C1 Network Layer & Physical Resilience

1. Layered Network Architecture

1.1 Motivations and Benefits

Organised as a stack of layers

- Offer services to the layers above it and passes data and control information to the layer below using a well-defined interface

Protocols

- Set of rules governing communication between two peering parties / computers
- Defines format, order of messages sent and received among network entities (computers), and actions taken on message transmission and receipt

Network Architecture

- Set of layers and protocols with specifications enabling hardware / software developers to build systems compliant with a particular architecture

Benefits

- Simplicity: easy to design once layers and interactions defined clearly
- Flexibility: easy to modify and develop networks by separate layers modifications
- Incremental Changes: easy to add new layers / functions to layer

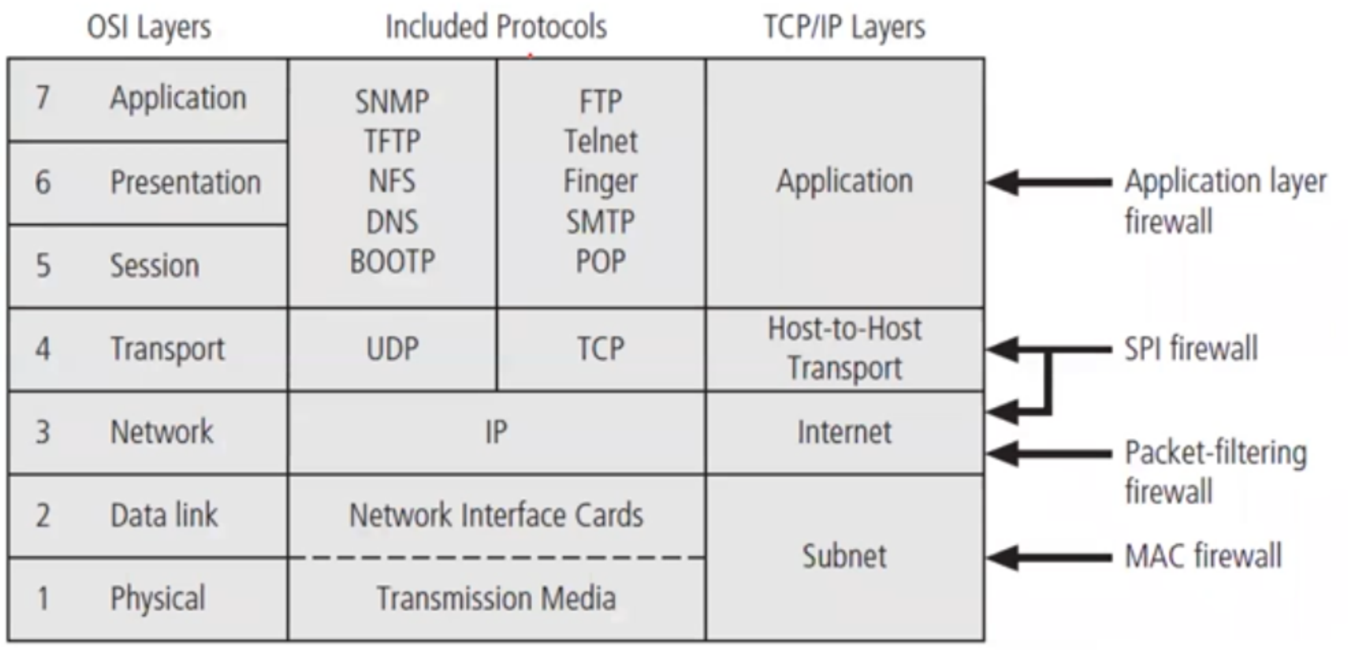
1.2 OSI 7-Layer Model

Media Layers (Layer - Data Unit) minimum requirement passed to Nodes

1. Physical - Bits (data cables, cat 6)
2. Data - Frames (Switching, MAC addresses)
3. Network - Packet (IP addresses, routing)

Host Layers

4. Transport - Segment (TCP/UDP)
5. Session - Data (session management)
6. Presentation - Data (WMV, JPEG, MOV)
7. Application - Data (HTTP, SMTP)



- Receiving (Ascending)
- Transmitting (Descending)
- **Troubleshooting starts from layer 1**

Function Decomposition

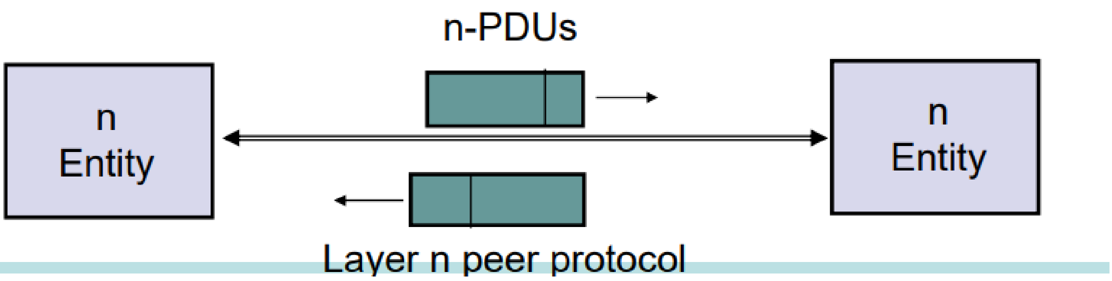
- Weakly-decoupled stack

Encapsulation

- Message begins at top of application layer (7) and moves down the layers to the physical layer with each layer adding a header to it as it descends
  - Headers are layer specific information which explains what functions the layer carries out
- Opposite occurs and headers are stripped from message as a system receives the message

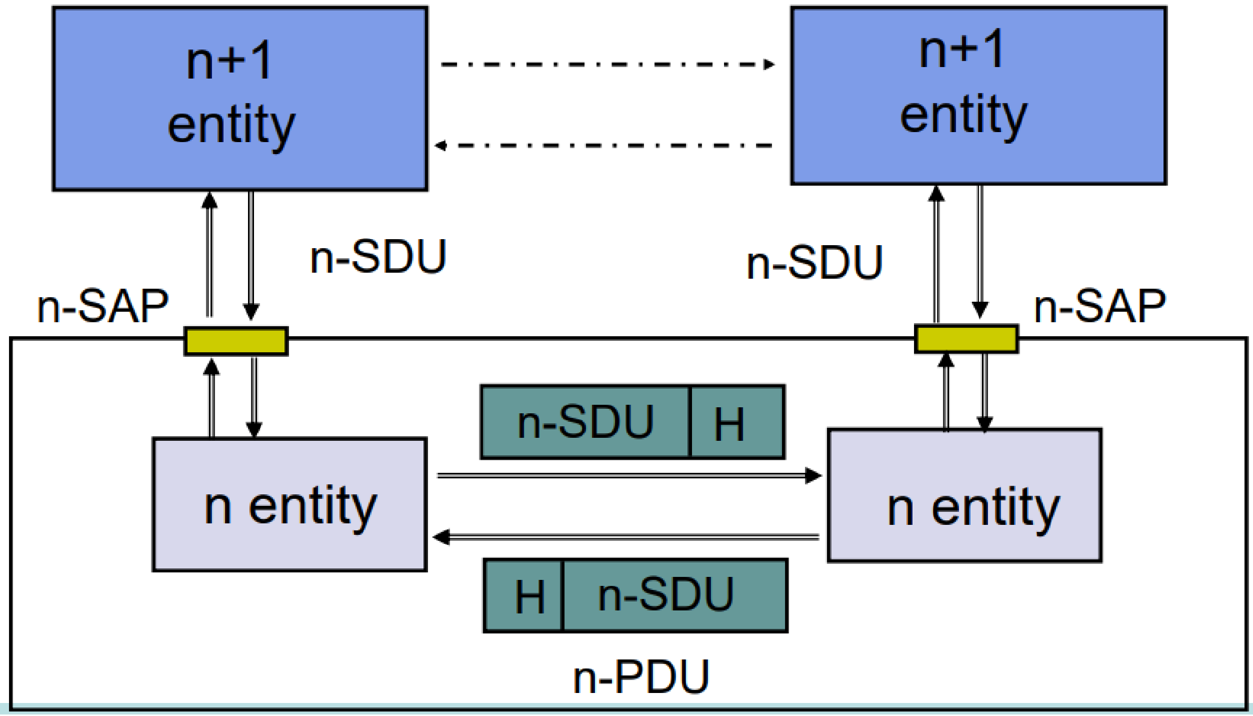
Peering (Protocols)

- Only peer layer communicating with each other
- Layer n in one machine interacts with layer n in another machine to provide a service to Layer $n+1$
- Entities comprising of corresponding layers on different machines are called peer processes and use a set of rules and conventions (Layer-n protocol)
  - Processes communicate by exchanging Protocol Data Units (PDU)



Peering (Services)

- Communication is virtual and indirect
- Layer $n+1$ transfers information by invoking services provided by Layer n which are available at Service Access Points (SAP)
- Each layer passes *data and control information* (i.e. Service Data Unit, SDU) to the layer below until the physical layer is reached and transfer occurs
  - SDUs are encapsulated in PDUs



1.3 5-Layer Implementation

Application

- Supporting network application
- File Transfer Protocol, Simple Mail Transfer Protocol, HTTP

Transport

- host-data transfer
- TCP, UDP

Network (Internet)

- Routing of datagrams from source to destination
- IP, routing protocols

Data Link (Network Access)

- Data transfer between neighbouring network elements
- PPP, Ethernet

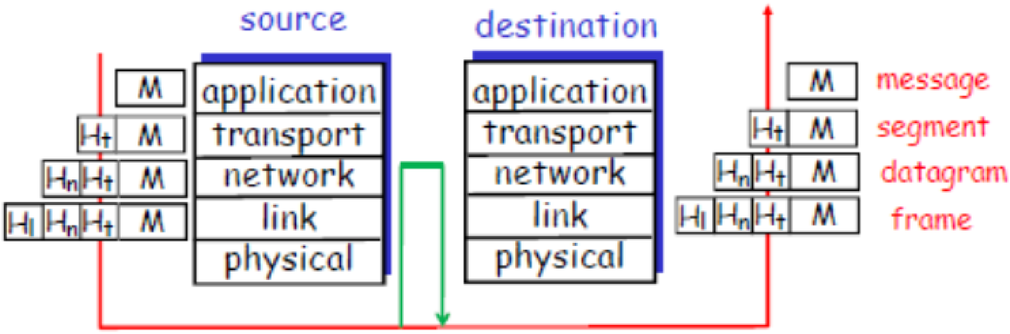
Physical

- Bits on the wire

Refer to slide 40 onwards for supplementary information

TCP / IP Internetworking

- Each layer takes data from above, add header information and passes new data unit to layer below (similar to OSI model)



2. Physical Resilience

Parameters

- Mean Time Between Failure (MTBF)
- Mean Time To Failure (MTTF)
- Mean Time to Repair (MTTR)
  - MTBF = MTTF + MTTR
- Availability = MTTF/MTBF
- Failure = MTTR/MTBF

Availability

Availability measures both system running time and downtime. It combines the MTBF and MTTR metrics to produce a result rated in 'nines of availability' using the formula: Availability = (1 – (MTTR/MTBF)) x 100%.

The greater the number of 'nines', the higher system availability. In mission-critical environments such as data centres, '5 nines' and above is fast becoming the desired standard.

Availability	Level	Downtime Per Year
99.9999%	6 nines	32 seconds
99.999%	5 nines	5 minutes 35 seconds
99.99%	4 nines	52 minutes 33 seconds
99.9%	3 nines	8 hours 46 minutes
99%	2 nines	87 hours 36 minutes
90%	1 nine	36 days 12 hours

2.1 Link Failure Probability

- **Percentage of time during which the link is dysfunctional**

- Given by r_i (availability of link i) and b_i (unavailability of link i / probability i is broken)
    - $r_i = 1 - b_i$

2.2 Network Resilience

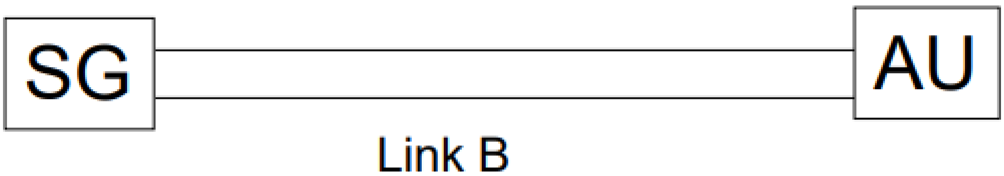
- Measure of Network Fault Tolerance and expressed in terms of probability that the network remains connected on the assumption that probability of link breaks are independent

Connectivity

- **Single**
    - Connection between two nodes

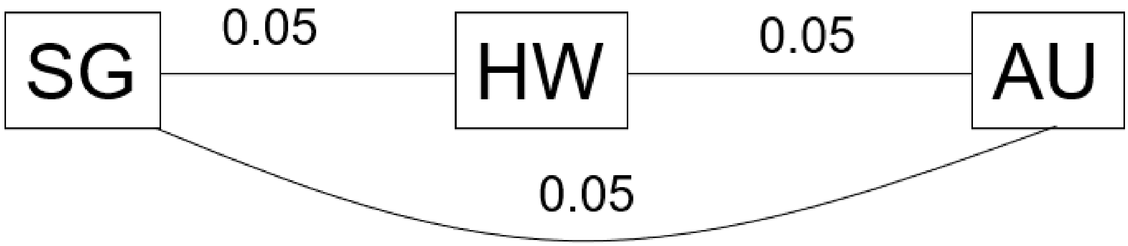
        - Link Break and Link Avail values are trivial
- **Series**
    - Nodes are connected in series

        - Connection between SG and AU is determined by both cables
        - Link Availability between SG and AU given probability of link break (0.05) can be calculated by the probability of link availability between SG and HW multiplied by link availability between HW and AU
- **Parallel**
    - Nodes are connected in parallel (i.e. two links between both nodes)



        - Link Availability can be calculated by subtracting the probability Link Break of both links from 1
- **Hybrid**

- Nodes have different styles of connection



  - Link Break between SG-HW-AU can be calculated by subtracting link availability from SG-HW-AU (0.95 * 0.95) from 1 (0.0975)
  - Link Break between SG-AU is 0.5
  - Probability of SG being disconnected from AU is given by $0.0975 \times 0.5 = 0.004875$

Calculating Link Availability

- **Series**
  - Calculate $P(\text{all links are working})$
- **Parallel**
  - Calculate $1 - P(\text{all links are broken})$
- **Hybrid**
  - Decompose into different paths
  - Calculate each path individually and multiply results