[네트워크프로그래밍]

지정 주제 프로젝트 보고서

소속 : IT대학 – 소프트웨어학부

학번 : 20192851, 20192829, 20192847

이름 : 윤성준, 박민수, 양조은

**목 차**

1. **프로토콜 플로우 및 패킷 구조**

1.1. Main server와 Working server간의 프로토콜 플로우

1.2. Main server와 Working server간의 패킷 페이로드 정의

1.3. 멀티프로세스(또는 쓰레드) 사용 시 역할에 대한 설명

1. **프로그램 설명**
2. **PoW nonce (8개)**

3.1.챌린지 학번 단독 실행 (난이도 7)

3.2. 챌린지 이름 단독 실행 (난이도 7)

3.3. 챌린지 학번 분산 실행 (난이도 7)

3.4. 챌린지 이름 분산 실행 (난이도 7)

3.5. 챌린지 학번 단독 실행 (난이도 8)

3.6. 챌린지 이름 단독 실행 (난이도 8)

3.7. 챌린지 학번 분산 실행 (난이도 8)

3.8. 챌린지 이름 분산 실행 (난이도 8)

1. **단독 실행 vs. 분산 실행**

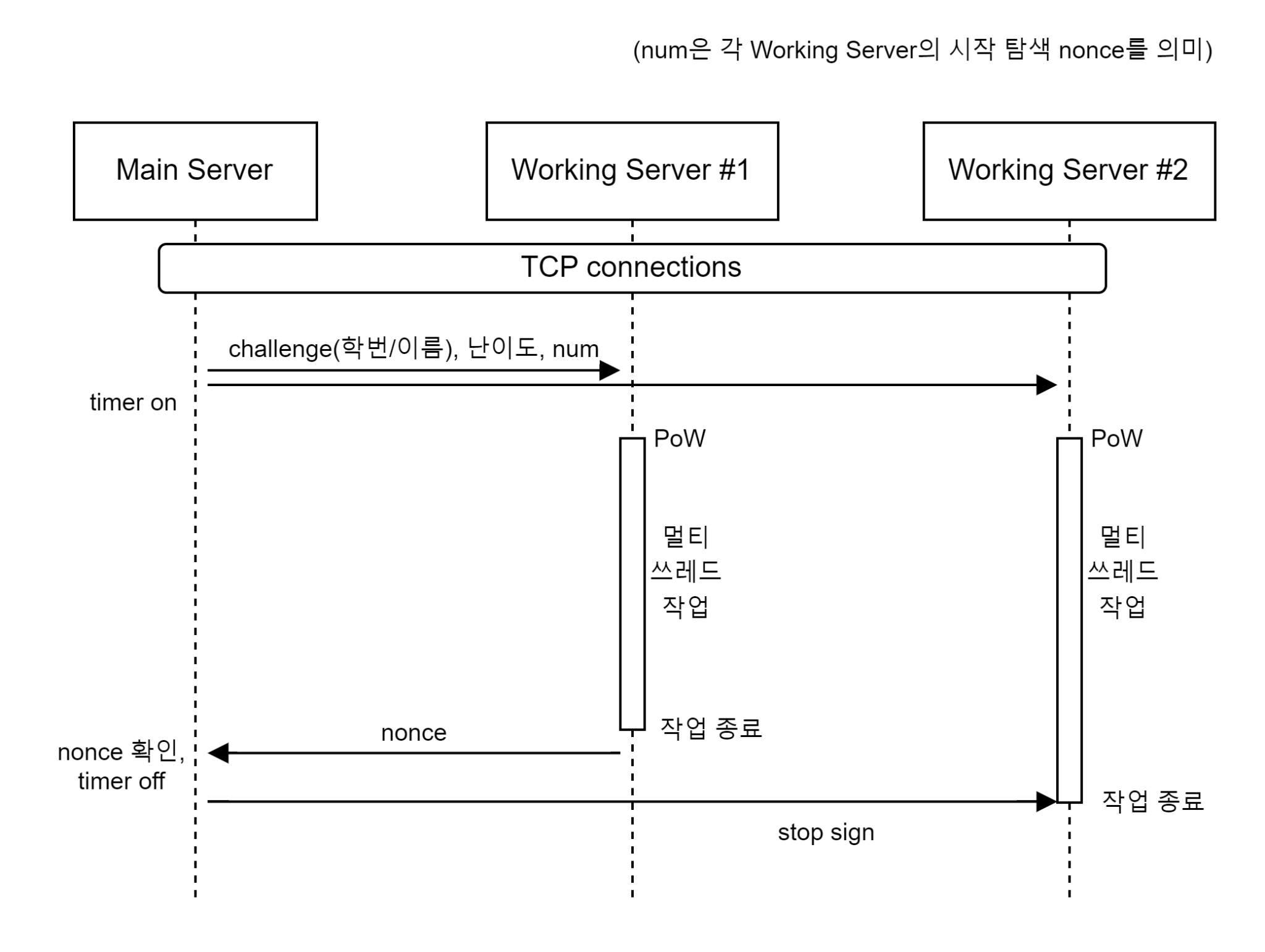
4.1. 챌린지 학번 또는 챌린지 이름의 난이도 7일 때의 실행시간 차이 (비율)

4.2. 챌린지 학번 또는 챌린지 이름의 난이도 8일 때의 실행시간 차이 (비율)

1. **Port Forwarding**
2. **프로젝트 회고**

1. **프로토콜 플로우 및 패킷 구조**

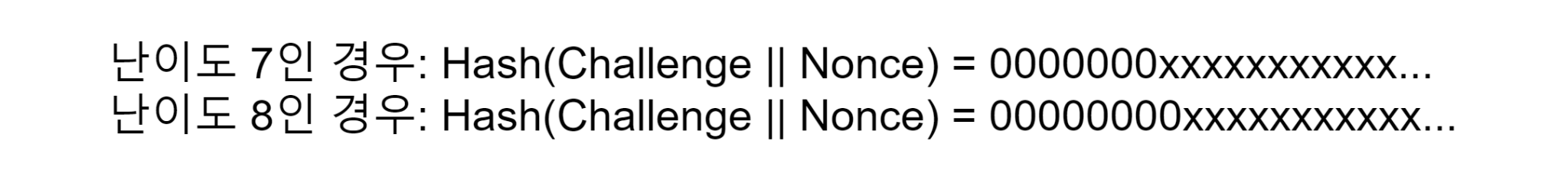
**1.1. Main server와 Working server간의 프로토콜 플로우**



먼저 Main Server 구동시키고 해당 IP와 Port를 통하여 두 Working Server가 접속하면 TCP 연결이 형성된다. Main Server에서 challenge와 난이도를 설정하고, 이 값들을 각 Working Server의 탐색 시작 nonce 값인 num과 함께 전송한다. 그럼 두 Working Server는 각각 주어진 num부터 시작해서 nonce값 탐색, 즉 PoW를 진행하게 된다. 이 과정에서 해시 연산을 통해 특정 조건을 만족하는 nonce 값을 찾았다면, 그 값을 Main Server에게 전송한다. 이 때, Main Server는 두 Working Server 중 어느 하나로부터 값을 먼저 받게 되면, 그 값을 채택하고 이를 나머지 서버에게 알린다. (stop sign)

**1.2. Main server와 Working server간의 패킷 페이로드 정의**

* Challenge:
  + 학번: 20192829||20192851||20192847
  + 이름: 박민수||윤성준||양조은
* 난이도: 7 or 8
* 탐색 시작 번호(num)
  + Working Server #1: 0 ~ 4,611,686,018,427,387,902
  + Working Server #2: 4,611,686,018,427,387,903 ~



**1.3. 멀티 쓰레드 사용**

본 프로젝트에서 Working Server는 5개의 PoW 연산 쓰레드와 1개의 Stop 리스너 쓰레드를 만들어 병렬처리를 한다.

**1.3.1 PoW 연산 쓰레드 함수**

#define NUM\_THREADS 5 // 작업을 수행할 스레드의 수

#define RANGE\_PER\_THREAD 20000 // 한 번에 각 스레드가 담당할 nonce 값 범위

#define MAX\_NONCE LONG\_MAX // 최대 nonce 값

void \*pow\_worker(void \*threadid)

{

long tid = (long)threadid;

unsigned char text[64];

unsigned char hash[SHA256\_DIGEST\_LENGTH];

for (long nonce = start\_nonce + tid \* RANGE\_PER\_THREAD; nonce < MAX\_NONCE; nonce += NUM\_THREADS \* RANGE\_PER\_THREAD)

{

for (long my\_nonce = nonce; my\_nonce < nonce + RANGE\_PER\_THREAD; my\_nonce++)

{

pthread\_mutex\_lock(&found\_mutex);

if (stop\_received || found\_nonce != -1)

{

pthread\_mutex\_unlock(&found\_mutex);

pthread\_exit(NULL);

}

pthread\_mutex\_unlock(&found\_mutex);

sprintf(text, "%s%ld", challenge, my\_nonce);

compute\_SHA256(hash, text, strlen(text));

if (is\_valid(hash, difficulty))

{

print\_hash(hash);

pthread\_mutex\_lock(&found\_mutex);

if (found\_nonce == -1)

{ // double check inside the lock

found\_nonce = my\_nonce;

found\_thread\_id = tid; // Store the thread ID

}

pthread\_mutex\_unlock(&found\_mutex);

pthread\_exit(NULL);

}

}

}

pthread\_exit(NULL);

}

**pow\_worker**함수는 NUM\_THREADS x RANGE\_PER\_THREAD의 총 합계를 NUM\_THREADS 수의 쓰레드가 RANGE\_PER\_THREAD 단위로 분할하여 연산을 수행하도록 구성된다. 현재 설정에 따르면, 10만 개의 숫자를 5개의 쓰레드가 각각 2만 개씩 나누어서 처리하게 된다. 쓰레드 수가 5개를 초과하면 오히려 연산 시간이 증가하는 결과가 나타나, 총 쓰레드 수는 5개로 결정했다. 그러나 RANGE\_PER\_THREAD의 최적값은 추가적인 연구를 통해 결정될 수 있을 것으로 보인다. MAX\_NONCE는 다양한 실험을 통해, 주어진 프로젝트 범위 내에서 Nonce의 범위가 대체적으로 int 타입보다는 더 넓어 long 타입을 사용하는 것이 적합하다고 판단된다.

각 쓰레드는 총 10만 개의 숫자 중 2만 개씩을 검사한다. 이 과정에서 전역변수인 stop\_received가 false이고 found\_nonce가 -1이 아닌 경우, 다른 워킹 서버 또는 쓰레드에서 이미 nonce를 찾았다고 판단하여 연산을 중단한다. 그렇지 않은 경우, compute\_SHA256 함수를 사용하여 해시 값을 계산하고, 해당 해시 값이 설정된 난이도 요구사항을 만족하는지 확인한다. 만약 만족하는 경우, 해당 해시 값을 화면에 출력하고, found\_nonce를 현재의 my\_nonce 값으로 변경하며, nonce를 찾은 쓰레드의 ID를 found\_thread\_id에 저장한다. 이러한 모든 작업은 각 쓰레드에서 동시에 실행되므로, 뮤텍스를 사용하여 쓰레드 간의 상호 배제를 보장한다.

**1.3.2 리스너 쓰레드**

void \*message\_listener(void \*arg)

{

int sock = \*((int \*)arg);

char message[BUF\_SIZE];

while (1)

{

if (read(sock, message, BUF\_SIZE - 1) > 0)

{

if (strcmp(message, "stop") == 0)

{

pthread\_mutex\_lock(&found\_mutex);

stop\_received = true;

printf("Stopped computation due to stop message\n");

pthread\_mutex\_unlock(&found\_mutex);

break;

}

}

}

pthread\_exit(NULL);

}

리스너 쓰레드는 message\_listener 함수를 통해 main server에서 stop 메세지를 보내는지 항시 확인한다. stop 메세지가 온다면 stop\_received를 true로 바꿈으로서 연산 쓰레드에게 stop 메세지를 알린다. 그리고 화면에 Stopped computation due to stop message을 출력한다.

1. **프로그램 설명**

2.1. 함수 설명

2.1.1. Main Server

**main 함수:**  main 함수는 총 5가지 단계로 동작한다.

1. 서버 소켓 설정 및 working server 연결한다.
2. 사용자에게 Challenge와 Difficulty 입력 받는다.
3. Working server에 Challenge와 Difficulty, Start\_nonce를 전송한다.
4. Select() 함수를 통해 수신 데이터를 감지하여 PoW결과와 소요시간을 출력한다.
5. 다른 클라이언트에게 중지 신호를 전송한다.

2.1.2. Working Server

* **compute\_SHA256** 함수: 이 함수는 주어진 데이터의 OpenSSL의 SHA-256 해시를 계산한다.
* **check\_4bits** 함수: 이 함수는 주어진 바이트에서 첫 4비트가 모두 0인지 확인한다.
* **is\_valid** 함수: 이 함수는 주어진 해시가 PoW의 난이도 요구사항을 충족하는지 확인한다.
* **print\_hash** 함수: 이 함수는 주어진 해시를 표준 출력에 출력한다.
* **pow\_worker** 함수: 이 함수는 각 쓰레드에서 실행되며 PoW를 수행한다. 주어진 nonce 범위에서 유효한 해시를 찾는 작업을 수행하며, 이 작업은 멀티스레딩 환경에서 병렬로 진행한다.
* **message\_listener** 함수: 이 함수는 메인 서버에서 stop 메시지를 수신하는 데 사용한다. stop 메시지를 수신하면, stop\_received 플래그를 설정하여 모든 pow\_worker 쓰레드가 작업을 중지하도록 한다.
* **main 함수**:

1. 소켓을 생성하고 메인 서버에 연결한다.
2. 메인 서버로부터 PoW에 필요한 정보를 수신한다.
3. PoW를 수행하는 작업자 쓰레드 5개와 stop 메시지를 듣는 리스너 쓰레드 1개를 생성한다.
4. 쓰레드 join()을 통해 작업자 쓰레드가 종료되길 기다린다.
5. 모든 작업자 쓰레드가 종료되면, 리스너 쓰레드를 취소한다.
6. PoW가 성공하면 성공 메시지와 nonce 값을 메인 서버에 전송한다. stop 메시지를 수신하거나 탐색에 실패하면 실패 메시지를 출력한다.

1. **PoW nonce (8개)**

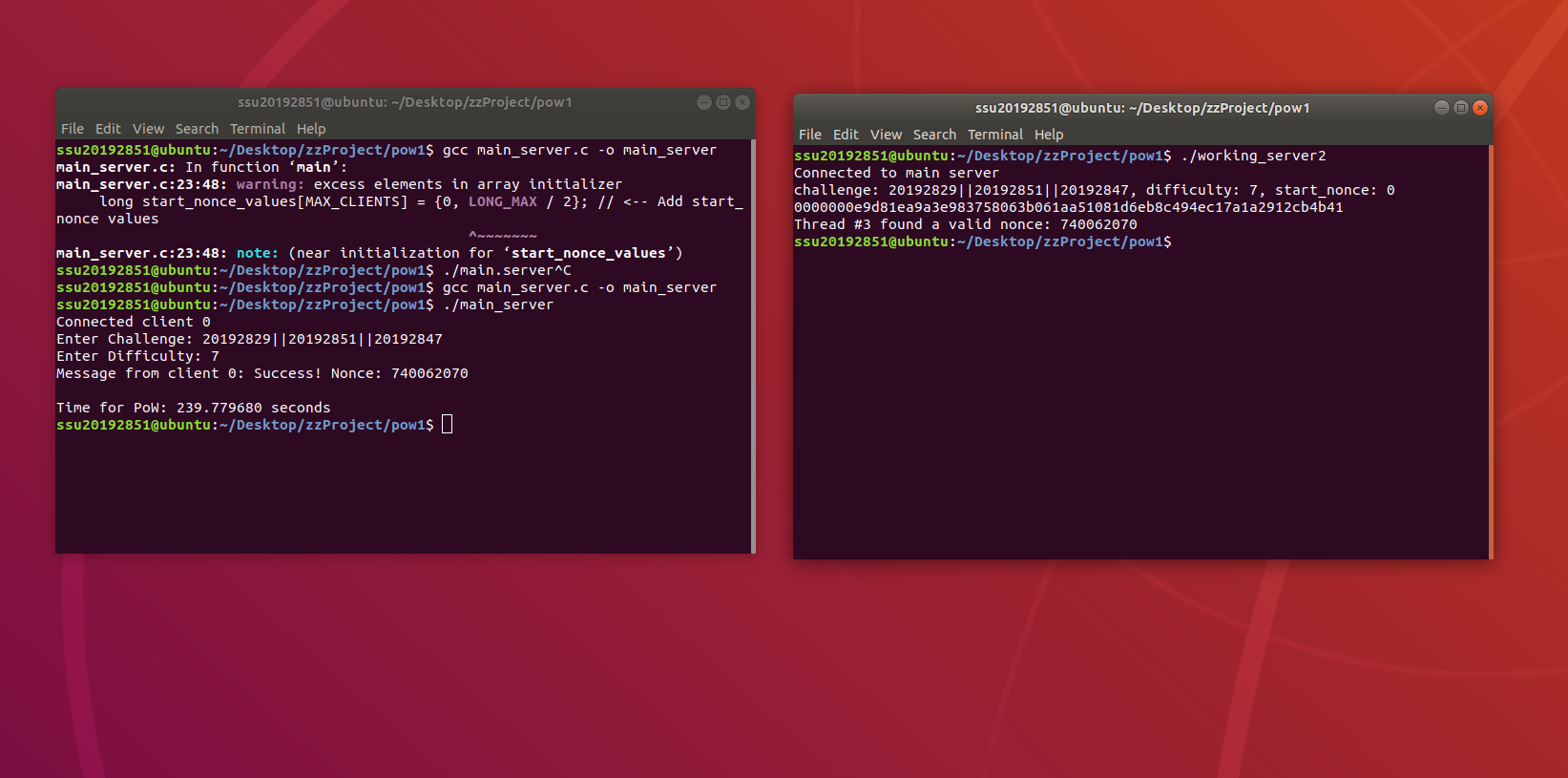
3.1.챌린지 학번 단독 실행 (난이도 7)

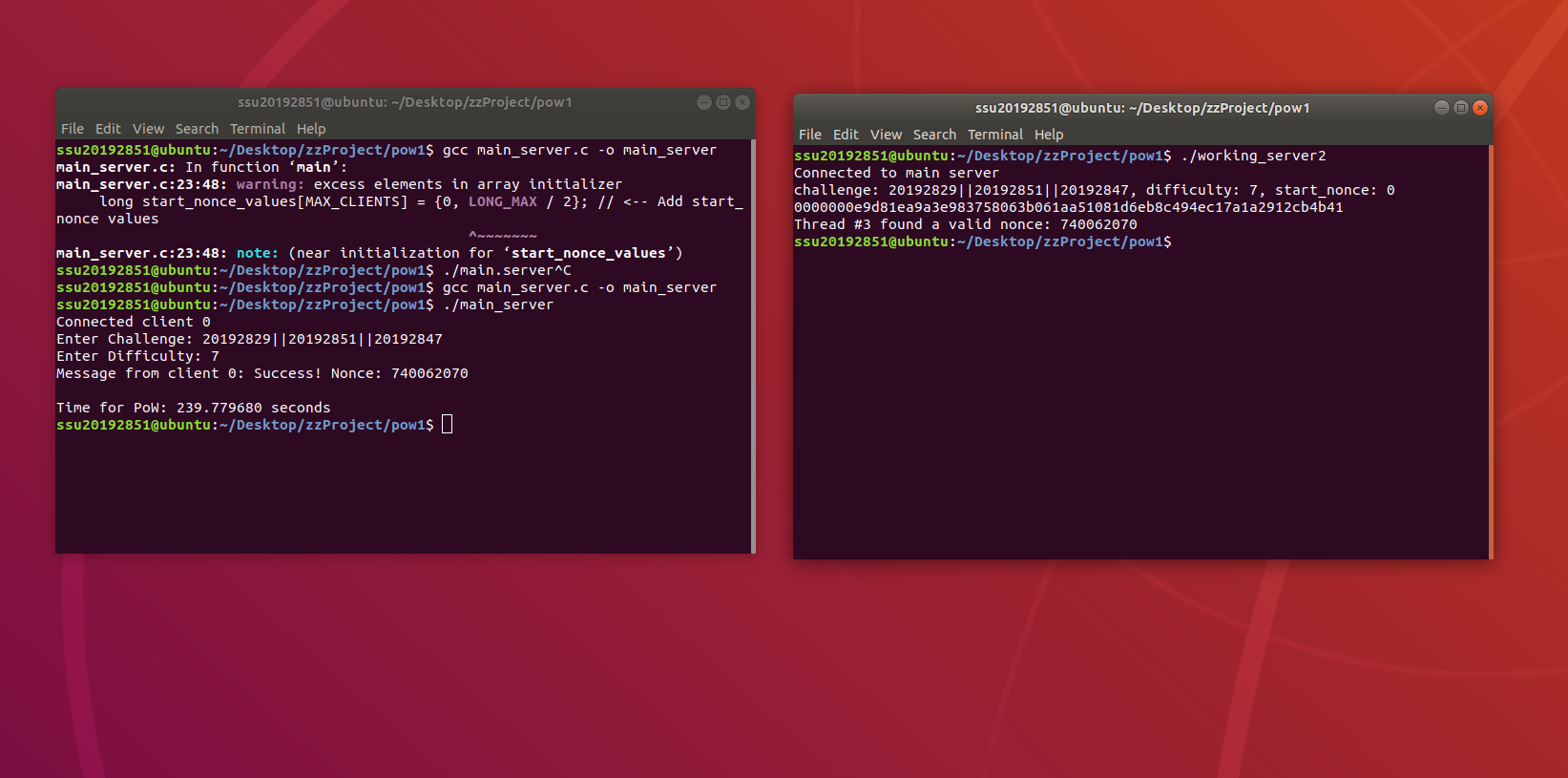
3.1.1. INPUT

* Challenge : 20192829||20192851||20192847
* 난이도 : 7

3.1.2. OUTPUT

* nonce: 740062070
* time: 239.779680초 = 3.996328분





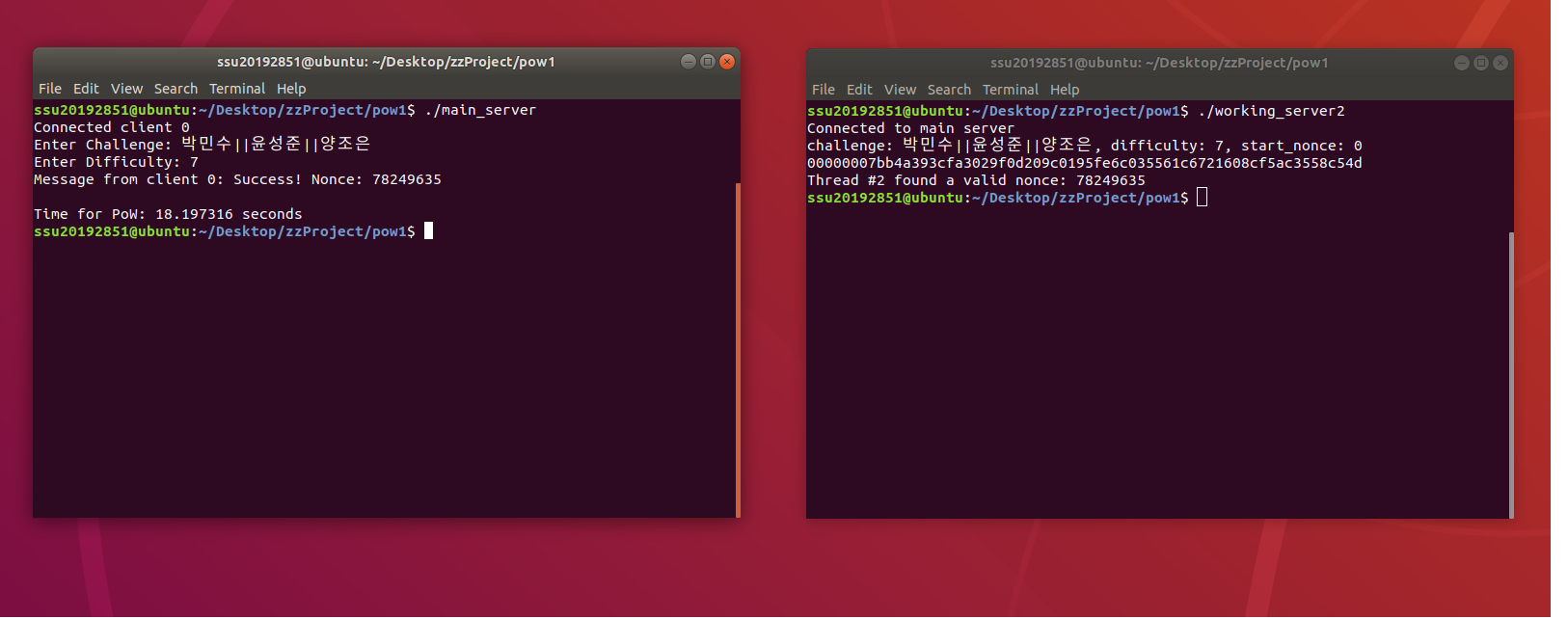
3.2. 챌린지 이름 단독 실행 (난이도 7)

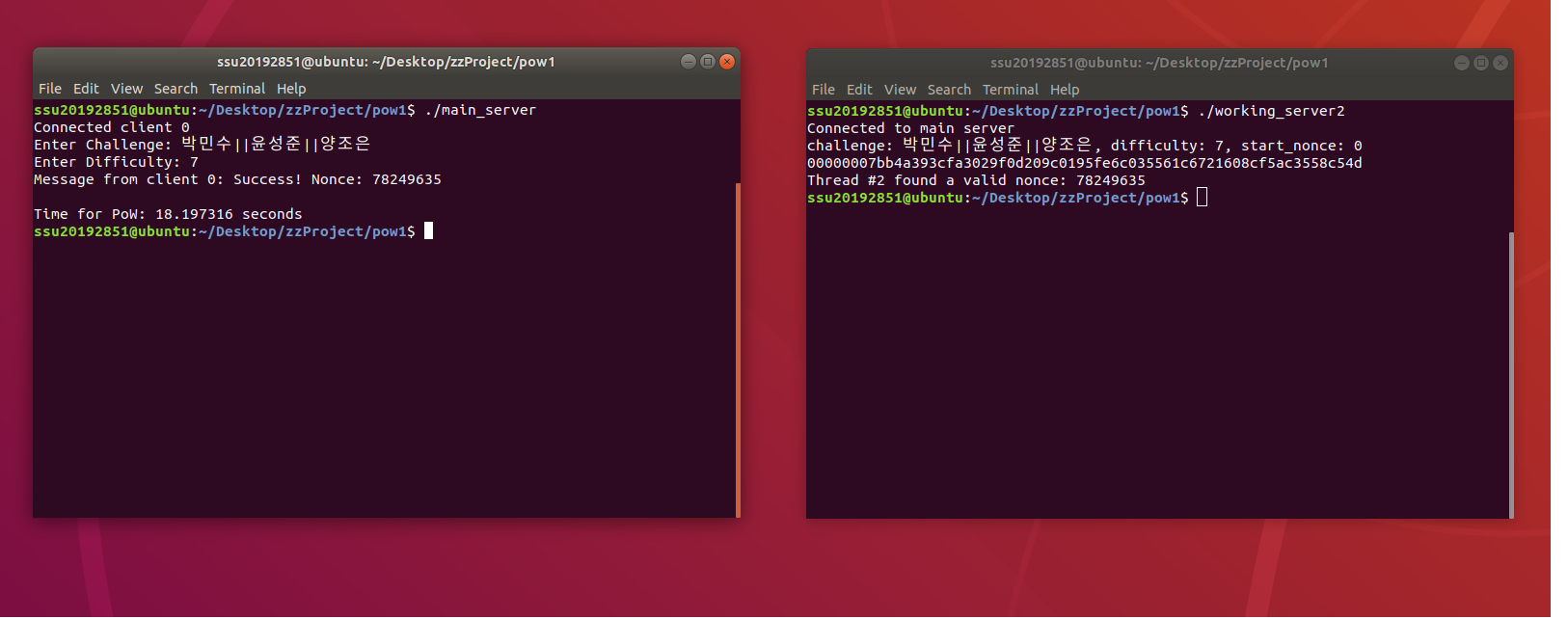
3.2.1. INPUT

* challenge: 박민수||윤성준||양조은
* time: 18.197316초

3.2.2. OUTPUT

* nonce: 78249635
* time: 18.197316초





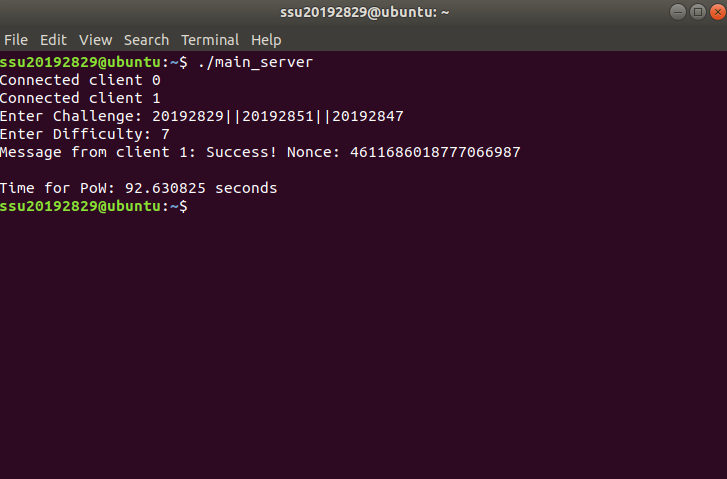
3.3.챌린지 학번 분산 실행 (난이도 7)

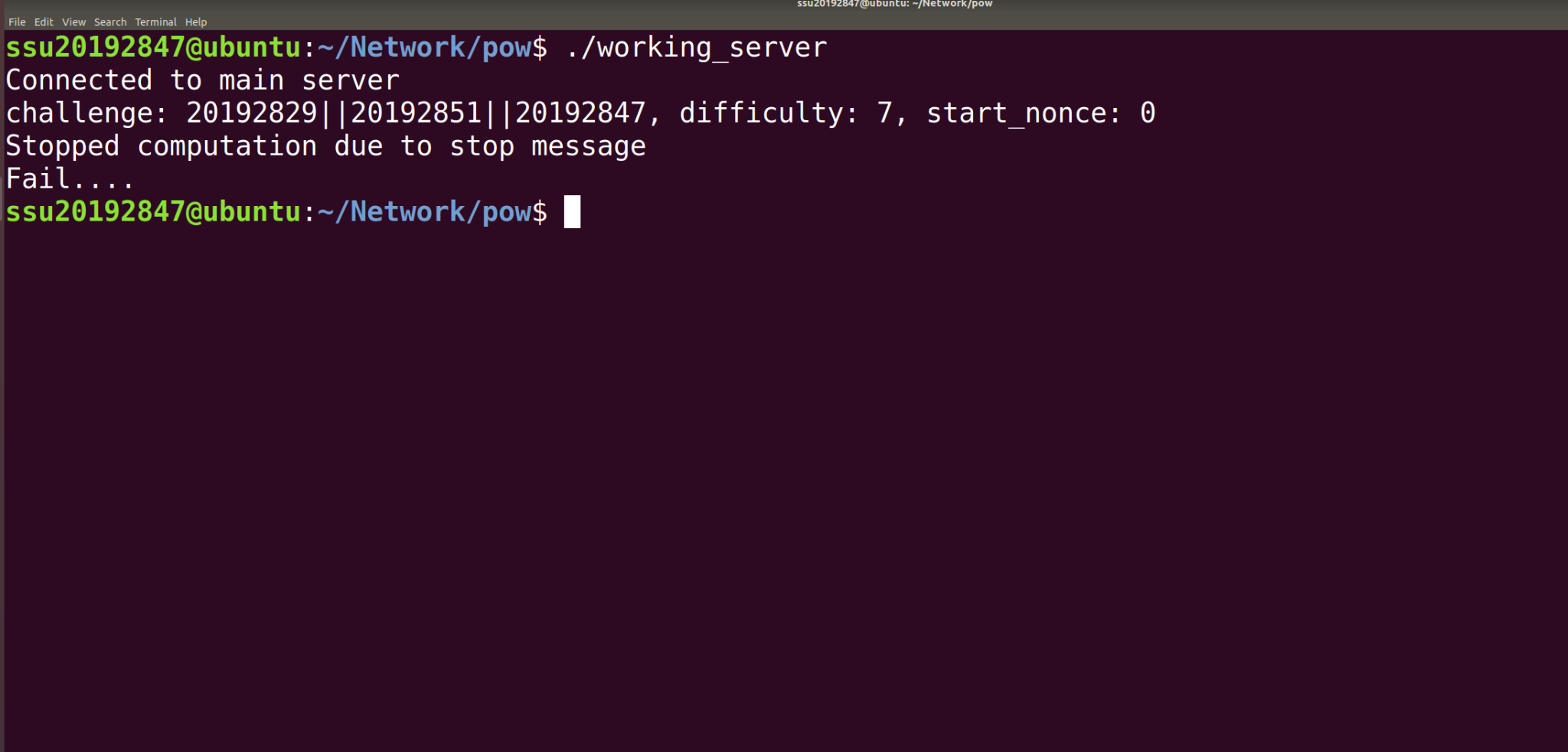
3.3.1. INPUT

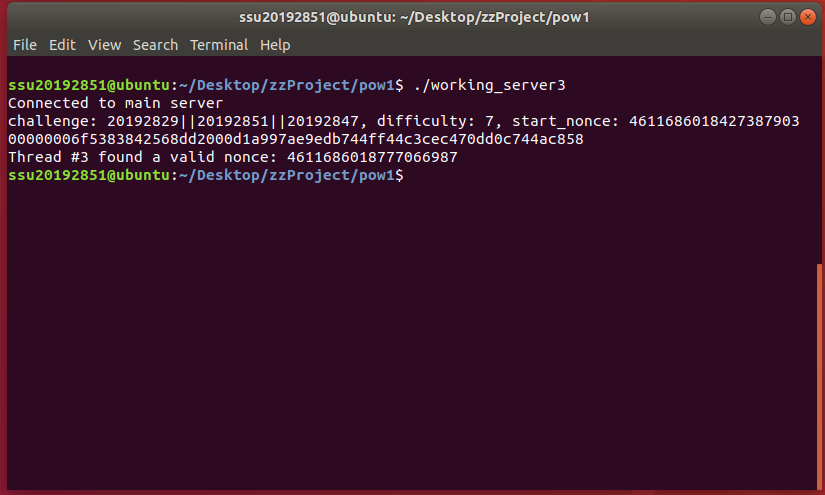
* Challenge : 20192829||20192851||20192847
* 업무분담 - Working Server 1 : 0 ~ 4,611,686,018,427,387,902
* 업무분담 - Working Server 2 : 4,611,686,018,427,387,903 ~
* 난이도 : 7

3.3.2. OUTPUT

* nonce: 4611686018777066987
* time: 92.630825초 = 1.54384708333분







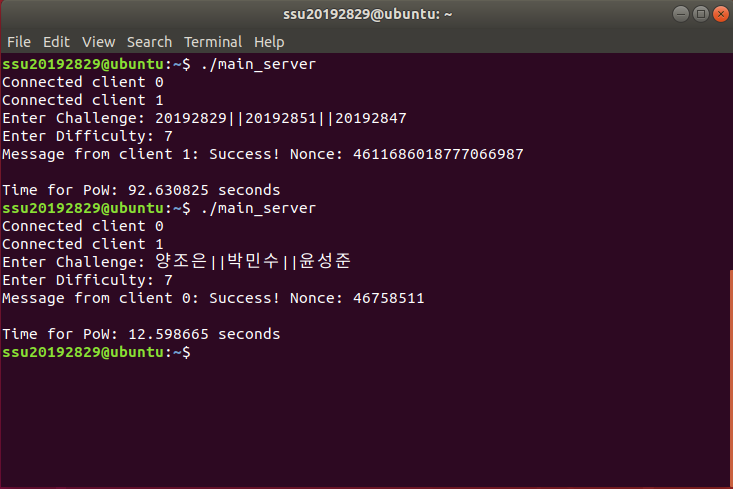
3.4. 챌린지 이름 분산 실행 (난이도 7)

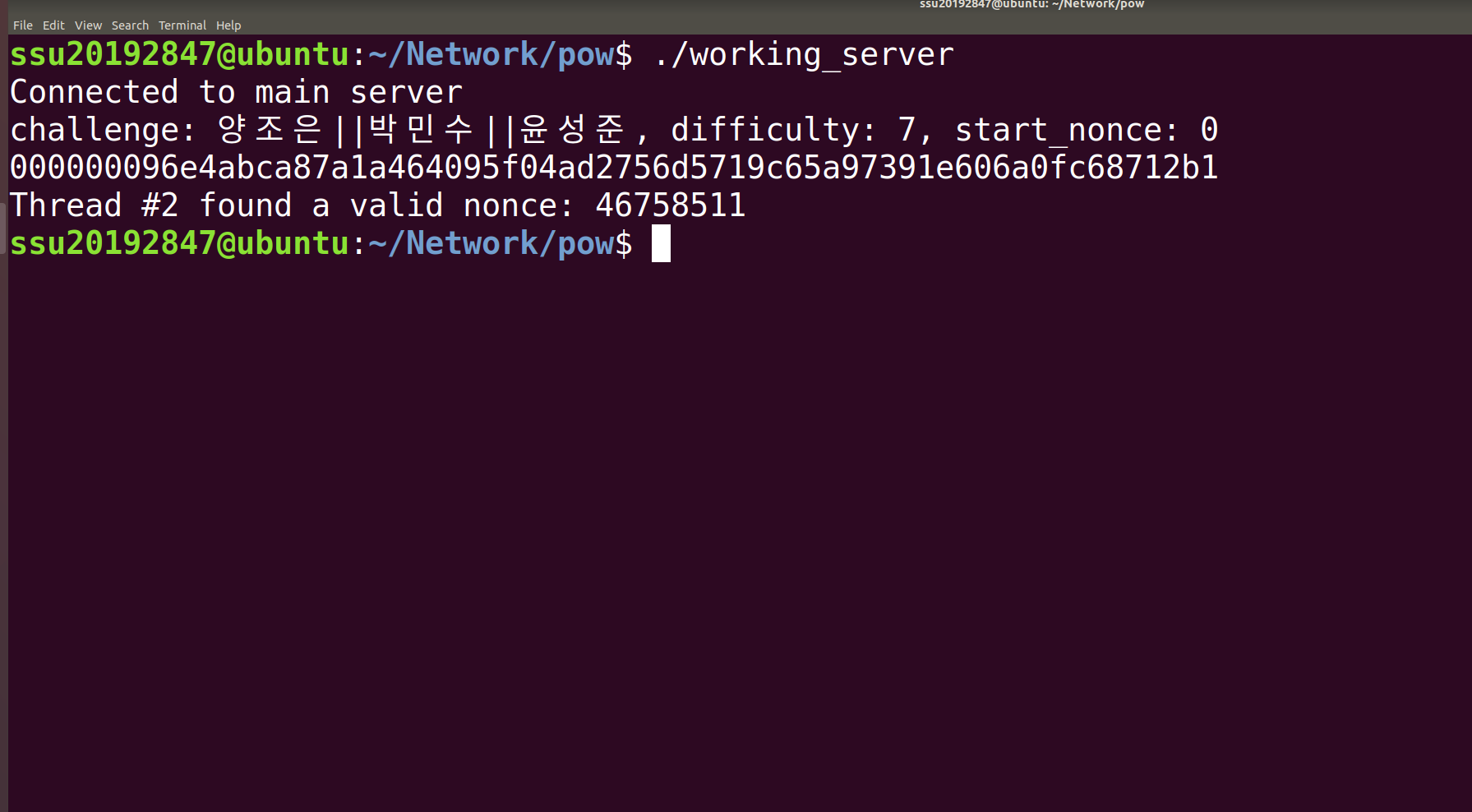
3.4.1. INPUT

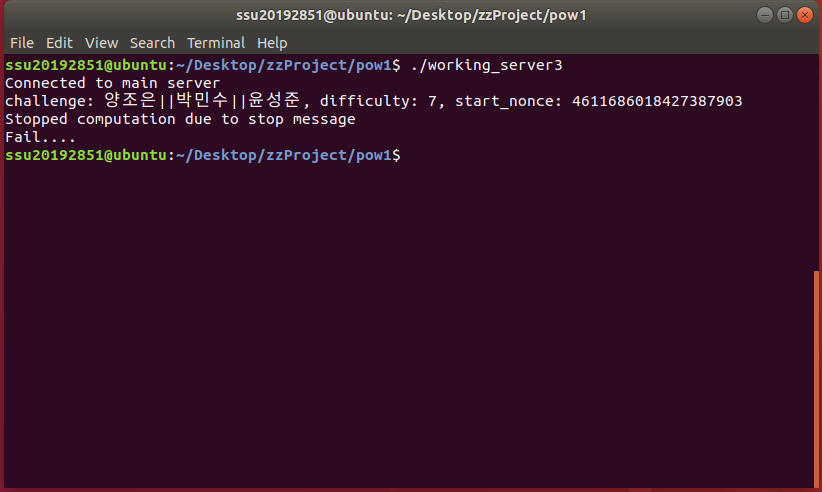
* Challenge : 박민수||윤성준||양조은
* 업무분담 - Working Server 1 : 0 ~ 4,611,686,018,427,387,902
* 업무분담 - Working Server 2 : 4,611,686,018,427,387,903 ~
* 난이도 : 8

3.4.2. OUTPUT

* nonce: 46758511
* time: 12.598665초







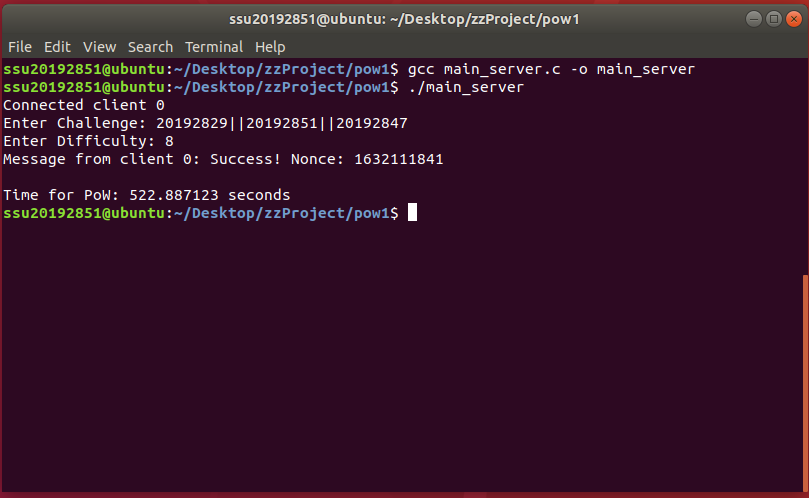
3.5. 챌린지 학번 단독 실행 (난이도 8)

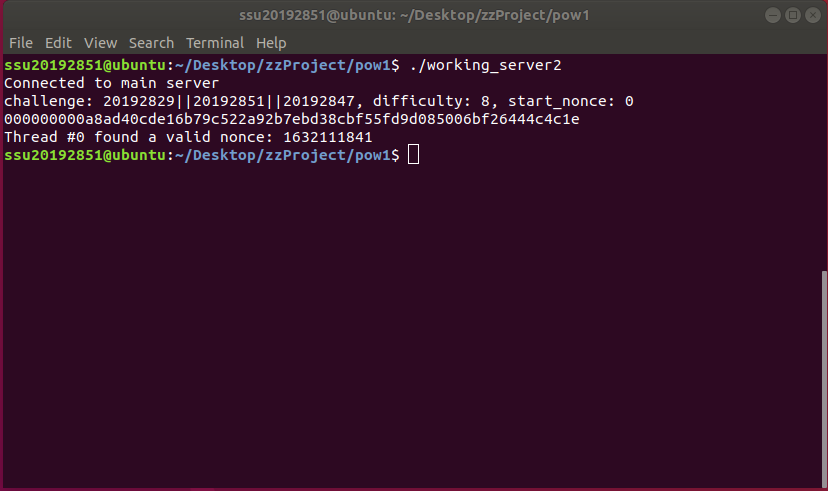
3.5.1. INPUT

* Challenge : 20192829||20192851||20192847
* 난이도 : 8

3.5.2. OUTPUT

* nonce: 1632111841
* time: 522.887123초 = 8.714785383333분





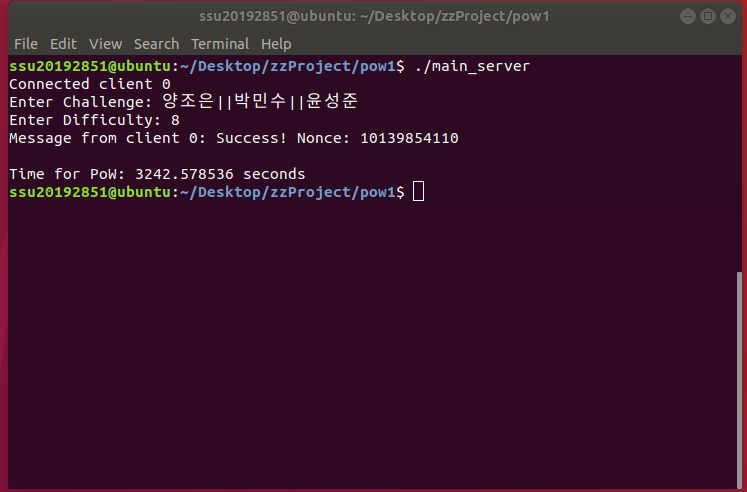
3.6. 챌린지 이름 단독 실행 (난이도 8)

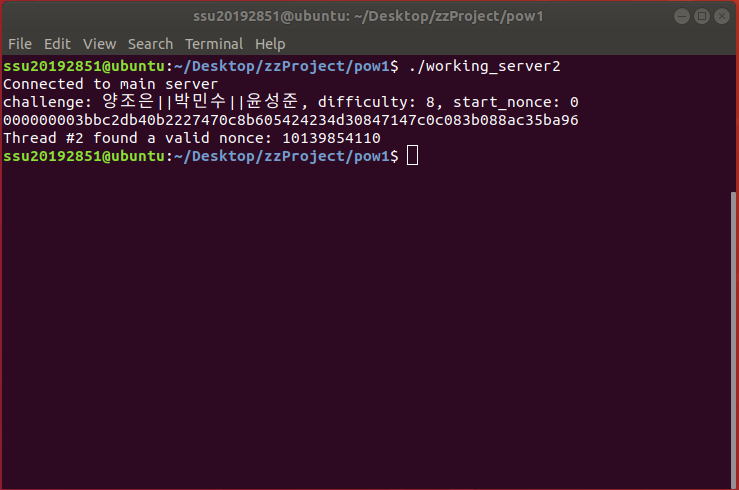
3.6.1. INPUT

* Challenge : 박민수||윤성준||양조은
* 난이도 : 8

3.6.2. OUTPUT

* nonce:
* time: 3242.578536초





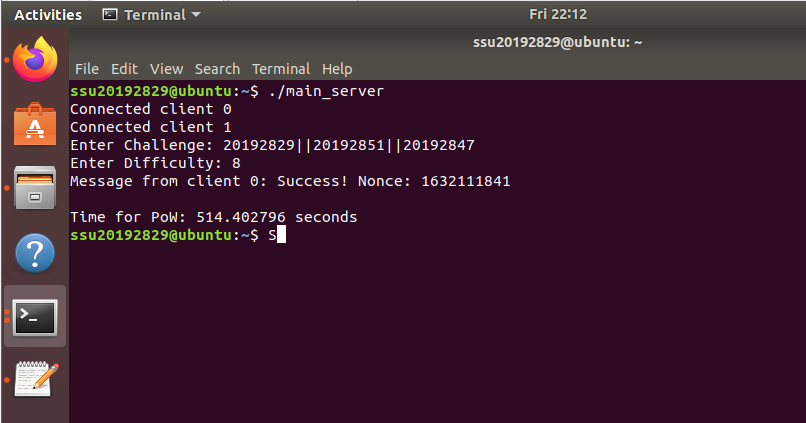
3.7. 챌린지 학번 분산 실행 (난이도 8)

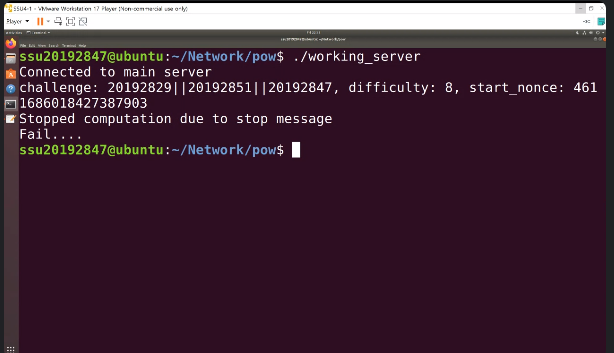
3.7.1. INPUT

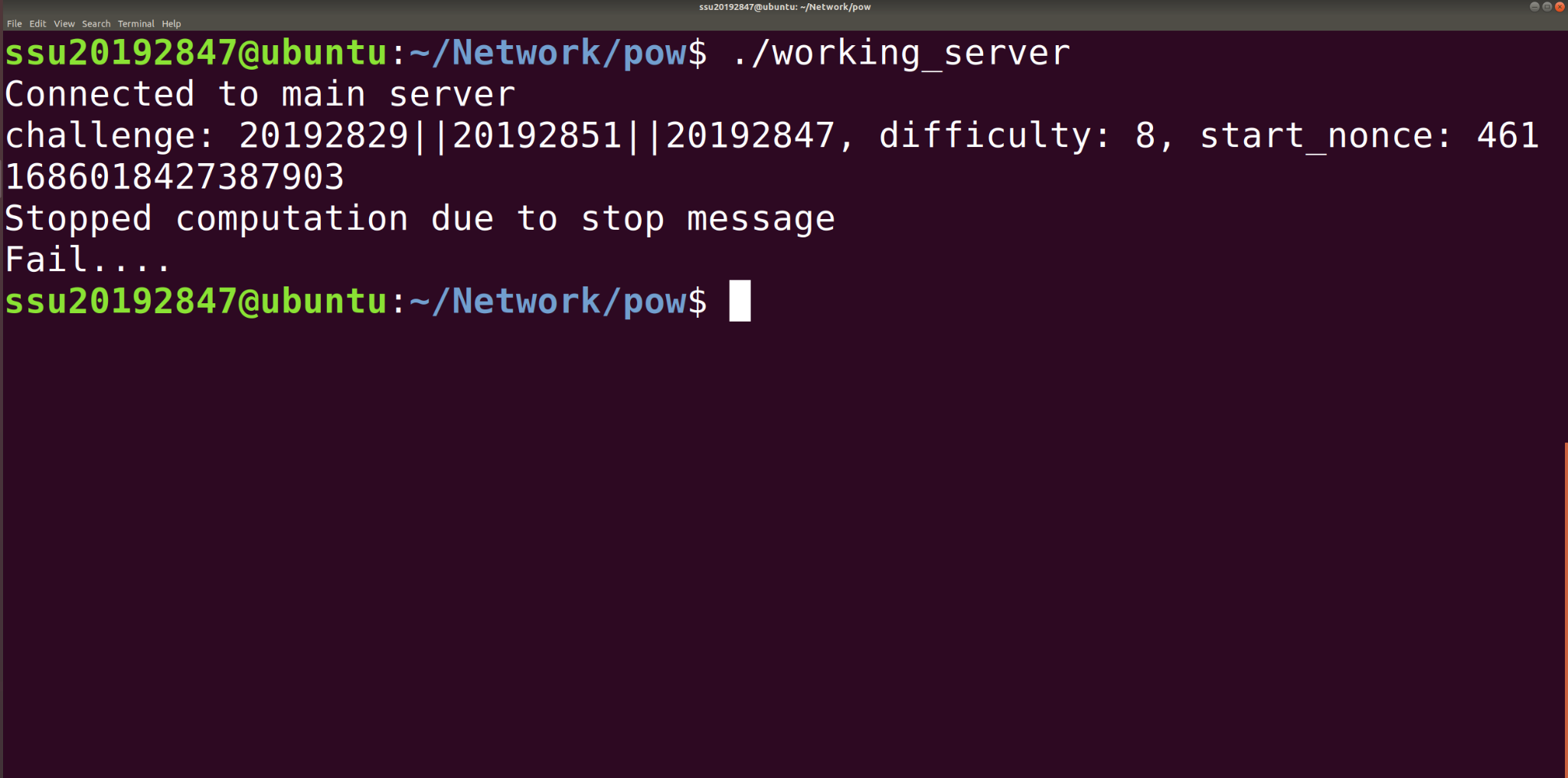
* Challenge : 20192829||20192851||20192847
* 업무분담 - Working Server 1 : 0
* 업무분담 - Working Server 2 : 4,611,686,018,427,387,903
* 난이도 : 8

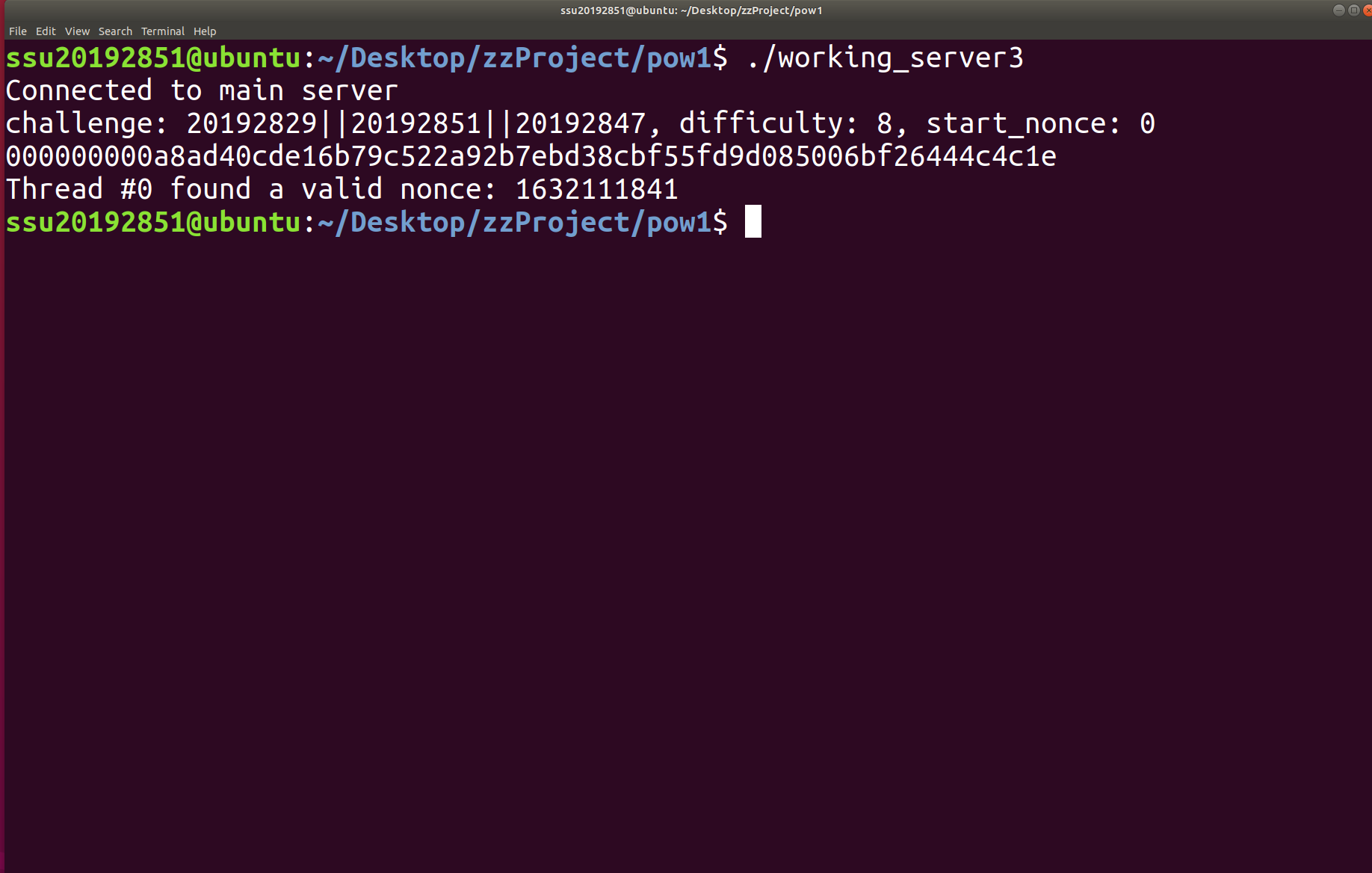
3.7.2. OUTPUT

* nonce: 1632111841
* time: 514.402796초









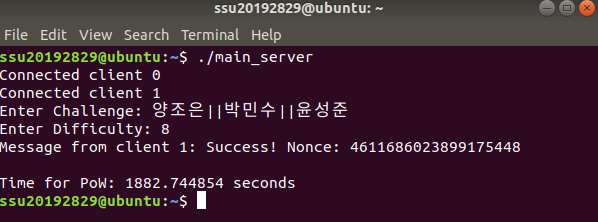
3.8. 챌린지 이름 분산 실행 (난이도 8)

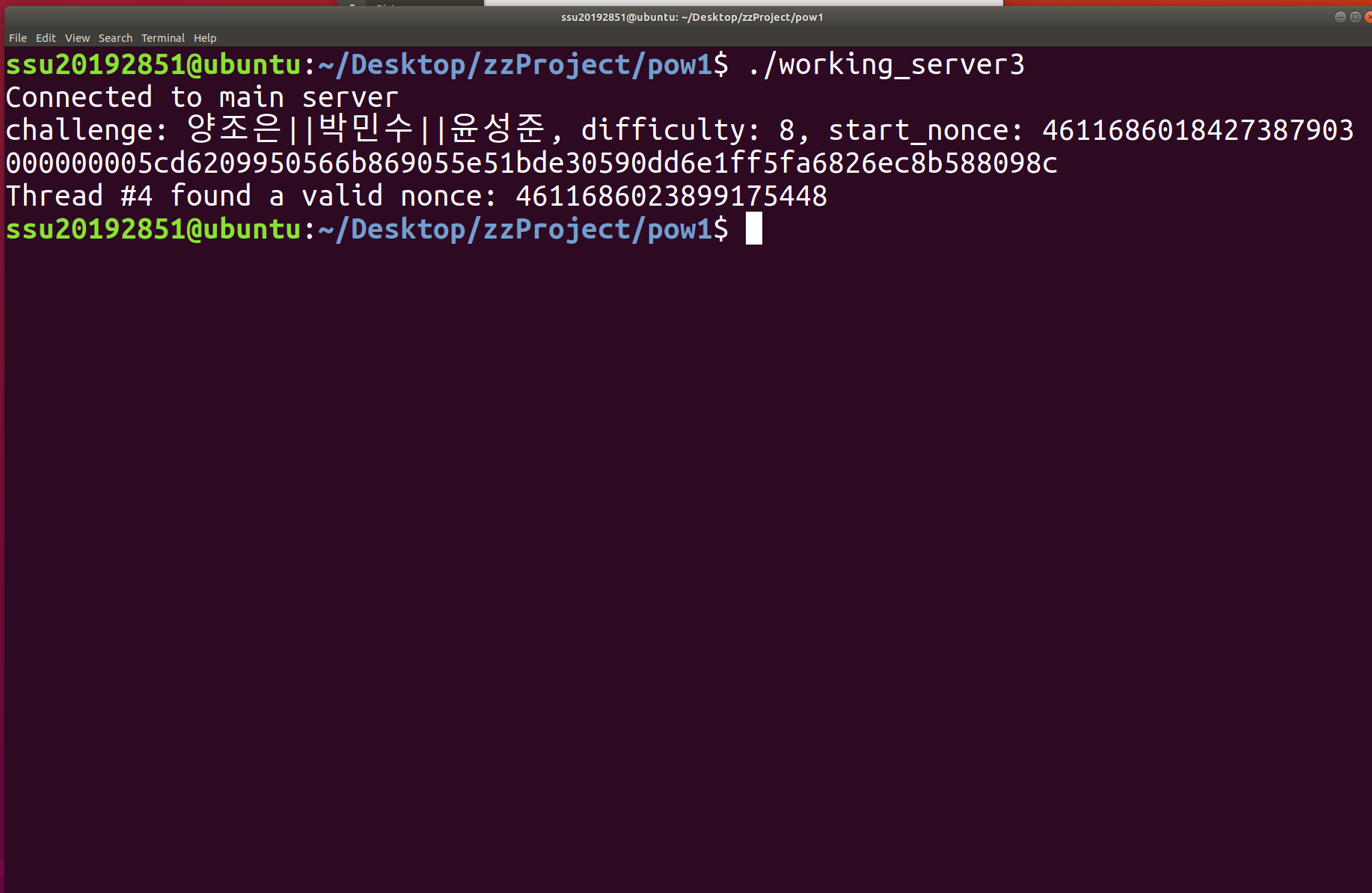
3.8.1. INPUT

* Challenge : 양조은||박민수||윤성준
* 업무분담 - Working Server 1 : 0 ~ 4,611,686,018,427,387,902
* 업무분담 - Working Server 2 : 4,611,686,018,427,387,903 ~
* 난이도 : 8

3.8.2. OUTPUT

* nonce: 4611686023899175448
* time: 1882.744854초 = 31.3790809분





1. **단독 실행 vs. 분산 실행**

아래 4.1, 4.2의 표는 각 챌린지, 난이도에 따른 단독 실행과 분산 실행의 실행시간을 보여준다. "단독 실행"은 하나의 working server만 사용하고 "분산 실행"은 여러 working server를 사용하는 시나리오를 나타낸다.

4.1. 난이도 7일 때의 실행시간 차이

|  |  |  |  |
| --- | --- | --- | --- |
| 난이도 7 | 단독 실행(초) | 분산 실행(초) | 실행 시간 비율  (분산/단독) |
| 학번 | 239.78 | 92.63 | 0.39 |
| 이름 | 18.20 | 12.60 | 0.69 |

학번 챌린지에서는 단독 실행 시 239.78초가 걸리는 반면, 분산 실행에서는 92.63초로 상당히 단축된 시간이 소요되었다. 실행 시간 비율은 0.39로, 분산 실행이 단독 실행에 비해 약 61% 단축하였다.

반면에 이름 챌린지에서는 단독 실행이 18.20초, 분산 실행이 12.60초로 이 경우에서도 분산 실행이 더 효율적이고 단독 실행에 비해 약 31% 단축하였다.

4.2. 난이도 8일 때의 실행시간 차이

|  |  |  |  |
| --- | --- | --- | --- |
| 난이도 8 | 단독 실행(초) | 분산 실행(초) | 실행 시간 비율  (분산/단독) |
| 학번 | 522.89 | 514.40 | 0.98 |
| 이름 | 3242.58 | 1882.74 | 0.58 |

학번 챌린지에서는 단독 실행 시 522.89초, 분산 실행 시 514.40초로 거의 비슷한 시간이 소요되었다. 실행 시간 비율은 0.98로 거의 동일하다.

이름 챌린지에서는 단독 실행 시간이 3242.58초, 분산 실행 시간이 1882.74초로 분산 실행이 단독 실행에 비해 시간을 많이 줄였다. 실행 시간 비율은 0.58로, 분산 실행이 단독 실행에 비해 약 42%의 시간을 절약하였다.

결론적으로 비슷한 환경이라는 가정 하에서 분산 실행이 일반적으로 더 빠르다. 하지만 하드웨어 성능의 차이 등으로 무조건 분산 실행이 더 빠른 결과가 나오지는 않았다. 예를 들어 난이도 8 과 같은 경우 똑같은 nonce값을 같은 working server가 찾기 때문에 분산실행과 단독실행의 실행 시간 비율이 1에 가깝다.

1. **Port Forwarding**

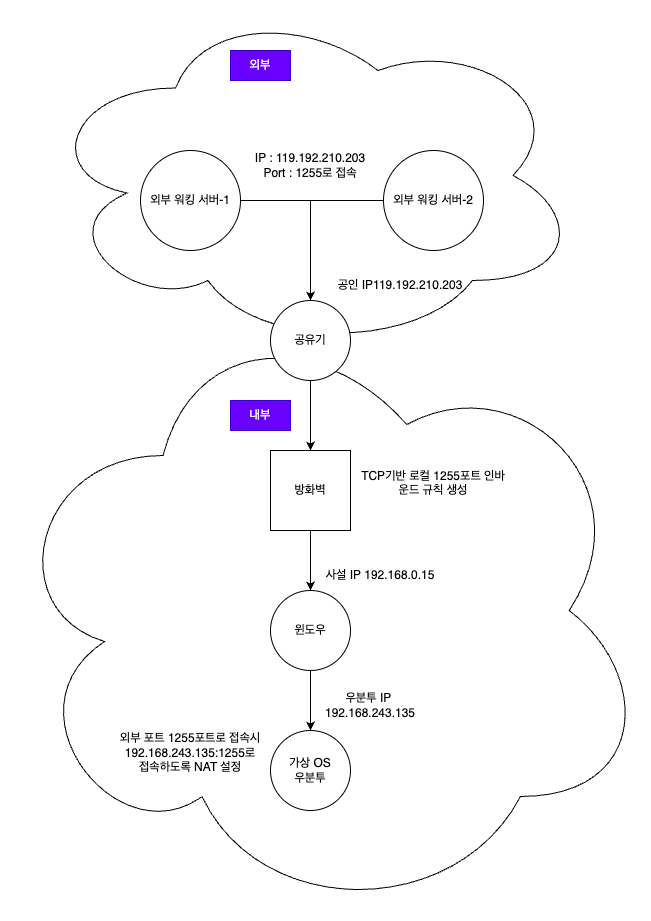
****

그림5.1. Port Forwarding Diagram

해당 그림5.1을 보면 외부 네트워크 영역에 있는 워킹 서버 두 대가 공인 IP 119.192.210.203과 1255 포트 번호로 접속하게 된다. 그러면, 그림5.2 공유기 포트 포워드 설정에서 ‘NAT/라우터 관리’->’포트 포워드 설정’ 카테고리에서 외부 포트 1255으로 들어오면 그림 5.3 윈도우 내부 IP주소로 AP로부터 할당받은 IP, 192.168.0.15와 1255 Port로 포트 포워딩이 되도록 설정한다. 그리고 그 포트가 윈도우 내부까지 들어올 수 있도록, 그림5.4 방화벽 인바운드 포트 규칙으로 TCP 기반으로 특정 로컬 포트인 1255포트를 허용하도록 한다. 그림5.5 가상 OS - Network Adapter에서 우분투 OS 가상 머신을 돌리고 있는 프로그램 ‘VMware’에 해당 가상 머신의 Network Adapter의 Network connection을 Custom 및 NAT을 지원하는 VMnet8(NAT)으로 설정한다. 그다음, 그림5.6. VMware NAT Settings를 보면 Host Port인 1255포트로 접근한다면, 현재 실행 중인 Virtual Machine IP address로 192.168.243.135, Port 1255로 NAT이 되도록 설정하였다. 이에 따른 결과로 그림5.7 VMware Virtual Network Editor가 설정된 것을 볼 수 있고, 최종적으로 외부 Working\_server 두 대가 1255포트로 접근 시 내부에 실행 중인 가상 머신 우분투 OS의 IP, 192.168.243.135 및 1255 Port로 포트 포워딩 되어서 Main\_Server 소켓에 붙도록 설정하였다.

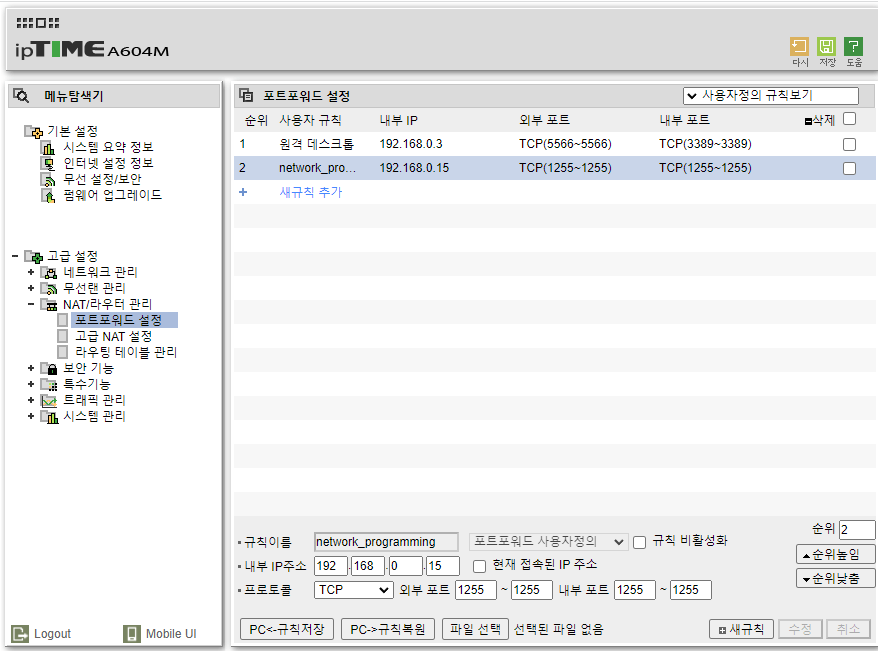
****

그림5.2. 공유기 포트포워드 설정

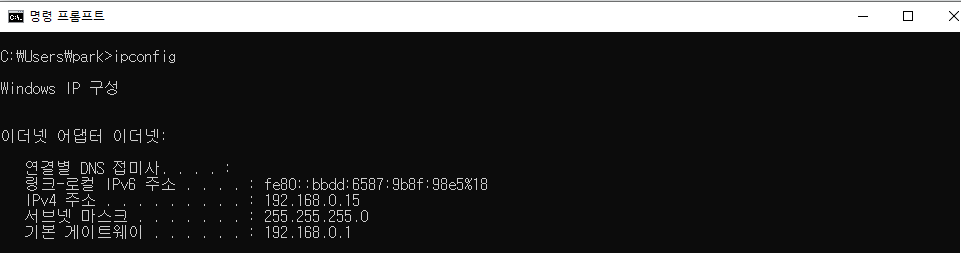


그림5.3. 윈도우 내부 IP주소

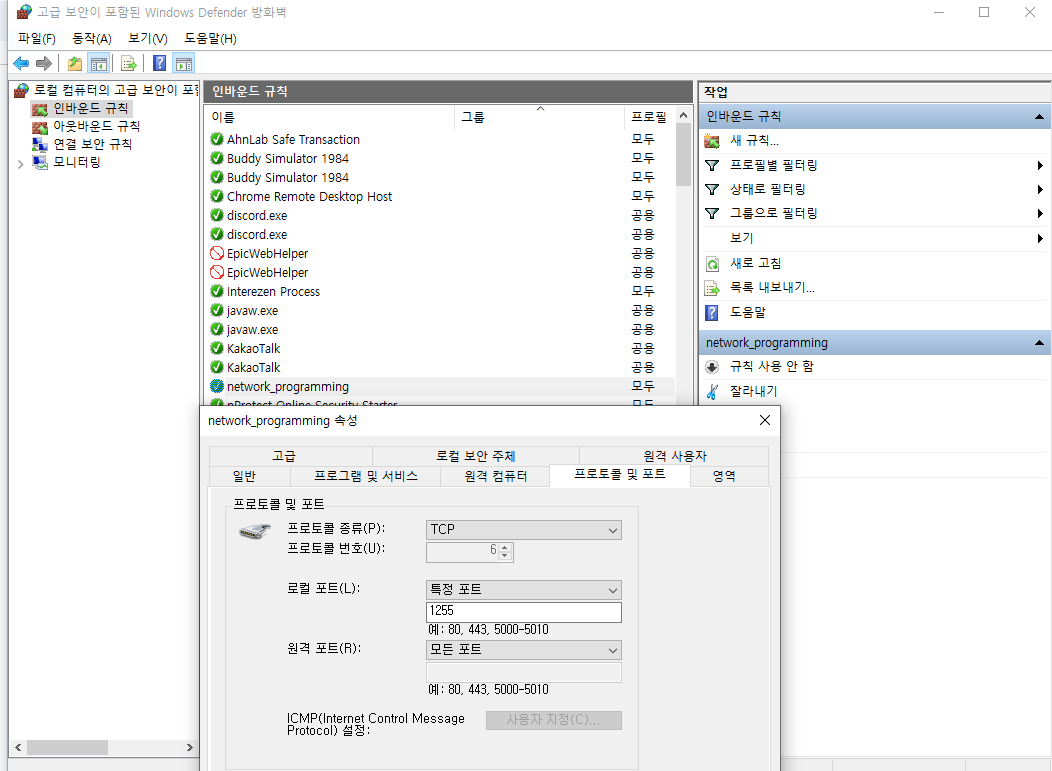
****

그림5.4. 방화벽 인바운드 포트 규칙

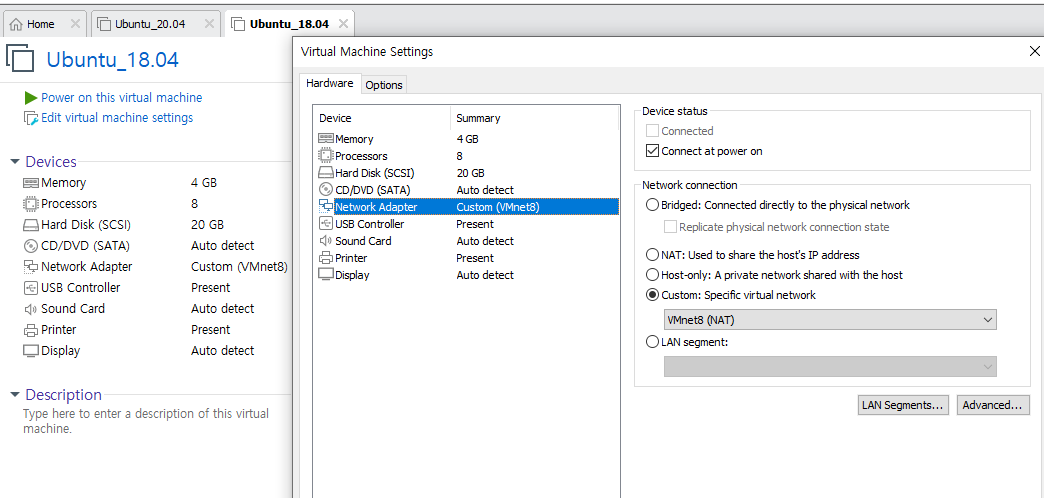


그림5.5. 가상 OS - Network Adapter

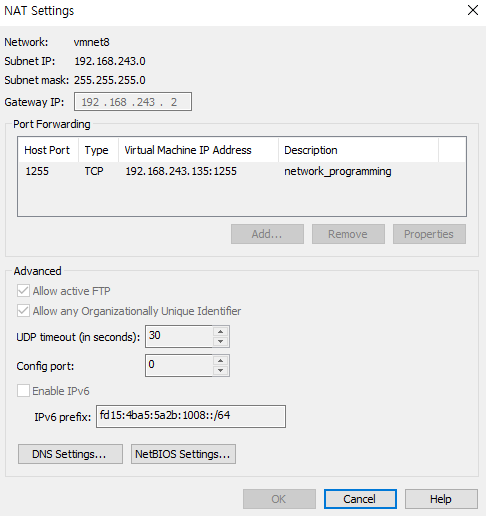
****

그림5.6. VMware NAT Settings

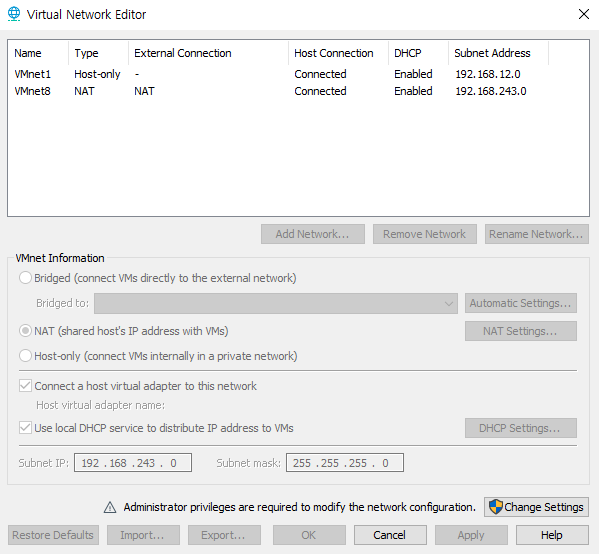
****

그림5.7. VMware Virtual Network Editor

1. **프로젝트 회고**

프로젝트를 작성하며, 어려웠던 점으로 초기 프로그램 작성 시 MAX\_nonce 값을 정해서 프로그램을 수행했다. 그러나 생각한 것보다 난이도가 올라갈수록 우리가 설정한 MAX\_nonce 값의 범위를 훨씬 초과했다. 그래서 MAX\_nonce 값을 제거하여 각 Working\_Server는 무한대를 향해 nonce 값을 찾도록 수행하는 코드를 바꿨다. 또한, 업무 분담 명세 내용을 진행하며 Main\_Server에서 Working\_Server마다 시작 탐색 nonce 값을 보내줄 때 1번 Working\_Server는 0부터 시작하기 때문에 문제가 없지만, 2번 Working\_Server에 보내 줄 시작 탐색 nonce 값을 정하는 과정에서 최적의 시작 탐색 nonce 값을 정하는 것과 각 Working\_Server마다 5개의 Threads가 한 번에 Thread가 담당할 nonce 값 범위를 몇으로 정해야지 훨씬 더 빠르게 찾을 수 있을지 고민하는 과정에서 많은 시간을 소비했었다. 그리고 프로그램 작성을 끝내 프로그램 실행 중에 정답과 ‘print\_hash()’ 함수를 통해 해시값과 정답이 뒤섞여서 나왔었다. 이 문제를 해결하려 노력하던 중, ‘print\_hash()’ 함수의 수행 속도가 너무 느리다고 생각해, 기존 ‘print\_hash()’ 함수는 ‘if (is\_valid(hash, difficulty))’에서 IF 문 바깥에 위치하여 정답을 찾았을 때뿐만 아니라 항상 해당 함수를 호출하도록 했으나, IF 문 안쪽으로 바꿔서 정답을 찾았을 때만 ‘print\_hash()’ 함수를 실행되도록 변경하여 해결했다. 해당 지정 주제 프로젝트를 수행하면서 블록체인 관련 주제와 한 학기 동안 배운 소켓 프로그래밍을 연관 지어 프로젝트를 해볼 기회가 있어 좋았다.