정보처리기술사 140회 대비

# 천기누설
# 핵심토픽 200제

## 네트워크
## (Network)

중급반

# NW

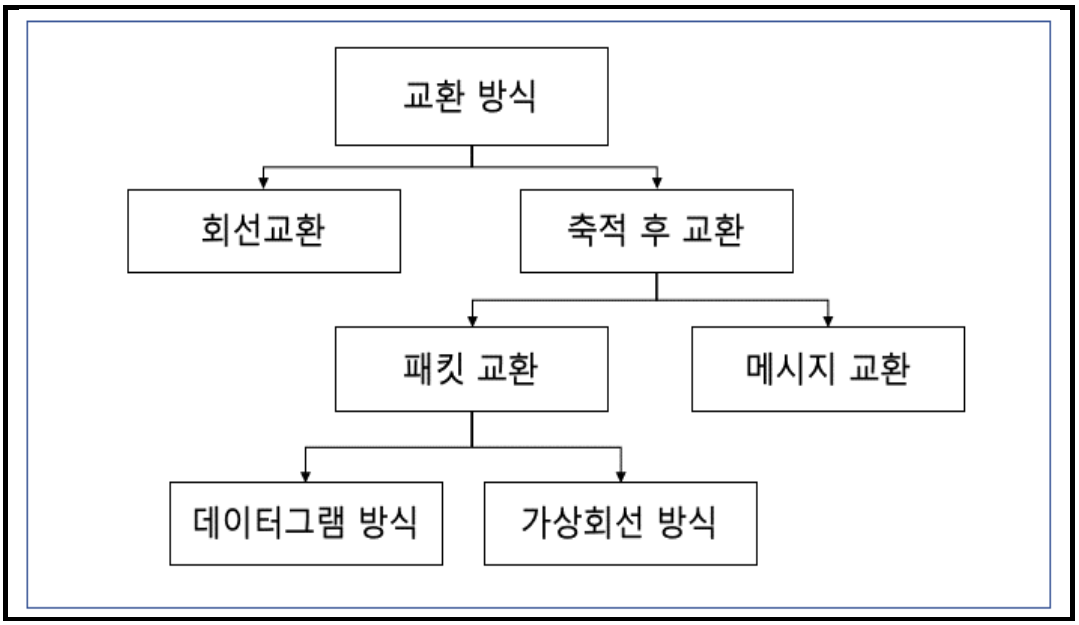
| NO.1 | NO.2 | 토픽명(대) | 토픽명(소) | 문제 | 출제 | 공통 | 번호 |
|---|---|---|---|---|---|---|---|
| 1 | 1 | 패킷 교환 | 회선교환, 패킷 교환 | 교환방식에 있어서 회선교환(Circuit Switching) 방식과 패킷교환(Packet Switching) 방식에 대하여 설명하고, 음성데이터나 영상데이터와 같은 실시간 트래픽 서비스를 패킷교환방식의 네트워크에서 제공하고자할 때 발생할 수 있는 문제점 및 해결방안에 대하여 설명하시오. | 120 | 컴시응 | 4 |
| 2 | 1 | NAT | NAT | NAT(Network Address Translation)의 핵심기능에 대하여 설명하시오. | 합숙_2019.01 | 공통 | Day-2 |
| 3 | 1 | OSI 7 Layer | OSI 7 Layer | ISO 7498이 필요한 이유와 각 계층별 역할 및 기능, 취급하는 자료 형태와 관련 장비에 대하여 설명하시오. | 120 | 컴시응 | 4 |
| | 2 | | 서비스 프리미티브 | 서비스 프리미티브(Service Primitive)에 대해 설명하시오. | 모의_2018.01 | 응용 | 1 |
| | 3 | | 스위치 | 네트워크 스위치(Network Switch)와 관련하여 다음을 설명하시오<br>(1) 스위치 개요<br>(2) OSI (Open System Interconnection) 참조 모델의 레이어에 따른 스위치 유형<br>(3) L4 스위치와 L7 스위치 비교 | 129 | 응용 | 3 |
| 4 | 1 | BEC, FEC | BEC, FEC | BEC와 FEC 를 비교하시오 | 합숙_2020.07 | 공통 | Day-4 |
| | 2 | | | 패킷 데이터의 송수신 과정의 후진오류수정 중 전송 데이터가 1011010, 디바이더(divider)가 1101 인 경우 CRC(Cyclic Redundancy Check) 값을 구하는 과정을 설명하시오. | 모의_2020.04 | 관리 | 2 |
| | 3 | | | 해밍코드에 관하여 아래의 내용에 대해 설명하시오.<br>가. 10110011O에 대한 해밍코드 후 데이터 값<br>나. '가' 의 데이터 수신 값에 대해 MSB 오류시 정정과정<br>(단, 해당 통신에서 Network byte Order 에 따라 수행하고, 짝수 패리티로 가정) | 모의_2017.06 | 응용 | 3 |
| | 4 | | | 데이터링크 계층은 네트워크에서 오류제어를 담당한다. 다음을 설명하시오.<br>가. 오류제어방식의 개념과 종류<br>나. 전진오류수정(FEC)과 검출 후 재전송(ARQ)방식 비교<br>다. ARQ 방식 3가지 | 125 | 응용 | 4 |
| 5 | 1 | ARP | ARP | ARP(Address Resolution Protocol)에 대하여 아래 사항들을 설명하시오.<br>가. ARP와 RARP<br>나. IP 프로토콜을 사용하는 서버 또는 네트워크 장비에서 ARP의 역할<br>다. ARP와 관련된 아래의 보안 취약점 및 이들의 대응 방안<br>1) ARP Spoofing<br>2) ARP Redirect | 116 | 컴시응 | 2 |
| 6 | 1 | IPv6 | IPv6 | IP 주소 부족문제를 해결하기 위한 IPv6에 대하여 아래 사항을 설명하시오.<br>가. IPv6 헤더구조<br>나. 패킷 단편화(fragmentation)에 대하여 설명하고, Ipv4와 Ipv6에서의 처리방식<br>다. 기존 IPv4망에서 IPv6망으로 전환하기 위한 방안 | 116 | 컴시응 | 4 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 7 | 1 | 라우팅 | 라우팅 | 네트워크 라우팅 기법 중 거리벡터라우팅(Distance Vector Routing)과 링크스테이트라우팅(Link State Routing) 기법을 설명하고, 두 기법의 차이점을 비교하시오. | 모의_2018.06 | 응용 | 3 |
| | 2 | | | 네트워크를 효율적으로 이용하기 위한 멀티캐스트의 개념과 멀티캐스트 라우팅 프로토콜 유형에 대해 설명하고, IGMP(Internet Group Management Protocol)의 동작 과정과 메시지 유형에 대하여 설명하시오 | 모의_2020.03 | 공통 | 2 |
| 8 | 1 | TCP 전송계층 | TCP, UDP, SCTP | TCP(Transmission Control Protocol)와 UDP(User Datagram Protocol) 프로토콜을 비교하여 설명하고, SCTP(Stream Control Transmission Protocol)을 상세하게 설명하시오. | 모의_2013.10 | 응용 | 4 |
| | 2 | | SCTP | SCTP(Stream Control Transmission Protocol)와 관련하여 다음을 설명하시오.<br>가. SCTP 개요와 특징<br>나. SCTP 프로토콜(Protocol) 구조 및 동작방식 | 132 | 관리 | 3 |
| | 3 | | TCP 제어 | TCP(Transmission Control Protocol)의 신뢰성 있는 전송을 가능케 하는 오류제어, 흐름제어, 혼잡제어에 대하여 설명하시오. | 120 | 컴시응 | 3 |
| | 5 | | TCP 전송계층 | 전송계층(Transport Layer)에서 전송 데이터의 단위는 Segment 이다. 전송계층 기능 중 흐름제어(Flow Control)에 대하여 다음을 설명하시오.<br>가. 흐름제어 방식 개념<br>나. 흐름제어 방식의 개념도<br>다. Sliding Windows와 Slow Start 비교 | 125 | 응용 | 3 |
| | 6 | | TCP 전송계층 | TCP 전송계층 프로토콜에 대하여 다음을 설명하시오.<br>가. TCP 전송계층 개념<br>나. 3-way handshake와 4-way handshake 설명<br>다. TCP와 UDP 비교 | 125 | 응용 | 3 |
| 9 | 1 | 수퍼네팅/서브네팅 | 수퍼네팅/서브네팅 | 네트워크 서브네팅(Subnetting)과 관련하여 다음을 설명하시오.<br>가. 슈퍼네팅(Supernetting)과 서브네팅(Subnetting) 개념<br>나. 192.168.0.0/22 네트워크 대역을 사용하여 인사팀 125 명, 영업팀 250 명, 보안팀 125 명, 개발팀 500 명이 사용할 수 있도록 4 개의 VLSM(Variable Length Subnet Mask)으로 분할한 각각의 Subnet Mask값과 할당 가능한 Host IP 대역 | 139 | 관리 | 4 |
| 10 | 1 | Multiple Access | Multiple Access | 데이터링크 계층에서 사용하는 다중 접근 프로토콜 (Multiple Access Protocol) 중 다음에 대하여 설명하시오<br>가. 임의 접근 프로토콜 (Random access protocols)<br>나. 제어 접근 프로토콜 (Controlled access protocols)<br>다. 채널화 프로토콜 (Channelization protocols) | 모의_2020.10 | 공통 | 4 |
| 11 | 1 | DHCP | DHCP | DHCP(Dynamic Host Configuration Protocol)의 구조와 동작 원리를 설명하시오. | 합숙_2019.01 | 응용 | Day-2 |
| 12 | 1 | DNS, DNSSEC | DNS, DNSSEC | 사물인터넷(IoT) 시대가 진입하면서 IoT Device기기를 이용한 DNS(Domain Name System)에 대한 공격과 피해가 급증하고 있다. 이와 관련하여 DNS(Domain Name System) 원리와 DNSSec(DNS Security Extensions)에 대하여 설명하시오. | 모의_2017.04 | 관리 | 2 |
| 13 | 1 | Ad-hoc | Ad-hoc 라우팅 | Ad-hoc Networking Routing Protocol | 119 | 컴시응 | 1 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 14 | 1 | QoS | IntServ, DiffSev | 네트워크 서비스 품질(QoS) 보장을 위한 기술 중 다음에 대해 설명하시오.<br>가. 패킷 처리 순서 결정을 위한 스케줄링 기술<br>나. 트래픽 처리량 제어를 위한 버킷(bucket) 기술<br>다. IntServ 모델과 DiffServ 모델 비교 | 모의 _2019.10 | 관리 | 4 |
| | 2 | | QoS | 네트워크 서비스 품질 향상을 위한 QoS(Quality of Service) 에 대하여 다음을 설명하시오.<br>가 . QoS 의 기술<br>나 . QoS 의 모델<br>다 . QoS 의 측정요소 | 모의 _2021.06 | 공통 | 4 |
| 15 | 1 | CDN | CDN | CDN(Contents Delivery Network)의 동작원리, 주요기술, 캐싱방식에 대해 설명하시오. | 합숙 _2020.01 | 응용 | Day-4 |
| 16 | 1 | HTTP | HTTP | HTTP 프로토콜을 설명하시오.<br>가. HTTP 프로토콜<br>나. QUIC 프로토콜<br>다. HTTP 프로토콜 3.0 과 2.0 비교 | 모의 _2021.05 | 공통 | 4 |
| 17 | 1 | SDN, NFV | SDN, NFV | 차세대 네트워크 기술로 부각되고 있는 SDN(Software Defined Network)과 NFV(Network Function Virtualization)의 구조와 특징을 비교 설명하시오. | 114 | 응용 | 3 |
| 18 | 1 | WiFi | Wi-Fi 7 | Wi-Fi 7 | 139 | 관리 | 1 |

| 6 | 교환방식 |
|---|---|
| 문제 | 교환방식에 있어서 회선교환(Circuit Switching)방식과 패킷교환(Packet Switching) 방식에 대하여 설명하고, 음성데이터나 영상데이터와 같은 실시간 트래픽 서비스를 패킷교환방식의 네트워크에서 제공하고자할 때 발생할 수 있는 문제점 및 해결방안에 대하여 설명하시오. |
| 도메인 | 네트워크 |
| 정의 | 회선교환 : 송수신 단말장치 사이에서 데이터를 전송할 때마다 통신경로를 설정하여 데이터를 교환하는 방식<br>패킷교환 : 일정한 크기의 데이터 블록인 패킷을 교환기가 수신측 주소에 따라 적당한 통신경로를 선택하여 전송하는 교환방식 |
| 키워드 | 회선교환, 독점, 1:1<br>패킷교환, 공유, MTU |
| 출제의도분석 | 패킷교환방식의 서비스 제공시 문제해결 능력 보유 여부 |
| 답안작성 전략 | 5G 시대 통신 시스템의 정보와 통신 채널, 부호화, 잡음, 연속메시지에 대한 다양한 통신 문제에 대한 해결 기법 모색 |
| 참고문헌 | 정보통신 기술용어해설(http://www.ktword.co.kr)<br>118 회 정보처리기술사 해설서(제 117 회 정보관리기술사, 조숙향 PE) |
| 풀이 기술사님 | 노정인 기술사 (제 119 회 컴퓨터시스템응용기술사 / 5nji5@naver.com) |

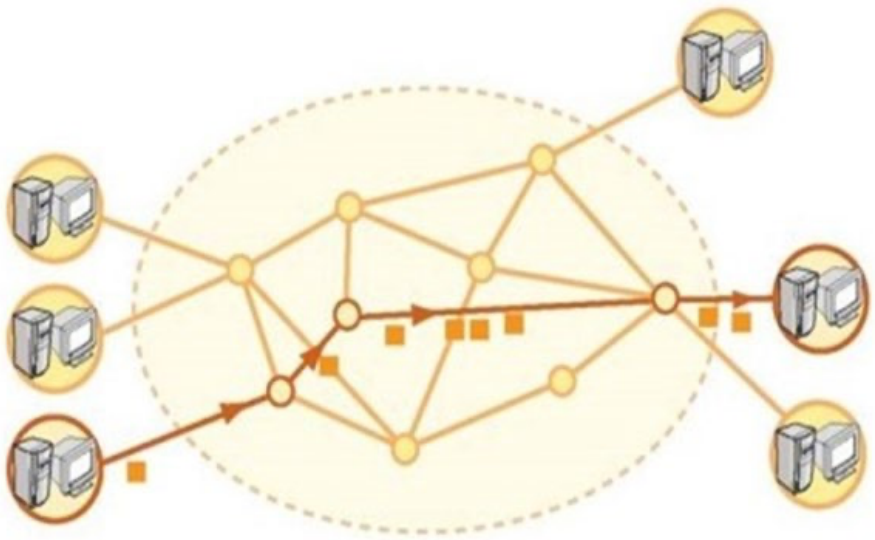
## 1. NW 장비간 정보교환방법, 교환방식의 개요



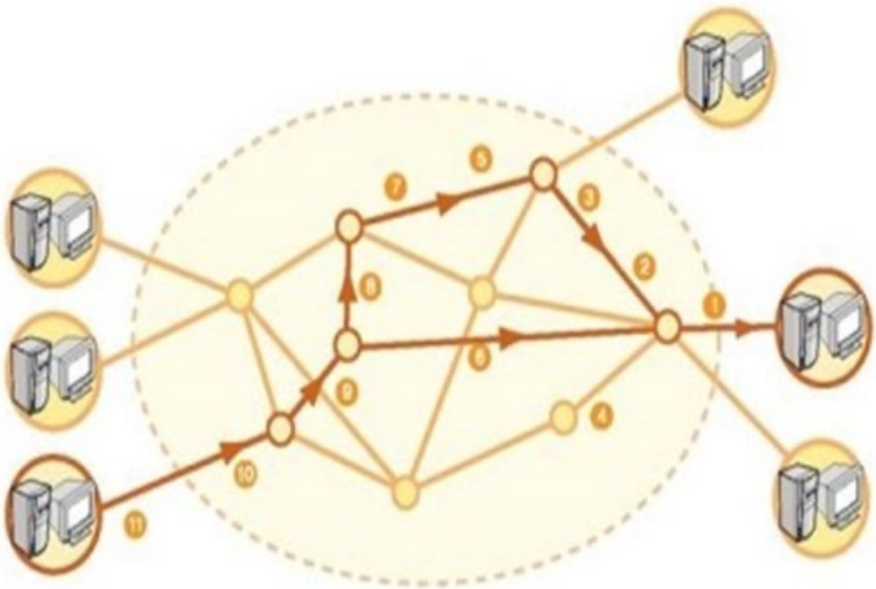

- 장비간 데이터교환방법으로 대표적으로 회선교환방식, 패킷교환방식 존재

## 2. 회선교환방식과 패킷교환방식에 대하여 설명

### 가. 회선교환방식에 대하여 설명

| 항목 | 설명 | |
|---|---|---|
| 개념도 |  | |
| 개념 | - 송수신 단말장치 사이에서 데이터를 전송할 때마다 통신경로를 설정하여 데이터를 교환하는 방식 | |
| 동작 원리 | 1. 회선설정 | - 데이터가 전송되기 전에 두 단말장치 간에 회선을 설정 |
| | 2. 데이터 전송 | - 연결후 1:1 의 안정적인 데이터 전송 |
| | 3. 회선 단절 | - 데이터 전송 완료 후 사용한 회선 자원 회수 |

### 나. 패킷교환방식에 대하여 설명

| 항목 | 설명 |
|---|---|
| 개념도 |  |
| 개념 | - 일정한 크기의 데이터 블록인 패킷을 교환기가 수신측 주소에 따라 적당한 통신경로를 선택하여 전송하는 교환방식 |

| | | |
|---|---|---|
| 기능 | 경로설정 | - 발신자와 목적지가 직접 연결되지 않으므로 각 패킷을 네트워크를 통해서 노드에서 노드로 보내는 기능 |
| | 트래픽제어 | - 네트워크에 전송되어지는 트래픽의 양을 효율적이고 안정하게 하기 위해서 통제하는 기능 |
| | 에러제어 | - 네트워크에서 유실되는 패킷에 대해 제어하는 기능 |

**다. 회선교환방식과 패킷교환방식 비교**

| 항목 | 회선교환방식 | 패킷교환방식 |
|---|---|---|
| 회선 효율성 | 전송전 회선 독점 | 회선 다중화로 효율증대<br>경제성 향상 |
| 신뢰성 | 독점사용<br>주변트래픽에 의한 회선 끊김없음 | 우회 기능 보유를 통한 신뢰성 확보 |
| Busy 시 | Busy 신호 | 전달 불가시 메시지 저장 |
| 메시지 저장 | 메시지 저장 안함 | 전달시까지 메시지 저장 |
| 데이터 길이 | 비교적 긴 데이터 전송 가능 | 데이터 단위의 길이가 제한됨 |
| 오버헤드 비트 | 없음 | 패킷마다 오버헤드 비트 존재 |
| 유형 | 공간분할 방식, 시분할 방식 | 데이터그램, 가상회선 방식 |
| 사례 | 전화망 | 인터넷망 |
| 장점 | 대용량+고속 데이터 처리 우수<br>고정적인 대역폭을 사용<br>연속적인 데이터 처리에 우수 | 회선의 이용률이 높음<br>애러 및 장애에 강함<br>다양한 통신망에서 사용가능 |
| 단점 | 대역폭 낭비<br>통신비용 고가 | 경로 탐색과정에서 지연이 발생<br>전송량 증가에 따른 지연율 상승<br>패킷헤더 추가 오버헤드 발생 |

## 3. 실시간 트래픽 서비스를 패킷교환방식의 네트워크에서 제공시 문제점 및 해결방안

**가. 실시간 트래픽 서비스를 패킷교환방식의 문제점**

| 항목 | 문제점 | 설명 |
|---|---|---|
| 성능 | 대역폭(Bandwidth) | - 실시간 트래픽 서비스를 위한 일정수준 이상의 대역폭 필요 |
| | 지연(Delay) | - 패킷 전송량 증가에 따른 지연율 상승 |
| | 패킷손실(Packet Loss) | - 정보가 원본에서 목적지로 전송하던 중 손실되는 현상 |
| | 지연변이(Delay Variation) | - 패킷 지연(Delay)이 일정하지 않고, 수시로 변하고, 패킷 간의 간격이 일정하지 않는 현상 |

| | | |
|---|---|---|
| 서비스 | 연결능력(Connectivity) | - 실시간 트래픽 서비스 연결에 의한 가용성 확보 필요 |
| | 신뢰성(Reliability) | - 실시간 트래픽 서비스의 실시간성, 저지연 |
| | 가용성(Availability) | - 트래픽 집중시에 실시간 트래픽 서비스사용이 가능하도록 구성 필요 |

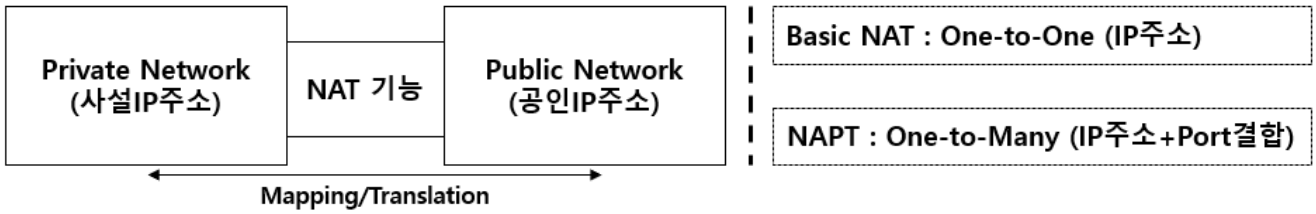
**나. 실시간 트래픽 서비스를 패킷교환방식의 네트워크에서 제공시 해결방안**

| 문제점 | 해결방안 | 설명 |
|---|---|---|
| 대역폭(Bandwidth) | 큰 대역폭 | - 큰 대역폭을 할당하여 실시간 트래픽 서비스 제공, 가장 근본적인 해결방법 |
| 지연(Delay) | 스케줄링<br>Queue | - 동기화, 타임스탬프(경과시간 수치값) 등<br>- FIFO, Priority, WRR, WFQ, DRR |
| 패킷손실(Packet Loss) | 혼잡제어, | - Open Loop, Closed Loop, |
| 지연변이(Delay Variation) | IntServ,<br>DiffServ | - 절대적 서비스품질, RSVP, T-Spec, R-Spec<br>- Classifier, Meter, Marker, Conditioner |
| 연결능력(Connectivity) | 버퍼 | - Session 유지 버퍼, Connection 유지 버퍼 |
| 신뢰성(Reliability) | MPLS | - 4Byte 헤더, 실시간 고속 스위칭 |
| 가용성(Availability) | CDN | - GSLB, 부하분산, 스트리밍, 동기화, 분산, 캐싱 |

"끝"

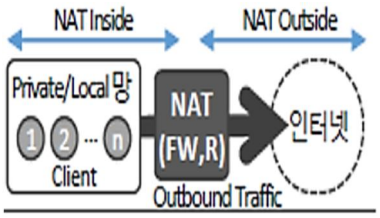
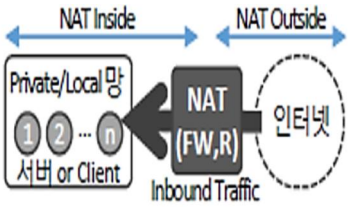
| 10 | NAT(Network Address Translation) | | |
|---|---|---|---|
| 문제 | NAT(Network Address Translation)의 핵심기능에 대하여 설명하시오. | | |
| 도메인 | 네트워크 | | |
| 출제배경/의도 | NAT 의 핵심 3 개 기능에 대한 이해여부와 116 회 DHCP 출제에 따른 고전 토픽 출제에 대한 대비 | | |
| 키워드 | NAT Binding Table(IP Mapping), 상호연결, IP Masquerading, Port Forwarding, Load Balancing | | |
| 목차예시 | 1. 네트워크 주소변환, NAT(Network Address Translation )의 개요<br>2. NAT 핵심기능 | | |
| 출제자 | 박재성 기술사(제 111 회 컴퓨터시스템 응용기술사 / kftc@naver.com) | 난이도 | ★ ★ ☆ ☆ ☆ |
| 참고문헌 | KPC 기출풀이 및 특강자료<br>http://www.e-infomax.com/ipmasq/howto-trans/kr/IP-Masquerade-HOWTO-2.html | | |

## 1. 네트워크 주소변환, NAT(Network Address Translation )의 개요

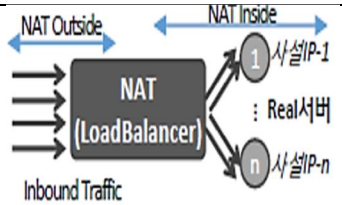



-NAT Binding Table(IP Mapping) 관리를 통해 Private 와 Public Network 간 상호연결 기능 제공

## 2. NAT 핵심기능

| 핵심기능 | 구성 | 설명 |
|---|---|---|
| IP Masquerading |  | -사설 IP 주소를 서버의 IP 로 가장하여 서버와 연결 되어 있는 네트워크 호스트와 함께 외부 인터넷 자원을 공유할 수 있는 기능 (리눅스 핵심기능)<br>- one-to-many변환(1 public IP : N private IP 매핑)<br>- Outbound Traffic 의 Source IP 와 Port 대상 변환 |
| Port Forwarding |  | -내부 네트워크에 대하여 Gateway 역할을 하는 서버의 특정 포트, 네트워크 연결이 들어오면 해당 연결을 내부 네트워크 네트워크의 특정 서버의 포트로 연결(Forward) 시켜주는 네트워킹 기능<br>- Inbound Traffic의 Destination Port 중심 동작<br>- Dest. Port 정보로 내부사설 IP(호스트) 식별 |
| Load Balancing | | |


Copyright ⓒ 2014 By Korea Productivity Center Convergence Knowledge Center. All rights reserved

| | | |
|---|---|---|
| |  | -하나의 인터넷 서비스에서 발생하는 트래픽이 많을 때 여러 대의 서버가 분산 처리하여 서버의 로드(부하) 증가, 부하량, 속도 저하 등을 해결하는 기술<br>- Inbound Traffic의 Destination Port 중심 동작<br>- 사설망 내 특정 서버로의 부하 집중 방지<br>: LoadBalancer의 Virtual IP + NAT 결합 활용 |

- NAT 기능은 one-to-many 변환 (1 public IP : N private IP 매핑)을 사용하는 NAPT 방식에 필수 사용
- NAT Binding(Mapping) Table 을 이용하여 Outbound 및 Inbound Traffic 주소변환 수행 끝.

**[기타자료] -NAT 유형**

| 유형 | 정리 | 설명 |
|---|---|---|
| Static NAT | 외부 IP 주소 : 내부 IP 주소 = 1 : 1 | -내부 IP 주소 하나에 외부 IP 주소 하나를 할당 |
| Dynamic NAT | 외부 IP 주소 : 내부 IP 주소 = m : n<br>(m>n 인 경우 일반적, 내부-> 외부) | -주로 외부 IP 보다 내부 네트워크의 실제 호스트 수가 적을 경우 , 또는 모든 내부 IP 주소를 일일이 외부용 IP 주소로 고정적으로 할당할 필요가 없을 경우 사용 |
| PAT | 외부 IP 주소 : 내부 IP 주소 = h : n<br>(h<n 인 경우 일반적, 내부-> 외부) | -하나 또는 하나 이상의 외부용 IP 주소를 여러 개의 내부 IP 주소들이 공유할 경우에 사용<br>-동일한 외부용 IP 주소로 변환이 되지만, Port 를 변환 사용 |
| LSNAT | 외부 IP 주소 : 내부 IP 주소 = 1 : n<br>(내부 <- 외부) | -Distributor NAT, 하나의 외부 IP 주소를 복수 개의 내부 IP 주소에 대응시켜, 외부 망에서 해당 IP 주소를 목적지로 하는 모드 세션을 할당된 각 내부의 IP 주소로 분산 변환 |

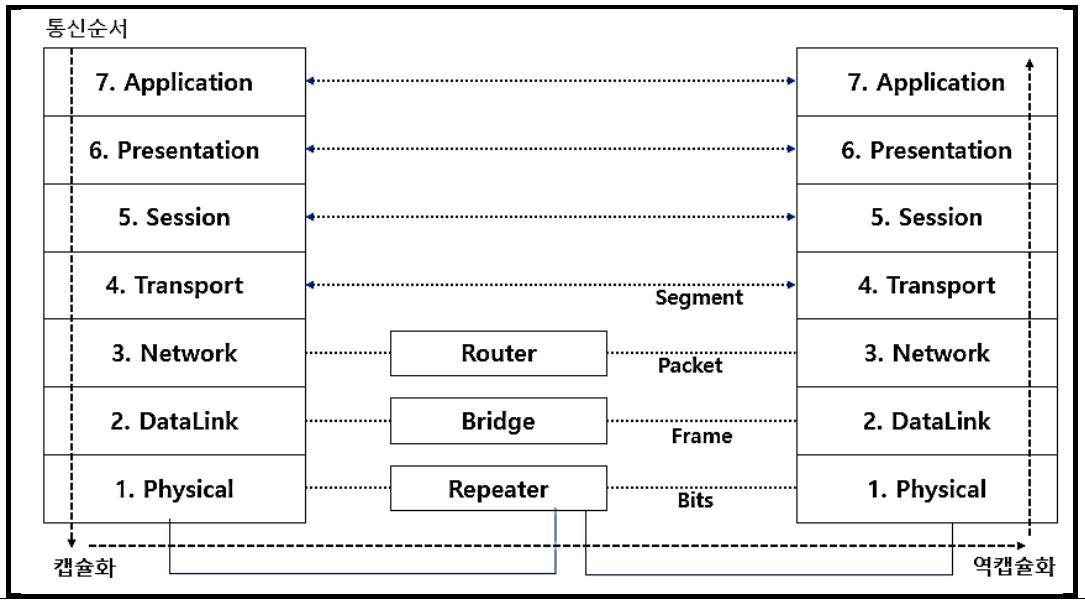
| 2 | OSI 7 계층 |
|---|---|
| 문제 | ISO7498 이 필요한 이유와 각 계층별 역할 및 기능, 취급하는 자료 형태와 관련 장비에 대하여 설명하시오. |
| 도메인 | 네트워크 |
| 정의 | OSI7 계층 : 개방형 시스템간의 상호접속하기 위한 참조모델(ISO7498) |
| 키워드 | ISO7498, OSI7 계층, 독립성 |
| 출제의도분석 | OSI 7 Layer 의 기본개념에 대한 이해 여부 확인 및 차별화 여부 |
| 답안작성 전략 | 답이 있는 문제이지만 실무경험 및 지식의 깊이에 따라 차별화가 가능한 문제, 실무에서 OSI7 계층이 사용되지 않는 이유, WAN 관점에서의 내용을 상세히 작성하여 추가 득점 가능 |
| 참고문헌 | 116 회 기출풀이 해설서(111 회 박재성 컴퓨터시스템응용기술사) |
| 풀이 기술사님 | 노정인 기술사 (제 119 회 컴퓨터시스템응용기술사 / 5nji5@naver.com) |

## 1. 개방형 시스템 상호접속 통신 참조모델 OSI 7 계층, ISO7498 이 필요한 이유

| | | |
|---|---|---|
| 개념 | - 모든 네트워크 통신에서 생기는 여러가지 충돌 문제를 완화하기 위하여 국제표준기구(ISO)에서 표준화된 네트워크 구조를 제시한 개방형 시스템 상호연결 기본 모델 | |
| 필요한 이유 | 통합 표준 | - 상호 이질적인 네트워크 간의 연결 지침 제공 |
| | 참조 모델 | - 네트워크 표준 개발, 의사소통 도구 |
| | 계층구조 | - 각 계층의 독립성 보장 |

## 2. 각 계층별 역할 및 기능

### 가. ISO7498 의 계층구조



- 각 계층마다 특정한 서비스를 제공하고, 이를 위한 각각의 프로토콜이 존재

**나. 각 계층별 역할 및 기능**

| 계층 | 계층명 | 역할 | 기능 |
|---|---|---|---|
| 7 | Application<br>(응용계층) | - 응용 프로세스간 정보교환,전자사서함, 파일전송 등 인터페이스 제공<br>- 사용자가 네트워크에 접근할 수 있는 계층<br>- HTTP, FTP, SMTP, Telnet | 데이터 의미/내용 제어서비스 제공 |
| 6 | Presentation<br>(표현 계층) | - 데이터 인코딩/디코딩, 암호화/복호화<br>- 입력/출력 데이터를 하나의 표현형태로 변환<br>- ASCII, MPEG,JPEG,MIDI | 표현양식 제어<br>포맷변환 |
| 5 | Session<br>(세션 계층) | - 통신 장비간의 연결관리<br>- 통신 세션을 구성하는 계층, 포트연결<br>- NetBIOS, SAP, SDP, NWlink | 대화 채널 제어 |
| 4 | Transport<br>(전송 계층) | - 송수신 시스템 간의 논리적 안정과 균일한 서비스 제공<br>- 종단간 신뢰성, 투명성 있는 데이터 전송제공<br>- 혼잡제어, 흐름제어, 오류제어<br>- TCP, UDP, ARP, RARP | 데이터 전송 제어 |
| 3 | Network<br>(네트워크 계층) | - 정보교환 및 중계기능, 경로선정, 흐름 제어<br>- 상위계층에 연결하는데 필요한 데이터 전송과 교환 기능을 제공<br>- 경로설정 기능<br>- IP, IPX, X25, ICMP, IGMP | 중계 제어 |
| 2 | Datalink<br>(데이터링크 계층) | - 정보전송, 전송오류 제어, 흐름제어 등 신뢰성있는 정보 전송 제공<br>- 물리적 링크를 통해 정보를 전송<br>- 접근제어, 회선제어<br>- Ethernet, Token Ring, HDLC, LLC,PPP, MAC | 전송 오류 제어 |
| 1 | Physical<br>(물리 계층) | - 전송매체에서의 전기신호 전송 기능, 제어 및 클럭 신호등 제공<br>- 비트 스트림을 전송매체 통해 제공<br>- RS232C, RS449/442/423 | 전기 신호 |

- 각 계층마다의 기능과 역할을 수행하고 서로 영향을 미치지 않는 상호 독립성을 제공

### 3. 취급하는 자료 형태와 관련 장비

| 계층 | 자료 형태 | 관련 장비 | 역할 |
|---|---|---|---|
| 응용, 표현, 세션 | Message | Gateway | - 프로토콜 변환 역할을 수행, OSI 참조모델 전 계층에서 동작<br>- 하나의 장비가 아니라 라우터, 브리지, 허브 등의 다양한장비를 이용해 구성 |
| | | L7 스위치 | - L4 스위치에서 확장된 개념, TCP/UDP 포트 번호와 URL 이나 Cookie 정보를 이용하여 웹 데이터에 대한 보다 효율적인 부하 분산기능수행 |
| 전송 | Segment | L4 스위치 | - TCP/UDP 포트 번호를 토대로 서비스별로 분류하여 포워딩 결정을 하는 장비<br>- 서버 접속에 대한 서버 부하분산(SLB:Server Load Balancing), 방화벽 부하분산가능(FLB: Firewall Load Balancing) |
| 네트워크 | Packet | Router | - 스위치 기능에 브로드캐스트 영역 구분 가능, 패킷 필터링, 로드 분배, QoS, WAN 접속, 라우팅 프로토콜이용 경로 설정<br>- 3 계층 장비로써 IP 주소를 기반으로 트래픽을 전송 |
| | | L3 스위치 | - L2 스위칭기능 (동일 네트워크)<br>+ L3 라우팅기능 (서로 다른 네트워크)<br>- ARP 테이블을 통해 특정 IP 와 특정 MAC 주소를 관리 |
| 데이터링크 | Frame | L2 스위치 | - 입력 포트를 통해 들어온 프레임을 MAC 주소기반으로 전송하는 장비 (MAC 테이블 기반으로 Forwarding 수행) |
| | | Switch | - 포트별로 collision domain 분리. 포트별로 다른 속도지원(브리지와 차이) |
| | | Bridge | - 허브에서 만들어진 collision domain 을 나누고 연결시킴.<br>- MAC 주소 테이블 관리. |
| 물리 | Bit | Repeater | - 데이터 전송 거리 증가를 위한 신호 증폭기 |
| | | Hub | - 단순히 선만 연결, 스위칭 장비 아님 |

- 최근에는 스위치에서 기능을 발전시킨 L3, L4, L7 스위치가 주류를 이루고, 고전적인 L2 전용 스위치, L3 전용 라우터는 거의 사용되지 않음 "끝"

| 9 | 서비스 프리미티브(Service Primitive) | | |
|---|---|---|---|
| 문제 | 서비스 프리미티브(Service Primitive)에 대해 설명하시오. | | |
| 도메인 | Network | 난이도 | ★ ★ ☆ ☆ ☆ (별 5개 기준) |
| 출제의도 | OSI 7 Layer와 관련된 출제되지 않은 토픽으로 기본 Topic에 대한 대응 점검 | | |
| 핵심 내용 키워드 | Request, Indication, Response, Confirm | | |
| 목차예시 | 1. Network 계층 구조의 서비스 추상화. 서비스 프리미티브(Service Primitive)의 개념<br>2. 서비스 프리미티브(Service Primitive)의 구성요소와 제공 기능<br>3. 서비스 프리미티브(Service Primitive)의 표현 사례 | | |
| 채점 점수 가이드 | ① 서비스 프리미티브(Service Primitive) 개념, 이해 부족 (1~2점)<br>② 서비스 프리미티브(Service Primitive) 기본 이해 수준 (3~5점)<br>③ 서비스 프리미티브(Service Primitive) 정확한 기술 제시 (5~6점)<br>④ 서비스 프리미티브(Service Primitive)추가요소 설명(+α) | | |
| 참고문헌 | KPC 114회 명품특강 1차 네트워크 심화 강의 자료<br>IT CookBook, 쉽게 배우는 데이터 통신과 컴퓨터 네트워크 (2016, 박기현 저, 한빛출판네트워크) | | |
| 고득점전략 및 답안작성 가이드 | OSI 7 Layer에서 각 계층간 Service 관점의 추상적 표현에 집중하여 접근.<br>서비스 프리미티브(Service Primitive)의 추상적 표현, 기능에 대해 정확한 표현과 키워드 제시<br>실제 적용 사례 제시 등을 통한 차별화 | | |
| 출제자 | 유희권 기술사(제 113회 컴퓨터시스템응용기술사 / itpe.you@gmail.com) | | |

Copyright ⓒ 2015 By Korea Productivity Center Convergence Knowledge Center. All rights reserved

## 1. Network 계층 구조의 서비스 추상화. 서비스 프리미티브(Service Primitive)의 개념

- OSI 기본 참조 모델에서, 서비스 이용자와 제공자 간의 상호 동작을 서비스를 제공하는 수단이 아니라 제공하는 서비스만을 주안점으로 하여 규정한 추상적 개념

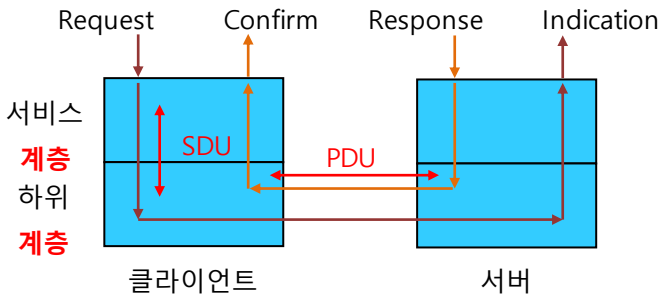
1) 내용 FACT 만 간략히 설명해 주세요(맑은 고딕, 10pt)

## 2. 서비스 프리미티브(Service Primitive)의 구성요소와 제공 기능

### 가. 서비스 프리미티브(Service Primitive)의 구성요소

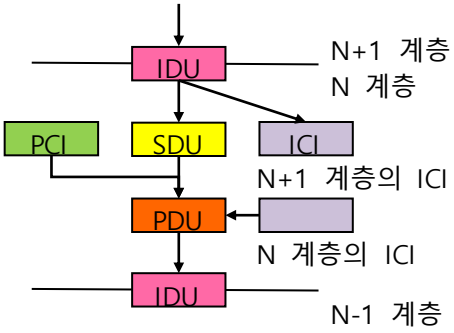
| 구성 요소 | 설명 | |
|---|---|---|
| 제공 계층(Layer) | - L → Link, N → Network, T → Transport, S → Session | |
| Service 종류 | - 연결형 서비스 | - 데이터 전송 전에 미리 연결을 설정하는 방식<br>- ⓐCONNECT【연결 설정】 ⓑDATA【데이터 전송】 ⓒDISCONNECT【연결 해제】 |
| | - 비연결형 서비스 | - ⓐDATA【데이터 전송】 |
| Primitive 기능/방향 | - Request, Indication, Response, Confirm | |
| Parameter | - Address, User Data, Service Type, Data max size 등 | |

### 나. 서비스 프리미티브(Service Primitive) 제공 기능




| 기능 | 사례 | 설명 |
|---|---|---|
| Request | CONNECT.Request | - Client가 Server에 Service 요구 |
| Indication | CONNECT.Indication | - Server에 Service 요구가 도착되었음을 통지 |
| Response | CONNECT.Response | - Server가 Client에 Service 응답 |
| Confirm | CONNECT.Confirm | - Client에 Service 요청에 대한 응답이 도착되었음을 통지 |

### 다. 서비스 프리미티브(Service Primitive) 동작 메커니즘(Mechanism)

| 동작 메커니즘 | 동작 요소 | 설명 |
|---|---|---|
|  | SDU (Service Data Unit) | - N+1 계층에 의해 N 계층과 N – 1 계층으로 전달되는 사용자 Data |
| | PCI (Protocol Control Information) | - Network의 다른 지역에 있는 동등 계층에 전송하는 정보이며, 해당 실체에게 특정 Service를 수행하도록 지시하는 헤더(Header) |
| | PDU (Protocol Data Unit) | - SDU와 PCI의 결합 |

| | | |
|---|---|---|
| | ICI (Interface Control Information) | - 서비스 기능 호출 목적으로 N과 N – 1 계층 사이에서 전달되는 임시 매개 변수 |
| | IDU (Interface Data Unit) | - 계층 경계를 통과하여 전달되는 정보의 전체 단위<br>- SDU + PCI + ICI는 SAP를 통하여 전달 |

- SAP(Service Access Point): 상·하위 계층의 개체들 간 통신 경계 역할을 하는 연결 통로

### 3. 서비스 프리미티브(Service Primitive)의 표현 사례

| 계층 | Service | Primitive 기능 | Parameter |
|---|---|---|---|
| - L: Link Layer<br>- N: Network Layer<br>- T: Transport Layer | - CONNECT<br>- DATA<br>- DISCONNECT | - Request<br>- Indication<br>- Response<br>- Confirmation | - Address<br>- User<br>- Data<br>- Service Type |

- T.CONNECT.request(called address, calling address, … , user data)
- Transport Layer 의 연결에 대한 요청으로 Parameter 를 Address, User Data 를 전달

- 끝 -

Copyright ⓒ 2015 By Korea Productivity Center Convergence Knowledge Center. All rights reserved

| | | | |
|---|---|---|---|
| 문 제 | 2. 네트워크 스위치(Network Switch)와 관련하여 다음을 설명하시오<br>(1) 스위치 개요<br>(2) OSI (Open System Interconnection) 참조 모델의 레이어에 따른 스위치 유형<br>(3) L4 스위치와 L7 스위치 비교 | | |
| 출 제 영 역 | 네트워크 | 난 이 도 | ★★☆☆☆ |
| 출 제 배 경 | 디바이스 통신 및 연결을 위한 하드웨어, 스위치에 대한 유형 및 특징 비교 | | |
| 출 제 빈 도 | 관리 121(3), 응용 116(3), 응용 110(1), 응용 104(4) | | |
| 참 고 자 료 | - OSI7 계층이란 (https://shlee0882.tistory.com/110)<br>- 시스코 스위치 기능 5 가지(https://hihighlinux.tistory.com/95)<br>- L4 스위치 vs L7 스위치 (https://kchanguk.tistory.com/181) | | |
| Keyword | MAC, IP, PORT, URL 기반<br>포트기반, 컨텐츠 기반 로드밸런싱 | | |
| 풀이 기술사님 | 공수재(111 회 컴퓨터시스템응용기술사 / ksujae22@naver.com) | | |

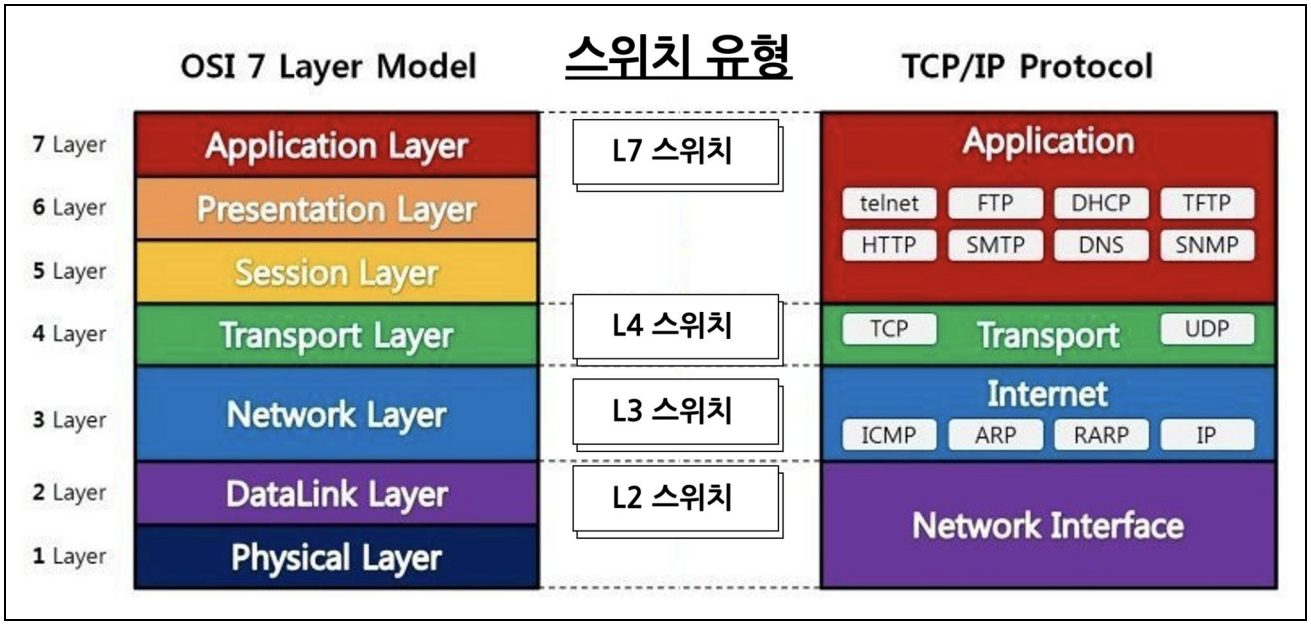
## 1. 하드웨어 처리 방식, 스위치의 개요

| | | |
|---|---|---|
| 개념 | - 노드간 패킷의 흐름을 선택적으로 전달할 수 있도록 하드웨어 방식으로 고속 제어해주는 연동 장치 | |
| 기능 | Learning | MAC 주소를 학습하여 MAC 테이블에 기록 |
| | Flooding | 인입된 포트를 제외하고 나머지 모든 포트로 전송(브로드캐스팅) |
| | Forwarding | 목적지 MAC 주소를 아는 경우 그대로 목적지로 프레임을 전달 |
| | Filtering | 목적지 MAC 주소를 아는 경우 나머지 포트는 필터링하여 전송 X |
| | Aging | MAC 테이블에 저장되는 MAC 주소 정보의 시간 지정 가능 |

- L3, L4, L7 스위치는 L2 스위치에 상위 계층의 네트워킹 기능을 추가한 장비

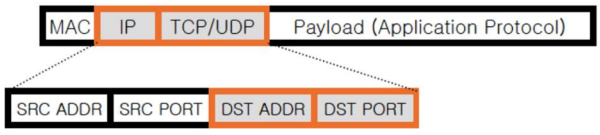
## 2. OSI (Open System Interconnection) 참조 모델의 레이어에 따른 스위치 유형

### 가. OSI (Open System Interconnection) 참조 모델의 레이어에 따른 스위치 유형도




- 계층에 따른 기능과 역할에 따른 다양한 스위치 유형이 활용되고 있음

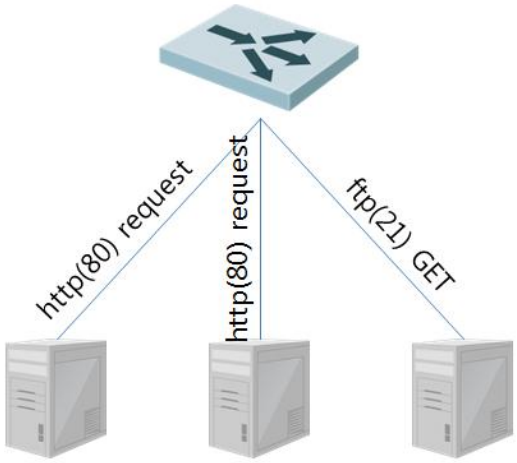
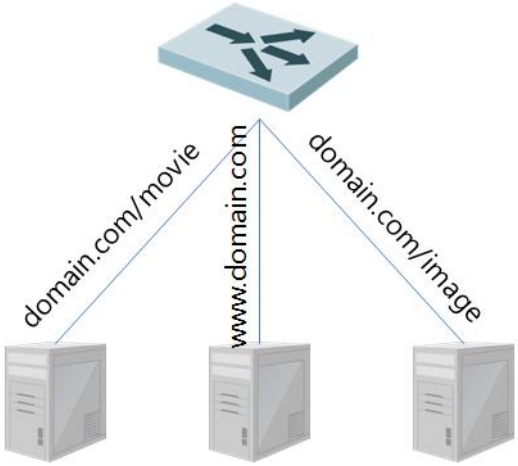
### 나. OSI (Open System Interconnection) 참조 모델의 레이어에 따른 스위치 상세 설명

| 스위치 | 참조 정보 | 설명 |
|---|---|---|
| L2 스위치 | | - 가장 기본적인 스위치이기 때문에 가격 낮음<br>- **MAC 주소** 기반 패킷 전송 |
| L3 스위치 | | - 라우팅 기능 추가<br>- **IP 주소 기반** 전송, 하드웨어 방식으로 높은 성능 |
| L4 스위치 |   | - **Port 기반** 스위칭 수행<br>- 부하분산 기능(로드밸런싱) |
| L7 스위치 | | - 페이로드 분석이 가능하여 네트워크 공격 방어 가능(DoS)<br>- **URL 기반** 로드 밸런싱 수행 |

- 시스템의 확장성과 가용성을 위한 로드밸런싱을 구현하는 L4/L7 스위치 활용

### 3. L4 스위치와 L7 스위치 비교

#### 가. L4 스위치와 L7 스위치 개념 비교

| 구분 | L4 스위치 | L7 스위치 |
|---|---|---|
| 개념 | IP 와 포트 정보를 참조하여 패킷을 확인하고 세션을 관리하여 로드밸런싱을 제공하는 스위치 | URL 과 데이터 페이로드 정보를 참조하여 보안에 더 유리하고 정교한 로드밸런싱을 제공하는 스위치 |
| 개념도 |  |  |

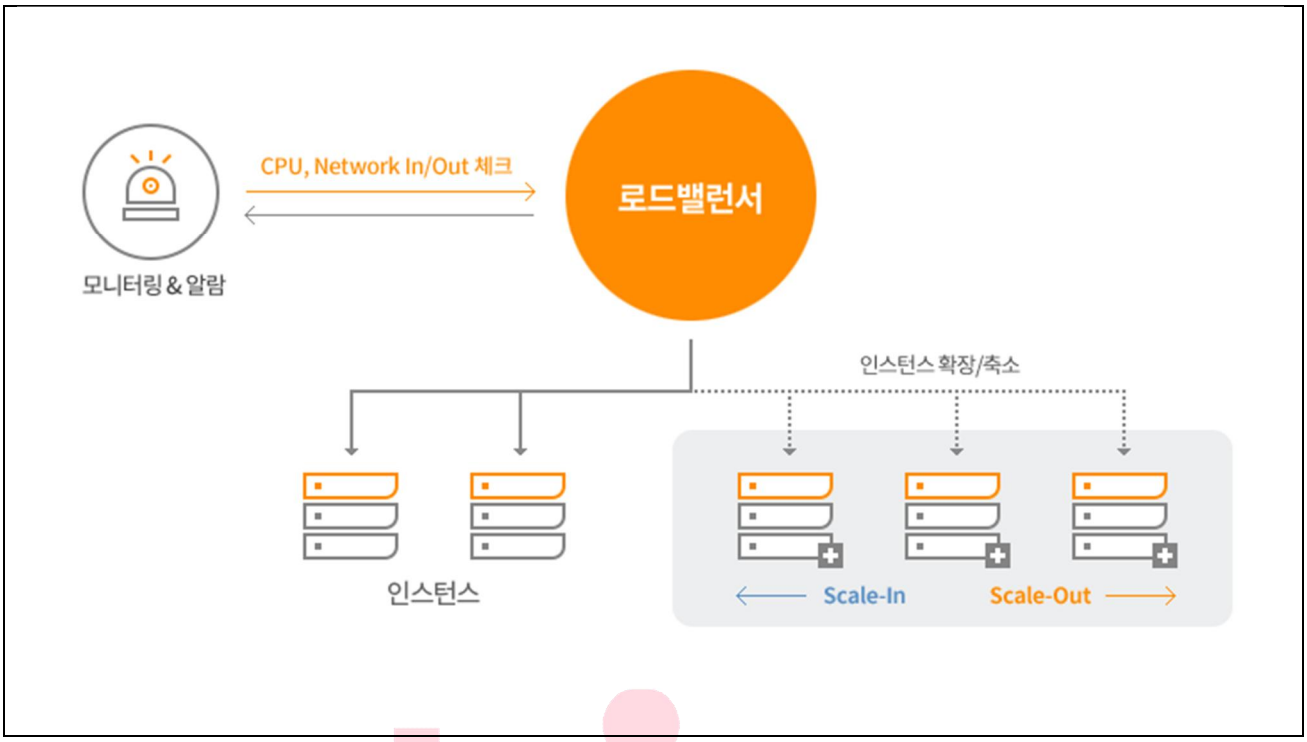
- 높은 계층일 수록 정교한 기능을 제공하지만 자원 소모에 따른 성능 부하 높음

#### 나. L4 스위치와 L7 스위치 설명 비교

| 구분 | L4 스위치 | L7 스위치 |
|---|---|---|
| 목적 | 4 계층 로드 밸런싱 | URL. HTTP Header 등 컨텐츠 기반 로드밸런싱 |
| 특징 | 포트 기반 필터링, 미러링, 로드밸런싱 등 | L4 스위치 기능 + 컨텐츠 기반 제어 |
| 보안 | L2 ~ L4 기반(ACL 등) 보안 기능 | 컨텐츠기반 필터링 안티바이러스 |
| 장점 | ASIC 기반 빠른 속도 L7 대비 저비용 | URL 등 컨텐츠 분석 기능 업데이트 가능 |
| 단점 | 서비스 유무만 확인 컨텐츠기반 제어 불가 | L4 대비 고비용 CPU 처리, 성능 저하 |

- 비용 및 기술 요구사항에 따라 L4/L7 스위치 선택

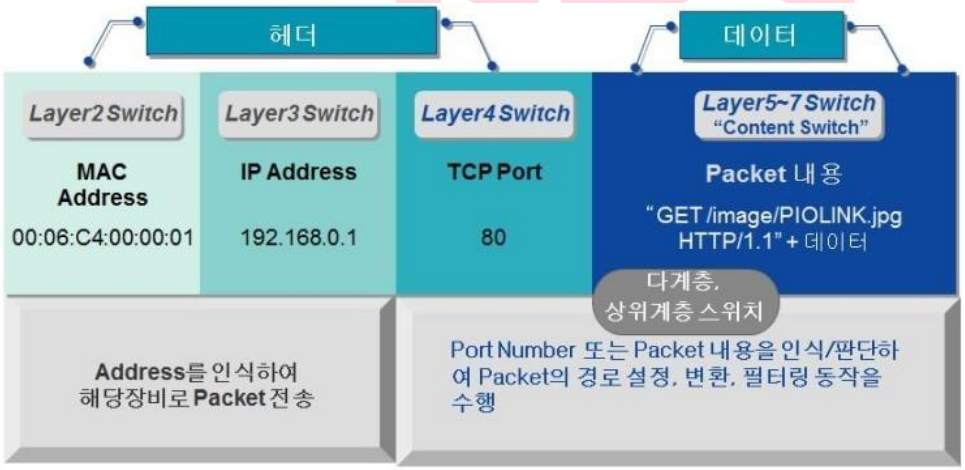
4. 로드밸런싱을 통한 오토스케일링 구현




- 작업 훔치기(Work Stealing)를 통해 다양한 마이그레이션 패턴에 대한 이동 결정

"끝"

[기타자료]

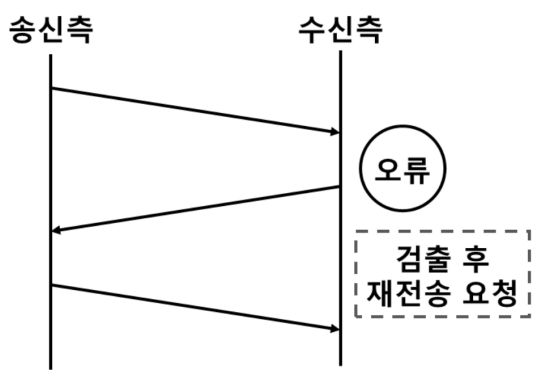
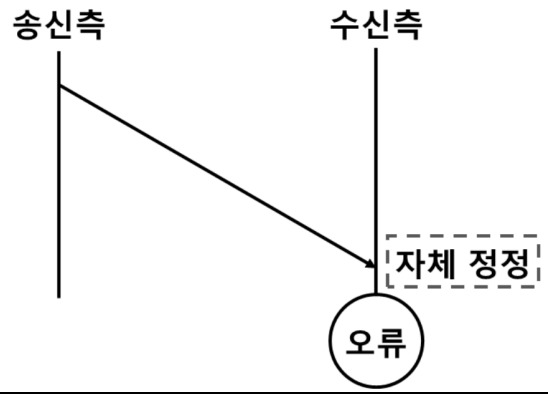



**기출풀이 의견**

2. 문제의 마지막을 읽어보면 각각 설명하라고 명시가 되어 있습니다. 문제에서 나와있는대로 단락을 구분하여 각 스케쥴링 방식을 설명하는 것이 반드시 필요합니다. 각각 쓰시되 반드시 2교시 답안의 특성을 살려, 각 단락이 연계될 수 있도록 설명하는 것이 중요합니다.

| 16 | 데이터링크 계층 오류제어 | | |
|---|---|---|---|
| 문제 | BEC 와 FEC 를 비교하시오 | | |
| 도메인 | 네트워크 | | |
| 출제배경/의도 | 117 회 컴시응 1 교시 '네트워크 전송계층 역할' 기출문제로 통신계층 출제 예상<br>네트워크 기본 토픽인 오류 정정(Error Correction)에 대해 학습 | | |
| 키워드 | ● BEC – 검출 후 재전송, FEC – 자체정정<br>● Parity Check, Stop and Wait, Go-back-N, Selective-Repeat, Adaptive ARQ, Block Sum, CRC, Check Sum, Hamming Code | | |
| 목차예시 | 1. BEC 와 FEC 의 개념 비교<br>2. BEC 와 FEC 의 상세 비교<br>3. H-ARQ 의 개요 | | |
| 출제자 | 문광석 기술사(제 117 회 정보관리기술사 / itpe.moon@gmail.com) | 난이도 | ★ ★ ☆ ☆ ☆ |
| 참고문헌 | http://ensxoddl.tistory.com/270<br>데이터통신과 컴퓨터 네트워킹(한빛아카데미, 강문식)<br>쉽게 배우는 데이터 통신과 컴퓨터 네트워크(박기현 저) | | |

**1. BEC(Backward Error Correction)과 FEC(Forward Error Correction)의 개념 비교**

| 비교 | BEC | FEC |
|---|---|---|
| 개념 | - 데이터 수신 측에서 오류 검출 후 송신측에 오류 사실을 알리고 재전송을 요청하여 오류를 수정하는 네트워크 오류제어 기술 | - 데이터 송신 시 여분의 잉여 비트를 추가하여 오류의 유무를 검출, 정정할 수 있도록 하는 네트워크 오류제어 기술 |
| 개념도 |  |  |

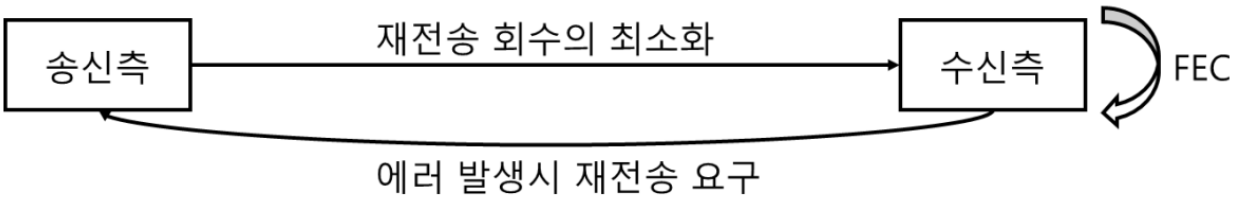
- BEC 는 오류제어를 위해 검출과 재전송 요청 기법이 필요, FEC 는 자체 정정하는 기법이 필요

**2. BEC(Backward Error Correction)과 FEC(Forward Error Correction)의 상세 비교**

| 비교 | FEC | BEC |
|---|---|---|
| 원리 | - 수신측이 에러를 발견 시 부가적 정보로 에러검출 및 에러정정을 하는 방식 | - 수신측이 에러를 발견 시, 재전송(검출 후 재전송, ARQ)을 송신측에 요구하는 방식 |
| 특징 | - 오류가 발생해도 재전송 요구 없이 오류 수정이 가능하므로, 실시간 처리 및 높은 처리율 제공 | - 재전송을 기반으로 링크의 신뢰성을 확보가능 |
| 전송 효율 | - 상대적으로 높음 | - 에러율이 낮은 네트워크에서는 효과적이나 잉여비트(Parity, CRC) 추가로 전송 효율이 떨어짐 |
| 정정 주체 | - 수신측(Receiver) | - 송신측 (Sender) |
| 재요청 | - 없음 (수신측 자체 처리) | - 에러 발생 시 요청 |
| 적용 분야 | - 단거리, 양방향 | - 장거리(위성통신 등), 단방향 |
| 용도 | - 송신측 한 곳, 수신측 여러 곳<br>- 재전송 피드백 어려운 곳 | - 실시간 처리에 곤란한 에러제어방법 |
| 유형 | - Hamming Code<br>- RS Code<br>- Convolutional Code<br>- Turbo Code | - Stop & Wait ARQ<br>- Go-Back N ARQ<br>- Selective ARQ<br>- Adaptive ARQ |

- FEC 를 이용해 정정 시도 후에도 수정이 안 될 경우만 재전송하는 **H-ARQ** 방식도 활용

**3. BEC(Backward Error Correction)과 FEC(Forward Error Correction)의 Hybrid 기술, H-ARQ 의 개요**



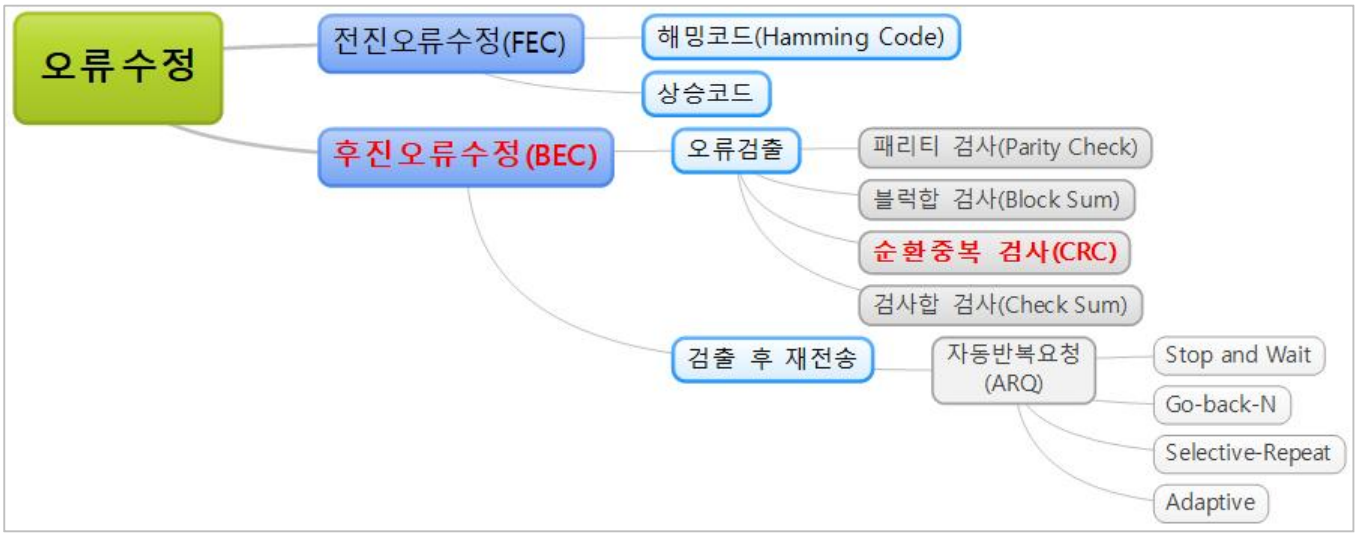

- BEC 와 FEC 의 장단점을 보완한 하이브리드 기술을 이용해서 안전하게 오류제어를 수행 가능.

"끝"


Copyright ⓒ 2014 By Korea Productivity Center Convergence Knowledge Center. All rights reserved

| 6 | CRC(Cyclic Redundancy Check) | | |
|---|---|---|---|
| 문제 | 패킷 데이터의 송수신 과정의 후진오류수정 중 전송 데이터가 1011010, 디바이더(divider)가 1101인 경우 CRC(Cyclic Redundancy Check) 값을 구하는 과정을 설명하시오. | | |
| 도메인 | 네트워크 | 난이도 | ★ ★ ☆ ☆ ☆ |
| 출제배경 | CRC 문제가 자주 출제됨에 따라 토픽에 대한 이해 확인차원 | | |
| 핵심 키워드 | BEC(후진오류수정), 데이터워드(Data word), 디바이더(Divisor: 제수), 코드워드(Code word), CRC | | |
| 참고문헌 | 데이터통신과 네트워킹 – Behrouz A. Forouzan 저 | | |
| 출제자 | 유ㅇㅇ기술사(제 113 회 컴퓨터시스템응용기술사 / itpe_you@naver.com) | | |

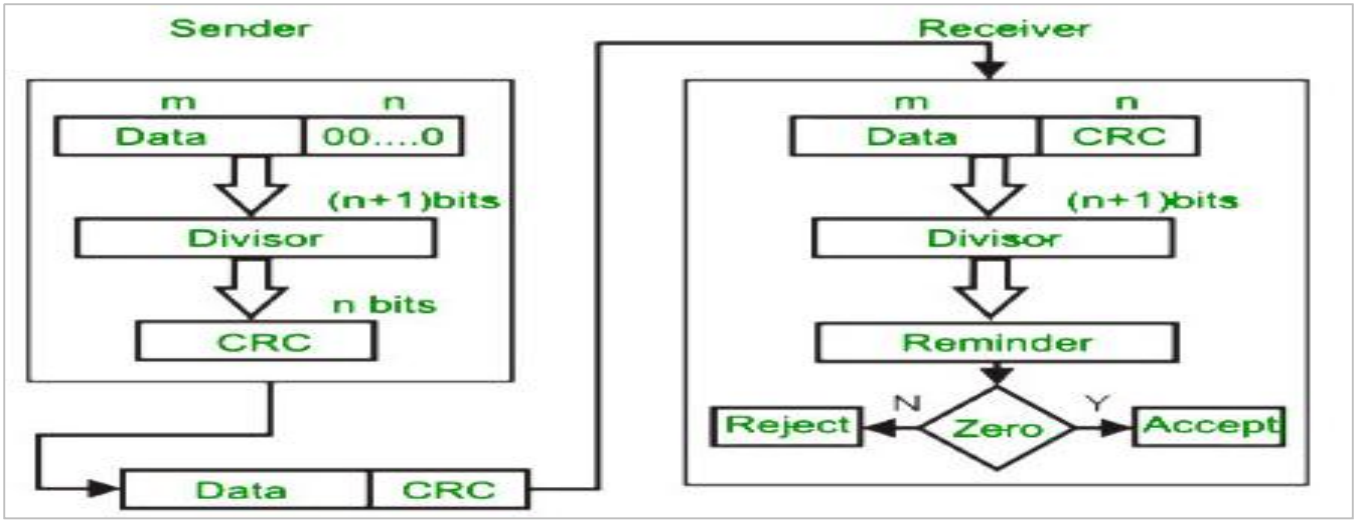
## 1. 데이터링크 계층에서의 오류수정 기법의 개요




- 송신한 데이터가 제대로 도달되지 않거나, 전송도중 에러 발생시 검출하고 오류를 수정하는 기능

## 2. CRC(Cyclic Redundancy Check) 기법

### 가. CRC 의 정의



- CRC, 송신측에서 데이터로부터 다항식에 의해 나온 결과를 여분의 오류검사필드에 덧붙여 보내면, 수신측에서는 동일한 방법으로 추출한 결과와의 일치성으로 오류를 검사하는 기술
- CRC 는 송신 측에서 수행되는 Encoding 단계에서 CRC 를 생성하여 송신 이후, 수신 측에서 Divisor 를 사용하여 나머지 값의 0 유무로 에러 발생 여부를 검증하는 기법

### 나. CRC 기법의 매커니즘

| 주체 | 단계 | 단계설명 | 비고 |
|---|---|---|---|
| 송신측 | ① Encoding (CRC 계산) | - 데이터워드 + n-bit (0..0)로 구성된 데이터를 (n+1)-bit Divisor로 나누어 CRC 정보 생성<br>- 데이터워드 + CRC로 이루어진 코드워드 생성 | -Divisor는 0과 1의 스트링 보다 대수다항식 표현<br>ex) $1x^3 + 1x^2 + 0x + 1$ |
| 송신측 | ② Transmission (Data + CRC) | - 코드워드(데이터워드+ CRC)를 수신측에 전송 | - Unreliable Transmission<br>- 손실, 순서 바뀜, 중복 등 에러 발생 가능 |
| 수신측 | ③ Decoding (에러체크) | - 수신된 코드워드를 Divisor를 이용하여 XOR연산 수행<br>- 나머지가 0이 될 경우 에러가 발생하지 않았으므로 데이터를 정상 수신 | - 0 이외의 나머지 발생시 전송 중 에러 발생으로 간주, 재전송 요청 |

## 3. CRC(Cyclic Redundancy Check) 계산값 풀이

- 전송 데이터(데이터워드)가 1011010, 디바이더(Divider:제수)가 1101 인 경우, *n*-bit 이진 CRC 계산을 위한 (*n*+1)-bit divider 가 1101(4bit)인 다항식은 $1x^3 + 1x^2 + 0x + 1$ 로, 다음과 같은 CRC 계산을 위한 테이블을 만듬

| 다항식 | 디바이더(제수) | 비트수 | CRC |
|---|---|---|---|
| $1x^3 + 1x^2 + 0x + 1$ | 1101 | 4bit | 3bit |

- 즉, 3-bit 이진 CRC 를 계산하기 위해 divider 로 나누는 과정을 반복하면,

**① Encoding (CRC계산)**

```
1011010 000
1101            ← 제수(divider) 4bit
---------------
0110010 000     ← 결과
 1101           ← 제수(divider) 4bit
---------------
0000110 000     ← 결과
    110 1       ← 제수(divider) 4bit
---------------
0000000 100     ← 나머지 3bit, 앞에 있는 데이터가 모두 0 이되고 뒤에 3bit 가 최종 CRC 값.
```


Copyright ⓒ 2015 By Korea Productivity Center Convergence Knowledge Center. All rights reserved

**② Transmission 코드워드 송신 (Data + CRC)**

ㅇ 코드워드 = 데이터워드+ CRC

➔ 1011010 100

ㅇ 송신 데이터는 1011010100

**③ Decoding (에러체크) : CRC값 계산 검증**

계산 결과의 검증을 위해 입력 전송데이터 다음에 CRC 결과를 붙여 divider 로 나누어 0 이 되는지 확인.

```
1011010 100
1101
---------------
0110010 100
 1101
---------------
0000110 100
     110 1
---------------
            0 ← 나머지 0
```

- 나머지가 0 이 아닐 경우, 데이터를 버리고 재전송 요청 "끝"

| 5 | 해밍코드 | | |
|---|---|---|---|
| 문제 | 해밍코드에 관하여 아래의 내용에 대해 설명하시오.<br>가. 101100110 에 대한 해밍코드 후 데이터 값<br>나. '가' 의 데이터 수신 값에 대해 MSB 오류시 정정과정<br>(단, 해당 통신에서 Network byte Order 에 따라 수행하고, 짝수패리티로 가정) | | |
| 도메인 | 네트워크 | 난이도 | ★ ★ ★ ☆ ☆ (별 5 개 기준) |
| 출제의도 | FEC 의 대표적인 오류정정 기법인 해밍코드 계산과 검증 과정 점검<br>CRC 의 정보관리 104 회, 110 회 기출에 따른 확장 출제 대비 | | |
| 핵심 내용 키워드 | 1bit 오류 정정, 2bit 오류 검출, 패리티비트 수 : 2^p >= d+p+1<br>패리티비트 위치 $2^n$ 번째 비트 위치, 패리티비트 값 , 빅엔디언, 리틀엔디언, MSB, LSB | | |
| 목차예시 | 1.오류데이터 검출 및 정정가능한 FEC 대표기법, 해밍코드 개요<br>2.101100110 에 대한 해밍 코드 후 데이터 값<br>3.해밍코드 값에 대해 MSB 오류시 정정과정 | | |
| 채점 점수 가이드 | ① 개념, 이해 부족 (1~8 점)<br>② 기본 이해 수준 (9~14 점)<br>④ 정확한 기술 제시 (14~15 점)<br>⑤ 결과값 및 검증과정의 도식화(+α) | | |
| 참고문헌 | -데이터 통신 (한국 맥그로힐 / 이재광 편저)<br>-처음 만나는 디지털 논리회로 (한빛미디어 / 임석구, 홍경호 [공]지음)<br>-컴퓨터 아키텍처 (한빛 아카데미 / 우종정 지음) | | |
| 고득점전략 및 답안작성 가이드 | -해밍코드의 이해를 바탕으로 정확하게 해밍코드 계산후 값제시 및 오류시 정정과정 제시<br>-기본적인 계산문제는 정확한 값의 제시를 통해 고득점 가능하며, 미리 답안의 포맷을 준비하여 도식화를 통한 정리된 형태로 작성 필요 | | |
| 출제자 | 박재성 기술사 제 111 회 컴퓨터시스템응용기술사 / kftc@naver.com ) | | |

## 1.오류데이터 검출 및 정정 가능한 FEC 대표기법, 해밍코드 개요

**가.해밍코드 정의**

| | | |
|---|---|---|
| 정의 | 데이터와 Redundancy의 관계를 이용하여, 어떤 길이의 데이터에 대해서도 단일 비트 오류정정 기능을 제공하는 대표적인 FEC 코딩 기법 | |
| 특징 | 정정과 검출 | 1bit 오류는 정정, 2bit 오류는 검출까지 가능 |
| | 음성 비적합 | 디지털 데이터 전송에는 효율적이나 음성정보에는 비 적합 |
| | 원거리 통신용이 | -ARQ등 재전송이 어려운 원거리 통신에 적합한 코딩 기법<br>-마이크로칩 디바이스에 채택되어 데이터 전송신뢰를 높이는데 사용 |

-오류검출 및 정정을 통해 재전송을 요구하기 어렵거나 시간이 많이 걸리는 장소로부터 데이터 전송 신뢰도에 많은 개선점을 제공

**나.해밍코드 계산 기본원리**

<table>
<tr><th>구분</th><th>설명</th></tr>
<tr><td>데이터와 패리티비트 관계<br><br>(패리티비트 수 결정)</td><td>
<table>
<tr><td>2^p >= d + p + 1<br>(d = Data,<br>p = Parity bit)</td><td>
<table>
<tr><th>데이터 비트 수</th><th>패리티 비트 수(중복 비트수)</th></tr>
<tr><td>1</td><td>2</td></tr>
<tr><td>2 ~ 4</td><td>3</td></tr>
<tr><td>5 ~ 11</td><td>4</td></tr>
<tr><td>12</td><td>5</td></tr>
</table>
</td></tr>
</table>
</td></tr>
<tr><td>패리티비트 위치 결정</td><td>
-총 비트 수에서 2^(0~(p-1))승 순으로 삽입 ($2^n$ 번째 비트 위치)<br>
1,2,4,8 (2^0, 2^1, 2^2)의 자리 (행 번호 기준)에 패리티 비트가 삽입<br><br>
<table>
<tr><td>비트위치</td><td>11</td><td>10</td><td>9</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td></tr>
<tr><td>기 호</td><td>D11</td><td>D10</td><td>D9</td><td>P8</td><td>D7</td><td>D6</td><td>D5</td><td>P4</td><td>D3</td><td>P2</td><td>P1</td></tr>
</table>
패리티 비트 위치 : 1,2,4,8,16...<br>
차트구성 : P (패리티비트), D(데이터) + 비트위치
</td></tr>
</table>


Copyright ⓒ 2015 By Korea Productivity Center Convergence Knowledge Center. All rights reserved

<table>
<tr><td>패리티비트<br>값 결정</td><td>
<table>
<tr><td>비트위치</td><td>11</td><td>10</td><td>9</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td></tr>
<tr><td>기 호</td><td>D11</td><td>D10</td><td>D9</td><td>P8</td><td>D7</td><td>D6</td><td>D5</td><td>P4</td><td>D3</td><td>P2</td><td>P1</td></tr>
<tr><td>P1영역</td><td>v</td><td></td><td>v</td><td></td><td>v</td><td></td><td>v</td><td></td><td>v</td><td></td><td>v</td></tr>
<tr><td>P2영역</td><td>v</td><td>v</td><td></td><td></td><td>v</td><td>v</td><td></td><td></td><td>v</td><td>v</td><td></td></tr>
<tr><td>P4영역</td><td></td><td></td><td></td><td></td><td>v</td><td>v</td><td>v</td><td>v</td><td></td><td></td><td></td></tr>
<tr><td>P8영역</td><td>v</td><td>v</td><td>v</td><td>v</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>
-P1 : 해당비트 포함하고 자릿수 1 만큼 검사하고 건너뜀. 1,3,5,7,9.. (1 자리 검사하고 1 자리 SKIP )<br>
-P2 : 해당비트 포함비트 자릿수 2 만큼 검사하고 건너뜀. 2,3,6,7,10,11 ( 2 자리 검사하고 2 자리 SKIP )<br>
-P4 : 해당비트 포함비트 자릿수 4 만큼 검사하고 건너뜀. 4,5,6,7 ( 4 자리 검사하고 4 자리 SKIP )<br>
-P8 : 해당비트 포함비트 자릿수 8 만큼 검사하고 건너뜀. 8,9,10,11 ( 8 자리 검사하고 8 자리 SKIP )<br><br>
: ➔ 참고자료 [**패리티 비트 오류 테이블**] **확인**
</td></tr>
</table>

## 2. 101100110에 대한 해밍 코드 후 데이터 값

: 해당 통신에서 Network byte Order에 따라 수행

➔ 네트워크 데이터 통신에서는 네트워크 바이트 순서 ( 빅엔디언 )를 따름

<table>
<tr><th>구분</th><th>설명</th></tr>
<tr><td>패리티비트<br>계산</td><td>1.패리티비트 : 2^p >= d + p + 1<br>2.데이터 d =9 -> 패리티 P =4 : 패리티 비트는 4개<br>( -> 데이터 비트 수 5 ~ 11 자리 일 경우 , 패리티 비트는 4개 )</td></tr>
<tr><td>패리티비트<br>위치</td><td>
<table>
<tr><td>비트위치</td><td>13</td><td>12</td><td>11</td><td>10</td><td>9</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td></tr>
<tr><td>기호</td><td>D13</td><td>D12</td><td>D11</td><td>D10</td><td>D9</td><td>P8</td><td>D7</td><td>D6</td><td>D5</td><td>P4</td><td>D3</td><td>P2</td><td>P1</td></tr>
<tr><td>해밍코드</td><td>1</td><td>0</td><td>1</td><td>1</td><td>0</td><td>P8</td><td>0</td><td>1</td><td>1</td><td>P4</td><td>0</td><td>P2</td><td>P1</td></tr>
</table>
-원본 데이터 101100110을 해밍코드에 맞게 비트 위치를 맞춤
</td></tr>
<tr><td>패리티비트<br>생성</td><td>-P1의 패리티 1,3,5,7,9,11,13 번째에서 '1'은 3개 존재 : P1 = 1<br>-P2의 패리티 2,3,6,7,10,11 번째에서 '1'은 3개 존재 : P2 = 1<br>-P4의 패리티 4,5,6,7,12,13 번째에서 '1'은 3개 존재 : P4 = 1<br>-P8의 패리티 8,9,10,11,12,13 번째에서 '1'은 3개 존재 : P8 = 1</td></tr>
</table>

| 비트위치 | 13 | 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 기호 | D13 | D12 | D11 | D10 | D9 | **P8** | D7 | D6 | D5 | **P4** | D3 | **P2** | **P1** |
| 원본데이터 | 1 | 0 | 1 | 1 | 0 | | 0 | 1 | 1 | | 0 | | |
| **P1영역** | 1 | | 1 | | 0 | | 0 | | 1 | | 0 | | **1** |
| **P2영역** | | | 1 | 1 | | | 0 | 1 | | | 0 | **1** | |
| **P4영역** | 1 | 0 | | | | | 0 | 1 | 1 | **1** | | | |
| **P8영역** | 1 | 0 | 1 | 1 | 0 | **1** | | | | | | | |

| 생성코드 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 1 | 1 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|

데이터 값

-P8,P4,P2,P1의 값은 짝수 패리티 적용시 '**1 1 1 1**' 도출

-최종 생성된 '**1 0 1 1 0 1 0 1 1 1 0 1 1**' 수신측에 전송

## 3. 해밍코드 값에 대해 MSB 오류시 정정과정

| 구분 | 설명 |
|---|---|

정정과정

| 순서 | 과정 | 상세 |
|---|---|---|
| 1 | 패리티 비트 확인 | 수신된 해밍코드의 길이에 따른 패리티 비트 위치확인 |
| 2 | 패리티 비트 분석 | 각 패리티 비트에 따른 비트 자리 수들의 값에 대한 짝수 패리티 계산 |
| 3 | 오류 정정 | 계산된 짝수 패리티를 2진수 값으로 변환하여 오류검출/정정 |

1.패리티비트 확인

| 생성코드 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 1 | 1 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 수신코드 | **0** | 0 | 1 | 1 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 1 | 1 |
| | MSB | | | | | | | | | | | | LSB |

-첫번째 비트 13번재 자리 (MSB) 오류로 1 -> 0으로 수신

-MSB (Most Significant bit) : 최대유효비트 , 최상위비트


Copyright ⓒ 2015 By Korea Productivity Center Convergence Knowledge Center. All rights reserved

2.패리티비트 위치

| 비트위치 | 13 | 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 기호 | D13 | D12 | D11 | D10 | D9 | **P8** | D7 | D6 | D5 | **P4** | D3 | **P2** | **P1** | 검증 |
| 수신데이터 | 0 | 0 | 1 | 1 | 0 | | 0 | 1 | 1 | | 0 | | | |
| **P1영역** | 0 | | 1 | | 0 | | 0 | | 1 | | 0 | | **1** | 오류 |
| **P2영역** | | | 1 | 1 | | | 0 | 1 | | | 0 | **1** | | 정상 |
| **P4영역** | 0 | 0 | | | | | 0 | 1 | 1 | **1** | | | | 오류 |
| **P8영역** | 0 | 0 | 1 | 1 | 0 | **1** | | | | | | | | 오류 |

-13 번째 자리의 데이터(D13)를 포함하여 해밍코드 검증하는 패리티 비트 위치에만 영향
-해당비트만 영향 -> P1, P4, P8 오류

3.오류 정정

| 패리티 | P8 | P4 | P2 | P1 |
|---|---|---|---|---|
| 검증결과 | 오류 | 정상 | 정상 | 오류 |
| 2 진수 | 1 * 2^3 =8 | 1 * 2^2 =4 | | 1 * 2^0 =1 |

-오류 패리티 P1,P4,P8의 2진수의 합 : 8 + 4 + 1 = 13
-> 13번째 자리오류검출 : 0 -> 1 로 정정
( 또는 **P1,P4,P8의 각각 비트위치의 합이 오류비트 위치** )
-수정된 값 '**1 0 1 1 0 1 0 1 1 1 0 1 1**'

-해밍코드는 오류검출 및 정정을 통해 원거리 통신이나 신뢰기반 통신에서 많이 활용.
-정보통신기기, 무선통신, TV방송, RAID2 (bit)등에서 활용. -끝-

[기타자료]

**1. 패리티 비트 오류 테이블**

| P8 | P4 | P2 | P1 | 오류비트 행번호 |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 없슴 |
| 0 | 0 | 0 | 1 | 1 |
| 0 | 0 | 1 | 0 | 2 |
| 0 | 0 | 1 | 1 | 3 |
| 0 | 1 | 0 | 0 | 4 |
| 0 | 1 | 0 | 1 | 5 |
| 0 | 1 | 1 | 0 | 6 |
| 0 | 1 | 1 | 1 | 7 |
| 1 | 0 | 0 | 0 | 8 |
| 1 | 0 | 0 | 1 | 9 |
| 1 | 0 | 1 | 0 | 10 |
| 1 | 0 | 1 | 1 | 11 |

-P1은 1,3,5,7,9,11번째 행으로 패리티 계산

-P2는 2,3,6,7,10,11번째 행으로 패리티 계산

-P4는 4,5,6,7번째 행으로 패리티 계산

-P8는 8,9,10,11번째 행으로 패리티 계산

**2. 빅엔디언/리틀 엔디언 방식**

| 구분 | 설명 | 사용환경 |
|---|---|---|
| 빅 엔디안<br>(Big-Endian) | -중요한 것 또는 큰 것이 먼저 표현/저장/전송<br>-High Order First<br>-일상적인 문자/숫자 표현 순서 방식 | -MIPS, IBM, Motorola 비롯한 대부분의 RISC아키텍처<br>-네트워크통신 (tcp/ip) |
| 리틀 엔디안<br>(Little- Endian) | -중요한 것 또는 큰 것이 나중에 표현/저장/전송<br>-일상적인 문자/숫자 표현 순서와는 반대 순서임 | -Intel, DEC, VAX-11 |

-ARM프로세서를 포함한 오늘날 아키텍처는 빅엔디언/리틀 엔디언을 선택가능

-**[네트워크 전송순서]**

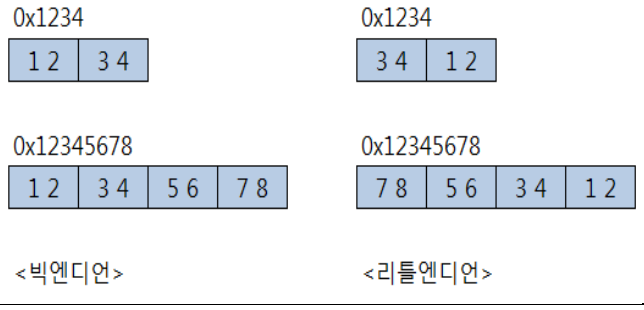
: 1. 인터넷 IP 패킷의 전송 순서표준 = 네트워크 표준 바이트 순서 (Network Byte Order)

2. 최상위 바이트(MSB)를 먼저 보내고, 최하위 바이트(LSB)는 맨나중에 보냄

3. 바이트 내에서의 비트 전송 순서도 최상위 비트를 먼저 보냄

=> **즉, 전체적으로 빅 엔디언(Big-Endian) 순서 = 인간의 시각에 맞게 보기 편한 방식**

-사례) 2개의 바이트로 구성된 1234의 16진수 경우, 빅엔디언 방식은 12를 포함하는 바이트가 34를 포함하는 바이트보다 앞에 위치하지만, 리틀 엔디언 방식으로 반대




[참고]

1.정보통신기술용어

http://www.ktword.co.kr/abbr_view.php?m_temp1=23532

**2.**www.packetinside.com/2010/10/리틀엔디안little-endian과-빅엔디안big-endian이해하기.html


Copyright ⓒ 2015 By Korea Productivity Center Convergence Knowledge Center. All rights reserved

## 3 빅엔디언/리틀 엔디언 해밍코드 계산 비교 ( 데이터 : 101100110 )

**패리티 비트 위치**

-[빅엔디언]

| 비트위치 | 13 | 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 기호 | D13 | D12 | D11 | D10 | D9 | P8 | D7 | D6 | D5 | P4 | D3 | P2 | P1 |
| 원본데이터 | 1 | 0 | 1 | 1 | 0 | P8 | 0 | 1 | 1 | P4 | 0 | P2 | P1 |

-[리틀엔디언]

| 비트위치 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 기호 | P1 | P2 | D3 | P4 | D5 | D6 | D7 | P8 | D9 | D10 | D11 | D12 | D13 |
| 해밍코드 | P1 | P2 | 1 | P4 | 0 | 1 | 1 | P8 | 0 | 0 | 1 | 1 | 0 |

➡ **<u>빅/리틀 엔디언 방식에서 데이터는 순서 변경없이 동일하게 적용(좌->우), 패리티의 순서만 변경</u>**

**패리티 비트 생성**

-[빅엔디언]

| 비트위치 | 13 | 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 기호 | D13 | D12 | D11 | D10 | D9 | P8 | D7 | D6 | D5 | P4 | D3 | P2 | P1 | **패리티** |
| 원본데이터 | 1 | 0 | 1 | 1 | 0 | | 0 | 1 | 1 | | 0 | | | |
| P1영역 | 1 | | 1 | | 0 | | 0 | | 1 | | 0 | | **1** | **1** |
| P2영역 | | | 1 | 1 | | | 0 | 1 | | | 0 | **1** | | **1** |
| P4영역 | 1 | 0 | | | | | 0 | 1 | 1 | **1** | | | | **1** |
| P8영역 | 1 | 0 | 1 | 1 | 0 | **1** | | | | | | | | **1** |

**-해밍코드 : 1011010111011**

-[리틀엔디언]

| 비트위치 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 기호 | P1 | P2 | D3 | P4 | D5 | D6 | D7 | P8 | D9 | D10 | D11 | D12 | D13 | **패리티** |
| 원본데이터 | | | 1 | | 0 | 1 | 1 | | 0 | 0 | 1 | 1 | 0 | |
| P1영역 | **1** | | 1 | | 0 | | 1 | | 0 | | 1 | | 0 | **1** |
| P2영역 | | **0** | 1 | | | 1 | 1 | | | 0 | 1 | | | **0** |
| P4영역 | | | | **1** | 0 | 1 | 1 | | | | | 1 | 0 | **1** |
| P8영역 | | | | | | | | **0** | 0 | 0 | 1 | 1 | 0 | **0** |

**-해밍코드 : 1011011000110**

**사례**

-데이터 1001 의 경우 : P1,P2,P4의 값이 빅/리틀 모두 동일 (P1=0, P2=0, P4=1)

빅엔디언

| 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|
| D7 | D6 | D5 | P4 | D3 | P2 | P1 |
| 1 | 0 | 0 | | 1 | | |

리틀엔디언

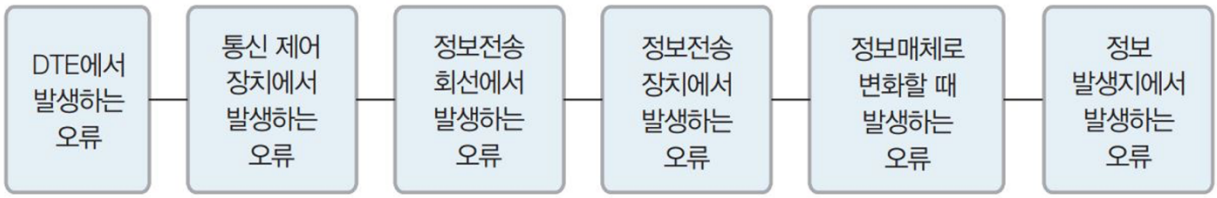
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|
| P1 | P2 | D3 | P4 | D5 | D6 | D7 |
| | | 1 | | 0 | 0 | 1 |

| | | | |
|---|---|---|---|
| 문 제 | 3. 데이터링크 계층은 네트워크에서 오류제어를 담당한다. 다음을 설명하시오.<br>가. 오류제어방식의 개념과 종류<br>나. 전진오류수정(FEC)과 검출 후 재전송(ARQ)방식 비교<br>다. ARQ 방식 3가지 | | |
| 출 제 영 역 | 네트워크 | 난 이 도 | ★★☆☆☆ |
| 출 제 배 경 | 데이터링크 계층의 오류제어에 대한 이해 | | |
| 출 제 빈 도 | 제 120 회 컴퓨터시스템응용기술사(오류제어), 제 110 회 컴퓨터시스템응용기술사(FEC) | | |
| 참 고 자 료 | 4 차 산업혁명 시대의 정보통신개론 (한빛아카데미) | | |
| Keyword | 오류 검출, 오류 정정, 재전송 요청 | | |
| 풀 이 | 이진주(123 회 정보관리기술사) | | |

## 1. 데이터링크 계층 오류제어방식의 개념과 종류

### 가. 데이터링크 계층 오류제어방식의 개념

< 데이터링크계층의 오류 발생 장소 >




- 데이터링크 계층에서 오류는 데이터단말장치나 통신회선, 전송매체 등의 기계적/구조적 원인에 따라 발생
- 오류가 발생하는 장소나 원인에 따라 적절한 오류제어방식을 사용하여 오류를 검출하고 수정 및 처리

### 나. 오류제어방식 종류

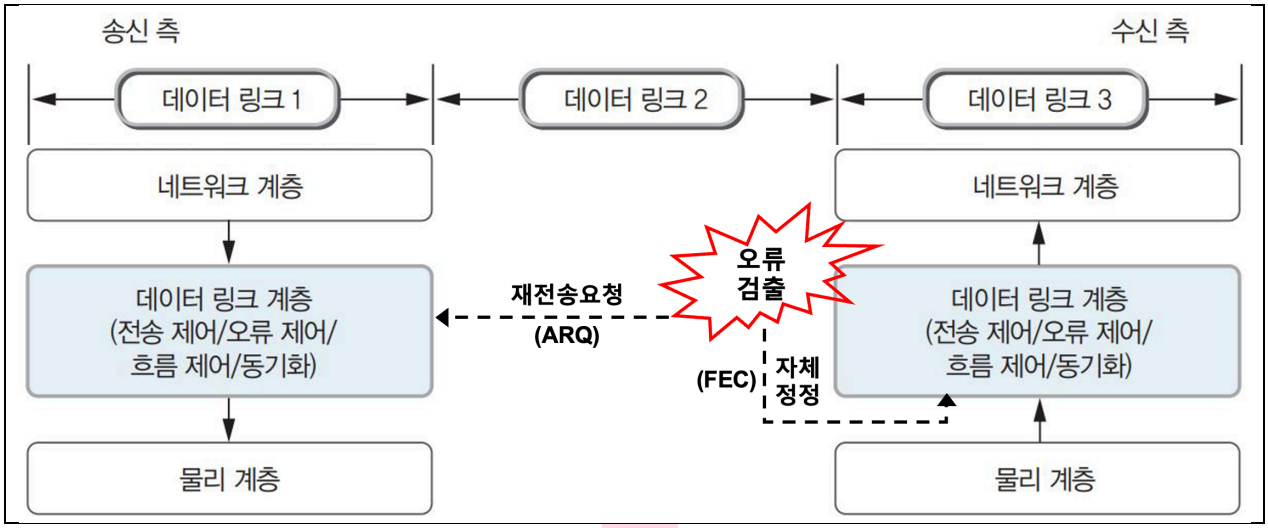
| 종 류 | 설 명 |
|---|---|
| 오류 무시 | - 영문 텍스트나 숫자가 포함되지 않은 간단한 데이터를 취급하는 데이터 통신에서 사용 |
| 반향(Echo) 검사 | - 루프(Loop)방식 이라고도 함<br>- 전송한 데이터와 수신한 데이터를 서로 비교하여 판단하는 방식 |
| 검출 후 재전송 (ARQ) | - 오류가 발생하면 수신 측은 송신 측에 오류가 발생한 사실을 알리고 재전송 요구<br>- 수신 측은 역채널을 통해 ACK/NAK 정보를 전송 |

| | |
|---|---|
| **전진 오류 수정 (FEC)** | - 수신 측에서 오류가 있음을 발견하면 오류를 검출할 뿐만 아니라 수정도 가능한 방식<br>- 연속적인 데이터 전송이 가능하며 역채널을 사용하지 않는 장점 |

- 통신 환경이나 전송 데이터를 고려하여 적합한 오류제어방식 선택 적용

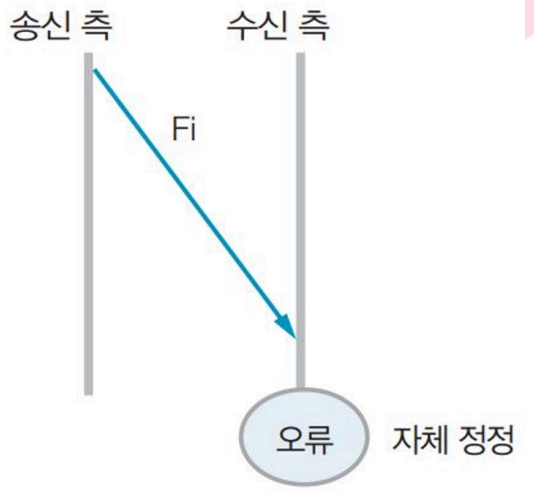
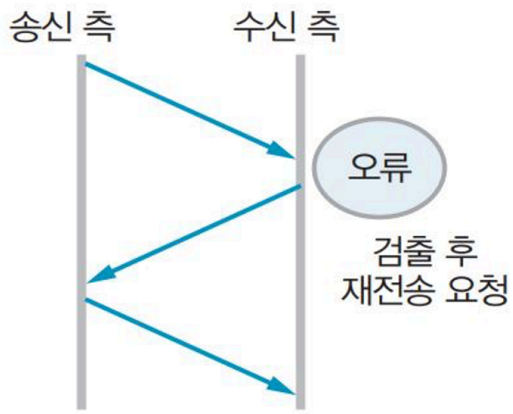
## 2. 전진오류수정(FEC)과 검출 후 재전송(ARQ)방식 비교

### 가. FEC와 ARQ의 오류제어방식 차이



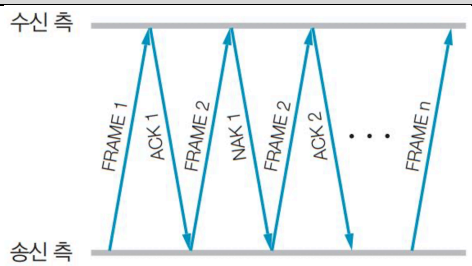
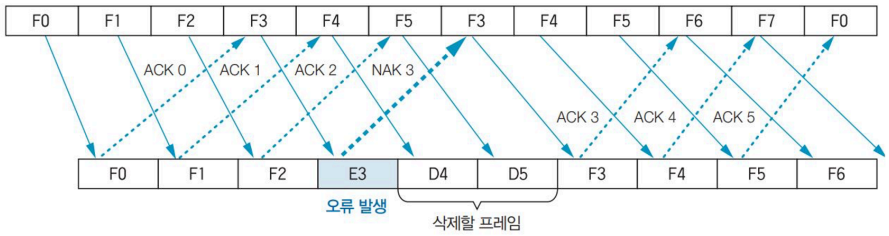
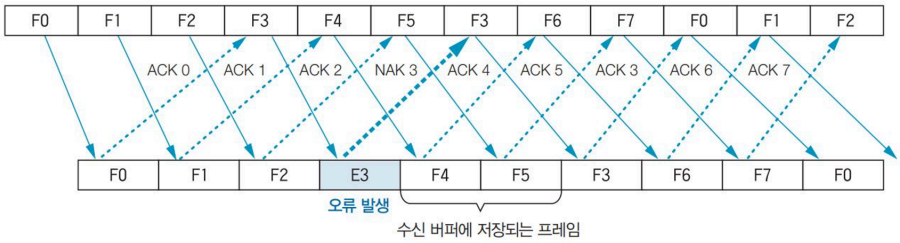

- FEC는 오류를 수신 측에서 자체적으로 정정하고 ARQ는 송신 측에 재전송 요청

### 나. FEC와 ARQ 비교

| 구 분 | FEC(Forward Error Correction) | ARQ(Automatic Repeat reQuest) |
|---|---|---|
| **오류제어 방식** |  |  |
| **원 리** | 수신 측에서 오류가 있음을 발견하면 오류를 검출 및 오류 자체 정정 | 오류가 발생하면 수신 측은 송신 측에 오류가 발생한 사실을 알리고 재전송 요청 |
| **장 점** | - 연속적인 데이터 전송 가능<br>- 전송 지연 없음<br>- 높은 효율성 | - 단순한 구조의 장비 사용<br>- 높은 전송 신뢰성<br>- 채널 적응 능력 우수 |
| **단 점** | - 잉여 비트에 의한 전송 채널 대역 낭비<br>- 장비 구조 및 코드 방식이 복잡 | - 역채널 구성 필요<br>- 송신 측은 프레임 저장을 위한 버퍼 필요 |
| **적용 환경** | - 무선 환경 | - 높은 데이터 정확도를 요구하는 채널 |

| | | |
|---|---|---|
| 종 류 | - Block code<br>- Convolution code | - Stop and Wait ARQ<br>- Continuous ARQ<br>- Adaptive ARQ |

### 3. ARQ 방식 3 가지

| 구 분 | | 설 명 |
|---|---|---|
| Stop and Wait ARQ | |  <br>- 송신 측에서 하나의 블록을 전송하면 수신 측은 오류 발생 여부 점검 후 ACK/NAK 응답<br>- 수신 측에서 응답을 받은 후 다음 프레임 전송하는 방식으로 효율이 떨어짐 |
| Continuous ARQ | Go-Back-N ARQ |  <br>- 송신 측에서는 프레임 연속 송신, 오류 발생 시 NAK+오류 프레임 번호 통보<br>- 송신 측에서는 오류 발생 프레임부터 나머지 프레임까지 재전송 |
| | Selective Repeat ARQ |  <br>- 송신 측에서는 프레임 연속 송신, 오류 발생 시 NAK+오류 프레임 번호 통보<br>- 송신 측에서는 오류 발생 프레임만 재전송 |
| Adaptive ARQ | | <br>- 전송 효율을 최대한 높이기 위해 데이터 블록의 길이를 동적으로 변경시켜 전송하는 방식<br>- 수신 측이 오류 발생률 판단하여 송신 측에 통보, 송신 측은 오류 발생률이 낮으면 긴 프레임, 높으면 짧은 프레임 전송 |

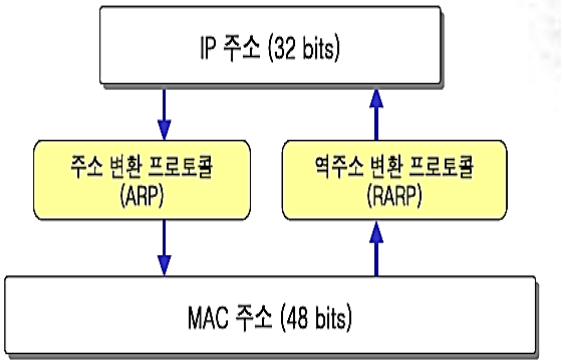
"끝"

**기출풀이 의견**

물어본 것이 많은 문제는 시간 내에 문제 별 적절한 양의 답안을 작성할 수 있도록 시간 관리에 특히 더 신경 쓰시는 것이 중요합니다.

| 4 | ARP, RARP |
|---|---|
| 문제 | ARP(Address Resolution Protocol)에 대하여 아래 사항들을 설명하시오.<br>가. ARP 와 RARP<br>나. IP 프로토콜을 사용하는 서버 또는 네트워크 장비에서 ARP 의 역할<br>다. ARP 와 관련된 아래의 보안 취약점 및 이들의 대응 방안<br>1). ARP Spoofing<br>2). ARP Redirect |
| 도메인 | 보안 |
| 정의 | -ARP : LAN 환경에서 논리적인 주소인 IP 주소를 물리적인 주소인 MAC 주소로 변환해 주는 네트워크 계층의 프로토콜<br>-RARP : 라우터등 특정 시스템이 MAC 주소는 알고 있으나 IP 주소를 모를 경우 MAC 주소를 IP 주소로 변환해주는 프로토콜 |
| 키워드 | 논리주소(IP), 물리주소(MAC), 주소변환, Broadcast, Unicast , Request, Reply<br>MITM 공격 방식, MAC 주소 속이기, 라우터 위장, ARP Cache Table<br>MAC Flooding, 정적 ARP 테이블 관리 |
| 출제의도분석 | ARP 와 RARP 의 기본 개념 이해 여부 확인<br>ARP 의 보안 취약점인 스푸핑과 리다이렉트에 대한 대응방안 인지여부 확인 |
| 답안작성 전략 | ARP 와 RARP 의 기본개념과 동작절차를 정확하게 기술하고 보안취약점인 ARP 스푸핑과 리다이렉트에 대한 상세한 접근이 필요 |
| 참고문헌 | KPC 보안 특강 자료<br>KPC 기출 풀이 해설집<br>정보보안 개론 (한빛 미디어) |
| 풀이 기술사님 | 박재성 기술사 (제 111 회 컴퓨터시스템 응용기술사 / kftc@naver.com ) |

## 1. 논리주소와 물리 주소 자동 변환 프로토콜 ARP 와 RARP




-호스트나 라우터로 패킷을 전달하기 위해서는 두 레벨의 주소지정이 필요

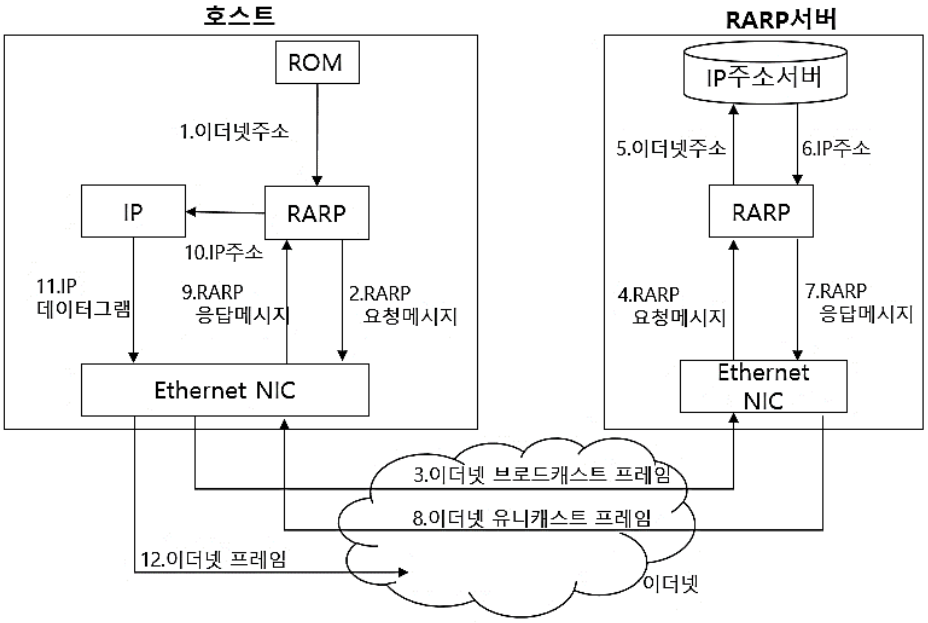
-논리 주소를 대응하는 물리 주소로 또는 그 반대로 변환하는 기능이 필요

### 가. ARP (Address Resolution Protocol)

| | |
|---|---|
| **개념** | -LAN 환경에서 논리적인 주소인 IP 주소를 물리적인 주소인 MAC 주소로 변환해 주는 네트워크 계층의 프로토콜 |
| **구성** | -Broadcast 인 ARP Request 와 Unicast 인 ARP Reply 쌍으로 구성 |
| **테이블 관리** | -동적 변환(dynamic mapping) : 송/수신자의 메시지 교환을 통해 ip 주소와 MAC 주소 변환 테이블을 동적으로 생성하는 ARP 프로토콜 이용 |

-ARP 는 물리주소를 논리주소로 변환하는 반면, RARP 는 논리주소를 얻기 위해 사용

### 나. RARP (Reverse Address Resolution Protocol)

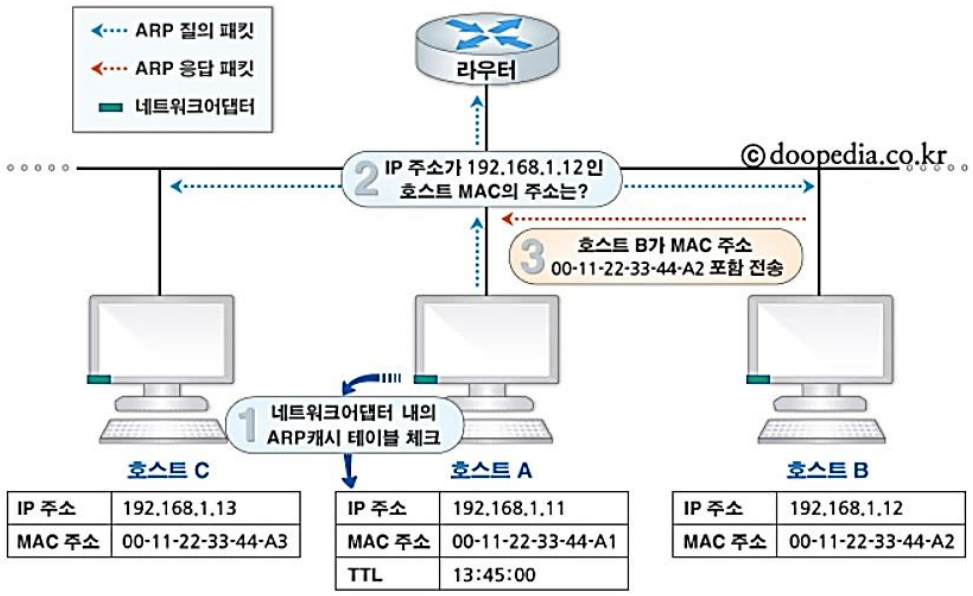
| | |
|---|---|
| **개념** | -라우터등 특정 시스템이 MAC 주소는 알고 있으나 IP 주소를 모를 경우 MAC 주소를 IP 주소로 변환해주는 프로토콜 (RFC 903) |
| **필요성** | -물리 주소는 알고 있으나 논리 주소를 모를 때 사용<br>-호스트의 IP 주소는 하드 디스크의 특정 위치에 보관<br>하드디스크가 없는 시스템은 LAN 카드에 내장된 자신의 MAC 주소는 알지만, 자신의 IP 주소는 알 수 없기 때문에 IP 주소 변환 RARP 필요. |
| **동작원리** |  <br><br>-① 모든 디스크리스 장비에 대한 하부망 주소와 대응되는 IP 주소 정보는 RARP 서버에 유지<br>-② 디스크리스 장비는 자신의 이더넷 주소(MAC 주소)를 담은 RARP 요청 메시지를 하부 통신망에 브로드캐스트.<br>-③ 브로드캐스트 프레임을 통해 RARP 요청 메시지를 수신한 RARP 서버는 IP 주소를 담은 RARP 응답 메시지를 해당 디스크리스 장비에게 전송.<br>-④ RARP 응답 메시지를 수신한 RARP 는 서버가 할당한 IP 주소를 IP 에게 전달 |

-RARP 는 IP 주소 이외의 추가정보를 얻을 수 없어 잘 사용하지 않으며, 대신 DHCP, BOOTP 를 많이 사용

-ARP 는 동일 네트워크 일 경우와 외부 네트워크일 경우로 나누어 역할을 수행

## 2. IP 프로토콜을 사용하는 서버 또는 네트워크 장비에서 ARP 의 역할

### 가. 동일 네트워크 ARP 동작 과정




①호스트 A 가 자신의 네트워크 어댑터 내의 **ARP Cache 테이블을 확인**

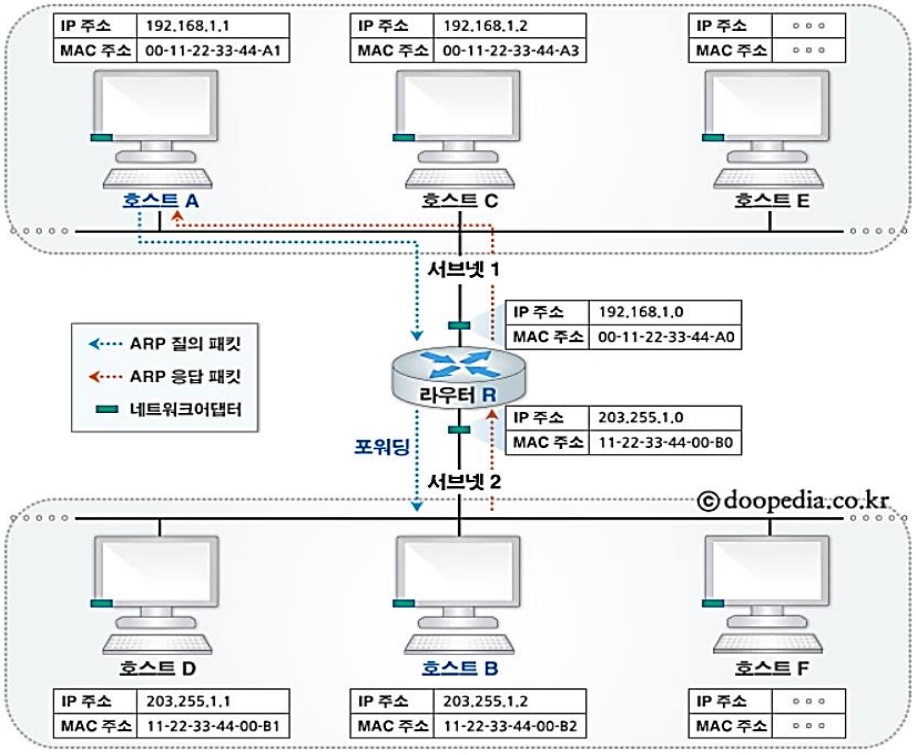
②ARP질의 패킷이 **Broadcast** (ARP 질의:IP 주소가 192.168.1.12의 MAC주소는 ?)

③호스트 B 는 ARP 응답 패킷을 호스트 A 로 전송 (**ARP Reply**)

④호스트 A 는 ARP 응답 패킷 주소를 이용해 자신의 **ARP Cache 테이블을 수정**

### 나. 외부 네트워크 ARP 동작 과정

-송신 호스트가 서브넷 상의 라우터의 MAC 주소를 이용하여 송신자로부터 목적지 경로상에 있는 첫 번째 라우터로 우선 전달



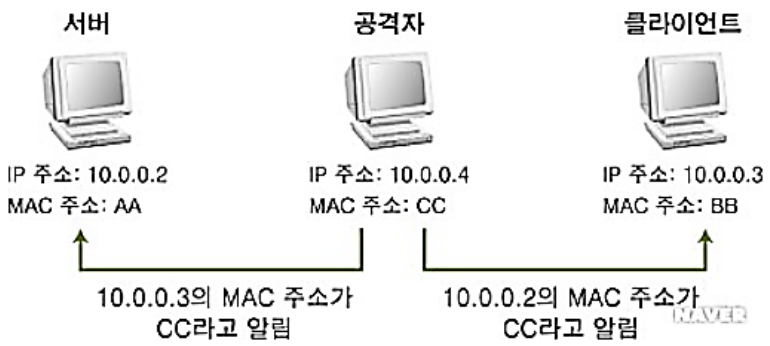
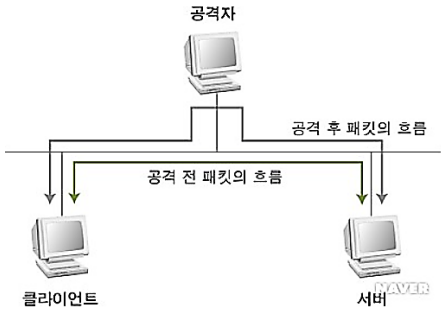
| |
|---|
| ① 서브넷 1 의 호스트 A 가 서브넷 2 의 호스트 B 로 IP 패킷을 전송<br>② 호스트 A 는 ARP 를 이용하여 R 의 MAC 주소를 획득<br>③ R 의 MAC 주소를 이용하여 호스트 A-B 간의 IP 패킷을 포함한 링크 계층 프레임 생성.<br>④ A 의 네트워크 어댑터에서 전송한 프레임을 R 에서 수신<br>⑤ R 은 ARP 를 이용하여 B 의 MAC 주소를 얻은 후 A 로부터 수신한 패킷을 B 로 전송 |

-ARP 는 Stateless 프로토콜이기 때문에 로컬 네트워크의 모든 호스트는 누가 요청을 보냈는지에 상관없이 자동적으로 캐시를 수행하고 또한 ARP 응답을 받아 Cache 테이블을 갱신함.

-어떤 호스트가 패킷을 보냈는지 인증수단을 제공하지 않기 때문에 취약점이 생기는데, 대표적인 취약점 공격으로는 ARP Spoofing, ARP Redirect 기법이 있음

## 3. ARP 의 보안 취약점 및 대응 방안

### 가. ARP Spoofing

| | |
|---|---|
| **개념** | -LAN 카드의 고유한 주소인 MAC address 를 동일 네트워크에 존재하는 다른 PC 의 LAN 카드 주소로 위장, 다른 PC 에 전달되어야 하는 정보를 가로채는 MITM 공격 방식 |
| **공격과정** |  <br>-공격자가 서버와 클라이언트 컴퓨터에 통신 상대방을 자기 자신으로 알렸기 때문에 서버와 클라이언트는 공격자에게 패킷을 전송<br>-공격자는 각자에게 받은 패킷을 읽은 후 서버와 클라이언트에게 서로 전송하려는 패킷을 전달 |
| **공격후 패킷** |  <br>증상)<br>① ARP Table 을 지속적으로 속이기 위해 ARP 패킷이 발송됨<br>② ARP Reply 패킷에 의한 ARP 패킷 수신량의 증가로 네트워크 응답 지연<br>- |

**대응방안**

| 구분 | 대응기법 | 설명 |
|---|---|---|
| 시스템 관리측면 | 정적 ARP 테이블 관리 | - ARP table 의 수동관리 통한 비정상 변경방지<br>- 재부팅 시에도 정정 TABLE 유지 |
| | 중요 패킷 암호화 | - 안전한 서버도 동일 서브넷 내 스푸핑된 서버에 의해 packet 스니핑 가능하기에 민감정보와 pw 암호화 수행 |
| | 보안수준 강화 | - 침입자가 설치한 프로그램으로 인해 네트워크 트래픽 변조 서버로 악용되지 않도록 서버보안 수준 강화 |
| 네트워크 관리측면 | MAC Flooding 관리 | - MAC 주소의 개수나 특정 MAC 주소 지정 네트워크 장비와 Host 시스템 양측에서 모두 정적인 ARP 관리 |
| | ARP 패킷검사 | - 방화벽의 동작과 유사하게 지정된 경로로만 ARP 패킷이 전송되도록 하는 기능을 사용 |
| | 사설 VLAN 기능활용 | - 동일 서브넷에서 지정된 호스트만 통신, 같은 서브넷의 서버도 통신 불필요 시 서로 격리 |

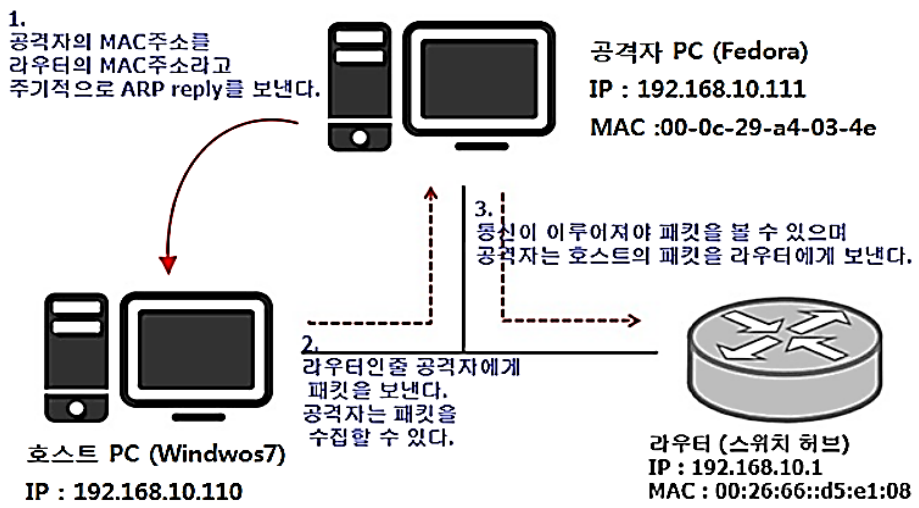
-ARP 항목의 정정관리를 통해 제 3 자의 개입을 어렵게 하여 방어 가능

### 나. ARP Redirect

**개념**

-라우터의 MAC 주소를 알아내어 공격대상에게 자신의 MAC 주소가 라우터인 것처럼 속인 후 브로드캐스트를 주기적으로 하여 패킷을 스니핑하는 기법

**공격과정**



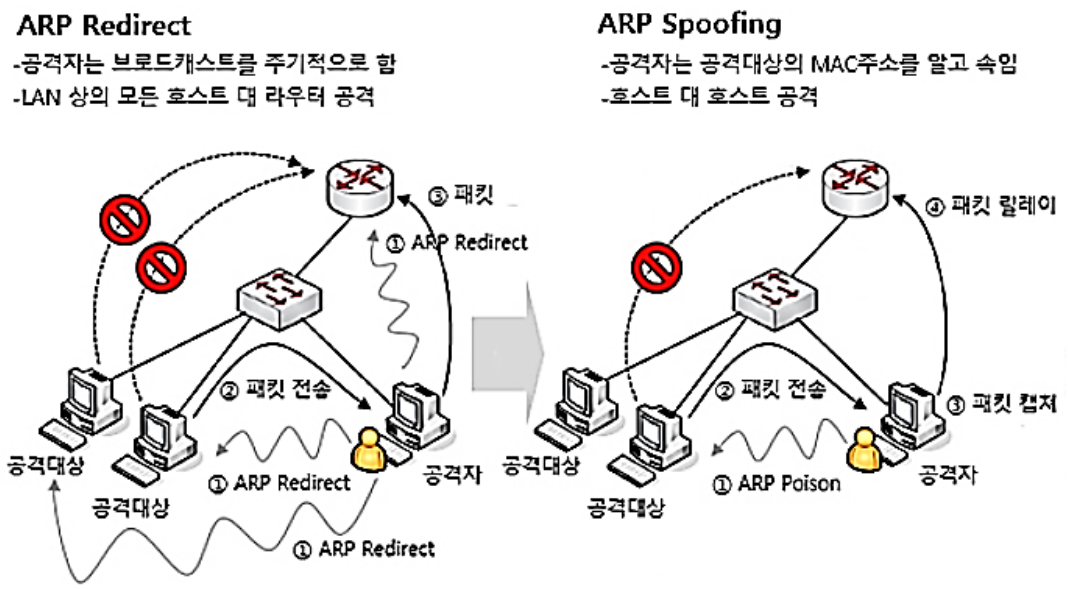

- 기본적으로 2 계층 공격, 랜에서 공격
- 공격자 자신은 원래 라우터의 MAC 주소를 알고 있어야 하며, 받은 모든 패킷은 다시 라우터로 릴레이 해줘야 함.

**대응방안**

- ARP 리다이렉트 공격 결과, 클라이언트 PC 의 ARP 테이블을 확인 해보면 라우터의 MAC 주소와 공격자의 MAC 주소가 중복

| | |
|---|---|
| | - ARP Cache table 의 내용을 static 으로 설정<br>- ARP Spoofing 대응방법과 동일 |

## 4. ARP Spoofing 과 ARP Redirect 관계




- ARP Spoofing 은 호스트 대 호스트 공격, ARP Redirect 는 랜의 모든 호스트 대 라우터라는 점 외에는 큰 차이가 없음

"끝"

| 3 | IPv6 |
|---|---|
| 문제 | IP 주소 부족문제를 해결하기 위한 IPv6 에 대하여 아래 사항들을 설명하시오.<br>가. IPv6 헤더 구조<br>나. 패킷 단편화(fragmentation)에 대해서 설명하고, IPv4 와 IPv6 에서의 처리 방식<br>다. 기존 IPv4 망에서 IPv6 망으로 전환하기 위한 방안 |
| 도메인 | 네트워크 |
| 정의 | IPv4 의 한계인 주소 표현의 제약으로 인한 주소고갈 및 멀티미디어서비스 대응 미약 등을 고려하여 IETF 의 IPng WG(2001.11 IPv6 개칭)에서 표준화시킨 차세대 인터넷 프로토콜 |
| 키워드 | 128 비트, MTU, 이중스택, 터널링 |
| 출제의도분석 | -. IPv6 의 상세 스펙과 패킨단편화의 방식을 확인하고 기존 IPv4 망에서 IPv6 망으로 전환하기 위한 다양한 방안을 숙지하고 있는지 확인 |
| 답안작성 전략 | -. 문제에서 물어본 것이 3 개로 이중 하나라도 정확하게 숙지하지 않았다면 자신있게 선택하기 힘들었을 문제임<br>-. 패킷단편화와 IPv4,IPv6 에서의 처리방식의 차이를 명확하게 제시<br>-. 기존 IPv4 망에서 IPv6 망으로 전환하기 위한 방안을 상세히 작성<br>-. 추가단락으로 IPv6 망으로 전환시 보안 위협과 대응방안 제시 |
| 참고문헌 | -. 한국정보통신기술협회<br>-. 차세대인터넷주소(IPv6) 전환 추진계획(방송통신위원회)<br>-. IPv6 환경의 보안 위협 및 공격 분석(전자통신동향분석) |
| 풀이 기술사님 | 박상현 기술사 (제 113 회 컴퓨터시스템응용기술사 / stepark.itpe@gmail.com) |

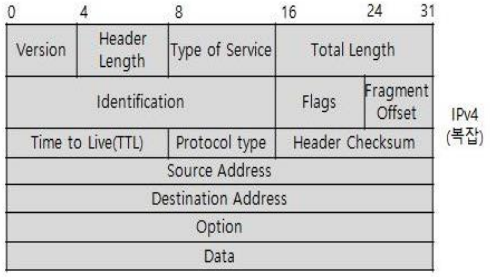
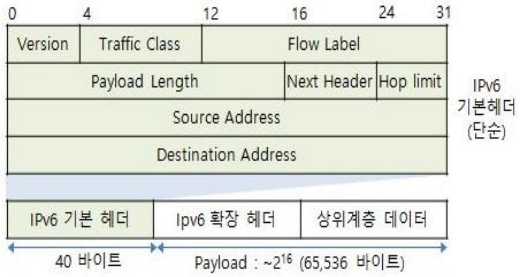
## 1. IP 주소 부족문제를 해결하기위한 IPv6 의 개요

| 구분 | 설명 | |
|---|---|---|
| IPv6 정의 | -. IPv6 주소는 총 2^128 개로 1998 년 IETF 에서 IPv4 주소부족 문제 해소와 무한대의 IP 주소 공급을 위해 개발한 차세대 인터넷주소 | |
| 등장배경 | 인터넷주소 수요급증 | 최근 유무선통합서비스 제공, 스마트 폰 보급 확산 등에 따른 무선 인터넷서비스 활성화로 인해 인터넷주소(IP) 수요가 급증 |
| | 인터넷주소 할당 종료 시점 도래 | 전세계 인터넷주소(IPv4)는 43 억개로 최근 IP 수요증가 추세로 볼 때 신규대응 불가능 |
| | 4 차 산업혁명 시대의 필수 불가결한 요소 | 스마트그리드, 스마트빌딩, 사물지능통신(M2M, IoT) 등 새로운 네트워크 융합 서비스 환경에서의 다양한 Smart 서비스 기반 제공을 위함 |

-. 인터넷주소(IPv4) 할당 종료시점이 가시화되고 있고, 차세대 인터넷서비스의 체계적인 준비를 위해 지금부터 본격적인 IPv6 전환의 가속화가 필요함

## 2. IP 주소 헤더 구조

**가.** IPv4 와 IPv6 의 헤더 구조 비교

| IPv4 | IPv6 |
|---|---|
|  |  |





-. IP 패킷의 앞부분에서 주소,길이등 각종 제어정보를 담고 있음

-. IPv6 는 주소길이를 128 비트로 확장하여 무한대의 주소개수를 할당할 수 있으며 헤더구조를 단순화하고 Flow Label 과 Next Header 를 추가하여 연결지향성, 확장성을 개선한 구조임

**나.** IPv4 와 IPv6 의 특징별 헤더 구조 비교

| 특징 | IPv4 | IPv6 |
|---|---|---|
| 헤더 크기 | 가변 크기 헤더 (옵션에 따라 달라짐)<br>32 비트짜리의 워드가 최대 15 개 (최대 60 바이트) | 고정 크기 헤더 (기본 헤더 40 바이트로 고정됨)<br>확장 헤더에 의해 연이어 붙여질 수 있으나, 기본 헤더 크기는 고정됨 |
| 주소 개수 | 약 43 억개 | 거의 무한대(43 억×43 억×43 억×43 억 개) |
| 주소 크기 | 32 비트 | 128 비트 |
| 옵션 | 옵션을 갖음. 그러나, 매우 드물게 사용 (IPv4 헤더 옵션) | 옵션 없음. 확장 헤더에서 옵션 역할 수행 (IPv6 옵션) |
| 헤더 길이 | 4 비트 | 삭제됨. IPv6 헤더는 고정 크기이므로 헤더 길이 필드는 불필요 |
| 혼잡 제어 | Type of Service 필드 | Traffic Class 필드 라고 호칭 |
| IPv6에 삭제된 필드 | -. Header Length(4 비트) : Ipv6 헤더 크기는 고정 크기<br>-. Identification(16),Flags(3),Fragment Offset(13 비트) : Ipv4 단편화시에 만 필요<br>-. Header Checksum(16 비트) : 데이터링크 신뢰성이 제고됨에 따라 삭제됨<br>-. Option : Ipv6 Payload에 포함됨 | |
| IPv6에 추가된 필드 | -. IPv6 Flow Label (20 비트) : IPv6 신규 추가됨. IP를 연결지향적 프로토콜로 사용할 수 있게 함. 실시간 서비스 등 같이 우선권을 주기위하여 특정 트래픽 Flow에 대한 라벨링<br>-. Next Header (8 비트) : IPv6 신규 추가됨. 기본헤더 다음에 위치하는 확장 헤더의 종류를 표시. IPv4의 프로토콜 번호와 같은 역할 | |

### 3. 패킷 단편화와 IPv4, IPv6 에서의 처리방식

#### 가. IP 패킷 단편화의 개념과 특징

| 구분 | | 설명 |
|---|---|---|
| 개념 | | -. 프로토콜 기본 교환 단위인 PDU(Protocol Data Unit)를 여러 더 작은 단위로 나누는 동작<br>-. 큰 IP 패킷들이 적은 MTU(Maximum Transmission Unit)를 갖는 링크를 통하여 전송되려면 여러개의 작은 패킷으로 조각화되어 전송되어야 함. |
| 특징 | 재조립(Reassembly) | 일단 단편화되면, 최종 목적지에 도달할 때까지 재조립되지 않는 것이 일반적임. 재조립은 항상 최종 수신지에서만 가능함 |
| | IPv4 | -. IPv4 에서는 발신지 뿐만 아니라 중간 라우터에서도 IP 단편화가 가능<br>-. IPv4 에서 MTU 최소 권고값 : 576 byte |
| | IPv6 | -. IPv6 에서는 IP 단편화가 발신지에서 만 가능<br>-. IPv6 에서 MTU 최소 권고값 : 1280 byte |

-. 단편화를 하는 이유는 기억장치의 낭비를 축소하고 공정한 엑세스, 네트워크 종류별로 다양한 크기 제약에 적응하기 위함

#### 나. IPv4 에서의 처리방식

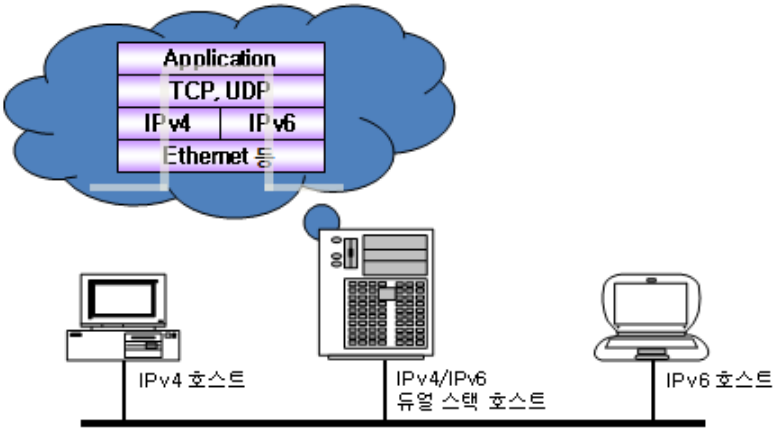
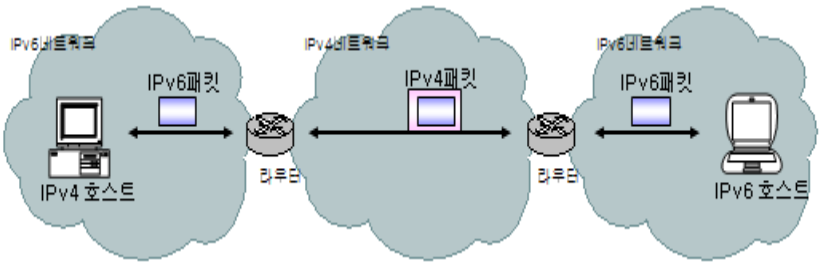
| 구분 | 처리 방식 | 설명 |
|---|---|---|
| 단편화 제어 필드 | Fragment Identifier (16 bits) | 각 조각이 동일한 데이터그램에 속하면 같은 일련번호를 공유함 |
| | Fragmentation Flag (3 bits) | -. 분열의 특성을 나타내는 플래그<br>-. 첫번 째 bit : 미사용 (항상 0) |
| | | -. 두번 째 bit : D F bit (Don't Fragment)<br>-. 분열(조각) 0 으로 셋팅되면 라우터에서도 분열(조각,단편)이 가능함을 뜻함<br>-. 미분열 1 로 셋팅되면 목적지 컴퓨터가 조각들을 다시 모을 능력이 없기 때문에 중간에 라우터로 하여금 데이터그램을 단편화하지 말라는 뜻임 |
| | | -. 세번 째 bit : M F bit (More Fragment)<br>-. 현재의 조각이 마지막이면 0, 더 많은 조각이 뒤에 계속 있으면 1 |
| | Fragmentation Offset (13 bits) | -. 8 바이트 단위(2 워드)로 최초 분열 조각으로부터 어떤 곳에 붙여야 하는 위치를 나타냄<br>-. 각 조각들이 순서 바뀌어 도착할 수도 있기 때문에 이 필드가 중요함 |
| 단편화 처리 | | -. 단편화 제어 필드(Fragment Identifier, Fragmentation Flag, Fragmentation Offset)는 IP 단편화(조각화,분열)과 재조립과 관련된 필드임.<br>-. 각 조각들은 최종 목적지 시스템에 전달되기 전에는 재조립되지 않고, 최종 목적지에 전달되면 목적지 시스템의 IP 소프트웨어가 원래의 데이터그램으로 재조립됨 |

**다. IPv6 에서의 처리방식**

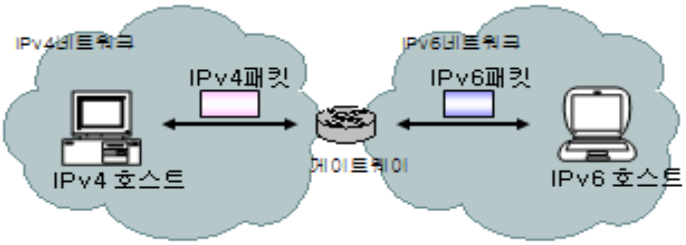
| 처리 방식 | 설명 |
|---|---|
| 헤더 확장 | -. IPv6 헤더 중 단편화 제어를 확장 헤더를 통하게 함<br>-. IPv4 와 달리, 기본 헤더 상에 단편화 제어 관련 필드를 두지 않고, 단편화 확장 헤더를 통해 단편화함 |
| MTU 크기 증가 | -. 기본 MTU 크기 증가<br>-. IPv4 최소 MTU 576 바이트 → IPv6 최소 또는 기본 MTU 1280 바이트 |
| 출발지 단편화 | -. 출발지에서만 단편화 시행<br>-. IPv4 와 달리, 경로 중간 라우터에서 단편화 시행 안함. 따라서, 발신지는 최소 MTU 1280 바이트로 발신해 보고, 경로 MTU 를 찾고, 이에 따라 단편화를 함 |

-. IPv6 에서는 라우팅 처리 효율을 높이기 위해, 가급적 IP 단편화를 필요없게 함

## 4. 기존 IPv4 망에서 IPv6 망으로 전환하기 위한 방안

| 기술 | 방안 | |
|---|---|---|
| 이중 스택 (Dual Stack) |  | |
| | IP 계층에 두 가지(IPv4, IPv6)의 프로토콜이 모두 탑재되어 있고 통신 상대방에 따라 해당 IP 스택을 선택하는 시스템 | |
| | 주소 설정 | -. IPv4 주소 : DHCP 기술을 사용<br>-. IPv6 주소 : 비상태형 주소 자동 설정(Stateless auto-configuration)<br>-. 이중 스택 시스템의 DNS 이름 해석, DNS 는 IPv4 와 IPv6 에서 모두 사용<br>-. DNS 주소해석기 라이브러리(DNS Resolver Library)가 A 와 AAAA 레코드를 모두 처리 |
| 터널링 (Tunneling) |  | |

Notes

| | | |
|---|---|---|
| | 어떤 프로토콜의 패킷을 다른 프로토콜의 패킷 안에 캡슐화하여 통신 | |
| | 설정 터널링 | -. 출발지/목적지의 호스트가 IPv6 호환 주소를 인식하지 못할 때 메뉴얼을 통한 정적 터널링<br>-. 6Bone(IPv6 Backbone)에서 사용 |
| | 자동 터널링 | -. IPv4 호환 주소(IPv4-compatible address)를 이용한 동적 터널링 (IPv6 패킷이 IPv4 네트워크를 경유하고자 할 때)<br>-. 6to4 터널링 방식, ISATAP(Intra-Site Automatic Tunnel Addressing Protocol) 방식이 사용 |
| IPv4/IPv6 변환 (Translation) |  | |
| | IPv4-IPv6 게이트웨이를 통해 서로 다른 네트워크 상의 패킷을 변환<br>네트워크 레벨의 게이트웨이 vs. 어플리케이션 레벨의 게이트웨이 | |
| | NAT-PT | -. IPv6, IPv4 네트워크 경계에서 주소변환을 수행<br>-. 프로토콜 변환 규칙을 기반으로 헤더 변환을 수행 |

-. IPv6 전환시 보안상의 위협요소인 프로토콜자체에서 발생되는 보안위협과 IPv4 연동환경에서 발생하는 보안위협을 파악하고 대응방안으로는 IPv6 환경에 맞는 방화벽, 라우터, 정책등이 필요함

-. 성공적인 IPv6 전환을 위해 국가 차원에서 정책적으로 IPv6 기반의 인터넷서비스를 활성화하고 전환이 취약한 중소기업을 지원하고 전환 전문인력을 양성하는 노력이 필요함

"끝"

| 6 | 라우팅(Routing) | | |
|---|---|---|---|
| 문제 | 네트워크 라우팅 기법 중 거리벡터라우팅(Distance Vector Routing)과 링크스테이트라우팅(Link State Routing) 기법을 설명하고, 두 기법의 차이점을 비교하시오. | | |
| 도메인 | 네트워크 | 난이도 | ★ ★ ☆ ☆ ☆ (별 5 개 기준) |
| 출제의도 | 기본토픽으로 라우팅 기법에 대한 이해 필요<br>(정보통신기술사 및 컴퓨터시스템응용기술사 기출문제) | | |
| 핵심 내용<br>키워드 | Metric 정보, 홉수(Hop count), 심볼길이(Symbolic length)<br>벨만-포드 알고리즘, 다익스트라 알고리즘 | | |
| 목차예시 | 1. 패킷을 목적지까지 전송 위한 최적경로배정, 라우팅 개념<br>2. 거리벡터 라우팅과 링크스테이트 라우팅 설명<br>3. 거리벡터 라우팅과 링크스테이트 라우팅 차이점 비교 | | |
| 채점 점수<br>가이드 | ① 개념, 이해 부족 (5~8점)<br>② 기본 이해 수준 (9~13점)<br>③ 정확한 기술 제시 (14~15점)<br>④ 추가요소 설명(+α) | | |
| 참고문헌 | KPC 모의고사 해설집<br>데이터통신과 컴퓨터 네트워킹, 강문식 저, 한빛아카데미 | | |
| 고득점전략 및<br>답안작성<br>가이드 | 비교 문제는 최대한 많은 비교항목 도출 필요.<br>답이 있는 문제로 라우팅 관련 키워드 배치로 고득점 가능 | | |
| 출제자 | 홍 OO 기술사(제 114 회 컴퓨터시스템응용기술사 / lkalover@naver.com) | | |


Copyright ⓒ 2015 By Korea Productivity Center Convergence Knowledge Center. All rights reserved

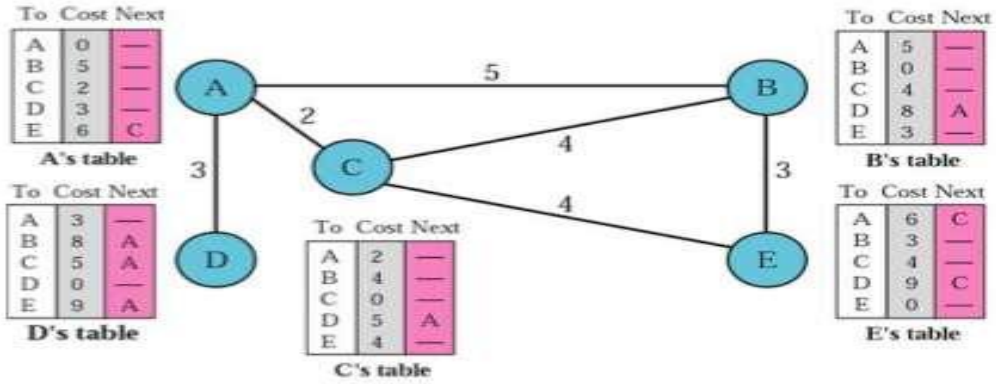
**1. 패킷을 목적지까지 전송 위한 최적경로배정, 라우팅 개념**

| 구분 | 설 명 | |
|---|---|---|
| 개념 | -N/W 상 임의의 location 에서 다른 location으로 패킷을 최적의 경로로 Forwarding 하는 과정<br>-N/W 의 logical topology 에 관한 정보를 주고 받고 logical topology 를 통해 배운 정보를 바탕으로 작성된 Map을 이용하여 Packet 을 전송하는 과정 | |
| 구성 | 라우터 | -네트워크계층에서 라우팅을 하기 위한 장비 |
| | 라우팅 알고리즘 | -최적의 경로설정을 위한 알고리즘 |
| | 라우팅 프로토콜 | -라우팅 정보를 주고 받기위한 프로토콜 |
| | 라우팅 테이블 | -라우팅을 위한 정보를 저장하는 데이터베이스 |

- 대표적인 라우팅 알고리즘으로 거리벡터(Distance Vector), 링크스테이트(Link State) 기법 존재

**2. 거리벡터 라우팅과 링크스테이트 라우팅 설명**

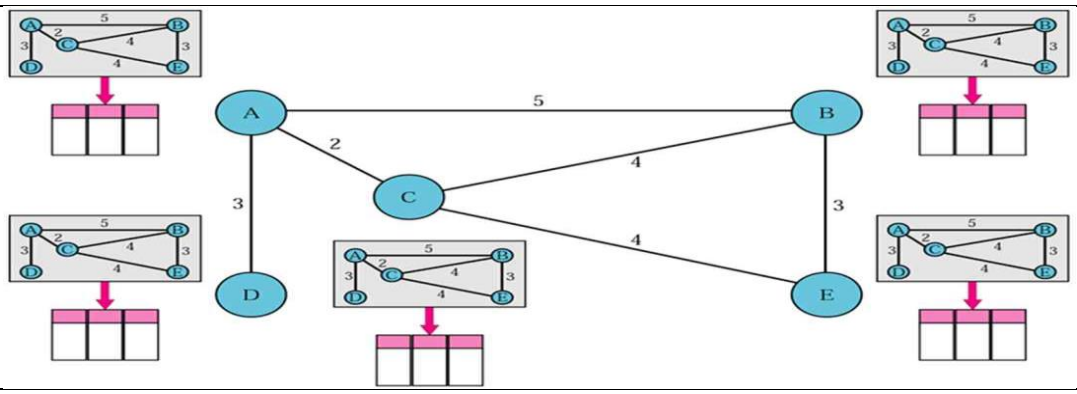
**가. 거리벡터 라우팅 설명**

| 구분 | 설 명 |
|---|---|
| 개념 | 각 라우터가 인접해 있는 라우터와 경로설정 정보를 교환하고 주기적인 갱신정보로부터 목적지 네트워크에 대한 라우팅 경로를 결정하는 기법 |
| 라우팅 구성도 |  |
| 동작과정 | 1)특정 라우터는 직접 연결된 이웃 라우터가 알려주는 최소 경로 비용 정보를 사용하여 모든 목적지 라우터로의 최소 경로 비용을 다시 계산<br>2)계산 결과 특정 목적지로의 최소 경로 비용이 변경되면 자신이 유지하고 있는 최소 경로 비용 테이블에 반영<br>3)이웃 라우터간에 최소 경로 비용 갱신에 대한 정보 교환이 없을 때까지 반복 |

-자신이 가지고 있는 정보를 주변 라우터와 주고 받으면서 라우팅을 빌드함

**나. 링크스테이트 라우팅 설명**

| 구분 | 설 명 |
|---|---|
| 개념 | 한 라우터가 목적지까지의 모든 경로 정보를 알고 토폴로지 DB를 기반으로 SPF(Shortest Path First) 알고리즘을 이용하여 라우팅 경로를 결정하는 기법 |

| | |
|---|---|
| 라우팅 구성도 |  |
| 동작과정 | 1) 개별 라우터는 자신과 직접 연결된 네트워크 정보를 담아 자신과 이웃한라우터에 전달<br>2) 개별 라우터는 자신의 LSP 생성, 다른 라우터는 flooding 과정 통해 LSP 받음<br>3) 개별 노드는 다른 모든 노드에 정보 전달<br>4) 신뢰성 있는 flooding: 전달 받은 라우터는 다른 라우터 정보를 수정하지 않고 자신의 정보와 함께 다른 라우터에게 전달<br>5) 전달된 자료 기반으로 모든 라우터는 전체 네트워크 구조 파악 |

-최초에 미리 네트워크 MAP을 그리고 난 후에 최단경로를 찾음. 다익스트라 알고리즘 사용.

### 3. 거리벡터 라우팅과 링크스테이트 라우팅 차이점 비교

| 차이점 항목 | 거리벡터 라우팅 | 링크스테이트 라우팅 |
|---|---|---|
| 패킷 전송 | 거리와 방향을 기준으로 전송 | 전체 토폴로지를 고려하여 전송 |
| 주요 메트릭 | Hop count | Symbolic length |
| 경로 설정 | 라우터 간의 거리를 더하여 계산 | 다른 라우터까지의 최단경로 계산 |
| 알고리즘 | 벨만포드 알고리즘 | 다익스트라 알고리즘 |
| 라우팅테이블 갱신 대상 | 인접한 라우터 | 동일 네트워크 내의 모든 라우터 |
| 갱신 시점 | 일정주기 | 링크상태 변화시(이벤트 기반) |
| 교환 정보 | 이웃한 라우터와 라우팅 테이블 교환 | 링크상태 정보만 교환 |
| 라우팅 테이블 정보 | 이웃 라우팅 정보 | 네트워크 전체 |
| 메모리 | 작은 라우팅 테이블, 메모리 절약 | 큰 라우팅 테이블, 큰 메모리 필요 |
| 전송 정보 | 자신이 알고 있는 모든 정보(포워딩 테이블 전체) 전송 | 변경된 정보만 전송 |
| 장점 | 1)모든 라우터 정보를 가질 필요가 없어 라우터 테이블 크기 감소<br>2)메모리 절약<br>3)구성 간단, 알고리즘 단순 | 1)컨버전스 타임이 빠름<br>2)라우팅 테이블 오버헤드 감소<br>3)이벤트기반으로 정보교환 트래픽 감소 |
| 단점 | 1)컨버전스 타임이 느림<br>2)주기적인 정보교환 발생, 대역폭 낭비<br>3)네트워크 변화 감지하는 시간 소요 | 1)큰 메모리 필요<br>2)SPF계산으로 HW부하 발생 |
| 프로토콜 | RIP, IGRP | OSPF, EIGRP |
| 라우팅 분류 | IGP | IGP |

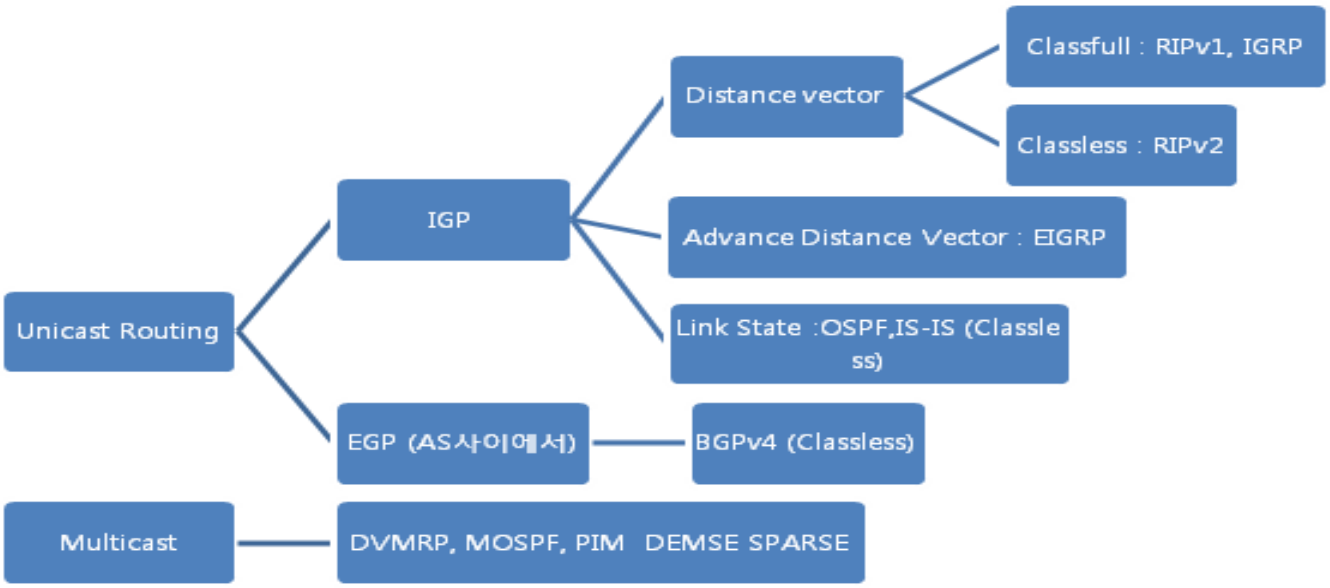

Copyright ⓒ 2015 By Korea Productivity Center Convergence Knowledge Center. All rights reserved

| 활용 | 소규모 네트워크 | 큰 규모 네트워크 |
|---|---|---|

- Distance Vector Algorithm 은 다루기 쉬운 반면, 대규모에 적용 어렵고, 장애 등의 원인 파악 어려운 단점 존재. 이러한 단점을 해결하기 위해서 Link State Algorithm 의 개발 활용

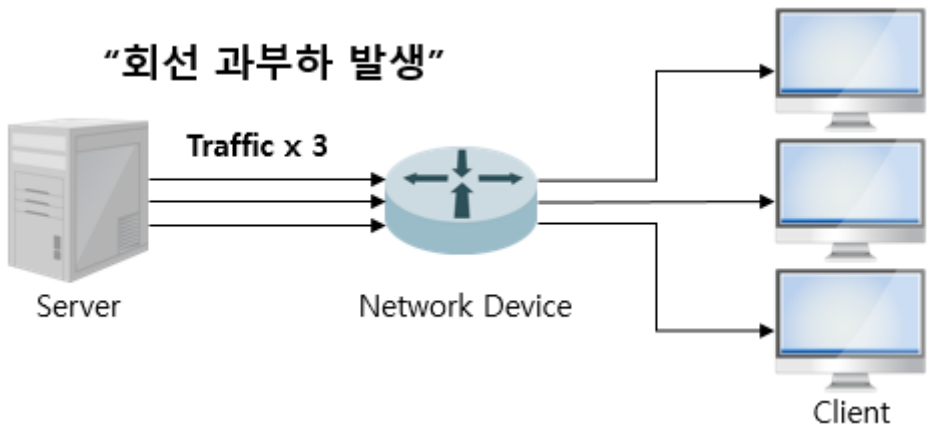
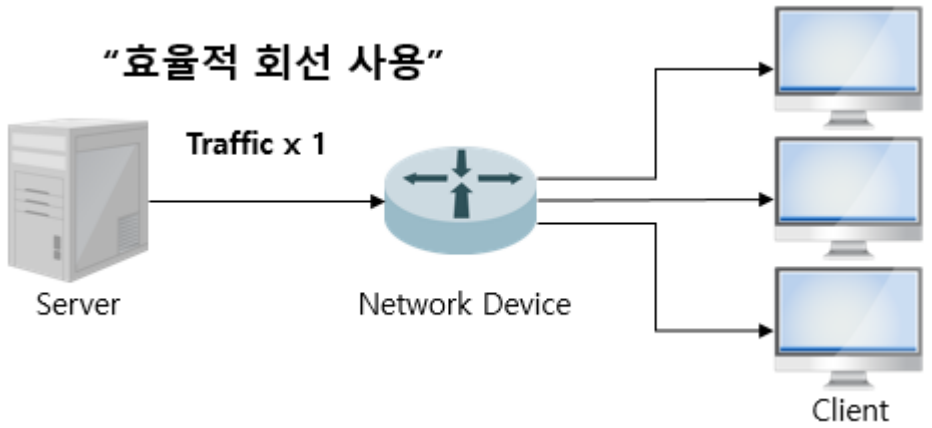
**[기타자료]**

**라우팅 유형**



| 1 | 멀티캐스트와 IGMP | | |
|---|---|---|---|
| 문제 | 네트워크를 효율적으로 이용하기 위한 멀티캐스트의 개념과 멀티캐스트 라우팅 프로토콜 유형에 대해 설명하고, IGMP(Internet Group Management Protocol)의 동작 과정과 메시지 유형에 대하여 설명하시오. | | |
| 도메인 | 네트워크 | 난이도 | ★ ★ ★ ☆ ☆ |
| 출제배경 | 실시간 스트리밍 서비스의 증가로, 효율적인 네트워크 구성을 위해 네트워크 이론의 기본이 되는 멀티캐스트 프로토콜과 IGMP 동작 과정, 메시지 유형에 대한 이해 여부 확인 | | |
| 핵심 키워드 | 멀티캐스트 라우팅 프로토콜: SBT (DVMRP, MOSPF, PIM-DM) / GST (PIM-SM, CBT)<br>멀티캐스트 그룹 관리 프로토콜 (IGMP): 가입, 멤버십 조사, 멤버십 연속, 탈퇴, Report / Query | | |
| 참고문헌 | 인터넷 멀티캐스트 라우팅 프로토콜 분석 (전자통신동향분석 14 권)<br>제 65 회 KPC 기술사 IMPACT 실전 모의고사 해설집 | | |
| 출제자 | 이시광 기술사(제 119 회 컴퓨터시스템응용기술사 / sk2ckr@naver.com) | | |

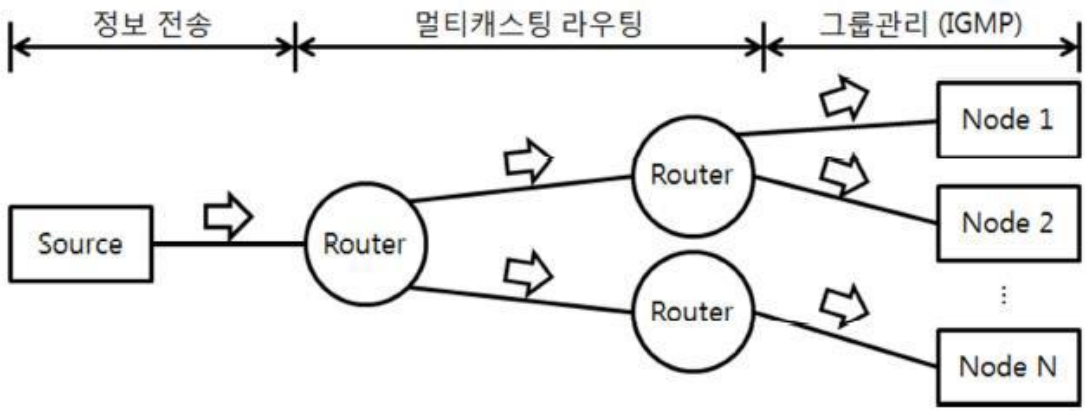
**1. 네트워크 자원 효율성 확보, 멀티캐스트의 필요성**

| | |
|---|---|
| Unicast 사용 시 문제점 |  <br>- 동일 데이터 다수 전송 시 Client 수만큼 트래픽이 발생하여 백본 회선 과부하 발생 가능 |
| Multicast 필요성 |  <br>- 동일 데이터 다수 전송 시 Client 수에 관계없이 최소 트래픽 발생, 효율적 회선 사용 |

Copyright ⓒ 2015 By Korea Productivity Center Convergence Knowledge Center. All rights reserved

## 2. 멀티캐스트의 개념과 프로토콜 유형

### 가. 멀티캐스트의 개념

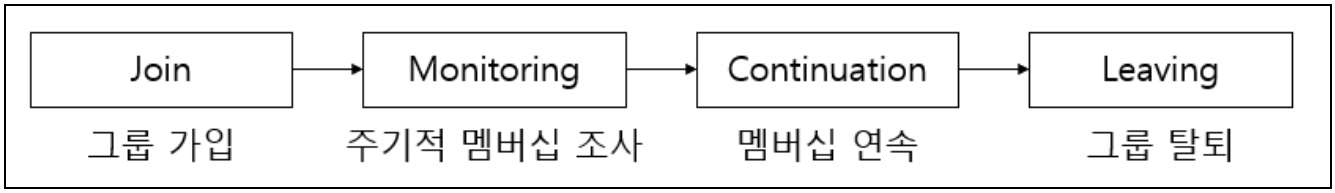
| | |
|---|---|
| 개념도 |  |
| 개념 | • 네트워크 대역폭 자원을 효율적으로 사용하기 위해 동일 데이터를 다수 노드의 특정한 그룹의 수신자들에게 동시에 전송할 수 있는 트래픽 전달 프로토콜 |

### 나. 멀티캐스트 라우팅 프로토콜의 유형

| 구분 | 라우팅 프로토콜 유형 | 프로토콜 설명 |
|---|---|---|
| 송신자 기반 트리 (Source-based Trees) | DVMRP (Distance Vector Multicast Routing Protocol) | - 각 목적지마다 최단 경로 브로드캐스트 트리 생성, 각 목적지들은 하나의 패킷만 수신하도록 보장하는 방식 |
| | MOSPF (Multicast Open Shortest Path First) | - OSPF 프로토콜의 확장 프로토콜 (다익스트라 알고리즘)<br>- OSPF 영역 내 모든 라우터는 같은 최단 경로 트리 구성 |
| | PIM-DM (Protocol Independent Multicast Dense Mode) | - 노드가 밀집되고 대역폭이 충분한 환경에 사용<br>- 각 라우터들이 멀티캐스트에 참여 가능성 높을 때 사용<br>- Flood and Prune 메커니즘: 입력 멀티캐스트 패킷을 다른 모든 인터페이스에 전파(Flooding)를 원칙으로 하고, 멀티캐스팅이 불필요한 곳마다 가지치기(Prune) |
| 그룹 공유 트리 (Group shared Trees) | CBT (Core-Based Tree) | - 랑데부 라우터만 그룹에 대한 최적 트리를 구성하여 각 그룹에게 전송하는 방식<br>- 송신측에서 랑데부 라우터에 데이터 전송 후 랑데부 라우터가 그룹 전체에 전송 |
| | PIM-SM (Protocol Independent Multicast Spare Mode) | - 노드가 분산되어 있고, 낮은 대역폭 환경에 사용<br>- 각 라우터가 멀티캐스팅에 참여 가능성이 낮을 때 사용<br>- Explicit Group Join 메커니즘: 모든 호스트가 멀티캐스팅 원하지 않다고 가정하며, 입력 멀티캐스트 패킷을 어떠한 인터페이스에도 포워딩하지 않음<br>- 필요 시 그룹 공유 트리에 각 수신자가 Join 하는 방식 |

### 3. IGMP 의 동작 과정과 메시지 유형

#### 가. IGMP 의 동작 과정




- IGMP 는 라우터와 네트워크 상 호스트와의 신호제어 프로토콜로 Query 와 Report Message 로 구성
- 라우터에서 네트워크에 존재하는 호스트들에게 주기적으로 Query Message 를 전송하여 멤버십 여부를 조사하고, 호스트는 라우터에게 Report Message 를 전송하여 멤버십 여부 응답
- 라우터에서는 Report Message 를 받아 멤버십을 관리하며, 무응답 호스트는 관리 그룹에서 제외

#### 나. IGMP 의 메시지 유형

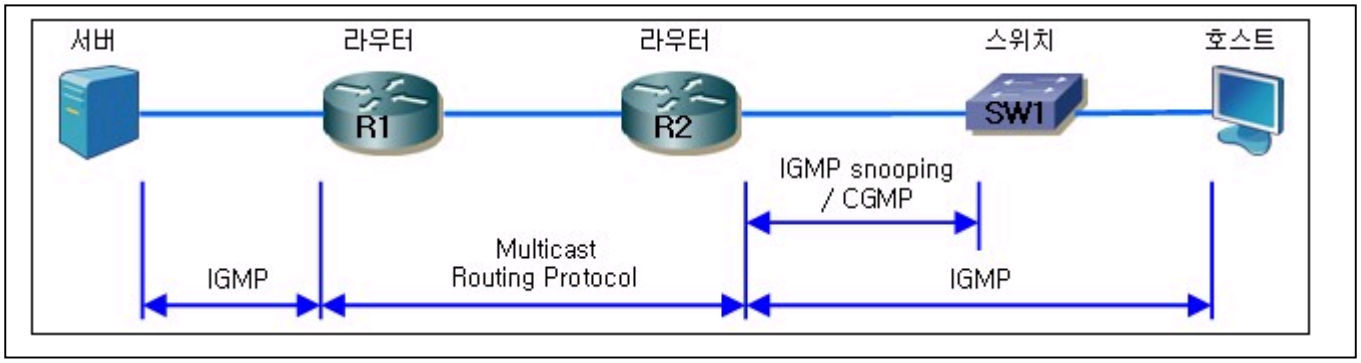
| 구분 | 메시지 유형 | 메시지 기능 설명 |
|---|---|---|
| 그룹 가입 (Membership Report) | | - 호스트는 그룹에 가입하기 위해 가입 요청 메시지 (Membership Report)를 멀티캐스트 라우터에 송신 |
| 일반 질의 메시지 (General Query) | | - 시스템이 갑자기 종료하여 탈퇴 메시지를 보내지 못할 상황에 대비 General query 전송<br>- General query 그룹주소는 0.0.0.0 으로 정의 |
| | | - 호스트가 탈퇴를 원하지 않으면 Membership Report 전송하여 그룹 유지<br>- 호스트가 탈퇴를 원하면 응답 메시지를 전송하지 않고, 라우터에서는 응답 메시지가 없으면 해당 호스트를 그룹에서 삭제 |
| 그룹 탈퇴 (Leave Report) | | - 탈퇴 요청 시 바로 탈퇴시키지 않음<br>- 호스트와 session 기반 메시지 전송하고 있는 그룹이 있을지 모르기 때문에 유지 |
| | | - 호스트가 진짜 종료를 원하는지 확인하기 위해 라우터에서 Special Query(특별 질의) 전송 |
| | | - 호스트가 탈퇴를 원하지 않으면 Membership Report 전송하여 그룹 유지<br>- 호스트가 탈퇴를 원하면 응답 메시지를 전송하지 않고, 라우터에서는 응답 메시지가 없으면 해당 호스트를 그룹에서 삭제 |

- IGMP 버전 1 의 경우에는 멀티캐스트 수신 호스트가 없음에도 불구하고 타이머(expire timer)가 만료되는 최대 3 분동안 불필요 멀티캐스트 스트림을 서브넷에 계속 전송하는 단점 존재


Copyright ⓒ 2015 By Korea Productivity Center Convergence Knowledge Center. All rights reserved

- 이를 해결한 것이 IGMP 버전 2 이며, IGMP 버전 2 에서 서브넷에서 멀티캐스트 그룹을 마지막으로 떠나는 호스트는 반드시 라우터에게 탈퇴(leave) 메시지를 전달하여 더이상의 멀티캐스트 수신을 원하는 호스트가 없음을 알림
- IGMP 버전 3 에서는 SSM(Source Specific Multicast) 기능 제공

**4. 효과적인 네트워크 사용을 위한 멀티캐스트 토폴로지**

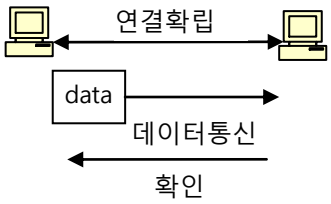
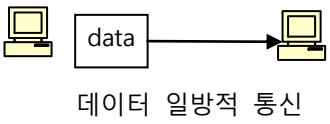



- 멀티캐스트는 라우터 간 멀티캐스트 프로토콜과 라우터-노드 간 IGMP 를 통해 효과적 트래픽 전송

"끝"

| 1 | 전송계층 프로토콜 |
|---|---|
| 문제 | TCP(Transmission Control Protocol)와 UDP(User Datagram Protocol) 프로토콜을 비교하여 설명하고, SCTP(Stream Control Transmission Protocol)을 상세하게 설명하시오. |
| 도메인 | 디지털네트워크 |
| 정의(개념) | UDP의 메시지 지향특성(Message-Oriented)과 TCP의 연결지향(Connection-Oriented) 및 신뢰성 특성을 조합한 차세대 전송 계층 프로토콜 |
| 키워드 | 메시지 지향, 연결지향, 멀티 호민, 멀티 스트리밍, 4-Way Handshaking, SACK |
| 목차제시 | 1. 전송계층 프로토콜의 개요<br>가. 전송계층 프로토콜의 문제점 나. TCP 와 UDP 의 비교<br>2. 차세대 전송계층 프로토콜 개념 및 특징<br>3. SCTP 프로토콜의 계층구조 및 동작절차<br>4. SCTP 프로토콜의 활용 |
| 출제배경 | All-IP 환경의 저변이 확대됨에 따라 차세대 전송 프로토콜에 대한 출제 가능성 증대 |
| 답안작성 전략 | 1 단락에서 기존 전송 프로토콜의 문제점을 TCP / UDP 비교를 통해서 설명<br>2 ~ 3 단락에서 문제점을 개선한 SCTP 프로토콜의 특징, 계층구조, 동작절차 설명<br>4 단락 SCTP 프로토콜의 활용 설명 |
| 난이도 | ★ ★ ★ ☆ ☆ (별 5 개 기준) |
| 참고문헌 | KPC 모의고사 |
| 출제자 | 김복주 기술사 (제 98 회 정보관리 / bjkim2004@gmail.com) |

■ **TCP 프로토콜과 UDP 프로토콜의 비교**

| 구분 | TCP | UDP |
|---|---|---|
| 정의 | 3,4 계층의 통신 프로토콜 집합으로 연결지향적(Connection Oriented) 설정을 제공하는 프로토콜 | 제어용 메시지 처리나 빠른 응답을 요구하는 응용서비스를 위하여 비연결형(Connectless) 설정을 제공하는 프로토콜 |
| 데이터순서 | 보내는 순서를 유지함 | 순서를 유지하지 않음 |
| 데이터중복 | 데이터 중복, 손실 없음 | 데이터 중복, 손실가능 |
| 에러제어 | 헤더 및 데이터에 대한 에러 검사 후 에러시 재전송 | 헤더 및 데이터에 대한 에러 검사 후 에러시 재전송 하지 않음 |
| 흐름제어 | 슬라이딩 윈도우 사용 | 흐름제어 없음 |
| 개념도 |  |  |
| 종류 | Telnet, FTP, SMTP | SNMP, TFTP |
| 장점 | 신뢰성 있는 경로 확립<br>메시지전송 감독<br>메시지를 세그먼트로 분할 전송 | 단순한 헤더<br>방송용 동영상 정보전송<br>멀티캐스트용 MBone |

Copyright ⓒ 2013 By Korea Productivity Center Convergence Knowledge Center. All rights reserved

| | | |
|---|---|---|
| | | 메시지 블록단위 전송 |
| 단점 | 전송에러 계속 감시<br>손실시 재전송 | 간단한 에러검사 기능<br>안전전송 여부확인 못함 |

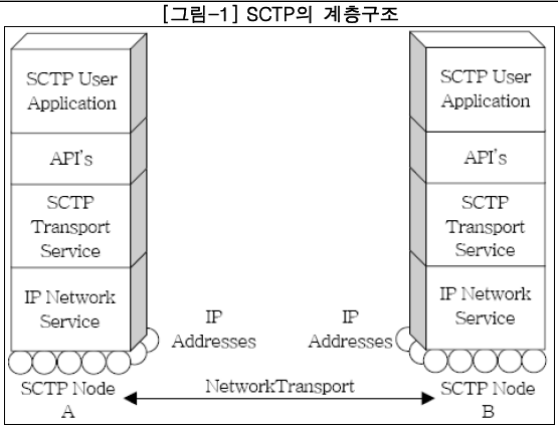
■ **SCTP(Stream Control Transmission Protocol) 프로토콜 개념**

- UDP의 메시지 지향특성(Message-Oriented)과 TCP의 연결지향(Connection-Oriented) 및 신뢰성 특성을 조합한 프로토콜로서, 멀티스트리밍(Multi-Streaming), 멀티호밍(Multi-homing)의 기능을 제공하는 차세대 전송 계층 프로토콜

■ **SCTP(Stream Control Transmission Protocol) 프로토콜 특징**

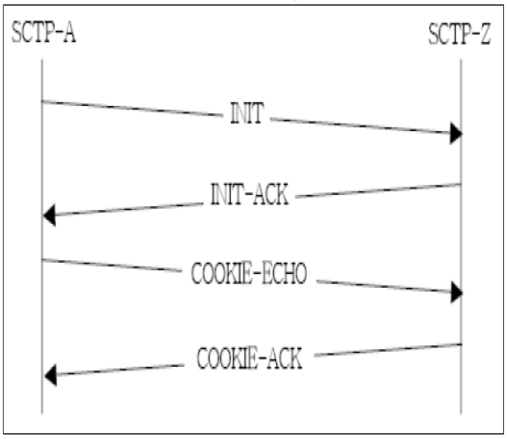
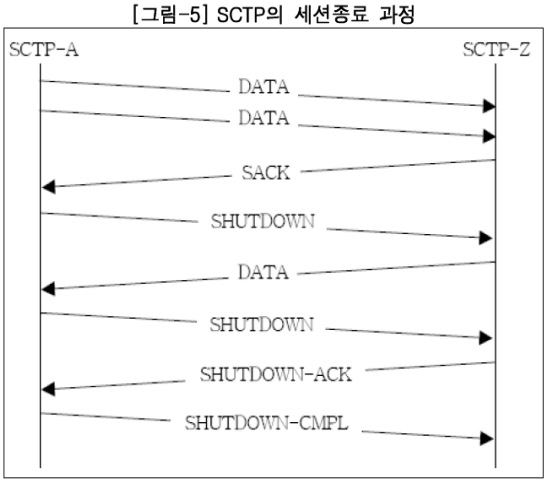
| 요구기술 | 설명 |
|---|---|
| 멀티호밍<br>(Multi-homing) | - SCTP 세션이 여러 개의 IP 주소를 동시에 사용<br>- 세션도중 네트워크 장애가 발생하는 경우 대체경로, 혹은 대체 IP 주소를 통해 세션 유지 |
| 멀티스트리밍<br>(Multi-streaming) | - 하나의 세션을 통해 다양한 종류의 응용데이터 전송<br>- 세션 초기화 단계에서 송신자는 전송할 스트림의 개수를 수신측에 통보, 전송 단계에서 각 스트림별 독립적으로 순서화(ordering) |
| 4-Way Handshake | - 초기화 과정에서 SCTP 는 TCP 의 3-Way Handshake 와는 달리, 4-Way Handshake 절차를 사용<br>- 외부의 DoS 공격 및 TCP SYN 공격 방지 |
| 세션 인증 및 SACK 메커니즘 | - SCTP 세션 초기화 과정에서, SCTP Endpoint간에 쿠키를 사용하여 인증을 위한 키 정보를 교환<br>– 세션 도중에 데이터 수신여부 및 재전송요구 등을 나타내기 위해 수<br>신자는 SACK(Selective ACK) 신호를 송신측에 전송 |
| 흐름 및 혼잡 제어 | - 흐름제어는 Association 별로, 혼잡제어는 전송경로 별로 수행<br>- 흐름제어를 위해 각 SCTP Endpoint는 수신 윈도를 송신자에게 통보하고, 혼잡제어를 위해 Congestion 윈도 크기를 적절히 조절 |

■ **SCTP(Stream Control Transmission Protocol) 프로토콜의 계층구조**

| 계층구조 | 설명 |
|---|---|
| [그림-1] SCTP의 계층구조<br>  <br> | - SCTP는 응용 계층과 네트워크 계층 사이에 위치<br>- SCTP peers 간에 응용 데이터를 APIs로 전달 받아 IP 망을 통해 전송하는 기능을 수행<br>- 각 SCTP 단말은 하나의 SCTP 세션에서 여러 개의 IP 주소를 사용<br>- 두 SCTP 지점간의 SCTP 연결을 "SCTP Association"이라 함 |

Copyright ⓒ 2013 By Korea Productivity Center Convergence Knowledge Center. All rights reserved

■ **SCTP(Stream Control Transmission Protocol) 프로토콜의 동작절차**

| 세션연결 | 세션종료 |
|---|---|
| - SCTP 세션종료 절차는 TCP의 3단계와는 달리, 4단계로 구성<br>- 세션에 대한 사용자 인증 및 TCP-SYN 보안 취약점 문제 해결 | - SCTP 세션종료 절차는 TCP의 4단계와는 달리, 3단계로 구성<br>- TCP의 half-open closing을 해결함으로써 프로토콜 상태관리를 최적화 함. |
| [그림-3] SCTP의 4-Way Handshake<br>  <br> | [그림-5] SCTP의 세션종료 과정<br>  <br> |

■ **SCTP(Stream Control Transmission Protocol) 프로토콜의 응용분야**

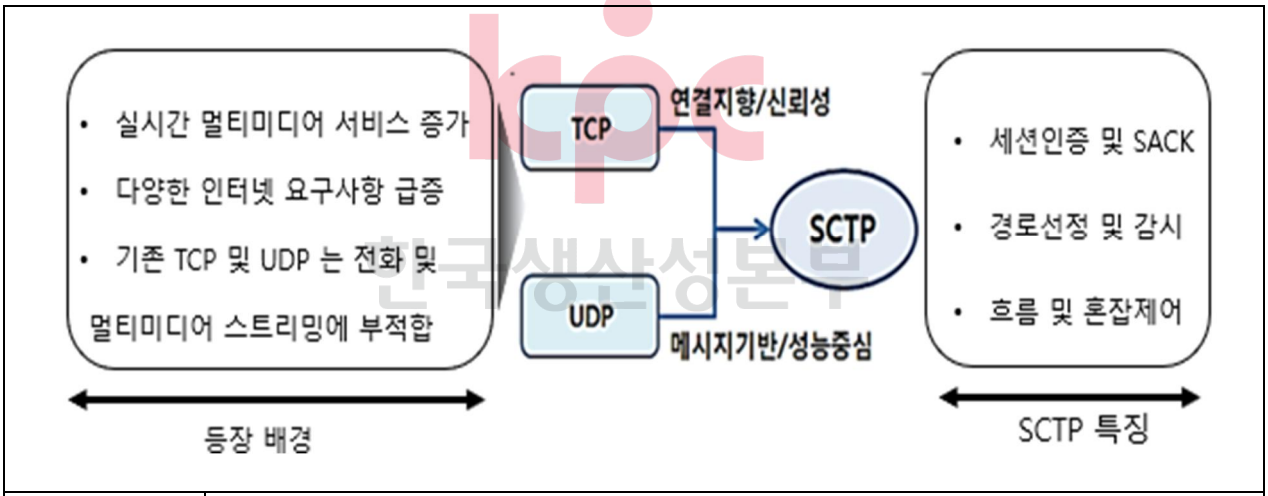
- VoIP 신호 전달, 실시간 다중 미디어를 전송하기 위한 웹 응용
- AAA(Authentication, Authorization, Accounting)등의 고도의 신뢰성을 요구하는 보안 응용
- 최근 이슈화 되고 있는 All-IP기반 이동통신망에서 핸드오버 기능을 용이하게 제공

Copyright ⓒ 2013 By Korea Productivity Center Convergence Knowledge Center. All rights reserved

| | | | |
|---|---|---|---|
| 문 제 | 4. SCTP(Stream Control Transmission Protocol)와 관련하여 다음을 설명하시오<br>가 . SCTP 개요와 특징<br>나 . SCTP 프로토콜 (Protocol) 구조 및 동작 방식 | | |
| 출 제 영 역 | 네트워크 | 난 이 도 | ★★★☆☆ (별 5 개 기준) |
| 출 제 배 경 | 고전 네트워크 토픽에 대한 숙지 | | |
| 출 제 빈 도 | 미출제 | | |
| 참 고 자 료 | - SCTP 표준기술 분석 및 전망, 고석주(S.J. Koh) 외 3 인<br>- https://patents.google.com/patent/KR20090024051A/ko | | |
| Keyword | TCP, UDP 연계, 멀티호밍, 멀티스트리밍, ACK | | |
| 풀이 기술사님 | 박은지(131 회 정보관리기술사 / melinda_u@naver.com ) | | |

## 1. RFC 4960, SCTP 개요와 특징

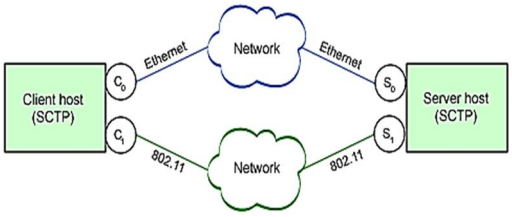
### 가. UDP 와 TCP 장점 수용, SCTP 개요

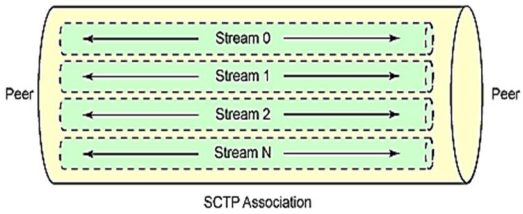
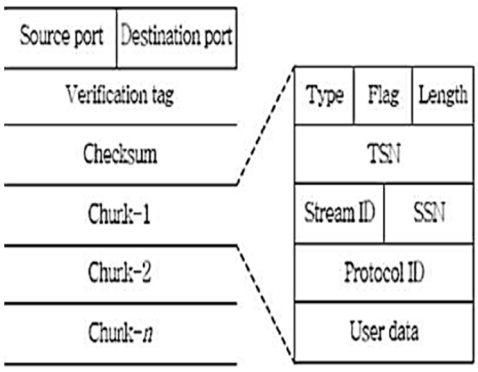



| | |
|---|---|
| 정의 | UDP 메시지 지향 특성과 TCP 연결 지향 및 신뢰성을 조합한 전송 계층 프로토콜 |

- UDP 와 TCP 의 장점을 수용하며 연결지향성 및 스트림 기반 프로토콜로 진화

### 나. SCTP 특징

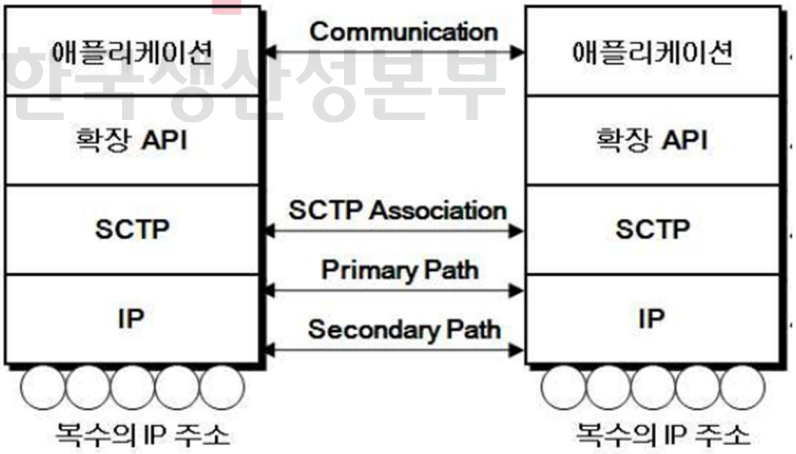
| 특징 | 개념도 | 상세 설명 |
|---|---|---|
| Multi-Homing |  | • SCTP 세션이 여러 개의 IP 주소를 동시에 사용할 수 있도록 하며, 세션 도중 네트워크 장애 발생시 대체 경로 통해 세션 유지<br>• 신뢰성 향상 |

| | | |
|---|---|---|
| **Multi-Streaming** |  | • 하나의 세션을 통해 다양한 종류의 응용데이터를 보낼 수 있는 기술<br>• 성능 향상 |
| **신뢰성 있는 메시지 지향적인 프로토콜** |  | • SCTP 의 데이터 단위는 데이터 청크(chunk)<br>• 128 bit 지원 – TCP 32bit 대비 개선<br>• 연결 : Association 통해 상호 연결 후 데이터 전송<br>• 신뢰성 : 오류제어, 흐름제어, 응답확인 |

- Datagram 지향성과 순서성 및 신뢰성을 결합함과 동시에, 멀티호밍 환경에서 다중스트림 및 메시지 지향성 전달 특징을 가짐

## 2. SCTP 프로토콜 (Protocol) 구조

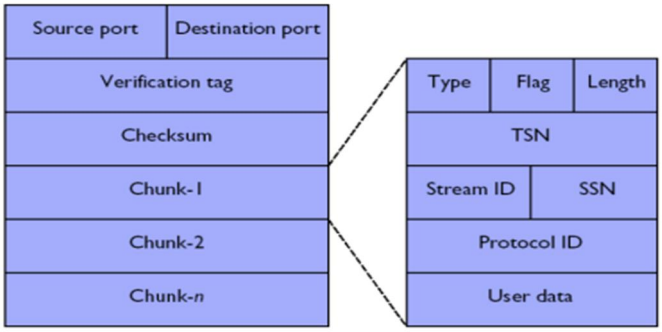
### 가. SCTP 프로토콜 계층구조

| | |
|---|---|
| **계층구조** |  |
| **설명** | - SCTP는 응용 계층과 네트워크 계층 사이 위치<br>- SCTP Peer 간 응용 데이터를 API로 전달받아 IP 망을 통해 전송하는 기능 수행<br>- SCTP 단말은 하나의 SCTP 세션에서 여러 개의 IP 주소를 사용 (Multi-homing)<br>- 두 지점 간에 메시지 전송 위해 다중 경로 및 다중 스트림 기능 사용 |

- 두 SCTP 지점 간의 SCTP 연결을 SCTP Association 이라 지칭함

kpc 한국생산성본부

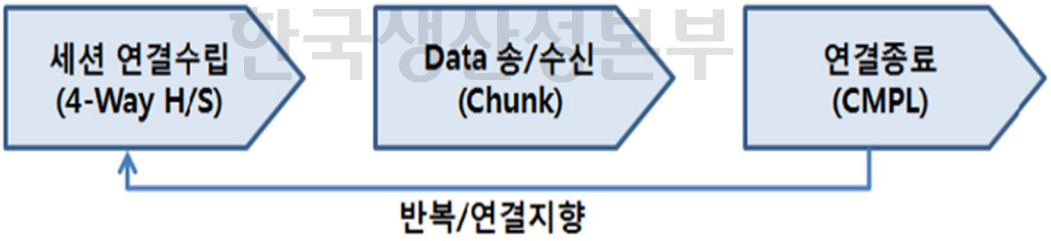
나. SCTP 패킷 구조

| | |
|---|---|
| 계층구조 |  |
| 설명 | - SCTP 패킷의 헤더에는 송신자 포트번호 (16 bits), 수신자 포트번호 (16 bits), verification tag(32 bits) 및 전체 패킷에 대한 Checksum (32 bits) 정보가 포함<br>- SCTP 패킷은 DATA chunk와 함께 여러 개의 제어(control) chunks를 사용<br>- 추후 SCTP 확장 작업과 함께 제어 chunk의 수는 증가할 수 있음 |

- Data chunk 의 경우 Type, Length 정보와 함께 해당 데이터 chunk 에 대한 TSN, SSN 번호를 포함하여, 추후 오류제어 및 흐름제어 등에 사용
- 전송 절차는 연결 초기화> 전송> 종료의 3 단계로 구성됨

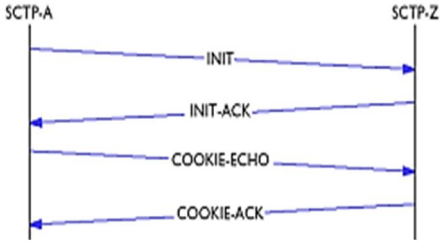
## 3. SCTP 프로토콜 (Protocol) 동작 방식

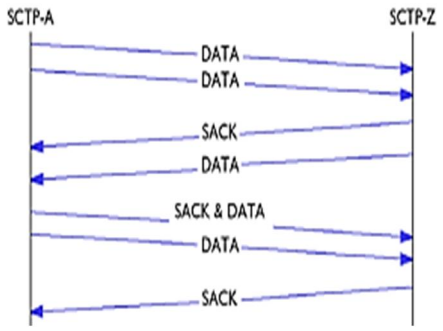
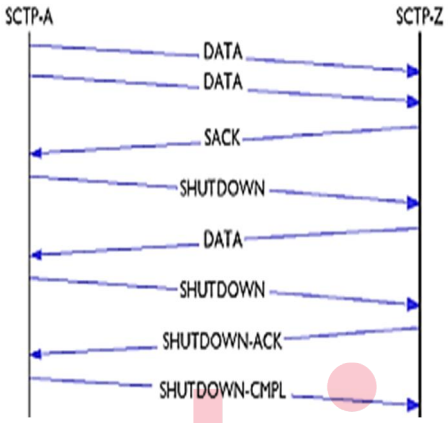
나. SCTP 동작 전체 매커니즘




- 4 Way handshake 로 연결 설정 후 3 way handshake 로 세션 종료

가. SCTP 동작 방식 상세 설명

| 단계 | 동작 구성도 | 세부 절차 |
|---|---|---|
| 1. 4-way Handshake 세션연결 수립단계 |  | 1) 세션 초기화 시작, 연결요청<br>2) INIT 요청 응답처리<br>3) COOKIE-ECHO 송신 – 서버 상태쿠키 답장으로 세션설정 마무리<br>4) COOKIE-ACK: ECHO 메세지 응답 |

| | | |
|---|---|---|
| **2. Data 송/수신** |  | 1) SACK(Selective ACK) 통하여 신뢰성 있는 송수신 처리<br>2) 재전송 타이머 및 흐름제어 고려<br>3) SACK Chunk 는 데이터 Chunks 와 동시 전송가능 |
| **3. 3-way Handshake 세션연결 종료** |  | 1) TCP 와 달리 3 단계 구성<br>2) TCP Half Open 문제 해결로 프로토콜 상태관리 최적화<br>3) Data 전송 종료 요청, Shutdown 메시지 전송<br>4) Shutdown Complete 로 세션종료 |

- SCTP 는 Half-Open, Half-Closed 상태를 지원하지 않음, 두 개체의 데이터 전송 종료가 통합적으로 이뤄짐
- 송신측은 Shutdown timer 를 가동하여 Shutdown ACK 가 오지 않는 경우 SHUTDOWN 메시지 재전송 가능

kpc 한국생산성본부

### 4. SCTP 발전 현황

| | |
|---|---|
| PR-SCTP (Partial Reliable SCTP) | • 실시간 응용을 위해 제정<br>• SCTP 데이터 전송 도중에 "time-critical" 스트림에 대해서는 오류제어를 중단하고 곧 바로 응용계층에 전달될 수 있는 기능을 정의 |
| Mobile SCTP | • 세션 도중에도 신규 IP 주소를 세션에 등록하거나 혹은 삭제하는 기능을 제공<br>• 이동 단말이 세션 도중에 다른 IP 망으로 이전하게 되는 경우에, seamless handover 기능 지원을 위해 필수적으로 요구되는 사항 |

- 실시간 멀티미디어 전송 및 고도의 신뢰성이 요구되는 앱 및 IP 이동성이 필요한 차세대 이동통신망에서 긍정적으로 사용이 검토됨

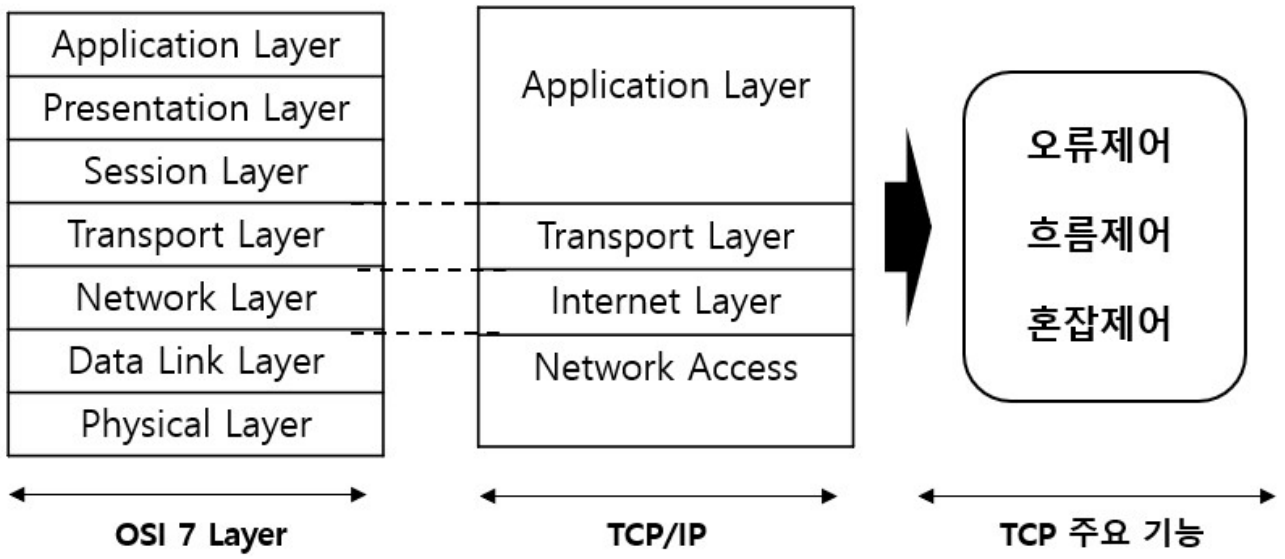
"끝"

**기출풀이 의견**

4. 네트워크 고전문제로 SCTP가 출제되었습니다. TCP와 UDP의 장점을 혼합한 제정 배경과 Handshake 및 멀티호밍, 멀티 스트리밍의 특징 및 절차를 명시하여 SCTP 의 고유 특징 측면을 제시하고 추후 활용방안까지 제시하면 좋은 답안 흐름으로 작성될 것으로 보입니다.

| 종목 | 컴퓨터 시스템 응용 | 문제번호 | 3교시 1번 |
|---|---|---|---|
| 1. TCP(Transmission Control Protocol)의 신뢰성 있는 전송을 가능케 하는 오류제어, 흐름제어, 혼잡제어에 대하여 설명하시오 | | | |
| 출제영역 | 네트워크 | 난이도 | 하 |
| 참고문헌 | 서브노트 | | |
| 주요 키워드 | 흐름제어: Sliding window, Window 크기 = 최소값(rwnd, cwnd)<br>오류제어: 세그먼트 재전송, p-ACK, Sequence number<br>혼잡제어: Slow-Start, Congestion Avoidance, Fast Retransmission, Fast Recovery | | |
| 답안전략/의견 | TCP 프로토콜의 개념, 기본 송수신 절차 및 흐름제어, 오류제어, 혼잡제어에 대한 정확한 이해 및 가독성 있는 도식 표현 | | |
| 작성자 | 이상헌 PE / bluesanta97@naver.com | | |

## I. 종단간 통신을 신뢰할 수 있도록 하는 Protocol, TCP의 개요

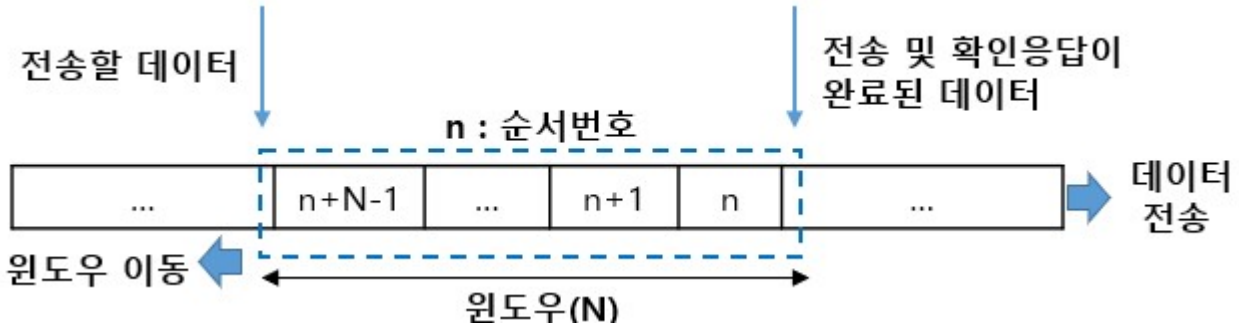



| 개요 | 설명 | |
|---|---|---|
| 정의 | OSI 7 Layer의 Transport Layer에 해당하며 양 종단 호스트 내 프로세스 상호 간에 신뢰적인 연결 지향성 서비스를 제공하는 프로토콜 | |
| 특징 | 신뢰성 | 패킷 손실, 중복, 순서 바뀜 등이 없도록 보장 |
| | 느린 속도 | 신뢰성 있는 주요 기능으로 인하여 UDP 보다 속도가 느림 |
| | 양방향성 | 종단간 양 프로세스가 서로 동시에 세그먼트를 전달 할 수 있음 |
| | Unicast | 종단간 1:1 전송 방식으로 단일 송신자와 수신자간 연결 설정 |

- 상호간 신뢰성 있는 데이터 통신을 구현하기 위하여 오류제어, 흐름제어, 혼잡제어와 같은 기술이 필요함.

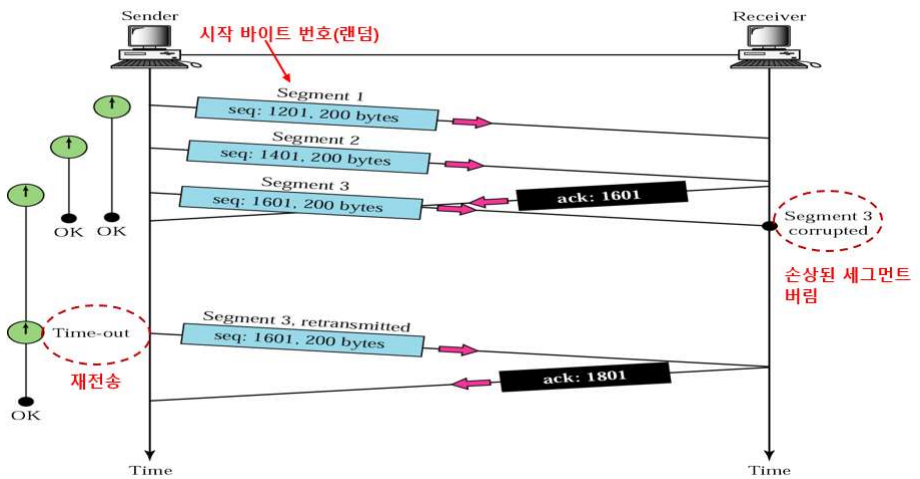
# II. TCP의 흐름제어, 오류제어 설명

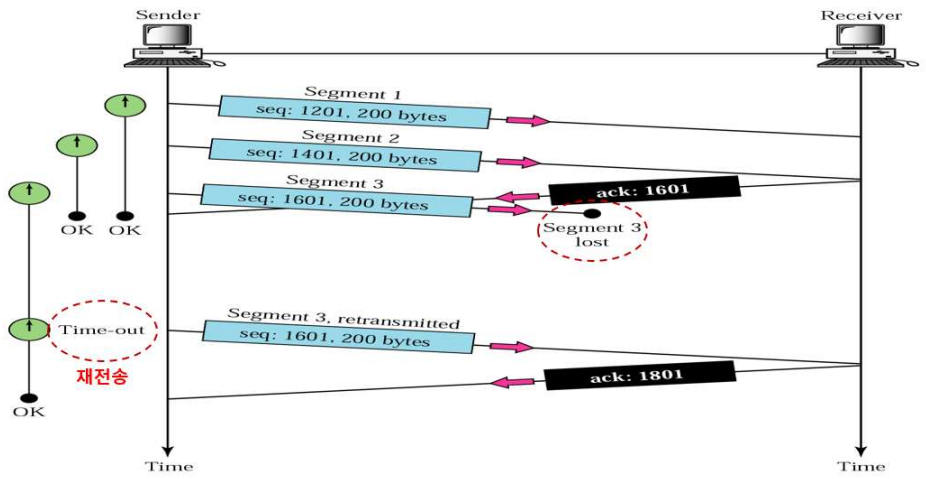
## 가. 종단간 트래픽 조절, 흐름제어 설명

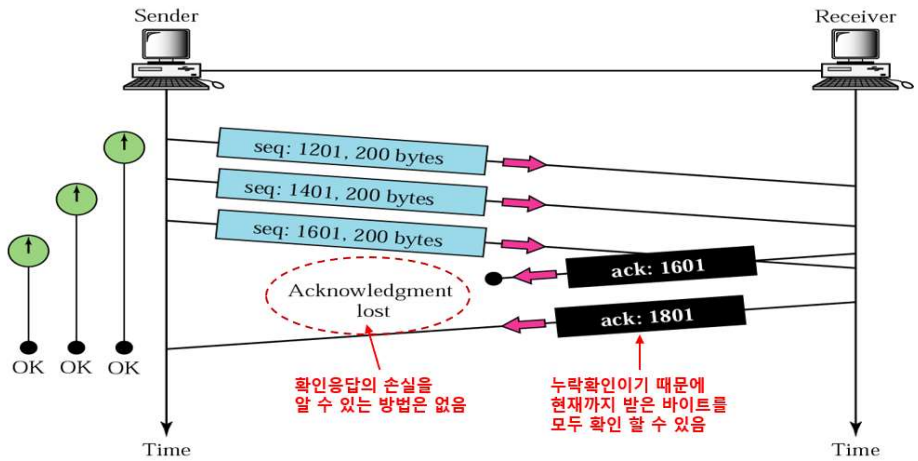



| 개요 | 설명 | |
|---|---|---|
| 정의 | 일정한 윈도우 크기 이내에서 한번에 여러 패킷을 송신하고, 이들 패킷에 대하여 단지 한 번의 ACK 로써 수신 확인을 하며, 윈도우 크기를 변경시키며 흐름제어를 하는 기법 | |
| 윈도우 크기 | Window Size = 최소값(rwnd, cwnd) | |
| 동작 메커니즘 | 열림 동작 | - 수신 측으로 부터 ACK가 도착하면, 윈도우 이동하여 사이즈 증가<br>- 늘어난 만큼 더 많은 데이터 전송 가능 |
| | 닫힘 동작 | - 데이터가 전송되면, 윈도우의 오른쪽 경계가 왼쪽으로 이동 |
| | 크기 결정 | - 수신측 윈도우와 혼잡 윈도우 사용<br>- 수신측 윈도우 : ACK를 포함하고 있는 세그먼트를 사용하여 상대방에게 알림<br>- 혼잡 윈도우 : 혼잡상태가 발생하지 않도록 네트워크에서 결정 |

## 나. 데이터의 오류방지, 오류제어 설명

| 개요 | 설명 | |
|---|---|---|
| 정의 | 신뢰성 있는 데이터 전송을 위해 전송된 세그먼트가 손실되었거나 훼손된 경우, 순서가 어긋나는 경우, 또는 중복되는 경우에 대한 처리기능을 수행 하는 기법 | |
| 오류 검출 방법 | 검사합 | - 각 세그먼트에는 데이터 손상 여부 확인용 검사 합 필드 존재<br>- 수신 TCP는 검사합 필드를 확인하여 손상 판정되면 그 세그먼트를 버림 |
| | 확인 | - 수신 TCP의 전송 데이터에 문제가 없으면 송신 측에 ACK 전송<br>- NAC 송신 하지 않음 |
| | 시간 초과 | - 시간 초과 전까지 ACK확인 없으면., 그 세그먼트는 오류 판정<br>- 오류 확인 후 재전송 |
| 오류 저장방법 | 훼손 세그먼트 |  |

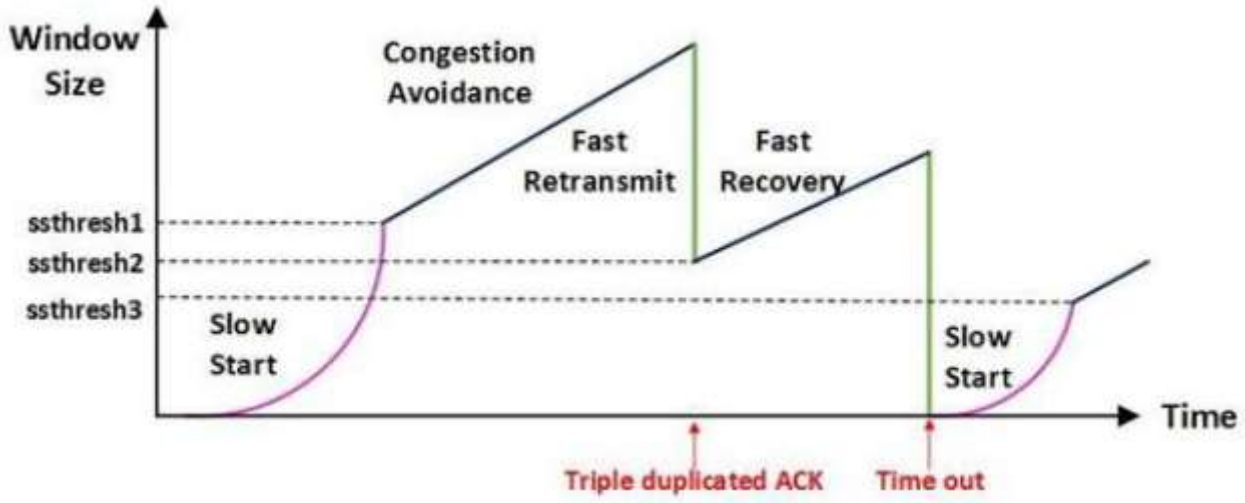
<table>
<tr><td rowspan="5">오류<br>검출 방법</td><td>훼손<br>세그먼트</td><td>- 수신 측에서 2개의 세그먼트(1201~1600) 받고 송신 측에 ACK 신호와 함께 다음 받을 세그먼트의 주소 송신(ACK + 1601)<br>- 수신 TCP는 송신 측에서 송신 한 3번째 세그먼트 오류 발견되어 버리고 아무런 응답(NAK)하지 않음<br>- 송신 TCP 에선 3번째 세그먼트 전송 후 타임 아웃 됐지만 수신 TCP 측으로 부터 ACK+1801 신호 없으므로 수신 실패로 판단하고 1601 세그먼트 재전송</td></tr>
<tr><td>손실<br>세그먼트</td><td> 

- 기본적인 동작 순서는 훼손 세그먼트와 같음<br>- TCP송신 측에서 전송한 데이터가 통신 중 손실되거나, 오류 판정되거나, 송신 TCP는 전송 한 세그먼트의 타이머가 Time-Out 되고 수신 측의 ACK 확인 없으면 재전송</td></tr>
<tr><td>중복<br>세그먼트</td><td>- 확인 응답이 도착하지 않은 세그먼트에 대한 송신 TCP의 재전송에 의해 발생<br>- 수신 TCP는 중복된 세그먼트 중에서 늦게 도착한 것 폐기</td></tr>
<tr><td>순서<br>어긋난<br>세그먼트</td><td>- TCP 세그먼트가 IP에 의해 전달되어 발생되는 문제<br>- IP는 각각의 세그먼트가 다른 경로로 전달 될 수 있음<br>- 순서가 뒤바뀐 세그먼트를 수신한 수신TCP는 올바르게 전송 받을 때까지 확인응답을 하지 않고 모두 폐기</td></tr>
<tr><td>확인응답<br>세그먼트</td><td> 

- 시간적 차이에 의해 전송 블록의 ACK가 시간차 두고 회신 되더라도 Time-Out 전에만 들어오면 다음 세그먼트 전송<br>- 설사 수신 측으로 부터의 응답인 "ACK+다음 세그먼트 번호"가 손실 되었다 하더라도 최종 회신이 들어오면 정상 전송 프로세스 실행</td></tr>
</table>

# III. 네트워크 유입 트래픽 조절, 혼잡제어 설명

## 가. 혼잡제어의 개요




| 개요 | 설명 | |
|---|---|---|
| 정의 | 네트워크로 유입되는 사용자 트래픽의 양이 네트워크 용량을 초과하지 않도록 송신 데이터 크기를 조절하는 메커니즘 | |
| 동작 메커니즘 | Slow Start | - ACKs가 정상적으로 도착할 때 작은 Windows Size부터 시작하여 지수적으로 증가하는 전송 방식<br>- Cwnd : 혼잡 window 크기 |
| | Congestion Avoidance | - Threshold(ssthresh)에 Window Size가 도달하면 혼잡이 곧 일어남을 간주하여 이를 회피하기 위해 cwnd 변수를 선형으로 증가 시키는 전송 방식 |
| | Fast Retransmission | - 송신자에게 세그먼트가 무질서하게 수신되었음을 알리고 다음 수신할 Sequence Number를 알려준 후 Slow Start로 전송하는 방식 |
| | Fast Recovery | - Fast Retransmission 통해 손실 세그먼트를 전송한 후 Slow Start가 아닌 Congestion Avoidance를 수행하는 전송방식<br>- 3 ACKs, Congestion Avoidance 적용 |

- 기본적인 메커니즘을 개선한 여러 TCP 혼잡 제어 기술이 존재함

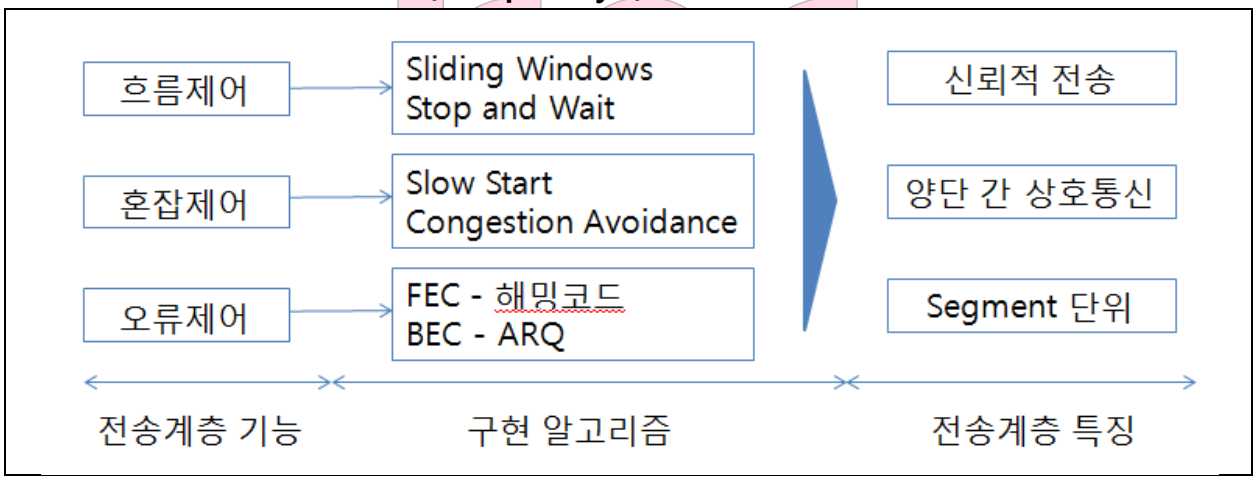
## 나. 주요 TCP 혼잡제어 기법 설명

| 개요 | 설명 |
|---|---|
| TCP Tahoe | - Slow Start, Congestion Avoidance, Fast Retransmit 세 알고리즘 사용<br>- Receiver측으로 부터 threshold 이상의 dup ACKs가 오면 Sender는 loss가 일어난 것으로 간주하고, 해당 패킷을 바로 Fast Retransmission 수행 |
| TCP Reno | - TCP Tahoe 알고리즘에 추가적으로 Fast Recovery 알고리즘 사용<br>- Dup ACKs 된 Segment에 대해 ACK가 발생하면 cwnd값을 1/2로 줄이고, Congestion Avoidance 단계로 진입 ( Tahoe는 cwnd는 1로 조정되고, slow Start 단계로 진입) |
| TCP New-Reno | - Dup ACKs가 왔을 때, 재전송 timeout이 일어났을 때, Full ACK가 왔을 때 이 세가지 경우에만 Fast Recovery를 시작 |
| TCP SACK | - Multiple loss에 적합한 기법<br>- Receiver가 TCP SACK block을 통해 Sender측에 성공적으로 전송된 segment 정보를 알려줌<br>- Sender는 TCP SACK block을 통해 알아낸 정보를 토대로, Retransmission timeout을 기다리지 않고 손실된 Segment를 전송 |
| TCP Vegas | - 실제 throughput과 예상되는 throughput의 차이를 계산하여 Congestion을 제어<br>- Cwnd를 이용하지 않고 RTT값을 매번 계산하여 사용<br>현재 throughput과 예상되는 throughput(Expected = Window Size / BaseRTT) 의 차이가 2를 넘지 않으면 cwnd를 증가, 4를 넘으면 cwnd를 감소 |

"끝"

| | |
|---|---|
| 문 제 | 1. 전송계층(Transport Layer)에서 전송 데이터의 단위는 Segment 이다. 전송계층 기능 중 흐름제어(Flow Control)에 대하여 다음을 설명하시오.<br>가. 흐름제어 방식 개념<br>나. 흐름제어 방식의 개념도<br>다. Sliding Windonws 와 Slow Start 비교 |
| 출 제 영 역 | 네트워크 / 난 이 도 ★★★☆☆ |
| 출 제 배 경 | 120 회 TCP 기능에 대한 심화 문제로 흐름제어/혼잡제어 대한 출제 |
| 출 제 빈 도 | 120 회, 117 회, 111 회 컴퓨터시스템응용 |
| 참 고 자 료 | 정보통신기술용어해설 (www.ktword.cokr)<br>쉽게 배우는 네트워크 (성균관대학교, 안성진 교수)<br>120 회, 117 회 컴퓨터시스템응용기술사 KPC 기출풀이 |
| Keyword | Sliding windows, 열림/닫힘/축소 동작, stop-and-wait, slow start, 지수적 증가, 신뢰성, cwnd, rwnd, awnd |
| 풀 이 | 임영균 (120 회 정보관리기술사) |

**1. 신뢰적 데이터 송수신, 전송계층(Transport Layer) 개요**




- OSI 7 layer 4 계층으로 종단간 사용자들이 신뢰성 있는 데이터를 송수신하기 위해 흐름/혼잡/오류 제어 기능을 통하여 데이터 유효성 및 전송 효율성을 수행하는 계층

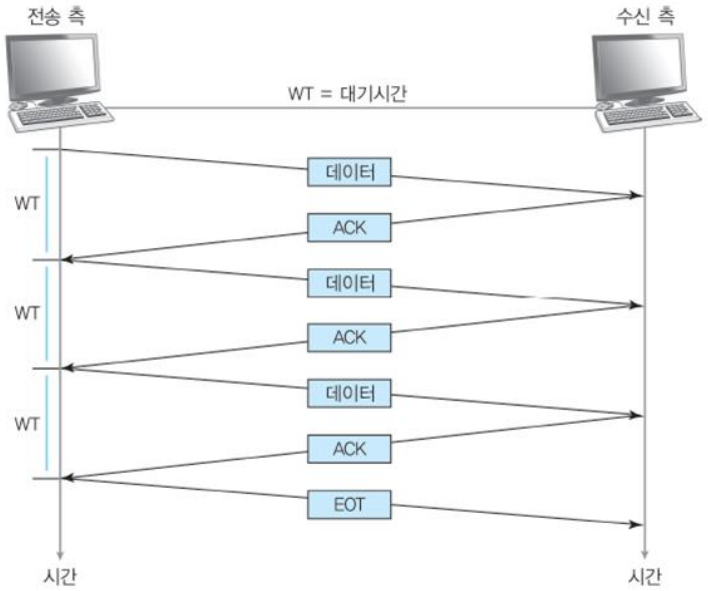
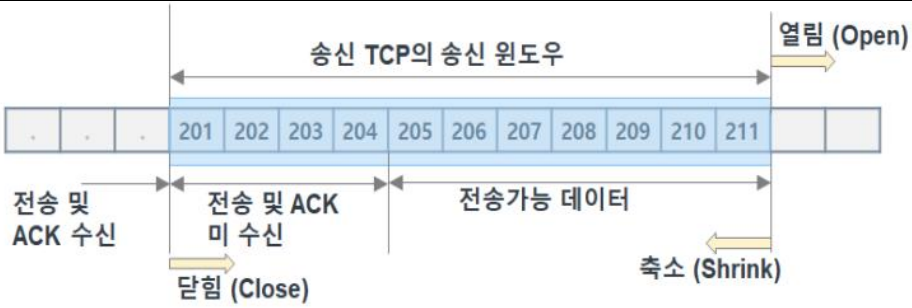
**2. 흐름제어 방식 개념 및 흐름제어 방식의 개념도**

**가. 흐름제어 방식 개념**

| 구 분 | 설명 | |
|---|---|---|
| 흐름제어의 개념 | - 송신 측과 수신 측의 데이터 처리 속도 차이로 인한 데이터의 손실을 방지하기 위해 송신 측의 데이터 속도를 통제하고 의도대로 동작하게 하는 기법. | |
| 흐름제어 방식 개념 | 정지대기 방식 | - 한 번에 1 개의 세그멘트 수신을 확인하며 전송하는 방식 |
| | 윈도우기반 방식 | - 여러 개의 세그멘트를 동시에 전송가능한 방식 |
| | 전송률 기반 방식 | - 데이터 송신률에 대한 임계값 관리를 통하여 전송하는 방식 |

- 정지대기방식은 전송효율이 낮아 윈도우기반 흐름제어 방식을 사용.

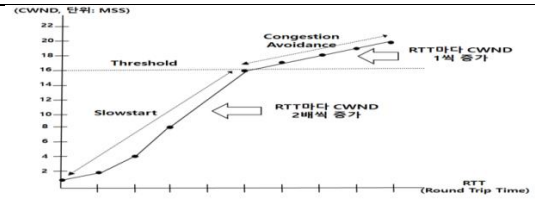
**나. 흐름제어 방식의 개념도**

| 흐름제어방식 | 설명 | |
|---|---|---|
| 정지 대기 방식 (Stop-and-Wait) |  | |
| | 동작절차 | 1. 전송 측 1 개의 세그먼트 전송<br>2. 수신 측 1 개의 세그먼트 수신 확인 후 ACK 전송<br>3. 데이터 수신 완료 시까지 1, 2 번 과정 반복 |
| 윈도우 기반 방식 (Sliding Windows) |  | |
| | 동작절차 | 1. 송신 윈도우크기 만큼 세그멘트 전송<br>2. Ack 수신 후 닫힘 동작 수행<br>3. 닫힘 동작 수행 후 윈도우크기 만큼 열린 동작 수행 |

- 흐름제어를 수행하는 중에도 네트워크가 혼잡한 경우 세그먼트의 손실이 발생할 수 있으므로 윈도우 사이즈를 통한 흐름제어와 혼잡제어를 동시 수행.

## 3. Sliding Windows 와 Slow start 비교

### 가. Sliding Windows 와 Slow start 개념 비교

| 구 분 | Sliding Windows | Slow start |
|---|---|---|
| 개념 | - 송신 측 윈도우사이즈 만큼의 여러 개의 세그멘트를 동시에 전송 가능한 방식 | - 데이터 초기 송신 시 네트워크의 혼잡한 상태를 알 수 없으므로 혼잡을 피하기 위한 방식 |
| 개념도 | |  |

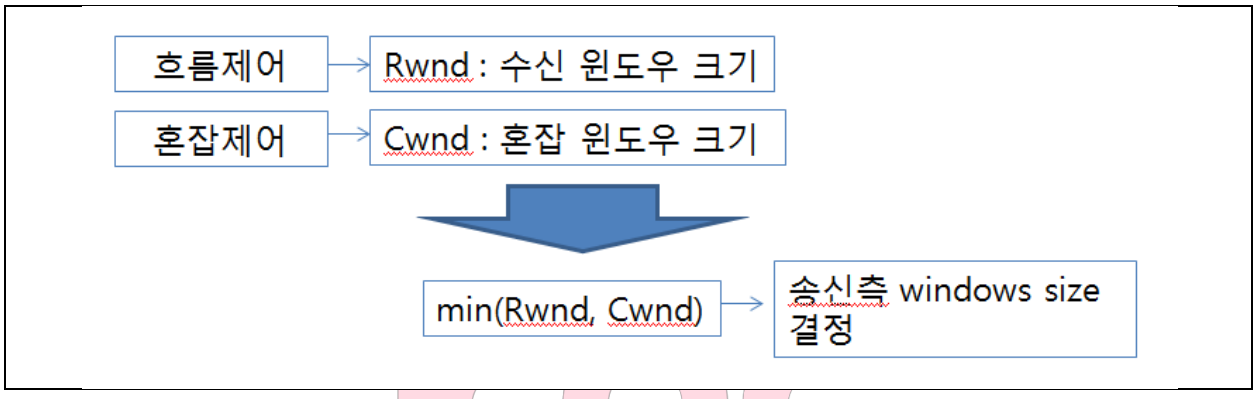
- Sliding Windows 방식은 흐름제어, Slow Start 는 혼잡제어를 위한 알고리즘.

나. Sliding Windows 와 Slow start 상세 비교

| 구 분 | Sliding Windows | Slow start |
|---|---|---|
| 목적 | - 송신/수신 단의 데이터 전송 속도 제어 | - 데이터 송신 시 초기 네트워크 혼잡 방지 |
| 동작절차 | 1. 송신 윈도우크기 만큼 세그멘트 전송<br>2. Ack 수신 후 닫힘 동작 수행<br>3. 닫힘 동작 수행 후 윈도우크기 만큼 열린 동작 수행 | 1. 초기 cwnd 사이즈 1 지정<br>2. 세그먼트 송신 후 Ack 수신 시 cwnd 1 증가 ( 윈도우 크기 지수적 증가)<br>3. 임계치 도달 시 Congestion Avoidance 변경 |
| 윈도우 사이즈 | - Awnd : 송신 윈도우 크기<br>- Rwnd 와 Cwnd 크기 중 작은 값을 채택 | - Cwnd : 혼잡 윈도우 크기<br>- 네트워크 상태에 따라 실시간으로 변화 |

- 흐름제어와 혼잡제어를 동시에 수행하기 위하여 송신 측의 윈도우사이즈를 Rwnd 와 Cwnd 를 고려하여 결정.

**4. 송신 측 Windows Size 결정**




- 흐름제어 / 혼잡제어 / 오류제어를 통하여 전송계층의 신뢰성을 구현.

"끝"

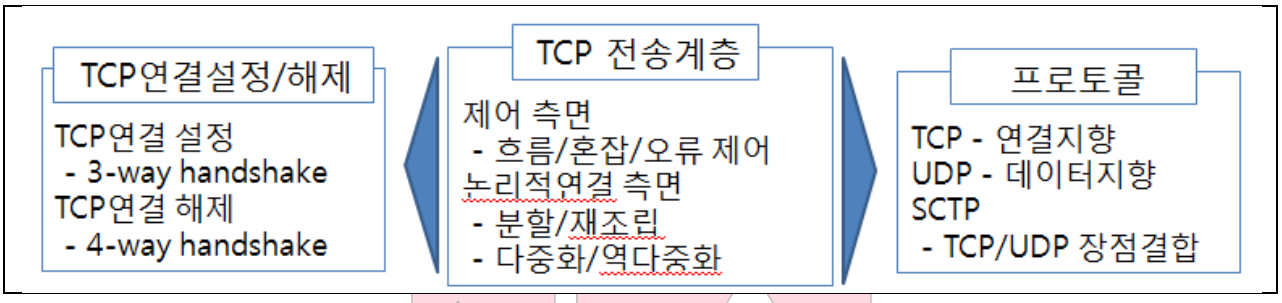
**기출풀이 의견**

네트워크 도메인은 정확한 답이 있는 문제가 대부분이므로 정확한 답안을 작성해야 합니다. 또한 전송계층의 기능과 같은 기본적 / 고전 문제의 경우 대부분의 예비기술사님이 답안을 작성하므로 최대한 알고 있는 것을 답안지에 표현하는 것이 고득점을 받을 수 있습니다.

| 문 제 | 2. TCP 전송계층 프로토콜에 대하여 다음을 설명하시오. |
|---|---|

| | |
|---|---|
| | 가. TCP 전송계층 개념<br>나. 3-way handshake 와 4-way handshake 설명<br>다. TCP 와 UDP 비교 |
| 출 제 영 역 | 네트워크 |
| 난 이 도 | ★★☆☆☆ |
| 출 제 배 경 | 120 회 TCP 기능에 대한 심화 문제로 흐름제어/혼잡제어 대한 출제 |
| 출 제 빈 도 | 120 회, 117 회, 116 회 컴퓨터시스템응용 |
| 참 고 자 료 | 정보통신기술용어해설 (www.ktword.cokr)<br>쉽게 배우는 네트워크 (성균관대학교, 안성진 교수)<br>120 회, 117 회, 116 회 컴퓨터시스템응용기술사 KPC 기출풀이 |
| Keyword | TCP 연결 설정/해제, 논리적 연결, 3-way handshake, SYN, SYN+ACK, ACK, 4-way handshake, FIN, ACK, FIN, ACK, TCP, 연결지향,가상회선방식, UDP, 메세지지향, 데이터그램, SCTP, RFC 4690 |
| 풀 이 | 임영균 (120 회 정보관리기술사) |

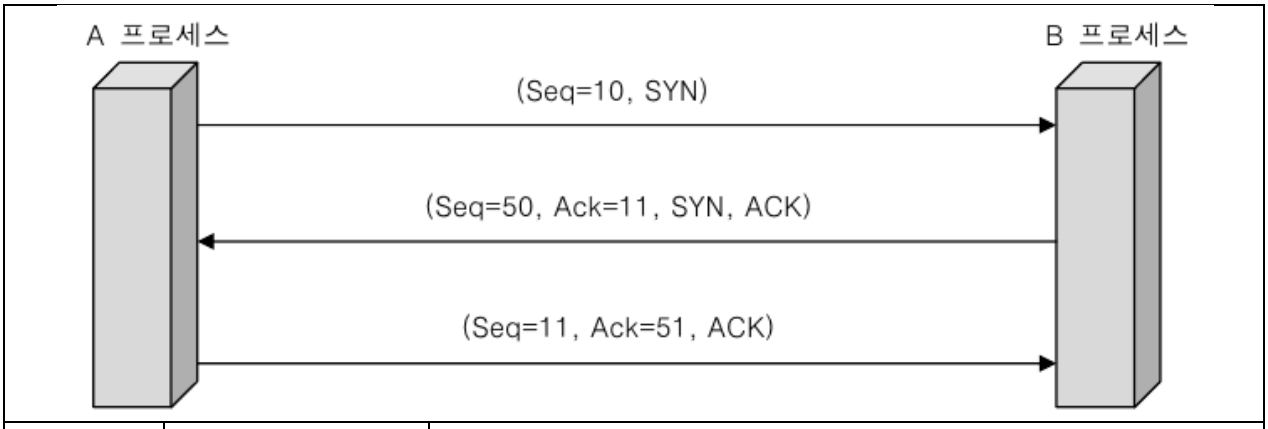
## 1. 신뢰성 데이터 전송, TCP 전송계층 개념




- (개념) 네트워크의 종단 간 어플리케이션 프로세스의 논리적 연결 및 신뢰성을 제공하기 위해 흐름/혼잡/오류 제어와 분할/재조립, 다중화/역다중화를 수행하는 TCP/IP 모델 전송계층.

## 2. 3-way handshake 와 4-way handshake 설명

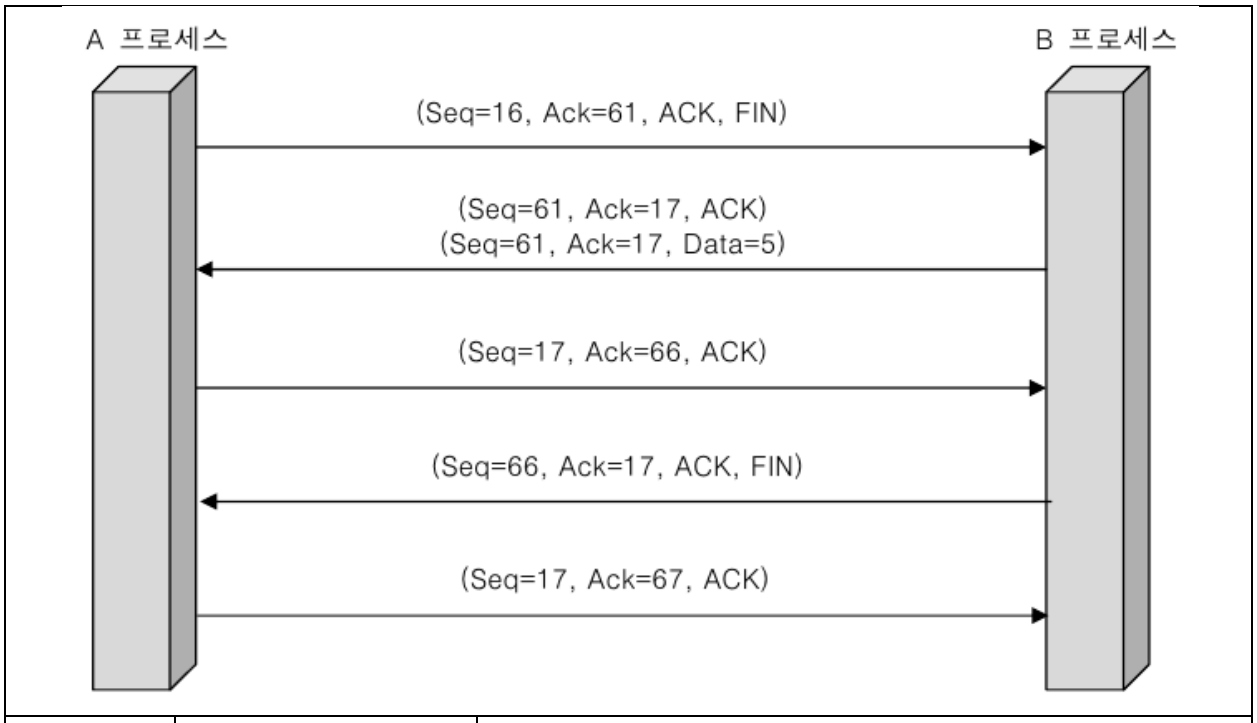
### 가. 3-way handshake 설명




| | | |
|---|---|---|
| 동작절차 | 1. 연결 설정 요구 | - 접속 요청 프로세스가 연결 메세지 전송 ( 플래그 : SYN ) |
| | 2. 연결 수락 | - 접속 요청을 받은 프로세스가 수락 ( 플래그, SYN + ACK ) |
| | 3. 연결 수락 확인 | - 접속 요청 프로세스가 수락 확인을 보내 연결 성립 ( 플래그, ACK ) |

- 네트워크 종단 간 어플리케이션 프로세스의 연결을 설정하기 위해 3-way handshake 사용.

나. 4-way handshake 설명

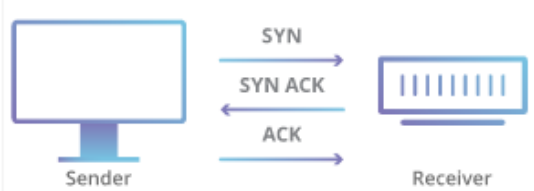
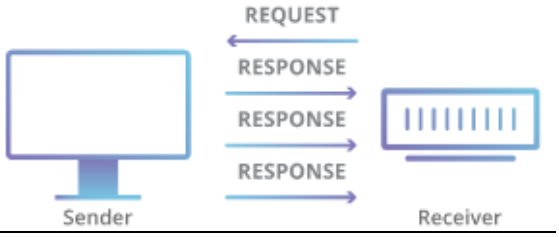



| | | |
|---|---|---|
| 동작절차 | **1. 연결해제 요구** | - 연결해제 요청하는 프로세스에서 FIN 전송 (플래그: FIN) |
| | **2. 연결해제 요구 확인** | - 수신 프로세스가 FIN 요청에 대한 응답 (플래그: ACK) |
| | **3. 연결해제 합의** | - 연결해제 요청을 받은 프로세스가 다시 FUIN 전송 (플래그:FIN) |
| | **4. 연결해제 합의 확인** | - 연결해제 요청 프로세스가 수락 시 연결 종료 (플래그:ACK) |

- 네트워크 종단 간 어플리케이션 프로세스의 연결을 종료하기 위해 4-way handshake 사용.
- TCP 는 통신을 위한 연결과 해제 과정을 사용하지만, UDP 는 연결과정 없이 요청만으로 데이터 통신 가능.

## 3. TCP 와 UDP 비교

### 가. TCP 와 UDP 개념 비교

| 구 분 | TCP(Transmission Control Protocol) | UDP(User Datagram Protocol) |
|---|---|---|
| 개념 | - 연결형 서비스 및 호스트간 신뢰성 있는 통신을 지원하는 전송 계층 프로토콜 | - 비연결형 서비스 및 통신 시 연결과정 없이 데이터 통신을 지원하는 전송 계층 프로토콜 |
| 개념도 |   |   |
| 특징 | - 연결 지향적 ( Connection Oriented )<br>- 신뢰성 ( 흐름/혼잡/오류제어 수행) | - 메세지 지향적 ( Messages Oriented )<br>- 빠른 전송 ( 통신 오버헤드 감소 ) |

- TCP 는 흐름/혼잡/오류 제어 등을 수행하여 신뢰성 있는 통신을 제공, UDP 는 데이터그램 단위로 데이터를 전송하기 때문에 TCP 에 비해 오버헤드 감소로 인한 빠른 속도의 통신을 제공함.

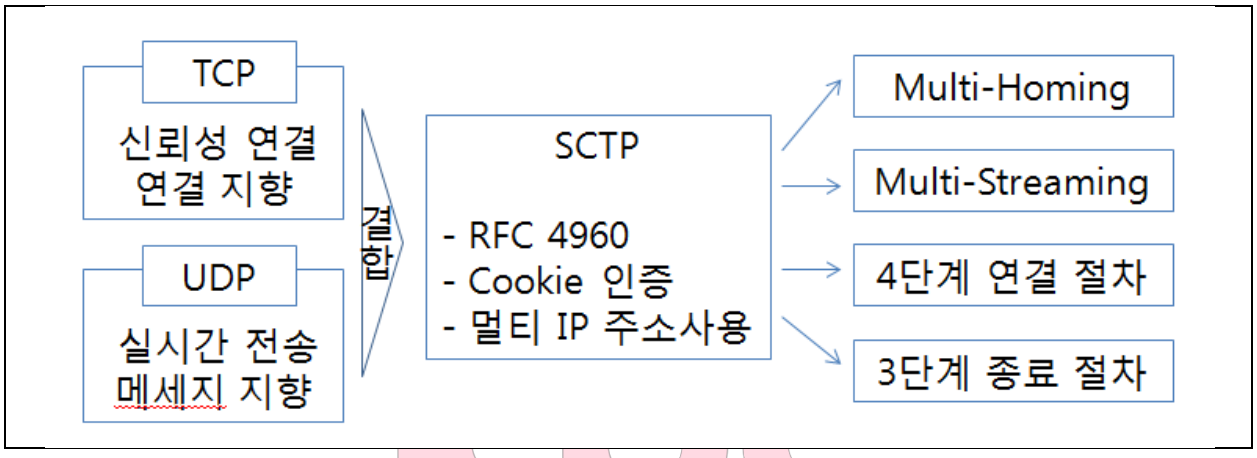
### 나. TCP 와 UDP 상세 비교

| 구 분 | TCP(Transmission Control Protocol) | UDP(User Datagram Protocol) |
|---|---|---|

| | | |
|---|---|---|
| **연결방식** | - 연결형 서비스 | - 비연결형 서비스 |
| **패킷교환방식** | - 가상 회선 방식 | - 데이터그램 방식 |
| **데이터 순서** | - 데이터 순서 유지 | - 데이터 순서 미 유지 |
| **에러 정정** | - 에러검사, 에러 시 재전송 | - 에러 발생 시 재전송 안함 |
| **흐름 제어** | - Stop-and-wait, SlidingWindows 등 | - 흐름제어 미수행 |
| **활용** | - 성능보다 신뢰성이 중요한 통신에 사용 | - 신뢰성보다 성능이 우선 시 되는 통신에 사용, 멀티미디어 서비스 등 |
| **프로토콜** | - HTTP, HTTPS, FTP, SMTP, SSH 등 | - DNS, SNMP, SYSLOG, NTP 등 |

- TCP 전송 계층 프로토콜은 TCP 와 UDP 장점을 결합한 SCTP, TCP 전송성능 향상을 위한 MPTCP 도 있음.

**4. TCP 와 UDP 결합, SCTP (Stream Control Transmission Protocol)**

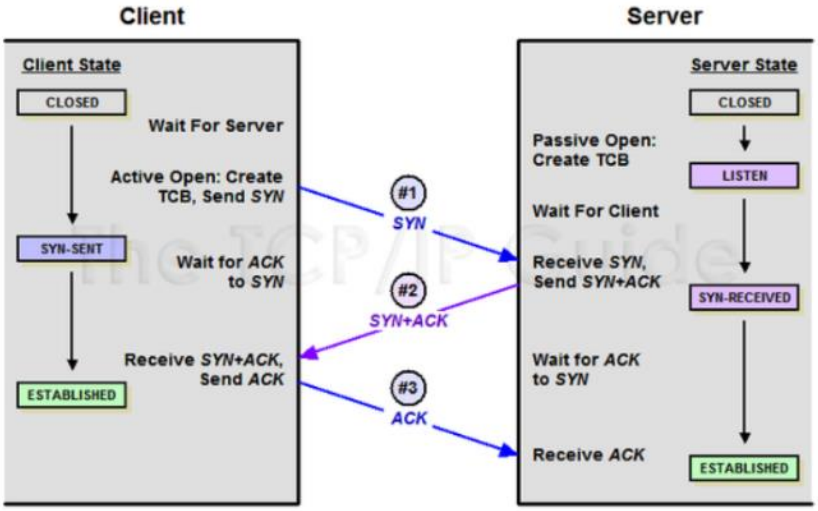



- SCTP 는 두 지점간에 통신을 위하여 다중경로 및 다중스트리밍 기능을 사용가능하며, 3 단계 종료 절차를 통하여 'Half-open closing' 문제를 해결.

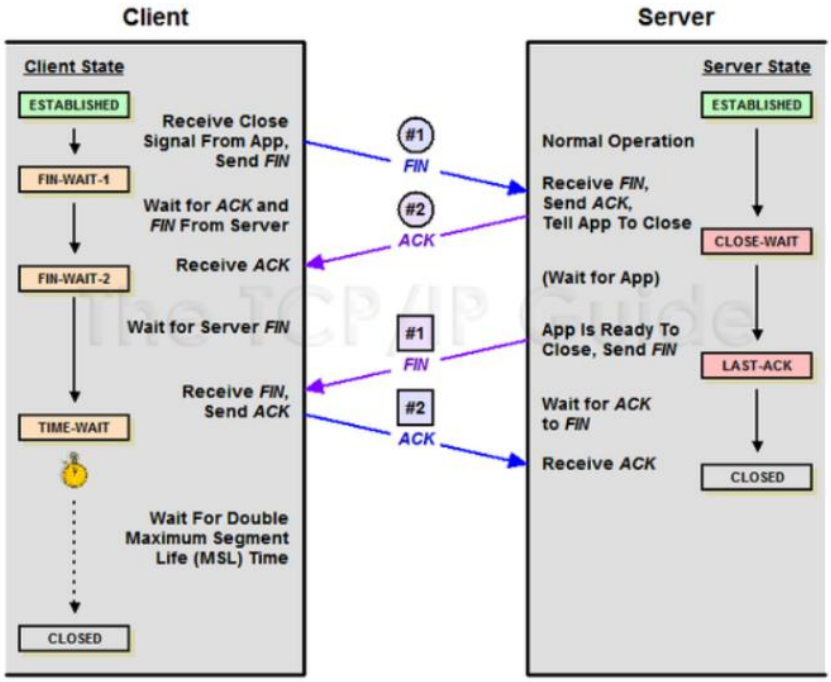
"끝"

**[참고자료]**

**3-way handshake - 서버와 클라이언트의 소켓함수 상태 확인 가능**



4-way handshake




## 기출풀이 의견

네트워크 전송계층에 문제로 정확한 정답이 있으므로, 되도록 정확하게 답안지를 작성해주셔야 합니다. 또한 대부분의 예비기술사님들께서 선택하는 문제이므로 다른 사람들보다 풍부하게 답안을 작성해주셔야 고득점을 받을 수 있습니다.

| | |
|---|---|
| 문 제 | 6. 네트워크 서브네팅(Subnetting)과 관련하여 다음을 설명하시오.<br>가. 슈퍼네팅(Supernetting)과 서브네팅(Subnetting) 개념<br>나. 192.168.0.0/22 네트워크 대역을 사용하여 인사팀 125 명, 영업팀 250 명, 보안팀 125 명, 개발팀 500 명이 사용할 수 있도록 4 개의 VLSM(Variable Length Subnet Mask)으로 분할한 각각의 Subnet Mask 값과 할당 가능한 Host IP 대역 |

| | | | |
|---|---|---|---|
| 출 제 영 역 | 네트워크 | 난 이 도 | ★★★☆☆ (별 5 개 기준) |
| 출 제 배 경 | CIDR 기반 주소 집계와 VLSM 기반 주소 분할 원리를 이해하고, 주어진 네트워크 대역에서 요구 호스트 수에 맞는 서브넷 마스크와 할당 가능 IP 대역 산정 능력 검증 | | |
| 출 제 빈 도 | 정보관리(130) | | |
| 참 고 자 료 | 정보관리 및 컴시응 기출풀이집, KPC 모의고사 해설집 | | |
| Keyword | CIDR, VLSM, Subnet Mask, Prefix, Network ID, Broadcast Address, Host IP Range | | |
| 풀이 기술사님 | 김하랑(139 회 정보관리기술사 / harangg26@gmail.com) | | |

## 1. 슈퍼네팅(Supernetting)과 서브네팅(Subnetting) 개념

### 가. 슈퍼네팅(Supernetting)의 개념

| | | |
|---|---|---|
| 정의 | 분할되어 있는 여러 개의 작은 네트워크 블록을 하나의 큰 네트워크 대역으로 통합하는 기술 | |
| 특징 | CIDR 기반 주소 집계 | CIDR(Classless Inter-Domain Routing) 기반 연속된 여러 네트워크를 하나의 Prefix 로 통합하여 경로를 요약(Route Aggregation) |
| | 라우팅 테이블 크기 감소 | 개별 경로 정보를 하나로 집계하여 라우터 메모리 사용량 감소 |
| | 패킷 전달 및 라우팅 효율 향상 | 경로 탐색 횟수를 줄여 패킷 포워딩 성능 향상 |

- CIDR 기반 주소 집계를 통해 다수의 네트워크를 하나의 경로 정보로 통합

### 나. 서브네팅(Subnetting)의 개념

| | | |
|---|---|---|
| 정의 | 하나의 큰 네트워크 대역을 여러 개의 작은 네트워크(Subnet)로 분할하는 기술 | |
| 특징 | VLSM 기반 유연한 주소 할당 | VLSM(Variable Length Subnet Mask) 기반 요구 Host 수에 맞는 가변 Prefix 적용하여 주소 공간 효율화 |
| | 브로드캐스트 도메인 분리 | 네트워크를 논리적으로 분리하여 불필요한 브로드캐스트 트래픽 감소 |
| | IP 주소 활용도 향상 | 필요한 크기만큼 서브넷을 할당하여 주소 낭비 최소화 |

- VLSM 을 활용하여 부서별 요구 호스트 수에 맞게 네트워크를 효율적으로 분할, 요구 Host 수가 가장 큰 네트워크부터 순차적으로 주소를 할당하여 주소 공간 낭비를 최소화하는 방식으로 진행



Copyright ⓒ 2026 By Korea Productivity Center ICT Education Center. All righ 1 ts reserved

## 2. 주어진 문제 풀이 설명

<table>
<tr><th>단계</th><th>과정 설명</th></tr>
<tr><td>조건</td><td>192.168.0.0/22 네트워크 대역을 인사팀 125 명, 영업팀 250 명, 보안팀 125 명, 개발팀 500 명이 사용할 수 있도록 4 개의 VLSM(Variable Length Subnet Mask)으로 분할</td></tr>
<tr><td>① 부서별 Host 수 산정</td><td>
<table>
<tr><td>부서</td><td>요구 Host 수</td><td>필요 Host 수 (요구 Host +2)</td></tr>
<tr><td>개발팀</td><td>500</td><td>502</td></tr>
<tr><td>영업팀</td><td>250</td><td>252</td></tr>
<tr><td>인사팀</td><td>125</td><td>127</td></tr>
<tr><td>보안팀</td><td>125</td><td>127</td></tr>
</table>
Network ID 와 Broadcast 주소를 고려하여 Host 수에서 +2 개의 주소 공간 필요
</td></tr>
<tr><td>② 호스트 비트 계산</td><td>
<table>
<tr><td>부서</td><td>Host Bit ($2^n$ -2 >= Host)</td></tr>
<tr><td>개발팀</td><td>9 Bit (502 < $2^9$ = 512)</td></tr>
<tr><td>영업팀</td><td>8 Bit (252 < $2^8$ = 256)</td></tr>
<tr><td>인사팀</td><td>7 Bit (127 < $2^7$ = 128)</td></tr>
<tr><td>보안팀</td><td>7 Bit (127 < $2^7$ = 128)</td></tr>
</table>
필요 주소 수를 수용하는 Host Bit 계산
</td></tr>
<tr><td>③ Prefix 및 Subnet Mask 결정</td><td>
<table>
<tr><td>부서</td><td>Prefix (32-Host Bit)</td><td>Subnet Mask</td></tr>
<tr><td>개발팀</td><td>/23 (32-9)</td><td>255.255.254.0</td></tr>
<tr><td>영업팀</td><td>/24 (32-8)</td><td>255.255.255.0</td></tr>
<tr><td>인사팀</td><td>/25 (32-7)</td><td>255.255.255.128</td></tr>
<tr><td>보안팀</td><td>/25 (32-7)</td><td>255.255.255.128</td></tr>
</table>
<table>
<tr><td rowspan="3">개발팀</td><td colspan="24">Prefix (/23)</td><td colspan="8"></td></tr>
<tr><td colspan="8">255</td><td colspan="8">255</td><td colspan="8">254</td><td colspan="8">0</td></tr>
<tr><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td></tr>
</table>
<table>
<tr><td rowspan="3">영업팀</td><td colspan="24">Prefix (/24)</td><td colspan="8"></td></tr>
<tr><td colspan="8">255</td><td colspan="8">255</td><td colspan="8">255</td><td colspan="8">0</td></tr>
<tr><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td></tr>
</table>
<table>
<tr><td rowspan="3">인사팀,<br>보안팀</td><td colspan="24">Prefix (/25)</td><td colspan="8"></td></tr>
<tr><td colspan="8">255</td><td colspan="8">255</td><td colspan="8">255</td><td colspan="8">128</td></tr>
<tr><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td></tr>
</table>
IP 전체 비트, 32 비트에서 Host Bit 를 차감하여 Prefix 길이를 계산<br>
계산된 Prefix 길이만큼의 상위 비트를 1 로 설정한 Subnet Mask 산출
</td></tr>
</table>



Copyright ⓒ 2026 By Korea Productivity Center ICT Education Center. All righ 1 ts reserved

| | |
|---|---|
| ④ Network ID 결정 및 IP 주소 할당 | |

| 부서 | Network ID | Host IP 범위 | Broadcast |
|---|---|---|---|
| 개발팀 | 192.168.0.0/23 | 192.168.0.1~ 192.168.1.254 | 192.168.1.255 |
| 영업팀 | 192.168.2.0/24 | 192.168.2.1~254 | 192.168.2.255 |
| 인사팀 | 192.168.3.0/25 | 192.168.3.1~126 | 192.168.3.127 |
| 보안팀 | 192.168.3.128/25 | 192.168.3.129~254 | 192.168.3.255 |

Host 수가 큰 네트워크부터 IP 순차적으로 할당(VLSM)

- 개발팀, 영업팀, 인사팀, 보안팀 순으로 510 개, 254 개, 126 개, 126 개 IP 를 할당

### 3. 문제 풀이 결과

| 부서명 | Network ID | Subnet Mask | Broadcast Address | 사용가능 Host 범위 | 사용가능 Host 수 |
|---|---|---|---|---|---|
| 개발팀 (500 명) | 192.168.0.0/23 | 255.255.254.0 | 192.168.1.255 | 192.168.0.1~ 192.168.1.254 | 510 개 |
| 영업팀 (250 명) | 192.168.2.0/24 | 255.255.255.0 | 192.168.2.255 | 192.168.2.1~254 | 254 개 |
| 인사팀 (125 명) | 192.168.3.0/25 | 255.255.255.128 | 192.168.3.127 | 192.168.3.1~126 | 126 개 |
| 보안팀 (125 명) | 192.168.3.128/25 | 255.255.255.128 | 192.168.3.255 | 192.168.3.129~254 | 126 개 |

- VLSM 을 적용하여 부서별 Host 수요에 적합한 서브넷을 할당함으로써 IP 주소 낭비를 최소화하고 네트워크 자원 활용 효율을 향상시킬 수 있음

"끝"

**기출풀이 의견**

1. 고전 토픽인 슈퍼네팅과 서브네팅의 계산 문제로 개념 설명과 풀이과정, 정확한 결과 도출이 필요합니다.

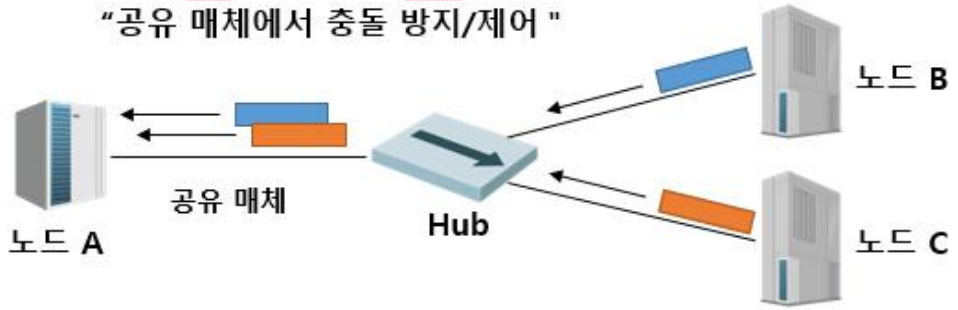


Copyright ⓒ 2026 By Korea Productivity Center ICT Education Center. All righ 1 ts reserved

| | | | |
|---|---|---|---|
| 문 제 | **1. 데이터링크 계층에서 사용하는 다중 접근 프로토콜(Multiple Access Protocol) 중 다음에 대하여 설명하시오.**<br>**가. 임의 접근 프로토콜(Random-access protocols)**<br>**나. 제어 접근 프로토콜(Controlled-access protocols)**<br>**다. 채널화 프로토콜(Channelization protocols)** | | |
| 출 제 영 역 | 네트워크 | 난 이 도 | ★★☆☆☆ (별 5 개 기준) |
| 출 제 배 경 | 데이터링크 계층 역할 이해, 다중 접근 프로토콜의 각 세부 프로토콜 분류, 특징 이해 여부 확인 | | |
| 출 제 빈 도 | 미출제 | | |
| 참 고 자 료 | - 컴퓨터 네트워크 (Mac Graw Hill, 이재광)<br>- KPC 기술사 IMPACT 실전모의고사 | | |
| Keyword | ALOHA, CSMA/CD, CSMA/CA, Reservation, Polling, Token Passing, FDMA, TDMA, CDMA | | |
| 풀이 기술사님 | 이시광(119 회 컴퓨터시스템응용기술사 / sk2ckr@naver.com) | | |

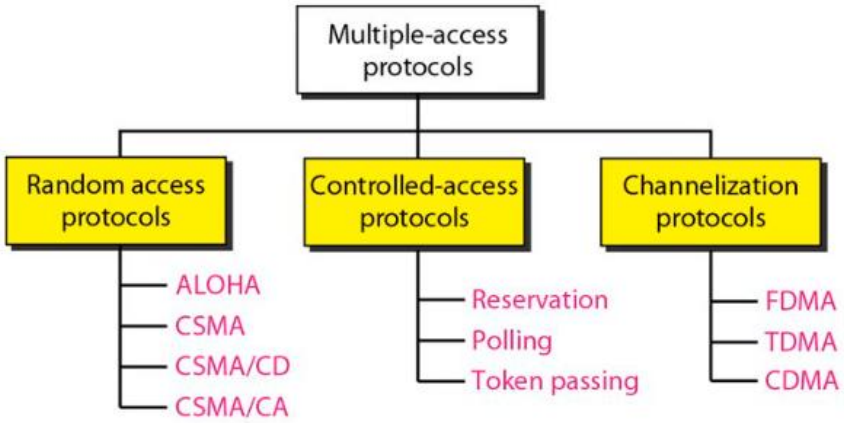
## 1. 데이터링크 계층에서의 다중 접근 프로토콜의 필요성 및 분류

**필요성**




- 노드 B 와 노드 C 에서 노드 A 로 연결되는 공유 매체에서 발생 가능한 충돌을 방지/제어
- 다른 사용자와 유/무선망 매체 공유를 위해 데이터링크 계층에서 다중 접근 프로토콜 사용

**분 류**




- 다중 접근 프로토콜은 공유 매체의 효율적인 자원 할당을 위해 경쟁/비경쟁 및 중앙 제어 방식을 이용하여 임의 접근, 제어 접근, 채널화 프로토콜로 분류

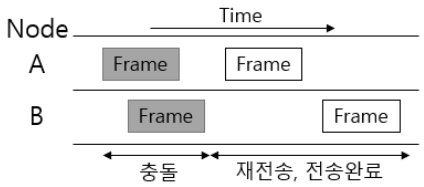
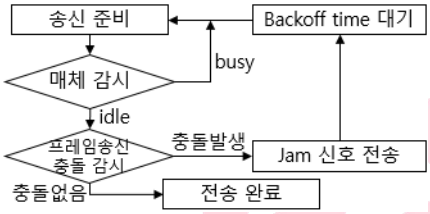
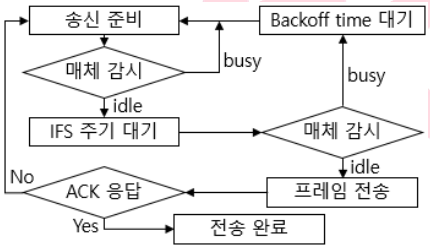
## 2. 경쟁 방식 매체 공유, 임의 접근 프로토콜 (Random-access protocols)

### 가. 임의 접근 프로토콜의 개념 및 특징

| | |
|---|---|
| 개 념 | 다수 노드가 공유 매체에서 프레임을 전송하기 위해 스케줄링 및 전송 순서 없이 충돌 감지 및 회피, 충돌 발생 시 재전송 하는 노드 간 경쟁 방식 프레임 전송 프로토콜 |
| 특 징 | - 각 노드는 다른 노드의 간섭을 받지 않고 공유 매체에 접근할 권한 보유<br>- 노드에 프레임을 전송하기 위한 스케줄링이 없으며, 전송은 노드 사이에서 임의로 발생<br>- 노드 간 프레임 전송 순서가 없으며, 각 노드는 공유 매체에 접근하기 위해 서로 경쟁 |

- 매체 접근 가능 여부, 매체 busy 여부, 전송 성공/실패 여부, 충돌 발생 여부 확인 후 프로토콜 별 동작

### 나. 임의 접근 프로토콜의 유형

| 유형 | 개념도 / 흐름도 | 특징 |
|---|---|---|
| ALOHA |  | - 다른 노드와 무관하게 프레임 전송, 충돌 허용<br>- 프레임 간 충돌 시 전송 실패 프레임 재전송<br>- pure ALOHA: 노드는 언제든지 프레임 전송<br>- slotted ALOHA: 타임 슬롯 시작 시 프레임 전송 |
| CSMA/CD |  | - 프레임 전송 전 공유 매체 사용 여부 체크<br>- 프레임 전송 후 충돌 발생 여부 체크<br>- 충돌 시 Jamming 신호 전송, Backoff time 대기<br>- IEEE 802.3 표준, 유선 이더넷 환경에서 사용 |
| CSMA/CA |  | - 프레임 전송 전 공유 매체 사용 여부 체크<br>- IFS 이후 매체가 idle 인 경우 프레임 전송<br>- 매체가 사용중인 경우 Backoff time 대기<br>- IEEE802.11 표준, 무선 이더넷 환경에서 사용 |

- 무선 매체 사용 시 송수신 노드가 아닌 제 3 의 노드에서 전송 신호 감지 불가로 인해 CSMA/CD 사용 불가

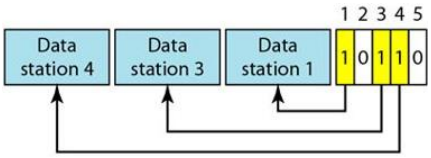
## 3. 비경쟁 방식 매체 공유, 제어 접근 프로토콜 (Controlled-access protocols)

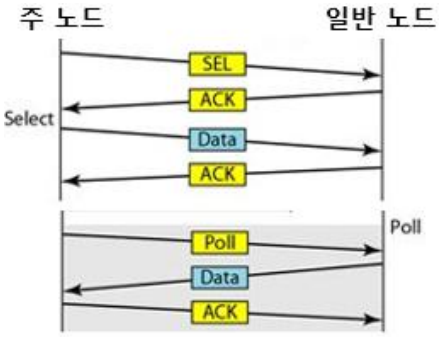
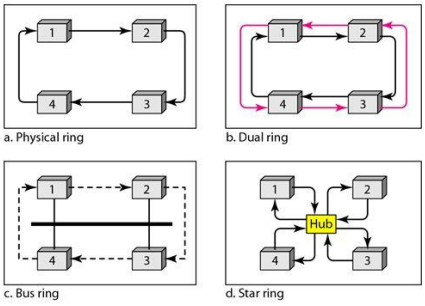
### 가. 제어 접근 프로토콜의 개념 및 특징

| | |
|---|---|
| 개 념 | 다수 노드가 공유 매체에서 프레임을 전송하기 위해 노드 간 협상하여 특정 노드에 프레임 전송 권한을 부여하는 비경쟁 방식 프레임 전송 프로토콜 |
| 특 징 | - 프레임 전송 권한이 부여된 노드만 공유 매체에 프레임 전송 가능<br>- 다른 노드에 의해 프레임 전송 권한이 승인될 때까지 공유 매체에 프레임 전송 불가 |

- 제어 접근 프로토콜은 어떤 노드에 프레임 전송 권한을 부여할지 선택하는 프로토콜

### 나. 제어 접근 프로토콜의 유형

| 유형 | 개념도 / 흐름도 | 특징 |
|---|---|---|
| Reservation |  <br>"station 별 예약 슬롯에 전송 예약" | - 예약 프레임에 노드 수만큼 예약 미니 슬롯 생성<br>- 프레임을 전송하기 전 미니 슬롯에 예약<br>- 해당 예약 프레임 뒤에 데이터 프레임 전송 가능<br>- 예약된 노드 외 데이터 프레임 전송 불가 |

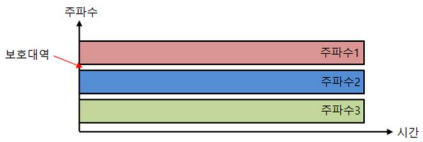
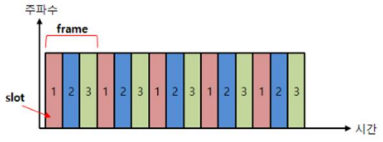
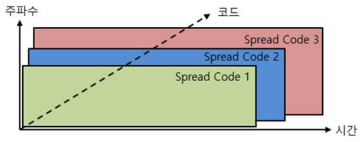
| | | |
|---|---|---|
| **Polling** |  | - 한 장치가 주 노드, 다른 장치가 부 노드로 지정<br>- 주 노드가 링크를 제어, 부 노드는 지시 이행<br>- select: 주 노드에서 일반 노드로 프레임 전송<br>- poll: 일반 노드에서 주 노드로 프레임 전송 |
| **Token Passing** |  | - 네트워크 내 노드가 고리 형태의 토폴로지로 구성<br>- 선행자(앞 노드)는 후행자(뒤 노드)로 프레임 전달<br>- 고리 내 토큰을 보유한 노드가 공유 매체 사용<br>- IEEE 802.5 표준, FDDI, CDDI 는 Token Ring 으로 사용 |

## 4. 중앙 제어 매체 공유, 채널화 프로토콜 (Channelization protocols)

### 가. 채널화 프로토콜의 개념 및 특징

| | |
|---|---|
| **개 념** | 노드 간 링크의 가용 대역폭을 주파수, 시간, 코딩 방식을 통해 중앙에서 제어하는 다중 접근 방식 프레임 전송 프로토콜 |
| **특 징** | - 한정된 매체 용량을 다수 노드가 효율적으로 나누어 사용<br>- 멀티플렉서 기반 변조와 복조를 통해 프레임 전송 비용 절감 |

### 나. 채널화 프로토콜의 유형

| 유형 | 개념도 | 특징 |
|---|---|---|
| **FDMA** |  **"서로 다른 주파수 대역으로 전송"** | - 넓은 대역폭을 다수 좁은 대역폭으로 분할<br>- 전송 매체를 각 주파수 대역으로 전송<br>- 송신측: 링크 대역폭을 분할하여 신호 변조<br>- 수신측: 필터를 통해 부 채널 신호 구분, 복조 |
| **TDMA** |  **"타임 슬롯 단위로 매체 점유"** | - 프레임을 일정한 시간 슬롯으로 분할 전송<br>- 하나의 회선을 복수 채널로 다중화<br>- 동기식: 할당된 타임슬롯 위치 고정 방식<br>- 비동기식: 할당된 타임슬롯 위치 조절 방식 |
| **CDMA** |  **"신호 별 서로 다른 코드 시퀀스 부여"** | - 여러 신호가 각기 다른 코드 시퀀스 부여<br>- 낮은 신호 스펙트럼으로 다경로 페이딩에 유리<br>- 도청이나 간섭에 강인하여 보안성 향상<br>- 수신부에서 인코딩 코드가 필요하며, 장치가 복잡 |

- 위 프로토콜 외 공간분할(SDMA), 파장분할(WDMA)이 있으며, 직교주파수분할(OFDMA) 등으로 발전

**5. 다중 접근 프로토콜 간 비교**

| 비교 항목 | 임의 접근 프로토콜 | 제어 접근 프로토콜 | 채널화 프로토콜 |
|---|---|---|---|
| **매체 점유 방식** | 노드 간 경쟁 | 노드에 권한 할당 | 노드에 자원 할당 |
| **매체 점유 범위** | 전체 점유 | 전체 점유 | 일부 점유 |
| **매체 제어 주체** | 매체 제어 없음 | 권한 부여된 노드 | 기지국 등 중앙 제어 |
| **주요 표준** | IEEE802.3, IEEE802.11 | IEEE 802.5 | CDMA2000, IMT-2020 |
| **활용 기술** | Ethernet, WLAN | FDDI, CDDI | DWDM, LTE, 5G |

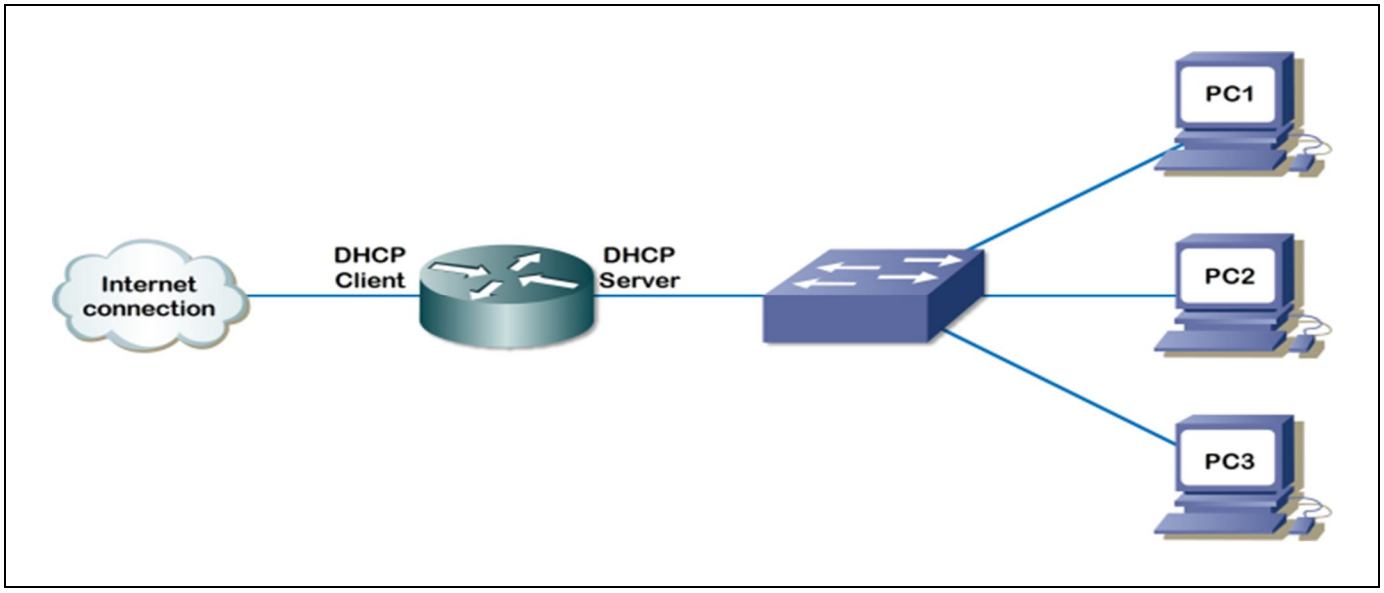
- 다중 접근 프로토콜의 세부 프로토콜은 각각 발전해왔으며, 여러 프로토콜을 혼합 사용하여 효율성 향상
- 고밀도 WLAN 환경에서 동일 채널 간섭 문제 해결을 위해 TDMA 알고리즘을 사용하여 무선망 품질 개선

"끝"

| 7 | DHCP(Dynamic Host Configuration Protocol) | | |
|---|---|---|---|
| 문제 | DHCP(Dynamic Host Configuration Protocol)의 구조와 동작원리에 대하여 설명하시오. | | |
| 도메인 | 네트워크 | | |
| 출제배경/의도 | 네트워크의 기본 토픽인 DHCP 에 대한 정확한 이해와 답안 표현을 파악 | | |
| 키워드 | ● 데이터 시각화, 정보 시각화, 인포그래픽, 빅데이터 시각화<br>● 정보 구조화, 정보 시각화 특성 저의, 정보 시각화 표현 | | |
| 목차예시 | 1. TCP/IP 자동할당 표준 DHCP 의 개요<br>2. DHCP 의 구조 및 구성요소<br>3. DHCP 의 동작원리<br>4. DHCP 와 NAT 의 비교 | | |
| 출제자 | 구환회 기술사(제 105 회 정보관리기술사 / kooryu@naver.com) | 난이도 | ★ ★ ☆ ☆ ☆ |
| 참고문헌 | 위키피디아, DHCP 구현(Microsoft), DHCP 기본 동작 원리(NMC Consulting Group) | | |

**1. TCP/IP 자동할당 표준 DHCP 의 개요**

**가. DHCP(Dynamic Host Configuration Protocol)의 정의**




- 네트워크 관리자가 조직의 중앙에서 일정한 시간 동안만 유효하도록 하는 임대 개념의 IP 주소를 할당하고 관리할 수 있도록 해 주는 프로토콜
- 네트워크 상에서 동적으로 IP 주소 및 기타 구성정보 등을 부여 및 관리하는 프로토콜
- DHCP 특징 : Client/Server 방식의 동작, Transport Layer 의 UDP 기반, 관리 용이성 및 보안성 강화

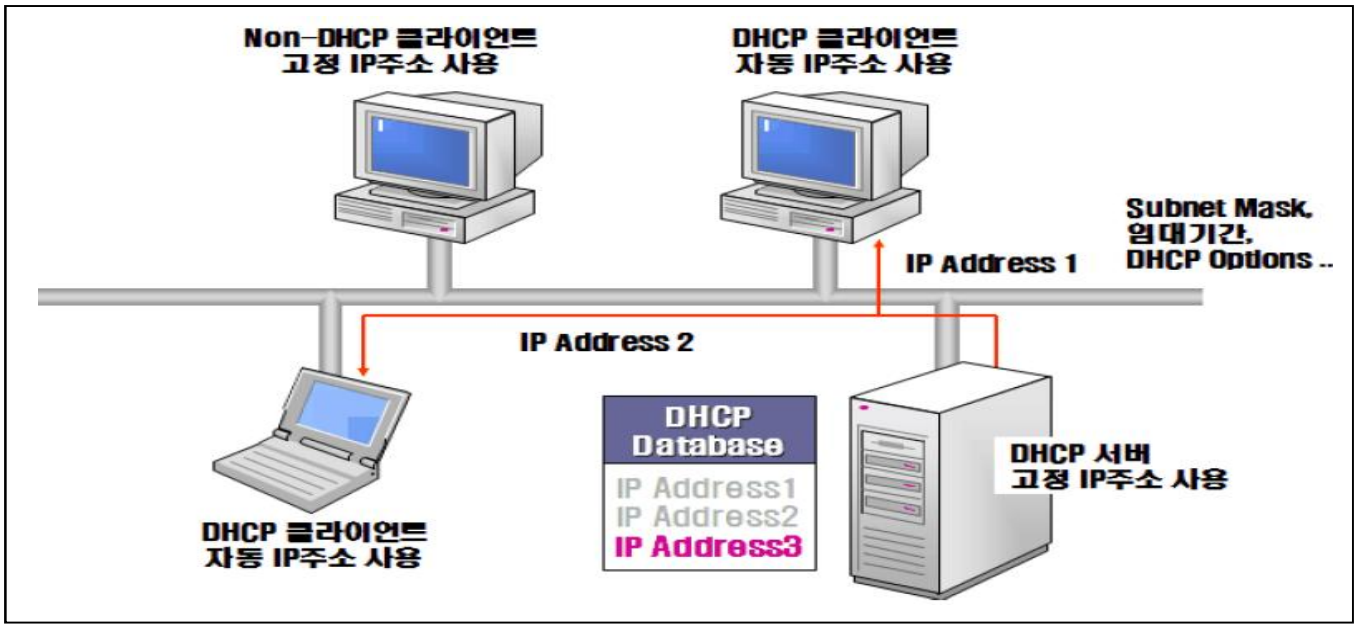

Copyright ⓒ 2014 By Korea Productivity Center Convergence Knowledge Center. All rights reserved

### 나. DHCP(Dynamic Host Configuration Protocol)의 IP 할당 종류

| 구분 | 내용 |
|---|---|
| Automatic Allocation | ● 클라이언트에게 영구적인 IP 할당 기법 |
| Dynamic Allocation | ● 클라이언트에게 한정된 시간 동안 IP 할당 기법<br>● 3가지 중에서 유일하게 IP 재사용이 자동으로 이루어짐 |
| Manual Allocation | ● 클라이언트의 IP Address를 네트워크 관리자가 할당하고 DHCP는 그 주소를 할당하는 기법 |

## 2. DHCP 의 구조 및 구성요소

### 가. DHCP 의 구조




### 나. DHCP 의 구성요소

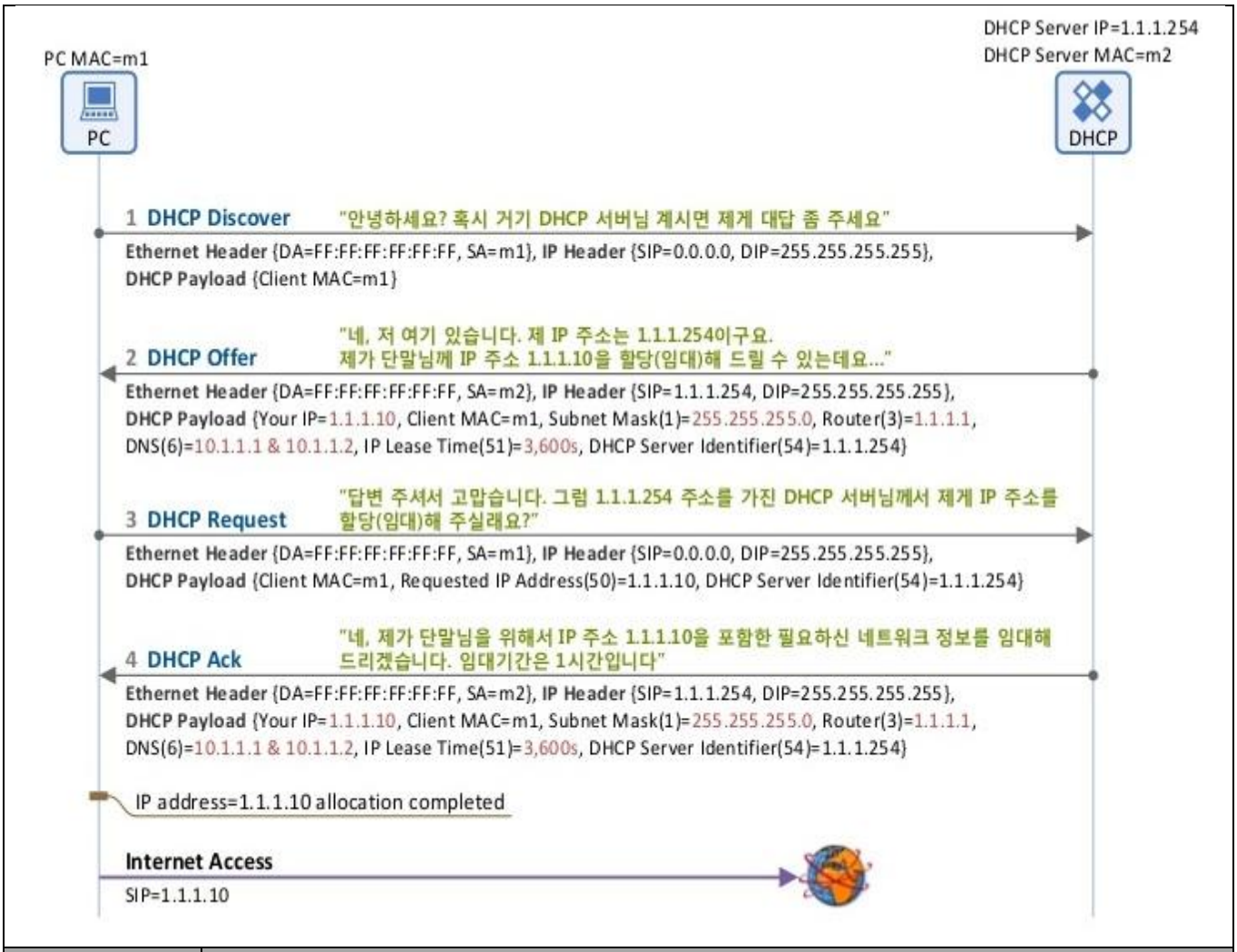
| 구성요소 | | 설명 |
|---|---|---|
| 기본 요소 | Non-DHCP Client | ● DHCP 서버로부터 IP를 할당 받지 않고 수동적으로 IP를 설정한 호스트 |
| | DHCP Client | ● 시스템 시작됨과 동시에 DHCP서버를 찾는 메시지를 네트워크에 발송, IP Address를 임대 요청하는 단말 |
| | DHCP Server | ● 클라이언트의 요청에 응답하여 자신의 DHCP 데이터베이스에서 IP Address를 임대하는 주체<br>● 각 클라이언트별 MAC 주소를 식별자로 하여, 이를 DB화하고 개별 관리 |
| | DHCP Database | ● DHCP 클라이언트가 할당되거나 해당 TCP/IP 주소 임대를 해제할 때 업데이트 되는 동적 DB<br>● 보통 영구적 메모리에 구성정보를 관리 및 저장 |
| 추가 요소 | DHCP Relay Agent | ● 서로 다른 서브넷에 위치하는 단말과 DHCP 서버간에도 DHCP 메시지 통신이 가능하게 하는 에이전트 |
| | DHCP Snooping | ● 네트워크 스위치에 지나다니는 DHCP 패킷을 감시, 어느 사용자가 어느 IP를 할당받았는지에 대한 Binding Table을 관리하는 기능 |

| | | |
|---|---|---|
| | DHCP Proxy Agent | ● 실제 IP를 분배하는 DHCP 서버의 앞단에 설치되며, DHCP Relay와 유사하게 DHCP 패킷을 중계 |

- 통상 서브넷 당 1 대 DHCP 서버를 두나 DHCP Relay Agent 를 사용하여 넓은 지역에 걸쳐 중앙집중 가능

### 3. DHCP 의 동작 원리

#### 가. IP 주소 할당(임대) 절차(IP Address Allocation Procedure)

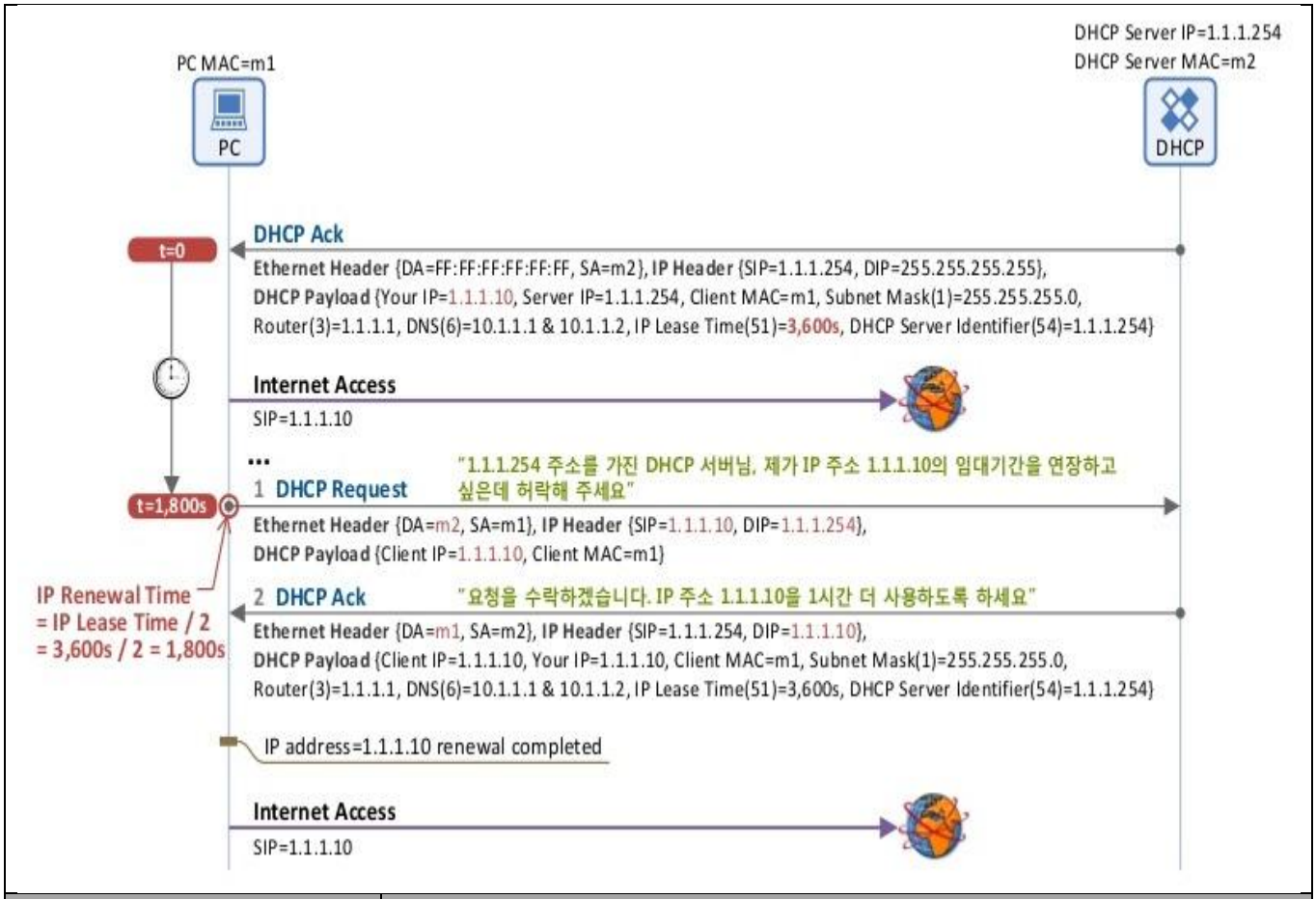



| 단계 | 설명 |
|---|---|
| 1. Discover | ● 단말이 부팅을 하면 동일 서브넷(랜)에 위치하는 DHCP 서버를 찾기 위해 DHCP Discover 메시지를 이더넷 망에 브로드캐스팅<br>● 이를 통해 동일 서브넷 상의 있는 모든 DHCP 서버들이 이 메시지 수신 |
| 2. Offer | ● DHCP 메시지를 수신한 DHCP서버는 자신의 존재를 알리기 위해 DHCP Offer 메시지를 이더넷 망에 브로드캐스팅<br>● 단말이 필요로 하는 네트워크 정보(단말 IP주소, Subnet Mask, Default Gateway IP 주소, DNS IP주소, Lease Time 등) 포함<br>● DHCP Offer 메시지는 동일 서브넷 상의 모든 단말들이 수신 |
| 3. Request | ● 단말 IP주소를 포함한 네트워크 정보를 요청 위해 DHCP서버에 DHCP Request 메시지를 이더넷 망에 브로드캐스팅<br>● 복수개의 DHCP 서버 존재 시 하나의 DHCP서버를 선택하여 서버의 IP주소를 DHCP Request 메시지 내에 Server Identifier필드에 기록 후 모든 DHCP서버에 브로드캐스팅 |


Copyright ⓒ 2014 By Korea Productivity Center Convergence Knowledge Center. All rights reserved

| | |
|---|---|
| 4. Ack | ● DHCP Request 메시지를 수신한 DHCP서버는 메시지 내에 Server Identifer에 기록된 IP 주소가 자신의 주소인지 확인 후, DHCP Ack 메시지를 이더넷 망에 브로드캐스팅<br>● 이를 수신한 단말은 DHCP서버가 전달해 준 정보를 기반으로 네트워크 환경 구성 |

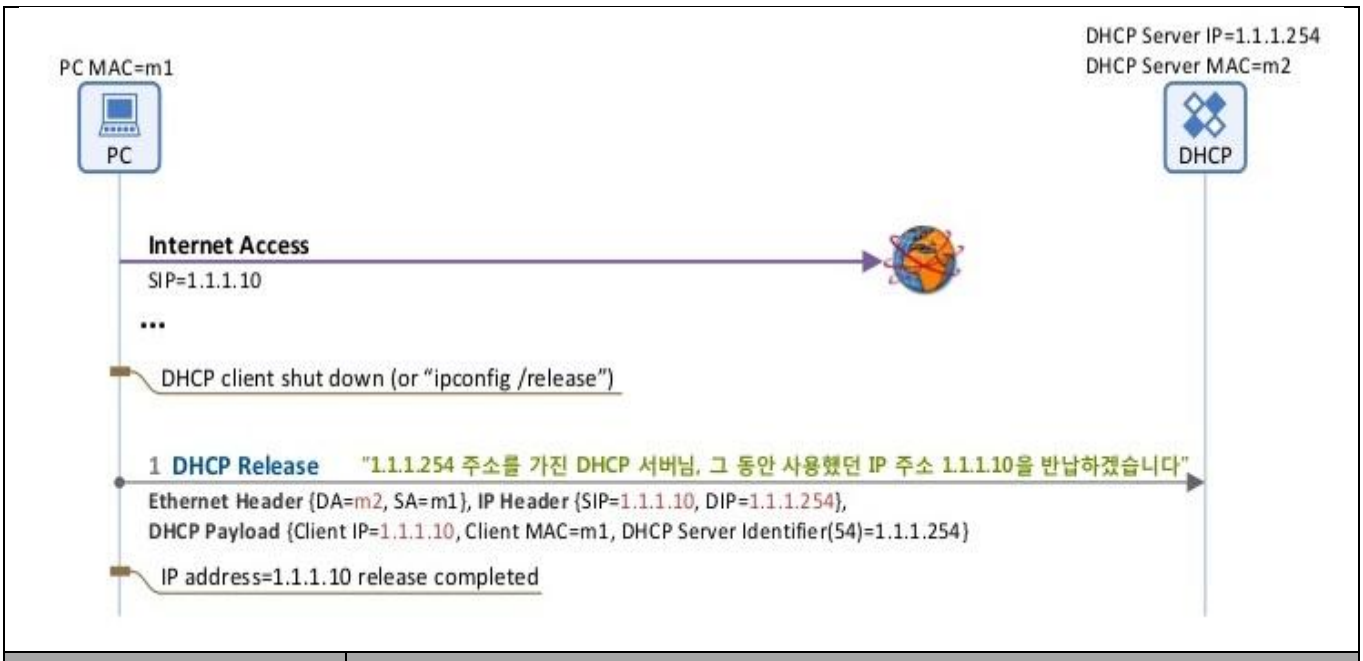
**나. IP 주소 임대기간 연장 절차(IP Address Renewal Procedure)**




| 단계 | 설명 |
|---|---|
| 1. Request | ● IP Lease Time의 절반이 되었을 때 단물은 IP주소 임대기간 연장을 위해 DCHP서버에 DHCP Request메시지 송신<br>● 서로 IP 주소를 알고 있기 때문에 유니캐스팅 |
| 2. Ack | ● DHCP Request를 수신한 DHCP서버가 단말의 요청을 수락하게 되면, DHCP Ack 메시지에 단말이 사용할 IP주소, Subnet Mask, Default Gateway IP 주소, DNS IP 주소, Lease Time 등을 포함 유니캐스팅<br>● 이를 수신한 단말은 DHCP Ack 메시지에 포함된 IP Lease Time 동안 IP 주소를 연장 사용 |

- 1/2 이 지난 후에 DHCP 서버가 DHCP Ack 를 보내지 못하면 7/8 이 되었을 때 DHCP Request 재송신

### 다. IP 주소 반납 절차(IP Address Release Procedure)




| 단계 | 설명 |
|---|---|
| 1. Release | ● 더 이상 임대 받았던 IP주소가 필요치 않은 단말은 DHCP Release메시지를 유니캐스팅으로 DHCP서버에 전달<br>● DHCP서버는 DHCP Release내에 Client IP 필드에 기록된 IP주소를 반환 |

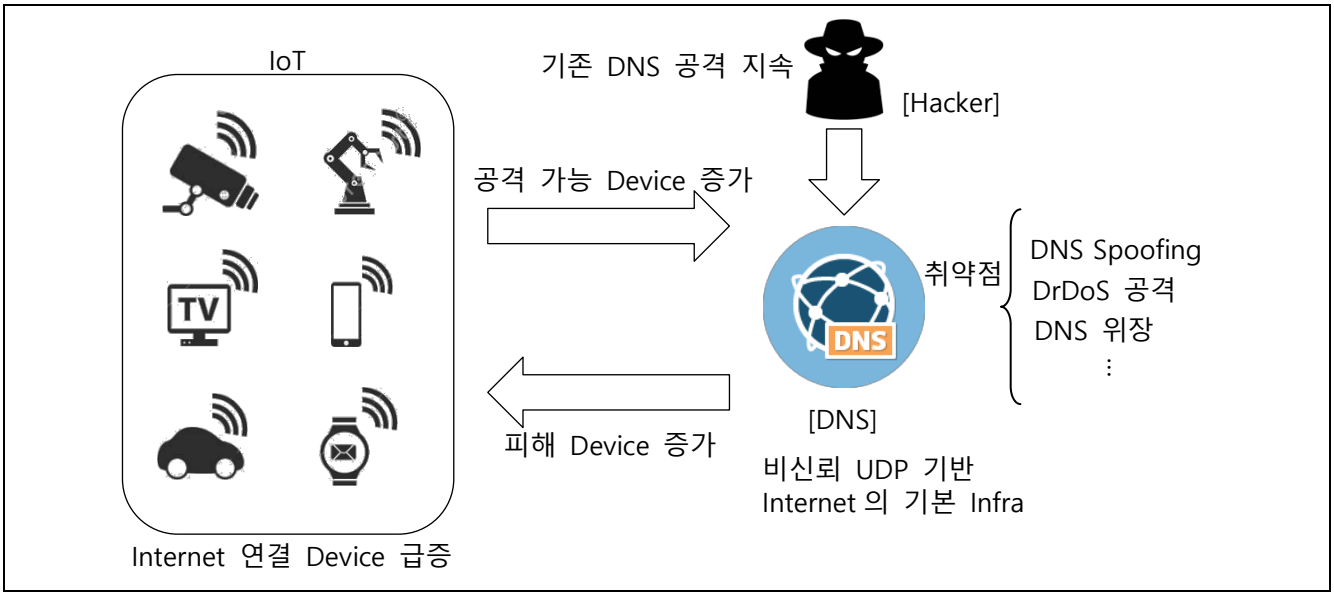
### 4. DHCP 와 NAT 의 비교

| 구분 | DHCP | NAT |
|---|---|---|
| IP 구분 | ● 공인/사설 IP 주소 할당 | ● 사설 IP 주소 할당 |
| 응용 제한 | ● 응용 서비스 제한 없음 | ● P2P 등 일부 응용 서비스 제한 |
| IP 임대 여부 | ● 일정 시간 임대 후 재 회수 | ● 고정 할당 |
| 해킹 추적 | ● 가능 | ● 어려움 |
| 사설망 보호 | ● 불가능 | ● 가능 |
| 지연 요소 | ● 상대적 유리 | ● 상대적 부리(NAT 동작 지연) |


Copyright ⓒ 2014 By Korea Productivity Center Convergence Knowledge Center. All rights reserved

| 4 | DNS(Domain Name System), DNSSec(DNS Security Extensions) | | |
|---|---|---|---|
| 문제 | 사물인터넷(IoT) 시대가 진입하면서 IoT Device 기기를 이용한 DNS(Domain Name System)에 대한 공격과 피해가 급증하고 있다. 이와 관련하여 DNS(Domain Name System) 원리와 DNSSec(DNS Security Extensions)에 대하여 설명하시오. | | |
| 도메인 | 디지털 보안(Digital Security) | 난이도 | ★ ★ ☆ ☆ ☆ (별 5 개 기준) |
| 출제의도 | IoT Device 와 DNS 를 이용한 웹호스팅 업체 딘(Dyn) 공격 발생<br>DNS Server 를 직접 겨냥한 디도스(DDoS) 공격의 급증(2016 년 기준 전년 동기 대비 75% 증가)<br>고전 Topic 이면서 미출제인 DNSSec 에 대한 학습 여부 | | |
| 핵심 내용 키워드 | DNS - Domain Name Space, Resource Record, Name Server, Resolver<br>DNSSec - 전자서명, DNSKEY, RRSIG, DS, NSEC / NSEC3 | | |
| 목차예시 | 1. IoT 환경에서 DNS(Domain Name System)의 공격<br>2. DNS(Domain Name System)의 원리<br>3. DNS 보안의 기초. DNSSec(DNS Security Extensions) 메커니즘<br>4. DNS 주요 공격과 대응 방안 | | |
| 채점 점수 가이드 | ① DNS와 DNSSec의 개념, 이해 부족 (5~8점)<br>② DNS와 DNSSec의 기본 이해 수준 (9~14점)<br>③ DNS와 DNSSec의 정확한 기술 제시 (14~15점)<br>④ DNS와 DNSSec의 추가요소 설명(+α) | | |
| 참고문헌 | 도메인네임시스템(DNS) (한국인터넷정보센터)<br>DNS 기본 동작 설명(DNS Basic Operation, NETMANIAS(netmanias.com), 유창모, 2011 년 12 월)<br>DNS 공격의 3 가지 유형, 그리고 대응법(IT World Korea, 2013 년 08 월)<br>Open DNS 보안조치 가이드(한국인터넷진흥원 & 인터넷침해사고대응지원센터, 2007 년 03 월) | | |
| 고득점전략 및 답안작성 가이드 | 기본 Topic 으로 추가 공격 기법과 대응 방안, 세부적 기술 요소들의 추가 통한 차별화 필요<br>DNS 와 DNSSec 의 정확한 동작 Process 에 대한 학습<br>DNSSec 은 미기출 Topic 에 해당되므로 이에 대한 대비 | | |
| 출제자 | 안경환 기술사(제 110 회 정보관리기술사 / akh.itpe@gmail.com) | | |

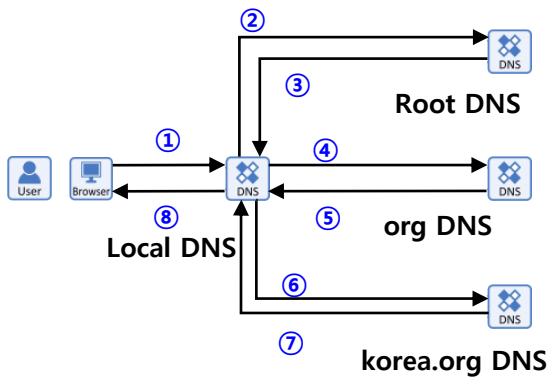
## 1. IoT 환경에서 DNS(Domain Name System)의 공격




- 기존 DNS 의 취약점은 완전한 해결이 안된 상태에서 IoT Device 의 증가로 인해 공격 가능 Device 와 피해 가능 Device 가 급증하는 문제 발생
- IoT Device 를 이용하여 호스팅 업체 딘(Dyn)의 공격으로 DNS 의 보안에 대한 문제가 재조명

## 2. DNS(Domain Name System)의 원리

### 가. DNS(Domain Name System)의 동작 방식

| DNS 동작 방식 | 단 계 | 동작 설명 |
|---|---|---|
|  | ① Host name IP 요청 | Host Name(www.korea.org)에 대한 IP 요청 |
| | ②③ Root DNS Query | Root DNS에 요청 후 Root DNS 가 정보 없을 경우 org DNS 전달 |
| | ④⑤ Top Level DNS Query | org DNS Query 후 IP 정보나 korea.org DNS 주소 전달 |
| | ⑥⑦ Secondary Level DNS Query | korea.org를 소유한 DNS로부터 IP Address 획득 |
| | ⑧ IP 정보 획득 | IP Address를 최종 PC에서 획득 |



- DNS = 체계적인 도메인 이름 체계 + 분산 구조형 계층적 도메인 데이터베이스 체계

### 나. DNS(Domain Name System)의 구성 요소

| 구성 요소 | 세부 구성 요소 | 설 명 |
|---|---|---|
| Domain Name Space | ". "(dot) 으로 구분된 레이블로 구조화 | - 최상위 Root DNS가 존재하고 하위에 Node들이 계층적으로 구성하여 Resource Records라는 정보 집합체로 표현 |
| Resource Record | Name, Type, Class, TTL, RD, A, SOA, NS, CNAME, PTR | - 도메인 네임(domain name)과 인터넷 자원(resource) 정보를 매핑하여 하나의 분산 구조형 데이터베이스를 구성하기 위한 수단 |

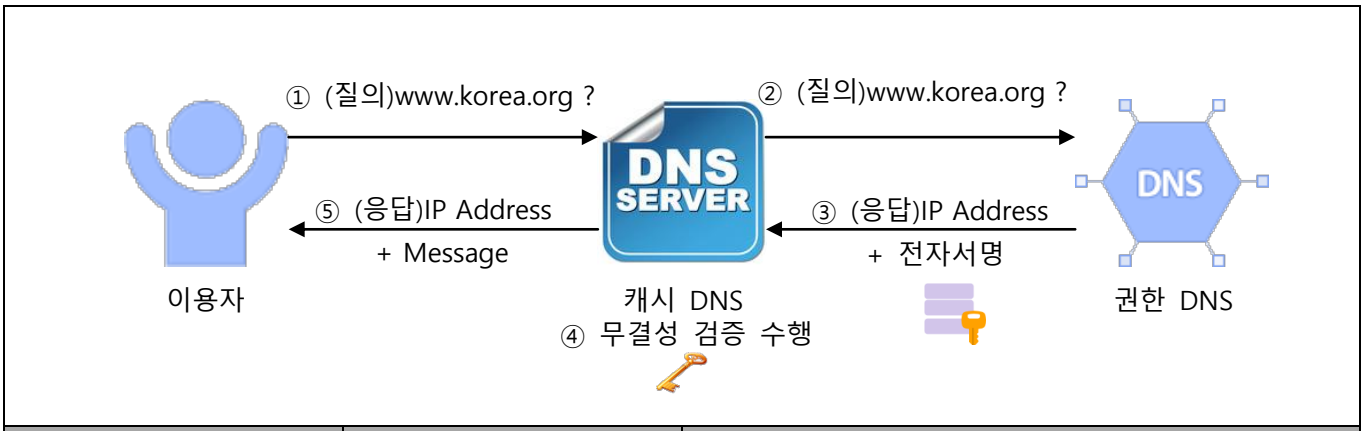

Copyright ⓒ 2015 By Korea Productivity Center Convergence Knowledge Center. All rights reserved

| | | |
|---|---|---|
| Name Server | Iterative DNS 서버 | - 특정 질의에 대해 자신이 소유한 도메인 존의 정보만 그 응답으로 제공하는 동작을 하는 DNS 서버 |
| | Recursive DNS 서버 | - 대부분의 DNS 서버 동작 방식으로 Client의 Recursive 요청에 대응하여 Resolver 질의 절차를 수행하는 DNS 서버 |
| | Authoritative DNS 서버 | - 도메인 네임 공간 상의 특정 영역에 대해 관리 권한이 위임된 서버 |
| Resolver | Full Resolver, Stub Resolver | - 응용 프로그램과 DNS 간의 인터페이스 역할로서 도메인 데이터베이스를 검색하는 기능 |

- DNS 는 질의 응답시 Recursive Name Server 의 Cache data 를 위・변조하는 DNS Cache Posioning 공격에 취약하며 이를 방어하기 위해 DNSSec 의 도입 필요

### 3. DNS 보안의 기초. DNSSec(DNS Security Extensions) 메커니즘

#### 가. DNSSec(DNS Security Extensions)의 동작 Process




| Process | 주요 특징 | 설명 |
|---|---|---|
| ①② Domain 질의 | Name Server의 Resolver 수행 | 요청 Domain에 대한 IP 정보 미소유시, 권한 DNS에 요청 |
| ③ IP 정보 응답 | 공개키 암호화 방식의 전자 서명 | IP 정보와 함께 각 리소스 레코드를 공개키 암호화 방식의 전자서명(Digital Signature)한 후 이를 RRSIG 리소스 레코드에 저장하여 응답 |
| ④ 무결성 검증 | Hash 알고리즘 통한 digest 상호 일치 검증 | 서명 대상 데이터에 대한 Hash 결과 값과 RRSIG RR의 Signature를 해독하여 얻은 digest 값을 상호 비교・일치 여부 확인 |
| ⑤ IP 정보 전달 | IP Address | 최종 요청 사용자에게 IP Address와 Secure Message 전달 |

- DNSSec(DNS Security Extensions)은 DNS 데이터의 위조-변조 가능성을 원천적으로 차단하기 위해, 공개키 암호화방식(Public Key Cryptography)의 전자서명 기술을 DNS 체계에 도입한 인터넷 표준 기술
- DNS Resource Record 데이터를 암호화하지 않고 해당 데이터가 변조되었는지 확인할 수 있는 메커니즘을 제공(DNSSec을 미인식하는 기존 Resolver와의 호환성 확보)

### 나. DNSSec(DNS Security Extensions) 적용을 위한 추가 Resource Record type

| Resource Record | 역할 | 설 명 |
|---|---|---|
| DNSKEY | 공개키 | - 도메인 존의 공개키 데이터 저장 위한 RR로 질의 응답을 통해 배포(존의 개인키는 안전한 장소에 따로 보관)<br>- 공개키는 ZSK와 KSK의 2종류 존재 |
| RRSIG | 서명 데이터 | - 도메인 존 안에 있는 RRSet에 대한 개인 키의 전자서명한 결과 값을 갖는 RR<br>- RRSIG는 DNS 응답 메시지에 전자서명 대상 RR과 함께 포함되어 전달 |
| DS | 원본 데이터 | - DNS 고유의 위치 체계에 따라 보안 측면의 인증된 위임 체계를 구성하기 위한 데이터를 저장하는 RR<br>- 부모 도메인과 자식 도메인간 인증사슬(Authentication chain) 형성 |
| NSEC / NSEC3 | 원본 데이터 | - "DNS 데이터 부재 인증"을 위해 정의된 RR<br>- 특정 리소스 레코드가 존재하지 않음을 전자 서명을 통해 인증할 수 있는 메커니즘 제공<br>- NES의 존목록화 문제를 해결하기 위해 NES3 레코드 추가 정의 |

- DNSSec은 DNS의 기본 방어 Infra로 구성되어 DNS Cache Poisoning 공격등은 방어가 되나 그 외 공격은 대응 불가하므로 추가적 대응 방안의 필요
- KSK(Key Signing Key): ZSK를 서명하는데 사용. Zone의 Secure Entry Point(SEP) 키로 사용. 암호화 비트를 길게 사용하고 기간을 길게 설정
- ZSK(Zone Signing Key): Zone의 모든 RR을 서명하는데 사용, 암호화 비트를 짧게 사용하고 기간을 짧게 설정

## 4. DNS 주요 공격과 대응 방안

| 공격 기법 | 공격 설명 | 대응 방안 |
|---|---|---|
| cache poisoning attack | Recursive DNS server에 악성 DNS 데이터를 삽입하여 해커의 Site로 유도 | - DNSSec의 설치 및 운영<br>- Name Server의 recursive 기능 제한 |
| 권한 DNS 탈취 | DNS의 OS 보안 취약점 등을 이용하여 DNS를 해커가 점령 후 악용 | - 강력한 Password 설정<br>- IP 기반의 ACL(Acceptable Client List) 적용<br>- DNS 운영자의 소셜 엔지니어링 등 보안 교육 |
| DNS의 DDoS 공격 거점 활용 | 공격 대상 System을 source IP로 설정 후 DNS Query 수행 | - Recursion 서비스를 신뢰된 host로 제한<br>- Recursion 기능 비활성화<br>- Blackhole 옵션 이용한 DNS 질의 제한 |

- 끝 -


Copyright ⓒ 2015 By Korea Productivity Center Convergence Knowledge Center. All rights reserved

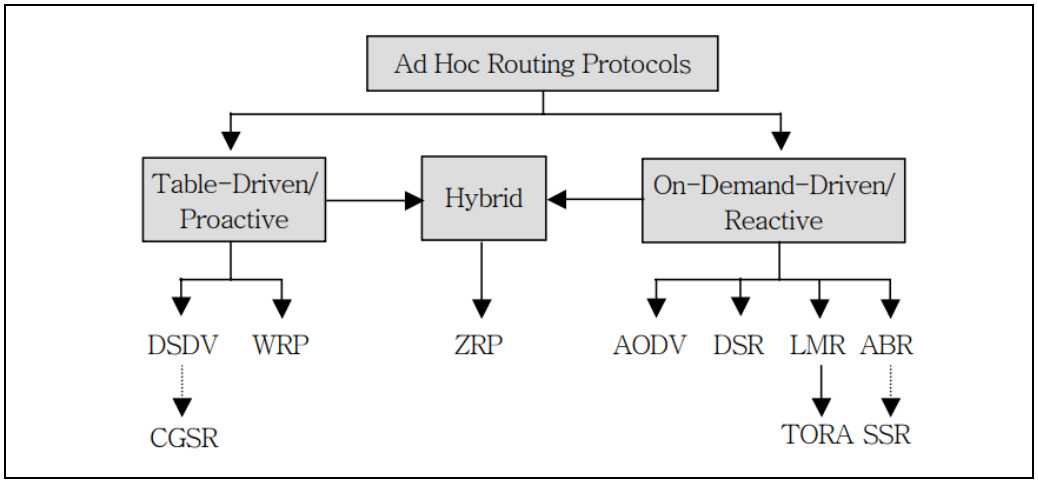
| 7 | Ad-hoc Network Routing Protocol (핵심요약) |
|---|---|
| 문제 | Ad-hoc Network Routing Protocol |
| 도메인 | 네트워크 |
| 정의 | 동적 Topology 로 구성된 Ad-hoc NW 망에서 NW 참여 노드 간 통신 경로 설정 및 유지를 위한 라우팅 프로토콜 |
| 키워드 | Proactive, Hybrid, Reactive(On-demand), DSDV, AODV |
| 출제의도분석 | IoT 기반 스마트 시스템(팩토리, 팜, etc) 구성 증가에 따른 Ad-hoc 기반 통신 프로토콜 출제 |
| 답안작성 전략 | 프로토콜 방식 분류 기반 상세 프로토콜 설명 후 추가적으로 실제 ad-hoc 라우팅 관련 시스템 구성 작성 |
| 참고문헌 | - 이동 Ad Hoc 네트워크 기술 동향(전자통신동향분석 제 18 권 제 2 호),<br>- 무선 Ad Hoc 네트워크에서 단방향 링크를 이용한 하이브리드 라우팅 |
| 풀이 기술사님 | 김승준 PE (제 117 회 컴퓨터시스템응용기술사 / kimsj2435@gmail.com) |

## 1. 동적 Topology NW 내 기기간 통신, Ad-hoc NW 라우팅 프로토콜 정의

- 동적 Topology 로 구성된 Ad-hoc NW 망에서 NW 참여 노드 간 통신 경로 설정 및 유지를 위한 라우팅 프로토콜
- (특징) Multi-hop Routing, 동적 Topology 구성, Peer-to-Peer 통신

## 2. Ad-hoc NW Protocol 분류 및 설명

### 가. Ad-hoc NW Protocol 분류




- RIP/OSPF 라우팅 프로토콜은 동적 변화가 빈번한 Ad-hoc NW 에서는 부적합

### 나. Ad-Hoc NW Protocol 설명

| 분류 | 프로토콜 | 설명 |
|---|---|---|
| Table-Driven Proactive (테이블 관리 방식) | - 주기적, 혹은 NW 변화 시, 라우팅 테이블 Broadcasting<br>- 항상 최신 경로 정보 유지, 경로 탐색 지연 없이 트래픽 라우팅<br>- Broadcasting Overhead 존재, 메시지 크기 최소화 필요(소규모 NW 에서 사용) | |
| | DSDV | - Destination Sequenced Distance Vector(벨만포드 알고리즘)<br>- Sequence Number 통해 최신 메시지 판단, 브로드캐스팅 시, 루프 문제 방지 |

| | | |
|---|---|---|
| | WRP | - Wireless Routing Protocol<br>- 거리/라우팅/링크비용/메시지 재전송 리스트 테이블 기반 라우팅 수행<br>- 메시지 재전송 리스트 테이블 기반 테이블 정보 송/수신 통해 라우팅 정보 유지<br>- 이웃 노드에게만 라우팅 정보를 전송 |
| | CGSR | - Clustered GW Switching Routing<br>- 클러스터 단위로 NW 구성 후, GW 역할 수행 클러스터 헤드 노드 선출, 이를 기반으로 라우팅 수행 프로토콜<br>- 클러스터 헤드 선출 Overhead 최소화 위해 LCC(Least Cluster Change) 알고리즘 기반 헤드 변경 |
| On-Demand-Driven Reactive (요구 기반 방식) | - 패킷 라우팅 필요한 순간(On-demand) 라우팅 경로 계산, 라우팅 수행<br>- 이동 노드 NW 경로 상시 유지하지 않고 필요할 때만 경로 계산, 유지<br>- 테이블 기반 라우팅의 단점 해결(Board Casting Overhead)<br>- 경로 계산으로 인한 지연 시간 발생하지만, 최신 경로로 라우팅 가능 | |
| | DSR | - Dynamic Source Routing<br>- 경로발견, 경로유지 메커니즘 기반 구성<br>- 다중 NW 홉 기반 소스 루트 발견, 리스트 기반 전송 |
| | AODV | - Ad Hoc On-demand Distance Vector<br>- 라우팅 경로 발견 시, 이웃 노드에 RREQ(Route Request) 브로드캐스팅, 이를 반복하여 목적지까지 경로 탐색<br>- 목적지 도달 시, RREP(Route Response) 통해 응답, 이를 기반으로 경로 탐색 |
| Hybrid | - 일정 영역 내의 경로 데이터를 Proactive 방식으로 유지, 영역 외의 경로는 Reactive 방식으로 라우팅 수행하는 방식<br>- 기존 2 방식의 장/단점을 보완하기 위한 프로토콜 방식 | |
| | ZRP | - Zone Routing Protocol<br>- 동일 영역(Zone) 내에서 Intra-zone Routing Protocol(IARP) 기반 Proactive 방식 라우팅<br>- 외부 영역 탐색 시 Inter-zone Routing Protocol(IERP)기반 Reactive 방식 라우팅 |

- NW 규모 및 노드 간 통신 요구사항(실시간성, 지연 등)에 따른 라우팅 프로토콜 선택 필요

[참고 – 1. 리눅스 시스템에서 ad-hoc NW 구성 방법(Ubuntu 기준)]

- 리눅스 시스템의 NW 설정 파일에 "ad-hoc" 모드 set 설정 후, network 데몬 재시작 시 반영
- Ubuntu 18.04 이전: /etc/network/interfaces.d 파일에 "wireless-mode ad-hoc" 추가
- Ubuntu 18.04 이후: /etc/netplan/adhoc.yaml 파일에 "mode: adhoc" 추가

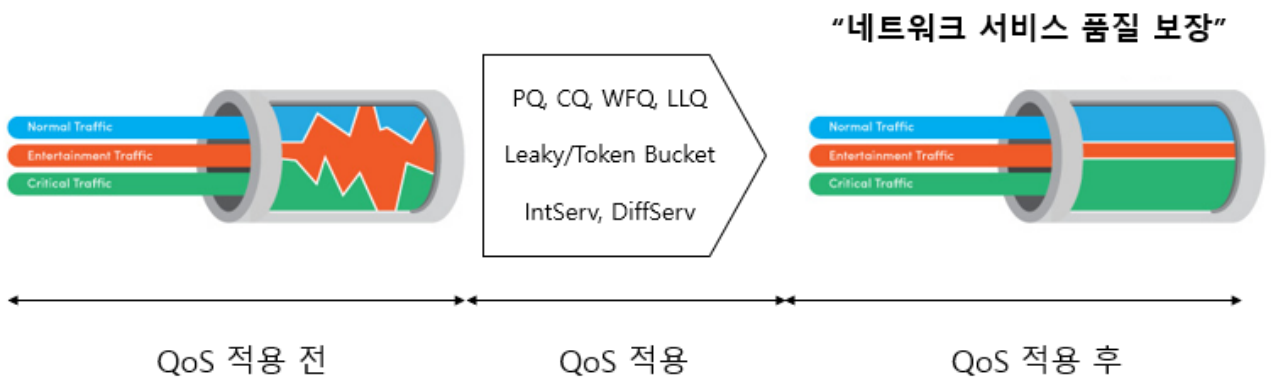
[참고 -2. 실제 DSR/AODV 소스코드 구현]

- select() 함수 기반 event-driven 방식으로 UDP 기반 구현
- NW 관련 프로세스 시작 시, HELLO 메시지를 주기적으로 송/수신하며 NW 참여 노드상태 체크

"끝"

| 6 | QoS | | |
|---|---|---|---|
| 문제 | 네트워크 서비스 품질(QoS) 보장을 위한 기술 중 다음에 대해 설명하시오.<br>가. 패킷 처리 순서 결정을 위한 스케줄링 기술<br>나. 트래픽 처리량 제어를 위한 버킷(bucket) 기술<br>다. IntServ 모델과 DiffServ 모델 비교 | | |
| 도메인 | 네트워크 | 난이도 | ★ ★ ★ ★ ☆ |
| 출제배경 | 디지털 트랜스포메이션으로 인해 폭증하는 데이터 트래픽과 네트워크 슬라이싱, 망중립성 이슈에 따른 네트워크 서비스 품질(QoS) 보장 기술에 대한 이해도 확인 | | |
| 핵심 키워드 | FIFO, PQ, CQ, WFQ, CBWFQ, LLQ, Leaky Bucket, Token Bucket, IntServ, DiffServ, RSVP, PHB | | |
| 참고문헌 | 컴퓨터 네트워크: A Top-Down Approach (Mc Graw Hill, 이재광 역)<br>기술사 서브노트 | | |
| 출제자 | 이ㅇㅇ 기술사 (제 117 회 정보관리기술사) | | |

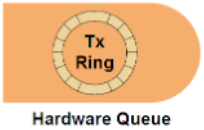
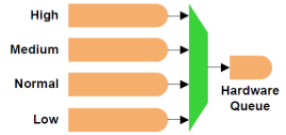
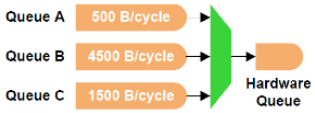
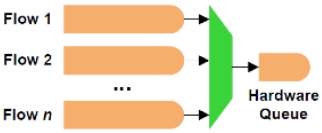
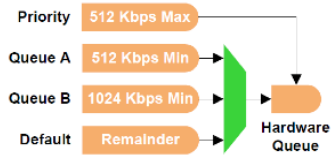
**1. 네트워크 서비스 품질(QoS)의 개념 및 필요성**




| | |
|---|---|
| 개념 | 사용자 또는 어플리케이션에 대해 중요도에 따른 서비스 수준을 차등화하여 한정된 네트워크 자원으로 트래픽과 대역폭을 정책적으로 관리하는 네트워크 서비스 품질 보장 기술 |
| 필요성 | - 데이터와 음성 통신 회선을 하나의 회선으로 통합하여 비용을 절감<br>- 한정된 네트워크 자원을 효과적으로 관리할 수 있는 정책 적용<br>- 음성통화 등 실시간 트래픽은 지연에 민감하므로 전송 성능 예측 및 보장 |

- 트래픽은 신뢰성, 지연, 지터, 대역폭의 특성을 가지고 있으며, 4가지 특성을 관리하여 서비스 품질을 보장
- FTP, HTTP 등 데이터 전송 트래픽의 경우 신뢰성의 민감도가 높으며, 지연이나 지터의 민감도는 낮음
- VoIP, VoD 등 멀티미디어 전송 트래픽의 경우 신뢰성보다는 지연이나 지터의 민감도가 높음

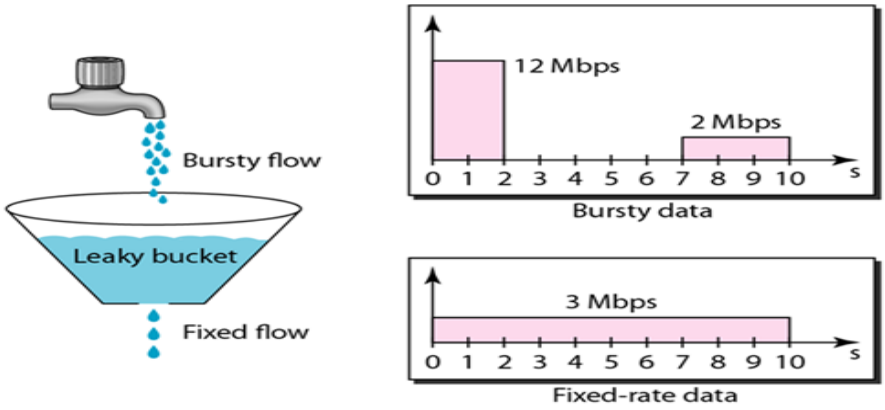
## 2. 패킷 처리 순서 결정을 위한 스케줄링 기술

| 기술 | 개념도 | 특징 | 장점/단점 |
|---|---|---|---|
| FIFO |  | - First In First Out<br>- 인입 순서대로 처리<br>- 단독 Queue<br>- Best Effort 방식 | - 구조가 단순<br>- QoS 적용 불가 |
| PQ |  | - Priority Queue<br>- 클래스별 우선순위 지정<br>- 4개의 클래스로 분류<br>- FIFO 단점을 해결 | - 차등 트래픽 서비스 가능<br>- 낮은 우선순위 트래픽의 기아 현상 발생 가능 |
| CQ |  | - Custom Queue<br>- 클래스 별 Round-Robin<br>- 16개의 클래스로 분류<br>- PQ 단점을 해결 | - 클래스 별 공평한 서비스<br>- 차등 트래픽 서비스 불가 |
| WFQ |  | - Weighted Fair Queue<br>- 클래스 별 가중치 부여<br>- 4096개의 클래스로 분류<br>- PQ와 CQ 단점을 해결 | - 차등 트래픽 서비스 가능<br>- 혼잡 회피 방식 Tail-Drop만 가능 RED, WRED 사용 불가 |
| CBWFQ | | - Class-Base WFQ<br>- 클래스마다 대역폭, 가중치, 패킷 제한 정책 정의<br>- WFQ의 단점을 해결 | - 혼잡 회피 방식으로 RED, WRED 사용 가능<br>- 긴급 트래픽도 정책에 따라 대기 |
| LLQ |  | - Low Latency Queue<br>- 긴급 트래픽 PQ 적용<br>- 나머지 트래픽 CBWFQ적용<br>- Voice 트래픽 처리 가능 | - 긴급 트래픽 우선 처리 가능<br>- 구현 및 정책 적용 어려움 |

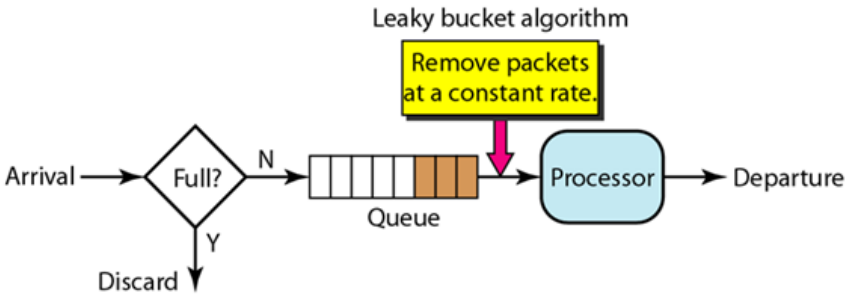
- 음성/동영상 등 멀티미디어 전송 시 우선 처리가능한 PQ, LLQ 사용하며, 일반 데이터 전송 시 CQ, WFQ 등 사용

## 3. 트래픽 처리량 제어를 위한 버킷(bucket) 기술

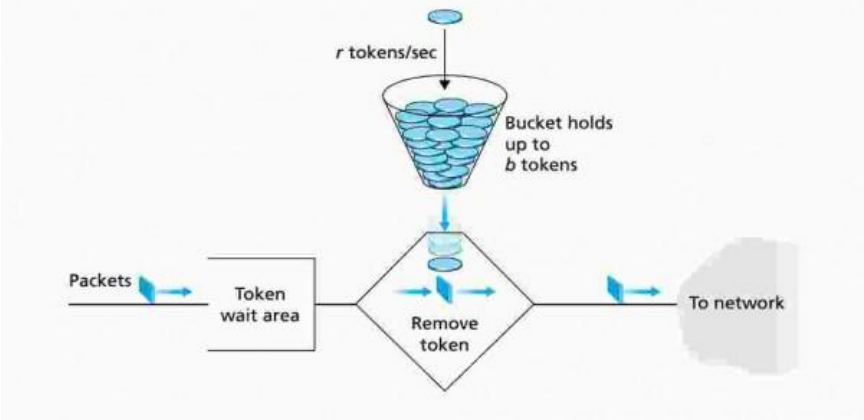
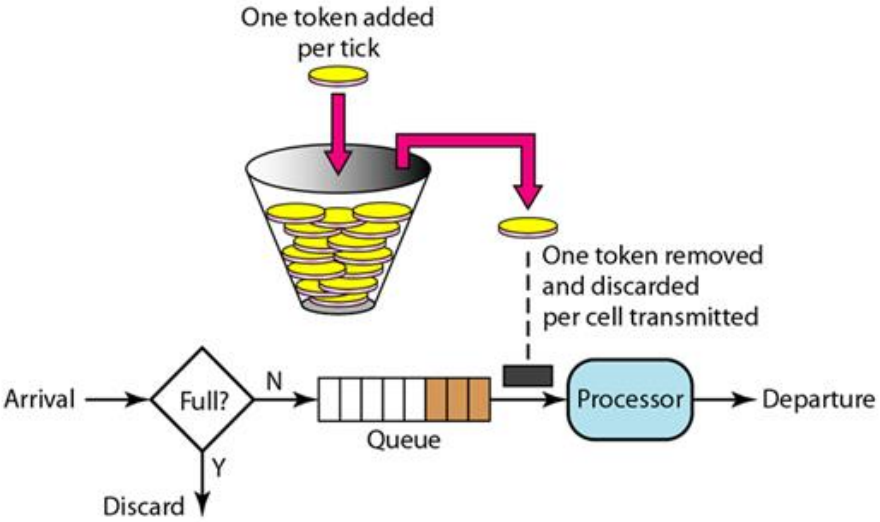
### 가. 리키 버킷 (Leaky Bucket)

| | |
|---|---|
| 개념 | 불규칙적으로 인입되는 트래픽의 데이터율을 평균으로 만들어 버스트 트래픽을 고정 데이터율 트래픽으로 조정하는 트래픽 처리량 제어 기술 |
| 개념도 |  |


Copyright ⓒ 2015 By Korea Productivity Center Convergence Knowledge Center. All rights reserved

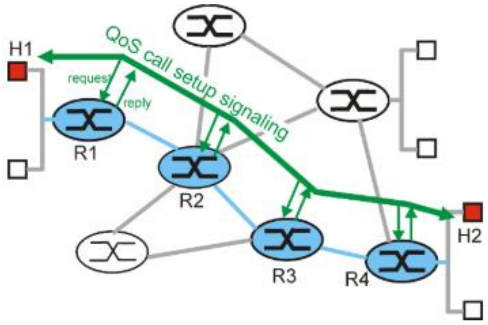
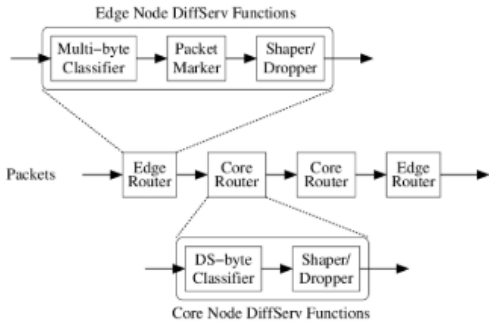
| | |
|---|---|
| 절차도 |  |
| 알고리즘 | ① 클럭의 틱에서 카운터를 버킷 크기 n으로 초기화<br>② n이 패킷 크기보다 크면 패킷을 송신하고 카운터를 패킷 크기만큼 감소<br>③ n이 패킷 크기보다 작을 때까지 ②단계를 반복<br>④ 카운터를 리셋(reset)하고 ①단계로 이동 |

**나. 토큰 버킷 (Token Bucket)**

| | |
|---|---|
| 개념 | 규정된 최고 데이터율 범위 내 버스트 트래픽을 허용하도록 트래픽 제어용 토큰의 유무에 따라 트래픽을 조정하는 트래픽 처리량 제어 기술 |
| 개념도 |  |
| 절차도 |  |
| 알고리즘 | ① 토큰을 카운터로 구현하며, 0으로 초기화<br>② 클럭의 틱 마다 토큰이 추가되며 카운터가 1씩 증가<br>③ 데이터 단위(unit) 하나가 송신될 때 마다 카운터가 1씩 감소<br>④ ② 단계와 ③단계를 반복하며 카운터가 0이 되면 호스트는 데이터 송신 불가 |

- 리키 버킷은 트래픽의 속도를 제한, 토큰 버킷은 트래픽이 사용하는 토큰을 제한하며 두 기술의 복합 사용 가능

**4. InServ 모델과 DiffServ 모델 비교**

| 항목 | InServ 모델 | DiffServ 모델 |
|---|---|---|
| 개념 | 종단 간 개별 트래픽 흐름 단위로 경로 상 라우터 자원을 예약(RSVP)하는 종단 간 QoS 보장 모델 | 패킷 DS(Diff-Service) 필드에 DSCP를 마킹하는 서비스 클래스 별 PHB 우선순위 기반 QoS 보장 모델 |
| 개념도 |  |  |
| QoS 보장 | Flow 별 종단 간 QoS 보장 | Class 별 QoS 보장 |
| QoS 보장 범위 | 단대단(End-to-End) | 도메인내(Edge-to-Edge) |
| 자원 예약 | 응용에 의해 제어 | Edge 노드에서 제어 |
| 자원 관리 | 분배형 자원 관리 | 집중형 자원 관리 |
| 망 규모 | 소규모(LAN) | 대규모(WAN, MAN) |
| 신호제어 형식 | RSVP 프로토콜 | IP 패킷 헤더 내 DSCP |
| 확장성 | 확장 제약 | 유연한 확장성 |
| 구현성 | 복잡한 구현성 | 구현이 단순 |

- 네트워크 환경에 따라 소규모 망에는 IntServ, 중/대규모 망에는 DiffServ 모델 사용을 고려할 수 있으며, Edge Router를 기준으로 외부 전송 시 IntServ, 내부 전송 시 DiffServ를 혼합하여 사용하는 통합 QoS 모델도 고려 가능


Copyright ⓒ 2015 By Korea Productivity Center Convergence Knowledge Center. All rights reserved

| | |
|---|---|
| 문 제 | **4. 네트워크 서비스 품질 향상을 위한 QoS(Quality of Service)에 대하여 다음을 설명하시오.**<br>**가. QoS 의 기술**<br>**나. QoS 의 모델**<br>**다. QoS 측정요소** |

| | | | |
|---|---|---|---|
| 출 제 영 역 | 네트워크 | 난 이 도 | ★★☆☆☆ (별 5 개 기준) |
| 출 제 배 경 | 81 회 이후 미 출제된 문제로 대비 필요 | | |
| 출 제 빈 도 | 81 회 조직응용 1 교시 | | |
| 참 고 자 료 | - 전자상거래를위한 전자시 | | |
| Keyword | Queuing, Policing, Shaping, intServ, diffServ, 대역폭, 지연, 지터, 패킷손실 | | |
| 풀이 기술사님 | 전정은(122 회 정보관리기술사 / jjee0423@naver.com) | | |

## 1. 네트워크 품질보장, QoS(Quality of Service) 개요

| 구분 | 내용 |
|---|---|
| 분 류 | QoS(Quality of Service)<br>QoS 기술: - Queuing - Policing - Shaping<br>QoS 모델: - IntServ - DiffServ - MPLS - CDN<br>QoS 측정요소: - 대역폭 - 지연 - 지터 - 패킷손실 |
| 개 념 | - 한정된 네트워크 망의 대역폭을 효율적으로 사용하게 하고, 네트워크 트래픽을 정책별로 제어하여 인터넷 종단간 서비스 품질을 향상시키는 기술 |

- QoS 기술, QoS 모델 적용 및 QoS 측정요소로 품질 측정 가능

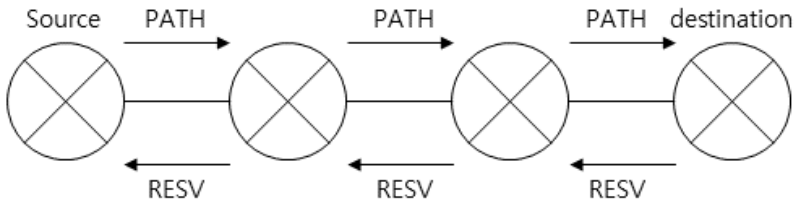
## 2. QoS(Quality of Service)의 기술

| 구분 | 기술 | 설명 |
|---|---|---|
| Queuing | FIFO | - 먼저 들어온 패킷이 먼저 나가는 선입선출 스케줄링 기법 |
| | PQ | - FIFO 문제점 해결 위해 High, Medium, Normal, Low 4 가지 클래스를 가지는 차등화 서비스 제공 |
| | CQ | - PQ 문제점 해결 위해 클래스 별 라운드 로빈 방식으로 돌아가며 처리 |
| | WFQ | - PQ, CQ 문제점 해결 위해 클래스 별 가중치 기반 처리 |
| | CBWFQ | - WFQ 의 확장판으로 각 클래스 마다 Bandwidth, Weight, Packet Limit 정책을 정의 |
| | LLQ | - CBWFQ 에 PQ 를 혼합하여 우선 처리해야 할 트래픽은 PQ 로 수행하고 나머지는 CBWFQ 로 수행 |

| | | |
|---|---|---|
| Policing | Tail Drop | - 큐에 패킷이 가득차면 신규 패킷을 drop 하는 방식 |
| | RED | - 혼잡 발생 전 패킷을 랜덤하게 drop 하는 방식 |
| | WRED | - RED 를 보완하여 버려지는 패킷에 가중치를 부여하여 drop |
| Shaping | Leaky Bucket | - 데이터율을 평균으로 만들어 트래픽을 고정 데이터율로 고정 |
| | Token Bucket | - 신용을 축적하여 최고 데이터율 버스트 트래픽 허용 |

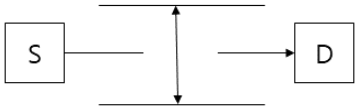
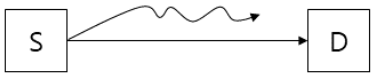
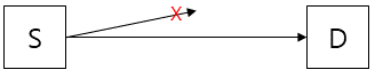
- Queuing, Policing, Shaping 방식을 이용하여 패킷의 임계치 초과 시 서비스 하는 방식 관리

### 3. QoS(Quality of Service) 모델

| 구분 | 기술 | 설명 |
|---|---|---|
| intServ | 개념 | - 유입되는 패킷을 패킷 흐름별 또는 연결 세션별로 분류 후 사전에 자원 예약하여 QoS 모델 |
| | 개념도 |  |
| | 서비스 유형 | - Best-Effort Service : 최선의 노력을 다하지만 확실한 전송 미보장 |
| | | - Controlled-Load Service : 다소 유연한 실시간 응용 지원 및 보다 나은 서비스 지원 |
| | | - Guaranteed Service : 실시간 절대적 품질 제공 |
| | 적용 | - 소규모 네트워크 |
| diffServ | 개념 | - DS 필드 및 PHB 를 정의하여 서비스 제공 유형을 ISP 가 결정하는 등급 기반 QoS 모델 |
| | 개념도 | |
| | 주요요소 | - Packet Classifier : 최종적으로 어떤 PHB(Per-Hop Behavior)를 할당할 것인지 패킷 헤더를 분석 |
| | | - DSCP (Differentiated Service Code Point) : 모든 IP 헤더에 DSCP 를 붙임 |
| | | - PHB (Per-Hop-Behaviour) : 패킷을 수신하는 홉 단위 동작 |
| | 적용 | - 대규모 네트워크 |

- intServ 는 소규모망, diffServ 는 백본망에 주로 적용

### 4. QoS(Quality of Service) 측정요소

| 측정요소 | 개념도 | 설명 |
|---|---|---|
| 대역폭 |  | - 일정시간에 처리한 데이터의 총량 |
| 지연 |  | - 종단간 송수신 지연 시간 |
| 지터 | | - 원래 신호로부터 왜곡되는 정도 |
| 패킷손실 |  | - 데이터를 전송하는 과정에서 패킷의 손실정도 |

- QoS 측정을 통해 트래픽 운용 관리가 적절히 운영되고 있는지 파악가능하며 서비스 품질을 보장함

"끝"

| 7 | CDN(Contents Delivery Network) | | |
|---|---|---|---|
| 문제 | CDN(Contents Delivery Network)의 동작원리, 주요기술, 캐싱방식에 대해 설명하시오. | | |
| 도메인 | 네트워크 | | |
| 출제배경/의도 | TV 시청방식의 개인화에 따른 인터넷 기반 OTT 서비스의 활성화에 따른 트래픽 몰림 현상의 대응 필요. 유튜브 및 넷플릭스와 같은 대표적 OTT 서비스 업체는 CDN 을 통한 트래픽 몰림에 대응 중 | | |
| 키워드 | Middle Mile, Caching, Global Server Load Balancing, Streaming, Static Caching, Dynamic Caching | | |
| 목차예시 | 1. Middle Mile 최소화를 통한 콘텐츠 전송, CDN 동작원리<br>2. CDN 의 주요 기술 상세 설명<br>3. CDN 의 캐싱 방식 분류<br>4. 해외 주요 CDN 구축 모델 동향 | | |
| 출제자 | 전일 기술사(제 114 회 정보관리기술사 / nikki6@hanmail.net) | 난이도 | ★ ★ ★ ★ ☆ |
| 참고문헌 | https://aonenetworks.tistory.com/212<br>https://ijbgo.tistory.com/32 | | |

## 1. Middle Mile 최소화를 통한 컨텐츠 전송, CDN 동작원리

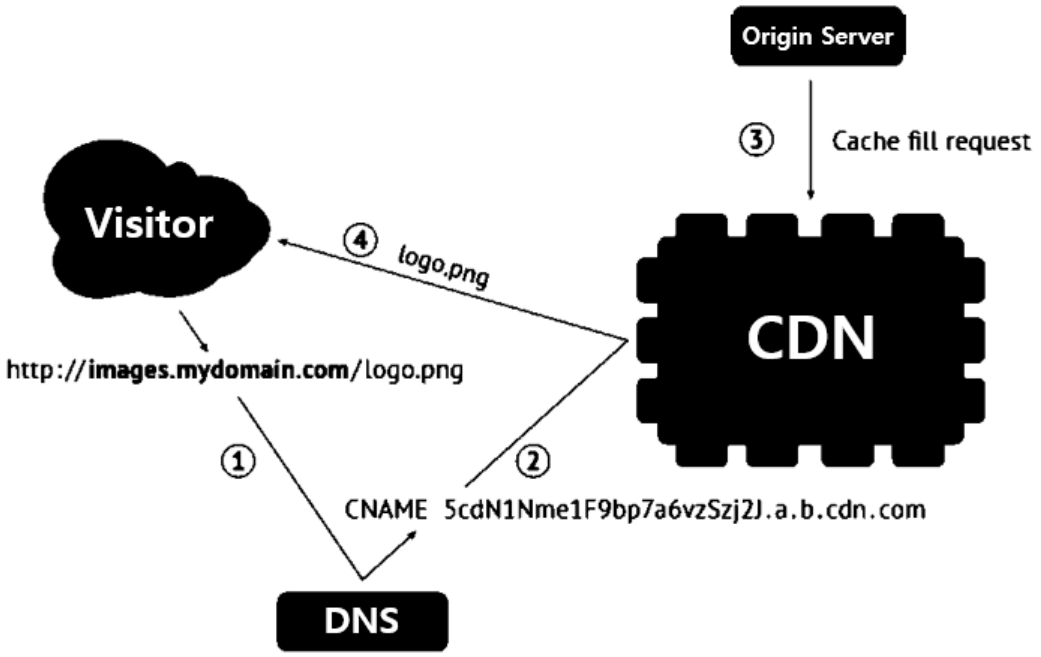
### 가. CDN(Contents Delivery Network) 개념

- 콘텐츠를 효율적으로 전달하기 위해 여러 노드(웹 캐시)를 가진 네트워크에 데이터를 저장하여 제공하는 시스템
- (장점) 네트워크 성능/비용/QoS/응답속도 향상, 다양한 컨텐츠 활용, 가입자 만족도 UP

### 나. CDN 의 동작원리 상세 설명

| 구분 | CDN 동작 원리 설명 |
|---|---|


Copyright ⓒ 2014 By Korea Productivity Center Convergence Knowledge Center. All rights reserved

<table>
<tr><td>동작<br>구성도</td><td colspan="2"> 
</td></tr>
<tr><td rowspan="3">동작<br>절차</td><td>①요청</td><td>웹 브라우저가 실행되는 디바이스인 PC나 모바일 기기의 사용자 에이전트가 특정 주소에 접근하여 HTML, 이미지, CSS, JavaScript 파일 등 렌더링하는데 필요한 콘텐츠를 서버로부터 요청</td></tr>
<tr><td>②확인</td><td>DNS는 콘텐츠에 대한 각 요청이 발생하면 End User와 가장 가까운 위치에 최적으로 배치된 CDN 서버에 End User가 매핑되고, 해당 서버는 요청된 파일의 캐싱된(사전 저장)버전으로 응답</td></tr>
<tr><td>③실패</td><td>서버가 파일을 찾는데 실패하는 경우 CDN 플랫폼의 다른 서버에서 콘텐츠를 찾은 다음 End User에게 응답을 전송<br>콘텐츠를 사용할 수 없거나 콘텐츠가 오래된 경우, CDN은 오리진 서버에 대한 요청</td></tr>
<tr><td></td><td>④리턴</td><td>② 또는 ③ 절차에서 확보된 컨텐츠를 디바이스로 전달</td></tr>
</table>

- 인터넷 망에 분산 배치되어 있는 많은 캐시 서버 중 이용자에게 최상의 서비스를 제공할 수 있는 캐시 서버를 선정하여 연결

## 2. CDN 의 기술 요소

| 기술 요소 | 주요 내용 | 특징/세부 기술 |
|---|---|---|
| Cashing | 자주 찾는 페이지를 컴퓨터에 복사해 저장한 후 사용자가 찾으면 저장된 정보를 전송하는 기술 | Pull & Push의 통합 모델 |
| Global Server Load Balancing | CDN서비스를 제공하기 위해 인터넷 망에 분산 배치되어 있는 많은 캐시 서버 중에 이용자에게 최상의 서비스를 제공할 수 있는 캐시 서버를 선정하여 연결하는 기술 | Cache server 선정 |
| Load Balancing | 서버 별로 트래픽 분산을 통해 웹 고객에 대한 서비스 성능 향상시키는 기술 | Product-based / Service-based |
| Streaming | 대용량의 멀티미디어 데이터를 down받지 않고 즉시 재생함 | Multicasting Streaming<br>On-Demand Streaming |
| 컨텐츠 배포 | CDN서버들이 각 지역에 여러 대가 분산되어 있어 동일 컨텐츠를 | 동기화 기술 |

| | | |
|---|---|---|
| | 정확히 배포해야 정상적인 서비스 제공 | |
| 동기화 | 분산 데이터 관리 및 분산 병렬 처리 기술 요구 | Grid Computing, Virtualization |

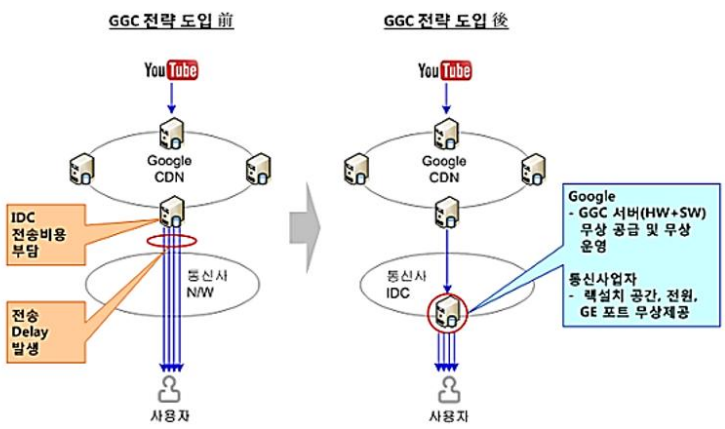
- Caching 기술 중 Pull 방식은 ISP 들의 POP 지점에 Cache 서버를 배치하며, Push 방식은 캐시 서버를 웹 서버 앞에 위치

### 3. CDN 캐싱 방식 분류

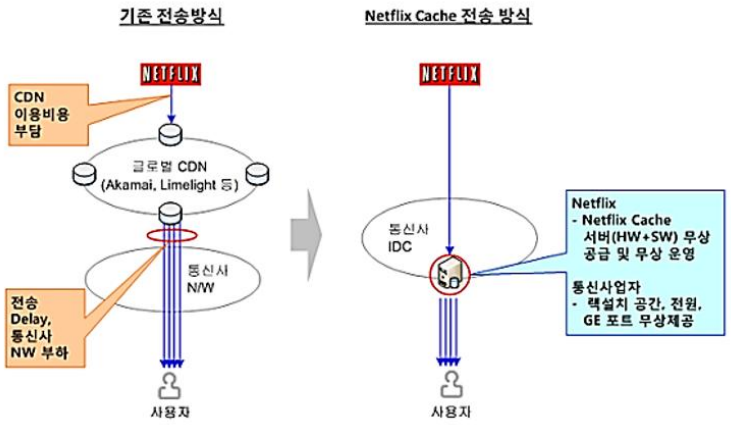
| 분류 | 주요 내용 | 사례 |
|---|---|---|
| Static Caching | - 사용자 요청 없어도 Origin Server에 있는 Content를 운영자가 미리 Cache Server에 복사함<br>- 사용자가 Cache Server에 접속하여 Content를 요청하면 무조건 Content는 Cache Server에 있음(100% Cache Hit) | 대부분의 국내 CDN (Pooq 동영상, 스트리밍/다운로드, NCsoft 게임파일 다운로드 등) |
| Dynamic Caching | - 최초 Cache Server에는 Content 없음<br>- 사용자가 Contents 요청하면 해당 Content 있는지 확인하고, 없으면(Cache Miss) Origin Server로부터 다운로드 받아(Cache Fill) 사용자에게 전달<br>- 이후 동일 Contents 요청 받으면 저장(캐싱)된 Content를 전달 | Akamai, Amazon과 같은 Global CDN 업체, 그리고 Cisco나 ALU 통신사업지향 CDN 장비 솔루션에서 지원 |

- Dynamic Caching 에서 일정시간 지나면(TTL) Cache 삭제될 수 있으며, 그렇지 않으면 Content Freshness 확인 후에 계속 가지고 있을 수 있음

### 4. 해외 주요 CDN 구축 모델 동향

| 구축 모델 | 구성도 | 특징 |
|---|---|---|
| Google (YouTube) |  | 통신사업자 망 내로 무상 Google CDN 확장하여 사용자들의 QoE 개선(Low RTT) |


Copyright ⓒ 2014 By Korea Productivity Center Convergence Knowledge Center. All rights reserved

| | | |
|---|---|---|
| Netflix |  | 통신사업자가 자사의 On-Net Internet Video CDN을 OTT에게 판매하여 신규 수익(B2B) 창출 |

- 이러한 OTT 사업자의 자체 CDN 전략은 통신사업장과 사용자들에게 일정 부분 이득을 주기는 하지만, 반대로 CDN 서비스 사업을 자체적으로 준비 및 제공 중인 On-Net CDN 사업자에 충돌하는 문제점을 내포

| | | | |
|---|---|---|---|
| 문 제 | **4. HTTP 프로토콜을 설명하시오.**<br>**가) HTTP 프로토콜**<br>**나) QUIC 프로토콜**<br>**다) HTTP 프로토콜 3.0 과 2.0 비교** | | |
| 출 제 영 역 | 디지털서비스 | 난 이 도 | ★★☆☆☆ (별 2 개 기준) |
| 출 제 배 경 | 초 연결시대에 빠른 웹 데이터 전송을 위한 HTTP 프로토콜 변화에 대응하기 위한 지식 점검 | | |
| 출 제 빈 도 | 미출제 | | |
| 참 고 자 료 | - 웹페이지 로딩시간 개선을 위한 IETF HTTP 표준화 개발 동향 / 정보통신기획평가원<br>- 실감미디어 전송을 위한 차세대 HTTP 기반 적응적 스트리밍 전송 프로토콜 연구 / 방송공학회 | | |
| Keyword | Request & Response, Connectionless & Stateless, Keep Alive, UDP, Zero-RTT, TCP HOL | | |
| 풀이 기술사님 | 서대웅(122 회 컴퓨터시스템응용기술사 / sdw0530@naver.com) | | |

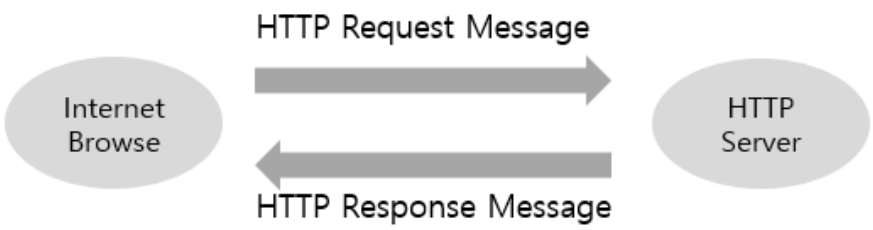
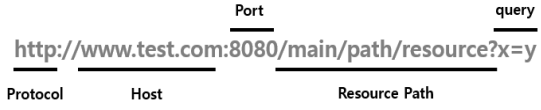
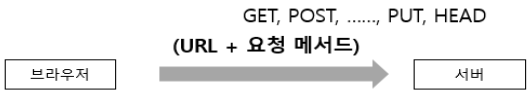
## 1. 웹 데이터 송수신 프로토콜, HTTP(Hypertext Transfer Protocol)

### 가. HTTP(Hypertext Transfer Protocol) 정의

| 개념 | 특징 | |
|---|---|---|
| - 인터넷상에서 웹 서버 및 웹 브라우저 상호 간의 데이터 송수신을 위한 TCP/IP 기반 응용계층 프로토콜 | Request & Response | - 클라이언트/서버 모델로 동작 |
| | Connectionless & Stateless | - 요청에 대한 응답 후 연결해제 |
| | Keep Alive | - TCP 연결 유지 (HTTP 1.1 이상) |
| | HTTPS 지원 | - 송수신 데이터 암호화 |

- 클라이언트(Browser)에서 요청(request)를 보내면 서버는 요청을 처리해서 응답(response)하는 구조

### 나. HTTP(Hypertext Transfer Protocol) 구조 및 구성요소

| | | | |
|---|---|---|---|
| 구조 |  | | |
| 구성 요소 | URL |  | - 전송 프로토콜<br>- Host 및 자원의 위치, query 로 구성 |
| | Method |  | - 클라이언트와 서버 사이에 요청과 응답 데이터 전송 (GET, POST ) 등) |

| | | | |
|---|---|---|---|
| | 상태코드 | 브라우저 ← 서버<br>(상태 코드 + 응답 Body)<br>200, 304, ..., 404, 500 | - HTTP 요청에 대한 응답<br>- 성공, 리다이렉트, 서버, 클라이언트 상태 알림 |

- 클라이언트는 메소드를 통해 요청 메시지를 전송, 서버는 응답 상태 코드를 통해 응답 결과를 전송

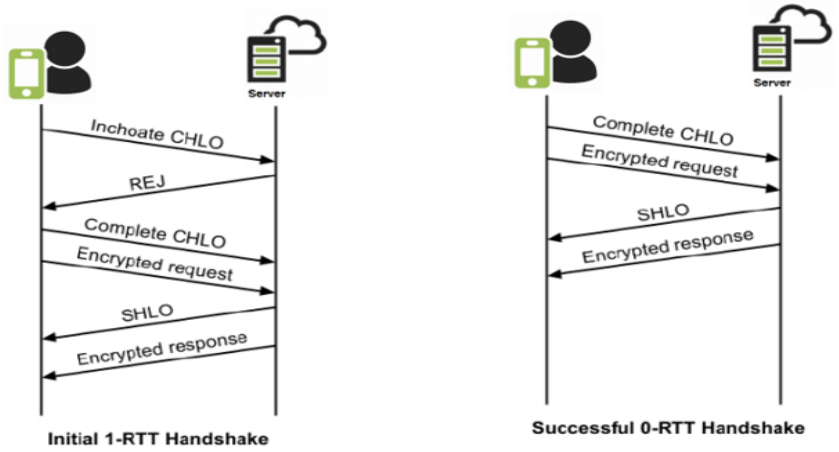
## 2. HTTP 트래픽 가속화를 위한 QUIC(Quick UDP Internet Connection) 프로토콜

### 가. QUIC(Quick UDP Internet Connection) 정의

| | | |
|---|---|---|
| 개념 | - 웹 페이지 대기시간 감소 및 클라이언트와 서버, 기기간 전송 지연 최소화를 위한 UDP 와 TLS 조합의 전송 프로토콜 | |
| 특징 | RTT-Zero | - RTT 최소화, TCP 혼잡회피 문제 최소화 |
| | TCP HOL 블로킹 해결 | - 다중 스트림 제공 및 개별 스트림 내 흐름 제어 기능 제공 |
| | 패킷 변조 방지 | - 헤더의 인증 및 암호화 (AEAD 알고리즘 내장) |

- 클라이언트와 서버 간 연결 및 전송 지연 최소화를 위해 UDP 와 TLS 조합의 프로토콜

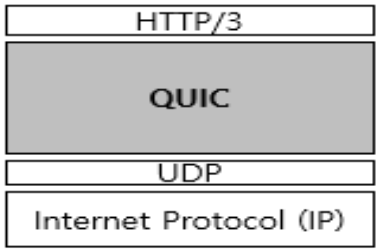
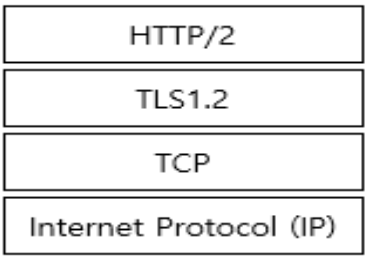
### 나. QUIC(Quick UDP Internet Connection) 연결 매커니즘

| | | | |
|---|---|---|---|
| **개념도** |  | | |
| **절차** | **Initial 1-RTT Handshake** | Client | - Inchoate CHLO(Client Hello) 서버로 전송 |
| | | Server | - Diffie-Hellman 공개키, 서버 인증서, 공인 IP 주소 암호화를 포함한 REJ(Rejection)을 Client 로 전송 |
| | | Client | - Complete CHLO 를 서버 전송 후 Handshake 완료<br>- 암호화된 데이터 패킷 전송 가능 |
| | **Successful 0-RTT Handshake** | Client & Server | - 이전 연결의 캐시된 자격 증명을 사용<br>- 암호화된 요청 서버로 전송 |
| | **Rejected 0-RTT Handshake** | Client & Server | - 클라이언트의 캐싱된 정보가 오래된 경우 다시 1-RTT Handshake 를 재수행 |

- 최초 1 회 수행한 후 재 연결시 캐싱 정보 사용으로 재 Handshake 과정 없이 암호화된 데이터 송수신 수행

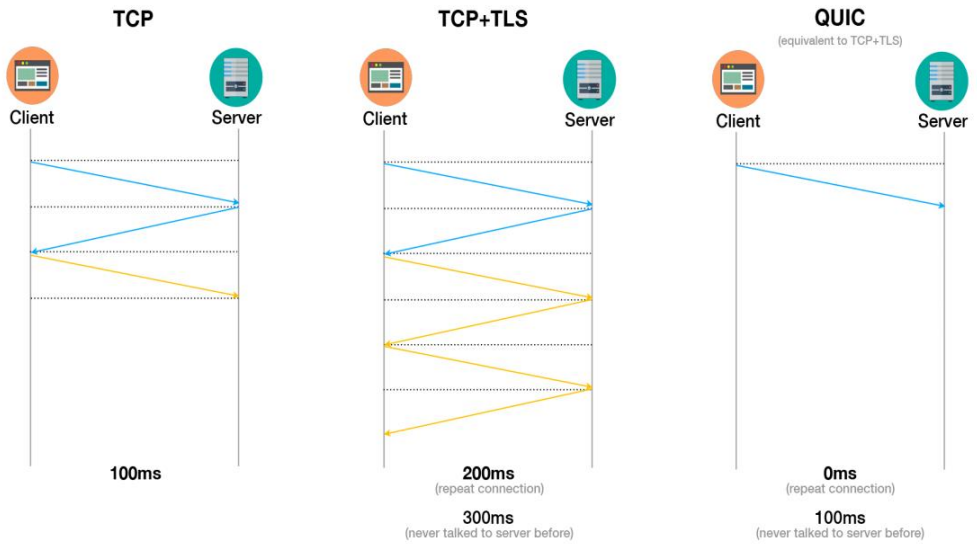
## 3. HTTP 3.0 과 HTTP 2.0 비교

### 가. HTTP 3.0 과 HTTP 2.0 개념 비교

| 구분 | HTTP 3.0 | HTTP 2.0 |
|---|---|---|
| 개념 | - QUIC 프로토콜 기반 웹 페이지 대기시간 감소를 위한 UDP/TLS 조합의 HTTP 프로토콜 | - SPDY 프로토콜 기반 웹 브라우저와 서버간 전송 속도 및 보안을 개선한 HTTP 프로토콜 |
| 구조 |  |  |

- HTTP3.0 은 UDP 기반의 QUIC 프로토콜을 HTTP2.0 은 TCP 기반의 SPDY 프로토콜을 사용함

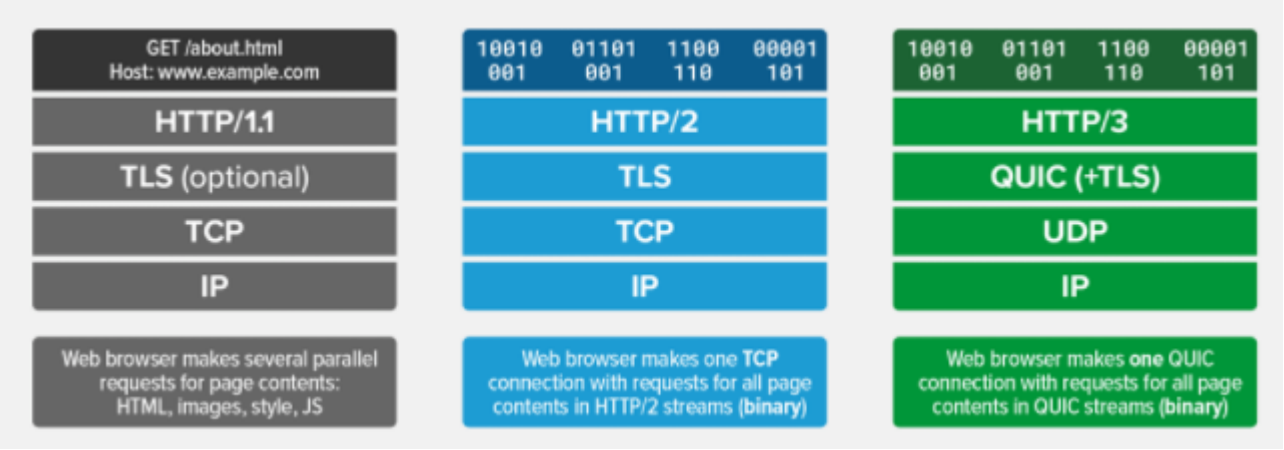
### 나. HTTP 3.0 과 HTTP 2.0 상세 비교

| 구분 | HTTP 3.0 | HTTP 2.0 |
|---|---|---|
| 표준기술 | - UDP 기반의 QUIC 프로토콜 | - TCP/TLS 기반의 SPDY 프로토콜 |
| 주요특징 | - TCP HOL(Head of line) 블로킹 문제 해결<br>- 멀티플렉싱 (요청/응답 동일 TCP 에서 수행)<br>- 인증 및 암호화 (AEAD 알고리즘 내장)<br>- TCP Cubic (혼잡 제어 알고리즘) | - HTTP HOL(Head of line) 블로킹 문제 해결<br>- 바이너리 프레임 (오류 감소, 성능 개선)<br>- 서버 푸쉬 (PUSH-PROMISE)<br>- Stream Priority (일관적인 뷰 렌더링 보장) |
| 연결 설정 |  | |
| 헤더압축 | - 제공 (QPACK 압축방식) | - 제공 (HPACK 압축방식) |
| 속도 | - 상대적으로 빠름 (빠른 Handshake) | - 상대적으로 느림 |
| 암호화 | - TLS 1.2+ 기반 암호화 | - TLS 1.3 기반 암호화 |

- QUIC 기반의 HTTP3.0 은 기존의 TCP+TLS 방식의 HTTP2.0 에 비해 지연시간을 최소화함

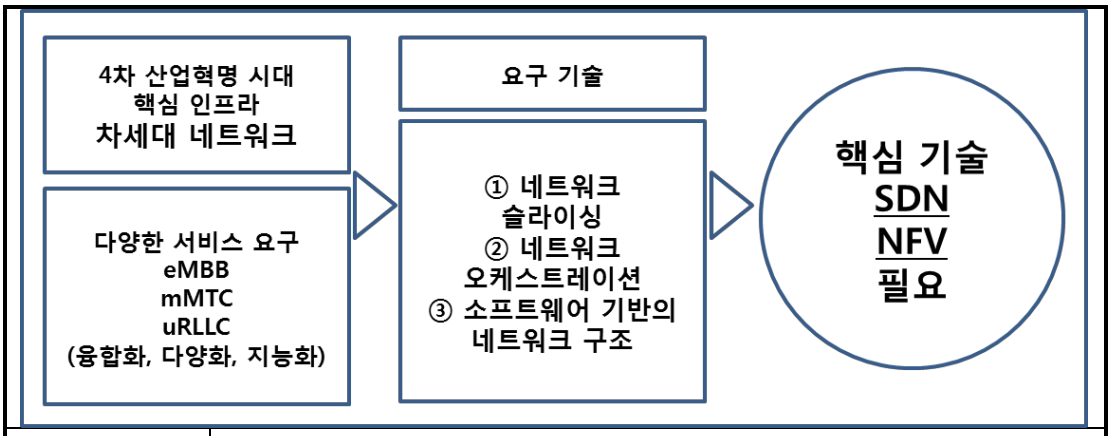
"끝"

[기타자료]


GET /about.html
Host: www.example.com
HTTP/1.1
TLS (optional)
TCP
IP
Web browser makes several parallel requests for page contents: HTML, images, style, JS
10010 01101 1100 00001
001 001 110 101
HTTP/2
TLS
TCP
IP
Web browser makes one TCP connection with requests for all page contents in HTTP/2 streams (binary)
10010 01101 1100 00001
001 001 110 101
HTTP/3
QUIC (+TLS)
UDP
IP
Web browser makes one QUIC connection with requests for all page contents in QUIC streams (binary)

| 2 | SDN, NFV |
|---|---|
| 문제 | 차세대 네트워크 기술로 부각되고 있는 SDN(Software Defined Networking)과 NFV(Network Function Virtualization)의 구조와 특징을 비교 설명하시오 |
| 도메인 | 네트워크 |
| 정의 | - SDN: 소프트웨어적으로 제어할 수 있도록 제어기능을 별도로 분리하여 중앙집중식으로 관리함으로써 데이터 전송만 담당하는 분산 하드웨어를 적시에 제어 가능한 유연한 네트워크 구조를 제공하는 기술<br>- NFV: 네트워크 장비 내의 여러 기능들을 분리시켜 소프트웨어적으로 제어 및 관리가 가능하도록 가상화시키는 기술 |
| 키워드 | - Application Layer, Control Plane, Data Planed, Control protocol(OpenFlow)<br>- VNFs, NFVI, MANO(Management & Orchestration) |
| 출제의도분석 | - 5G 네트워크 핵심 기술 SDN, NFV 의 이해와 차이점 확인<br>- NFV 와 SDN 의 관계와 5G 연계 네트워크 서비스 확인 |
| 답안작성 전략 | - SDN 과 NFV 의 필수 구성요소와 구조 및 특징 비교에 대하여 충분히 제시<br>- SDN 과 NFV 의 상호 보완적 관계와 연계되는 서비스 설명(Hybrid SDN, NFV, 네트워크 슬라이스) |
| 참고문헌 | - 스마트 인터넷을 위한 SDN 및 NFV 표준기술 동향 분석, ETRI<br>- 5G 네트워크 슬라이싱 및 네트워크 관리 기술 표준화 동향<br>- SKT SDDC White paper<br>- 국내 SDN 시장 현황과 개선 과제, 주간기술동향<br>- KPC 모의고사 74 회 관리 3 교시<br>- Insight Report 도메인 분석서 지능신뢰 네트워크, ETRI<br>- 차세대 네트워킹 시대를 견인하는 SDN 과 NFV, SPRI |
| 모범목차 | 1. 4 차 산업혁명 핵심 인프라, 차세대 네트워크 기술 SDN, NFV 의 개요<br>2. SDN, NFV 의 구조 설명<br>가. SDN 의 구조 설명<br>나. NFV 의 구조 설명<br>3. SDN 과 NFV 특징 비교 설명<br>가. 목적/활용 측면의 SDN 과 NFV 특징 비교<br>나. 기술 측면의 SDN 과 NFV 특징 비교<br>4. SDN 과 NFV 를 통한 네트워크 슬라이스 구현 |
| 풀이 기술사님 | 공수재 기술사 (제 111 회 컴퓨터시스템응용기술사 / ksujae22@naver.com) |

## 1. 4 차 산업혁명 핵심 인프라, 차세대 네트워크 기술 SDN, NFV 의 개요

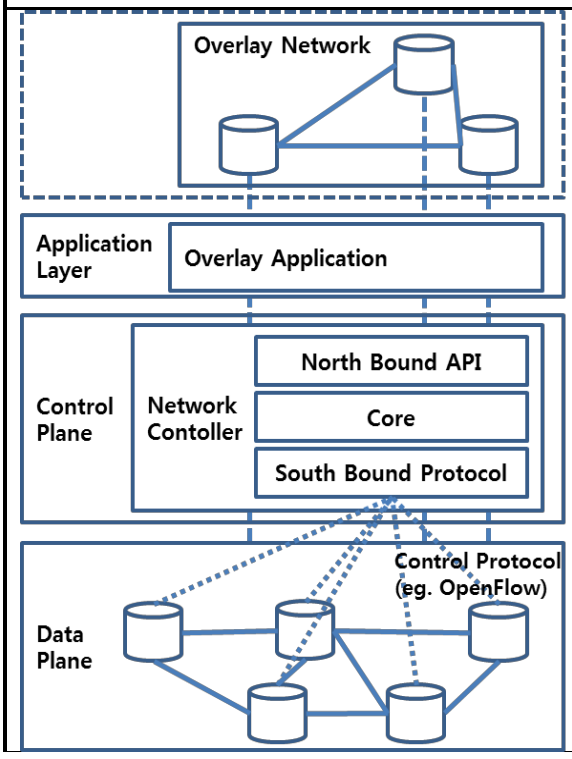



| | |
|---|---|
| SDN | - 소프트웨어적으로 제어할 수 있도록 **제어기능을 별도로 분리**하여 **중앙집중식으로 관리**함으로써 데이터 전송만 담당하는 분산 하드웨어를 적시에 제어 가능한 유연한 네트워크 구조를 제공하는 기술 |
| NFV | - 네트워크 장비 내의 여러 **기능**들을 분리시켜 소프트웨어적으로 제어 및 관리가 가능하도록 **가상화**시키는 기술 |

-SDN/NFV 시장은 **①네트워크 복잡도 증가, ②확장 가능성 및 유연성에 대한 요구 증가, ③인프라 획득 및 유지비용 증가, ④장비시장 폐쇄성에 대응**하기 위해 지속적인 수요 증가

## 2. SDN, NFV 의 구조 설명

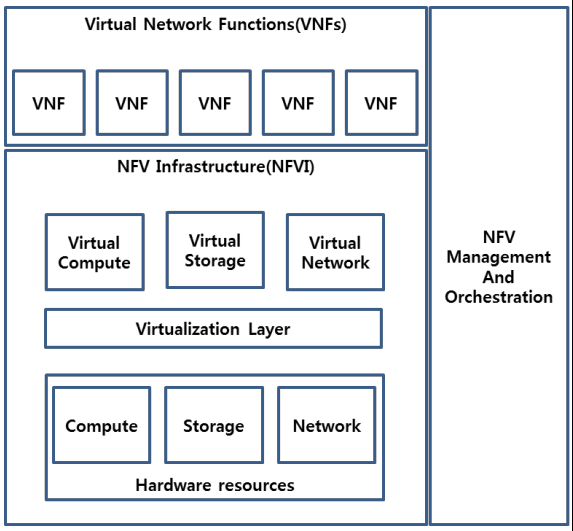
**가.** SDN 의 구조 설명

| 구조도 | 구조 | 설명 |
|---|---|---|
|  | Application Layer | - Overlay network: 서비스별 가상 네트워크 중앙컨트롤러 api 사용 |
| | Control Plane | - Openflow를 통한 네트워크 장비 제어<br>- Forwarding, Drop, Shaping, Reactive Processing |
| | Data Plane | - Merchant Silicon: 스위치에 탑재되어 패킷전송 수행하는 칩셋<br>- Bare Metal Switch: 저가 White box의 오픈소스 스위치 |



-. 기존 vendor 가 하드웨어와 소프트웨어를 vertical 하게 제공하는 방식에서 벗어나, 사용자가 표준 API 나 개방형 인터페이스를 통해 새로운 기능을 추가하여 사용자 정의 네트워크로 전환

**나.** NFV 의 구조 설명

| 구조도 | 구조 | 설명 |
|---|---|---|
|  | VNFs | - 여러 응용 프로그램을 지원하기 위한 소프트웨어로 개발된 네트워크 기능들의 집합 |
| | NFVI | - 컴퓨팅, 저장소, 네트워크 기능을 지원하는 물리적 하드웨어 자원, 가상화 지원 기능 및 VNF 실행을 지원하는 기능 제공 |
| | Management & Orchestration | - 물리적 그리고 소프트웨어적 자원 관리, 전달, VNF 관리 기능 제공 |

- 엔터프라이즈 액세스 라우터, Firewall, DPI, CDN, 로드밸런싱 등의 VNF 기능 제공

## 3. SDN 과 NFV 특징 비교 설명

### 가. 목적/활용 측면의 SDN 과 NFV 특징 비교

| 구분 | SDN | NFV |
|---|---|---|
| 주안점 | - NW 의 제어와 데이터 영역 분리<br>- 제어영역의 중앙 집중화 관리 | - 전용 Appliance 기능들을 가상화하여 일반적인 서버에 재배치 |
| 동기 | - 네트워크 프로그래밍을 통한 중앙화된 관리로써 유연성 확보 | - 특정장비에 귀속된 네트워크 기능을 일반 서버에 재배치(vendor lock-in 탈피) |
| 적용 위치 | - 기업 본사/지사, 캠퍼스, Data center | - Service Provider Network |
| 효과 | - NW 기반 비즈니스 확대<br>(데이터 센터의 SDDC 진화,<br>실시간 Provisioning 이 가능한 Private Cloud, 수요자 맞춤형 Intelligent Bandwidth 서비스)<br>- NW 투자/운영 비용 절감<br>(저가 하드웨어 NW 구축,<br>중앙 집중식의 NW 자동 관리,<br>NW 구성요소 SW 통한 가상화) | - 경제성, 유연성/신속성<br>(저렴한 표준 장비 활용,<br>제조사에 대한 의존성 완화,<br>중소 소프트웨어 개발사 참여 확대)<br>- 개방성<br>(장비 제조사 중심이 아닌 사용자 중심의 장비 시장 구조 혁신) |

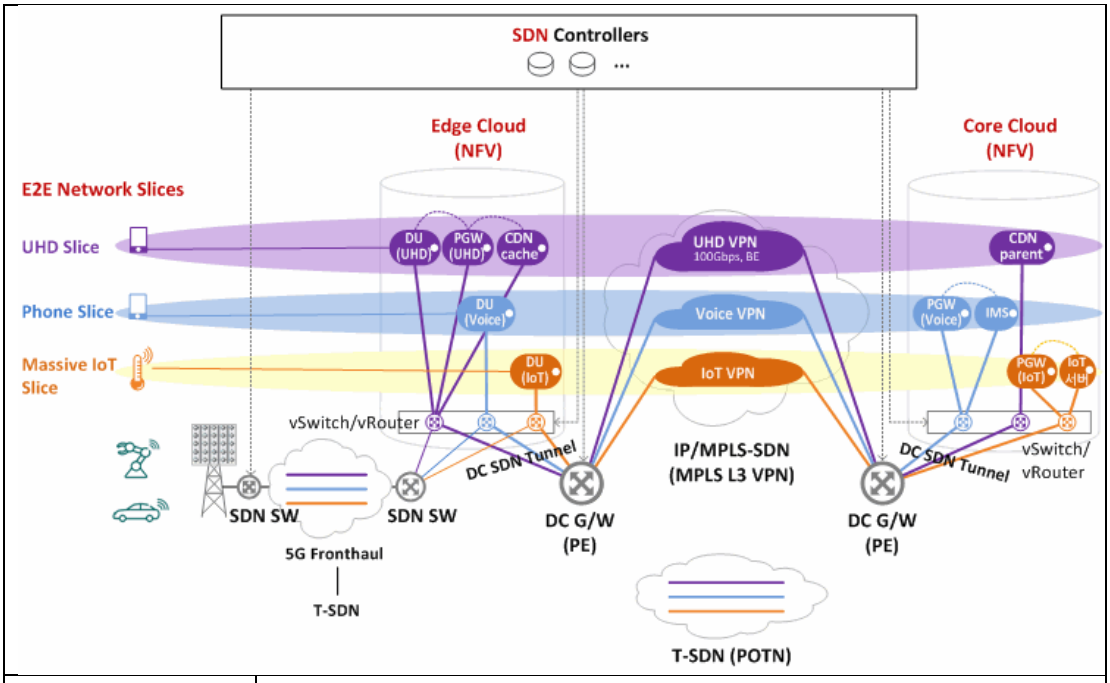
- SDN/NFV 이용은 NW 의 복잡성 증가, 유연한 NW 에 대한 요구 증대, 관리의 편의성, 일반 상용기기(commodity) 활용에 따른 투자비 절감 효과

### 나. 기술 측면의 SDN 과 NFV 특징 비교

| 구분 | SDN | NFV |
|---|---|---|
| 응용 분야 | - Cloud Orchestration<br>- Networking | - 라우터, 방화벽, 게이트웨이, CDN, WAN 가속기, SLA assurance 등 |
| 디바이스 | - 상용서버, 스위치 | - 상용서버, 스위치 |
| 플랫폼 | - OpenDaylight (스위치벤더 중심)<br>- ONOS (통신사업자 요구 반영) | - OPNFV<br>(공개 플랫폼에 기반한 Open API 제공) |
| 프로토콜 | - Openflow<br>- OVSDB<br>- NETCONF | - 아직 제정 안됨 |
| 표준화 기구 | - Open Networking Forum(ONF)<br>- OpenDaylight | - ETSI NFV Working |

- SDN 과 NFV 는 개방성에 기반한 상호 보완적관계로서 두 솔루션이 결합 되었을 때 시너지 발생

## 4. SDN 과 NFV 를 통한 네트워크 슬라이스 구현




| | |
|---|---|
| NFV 의 역할 | 네트워크 장비가 아닌 가상화된 상용 서버(COTS)에 Network Function S/W (Packet Core 의 MME, S/P-GW, PCRF, RAN 의 DU)을 VM 에 탑재 |
| SDN 의 역할 | 에지 클라우드와 코어 클라우드에 있는 VM 들간의 네트워크 연결은 SDN 으로 설정 |

- 서비스별로 슬라이스(Phone 슬라이스, Massive IoT 슬라이스, Mission-critical IoT 슬라이스)를 생성

"끝"

| 문 제 | 10. Wi-Fi 7 | | |
|---|---|---|---|
| 출 제 영 역 | 네트워크 | 난 이 도 | ★★☆☆☆ (별 5 개 기준) |
| 출 제 배 경 | Wi-Fi 8 도입 전 Wi-Fi 7 의 스펙과 기술에 대한 이해 확인 | | |
| 출 제 빈 도 | 134 회 컴시응 1 교시, 135 회 정보관리 1 교시 (Wi-Fi 8) | | |
| 참 고 자 료 | - https://www.intel.co.kr/content/www/kr/ko/products/docs/wireless/wi-fi-7.html<br>- IEEE 802.11be Draft (P802.11be/D7.0) | | |
| Keyword | 3 대역 운영, IEEE 802.11be, EHT, 4096-QAM, 320MHz, 30Gbps, 혼합 빔포밍, MAC, PHY, MLO | | |
| 풀이 기술사님 | 이영학 PPE (138 회 정보관리기술사 / dudgkr159@naver.com) | | |

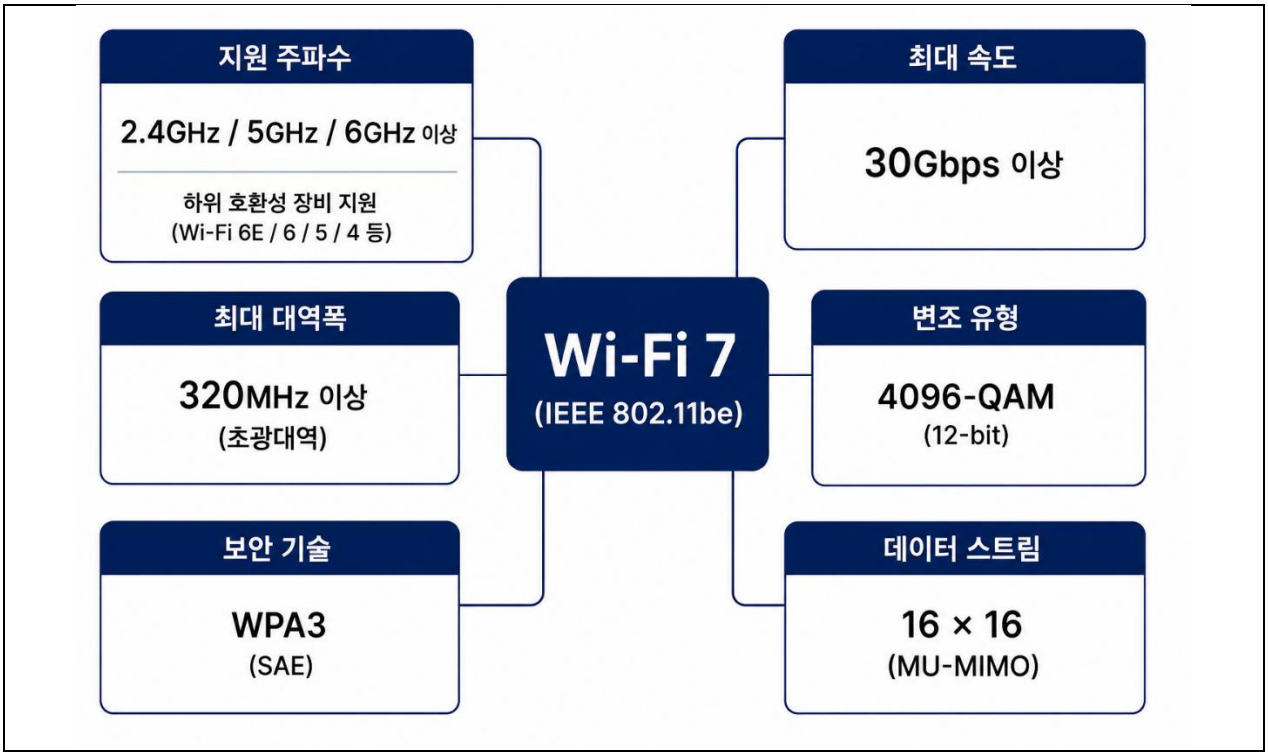
## 1. "IEEE 802.11be", Wi-Fi 7 정의와 특징 설명

| | | |
|---|---|---|
| 정의 | 초고속, 초저지연 무선 통신을 제공하기 위해 320MHz 및 4096 QAM 등을 지원하는 차세대 무선 LAN 기술 | |
| 특징 | - 고밀도 환경 최적화 | - 넓은 대역폭을 통한 대용량 데이터 전송 |
| | - 멀티 링크 작동 | - 처리량, 안정성, 지연 시간 단축, 동시에 송수신 |
| | - 3대역 운영 | - 2.4GHz, 5GHz, 6GHz 주파수 대역의 작동을 정의 |

- Wi-Fi 7 은 기존 Wi-Fi 6 를 넘어 **"EHT(Extremely High Throughput)"**를 제공하기 위해 설계된 차세대 무선 통신

## 2. Wi-Fi 7 의 기술 스펙 및 기술요소

### 가. Wi-Fi 7 의 기술 스펙 구성도 설명




- Wi-Fi 7 은 **2024 년에 상용화**되어 2025 년 하반기에 **점차 민간 및 공공 환경에 적용** 진행 중



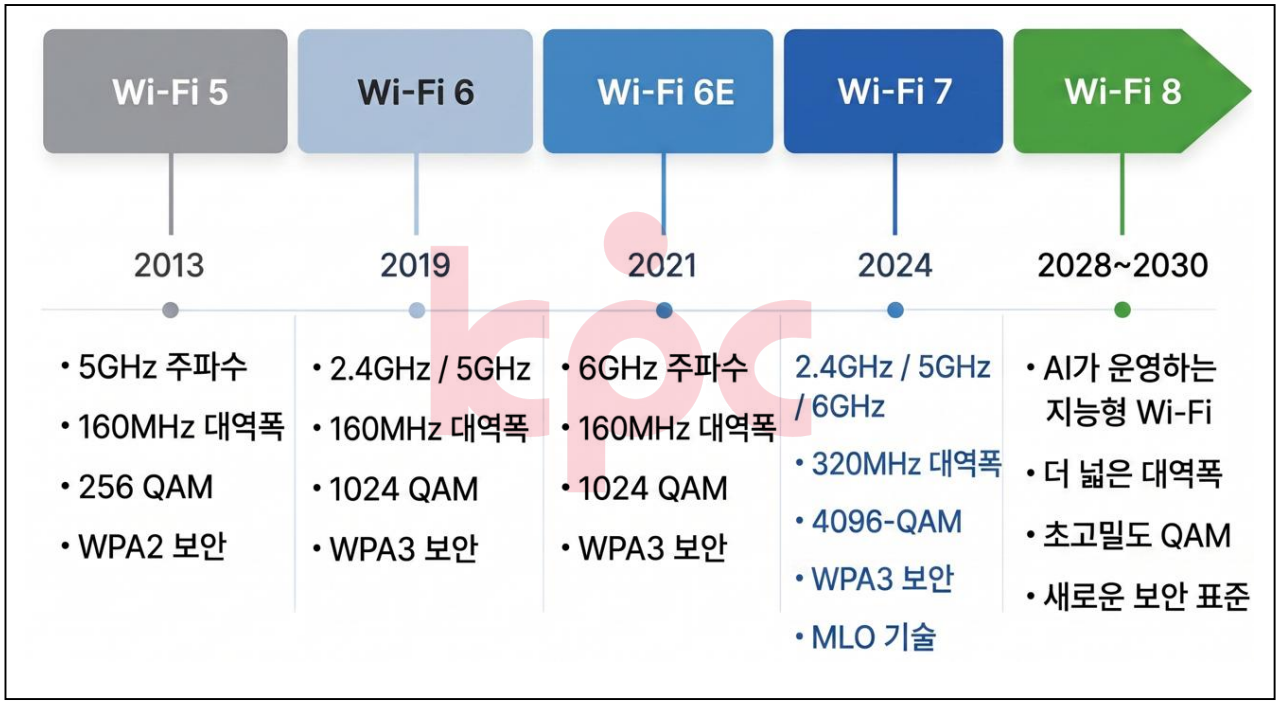
Copyright ⓒ 2026 By Korea Productivity Center ICT Education Center. All righ 1 ts reserved

나. Wi-Fi 7 의 기술요소 설명

| 구분 | 기술요소 | 설명 |
|---|---|---|
| MAC (Media Access Control) | - MLO (Multi-Link Operation) | - 여러 대역폭을 하나의 논리적 링크로 묶음 |
| | - Multi-AP Coordination | - 주변 AP 협력하여 전체 NW 처리량 최적화 |
| | - H-ARQ (ARQ + FEC), QoS | - MLO 연동, TSN 도입, 데이터 전송 신뢰성 확보 |
| PHY (Physical Layer) | - 16x16 MU-MIMO | - 동시 접속 용량 및 처리 속도 극대화 |
| | - 4K-QAM (4096-QAM) | - 변조 밀도를 높여 단위 시간당 데이터 전송 개선 |
| | - 전이중 멀티플렉싱 | - 주파수 자원 공유를 통해 전송 효율 극대화 |
| | - 혼합 빔포밍 | - 안테나 효율 위한 대역폭 분할 프리코딩 수행 |
| | - 320MHz 채널 대역폭 | - 전송 대역폭을 확장하여 데이터 전송 속도 향상 |

- 최근 Wi-Fi 7 을 기반으로 안정적 및 효율성 있게 고도화하기 위한 Wi-Fi 8 개발 진행 중

3. Wi-Fi 발전 동향 설명




- **Wi-Fi 8(802.11bn)** 은 2028 년 상용화를 목표로 **초고신뢰성(UHR)**을 기반 무선 LAN 기술

"끝"

**기출풀이 의견**

- Wi-Fi 7의 표준 언급과 상세 스펙, 기술 요소를 작성해 주시고, 추가로 발전 흐름과 Wi-Fi 8로 이어지는 동향을 언급해 주신다면 좋은 점수가 예상됩니다.



Copyright ⓒ 2026 By Korea Productivity Center ICT Education Center. All righ 1 ts reserved