ROUTING AND VPN

RECAP

routing algorithms (shortest path)

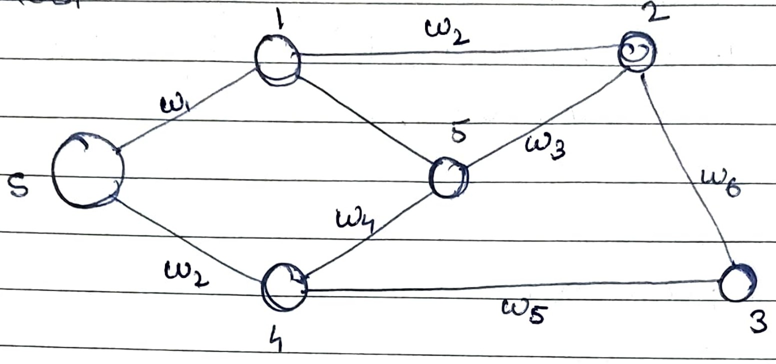
dijkstra - greedy

bellman-ford } dynamic programming

flgodyd-warshall

unicast - routing

broadcast

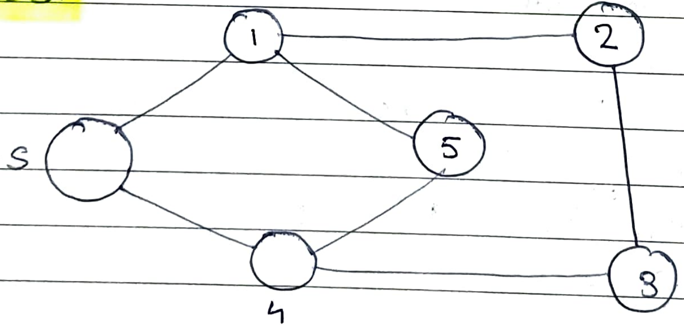


min (s,2)

min. $\sum_{i} c(s,i)$

MST → Kruskal's
→ prim's

multicast



s → {1,3,5}

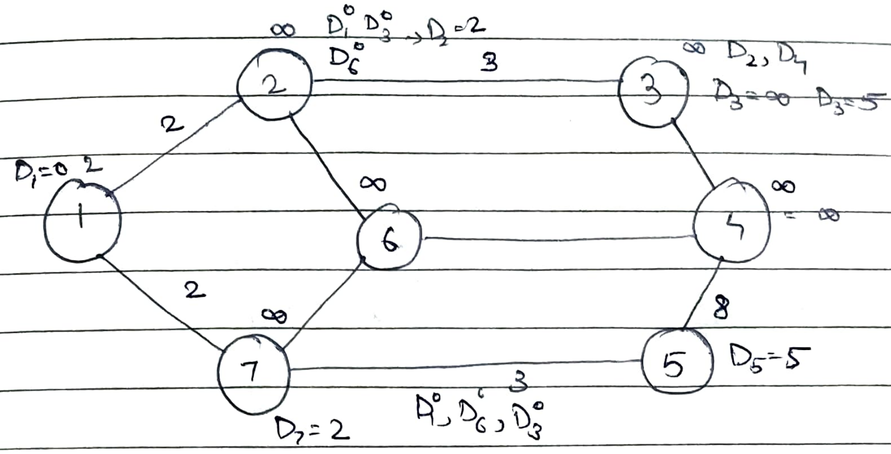
M st M spans {1,3,5}

Cost (M) = $\sum_{e \in M} w_e$ is minimized.

min cost Steiner tree → NP-complete

PIM

ARPANET (1969)



BELLMAN-FORD

$$\forall h\ \ D_1^h = 0,\qquad D_i^0 = \infty \quad \forall i$$

$$D_i^h = \min_{j\in N(i)} \left[d_{ij} + D_j^{h-1}\right] \qquad i \neq 1$$

$$\underbrace{d_{i3}\quad d_{i5}\quad d_{i1}}_{?}$$

what if each node synchronously start.

this is challenging

if node == 1
$D_1^h = 0 \quad \forall h$

if node == i
$D_i^0 = \infty$

- - - - - - - - - - - - - - - - - - - -

$$D_i^h = \underbrace{\min_{j\in N(i)} d_{ij} + D_j^{h-1}}$$

the algorithm will also converge

$$D_i^{t+1} = \min_{j\in N(i)} d_{ij} + D_j^{t-1}$$

825 ms will broadcast D_i's to its neighboors.

DYNAMIC ROUTING

distance vector routing	link state routing
routers should know only its neighboors	routers should know whole network.
(you keeps only dist. to neighbours)	(you keep whole network and all link states & delays)
bellman-ford (slower)	dijkstra (faster)
(if some link goes dow, knowledge passing is slow)	(more BW as more traffic is generated)
less BW & less traffic	

Static routing

typically routing is fixed
(smaller organizations)

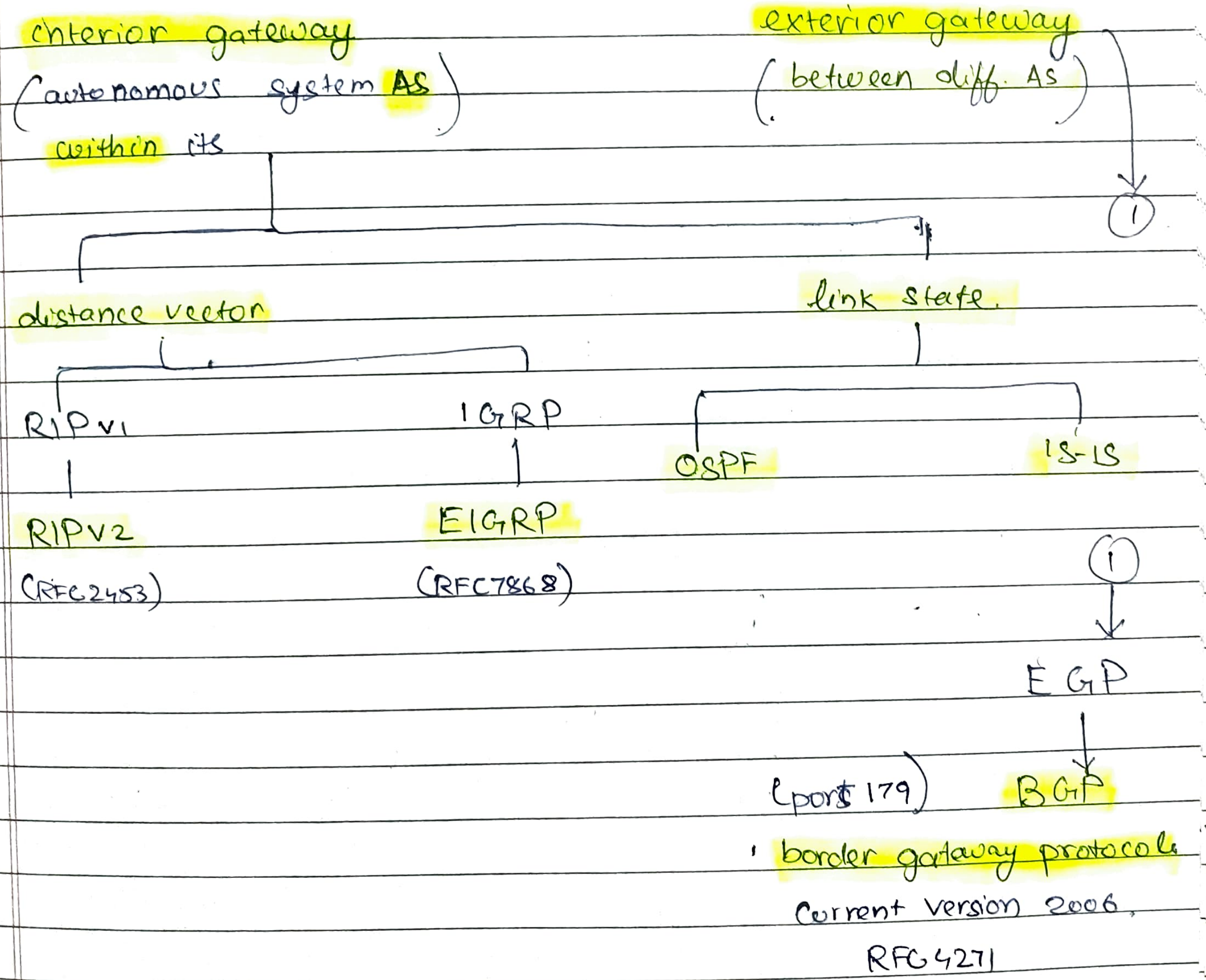
ARPANET

distance vector routing (1969)

RIP (v1) ⟶ RIP(v2) (1998) → RFC 2453 request for comments.

hops allowed to be 15

DYNAMIC ROUTING



cnterior gateway (autonomous system AS within its)

exterior gateway (between diff. AS)

distance vector

link state.

RIPv1

RIPv2 (RFC2453)

IGRP

EIGRP (RFC7868)

OSPF

IS-IS

1

EGP

BGP

border gateway protocols (port 179)

current version 2006,

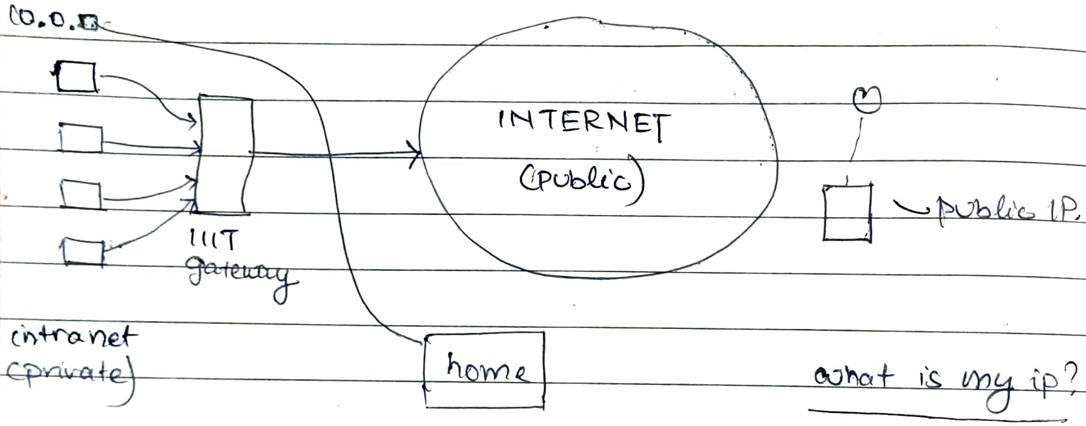
RFC4271

VPN

What is VPN?

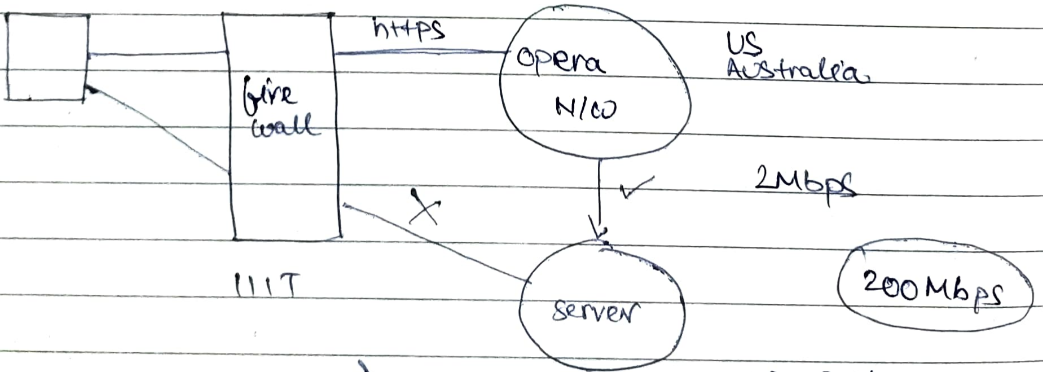
- virtual private network
to access the mess portal.
- Connect to corporate network.
- to access computing resources within IIIT when outside campus.

secure communication.



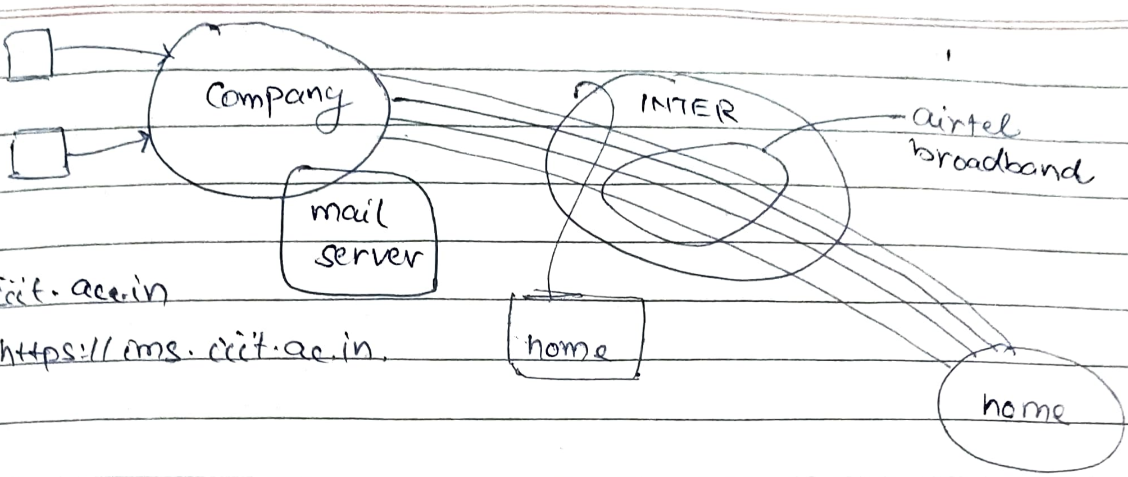
what is my ip?

opera VPN or some VPN clients to browse



whatsApp call (port)

10-12 Mbps



ciit.ac.in

https://ms.ciit.ac.in.

purpose of VPN

IPv4

provide data confidentiality
data integrity

10.x.x.x
256 256 256
192.x.x.x

authentication
(use hash fns)

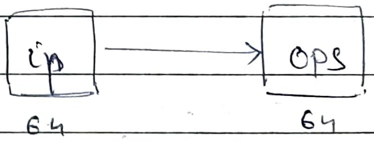
encryption

① (public key) assymmetric key
② symmetric key

SHA SHA2
MD5
RIPEMD

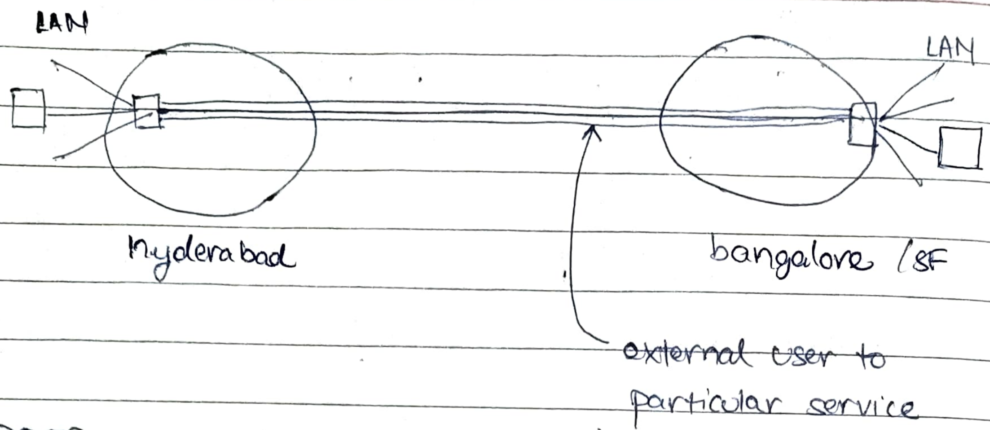
DES, 3DES, AES, blowfish.

RSA, Elgamael
EC



VPN

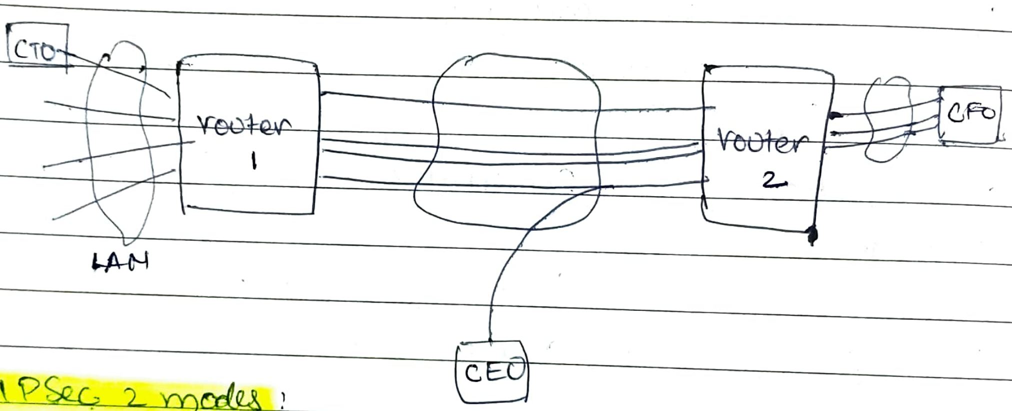
- user to service (SSL)
- user to LAN
- across two LAN.



PPTP - windows 95 (RFC2637)

L2TP - RFC 2661, 3931

IPSec - used for 2 LANs. RFC4301



IPSec 2 modes:

- transport — device-device
- tunnel — router-router, or device - router

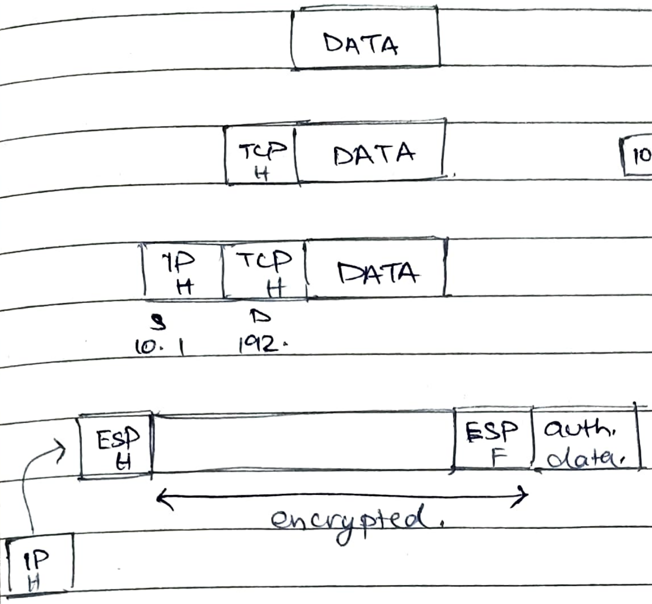
ENC → ESP RFC4303 IKE - RFC 4306

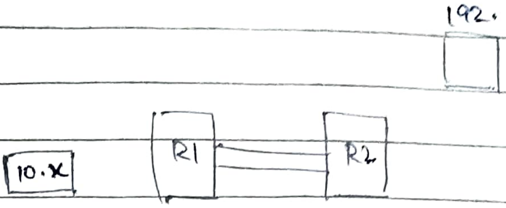
AH → AH RFC4302

ESP → encrypt the data (authentication possible) → nullencryption

AH → authenticate the data

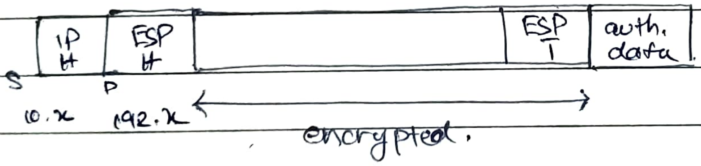
IPSec tunnel in ESP





~~IPsec in transport mode with ESP~~

IPSec in transport mode with ESP



VPN-A	VPN-B
3DES-CBC	AES
HMAC-SHA1	AES-XCBC
1024 bit	2048-bit

IKE (diffie hellman)

RFC 4869 what all cryptographic operation supported.