



추가 네트워킹 프로토콜

네트워킹 기본 사항

학습 내용

강의 핵심 내용

학습 내용:

- 다른 유형의 통신 프로토콜을 식별합니다.
- 공통되는 전송, 애플리케이션 및 네트워크 관리 프로토콜을 설명합니다.
- 도구를 사용하여 네트워크 통신에 대한 정보를 검색합니다.

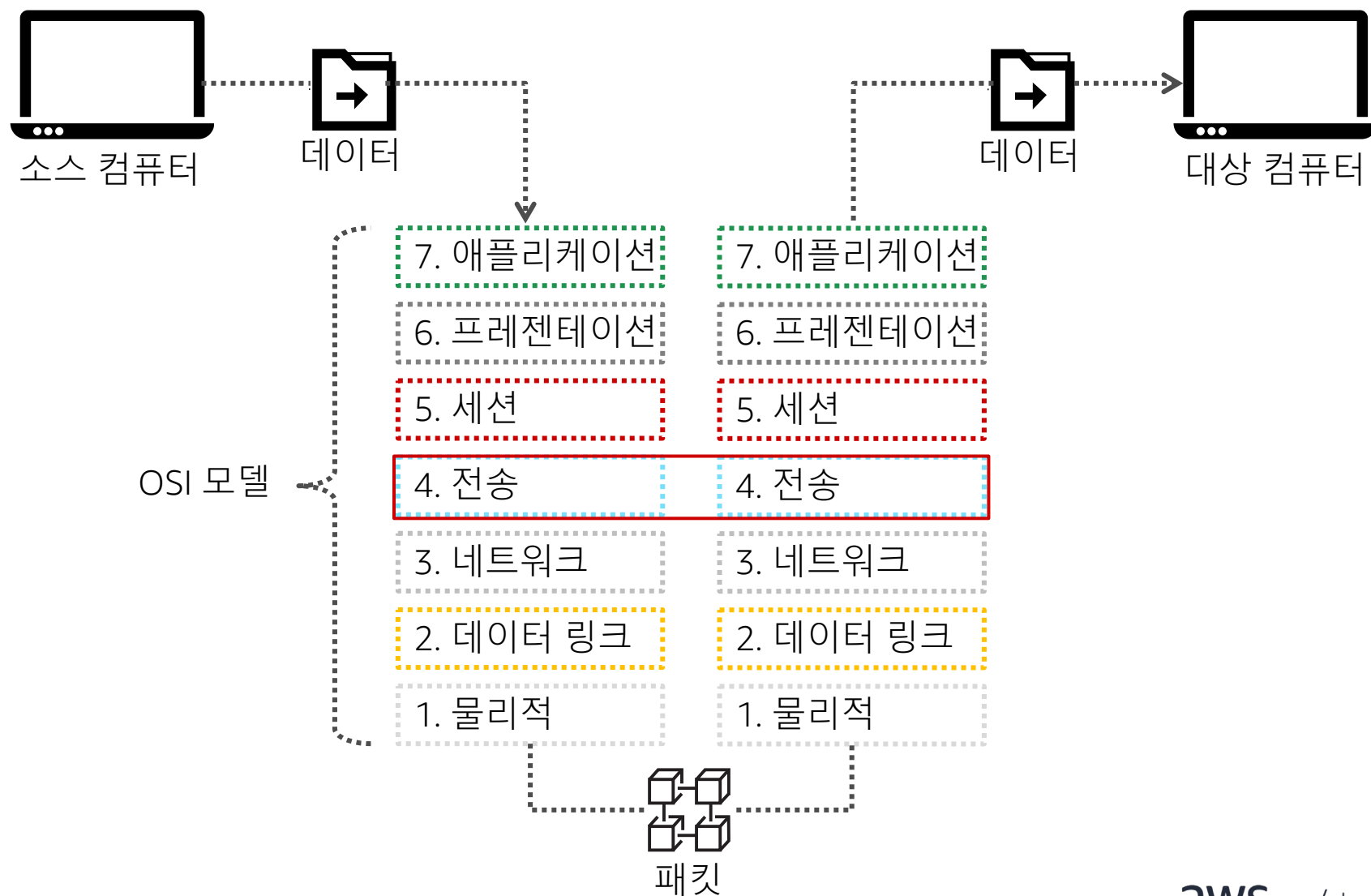


전송, 애플리케이션, 관리 및 지원 프로토콜

전송 프로토콜	애플리케이션 프로토콜	관리 및 지원 프로토콜
전송 제어 프로토콜(TCP) 사용자 데이터그램 프로토콜(UDP)	하이퍼텍스트 전송 프로토콜(HTTP) 보안 소켓 계층(SSL) 및 전송 계층 보안(TLS)	도메인 이름 시스템(DNS) 파일 전송 프로토콜(FTP)
	메일 프로토콜: <ul style="list-style-type: none">간이 전자 우편 전송 프로토콜(SMTP)전자 우편 프로토콜(POP)인터넷 메시지 액세스 프로토콜(IMAP)	동적 호스트 구성 프로토콜(DHCP)
	원격 데스크톱 프로토콜: <ul style="list-style-type: none">원격 데스크톱 프로토콜(RDP)Secure Shell(SSH)	인터넷 제어 메시지 프로토콜(ICMP)

OSI 모델

Open Systems
Interconnection(OSI)
모델은 컴퓨터가
네트워크로 정보를
공유하는 방법에 대한
스탠더드를 정의합니다.

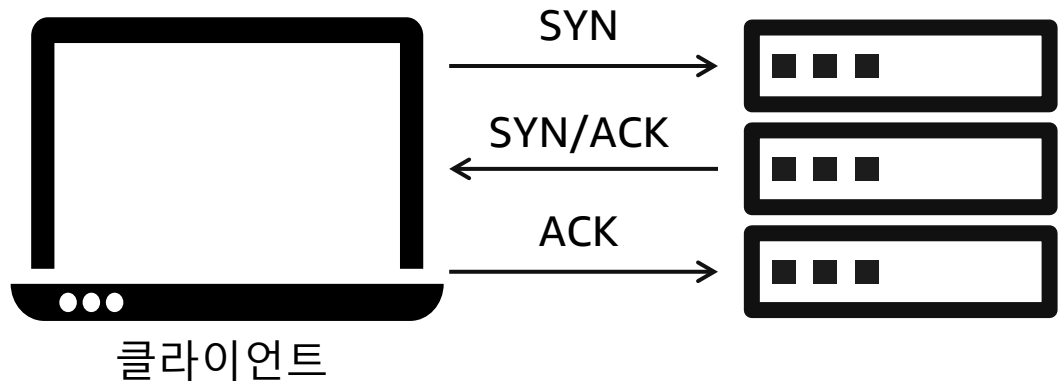




전송 프로토콜

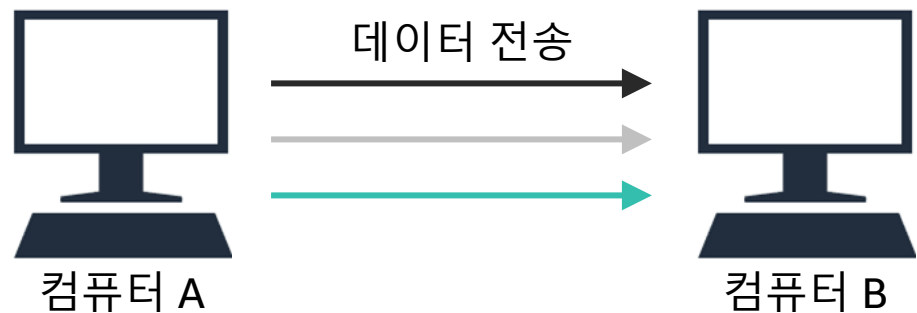
TCP

TCP/IP는 연결 지향형 프로토콜입니다. 애플리케이션이 데이터를 교환할 수 있는 네트워크 통신을 설정하고 유지 관리하는 방법을 정의합니다. 이 프로토콜을 통해 전송되는 데이터는 패킷이라고 하며 더 작은 청크로 나뉩니다.



UDP

UDP는 간단한 비연결형 통신 모델을 사용해 IP 네트워크로 데이터를 전달합니다. TCP와 비교해 볼 때 UDP는 최소한의 기능만 제공합니다. 데이터의 전달이나 순서를 보장하지 않기 때문에 신뢰할 수 없는 것으로 간주합니다. UDP의 장점은 오버헤드가 낮아 TCP보다 속도가 빠르다는 점입니다.



TCP와 UDP의 비교

기본 비교 항목	TCP	UDP
정의	TCP는 데이터를 전송하기 전에 가상 서킷을 설정합니다.	UDP는 수신기의 수신 준비 상태를 확인하지 않고 대상 컴퓨터에 직접 데이터를 전송합니다.
연결 유형	연결 지향형 프로토콜입니다.	비연결형 프로토콜입니다.
속도	느림	빠름
신뢰성	신뢰할 수 있는 프로토콜입니다.	신뢰할 수 없는 프로토콜입니다.
헤더 크기	20바이트	8바이트
승인	데이터 승인을 기다리며 손실된 패킷을 다시 보낼 수 있습니다.	승인받지도 않고, 손상된 프레임을 재전송하지도 않습니다.

네트워크 프로토콜



연결 지향형 프로토콜은 두 명이 주고받는 전화 통화와 유사합니다.



비연결형 프로토콜은 한 사서함에서 다른 사서함으로 편지를 보내는 것과 같습니다.

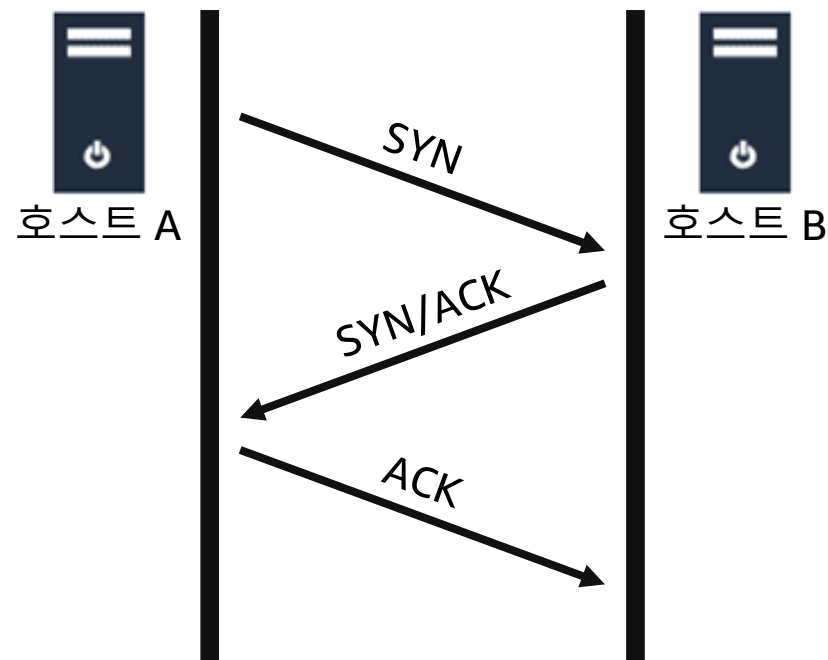
연결 지향형 프로토콜	비연결형 프로토콜
연결을 설정하고 응답을 기다립니다.	대상이 사용 가능하고 데이터를 수신할 준비가 되었는지 확인하지 않고 하나의 엔드포인트에서 다른 엔드포인트로 메시지를 전송합니다.
발신자와 수신기 간에 세션을 생성합니다.	발신자와 수신기 간에 세션이 필요하지 않습니다.
동기식 통신을 사용합니다.	비동기식 통신을 사용합니다.

TCP 핸드셰이크

TCP

- TCP는 연결 지향형입니다.
- TCP 핸드셰이크는 발신자와 수신기가 주고받는 다음 세 가지 메시지로 구성됩니다.
 - 동기화(SYN)
 - 동기화/확인(SYN/ACK)
 - 확인(ACK)

3단계 핸드셰이크 중에 프로토콜은 데이터 전송을 지원하는 파라미터를 설정합니다.



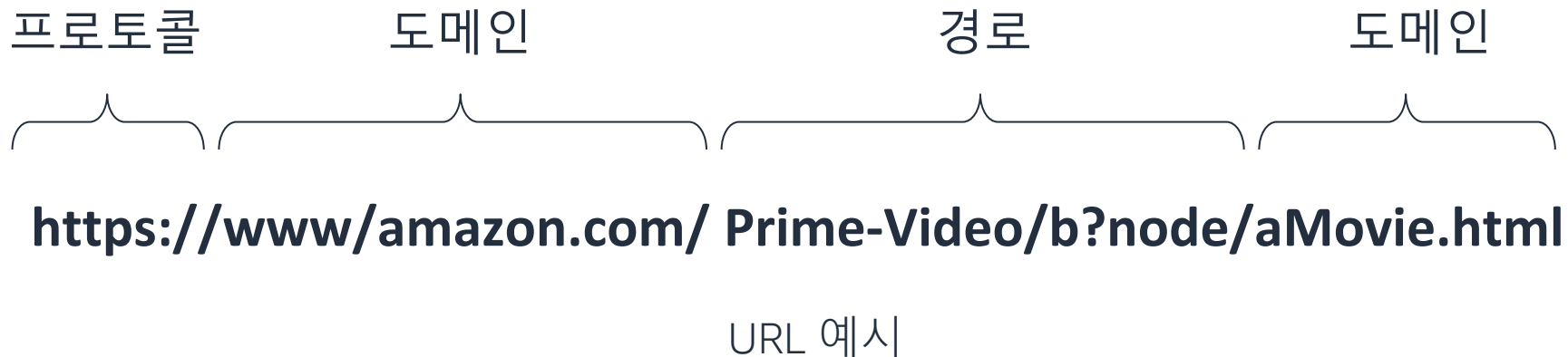


애플리케이션 프로토콜

HTTP

HTTP는 웹 페이지에 도달하는 데 사용되는 프로토콜입니다. 전체 HTTP 주소는 Uniform Resource Locator(URL)로 표현됩니다.

보안이 추가된 하이퍼텍스트 전송 프로토콜(HTTPS)은 HTTP와 SSL/TLS 프로토콜의 조합입니다.



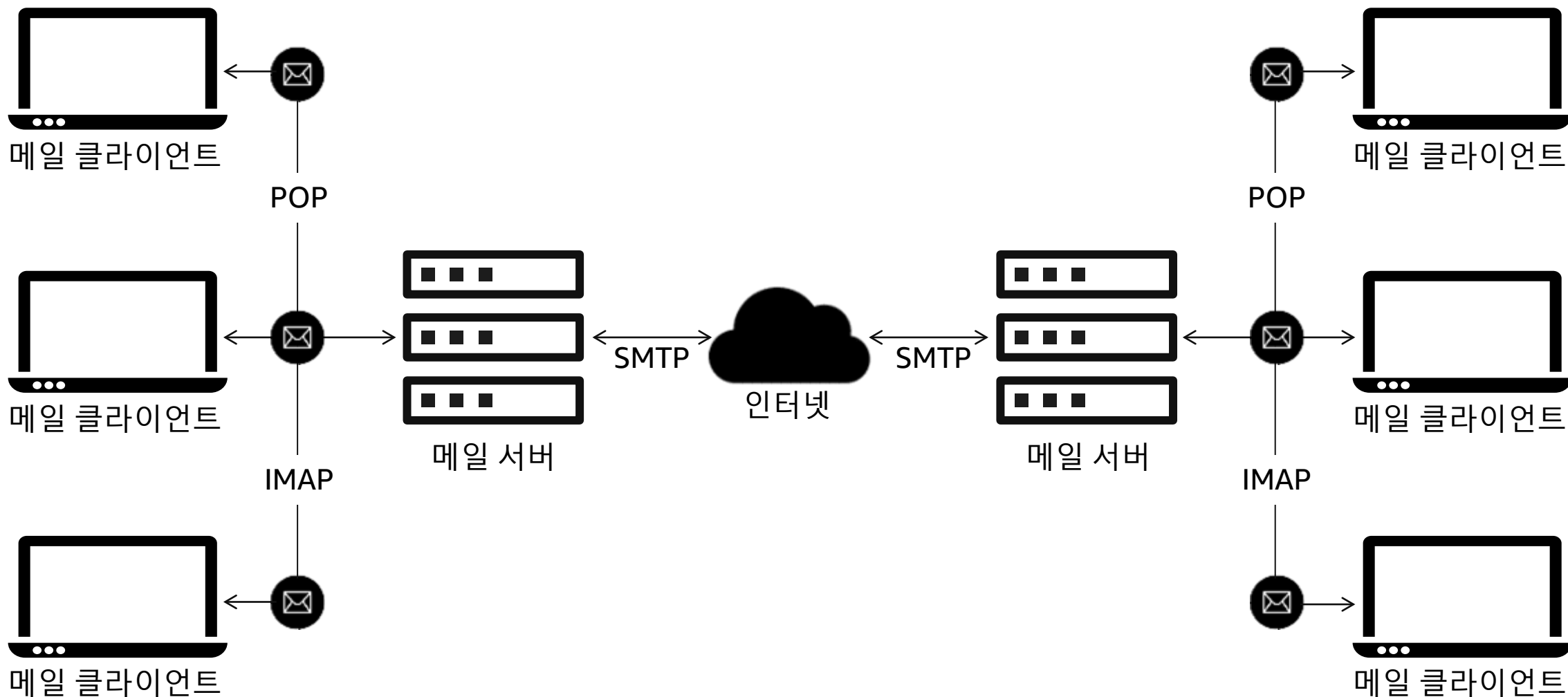
SSL과 TLS

SSL은 암호화를 사용해 두 시스템 간의 통신을 보호하고 안전하게 지키기 위한 스탠더드입니다.

TLS는 보안 성능이 한층 강화된 업데이트 버전의 SSL입니다. Payment Card Industry Security Standards Council(PCI SSC) 같은 많은 보안/스탠더드 조직은 해당 조직에서 TLS 버전 1.2를 사용해 자격증을 유지해야 합니다.

TLS 핸드셰이크는 통신 세션을 시작하는 프로세스로, **TLS 암호화**를 사용합니다. TLS 핸드셰이크 중에 통신하는 양측은 메시지를 교환해 서로를 승인하고 확인합니다. 이들은 사용할 암호화 알고리즘을 설정하고 세션 키에 동의합니다. TLS 핸드셰이크는 HTTPS 작동 방식의 근간을 이루는 부분입니다.

메일 프로토콜(SMTP, POP, IMAP)



원격 데스크톱 프로토콜(RDP, SSH)



RDP과 SSH는 시스템 및 기타 서버에 원격으로 액세스하는 데 사용됩니다. 둘 다 클라우드 기반 서버에 안전하게 액세스하는 데 반드시 필요하며, 원격 직원이 온프레미스 인프라를 사용하는 데에도 도움이 됩니다.

애플리케이션 프로토콜 포트 번호

다음 테이블에는 일반적인 애플리케이션 프로토콜이 사용하는 네트워크 프로토콜과 포트 번호가 나와 있습니다.

애플리케이션 프로토콜	전송 프로토콜	포트 번호
HTTP	TCP	80
HTTPS	TCP	443
FTP	TCP	21
SSH	TCP	22
DNS	TCP	53

사용하지 않은 포트 번호는 일반적으로 보안상의 이유로 닫힙니다. 클라이언트 컴퓨터에 설치된 소프트웨어와 서버 사이의 게이트웨이 역할을 하는 포트는 악의적인 공격의 경로 역할도 할 수 있습니다.



관리 및 지원 프로토콜

관리 및 지원 프로토콜의 예제

- 관리 프로토콜은 네트워크 장비를 구성하고 유지하는 데 사용됩니다.
- 지원 프로토콜은 네트워크 통신을 촉진하고 개선합니다.

다음 테이블에는 관리 및 지원 프로토콜의 몇 가지 예제가 설명되어 있습니다.

관리 및 지원 프로토콜의 예제

도메인 이름 시스템(DNS)

인터넷 제어 메시지 프로토콜(ICMP)

동적 호스트 구성 프로토콜(DHCP)

파일 전송 프로토콜(FTP)

DNS

DNS는 도메인 이름에 대한 데이터베이스로, 휴대폰의 연락처 목록과 유사합니다. 연락처 목록은 사람(또는 조직) 이름과 전화번호를 매칭합니다. DNS는 인터넷의 연락처 목록과 같은 기능을 합니다.

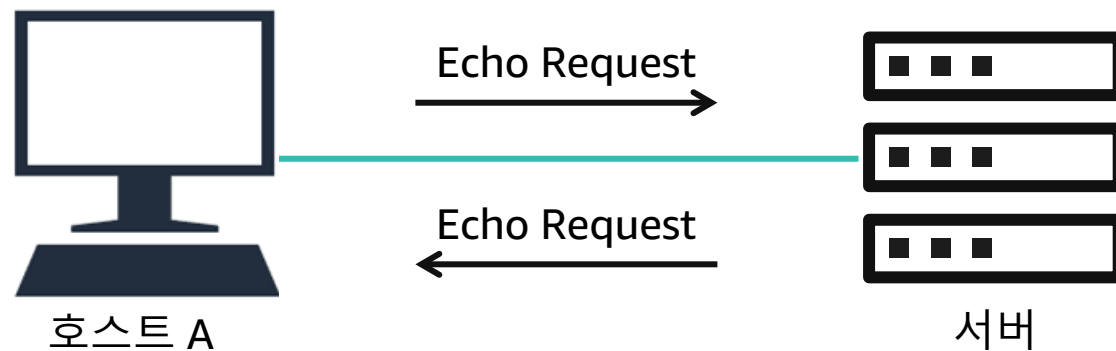
DNS는 사람이 읽을 수 있는 도메인 이름(예: `www.amazon.com`)을 컴퓨터에서 읽을 수 있는 IP 주소(예: `192.0.2.44`)로 변환합니다. DNS 서버는 IP 주소를 도메인 이름에 자동 매핑합니다.



ICMP

네트워크 디바이스는 ICMP를 사용해 네트워크 통신 문제를 진단하고 IP 네트워크의 오류에 대한 응답을 생성합니다.

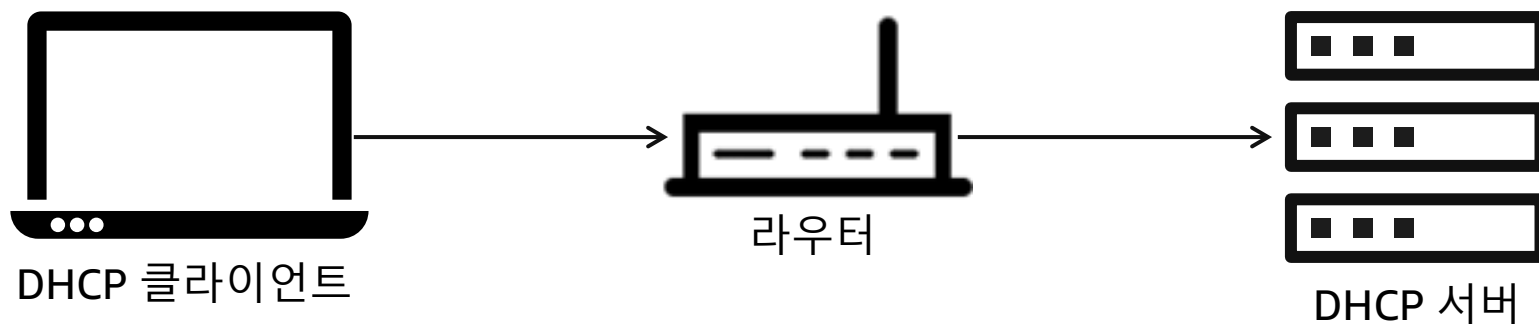
적절한 예로는 ICMP 요청과 ICMP 응답 메시지를 사용하는 **ping** 유틸리티가 있습니다. 특정 호스트 또는 포트에 연결할 수 없는 경우 ICMP가 소스에 오류 메시지를 보낼 수 있습니다.



DHCP

DHCP는 IP 주소, 서브넷 마스크, 게이트웨이 및 기타 IP 파라미터를 네트워크에 연결된 디바이스에 자동으로 할당합니다.

DHCP 옵션의 몇 가지 예로는 라우터(기본 게이트웨이)와 DNS 서버, DNS 도메인 이름을 들 수 있습니다.



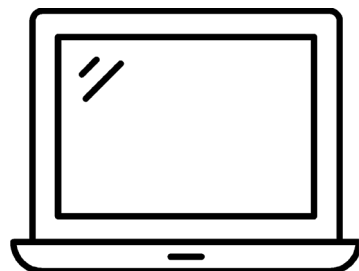
FTP

FTP는 한 컴퓨터에서 다른 컴퓨터로 파일을 전송할 수 있는 네트워크 프로토콜입니다.



일반적인 네트워크 유틸리티

일반적인 네트워크 유틸리티의 예는 다음과 같습니다.



- **ping**은 연결을 테스트합니다. 이 도구는 원격 디바이스(서버 또는 데스크톱)가 네트워크에 있는지 여부를 테스트합니다.
- **nslookup**은 DNS와 해당 서버를 쿼리합니다. 주어진 도메인 이름과 연결된 IP 주소를 보여 줍니다.
- **tracert**은 사용자가 이용 중인 네트워킹 경로를 볼 수 있게 해 줍니다. 연결 문제를 해결하는 데 유용합니다.
- **telnet**은 서비스 응답에 사용됩니다. 이 도구는 원격 디바이스에서 실행되는 서비스가 요청에 응답하는지 여부를 테스트합니다.

일반적인 네트워크 진단 도구: hping3

```
hping3 -S -c 50 -V
<Public IP of EC2 instance or on-premises host>
HPING 72.14.207.99 (eth1 72.14.207.99): S set, 40
headers + 0 data bytes
len=46 ip=72.14.207.99 ttl=244 id=64932 sport=80 flags=SA seq=0 win=8190 rtt=266.4 ms

--- 72.14.207.99 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 266.4/266.4/266.4 msemises host>
```

명령 프롬프트에서 다음 **hping3** 명령을 실행합니다.

```
hping3 -S -c 50 -V <Public IP of
EC2 instance or on-premises host>
```

- **hping3**는 패킷 손실 외에 TCP를 통한 **최소/평균/최대** 엔드 투 엔드 대기 시간을 결과로 보여 줍니다.

일반적인 네트워킹 진단 도구: traceroute

```
traceroute google.com
```

```
traceroute to google.com (172.217.23.14), 30 hops max, 60 byte packets
```

```
1  10.8.8.1 (10.8.8.1)                14.499 ms  15.335 ms  15.956 ms
2  h37-220-13-49.host.redstation.co.uk (37.220.13.49) 17.811 ms  18.669 ms  19.346 ms
3  92.zone.2.c.dc9.redstation.co.uk (185.20.96.137) 19.096 ms  19.757 ms  20.892 ms
4  203.lc3.redstation.co.uk (185.5.3.221) 28.160 ms  28.415 ms  28.665 ms
5  100.core1.the.as20860.net (62.128.218.33) 26.739 ms  27.840 ms  28.847 ms
6  110.core2.thn.as20860.net (62.128.218.26) 29.112 ms  18.466 ms  19.835 ms
7  be97.asr01.thn.as20860.net (62.128.222.205) 19.986 ms  20.488 ms  21.354 ms
8  * * *
9  216.239.48.143 (216.239.48.143) 24.364 ms  216.239.48.113
(216.239.48.113) 25.069 ms  25.592 ms
10 108.170.233.199 (108.170.233.199) 26.239 ms  27.369 ms  28.031 ms
11 lhr35s01-in-f14.1e100.net (172.217.23.14) 28.642 ms
```

명령 프롬프트에서 다음 `traceroute` 명령을 실행합니다.

```
sudo traceroute -n -T -p 22 <Public IP
of EC2 instance/on-premises host>
```

- `-T -p 22 -n` 인수는 포트 22에서 TCP 기반 추적을 수행합니다.
- 요청 중 일부가 시간 초과되는 경우가 많으므로, 경로의 마지막 홉(hop)이나 대상 주소에서 패킷 손실이 발생하는지 확인하십시오. 여러 홉(hop)에 대한 패킷 손실은 문제를 나타낼 수 있습니다.

일반적인 네트워킹 진단 도구: mtr

```
My traceroute [v0.80]
traceroute (0.0.0.0) Tue Oct 22 20:39:42 2013
Resolver: Received error response 2. (server failure)er of fields quit
Packets
Host Loss% Snt Last Avg Best Wrst StDev
1. 192.241.160.253 0.0% 371 0.4 0.6 0.1 14.3 1.0
2. 192.241.164.241 0.0% 371 7.4 2.5 0.1 37.5 4.8
3. xe-3-0-6.ar2.nyc3.us. 2.7% 371 3.6 2.6 1.1 5.5 1.1
4. sl-gw50-nyc-.sprintli 0.0% 371 0.7 5.0 0.1 82.3 13.1
```

명령 프롬프트에서 다음 **mtr** 명령을 실행합니다.

```
mtr -n -T -c 200 <Public IP EC2
instance/on-premises host> --report
```

- **-T** 인수는 TCP 기반 MTR을 수행하고 **--report** 옵션은 MTR를 보고서 모드로 전환합니다. MTR는 **-c** 옵션을 사용해 지정한 횟수의 주기 동안 실행됩니다.
- 통계 데이터를 인쇄하고 종료합니다.

일반적인 네트워킹 진단 도구: Telnet

```
C:\>telnet 8.8.8.8 54
Connecting To 8.8.8.8...Could not open connection to the host, on port 54: Connect failed
C:\>
```

명령 프롬프트에서 다음 **telnet** 명령을 실행합니다.

```
telnet [domain name or ip] [port], for
example: telnet 192.168.1.1 443
```

- 컴퓨터 포트가 열리면 빈 화면이 나타나거나, 'connected to [domain name or ip]'라는 메시지가 표시되어 연결되었음을 의미합니다.
- 컴퓨터 포트가 닫혀 있으면 'could not open connection to the host, on port [port number]: Connect failed.'라는 메시지가 표시됩니다. 이 메시지는 방화벽이 포트에 대한 액세스를 차단하고 있거나 포트가 닫혀 있음을 의미할 수 있습니다.

일반적인 네트워킹 진단 도구: nslookup

```
$ nslookup redhat.com

Server:          192.168.19.2
Address:         192.168.19.2#53

Non-authoritative answer:
Name:            redhat.com
Address:         209.132.183.181
```

명령 프롬프트에서 다음 `nslookup` 명령을 실행합니다.

```
C:\>nslookup -type=NS ses-example.com
```

- `nslookup`은 도메인 URL을 입력하고 해당 서버 IP 주소를 검색하는 DNS를 조회합니다.
- 이 프로세스를 역순으로 수행하고 IP 주소를 입력하여 해당 도메인 URL을 검색할 수도 있습니다.

활동: ping 및 nslookup

터미널 창 또는 명령 프롬프트 창을 열고 다음 단계를 완료하십시오.

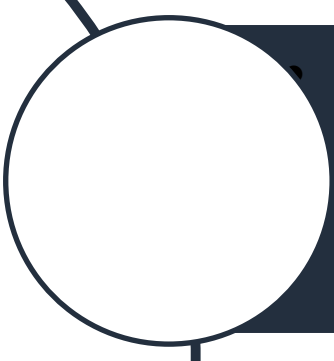
1. `ping amazon.com`을 입력합니다.
 - 이 명령은 응답 서버의 IP 주소를 반환합니다.
 - 추가 연결 정보를 확인할 수 있습니다.
2. `nslookup amazon.com`을 입력합니다.
 - 컴퓨터가 `amazon.com`에 연결하는 데 사용되는 경로를 확인할 수 있습니다.

활동(Linux 또는 macOS만 해당): traceroute

터미널 창 또는 명령 프롬프트 창을 열고
다음 단계를 완료하십시오.


1. `traceroute amazon.com`을 입력합니다.
 - 요청에서 몇 홉(hop)이 걸렸는지 관찰할 수 있습니다.
 - 각 홉(hop)의 대기 시간을 관찰할 수 있습니다.
 - 홉(hop)에 별표(*)가 있으면 홉 시간이 초과되었음을 의미합니다.

확인 질문(1/4)



개발자가 해당 IP 주소를 사용하여 회사의 로컬 파일 전송 프로토콜(FTP) 서버에 연결하려고 했지만, 연결하지 못했습니다. 연결에 실패함에 따라 시스템 관리자가 이 개발자의 문제를 해결하기로 결정했습니다.

관리자가 개발자의 연결 문제를 해결하기 위해 따라야 할 절차는 무엇입니까?



디바이스가 다른 IP 네트워크와 통신할 수 있도록 네트워크의 각 디바이스에 IP 주소와 기타 IP 파라미터를 자동으로 할당하는 프로토콜은 무엇입니까?

확인 질문(2/4)


원격 컴퓨터의 포트가 열려 있는지 여부를 테스트하는 명령은 무엇입니까?

동영상 스트리밍 서비스와 같이 보장된 데이터를 제공하는 것보다 속도를 우선시하는 애플리케이션에서 사용하는 프로토콜은 무엇입니까?

확인 질문(3/4)

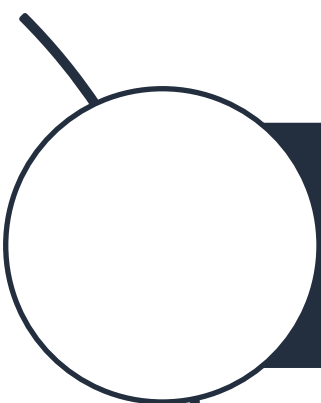


도메인 이름 시스템(DNS) 서버의 역할은 무엇입니까?




클라이언트의 메일을 서버에 전송하거나 이메일 서버 간에 이메일을 전송할 수 있는 프로토콜은 무엇입니까?

확인 질문(4/4)



네트워크 통신을 설정, 유지하는 방법을 정의하고 데이터 패킷의 전송을 보장하는 프로토콜은 무엇입니까?



ICMP를 사용하여 네트워크 통신 문제를 진단하고 IP 네트워크의 오류에 대한 응답을 생성하는 프로토콜 네트워크 디바이스는 무엇입니까?

요점



- TCP와 UDP는 전송 프로토콜입니다. TCP는 연결 지향형, UDP는 비연결형입니다.
- 인터넷에서 사용되는 일반적인 애플리케이션 프로토콜에는 HTTP, TLS/SSL, SMTP, FTP가 있습니다.
- 일반적인 네트워크 관리 및 지원 프로토콜에는 DNS, DHCP, ICMP가 있습니다.
- 네트워크 통신을 검색하고 문제를 해결하는 데 사용되는 일반적인 유틸리티에는 **ping**, **nslookup**, **traceroute**가 있습니다.

감사합니다.



© 2022 Amazon Web Services, Inc. 또는 계열사. All rights reserved. 본 내용은 Amazon Web Services, Inc.의 사전 서면 허가 없이 전체 또는 일부를 복제하거나 재배포할 수 없습니다. 상업적인 복제, 임대 또는 판매는 금지됩니다. 수정해야 할 사항, 피드백 또는 기타 질문이 있다면 <https://support.aws.amazon.com/#/contacts/aws-training>에서 문의해 주십시오. 모든 상표는 해당 소유자의 자산입니다.