BSCIT

Network Security

Unit 4

Transport Level Security

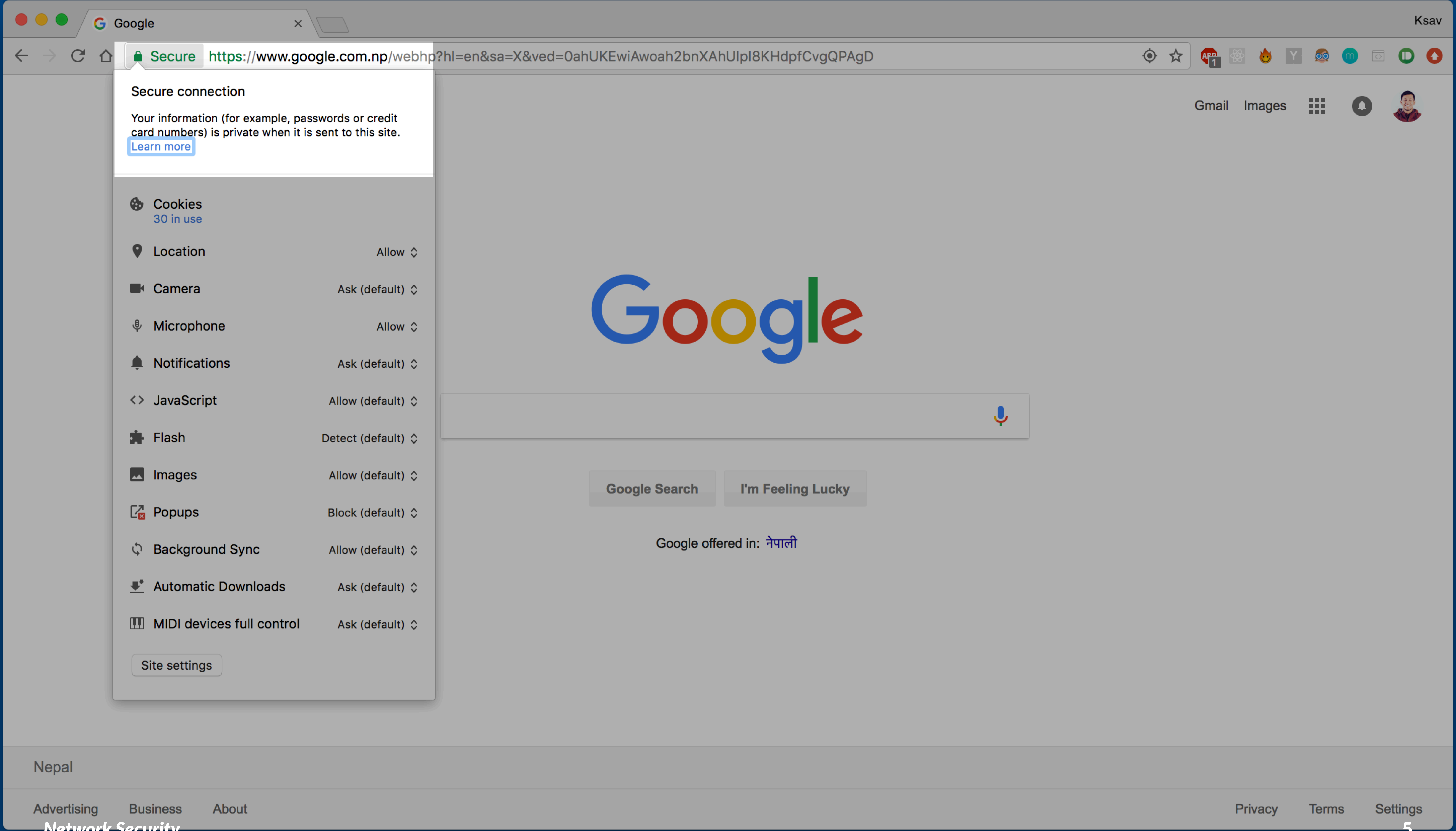
Unit 4

Transport Level Security

Topics

1. Web Security Issues
2. Secure Socket Layers (SSL)
3. Transport Layer Security (TLS)
4. HTTPS (HyperText Transfer Protocols)
5. Secure Shell (SSH)

4.1 *Web Security* Issues



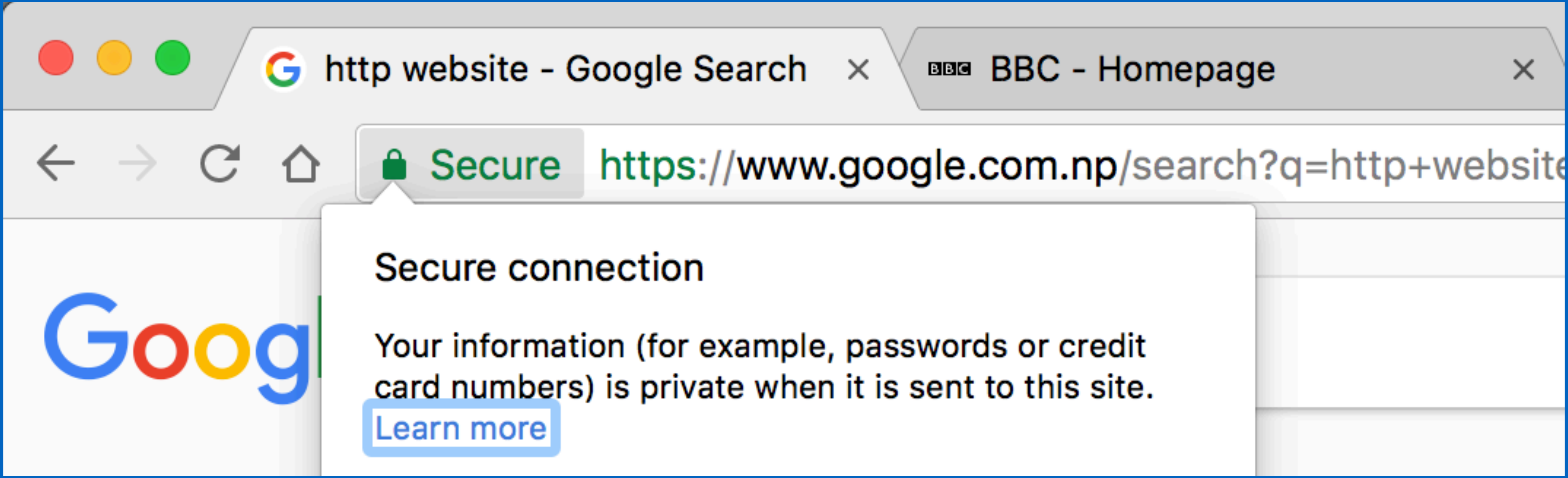
Secure connection

Your information (for example, passwords or credit card numbers) is private when it is sent to this site. Learn more

Cookies
30 in use

Location	Allow
Camera	Ask (default)
Microphone	Allow
Notifications	Ask (default)
JavaScript	Allow (default)
Flash	Detect (default)
Images	Allow (default)
Popups	Block (default)
Background Sync	Allow (default)
Automatic Downloads	Ask (default)
MIDI devices full control	Ask (default)

Google offered in: नेपाली



http website - Google Search
BBC
BBC - Homepage
Secure
https://www.google.com.np/search?q=http+website
Goog

Secure connection

Your information (for example, passwords or credit card numbers) is private when it is sent to this site.

Learn more

http:// ⚔️ https://

4.1.1 Web Security Threats

4.1.2 Web Traffic Security Approaches

4.1.1 Web Security Threats

Two way of grouping Web Security Threats

> Nature of attack.

> Location of Attack.

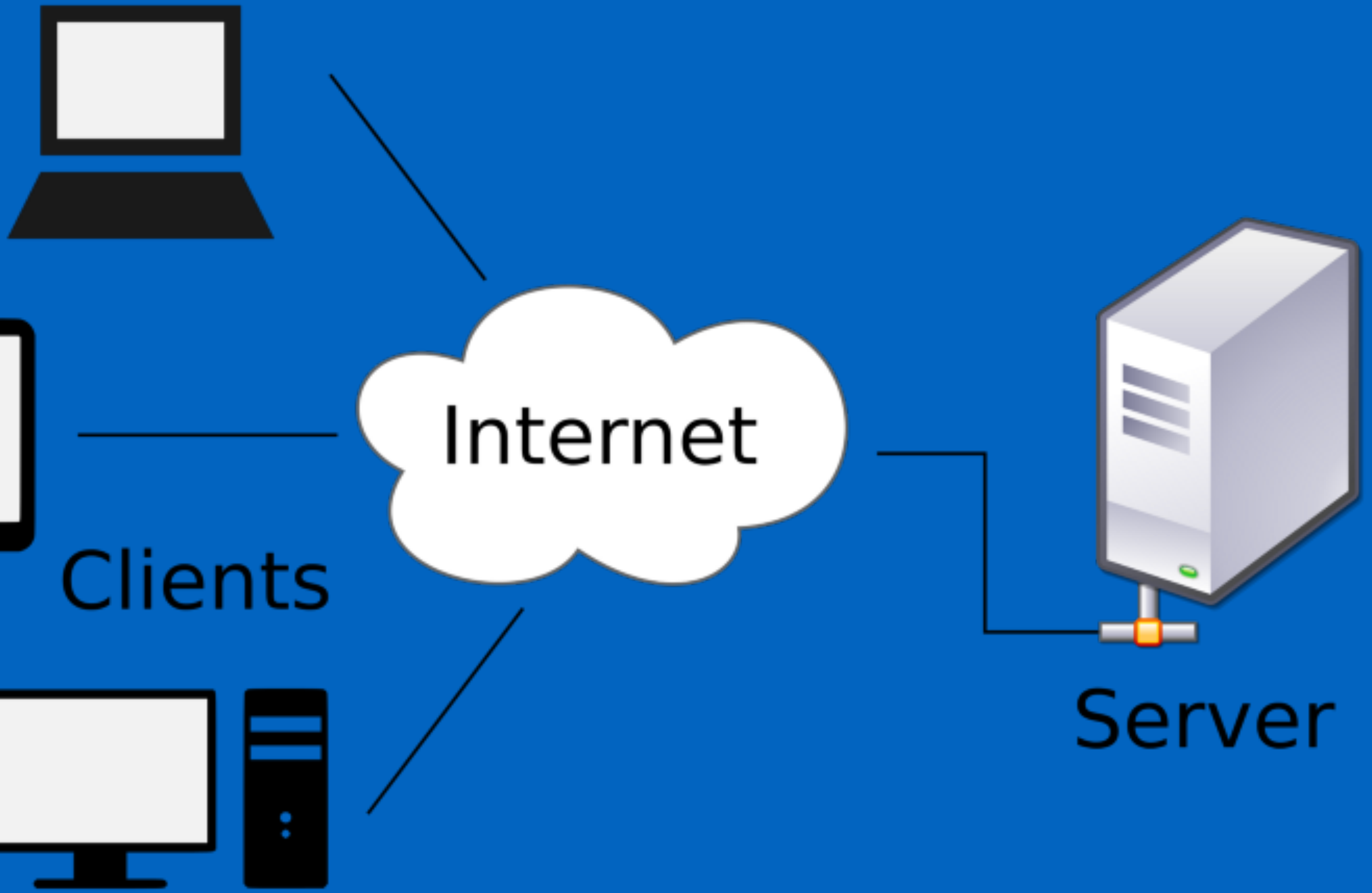
Nature of attack.

1 Active Attack

2 Passive Attack

Location of Attack.

Client Server Architecture



3 Locations for attack

1. Client

2. Server

3. Network

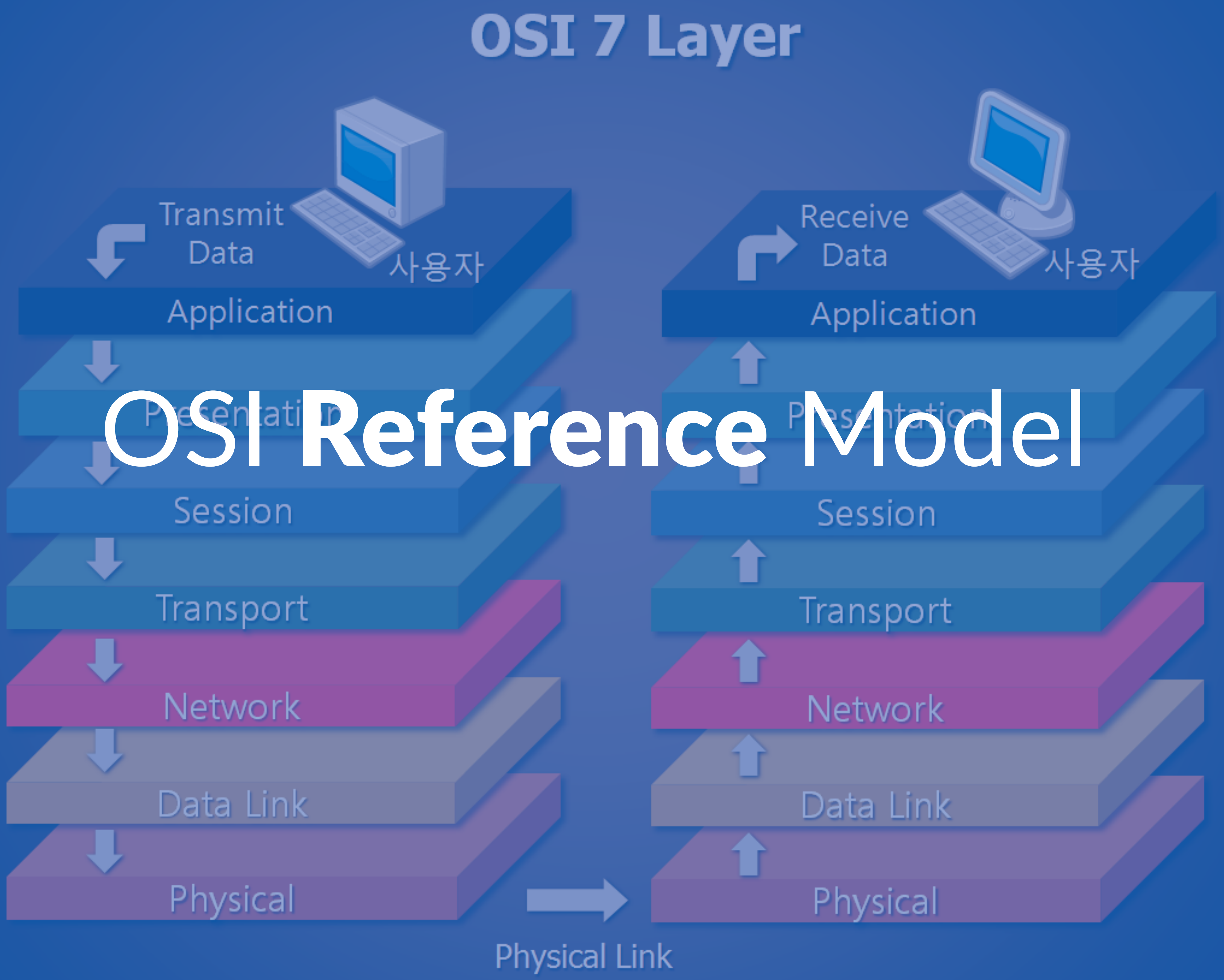
In the context of web

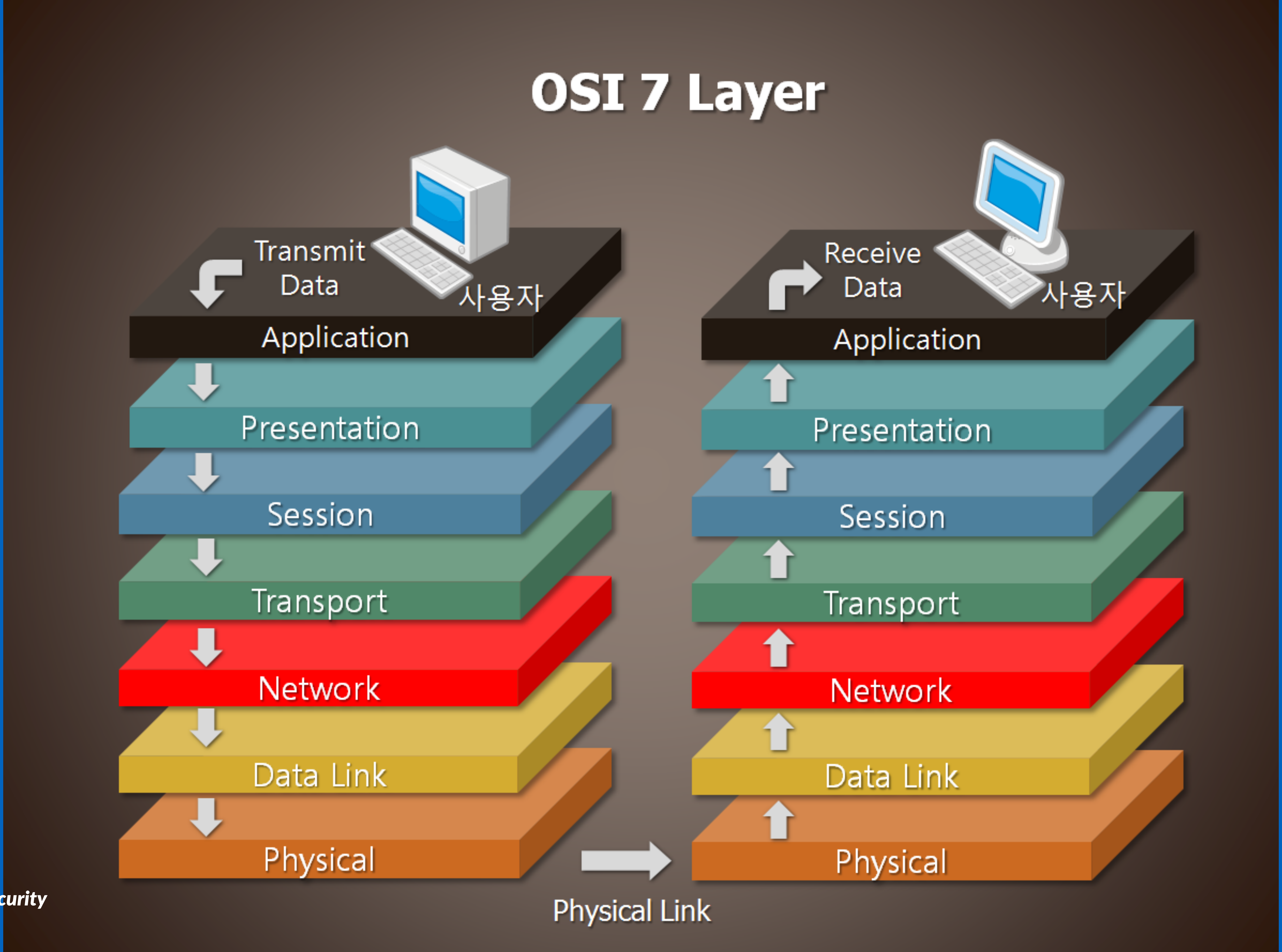
1. Web browser

2. Web server

3. Network traffic in between them

OSI **Reference** Model





OSI 7 Layer

Transmit Data

사용자

Application

Presentation

Session

Transport

Network

Data Link

Physical

Receive Data

사용자

Application

Presentation

Session

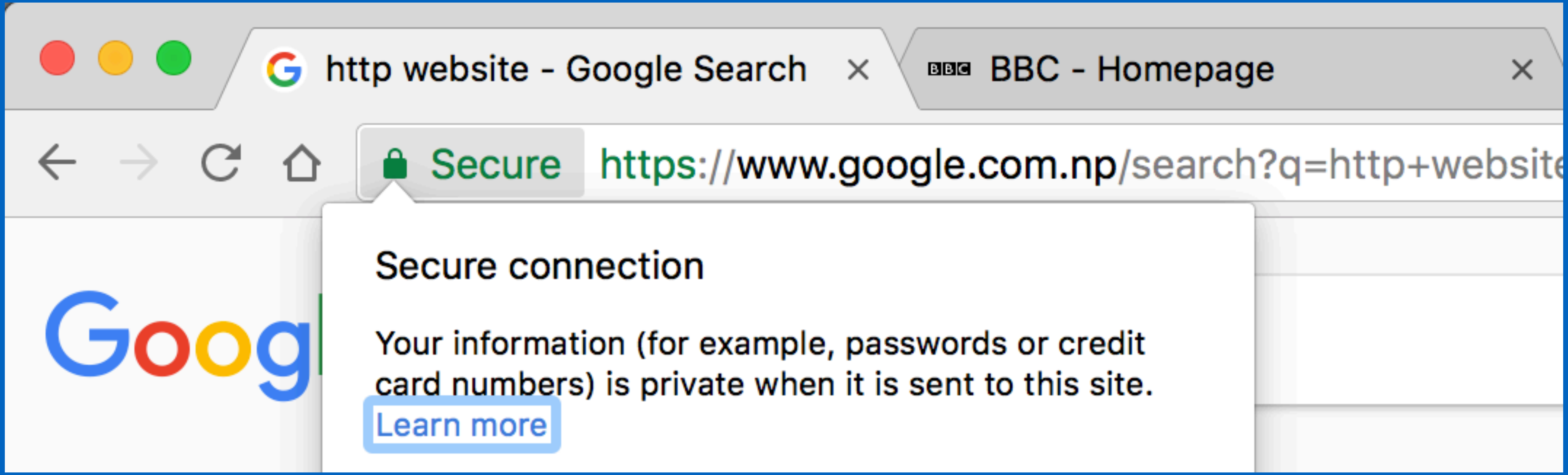
Transport

Network

Data Link

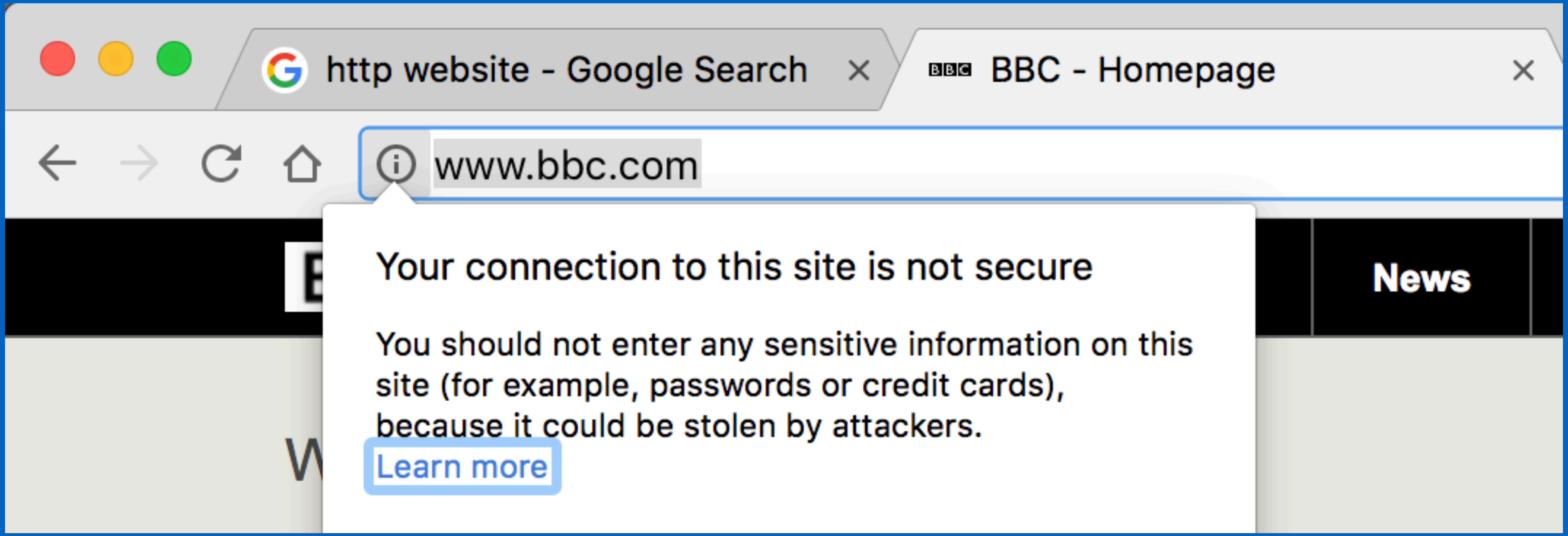
Physical

Physical Link


http website - Google Search
BBC - Homepage
Secure
https://www.google.com.np/search?q=http+website
Goog

Secure connection

Your information (for example, passwords or credit card numbers) is private when it is sent to this site. Learn more



Your connection to this site is not secure

You should not enter any sensitive information on this site (for example, passwords or credit cards), because it could be stolen by attackers. Learn more

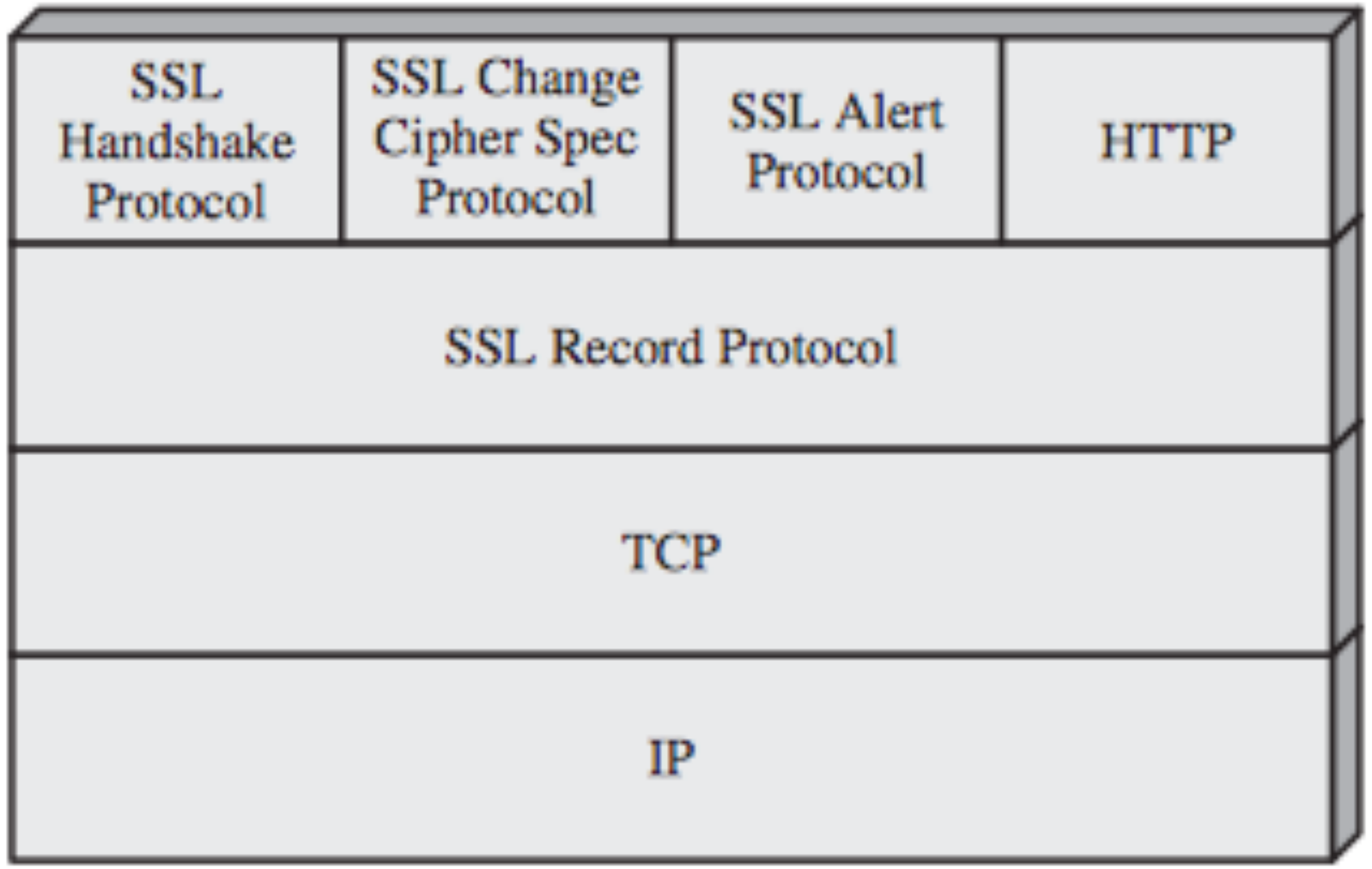
SSL History

- SSL V1
- SSL V2
- SSL V3 / TLS V1.0
- TLS V1.1
- TLS V1.2 (Latest)
- TLS V1.3 (Draft)

SSL Concepts

- SSL Connection
- SSL Session

SSL Architecture



SSL Handshake Protocol

SSL Change Cipher Spec Protocol

SSL Alert Protocol

HTTP

SSL Record Protocol

TCP

IP

Figure 16.2 SSL Protocol Stack

SSL Architecture

- SSL Record Protocol

1. The Change Cipher Spec Protocol
2. The Alert Protocol
3. The Handshake Protocol

SSL Record Protocol

- Services
  - Message Integrity using MAC
  - Confidentiality using Symm. Enc.
- Operation (6 Steps)

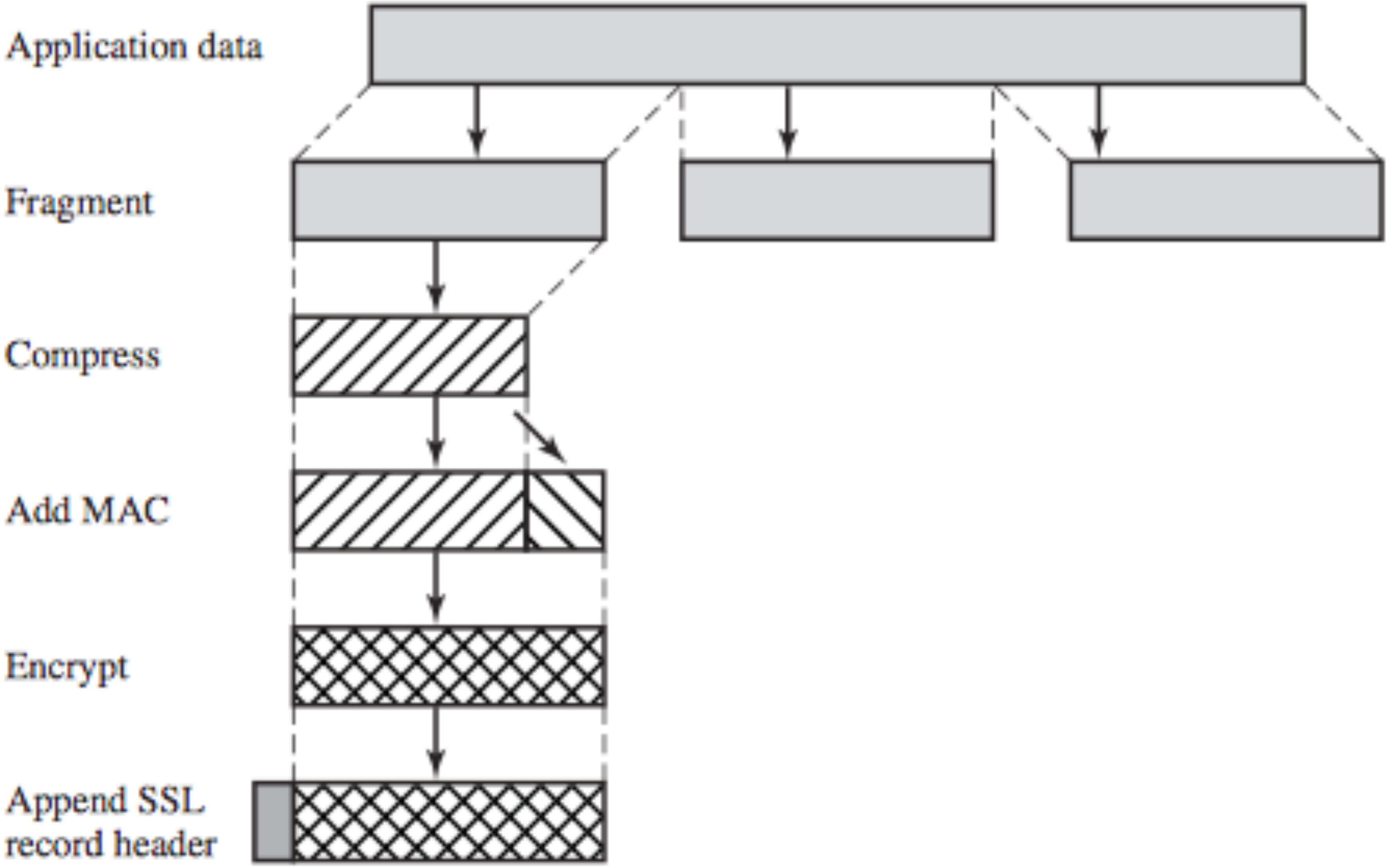


Figure 16.3 SSL Record Protocol Operation

Operation (6 Steps)

1. App Data from Application Layer

2. Fragmentation

3. Compass

4. Add MAC

5. Encrypt

6. Add SSL Record Header

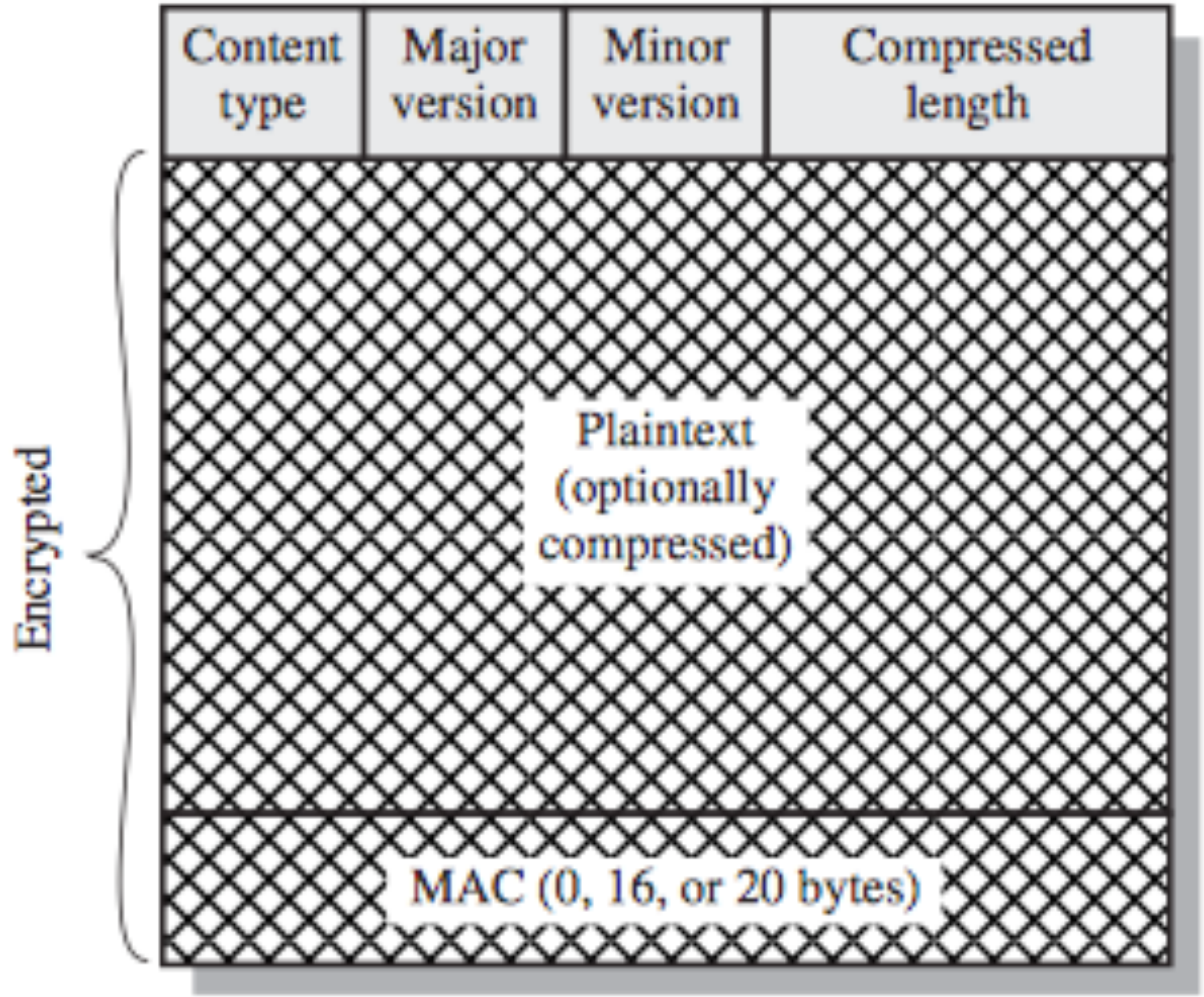


Figure 16.4 SSL Record Format

SSL Record Header

- Content Type ('text/html', 'audio/mp3', 'image/png')
- Major Version
- Minor Version
- Compressed Length

SSL Record Protocol

- 1. The Change Cipher Spec Protocol
- 2. The Alert Protocol
- 3. The Handshake Protocol

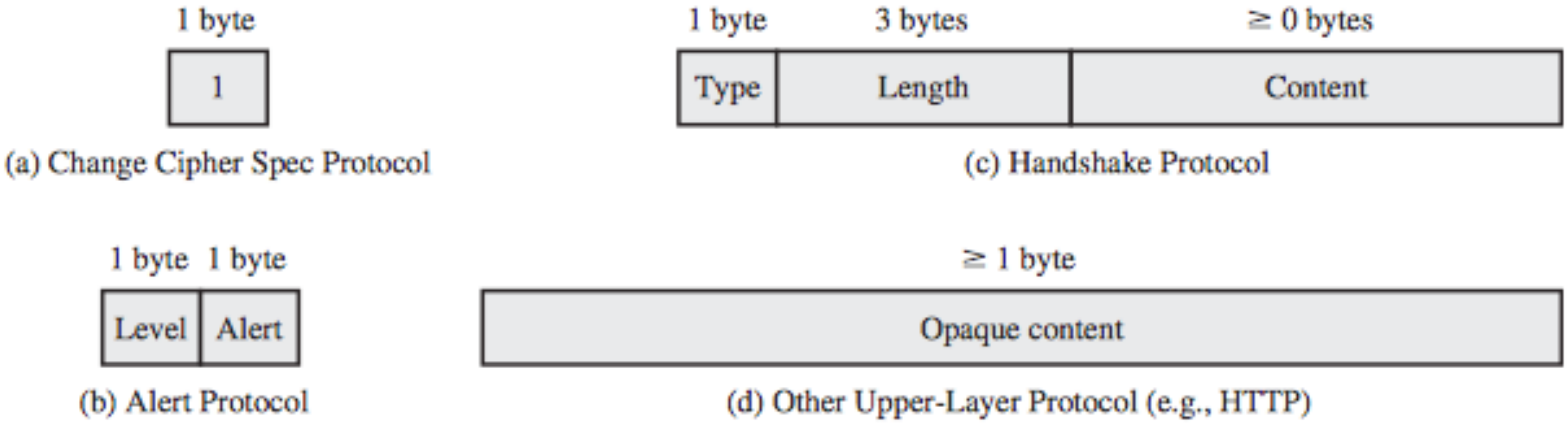
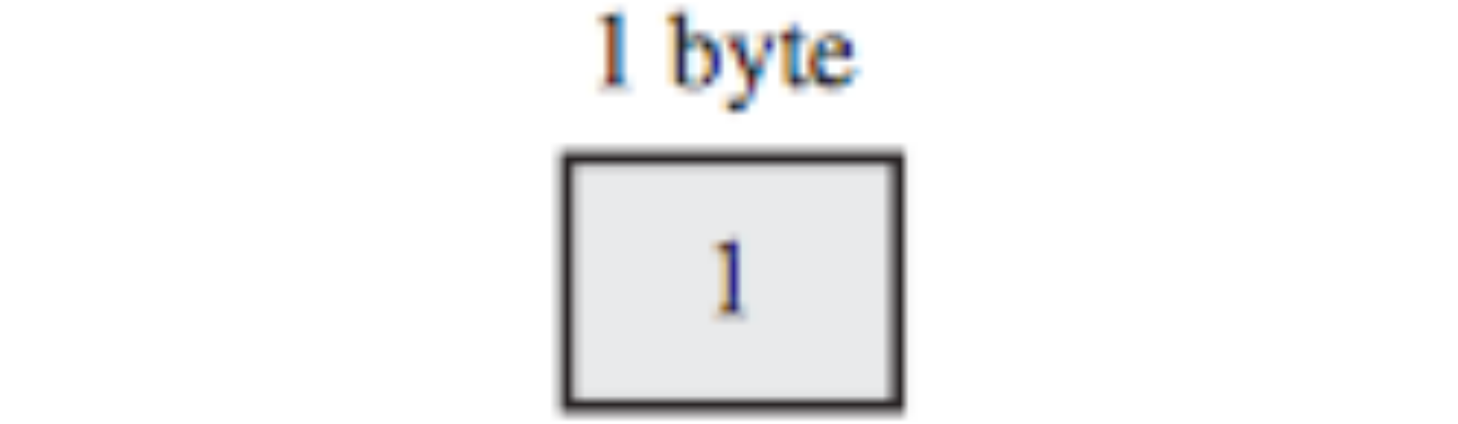


Figure 16.5 SSL Record Protocl Payload

1. The Change Cipher Spec Protocol

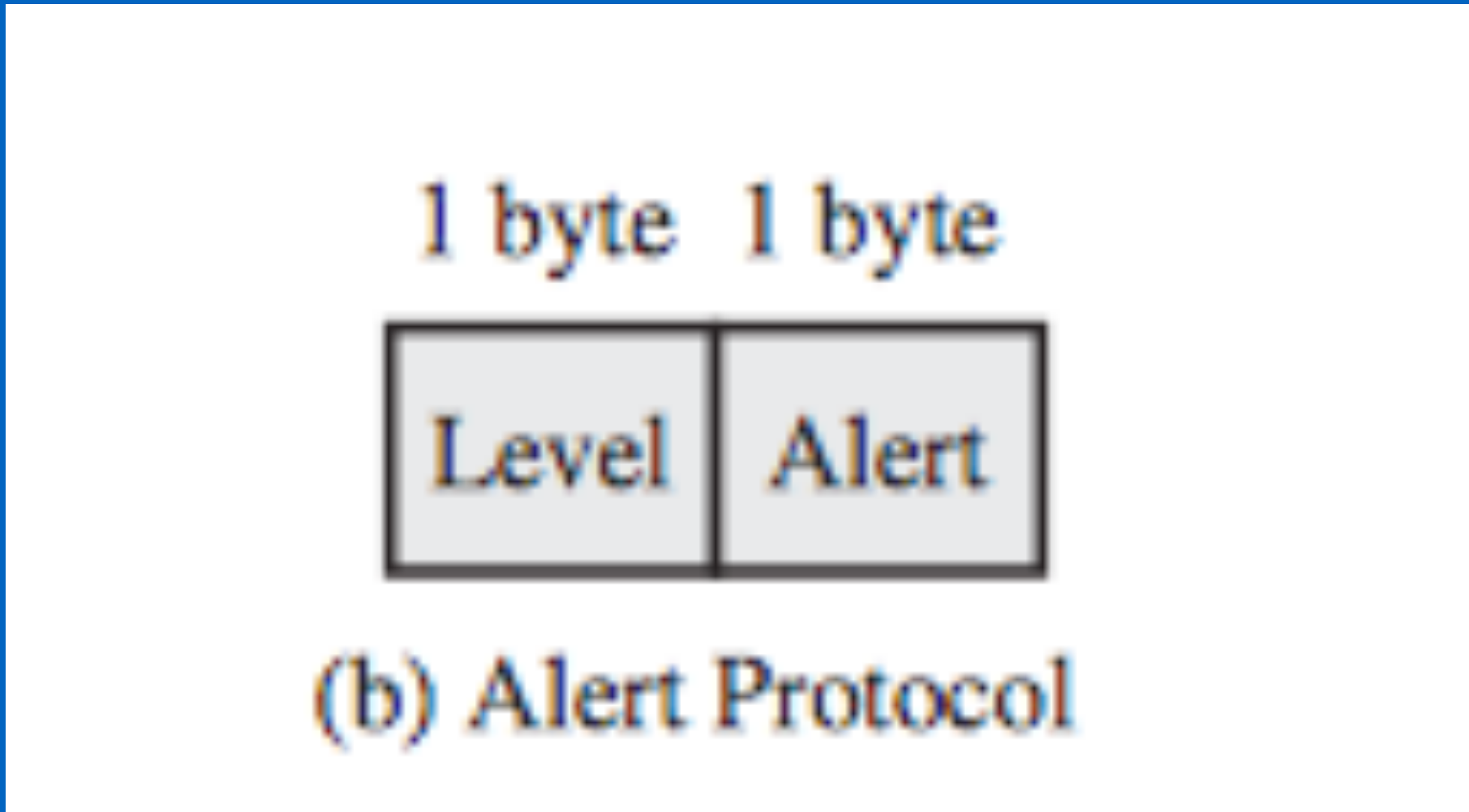
- Simplest
- Consists of single message
- Single Byte with Value 1
- Causes the pending state to be copied into the current state, which updates the cipher suite to be used on this connection.



(a) Change Cipher Spec Protocol

2. Alert Protocol

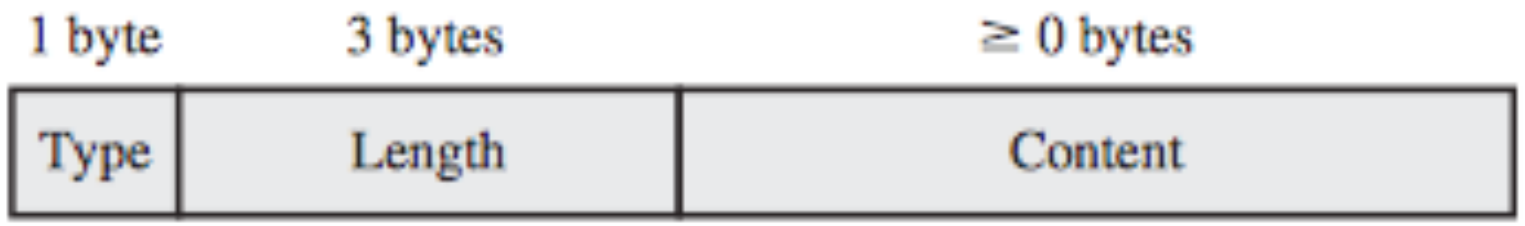
- Convey SSL alerts to the peer-entity
- 2 Bytes
- First Byte - Denotes level of the message
  - Warning
  - Fatal
- Alert code for specific alert



(b) Alert Protocol

3. Handshake Protocol

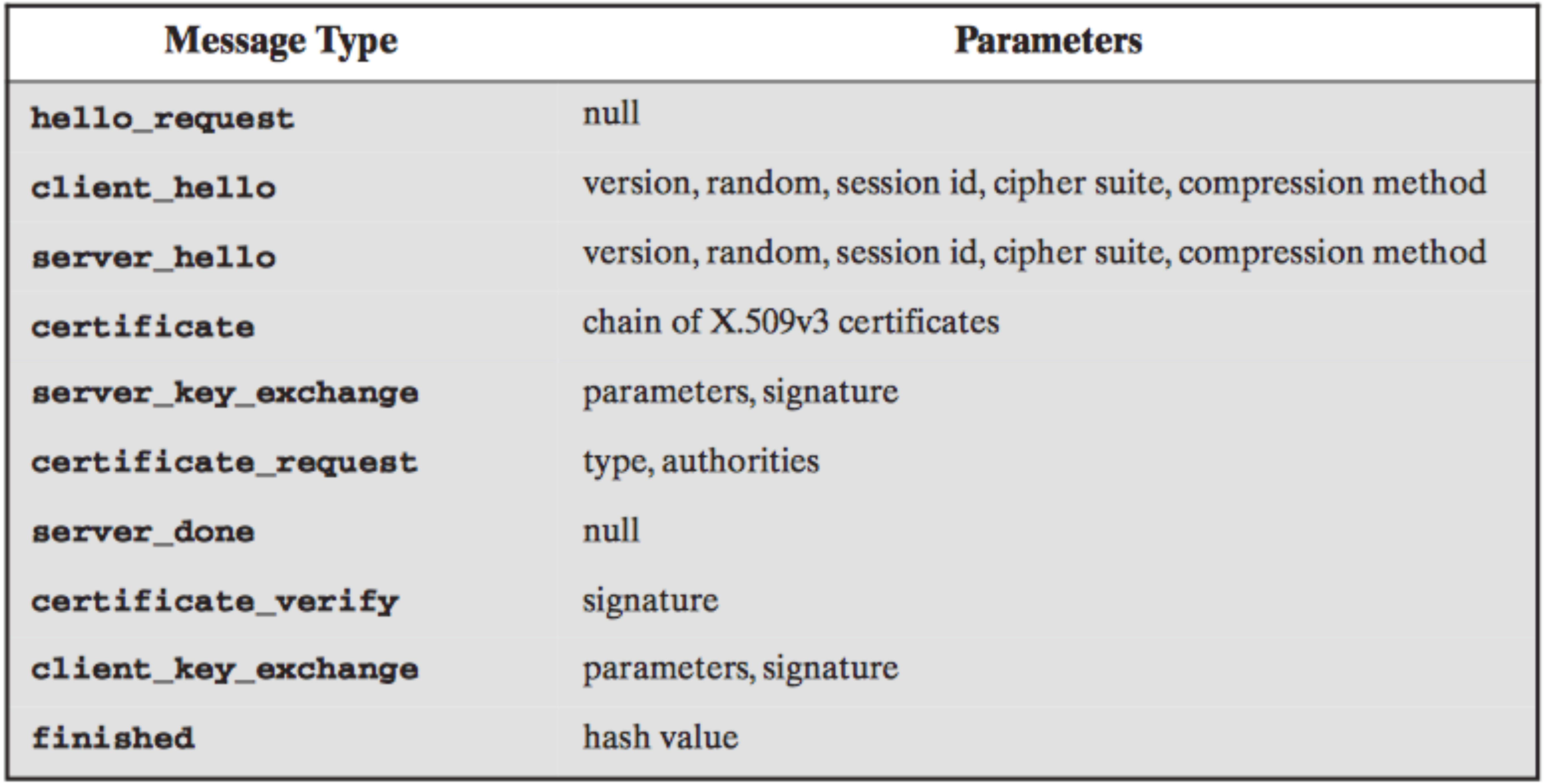
- Size: Minimum 4 Bytes
- *Type* (1B) indicates one of 10 SSL Handshake Protocol Message Types
- *Length* (3B) indicates length of message in Bytes
- *Content* (>=0B) indicates the parameters associated with the messages



1 byte	3 bytes	≥ 0 bytes
Type	Length	Content

(c) Handshake Protocol

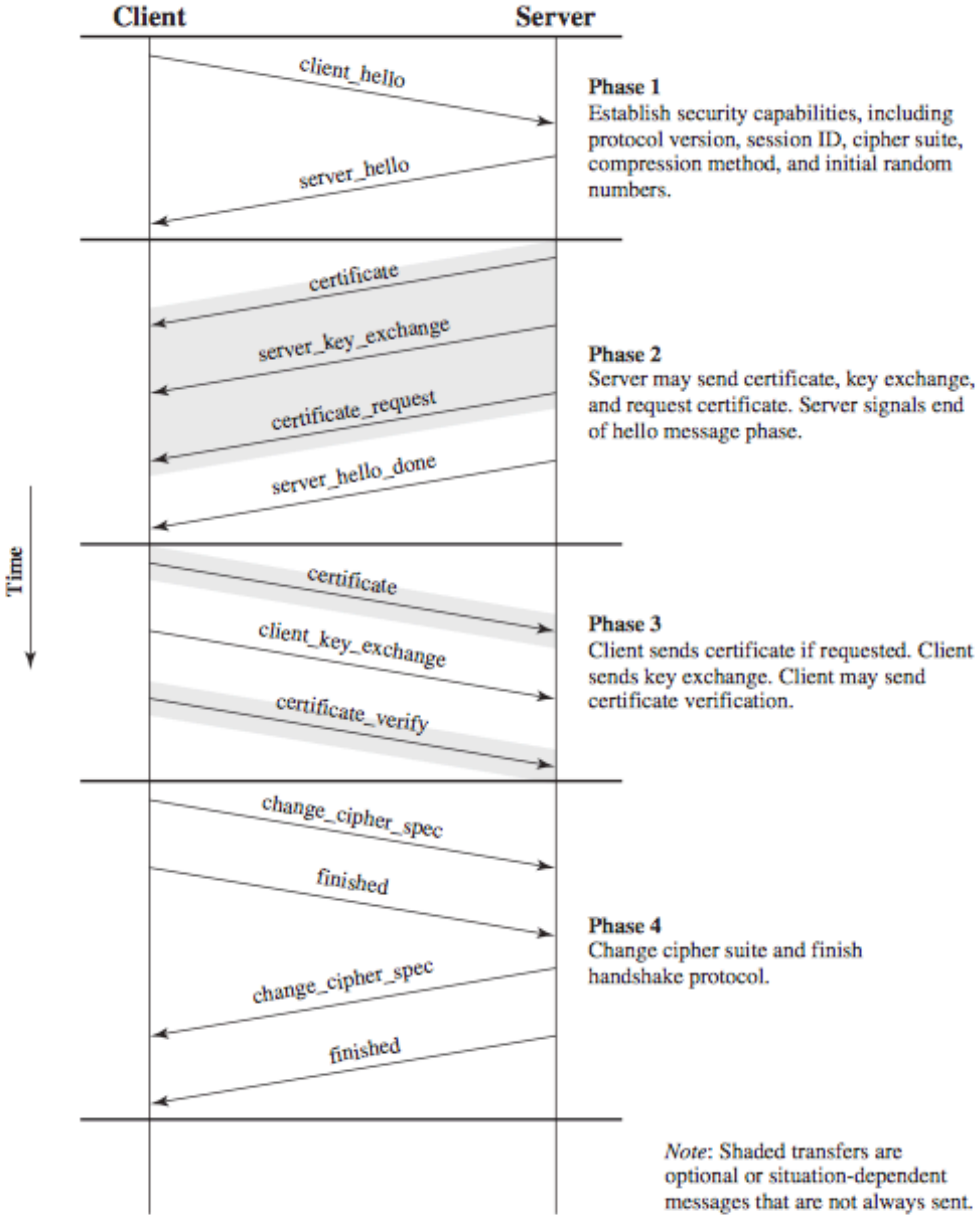
Table 16.2 SSL Handshake Protocol Message Types



Message Type	Parameters
`hello_request`	null
`client_hello`	version, random, session id, cipher suite, compression method
`server_hello`	version, random, session id, cipher suite, compression method
`certificate`	chain of X.509v3 certificates
`server_key_exchange`	parameters, signature
`certificate_request`	type, authorities
`server_done`	null
`certificate_verify`	signature
`client_key_exchange`	parameters, signature
`finished`	hash value

4 Phases of SSL Handshake

1. Establish Security Capabilities
2. Server Authentication and Key Exchange
3. Client Authentication and Key Exchange
4. Finish



Phase 1
Establish security capabilities, including protocol version, session ID, cipher suite, compression method, and initial random numbers.

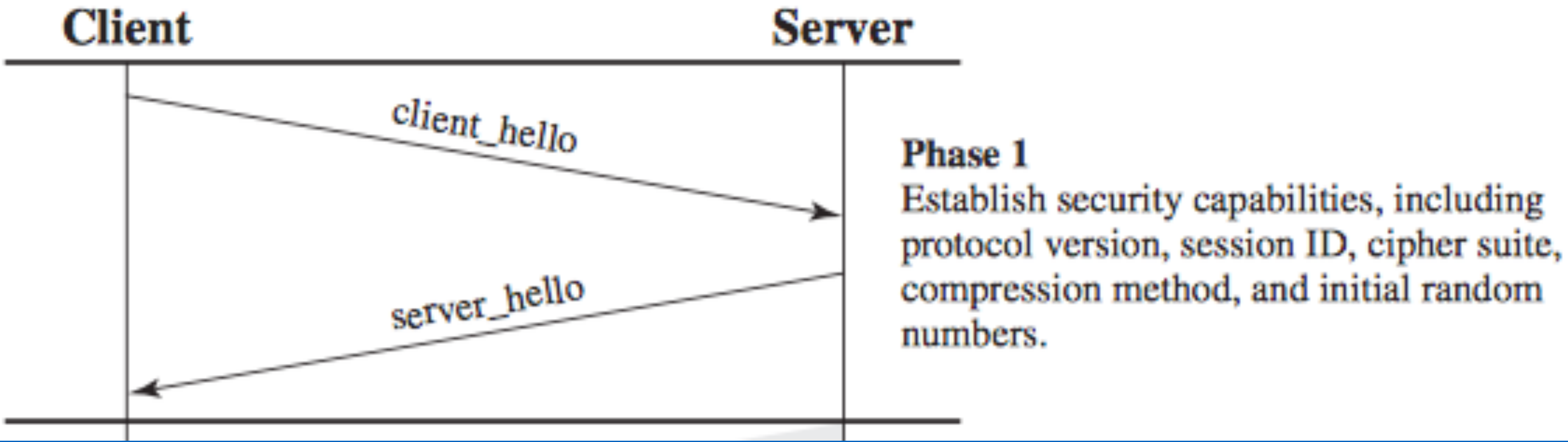
Phase 2
Server may send certificate, key exchange, and request certificate. Server signals end of hello message phase.

Phase 3
Client sends certificate if requested. Client sends key exchange. Client may send certificate verification.

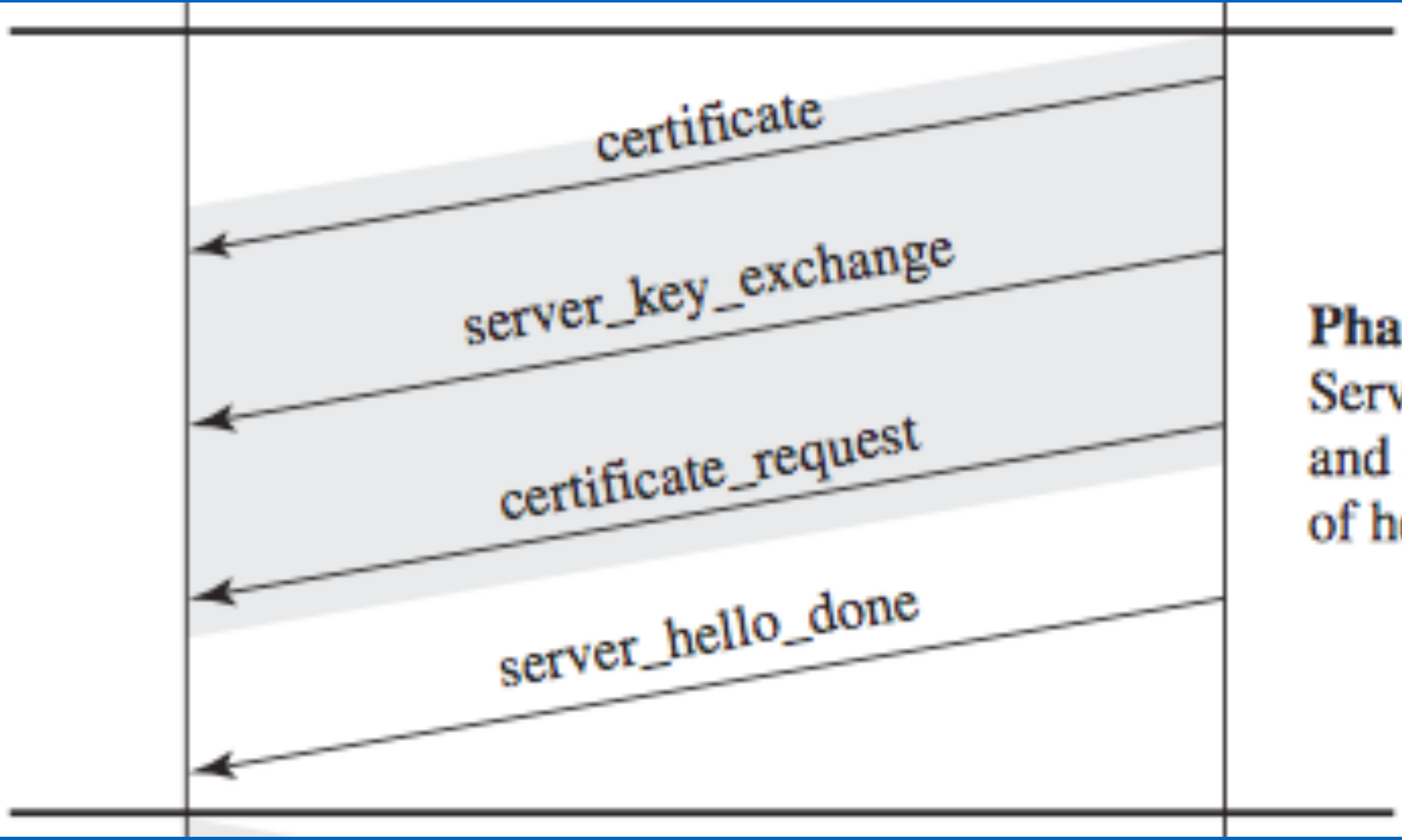
Phase 4
Change cipher suite and finish handshake protocol.

Note: Shaded transfers are optional or situation-dependent messages that are not always sent.

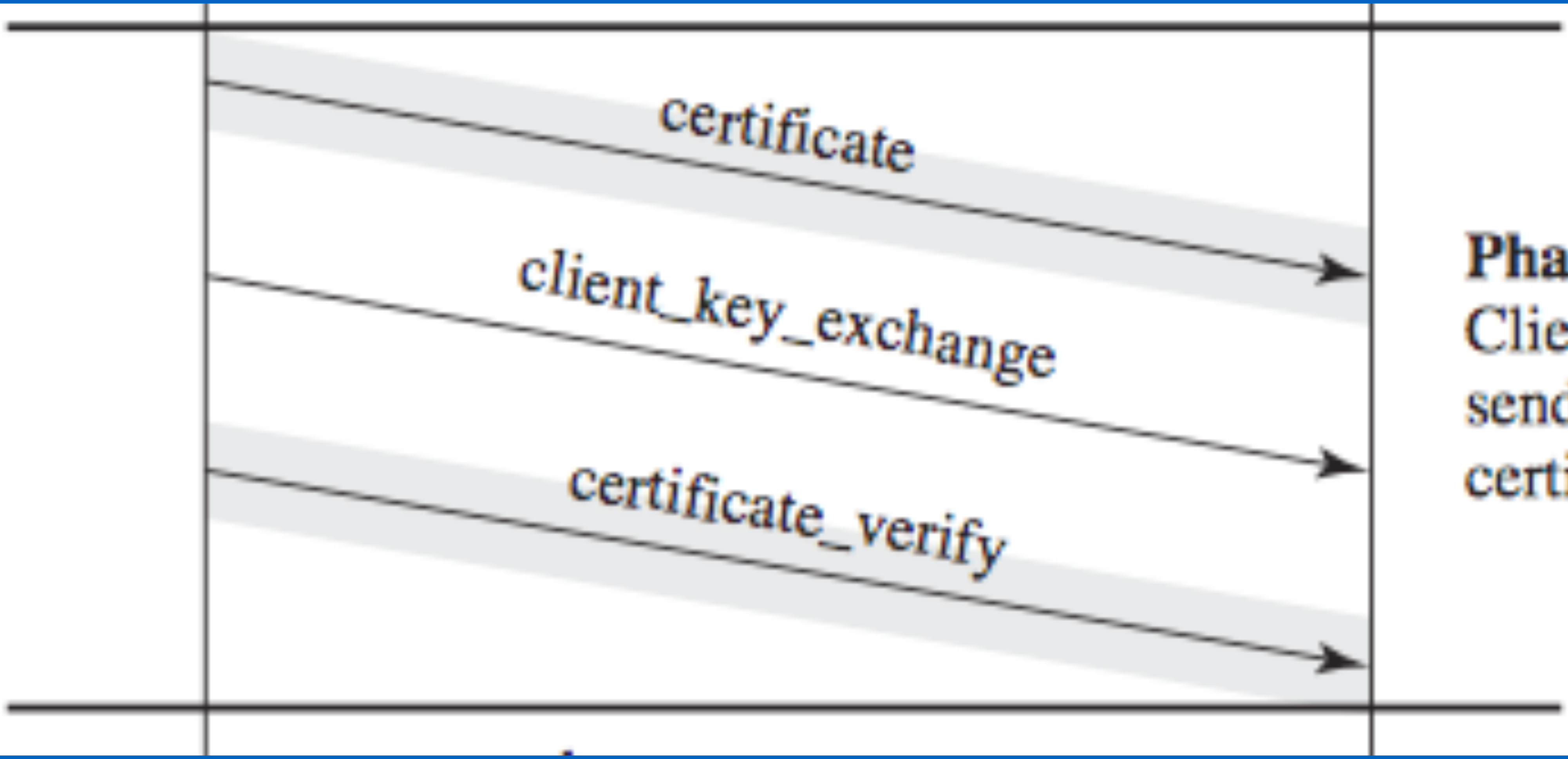
Figure 16.6 Handshake Protocol Action



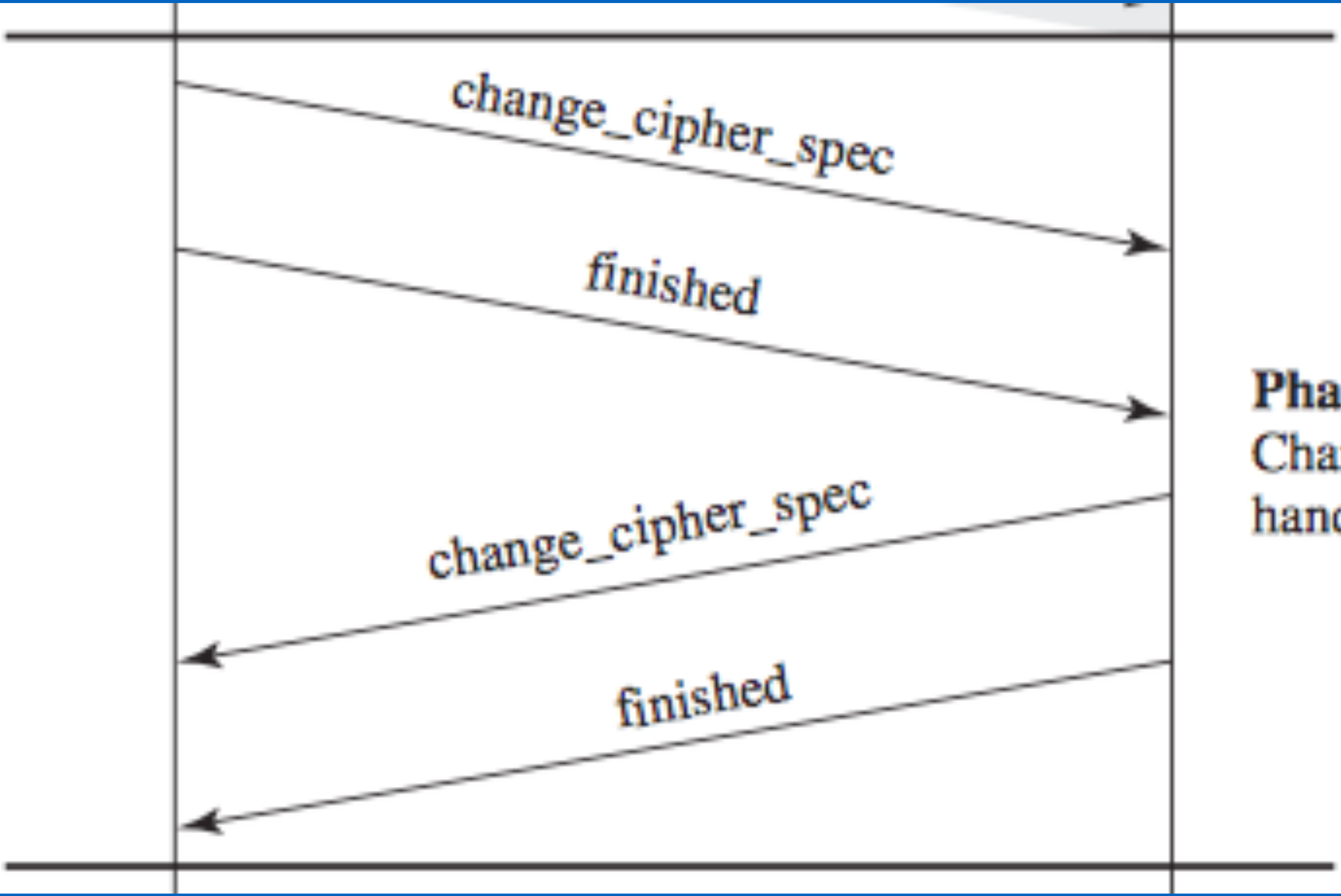
Phase 1
Establish security capabilities, including protocol version, session ID, cipher suite, compression method, and initial random numbers.



Phase 2
Server may send certificate, key exchange, and request certificate. Server signals end of hello message phase.



Phase 3
Client sends certificate if requested. Client sends key exchange. Client may send certificate verification.



Phase 4
Change cipher suite and finish handshake protocol.

Transport Layer Security (TLS)