**정보보안기사**

**5장 네트워크 보안**

**19절 네트워크 개요(최종수정일 7/27)**

**프로토콜:** 신뢰/효율/안전하게 정보를 주고받기 위해 정보의 송/수신자측 또는 네트워크 내에서 사전에 약속된 규약 또는 규범. 송신자가 수신자를 호출해 연결하는 과정, 통신회선에서의 접속방식, 전달하는 정보의 형태, 오류 제어, 송/수신자측 간의 동기방식 등에 대한 약속.

**프로토콜의 구성 요소: 구문(Syntax) – 데이터의 구조와 형식 표현순서, 의미(Semantics) – 비트의 영역별 의미, 타이밍(Timing) – 데이터를 언제 얼마나 빨리 전송할 것인지**

**물리적/논리적 프로토콜:** 물리적 프로토콜은 데이터 전송에 사용되는 전송 매체, 접속용 커넥터 및 전송 신호등 물리적 요소에 관한 규약.(RS-232C, V.21) 논리적 프로토콜은 데이터 표현 형식 단위인 프레임의 구성, 프레임 내의 각 항목의 의미와 기능, 데이터 전송 절차 등을 말한다. SNA, SDLC 등 IBM에서 만든 전용 프로토콜(동일 회사 제품끼리 이용)과 TCP/IP 등의 범용 프로토콜로 나뉜다.

**OSI 모델과 TCP/IP 프로토콜**

**OSI 모델:** ISO 표준은 **개방 시스템 상호연결**(OSI, Open System Interconnection) 모델이다. 기반 구조에 관계없이 모든 정보 처리 시스템의 통신을 가능하게 하는 프로토콜의 집합. OSI 모델은 하드웨어나 소프트웨어 기반에 관계없이 다른 시스템 간의 통신을 원활하게 하는데 목적을 둔다.

**물/데/네: 물리, 데이터 링크, 네트워크 계층 -> 물리적인 면(전기 규격, 물리적 연결, 물리 주소, 전송시간과 신뢰도 등) 처리**

**전송 계층: 위 아래 두 그룹을 연결하고 하위 계층(물/데/네)에서 전송한 내용을 상위 계층이 사용할 수 있는 형태가 되도록 보장**

**세/표/응: 세션, 표현, 응용 계층 -> 사용자 지원 계층(관련이 없는 소프트웨어 시스템 간의 상호 연동을 가능하게 함)**

|  |  |  |  |
| --- | --- | --- | --- |
| **계층** | **특징** | **데이터 종류** | **예** |
| **응용** | 각종 응용프로그램  네트워크 관리 | 메시지 | FTP, TFTP, SNMP, SMTP,  Telnet, HTTP, DNS, DHCP |
| **표현** | 네트워크 보안(암,복호화)  압축/압축해제, 포맷 변환 수행 | ASCII, Mpeg, jpg, MME |
| **세션** | 소켓 프로그램  동기화  세션 연결/관리/종료 | 전송모드 결정(반이중, 전이중), SQL, RPC |
| **전송** | 데이터 전송보장  흐름 제어  Quality Of Service(QOS) | 세그먼트 | TCP, UDP, SCTP |
| **네트워크** | 통신경로 설정, 중계기능 담당  라우팅  IPv4 & IPv6 | 패킷 | IP, ICMP, IGMP, ARP, RARP, NAT, RIP, BGP |
| **데이터 링크** | 오류제어, Frame화  매체제어(MAC)  에러검출, 에러정정, 흐름제어 | 프레임 | 이더넷, 토큰링, PPP, SLIP, 802.11(WLAN) |
| **물리** | 물리적 연결설정, 해제  전송방식, 전송매체 | 비트 스트림 | 기계적 전기적, 절차적 규칙 |

**TCP/IP 프로토콜 그룹**

현재 인터넷에서 사용하는 프로토콜 그룹. 상호작용하는 모듈로 이루어진 계층적 프로토콜이다. 각 모듈은 특정 기능을 제공한다. 4 or 5 계층 모델로 간주된다. 두 모델 모두 적용 가능하다.

응용, 표현, 세션 -> 애플리케이션, 전/네/데/물 로 나뉜다.

|  |  |
| --- | --- |
| 계층 | 설명 |
| 데이터링크 | 전송 매체에 프레임을 송수신하는 역할 |
| 네트워크 | IP -> 호스트 네트워크 주소를 관리, 패킷을 라우팅  ARP -> 네트워크 호스트들의 하드웨어 주소를 얻는데 사용  ICMP -> 패킷 전송에 관한 오류 처리를 담당 |
| 전송 | 종단간 통신 서비스 제공을 담당한다. TCP/UDP가 있다. TCP는 데이터의 확실한 전송이 필요한 경우 사용, UDP는 데이터의 정확한 전달 보장 x |
| 응용 | 응용프로그램이 네트워크에 접근 가능하도록 인터페이스 기능 수행 |

**통신단위**

물리 – 비트, 네트워크 – 패킷, 전송 – 세그먼트 || 데이터그램 || 패킷, 응용 – 메시지

**캡슐화와 역캡슐화**

발신지 – 캡슐화, 수신지 – 역캡슐화, 데이터 링크 – 캡슐화/역캡슐화 이뤄지지 않음

**주소 지정**

TCP/IP 프로토콜을 이용한 인터넷은 3개의 다른 주소를 이용한다. -> 물리(MAC), 논리(IP), 포트 주소

**논리 주소:** 물리 주소는 홉에서 홉으로 갈 때마다 변경되지만 논리 주소는 변경되지 않는다. 물리 네트워크와 독립적으로 전세계적인 통신 서비스를 위해 필요. 현재 인터넷에 연결된 호스트를 유일하게 식별할 수 있는 32비트 주소 체계를 사용한다. 인터넷상의 두 호스트는 동일한 IP 주소를 사용할 수 없다.

**포트 주소:** 인터넷의 최종 목적은 한 프로세스가 다른 프로세스와 통신할 수 있도록 하는 것이다. A가 TELNET을 이용해 C와 통신하는 동시에 FTP를 이용해 B와 통신하려면 서로 다른 프로세스를 식별하기 위한 포트가 필요하다.

**다중화와 역다중화:** TCP/IP는 몇몇 계층에서 여러 프로토콜을 사용하기 때문에 발신자측은 다중화, 수신자측은 역다중화한다.

20절. TCP/IP