Network Security Contd

Internet Technologies
COMP90007

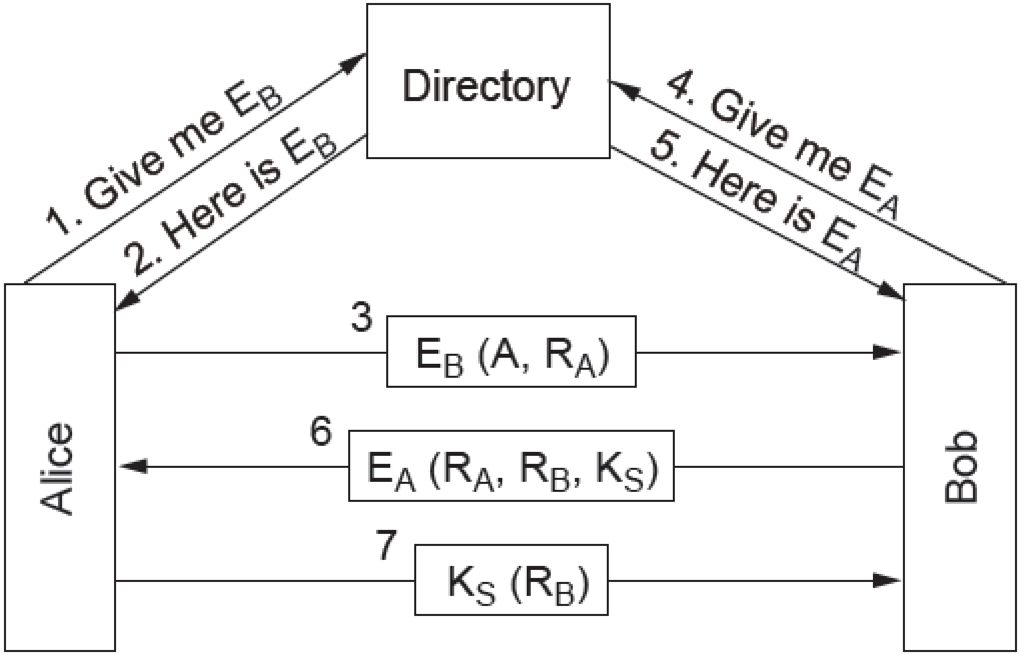
Authentication Using a Key Distribution Center

- In this method, **a trusted intermediary is used** to facilitate
- Users each share a key with a central key distribution centre, and authenticate to the KDC directly
- The KDC acts as a relay between the two parties
- There are issues here as well:
  - Open to **replay-attack**
- Solutions exist to patch the KDC mechanism
  - E.g. timestamps

Authentication Using Kerberos

- Similar to KDC a popular protocol emerged and in frequent use today: Kerberos, e.g. in Windows systems
- In this method, a multi-component system is required
  - Authentication Server
  - Ticket Granting Server (TGS)
  - Recipient
- Authentication is managed centrally, and then **party to party communication is facilitated by single use tickets**
- Still disadvantages remains: Does not scale to large numbers; different businesses need to trust each other’s TGSs…

Authentication Using Public Key Cryptography



IPSec

- But where to put security?
  - Some say application layer: but users may not want such things
  - Some say lower layers: but not as strong as having it at app layer
  - Outcome is **security can/should be in multiple layers**
- One can put security at application level but also…
- **IPSec designed (RFC 2401,..) puts it at the network**
- In the IPSec, **encryption is compulsory, but a null encryption algorithm can be used** between points
- The main IPSec framework features are **secrecy, data integrity, and replay** attack protection
- The IPSec framework allows multiple algorithms and multiple levels of granularity,… connection-oriented (**connections are named as SA's, security associations**)

IPSec Implementation

- IPSec has two main implementation components
  - Things being added to packets in transit
  - ISAKMP key management: Internet Security Association and Key Management Protocol for establishing keys

- IPSec has 2 modes
  - Transport mode - uses header insertion after IP Header
  - Tunnel mode - uses packet encapsulation

Virtual Private Networks

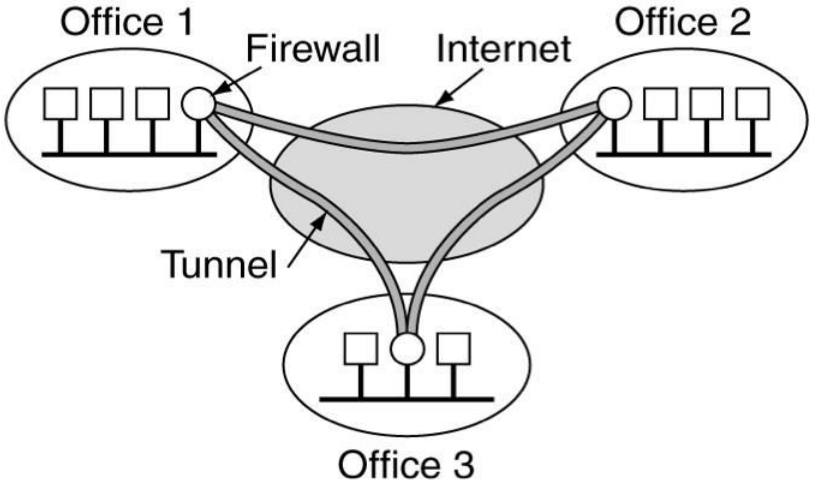
- Unlike a physical network based on leased lines between locations for which secure transit is required

- A Virtual Private Network (VPN) is **a virtual layer on top of an IP network which provides a secure end-to-end connection** over public infrastructure

- A common VPN implementation model:
  - **Use a firewall at each end of a connection**
  - Setup a **SA to create an IPSec tunnel between the two end points**
- Communication on this infrastructure is **transparent to end users**

VPN

A virtual private network



Firewalls

- While IPSec ensures security in transit, a **firewall ensures security at the network perimeter**
- Firewalls are positioned at the network boundary, and **provide a controlled series of routes between the internal and external networks**
- Three characteristics of firewalls
  - All inbound and outbound traffic must transit the firewall
  - Only authorised traffic must pass through the firewall
  - Firewalls should be immune to penetration themselves

Firewall Scope

- Check packets for “bad” packets
  - Administrators can **write rules for this**, e.g., distinguish regular HTTP from P2P related HTTP
- **Not everything is inside the wall**
- Web servers and email servers etc **need to be exposed to allow more open communication**
  - Best firewall is NOT disconnecting everything from the Internet
- Through **further rules packets go in-between this gray area and the LAN**
- Firewalls dont provide protection against inhouse threats
- Applications can still distribute viruses (via bad attachments for example)

Wireless Security Context

- Wired networks are relatively easy to secure because they require physical access to intercept traffic at times
- Wireless networks are more difficult to secure because of **omnidirectional signal propagation**
- Additionally by default **most wireless network equipment operates in an insecure and promiscuous manner**
- 802.11 has a native secure protocol, **Wired Equivalency Protocol** (WEP), which is a 40-bit encryption based on RC4 algorithm

Wireless Security Issues

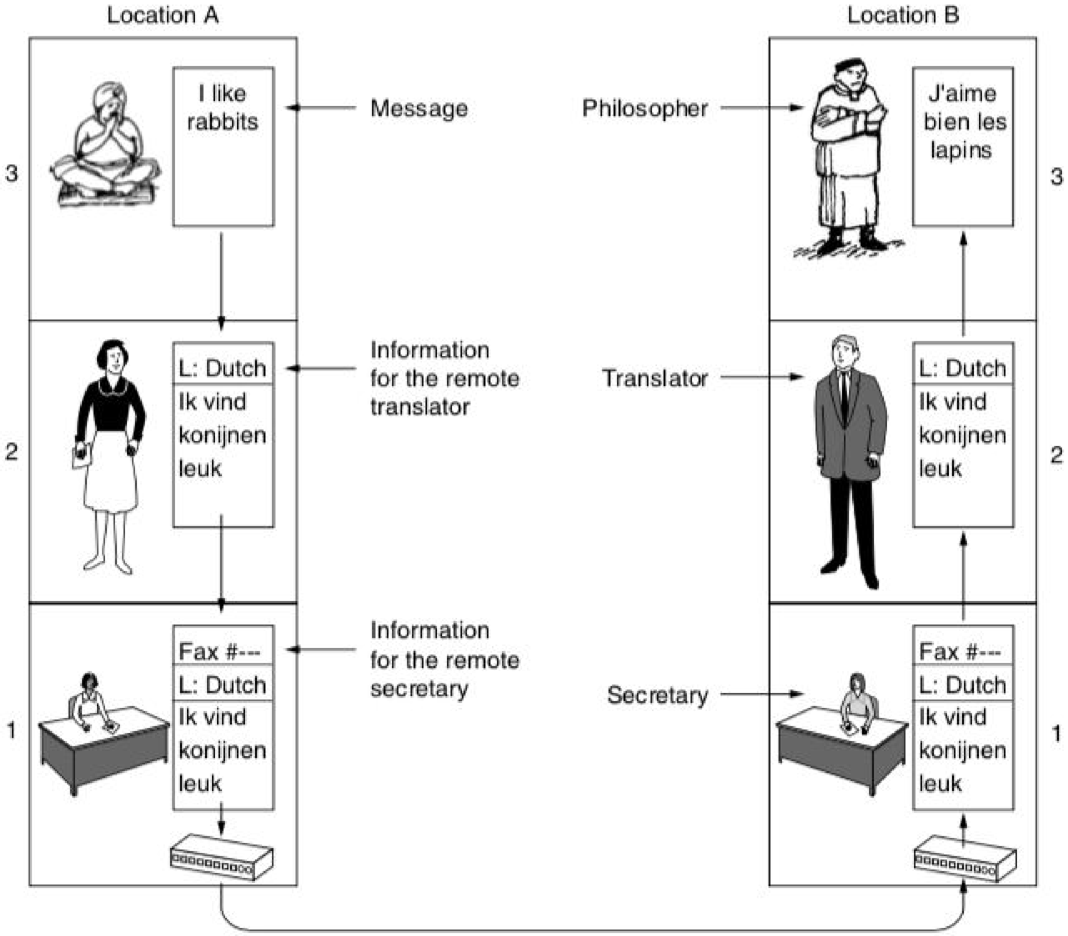
- Two inherent insecurities
  - 40 bit encryption is breakable with low-moderate computational resources
  - RC4 re-uses keys, so capturing a small volume of encrypted traffic will guarantee key identification
- Given these constraints, how can wireless networks be secured?

Securing Wireless

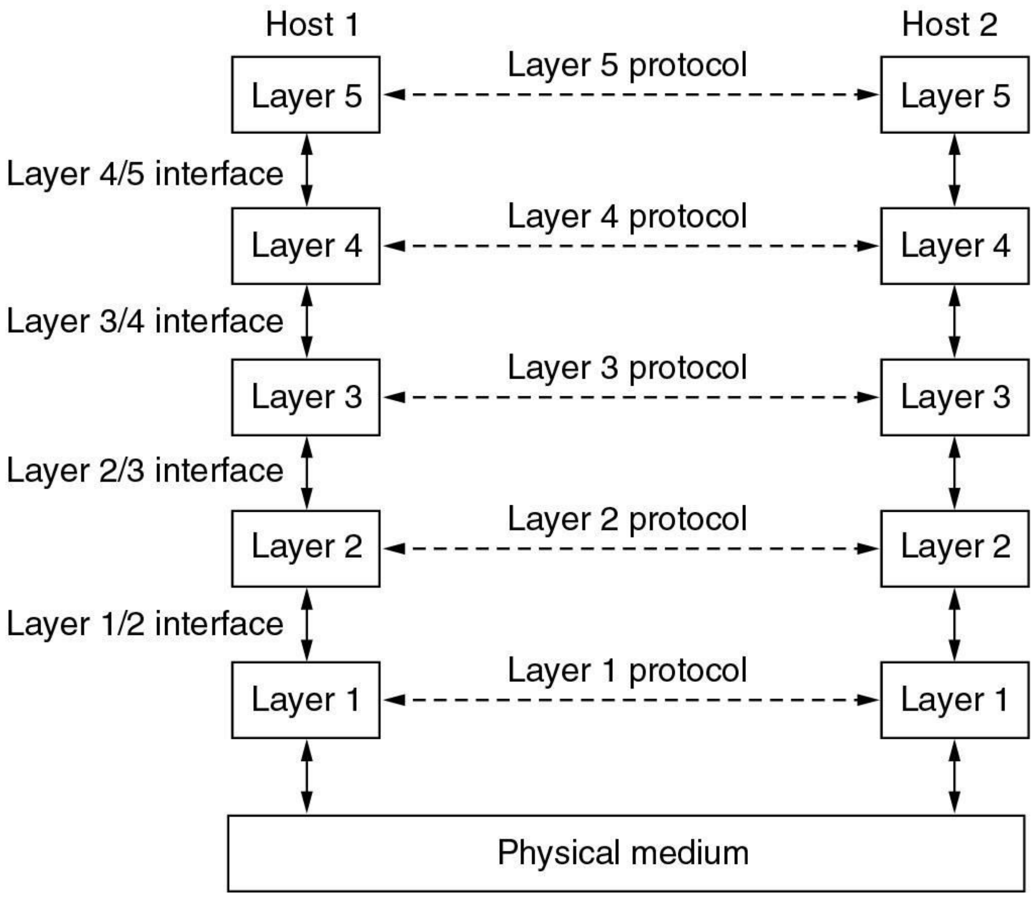
- Additional encryption (128bit WEP)
  - Increased security through longer key lengths
- MAC Address Filtering
  - Only allow specified MAC interfaces to establish connections
- …
- WPA2 (WiFi Protected Access 2)
- …
- Multilayered security
  - Use a VPN over wireless
- Hot area of study…

Internet Technologies: Putting Things Together

The Philosopher Architecture



How is Network Software done

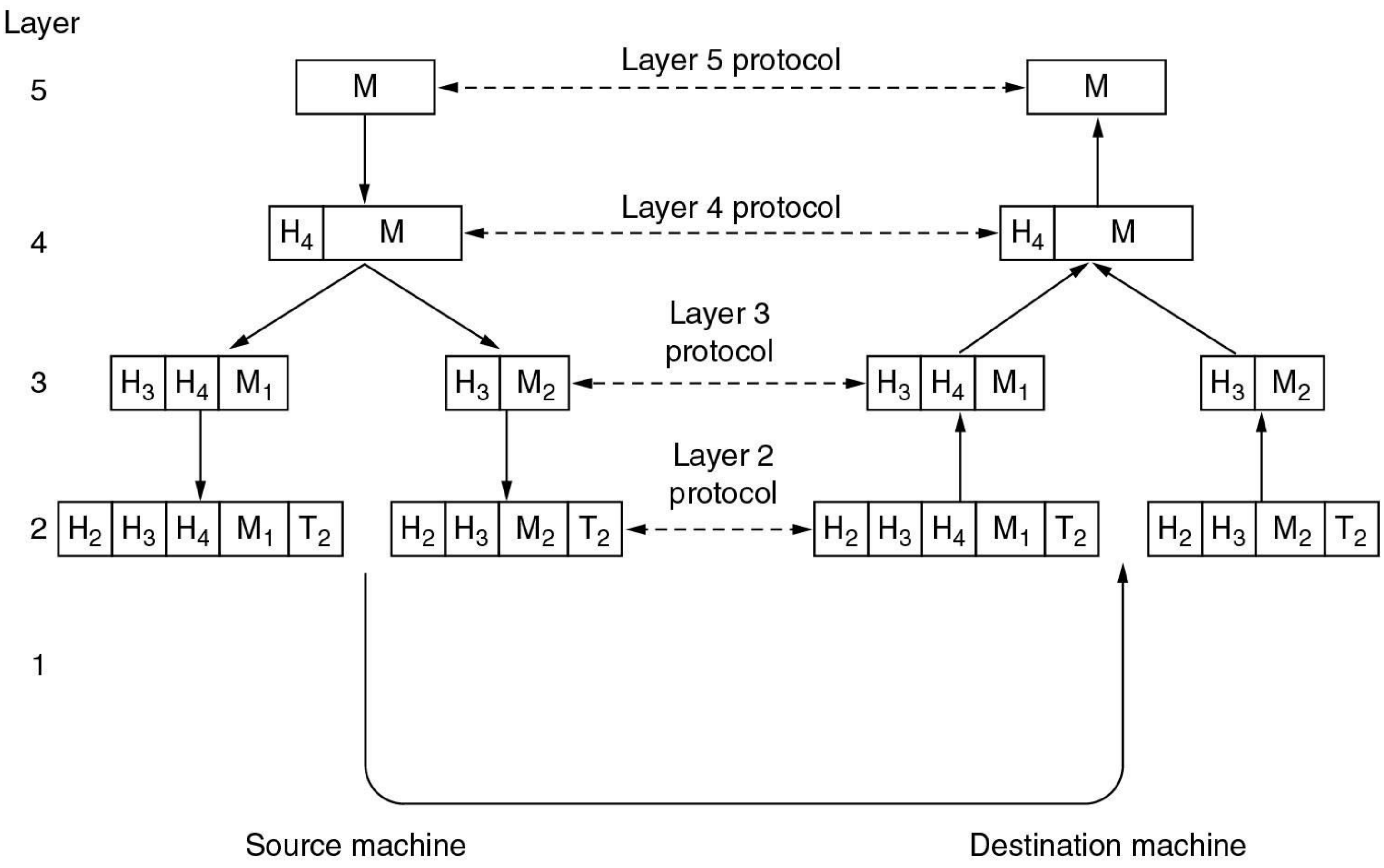


Consider the network as a stack of layers

Each layer offers services to layers above it

Inter-layer exchanges are conducted according to a protocol

What happens to a Message then…



Going from Bottom to Top: Physical Layer First

Many mediums can be used for data transfer with each having its own benefits and disadvantages

Property	**Wires**	**Fiber**
Distance	Short (100s of m)	Long (tens of km)
Bandwidth	Moderate	Very High
Cost	Inexpensive	More Expensive
Convenience	Easy to use	Harder to use
Security	Easy to tap	Hard to tap

Next Layer Up: Data Link Layer

Does a lot of work that we covered such as:

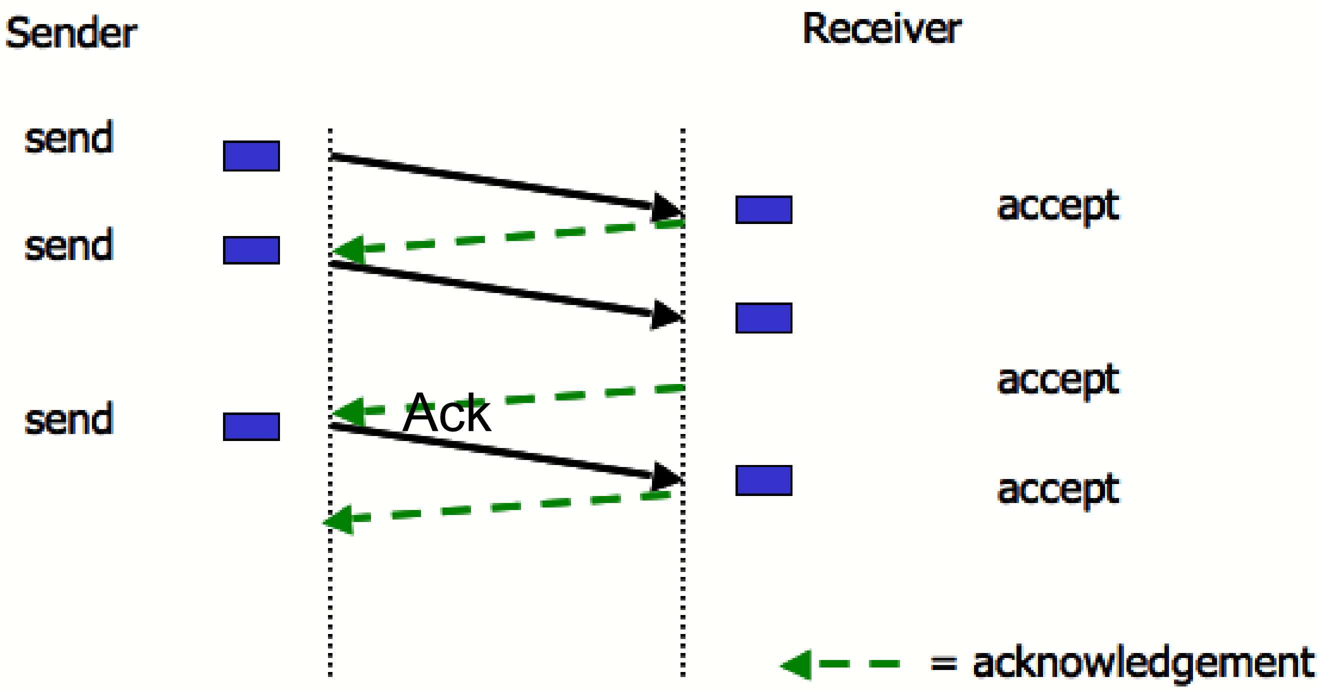
1. Handling transmission errors
2. Data flow regulation
3. …

- Take **packets from network layer**, and encapsulate them **into frames** (containing a header, a payload, a trailer)

Key topics had: Error Control

- Ensuring that a garbled message by the physical layer is not considered as the original message by the receiver by adding check bits
- Error Control deals with
  - **Detecting** the error
  - **Correcting** the error
  - **Re-transmitting** etc if need be..

We also Did a lot of Flow Control



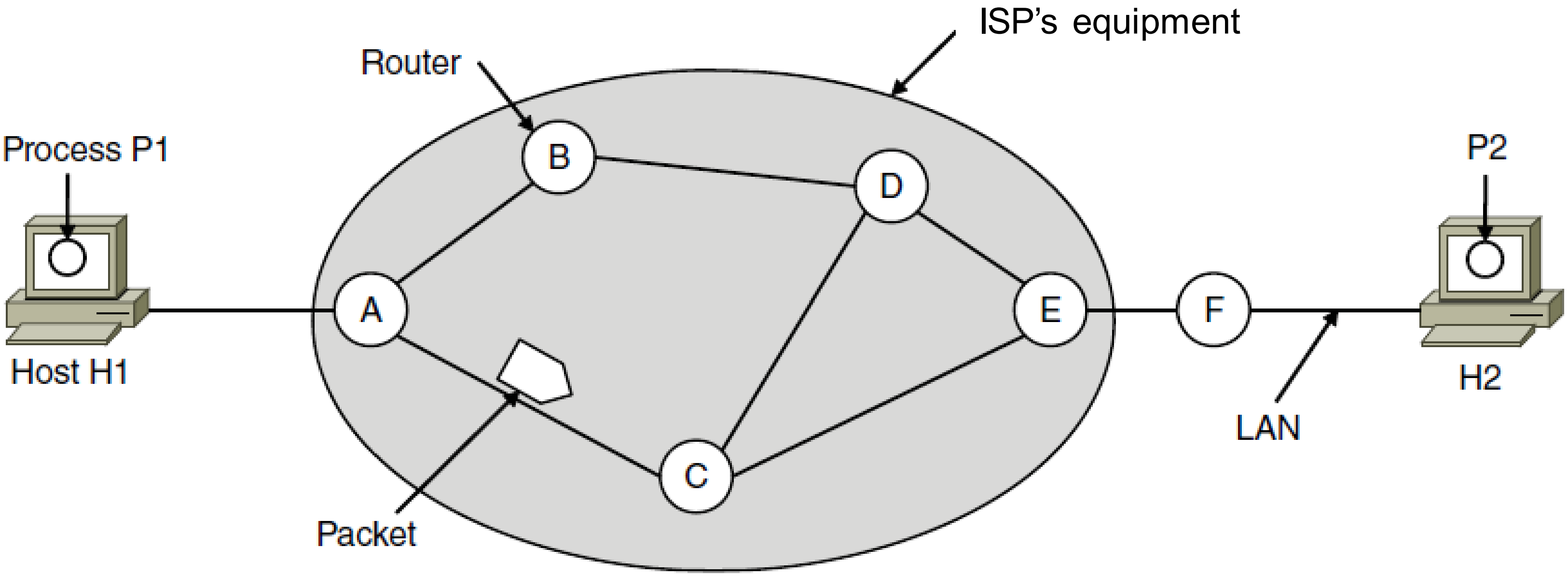
In the middle: MAC Layer

- ALOHA
- Carrier Sense Multiple Access
- Collision Free
- Limited Contention
- MACA

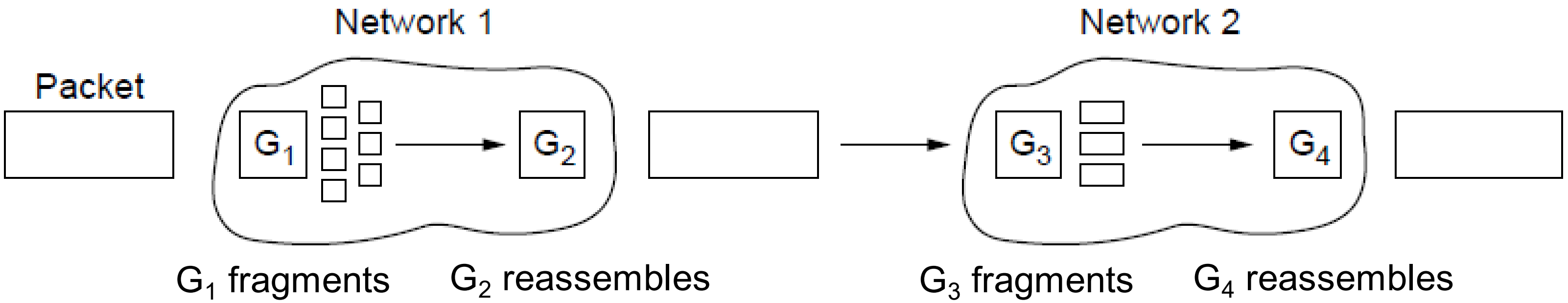
… many algorithms here…

Going higher up: Network Layer

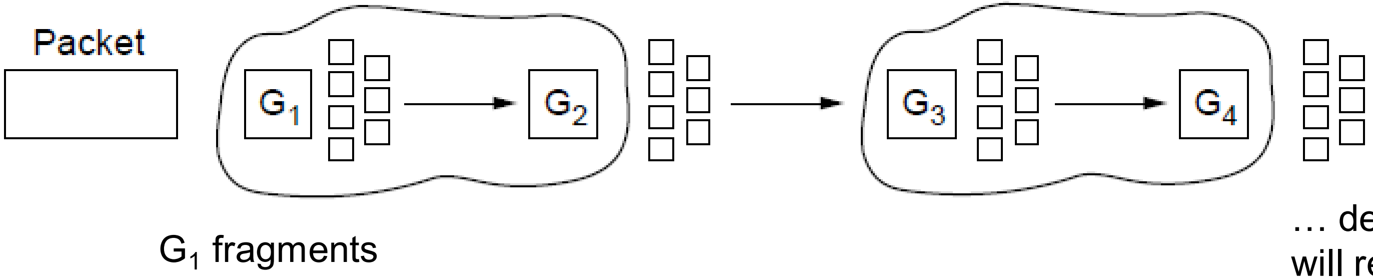
- Hosts generate packets and injects into the network
- Routers deal with packets, receiving (storing) them and then forwarding them based on how they are addressed
- **<u>Router routes packets through the network</u>**



This Layer does other things too: E.g. Fragmentation



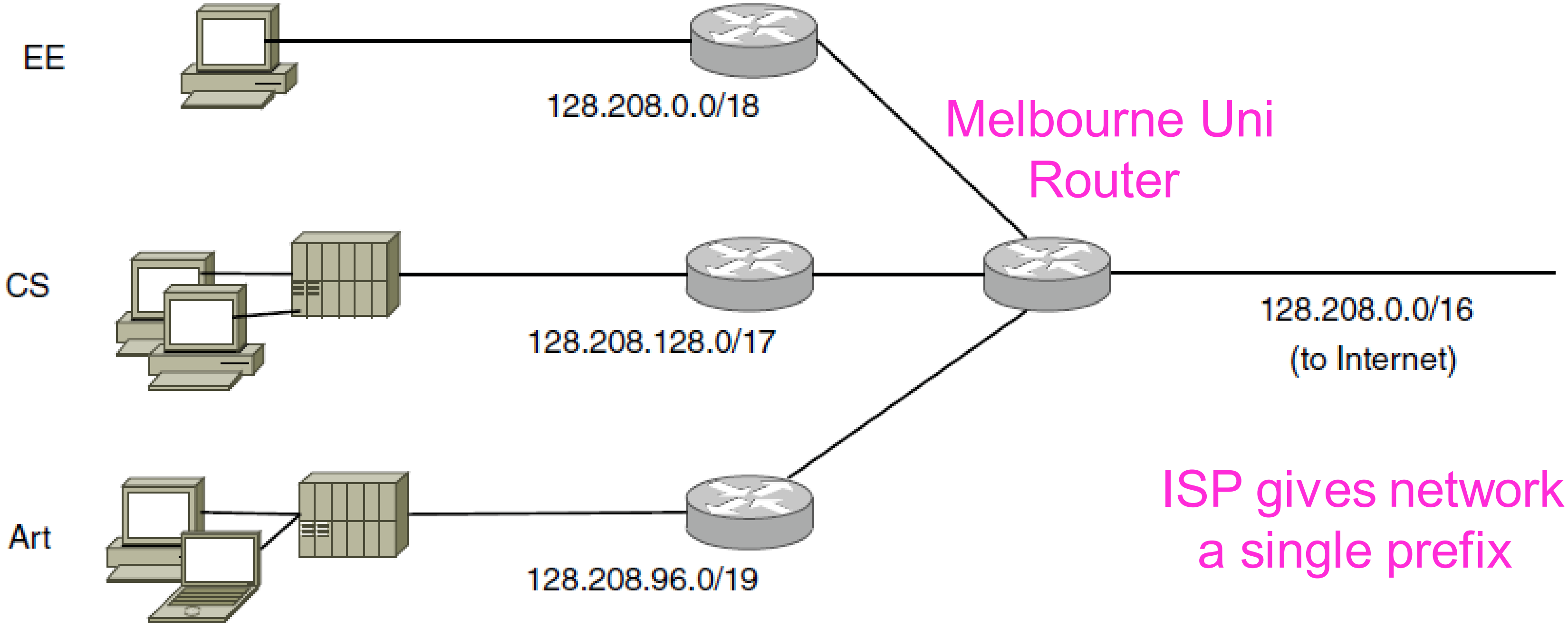
Transparent



… destination
will reassemble

Non-transparent

Also does Addressing…



ISP gives network a single prefix

Network divides it into subnets internally

Next Layer: Transport Layer

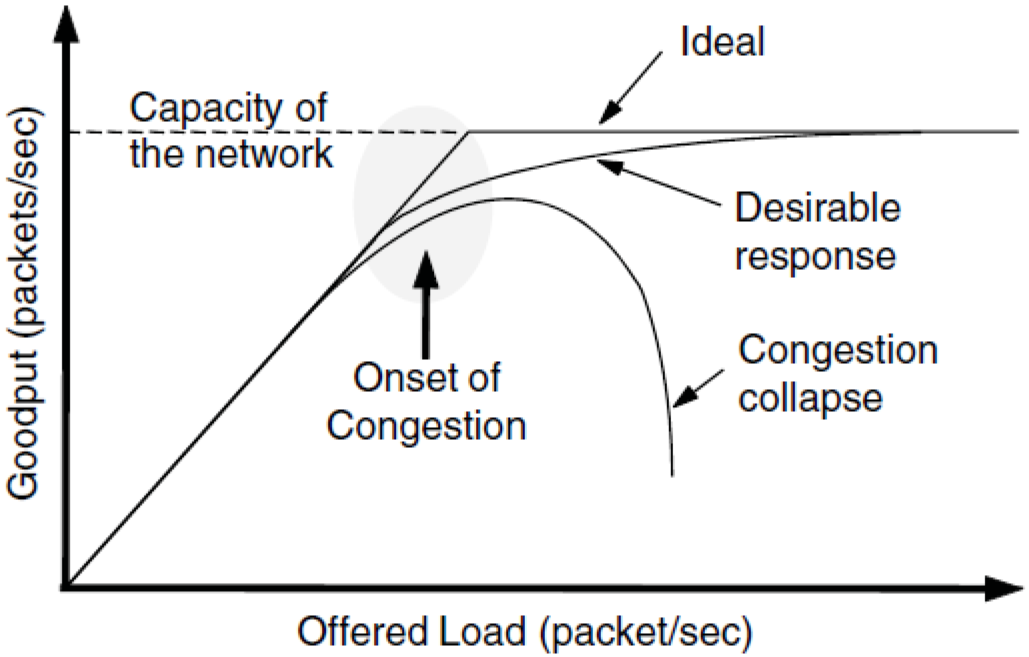
- Provide **efficient, reliable & cost-effective data transmission service to the processes in the application layer…independent** of physical or data networks

Programming on a Network

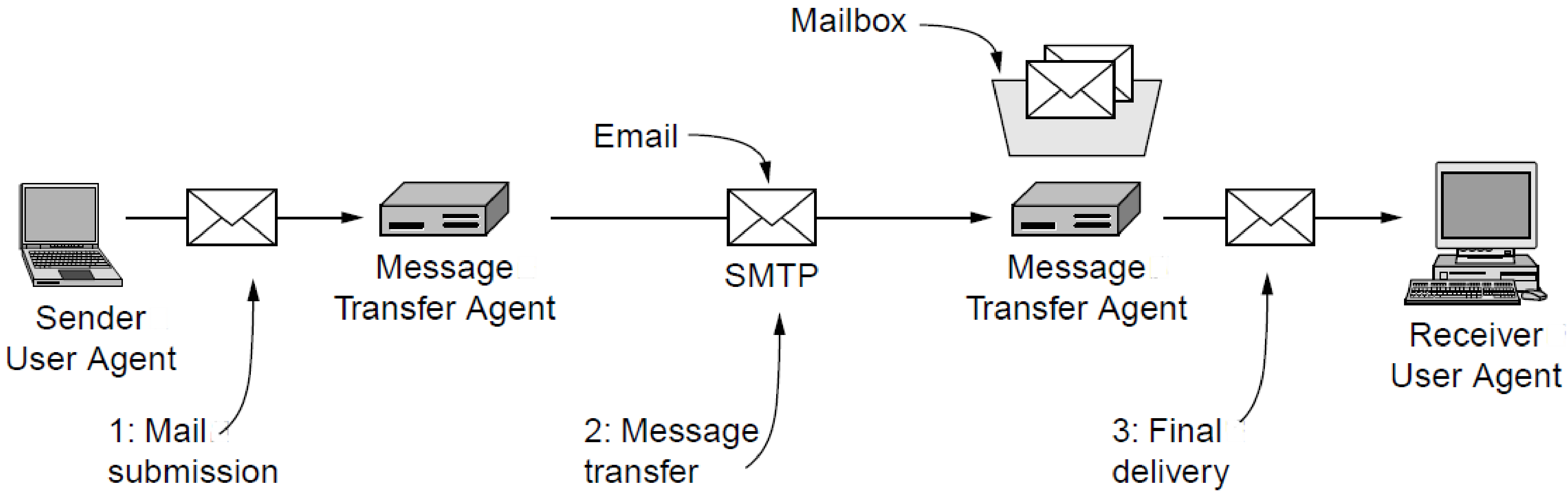
```
ServerSocket serverSocket = new ServerSocket([parameters]);

While (true) {
        ….
```

NO NEED TO KNOW HOW TO WRITE A WHOLE PROGRAM BUT NEED TO UNDERSTAND THE BASICS…

A Separate Topic from Network + Transport Layers: What happens in congestion?



Application Layer by Examples: Email etc



Special Topic: Network Security

- Network security is a combo of related areas:
  - **Secrecy**
  - **Authentication**
  - **Non-repudiation**
  - **Integrity control**

Modern Key-based Algorithms

- **Two main categories**

- Symmetric key
- Public key

Also…

- **Do not forget to check out missing layers and guest lectures…**

Exam Logistics

- Everything included in the exam but focus is on things that we spent more time…
- Basic info about exams such as dates etc are already available from the Uni, please check
- Exam runs like an online assignment. You will be able to see the exam at the exam date/time and need to submit a file at the deadline.
- The exam is similar to our tutes/assignments in style.
- You will be able to use your preferred text editor to write your answers on your machine during the exam period for this subject. Mostly you will be required to use simple editing functions of your editor.
- During the exam you potentially will have materials with you such as the book etc: General advise on this is --- having calculators and other materials will not help much and that these are not key to have a successful exam for this subject. In fact if you need say a calculator, it is a sign that you may even be on the wrong track. Browsing advanced books on networking will also not going to be of much use for this exam during the exam. If you spend a lot of time browsing a lot of content for finding answers, you will likely lose precious time and likely not find an answer in a book. It is best to study this exam as if it is a classical exam in our view.
- Once you are done with the exam, you will need to upload a PDF version of your answers.
- There will be means to get help technical or otherwise during the exam.
- Until the exam please join/monitor discussion forums and announcements from LMS.