

**HỌC VIỆN KỸ THUẬT MẬT MÃ
KHOA AN TOÀN THÔNG TIN**

GIAO THỨC AN TOÀN MẠNG

Bài 2.2. Một số giao thức xác thực

1

Giao thức PAP, CHAP

2

Giao thức Kerberos

3

Giao thức EAP,
802.1X và RADIUS

Mục tiêu bài học

□ Kiến thức

- Hiểu được hoạt động của một số giao thức xác thực thường gặp
- Hiểu được cơ chế xác thực qua bên thứ ba tin cậy nói chung, SSO nói riêng
- Hiểu được ý nghĩa của tính năng khả mở rộng của giao thức xác thực

□ Kỹ năng

- Phân tích cơ chế xác thực của các giao thức
- Phân tích hoạt động của giao thức qua việc chặn thu lưu lượng mạng

Tài liệu tham khảo

1. Giáo trình "Giao thức an toàn mạng máy tính">// Chương 2 "**Các giao thức xác thực**"
2. "**Authentication and Identity Protocols**", <https://goo.gl/aWuGxb>
3. William Stalling, **Cryptography and Network Security Principles and Practice (5e)//Chapter 15.3**, Prentice Hall, 2011
4. Dirk van der Walt, **FreeRADIUS Beginner's Guide**, Pack Publishing, 2011

Thuật ngữ tiếng Anh

- **Supplicant** (hoặc **Peer**) Bên được xác thực
- **Authenticator**: Bên xác thực
- **Authentication Server** (AS): Máy chủ xác thực
- **Network Access Server** (NAS): Máy chủ truy cập

Thuật ngữ tiếng Anh

- **Supplicant** (hoặc **Peer**) Bên được xác thực
- **Authenticator**: Bên xác thực
- **Authentication Server** (AS): Máy chủ xác thực
- **Network Access Server** (NAS): Máy chủ truy cập

Authentication Server: Máy chủ xác thực.

- Giúp Authenticator xác thực Supplicant
- Tức là cung cấp dịch vụ xác thực cho Authenticator

Thuật ngữ tiếng Anh

- **Supplicant** (hoặc **Peer**) Bên được xác thực
- **Authenticator**: Bên xác thực
- **Authentication Server** (AS): Máy chủ xác thực
- **Network Access Server** (NAS): Máy chủ truy cập

Network Access Server : Máy chủ dịch vụ

- Là một authenticator
- Cung cấp dịch vụ cho supplicant

1

Giao thức PAP, CHAP

2

Giao thức Kerberos

3

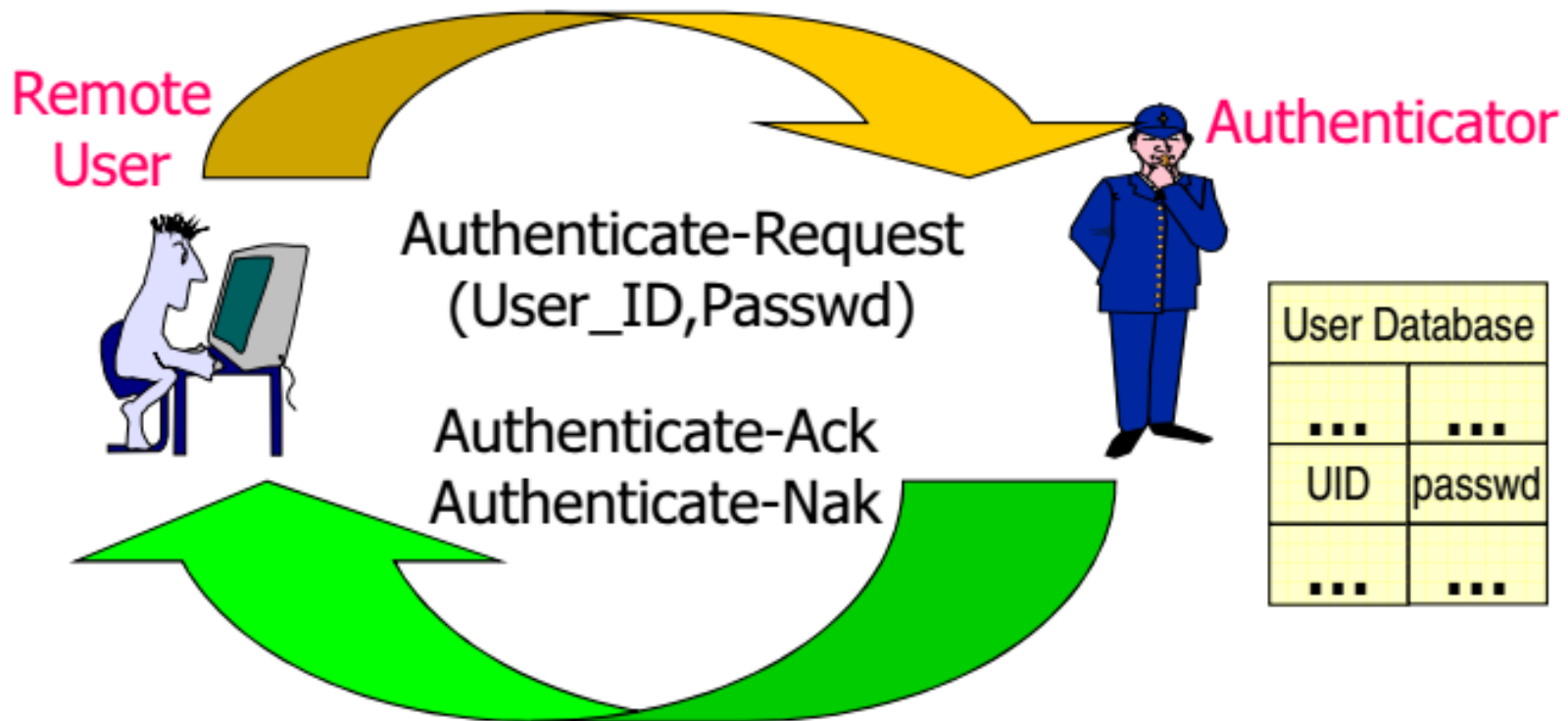
Giao thức EAP,
802.1X và RADIUS

PAP và CHAP

- ❑ PAP và CHAP là 2 giao thức xác thực được sử dụng trong giao thức PPP
- ❑ PAP (0xC023) và CHAP (0xC223) đều sử dụng mật khẩu để xác thực
 - PAP (RFC 1334, Password Authentication Protocol) truyền mật khẩu dạng rõ
 - CHAP (RFC 1994, Challenge Handshake Authentication Protocol) sử dụng cơ chế thách đố, giải đố

Giao thức PAP

- Password Authentication Protocol
- Là giao thức bắt tay 2 bước (2-way)
- Xác thực bằng mật khẩu



Giao thức PAP

Initiator

Responder

(LCP Link Establishment)

(LCP Link Establishment)

Initiate Authentication

Authenticate-Request

Validate Name and
Password In Request

If Successful,
Authenticated. Otherwise,
Try To Authenticate Again

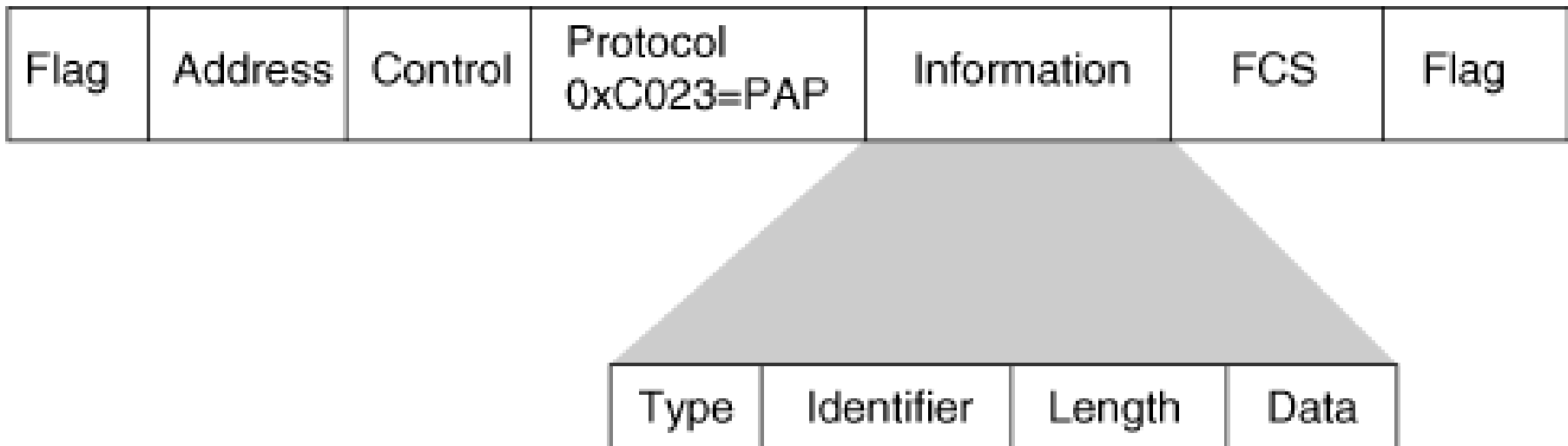
Authenticate-Ack
or
Authenticate-Nak

(NCP Link Establishment,
Normal Operation)

(NCP Link Establishment,
Normal Operation)



Three PPP PAP Frame Types



Type code: 1) Authentication Request
2) Authenticate-Ack
3) Authenticate-Nak

Identifier: One Octet and Aids in Matching Requests and Replies

Length: Two Octets and Indicates Length of PAP Packet, Including Code, Identifier, Length, and Data Fields

Data: 0 or More Octets

PPP PAP Authentication Request

Code = 1	Identifier	Length	Data
Peer-ID Length	Peer-ID	Password-Length	Password

Giao thức PAP: 2 bước xác thực

Chương 2. PAP.cap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools

pap

No.	Source	Destination	Protocol	Length	Info
17	20.0.0.2	20.0.0.1	PPP PAP	68	Authenticate-Request (Pe
18	20.0.0.1	20.0.0.2	PPP PAP	60	Authenticate-Ack (Messag

PPP PAP Authentication Request

No.	Source	Destination	Protocol	Length	Info
17	20.0.0.2	20.0.0.1	PPP PAP	68	Authenticate-Request (Peer-ID='i
18	20.0.0.1	20.0.0.2	PPP PAP	60	Authenticate-Ack (Message='')

```
> Internet Protocol Version 4, Src: 20.0.0.2, Dst: 20.0.0.1
> Generic Routing Encapsulation (PPP)
> Point-to-Point Protocol
▼ PPP Password Authentication Protocol
```

Code: Authenticate-Request (1)

Identifier: 0

Length: 14

▼ Data

Peer-ID-Length: 4

Peer-ID: ixia

Password-Length: 4

Password: ixia

0000	00 09 e9 55 c0 1c 00 14	00 00 02 00 08 00 45 00	...U....E.
0010	00 36 18 d3 00 00 40 2f	39 c4 14 00 00 02 14 00	.6....@/ 9.....
0020	00 01 30 81 00 01 00 12	00 18 00 00 00 03 00 00	..0.....
0030	00 02 ff 03 c0 23 01 00	00 0e 04 69 78 69 61 04#..ixia.
0040	69 78 69 61		ixia

Giao thức PAP: Auth Ack

No.	Source	Destination	Protocol	Length	Info
17	20.0.0.2	20.0.0.1	PPP PAP	68	Authenticate-Request (Peer-ID=)
18	20.0.0.1	20.0.0.2	PPP PAP	60	Authenticate-Ack (Message='')

```
> Frame 18: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
> Ethernet II, Src: Cisco_55:c0:1c (00:09:e9:55:c0:1c), Dst: MinervaK_00:00:00:00:00:00
> Internet Protocol Version 4, Src: 20.0.0.1, Dst: 20.0.0.2
> Generic Routing Encapsulation (PPP)
> Point-to-Point Protocol
▼ PPP Password Authentication Protocol
```

Code: Authenticate-Ack (2)

Identifier: 0

Length: 5

▼ Data

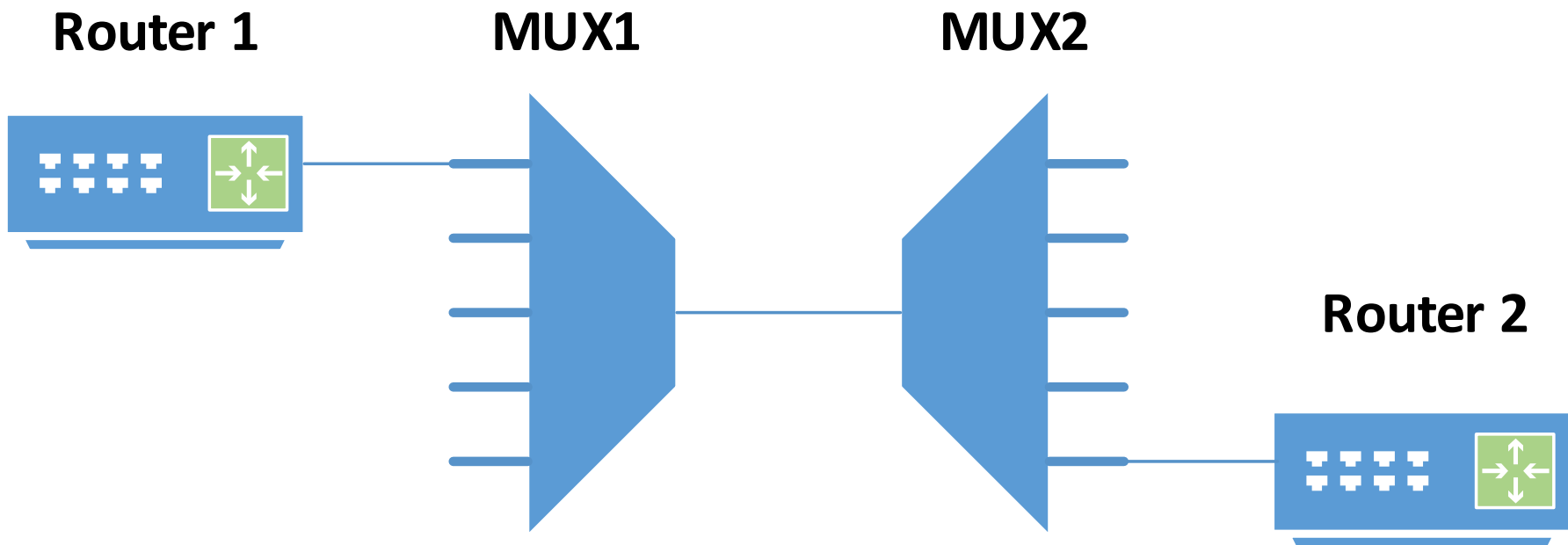
Message-Length: 0

Message:

0000	00 14 00 00 02 00 00 09 e9 55 c0 1c 08 00 45 00U....E.
0010	00 2d 1a dc 00 00 ff 2f 78 c3 14 00 00 01 14 00	.-...../ x.....
0020	00 02 30 81 88 0b 00 09 00 01 00 00 00 03 00 00	..0.....
0030	00 03 ff 03 c0 23 02 00 00 05 00 00#..

Giao thức PAP: Vấn đề an toàn

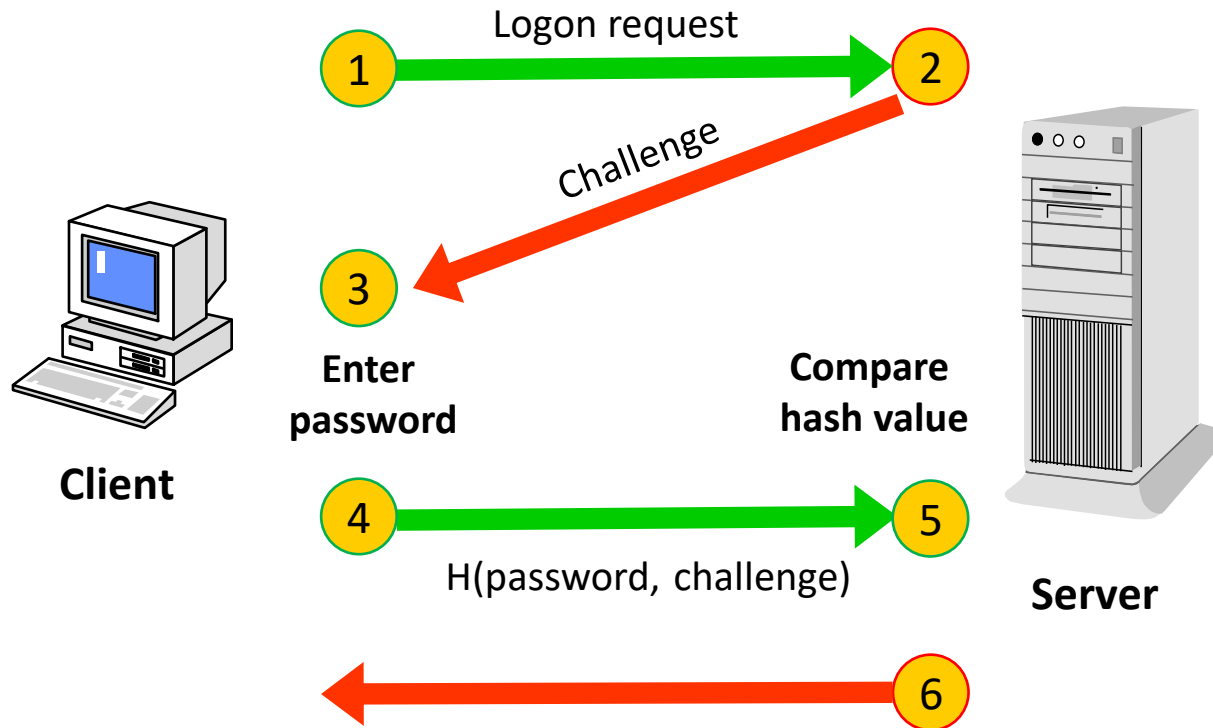
- Mật khẩu truyền ở dạng rõ
- Có thể bị chặn thu trên đường truyền



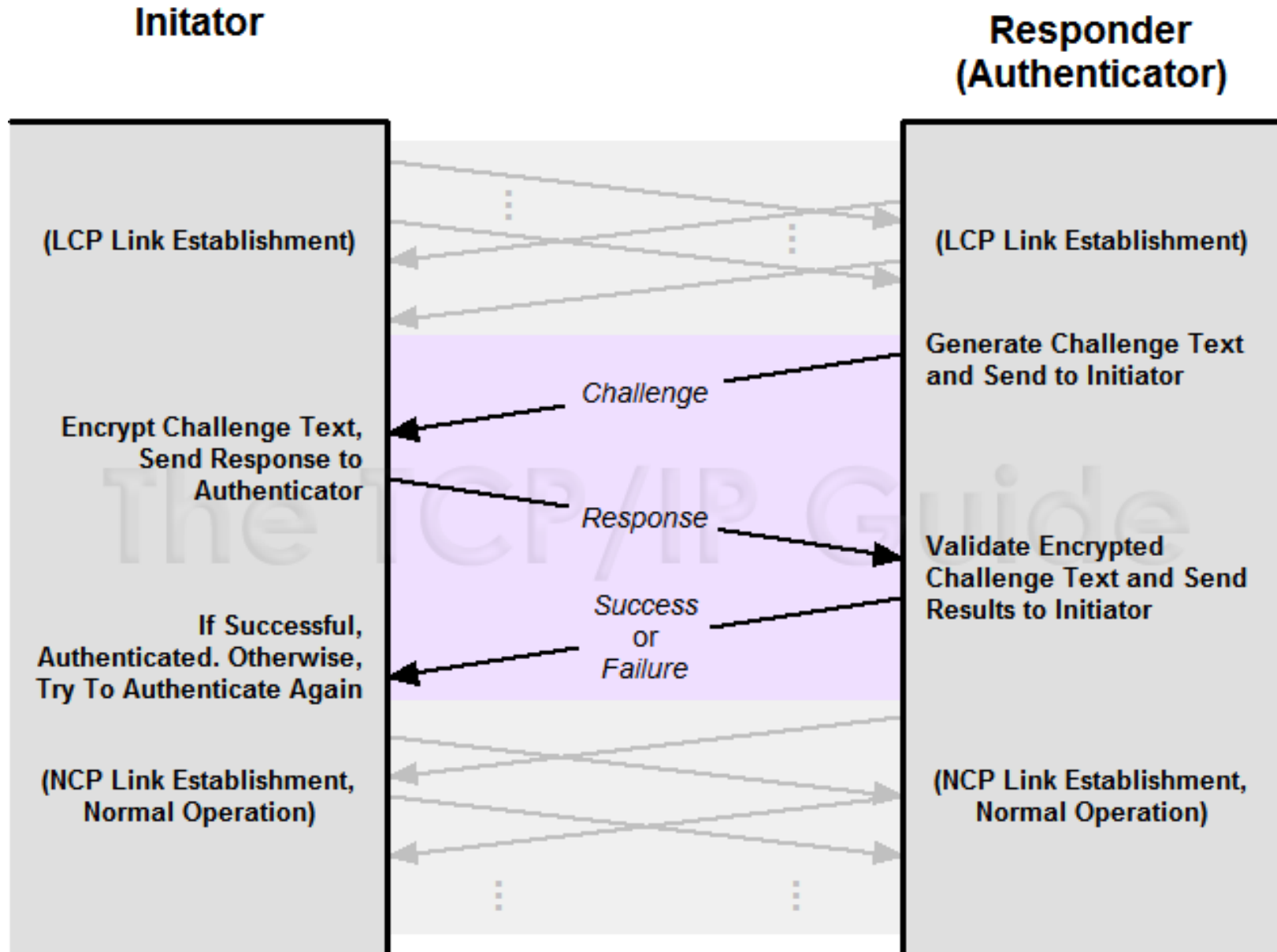
Giao thức CHAP

- CHAP = Challenge Handshake Authentication Protocol
- Là giao thức bắt tay 3 bước (3-way)
- Xác thực sử dụng mật khẩu
- Không truyền mật khẩu dạng rõ (nhưng vẫn lưu mật khẩu dạng rõ)

Giao thức CHAP



Giao thức CHAP



Giao thức CHAP: Xác thực 3 bước, 2 chiều

Chương 2. CHAP.cap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools

chap

No.	Source	Destination	Protocol	Length	Info
6	N/A	N/A	PPP CHAP	27	Challenge (NAME='R1', VA
7	N/A	N/A	PPP CHAP	27	Challenge (NAME='R0', VA
8	N/A	N/A	PPP CHAP	27	Response (NAME='R0', VAL
9	N/A	N/A	PPP CHAP	27	Response (NAME='R1', VAL
10	N/A	N/A	PPP CHAP	8	Success (MESSAGE='')
11	N/A	N/A	PPP CHAP	8	Success (MESSAGE='')

Giao thức CHAP: Challenge

No.	Source	Destination	Protocol	Length	Info
6	N/A	N/A	PPP CHAP	27	Challenge (NAME='R1', VALUE=)
7	N/A	N/A	PPP CHAP	27	Challenge (NAME='R0', VALUE=)
8	N/A	N/A	PPP CHAP	27	Response (NAME='R0', VALUE=0:

>	Point-to-Point Protocol
▼	PPP Challenge Handshake Authentication Protocol
	Code: Challenge (1)
	Identifier: 1
	Length: 23
▼	Data
	Value Size: 16
	Value: 41528c199fe22713cda522d45c7af9ad
	Name: R1

0000	ff 03 c2 23 01 01 00 17 10 41 52 9f e2 27 ...#.... .AR....'
0010	13 cd a5 22 d4 5c 7a f9 ad 52 31 ...".\z. .R1

Giải thích đại lượng này!

Giao thức CHAP: Response

No.	Source	Destination	Protocol	Length	Info
6	N/A	N/A	PPP CHAP	27	Challenge (NAME='R1', VALUE=0x)
7	N/A	N/A	PPP CHAP	27	Challenge (NAME='R0', VALUE=0x)
8	N/A	N/A	PPP CHAP	27	Response (NAME='R0', VALUE=0x)

> Point-to-Point Protocol
▼ PPP Challenge Handshake Authentication Protocol

Code: Response (2)

Identifier: 1

Length: 23

▼ Data

Value Size: 16

Value: dc73196880578b12670b8d231b8e69f9

Name: R0

0000	ff 03 c2 23 02 01 00 17 10 dc 73 70 57 8b	...#.... ..s.h.W.
0010	12 67 0b 8d 23 1b 8e 69 f9 52 30	.g..#...i .R0

Giải thích đại lượng này!

Giao thức CHAP: Success

No.	Source	Destination	Protocol	Length	Info
9	N/A	N/A	PPP CHAP	27	Response (NAME='R1',
10	N/A	N/A	PPP CHAP	8	Success (MESSAGE='')
11	N/A	N/A	PPP CHAP	8	Success (MESSAGE='')

> Frame 10: 8 bytes on wire (64 bits), 8 bytes captured (64 bits)

> Point-to-Point Protocol

▼ PPP Challenge Handshake Authentication Protocol

Code: Success (3)

Identifier: 1

Length: 4

0000 ff 03 c2 23 03 01 00 04

...#....

1

Giao thức PAP, CHAP

2

Giao thức Kerberos

3

Giao thức EAP,
802.1X và RADIUS

Thông tin chung về Kerberos

- ❑ Mục tiêu: xác thực hai chiều trong mô hình client-server
- ❑ Dựa trên giao thức Needham-Schroeder
- ❑ Sử dụng mật mã đối xứng; có bên thứ ba tin cậy là “Trung tâm phân phối khóa” (Key Distribution Center).
- ❑ Là giao thức Single Sign-On (SSO)
- ❑ Có nhiều phiên bản: 1, 2, 3 và 4, 5

Giao thức Needham-Schroeder

□ Điều kiện ban đầu:

- Alice và Bob cùng tin tưởng Sandy
- Alice và Sandy chia sẻ khóa K_{AS} ;
- Bob và Sandy chia sẻ K_{BS} ;

□ Yêu cầu:

- Alice và Bob thiết lập khóa chia sẻ K

Giao thức Needham-Schroeder

1. $A \rightarrow S$: Alice, Bob, N_A
2. $S \rightarrow A$: $\{N_A, K, \text{Bob}, \{K, \text{Alice}\}K_{BS}\}K_{AS}$
3. $A \rightarrow B$: Sandy, $\{K, \text{Alice}\}K_{BS}$
4. $B \rightarrow A$: $\{\text{"I'm Bob"}, N_B\}K$
5. $A \rightarrow B$: $\{\text{"I'm Alice"}, N_B - 1\}K$

Giao thức Needham-Schroeder

Tấn công: dùng lại khóa cũ

3'. $M("A") \rightarrow B$: Sandy, $\{K', \text{Alice}\}_{K_{BS}}$

4. $B \rightarrow M("A")$: $\{"I'm Bob", N_B\}_{K'}$

5. $M("A") \rightarrow B$: $\{"I'm Alice", N_B - 1\}_{K'}$

Bổ sung timestamp và timespan
để chống tấn công

Giao thức Needham-Schroeder

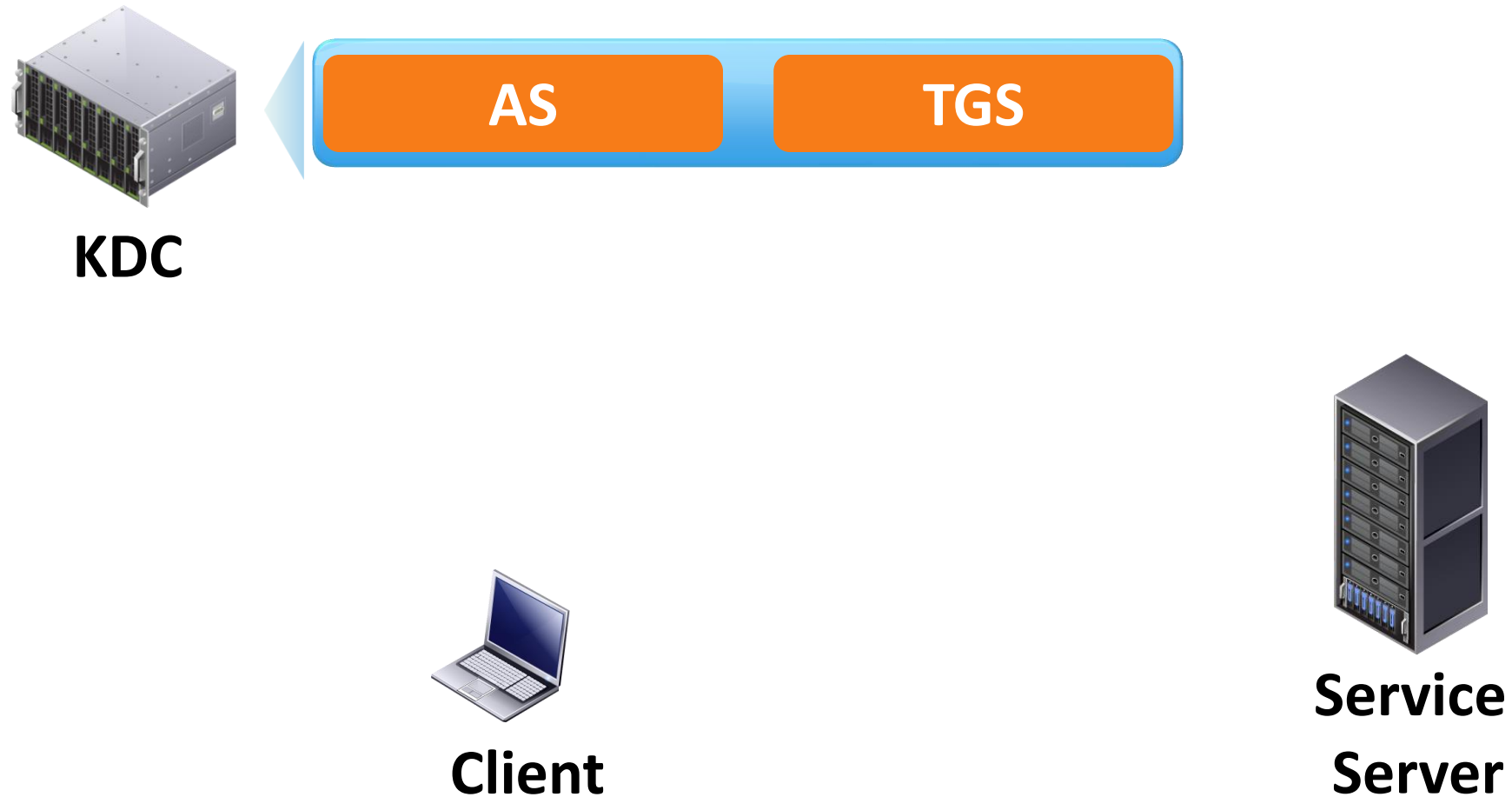
1. $A \rightarrow S$: Alice, Bob
2. $S \rightarrow A$: $\{T_S, L, K, \text{Bob},$
 $\{T_S, L, K, \text{Alice}\}K_{BS}\}K_{AS}$
3. $A \rightarrow B$: $\{T_S, L, K, \text{Alice}\}K_{BS}, \{Alice, T_A\}K$
4. $B \rightarrow A$: $\{T_A+1\}K$

Giao thức Kerberos

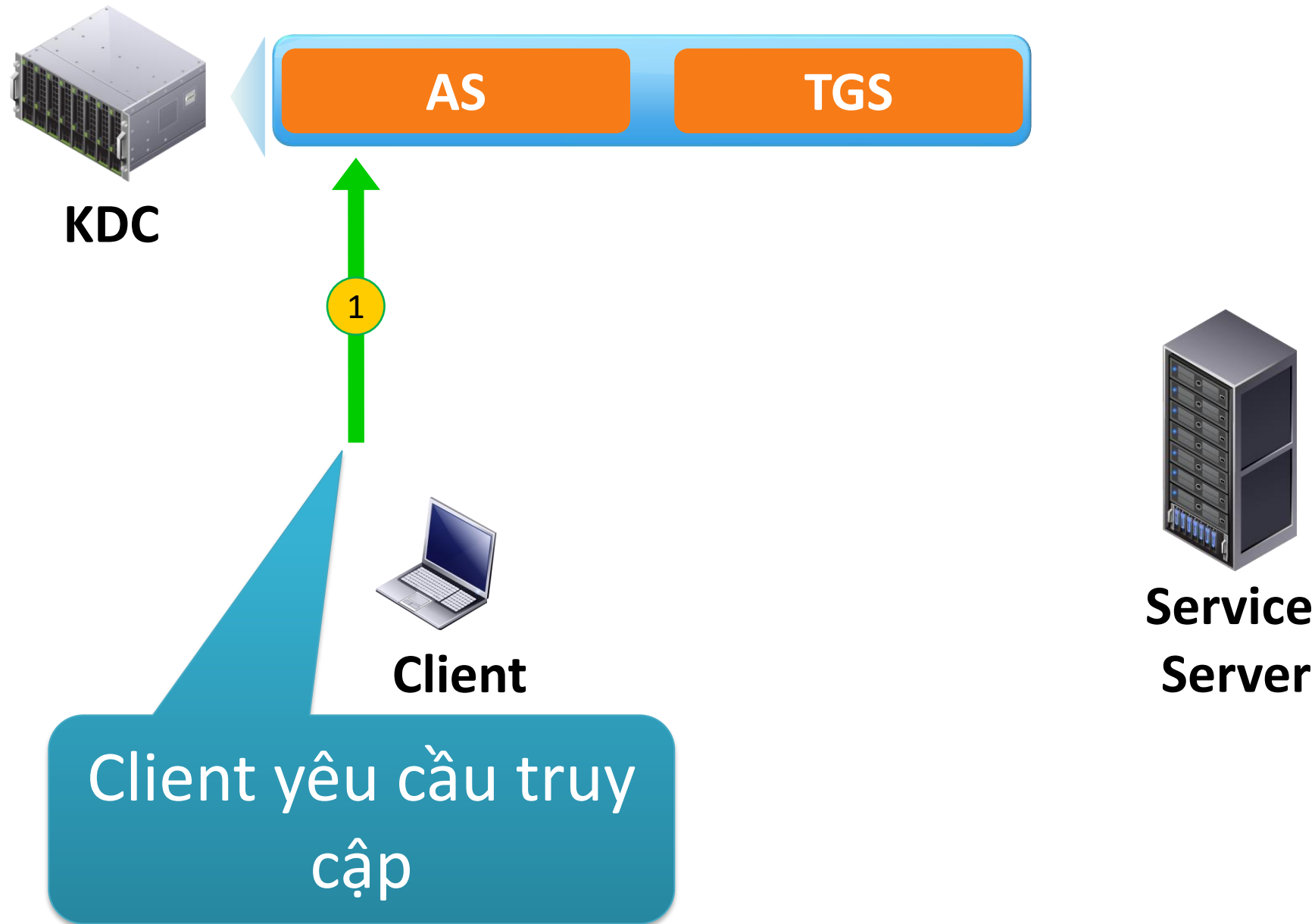
□ Từ viết tắt

- AS: Authentication Server
- TGS: Ticket Granting Server
- KDC (= AS+TGS): Key Distribution Center
- SS: Service Server
- TGT: Ticket Granting Ticket
- ST: Service Ticket

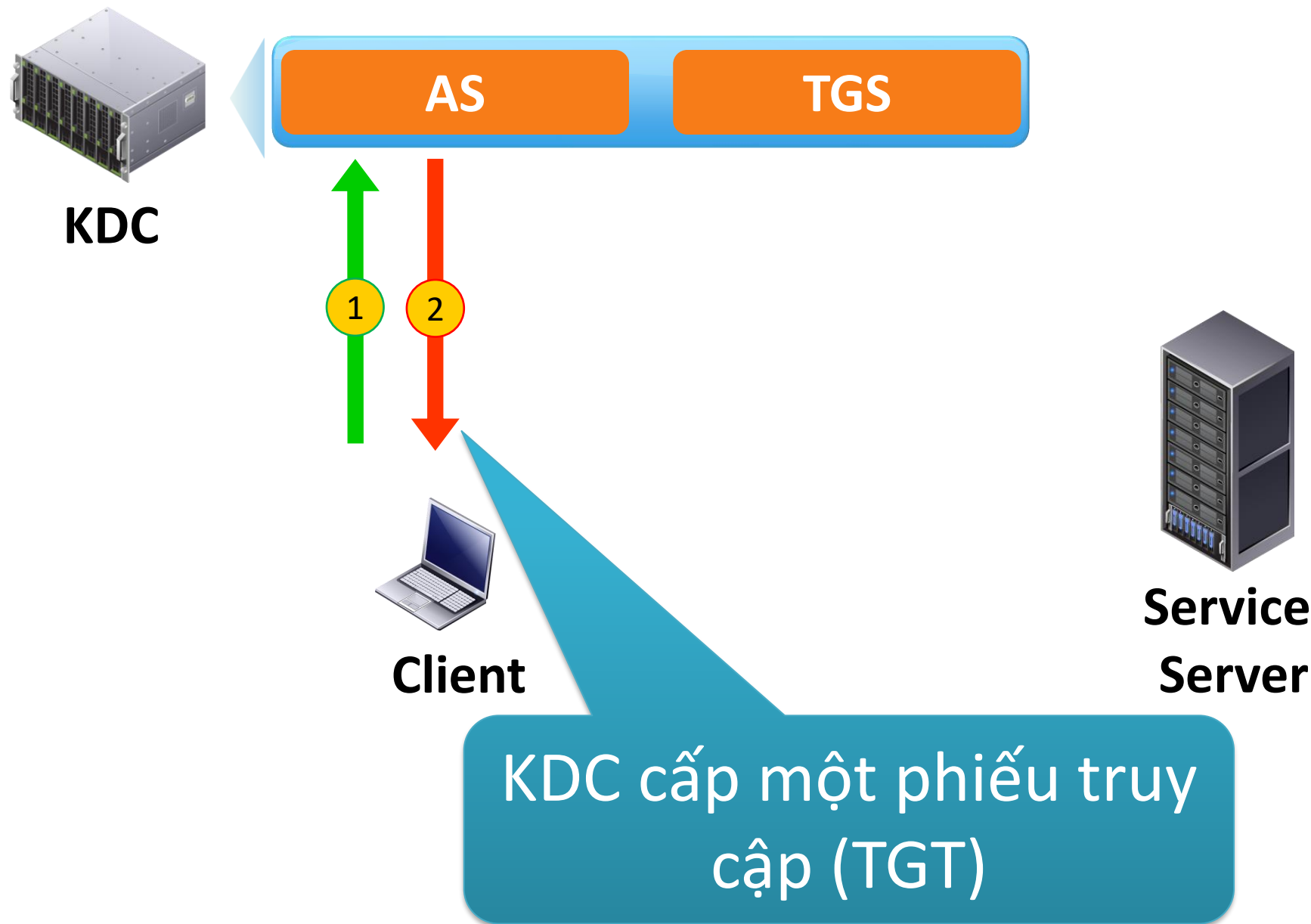
Giao thức Kerberos: Nguyên lý chung



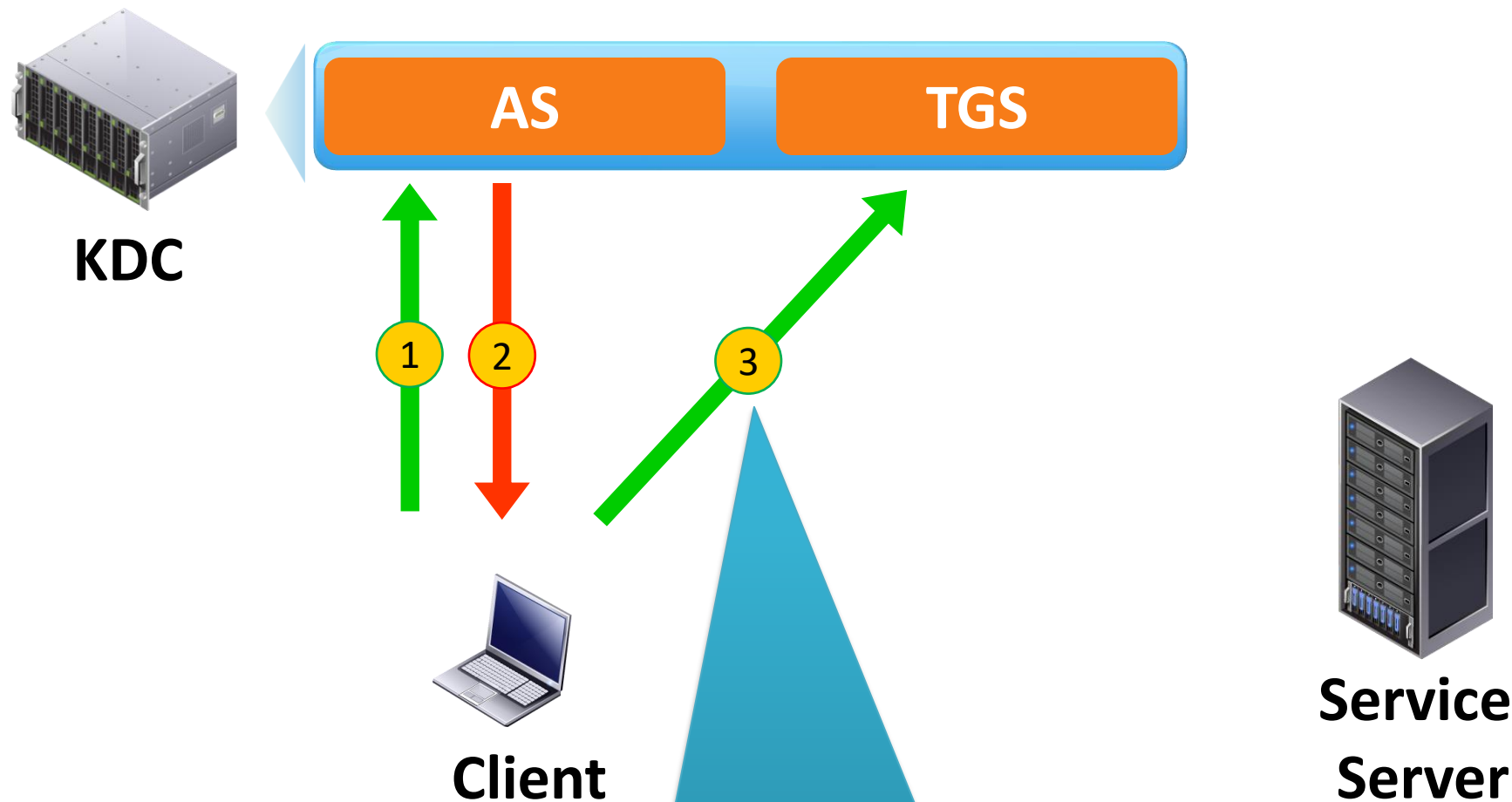
Giao thức Kerberos: Nguyên lý chung



Giao thức Kerberos: Nguyên lý chung

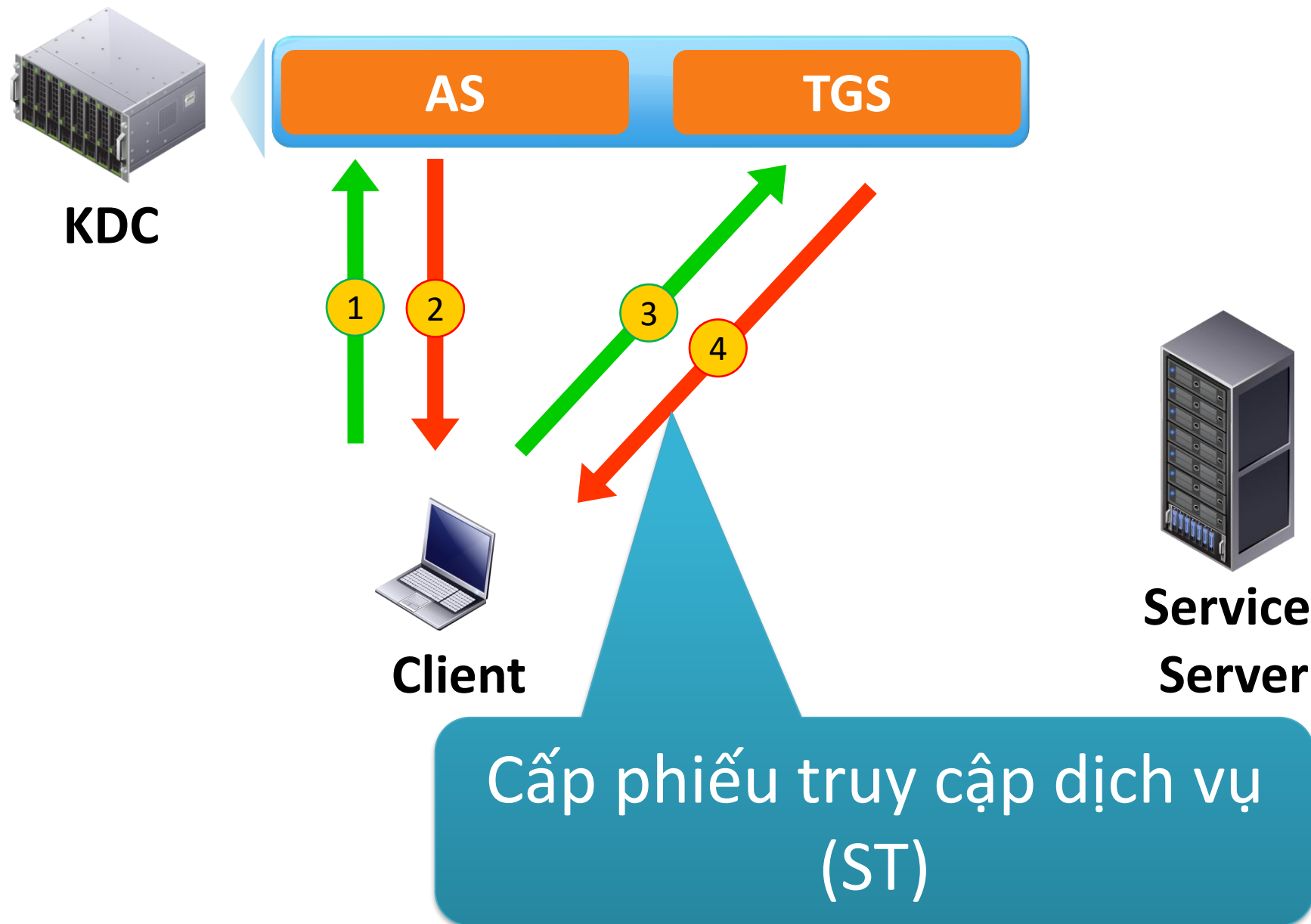


Giao thức Kerberos: Nguyên lý chung

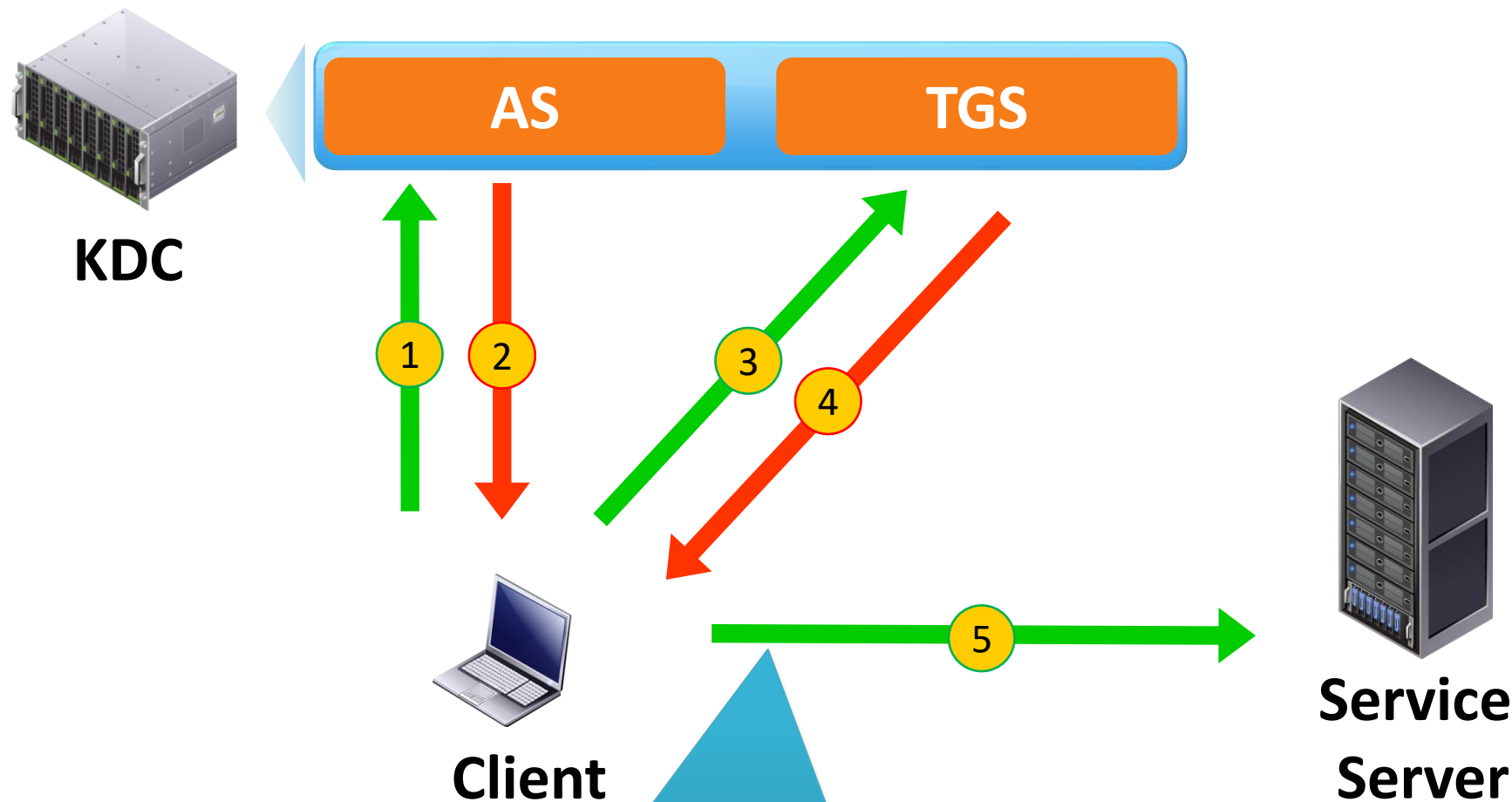


Sử dụng TGT để yêu cầu truy cập một dịch vụ cụ thể

Giao thức Kerberos: Nguyên lý chung

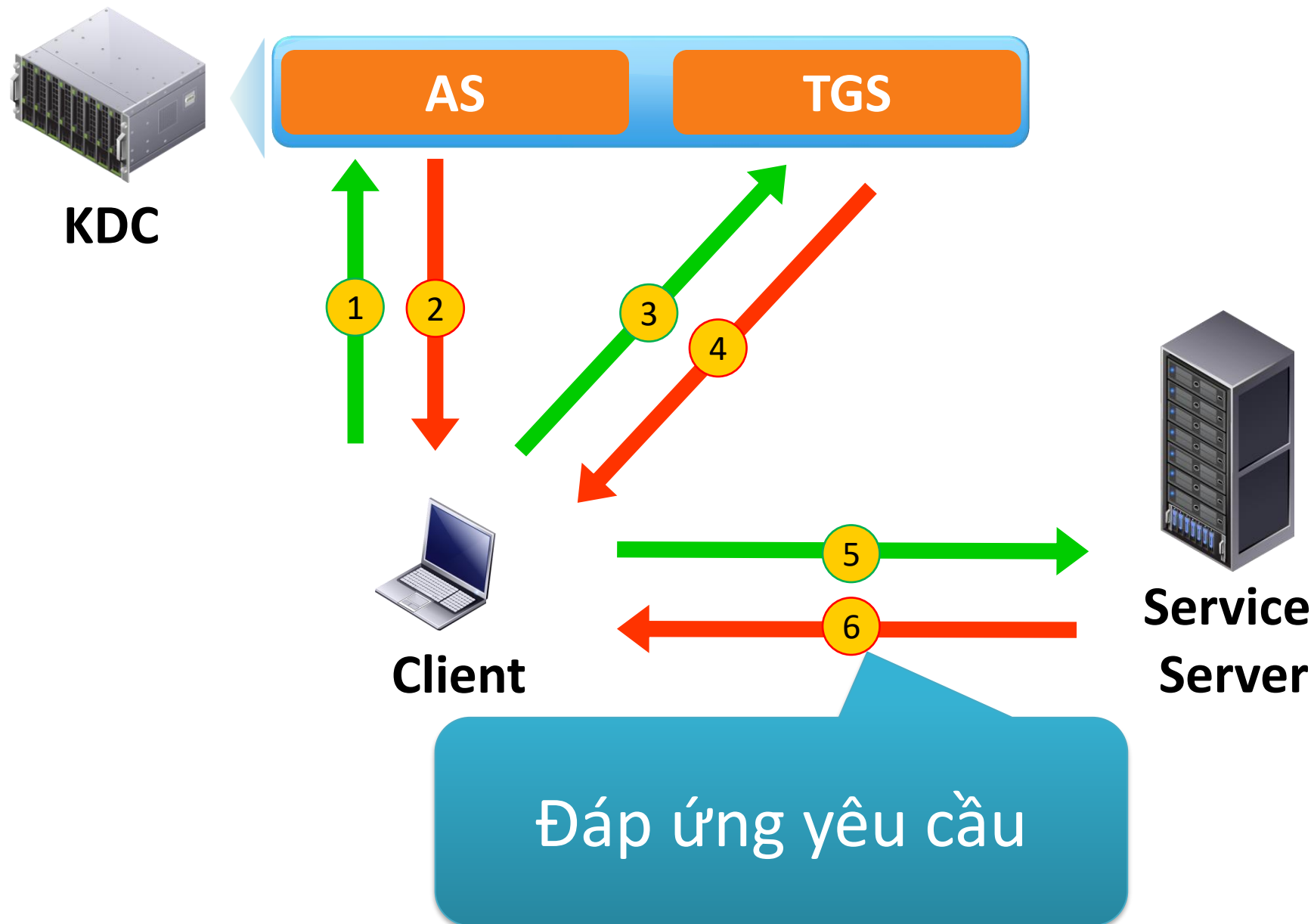


Giao thức Kerberos: Nguyên lý chung

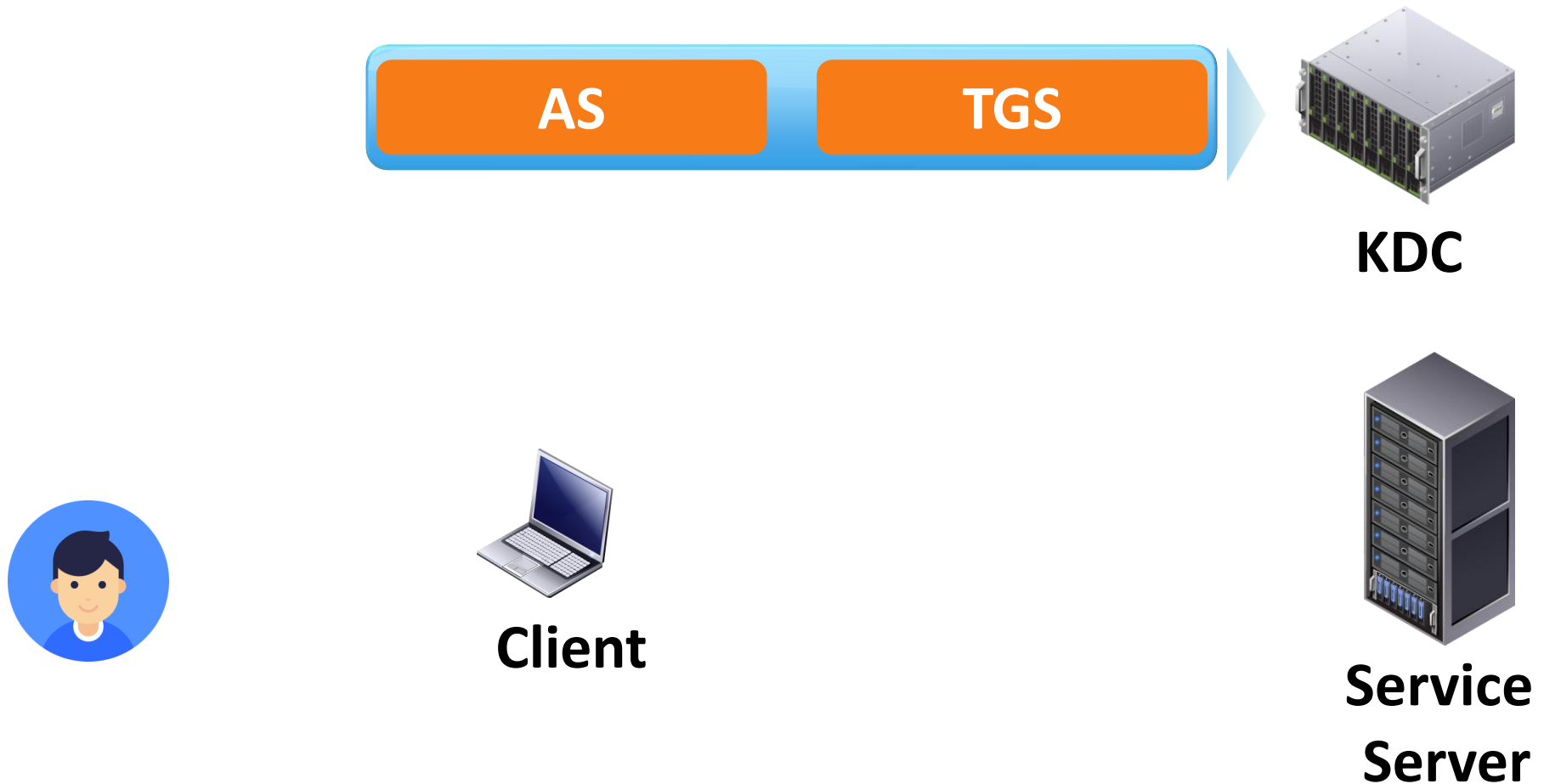


Sử dụng ST để yêu cầu phục vụ

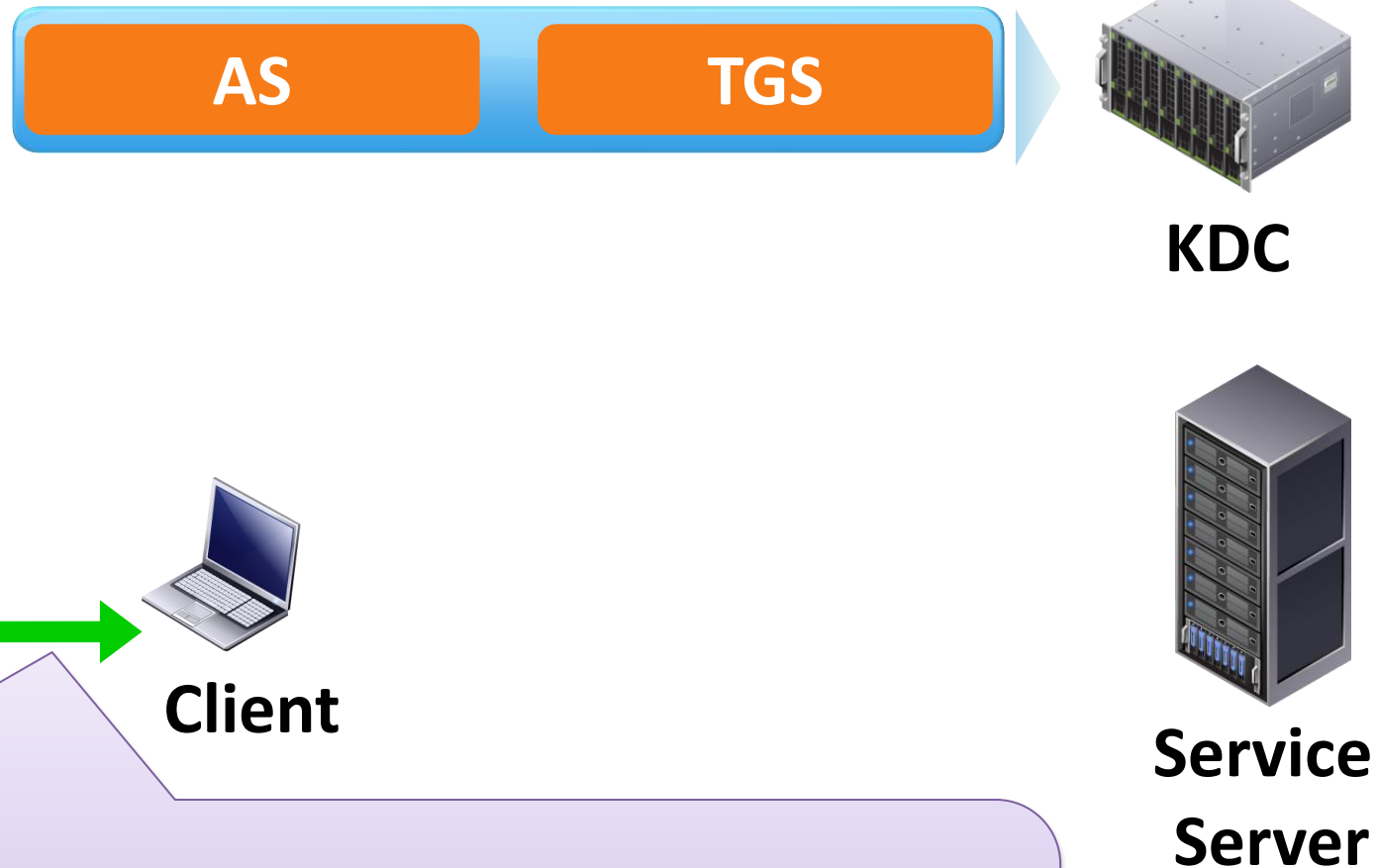
Giao thức Kerberos: Nguyên lý chung



Giao thức Kerberos: Các thông điệp



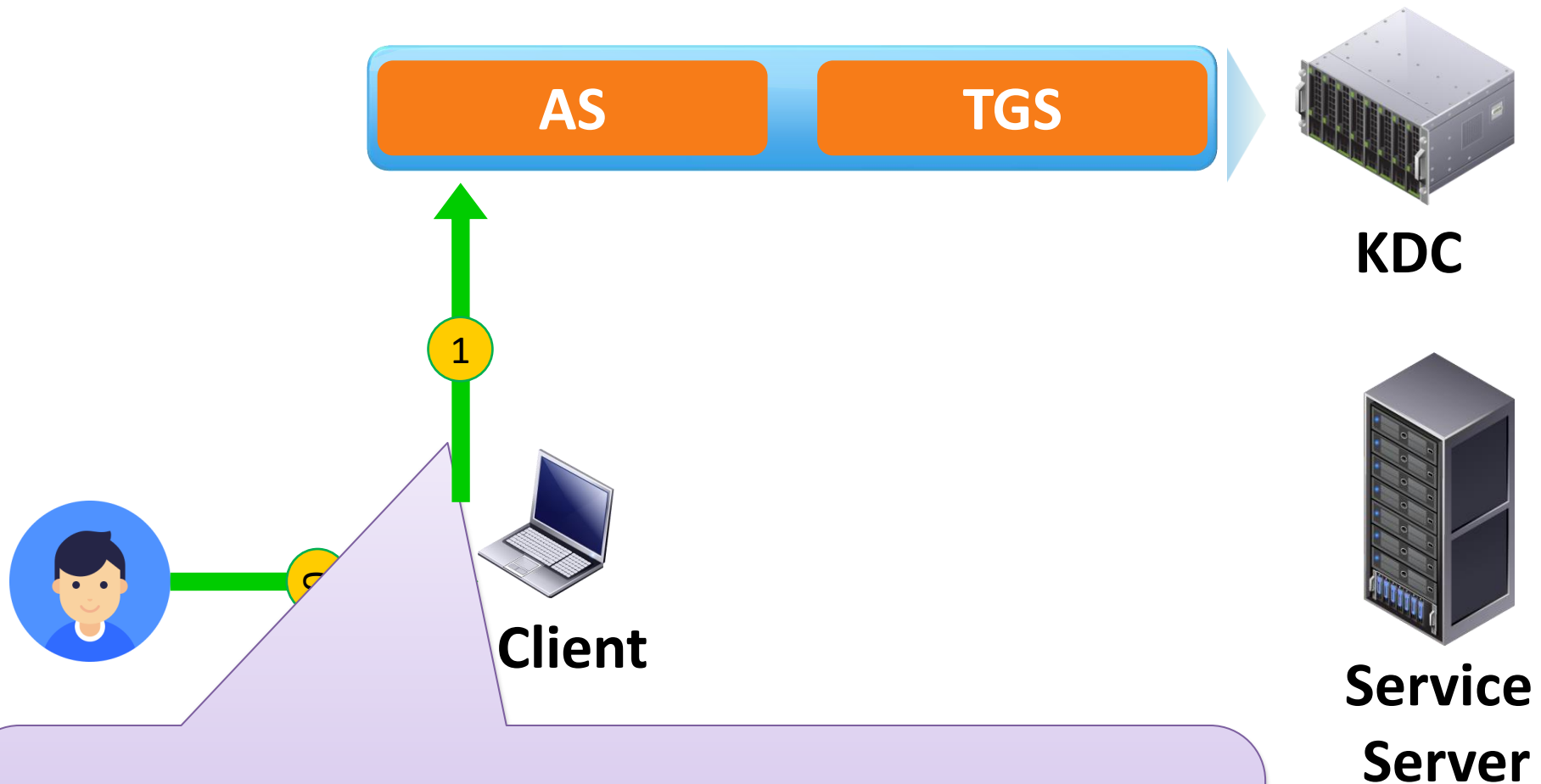
Giao thức Kerberos: Các thông điệp



User: Enter username, password

Client: $K_c = \text{PBKDF}(\text{password})$

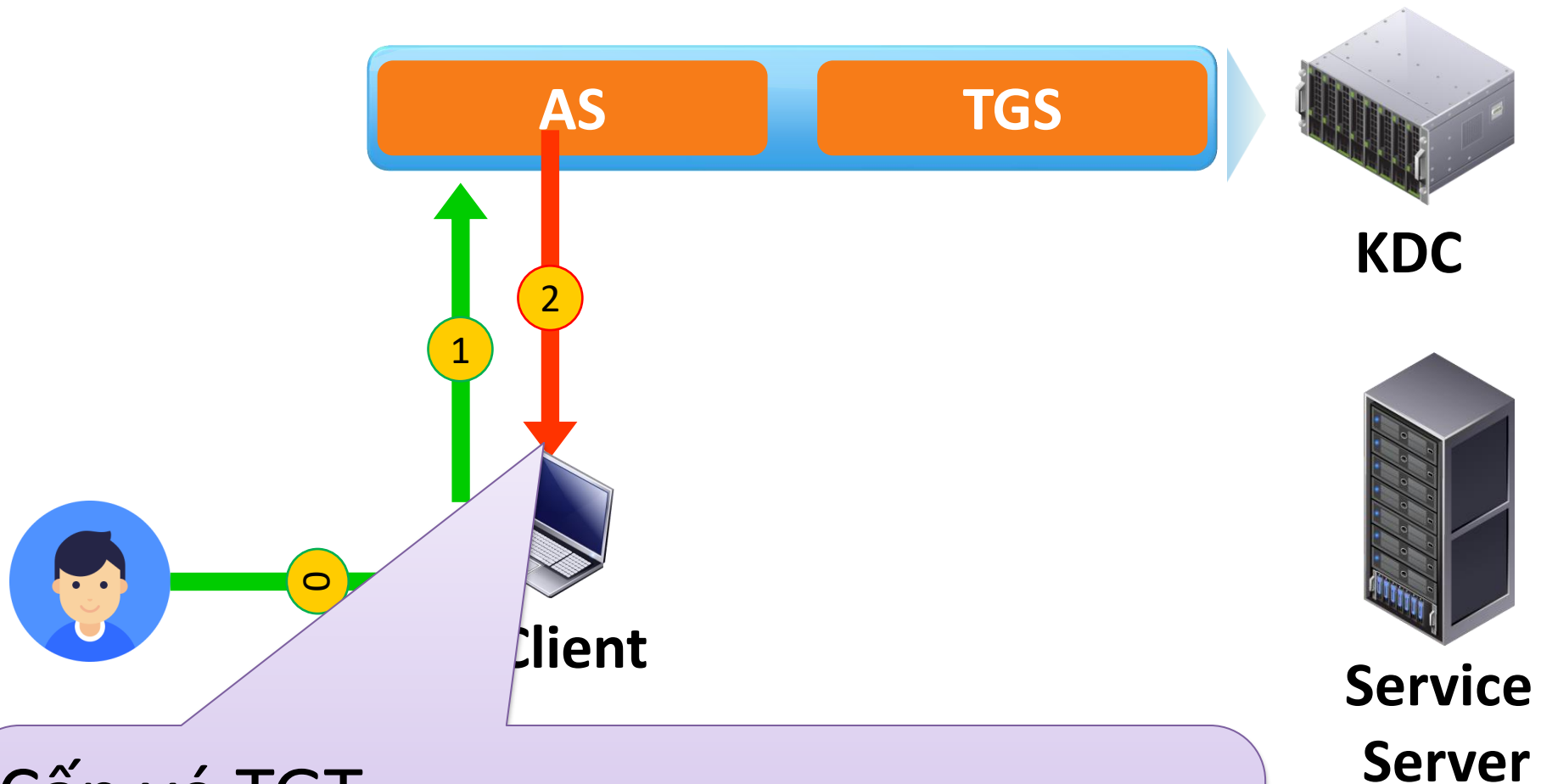
Giao thức Kerberos: Các thông điệp



Client yêu cầu truy cập

$C \rightarrow AS: ID_C, ID_{TGS}$

Giao thức Kerberos: Các thông điệp

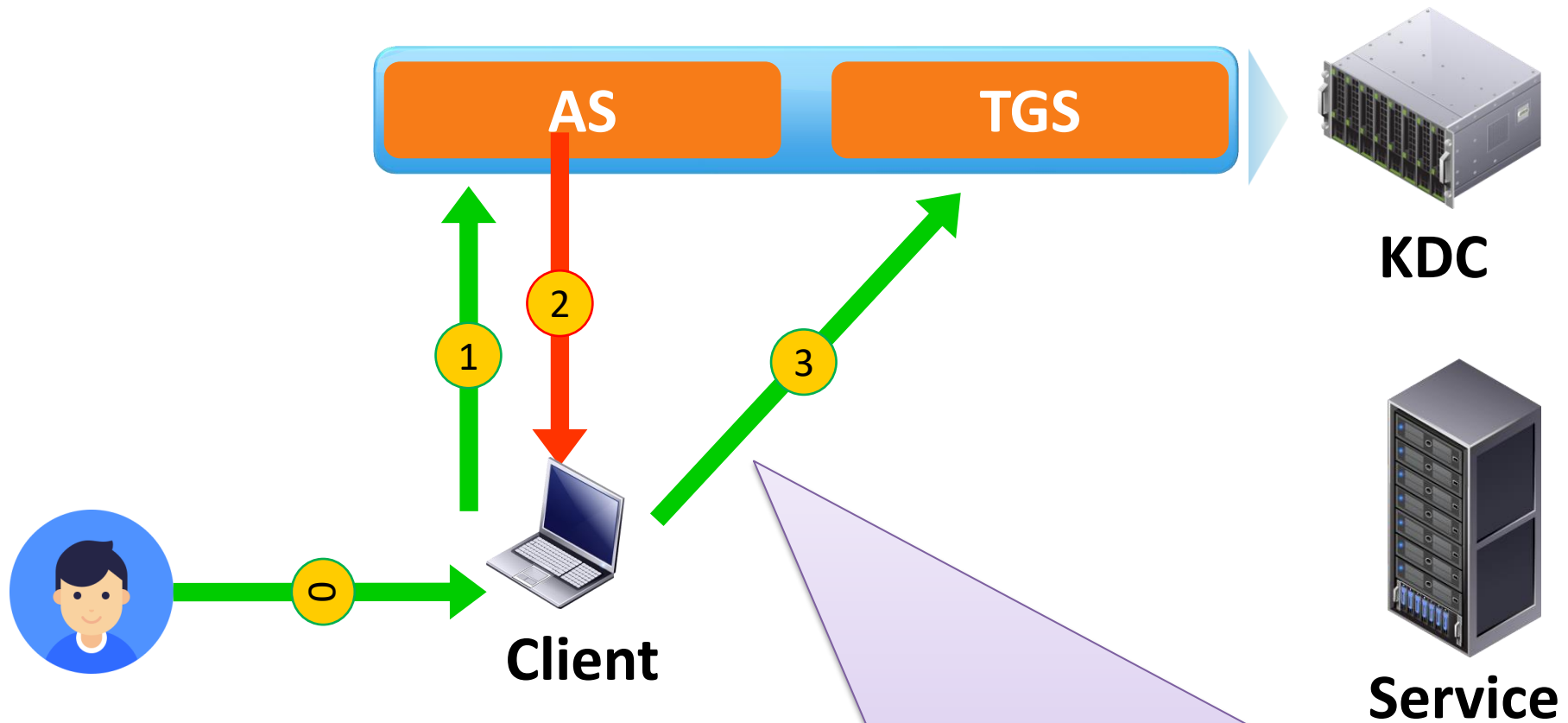


Cấp vé TGT

$AS \rightarrow C: \{\{\text{TGT}\}K_{AS_TGS}, K_{C_TGS}\}K_C$

$TGT = \{ID_C, ID_{TGS}, t_1, p_1, K_{C_TGS}\}$

Giao thức Kerberos: Các thông điệp

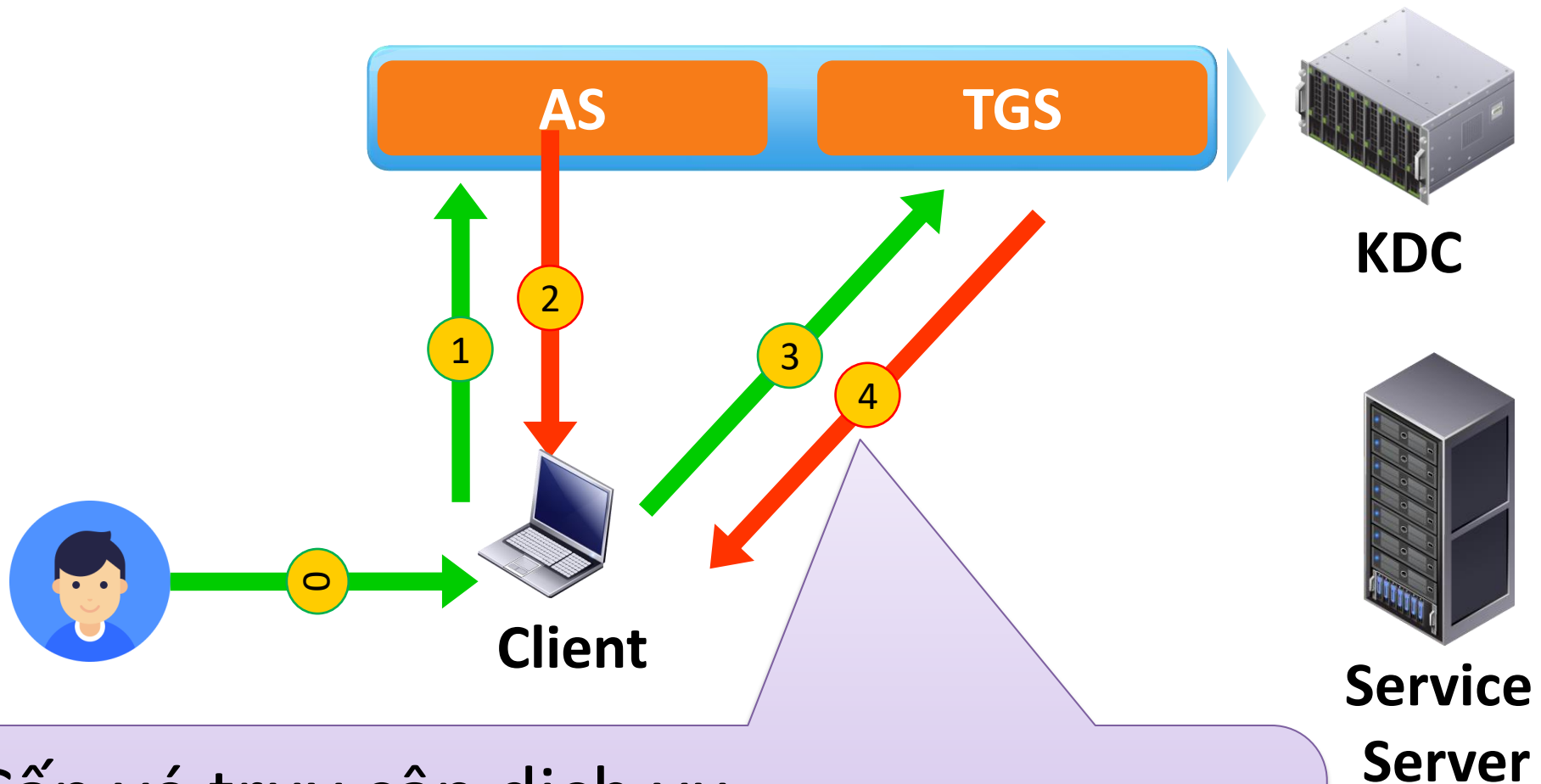


Yêu cầu một dịch vụ cụ thể

$C \rightarrow TGS: \{TGT\}K_{AS_TGS}, \{Aut_1: ID_C, t_2\}K_{C_TGS}, ID_{SS}$

$TGT = \{ID_C, ID_{TGS}, t_1, p_1, K_{C_TGS}\}$

Giao thức Kerberos: Các thông điệp

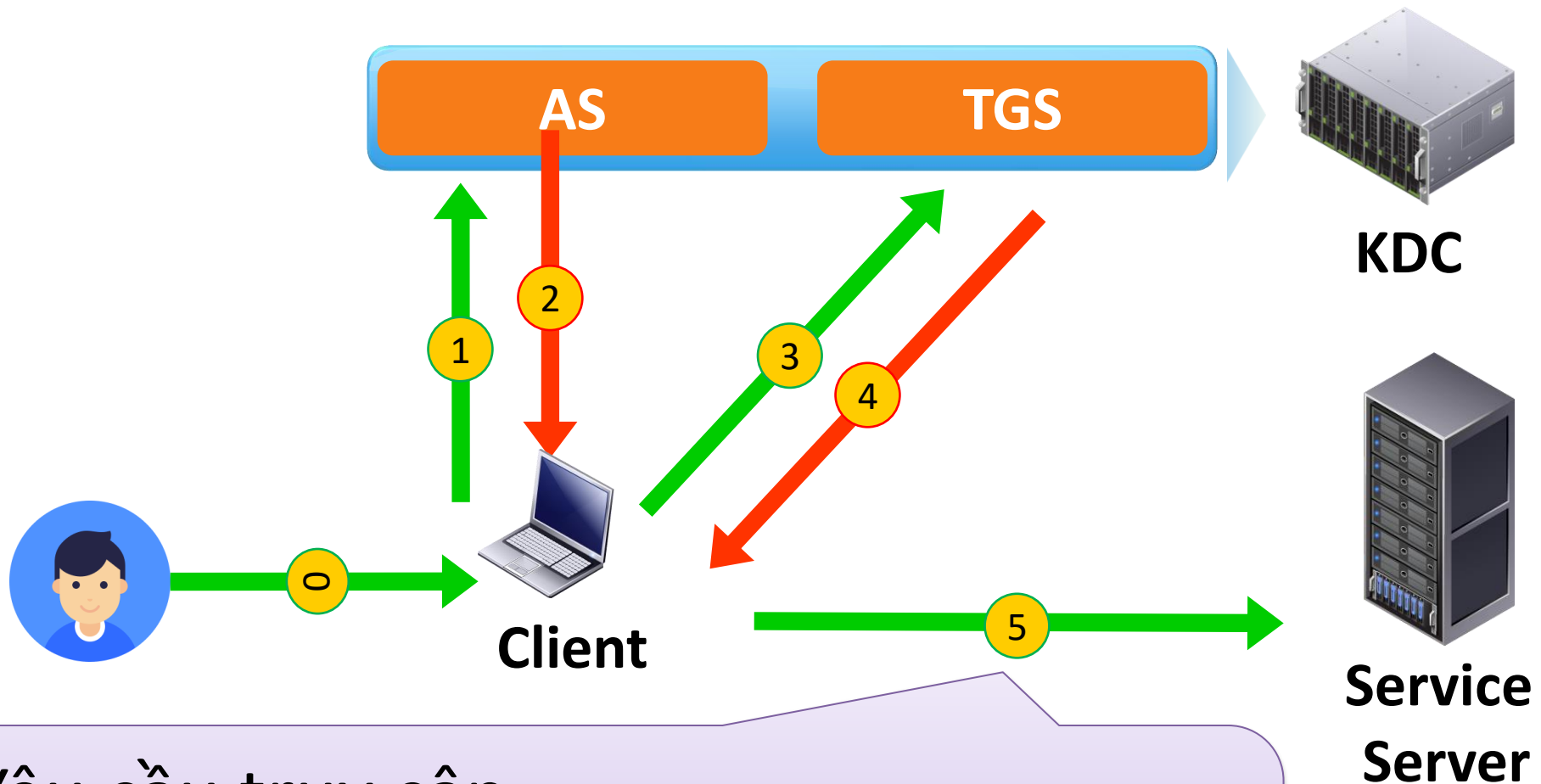


Cấp vé truy cập dịch vụ

$TGS \rightarrow C: \{\{ST\}K_{TGS_SS}, K_{C_SS}\} K_{C_TGS}$

$ST = \{ID_C, ID_{SS}, t_3, p_2, K_{C_SS}\}$

Giao thức Kerberos: Các thông điệp

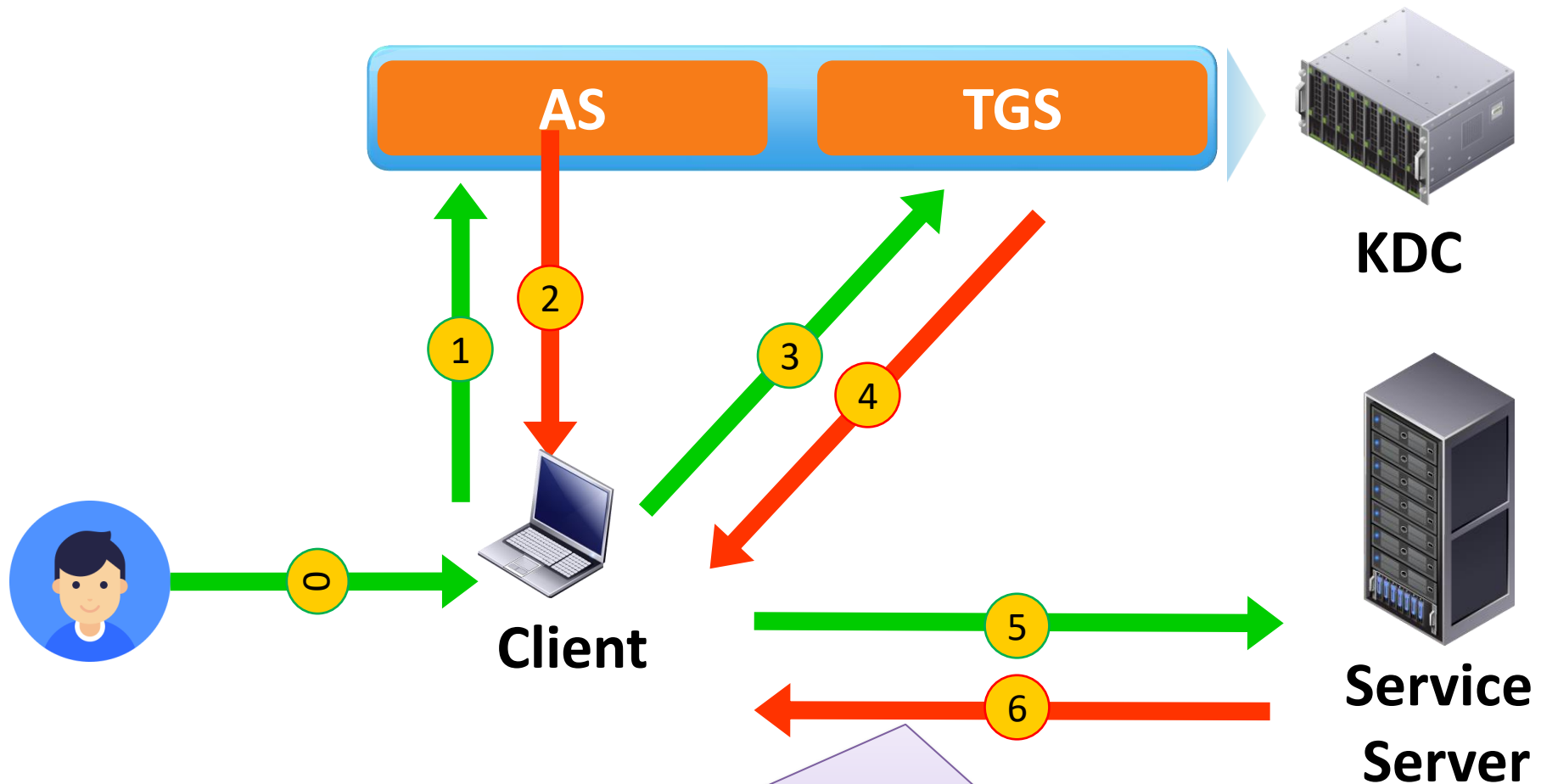


Yêu cầu truy cập

$C \rightarrow SS: \{ST\}K_{TGS_SS}, \{Aut2: ID_C, t_4\}K_{C_SS}$

$ST = \{ID_C, ID_{SS}, t_3, p_2, K_{C_SS}\}$

Giao thức Kerberos: Các thông điệp



Đáp ứng dịch vụ

1

Giao thức PAP, CHAP

2

Giao thức Kerberos

3

Giao thức EAP,
802.1X và RADIUS

Extensible Authentication Protocol

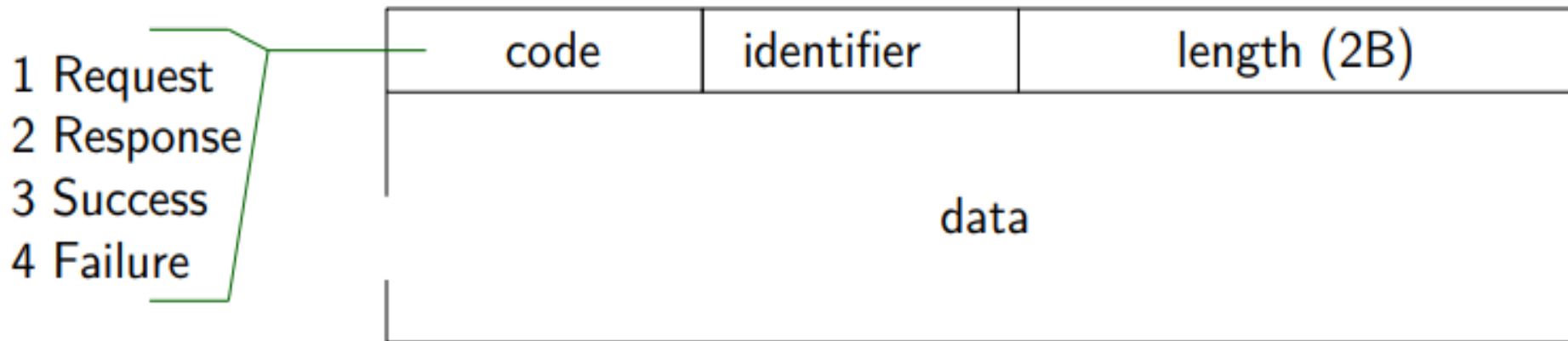
- EAP = Extensible Authentication Protocol
- Giao thức xác thực (khả) mở rộng
- RFC 3748
- thường được sử dụng trong mạng không dây và trong kết nối điểm-điểm.

"Extensible"

- Không cố định phương thức xác thực
- Phương thức xác thực được xác lập trong quá trình xác thực (khi đã bắt đầu pha xác thực)
- Cho phép tùy chọn phương thức xác thực phù hợp với yêu cầu về an toàn.
- Cho phép thay đổi phương thức xác thực với sự thay đổi tối thiểu trong phần cứng, phần mềm.

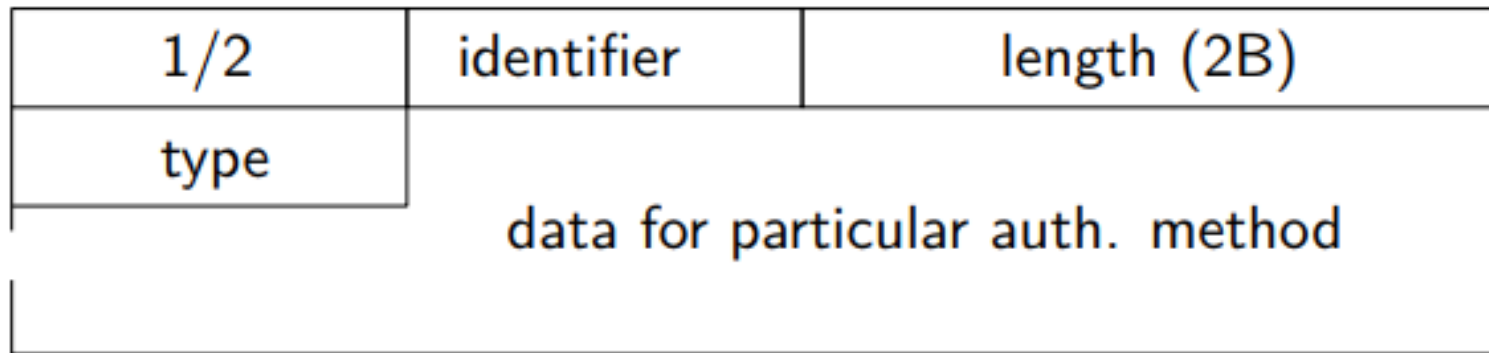
Extensible Authentication Protocol

❖ Định dạng gói tin EAP: Có 4 loại EAP message:



Extensible Authentication Protocol

- ❖ Có nhiều phương thức xác thực khác nhau (khoảng hơn 40):



- ❖ Chẳng hạn, type =

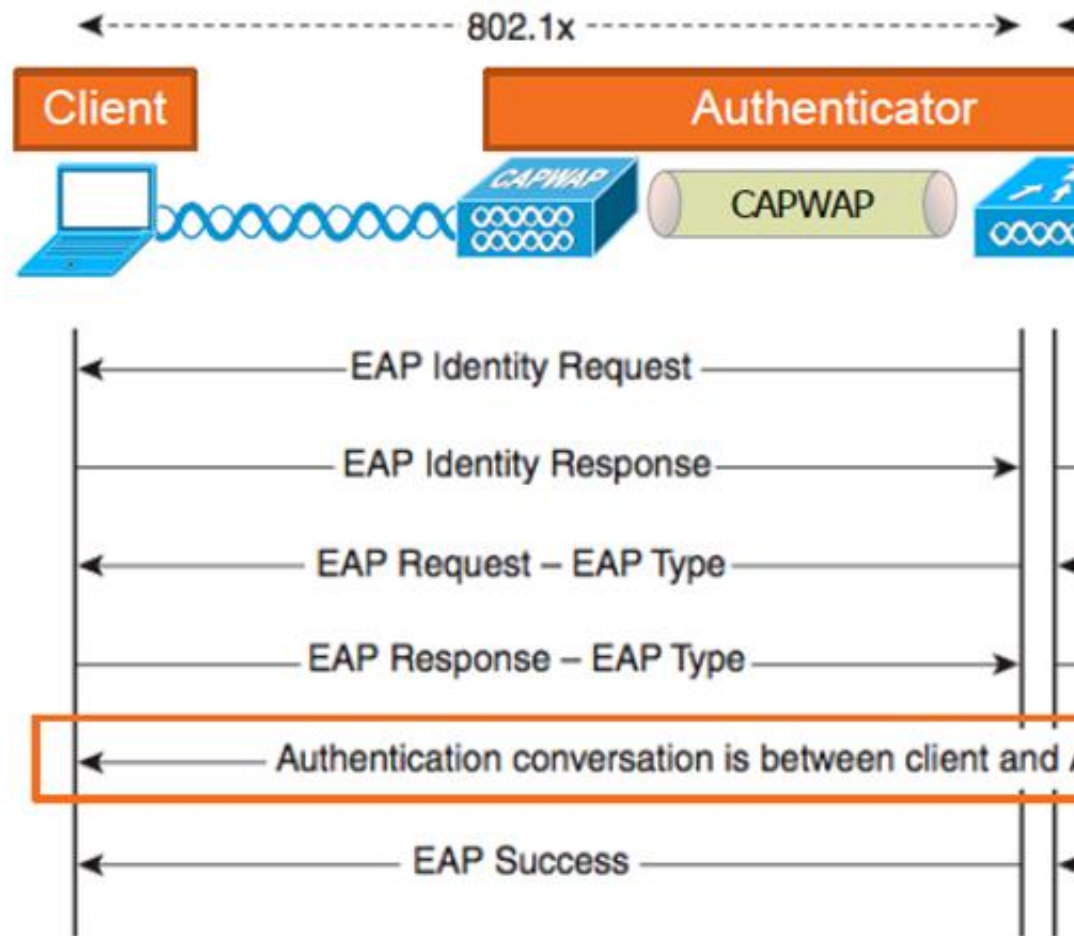
4	MD5	21	PEAP
13	TLS	43	FAST
21	TTLS	49	IKEv2

Phương thức xác thực

- EAP-MD5
- LEAP: Lightweight Extensible Authentication Protocol
- EAP-TLS: EAP Transport Layer Security
- EAP-POTP: EAP Protected One-Time Password
- EAP-PSK: EAP Pre-Shared Key
- EAP-PWD: EAP Password
- EAP-TTLS: EAP Tunneled Transport Layer Security
- EAP-IKEv2: EAP Internet Key Exchange v.2
- EAP-SIM: EAP Subscriber Identity Module
- EAP-AKA: EAP Authentication and Key Agreement
-

PPP Extensible Authentication Protocol

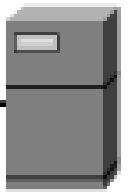
EAP — Protocol Flow



PPP Extensible Authentication Protocol

Branch Router
"Twiggy"

NAS
"Timbuktu"



Xác định
phương
thức xác
thực

Request (Identity)

1

Request (Authentication Challenge)

Response (Identity)

2

Response (Authentication Challenge)

Success or Failure

3

CÓ THỂ
yêu cầu
phương
thức khác



PPP EAP 2-way Authentication

Chương 2. PPP EAP 2-way Authentication.cap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help



eap

No.	Source	Destination	Protocol	Length	Info
5	N/A	N/A	EAP	9	Request, Identity
6	N/A	N/A	EAP	9	Request, Identity
7	N/A	N/A	EAP	11	Response, Identity
8	N/A	N/A	EAP	11	Response, Identity
9	N/A	N/A	EAP	28	Request, MD5-Challenge EAP (EAP-MD5-CHALLENGE)
10	N/A	N/A	EAP	28	Request, MD5-Challenge EAP (EAP-MD5-CHALLENGE)
11	N/A	N/A	EAP	28	Response, MD5-Challenge EAP (EAP-MD5-CHALLENGE)
12	N/A	N/A	EAP	28	Response, MD5-Challenge EAP (EAP-MD5-CHALLENGE)
13	N/A	N/A	EAP	8	Success
14	N/A	N/A	EAP	8	Success

PPP Configuration Request for EAP

No.	Source	Destination	Protocol	Length	Info
1	N/A	N/A	PPP LCP	18	Configuration Request
2	N/A	N/A	PPP LCP	18	Configuration Request
3	N/A	N/A	PPP LCP	18	Configuration Ack

▼	PPP Link Control Protocol
	Code: Configuration Request (1)
	Identifier: 69 (0x45)
	Length: 14
▼	Options: (10 bytes), Authentication Protocol, Magic Number
▼	Authentication Protocol: Extensible Authentication Protocol (0xc227)
	Type: Authentication Protocol (3)
	Length: 4
	Authentication Protocol: Extensible Authentication Protocol (0xc227)
➤	Magic Number: 0x012f4de5

0000	ff 03 c0 21 01 45 00 0e 03 04 c2 27 05 06 01 2f	...!.E... ..'.../
0010	4d e5	M.

Request, Identity

No.	Source	Destination	Protocol	Length	Info
4	N/A	N/A	PPP LCP	18	Configuration Ack
5	N/A	N/A	EAP	9	Request, Identity
6	N/A	N/A	EAP	9	Request, Identity

- > Frame 5: 9 bytes on wire (72 bits), 9 bytes captured (72 bits)
- > Point-to-Point Protocol
- ▼ Extensible Authentication Protocol

Code: Request (1)

Id: 91

Length: 5

Type: Identity (1)

0000 ff 03 c2 27 01 5b 00 05 01

...'.[...]

Response, Identity

No.	Source	Destination	Protocol	Length	Info
6	N/A	N/A	EAP	9	Request, Identity
7	N/A	N/A	EAP	11	Response, Identity
8	N/A	N/A	EAP	11	Response, Identity

> Point-to-Point Protocol

▼ Extensible Authentication Protocol

Code: Response (2)

Id: 91

Length: 7

Type: Identity (1)

Identity: R2

0000 ff 03 c2 27 02 5b 00 07 01 52 32 ...'.[...R2

Request, MD5-Challenge

No.	Source	Destination	Protocol	Length	Info
8	N/A	N/A	EAP	11	Response, Identity
9	N/A	N/A	EAP	28	Request, MD5-Challenge EAP (EAP-MD5-CH
10	N/A	N/A	EAP	28	Request, MD5-Challenge EAP (EAP-MD5-CH

> Point-to-Point Protocol
v Extensible Authentication Protocol

Code: Request (1)

Id: 92

Length: 24

> Type: MD5-Challenge EAP (EAP-MD5-CHALLENGE) (4)

EAP-MD5 Value-Size: 16

EAP-MD5 Value: bf09adbc1bedcb9fcda522d4262e3484

EAP-MD5 Extra Data: 5231

0000	ff 03 c2 27 01 5c 00 18 04 10 bf 09	1b ed	...'.\... ..
0010	cb 9f cd a5 22 d4 26 2e 34 84 52 37	".&. 4.R1

Giải thích đại lượng này!

Response, MD5-Challenge

No.	Source	Destination	Protocol	Length	Info
9	N/A	N/A	EAP	28	Request,
10	N/A	N/A	EAP	28	Request,
11	N/A	N/A	EAP	28	Response

Nếu gửi lại "Nak" (3) thì sẽ phải thống nhất lại phương thức xác thực

```
> Point-to-Point Protocol
< Extensible Authentication Protocol
  Code: Response (2)
  Id: 92
  Length: 24
  > Type: MD5-Challenge EAP (EAP-MD5-CHALLENGE) (4)
    EAP-MD5 Value-Size: 16
    EAP-MD5 Value: b7df13cffeceb05d28d25a06e49322e6
    EAP-MD5 Extra Data: 5232
```

```
0000  ff 03 c2 27 02 5c 00 18 04 10 b7 df 10 fe ce ...'.\... ..
0010  b0 5d 28 d2 5a 06 e4 93 22 e6 52 32 00 00 00 00 .](.Z... ".R2
```

Giải thích đại lượng này!

EAP Success

No.	Source	Destination	Protocol	Length	Info
12	N/A	N/A	EAP	28	Response, MD5-Challenge EAP (
13	N/A	N/A	EAP	8	Success
14	N/A	N/A	EAP	8	Success

> Frame 13: 8 bytes on wire (64 bits), 8 bytes captured (64 bits)
> Point-to-Point Protocol
v Extensible Authentication Protocol

Code: Success (3)

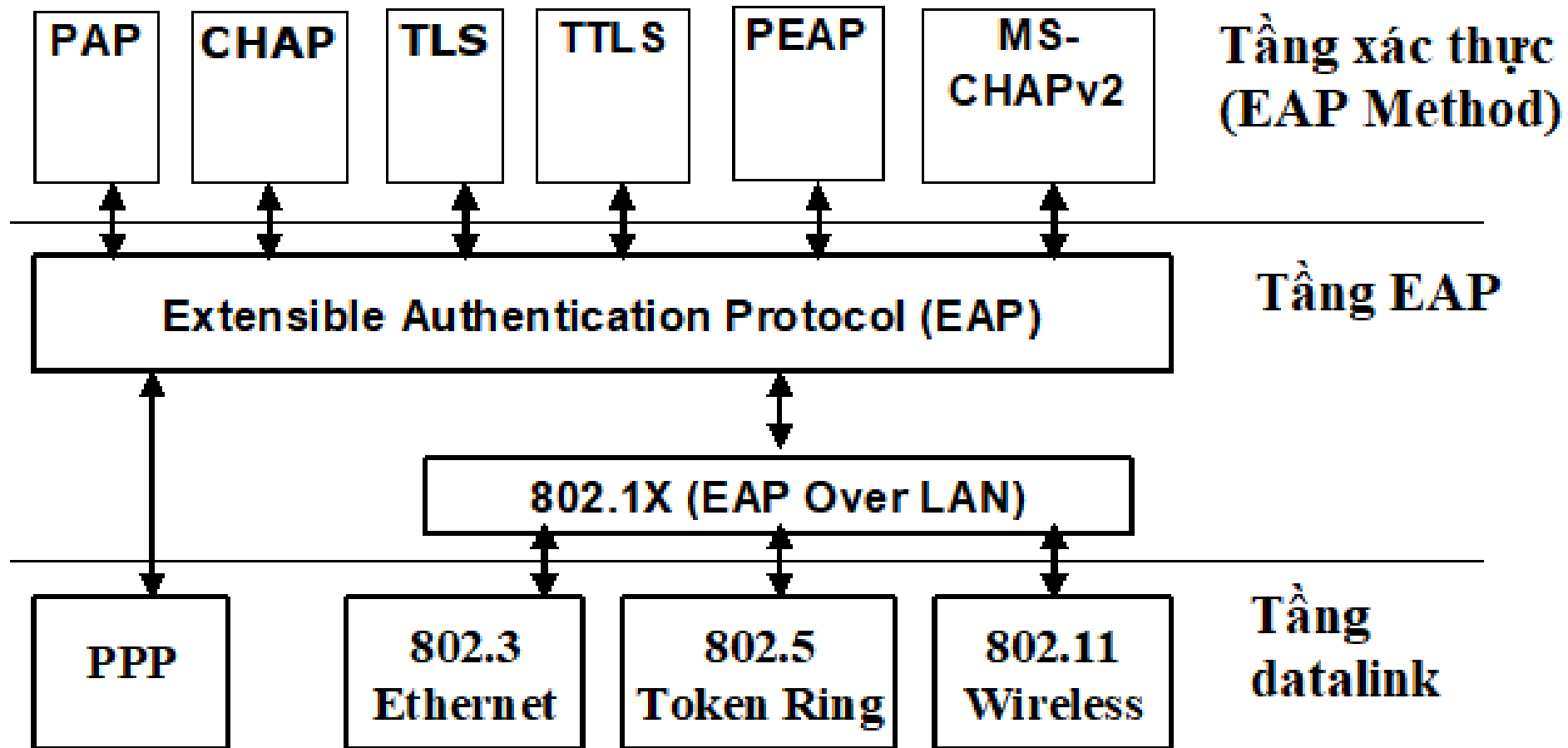
Id: 92

Length: 4

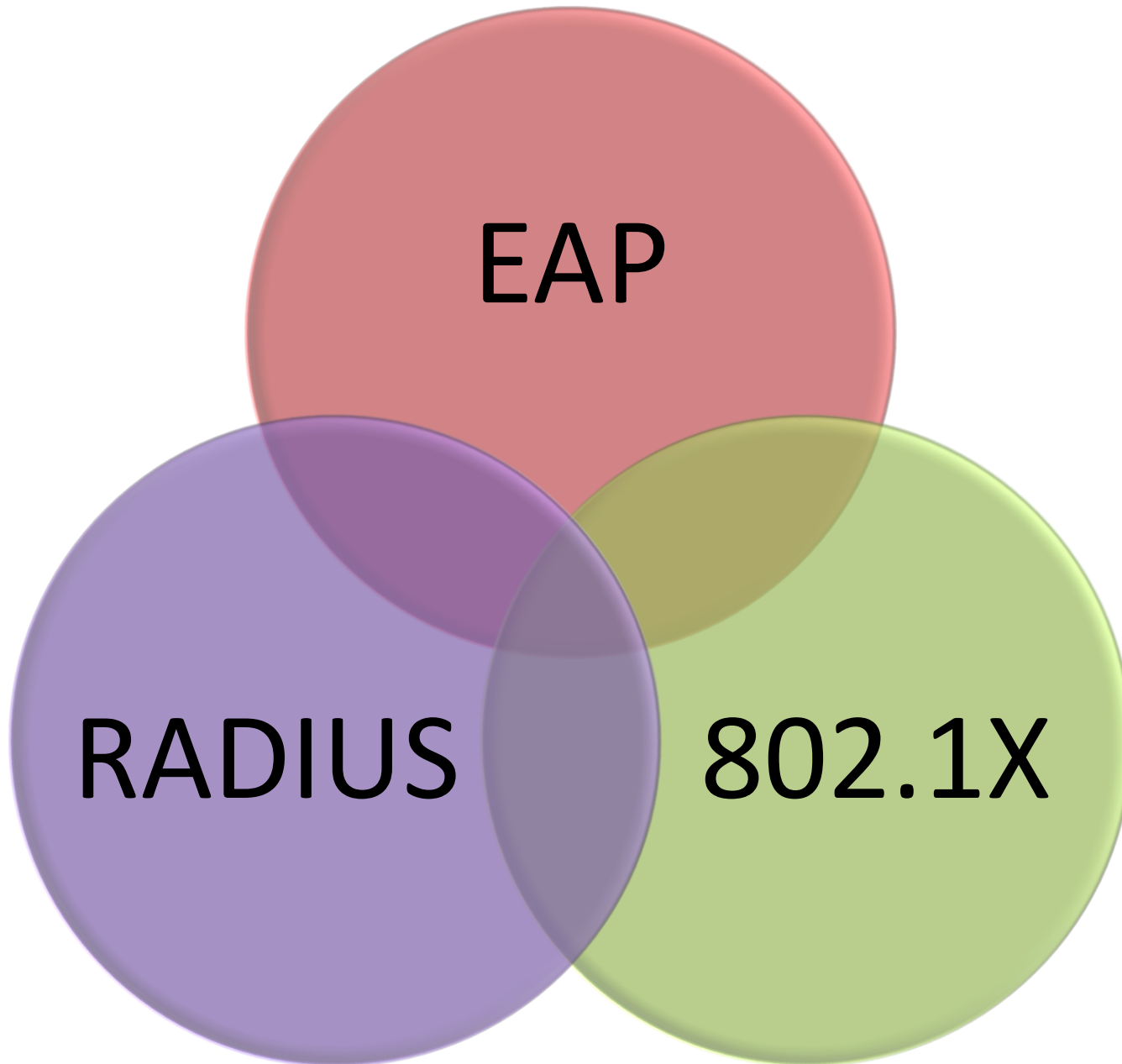
0000 ff 03 c2 27 03 5c 00 04

...'.\...

Kiến trúc phân tầng của EAP



EAP với RADIUS và 802.1x



802.1X

□802

- 802: IEEE standards for networking protocols
- 802.11: wireless LAN protocols and standard
- 802.1: general concepts relating to LANs/WANs
- “802.1X” (not 802.11X): standards for LANs

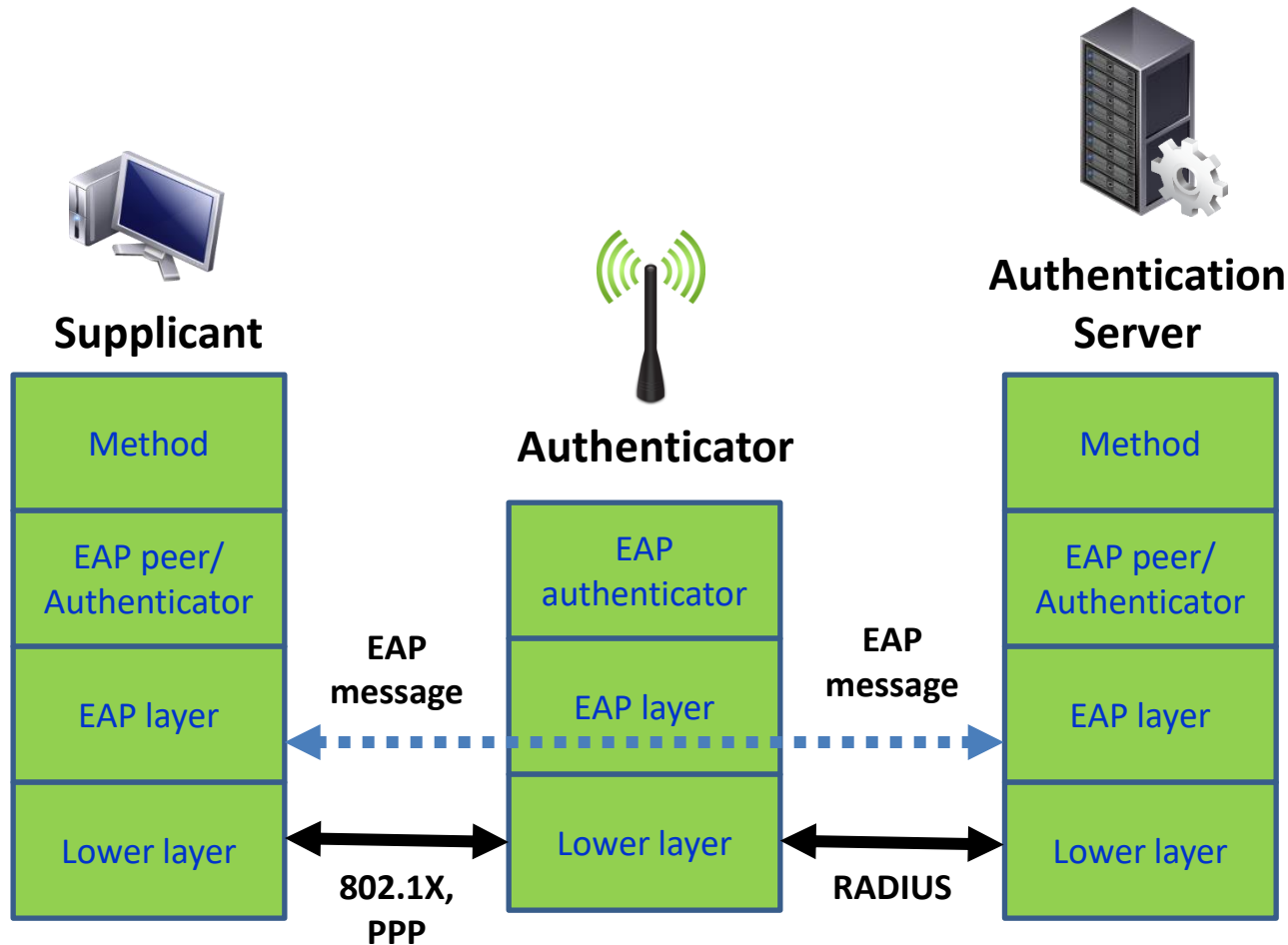
□**802.1X** là chuẩn quy định sử dụng EAP qua môi trường LAN (ở tầng MAC)

➔ 802.1X = EAPOL

RADIUS

- RADIUS = Remote Authentication Dial-In User Service
- RFCs: 2865, 2866, 3579...
- Được thiết kế theo kiến trúc AAA (Authentication-Authorization-Accounting)
- Xác thực: EAP, PAP, CHAP...

EAP trong 802.1X và RADIUS

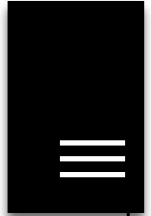


EAP trong 802.1X và RADIUS

Supplicant

Authenticator

Authentication Server



EAPOL-Start



EAP-Request/Identity



EAP-Response/Identity



EAP-Request/Auth



EAP-Response/Auth



EAP-Success



RADIUS Access-Request



RADIUS Access-Challenge



RADIUS Access-Request

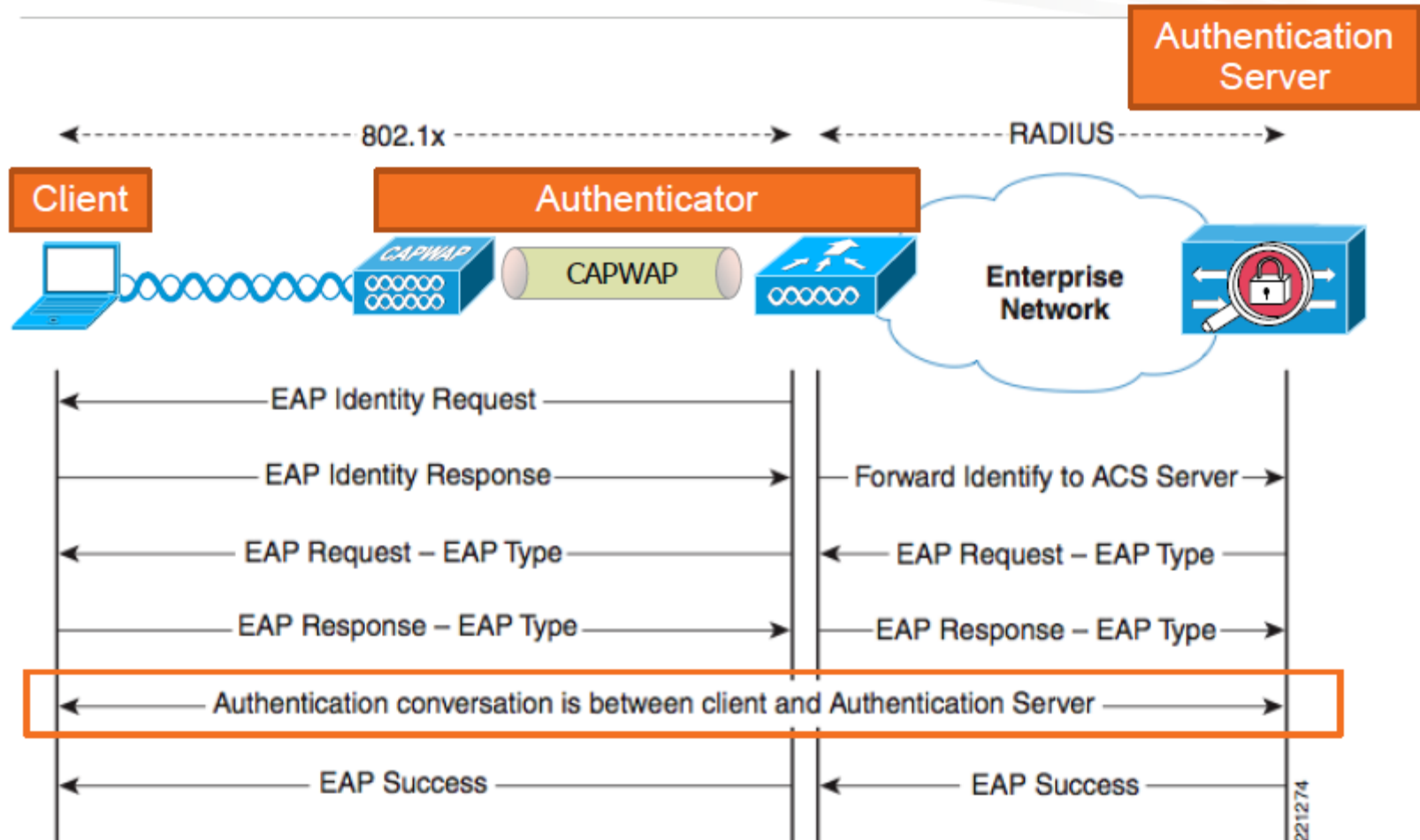


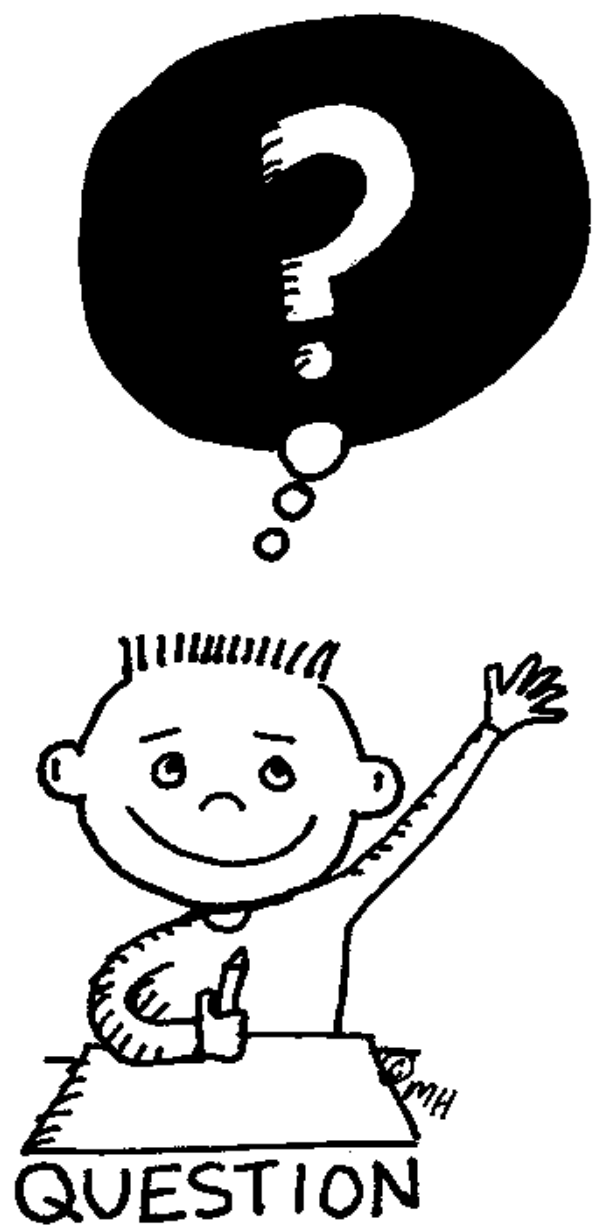
RADIUS Access-Accept



EAP trong 802.1X và RADIUS

EAP — Protocol Flow





Sinh viên tự nghiên cứu



 OpenID

Oath:
A Verizon company