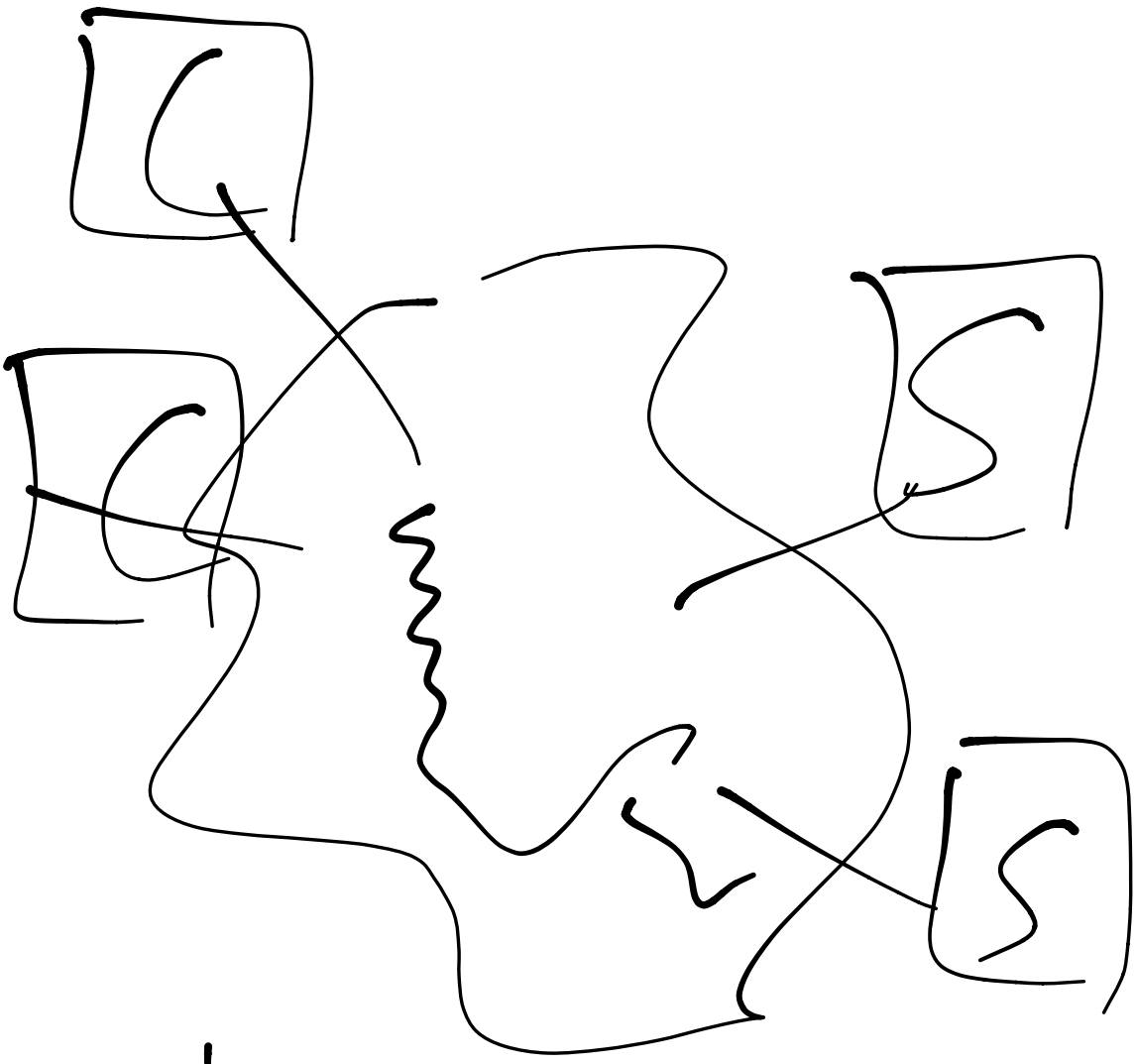
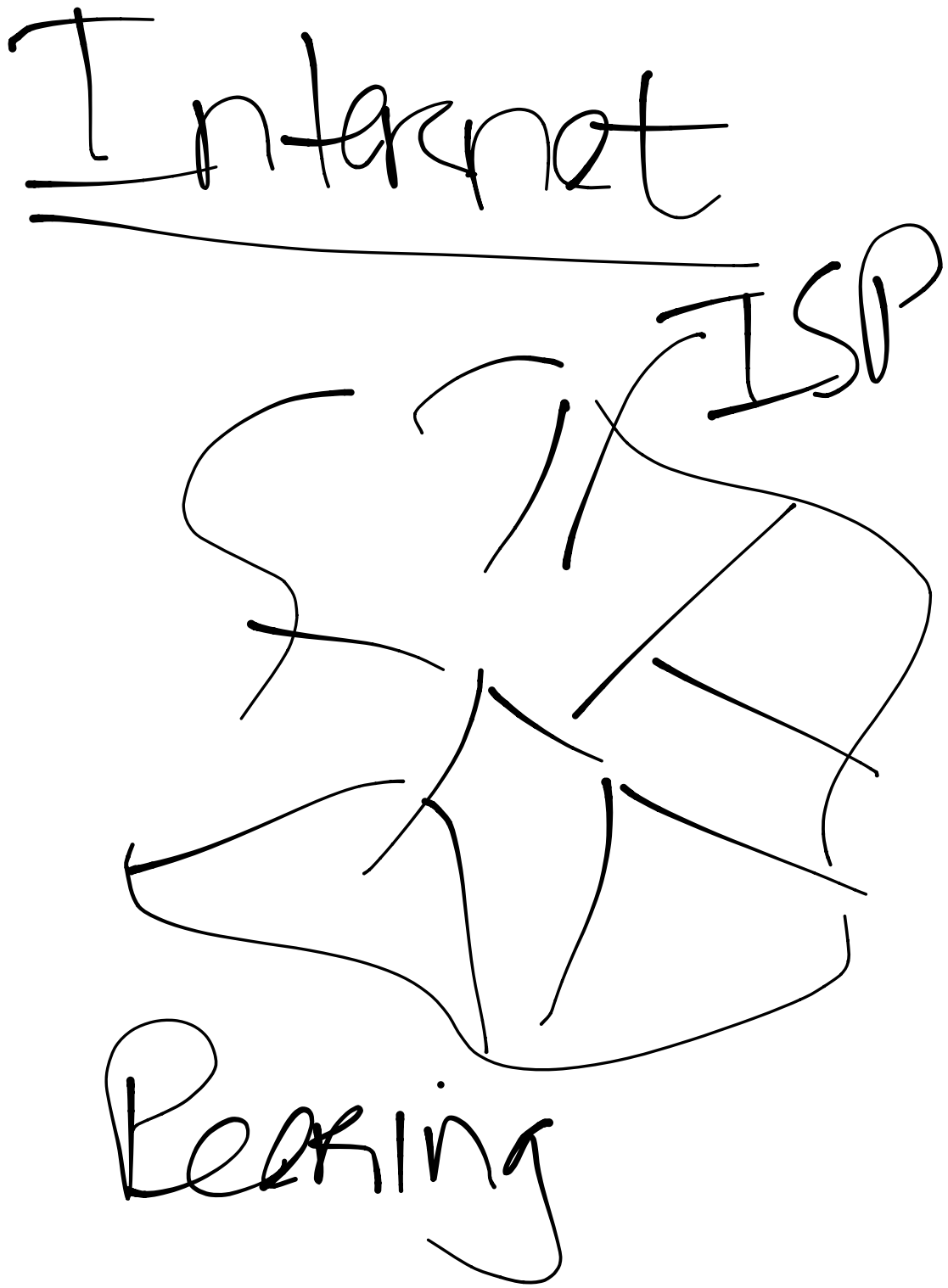
6.858

Network Security



Liveness


Internet
ISP
Peering

TCP dns

IP

BGP

telnet/ssh

ftp IETF

Internet today

Core: Liveness

Security:
end nodes

Good design

telnet ethernet

No crypto

attacker.

modify data
inject data
listen steal pw
MITM

Rlogin

don't send pw

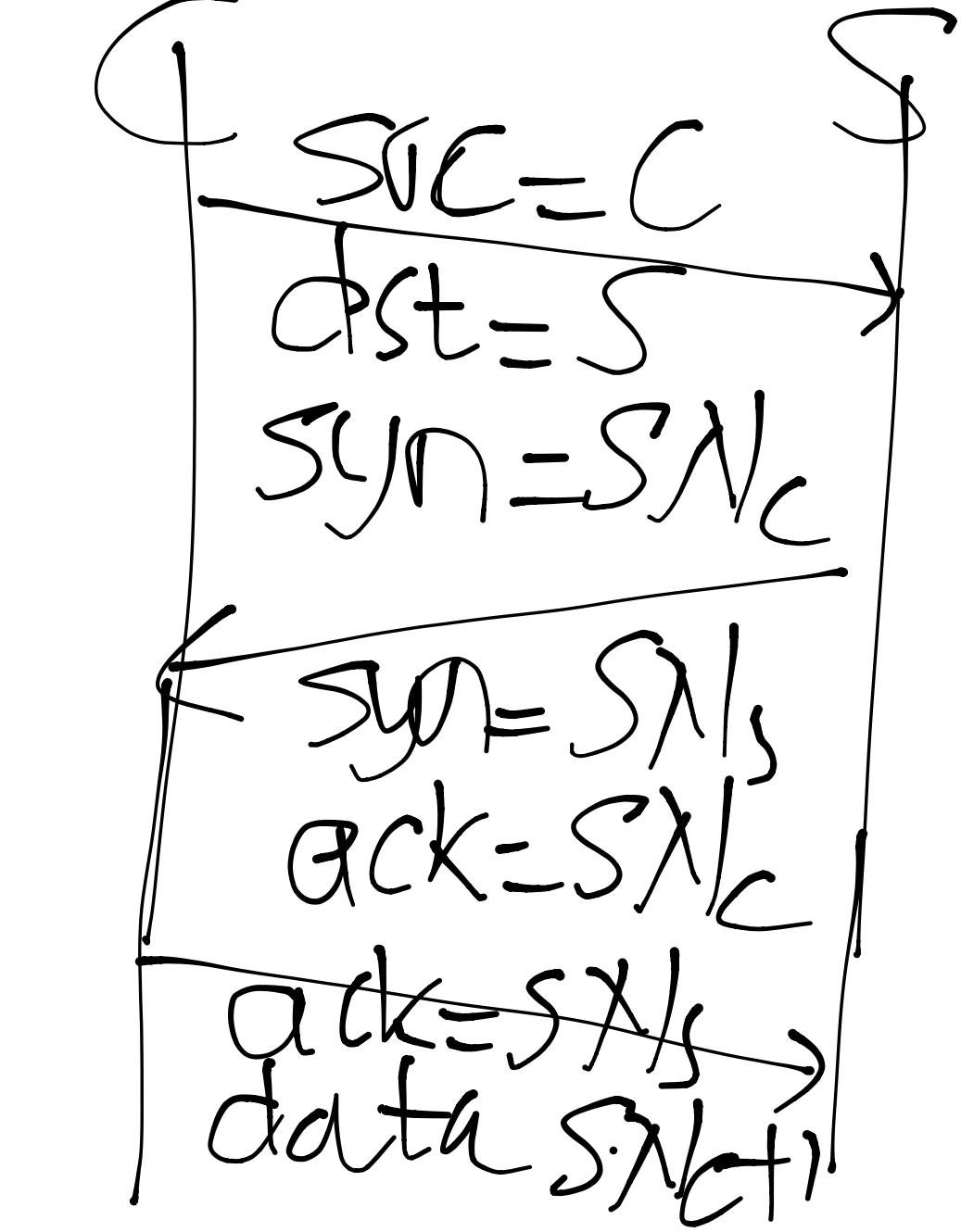
trusted host file

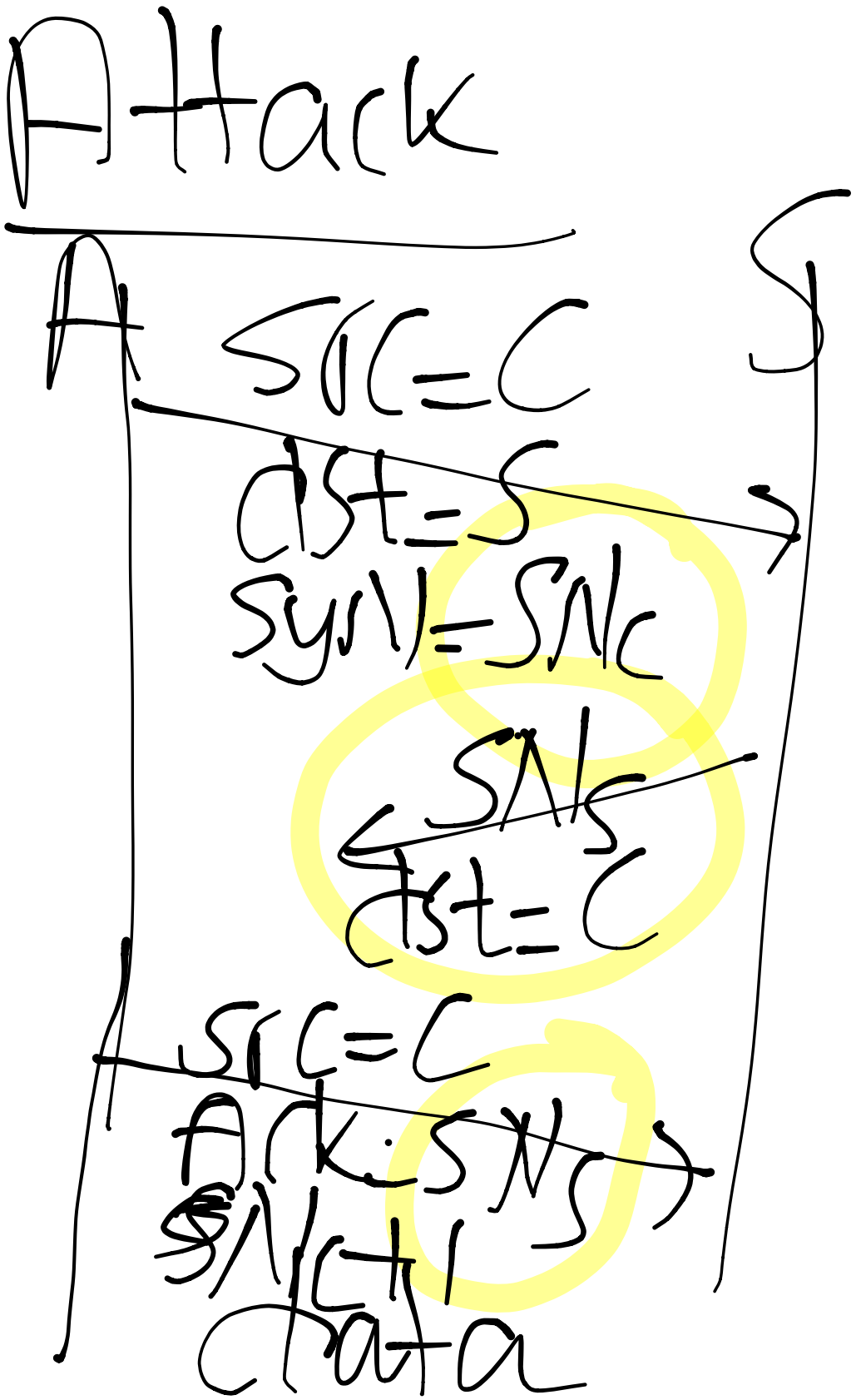
$\Downarrow$

hard to fake

src address.

TCP handshake




Attack
A
S
SYN C=C
dst=S
syn1=SN C
SN S
dst=C
SYN C=C
ACK SN S
SN C+1
Data

Guess SNs

ISN

+128 per sec

+64 per new conn.

⟹ make regular +64

Seq # ⇒ Attack

1) forge src address

2) DoS BGP

3) Hijack 2016

Mitigations

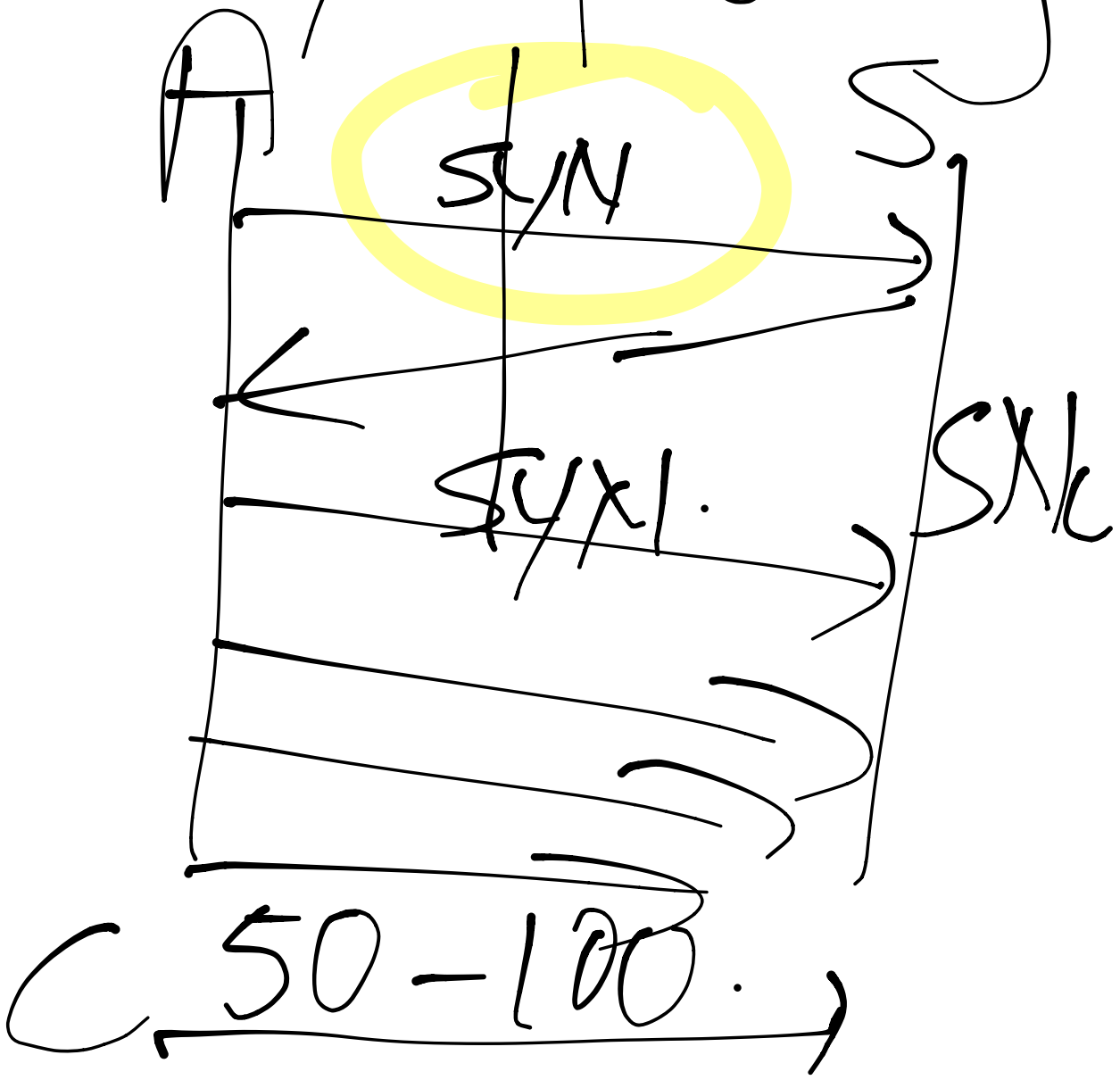
- E2E crypto-based authent. (SSL/SSH)
- ISP & Her pkts (bt multihoming
- firewalls

Harden tcp

- Random seq?
- Random ina?
  (src, dst)
- SNS = ISN(old) + SHA1(src, dst, secret)
  X No extra state

Liveness/DoS

Syn flooding

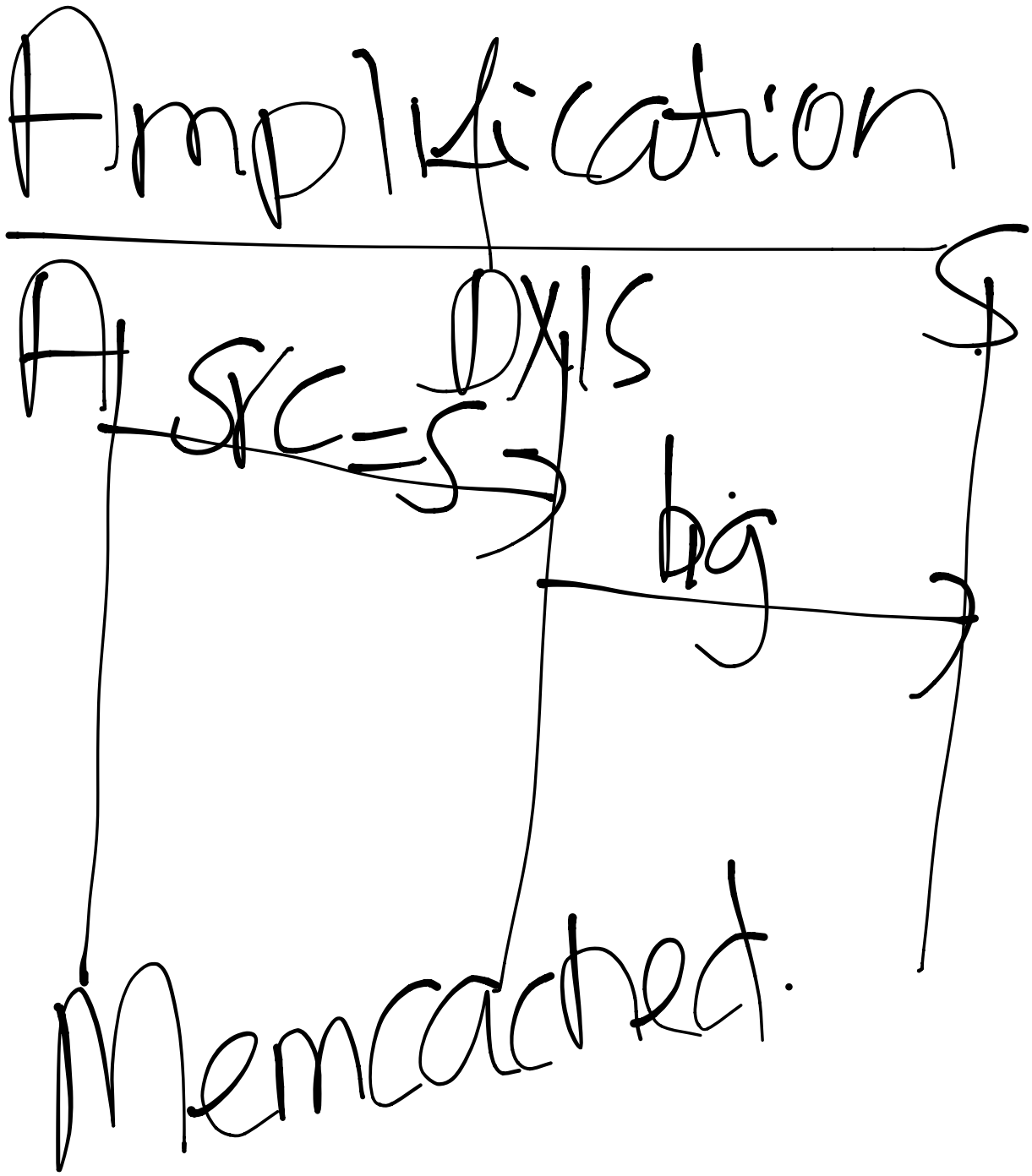


SYN cookies

$SN_S = SN_C + (ts \,||\, SHA1(src, dst, secret, ts))$.

$\rightarrow SN_C + 1$

SN_S

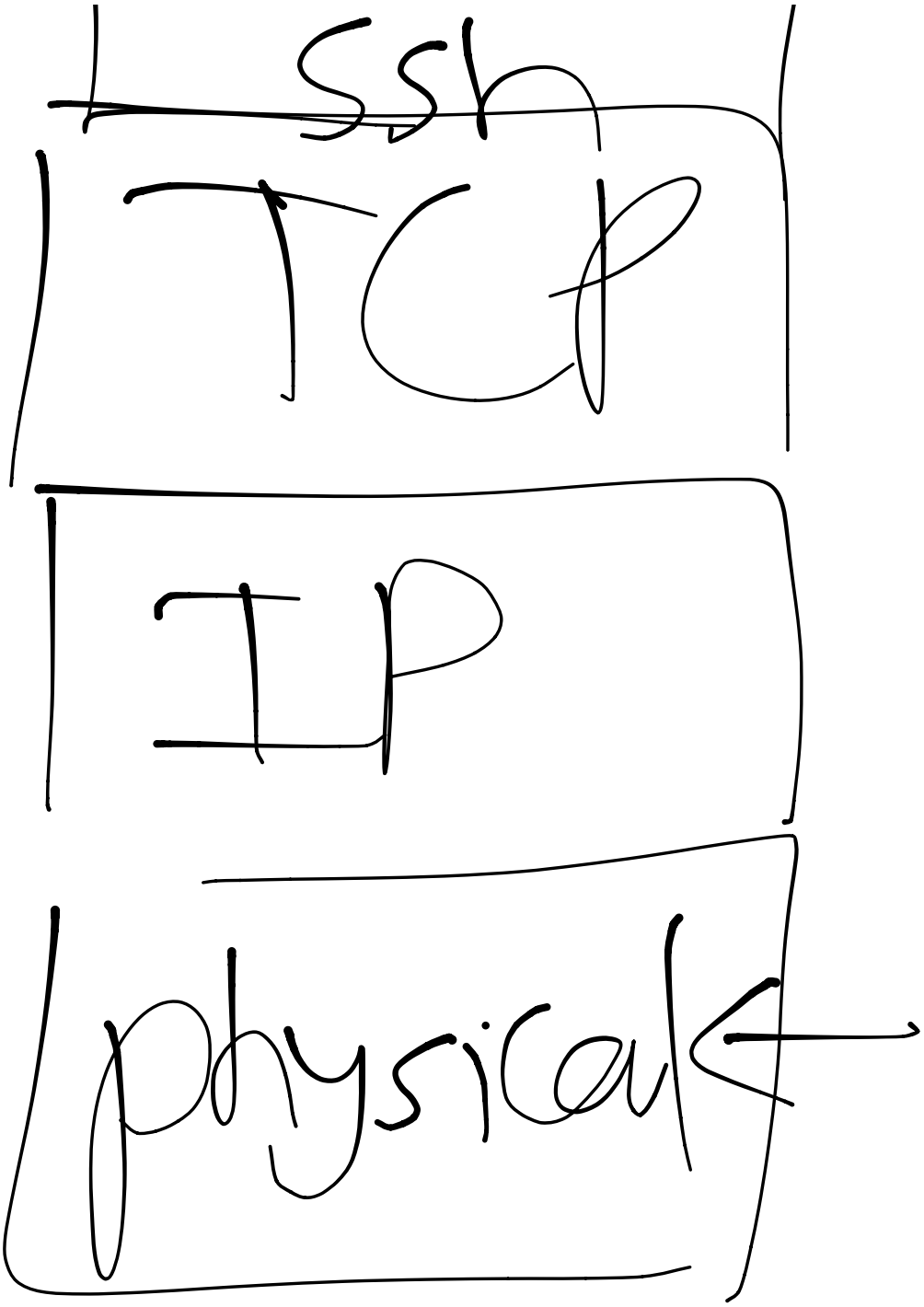

Application
A
DNS
S
src=5
bg
Memcached.

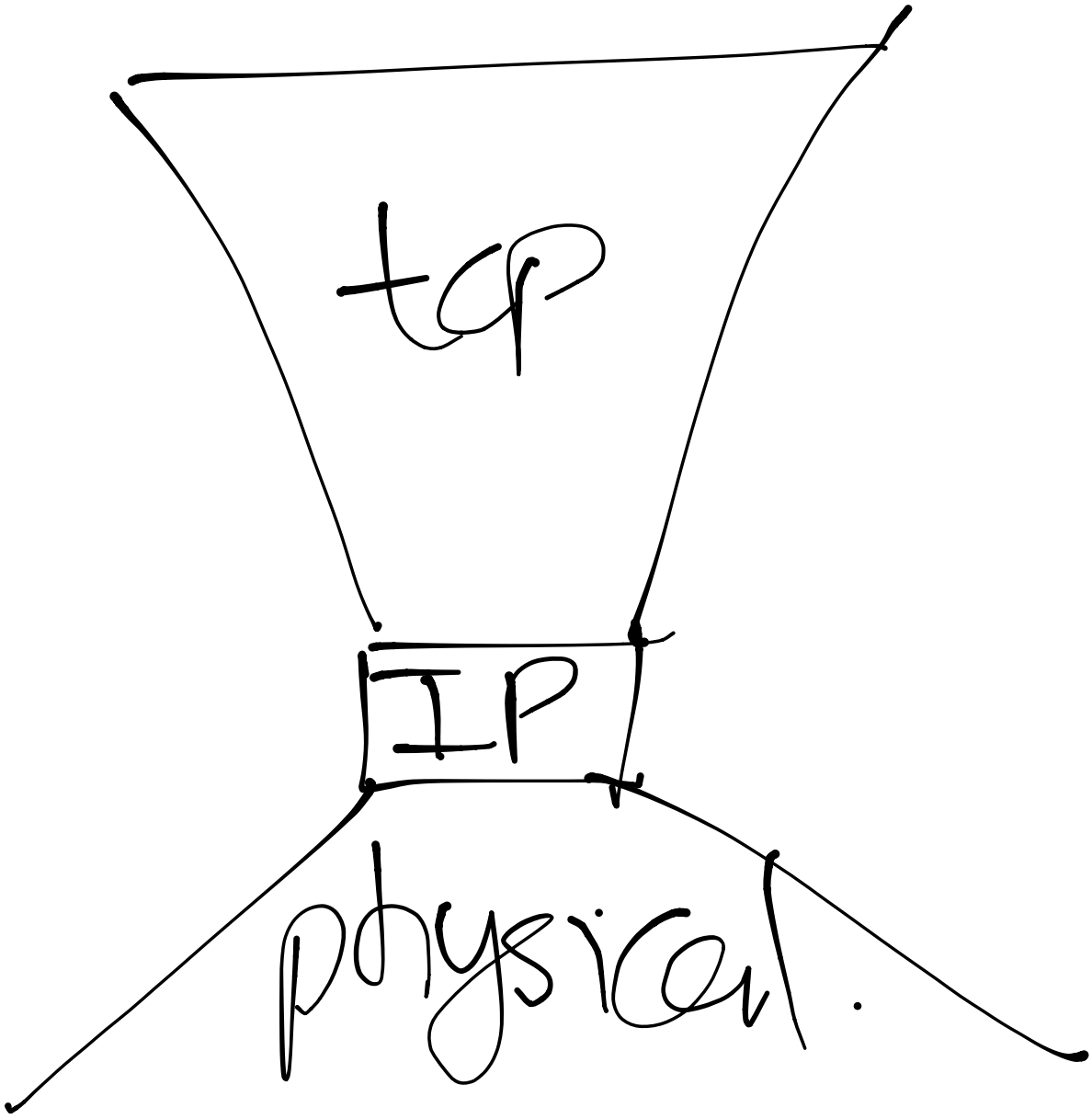
Routing protocols.

- DHCP (ARP)
- BGP (RIP)
  - open net
  - SBGP, ...
  - MANRS

Summary

Openet Core: liveness Pas Higher-level SSL/TLS


ssh
TCP
IP
physical


tcp
IP
physical