TCP/IP 교과서

14장 클래식 도구

14.1 연결 문제

TCP/IP 교과서

» 주로 발생하는 네트워크 연결 문제는 일반적으로 다음 네 가지 형태

- **프로토콜 장애 또는 잘못된 구성:** 프로토콜 소프트웨어가 작동하지 않거나 네트워크에서 올바르게 작동하도록 구성되지 않았음
- **회선 문제:** 케이블이 연결되지 않았거나 작동하지 않음. 허브, 라우터, 스위치가 작동하지 않음
- **잘못된 이름 확인:** DNS 혹은 NetBIOS 이름이 확인되지 않음. IP 주소로 리소스에 접근할 수 있지만, 호스트 이름 혹은 DNS 이름(www.microsoft.com)으로는 접근할 수 없음
- **과도한 트래픽:** 네트워크가 작동하는 것처럼 보이지만, 느리게 작동

14.2 프로토콜 장애와 잘못된 구성

» TCP/IP가 작동하고 올바르게 구성되었는지 확인할 수 있는 유용한 유틸리티들

- **ping:** 이 유틸리티는 간단한 네트워크 연결 테스트를 진행해 다른 컴퓨터 혹은 네트워크 장치가 반응하는지 알려주는 굉장히 유용한 진단 도구
- **구성 정보 유틸리티:** 각 OS 공급 업체는 TCP/IP 구성 정보를 표시하고 IP 주소, 서브넷 마스크, DNS 서버 및 다른 매개변수가 올바르게 구성되었는지 확인할 수 있는 유틸리티를 제공
- **arp:** 이 유틸리티로 IP 주소를 물리 주소로 연결하는 ARP 캐시의 콘텐츠를 확인하고 구성할 수 있음

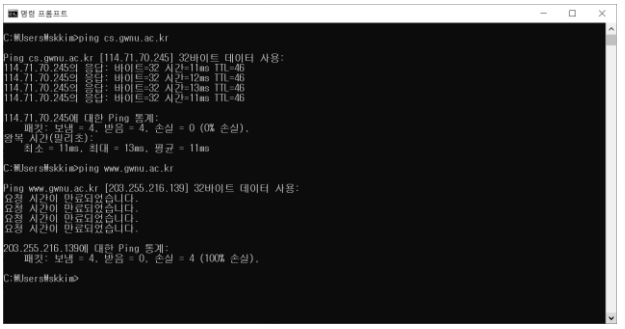
14.2 프로토콜 장애와 잘못된 구성

» ping

- ping 명령의 기본적인 형태는 다음과 같음

  `ping` *IP_address*

- IP_address 는 연결하고자 하는 컴퓨터의 주소
- ping 유틸리티는 인터넷 제어 메시지 프로토콜(ICMP) Echo Request 명령을 사용해 수신 컴퓨터에 메시지를 전송
- 수신 컴퓨터가 존재하고 작동 중이면 ICMP Echo Reply 메시지를 사용해 응답



14.2 프로토콜 장애와 잘못된 구성

TCP/IP 교과서

ping

- 일반적인 문제 해결 시나리오에서는 네트워크 관리자가 다음 ping 명령을 수행

1. 루프백 주소(127.0.0.1)로 핑을 보내서 TCP/IP가 로컬 컴퓨터에서 올바르게 작동하는지 확인
2. 로컬 IP 주소로 핑을 보내서 네트워크 어댑터가 작동하고 로컬 IP 주소가 구성되어 있는지 확인
3. 기본 게이트웨이를 핑해서 컴퓨터가 로컬 서브넷과 통신하는지 확인하고 기본 게이트웨이가 온라인 상태인지 확인
4. 기본 게이트웨이 이외의 주소로 핑을 보내서 게이트웨이가 성공적으로 로컬 네트워크 세그먼트를 넘어서 패킷을 전달하는지 확인
5. 호스트 이름으로 로컬 호스트와 원격 호스트에 핑을 보내서 이름 확인이 작동하는지 확인

14.2 프로토콜 장애와 잘못된 구성

TCP/IP 교과서

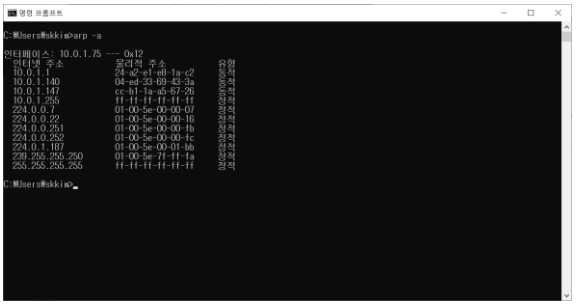
구성 정보 유틸리티

- 운영 체제 대부분은 현재 TCP/IP 구성을 볼 수 있는 유틸리티를 제공
- 이러한 유틸리티는 로컬 컴퓨터의 IP 주소, 서브넷 마스크 및 기본 게이트웨이 등의 정보를 출력
- 유닉스와 리눅스 시스템은 ifconfig, 윈도는 ipconfig 명령어 사용

14.2 프로토콜 장애와 잘못된 구성

TCP/IP 교과서

- arp
  - 주소 확인 프로토콜(ARP)은 IP 주소와 상응하는 물리 주소를 확인하기 위해 사용되는 프로토콜
  - 각 호스트는 IP 주소를 물리 주소로 연관시키는 데 사용되는 테이블인 ARP 캐시를 유지
  - arp 명령은 로컬 컴퓨터 또는 다른 컴퓨터의 ARP 캐시의 현재 콘텐츠를 볼 수 있도록 함



14.3 회선 문제

TCP/IP 교과서

- ping과 같은 TCP/IP 진단 유틸리티로 회선 문제를 진단할 수 있음
- 일반적으로 네트워크가 잘 되다가 갑자기 멈춰버렸다면 보통 회선 문제가 원인
- 모든 네트워크 케이블이 올바르게 꽂혀 있는지 확인
- 네트워크 카드, 허브, 스위치 및 라우터 대부분은 해당 장치가 켜져 있고 데이터를 받을 준비가 되었는지 알려 주는 표시등이 있음
- 각 허브, 라우터 혹은 스위치의 포트는 활성 네트워크 연결이 해당 포트를 통해 작동 중인지 보여 주는 링크 상태 등도 가지고 있음

14.4 이름 확인 문제

TCP/IP 교과서

DNS 서버 문제

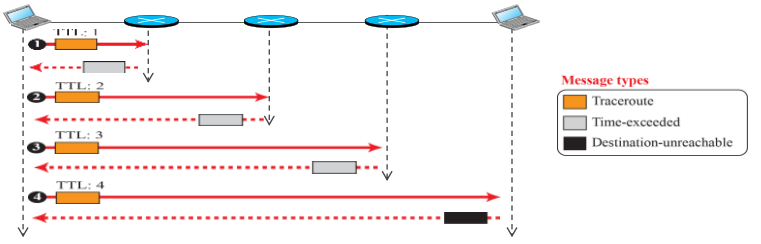
- 이름 확인 문제는 메시지 주소가 지정된 호스트 이름이 네트워크에서 확인되지 않을 때 발생
- 이름 확인 문제는 송신 컴퓨터가 대상에 연결할 수 없음을 의미하지 않기 때문에 (틀림없이) 연결 문제는 아님
- 일반적으로 이름 확인 문제의 증상은 송신 컴퓨터가 IP 주소로는 대상에 도달할 수 있지만 대상 호스트 이름으로는 도달할 수 없음

14.5 네트워크 성능 문제

TCP/IP 교과서

traceroute(tracert)

- traceroute 유틸리티는 데이터그램이 여러 게이트웨이를 통해 목적지 호스트로 이동하면서 통과하는 경로를 추적할 때 사용
- 데이터그램이 항상 해당 경로를 따라간다는 어떠한 보장이나 가정도 할 수 없음
- ICMP 프로토콜을 사용



$ *traceroute* printers.com

***traceroute* to printers.com (13.1.69.93), 30 hops max, 38-byte packets**

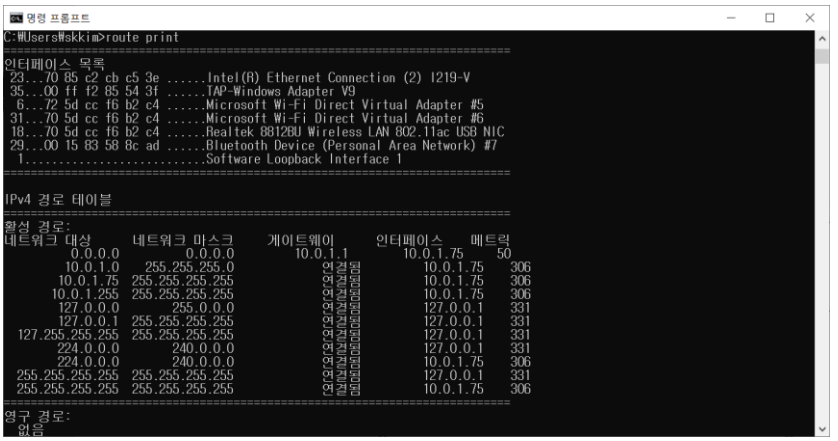
1 route.front.edu	(153.18.31.254)	0.622 ms	0.891 ms	0.875 ms
2 ceneric.net	(137.164.32.140)	3.069 ms	2.875 ms	2.930 ms
3 satire.net	(132.16.132.20)	3.071 ms	2.876 ms	2.929 ms
4 alpha.printers.com	(13.1.69.93)	5.922 ms	5.048 ms	4.922 ms

14.5 네트워크 성능 문제

TCP/IP 교과서

route

- route 명령어는 라우팅 테이블을 출력하기 위해 사용

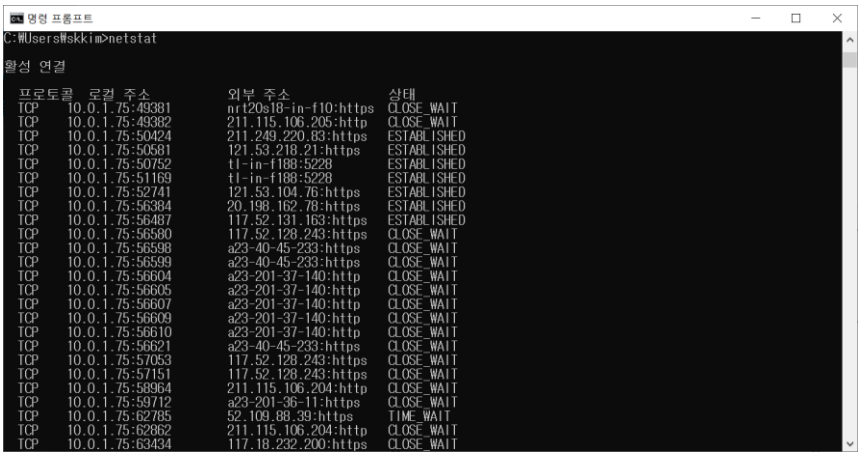


14.5 네트워크 성능 문제

TCP/IP 교과서

Netstat

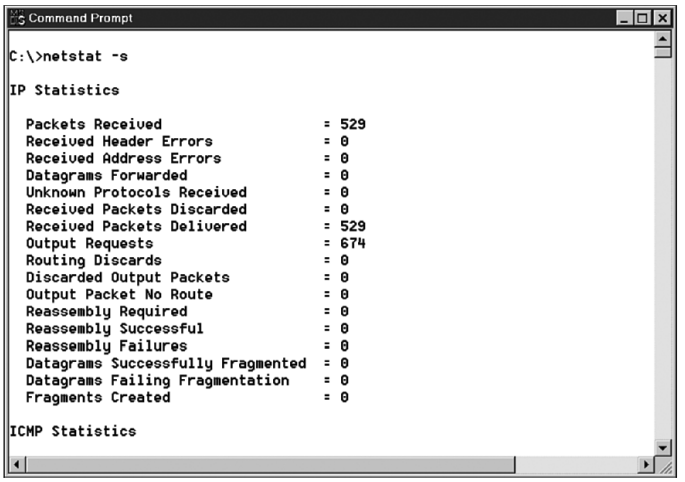
- IP, TCP, UDP 및 ICMP 프로토콜과 관련된 통계 및 네트워크 연결 상태를 표시



14.5 네트워크 성능 문제

» netstat

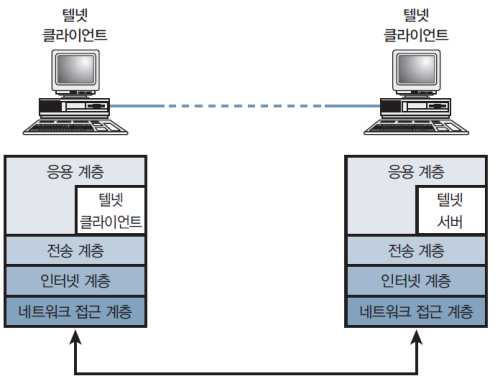
- IP, TCP, UDP 및 ICMP 프로토콜과 관련된 통계 및 네트워크 연결 상태를 표시



14.6 텔넷

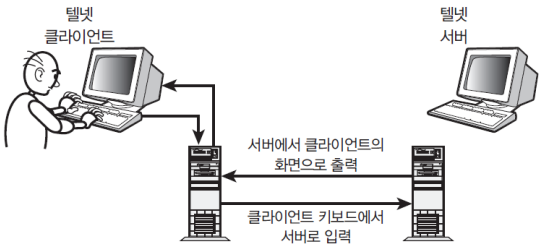
» 원격 로그인 서비스를 제공하는 범용의 클라이언트/서버 응용 프로그램

- TErminaL NETwork의 약자
- 가상 터미널 서비스를 위한 표준 응용 프로토콜



14.6 텔넷

- 텔넷은 텔넷 서버와 텔넷 클라이언트 간의 상호 작용을 정의하는 규칙 시스템인 프로토콜
- 원격 사용자가 입력한 키보드 명령어가 네트워크를 거쳐 다른 컴퓨터의 입력이 되는 수단을 제공
- 세션과 관련된 화면 출력은 다른 컴퓨터(서버)에서 클라이언트 시스템으로 네트워크를 통과
- 그 결과로 원격 사용자는 로컬에 로그인한 것처럼 서버와 상호 작용할 수 있음
- 이질적 클라이언트와 서버 시스템 간 사용 가능



14.6 텔넷

» 유닉스에서 telnet 명령어는 다음과 같이 명령 프롬프트에서 입력

```
telnet hostname
```

» hostname 은 연결하고자 하는 컴퓨터의 이름(호스트 이름 대신 IP 주소를 입력해도 됨)

» 이 명령은 텔넷 애플리케이션을 실행하며, 텔넷이 실행되면 입력한 명령어는 원격 컴퓨터에서 실행

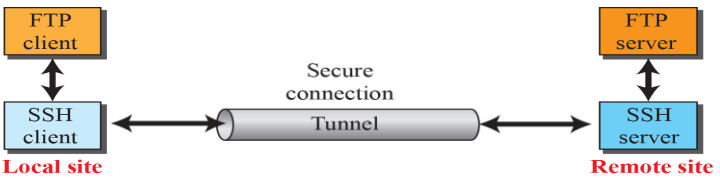
» 보안성이 부족하여 SSH(Secure Shell)을 대체하여 사용해야 함

14.7 버클리 원격 유틸리티

- 원격 접근 제공을 위해 설계된 명령줄 유틸리티 집합
- 이 유틸리티 집합은 각 유틸리티의 이름이 원격(remote)을 뜻하는 r로 시작하기 때문에 버클리 r* 유틸리티로 불림
- 많은 r* 유틸리티가 SSH 프로토콜 스위트에서 새롭고 더 안전한 형태로 거듭 났음
  - **rlogin:** 사용자가 원격으로 로그인할 수 있게 허용
  - **rcp:** 원격 파일 전송을 지원
  - **rsh:** rshd 데몬을 통해 원격 명령을 실행
  - **rexec:** rexecd 데몬을 통해 원격 명령을 실행
  - **ruptime:** 실행 시간 및 연결된 사용자 수 같은 시스템 정보를 표시
  - **rwho:** 현재 연결된 사용자의 정보를 표시

14.8 보안 셸

- Telnet을 대체하기 위해서 설계된 보안성 있는 범용의 응용 프로토콜 (SSH-2)
  - **ssh:** rlogin, rsh 및 telnet을 대체하는 원격 셸 프로그램
  - **scp:** Rcp를 대체하는 파일 전송 유틸리티
  - **sftp:** FTP를 대체하는 파일 전송 유틸리티



14.9 네트워크 관리

TCP/IP 교과서

» 서비스 품질 등의 요구사항을 충족하기 위해 네트워크 구성 요소를 감시하고, 시험하고, 구성하고, 문제점을 해결하는 것

» **단순 망 관리 프로토콜**(SNMP, Simple Network Management Protocol)과 **원격 모니터링**(RMON, Remote Monitoring) 프로토콜 이용

» 단순 망 관리 프로토콜

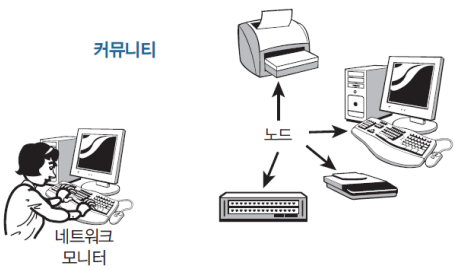
- 네트워크에서 원격 장치를 관리하고 모니터링하기 위해 설계된 프로토콜
- 단일 네트워크 관리자가 SNMP를 사용해 컴퓨터, 라우터 및 다른 네트워크 장치를 관리하고 모니터링할 수 있는 단일 워크스테이션을 원격으로 운영

14.9 네트워크 관리

TCP/IP 교과서

» SNMP 아키텍처의 주 구성 요소

- **네트워크 모니터:** 관리 또는 네트워크 관리 콘솔로도 불리는 관리 콘솔은 네트워크에서 장치를 관리할 수 있게 중앙 위치를 제공. 네트워크 모니터는 일반적으로 SNMP 관리 소프트웨어를 가진 일반 컴퓨터
- **노드:** 네트워크에 있는 장치
- **커뮤니티:** 공통 관리 프레임워크의 노드 그룹

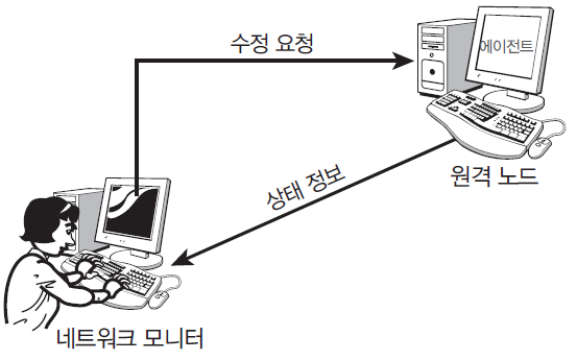


14.9 네트워크 관리

TCP/IP 교과서

» 단순 망 관리 프로토콜

- **에이전트**(agent)라고 불리는 프로그램이 원격 노드에서 작동해 네트워크 모니터에서 실행 중인 관리 시스템과 통신

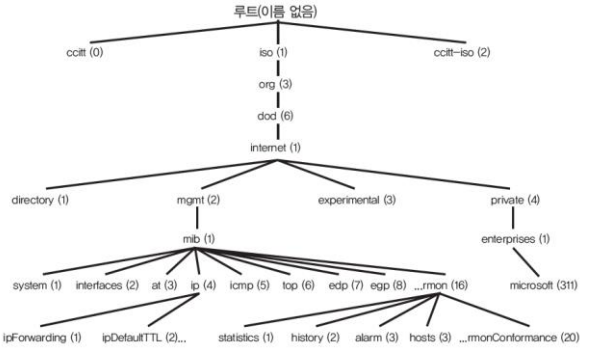


14.9 네트워크 관리

TCP/IP 교과서

» 단순 망 관리 프로토콜

- 모니터와 에이전트가 SNMP를 통해 어떠한 데이터를 주고받을까?
- SNMP는 광범위한 관리 매개변수 모음을 정의
- 네트워크 모니터는 **관리 정보 베이스**(MIB, Management Information Base)의 매개변수를 사용해 에이전트로부터 정보를 요청하고 구성 설정을 변경



14.9 네트워크 관리

- SNMP 주소 공간 – MIB
  - MIB 구조는 항상 루트에서 시작해서 읽고자 하는 설정을 고유하게 식별할 때까지 계층 구조를 통해 진행
  - 예를 들어, ipDefaultTTL과 ipInReceives MIBs를 알기 위해 SNMP 모니터가 다음 MIB 주소를 SNMP 에이전트에 전송

```
.iso.org.dod.internet.mgmt.mib.ip.ipDefaultTTL
.iso.org.dod.internet.mgmt.mib.ip.ipInReceives
```

14.10 요약

- TCP/IP 연결 유틸리티의 툴킷은 사용자가 네트워크 연결을 구성하고 문제 해결을 도와줌
- 각 유틸리티는 소량의 정보만을 표시
- 이러한 도구를 사용하는 방법을 알고 있다면 문제를 빠르게 해결하고 잠재적인 문제를 파악할 수 있음
- 이 장에서는 프로토콜 장애와 잘못된 구성, 회선 문제, 잘못된 이름 확인 및 과도한 트래픽에서 발생하는 문제와 ping, ifconfig, ipconfig, arp 같은 도구로 이러한 문제를 해결하는 방법을 살펴보았음
- 성능 문제 해결, 원격 접근 및 네트워크 모니터링을 위한 도구도 살펴보았음

14.13 핵심 용어

- **에이전트:** SNMP 소프트웨어는 MIB을 읽을 수 있는 호스트에 로드되고 원하는 결과를 모니터에 응답
- **arp:** ARP(주소 확인 프로토콜) 테이블의 콘텐츠를 구성하고 표시하는 유틸리티
- **ifconfig:** TCP/IP 구성 정보를 표시하는 유닉스/리눅스 유틸리티
- **ipconfig:** TCP/IP 구성 정보를 표시하는 파워셸 이전 윈도 유틸리티
- **MIB(관리 정보 베이스):** SNMP 모니터와 에이전트가 사용하는 계층적 주소 공간
- **netstat:** TCP/IP 프로토콜에 통계와 진단 정보를 제공하는 유틸리티
- **ping:** 다른 호스트와의 연결 상태를 확인할 때 사용하는 유틸리티
- **SSH(보안 셸):** 안전하고 암호화된 원격 셸 접근 솔루션을 형성하는 유틸리티의 집합
- **SNMP(단순 망 관리 프로토콜):** TCP/IP 네트워크의 리소스를 관리하기 위해 사용하는 프로토콜
- **텔넷:** 대부분은 더 안전한 SSH로 대체된 한때 인기 있던 원격 터미널
- **traceroute:** 패킷이 송신지에서 대상지까지 지나온 라우터 경로를 표시하는 유틸리
- **tracert:** traceroute 유틸리티와 동일한 파워셸 이전 마이크로소프트 유틸리티