Networks and Systems Security (NSS)

Dr Sudipta Saha

https://www.iitbbs.ac.in/profile.php/sudipta/

Decentralized and Smart Systems Research Group (DSSRG)

https://sites.google.com/iitbbs.ac.in/dssrg

Computer Science & Engineering, School of Electrical Sciences
Indian Institute of Technology Bhubaneswar

Agenda

- Logistics
- General Background
- Introduction to NSS and it's Bold vision
- Syllabus and course plan

Logistics

3-1-0 course – Code - CS6L002

Lecture

Thursday 1:30 PM – 3:20 PM

Friday 4:30 PM – 6:30 PM

Logistics

- No Prerequisites –
- **Considering heterogeneous batch composition**

- Office Hours: After class or by appointment

- Course Webpage: TBD

- Email: sudipta@iitbbs.ac.in

Grading Policy

End Sem – 30% to 40%

Mid Sem – 20 to 30%

Internal - 30% to 40% - **Class Test**

Grades: As per Institute prescription

Grading Policy

- Term Project
  - Form a group of 4
  - *Decide an interesting topic* as an use case of Networks (As a possible application, little innovative one)
  - Arduino boards and necessary sensors can be used
  - Demonstration and presentation of the project
  - **Last two weeks of the semester**

Class Participation

- Come to the class
- Attendance will be taken first / mid / end
- Participate in discussions
- Discussion on possible issues on projects

Syllabus

https://www.iitbbs.ac.in/curriculum_doc/MTech_CSE_Curriculum_Latest.pdf

- **Introduction to Networking principles:** Introduction to networking, datalink layer, network layer and transport layer protocols, DNS, mail servers, web servers, peer-to-peer network Security, wireless communication protocol.

- **Overview of System Security:** Exploiting bugs in programs. Buffer overflows, fuzzing, Certification, secure socket layer (SSL), Kerberos, SQL injection, concepts of vulnerability, risk management, worm, virus, malwares, IDS, anti-viruses.

- **Basics of Cryptography:** Basic cryptography and techniques, block ciphers, message authentication, symmetric-key encryption, hash functions, public-key encryption, digital signatures.

- **Data Privacy:** Privacy changing online, mathematical definitions of privacy, attacks on privacy and anonymity, K-anonymity, Differential privacy, Private information retrieval, basics of multiparty computation and relationship to privacy.

- **Network Security:** Access control, sate full firewall, IPSec, modeling and analysis of various security violation in wireless and sensor networks, trusted computing techniques, ARP Poisoning, IP spoofing, hidden tunnels, denial of service attack, firewalls.

Main Modules

- **Computer Networks –**
- Basic, Application Layer Protocols and Wireless Communication etc.

- **Network Security** – Needs the knowledge of Computer Networks

- **System Security** – Needs the knowledge of Systems – Operating Systems as well as Network Systems

---

- Basics of Cryptography –

- Data-privacy –

Books on Computer Networks

1. Computer Networks – **by Andrew S. Tanenbaum**

2. Computer Networking: A Top-down Approach **- by Kurose, Ross**

3. Data Communications and Networking with TCPIP Protocol Suite - **by Behrouz A. Forouzan**

4. Computer Networks: A Systems Approach **- by Larry L. Peterson, Bruce S. Davie**

Books on Security

Network Security Essentials (Applications and Standards)

by William Stallings, Pearson Education.

Hack Proofing your network

by Ryan Russell, Dan Kaminsky, Rain Forest Puppy, Joe Grand, David Ahmad, Hal Flynn Ido Dubrawsky, Steve W.Manzuik and Ryan Permeh, Wiley Dreamtech

Reference Books:

Network Security and Cryptography: Bernard Menezes, CENGAGE Learning.

Network Security - Private Communication in a Public World: Charlie Kaufman, Radia Perlman and Mike Speciner, Pearson/PHI.

Cryptography and network Security, Third edition, Stallings, PHI/Pearson 4. Principles of Information Security, Whitman, Cengage Learning.

What is a “Network”

Network is a platform to connect with each other and in general provide the service of “connectivity”

Imagine we have a group of 4 students –

What is needed to make a fruitful collaboration among the students to carry out some project

They need to speak to each other – or pass messages

The intention is to convey the intention from student to the other – either verbally or through message

What is a “Network”

- When we have **two** students the **communication** among them and their collaboration becomes easier

- However when we have **many students** – it starts getting **chaotic** – IF there is no **systematic** communication among them

- It brings the requirement of a **leader** – which will be arbitrating the whole process – through polling or other mechanism

What is a “Network”

- Thus – multiple objects / entities when need to do some work together – **we need a platform which will allow them to get connected, communicate and collaborate – which is the responsibility of a NETWORK**

- A Computer network is a platform when multiple computer avail the service of connectivity among each other

- **Examples:**

- IoT is fundamentally a computer network where the objects / entities are “things” – i.e. in general anything.

- Internet – Connects everything in the world

- IIT Local Area Network

Internet of Things

- "The next era of information technology will be dominated by [IoT] devices, and networked devices will ultimately gain in popularity and significance to the extent that they will far exceed the number of networked computers and workstations."

- Medical devices and industrial controls would become dominant applications of the technology.

- Defining the Internet of things as "simply the point in time when more 'things or objects' were connected to the Internet than people"

- Cisco Systems estimated that the IoT was "born" between 2008 and 2009, with the things/people ratio growing from 0.08 in 2003 to 1.84 in 2010.[29]

Take a simple example

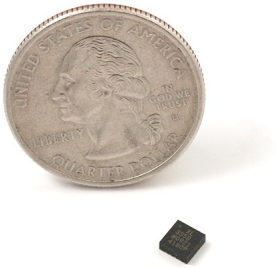
- **Smart Class room**
- Smartness is defined from multiple perspectives
- However, we focus on one specific issue here – The classroom should be able to quickly asses how many students are there –
- Constraints –
  - Accurately
  - Seamless installation of the system
  - Low cost
  - Durable
  - Low or negligible maintenance cost

Gist of Technologies involved in IoT

- Sensor Technology – Tiny, Cheap
- Low cost embedded systems
- Low Power Connectivity
- Capable of including Mobile Devices (Not always)
- Cloud

Sample Sensors

Pulse Sensor



Accelerometer
(4mm diameter)

Force Sensor
(0.1N – 10N)

https://www.sparkfun.com/,

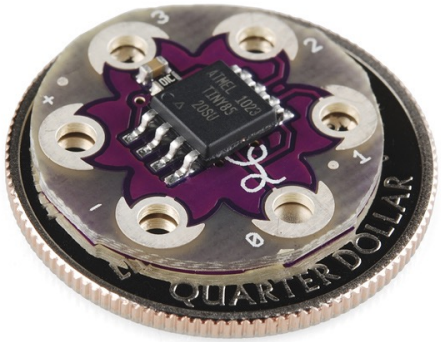
https://www.adafruit.com/

Sensor Technology

- Instrumentations
- Any physical quantity – Convert to electrical Signals
- They usually depend on some property of some material – say with pressure the resistance changes
- Sensors are built –
  - Pressure sensor, Temperature sensor, …
  - The power consumption of these sensors has to be quite low
  - The size of the sensors have to be quite small
  - Cost of the sensor has to be also very low

Embedded Systems

- Cheap and Tiny Embedded Systems



Lily Tiny: ($5.00)

http://www.atmel.com/devices/ATTINY85.aspx?tab=parameters

Key Parameters

Flash: 8 Kbytes

Pin Count: 8

Max. Operating Freq: 20 MHz

CPU: 8-bit AVR

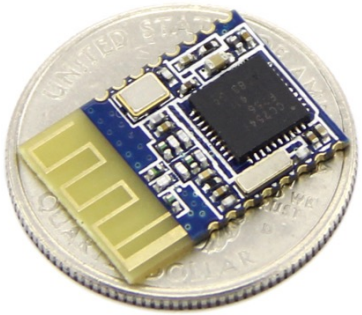
Max I/O Pins: 6

Ext Interrupts: 6

SPI: 1

I2C: 1

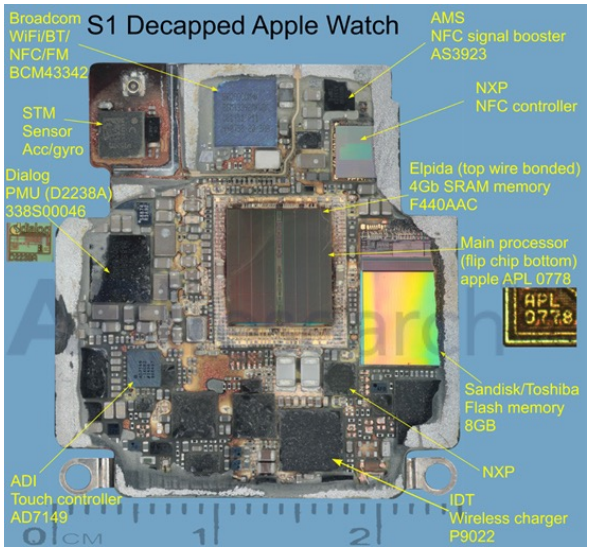
Low-Power Connectivity



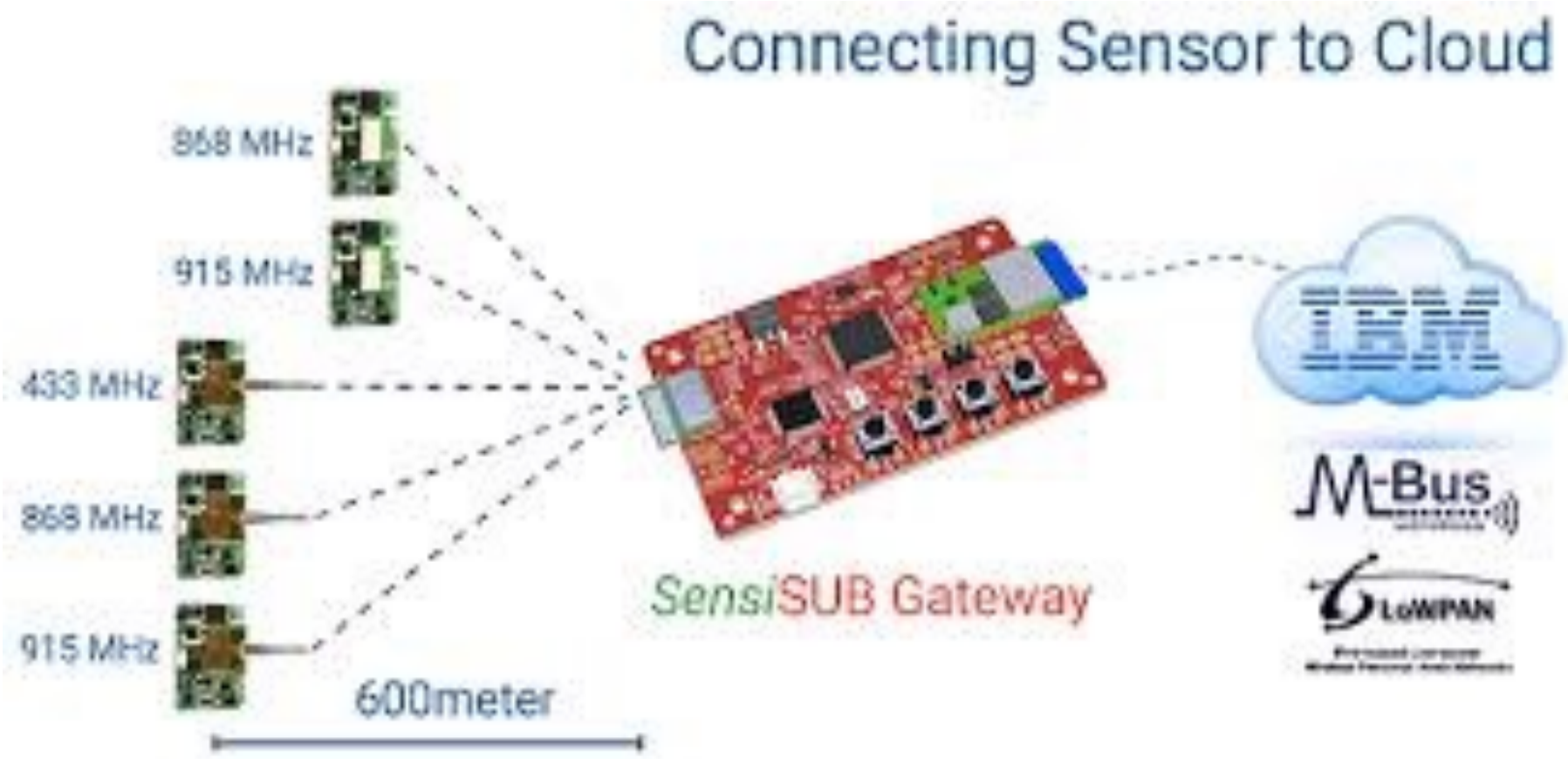
Bluetooth Smart (4.0) (Up to 2 years with a single Coin-cell battery)

Mobile Devices

Quad Core 1.5 GHz
128 GB Internal Memory
3 GB RAM
16 MP Camera
2160p@30fps video
WiFI, GPS, BLE



Connecting Sensors to Cloud



Source: sensiedge.com

Cloud Platforms

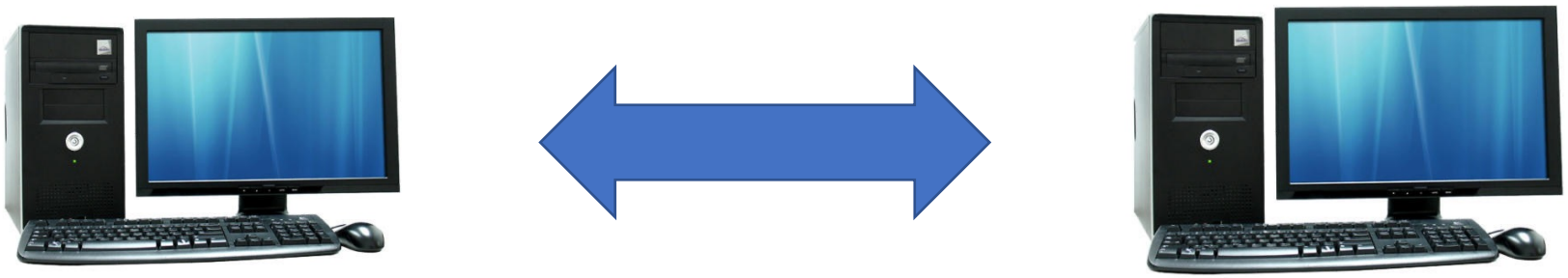
Applications

- Healthcare
- Transportation
- Food
- Weather
- Disaster prediction
- Smart homes

Basics of Networking

Connectivity between two computers/machines

How to connect two computers / two machines so that they can talk to each other

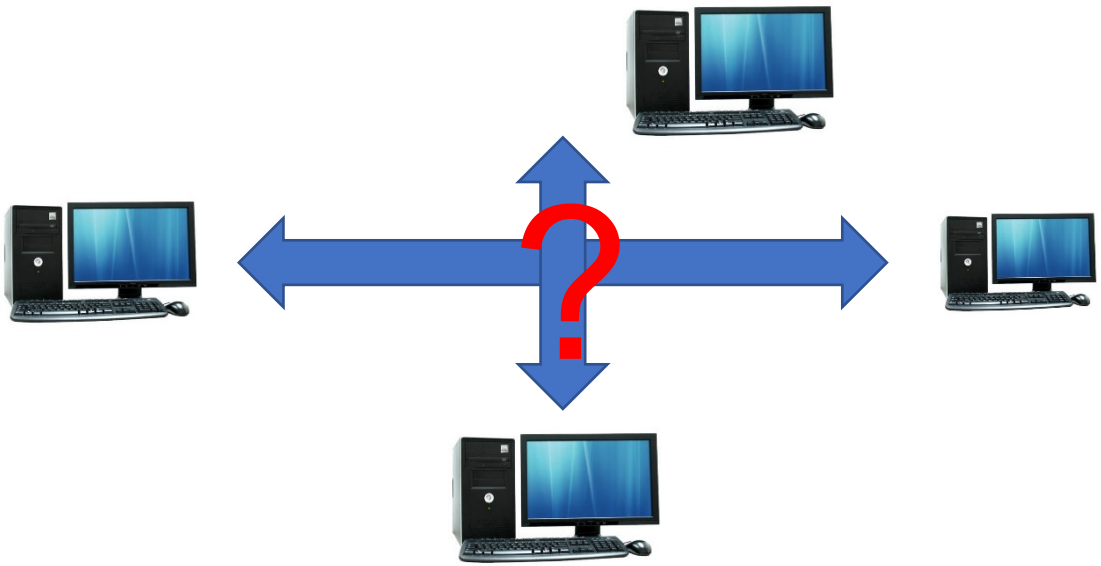


Basics of Networking

Next level (multiple-access)

Connectivity within an area

How to connect multiple computers / multiple machines so that they can talk to each other

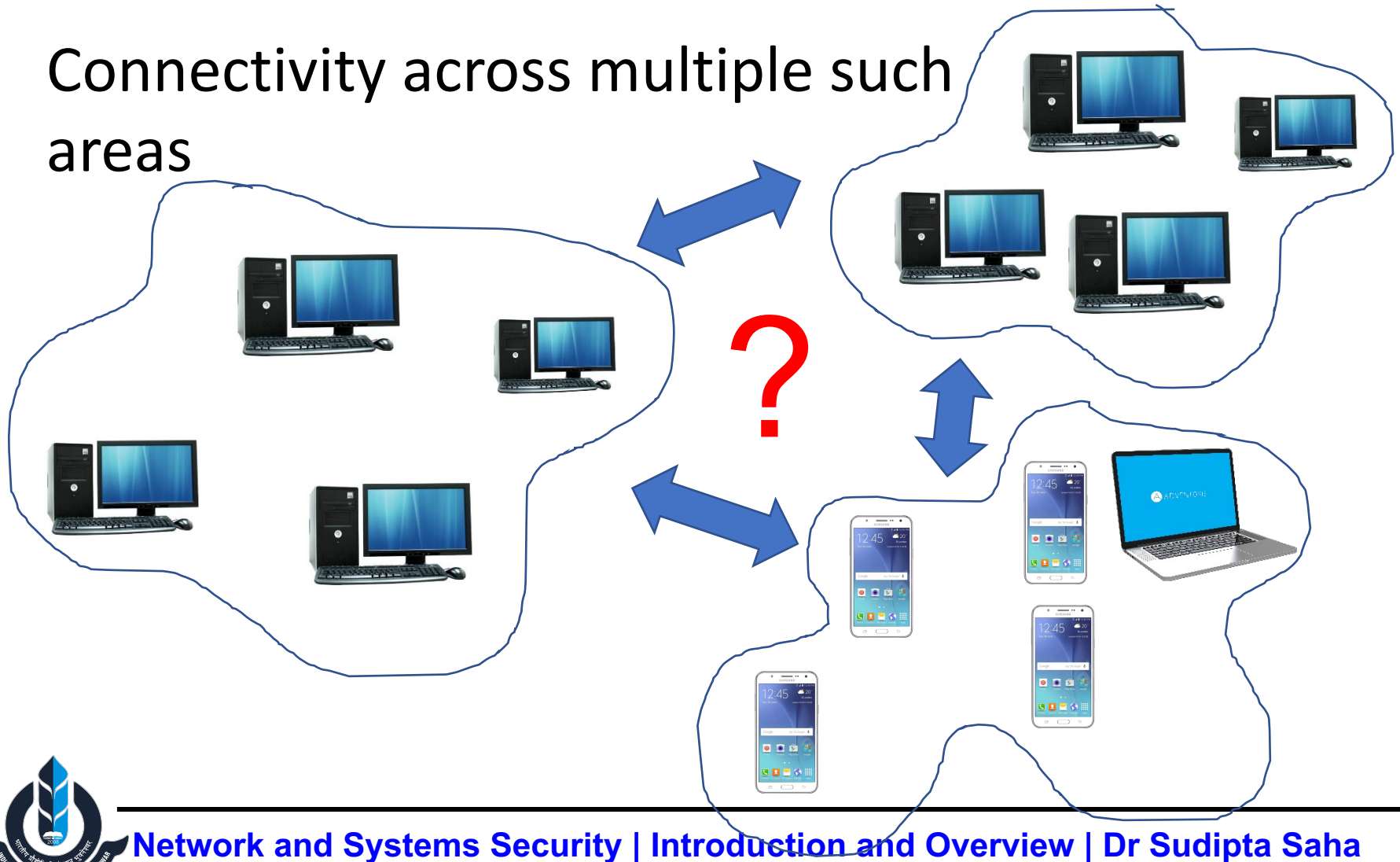


Possible problems ?

Basics of Networking

Next Level (internetworking)

Connectivity across multiple such areas



Basics of Networking

What is the difference between information and substance ?

Basics of Networking

Information:

Anything that is represented in bits ..

Infinitely replicable

Substance:

Can not be represented in bits

Cannot be replicable ….! (?)

Basics of Networking

Computers can *"manipulate"* information
Networks create *"access"* to information

Basic purpose of networks –

Move bits everywhere, cheaply, and with desired performance characteristics.

Long term goal of networks - Break the space barrier for information (not for substances)

Basics of Networking

Network provides connectivity

What is "*Connectivity*" ?

Connectivity is the magic needed to communicate if you do not have a direct point to point physical link.

Tradeoff: Performance characteristics worse than true physical link!

Direct or indirect access to every other node in the network

Basics of Networking

- Building Blocks
  - links: coax cable, optical fiber...
  - nodes: general-purpose workstations...

- *Direct* connectivity:
  - point-to-point

  - Multiple access e.g. Bus, Ring

Basics of Connectivity

In-direct connectivity –

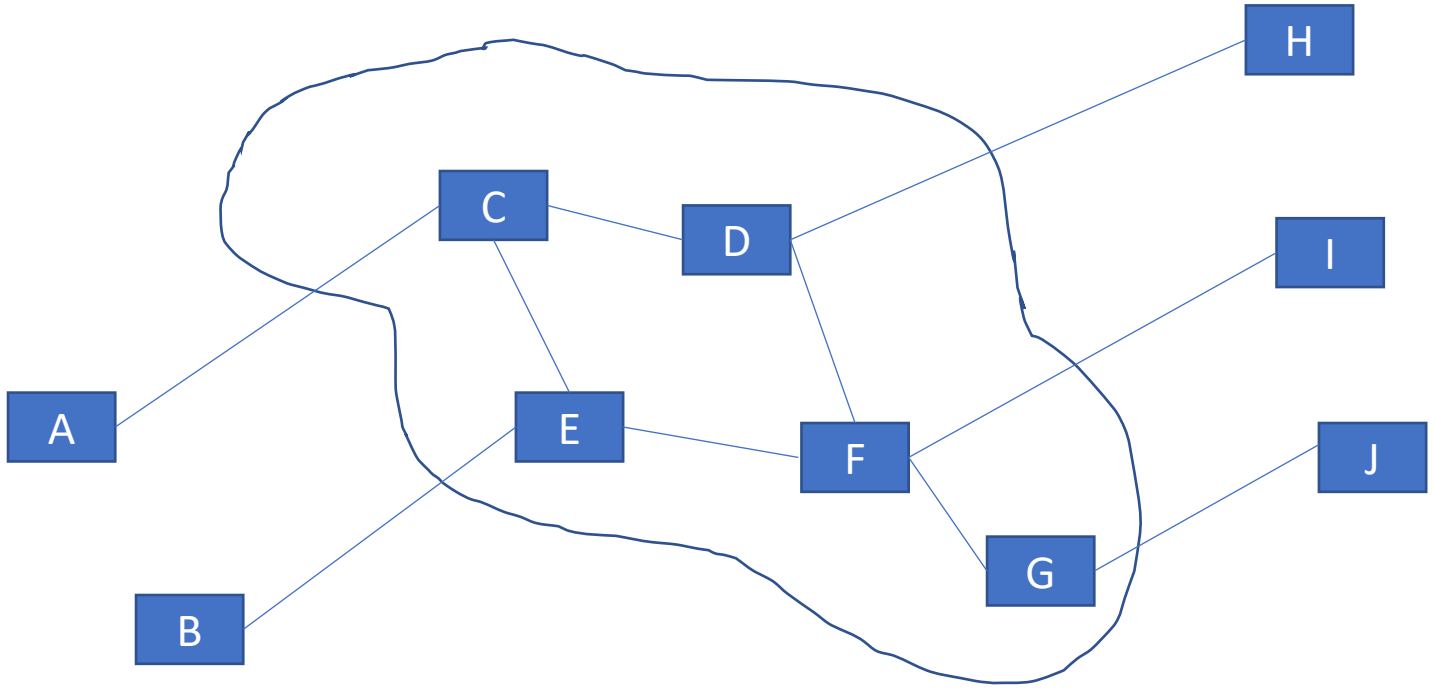
There are intermediate nodes

Instead of connecting to all others in the other zone we connect to the intermediate node

Basics of connectivity

There are intermediate nodes

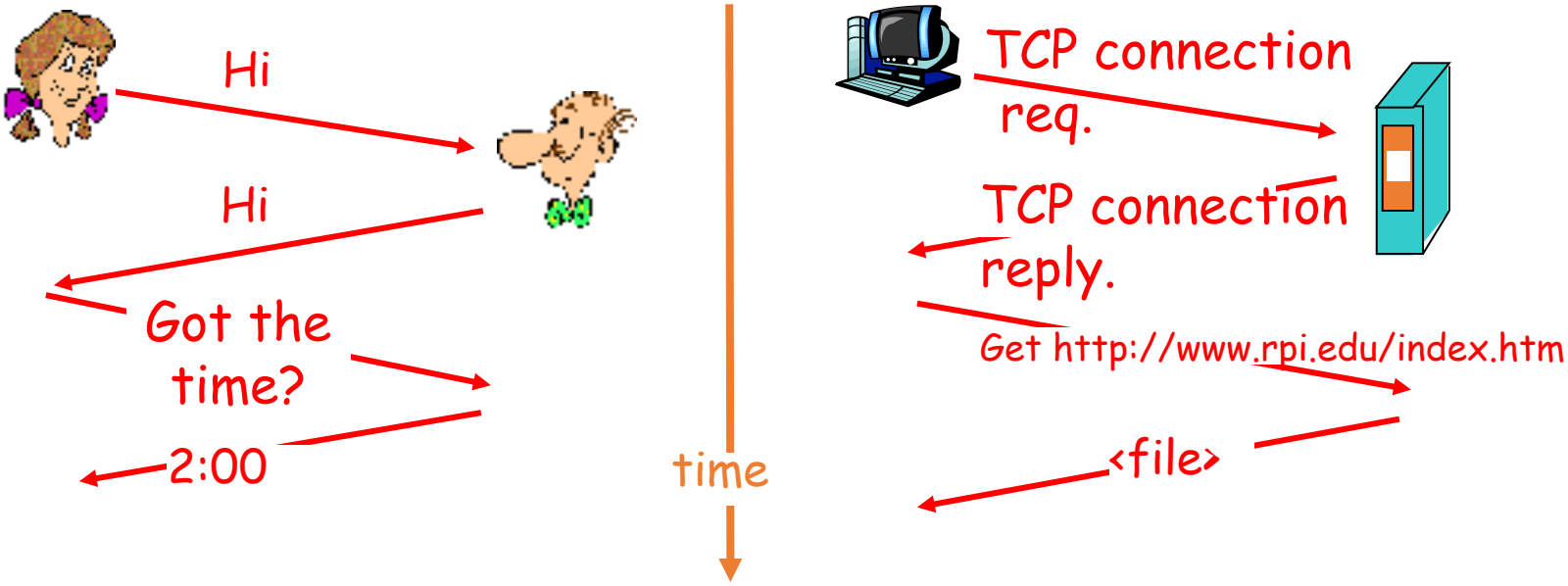
Instead of connecting to all others in the other zone we connect to the intermediate node



Protocols

Some set of rules – when we have two systems to talk to each other

- Networking software is organized as *protocols*
- Eg: Human protocol vs network protocol:



Layering – Vertical Horizontal View

Airline system

So many things clubbed together in a single system –

Ticketing agents,

Baggage checkers,

Gate personnel,

Pilots,

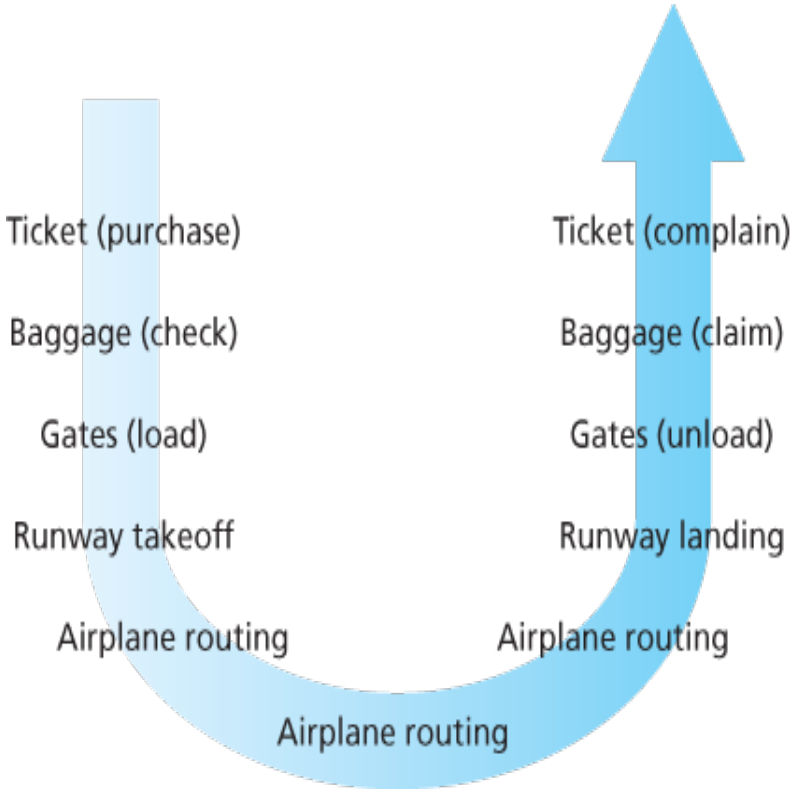
Airplanes,

Air traffic control, and

A worldwide system for routing airplanes

Airline system

You purchase your ticket …



Check your bags

Go to the gate, and

Eventually get loaded onto the plane.

The plane takes off and

The plane is routed to its destination

After your plane lands

you deplane at the gate and

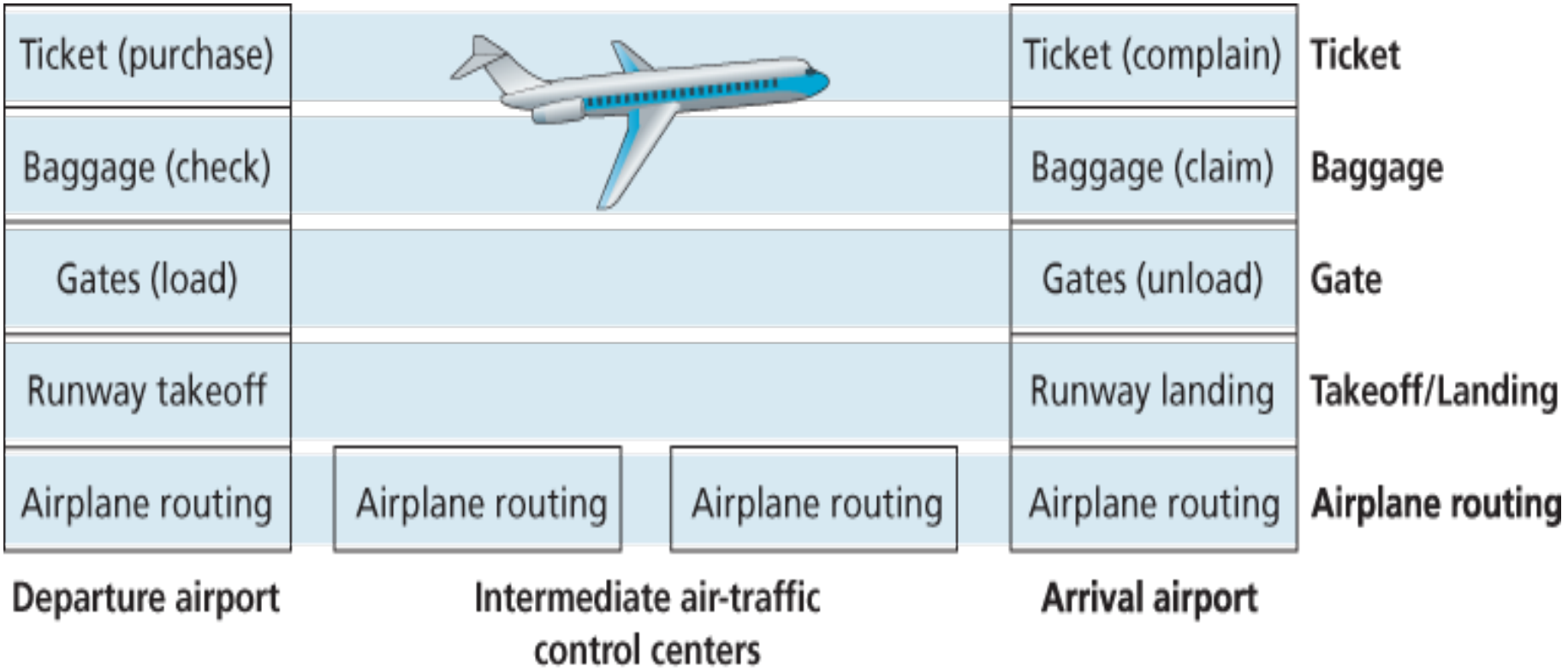
claim your bags.

If the trip was bad, you complain about the flight to the ticket agent

Trying to find a structure …

- We note that there is a ticketing function at each end;
- There is also a baggage function for already-ticketed passengers,
- A gate function for already-ticketed and already-baggage-checked passengers.
- Passengers who are already ticketed, baggage-checked, and through the gate, there is a take-off and landing function,
- While in flight, there is an airplane-routing function.
- **This suggests that we can look at the functionality in *horizontal* manner**

We are looking at some structure -



Service and functionality at a layer

- Note that each layer, combined with the layers below it, implements some functionality, some *service.*
- At the ticketing layer and below, **airline-counter-to-airline-counter transfer** of a person is accomplished.
- At the baggage layer and below, **baggage-check-to-baggage-claim transfer of a person and bags is accomplished** - Only to an already-ticketed person.
- At the gate layer, **departure-gate-to-arrival-gate transfer** of a person and bags is accomplished.
- At the takeoff/landing layer, **runway-to-runway** transfer of people and their bags is accomplished.

Service and Functionality at a Layer

- Each layer provides its service by

(1) Performing certain actions within that layer (for example, at the gate layer, loading and unloading people from an airplane) and by

(2) Using the services of the layer directly below it (for example, in the gate layer, using the runway-to-runway passenger transfer service of the takeoff/landing layer)

Protocol Layering

- Network designers organize protocols and the network hardware and software that implement the protocols—in **layers**

- Layer *n* may include reliable delivery of messages from one edge of the network to the other.

- This might be implemented by using an unreliable edge-to-edge message delivery service of layer n−1, and adding layer *n* functionality to detect and retransmit lost messages.

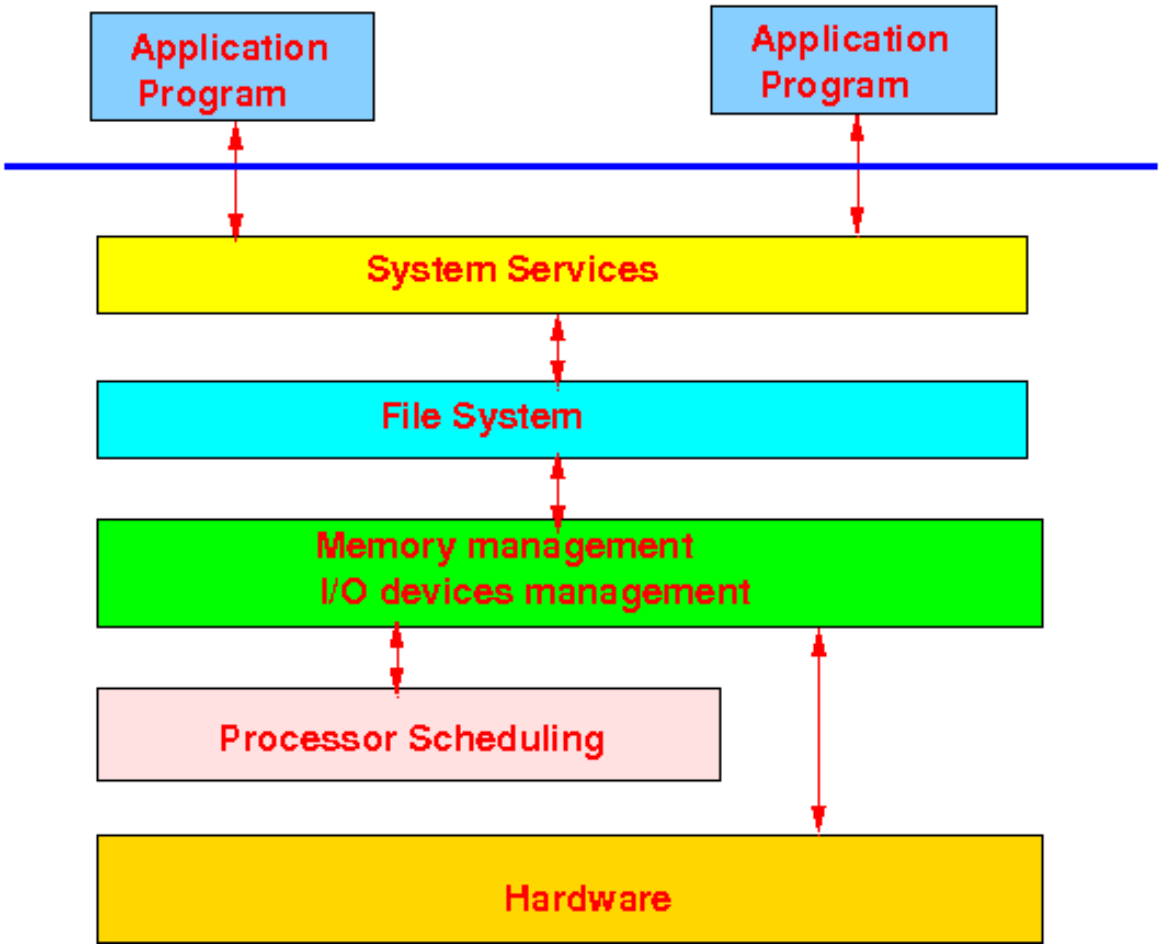
The *ISO* Architecture of computer networks

Software Engineering principle

***Every* (operational) complex software systems** created by **humans** are **designed** using a ***modular* (layer) approach**

Example

UNIX Operating System is layered:



Communication Architecture:

A **system** that allows
a ***large*** **number** of **computers** to **communicate** with each other over ***large*** **distances**

- *is* a ***very*** **complex software system**....

The **design** of the present day **communication systems** are ***layered***....

An international standard layered design of a Communication architecture

ISO = International Standard Organization

Communication Architecture:

In the late 1970s, two projects began independently, with the same goal:

to define a **unifying standard** for
the **architecture** of **networking (communication) systems**

One project was administered by the **International Organization for Standardization** (**ISO**)

The other was undertaken by the **International Telegraph and Telephone Consultative Committee**, or **CCITT**
(the abbreviation is from the French version of the name)

Communication Architecture:

These **two** international standards bodies each developed a **document** that defined ***similar*** **networking models**.

In **1983**, these **two documents** were **merged** to form a **standard** called:

The **Basic Reference Model** for **Open Systems Interconnection**.

ISO OSI reference model

- The 7 ***layers*** in the **ISO OSI reference model**:

Application layer	make sure the program communicate according to proper procedure (+ error recovery)
Presentation layer	make sure that all data are acceptable to all participants (encrypt, translate)
Session layer	make sure that all participants are aware of each other
Transport layer	make sure final destination receive data from source reliably
Network layer	determine which neighbor node to forward message to reach final destination
Datalink layer	make sure node receive data reliably from neighbor node
Physical layer	connect to your neighbor nodes

Physical Layer

- Physical Layer - Move the ***individual bits*** within the frame from one node to the next.

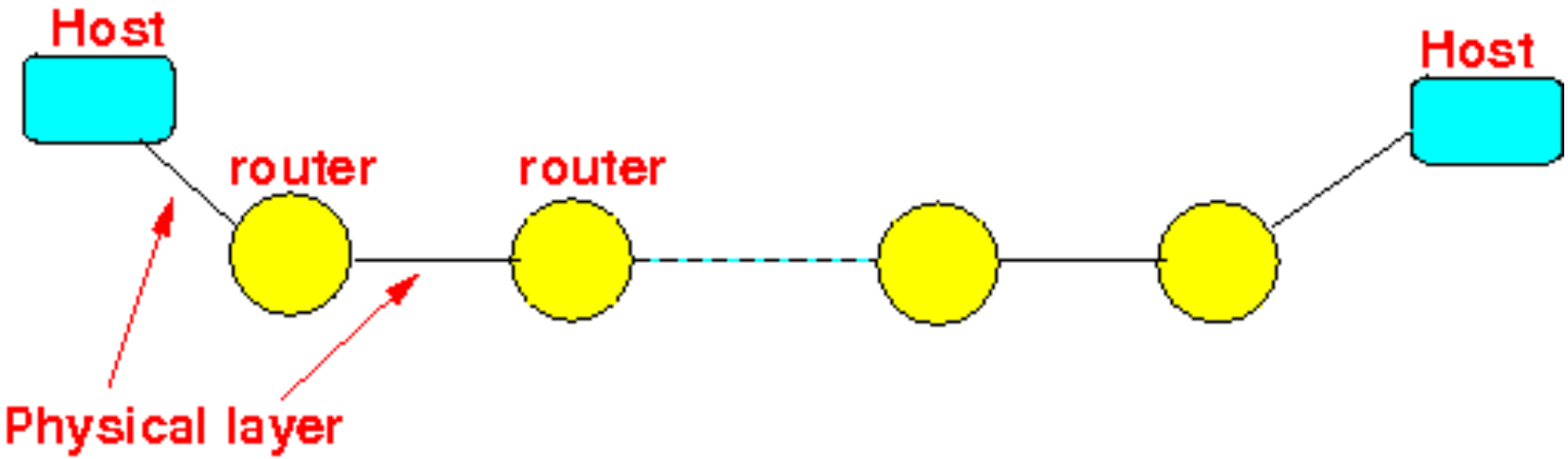
- The protocols in this layer are link dependent and further depend on the actual transmission medium of the link (for example, twisted-pair copper wire, single-mode fiber optics).

- For example, Ethernet has many physical-layer protocols: one for twisted-pair copper wire, another for coaxial cable, another for fiber, and so on. In each case, a bit is moved across the link in a different way.

Physical layer

Is the **only** ***hardware*** "layer"

The **Physical hardware "layer"** provides
the **ability** to **transmit *and* receive (electrical) signals**.



Data Link Layer

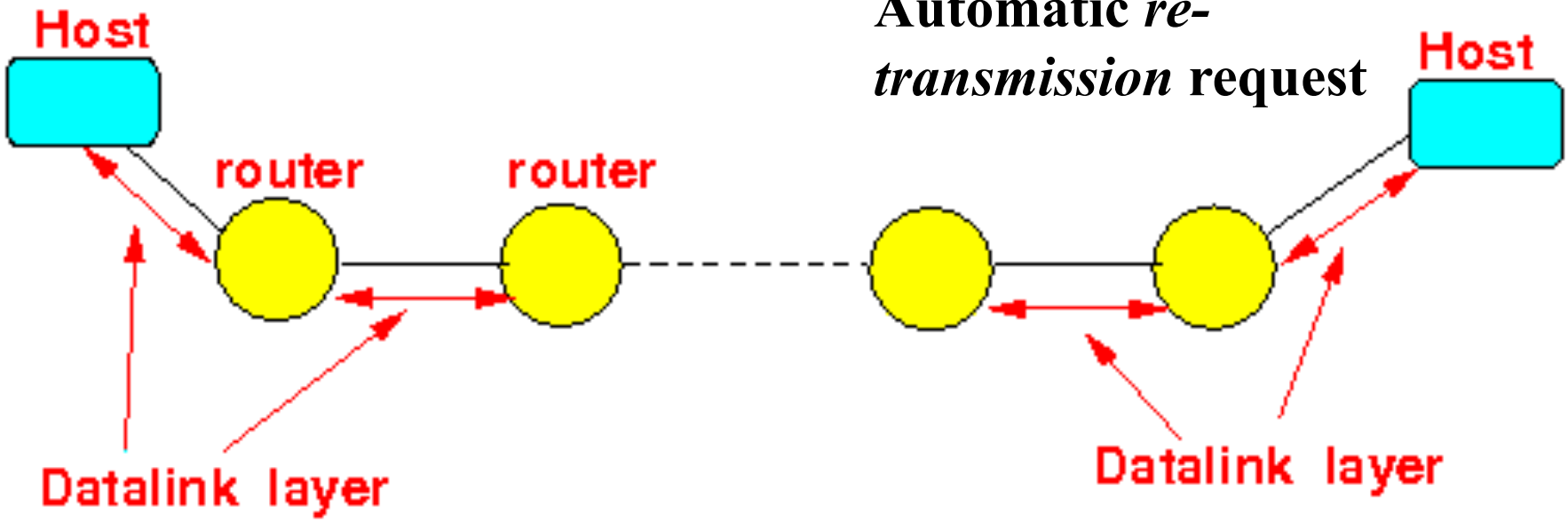
- Physical Layer Provides the basic communication service
- What about multiple access – multiple nodes sharing the same medium
- What is there is any error in transmission
- How to ensure chances of errors are low
- How to ensure reliable data delivery
- Link-layer packets as **frames**.

Datalink layer

The **first software layer**

The **datalink layer ensures** that the **transmitted data** is **received** ***correctly***

Techniques used:
(discussed later in course)
Sequence numbers, error detection/correction (e.g., **checksum**), **Automatic *re-transmission* request**



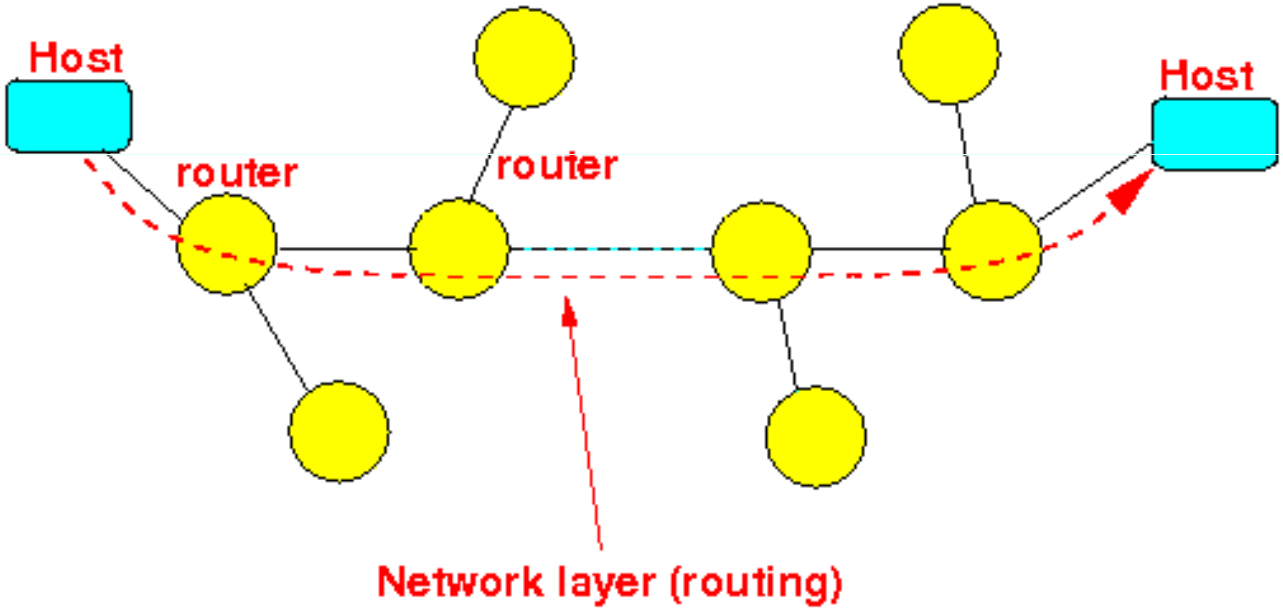
Network Layer

- Data Link Layer allows multiple nearby nodes to communicate with each other
- However, what about when the data needs to travel longer distance from one zone to another zone?
- Moving network-layer packets known as **datagrams** from **one host to another**.

Network layer

- **Determine** the ***next*** **node** to **forward a packet** to its **(final) destination**

•**Topology *discovery***
•**Routing computation** algorithms (e.g., **Shortest Path** (Dijkstra))



Transport Layer

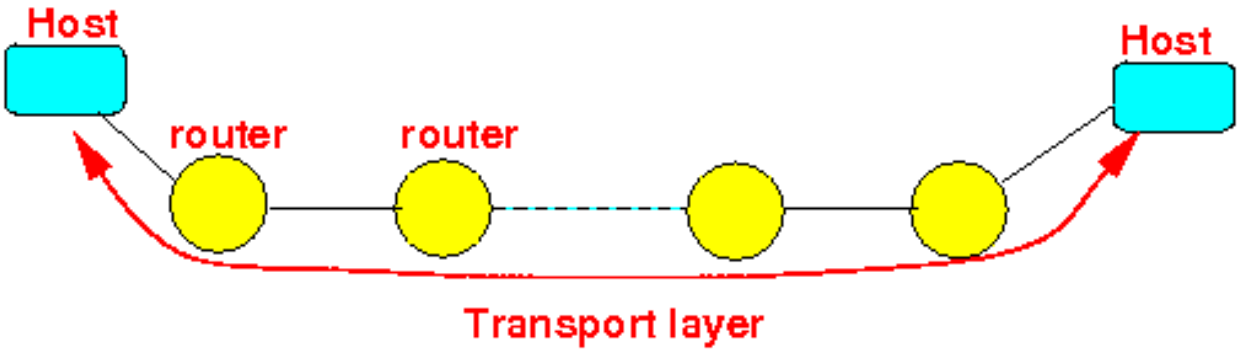
- Network Layer ensures **host to host communication**
- What about there is any errors while switching from one zone to another zone – because of buffer overflow
- Reliable data delivery from one end to another is to be ensured
- Multiple communication between one or more hosts are also necessary to be executed
- **Process to process communication**

Transport layer

Ensure that the **data (packet) transmitted** between the **source** and the **destination node** is **received** ***correctly***

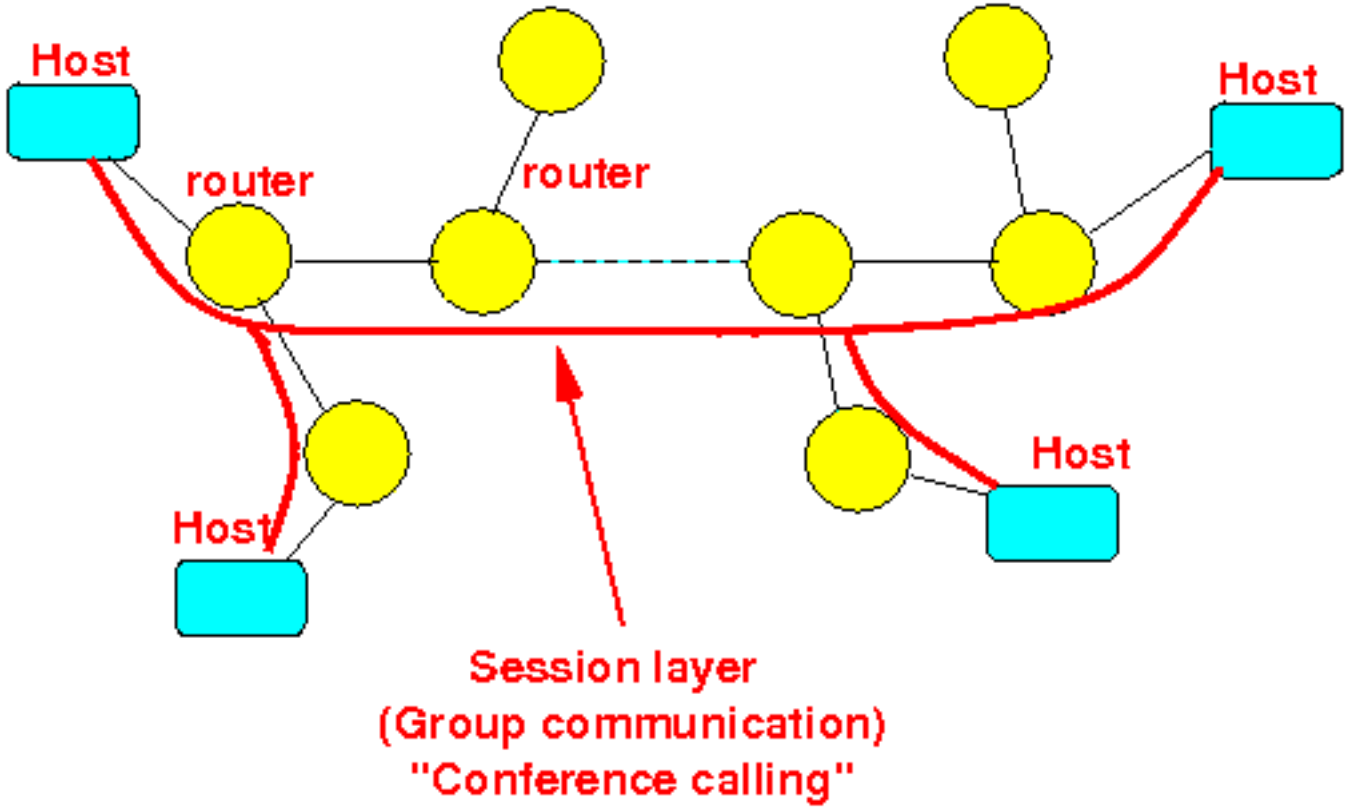
You may have **heard** the term: **TCP/IP**
TCP = the ***Transport*** **Control Protocol** used in the **Internet**

Techniques used: (discussed later in course)
Sequence numbers, error detection/correction (e.g., **checksum**)
Automatic *re-transmission* request



Session layer

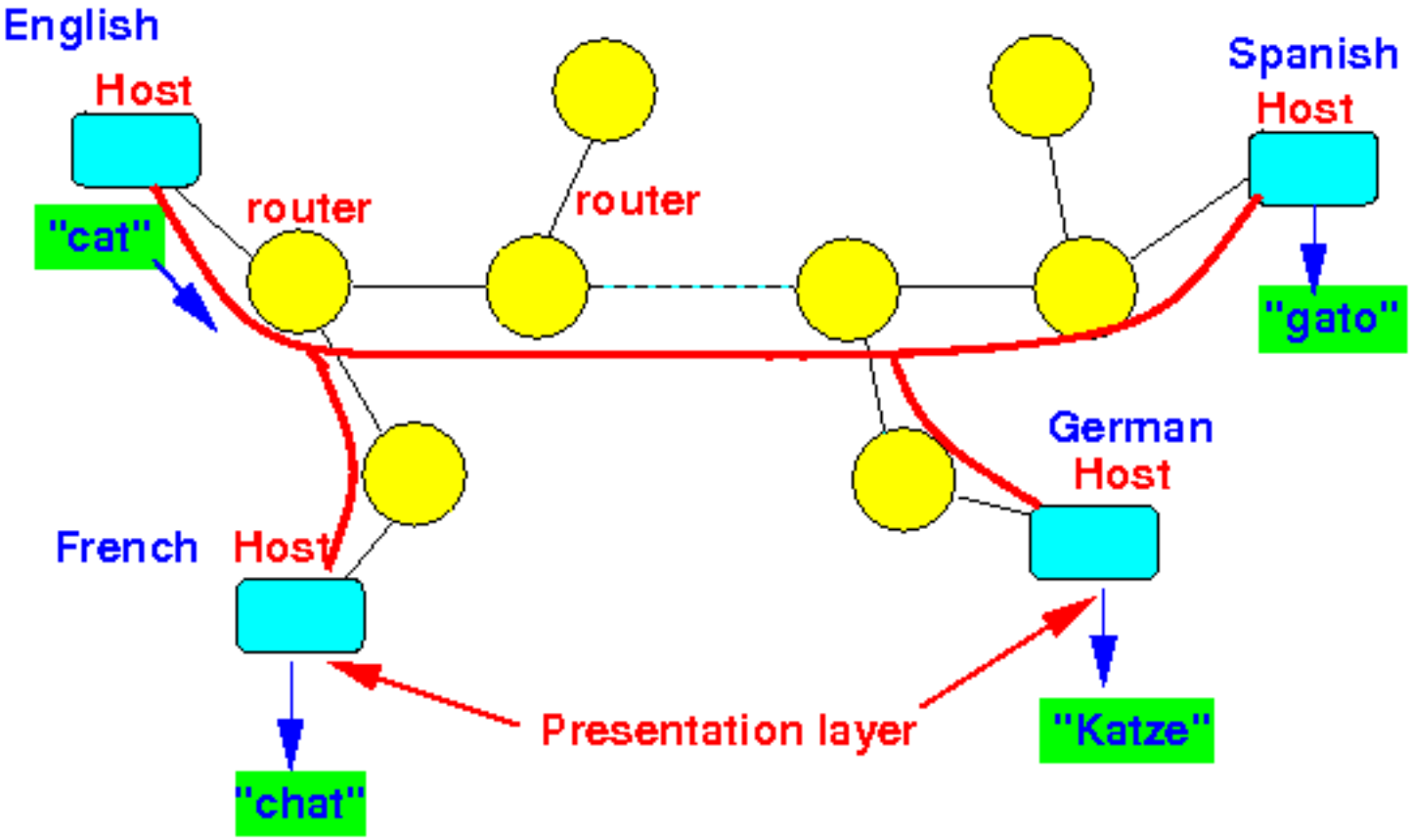
- **manage** the **connections and services** between ***multiple*** **end-points**
- (I.e.: ***group*** **communication** !!!)



Presentation layer

Translation of the **message content** so that it is **suitable** for **consumption** at a ***particular*** **host**

Language translation services:



Application layer

The **application layer** are ***user*** **programs** that **communicate** with **each other**

These **programs** usually implement a **request/reply exchange protocol**

Web service

Email service

Application Layer

- Applications …
- HTTP protocol (which provides for Web document request and transfer),
- SMTP (which provides for the transfer of e-mail messages),
- FTP (which provides for the transfer of files between two end systems).
- Domain name system (DNS).
- Very easy to create and deploy our own new application-layer protocols.

Application Layer

- An application-layer protocol is distributed over multiple end systems, with the application in one end system using the protocol to exchange packets of information with the application in another end system.

- Packet of information at the application layer as a **message**.

The *layers* of the Internet

The **design** of the **Internet** is ***very close*** to **ISO OSI reference model**

First **4 layers** of the **Internet**:

- **Physical**
- **Datalink**
- **Network**
- **Transport**

as ***identical*** to the the **ISO OSI reference model**

The *layers* of the Internet

- **Layers 5**: Was **implemented (later)** around **1994**

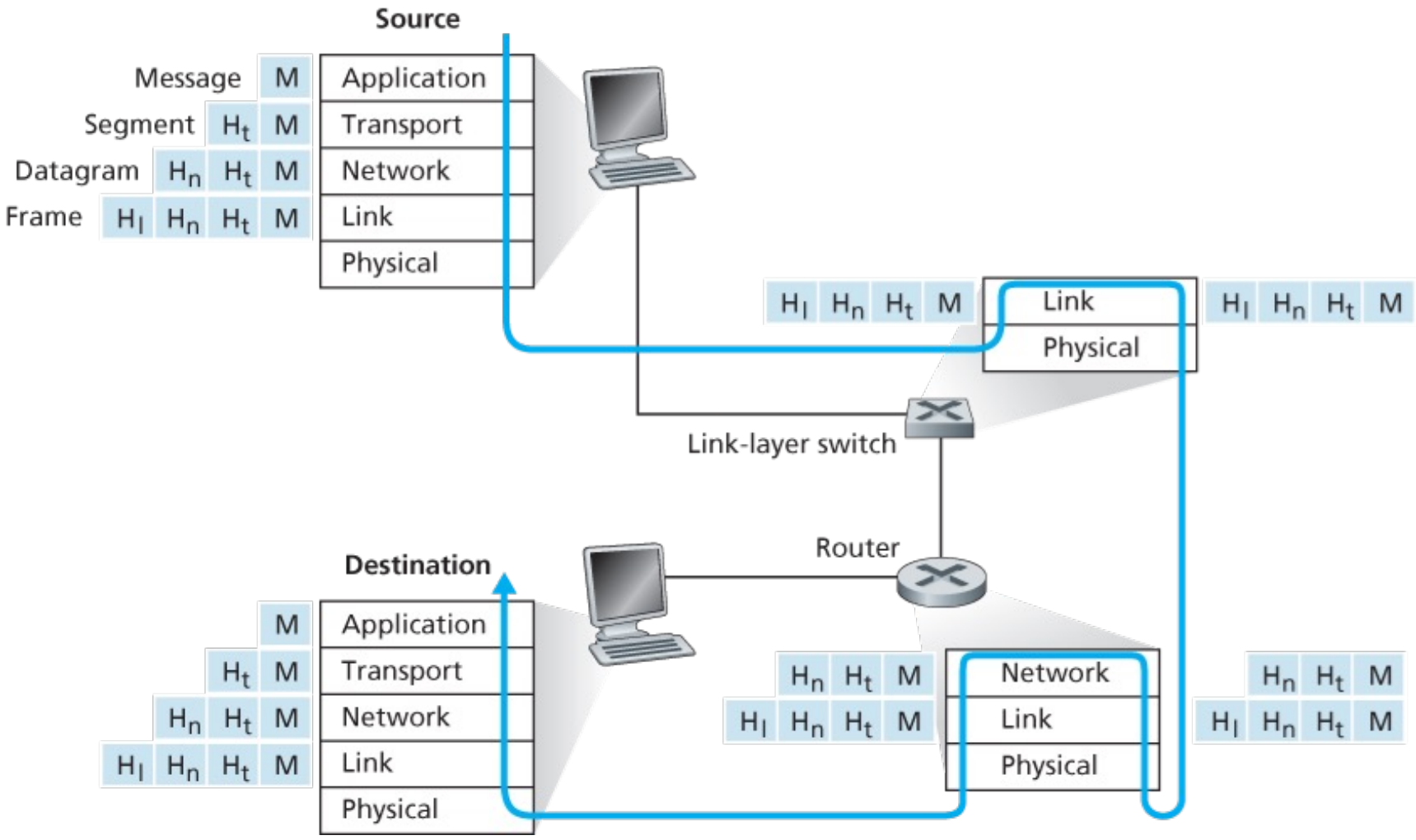
- It's known as the **IP Multicast** service.

- **Layer 6: Presentation Layer -** is **not available**....

- **Layer 7: Application Layer**

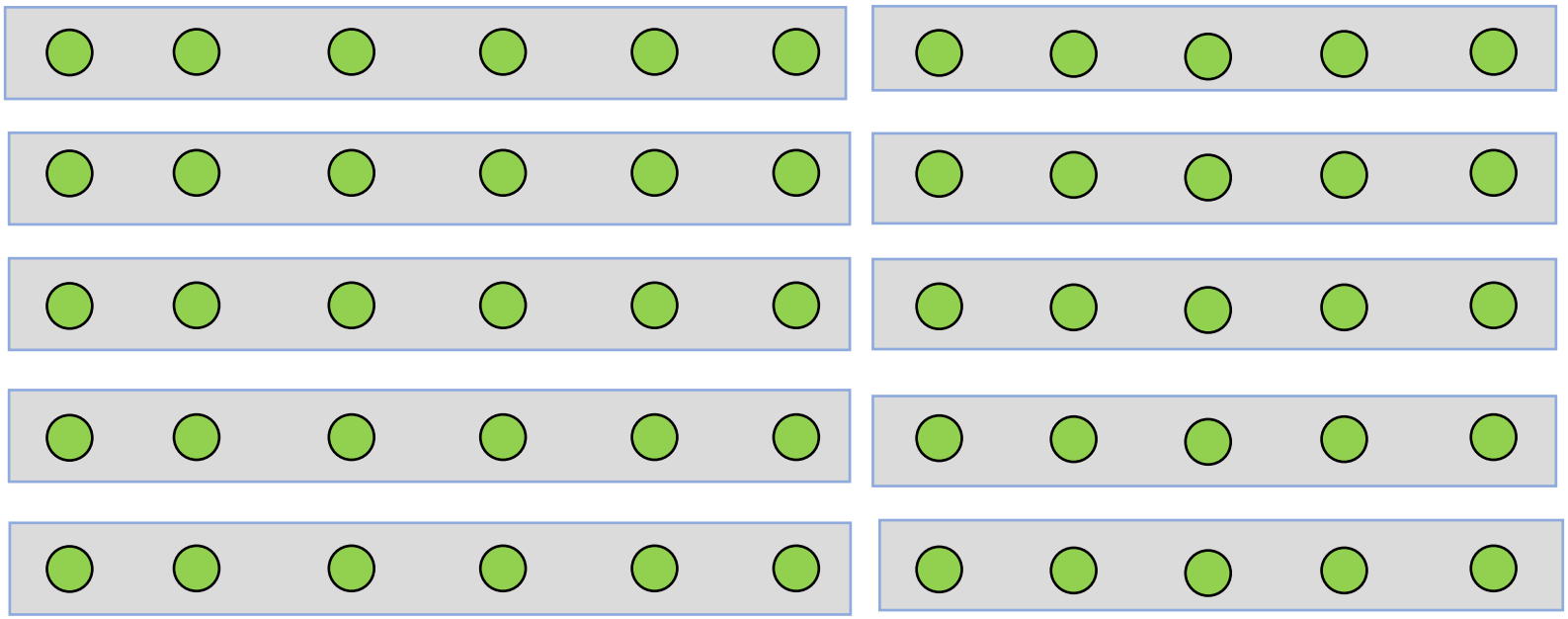
- Specifies the **network applications** is **nothing** more than the **network applications** that **user** develop....

Encapsulation



Example

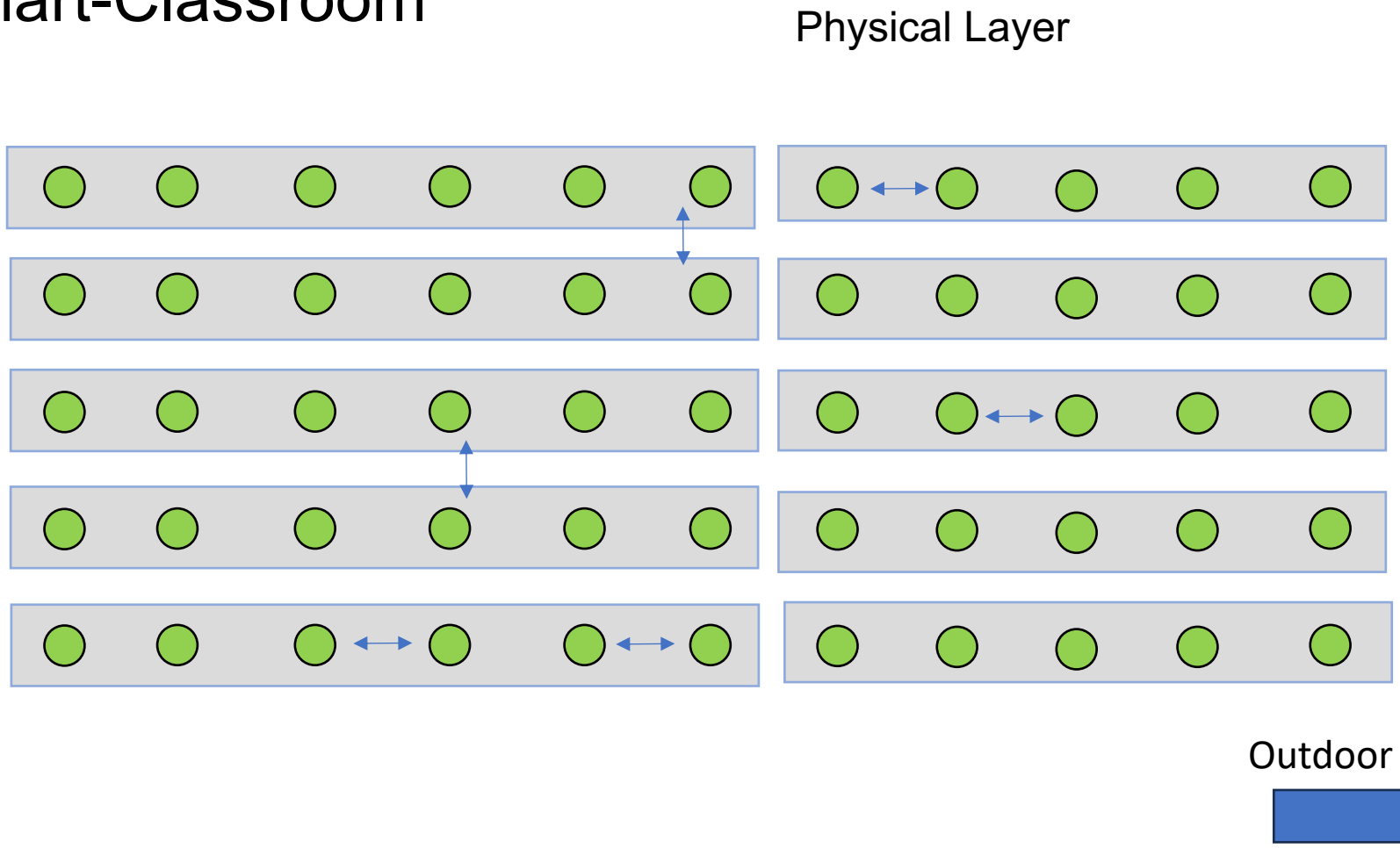
Smart-Classroom



Outdoor unit

Example

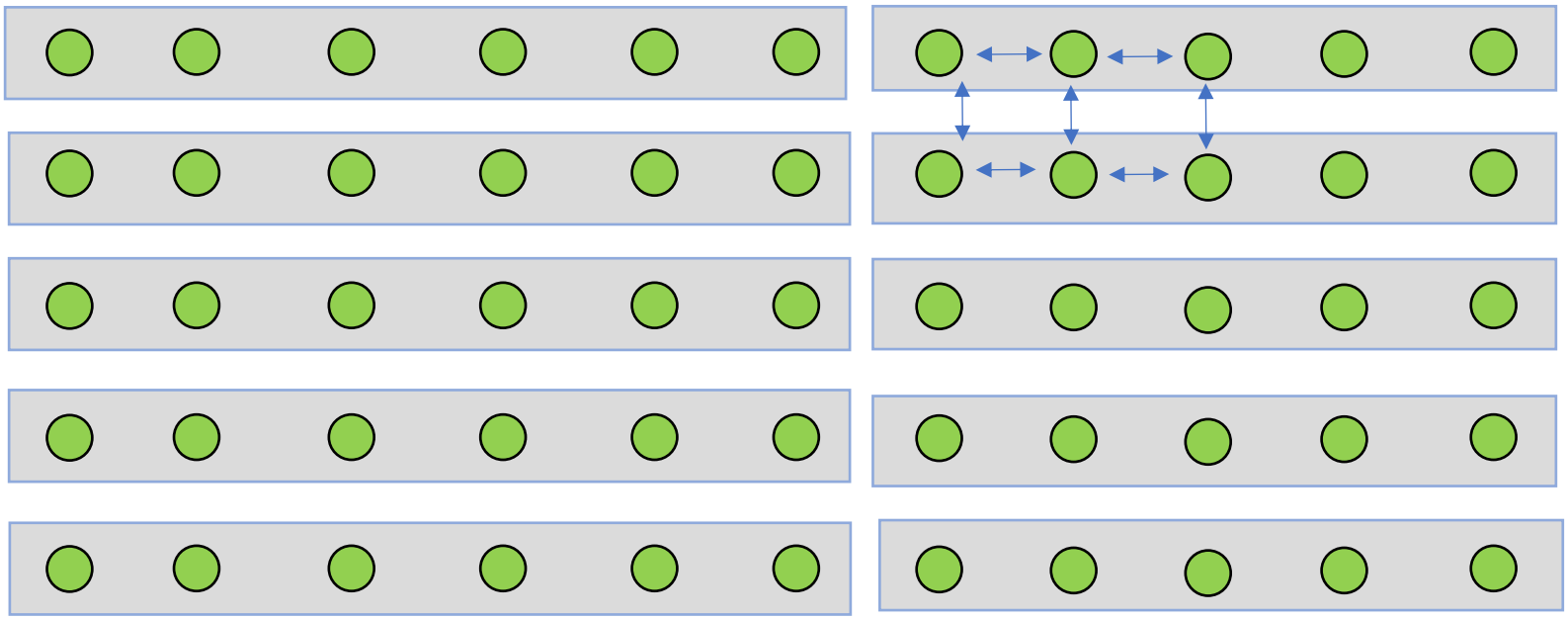
Smart-Classroom



Example

Smart-Classroom

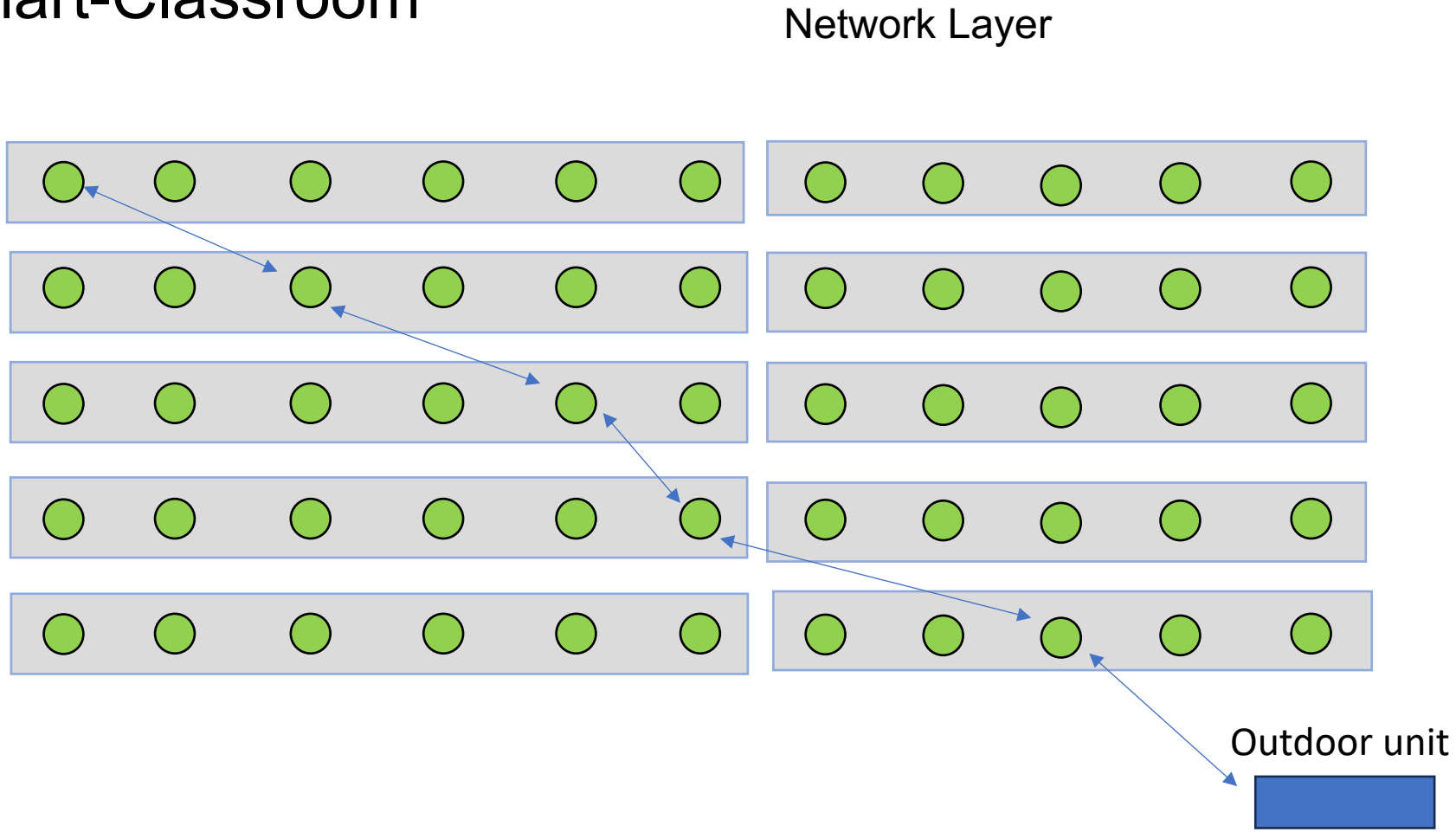
Data Link Layer



Outdoor unit

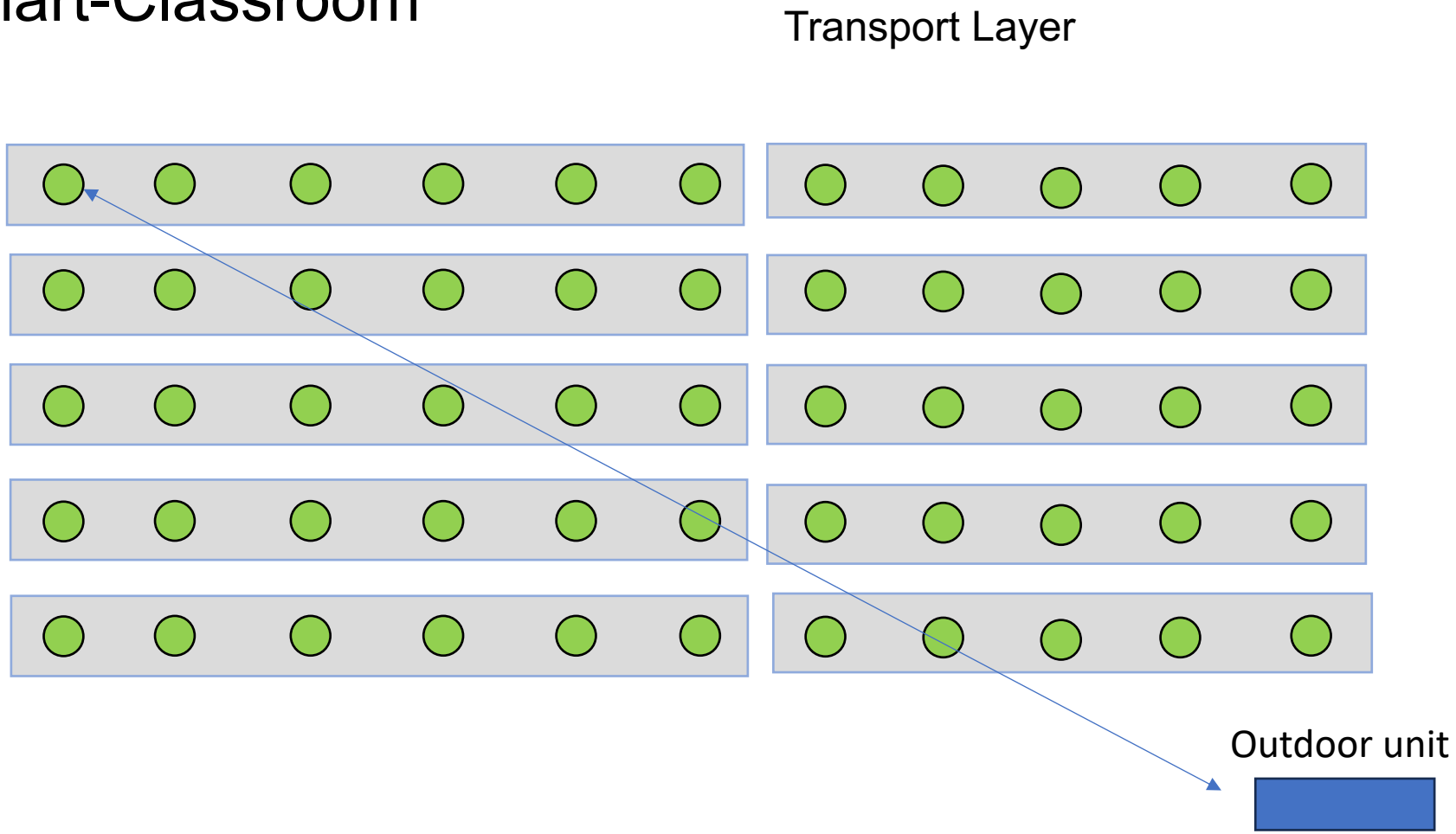
Example

Smart-Classroom



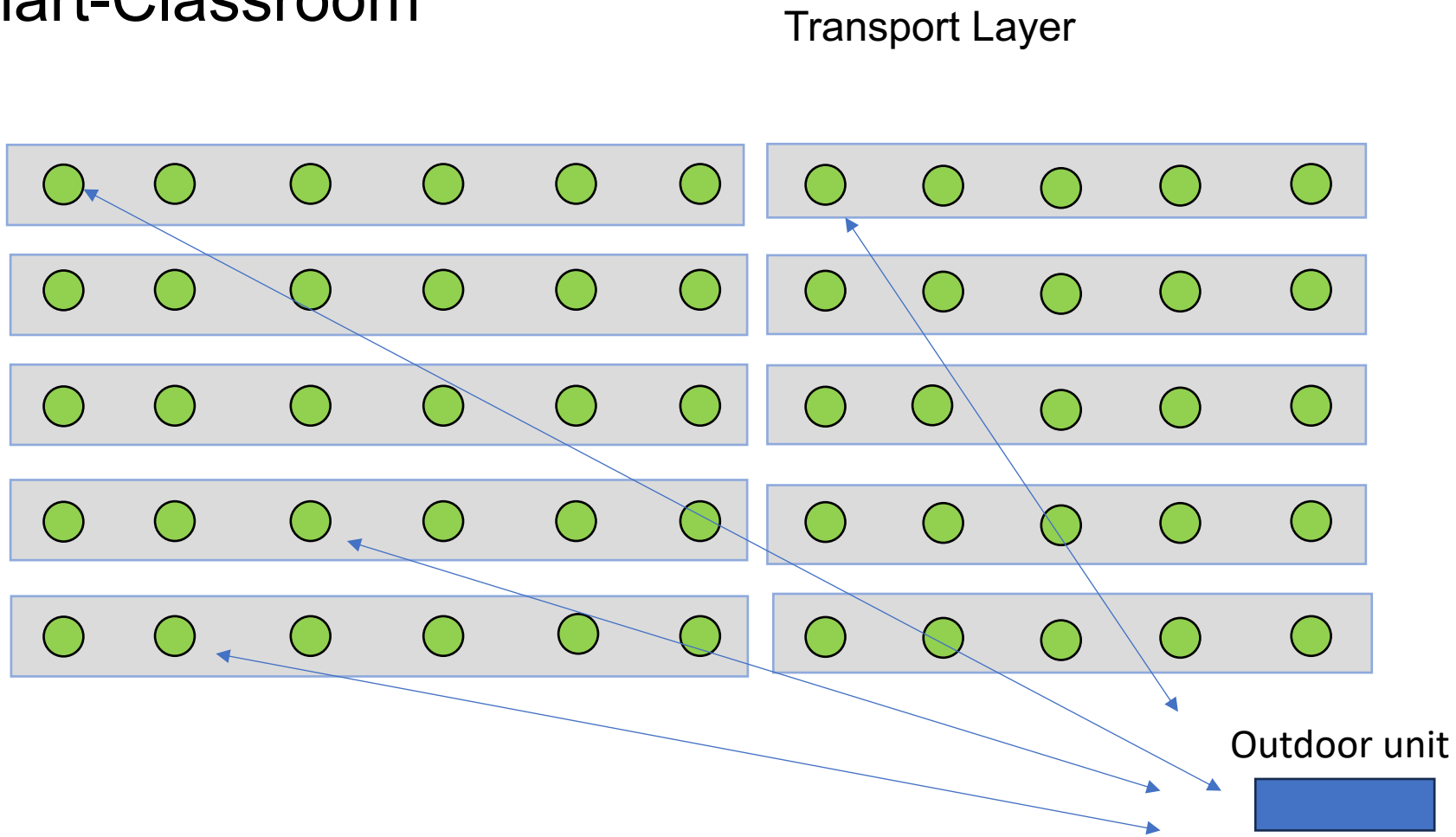
Example

Smart-Classroom



Example

Smart-Classroom



Example

Smart-Classroom