# 2017년 국가직 9급 네트워크 보안 해설

by 호이호이꿀떡

## 정답 체크

| 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 10 |
|---|---|---|---|---|---|---|---|---|---|
| ① | ④ | ① | ④ | ③ | ② | ② | ① | ③ | ② |
| **11** | **12** | **13** | **14** | **15** | **16** | **17** | **18** | **19** | **20** |
| ④ | ② | ② | ② | ④ | ③ | ③ | ③ | ③ | ④ |

**문 1. 네트워크에 연결된 노드가 사용할 IP 주소를 자동으로 할당해주는 프로토콜은?**

① DHCP(Dynamic Host Configuration Protocol)
② ICMP(Internet Control Message Protocol)
③ ARP(Address Resolution Protocol)
④ IGMP(Internet Group Management Protocol

답 ①

① **DHCP**(Dynamic Host Configuration Protocol, 동적 호스트 구성 프로토콜)
조직 내의 네트워크 상에서 IP 주소를 중앙에서 관리하고 할당해주는 프로토콜이다. 네트워크에 연결된 모든 기기가 각각 고유의 IP주소를 가지는 게 아니라, 네트워크 접속이 필요할 때만 IP 주소를 할당받아 사용하기 때문에 IP 주소의 낭비를 줄일 수 있다.

**<오답 체크>** ② **ICMP**(Internet Control Message Protocol, 인터넷 제어 메시지 프로토콜)
호스트와 게스트 간의 통신 중에 발생하는 에러 및 제어 정보를 제어하는 프로토콜

③ **ARP**(Address Resolution Protocol, 주소 결정 프로토콜)
IP 주소를 대응하는 MAC 주소값로 변환해주는 프로토콜

④ **IGMP**(Internet Group Management Protocol, 인터넷 그룹 관리 프로토콜)
하나의 라우터와 여러 호스트로 구성되는 서브 네트워크(Sub-Network) 상에서 멀티캐스트 전송을 할 때, 어느 호스트가 멀티캐스트 전송을 받을지 정보를 전달하는 프로토콜
여러 호스트 중 멀티캐스트 전송을 받을 호스트로만 선택해 전송하기 때문에, 트래픽 낭비를 방지할 수 있다.

**문 2. 공격 유형에 관한 설명으로 옳지 않은 것은?**

① 사회공학적 공격은 신뢰 관계나 인간의 심리를 이용하여 중요한 정보를 획득하는 것이다.
② 무차별(brute force) 공격은 특정 값을 찾아내기 위해 가능한 모든 조합을 시도하는 공격이다.
③ 스니핑은 네트워크상에서 다른 사용자들의 트래픽을 도청하는 것이다.
④ 재연(replay) 공격은 두 개체 간의 패킷을 중간에서 가로채서 변조하여 전송함으로써 정당한 사용자로 가장하는 공격이다.

답 ④

④ 스푸핑(spoofing)에 대한 설명이다.
재연(replay) 공격(재전송 공격)은 공격자가 네트워크상에 흐르는 메시지 스트림을 복사해두었다가, 나중에 재전송하는 공격이다.

**문 3. 외부와 내부 네트워크의 경계에서 기본적인 패킷 필터링 기능만을 제공하는 데 적합한 네트워크 보안 구성은?**

① 스크리닝 라우터
② 스크린드 호스트 게이트웨이
③ 스크린드 서브넷 게이트웨이
④ 응용레벨 게이트웨이

답 ①

① **스크리닝 라우터**(Screening Router)
외부 네트워크와 내부 네트워크의 경계에 놓이며, 보통 일반 라우터에 패킷 필터링 규칙을 적용하여 3, 4계층 사이에서 방화벽 역할을 수행

**<오답 체크>** ② **스크린드 호스트 게이트웨이**(Screened Host Gateway)
라우터와 방화벽을 구분하여 운영
스크리닝 라우터와 듀얼 홈드 게이트웨이의 조합
외부에서 내부로 들어오는 트래픽을 외부 네트워크와 연결된 스크리닝 라우터에서 패킷 필터링을 함으로써 1차 방어를 한 뒤, 내부 네트워크와 연결된 베스천 호스트에서 2차 방어를 함

③ **스크린드 서브넷 게이트웨이**(Screened Subnet Gateway)
외부 네트워크와 내부 네트워크 사이에 서브넷(Subnet)이라는 완충지대를 두며, 서브넷에는 주로 DMZ와 방화벽이 위치한다.
내부 네트워크와 서브넷 사이에 스크리닝 라우터 1개, 외부 네트워크와 서브넷 사이에도 스크리닝 라우터 1개, 총 2개의 스크리닝 라우터가 들어간다.

④ **응용 레벨 게이트웨이**(Application Level Gateway)
프록시(proxy) 기능을 적용하여, 내부와 외부 간의 응용 계층의 모든 트래픽에 대해 인증 기능을 제공

**문 4. 스위칭 환경에서의 스니핑 기법이 아닌 것은?**

① ICMP 리다이렉트
② 스위치 재밍(jamming)
③ ARP 리다이렉트
④ TCP 세션 하이재킹

답 ④

④ **TCP 세션 하이재킹**(TCP Session Hijacking)
시스템에 접근할 적법한 사용자 아이디와 패스워드를 모를 때, 이미 시스템에 접속되어 세션이 연결되어 있는 사용자의 세션을 가로채어, 인증 절차를 거치지 않고 서버에 접속하여 공격 대상인 척 행세한다.

**<오답 체크>** ① **ICMP 리다이렉트**(또는 ICMP 스푸핑)
공격자는 공격 대상에게 ICMP 리다이렉트 메시지를 보내, 자신이 공격 대상의 게이트웨이 역할을 하게 만든다. 그러면 공격 대상이 보내는 메시지는 게이트웨이인 공격자를 통하게 되므로 스니핑이 가능해진다.
ARP 스푸핑은 모든 패킷에 대해 중간에서 리다이렉트를 하는 반면, ICMP 리다이렉트는 특정 목적지 주소를 가진 패킷만 선택해서 리다이렉트하는 게 가능하다.

② **스위치 재밍**(jamming)
위조된 MAC 주소를 지속적으로 보내 스위치가 관리하는 매핑 테이블을 넘치게 만드는 스니핑 기법이다.
스위치는 매핑 테이블이 가득 차게 되면, 스위치는 브로드캐스팅(broadcasting) 모드로 전환하게 되어 스니핑이 가능해진다.

③ **ARP 리다이렉트**(ARP Redirect)
공격 대상이 접속하는 라우터의 MAC 주소를 알아내어, 공격자는 공격 대상에게 자신이 라우터라고 속여, 공격 대상과 라우터 사이의 정보들을 스니핑하는 것이다.

▶ **ARP 스푸핑**(ARP Spoofing)
공격자가 자신의 MAC 주소를 공격 대상의 MAC 주소로 바꾸어 마치 자신이 공격 대상인 척 속이는 공격이다.

**문 5. 다음의 ㉠ ~ ㉢에 들어갈 용어를 바르게 연결한 것은?**

> 무선 랜에서의 프라이버시 강화를 위하여 IEEE 802.11에서 ( ㉠ )를 정의하였으나, 이 표준에서 무결성 보장과 키 사용의 심각한 약점이 발견되었다. ( ㉡ )에서 이를 개선할 목적으로 IEEE 802.11i의 초안에 기초한 중간 조치로 ( ㉢ )를 공표하였고, 이후 IEEE 802.11i 전체 표준을 따르는 새로운 보안 대책이 등장하게 되었다.

| ㉠ | ㉡ | ㉢ |
|---|---|---|
| ① WPA | Wi-Fi Alliance | WPA2 |
| ② WPA | IETF | WPA2 |
| ③ WEP | Wi-Fi Alliance | WPA |
| ④ WEP | IETF | WPA |

**답 ③**

WPA(Wi-Fi Protected Access, 와이파이 보호 접속)은 이전의 WEP(Wired Equivalent Privacy, 유선 동등 프로토콜)의 취약점 때문에 그 대안으로 나온 것으로, Wi-Fi alliance(와이파이 얼라이언스)가 책정한 보안 프로토콜이다.

**WEP** 방식
암호화를 위해 RC4 사용하며(암호키 계속 사용)
암호화와 인증에 동일한 키를 사용
**WPA** 방식
RC4-TKIP를 통한 암호화(암호키 주기적인 변경)
EAP를 통한 사용자 인증
48비트 길이의 초기벡터(IV) 사용
**WPA2** 방식
AES-CCMP 사용
EAP를 통한 사용자 인증

**문 6. 거리 벡터가 아닌 링크 상태를 활용하는 자율시스템(autonomous system) 도메인 내의 라우팅 프로토콜은?**

① RIP(Routing Information Protocol)
② OSPF(Open Shortest Path First)
③ BGP(Border Gateway Protocol)
④ IGRP(Interior Gateway Routing Protocol)

**답 ②**

◈ IGP(Interior Gateway Protocol, 내부 게이트웨이 프로토콜)
같은 자율 시스템 내부에서만 라우팅 정보를 교환하는 프로토콜
▷ RIP(Routing Information Protocol, 라우팅 정보 프로토콜)
- 단일 경로 라우팅 프로토콜
- **DVA(Distance Vector Algorithm, 거리 벡터 알고리즘)**을 이용해서 인접 호스트와의 경로를 동적으로 교환
- 소규모 또는 교육용 등 비교적 간단한 네트워크에 주로 사용
- 경로비용을 단지 홉 수(hop count)로만 판단
- 최대 홉 수 15로 제한
- 속도나 거리 지연 등을 고려하지 않아 최적의 경로 산정에 비효율적
- 라우팅 정보의 변화가 없더라도 매 30초 마다 자동으로 라우팅 정보를 브로드캐스팅하는데, 이는 트래픽에 부하가 줌

▷ IGRP(Interior Gateway Routing Protocol, 내부 게이트웨이 라우팅 프로토콜)
- 다중 경로 라우팅 프로토콜
- **DVA(거리 벡터 알고리즘)** 이용
- 경로비용을 다양한 요소를 이용하여 계산
- 90초마다 라우팅 정보를 갱신
- 홉수 255까지 지원, IP 사용

▷ **OSPF**(Open Shortest Path First)
- **링크상태 라우팅 프로토콜**
- 자치시스템(AS) 내부의 라우터들끼리(IGP) 라우팅 정보를 교환
- 최단 경로를 선택하기 위해 Dijkstra의 SPF(Shortest Path First) 알고리즘을 사용
- 링크 상태의 변화시에만 라우팅 정보를 전송

▷ 이 외 IGRP, IS-IS 등

◈ EGP(Exterior Gateway Protocol, 외부 게이트웨이 프로토콜)
다른 자율 시스템과도 라우팅 정보를 교환하는 프로토콜
▷ **BGP**(Border Gateway Protocol)
- 프로토콜자치시스템(AS) 상호 간에 적용되는 라우팅 프로토콜
- 순환을 피할 수 있도록 목적지까지 가는 경로 정보를 제공
- 발전된 거리 벡터 라우팅 프로토콜 또는 경로 벡터 라우팅 프로토콜
- BGP는 주기적으로 정보를 갱신하지 않고, 단지 변화가 있을때만, 이웃 라우터에게 갱신 정보 전송
- 네트워크 변화가 전혀 없으면 주고받는 정보가 없게 되는데, 이를 위해 자신이 살아있음을 알리는 BGP 킵얼라이브 메세지(BGP Keepalive Message)를 60초 마다 교환

**문 7. SSL(Secure Socket Layer)에서 서버와 클라이언트 간의 인증과 키 교환 메시지를 주고받는 프로토콜은?**

① Record
② Handshake
③ Change Cipher Spec
④ Alert

**답 ②**

**SSL/TLS 구조**

- 핸드셰이크 프로토콜(handshake protocol)
  서버와 클라이언트가 서로를 인증하고 암호, MAC알고리즘 레코드 데이터 보호에 사용될 암호화 키를 협상
- 암호 사양 변경 프로토콜(change cipher spec protocol)
  핸드쉐이크 프로토콜의 일부로 암호 방법을 변경
- 경고 프로토콜(alert protocol)
  에러 코드를 전송
- 애플리케이션 데이터 프로토콜(application data protocol)
  HTTP를 포함한 다양한 상위계층의 보안 서비스 제공
- 레코드 프로토콜(record protocol)
  SSL의 실제 데이터를 다루며, Data를 단편화 및 압축하고 MAC을 적용하고 암호화하여 이를 TCP에 전달

**문 8. 클라이언트가 위조된 웹사이트에 접속하게 하는 것을 목적으로 하는 공격 기법은?**

① DNS 스푸핑
② ARP 스푸핑
③ 스니핑
④ SYN flooding

**답 ①**

① **DNS 스푸핑**(DNS spoofing) 공격
공격 대상자가 접속하려는 URL 주소 이름을 요청할 때, 거짓 IP 주소를 반환하여 사용자가 의도하지 않은 주소로 접근하게 만드는 공격이다.
위조된 웹사이트로 접속하게 유도하여 개인정보를 빼내는 것이 목적이다.
DNS 스푸핑을 하는 방법에는 스니핑을 통해 DNS 서버보다 먼저 거짓 응답을 사용자에게 전달하는 방법, 대상자의 PC에 저장된 host파일을 수정하는 방법, DNS 서버 가진 IP 주소 자체를 변조시키는 방법 등이 있다.

**<오답 체크>** ② **ARP 스푸핑**(ARP spoofing)
ARP테이블 내의 공격 대상자의 MAC주소를 공격자의 MAC주소로 바꾸어, 공격자가 공격 대상자 행세를 하는 것이다.
ARP 스푸핑은 공격 대상자로 보내지는 패킷을 가로채 스니핑을 하는 것이 목적이다.

③ **스니핑**(sniffing)
네트워크 상에서 자신이 아닌 다른 상대방들의 패킷 교환을 엿듣는 것을 말한다.

④ **SYN flooding**
TCP 3-way handshaking을 이용한 DoS공격으로, 공격 대상 서버에 무수히 많은 SYN패킷을 보낸 뒤, 서버로부터 오는 SYN+ACK패킷을 무시하여, 서버가 SYN Received 상태로 끊임없이 기다리게 만드는 공격이다.
서버의 자원을 낭비시키고 가용성을 떨어뜨려 서비스 불능 상태에 빠뜨리는 것이 목적이다.

**문 9. 네트워크상의 호스트를 발견하고 그 호스트가 제공하는 서비스와 사용하는 운영체제 등을 탐지할 목적으로 고든 라이언에 의해 개발된 네트워크 스캐닝 유틸리티로, TCP Xmas 스캔과 같은 스텔스 포트 스캐닝에 활용되는 것은?**

① ping
② netstat
③ nmap
④ nbtstat

**답 ③**

③ nmap(network mapper)은 스캐닝 프로그램으로 운영 체제, 장치 종류, 운영 시간, 서비스에 쓰이는 소프트웨어 제품, 그 제품의 정확한 버전, 방화벽 기술의 존재와 네트워크 카드의 공급자 등의 컴퓨터 정보를 알아낼 수 있다.

**<오답 체크>** ① ping은 IP 네트워크를 통해 특정한 호스트가 도달할 수 있는지의 여부를 테스트하는 데 쓰이는 컴퓨터 네트워크 도구

② netstat는 네트워크의 연결상태, 네트워크 인터페이스 상태를 확인하는 명령어이다.

④ nbtstat(NetBIOS over TCP/IP state)는 NetBIOS가 사용하는 통계 및 이름 정보를 표시하는 명령어이다.

**문 10. 유닉스 시스템의 'traceroute'가 발신지에서 목적지까지의 패킷 전달 경로를 추적하는 과정에서 사용하지 않는 것은?**

① ICMP
② TCP
③ UDP
④ IP 패킷의 TTL(Time To Live) 필드

**답 ②**

tracert(traceroute) 명령어는 특정 IP에 도달할 때까지의 전체 경유 경로 내역을 보여준다.
ICMP 와 IP 헤더의 TTL필드를 사용한다.
TTL 필드의 목적은 데이터그램이 전송 도중 무한 라우팅 루프에 빠지는 것을 방지하기 위한 것으로 초기값은 64로 설정되어 있다. 라우터 하나를 거칠 때마다 TTL 필드값은 1씩 줄어드는데, 라우터는 TTL필드가 0또는 1인 IP 데이터그램을 받았다면 그 데이터그램을 포워드하지 않는다.
대신에 라우터는 데이터그램을 버리고 원래 호스트에게 ICMP 메시지에 '시간초과(time exceeded)'를 알리는데, 이를 통해서 데이터그램이 네트워크상에서 계속 떠돌게 되는 루프 현상을 방지할 수 있다.
또한 traceroute는 목적지 호스트가 사용하지 않은 것 같은 UDP 포트 번호 (30,000 보다 큰 값)를 선택하여 데이터그램을 보내는데, 데이터그램이 목적지에 도달하면 적절한 포트 번호가 아니기 때문에 UDP 모듈이 ICMP 'port unreachable' 에러를 발생시킨다. 이를 통해 ICMP 패킷이 목적지에 도달했다는 걸 확인할 수 있다.

**문 11. DMZ(demilitarized zone) 네트워크내에 일반적으로 두지 않는 것은?**

① 웹 서버
② 이메일 서버
③ DNS 서버
④ 내부 접속용 데이터베이스 서버

**답 ④**

DMZ(demilitarized zone, 비무장지대) 네트워크
내부 방화벽과 외부 방화벽 사이에 위치한 서브넷
내부 네트워크와 외부 네트워크가 DMZ로 연결할 수 있도록 허용하면서도, DMZ 내의 컴퓨터는 오직 외부 네트워크에만 연결되어 있고, 내부 네트워크로 연결할 수 없다.
이것은 DMZ 안의 호스트의 침입으로부터 내부 네트워크를 보호하면서, 외부 네트워크로 서비스를 제공할 수 있도록 한다.
DMZ 안의 호스트는 메일서버, 웹 서버, DNS 서버 등 외부 이용자에게 서비스를 제공하는 서버들이 포함된다.

④ 내부 접속용 데이터베이스 서버는 외부 이용자들에게 서비스를 제공할 필요도 없고, 오히려 외부 공격자들로부터 보호해야 하기 때문에 내부 방화벽 안쪽에 위치해야 한다.

**문 12. 다음 설명에 해당하는 네트워크 장비가 바르게 연결된 것은?**

(가) 두 개 이상의 LAN을 하나로 연결하는 장치
(나) 여러 대의 컴퓨터를 손쉽게 연결할 수 있도록 여러 개의 입력과 출력 포트를 가지고 있으며, 한 포트에서 수신된 신호를 다른 모든 포트로 재전송하는 장치
(다) 이종 통신망 간에도 프로토콜을 변환하여 정보를 주고받을 수 있는 장치
(라) 패킷의 수신 주소를 토대로 경로를 정해서 패킷을 전송함으로써 둘 이상의 네트워크를 연결하는 장치

| | (가) | (나) | (다) | (라) |
|---|---|---|---|---|
| ① | 브리지 | 허브 | 라우터 | 게이트웨이 |
| ② | 브리지 | 허브 | 게이트웨이 | 라우터 |
| ③ | 허브 | 브리지 | 게이트웨이 | 라우터 |
| ④ | 허브 | 브리지 | 라우터 | 게이트웨이 |

**답 ②**

(가) 동일한 프로토콜을 사용하는 LAN을 연결하는 장치
-> **브리지(bridge)**
(나) 여러 대의 컴퓨터를 연결, 모든 포트로 재전송
-> **허브(hub)**
(다만, 더미 허브(dummy hub)는 모든 포트로 재전송(브로드캐스팅)하지만,
스위칭 허브(switching hub, 보통 스위치라고 부른다)의 경우는 MAC 주소를 사용해 해당 포트로만 전송한다.)
(다) 이종 통신망 간에도 프로토콜을 변환
-> **게이트웨이(gateway)**
(라) 경로를 정해서, 둘 이상의 네트워크를 연결
-> **라우터(router)**

**문 13. IPv4의 주소 부족 현상을 해결하기 위한 접근 방법이 아닌 것은?**

① NAT ② SNMP
③ IPv6 ④ DHCP

**답 ②**

② SNMP(Simple Network Management Protocol, 간이 망 관리 프로토콜)
IP 네트워크상의 장치로부터 정보를 수집 및 관리하며, 또한 정보를 수정하여 장치의 동작을 변경하는 데에 사용되는, 네트워크를 모니터링하는 프로토콜이다.

IP 주소 고갈 문제를 해결하기 위한 방법
- IPv6
- NAT(Network Address Translation): 공인 IP 주소를 다수가 함께 공유하여 사용
- DHCP(Dynamic Host Configuration Protocol, 동적 호스트 구성 프로토콜)

IPv4와 IPv6 전환 기술
- 터널링(Tunneling): IPv4 망에 터널을 만들어 IPv6가 지나갈 수 있게 하는
- 듀얼 스택(Dual Stack): 하나의 시스템에서 IPv4와 IPv6프로토콜을 함께 처리
- 헤더 변환(Header Translation) IPv4와 IPv6 사이의 헤더 변환

**문 14. 패킷 재조합의 문제를 악용하여 오프셋이나 순서가 조작된 일련의 패킷 조각들을 보냄으로써 자원을 고갈시키는 서비스 거부(DoS) 공격은?**

① Land
② Teardrop
③ SYN flooding
④ Smurf

**답 ②**

② **Teardrop**, Bonk, Boink 공격은 신뢰성을 제공하는 프로토콜의 취약점을 이용한 DoS공격으로, 패킷의 순서번호를 조작하는 공격이다.
목표 대상 시스템은 이렇게 보내진 패킷들을 재조합하려고 시도하지만, 계속 실패하여 시스템 자원이 고갈되어 서비스 불능 상태에 빠진다.
- Teardrop 공격은 UDP를 이용하여 패킷의 순서번호가 서로 중복되도록 조작하는 공격
- Bonk 공격은 패킷의 순서번호를 모두 1로 조작하여 보내는 공격
- Boink 공격은 패킷의 순서번호를 처음에는 순서대로 보내다가 중간부터 반복되는 순서번호를 보내는 공격이다.

**<오답 체크>** ① **Land 공격**(Land Attack)은 패킷의 출발지 IP 주소와 목적지 IP 주소 값을 모두 공격자의 IP 주소 값으로 만들어 전송하는 공격이다.
출발지 주소와 목적지 주소가 같기 때문에 이 패킷은 공격대상을 떠났다가 그대로 다시 공격대상에게 들어가는데, SYN Flooding 처럼 동시 사용자 수를 점유해버리며, CPU 자원을 고갈시킨다.

③ **SYN flooding**
TCP 3-way hancshaking을 이용한 DoS공격
공격 대상 서버에 존재하지 않는 IP 주소로 위조한 무수히 많은 SYN패킷을 보낸 뒤, 서버로부터 오는 SYN+ACK패킷을 무시하여, 서버가 SYN Received 상태로 끊임없이 기다리게 만드는 공격방법이다.

④ **Smurf**(ICMP flooding)
공격대상 호스트의 IP주소로 위장된 소스 IP주소의 ICMP Echo 메시지를 브로드캐스트함으로써, 공격대상이 많은 양의 ICMP Echo 응답 패킷을 받아 시스템의 자원을 고갈된다.

**문 15. IEEE 802.11i RSN(Robust Security Network) 동작 단계에 대한 설명으로 옳지 않은 것은?**

① 발견 단계에서는 STA(Station)와 AP(Access Point)가 서로를 인지하여 일련의 보안 능력에 합의하고, 해당 보안 능력을 이용하여 향후 통신에 사용할 연관을 설정한다.
② 인증 단계에서는 STA와 AS(Authentication Server) 간의 상호 인증을 위하여 EAP(Extensible Authentication Protocol)를 교환한다.
③ 키 관리 단계에서는 STA와 AP간에 사용되는 한 쌍의 쌍별 키와 멀티캐스팅 통신에 사용되는 그룹 키가 정의된다.
④ 보호 데이터 전송 단계에서는 CRC(Cyclic Redundancy Check)로 메시지 인증과 데이터 기밀성을 제공한다.

**답 ④**

④ IEEE 802.11 초기 버전에서는 CRC를 통해 메시지를 인증하였으나 이후 보안에 문제가 발견되어, 802.11i에서는 TKIP와 CCMP 알고리즘을 이용한다.

◈ IEEE 802.11i 동작 단계
▷ 1단계: 탐색(Discovery) 단계
보안 정책을 브로드캐스트
STA(Staion, 단말기)는 이 메시지로 현재 통신을 원하는 WLAN의 AP(Access Point, 액세스 포인트)를 찾아, AP와 연관 설정, 연관을 이용해서 암호 도구와 인증 메커니즘을 선택
▷ 2단계: 인증(Authentication) 단계
STA와 AS(Authentication Server, 인증 서버)는 자신의 ID를 상호 인증, ESP 교환
AP는 STA와 AS 사이의 통신을 전달만 할 뿐 인증에는 참여하지 않음
▷ 3단계: 키 생성 및 분배(Key Generation and Distribution) 단계
AP와 STA는 몇 개의 동작을 통해 암호키를 생성하고AP와 STA에 키를 배치
프레임은 AP와 STA끼리만 교환
▷ 4단계: 안전 데이터 전송(Protected Data Transfer)
STA와 종단 지국은 AP를 통해 프레임을 교환
**TKIP**(Temporal Key Integrity Protocol, 임시 키 무결성 프로토콜) 또는 **CCMP**(Counter Mode-CBC MAC Protocol, 카운터 모드 CBC MAC 프로토콜) 이용
안전한 데이터 전송은 STA와 AP 사이에서만 이루어짐
종단-대-종단 전체에 보안이 제공되는 게 아님
▷ 5단계: 연결 중단(Connection Termination) 단계
안전한 연결이 해제되고 연결은 원래의 상태로 환원

**문 16. 128.23.16.0/20이 시작 주소인 IP 주소 블록을 동일한 크기의 8개 주소 블록으로 나눌 경우 얻어지는 서브넷의 시작 주소로 옳은 것은?**

① 128.23.0.0/23
② 128.23.2.0/23
③ 128.23.20.0/23
④ 128.23.32.0/23

**답 ③**

'128.23.16.0/20'의 의미는, 전체 32비트 IP 주소 중 앞의 20비트가 네트워크 식별자(networkid)이다.
128.23.16.0을 2비트로 바꾸면
'**10000000 . 00010111 . 0001** 0000 . 00000000'이다.
(굵은 부분인 앞의 20비트가 네트워크 식별자)
이것을 8개의 서브넷으로 나눈다면, 네트워크 식별자 뒤에 3비트를 추가해서 총 23비트까지가 서브넷 마스크가 된다.
따라서 서브넷으로 가능한 네트워크 식별자는 다음의 8개이다.
(세 번째 옥탯만 표시하고 나머지는 *로 표시)
*.*. **0001 000** 0 .* (16)
*.*. **0001 001** 0 .* (18)
*.*. **0001 010** 0 .* (20)
*.*. **0001 011** 0 .* (22)
*.*. **0001 100** 0 .* (24)
*.*. **0001 101** 0 .* (26)
*.*. **0001 110** 0 .* (28)
*.*. **0001 111** 0 .* (30)

**문 17. 윈도우즈 시스템에서 "route PRINT -4" 명령을 실행한 결과로 표현되는 정보가 아닌 것은?**

① 네트워크 마스크
② 게이트웨이
③ TCP/UDP 포트
④ 인터페이스

**답 ③**

③ 현재 내 컴퓨터에 연결 중이거나 연결 대기중인 포트를 확인하는 명령어는 'netstat' 명령어이다.

**'route'**는 라우팅 테이블에 대한 정보를 표시하는 명령어이다.
PRINT 옵션은 경로를 인쇄하는 옵션이며, -4는 IPv4를 이용하여 경로를 나타내는 옵션이다.
IPv4 경로 테이블에 표시되는 정보는 다음과 같다.
네트워크 대상(Network Destination)
패킷이 전달될 목적지 주소
네트워크 마스크(Netmask)
네트워크 목적지를 구별하기 위한 서브넷 마스크
게이트웨이(Geteway)
인터페이스를 빠져 나간 패킷이 전달될 주소
인터페이스(Interface)
네트워크 목적지가 일치하는 패킷이 전달될 인터페이스 카드의 IP 주소
메트릭(Metric)
목적지까지의 라우터 경로 수, hop(홉 수)

**문 18. UDP(User Datagram Protocol)의 헤더 포맷에 포함되어 있는 필드는?**

① 시퀀스 번호(sequence number)
② 목적지 IP 주소(destination IP address)
③ 체크섬(checksum)
④ 헤더 길이(header length)

**답 ③**

③ UDP는 순서제어 기능이 없기 때문에, 순서번호(sequence number)가 필요 없다.
▶ UDP 헤더 패킷
- Source Port(송신자 포트)
- Destination Port(목적지 포트)
- Length(길이)
- Checksum(체크섬, 검사합)
  데이터가 전송 중에 손상되지 않고 원본과 동일한지 여부를 확인하는 기능

UDP(User Datagram Protocol)
- 비연결형, 신뢰성이 없음, 순서화되지 않은 데이터그램(Datagram) 서비스 제공
- 메세지가 제대로 도착했는지 확인하지 않음 (확인응답 없음)
- 수신된 메세지의 순서를 맞추지 않음(순서제어 없음)
- 흐름 제어를 위한 피드백을 제공하지 않음 (흐름제어 없음)
- checksum(검사합)을 제외한 특별한 오류 검출 및 제어 없음 (기본적인 오류검출 기능만 함)
- 그러므로, UDP를 사용하는 응용 프로그램에서 오류제어 기능을 스스로 갖추어야 함
- 데이터그램 지향의 전송계층용 프로토콜 (논리적인 가상회선 연결이 필요 없음)
- 실시간 응용 및 멀티캐스팅 가능
- 빠른 요청과 응답이 필요한 실시간 응용에 적합
- 여러 다수 지점에 전송 가능(1:다(多) 전송)
- 헤더가 단순함, 헤더 크기 8 바이트(TCP는 20 바이트)
- UDP 위에서 동작되는 다양한 프로토콜들 또는 응용분야
  TFTP, SNMP, DHCP, NFS, DNS, RIP, NTP, RTP 등

**문 19. IPsec에 대한 설명으로 옳지 않은 것은?**

① 전송모드에서 AH(Authentication Header)는 IP 페이로드와 IP 헤더의 선택된 부분을 인증한다.
② 전송모드에서 ESP(Encapsulating Security Payload)는 IP 헤더는 암호화하지 않고 IP 페이로드를 암호화한다.
③ 터널모드에서는 패킷 암호화를 지원하는 ESP와 인증을 제공 하는 AH가 같이 사용되어야 한다.
④ IKE(Internet Key Exchange) 프로토콜을 사용하여 보안 연관 (Security Association)을 설정한다.

**답 ③**

③ 전송 모드에서는 AH 단독 사용, ESP 단독 사용, AH+ESP 함께 사용이 가능하지만,
터널 모드에서는 AH 단독 사용, ESP 단독 사용은 가능하지만, **AH+ESP 함께 사용은 불가능하다.**

**<오답 체크>** ① 전송 모드에서 AH는 IP 페이로드와 IP 헤더 일부를 인증하며,
터널 모드에서 AH는 내부 IP 패킷 전체(헤더+페이로드)를 인증하고, 외부 헤더 일부를 인증한다.

② 전송 모드에서 ESP는 IP 페이로드만 암호화하지만,
터널 모드에서 ESP는 내부 IP 패킷 전체를 암호화한다.

④ Internet Key Exchange(IKE, 인터넷 키 교환)
RSA와 디피 헬만 등의 공개키 기술을 기반으로, 암호화에 사용할 세션키를 관리하고 SA(Security Association, 보안 연계)를 협의하기 위한 프로토콜

**문 20. ARP(Address Resolution Protocol)에 대한 설명으로 옳지 않은 것은?**

① ARP는 논리 주소를 물리 주소로 변환해준다.
② ARP 패킷에는 발신자와 해당 수신자의 물리 주소와 논리 주소가 포함된다.
③ ARP 패킷은 데이터링크 프레임에 캡슐화된다.
④ 같은 네트워크상에서 ARP 요청 패킷과 ARP 응답 패킷은 브로드캐스트 된다.

**답 ④**

④ 송신자는 연결하기 원하는 IP 주소에 해당하는 MAC 주소를 알기 위해, 같은 도메인 내의 모든 호스트들에게 **ARP 요청 패킷(ARP request packet)에 IP 주소를 담아 브로드캐스트**한다.
ARP 요청 패킷을 받은 호스트들은 자신의 IP 주소가 아니라면 무시하고, 자신의 IP가 맞는 호스트만 자신의 MAC 주소를 담아 송신자에게 **ARP 응답 패킷(ARP reply packet)을 유니캐스트**(1대1 전송)한다.
ARP 응답 패킷을 받은 송신자는 ARP 테이블에 해당 IP 주소와 MAC 주소를 갱신하여 기록한다.

**<오답 체크>** ①② ARP(Address Resolution Protocol)은 논리 주소인 IP를 물리 주소인 MAC으로 매핑해주는 프로토콜이다.

③ ARP는 네트워크 계층의 IP 주소와 데이터 링크 계층의 MAC 주소를 다루기 때문에, 데이터링크 계층의 프레임에 캡슐화된다.