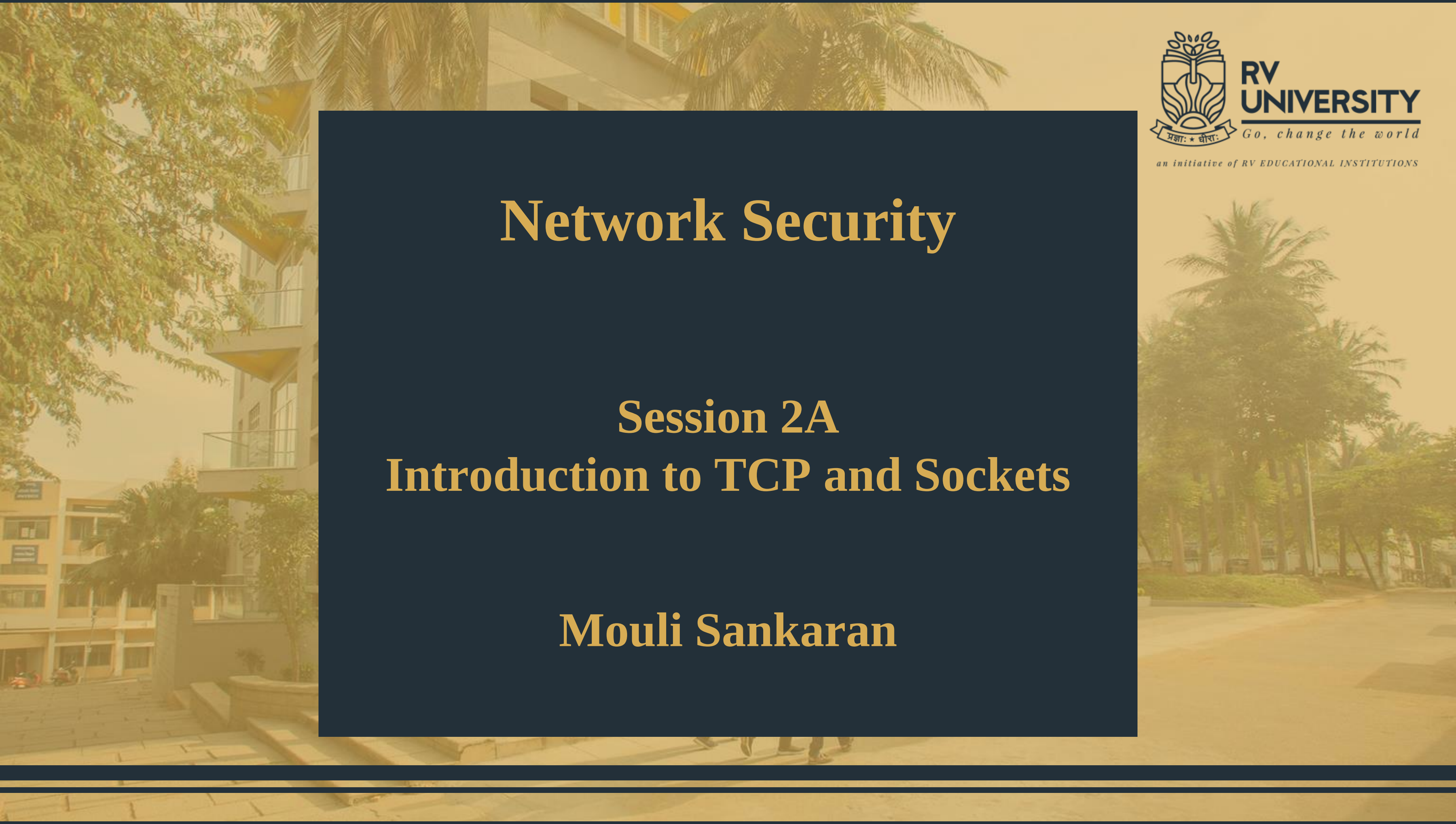


RV UNIVERSITY
Go, change the world
an initiative of RV EDUCATIONAL INSTITUTIONS

Network Security

Session 2A
Introduction to TCP and Sockets

Mouli Sankaran

Session 2A: Focus

- TCP: How is it implemented?
  - Multiple TCP Connections
  - What are Sockets?
  - How is each connection uniquely identified with sockets?

Course page where the course materials will be posted as the course progresses:

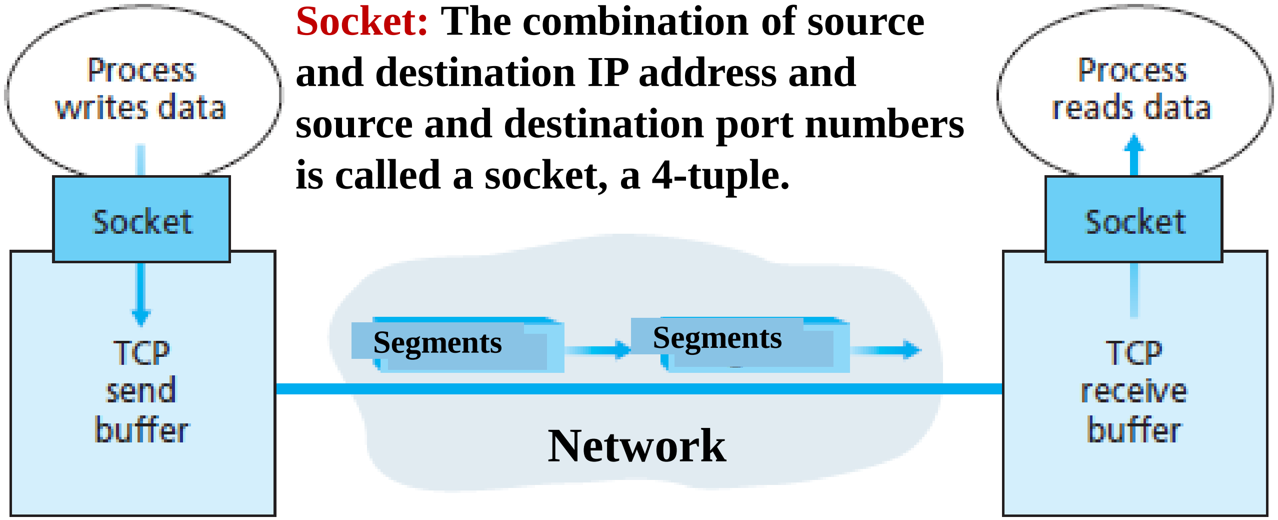
TCP
(Connection-Oriented)

TCP: Transmission Control Protocol

Layer 4

TCP Sockets

Socket: The combination of source and destination IP address and source and destination port numbers is called a socket, a 4-tuple.



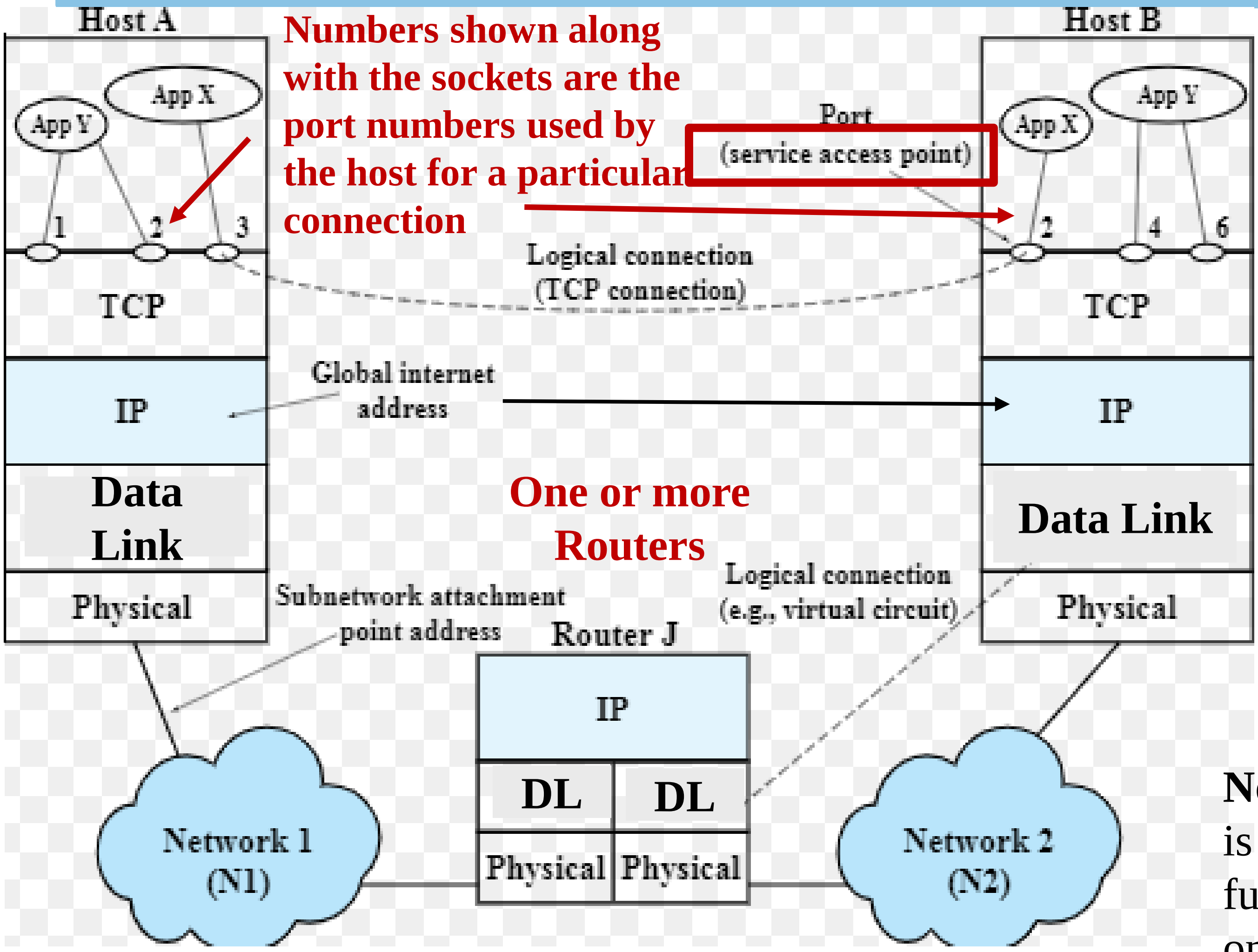
TCP connections are between two: c

a. Hosts
b. Subnets
c. Processes running on Hosts
d. None

Port numbers are some 16 bits values

- TCP is said to be **connection-oriented** because before one application process can begin to send data to another, the **two processes** must first “**handshake**” with each other
  - That is, they must send some **preliminary segments** to each other to establish the parameters for ensuing reliable data transfer, including the size of data in each segment
- As part of **TCP connection establishment**, both sides of the connection will initialize many TCP state variables

Multiple TCP connections on Host



Numbers shown along with the sockets are the port numbers used by the host for a particular connection

One or more Routers

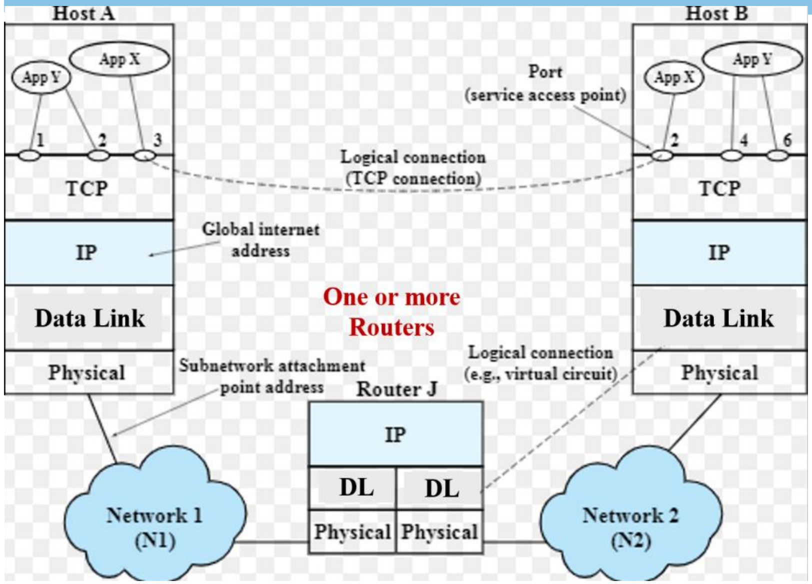
Note1: While a TCP connection between Host A and Host B already active, both hosts can establish multiple new TCP connections with many other hosts as well.

Note2: Remember that the TCP/IP protocol stack running on the hosts maintains the state of each active TCP connections that the hosts are currently having.

Note3: The TCP/IP stack is responsible for the functioning of all connections on a host.

SAP: **Service Access Point** is an identifying label for network endpoints used in Open System Interconnect (**OSI**) networking.

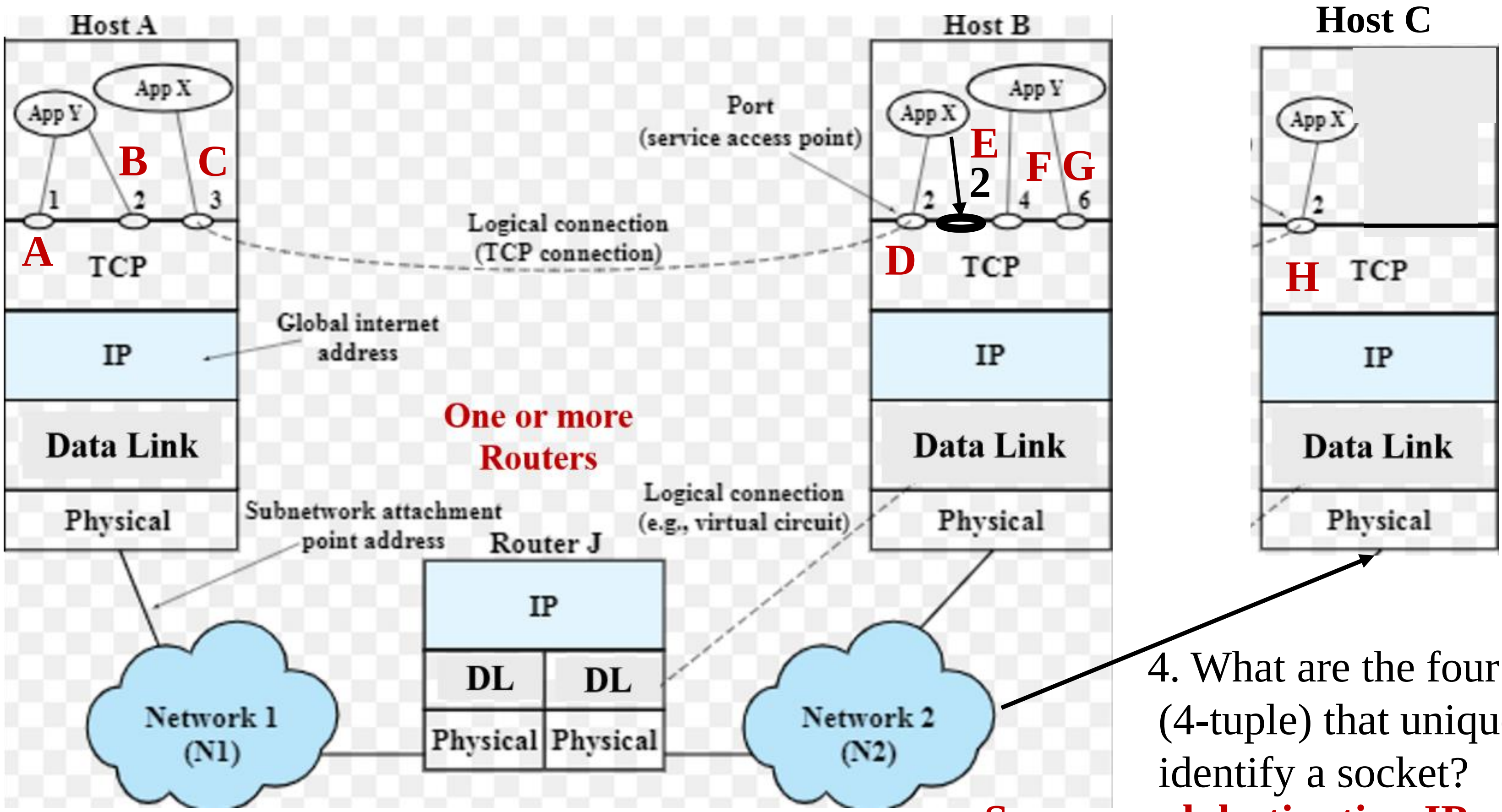
TCP connections: Explained



- Each host can have multiple TCP connections simultaneously
- The connections can be between the same set of hosts or different hosts
- TCP connections are **duplex**
  - i.e., the data transfer can happen in both directions, in parallel, independent of each other

- There are **exactly two end points** (hosts) communicating with each other on a TCP connection.
  - Broadcasting and multicasting aren’t applicable to TCP
- The TCP datagram is called a segment, which includes TCP header + data
- Each TCP segment contains the **source** and **destination port number** to identify the sending and receiving applications
- These above two values along with the **source** and **destination IP addresses** in the IP header, **uniquely** identifies each **connection**

How does a Socket Identify a Unique Connection?



4. What are the four values (4-tuple) that uniquely identify a socket?

Source and destination IP addresses, source and destination Port numbers

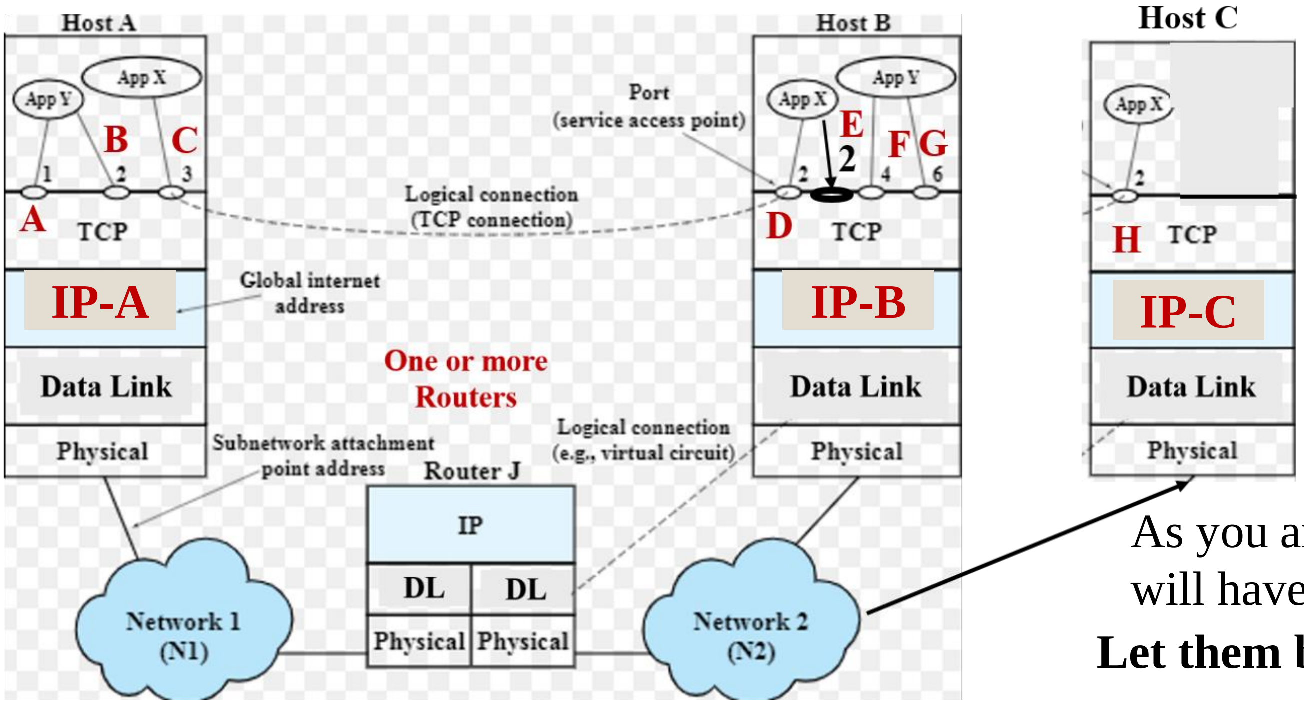
1. How many Hosts are involved here? **3**

2. How many sockets are shown here? **8**

3. Let us name the sockets from **A to H**

Check if these sockets can be uniquely identified?

What are the values of the Sockets here?



Socket is a 4-tuple:

Source IP address, destination IP addresses, source Port Number and destination Port number

As you are aware, each host will have an unique IP address each

Let them be: IP-A, IP-B, IP-C

Let the **socket pairs** which are **forming a TCP connection** are: **(A-F), (B-G), (C, D), (E-H)**

Now, give the 4-tuple values of each Socket: (SrcIP, DestIP, SrcPort, DestPort)

On Host A

Socket A: (IP-A, IP-B, 1, 4)

Socket B: (IP-A, IP-B, 2, 6)

Socket C: (IP-A, IP-B, 3, 2)

On Host B

Socket D: (IP-B, IP-A, 2, 3)

Socket E: (IP-B, IP-C, 2, 2)

Socket F: (IP-B, IP-A, 4, 1)

Socket G: (IP-B, IP-B, 6, 2)

On Host C

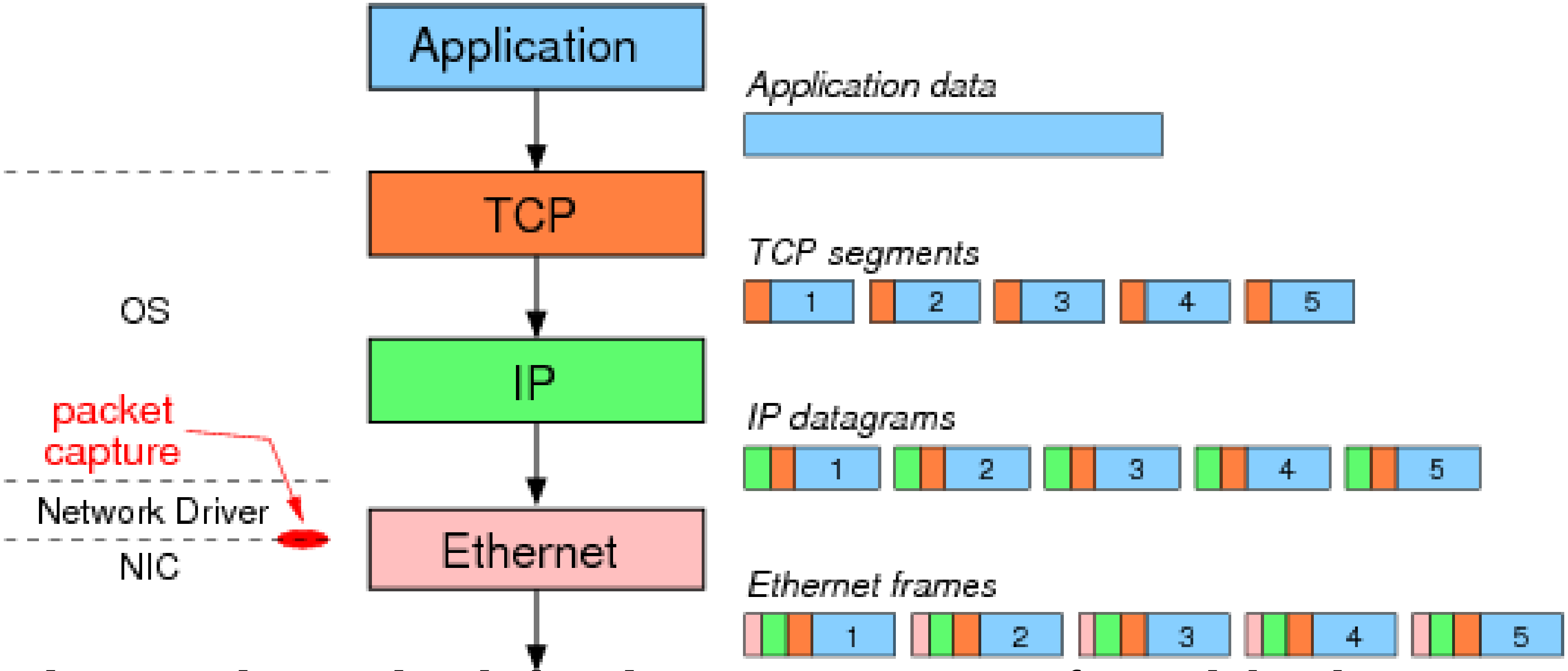
Socket H: (IP-C, IP-B, 2, 2)

Each connection is uniquely Identified with 4-tuple.

TCP Connection between two hosts

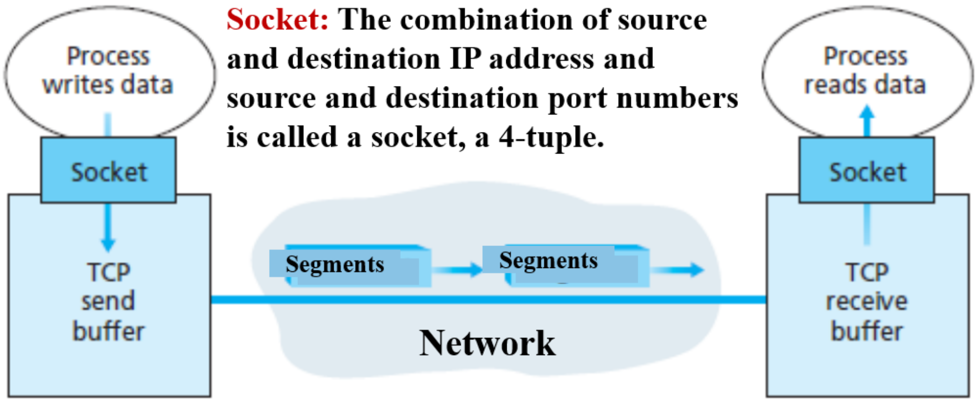
- TCP connection is always between only two end-points (two hosts)
- The socket values of each end is the same (order is different)
  - Thus, a socket identifies a connection uniquely
- The sockets within a host will also have a unique value because there cannot be more than one connection between the same set of ports on the same set of hosts
- So, it is not possible to create more than one connection with the same source port on a host, unless they are from different destination IP addresses (hosts)

TCP Segments going over the Network



- Application data is divided and TCP segments are formed, by the TCP layer.
  - The amount of application data on each segment is based on what has been decided by the hosts during the connection establishment
- Which is then made into IP datagrams and sent as Frames over the physical network (here Ethernet frames)

TCP Connections



Socket: The combination of source and destination IP address and source and destination port numbers is called a socket, a 4-tuple.

TDM: Time Division Multiplexing
FDM: Frequency Division Multiplexing
Note: In TDM or FDM, there is a physical circuit established between two nodes.

In **Virtual circuit**, the intermediate nodes maintains the information about a connection established between two nodes. E.g.: **VCI**: Virtual Circuit Identifier

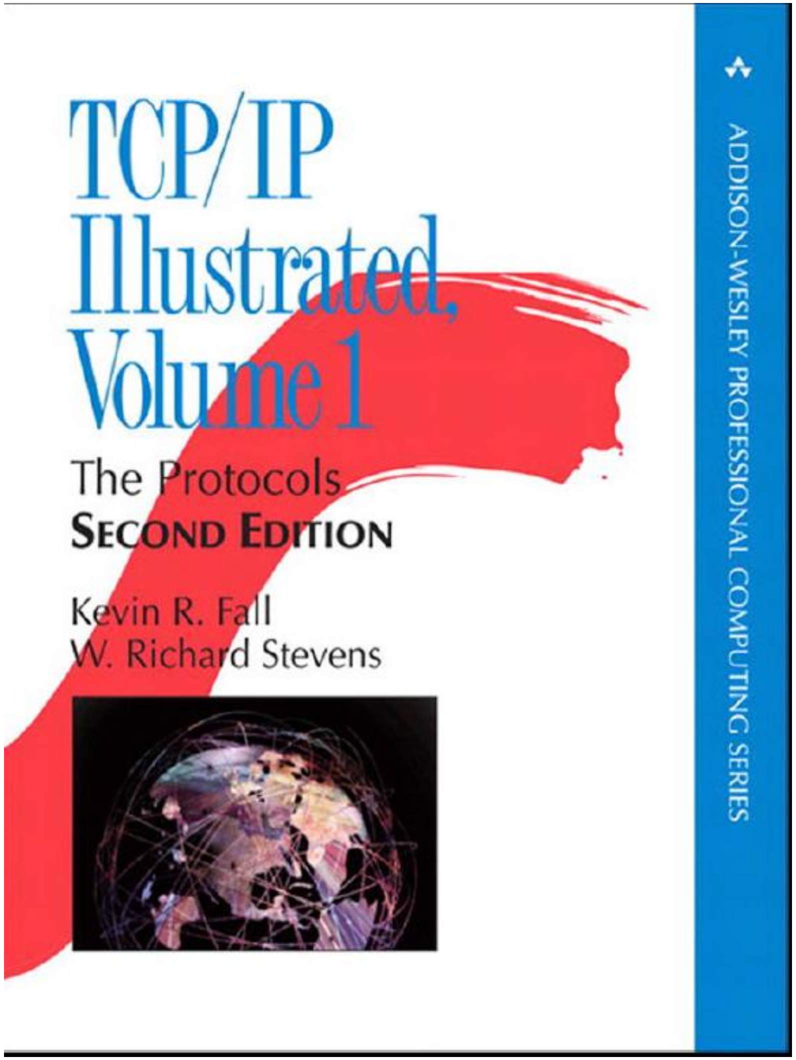
- The TCP “connection” is not an end-to-end TDM or FDM circuit as in a circuit switched network. Nor is it a virtual circuit, as the **connection state** resides **entirely** in the **two end systems**.
- Because the **TCP protocol runs only in the end systems** and not in the intermediate network elements (routers and link-layer switches), the intermediate network elements do not maintain TCP connection state
- In fact, the intermediate routers are completely oblivious (unaware of) to TCP connections; they just see IP datagrams, not TCP connections or segments.
  - Segments are put inside an IP datagram; routers see only the IP header and not its payload

Session 2A: Summary

- TCP: How is it implemented?
  - Multiple TCP Connections
  - What are Sockets?
  - How is each connection uniquely identified with sockets?

References

Ref 1



TCP/IP Illustrated, Volume 1

The Protocols

SECOND EDITION

Kevin R. Fall
W. Richard Stevens

ADDISON-WESLEY PROFESSIONAL COMPUTING SERIES

Ref 2

TCP Congestion Control: A Systems Approach

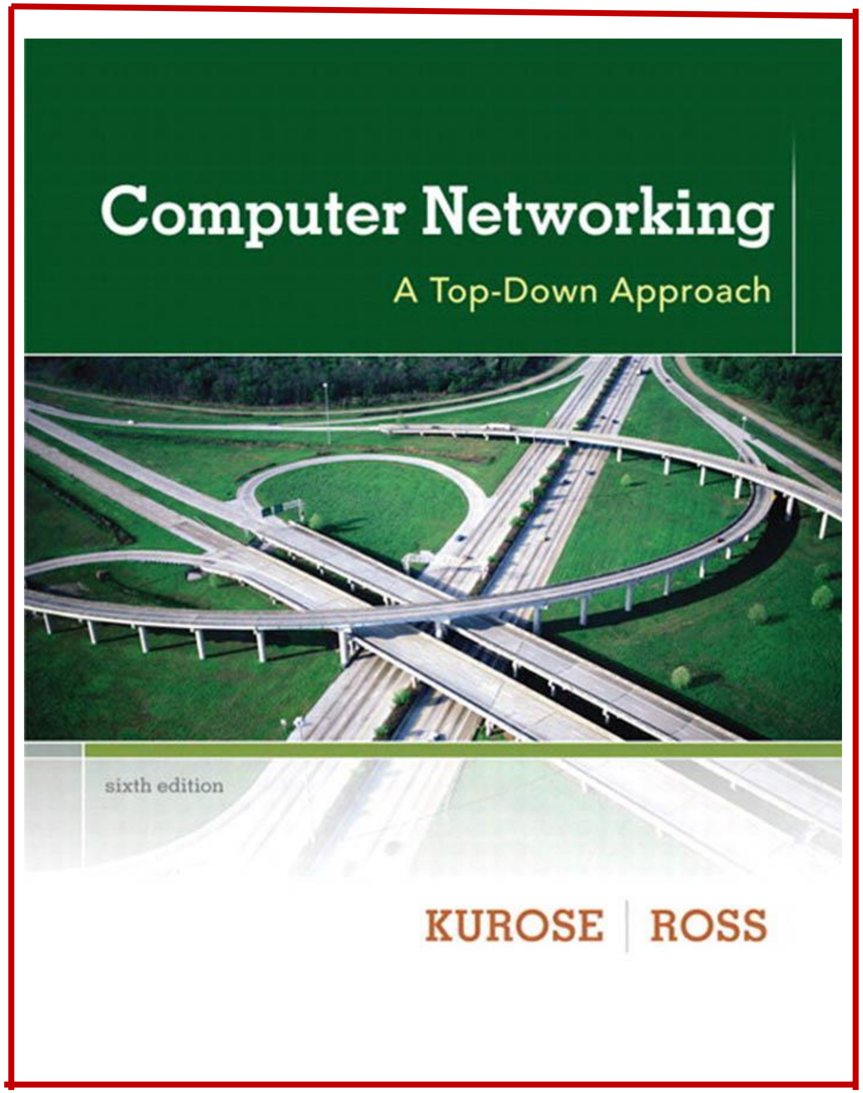
HTTPS://SYSTEMSAPPROACH.ORG

TCP Congestion Control: A Systems Approach

Peterson, Brakmo, and Davie

References

Ref 3



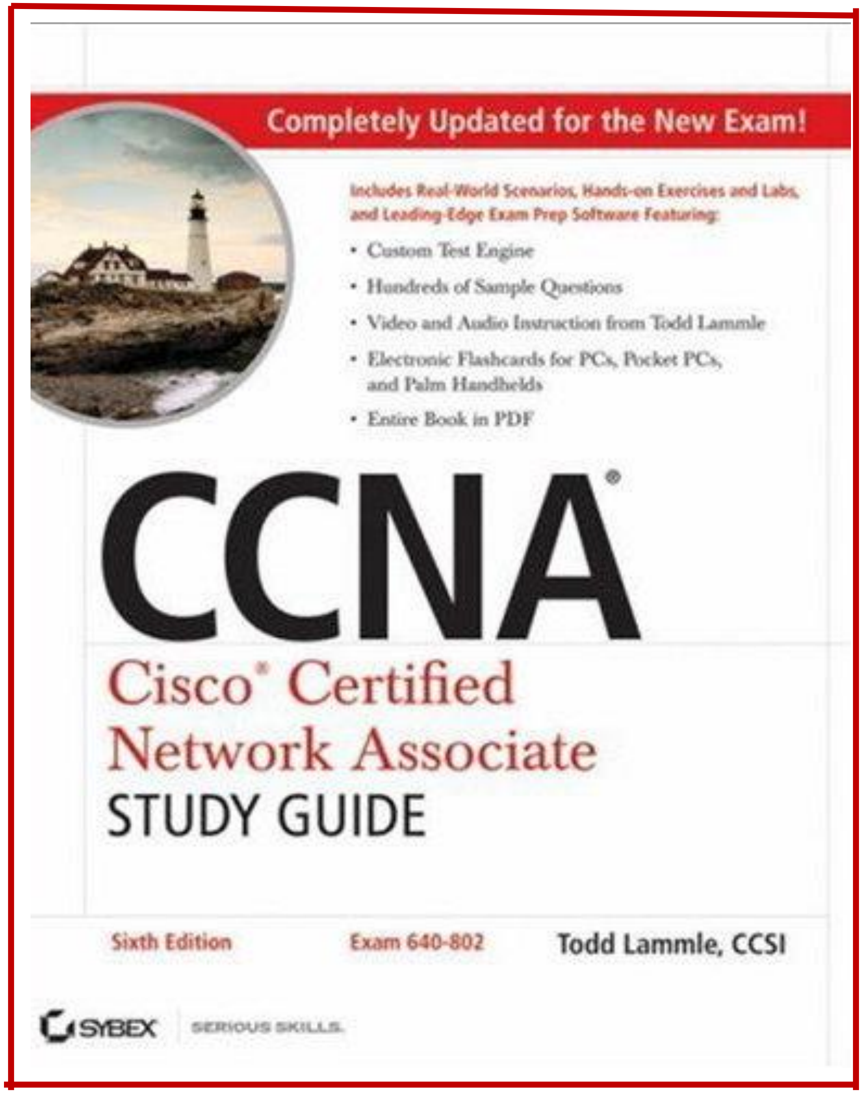
Computer Networking

A Top-Down Approach

sixth edition

KUROSE | ROSS

Ref 4



Completely Updated for the New Exam!

Includes Real-World Scenarios, Hands-on Exercises and Labs, and Leading-Edge Exam Prep Software Featuring:

- Custom Test Engine
- Hundreds of Sample Questions
- Video and Audio Instruction from Todd Lammle
- Electronic Flashcards for PCs, Pocket PCs, and Palm Handhelds
- Entire Book in PDF

CCNA®

Cisco® Certified Network Associate

STUDY GUIDE

Sixth Edition Exam 640-802 Todd Lammle, CCSI

SYBEX SERIOUS SKILLS.