University of BRISTOL

Computer System B

bristol.ac.uk

University of BRISTOL

What did we learn?

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

bristol.ac.uk

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

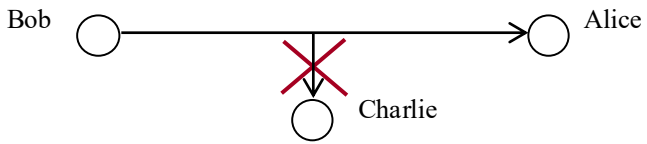
Integrity

- 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

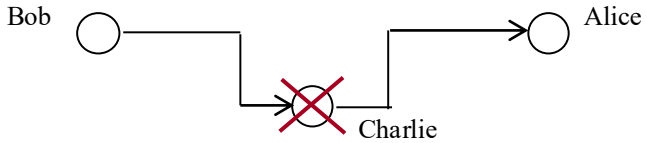
Availability

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

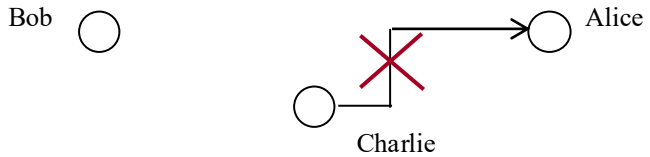
1. Confidentiality

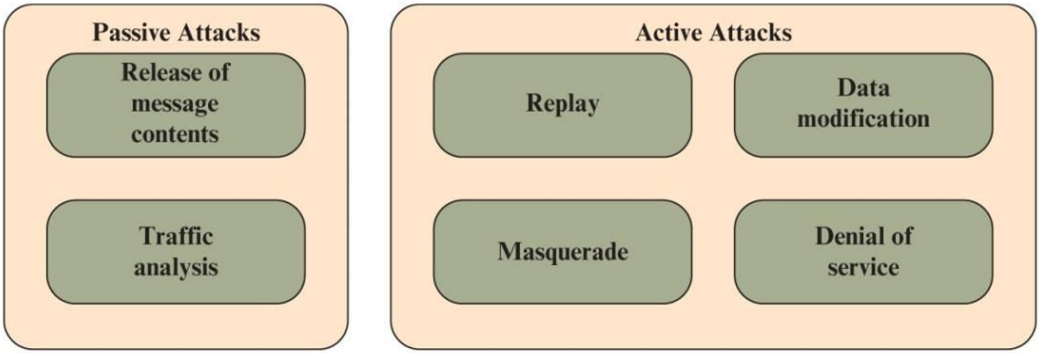


2. Message integrity

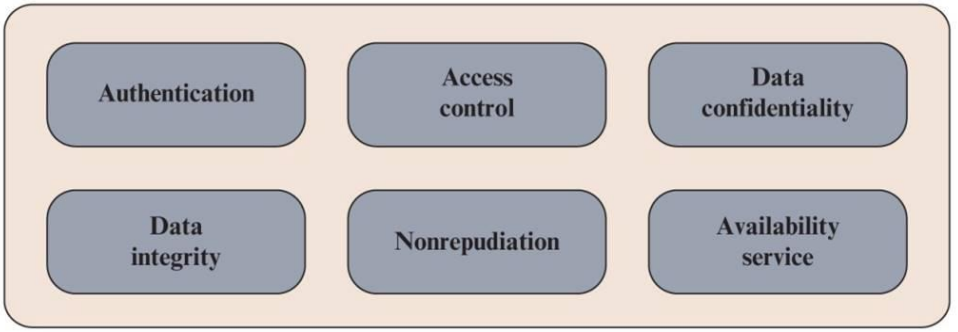


3. Message authentication

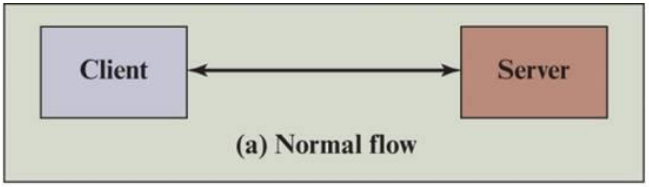




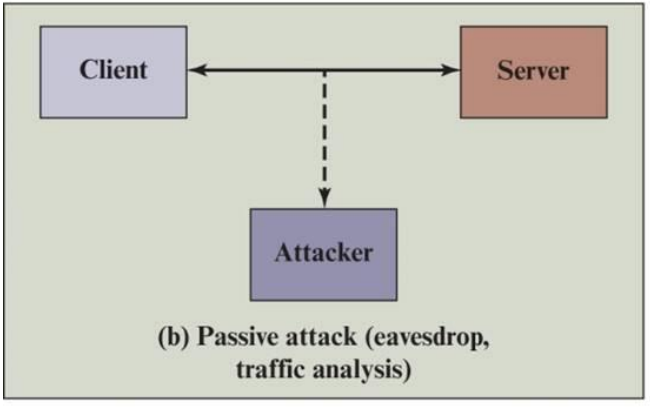
(a) Attacks



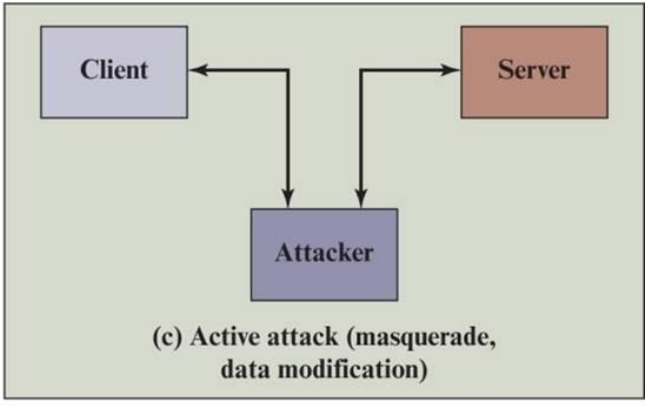
(b) Services



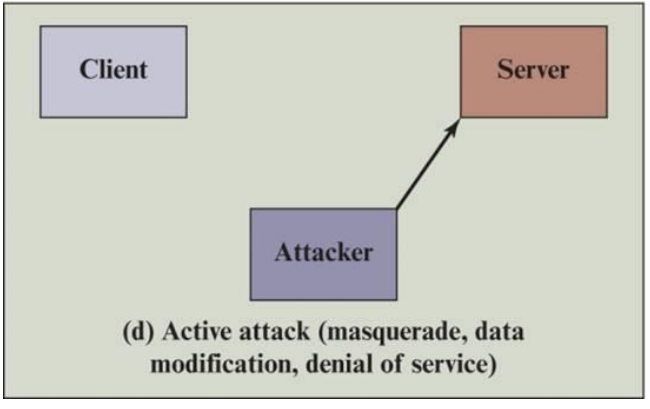
(a) Normal flow



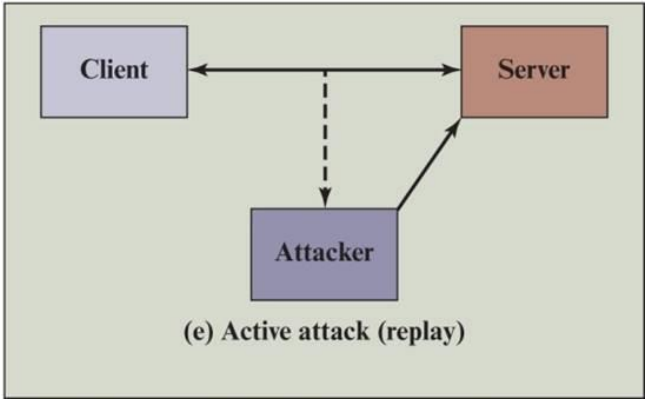
(b) Passive attack (eavesdrop, traffic analysis)



(c) Active attack (masquerade, data modification)



(d) Active attack (masquerade, data modification, denial of service)



(e) Active attack (replay)

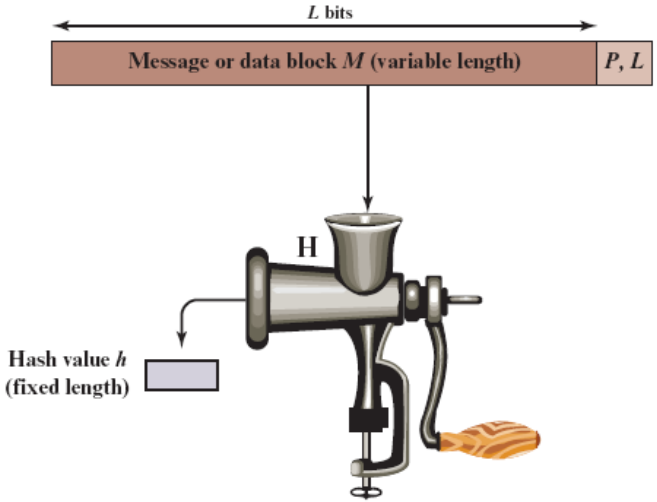
Security Mechanisms (1 of 2)

- **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* = 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

University of BRISTOL

Today!

- Introduction to Cryptography!
- Introduction to Network Security

bristol.ac.uk

University of BRISTOL

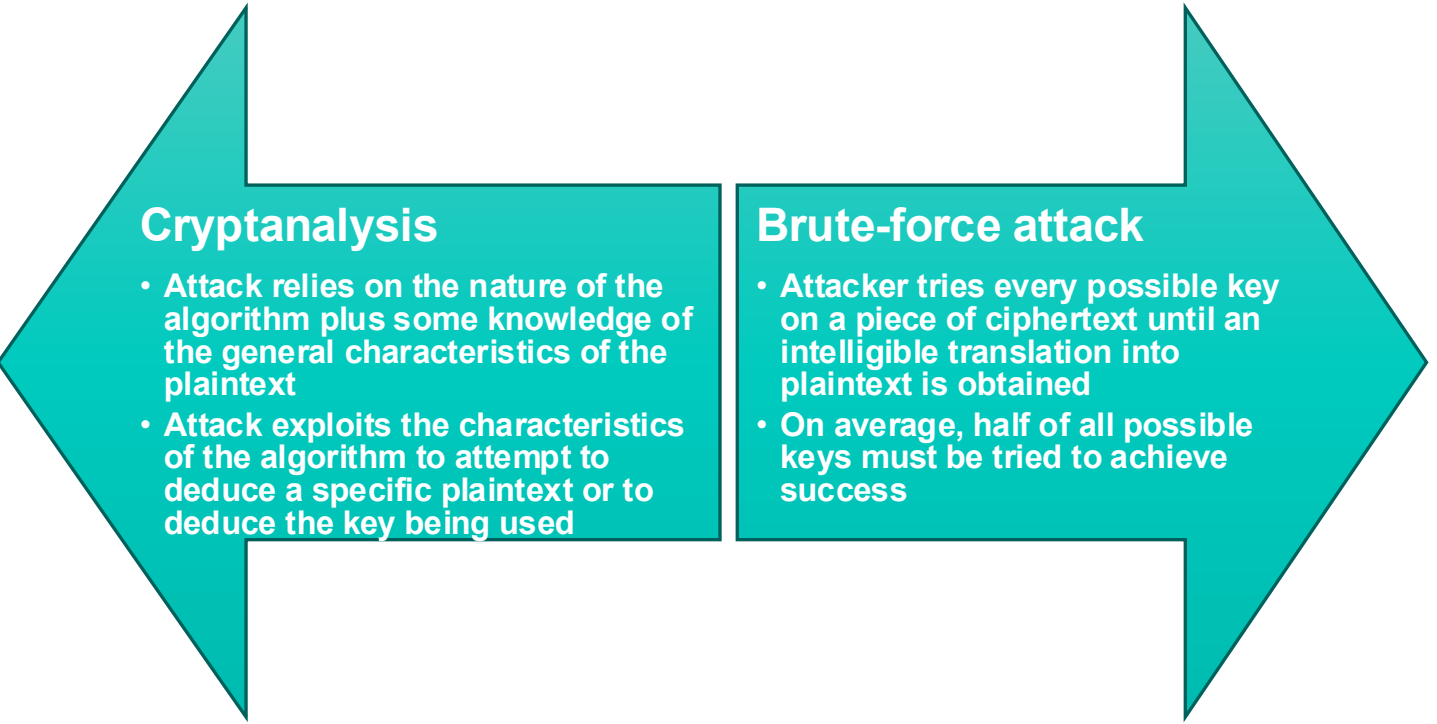
Classical Encryption Techniques

bristol.ac.uk

Basic Terminology

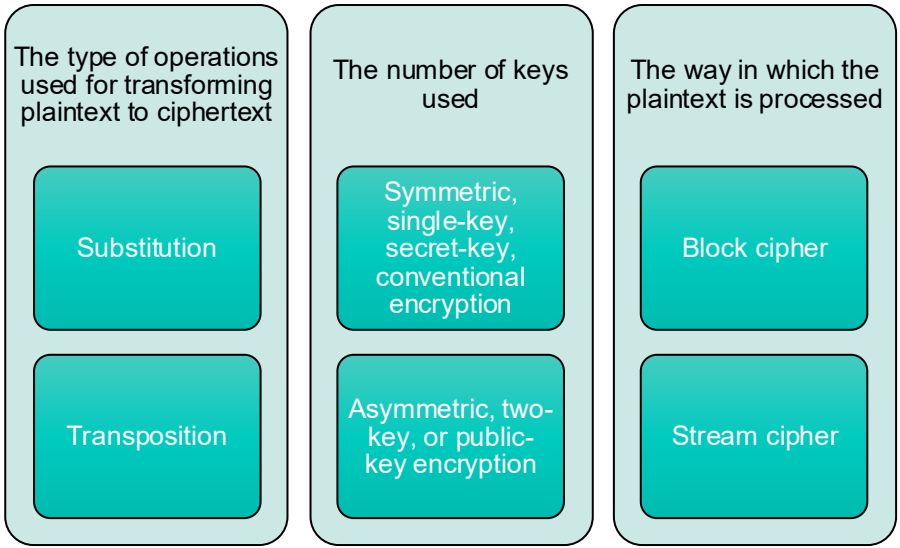
- Plaintext
  - The original message
- Ciphertext
  - The coded message
- Enciphering or encryption
  - Process of converting from plaintext to ciphertext
- Deciphering or decryption
  - Restoring the plaintext from the ciphertext
- Cryptography
  - Study of encryption
- Cryptographic system or cipher
  - 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



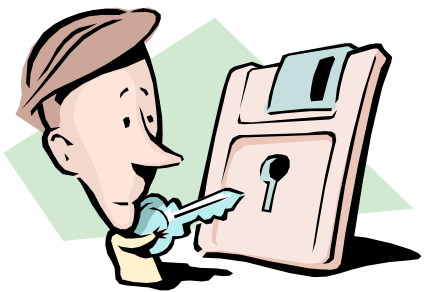
Cryptographic Systems

- Characterized along three independent dimensions:

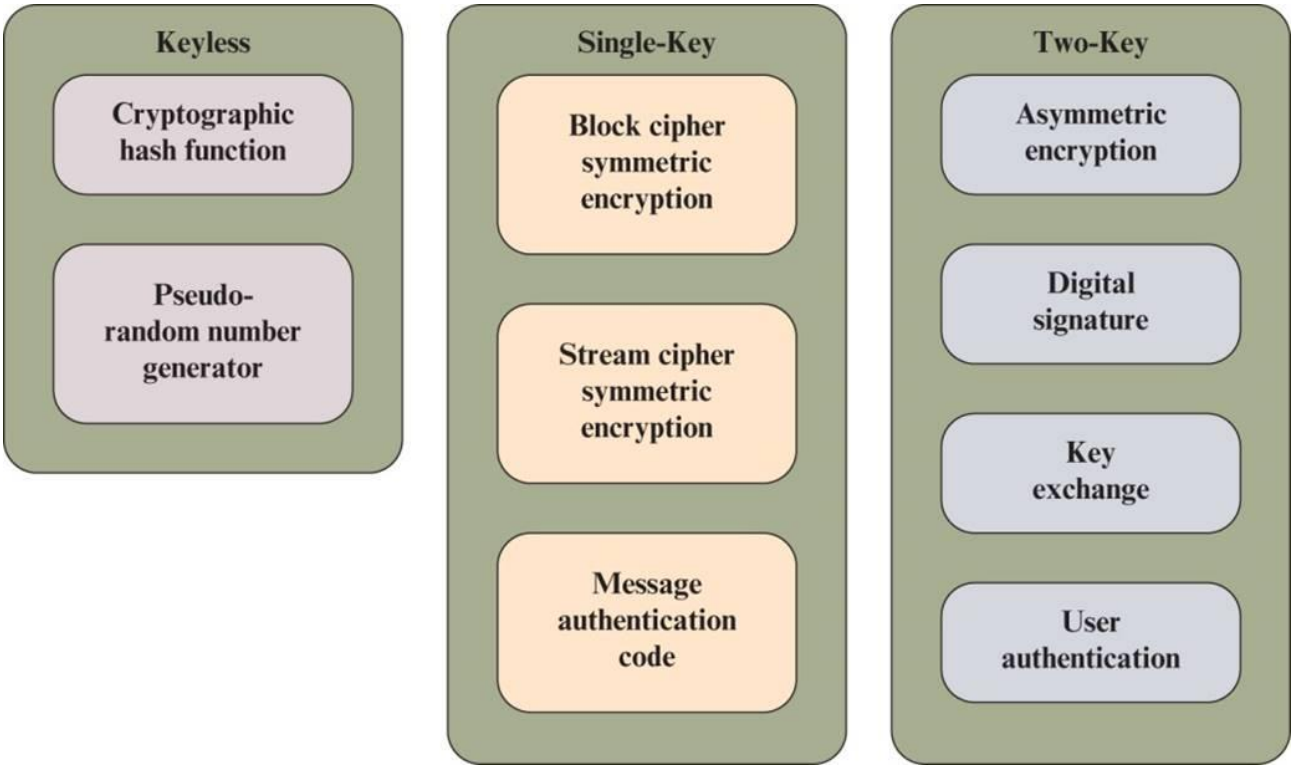


Cryptographic Systems

- 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



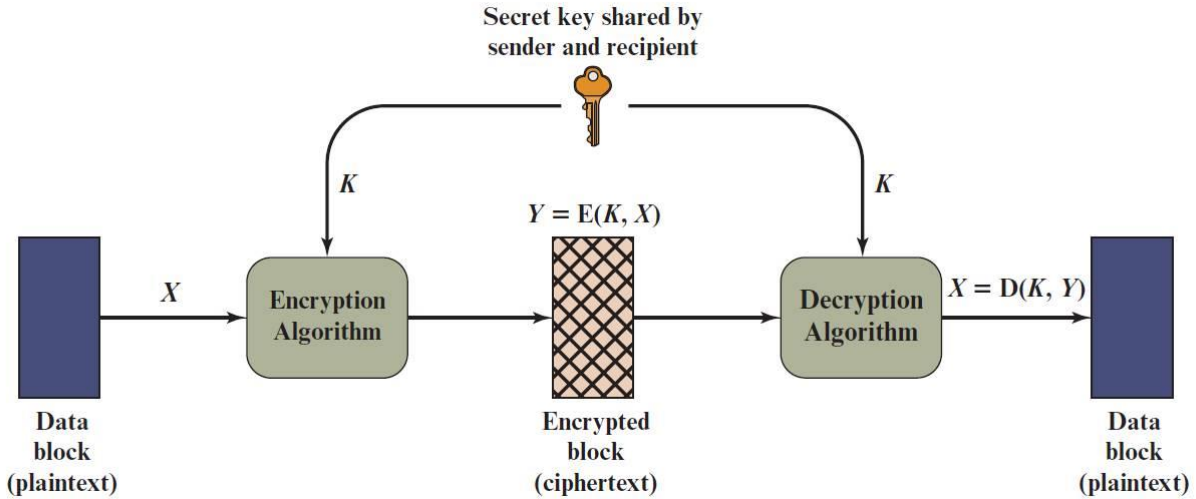
Cryptographic Algorithms based on number of keys



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



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

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

University of BRISTOL

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

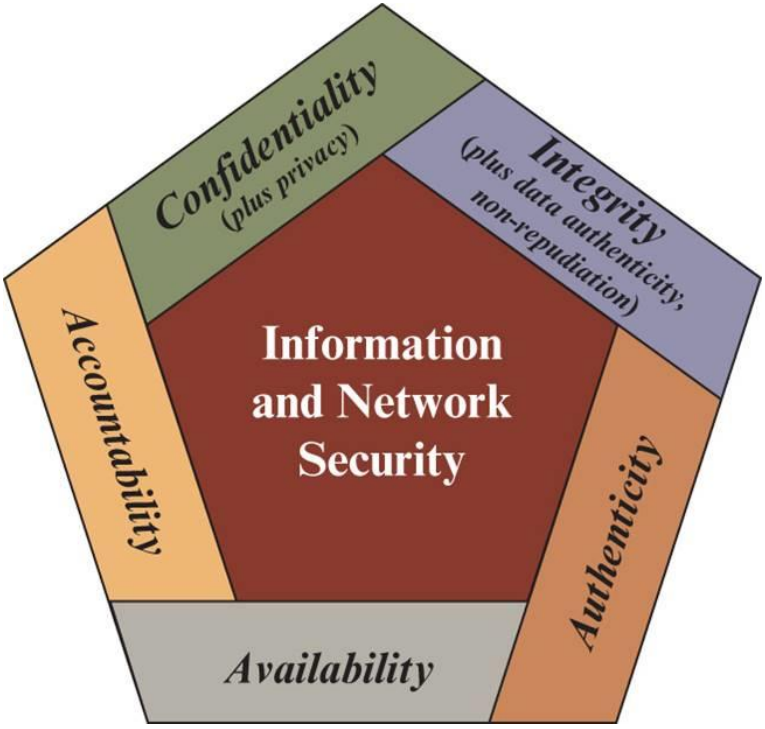
Cybersecurity

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

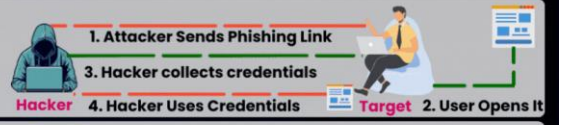

Confidentiality
(plus privacy)
Integrity
(plus data authenticity, non-repudiation)
Information and Network Security
Accountability
Authenticity
Availability

Top 8 Cyber Attacks - 2024

Cyber Writes

1 Phishing Attack

The use of deceptive emails, texts, or websites to gain sensitive information.



2 Ransomware

Malware that can encrypt data and make you pay to get them back.

3 Denial-of-Service (DoS)

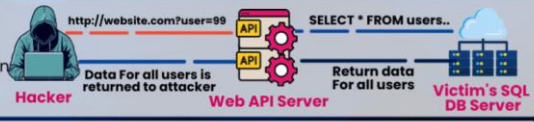
Loading excessive load on a machine or network so that it stops working normally.

4 Man-in-the-Middle (MitM)

Engaging in covert interception and manipulation of communication between two parties without noticing it.

5 SQL Injection

To get the Access to the database, Vulnerabilities in Database queries can be exploited



6 Cross-Site Scripting (XSS)

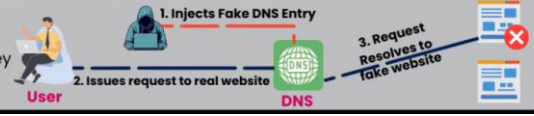
Putting malicious code into websites that other people visit.

7 Zero-Day Exploits

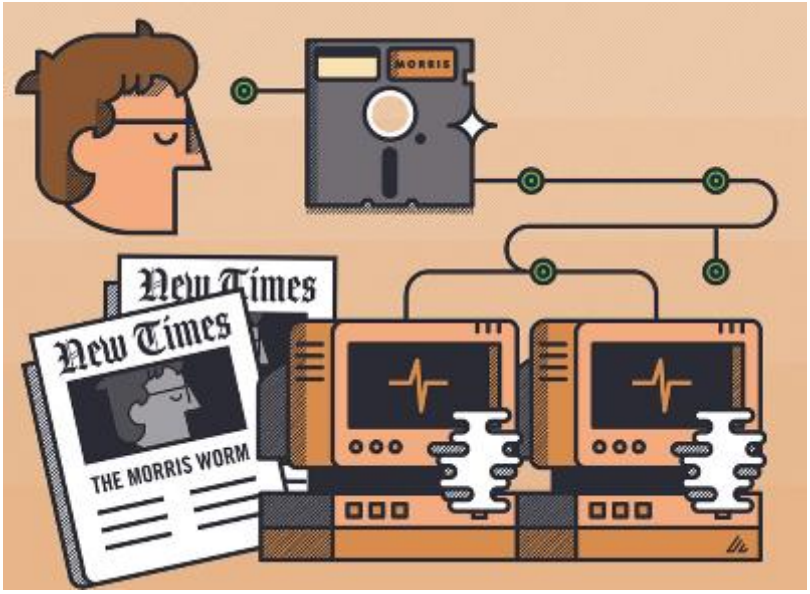
Attacks take advantage of unknown vulnerabilities before programmers can fix them.

8 DNS Spoofing

Sending DNS queries to malicious sites so that they can be accessed without permission.



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?

What is network security?

Model for Network Security

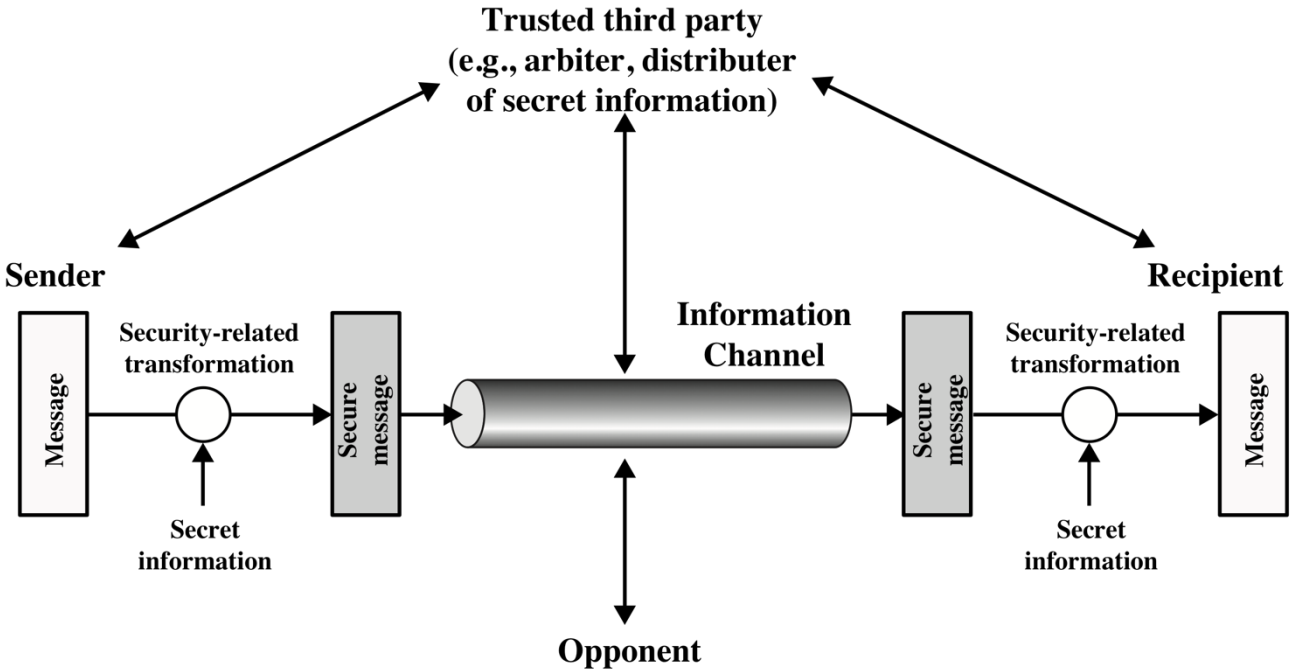


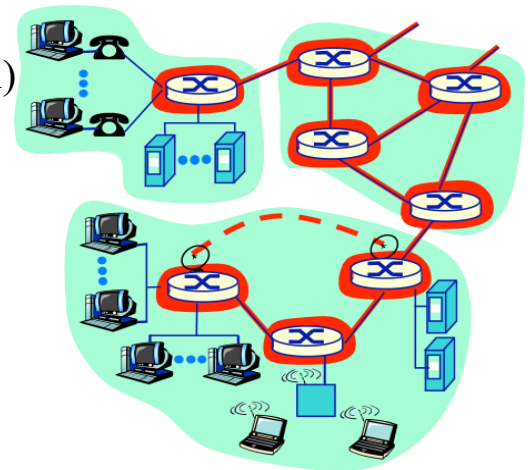
Figure 1.2 Model for Network Security

Network Structure

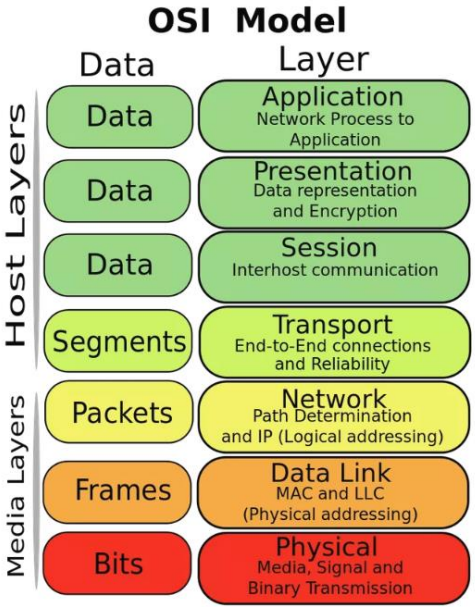
The network core

- 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"

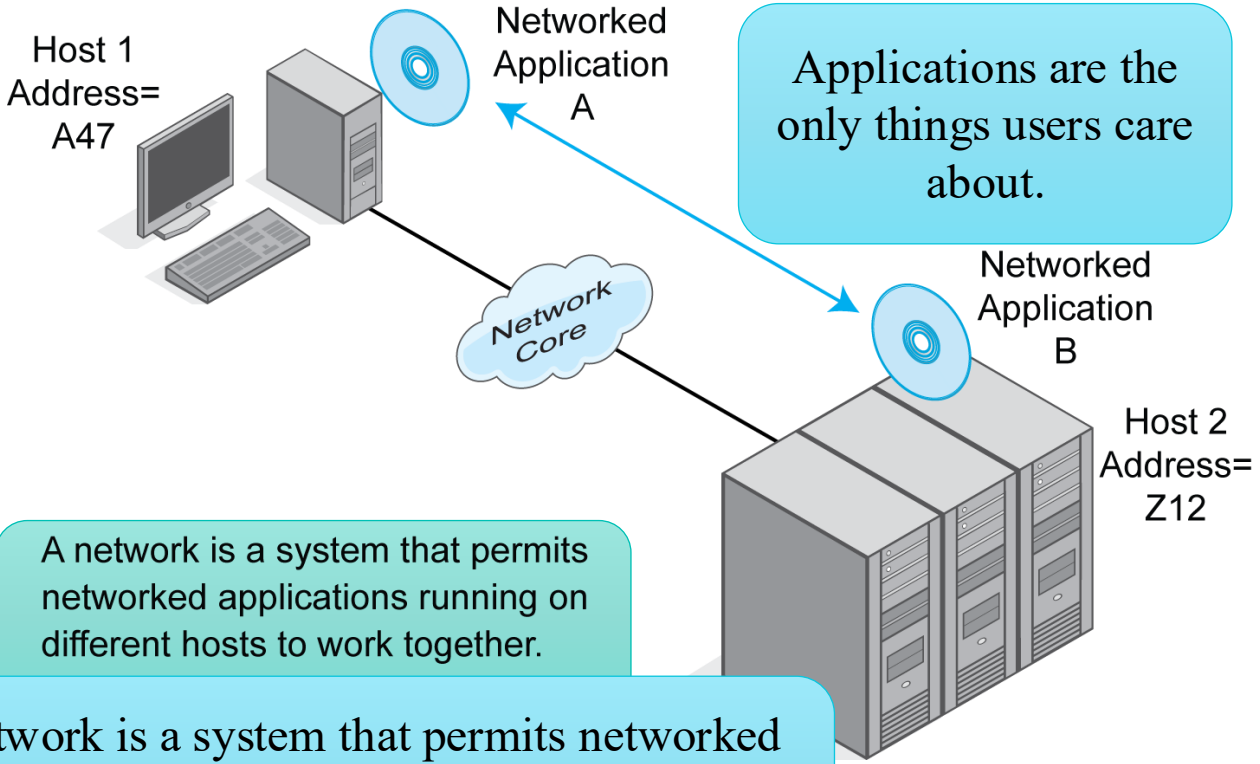
    (packets); each has a path chosen for it



Bits, Frames, Segments, Data?

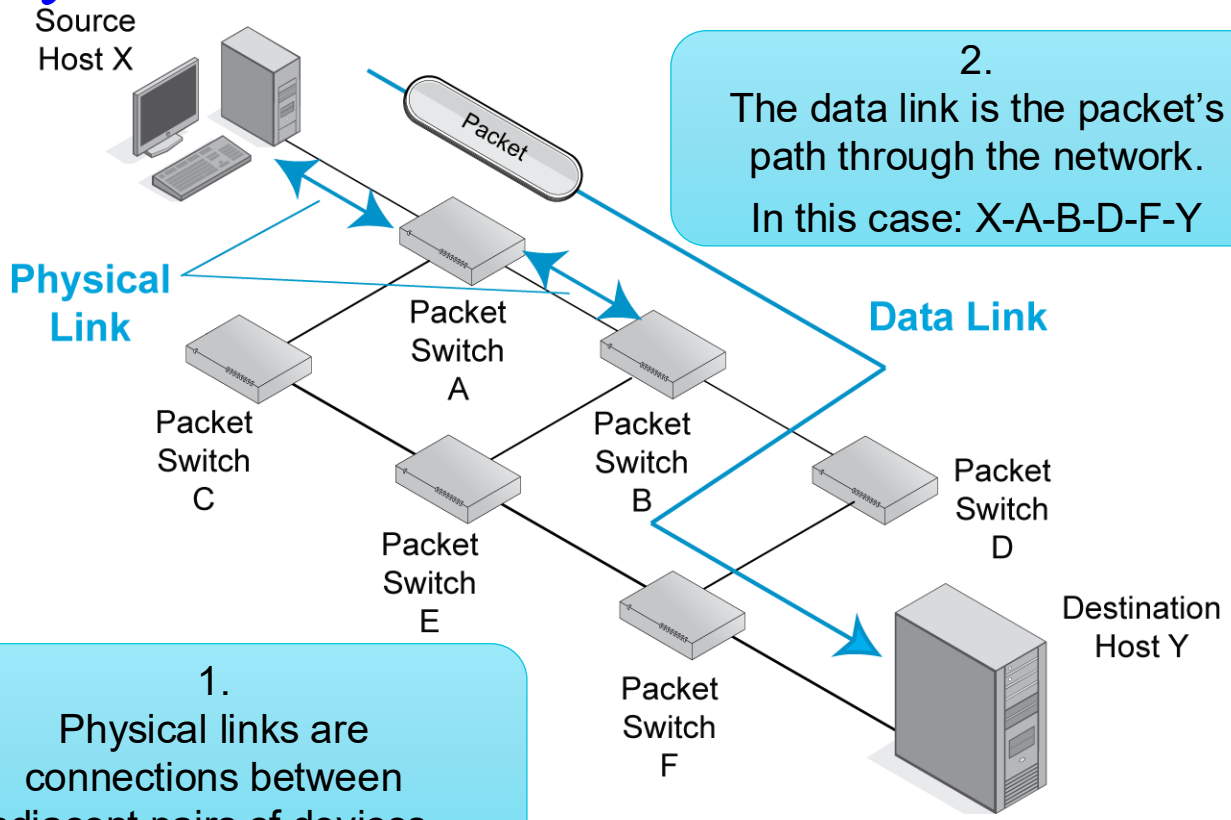


Basic Network Terminology



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

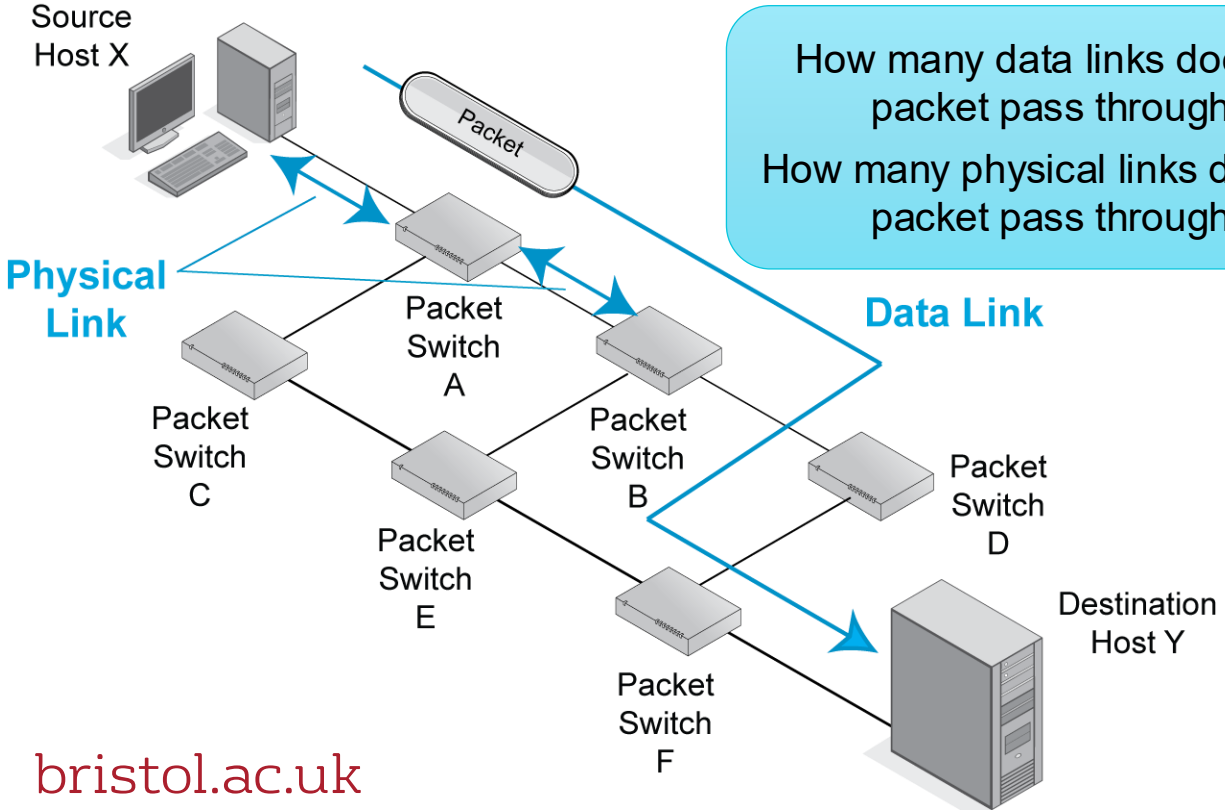
Physical Links and Data Links



2.
The data link is the packet's path through the network.
In this case: X-A-B-D-F-Y

1.
Physical links are connections between adjacent pairs of devices.

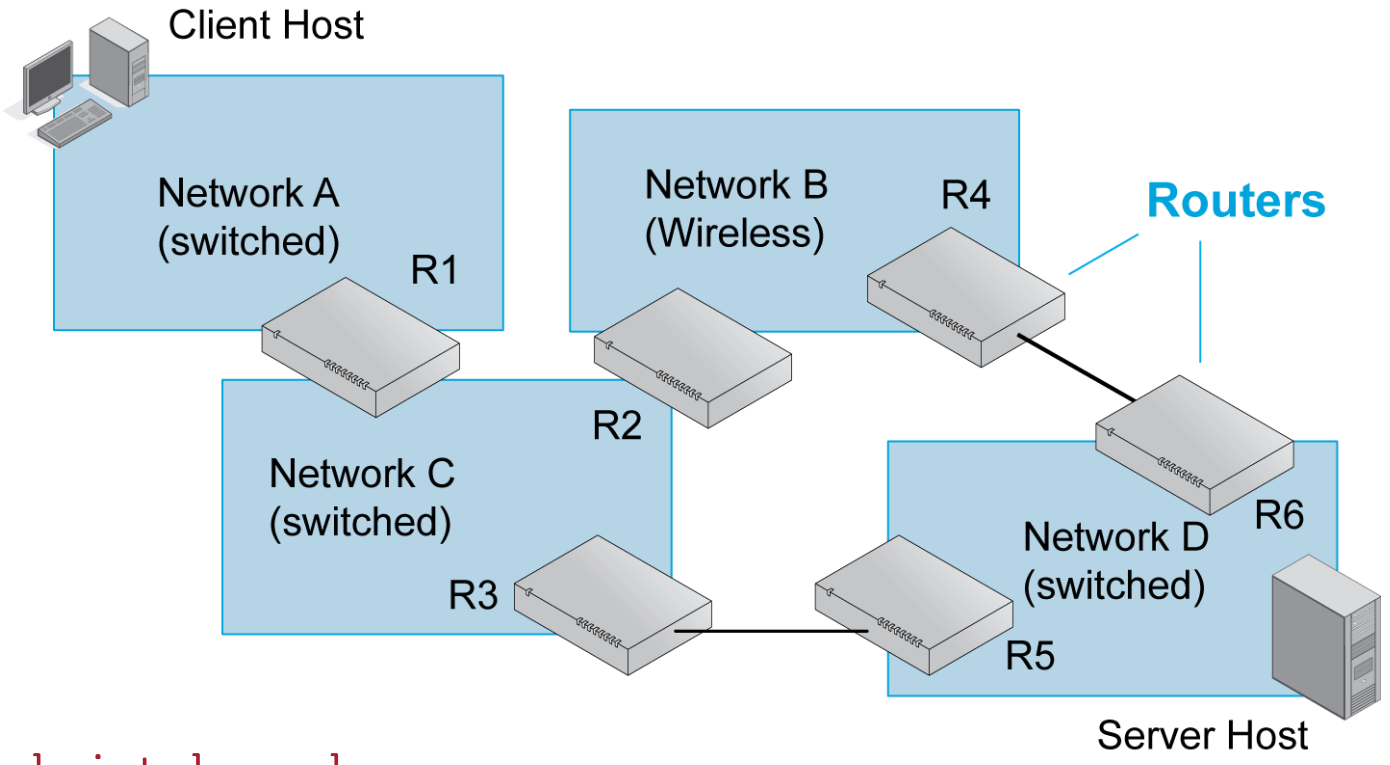
Physical Links and Data Links

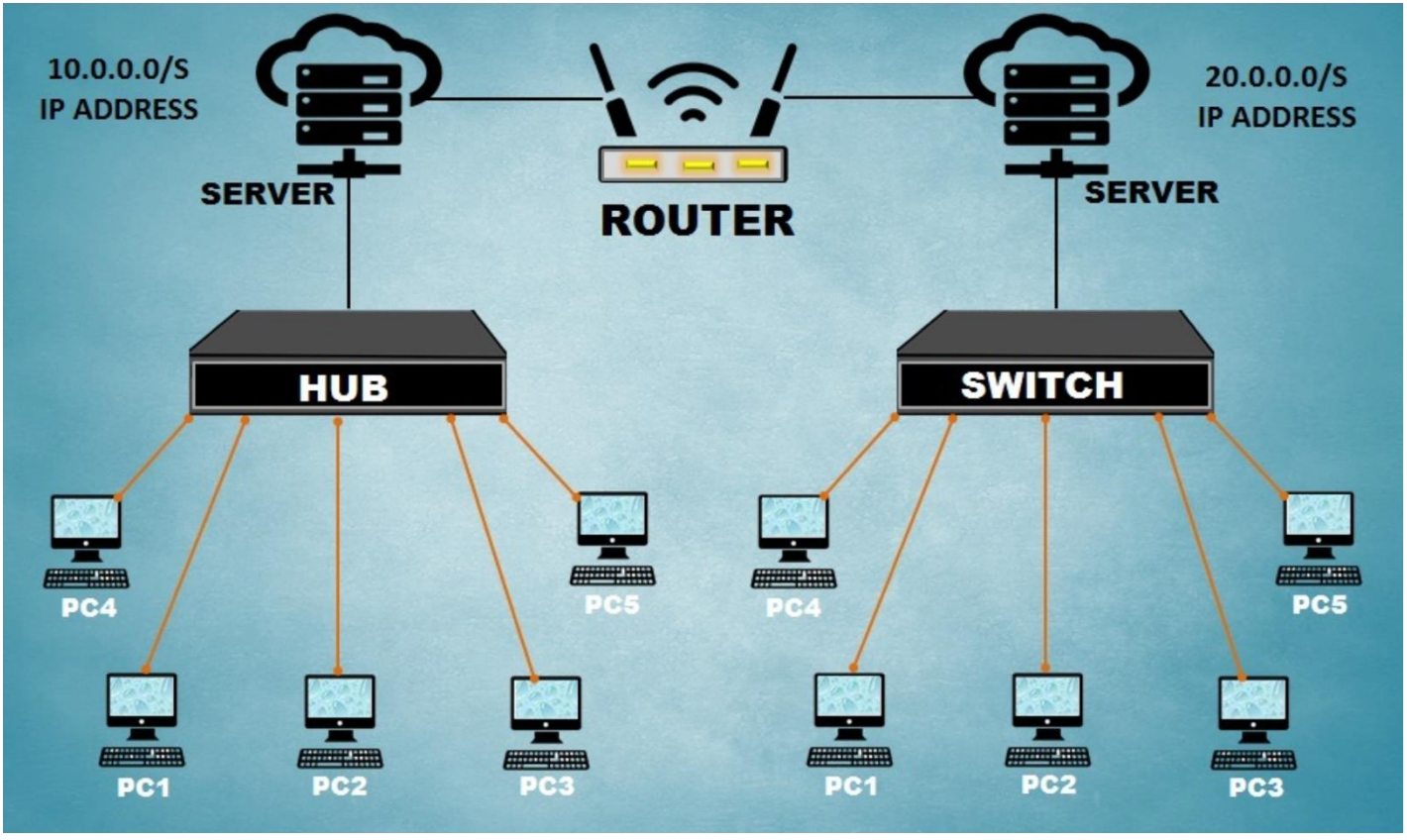


How many data links does the packet pass through?

How many physical links does the packet pass through?

Internetworking




10.0.0.0/S
IP ADDRESS
SERVER
ROUTER
20.0.0.0/S
IP ADDRESS
SERVER
HUB
SWITCH
PC4
PC5
PC1
PC2
PC3
PC4
PC5
PC1
PC2
PC3

Packets and Frames

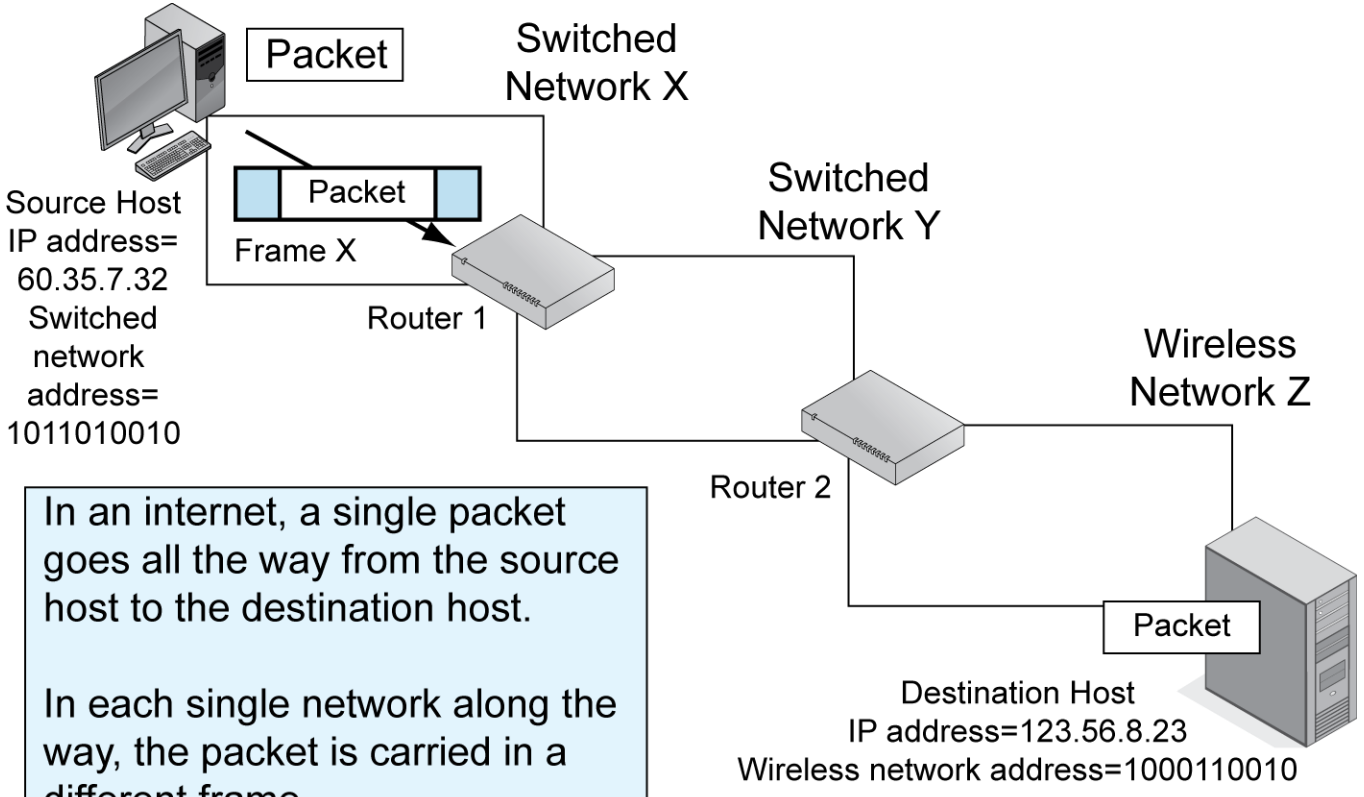
- **WHAT IS A FRAME?**
  - The term *frame* is most frequently used to describe a chunk of data created by network communication hardware such as a network interface cards (NIC cards) and router interfaces. Switch ports primarily forward existing frames and don't usually create frames of their own.

- **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.

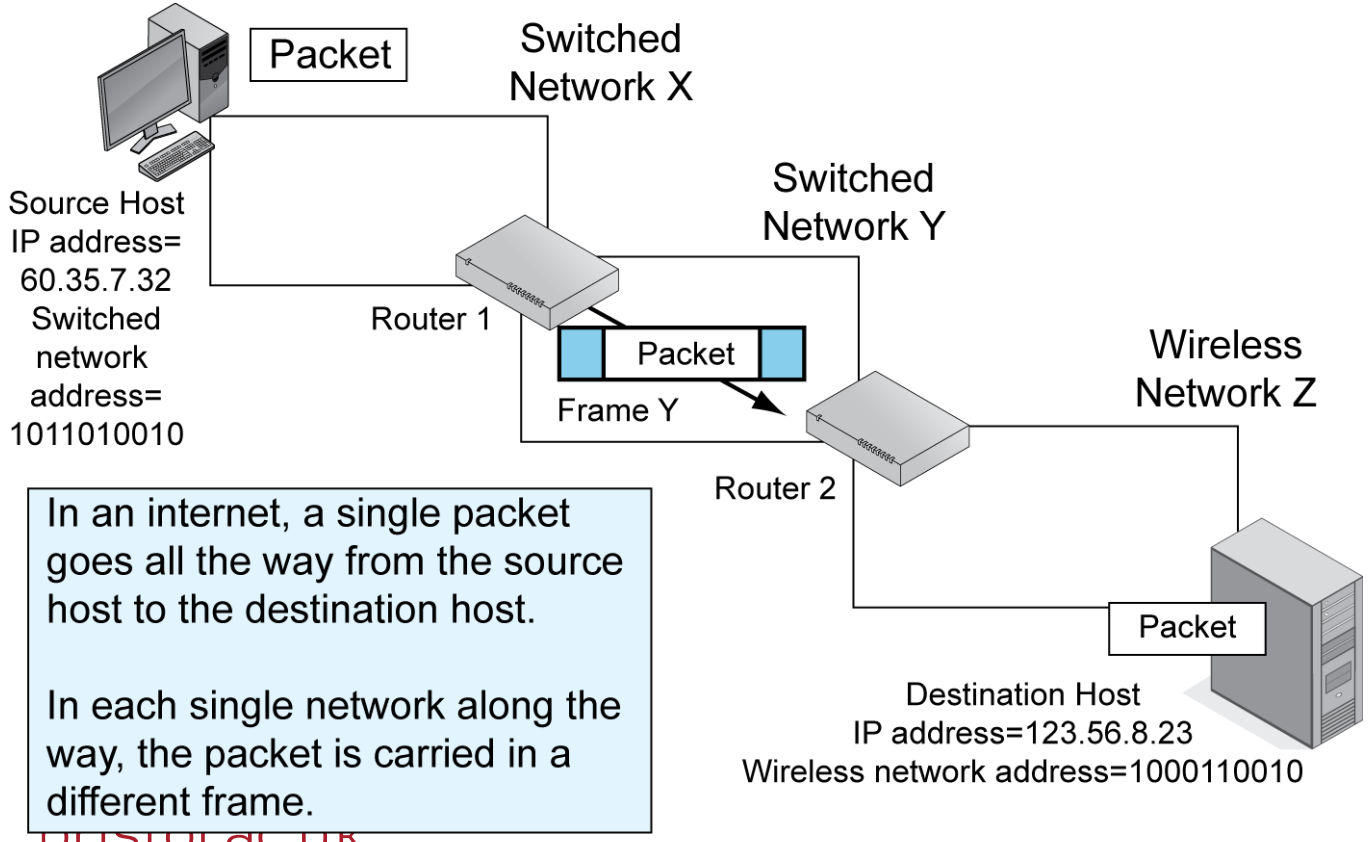
Packets and Frames



In an internet, a single packet goes all the way from the source host to the destination host.

In each single network along the way, the packet is carried in a different frame.

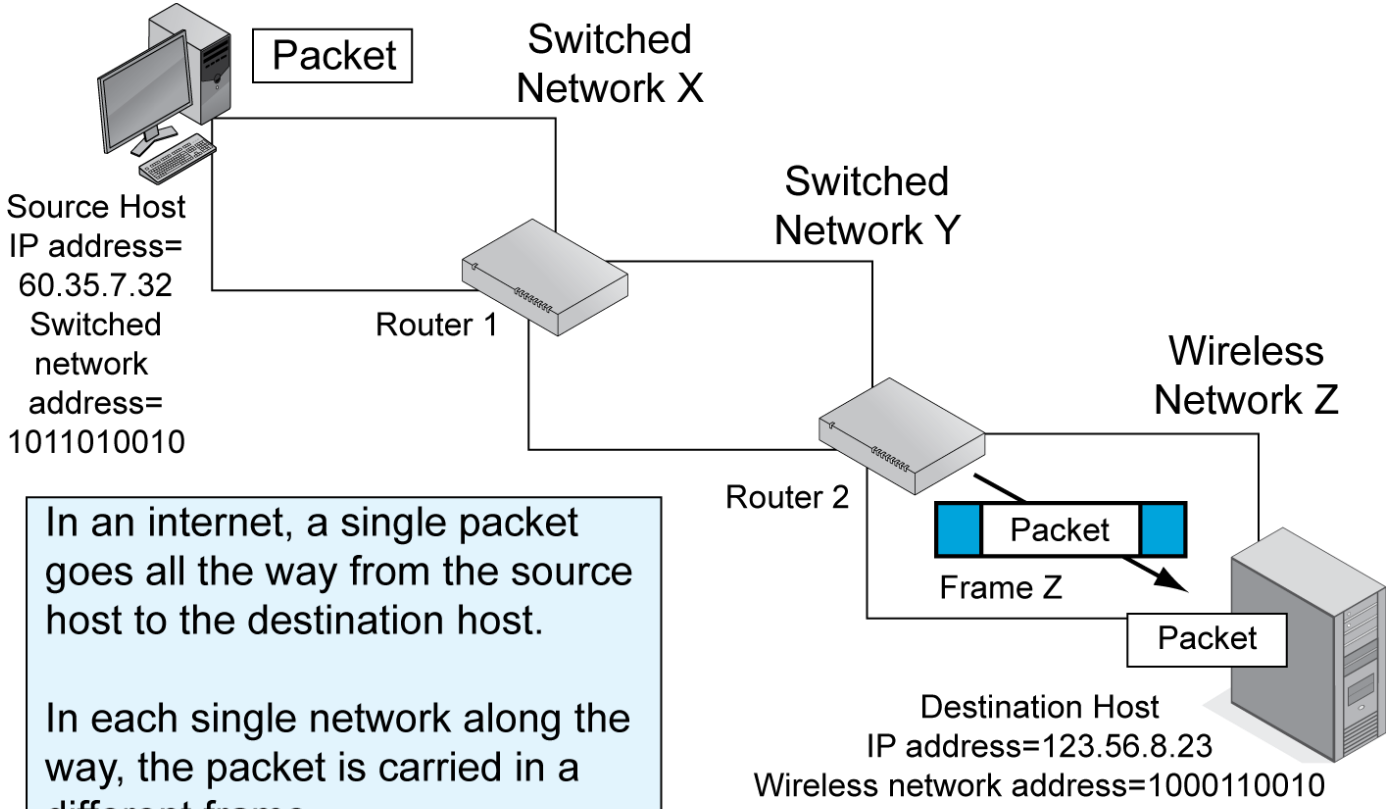
Packets and Frames



In an internet, a single packet goes all the way from the source host to the destination host.

In each single network along the way, the packet is carried in a different frame.

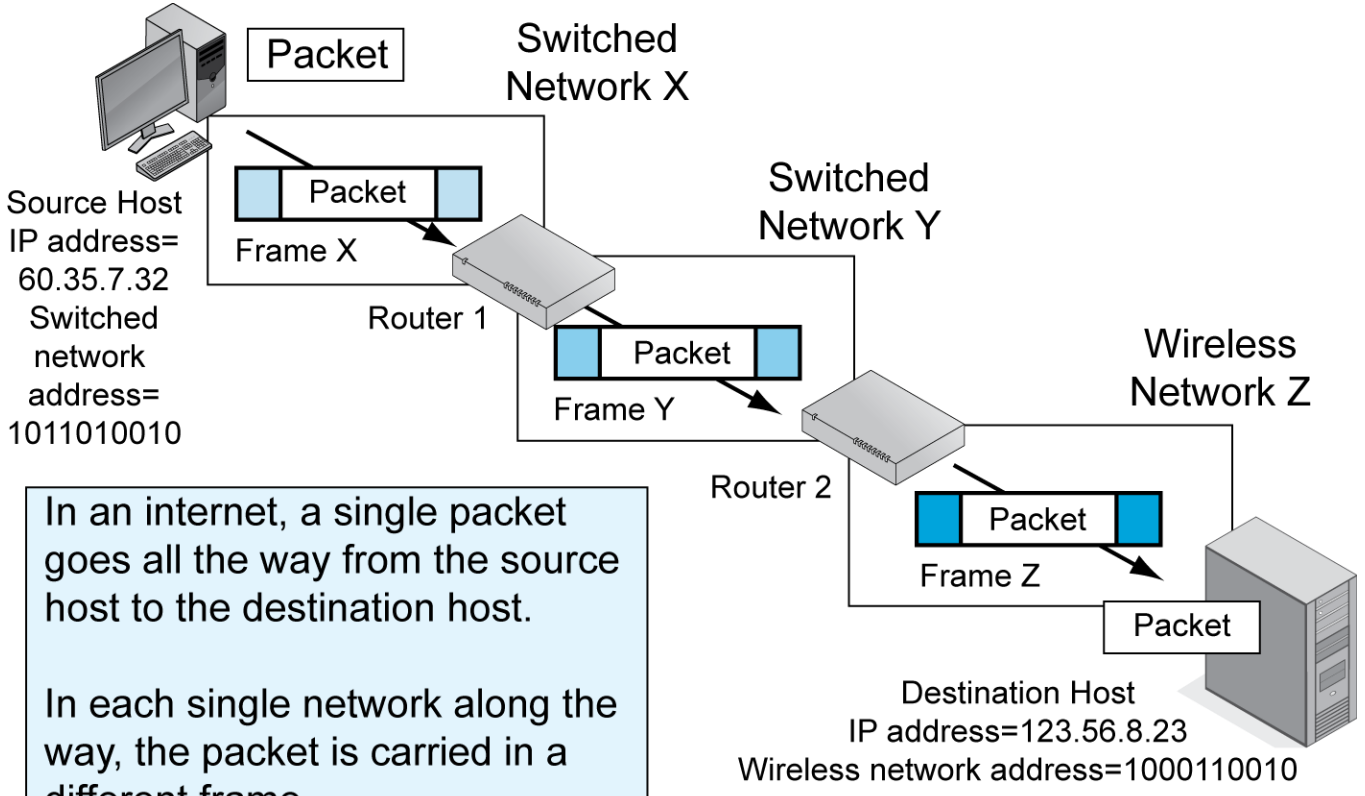
Packets and Frames



In an internet, a single packet goes all the way from the source host to the destination host.

In each single network along the way, the packet is carried in a different frame.

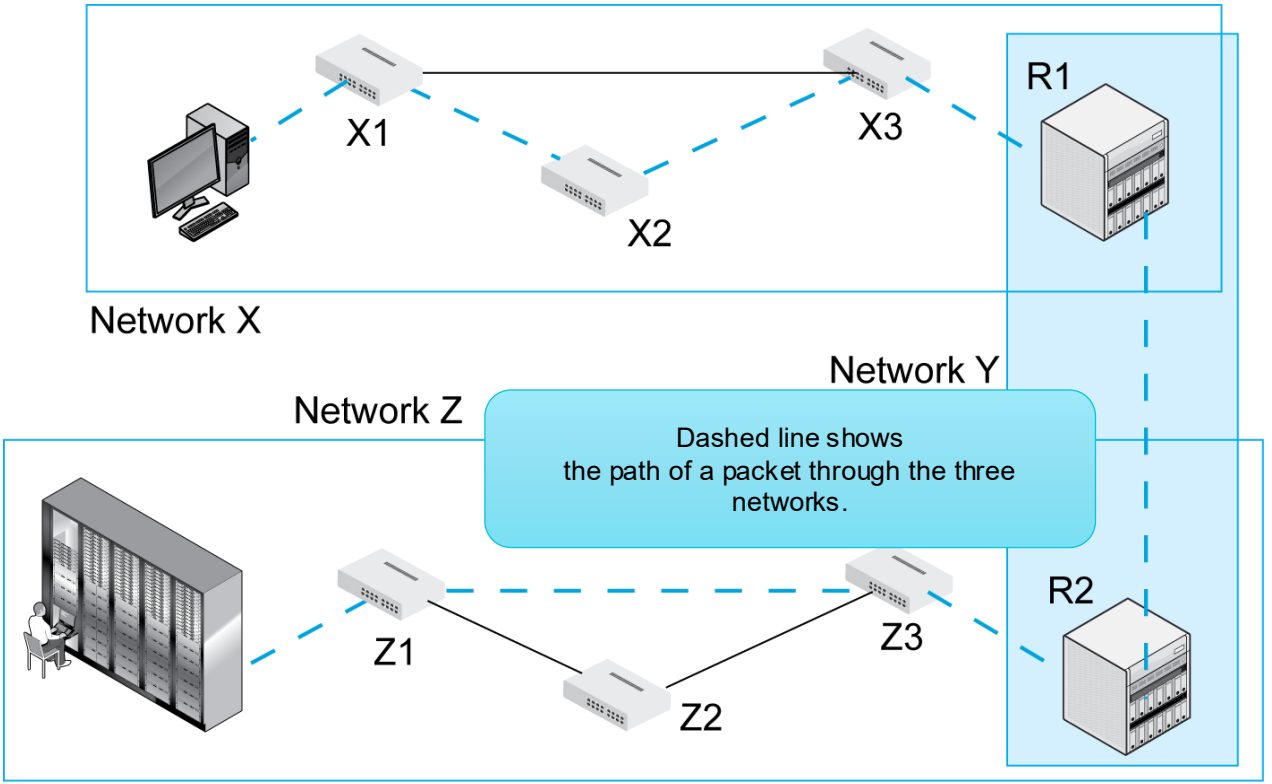
Packets and Frames



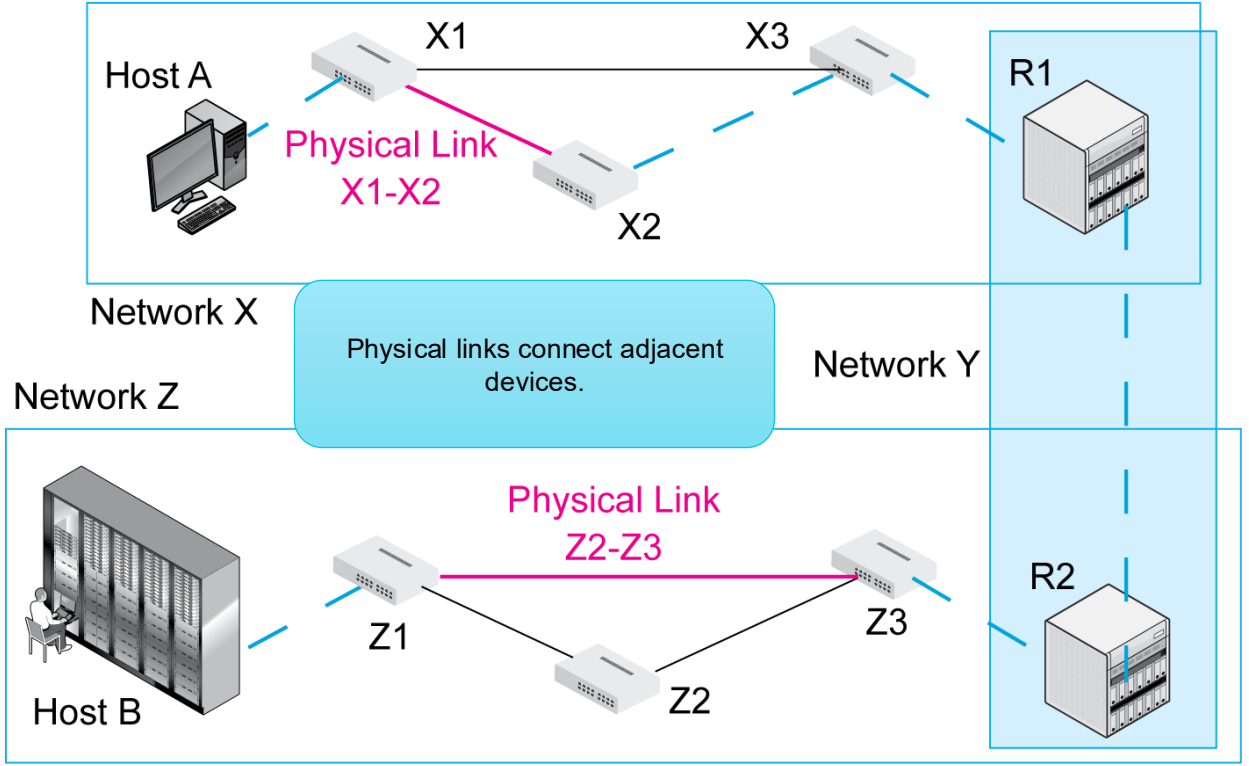
In an internet, a single packet goes all the way from the source host to the destination host.

In each single network along the way, the packet is carried in a different frame.

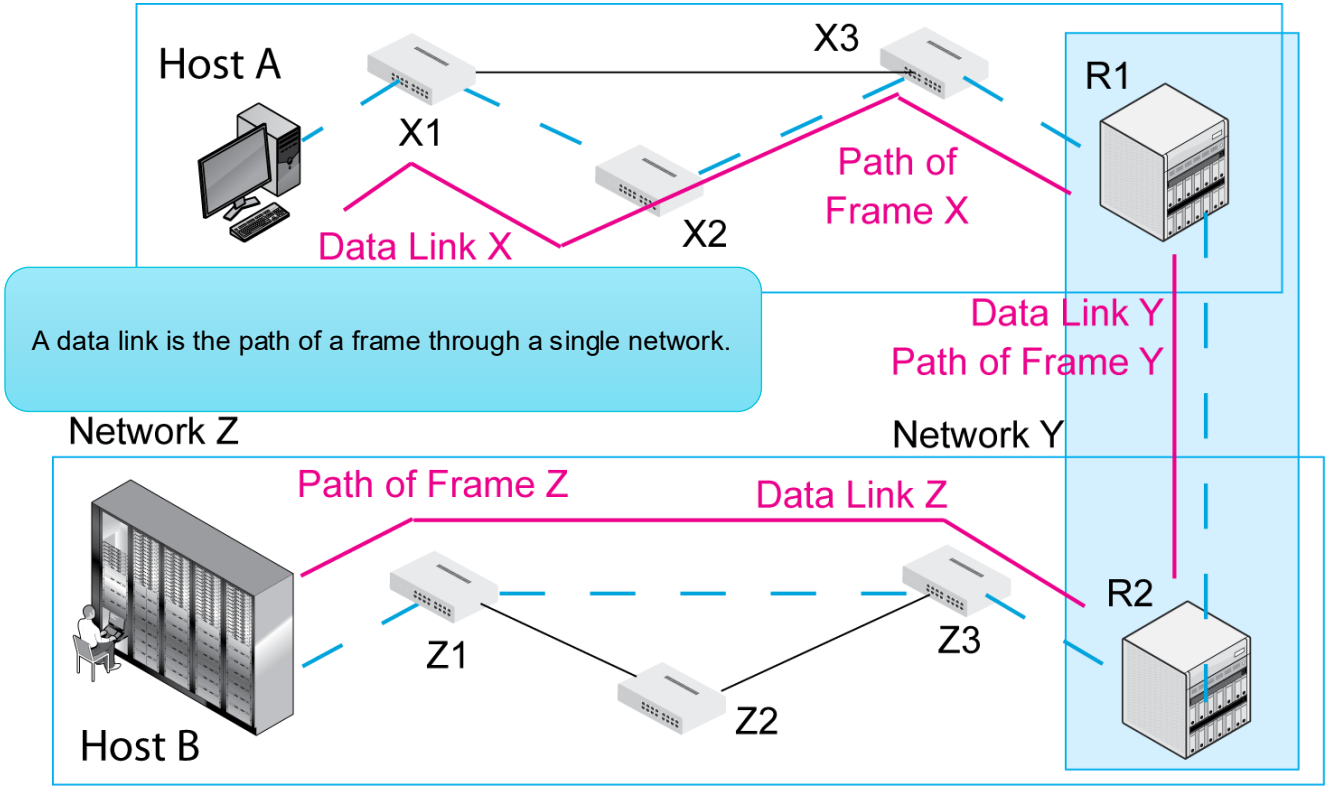
Physical Links, Data Links, and Routes



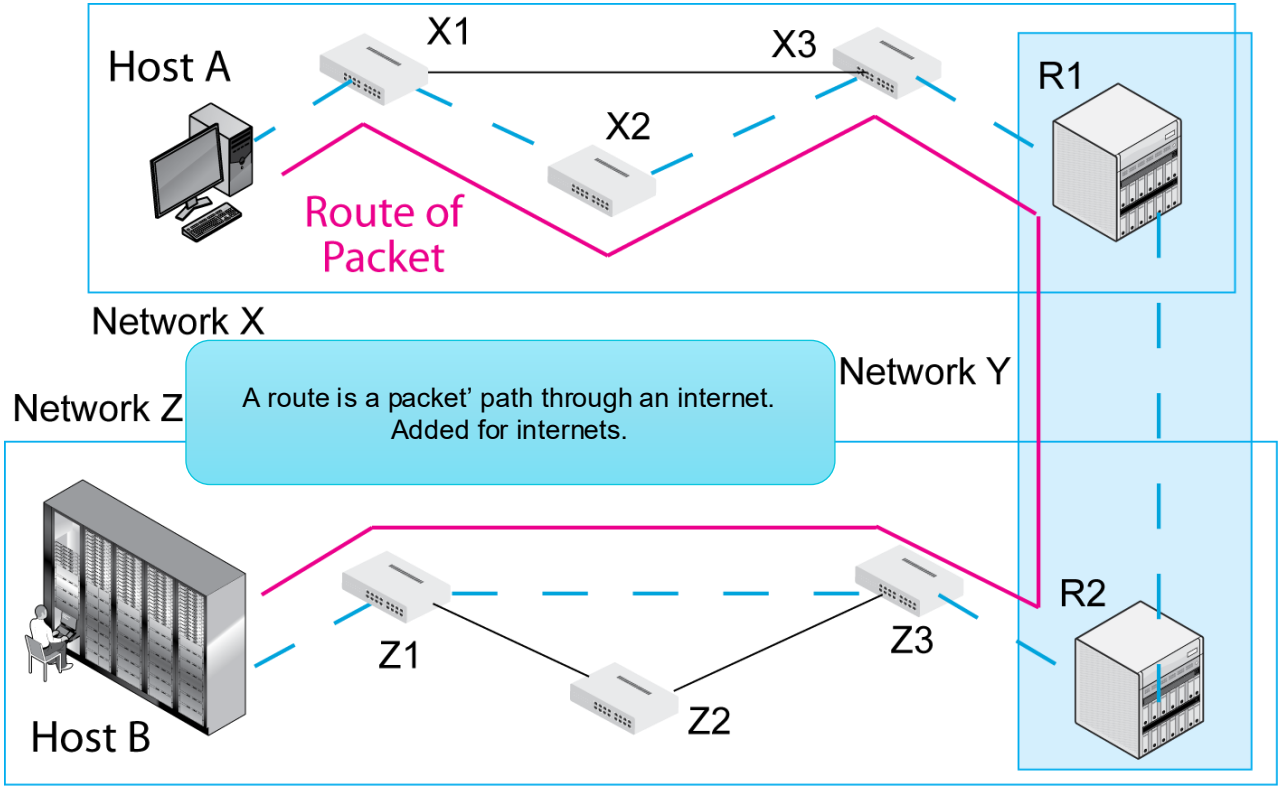
Physical Links, Data Links, and Routes



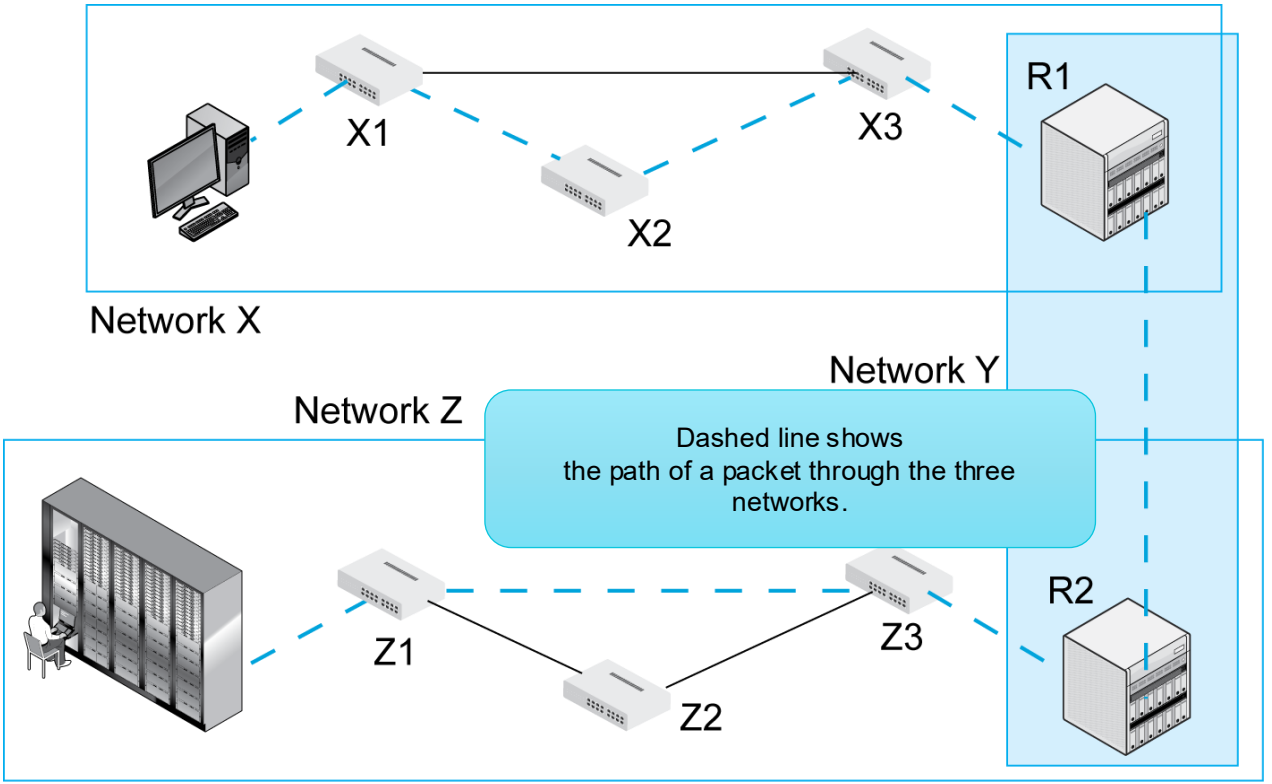
Physical Links, Data Links, and Routes



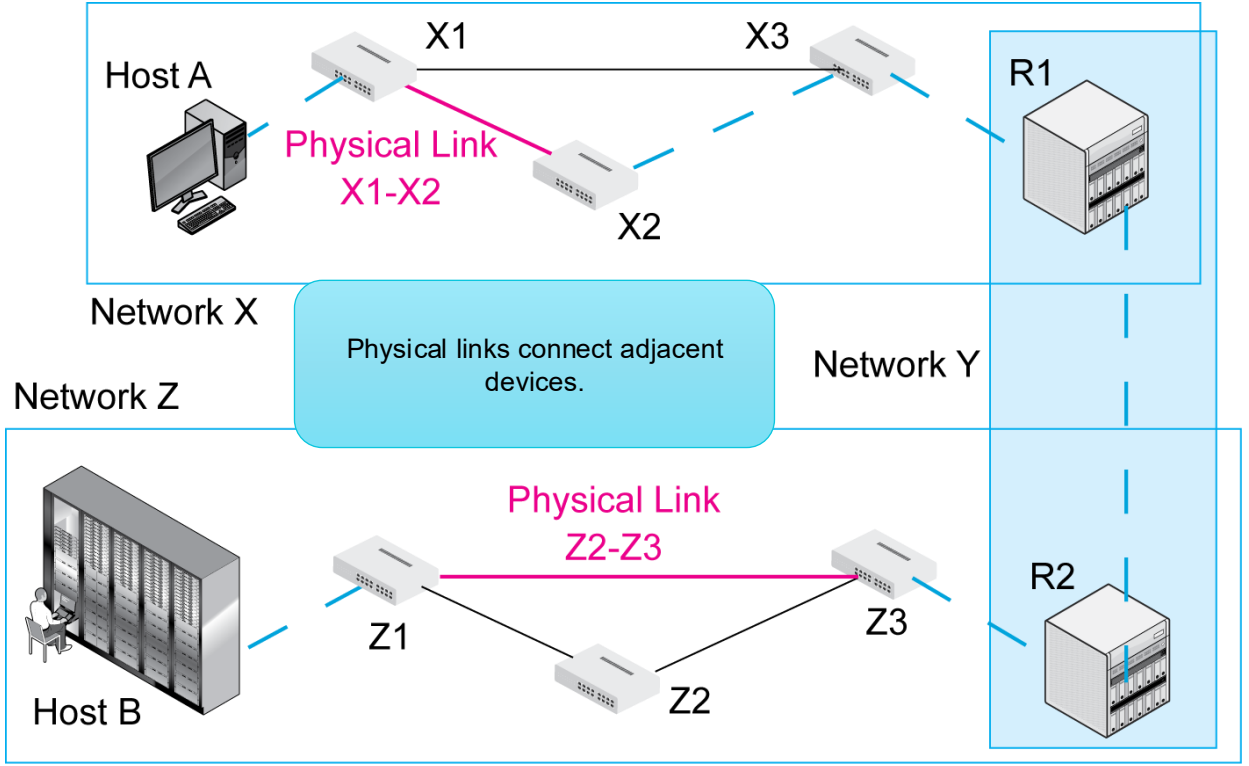
Physical Links, Data Links, and Routes



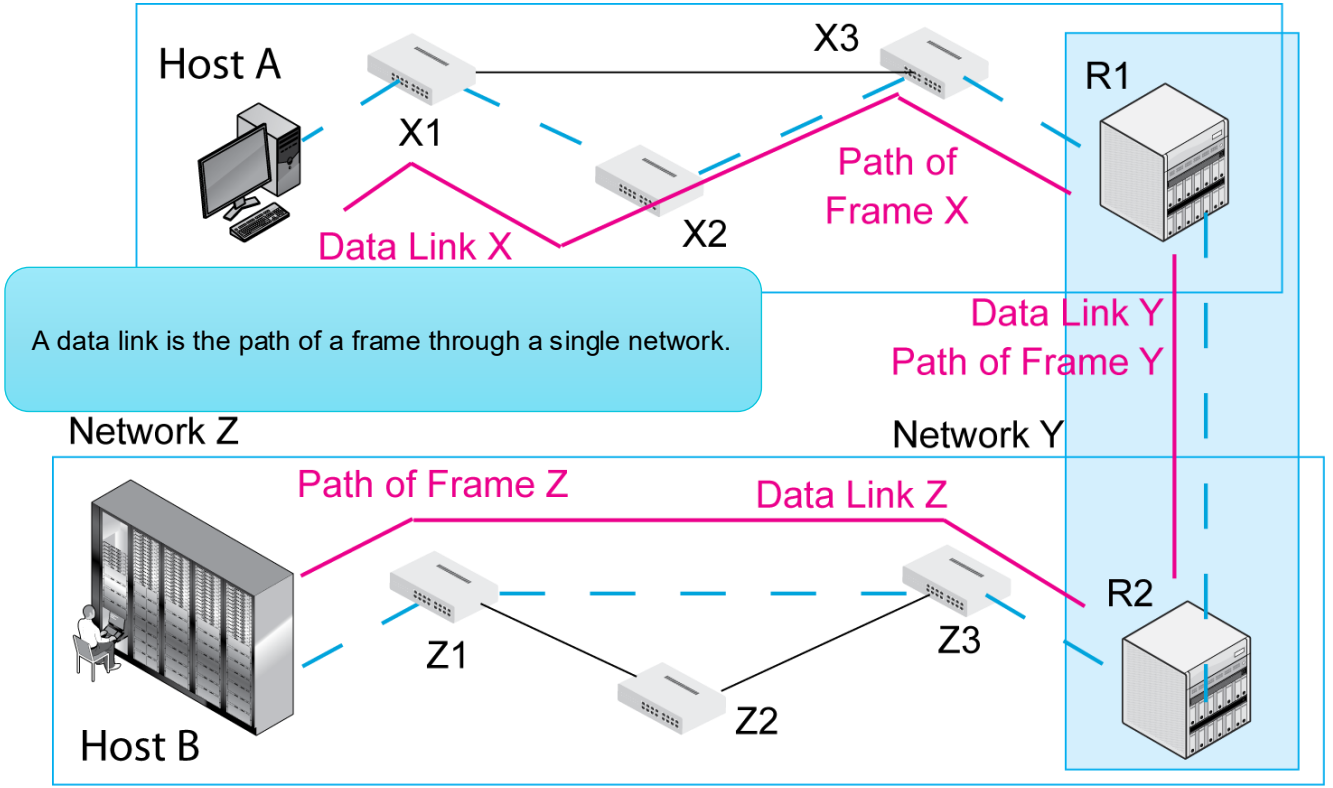
Physical Links, Data Links, and Routes



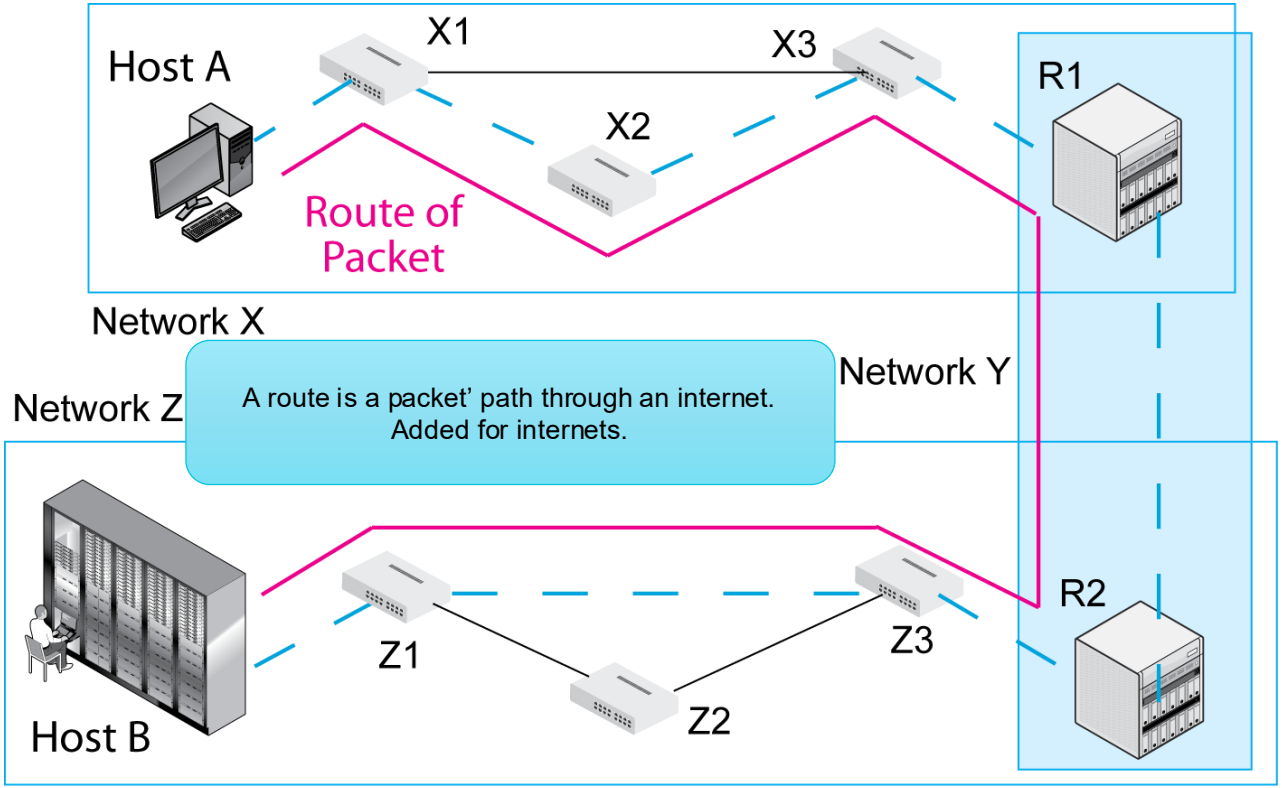
Physical Links, Data Links, and Routes



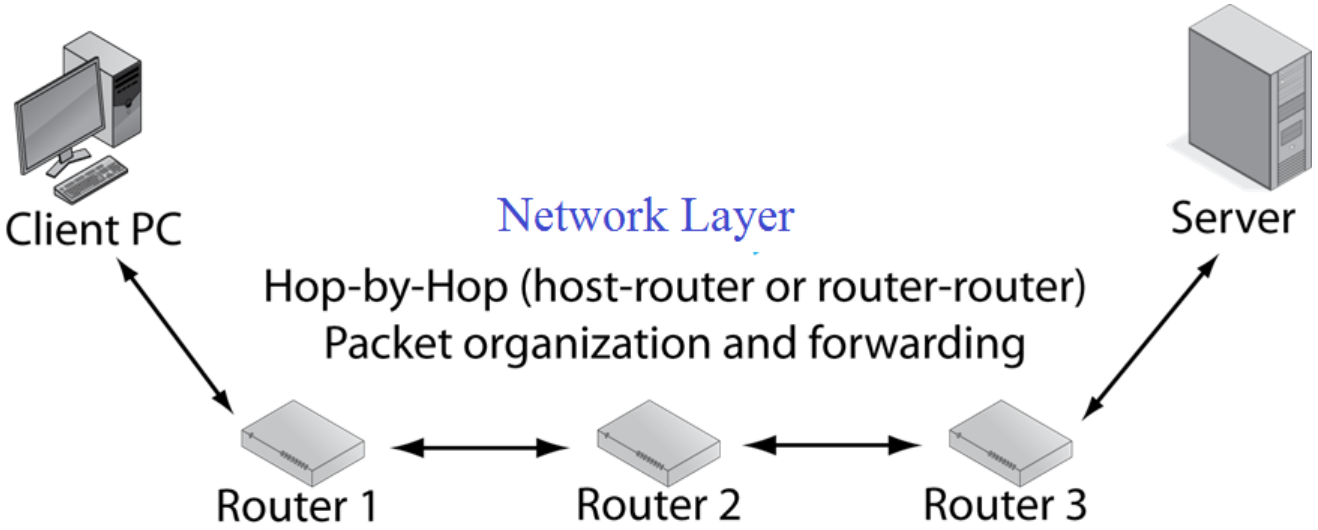
Physical Links, Data Links, and Routes



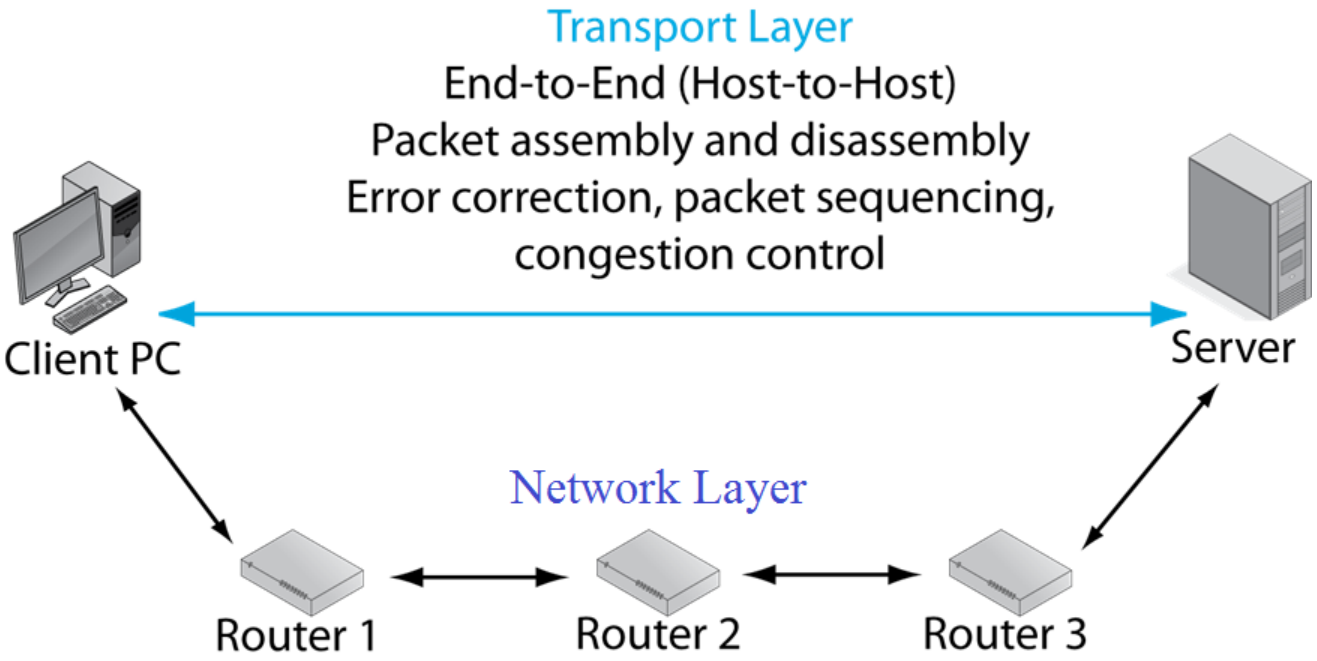
Physical Links, Data Links, and Routes



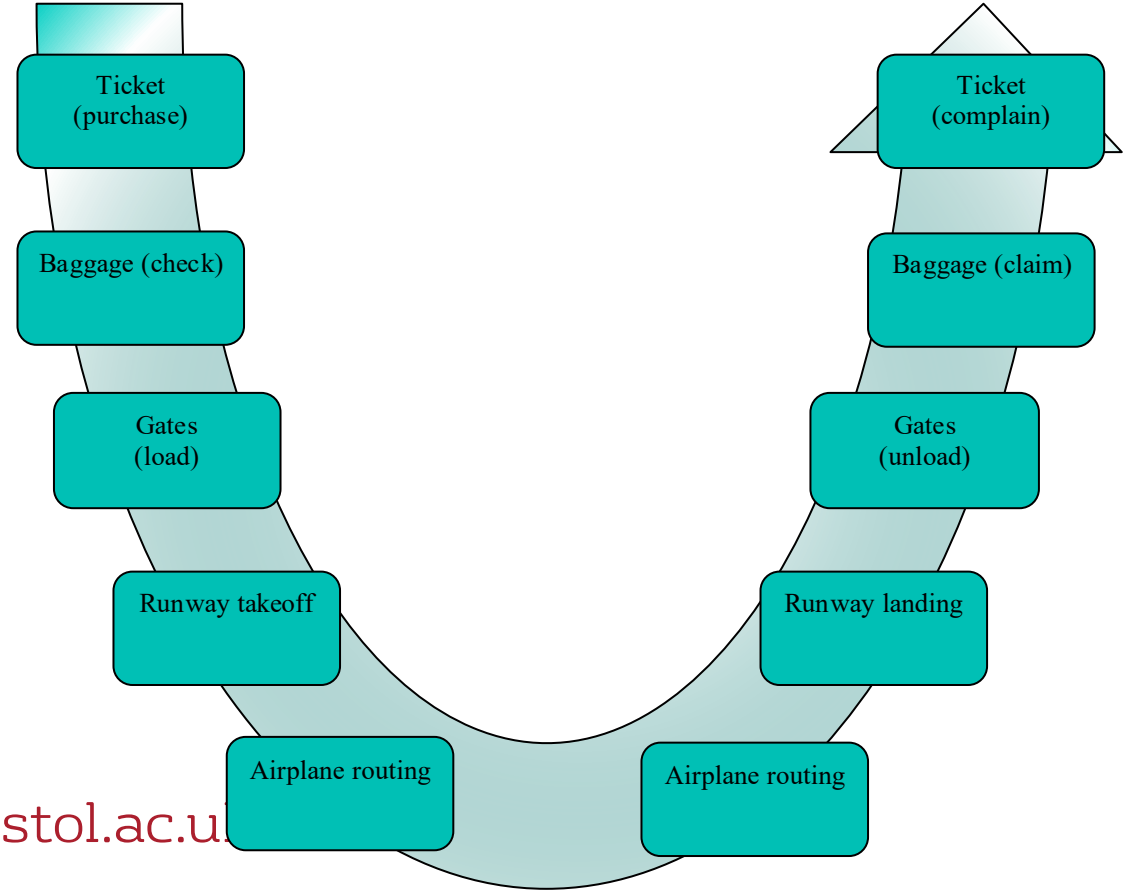
The Network and Transport Layers



The Network and Transport Layers



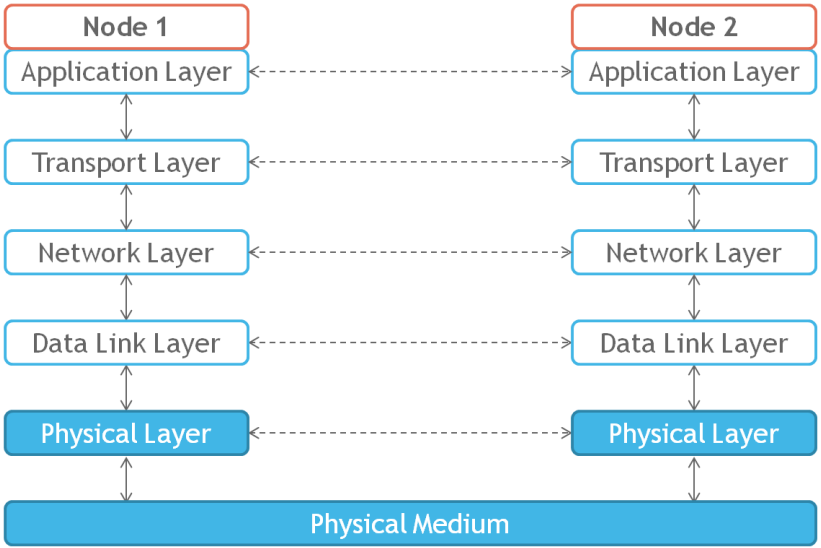
Taking an airplane: actions



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


Node 1
Application Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer
Node 2
Application Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer
Physical Medium

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

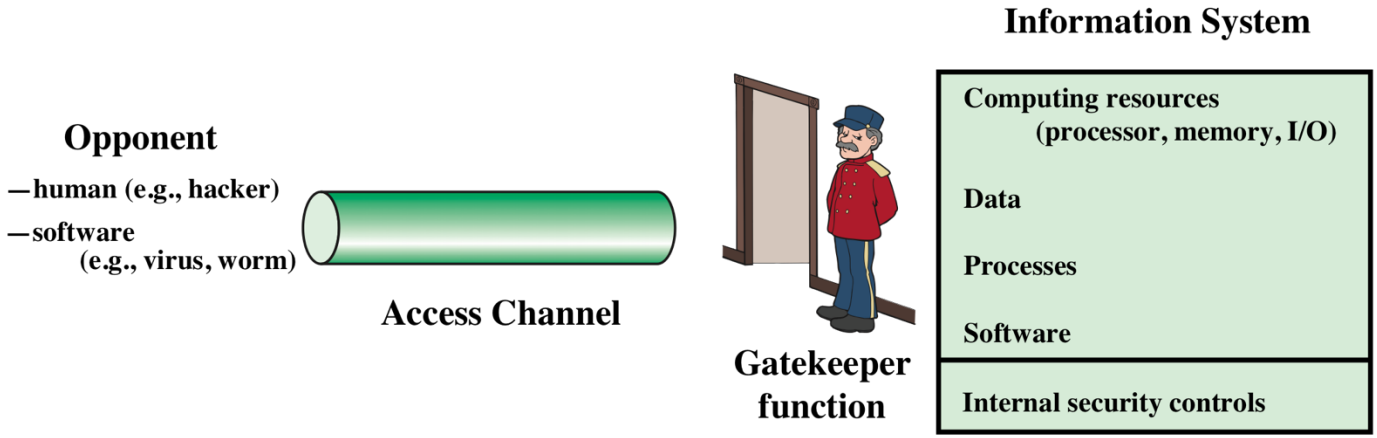
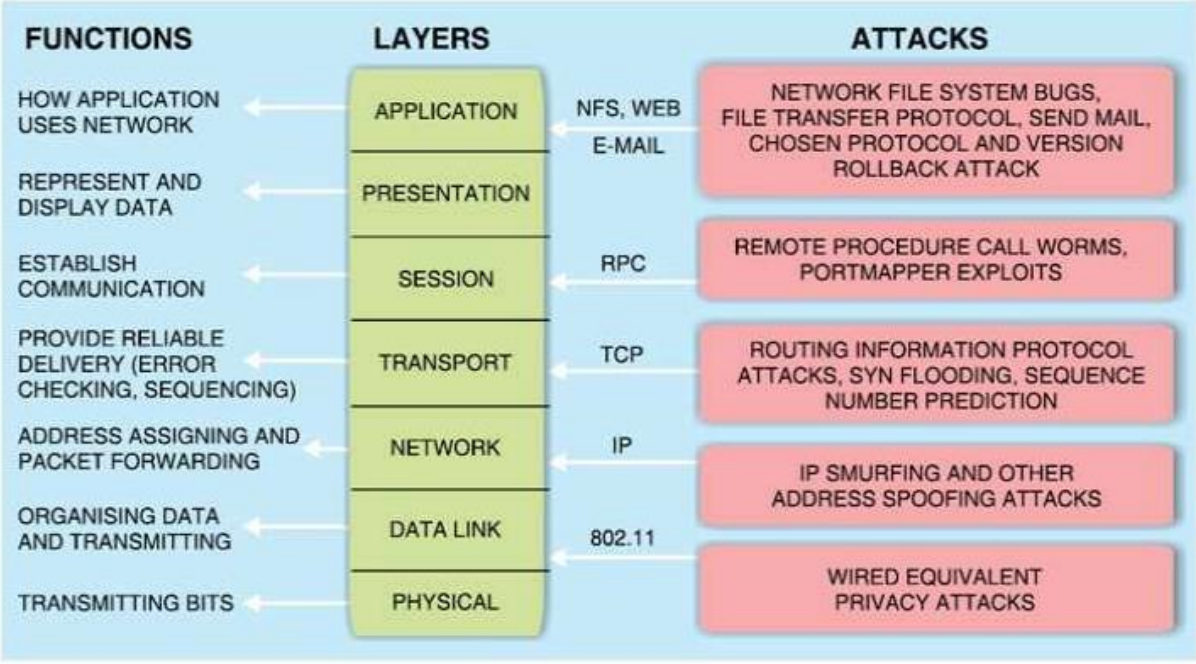


Figure 1.3 Network Access Security Model

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

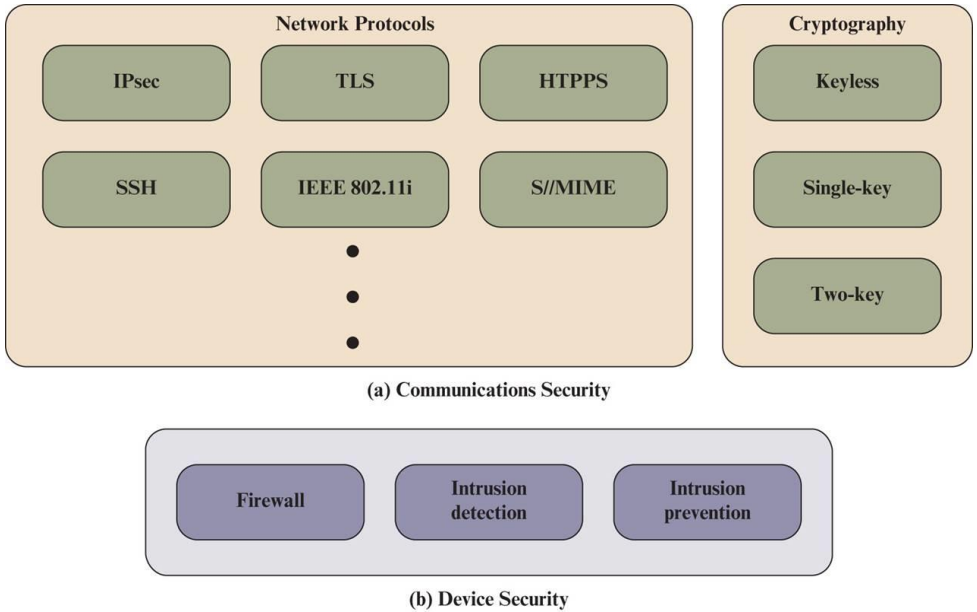
Attacks on different layers



Attacks on different layers

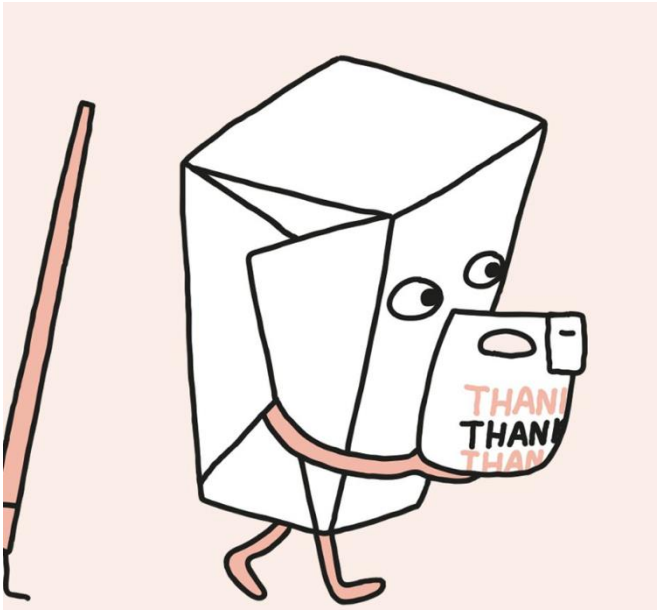
Layers	Attacks
Application layer	Repudiation, Data Corruption
Transport layer	Session Hijacking, Sync flooding
Network layer	Warm-hole, Black-hole, Gray-hole, Byzantine, Flooding, Resource consumption, Location-disclosure, Sybil attack, Jelly-fish, Fabrication, Modification attack
Data-Link layer	Traffic 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