Week 12: Revision Lecture

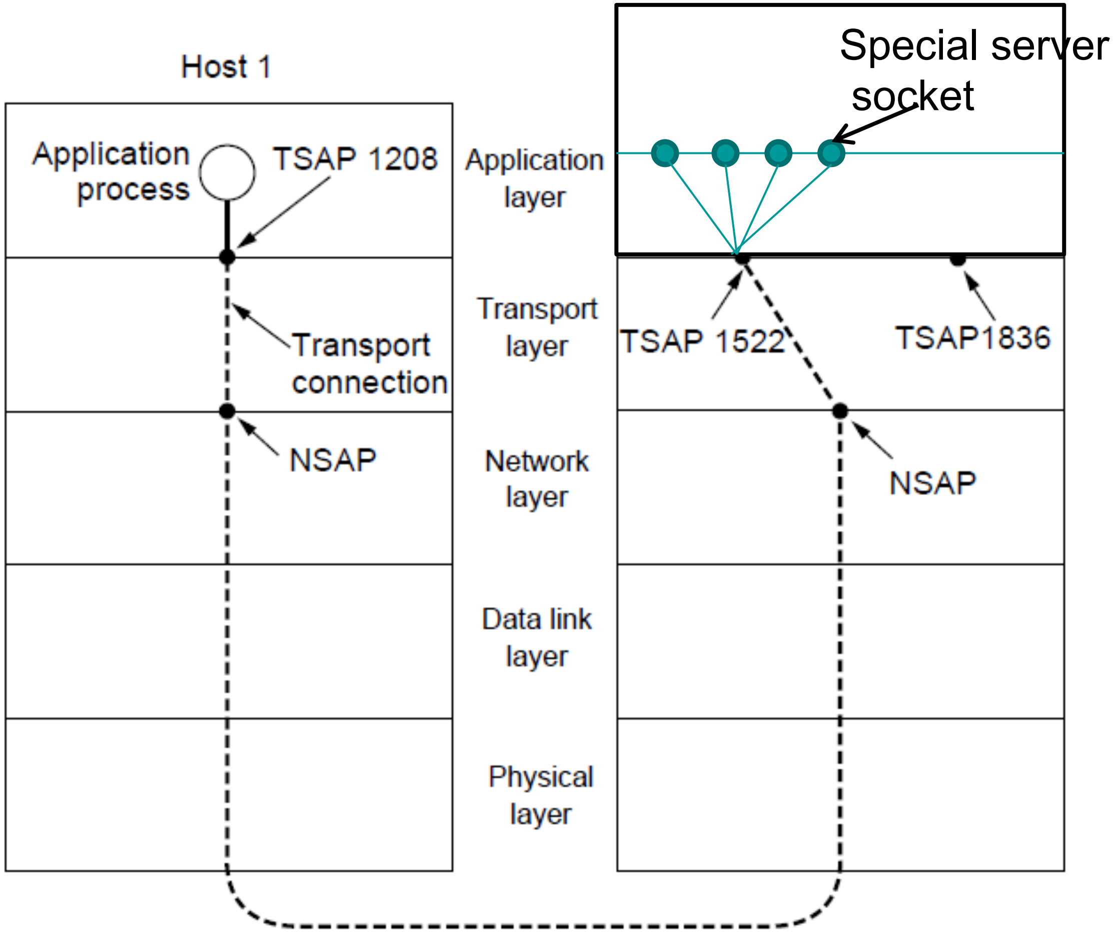
Internet Technologies COMP90007

Lecturer: Muhammad Usman

Semester 2, 2020

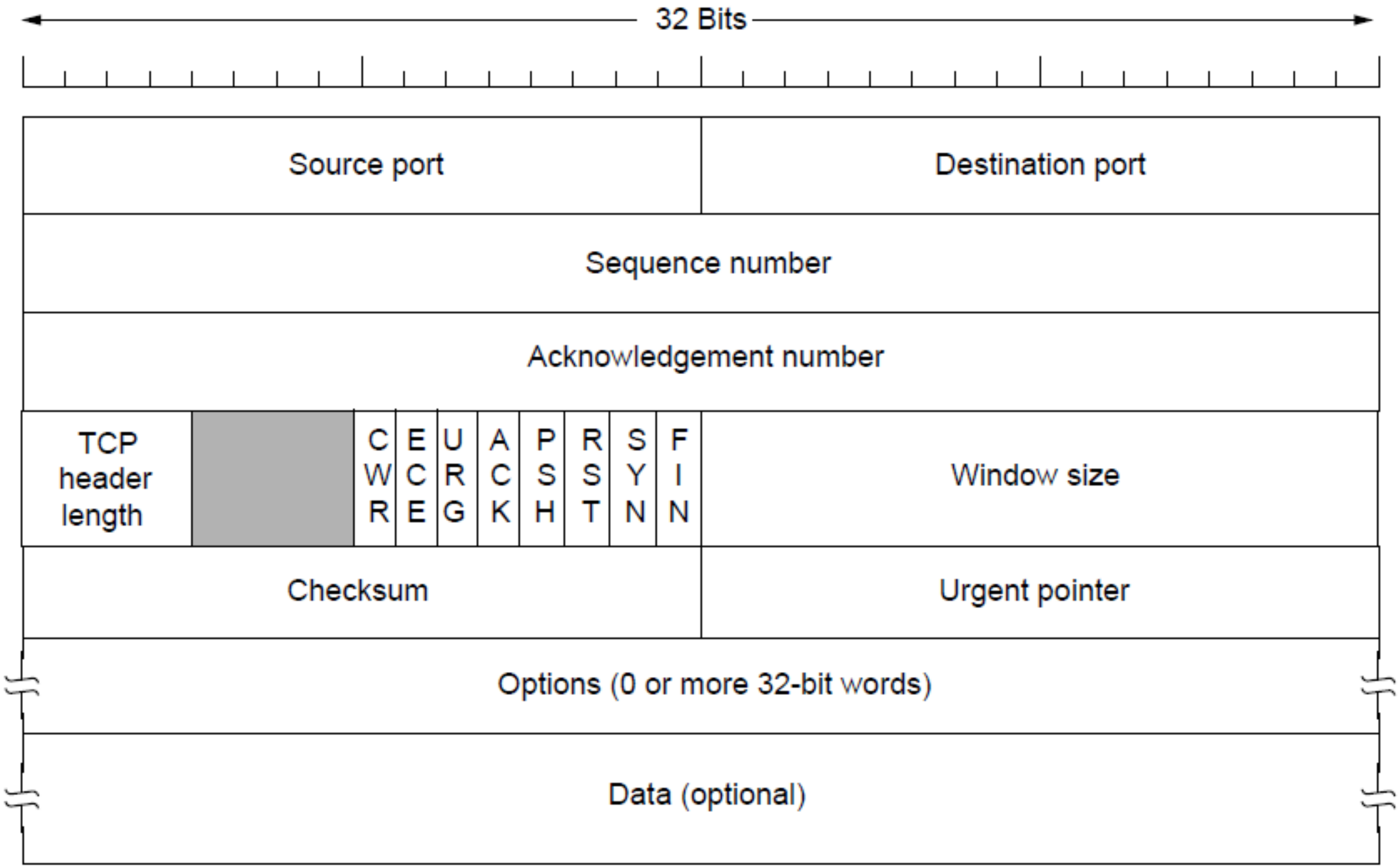
Addressing at Transport Layer

- Socket library provides a multiplexing tool on top of TSAPs to allow servers to service multiple clients
- It simulates the server using a different port to connect back to the client



TCP Segment Header

- TCP header includes addressing (ports), sliding window (seq. / ack. number), flow control (window), error control (checksum) and more



32 Bits

Source port

Destination port

Sequence number

Acknowledgement number

TCP header length

CWR

ECE

URG

ACK

PSH

RST

SYN

FIN

Window size

Checksum

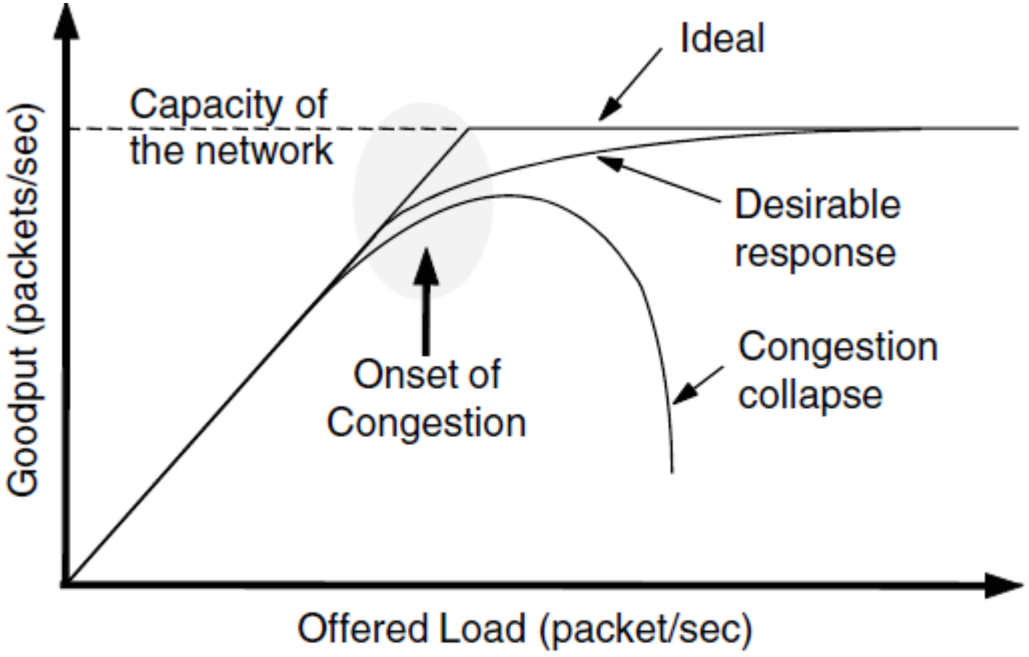
Urgent pointer

Options (0 or more 32-bit words)

Data (optional)

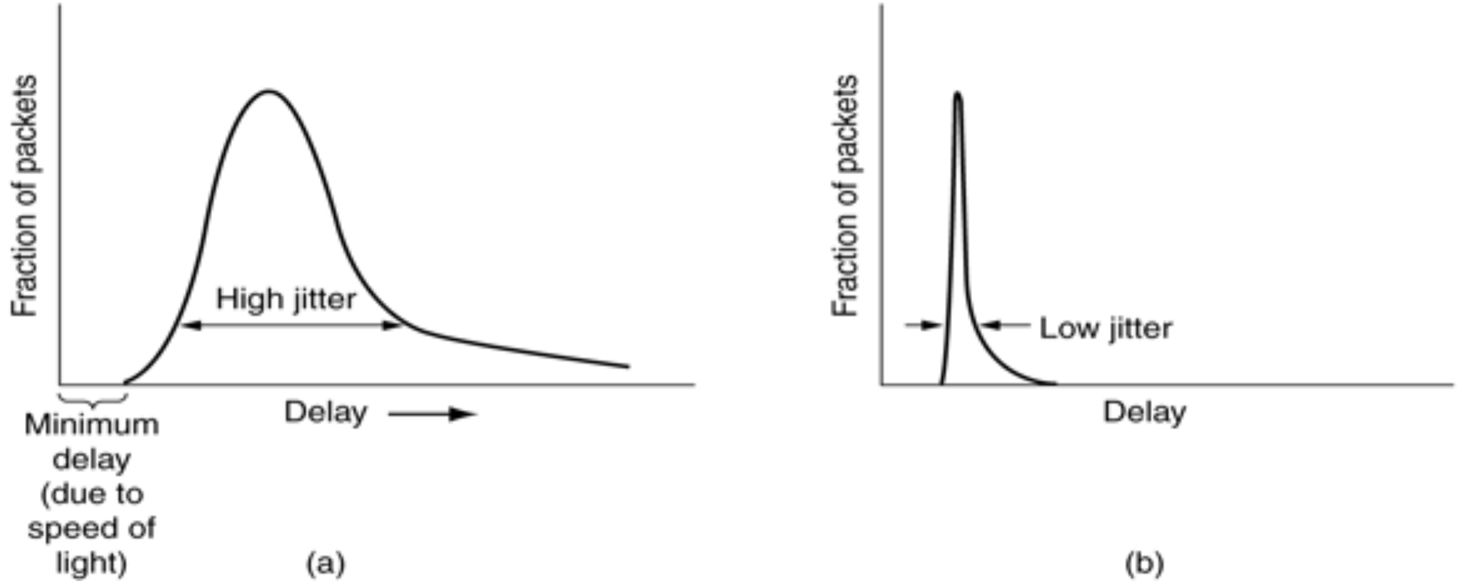
What happens in congestion?

- Congestion results when too much traffic is offered; performance degrades due to loss/retransmissions
  - Goodput (=useful packets) trails offered load



What is Jitter?

- Jitter is the **variation in packet arrival times**
  - a) high jitter
  - b) low jitter



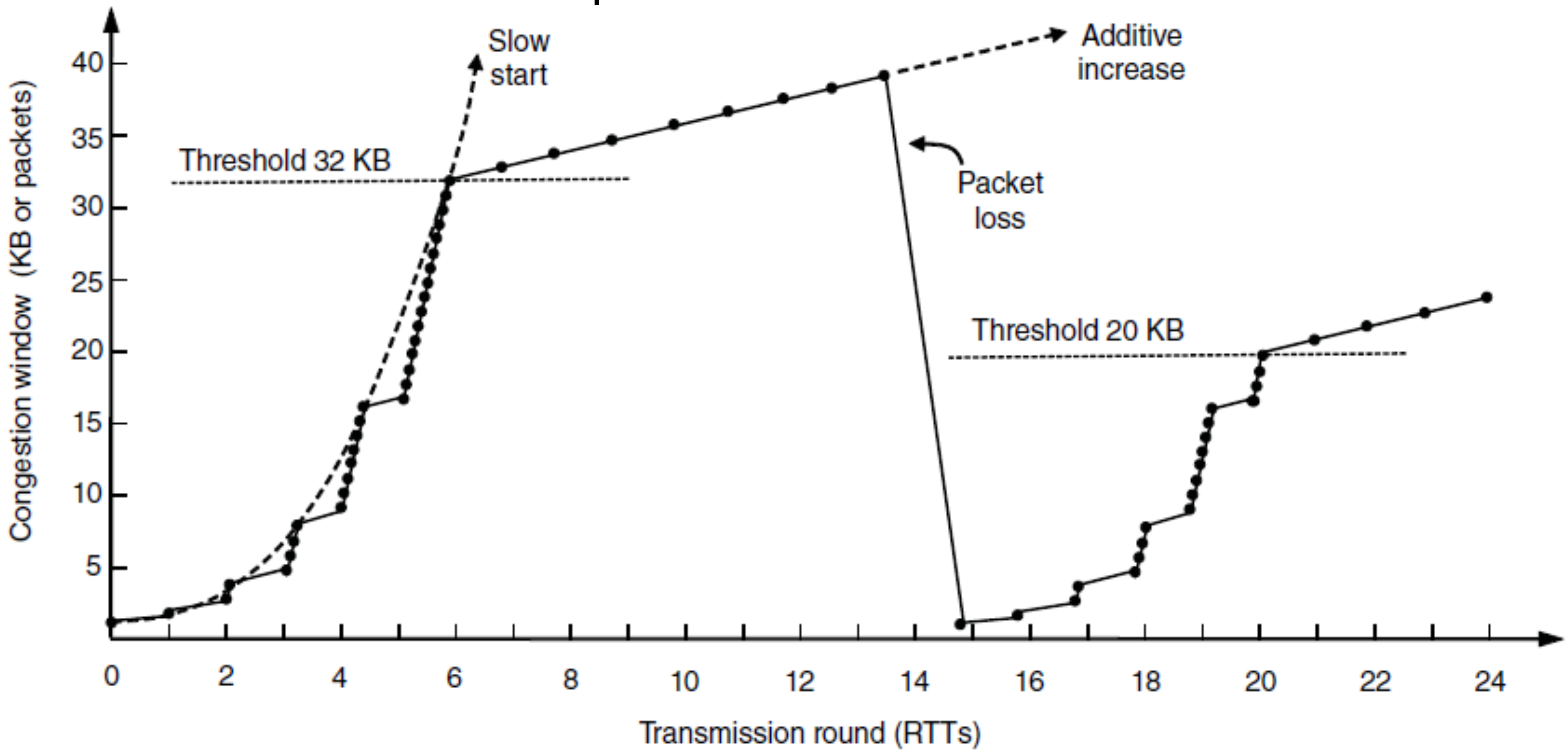
Techniques for Achieving Good QoS

- **Over-provisioning**
  - more than adequate buffer, router CPU, and bandwidth (expensive and not scalable ...)
- **Buffering**
  - buffer received flows before delivery - increases delay, but smoothes out jitter, no effect in reliability or bandwidth
- **Traffic Shaping**
  - regulate the average rate of transmission and burstiness of transmission
  - **leaky bucket**
  - **token bucket**
- **…**

Internet Congestion Control

Slow start followed by additive increase (TCP Tahoe)

Threshold is half of previous

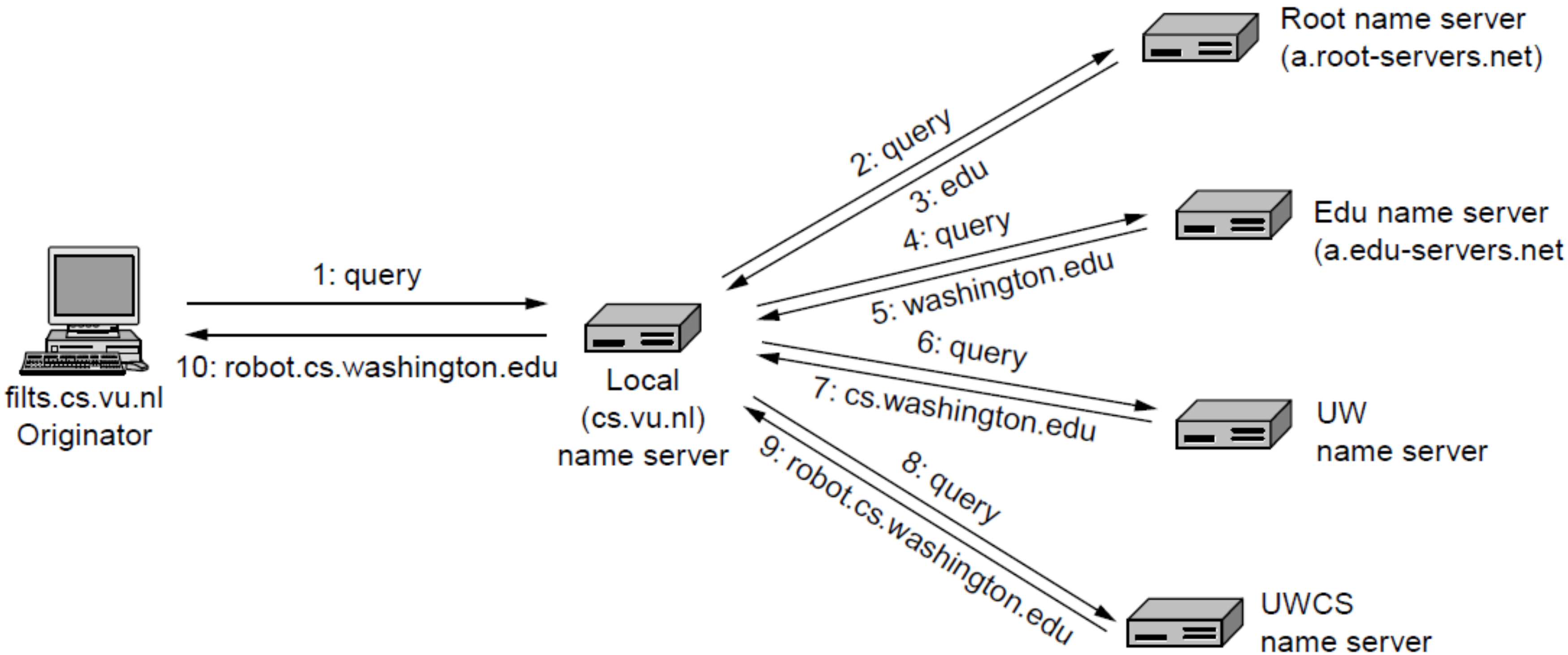


Application Layer: DNS First

- Problem?
  - IP address (32 bit), e.g., 121.7.106.83 – used for addressing datagrams
  - **www.yahoo.com – used by humans**
- Question: how do you map between IP address and name, and vice versa?
- Domain Name System:
  - *distributed database* implemented in a hierarchy of many *name servers*
  - *application-layer protocol* that allows a host to query the database in order to *resolve* names (address/name translation)
  - used by other application-layer protocols (http, ftp, smtp)

Example

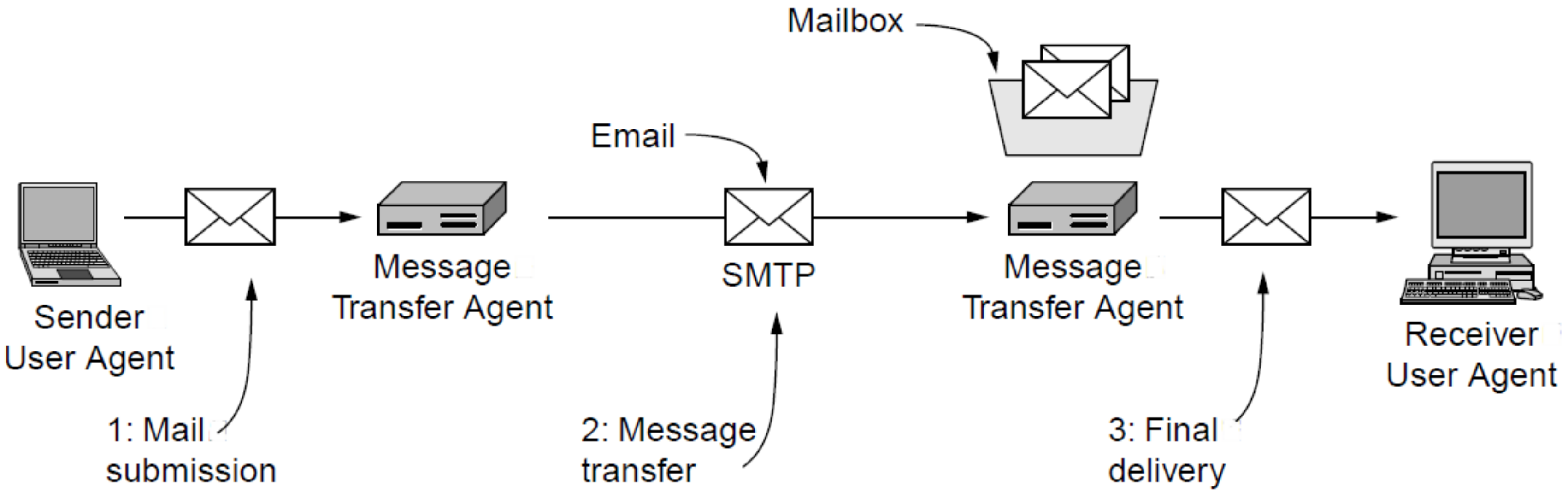
- Example of a computer looking up the IP for a name



The World Wide Web (WWW)

- World Wide Web key components are?
  - Client and Server software – **Firefox** is the client software for web access where **Apache** is on the server side
  - Web mark-up languages - **HTML** – how webpages are coded
  - Web scripting languages – More dynamicity to webpages - **Javascript**
  - **HTTP** – about how to transfer

Email



<span style="color:red">User agents</span>

Allow user to read and send email

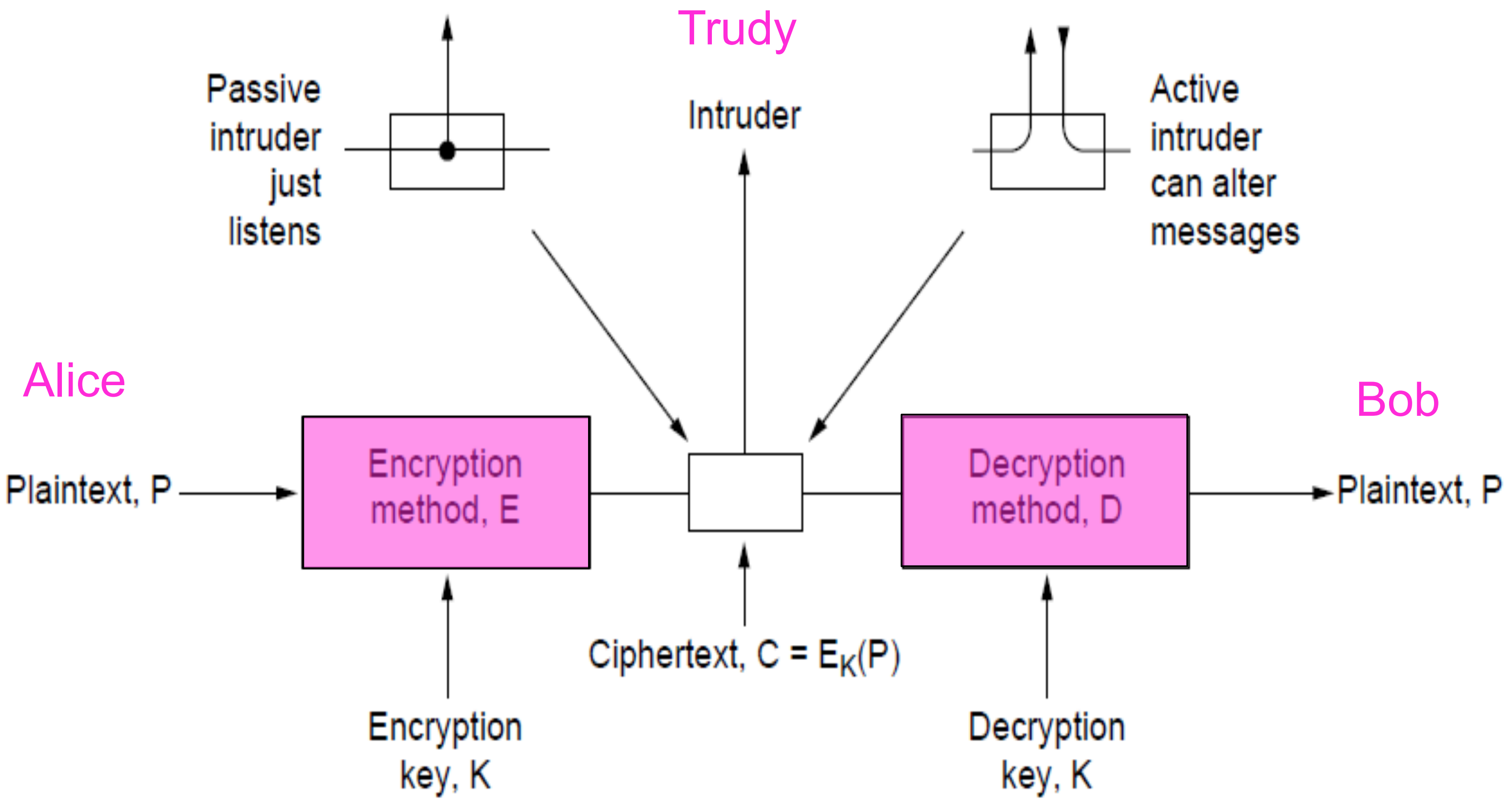
Message transfer agents

Transport messages from source - destination

Special Topic: Network Security

- Network security is a combo of 4 related areas:
  - **Secrecy** (Keeping information hidden from a general audience)
  - **Authentication** (Ensuring the user you are giving content to has valid credentials)
  - **Non-repudiation** (Prove a content was created by a named user)
  - **Integrity control** (Ensure that a content has not been tampered with)

Basics of Crypto: The Model



Modern Key-based Algorithms

- **Two main categories**

- Symmetric key algorithms use the same key for both encryption and decryption

- Symmetric key algorithms can use permutation, substitution and a combination of both to encrypt and decrypt

- **Symmetric Key Algorithms**

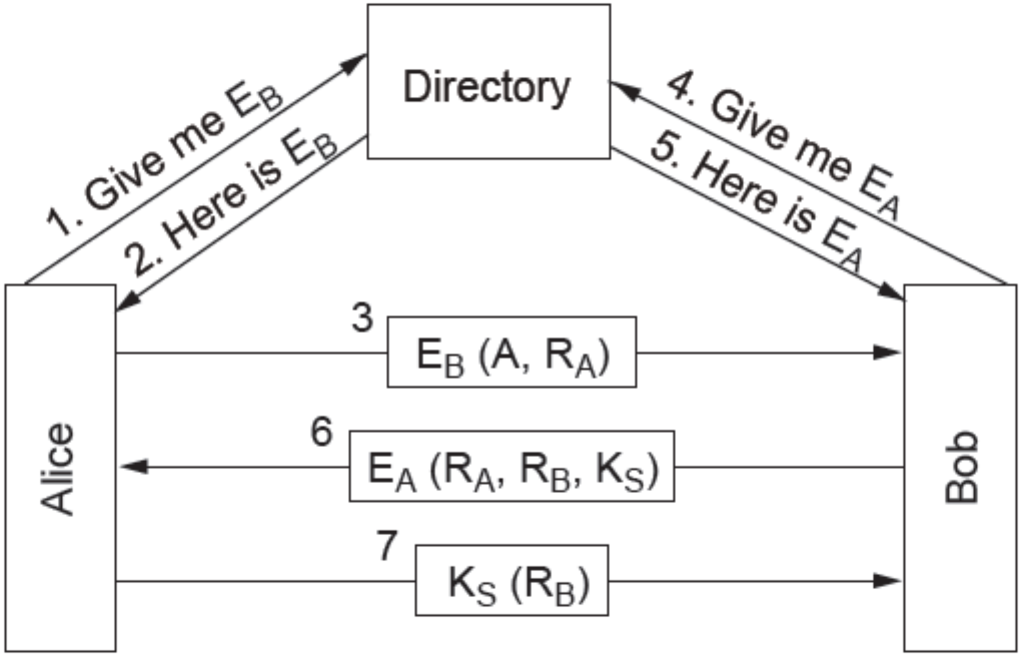
  Numerous algorithms exist

  We saw key solutions to certain types of attacks/problems

Asymmetric Key Algorithms

- **RSA - Rivest, Shamir, Adleman**
- Famous and robust algorithm
- Key generation:
  - Choose two large primes, p and q
  - Compute $n = p \times q$ and $z = (p - 1) \times (q - 1)$.
  - Choose d to be relatively prime to z, i.e., no common factors
  - Find e such that
    - **$(d \times e) \bmod z = 1$**
  - Public key is (e, n), and private key is (d, n)
- Encryption:
  - $\text{Cipher} = \text{Plain}^{e} \pmod{n}$
- Decryption:
  - $\text{Plain} = \text{Cipher}^{d} \pmod{n}$

An Application: Authentication Using Public Key Cryptography


Directory
1. Give me E_B
2. Here is E_B
4. Give me E_A
5. Here is E_A
Alice
Bob
3
E_B (A, R_A)
6
E_A (R_A, R_B, K_S)
7
K_S (R_B)