Network Security

Session 7A

NAT and Introduction to Security

Mouli Sankaran

Session 7A: Focus

- Network Address Translation (NAT)
  - How it works
  - Three Types of NAT
  - Drawbacks of NAT
- Introduction to Computer Security
  - CIA Triad
  - Authenticity and Accountability
  - Different Types of Attacks
  - Security Services
  - Network Security Model
  - Network Security Protocols

Course page where the course materials will be posted as the course progresses:

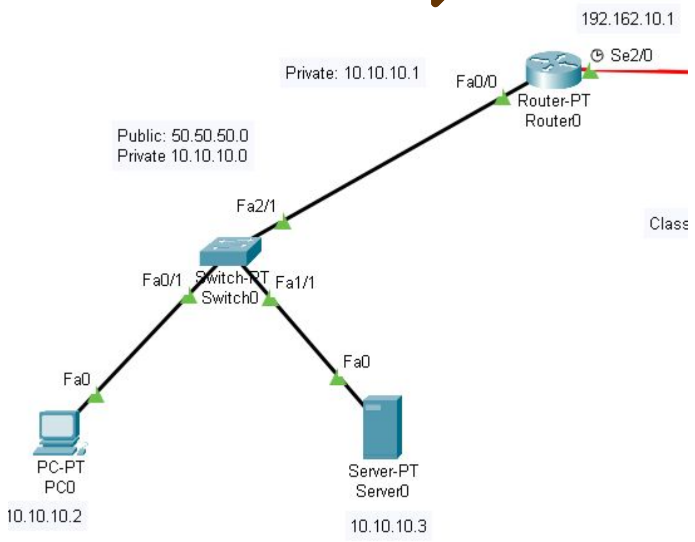
Network Address Translation (NAT)

NAT: An Introduction

- NAT is essentially a mechanism for allowing the same sets of IP addresses (Private IPs) to be reused in different parts of the Internet
- The primary motivation for the creation of NAT was the limited and diminishing availability of IP address space.
- NAT was introduced to solve two problems: **address depletion** and **concerns regarding the scalability of routing**.
  - Reduced number of globally routable Public IP addresses in the Internet
- It also protects the hosts within private network by not exposing their private IP addresses (**security**)

NAT: How it Works

Private IP
Src IP: 10.10.10.2 ➡ **Public IP**
Src IP: 50.50.50.2



4. NAT is configured in the router which is interfacing a private NW with the Public NW
5. Source IP address of every IP pkt going out is replaced with a public IP and checksum of the IP header recalculated.
6. Src IP is again replaced with its own private IP addr on incoming packets before delivering it to the respective hosts.

1. NAT modifies IP addresses in packet headers while they are sent out of a private network to public network (Internet).
2. The **Private source IP addresses** of the hosts are **replaced** with **Public IP addresses**
3. It allows multiple devices on a private network to share a single or a limited set of public IP addresses to access the Internet.

NAT: Three Types

- **Static (one-to-one):**

Q1:Is there any saving of IP addresses here?

ANS: NO

  - Maps one private IP to one public IP.
  - Useful for servers that need to be publicly accessible.
  - IP translation remains fixed.

- **Dynamic (many-to-many):**

Q2:Which pool of IPs is likely to be more in numbers?

ANS: Private Pool of IPs

  - Uses a pool of public IPs and maps internal private IPs dynamically.
  - The router assigns an available public IP whenever a device needs access.
  - Normally the available public IP addresses are much lower than no. of Private hosts using them.

- **Port-based (many-to-one):**

Q3:Can the same Public IP be sent out by different applications?

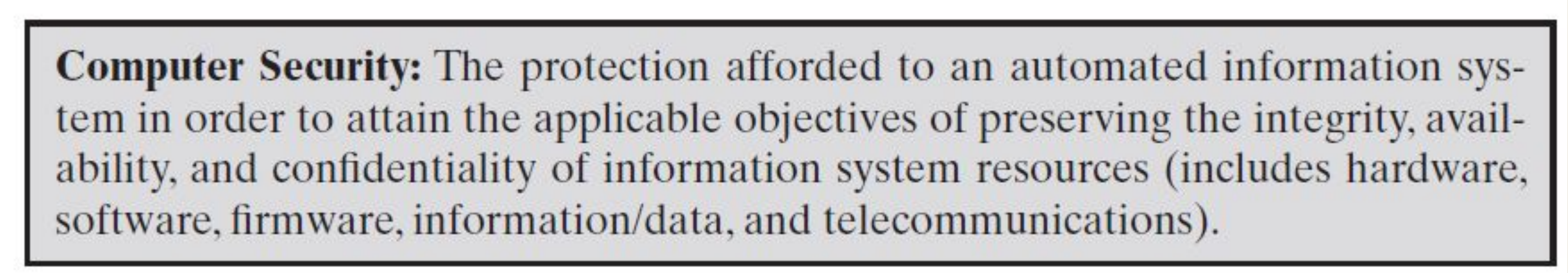
ANS: Yes

  - Also called NAT Overload.
  - Multiple private IPs share a single public IP.
  - Uses different port numbers for each connection.

NAT: Drawbacks

- Offering Internet-accessible services from the private side of a NAT requires special configuration because privately addressed systems are not directly reachable from the Internet
- For a NAT to work properly, every packet in both directions of a connection or association must pass through the same NAT (router).
- NATs require connection state on a per-association (or per-connection) basis and must **operate across multiple protocol layers**, unlike conventional routers.
- NAT poses problems for some application protocols (File Transfer Protocol), because it sends IP addressing information inside the application-layer payload.
  - FTP uses two connections (control and data) before transferring data
  - FTP shares the IP address and port number for the data transfer through control connection (as application payload)

Computer Security



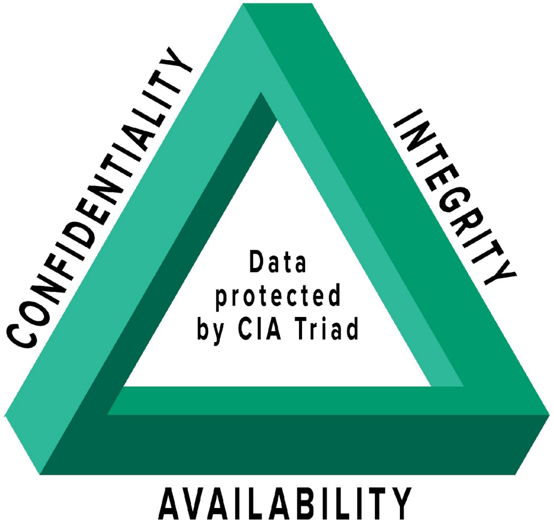
Computer Security: The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications).

Types of Security

- **Network Security:**
  - Protects networks from unauthorized access, cyberattacks, and threats
- **Application Security:**
  - Protects software and applications from vulnerabilities and attacks
- **Endpoint Security:**
  - Protects devices (laptops, mobile phones, servers) from malware and threat
- **Cloud Security:**
  - Protects cloud-based applications, data, and services
- **Cyber Security:**
  - Protects against cyber threats like hacking, malware, phishing, and cyber espionage.
- **Database Security:**
  - Protects databases from breaches, SQL injections, and unauthorized access.

CIA Triad

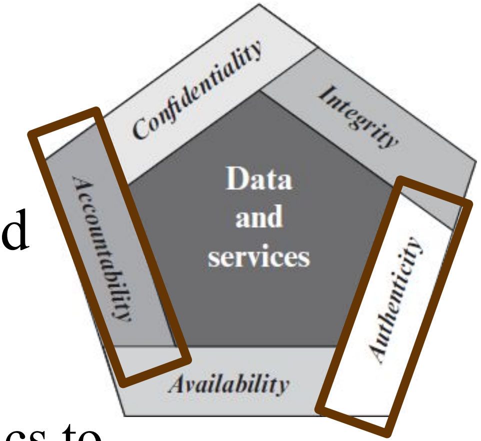
- **Confidentiality**: Assures that private or confidential information is not made available or disclosed to unauthorized individuals
  - A loss of confidentiality is the unauthorized disclosure of information.



- **Integrity**: Assures that data (both stored and in transmitted packets) and programs are changed only in a specified and authorized manner
  - A loss of integrity is the unauthorized modification or destruction of information
- **Availability**: Assures that systems work promptly and service is not denied to authorized users.
  - A loss of availability is the disruption of access to or use of information or an information system
- These **three concepts** form what is often referred to as the **CIA triad**.

Authenticity and Accountability

- Additional Concepts for completion:
  - **Authenticity**
  - **Accountability**



- **Authenticity**: It ensures that data, users, devices, and communications are genuine, verified, and trusted.
  - It involves mechanisms like digital signatures, cryptographic authentication, certificates, and biometrics to confirm the identity of users and the integrity of data

- **Accountability**: It refers to the ability to trace actions and events in a system back to a specific user, process, or entity to ensure responsibility and compliance.
  - It is achieved through mechanisms like user authentication, logging, auditing, and access control, ensuring that actions are recorded, monitored, and verifiable

Different Types of Attacks

- **Threat**: It is a possible danger that might exploit a vulnerability.
- **Attack**: An assault on system security that derives from an intelligent threat.
- **Passive attacks**: Eavesdropping on, or monitoring of, transmissions.
  - The goal of the opponent is to obtain information that is being transmitted.
- **Active attacks**: Involves some modification of the data stream or the creation of a false stream
  - **Masquerade** takes place when one entity pretends to be a different entity
  - **Replay** involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect
  - **Modification of messages** simply means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect
  - **Denial of Service (DoS)** prevents or inhibits the normal use or management of communications facilities

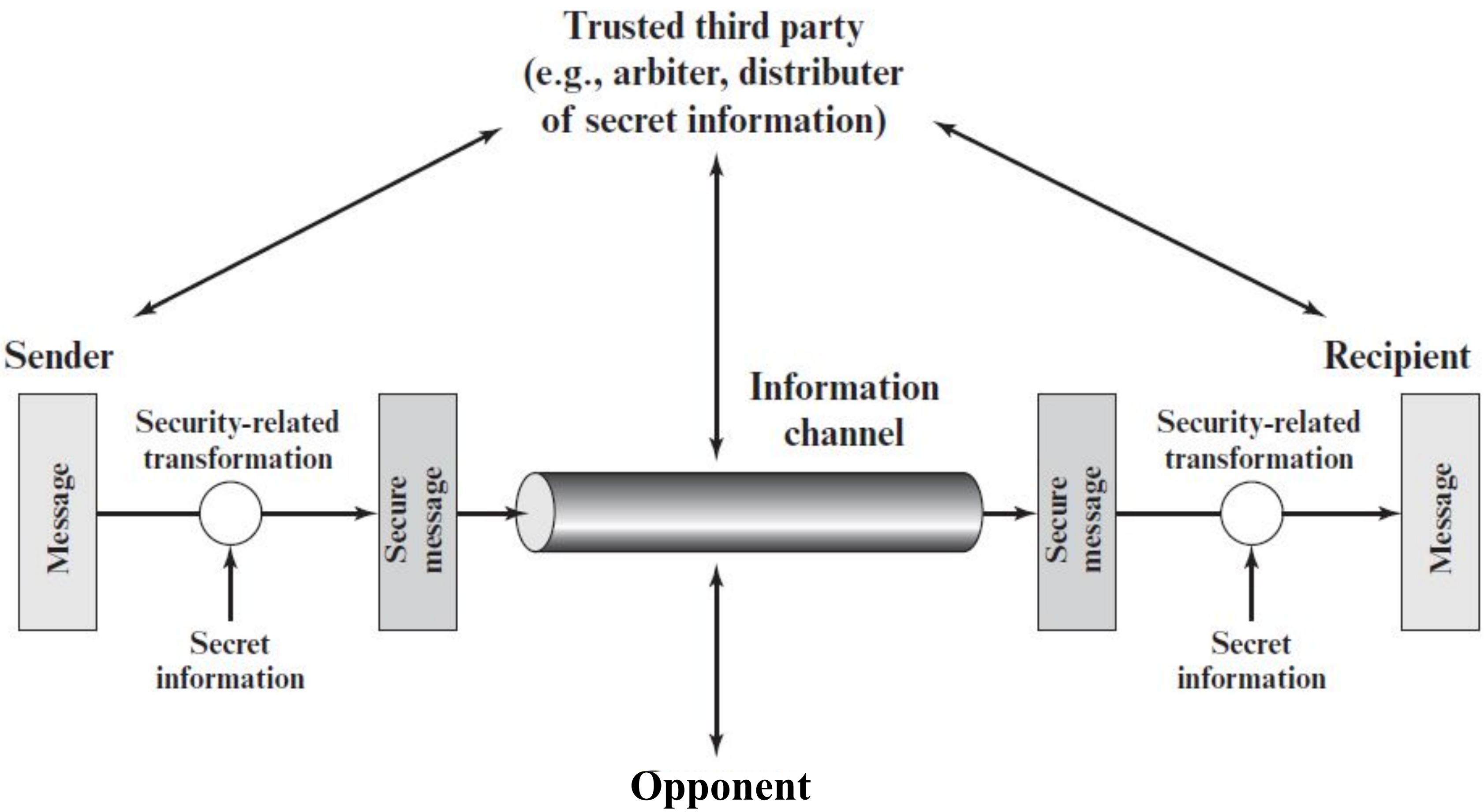
Security Services

- **Authentication**: It is concerned with assuring that a communication is authentic
  - It is to assure the recipient that the message is from the source that it claims to be from
- **Access Control**: It is the ability to limit and control the access to host systems and applications via communications links.
  - To achieve this, each entity trying to gain access must first be identified, or authenticated, so that access rights can be tailored to the individual.
- **Data Confidentiality**: It is the protection of transmitted data from passive attacks. Protection of traffic flow from analysis.
- **Data Integrity**: It assures that messages are received as sent with no duplication, insertion, modification, reordering, or replays.
  - The destruction of data is also covered under this service. DoS is also covered here.
- **Nonrepudiation:** It prevents either sender or receiver from denying a transmitted message.

Network Security

Network security is a set of policies, procedures, and technologies that protect networks from unauthorized access, misuse, and data loss.
It includes hardware and software components.

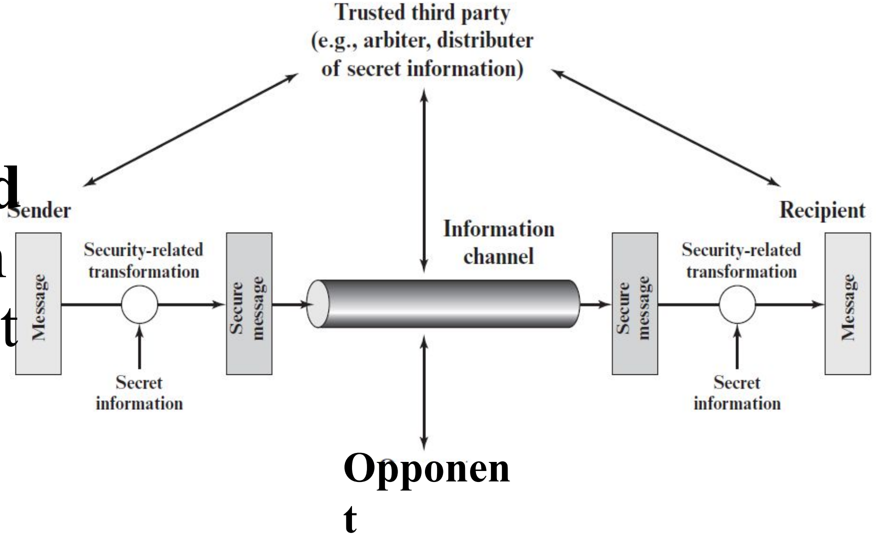
Network Security Model



Network Security Model: Explained

- There are **four basic tasks** to implement a **security service**

1. Design an **algorithm** for performing the **security-related transformation**. The algorithm should be such that an opponent cannot defeat its purpose. (encryption algorithms)



2. Generate the **secret information** to be used with the algorithm. (keys)
3. Develop methods for the **distribution and sharing** of the secret information. (key exchange protocol)
4. Specify a **protocol** to be used by the two principals that make use of the security algorithm and the secret information to achieve a particular security service. (TLS: Transport Layer Security)

Network Security Protocols

- **IPsec** (Internet Protocol Security): Secures IP traffic with encryption and authentication; widely used in VPNs.
- **TLS/SSL** (Transport Layer Security / Secure Sockets Layer): Ensures encrypted and authenticated communication over the Internet (in HTTPS).
- **HTTPS** (Hypertext Transfer Protocol Secure): Secure version of HTTP using TLS; protects web traffic like login and payment data.
- **SSH** (Secure Shell): Encrypts remote terminal sessions; used for secure login and remote command execution.
- **WPA2/WPA3** (Wi-Fi Protected Access): Secures wireless networks; WPA3 offers stronger encryption and better brute-force protection.
- **Kerberos**: Ticket-based authentication protocol; used in enterprise networks for secure user identity verification.
- **S/MIME** and **PGP**: Secure email protocols that provide encryption and digital signatures for email privacy and authenticity.

S/MIME: Secure/Multipurpose Internet Mail Extensions

PGP: Pretty Good Privacy

S/MIME, PGP and Kerberos

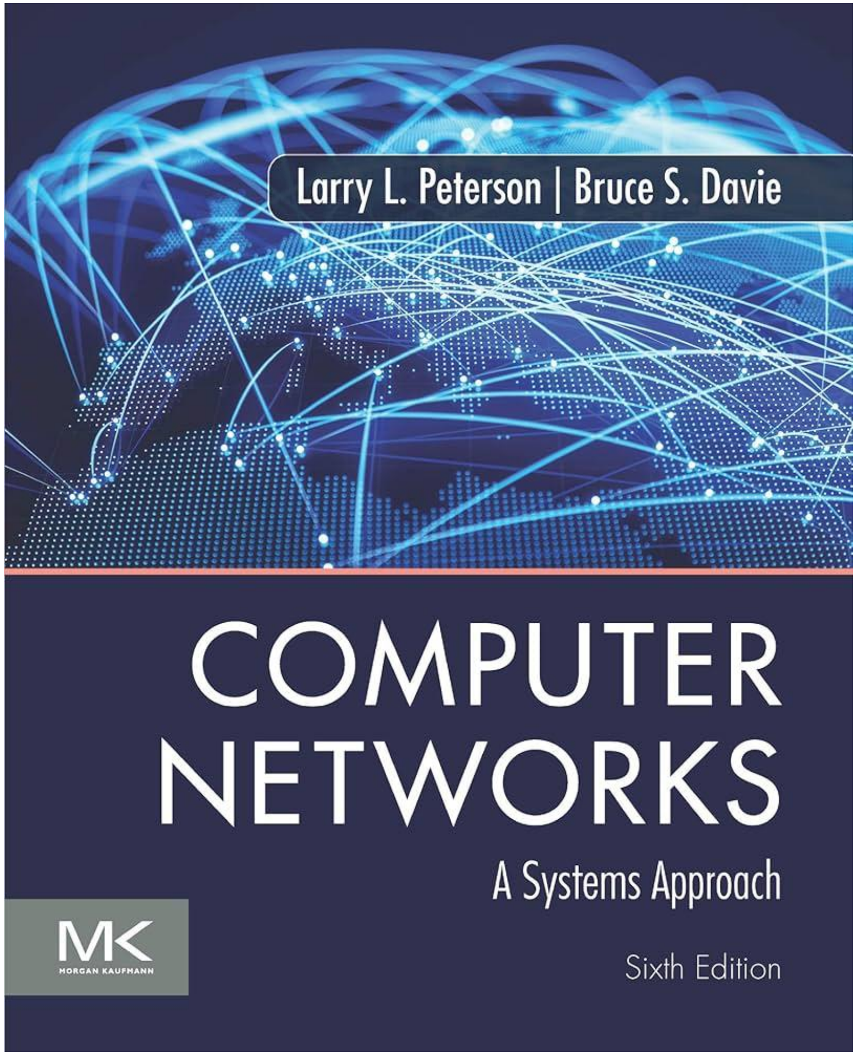
- **S/MIME:** Secure/Multipurpose Internet Mail Extensions, for business emails.
- **PGP**: Pretty Good Privacy: The sender uses their private key to encrypt the data.
- The recipient uses the sender's public key to decrypt the data
- **Kerberos**: **Single Sign-on**, providing **tickets** to users logging in. Uses **secret-key** crypto

Session 7A: Summary

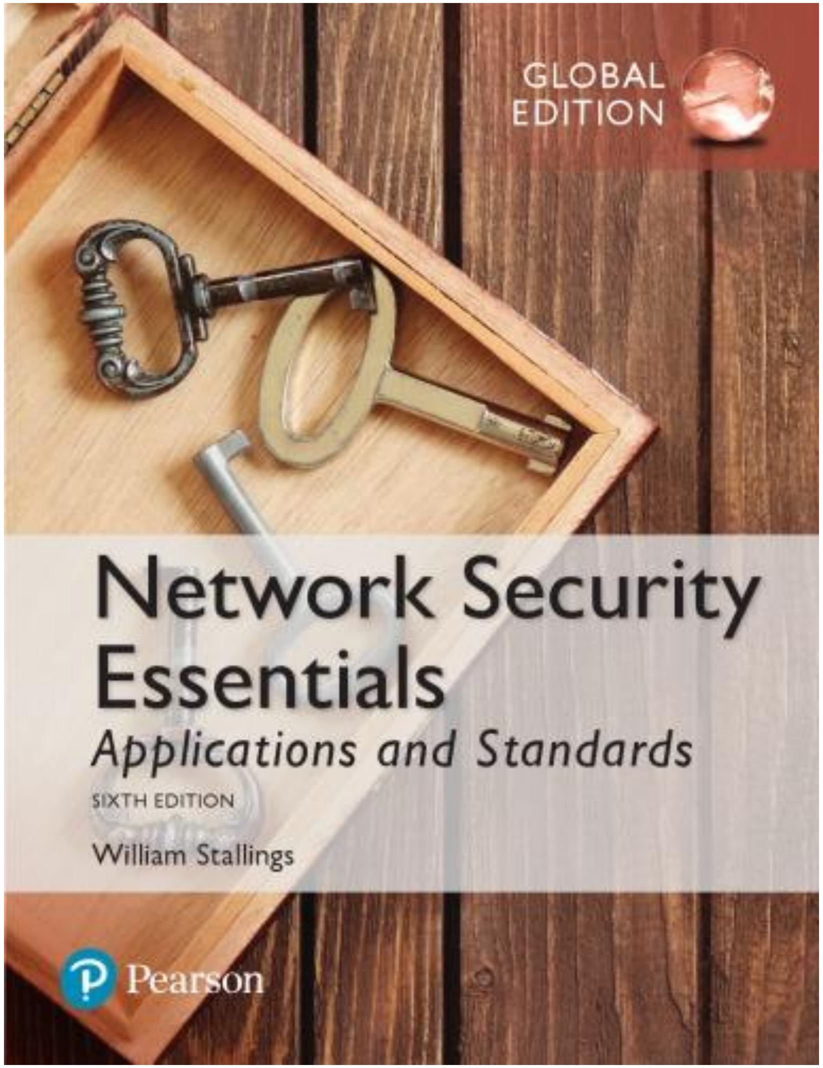
- Network Address Translation (NAT)
  - How it works
  - Three Types of NAT
  - Drawbacks of NAT
- Introduction to Computer Security
  - CIA Triad
  - Authenticity and Accountability
  - Different Types of Attacks
  - Security Services
  - Network Security Model
  - Network Security Protocols

Textbooks

Textbook 1

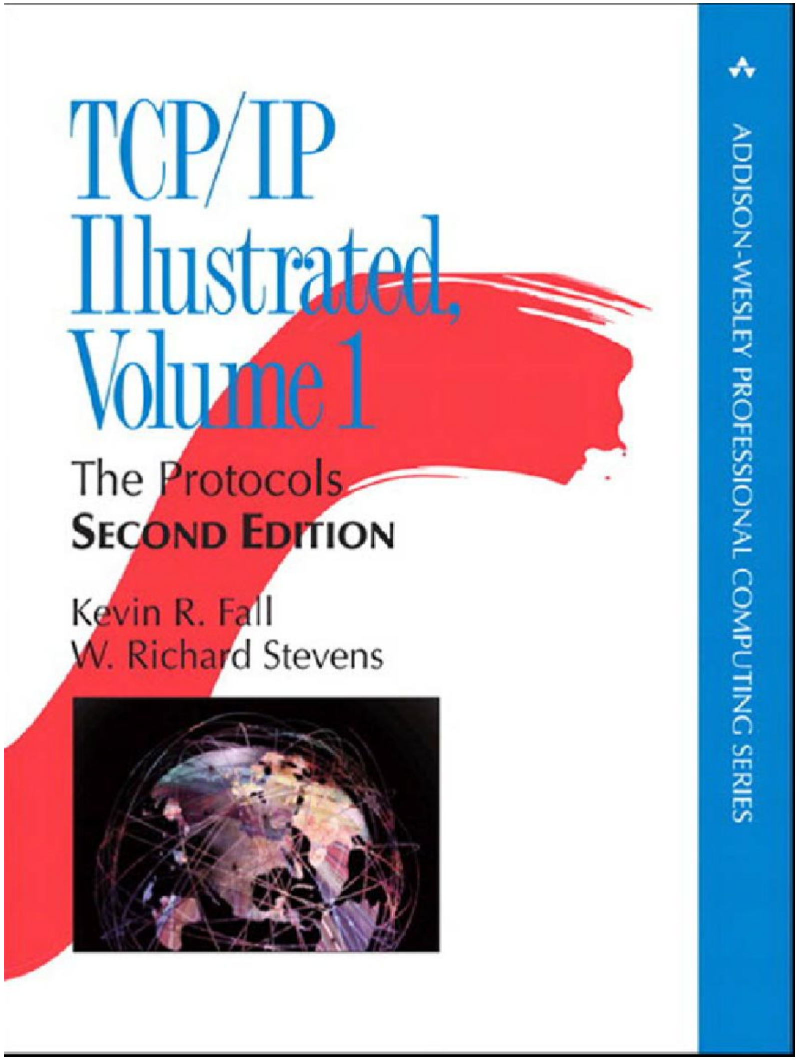


Textbook 2



References

Ref 1



TCP/IP Illustrated, Volume 1

The Protocols

SECOND EDITION

Kevin R. Fall
W. Richard Stevens

ADDISON-WESLEY PROFESSIONAL COMPUTING SERIES

Ref 2

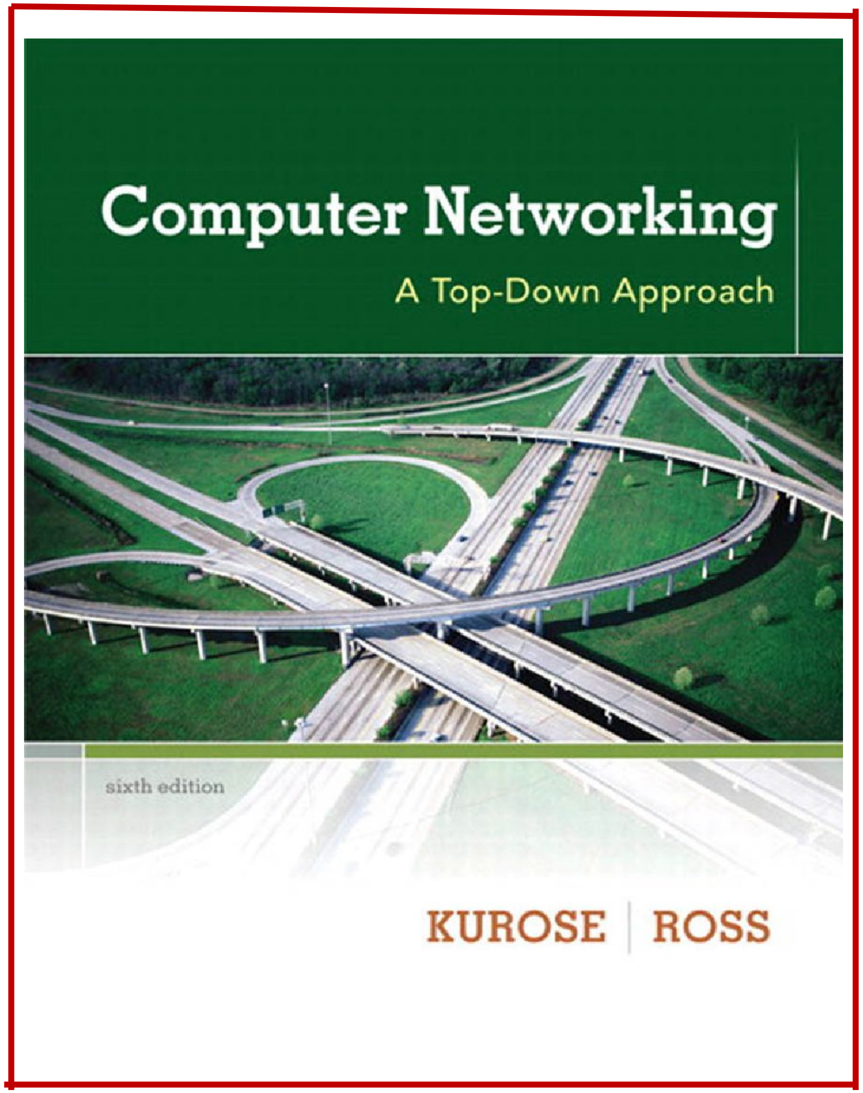
[TCP Congestion Control: A Systems Approach]

TCP Congestion Control: A Systems Approach

Peterson, Brakmo, and Davie

References

Ref 3



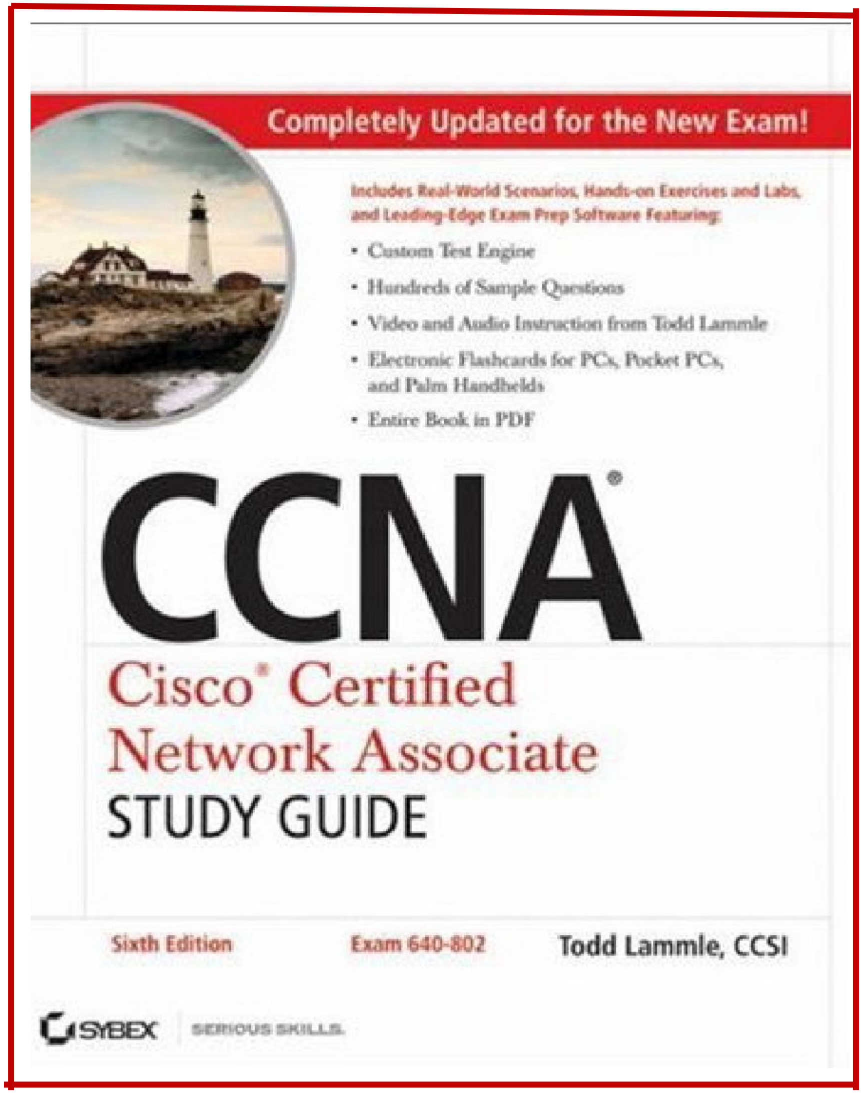
Computer Networking

A Top-Down Approach

sixth edition

KUROSE | ROSS

Ref 4



Completely Updated for the New Exam!

Includes Real-World Scenarios, Hands-on Exercises and Labs, and Leading-Edge Exam Prep Software Featuring:

- Custom Test Engine
- Hundreds of Sample Questions
- Video and Audio Instruction from Todd Lammle
- Electronic Flashcards for PCs, Pocket PCs, and Palm Handhelds
- Entire Book in PDF

CCNA®

Cisco® Certified Network Associate

STUDY GUIDE

Sixth Edition Exam 640-802 Todd Lammle, CCSI

SYBEX SERIOUS SKILLS.

References

Ref 5