2ip 2STON™ SPN

- 공공 Wi-Fi 적용 가능성 타진 -

2ip, Inc.

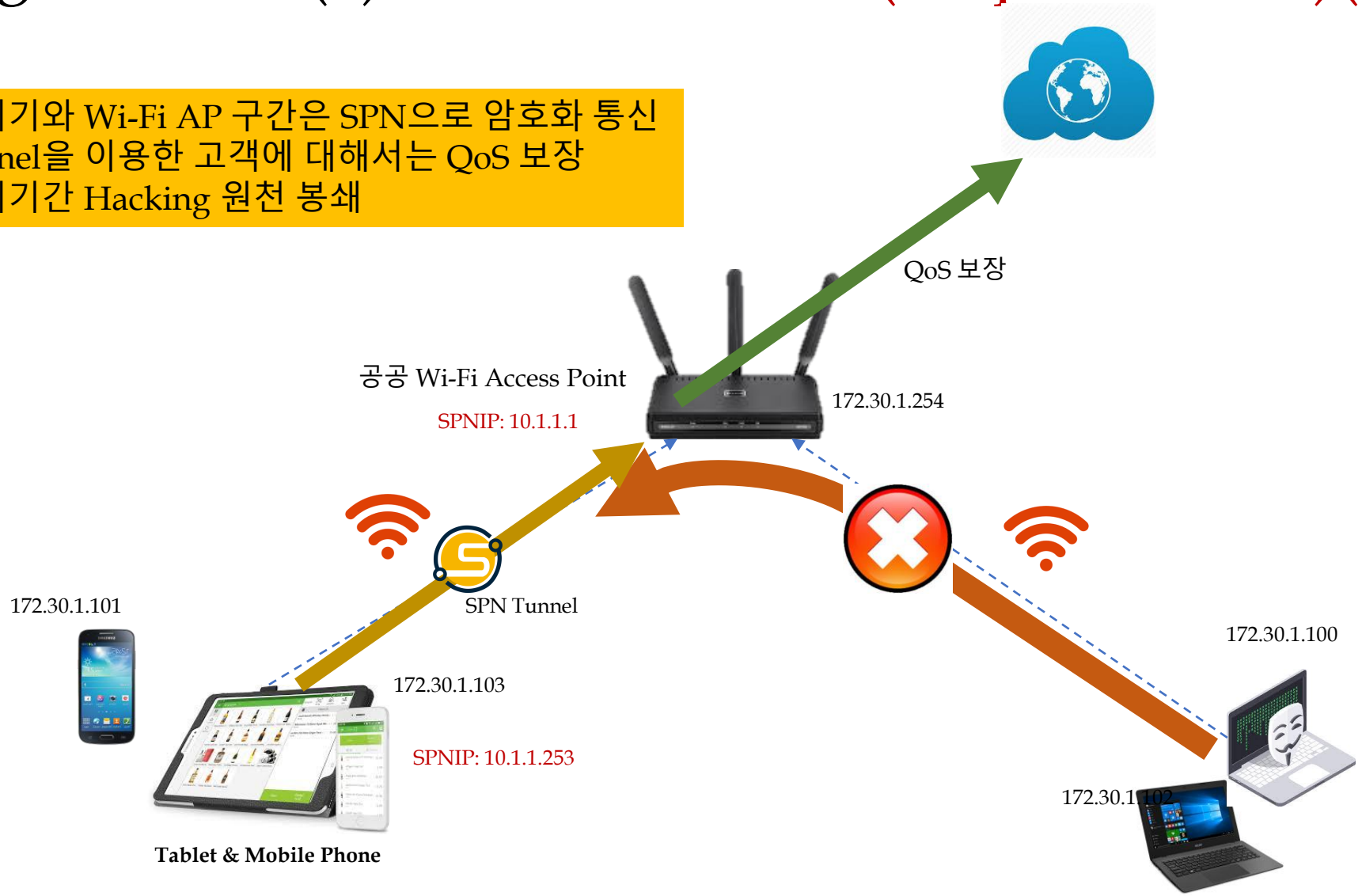
Doc. Revision: 0.5

1. Target 시스템(1) – 기술 요구사항(Requirements)(1)

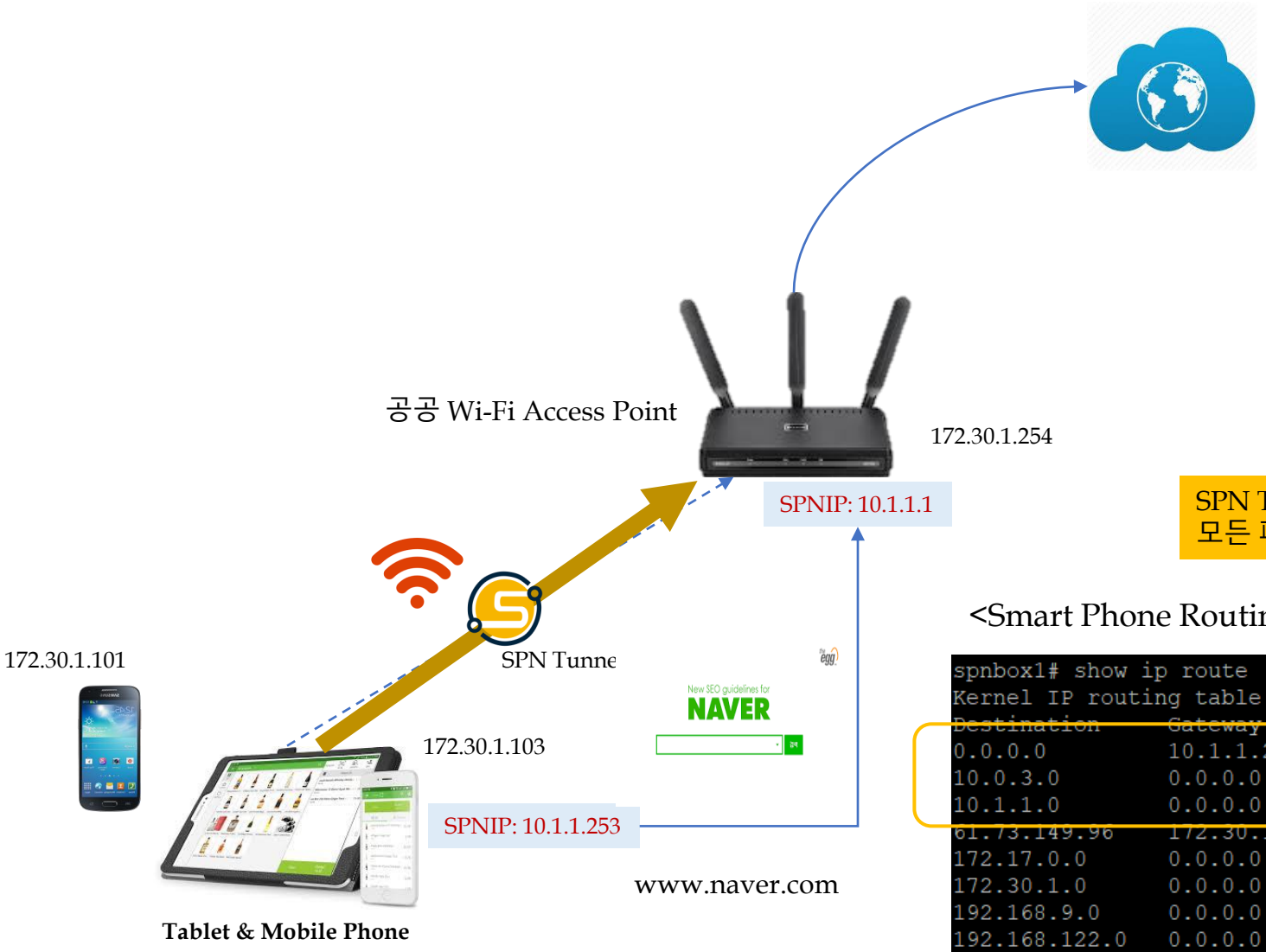
- 1) 공공 Wi-Fi AP(Access Point)에 연결된 기기(Smart Phone, Notebook 등)는 SPN Tunnel을 통해 인터넷을 사용할 수 있어야 한다.
- 2) 공공 Wi-Fi AP에 연결된 기기는 (이동 중)AP가 바뀌더라도 SPN 연결을 자동으로 유지(자동 연결)할 수 있어야 한다.
  - *Wi-Fi 환경의 특성 상 Wi-Fi 연결마다 SPN 연결을 자동으로 해주어야 할 듯.*
- 3) (보안을 위해) Wi-Fi AP 연결된 기기(Station) 간에는 상호 통신이 이루어져서는 안된다. 즉, 공공 Wi-Fi AP를 경유한 어떠한 Hacking 시도도 차단할 수 있어야 한다.
- 4) SPN Tunnel을 사용하여 인터넷을 사용하는 경우에는 QoS를 보장해 줄 수 있어야 한다. SPN Tunnel을 사용하지 않고서도 인터넷을 이용할 수는 있겠으나, 이 경우는 QoS가 보장되지 말아야 한다.
  - *그래야 나름의 merit가 있을 것임.*

1. Target 시스템(1) – 기술 요구사항(Requirements)(2)

1) Mobile 기기와 Wi-Fi AP 구간은 SPN으로 암호화 통신
2) SPN Tunnel을 이용한 고객에 대해서는 QoS 보장
3) Mobile 기기간 Hacking 원천 봉쇄



1. Target 시스템(2) – SPN Tunnel(1)

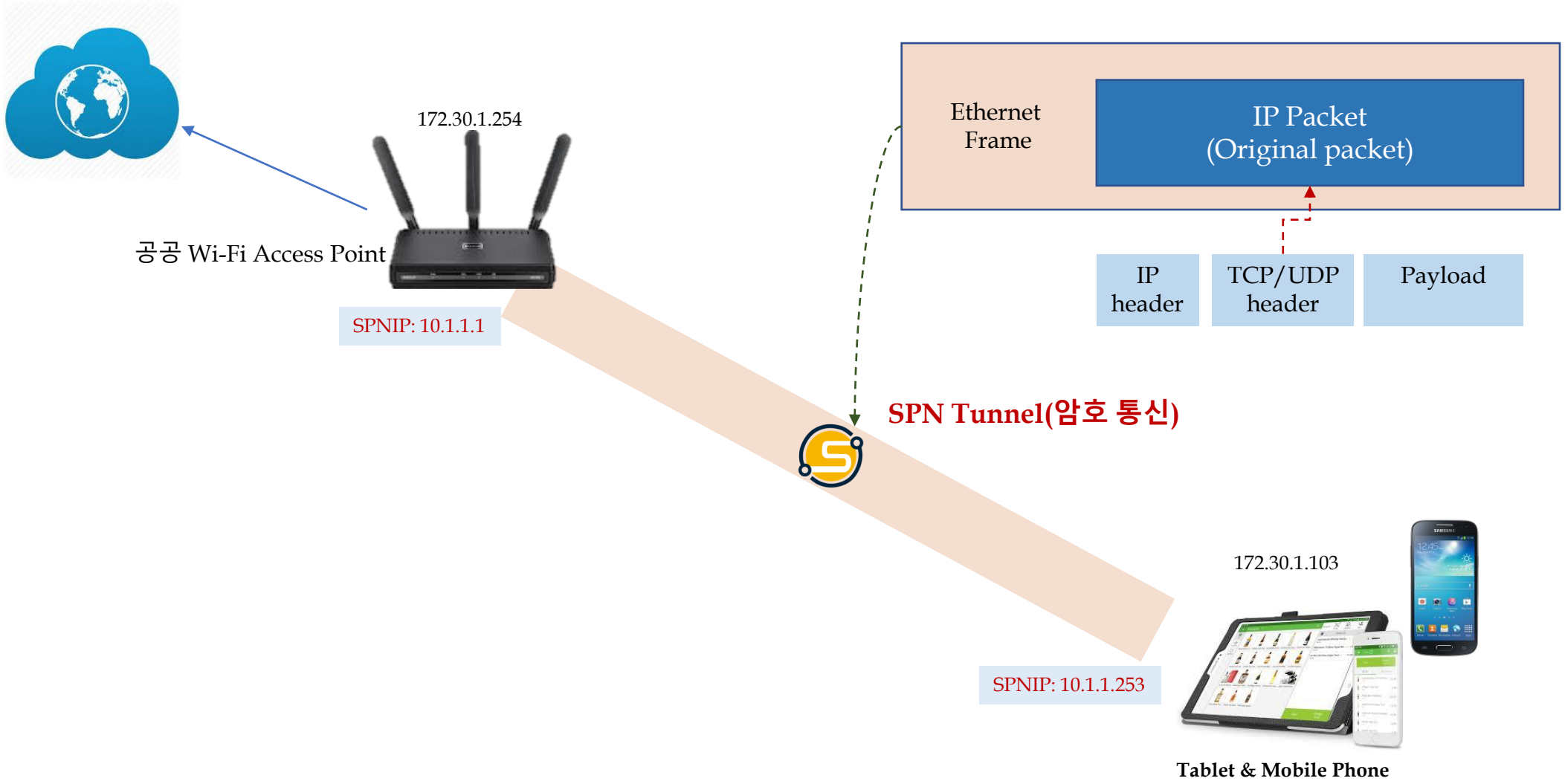


SPN Tunnel 생성시 Phone의 Routing table을 조작하여 ,
모든 패킷이 SPN Tunnel의 적용 대상이 되도록 만들어 주어야만 한다.

<Smart Phone Routing Table 예>

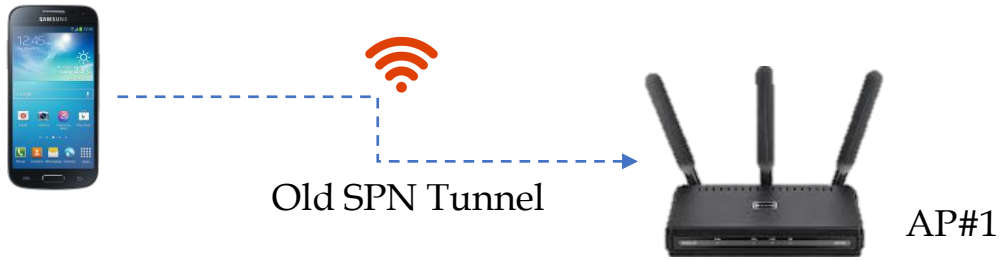
```
spnbox1# show ip route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         10.1.1.253      0.0.0.0         UG    0      0        0 spn0
10.0.3.0        0.0.0.0         255.255.255.0   U     0      0        0 lxcbr0
10.1.1.0        0.0.0.0         255.255.255.0   U     0      0        0 spn0
61.73.149.96    172.30.1.254    255.255.255.255 UGH   0      0        0 eth1
172.17.0.0      0.0.0.0         255.255.0.0     U     0      0        0 docker0
172.30.1.0      0.0.0.0         255.255.255.0   U     0      0        0 eth1
192.168.9.0     0.0.0.0         255.255.255.0   U     0      0        0 eth0
192.168.122.0   0.0.0.0         255.255.255.0   U     0      0        0 virbr0
spnbox1#
```

1. Target 시스템(2) – SPN Tunnel(2)

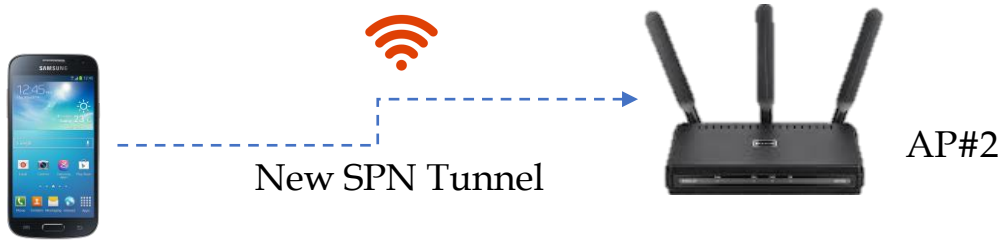


SPN 기능을 사용하면, L3 packet(IP packet)을 안전하게 실어 나를 수 있습니다.

1. Target 시스템(3) – AP 전환 시 SPN 연결(1)



이동 중 새로운 Wi-Fi AP를 만나면 새로운 SPN Tunnel 자동으로 확립할 수 있어야 한다.

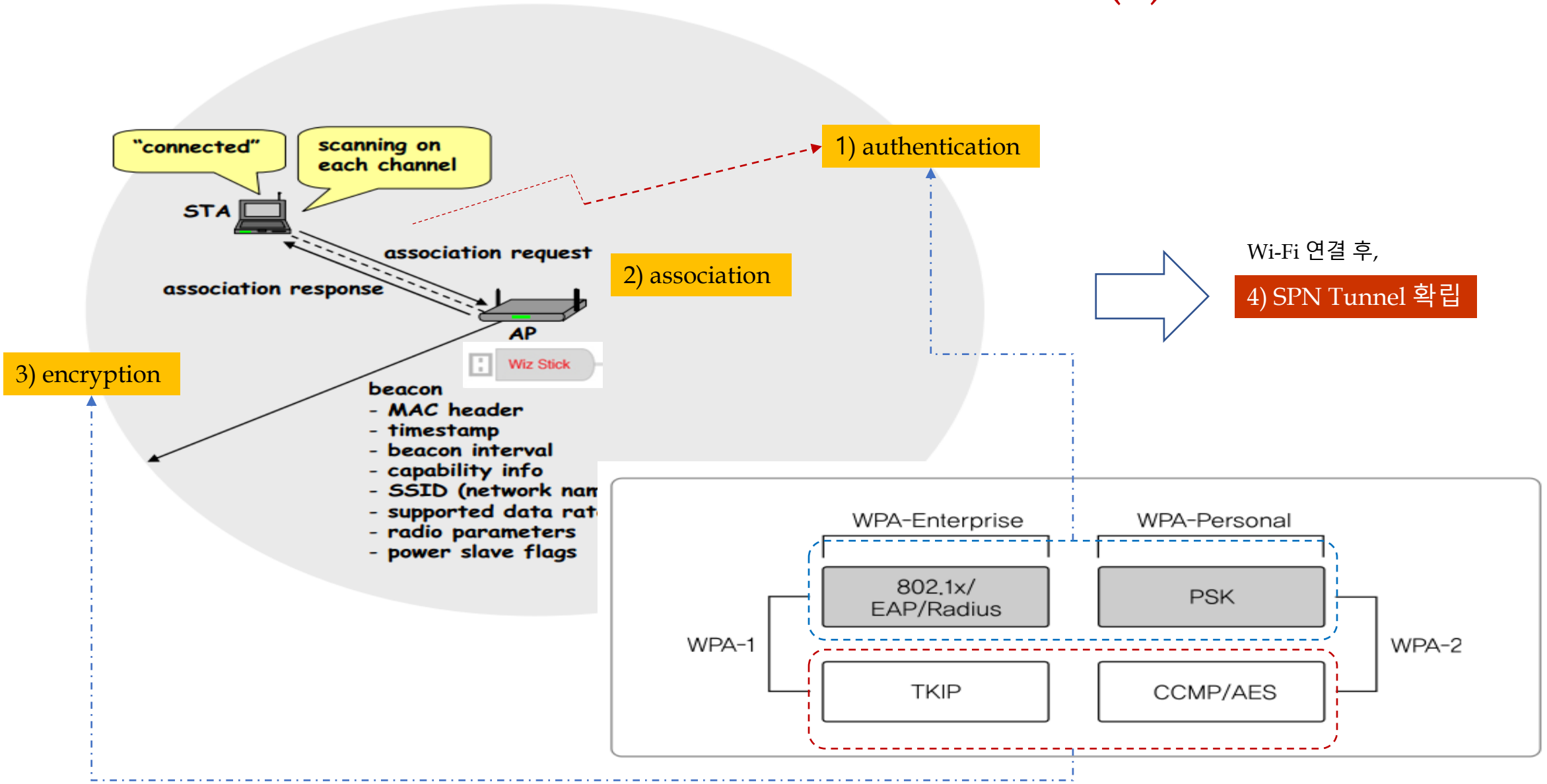


1. Target 시스템(3) – AP 전환 시 SPN 연결(2)

아래와 같은 SPN Tunnel 연결정보를 안전하게 자동으로 교환해 주는 기능이 구현되어야 한다.

YYYYYYYYYYYYY	Peer's Public key	정보 교환	Peer's Public key	XXXXXXXXXXXXXXXX
10.1.253	Peer's SPN IP Address		Peer's SPN IP Address	10.1.1.1
172.30.1.100:59760	Peer's Endpoint(RealIP:Port)		Peer's Endpoint(RealIP:Port)	172.30.1.254:59760
172.30.1.100/32	Peer's Allowed Networks		Peer's Allowed Networks	172.30.1.254/32

1. Target 시스템(3) – AP 전환 시 SPN 연결(3)



1. Target 시스템(3) – AP 전환 시 SPN 연결(4)

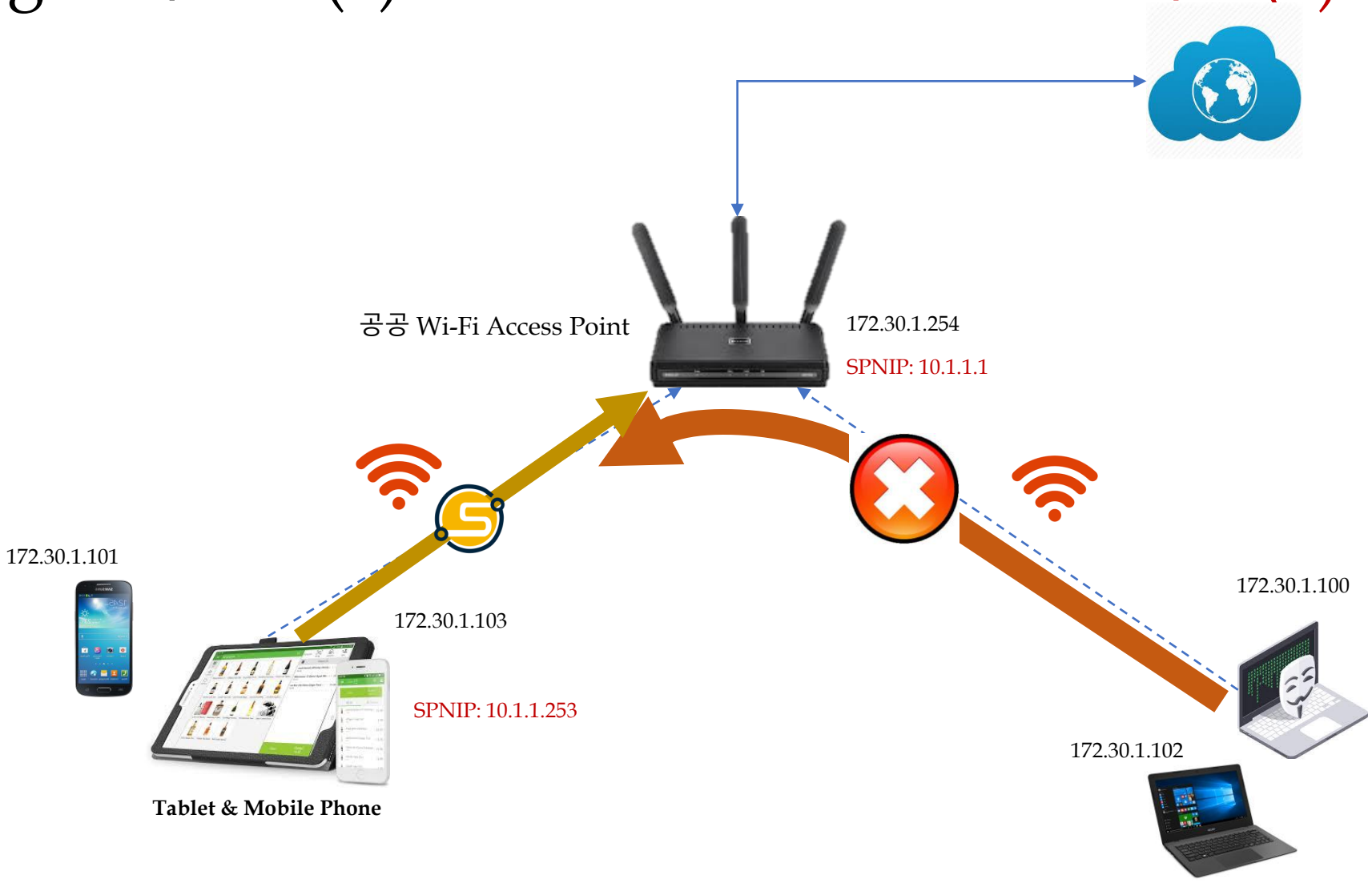
Wi-Fi 연결 화면

이 과정이 자동으로(매끄럽게) 진행되어야 함.

SPN Tunnel 설정 화면

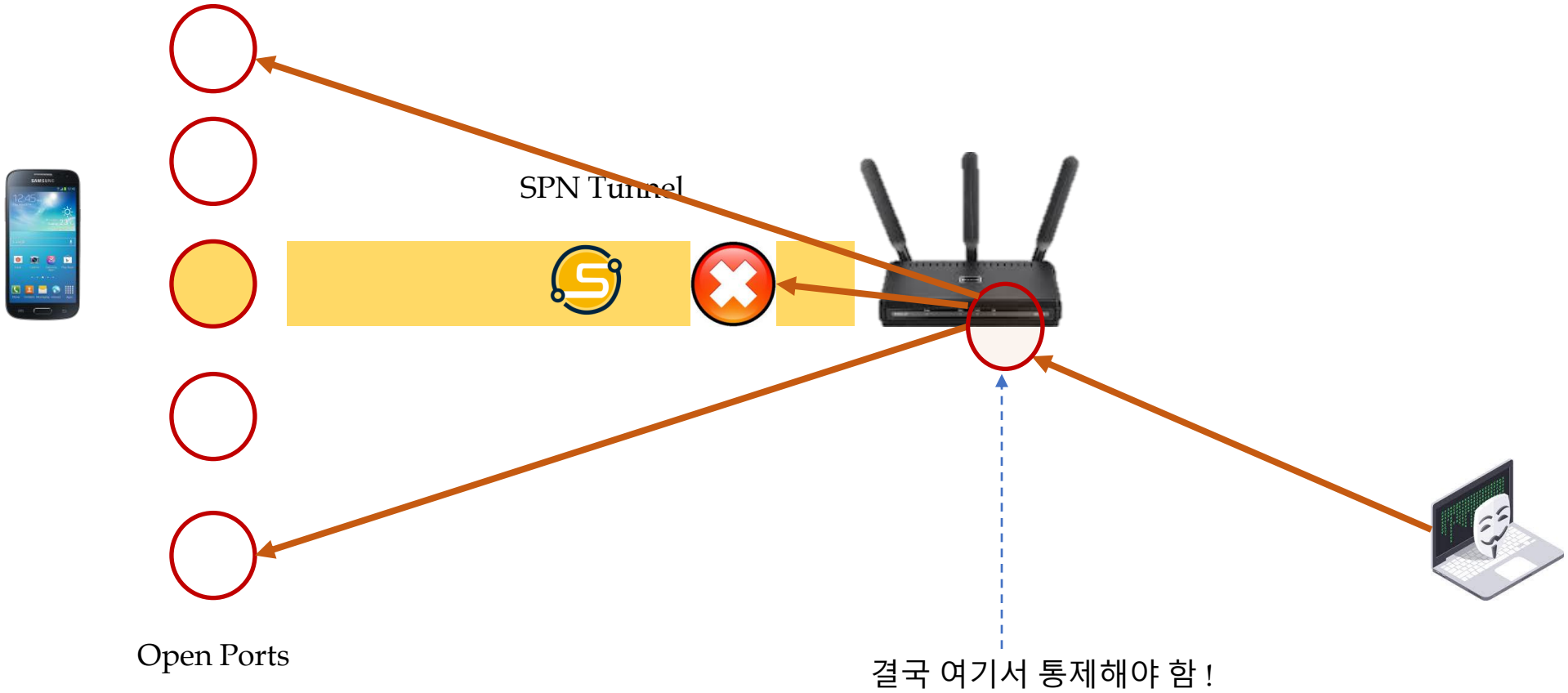
- iPhone도 고려해 주어야 함.

1. Target 시스템(4) – Wi-Fi Station 간 접근 차단(1)

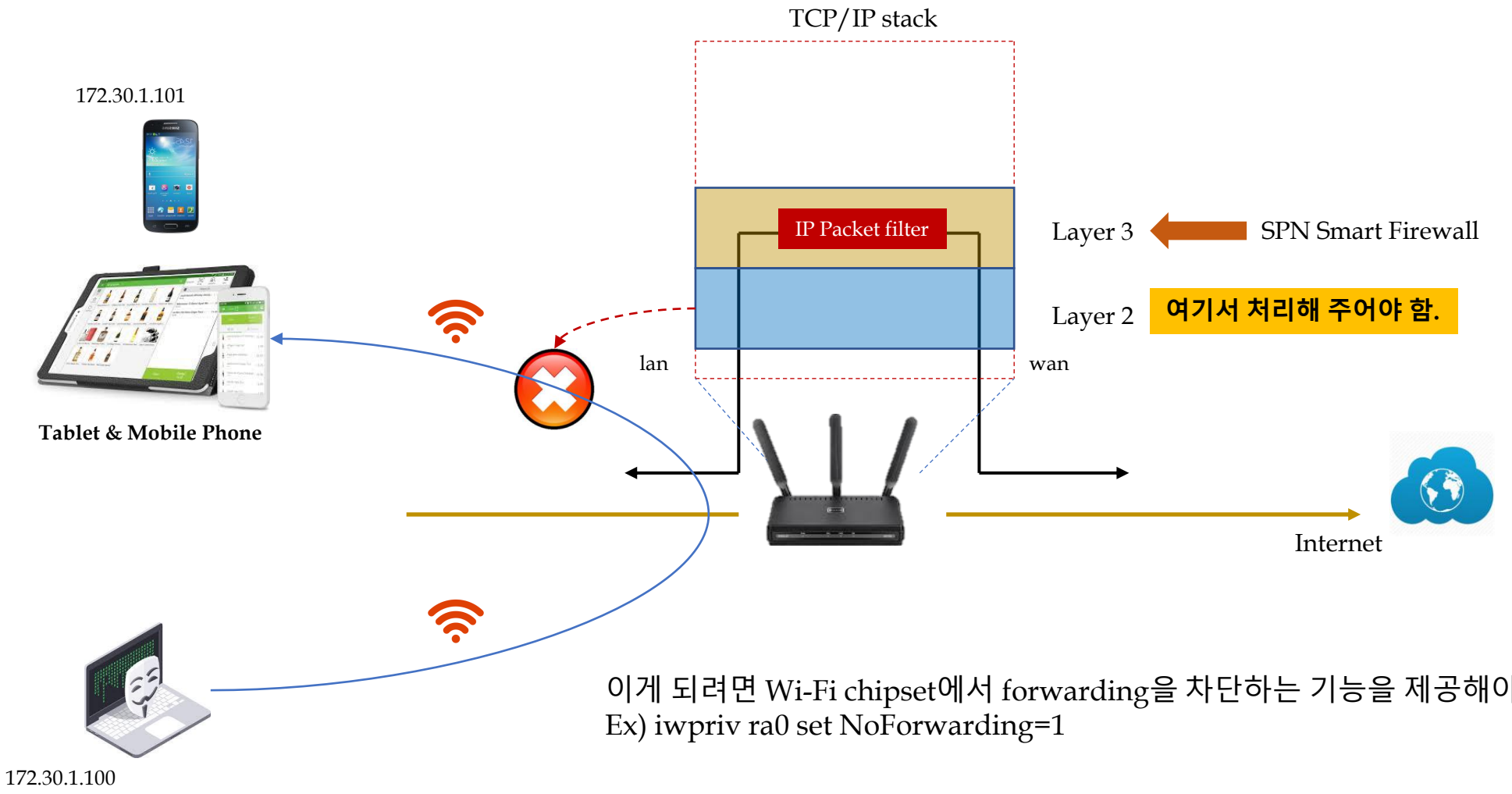


1. Target 시스템(4) – Wi-Fi Station 간 접근 차단(2)

(루팅을 하지 않는 한) Phone에 탑재된 SPN S/W(app)가 오픈된 포트를 통제하기는 쉽지 않다.



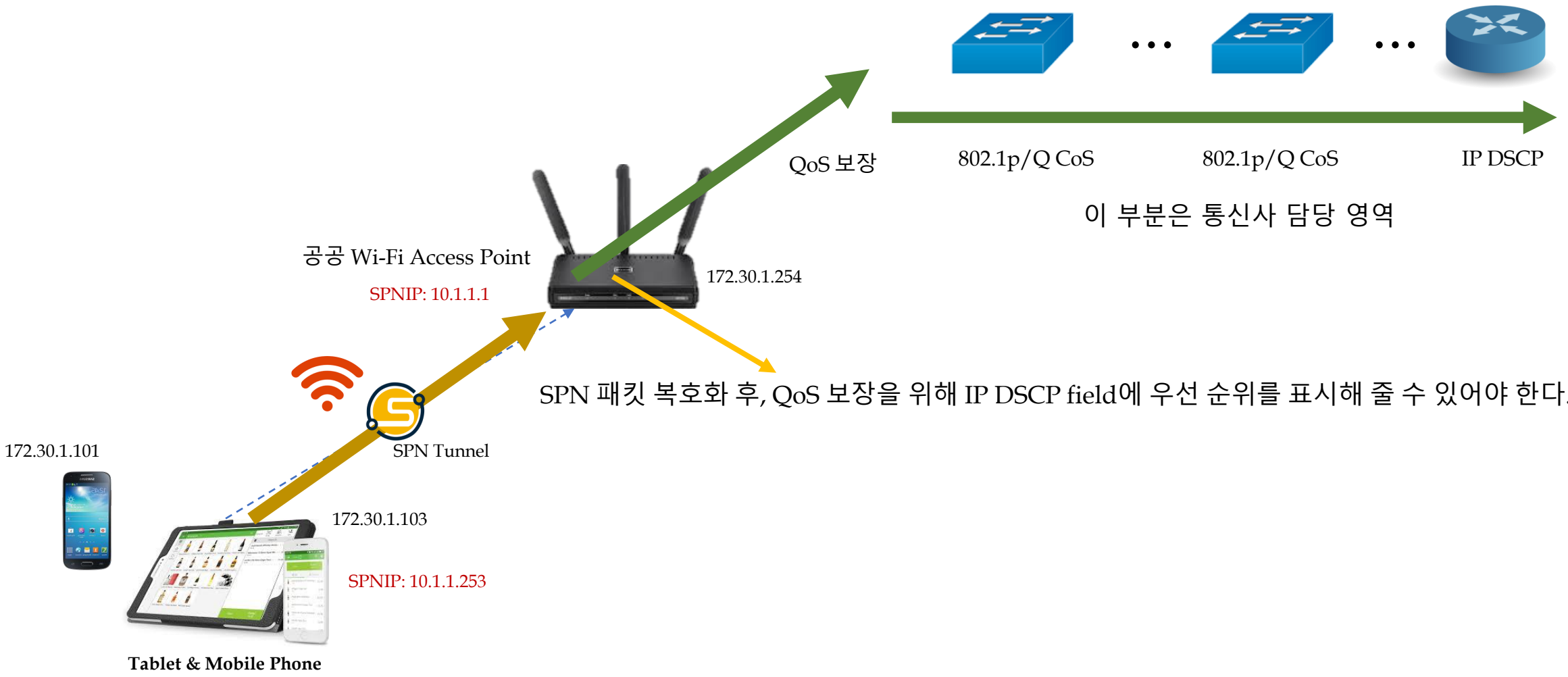
1. Target 시스템(4) – Wi-Fi Station 간 접근 차단(3)



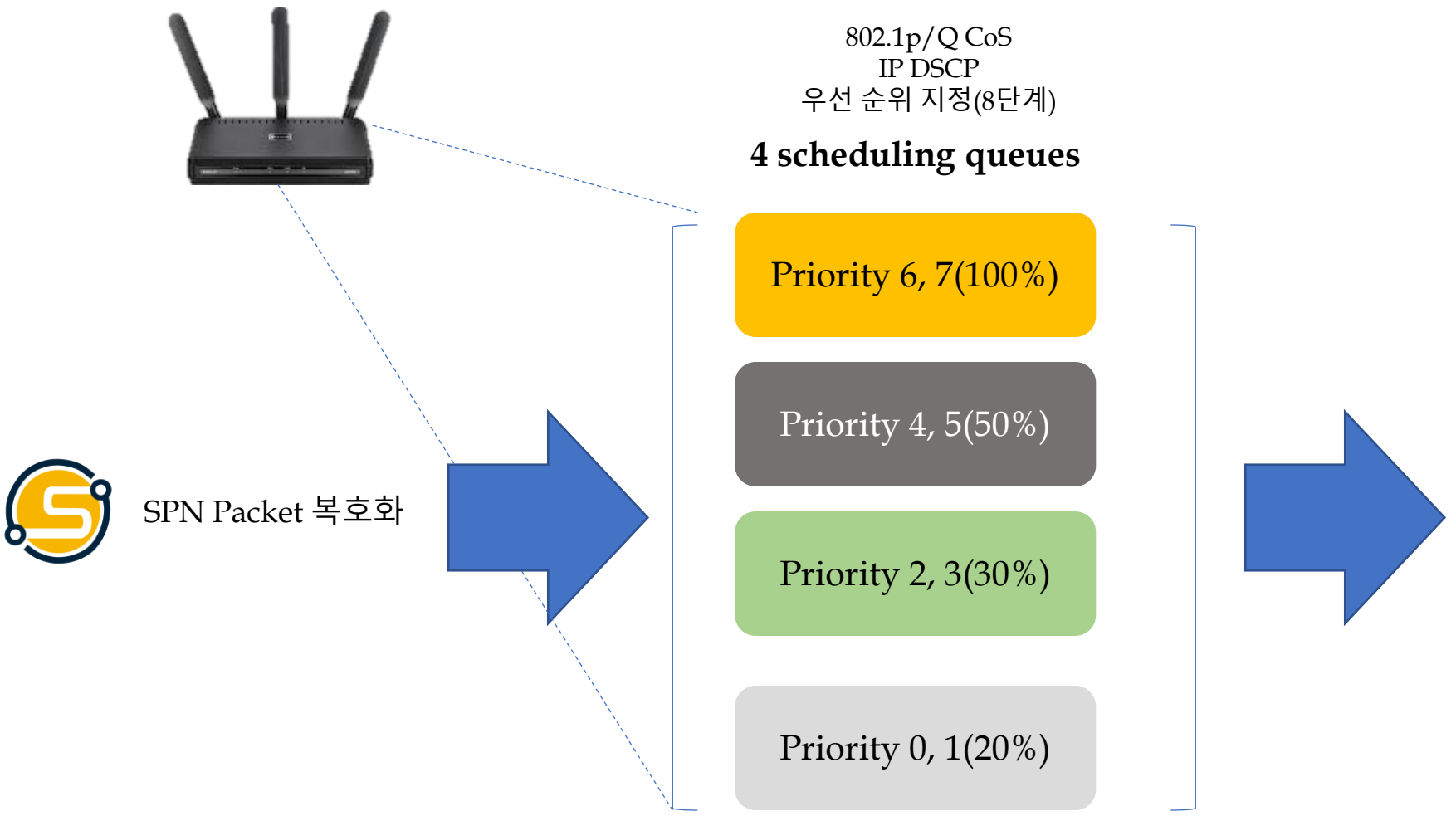
이게 되려면 Wi-Fi chipset에서 forwarding을 차단하는 기능을 제공해야 함.
Ex) iwpriv ra0 set NoForwarding=1

Wi-Fi 연결을 통한 접근 제어는 AP Layer 3에서 불가능함. 따라서 Wi-Fi MAC Layer에서 차단하는 방법이 강구되어야 한다.

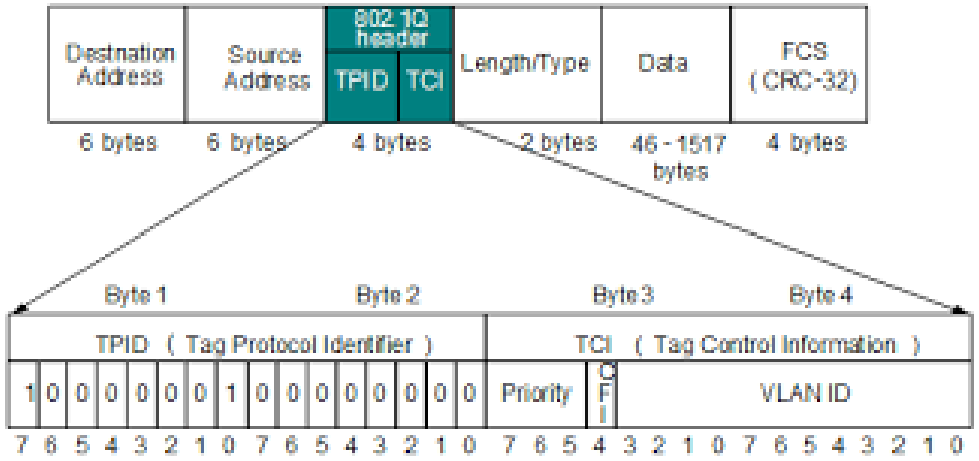
1. Target 시스템(5) – SPN Tunnel 사용 시 QoS 보장(1)



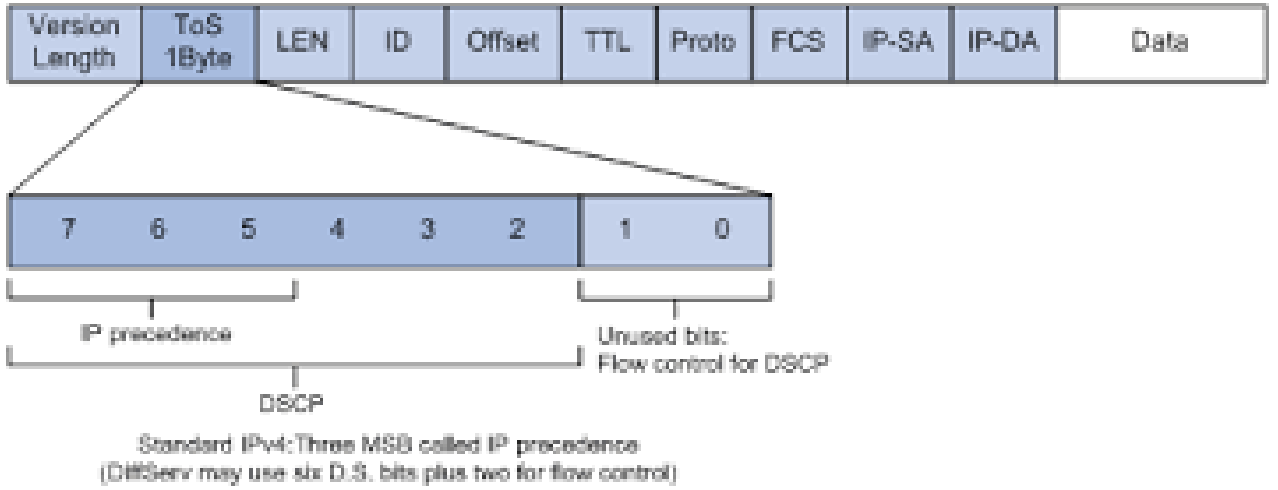
1. Target 시스템(5) – SPN Tunnel 사용 시 QoS 보장(2)



1. Target 시스템(5) – SPN Tunnel 사용 시 QoS 보장(3)



802.1p/Q CoS
(L2 장비에서 처리)



IP DSCP
(L3 장비에서 처리)

Thank You

We Secure the Internet of Things with 2STON™