

Computer System B

Dr. Alma Oracevic
alma.oracevic@bristol.ac.uk

bristol.ac.uk



What did we learn?

- What is security?
- CIA
- Authentication
- Authorization
- Accountability (logs)



Computer Security Objectives

Confidentiality

- Data confidentiality
 - Assures that private or confidential information is not made available or disclosed to unauthorized individuals
- Privacy
 - Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed

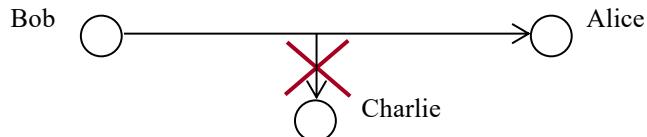
Integrity

- Data integrity
 - Assures that information and programs are changed only in a specified and authorized manner
- System integrity
 - Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system

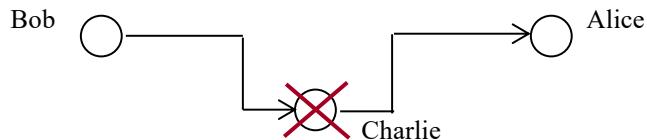
Availability

- Assures that systems work promptly and service is not denied to authorized users

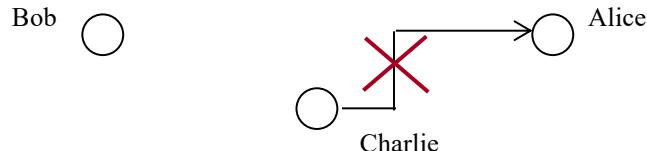
1. Confidentiality

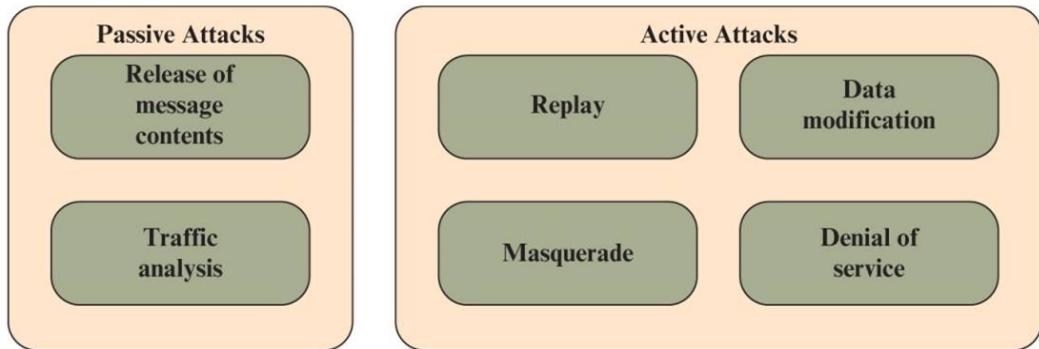


2. Message integrity

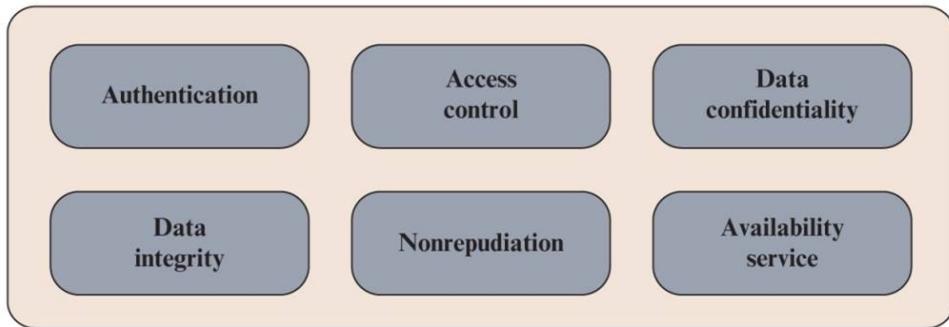


3. Message authentication

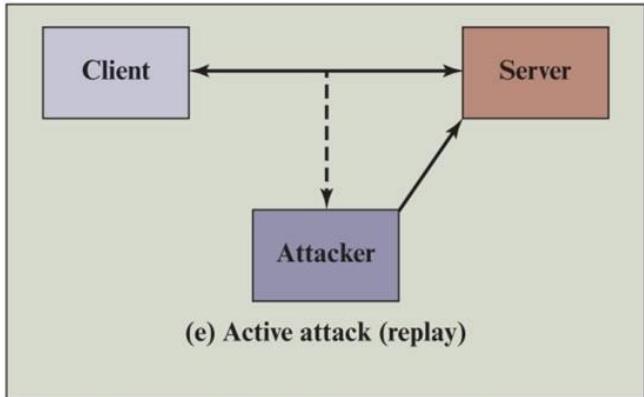
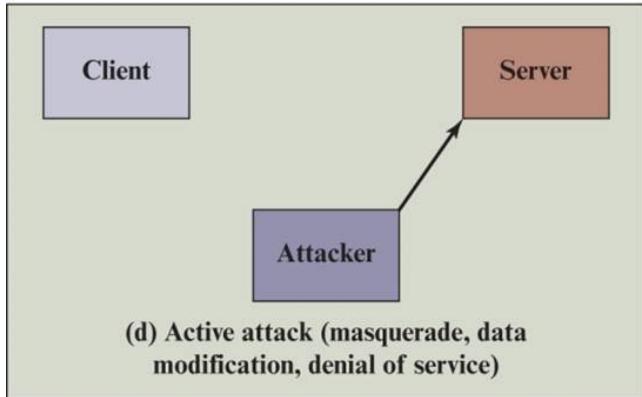
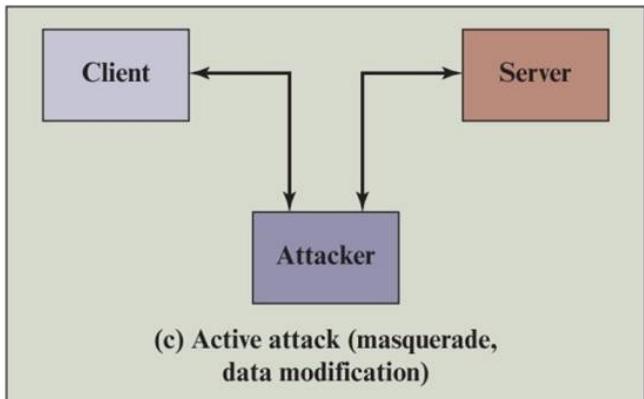
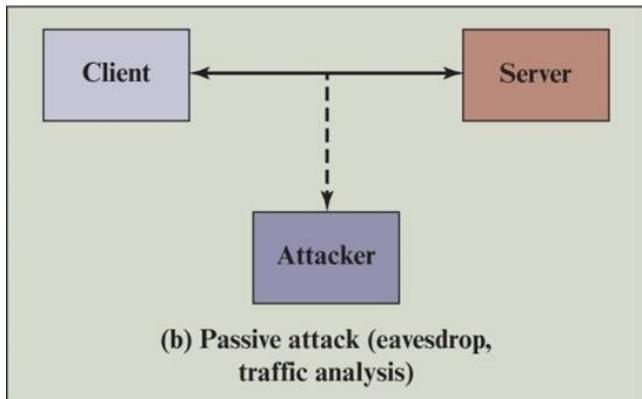
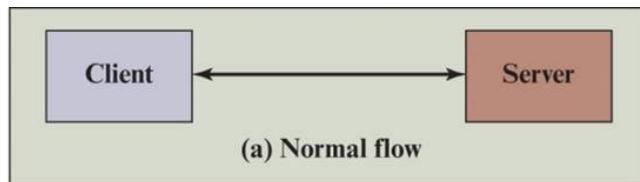


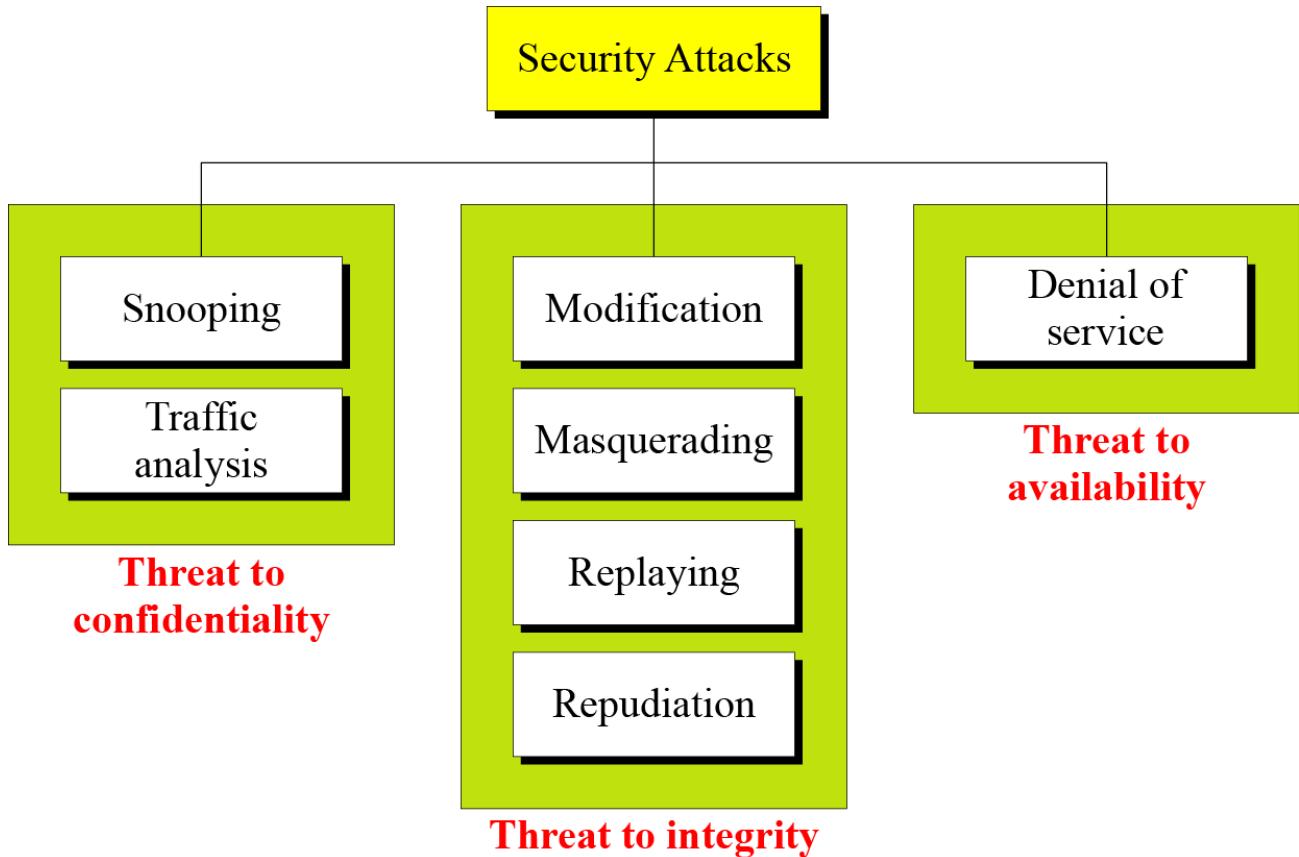


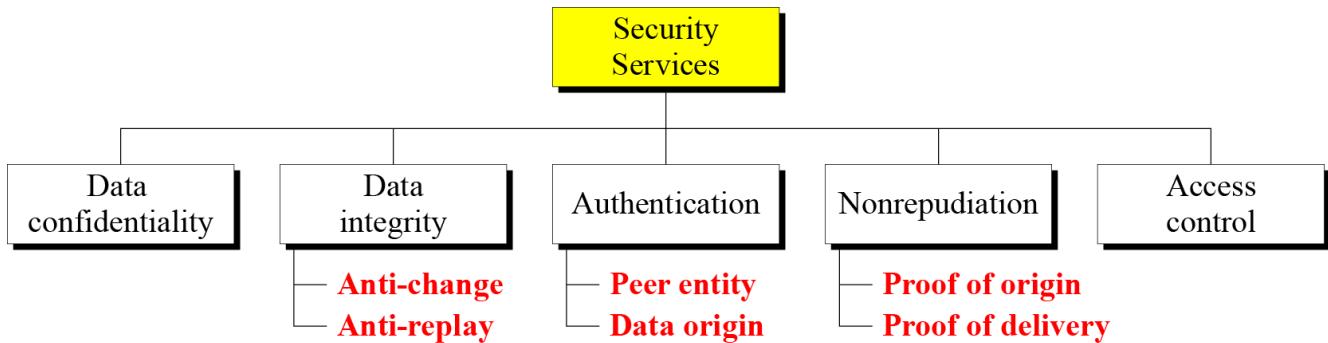
(a) Attacks



(b) Services







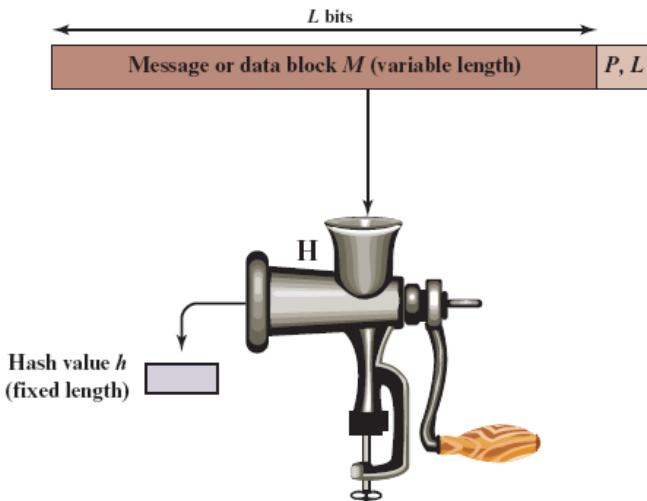
Security Mechanisms (1 of 2)

- **Cryptographic algorithms:** We can distinguish between reversible cryptographic mechanisms and irreversible cryptographic mechanisms. A reversible cryptographic mechanism is simply an encryption algorithm that allows data to be encrypted and subsequently decrypted. Irreversible cryptographic mechanisms include hash algorithms and message authentication codes, which are used in digital signature and message authentication applications.
- **Data integrity:** This category covers a variety of mechanisms used to assure the integrity of a data unit or stream of data units.
- **Digital signature:** Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery.

Security Mechanisms (2 of 2)

- **Authentication exchange:** A mechanism intended to ensure the identity of an entity by means of information exchange.
- **Traffic padding:** The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.
- **Routing control:** Enables selection of particular physically or logically secure routes for certain data and allows routing changes, especially when a breach of security is suspected.
- **Notarization:** The use of a trusted third party to assure certain properties of a data exchange
- **Access control:** A variety of mechanisms that enforce access rights to resources.

Hash function



$P, L = \text{padding plus length field}$

Message Authentication Code (MAC)

- Also known as a *keyed hash function*
- Typically used between two parties that share a secret key to authenticate information exchanged between those parties
- Takes as input a secret key and a data block and produces a hash value (MAC) which is associated with the protected message
 - If the integrity of the message needs to be checked, the MAC function can be applied to the message and the result compared with the associated MAC value
 - An attacker who alters the message will be unable to alter the associated MAC value without knowledge of the secret key

Today!

- Introduction to Cryptography!
- Introduction to Network Security

bristol.ac.uk



Classical Encryption Techniques

bristol.ac.uk

Basic Terminology

- Plaintext
 - The original message
- Ciphertext
 - The coded message
- Enciphering or encryption
 - Process of converting from plaintext to ciphertext
- Deciphering or decryption
 - Restoring the plaintext from the ciphertext
- Cryptography
 - Study of encryption
- Cryptographic system or cipher
 - Schemes used for encryption
- Cryptanalysis
 - Techniques used for deciphering a message without any knowledge of the enciphering details
- Cryptology
 - Areas of cryptography and cryptanalysis together

Cryptanalysis and Brute-Force Attack

Cryptanalysis

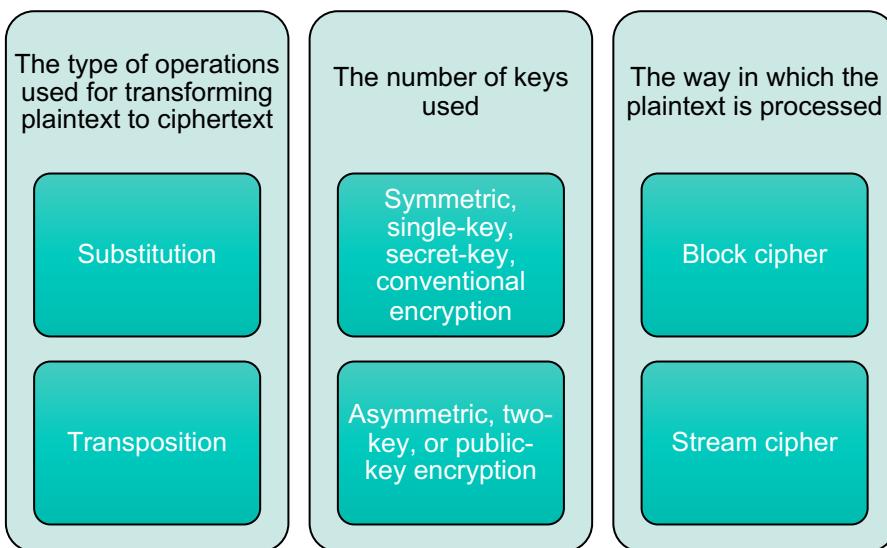
- Attack relies on the nature of the algorithm plus some knowledge of the general characteristics of the plaintext
- Attack exploits the characteristics of the algorithm to attempt to deduce a specific plaintext or to deduce the key being used

Brute-force attack

- Attacker tries every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained
- On average, half of all possible keys must be tried to achieve success

Cryptographic Systems

- Characterized along three independent dimensions:



Brute-Force Attack

Involves trying every possible key until an intelligible translation of the ciphertext into plaintext is obtained

On average, half of all possible keys must be tried to achieve success

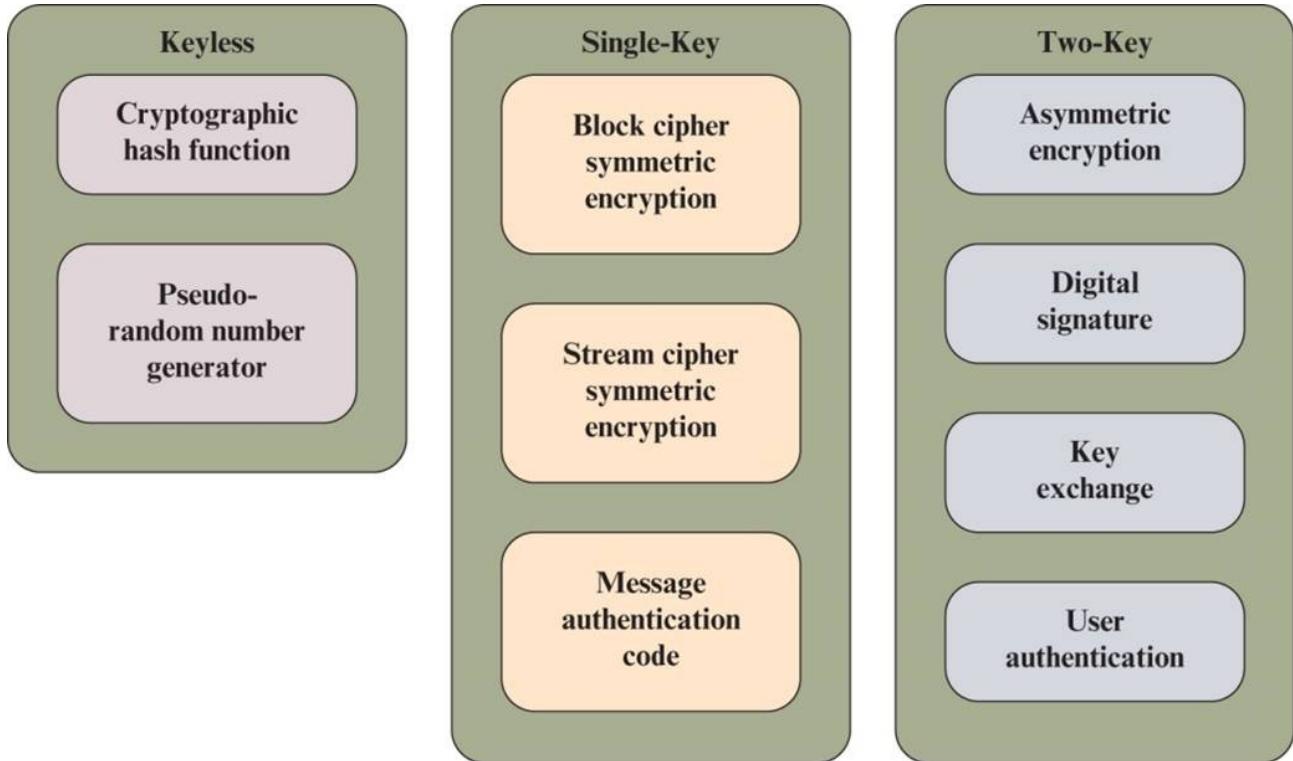
To supplement the brute-force approach, some degree of knowledge about the expected plaintext is needed, and some means of automatically distinguishing plaintext from garble is also needed

Cryptographic Systems

- The type of operations used for transforming plaintext to ciphertext
 - Substitution
 - Transposition
- The number of keys used
 - Symmetric, single-key, secret-key, conventional encryption
 - Asymmetric, two-key, or public-key encryption
- The way in which the plaintext is processed
 - Block cipher
 - Stream cipher



Cryptographic Algorithms based on number of keys

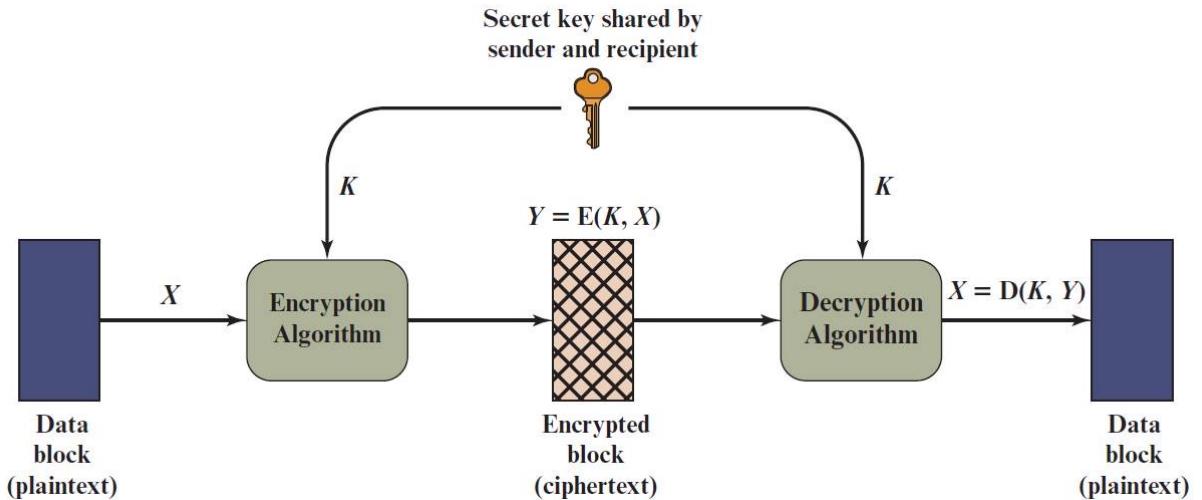


Symmetric Encryption

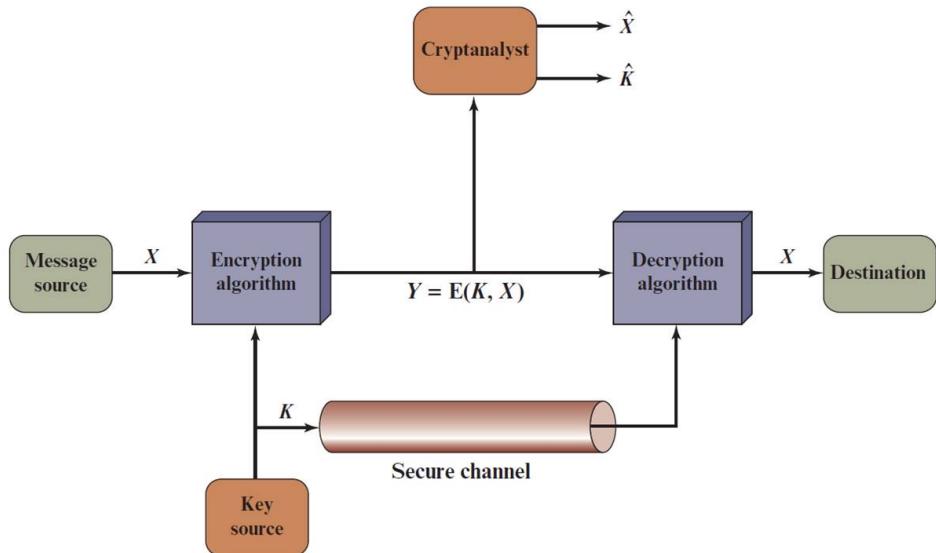
- Also referred to as conventional encryption or single-key encryption
- Was the only type of encryption in use prior to the development of public-key encryption in the 1970s
- Remains by far the most widely used of the two types of encryption



Simplified Model of Symmetric Encryption

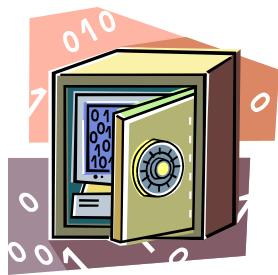


Model of Symmetric Cryptosystem



Encryption Scheme Security

- Unconditionally secure
 - No matter how much time an opponent has, it is impossible for him or her to decrypt the ciphertext simply because the required information is not there
- Computationally secure
 - The cost of breaking the cipher exceeds the value of the encrypted information
 - The time required to break the cipher exceeds the useful lifetime of the information



Substitution Technique

- Is one in which the letters of plaintext are replaced by other letters or by numbers or symbols
- If the plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with ciphertext bit patterns

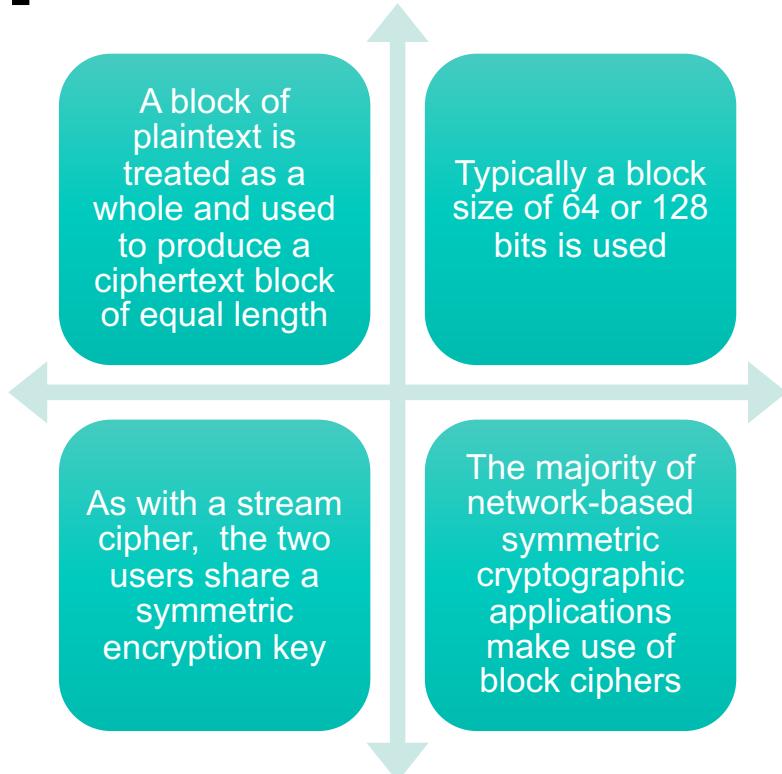


Caesar Cipher

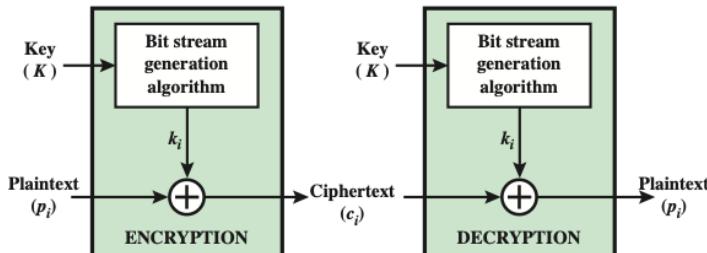


- Simplest and earliest known use of a substitution cipher
- Used by Julius Caesar
- Involves replacing each letter of the alphabet with the letter standing three places further down the alphabet
- Alphabet is wrapped around so that the letter following Z is A
 - plain: meet me after the toga party
 - cipher: PHHW PH DIWHU WKH WRJD SDUWB

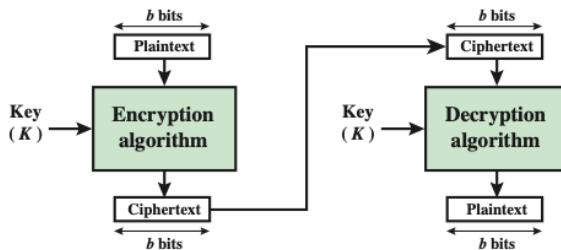
Block Cipher



Block Cipher



(a) Stream Cipher Using Algorithmic Bit Stream Generator

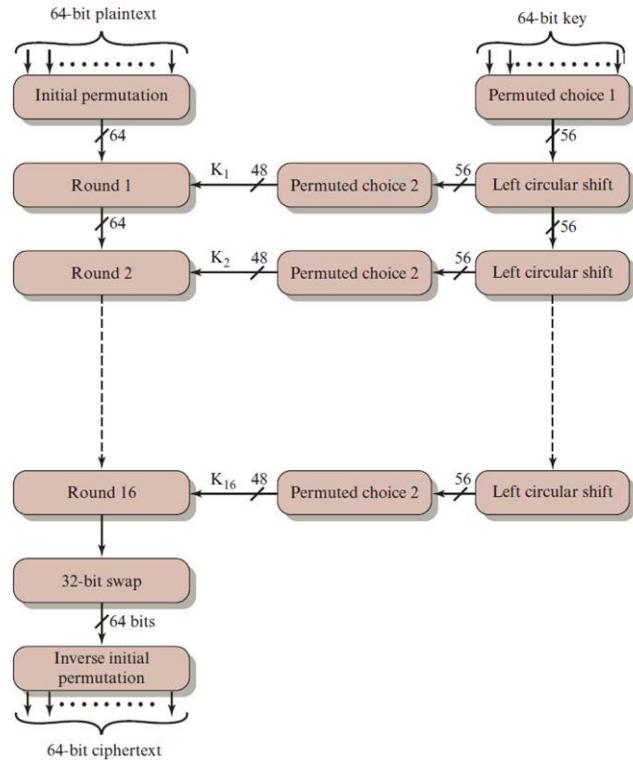


(b) Block Cipher

Data Encryption Standard (DES)

- Issued in 1977 by the National Bureau of Standards (now NIST) as Federal Information Processing Standard 46
- Was the most widely used encryption scheme until the introduction of the Advanced Encryption Standard (AES) in 2001
- Algorithm itself is referred to as the Data Encryption Algorithm (DEA)
 - Data are encrypted in 64-bit blocks using a 56-bit key
 - The algorithm transforms 64-bit input in a series of steps into a 64-bit output
 - The same steps, with the same key, are used to reverse the encryption

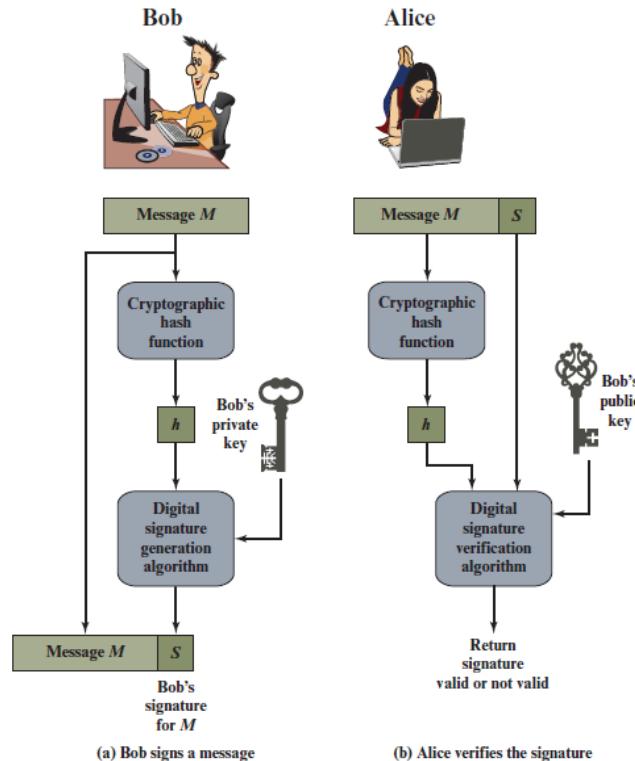
General Depiction of DES Encryption Algorithm



Asymmetric Algorithms

- Encryption algorithms that use a two keys are referred to as *asymmetric encryption algorithms*
- Digital signature algorithm
 - A digital signature is a value computed with a cryptographic algorithm and associated with a data object in such a way that any recipient of the data can use the signature to verify the data's origin and integrity
- Key exchange
 - The process of securely distributing a symmetric key to two or more parties
- User authentication
 - The process of authenticating that a user attempting to access an application or service is genuine and, similarly, that the application or service is genuine

Digital Signature



Digital Signature Properties

- It must verify the author and the date and time of the signature
- It must authenticate the contents at the time of the signature
- It must be verifiable by third parties to resolve disputes

Introduction to Network security

bristol.ac.uk



Security?

- widespread use of data processing equipment:
computer security
- widespread use of computer networks and distributed computing systems:
network security

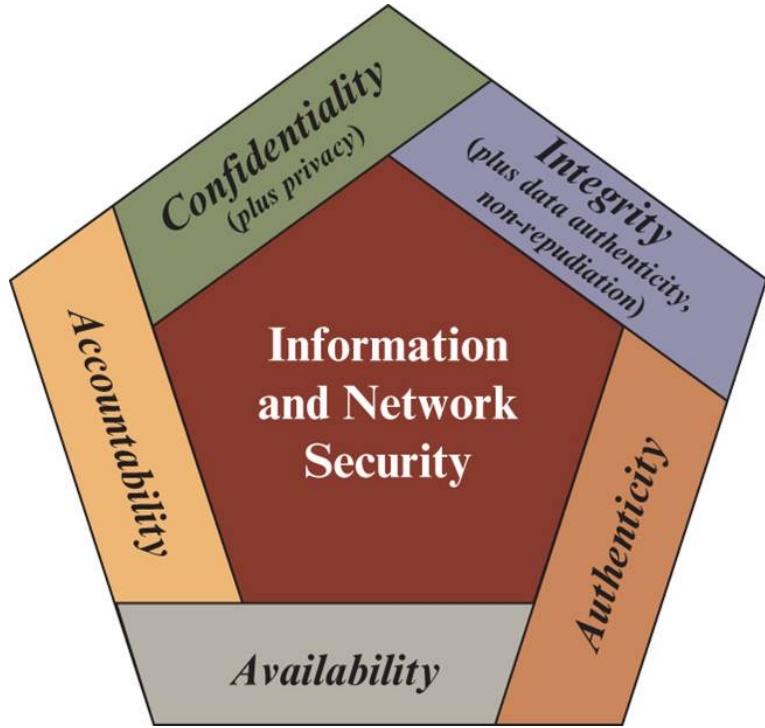
Cybersecurity

Information Security

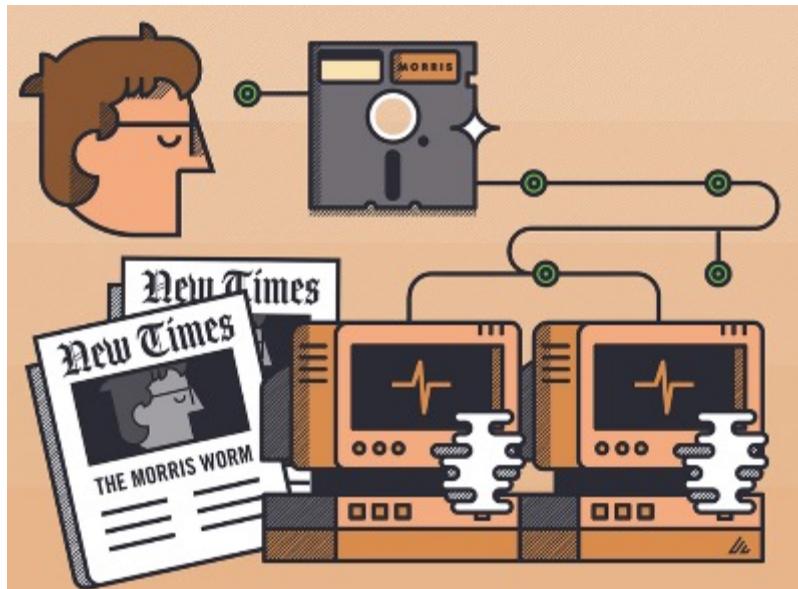
- This term refers to preservation of confidentiality, integrity, and availability of information. In addition, other properties, such as authenticity, accountability, nonrepudiation, and reliability can also be involved

Network Security

- This term refers to protection of networks and their service from unauthorized modification, destruction, or disclosure, and provision of assurance that the network performs its critical functions correctly and there are no harmful side effects



The day that changed everything



The Brain



Welcome to the Dungeon

© 1986 Basit & Amjads (pvt). BRAIN COMPUTER SERVICES 730 NIZAM

BLOCK ALLAMA IQBAL TOWN LAHORE-PAKISTAN PHONE:
430791,443248,280530.

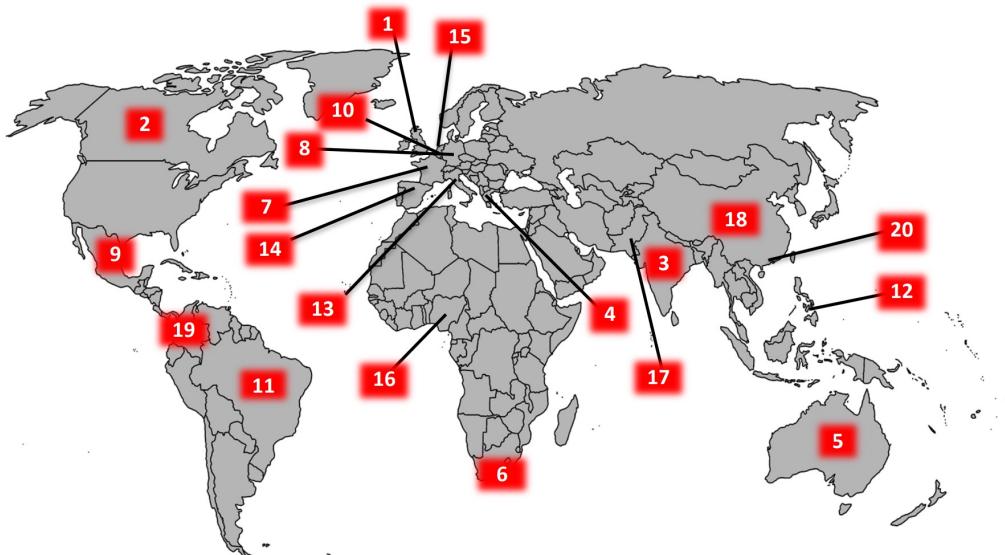
Beware of this virus.... Contact us for vaccination....

But why do we need security?



2020 - TOP 20 INTERNATIONAL VICTIM COUNTRIES

Excluding the United States⁸



1. United Kingdom	216,633	6. South Africa	1,754	11. Brazil	951	16. Nigeria	443
2. Canada	5,399	7. France	1,640	12. Philippines	898	17. Pakistan	443
3. India	2,930	8. Germany	1,578	13. Italy	728	18. China	442
4. Greece	2,314	9. Mexico	1,164	14. Spain	618	19. Colombia	418
5. Australia	1,807	10. Belgium	1,023	15. Netherlands	450	20. Hong Kong	407

2020 CRIME TYPES

By Victim Count

Crime Type	Victims	Crime Type	Victims
Phishing/Vishing/Smishing/Pharming	241,342	Other	10,372
Non-Payment/Non-Delivery	108,869	Investment	8,788
Extortion	76,741	Lottery/Sweepstakes/Inheritance	8,501
Personal Data Breach	45,330	IPR/Copyright and Counterfeit	4,213
Identity Theft	43,330	Crimes Against Children	3,202
Spoofing	28,218	Corporate Data Breach	2,794
Misrepresentation	24,276	Ransomware	2,474
Confidence Fraud/Romance	23,751	Denial of Service/TDoS	2,018
Harassment/Threats of Violence	20,604	Malware/Scareware/Virus	1,423
BEC/EAC	19,369	Health Care Related	1,383
Credit Card Fraud	17,614	Civil Matter	968
Employment	16,879	Re-shipping	883
Tech Support	15,421	Charity	659
Real Estate/Rental	13,638	Gambling	391
Advanced Fee	13,020	Terrorism	65
Government Impersonation	12,827	Hacktivist	52
Overpayment	10,988		

Descriptors*

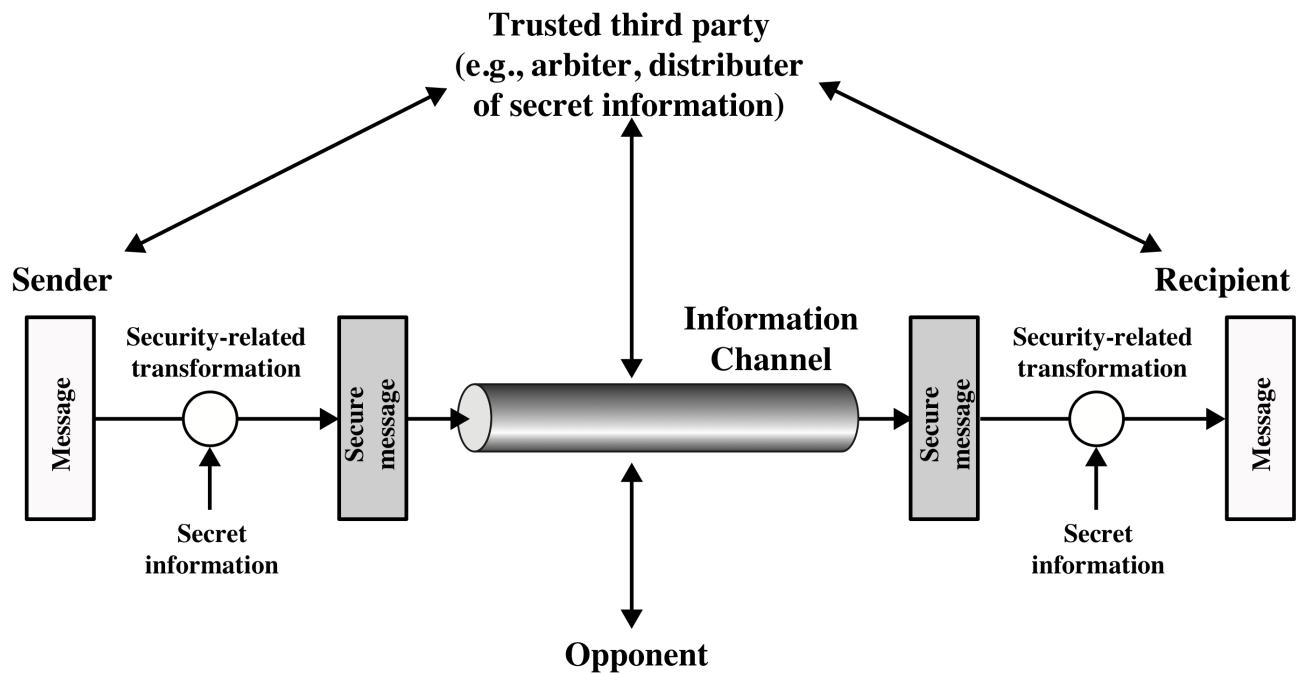
Social Media	35,439	*These descriptors relate to the medium or tool used to facilitate the crime and are used by the IC3 for tracking purposes only. They are available as descriptors only after another crime type has been selected. Please see Appendix B for more information regarding IC3 data.
Virtual Currency	35,229	

What is network security?

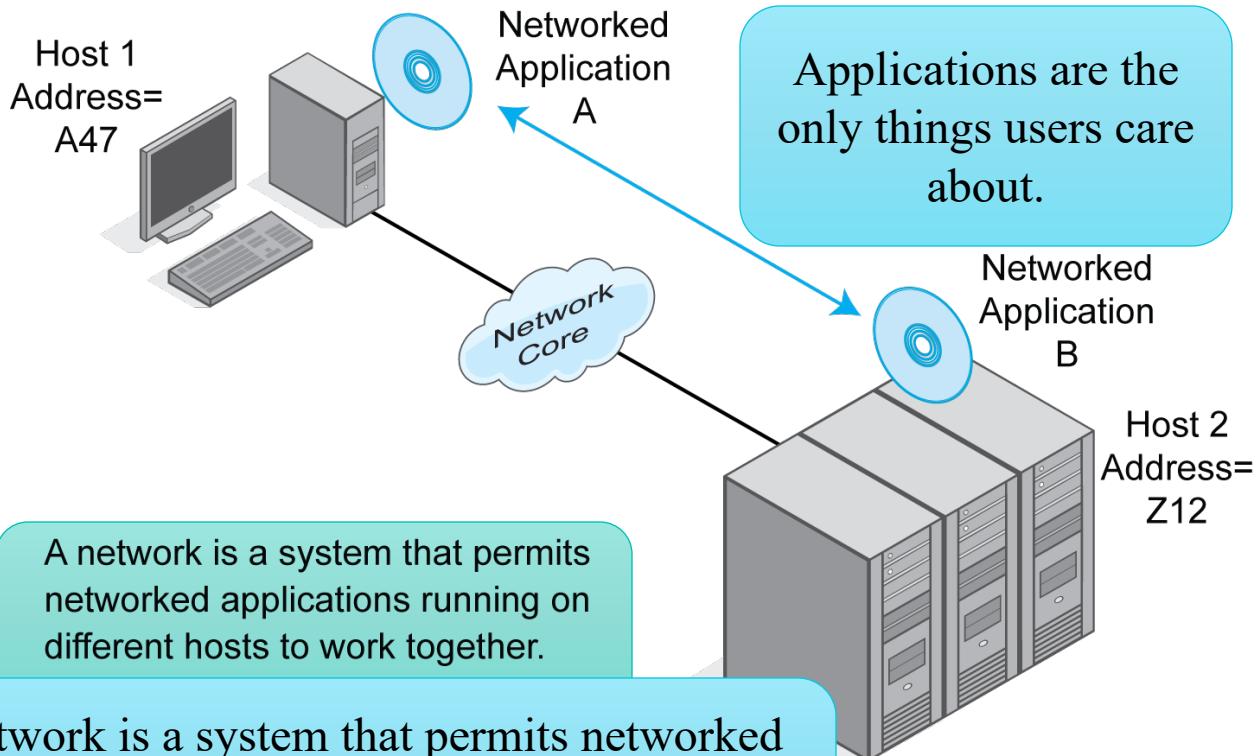
bristol.ac.uk



Model for Network Security

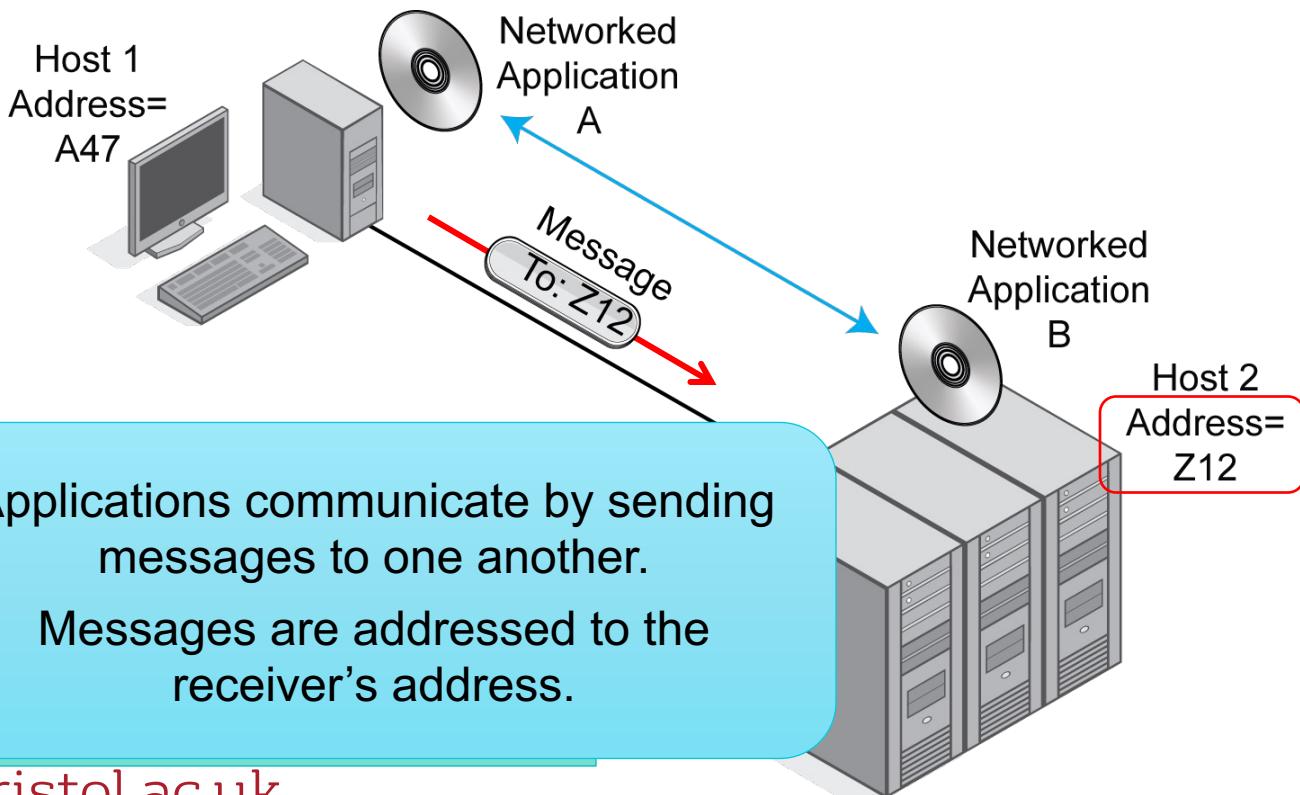


Basic Network Terminology

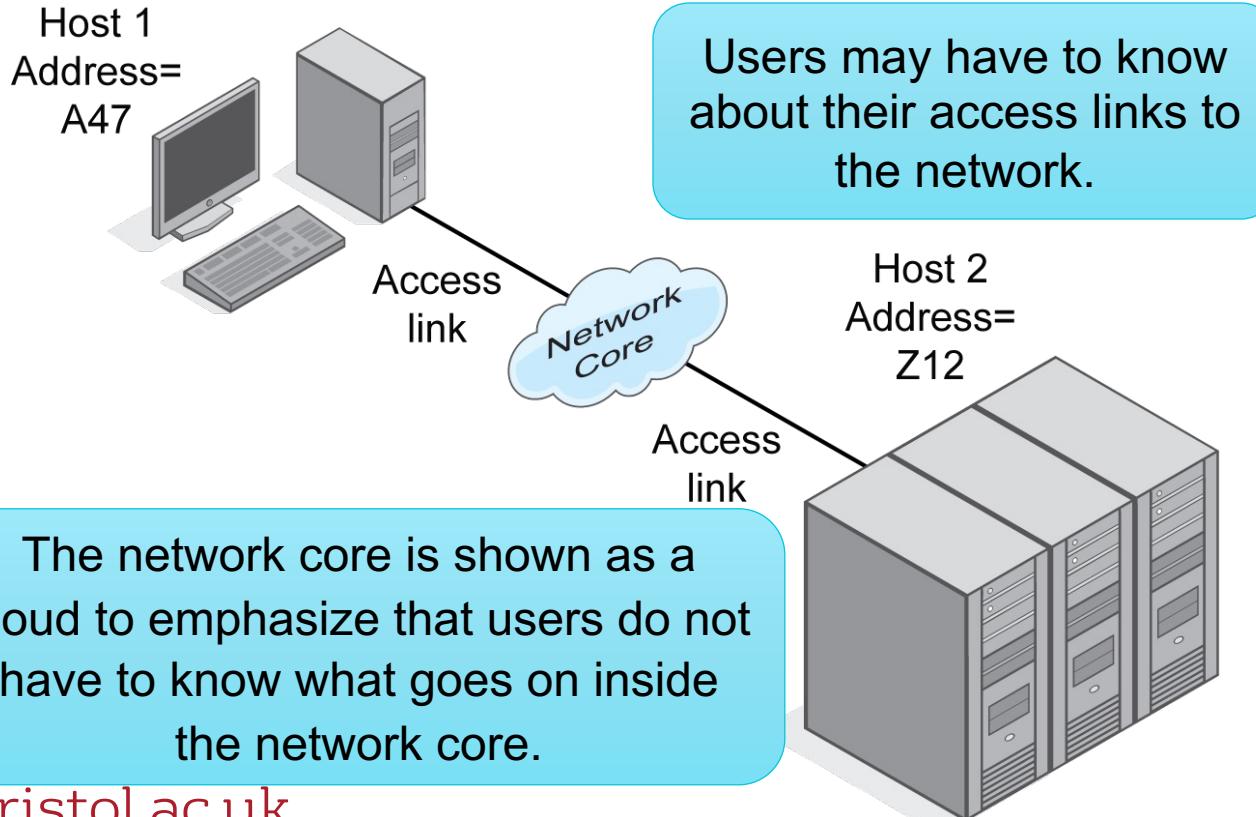


A network is a system that permits networked applications running on different hosts to work together.

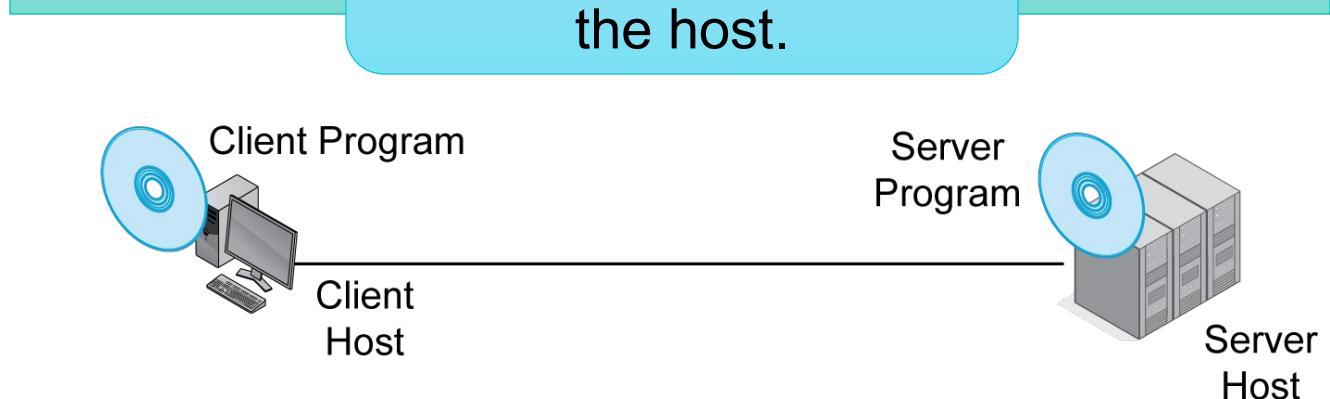
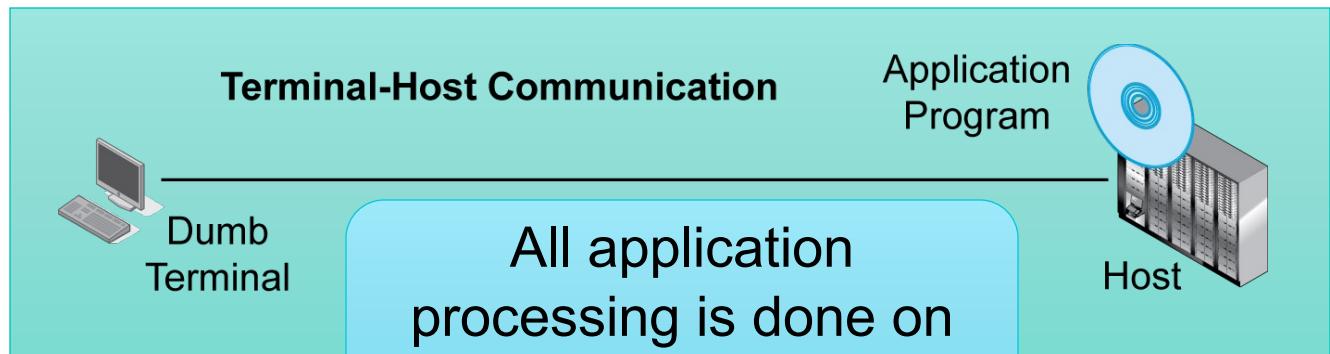
Basic Network Terminology



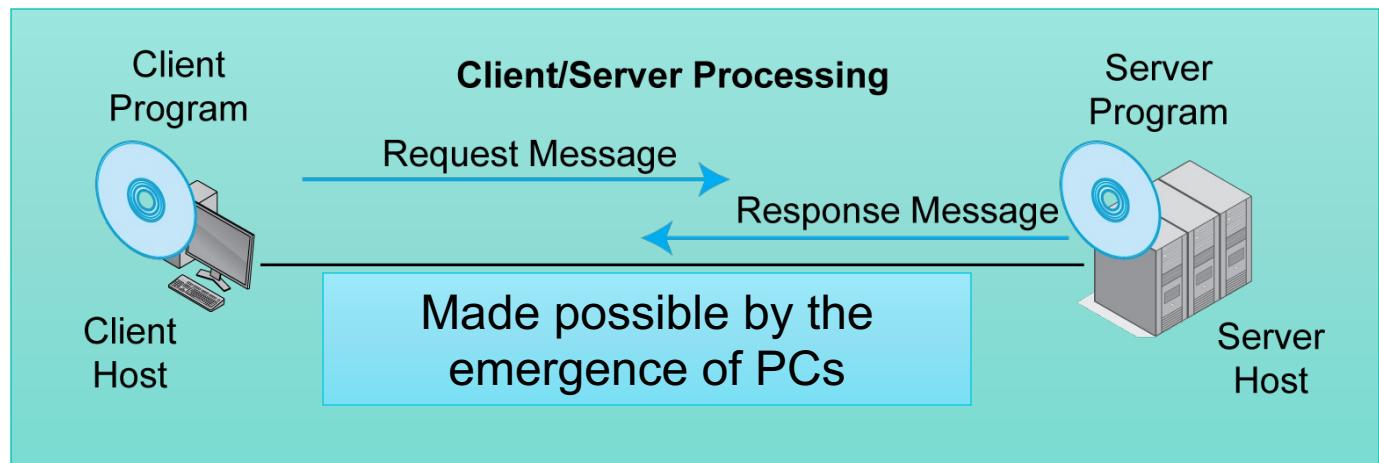
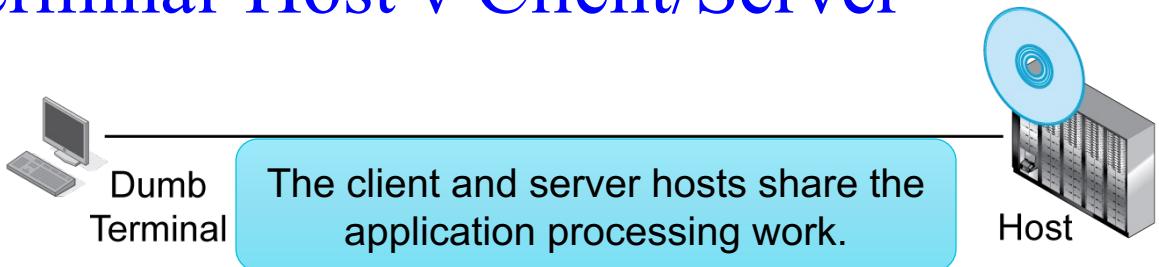
Basic Network Terminology



Terminal-Host v Client/Server



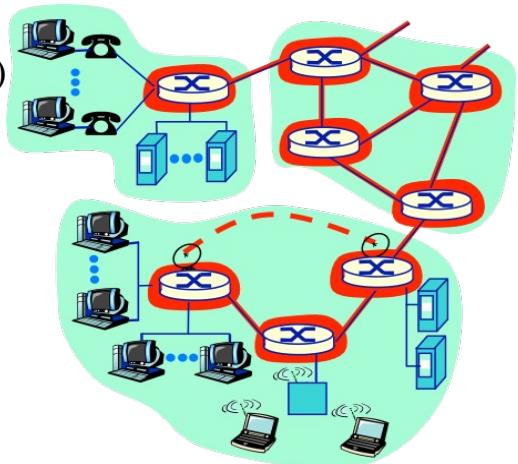
Terminal-Host v Client/Server



Network Structure

The network core

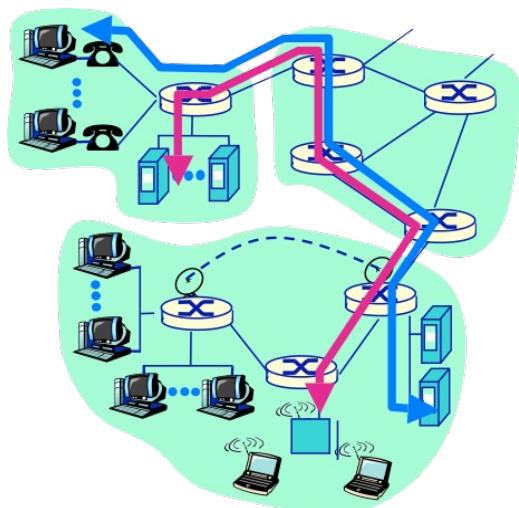
- A mesh of interconnected routers
- **The fundamental question:** How is data routed through the network?
 - **Circuit switching:** dedicated circuit (path) per call used by all data (e.g., telephone)
 - **Packet switching:** data sent in discrete “chunks”
(packets); each has a path chosen for it



The Network Core

Circuit Switching

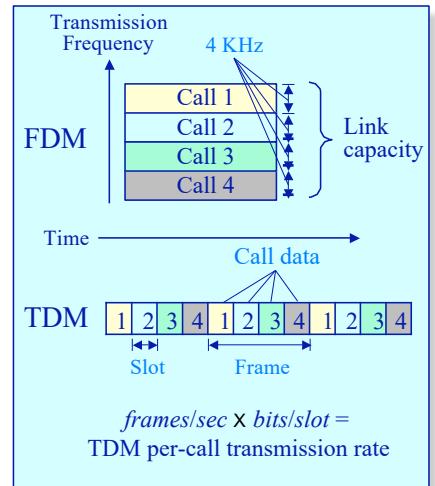
- Resources reserved end-to-end for the connection (“call”)
 - **Resources:** Link bandwidth, switch capacity
 - **Reservation:** Dedicated fraction of available bandwidth, buffers, etc.
- Circuit-like (guaranteed) performance
 - Call setup required
 - Call rejection (“busy signal”) possible



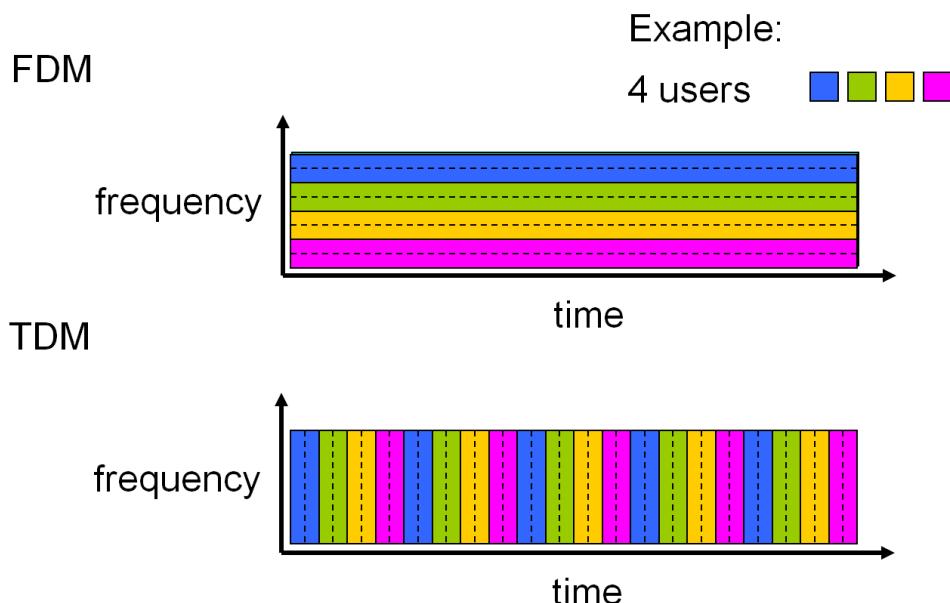
Circuit Switching

Allocating fractions of bandwidth — Multiplexing

- Network bandwidth divided into transmission “slots”
 - Slots allocated to calls
 - Slots are unused (“idle”) if not used by owning call
 - No sharing of slots!
- How to divide link bandwidth into slots?
 - Frequency division multiplexing (FDM)
 - Time division multiplexing (TDM)

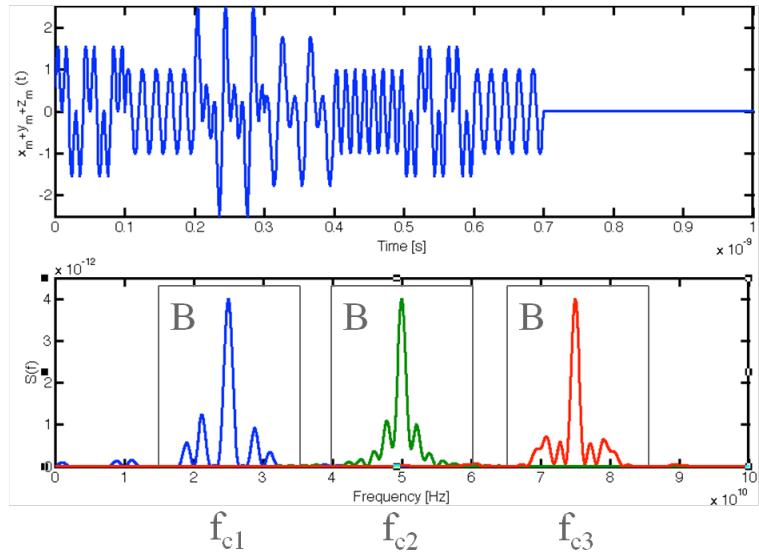


Multiplexing



TDM/FDM

$x(t) + y(t) + z(t)$



$S_X(f) + S_Y(f) + S_Z(f)$

The Network Core

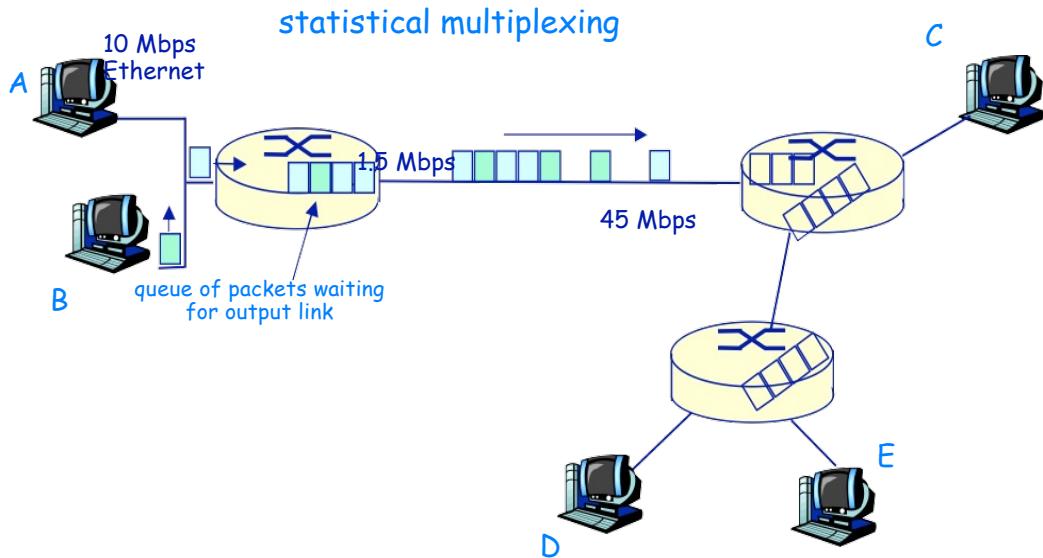
Packet Switching

- Each sender divides its messages *into packets (sequence of bits)*
 - Senders' packets share (compete for) network resources
 - Each packet uses full link capacity until transmission completed
 - Resources allocated & used as needed
- But now we have resource contention!
 - Aggregate resource demand can exceed amount available
 - packets queue, wait for link availability
- Store and forward: packets move **one hop** at a time
 - Transmit over link
 - Wait turn at next link

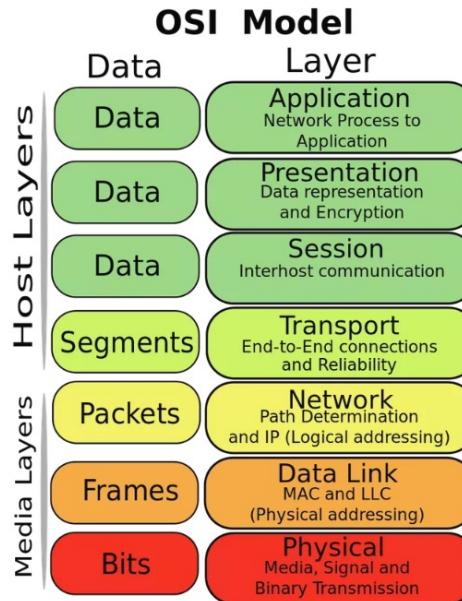
- 
- ◆ Bandwidth division into slots
 - ◆ Dedicated allocation
 - ◆ Resource reservation

Packet Switching

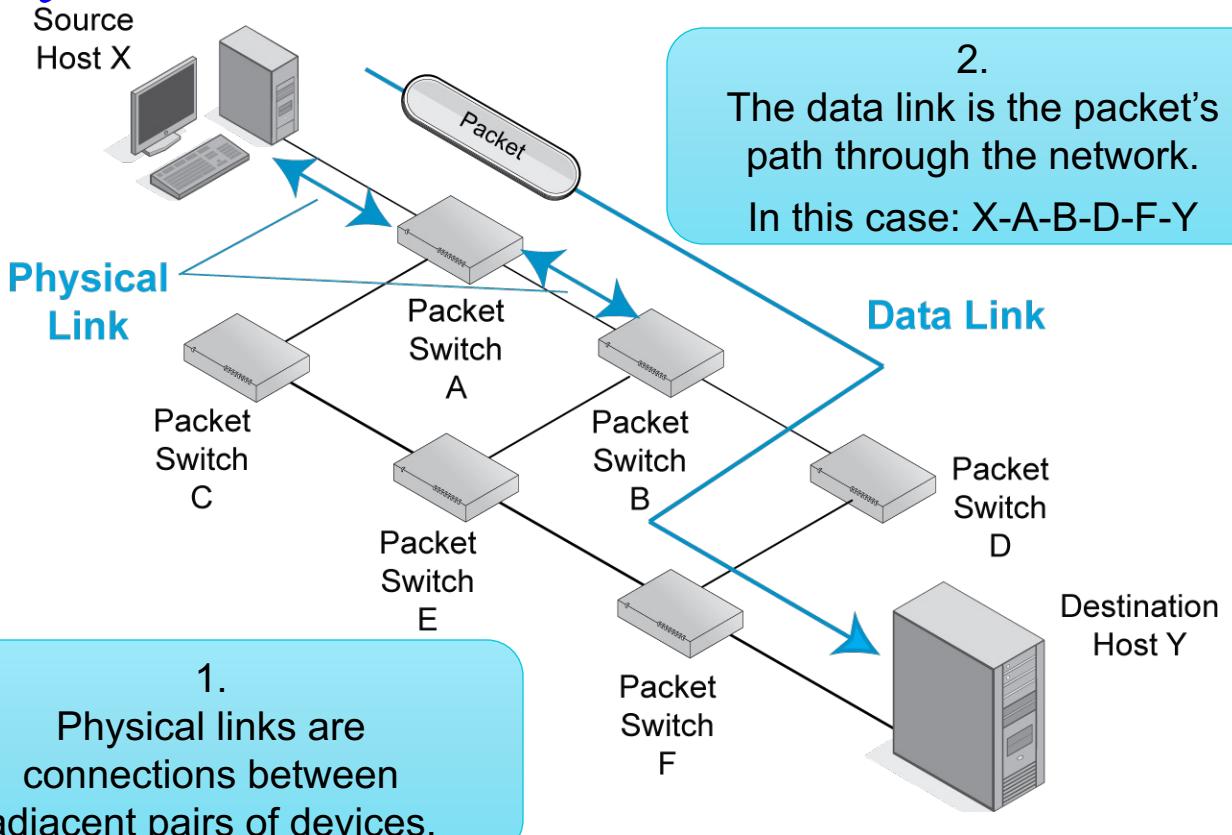
Statistical multiplexing



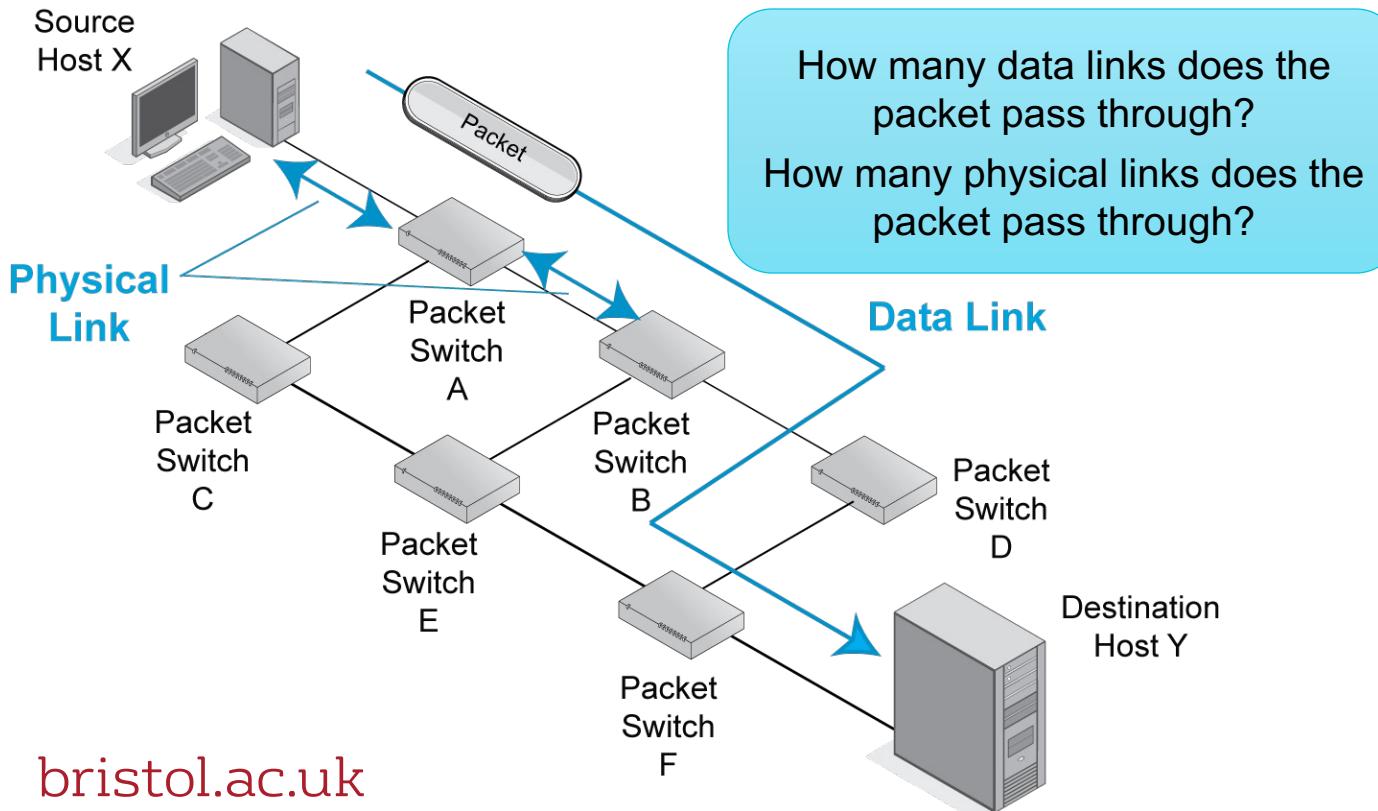
Bits, Frames, Segments, Data?



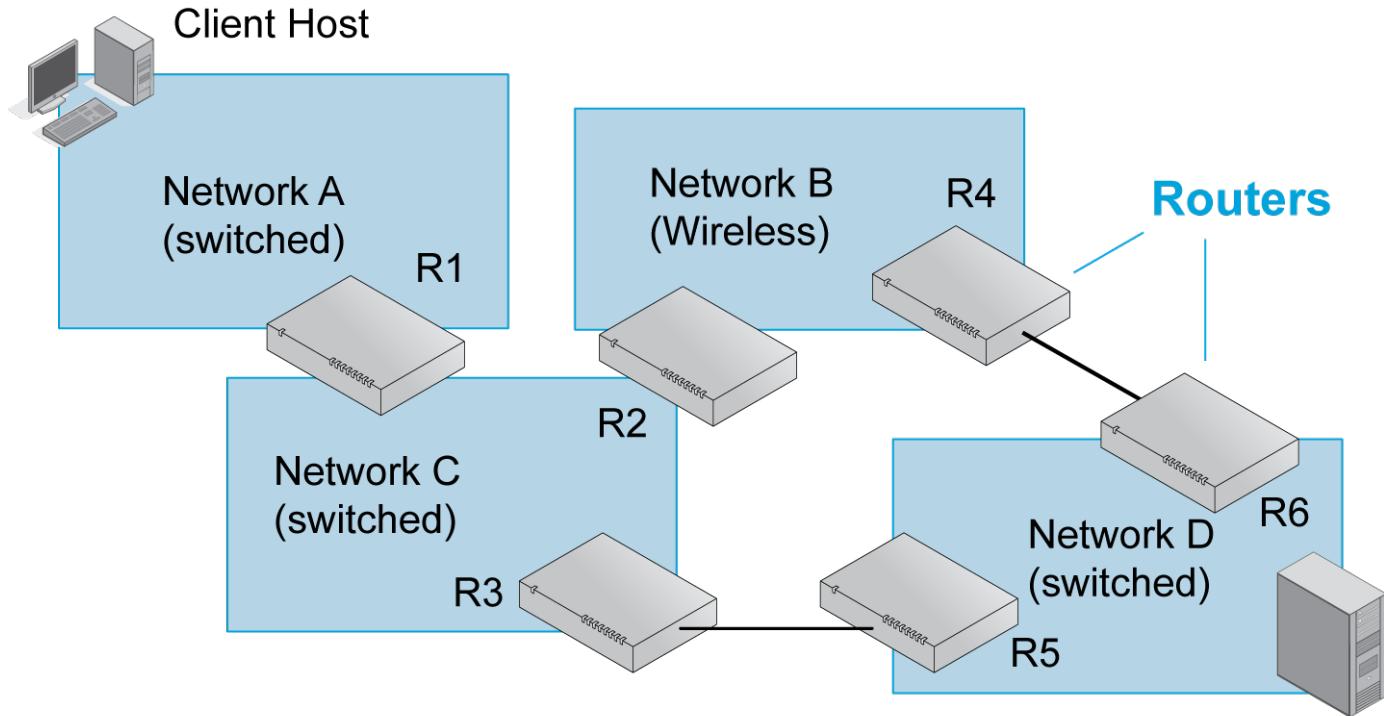
Physical Links and Data Links



Physical Links and Data Links

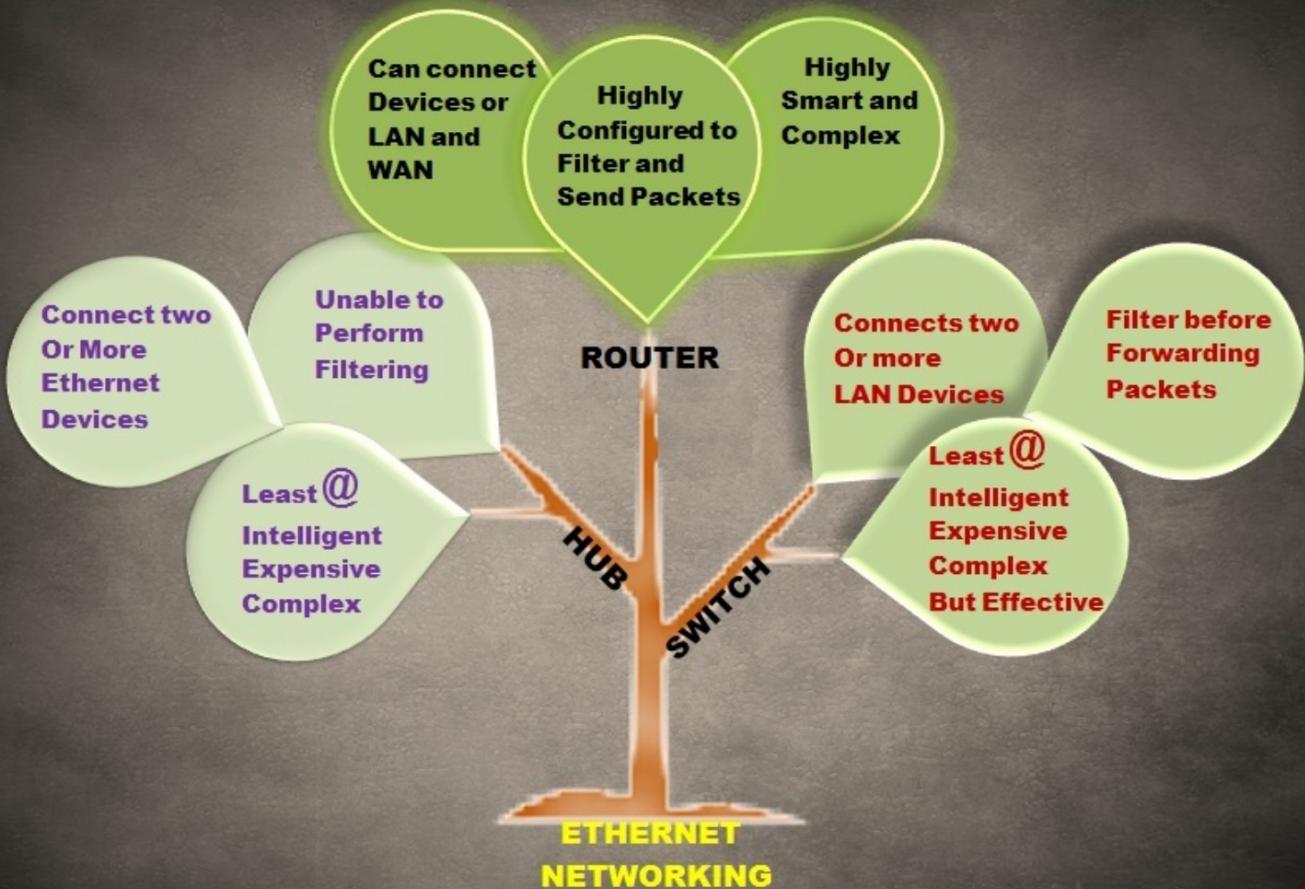


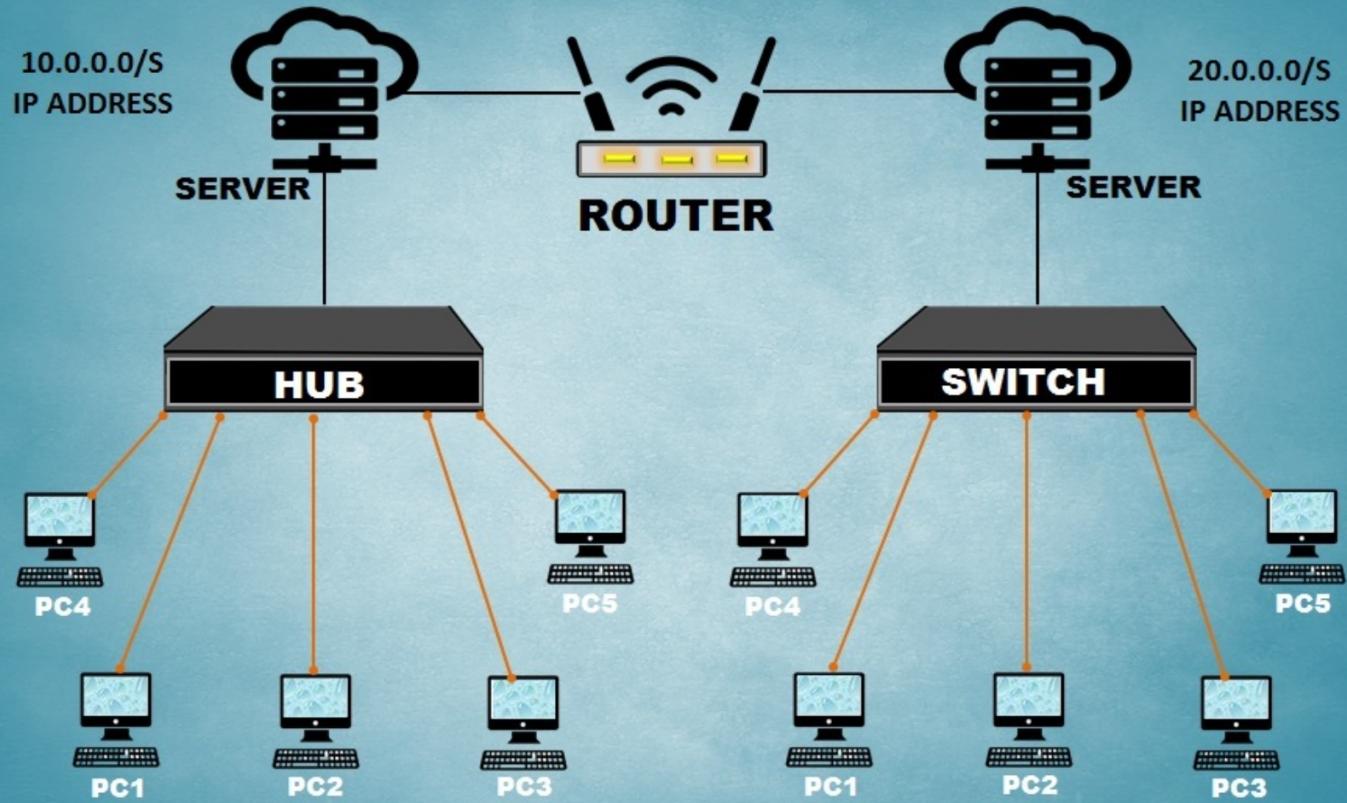
Internetworking



Router, Switch, Hub, Bridge?







Packets and Frames

▪ WHAT IS A FRAME?

- The term *frame* is most frequently used to describe a chunk of data created by network communication hardware such as a network interface cards (NIC cards) and router interfaces. Switch ports primarily forward existing frames and don't usually create frames of their own.

▪ CONTENTS OF FRAMES

- Frames contain frame delimiters, hardware addresses, such as the source and destination MAC addresses, and data encapsulated from a higher layer protocol.

Packets and Frames

▪ **WHAT IS A PACKET?**

- The Request For Comments (RFC) documents frequently use the term *packet* to mean a stream of binary octets of data of some arbitrary length. It is typically used to describe chunks of data created by software, not by hardware. Internet Protocol (IP) creates packets. This term is NOT synonymous with the term *frame* even though many people make that mistake. Information that has been broken into packets is sometimes described as *packetized*.

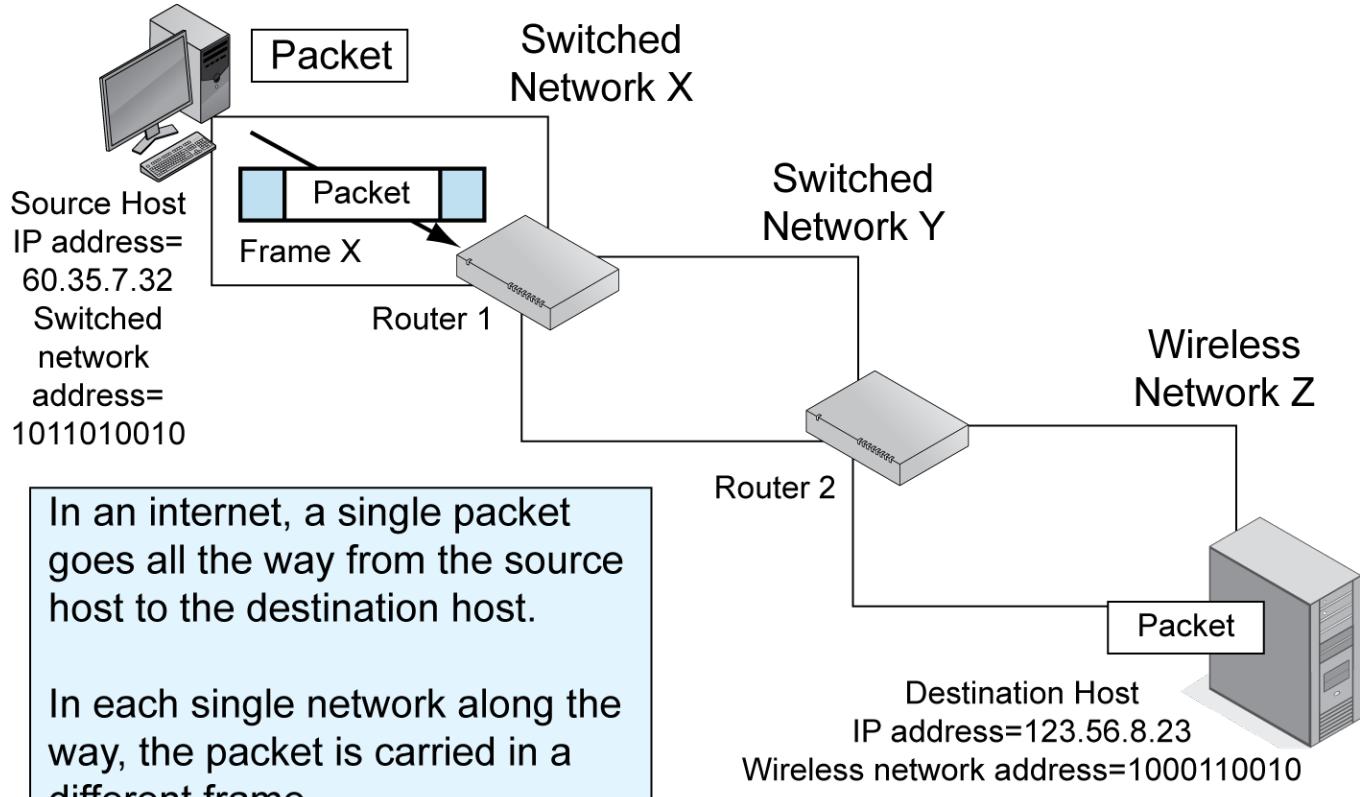
▪ **Types of Packets**

- Internet Protocol is often described as transmitting packets.

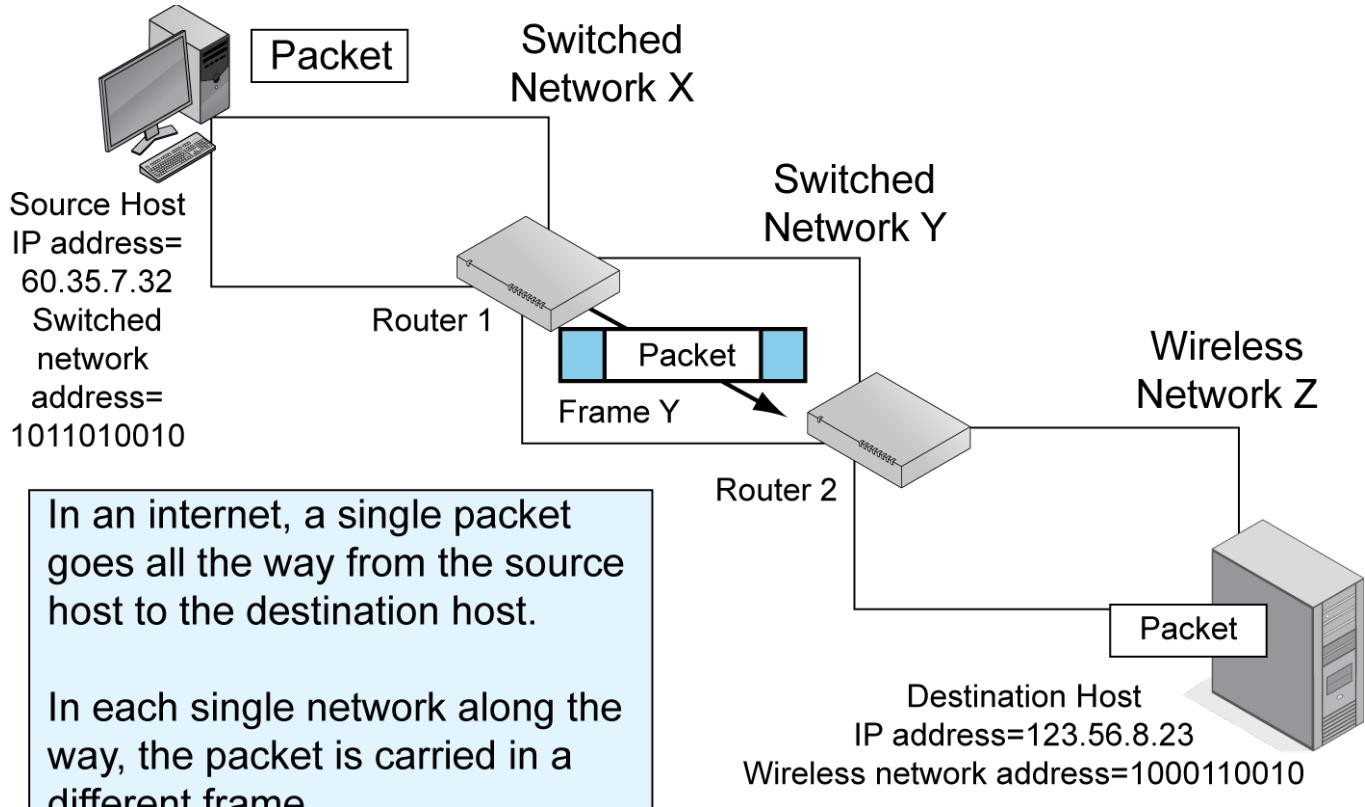
• **Contents of Packets**

- Packets contain logical addressing information, such as an IP address, and data.

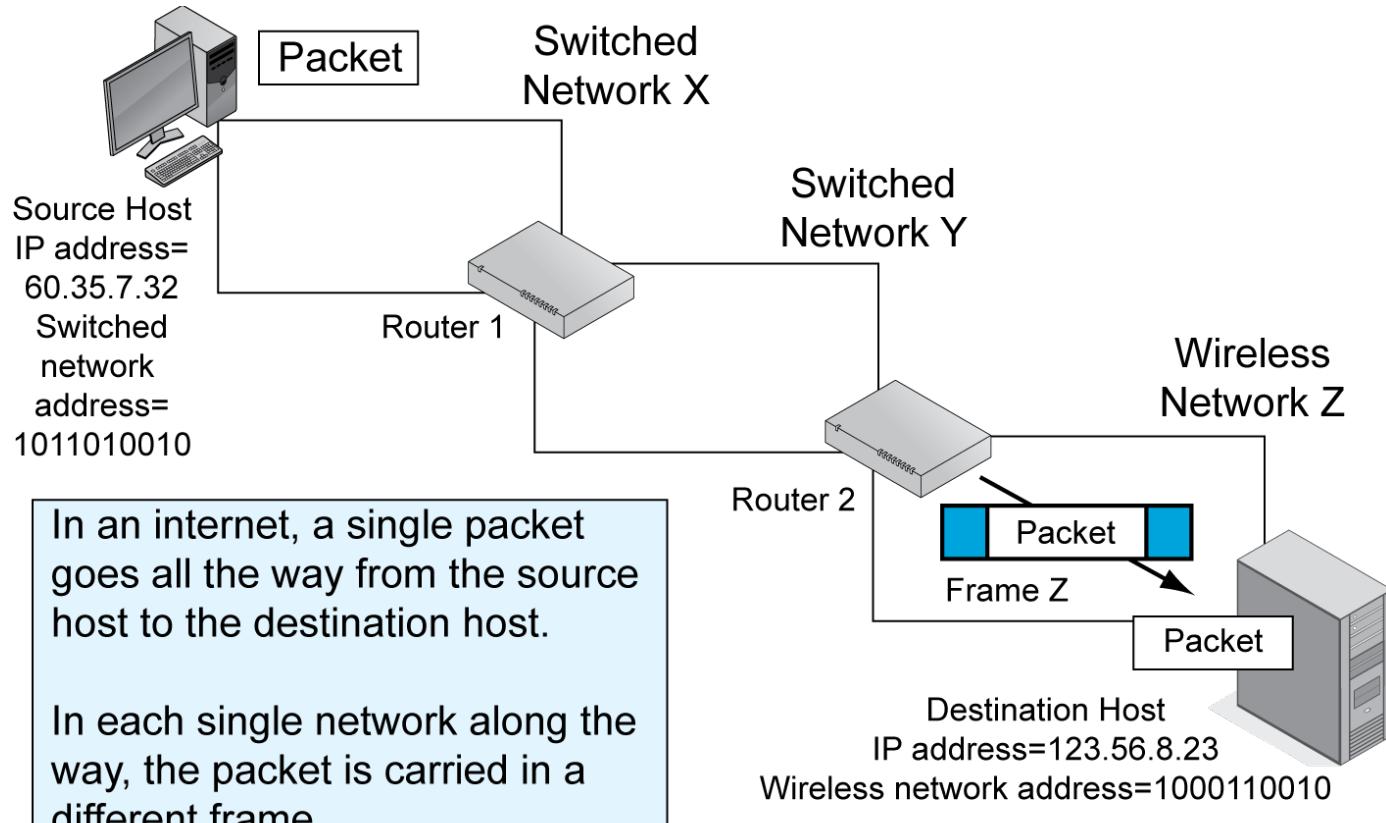
Packets and Frames



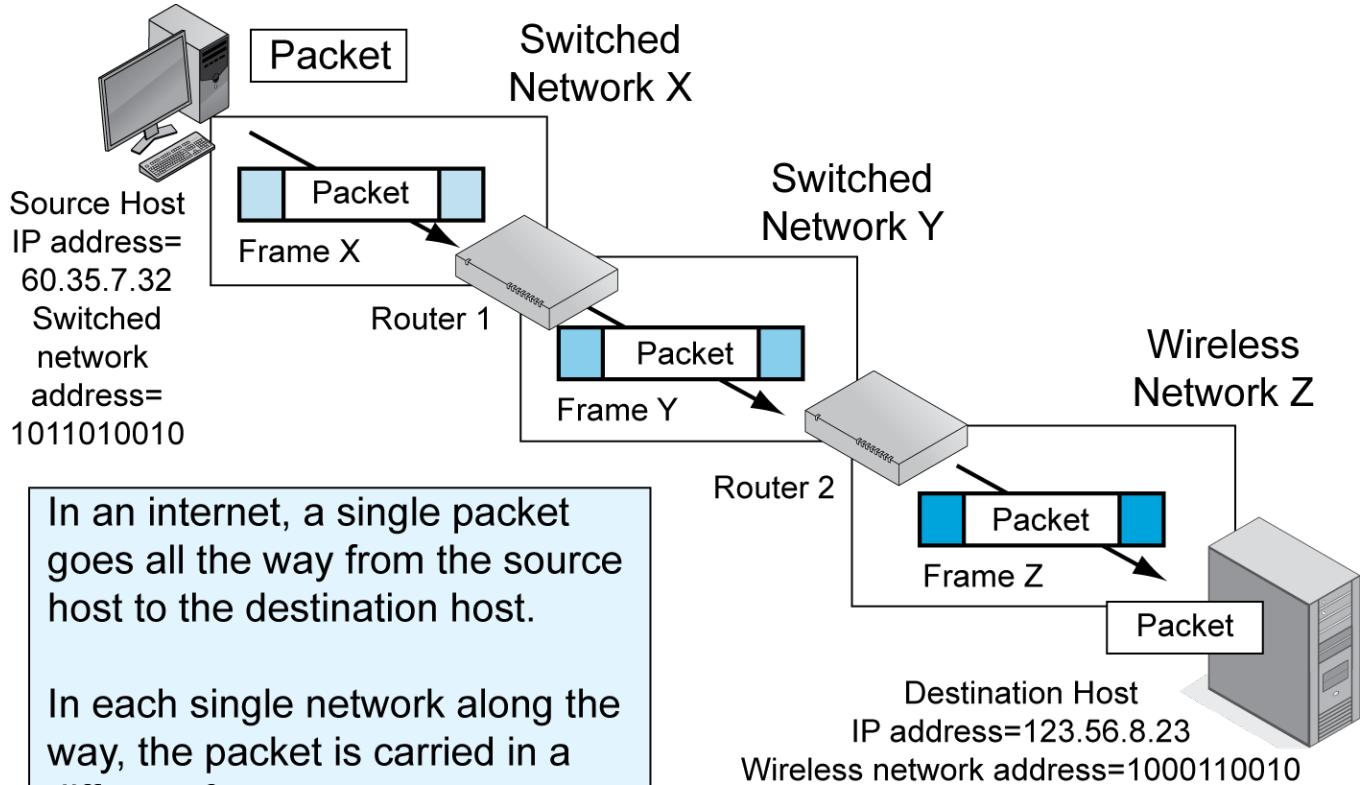
Packets and Frames



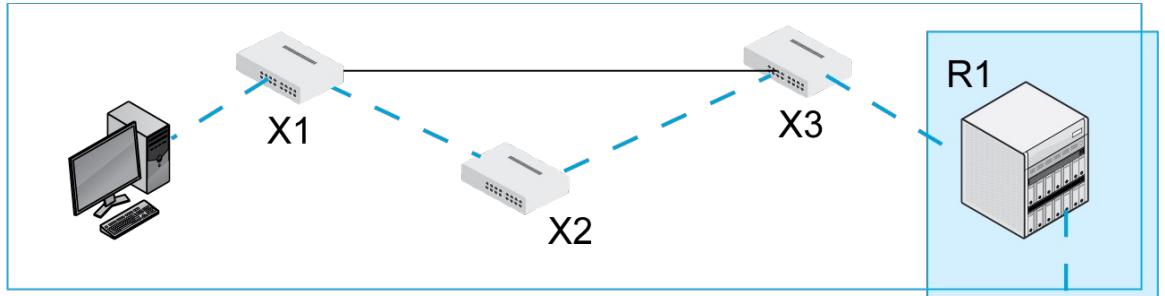
Packets and Frames



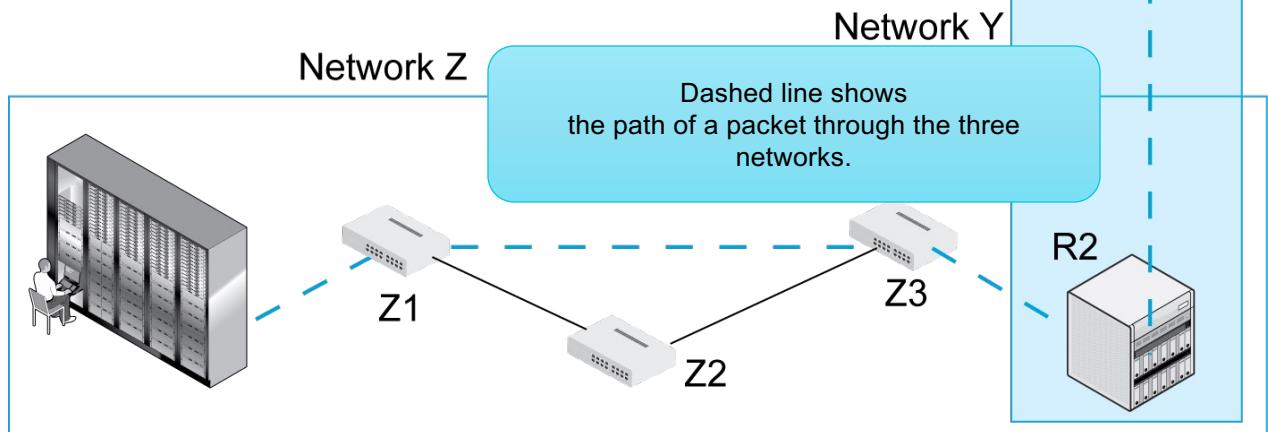
Packets and Frames



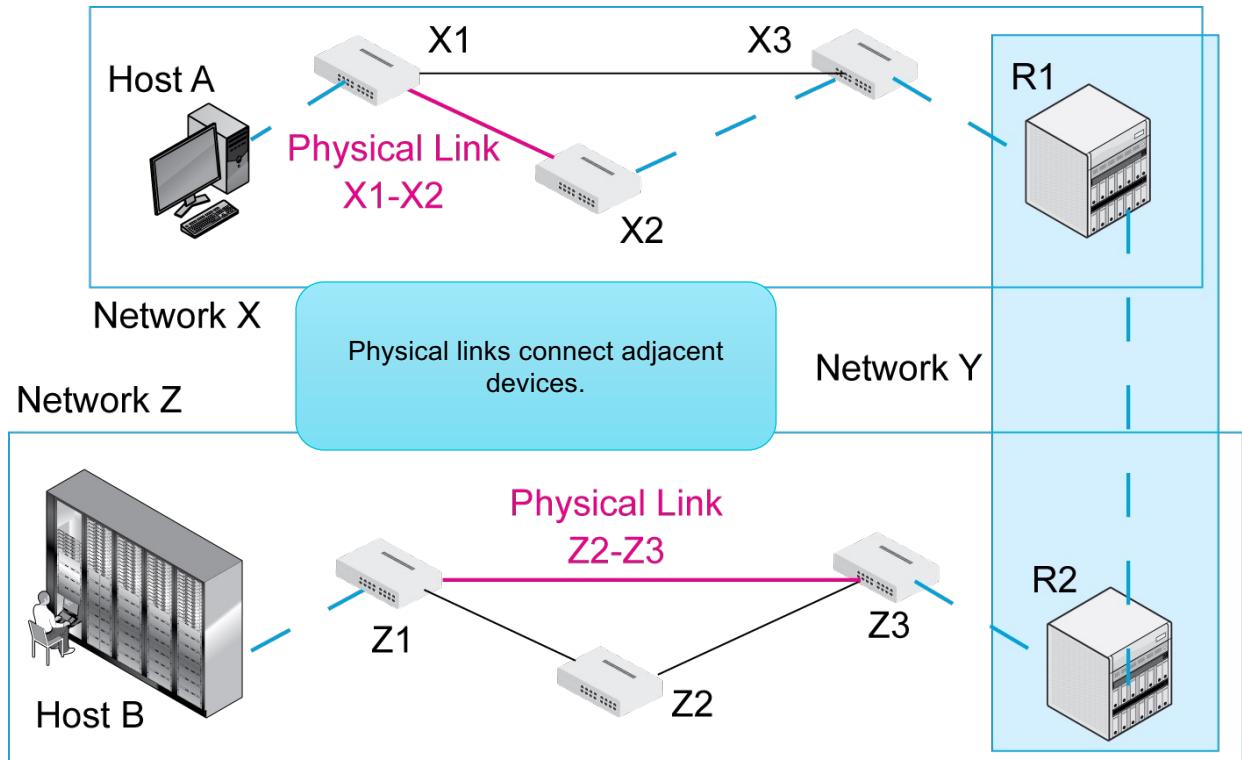
Physical Links, Data Links, and Routes



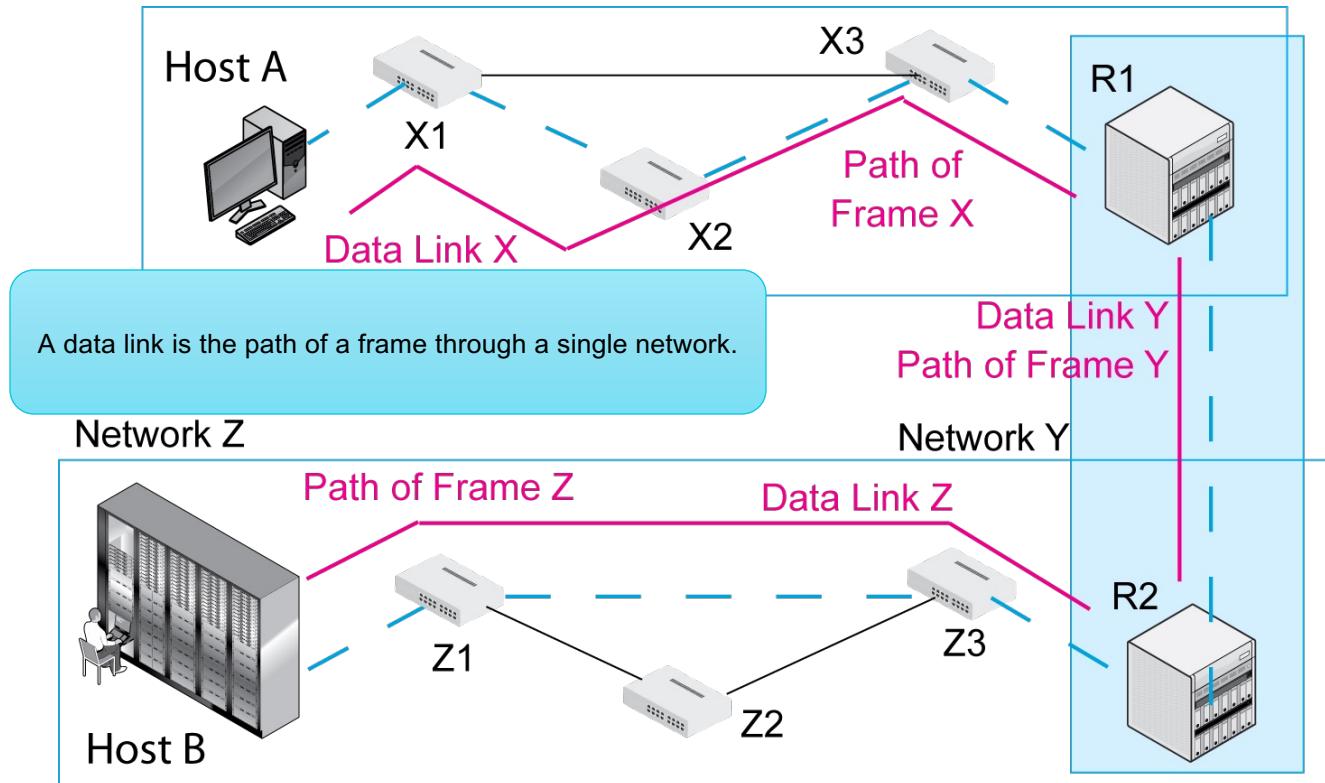
Network X



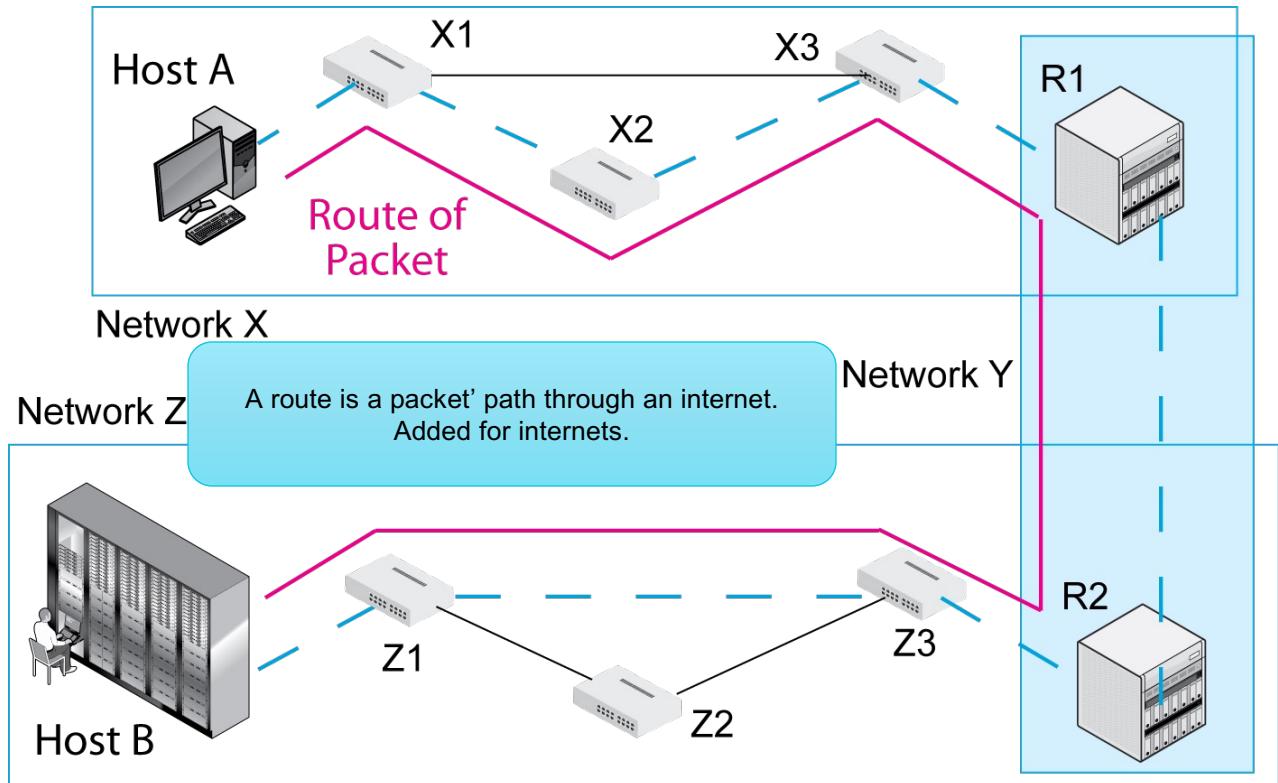
Physical Links, Data Links, and Routes



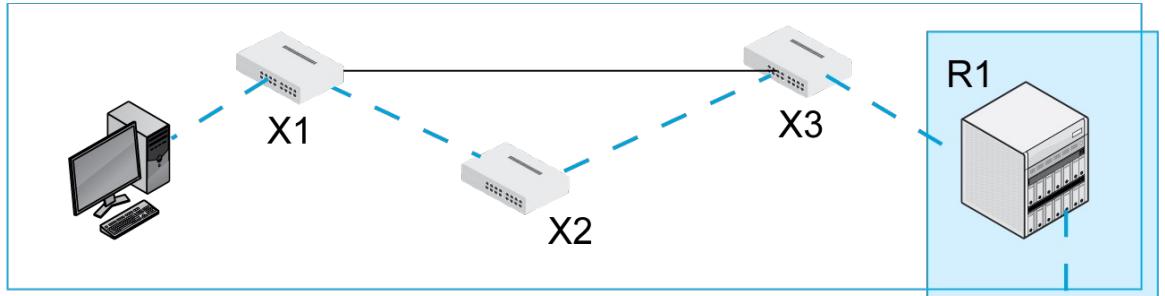
Physical Links, Data Links, and Routes



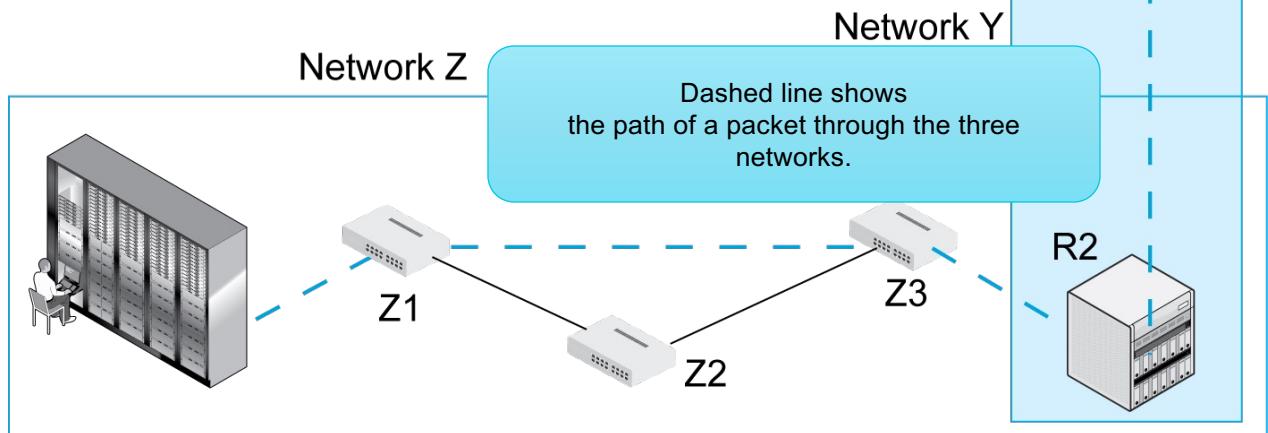
Physical Links, Data Links, and Routes



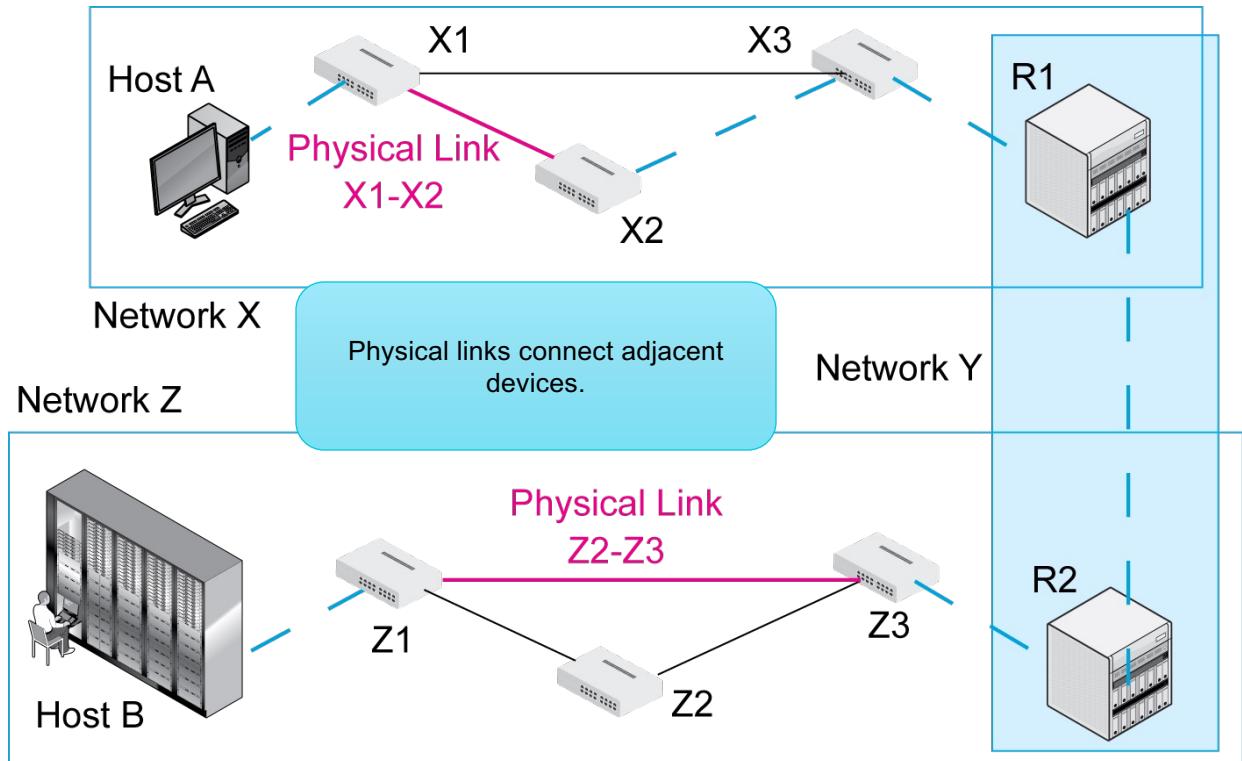
Physical Links, Data Links, and Routes



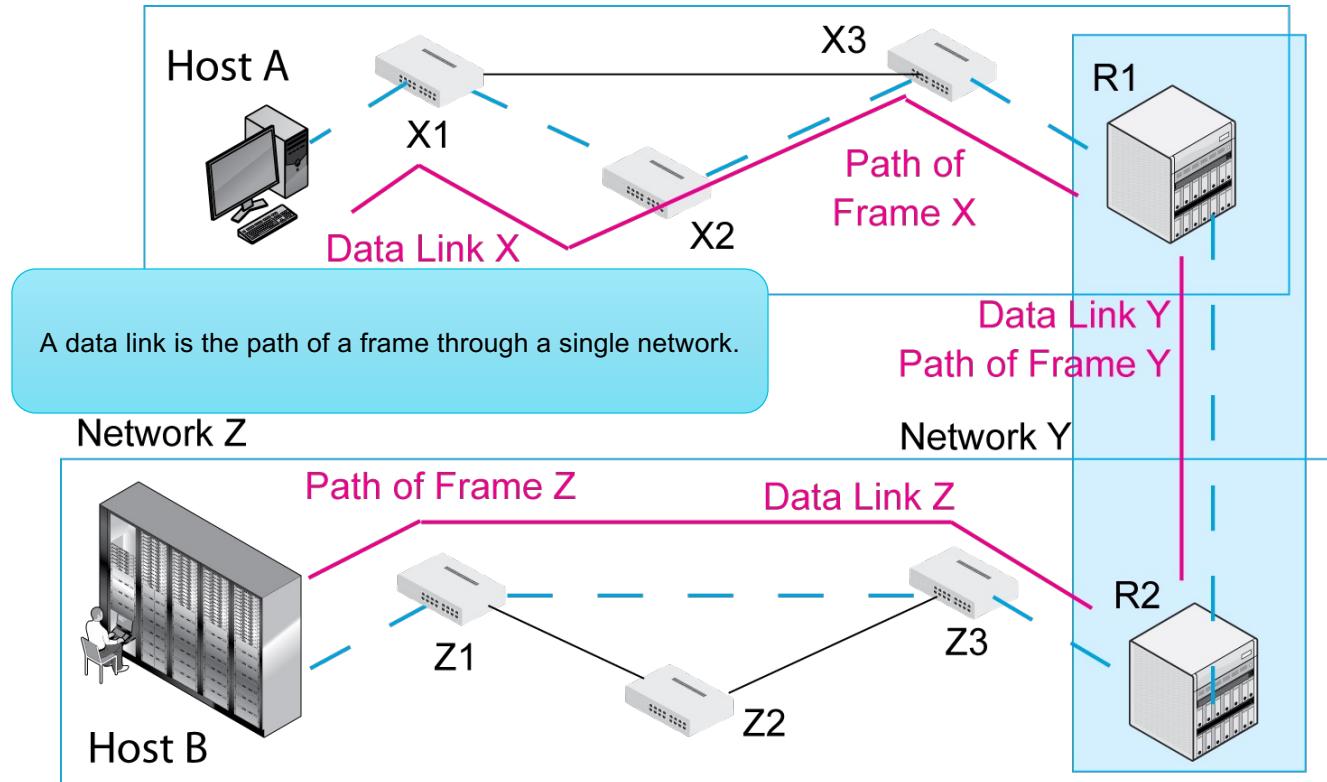
Network X



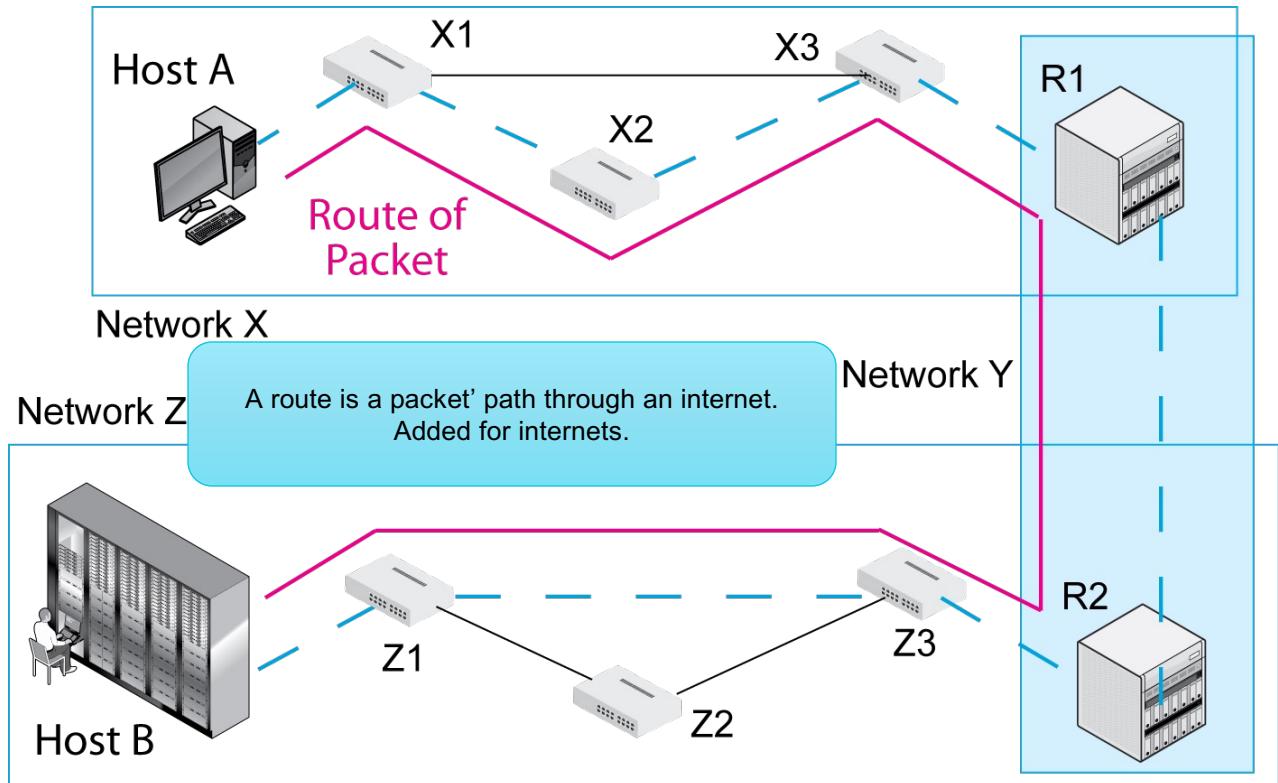
Physical Links, Data Links, and Routes



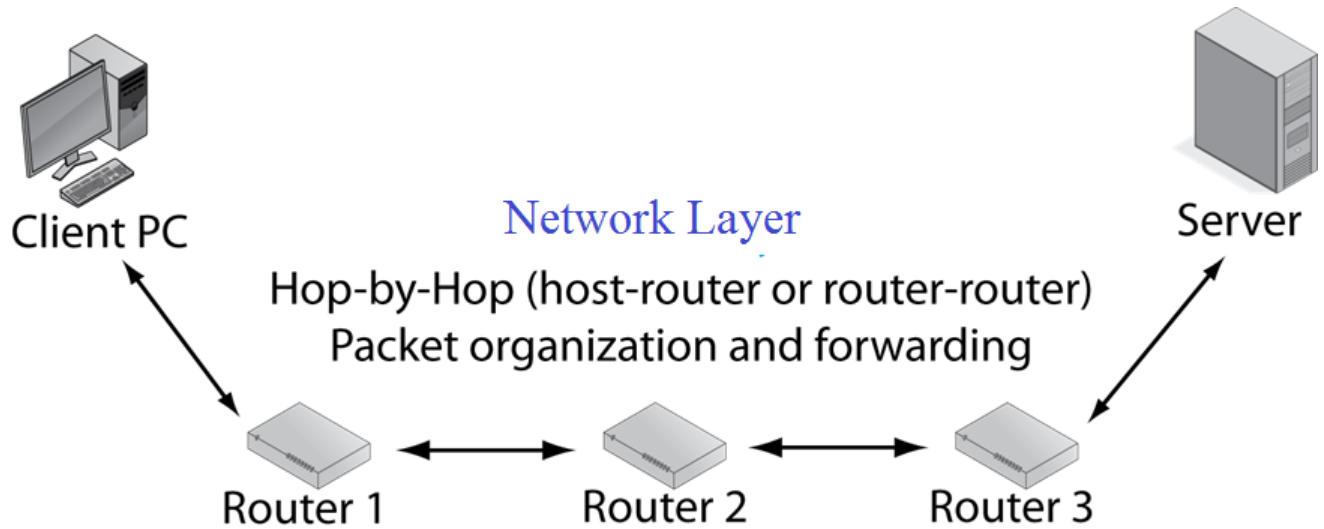
Physical Links, Data Links, and Routes



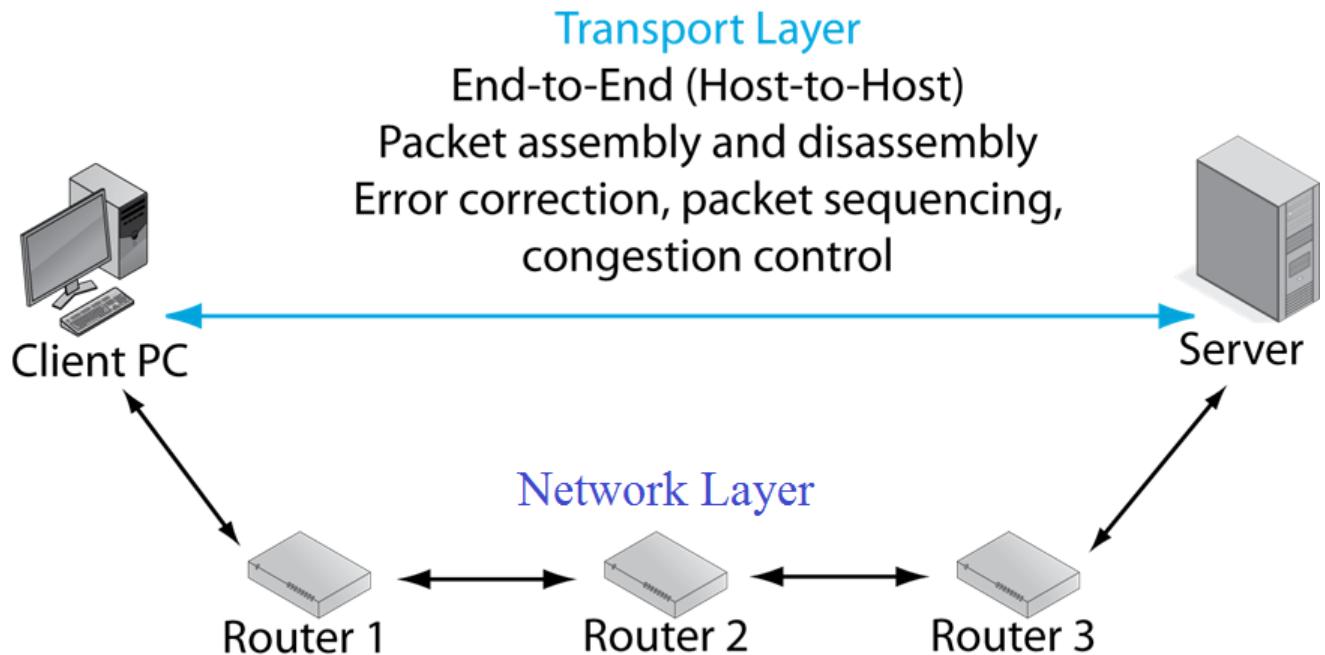
Physical Links, Data Links, and Routes



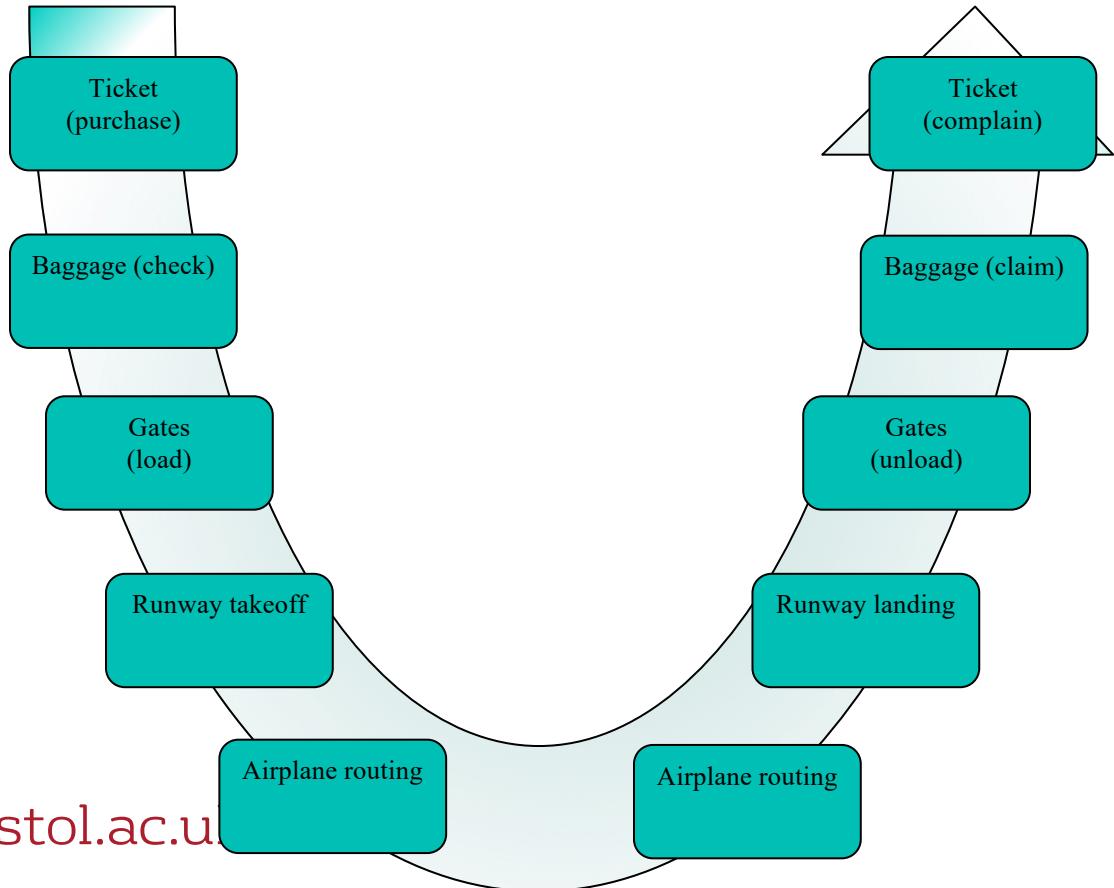
The Network and Transport Layers



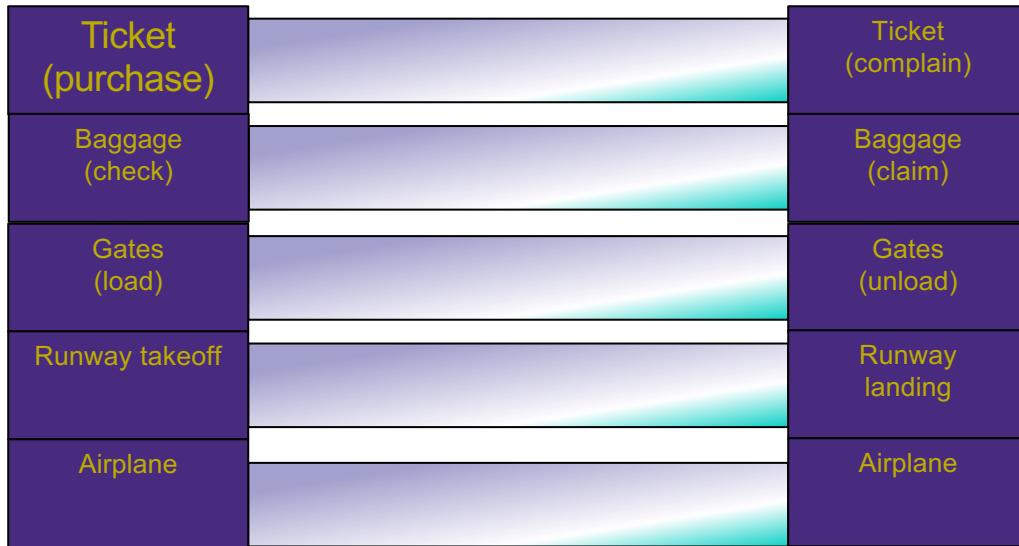
The Network and Transport Layers



Taking an airplane: actions



Again – Airplane example



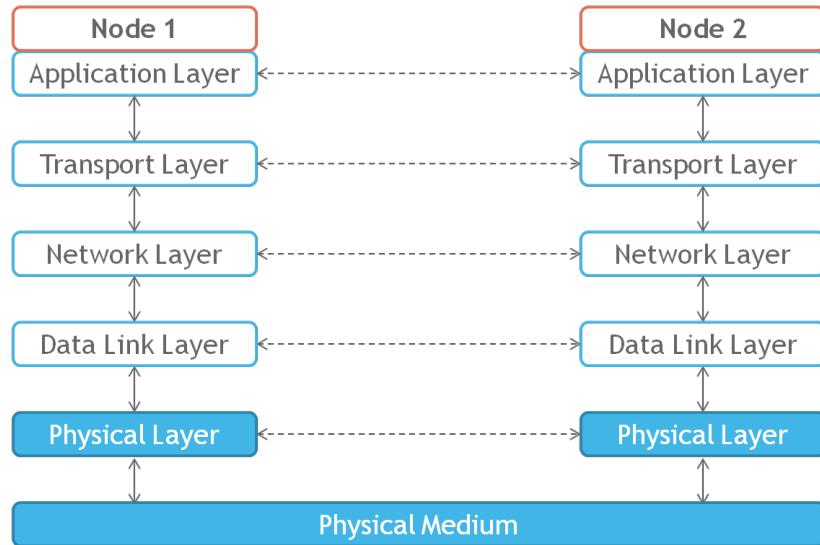
Departure
airport

Arrival
airport

ISO/OSI model

Layer	Description	Protocols
Application	This layer interfaces directly to applications and performs common application services for the application processes.	POP, SMTP, DNS, FTP, Telnet
Presentation	The presentation layer relieves the application layer of concern regarding syntactical differences in data representation within the end-user systems.	Telnet, Network Data Representation (NDR), Lightweight Presentation Protocol (LPP)
Session	The session layer provides the mechanism for managing the dialogue between end-user application processes.	NetBIOS
Transport	This layer provides end-to-end communication control.	TCP, UDP
Network	This layer routes the information in the network.	IP, ARP, ICMP
Data link	This layer describes the logical organization of data bits transmitted on a particular medium. The data link layer is divided into two sublayers: the Media Access Control layer (MAC) and the Logical Link Control layer (LLC).	SLIP, PPP
Physical	This layer describes the physical properties of the various communications media, as well as the electrical properties and interpretation of the exchanged signals. In other words, the physical layer is the actual NIC, Ethernet cable, and so forth.	IEEE 1394, DSL, ISDN

TCP/IP model



Five Layers in the Internet Network Model

1. Physical Layer:

- Is the physical connection between the sender and the receiver.
- It includes all the hardware devices (computers, modems, and hubs) and physical media (cables and satellites).
- This layer specifies the type of connection and the electrical signals, radio waves, or light pulses that pass through it.

Five Layers in the Internet Network Model

2. Data Link Layer:

- Is responsible for moving a message from one computer to the next computer in the network path from the sender to the receiver. This layer has 3 functions:
 - Control the physical layer by deciding when to transmit messages over the media.
 - Format the messages by creating a frame to encapsulate packets and add a header to it.
 - Detects and recovers from errors that have occurred during transmission.

Five Layers in the Internet Network Model

3. Network Layer:

- Routing, selecting the next computer to which the message should be sent.
- Find the address of that computer if it doesn't already know it.

Five Layers in the Internet Network Model

4. Transport Layer:

- It performs three functions:
 - It is responsible for linking the application layer software to the network and establishing end-to-end connections between the sender and receiver when such connections are needed.
 - It breaks long messages into several smaller messages to make them easier to transmit.
 - Detect lost messages and request that they be resent.

Five Layers in the Internet Network Model

5. Application Layer:

- This is the application software used by the network user.
- With this layer the user defines what messages are sent over the network.
- Examples of this layer are the internet explorer and outlook.

Networking Layers

Number	Name	Broad Purpose	Specific Purpose
5	Application	Communication between applications	Same
4	Transport		
3	Network		
2	Data Link		
1	Physical		

Networking Layers

Layer	Name	Broad Purpose	Specific Purpose
5	Application		
4	Transport	Internet Transmission	Application message fragmentation, error correction, congestion reduction, etc.
3	Network		Transmission of packet across an internet. Packet formats, router operation.
2	Data Link		
1	Physical		

Networking Layers

Layer	Name	Broad Purpose	Specific Purpose
5	Application		
4	Transport		
3	Internet		
2	Data Link	Single-network transmission (switched or wireless)	Connection across a single network. Frame formats and switch operation.
1	Physical		Physical connections between adjacent devices

Network Access Security Model

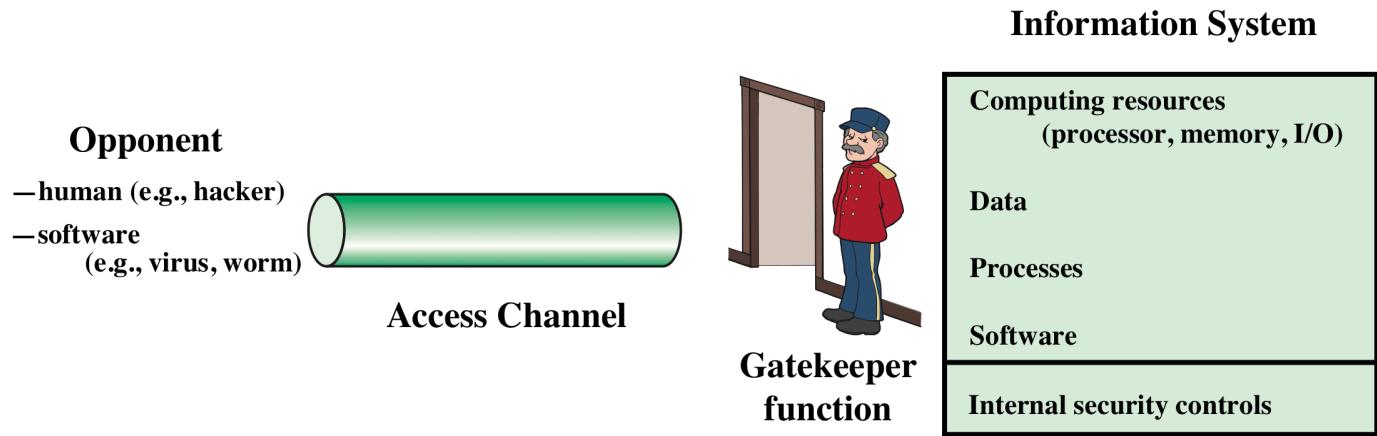


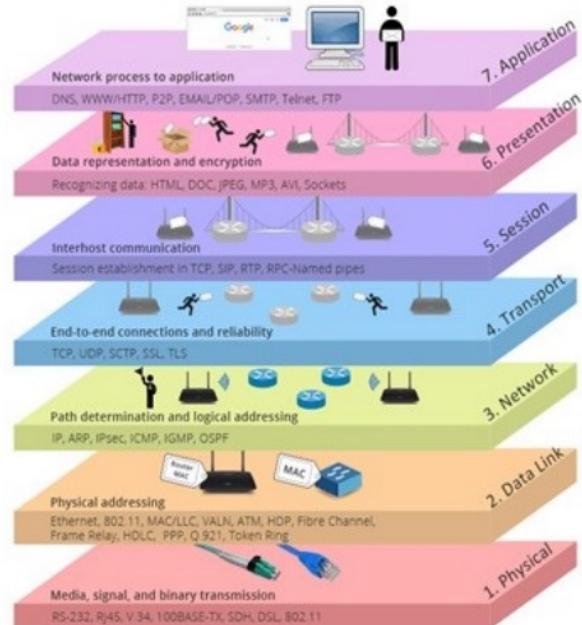
Figure 1.3 Network Access Security Model

Unwanted Access

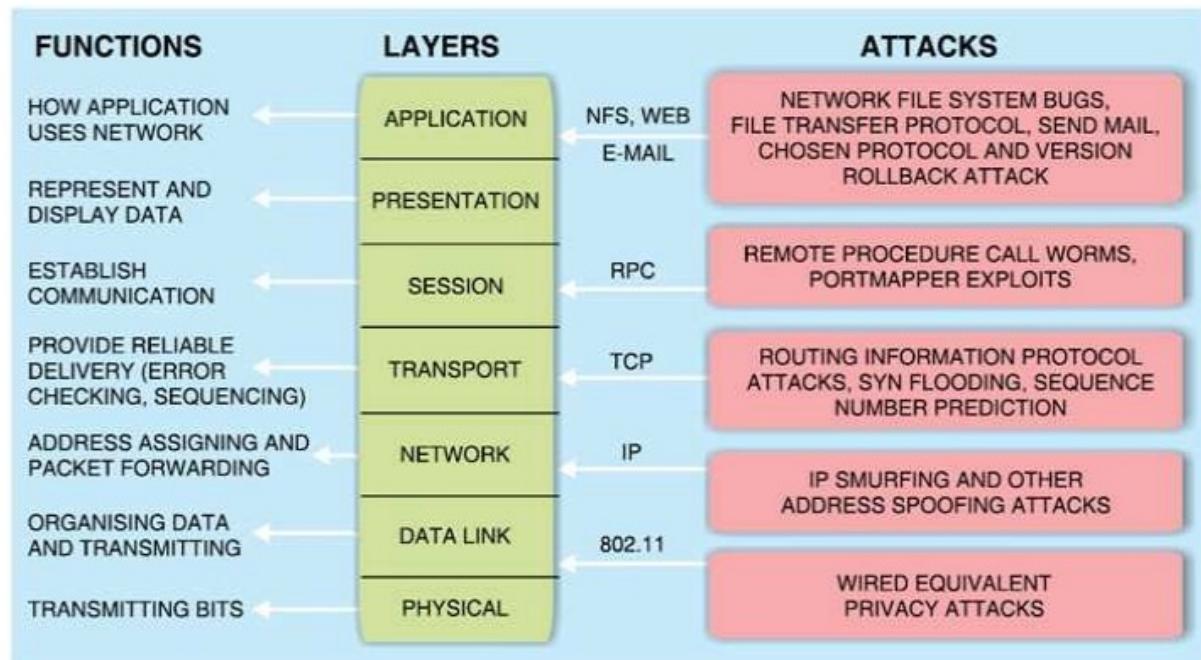
- Placement in a computer system of logic that exploits vulnerabilities in the system and that can affect application programs as well as utility programs such as editors and compilers
- Programs can present two kinds of threats:
 - Information access threats
 - Intercept or modify data on behalf of users who should not have access to that data
 - Service threats
 - Exploit service flaws in computers to inhibit use by legitimate users



ISO/OSI



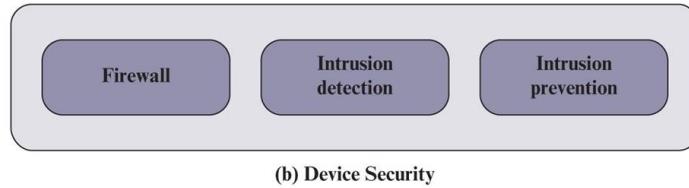
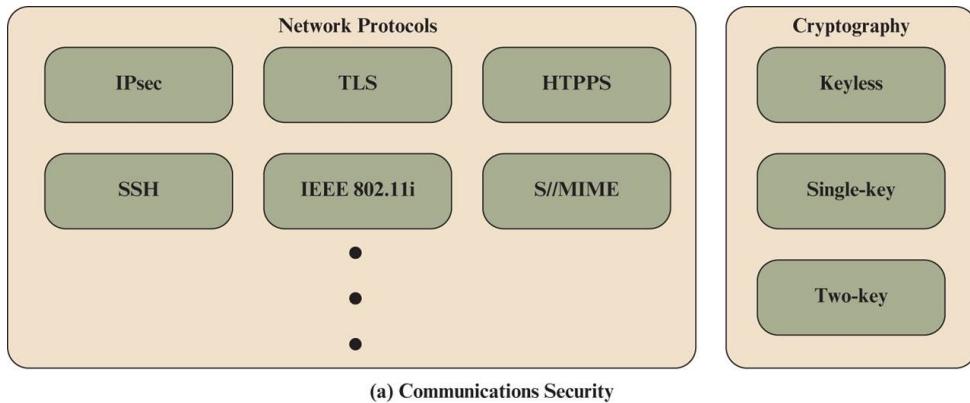
Attacks on different layers



Attacks on different layers

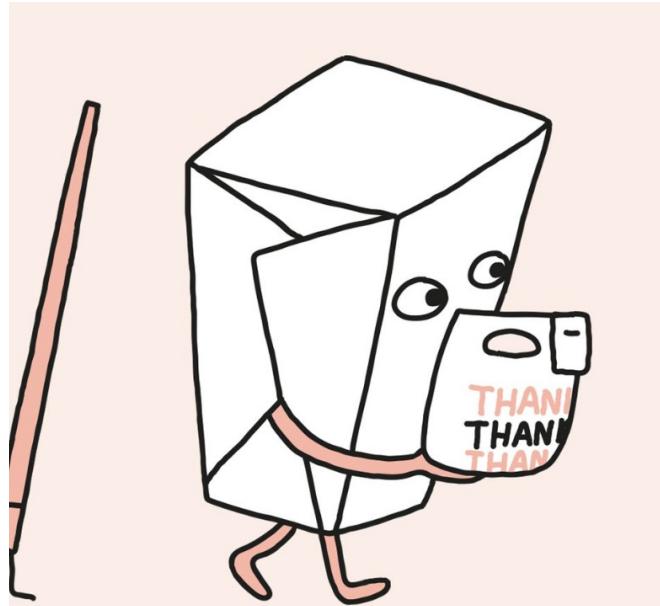
Layers	Attacks
Application layer	Repudiation, Data Corruption
Transport layer	Session Hijacking, Sync flooding
Network layer	Warm-hole, Black-hole, Gray-hole, Byzantine, Flooding, Resource consumption, Location-disclosure, Sybil attack, Jelly-fish, Fabrication, Modification attack
Data-Link layer	Traffic analysis, Monitoring, Disruption MAC(802.11), WEP weakness, Selfish-node
Physical layer	Jamming, Interception, Eavesdropping
Multi-layer Attacks	Dos attacks, Impersonation, Replay, Man-in-the-middle

What we will learn next time?



What did we learn today?

- Classical Encryption Techniques
- First virus
- What is network security?
- Model for network security
- Basics of networking!
- Attacks on different layers





bristol.ac.uk