Session 7B

IPSec and VPN

Mouli Sankaran

Session 7B: Focus

- IP Security (IPSec)
  - Use Cases
  - Implementation: BITS, BITW and Integrated
  - Protocols and Components
  - Modes: Transport and Tunnel
  - AH and ESP
  - Summary of Features
  - Quiz 1 to 4
- Virtual Private Network (VPN)
  - VPN Server
  - VPN Tunnels
  - Quiz 5

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

IP Security
(IPSec)

IPSec: An Introduction

- Enterprises can run a secure, private IP network by disallowing links to untrusted sites.
- IPSec encrypts IP packets that leave the premises, and authenticating packets that enter the premises.
  - It ensures secure networking not only for applications that are aware of security mechanisms but also for the many security-ignorant applications.
- It encompasses **three functional areas**:
  1. The **authentication** mechanism assures that a received packet was, in fact, transmitted by the party identified as the source in the packet header.

     Note: In addition, this mechanism assures that the packet has not been altered in transit.
  2. The **confidentiality** facility enables communicating nodes to encrypt messages to prevent eavesdropping by third parties during transit.
  3. The **key management** facility is concerned with the secure exchange of keys between the sender and receiver.

Use cases of IPSec

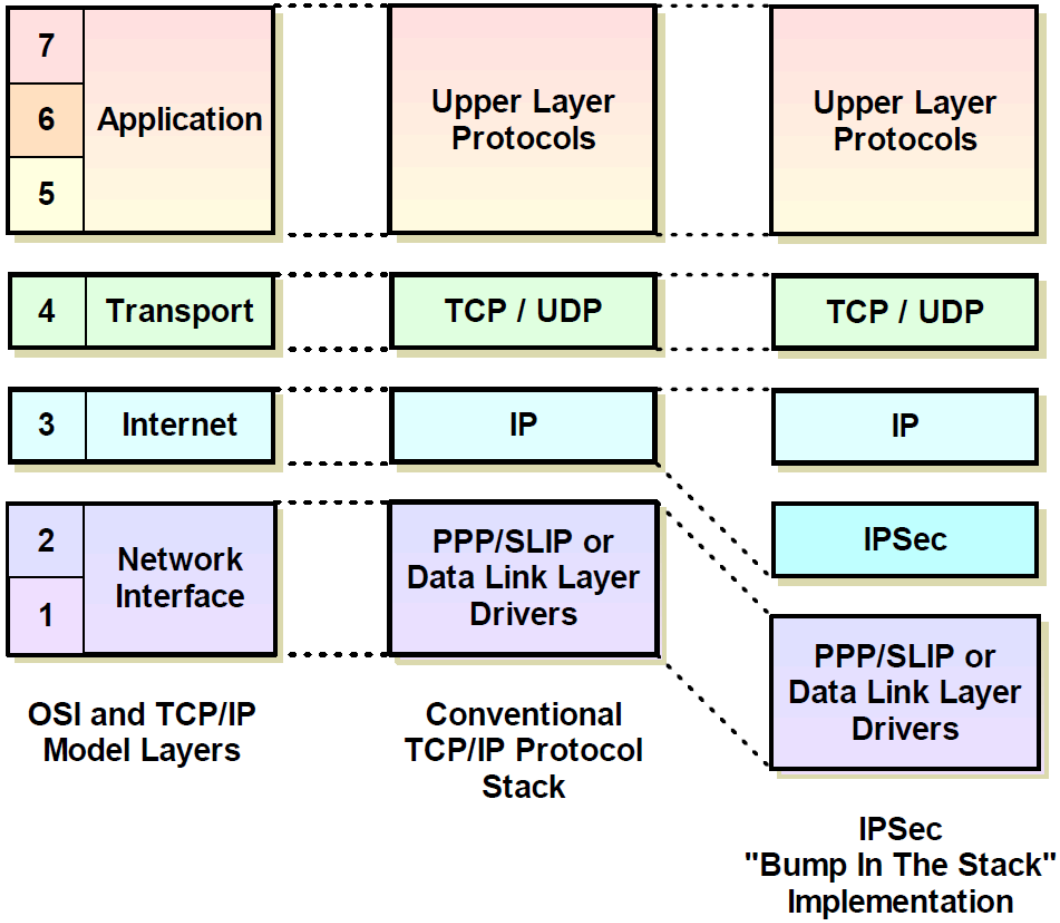
- IPSec can **encrypt** and/or **authenticate** all traffic at the IP level
- It provides the capability to secure communications across a LAN, across private and public WANs, and across the Internet.
- Enterprises can build a secure Virtual Private Network over the Internet or over a public WAN to have secure connectivity between different branches of the enterprise using the Internet.
- An end user whose system is equipped with IP security protocols can make a local call to an Internet Service Provider (ISP) and gain secure access to a company network.
- It can be used to have a secure communication with other organizations.
- Even though some Web and electronic commerce applications have built-in security protocols, the use of IPsec enhances that security.

IPSec Protocols and Components

IPSec Implementation: 1. BITS

BITS: Bump In The Stack

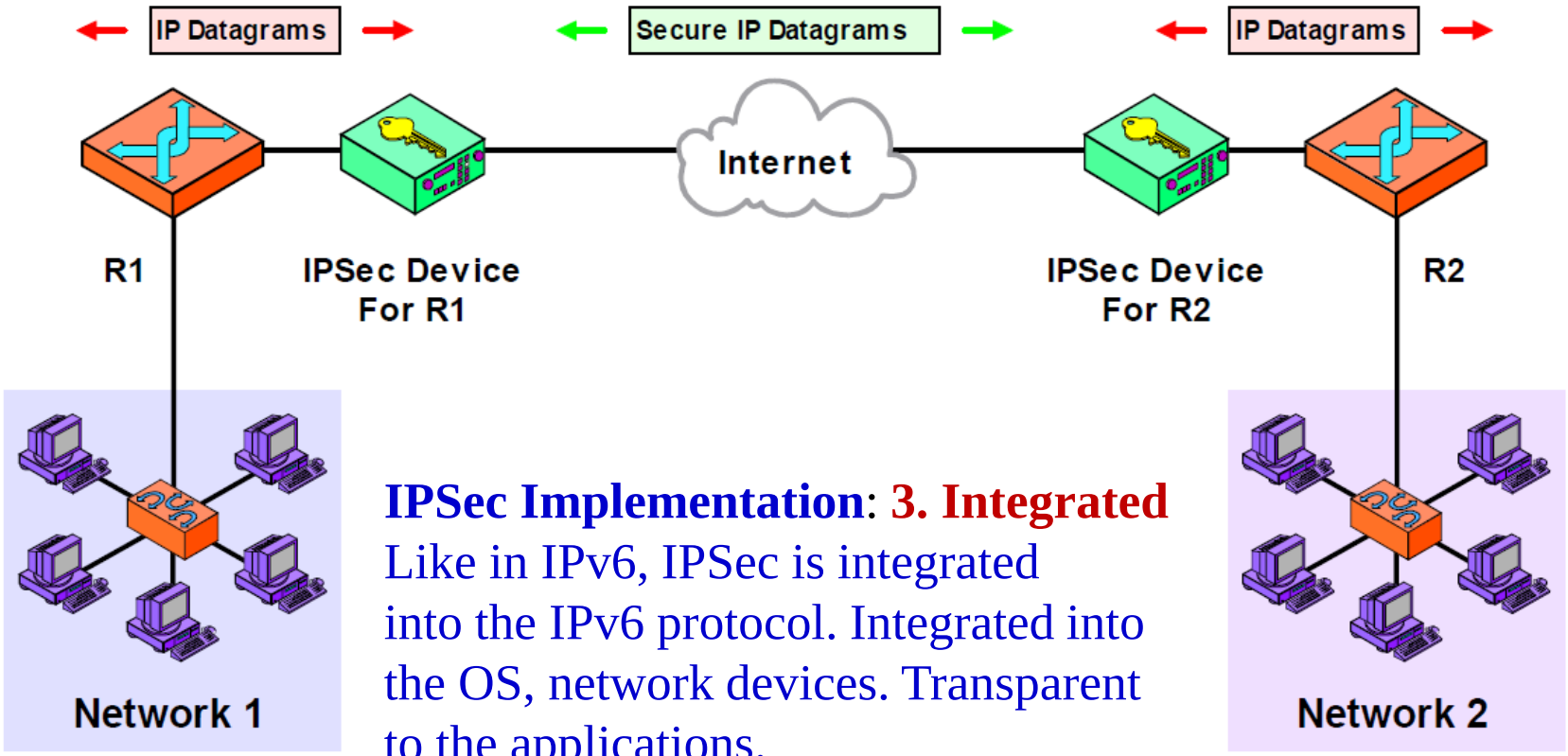
IPSec is integrated within the host's network stack, enabling end-to-end protection directly from the host itself.



IPSec Implementation: 2. BITW

BITS: Bump In The Wire

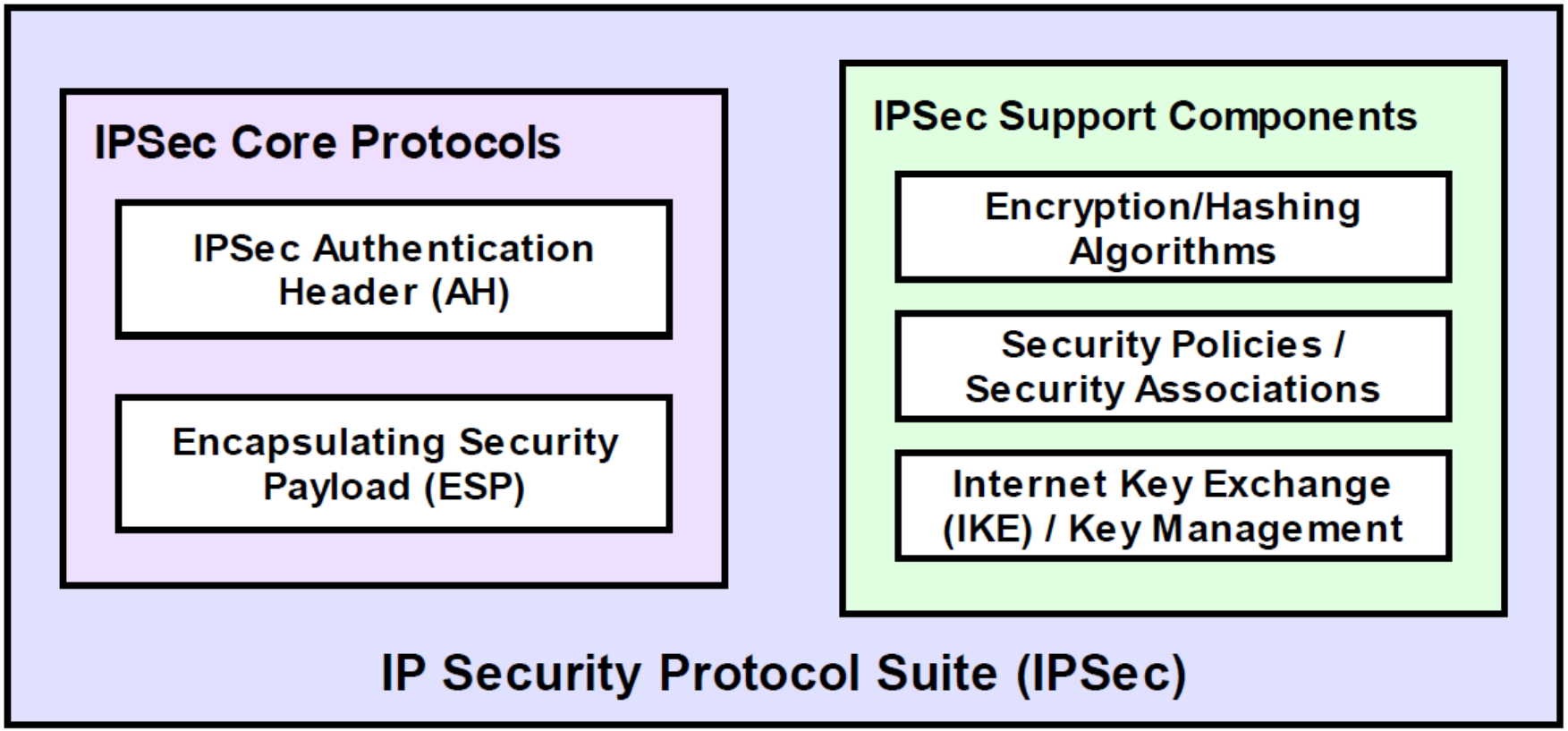
IPSec is implemented in an external hardware device placed between the host and the network, requiring no changes to host systems.



IPSec Implementation: **3. Integrated**
Like in IPv6, IPSec is integrated into the IPv6 protocol. Integrated into the OS, network devices. Transparent to the applications.

Modes of IPSec, AH and ESP

IPSec Protocols and Components



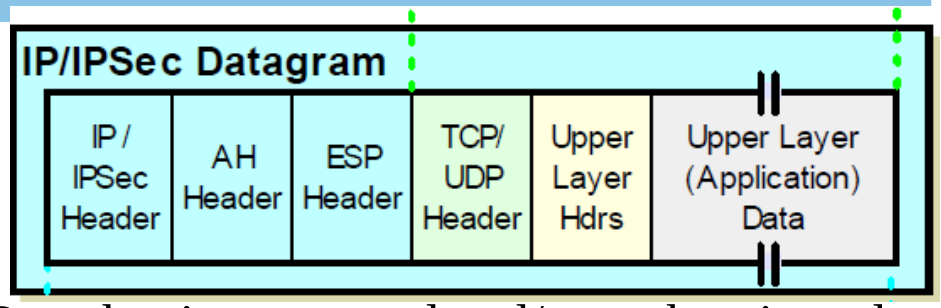
AH: For Authentication
ESP: For Integrity

IPSec Protocols and Components: Explained

- **Authentication Header** (**AH**): Provides **authentication** and **integrity** for IP packets but does not encrypt the payload.
- **Encapsulating Security Payload** (**ESP**): Provides encryption, authentication, and integrity, securing both payload and optional header fields.
- **Security Association** (**SA**): A unidirectional logical connection that defines the security parameters (algorithms, keys) used in IPsec communication.
- **Internet Key Exchange** (**IKE**): Handles automated negotiation of security associations (SAs) and key management for IPSec.
- **Security Policy Database** (**SPD**): Contains rules and policies that determine which traffic should be protected by IPsec.
- **Security Association Database** (**SAD**): Stores active security associations, including encryption/authentication keys and algorithms

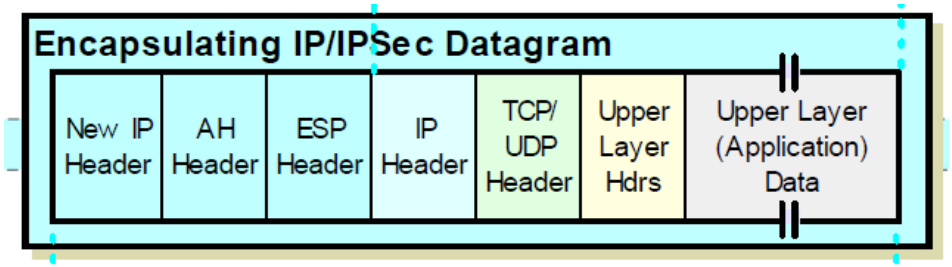
Modes of IPSec

1. Transport Mode:



- Secures end-to-end communication between two hosts (client ↔ server)
- Only the payload (data part) of the IP packet is encrypted and/or authenticated.
- The original IP header is left intact.
- **Example**: SSH, Telnet, or remote access.

2. Tunnel Mode:



- Secures network-to-network or host-to-network communication (e.g., via VPNs).
- Entire IP packet (header + payload) is encapsulated inside a new IP packet.
- A new outer IP header is added for routing.
- **Example**: A branch office connecting securely to headquarters via VPN

AH: Authentication Header **ESP**: Encapsulating Security Payload

Authentication Header (AH) : Explained

- AH provides **data integrity**, **origin authentication**, and **optional anti-replay protection** for IP packets — but **does not provide encryption**.
- **AH** calculates a **cryptographic hash** over the **IP header fields** and its **payload** and inserts the **resulting hash** into the AH header.
  - It uses a special hashing algorithm and a specific key known only to the source and destination.
  - SA between the source and destination specifies these particulars, so they know how to perform these operations but no one else can.
- The receiver **recalculates the hash** and compares it to the one received to verify **authenticity** and **integrity**.
- The presence of AH header allows **verification of integrity** of the message, but doesn't encrypt it.
- **AH provides authentication but not privacy!! (that's what ESP is for)**
- AH is normally not used because of its incompatibility with NAT. So, ESP is the preferred and complete solution.

Resulting Hash: Integrity Check Value (ICV)

Encapsulating Security Payload (ESP) : Explained

- ESP uses **encryption algorithm** and a **key** to transform the datagram into an encrypted form, so that privacy of IP datagram in transit is achieved.
- Since some encryption algorithms only work on **fixed block size of data**, **there is a need** to perform **padding** of IP datagram before encryption
- Apart from the **ESP header**, **ESP trailer** is also required here to take care of padded data for encryption
- The receiver performs decryption of the received data (including the ESP trailer, based on the algorithm) to get the original data back.
- To make sure that the encrypted data is not tampered with while in transit, there is an additional **ESP Authentication Data** field is also added.
  - This field is used when the ESP's optional authentication feature is employed.
  - It is similar to the ICV used by AH.

Integrity Check Value (ICV)

IPSec: Summary of Features

1. Features of IPSec

- **Authentication**: IPSec provides authentication of IP packets using digital signatures or shared secrets. This helps ensure that the packets are not tampered with or forged.
- **Confidentiality**: IPSec provides confidentiality by encrypting IP packets, preventing eavesdropping on the network traffic.
- **Integrity**: IPSec provides integrity by ensuring that IP packets have not been modified or corrupted during transmission.
- **Key management**: IPSec provides key management services, including key exchange and key revocation, to ensure that cryptographic keys are securely managed.

2. Features of IPSec

- **Tunneling**: IPSec supports tunneling, allowing IP packets to be encapsulated within another protocol, such as GRE (Generic Routing Encapsulation) or L2TP (Layer 2 Tunneling Protocol).
- **Flexibility**: IPSec can be configured to provide security for a wide range of network topologies, including point-to-point, site-to-site, and remote access connections.
- **Interoperability**: IPSec is an open standard protocol, which means that it is supported by a wide range of vendors and can be used in heterogeneous environments.

IPSec: Quiz 1 to 5

Quiz 1: IPSec: AH

- Which of the following security services is not provided by IPsec's Authentication Header (AH)?

ANS: B

A. Data Integrity
B. Data Confidentiality
C. Source Authentication
D. None of the above options is correct

Note:
AH provides integrity, authentication, and optional anti-replay protection.
It does not encrypt the data, so it does not provide confidentiality.

Quiz 2: IPSec: ESP

- Which of the following statements about IPsec **ESP** (Encapsulating Security Payload) is true when used with authentication?

A. ESP can provide encryption, but authentication must be done using AH
B. ESP provides confidentiality, but cannot verify data integrity
C. ESP can provide both encryption and integrity if configured with authentication
D. ESP encrypts only the IP header, not the payload.

ANS: C

Note:
ESP supports encryption (confidentiality) and optional integrity/authentication. When authentication is enabled, ESP can secure both confidentiality and integrity without needing AH.

Quiz 3: IPSec Modes

- In which IPsec mode is the original IP header encrypted along with the payload?

A. Transport mode
B. Tunnel mode
C. Gateway mode.
D. AH Mode

ANS: B

Note:
In **Tunnel Mode**, the entire original IP packet (header + payload) is encrypted and placed inside a new IP packet.
In **Transport Mode**, only the payload is encrypted; the IP header is left intact.

Quiz 4: IPSec Protocols

- Which protocol is responsible for negotiating and establishing Security Associations (SAs) in IPsec?

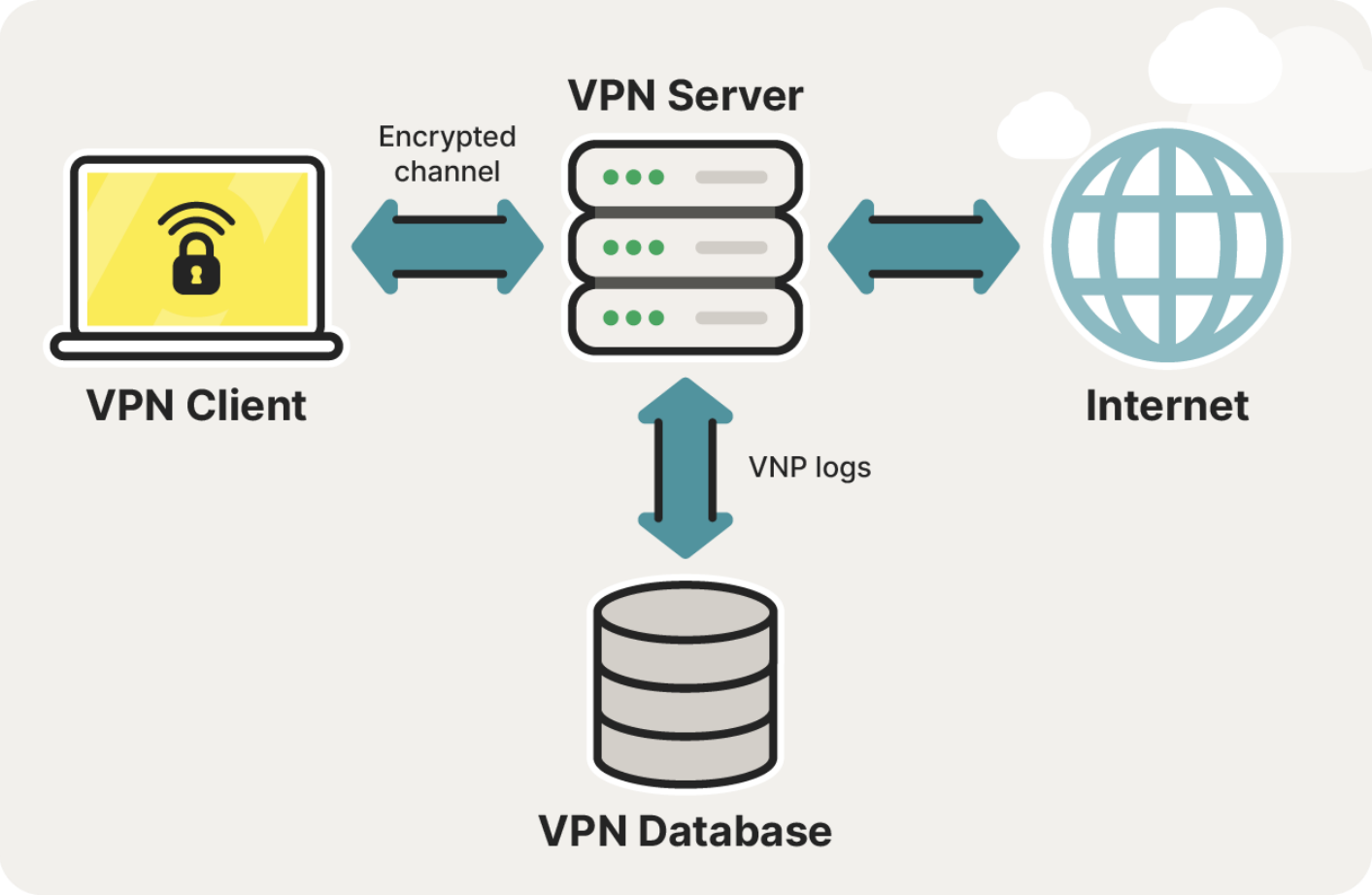
A. ESP
B. AH
C. IKE
D. SSL

ANS: C

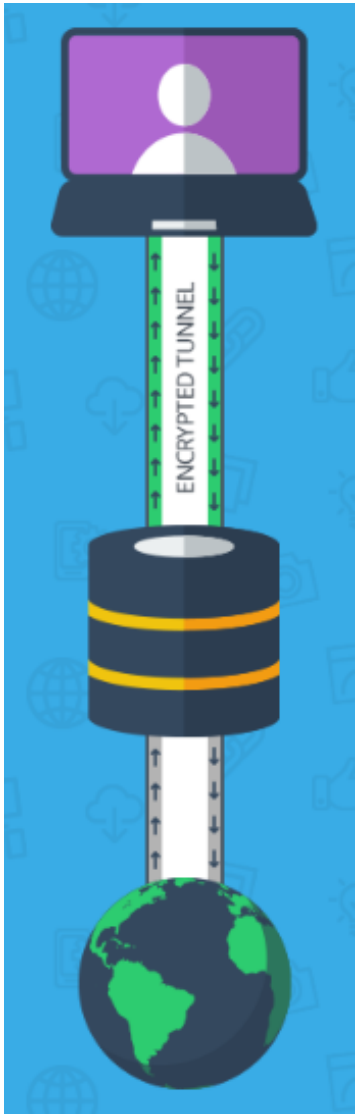
Note:
IKE is the protocol used to automate the negotiation of cryptographic keys and policies in IPsec.
ESP and AH are used to protect traffic after SAs are established.

VPN

Connecting through VPN Server



VPN: Explained



As long as you can connect to the internet, you can **connect to a VPN**. You can be at home on your own network or in a public place such as a cafe or library and connect through a public wifi.

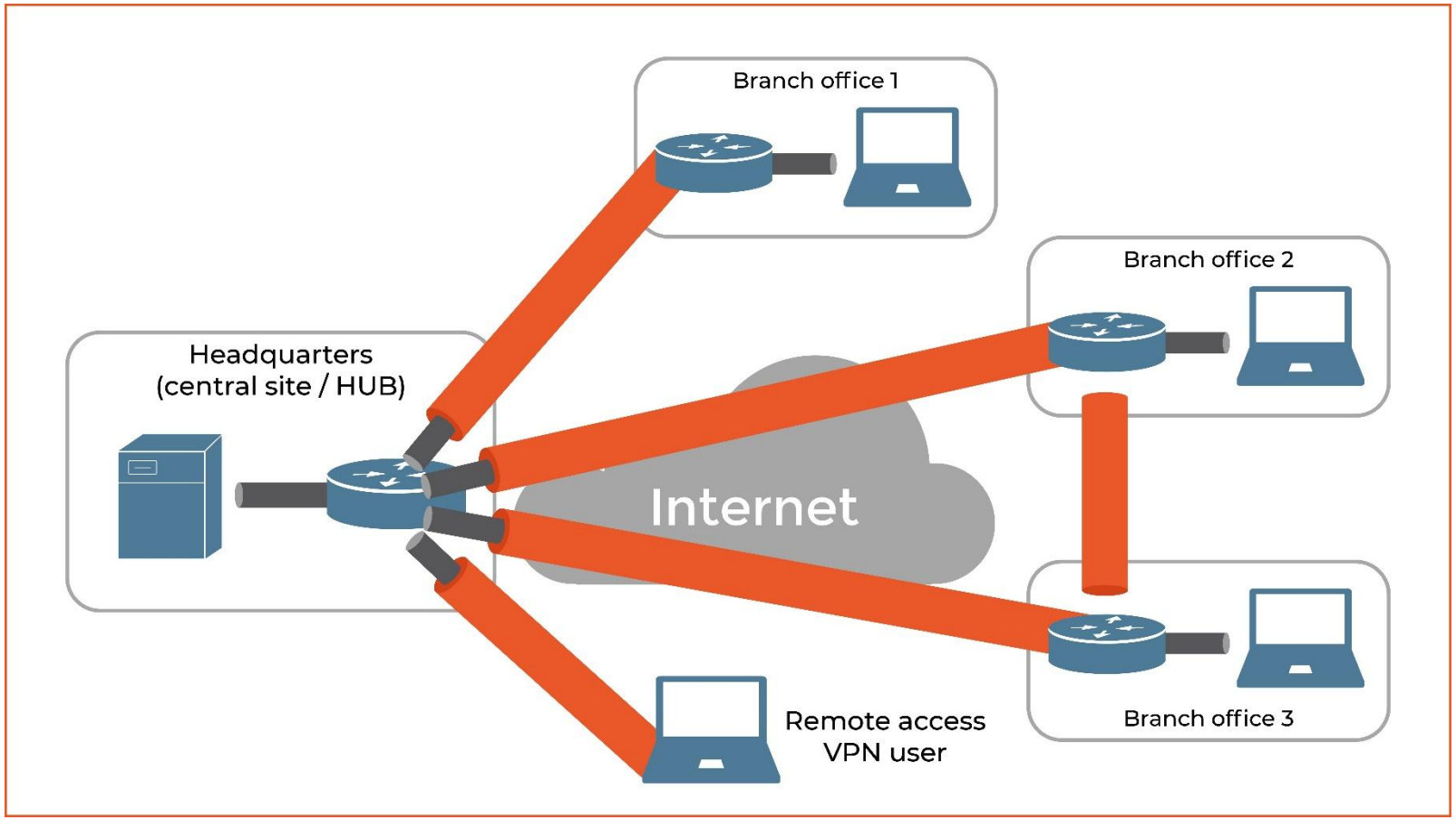
Once connected to a VPN server, the VPN provider sets up a **private tunnel**. As long as your online traffic is routed through this tunnel, **all your data is encrypted** on the way to the VPN's server. Its origin (determined by IP address) is also hidden for other internet users and websites.

Once your VPN provider **encrypts your traffic** and routes it through its own server, it's passed to the destination website. The website responds and the traffic is routed right back to the VPN's server which then sends it back to your device. **Encrypted and safe** from prying eyes.

Password + token

VPN for Connecting Branch Offices

Ref: Lab 8 Implementation of VPN using CISCO Packet Tracer.



Note: Once a VPN tunnel is successfully established, it acts like a virtual pipe through which IP packets flow both ways

Quiz 5: VPN

- Which of the following is a commonly used VPN protocol that supports encryption and runs at Layer 3 of the OSI model?

A. FTP
B. HTTP
C. IPSec
D. None of the above.

ANS: C

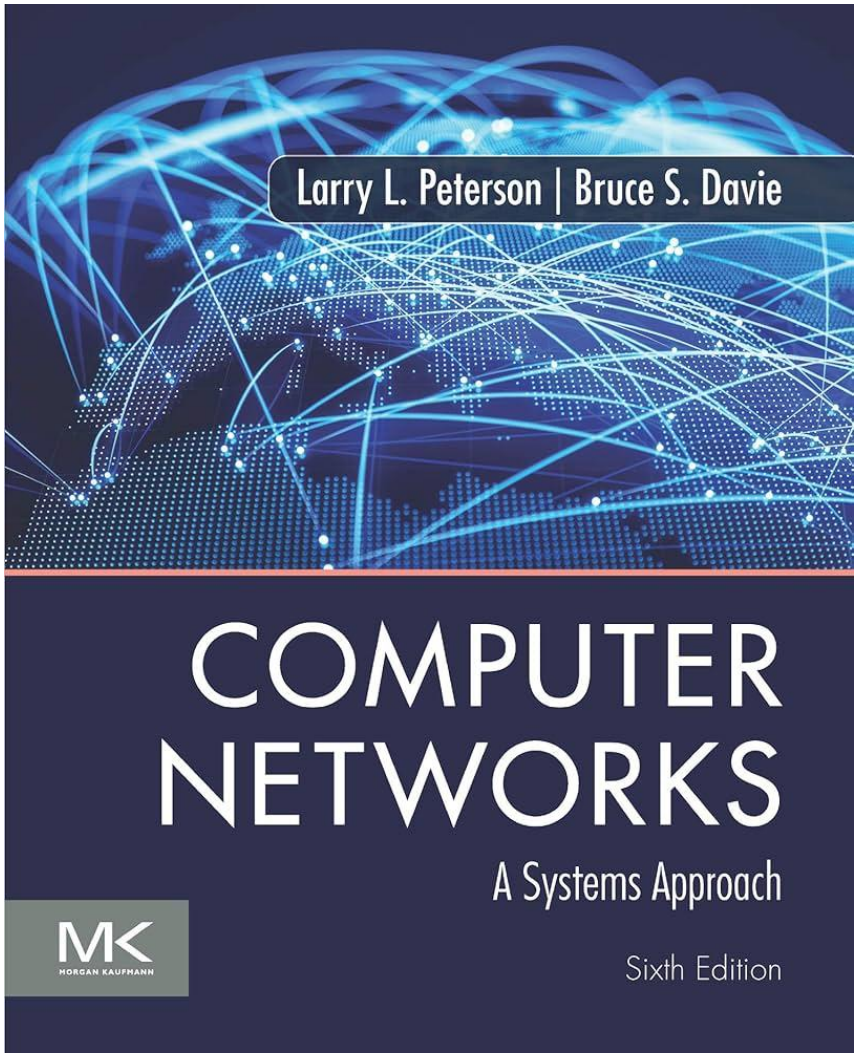
Note:
IPSec is a widely used **VPN** protocol that works at the Network Layer (Layer 3) of the OSI model and provides encryption, authentication, and integrity.

Session 7B: Summary

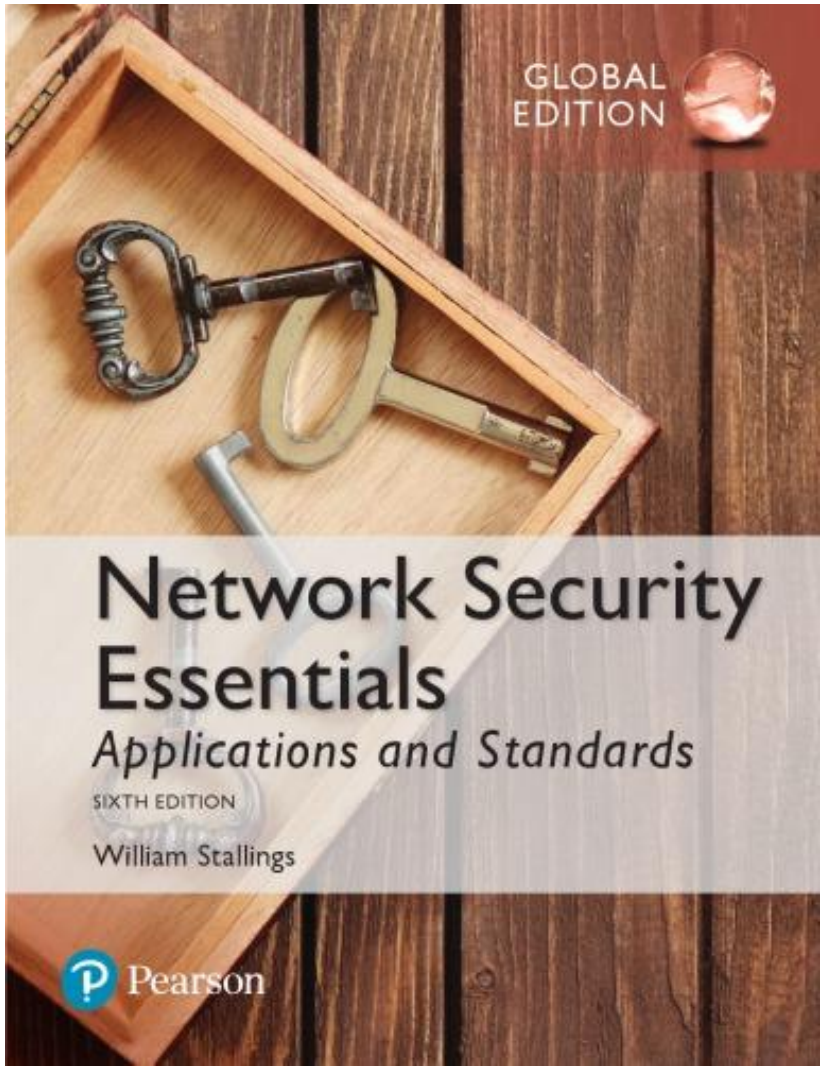
- IP Security (IPSec)
  - Use Cases
  - Implementation: BITS, BITW and Integrated
  - Protocols and Components
  - Modes: Transport and Tunnel
  - AH and ESP
  - Summary of Features
  - Quiz 1 to 4
- Virtual Private Network (VPN)
  - VPN Server
  - VPN Tunnels
  - Quiz 5

Textbooks

Textbook 1

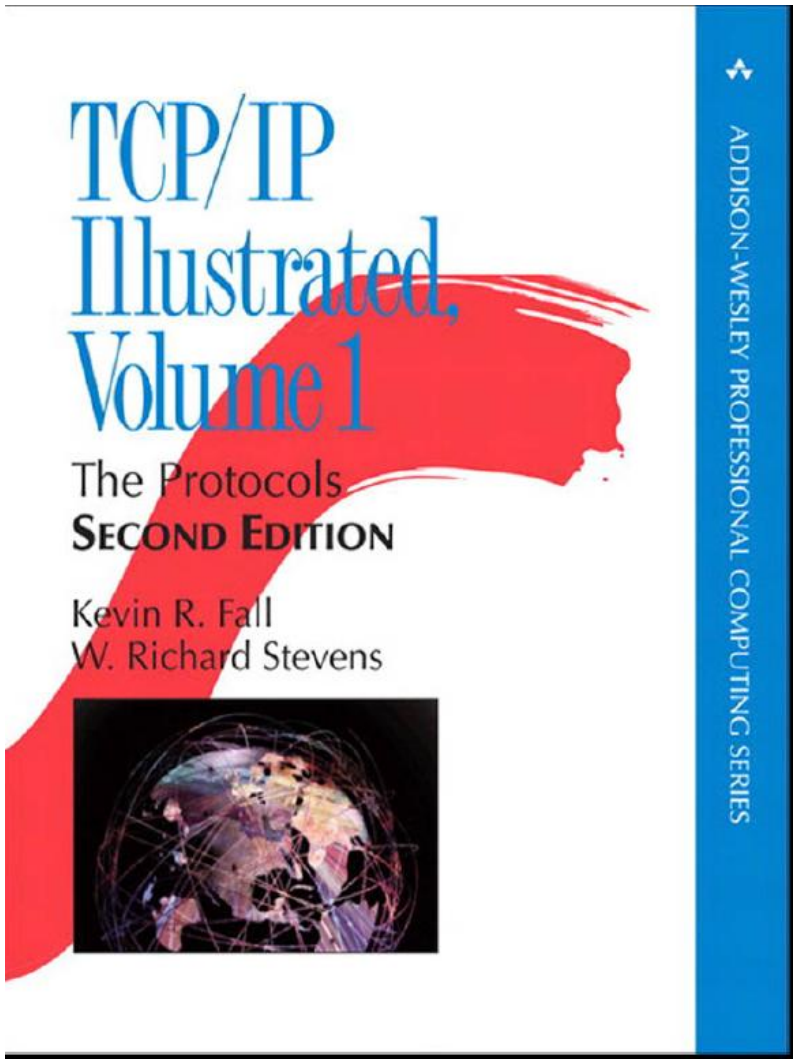


Textbook 2



References

Ref 1



Ref 2

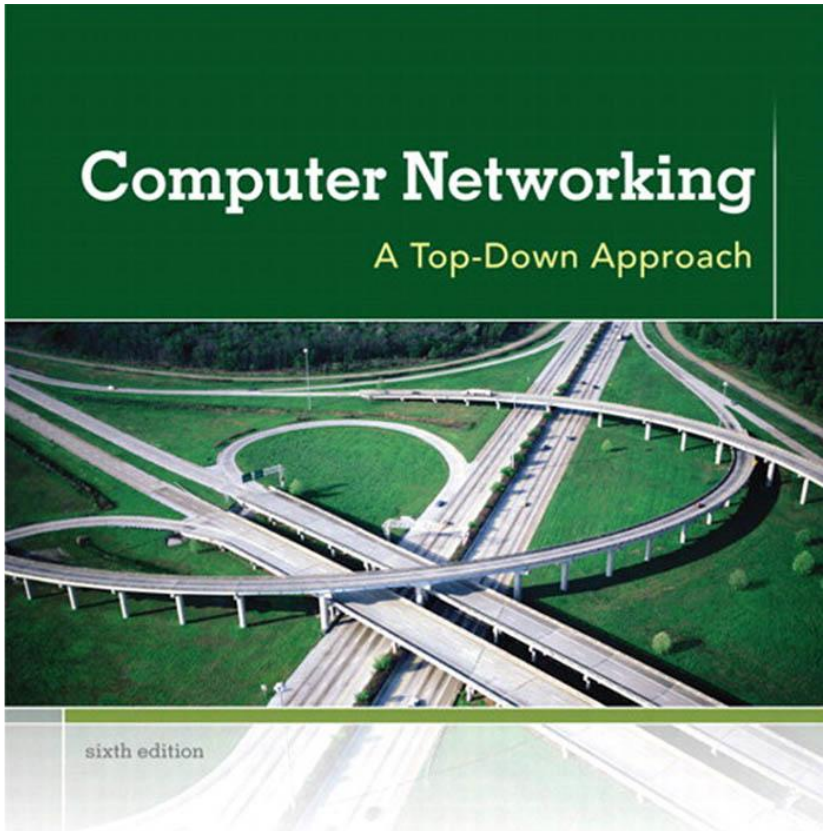
TCP Congestion Control: A Systems Approach

TCP Congestion Control: A Systems Approach

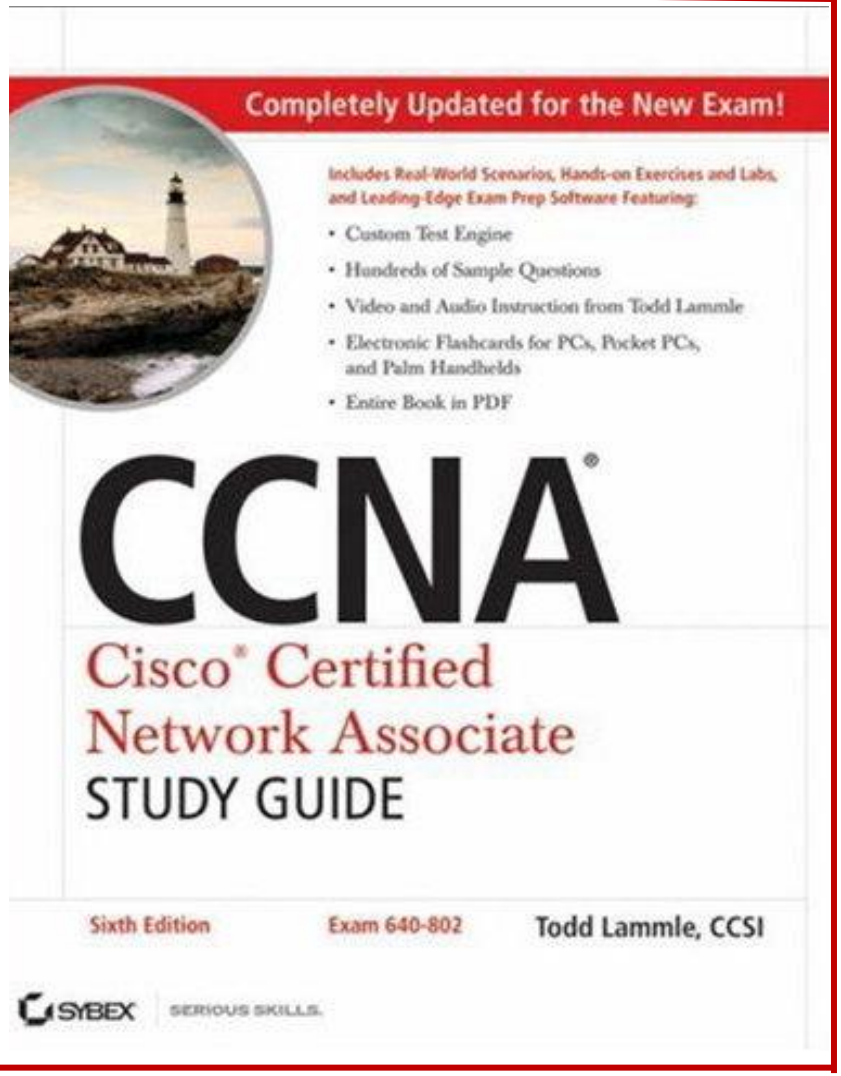
Peterson, Brakmo, and Davie

References

Ref 3



Ref 4



References

Ref 5