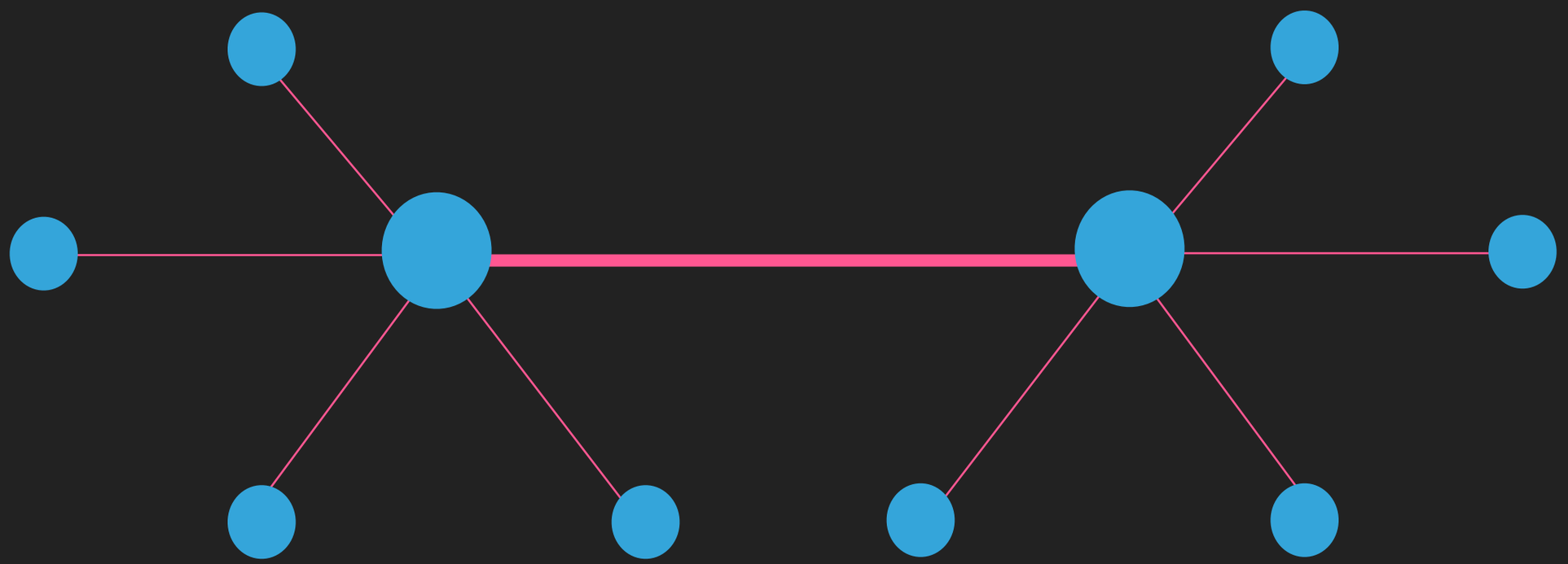
THE INTERNET AND SECURITY

N ANAND

WHAT IS INTERNET?

- Interconnected Network of Networks

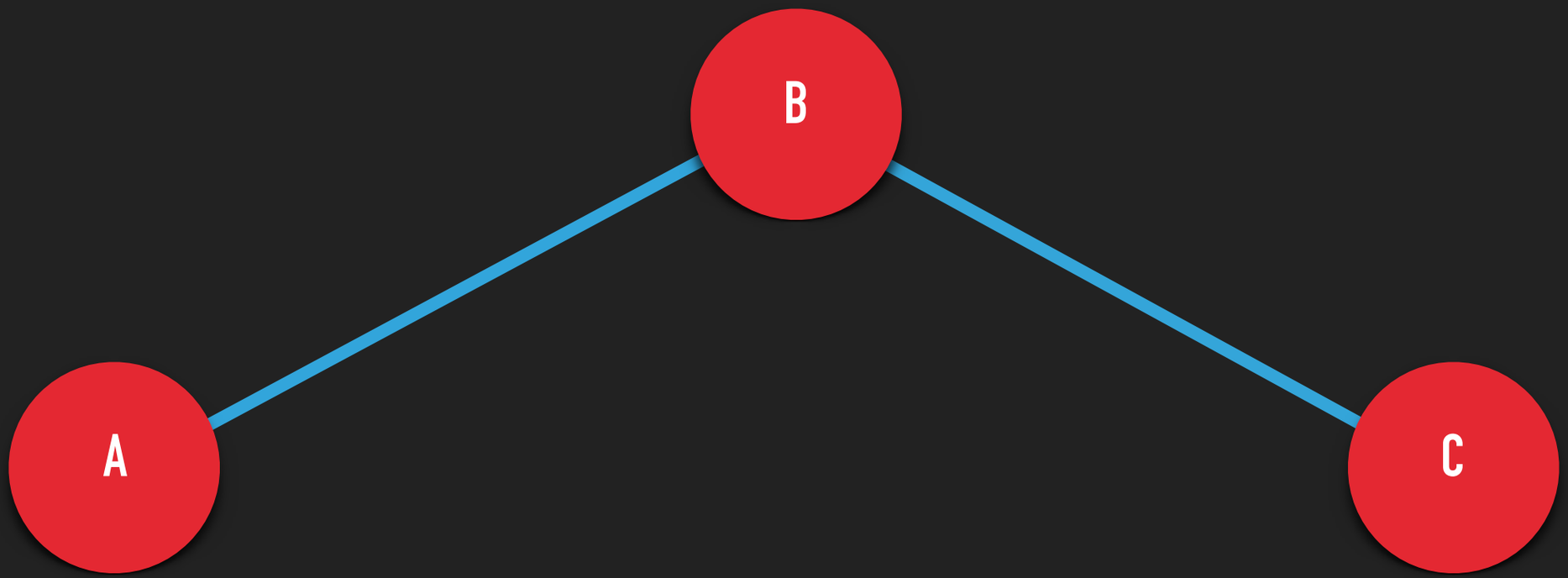


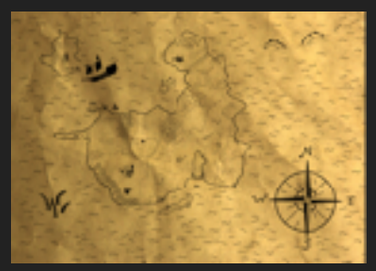
LET'S GO BACK IN TIME.! (1960 –70)

- Packet Switching - core of the Internet
- A move from
  - Circuit Switching
  - Message Switching

SWITCHING TECHNIQUES – CIRCUIT SWITCHING

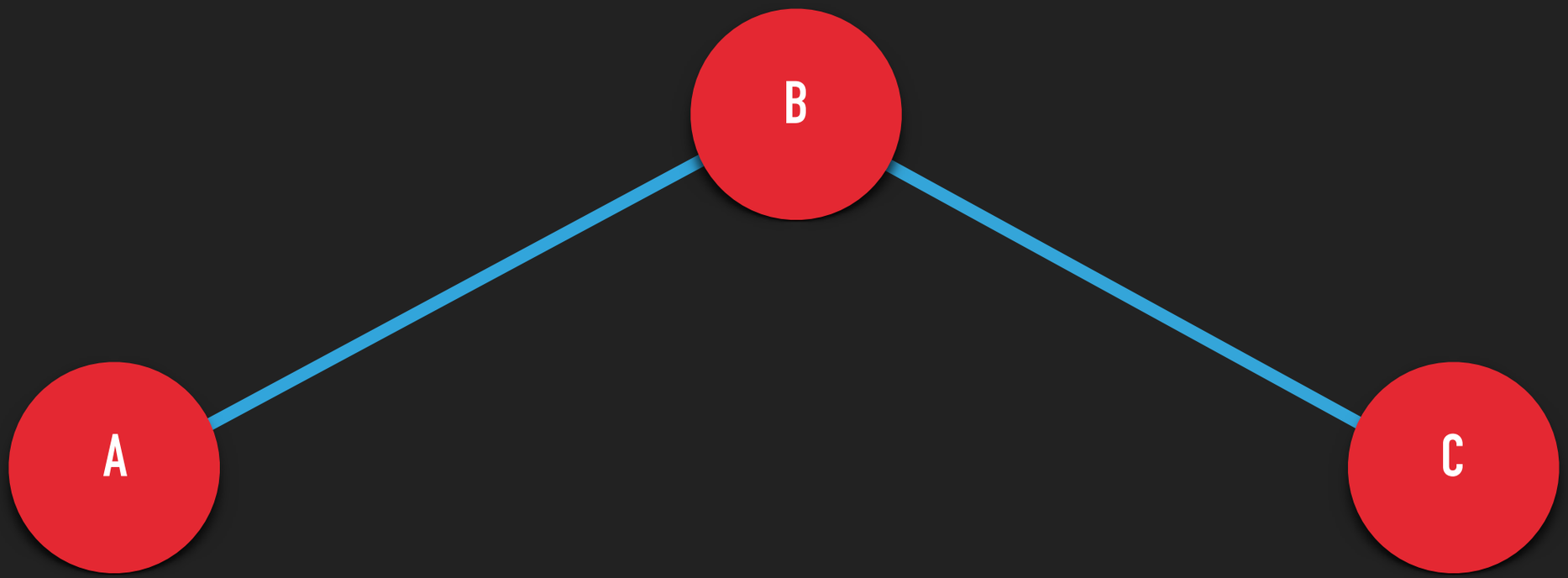
Wait for the circuit to be established!

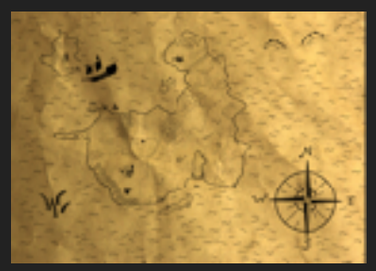




SWITCHING TECHNIQUES – MESSAGE SWITCHING

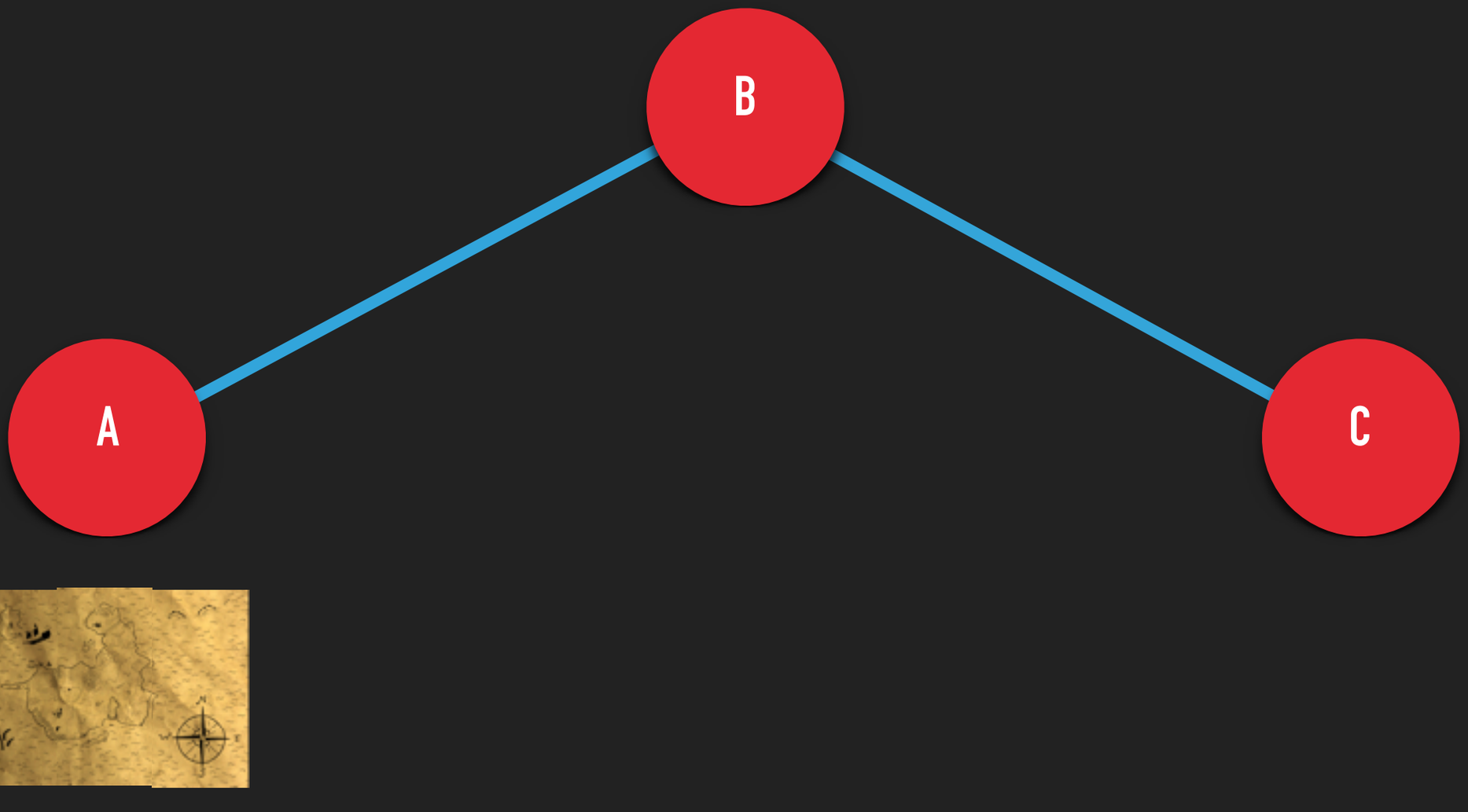
Message buffered at intermediate nodes





SWITCHING TECHNIQUES – PACKET SWITCHING

Message split into smaller packets!



ARPANET – ADVANCED RESEARCH PROJECTS AGENCY NETWORK

- First packet switched Wide Area Network
- ‘lo’ sent at 10:30 pm on October 29, 1969
- TCP/ IP development began.
- Eventually more computers were connected
- ARPANET was decommissioned on 28 February 1990

PROTOCOL

- Defines rules of Communication

A B

Hello.!? Over

Hello.!! Over

How are You? Over

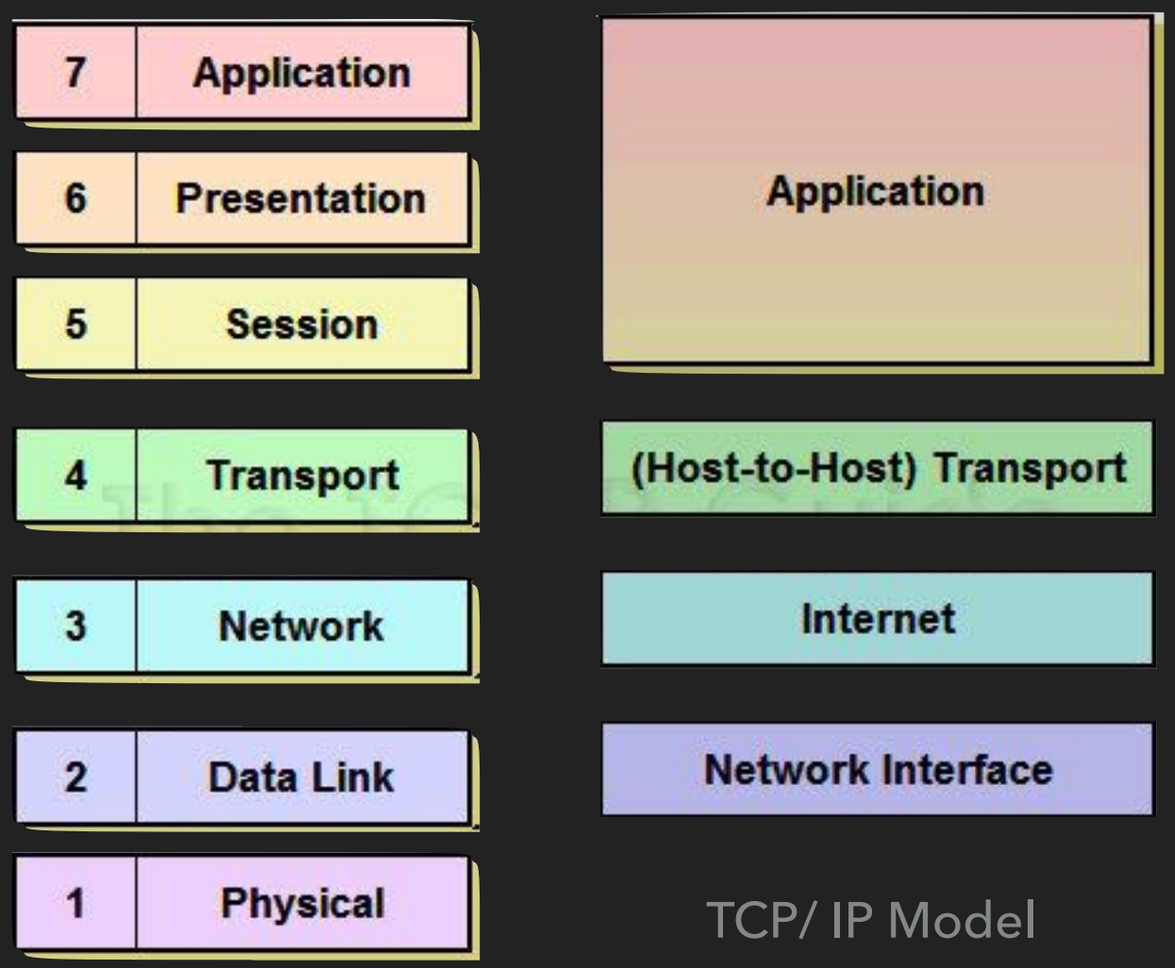
Fine.!! Over

Over! Over

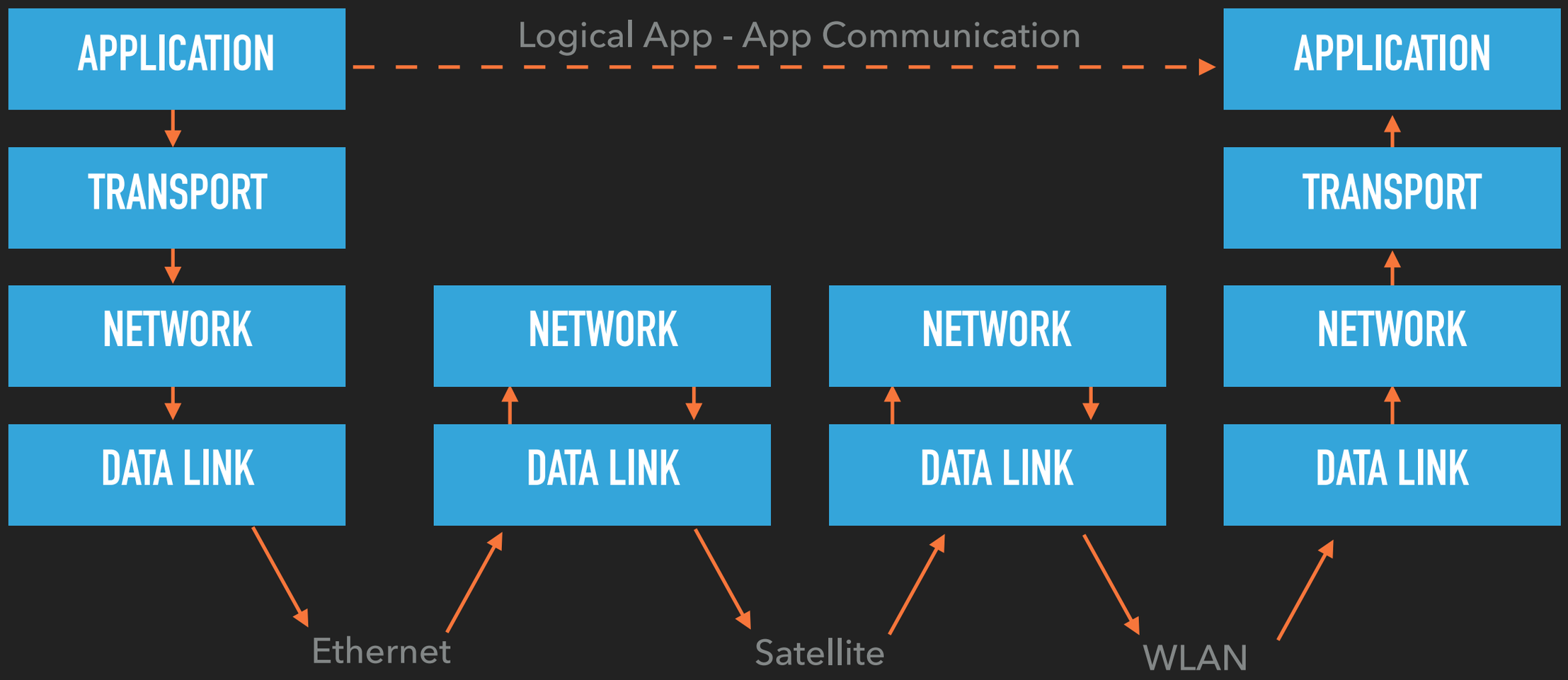
Over! Over

WHAT MAKES INTERNET?

- Layering - Protocol Stack

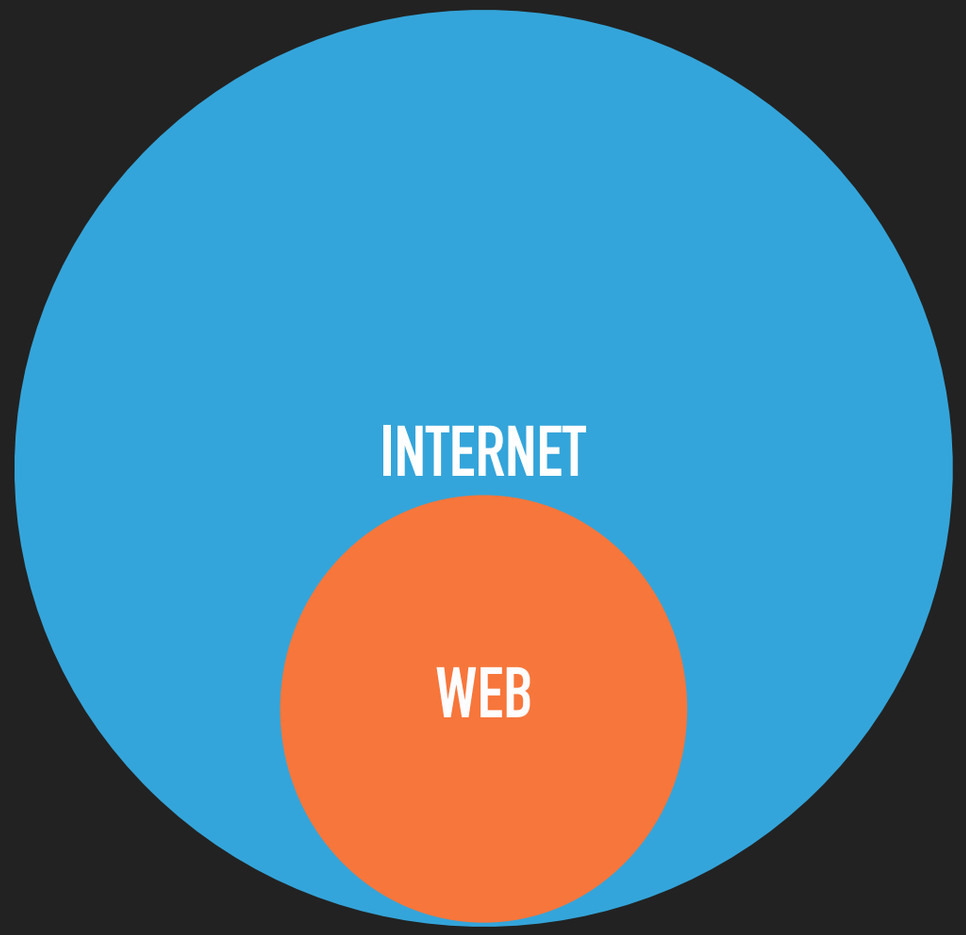


DATA FLOW


APPLICATION
Logical App - App Communication
APPLICATION
TRANSPORT
TRANSPORT
NETWORK
NETWORK
NETWORK
NETWORK
DATA LINK
DATA LINK
DATA LINK
DATA LINK
Ethernet
Satellite
WLAN

APPLICATION LAYER

- Internet vs Web?
- HTTP, SMTP, ICMP, DNS
- Unique ID: (IP, Port)



APPLICATION LAYER – CTND

- IP address works until Network layer of destination
- Above that, Port uniquely identifies the application
- Socket vs Port

TRANSPORT LAYER

- Takes care of host to host communication
- Reliability
- Stream / Datagram Transmission
- Flow Control
- Congestion control
- Multiplexing

TRANSMISSION CONTROL PROTOCOL (TCP)

- Connection Oriented
- Reliable
- Stream

Client

s = socket()

s.connect((ip, port))

s.send() / s.recv()

s.close()

Server

s = socket()

s.bind((ip, port))

s.listen(x)

y = s.accept()

y.send() / y.recv()

y.close()

s.close()

USER DATAGRAM PROTOCOL (UDP)

- connection less
- Unreliable
- Doesn’t ensure order

Server

s = socket()

s.bind((ip, port))

y.sendto() / y.recvfrom()

y.close()

s.close()

Client

s = socket()

s.sendto() / s.recvfrom()

s.close()

NETWORK LAYER

- Unique Host addressing
- Routing and Forwarding messages
- Fragmentation / Reassembly

IPv4 - 32 bit address - 2**32 = 4,294,967,296

IPv6 - 128 bit address - 2**128 = 3.40 * 10^38

ROUTING

- Several routing algorithms
- Routing table maintained at Network layer
- Centralized / decentralized

DATA LINK LAYER

- Responsible to get the packet across to the next node over the link
- Framing data
- Medium Access Control
- Unique hard-wired physical address

PHYSICAL LAYER

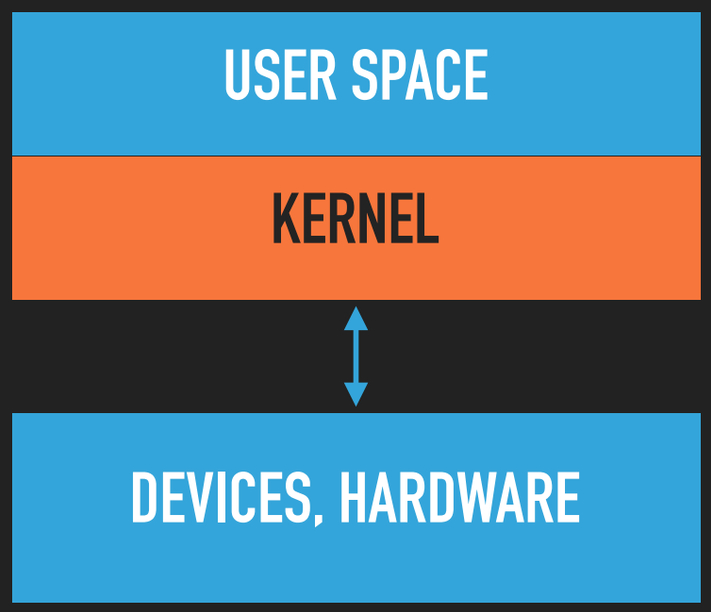
- Ethernet cable
- WiFi
- Satellite Link
- Fiber Optic Cable

SECURITY

- Malware
- Denial of Service Attacks
- Botnets
- Trojans
- Phishing
- Protocol and Application vulnerability

MALWARE

- Any software that functions with a malicious intent.
- Rootkits are the worst of kind
- They could potentially lodge the malware into kernel space and in some cases even at the firmware level



IDENTIFICATION AND REMOVAL – ROOTKITS

- Signature Detection
- Memory Dump
- OS reinstall
- Change of Hardware

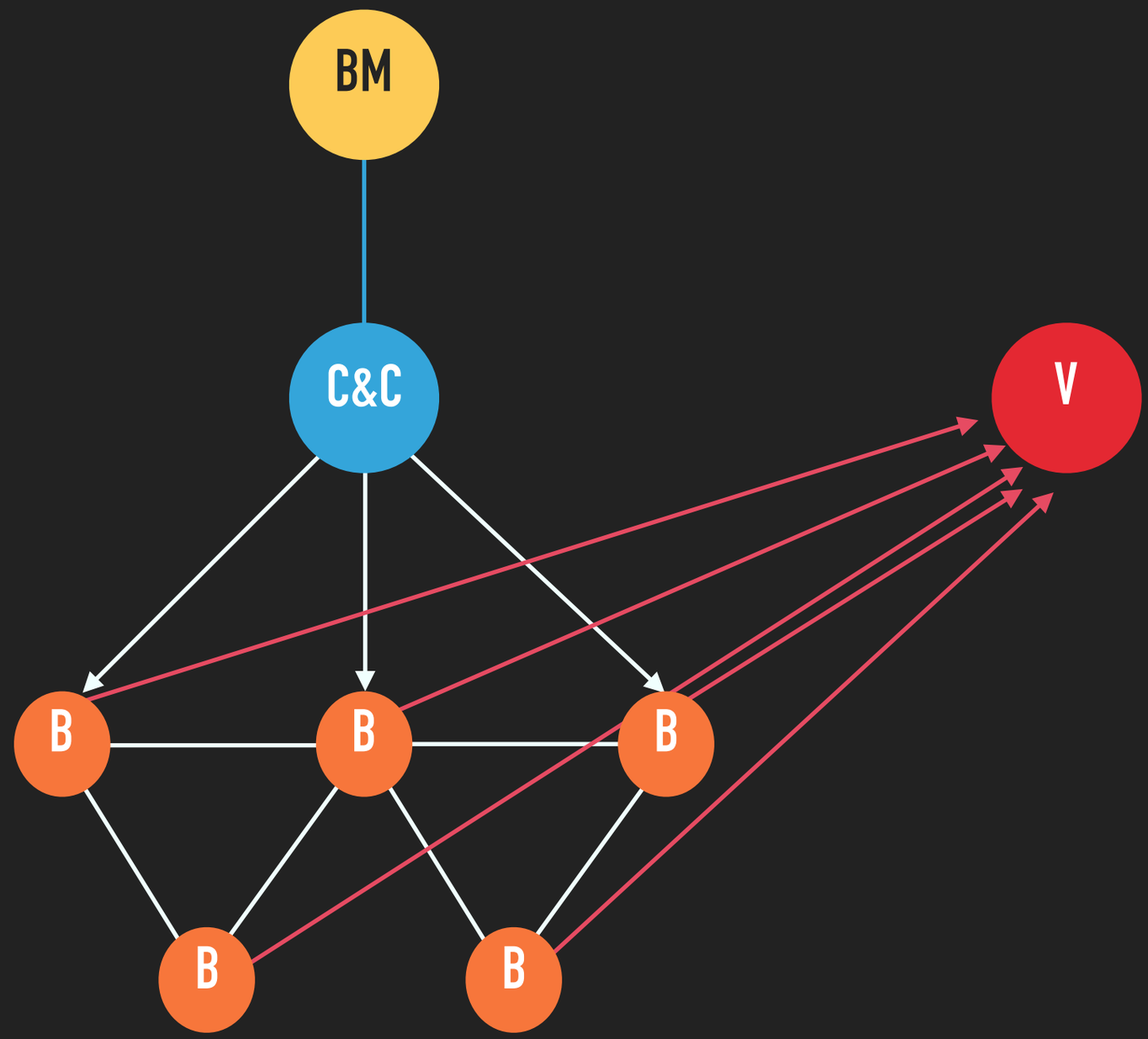
DENIAL OF SERVICE ATTACKS

- Steep artificial increase in contention for a shared resource
- Prevents legitimate users from accessing
- Utilizes protocol vulnerability
  - Ping of death
  - R-U-Dead-Yet?
  - SYN flood
  - SMS bomb
  - Farewell Attack

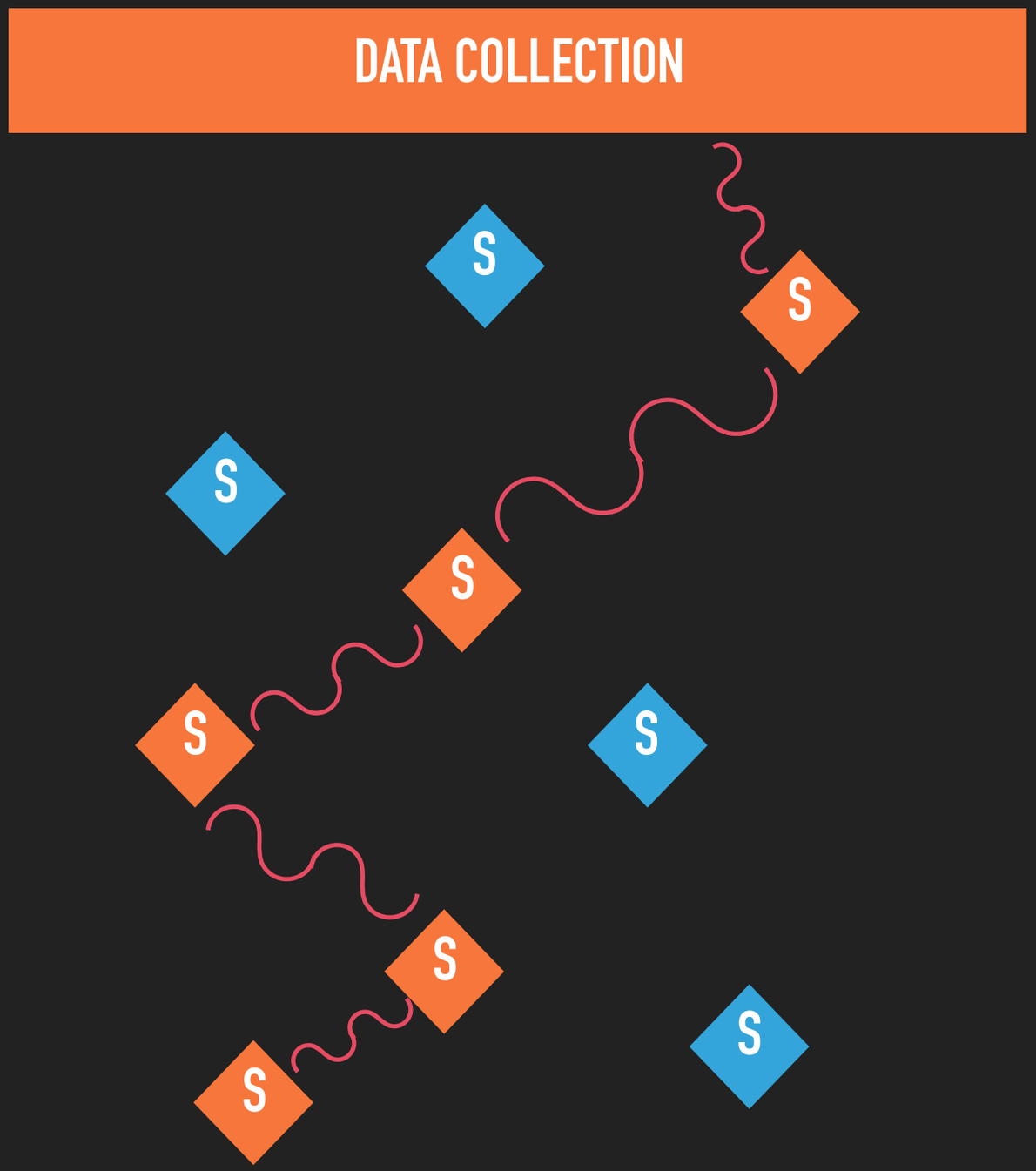
BOTNETS

- Network of compromised devices under the command of an the attacker.
- They are capable of performing Distributed Denial of Service (DDoS)
- Bots could potentially steal information out using Backdoors

BOTNET ARCHITECTURE

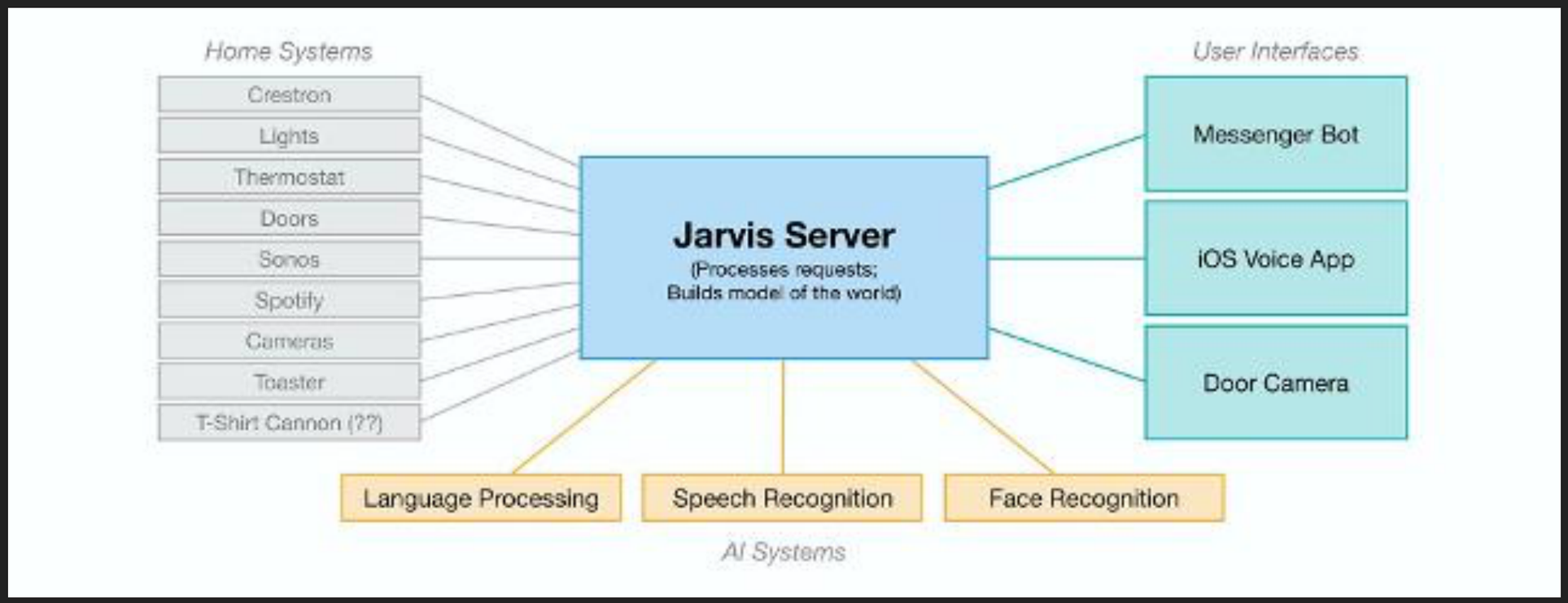


JARGON – WIRELESS SENSOR NETWORKS

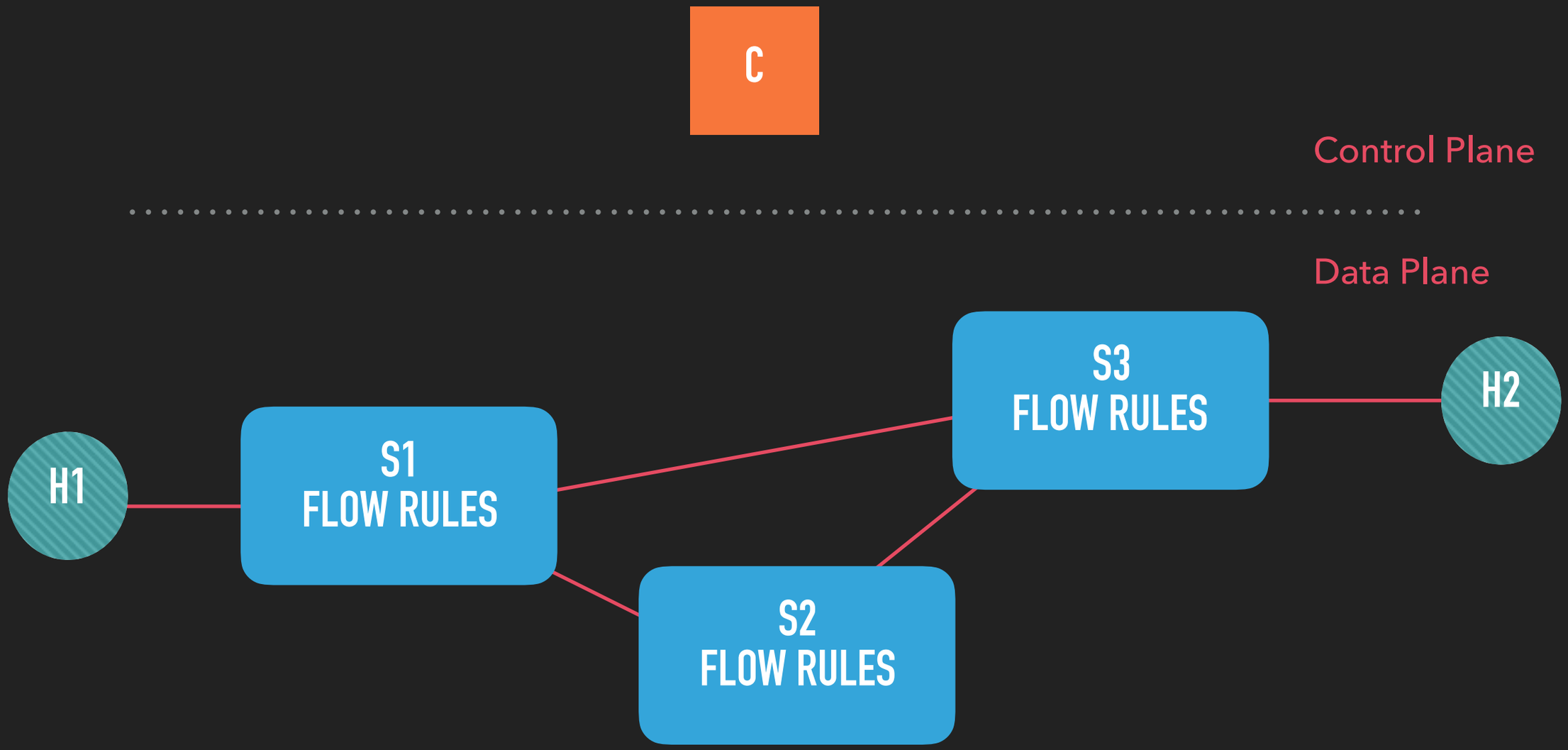


JARGON – INTERNET OF THINGS (IOT)

- Inter-networking of everyday things such as
  TV, AC, Doors, Mobiles, Audio system, Vehicles, Stove etc
- Mark Zuckerberg's ambitious goal for 2016 - J.A.R.V.I.S



JARGON – SOFTWARE DEFINED NETWORKING



QUESTIONS?

anandsanto@live.in

THANK YOU