases packet processing times at routers. Matters especially when

router is busy

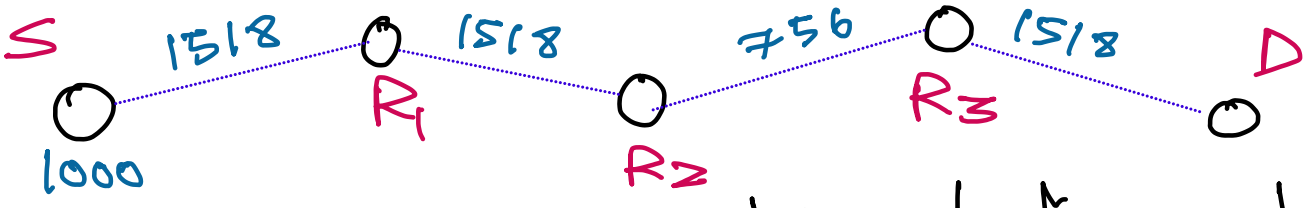
Functions of n/w Layer

- Routing (Both building the routing Table and forwarding packets) — Primary
- Fragmentation & Reassembly



65836

1518 Ethernet



⟹ For an IP datagram, that is not fragmented

MF=0, DF=0, Offset=0

⟹ For an IP datagram that is fragmented

first packet, MF=1, offset=0

For all but last, MF=1, offset≠0

Last MF=0, offset≠0

⟹ Reassembly at destination only

⟹ How to Know bottleneck MTU?

⟹ Send 1500 with DF=1

⟹ If no error rcvd. Assume all 1500

→ Some Router drops, Send back ICMP to Source

⟹ Binary Search

(Issue: ICMP packet may get lost)

Issue With ICMP Ping

⟹ ICMP creates congestion

⟹ Affects the state it is trying to measure

⟹ Ideally should measure when it is doing nothing

Bandwidth?

⟹ Ping with data length of different sizes along with header.

ICMP ⟹ Say the Reason why it was dropped

→ Source addr in ip packet ⟹ We can get the Router's address.

TTL=0 → Send icmp

1) TTL=1, 2000 bytes data
2) TTL=1, 10000 " "
3) TTL=2, 2000 " "
4) :

Bandwidth

Dest does not send Icmp (No Error)

Routing Algorithms:-

Any dynamic cost like traffic carried you need to measure it periodically

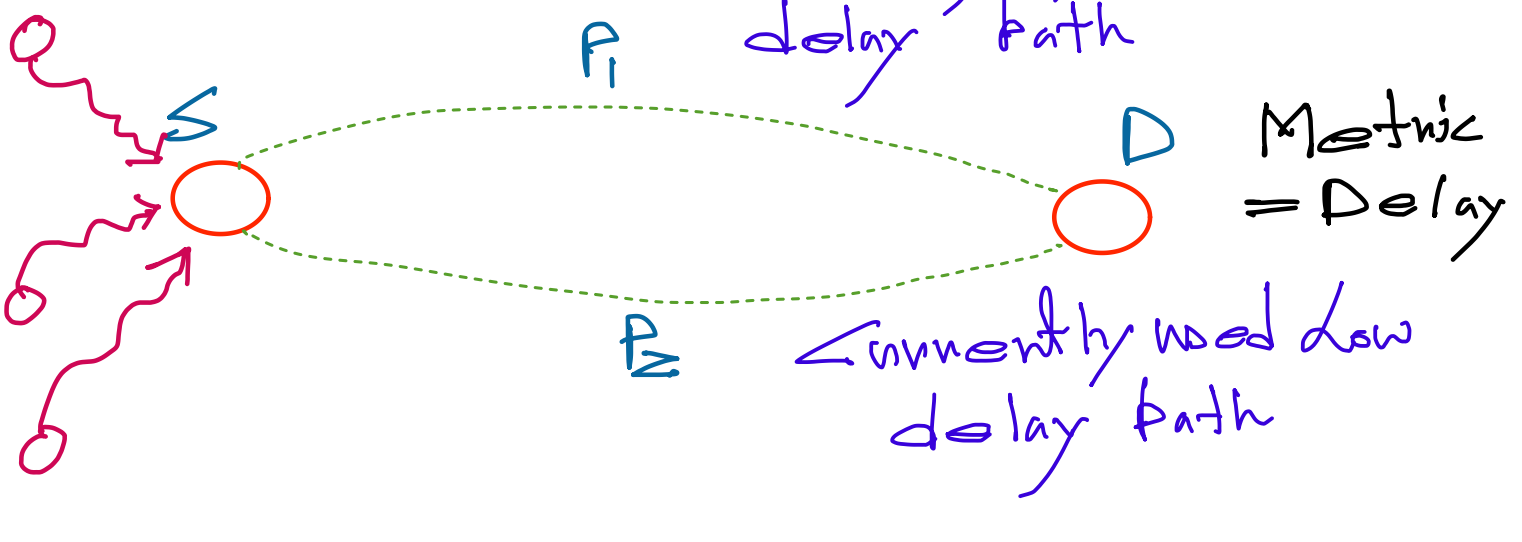
⟹ higher no of messages + other problem

⟹ We do:-

How the internet works?

Distributed:-

Table built even if no packet is sent.



⇒ Change the table if delay persists for a long time

Distance Vector Routing:-

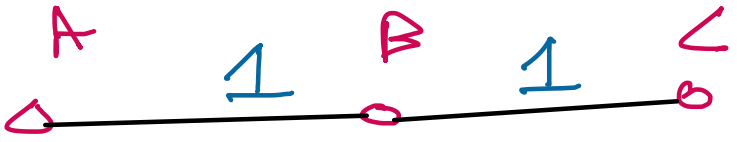
Dest	Next Hop	Cost

<p,q,<> → <p,q,<>

Even if <'><
if q is telling us so.

("always trust the next hop")

⇒ What about deleted nodes?

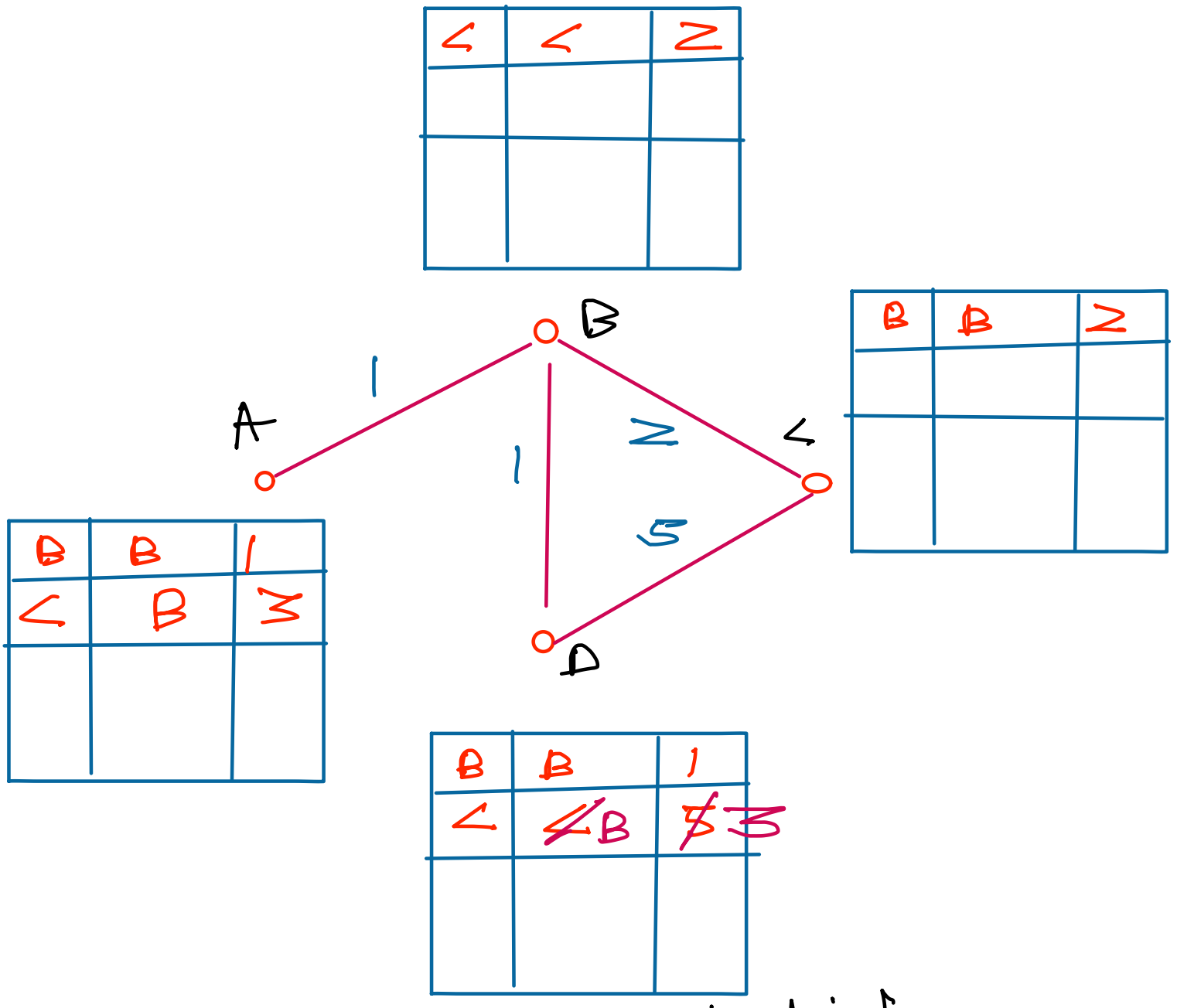


(B,<) goes down

B removes (<,<,1)

So by the simple code we write (C,B,2) stay forever at A.

⇒ This is why routes are not removed immediately



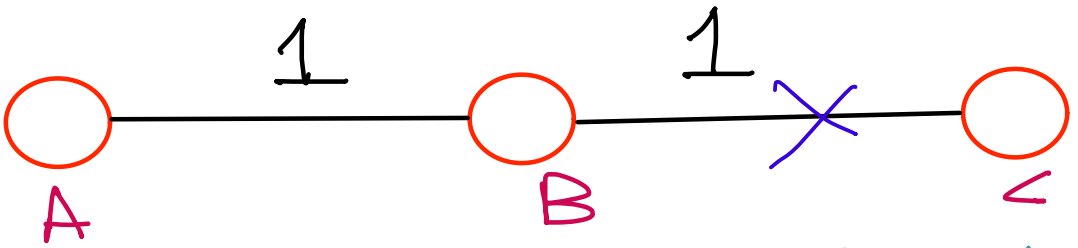
After 1 round, You Know 1 hat info

" 2 " " " 2 —" —

" 3 " " " 3 —" —

d-th ——————— full info

(d = diameter)



<A, 2>

<B, 1>

<C, ∞>

B <C goes down

Good Case!

<B, 2> ←

Trust the next hop

Bad Case!

→ <A, 3> → ∞ is lost

<B, 4> ←

→ <A, 5>

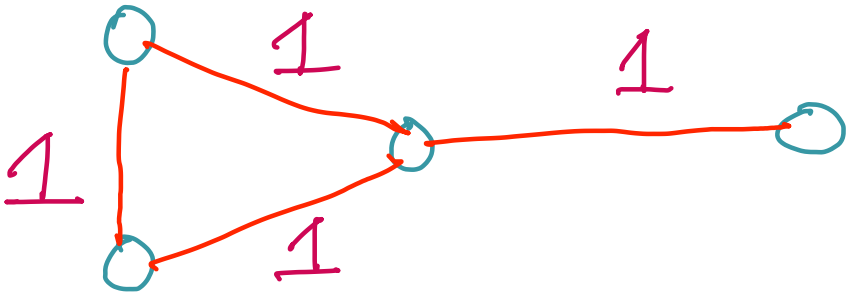
Counting to Infinity

Sol:

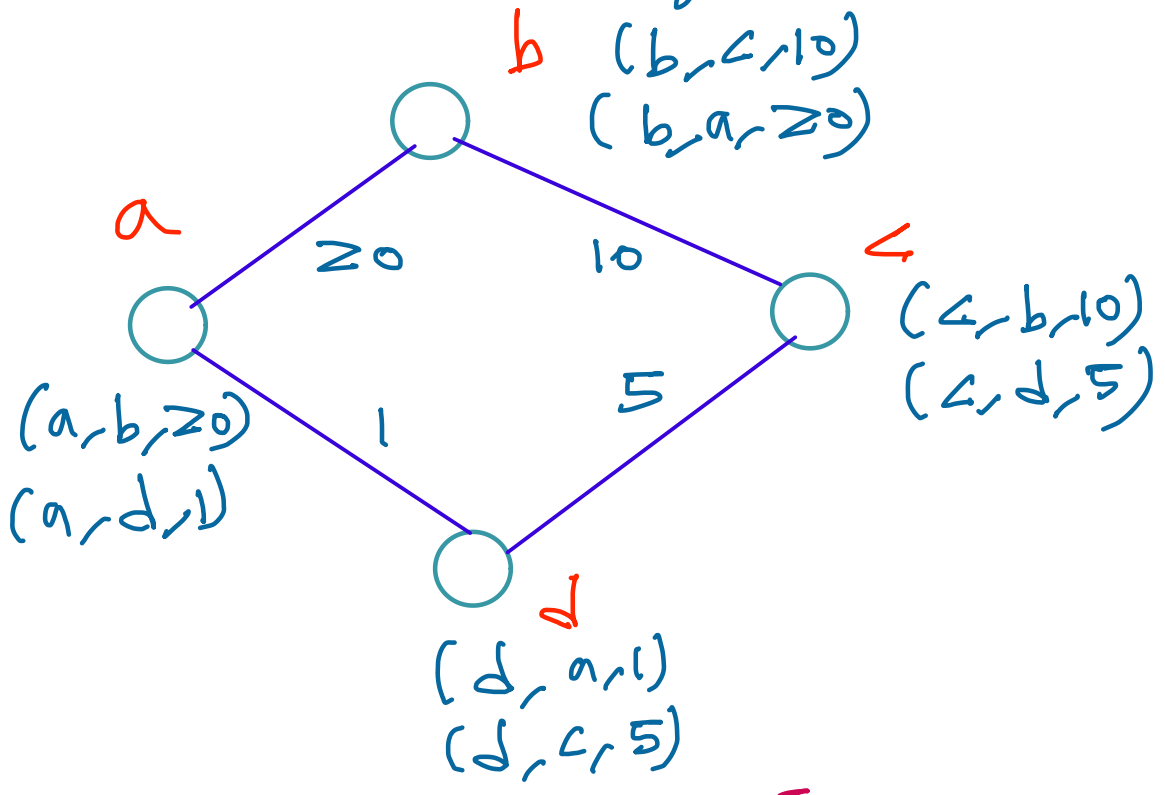
Fix Infinity (typically 16)

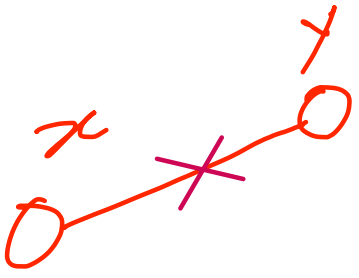
∞ = 1 + max possible path length

Constraints on the size of the N/W



Link State Routing :-

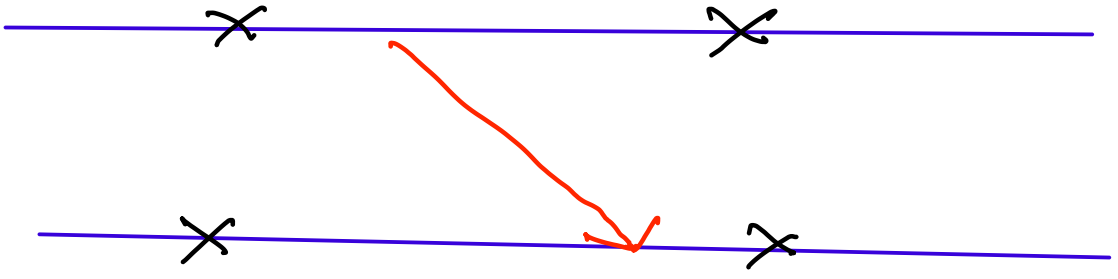




(x, y, down) 5 $t=5$

(x, y, 5) 6 $t=8$

} Add Seq No.



$\Longrightarrow$ Updates: flooded $\rightarrow$ Less chance of loss

d	h	c

Used by forwarding

filled by routing protocols (dist Vect, Link State)

(No forwarding here. Does not care how you will use the table)

⟹ Routing loops can cause a packet to be forwarded forever (upto Max TTL) in a graph.

Too many updates :-

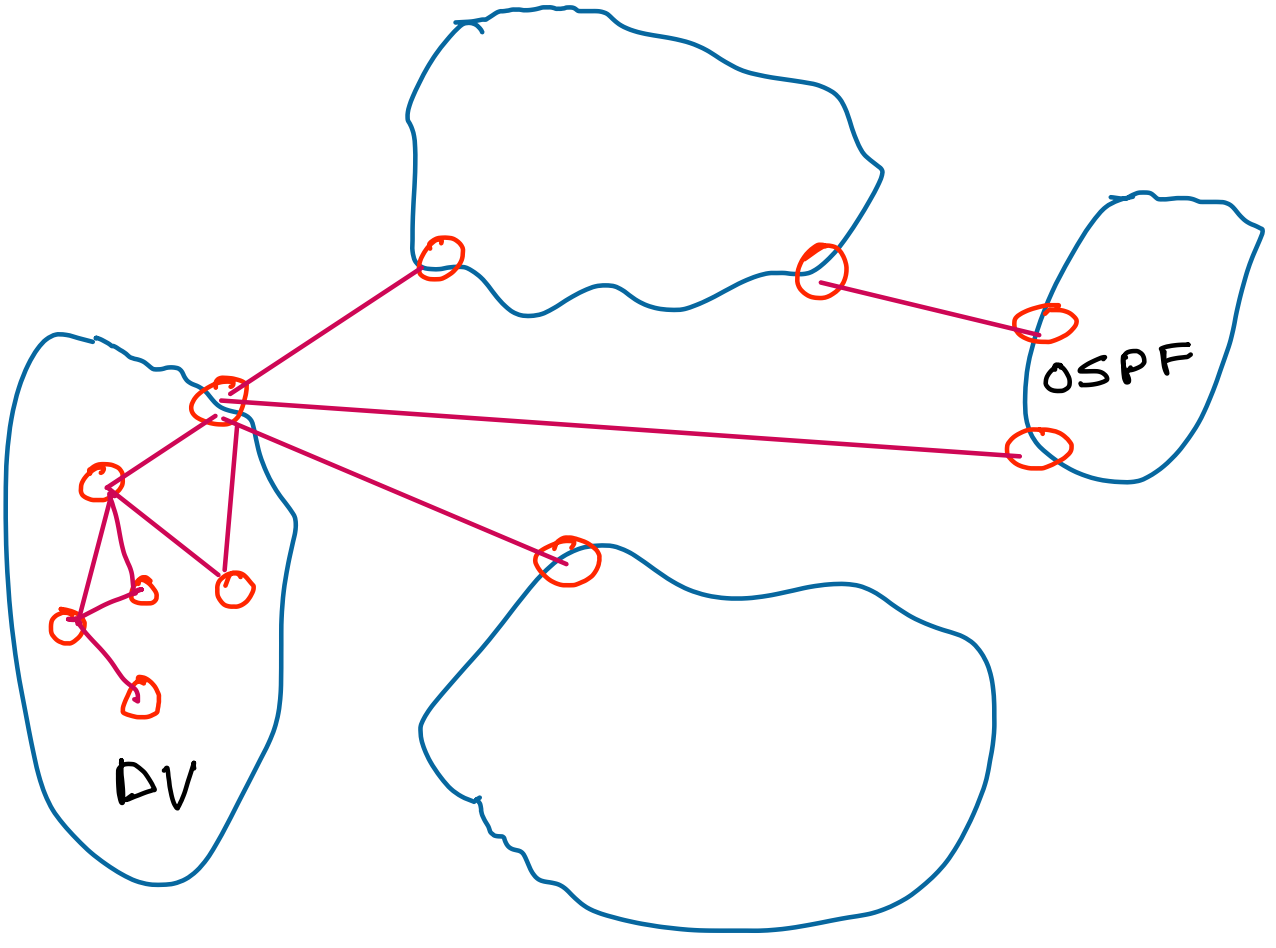
D.V

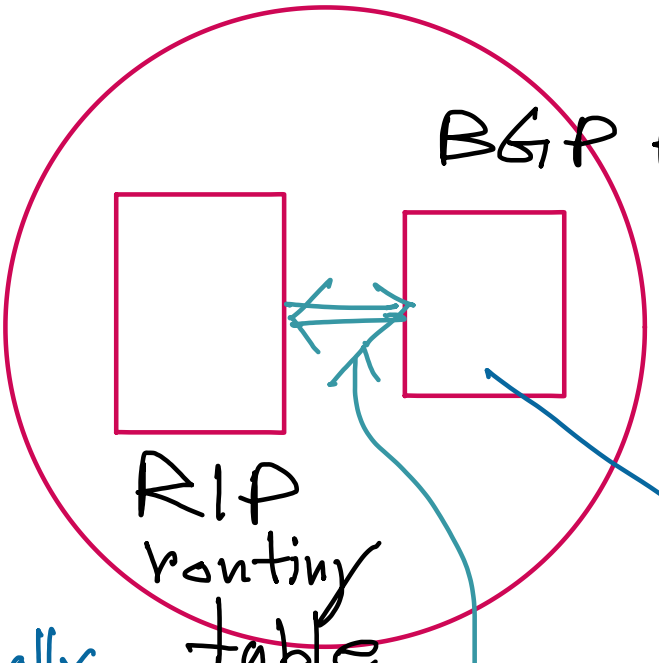
Slow Convergence → Message drop.

LSR

Too many messages

Internet Routing Architecture





Talking say RIP Internally

talking BGP btw^n AS's

Inject route for each other subject to policy

RIP!— In the update rule

if new route found

Cost → existing route Cost

do not replace

(So strictly < instead of ≤)

RIP

TCP/UDP

IP

Ethernet

RIP → Application Layer?

Network Layer?

⟹ typically N/W Layer

But by definition Application Layer

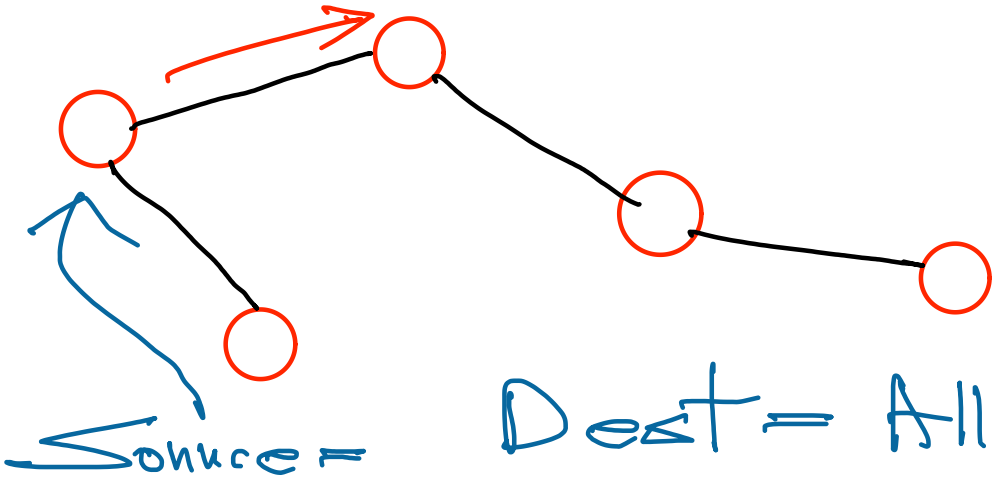
Route tag ⇒ From where is the Route Learned

All 1's → First Entry of ≥5 entries is going to be authentication

RIP Version 1 ⇒ No Subnet Mask
⇓
Classful Addressing

⇒ No update for a certain time (T_R) Remove. But then periodic update time (T_P) ⇒ $T_P << T_R$

TTL=1 → Get & reflood

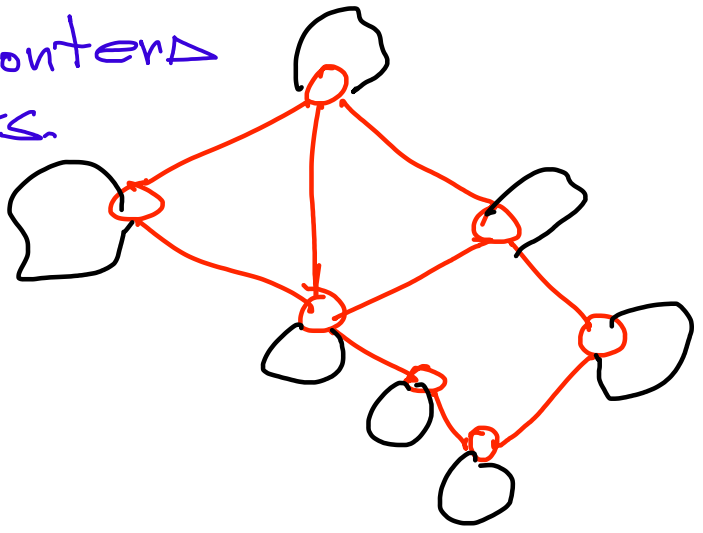


Source = Dest = All 1/ Neighbours

TTL=0 → OSPF
⇒ Don't Drop
⇒ Process and Drop

⇒ Option to ask neighbours for their info

Nodes = Routers not hosts.



ICMP

→ Required protocol with IP

→ An ICMP packet is sent if an IP packet is dropped/ Error detection or in a few cases, otherwise also

→ ICMP packet

IP header	ICMP header	Optional data

→ ICMP packet not sent for dropped ICMP packet

ICMP header:-

Type } Together define what error
Code }

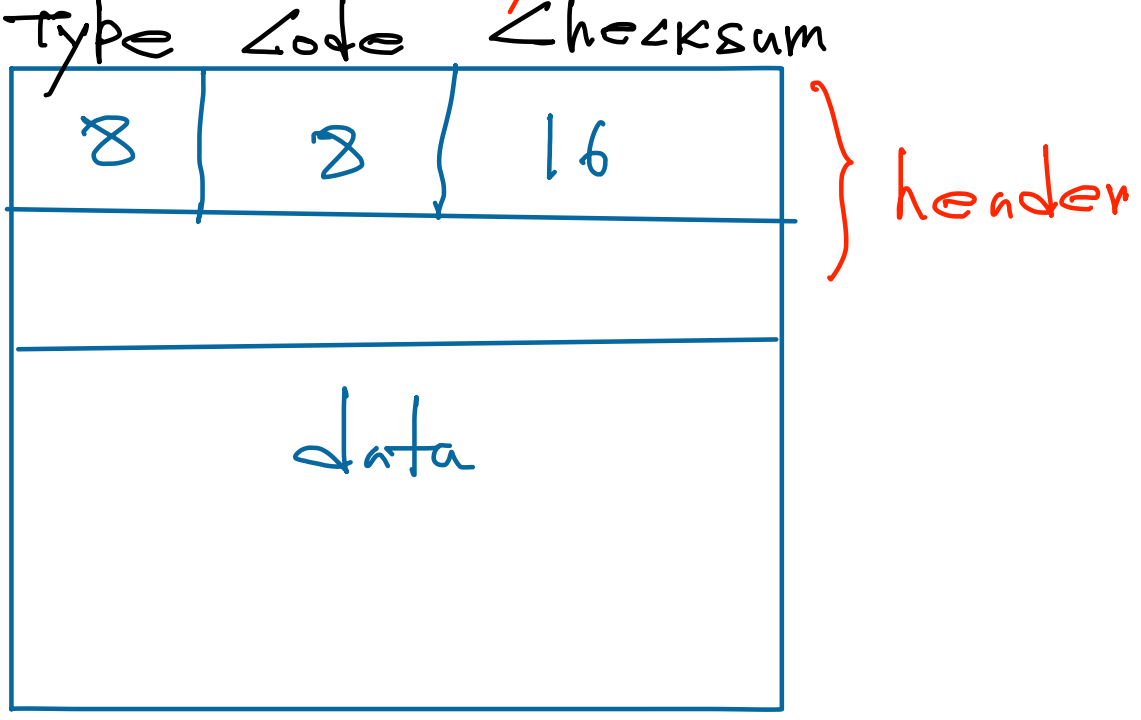
Type → 8-bit

Code → 8-bit

Checksum — 16 bit

+ 16 bits

Optional data — Vary



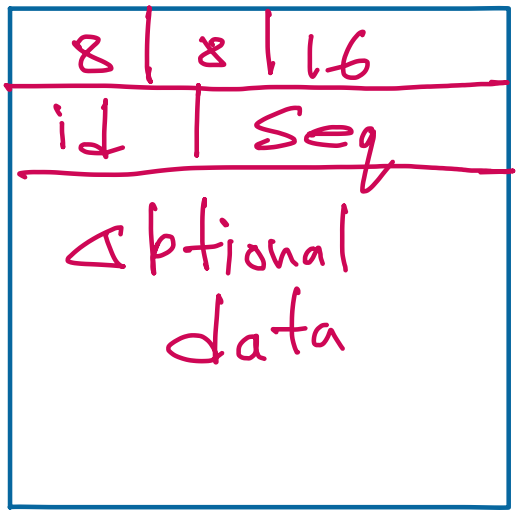
Type :-

Non Error ICMP

— Echo Request

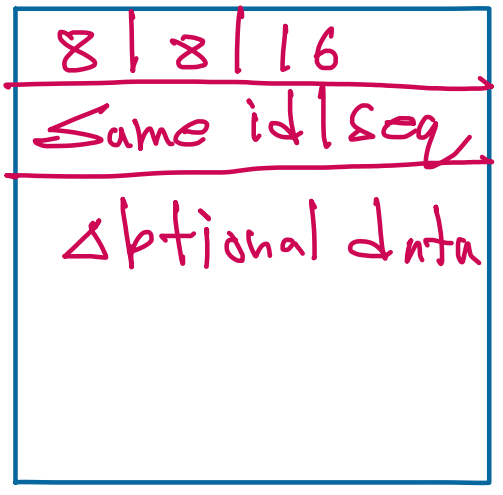
— Echo Reply

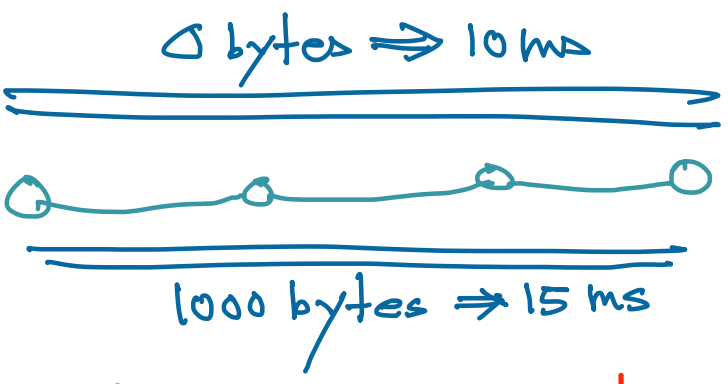
Echo Request



for matching Request with Reply

Echo Reply





Optional data
⇒ Measure Bandwidth

Error Notification ICMPs

Type

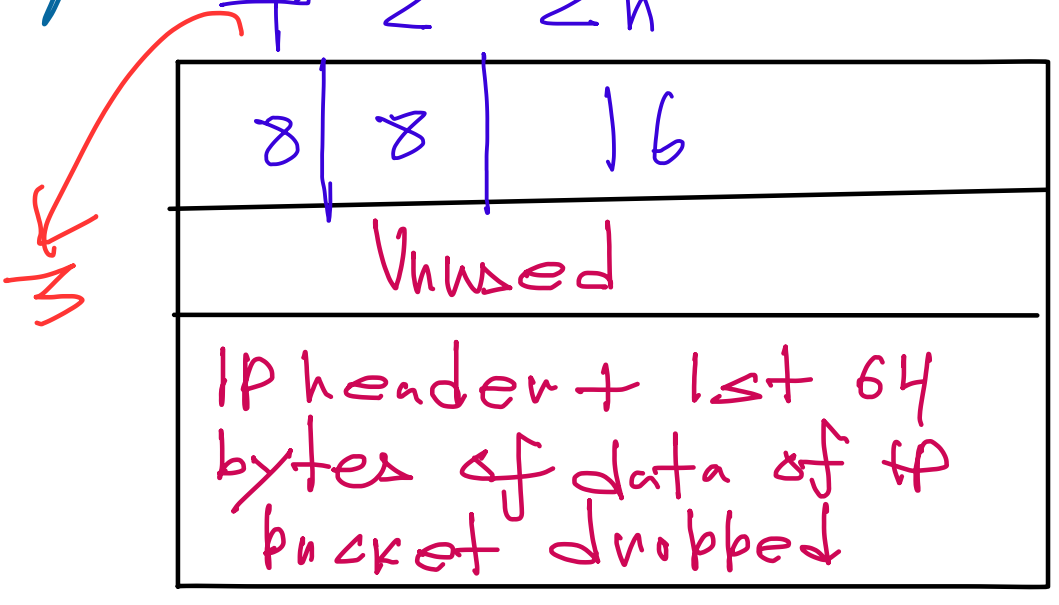
Time Exceeded → Sent when packet is dropped if TTL=0

Destination Unreachable

Code

N/W unreachable
Host "
Port "
Fragmentation needed & DF=1

→ Done by TCP



⇒ IP header identifies for which IP packet the ICMP is sent

⇒ 64 bytes should have the full header of the higher layer protocol above IP

NAT:-

Why has IPv4 address not run out?

1) Systematic allocation
2) IPv6
3) Private IP & NAT

↓

Will never be a source/dest IP fields of an IP packet internet outside the organization

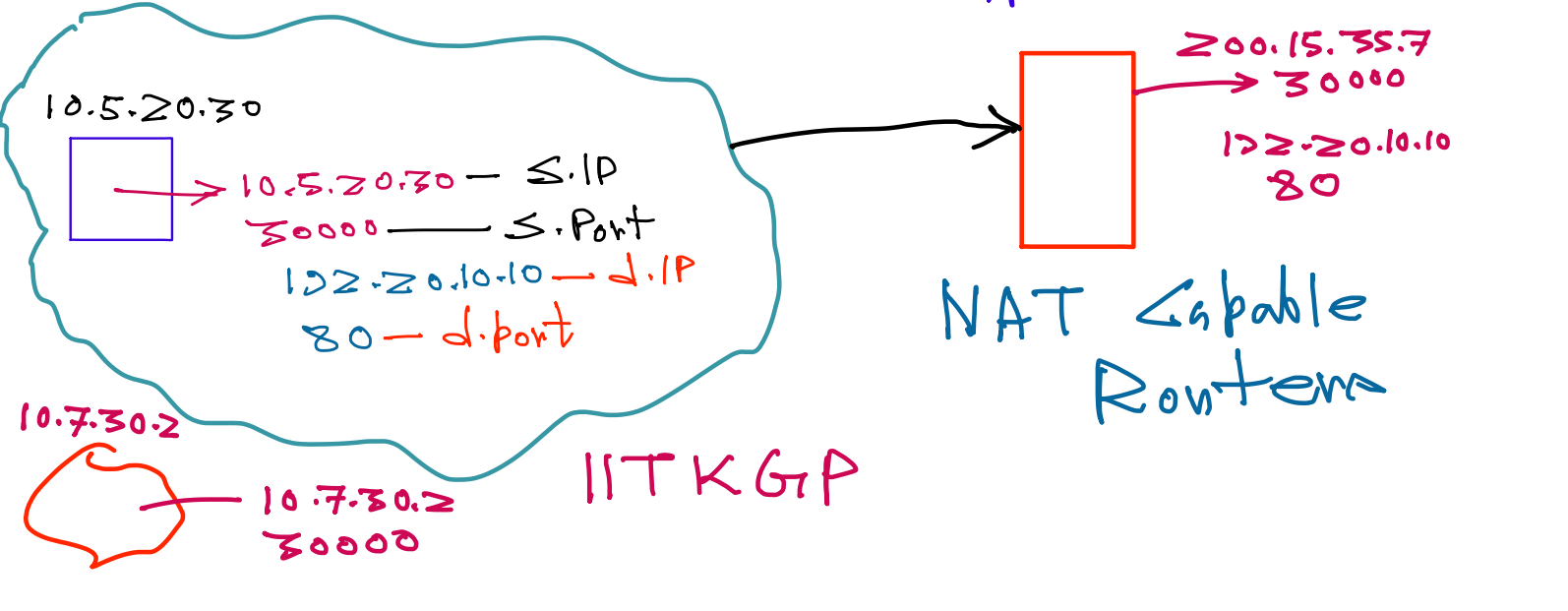


Table in Router

Int IP	Int Port	Ext IP	Ext port
10.5.20.30	50000	192.20.10.10	80
10.7.30.2	30000	192.20.10.10	80

Distinguish b/w

- 192.20.10.10
- 80
- 200.10.35.7
- 30000

Sol!

Have a pool of K public IPs. Assign one for each outgoing connect

→ Does not scale, too many public IPs needed

NAT!

So, use port also. NAPT

Int IP	Int Port	Ext IP	Ext port	NAT port
0.5.20.30	50000	192.20.10.10	80	40000
0.7.30.2	30000	192.20.10.10	80	41000

Assigned by NAT Device

→ If all have same ip the receiver will blacklist it