동아리방에 지금 누가 있나요?

Who is in the club room?

Freeradius부터 ARP Scanner까지

From Freeradius to ARP Scanner

발표자 소개 Speaker Information

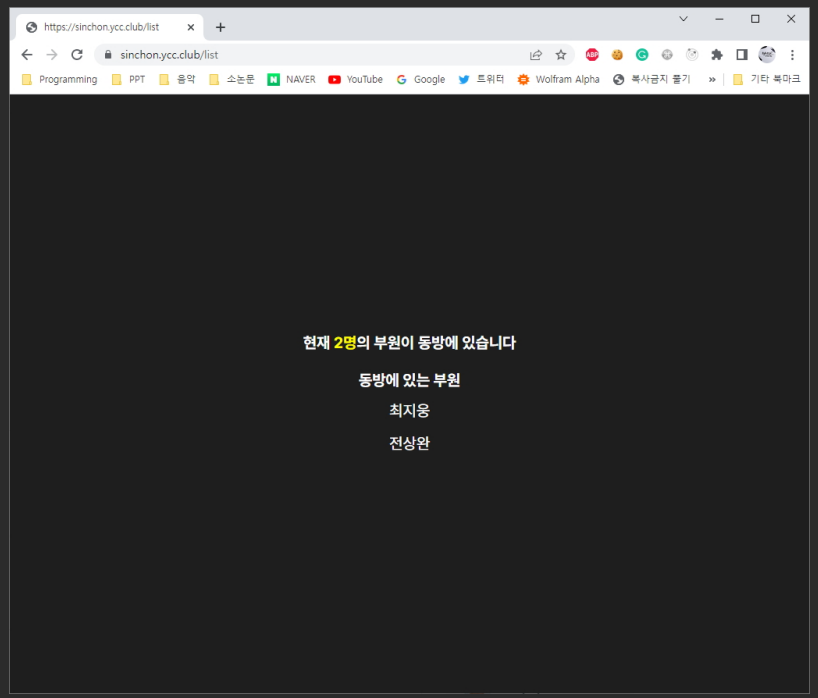
전상완 Sangwan Jeon

- 연세대학교 전기전자공학부 학부생
- YCC (Yonsei Computer Club) 임원진

Q&A

maxswjeon@codingbear.kr
maxswjeon
maxswjeon
maxswjeon
https://blog.codingbear.kr

발표 주제 Presentation Topic



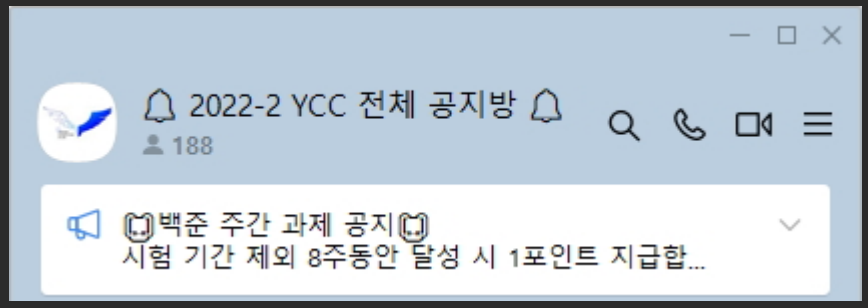
1. 동아리방에 있는 WiFi에 802.1x을 적용하는 방법
2. WiFi를 이용해 동아리방에 누가 있는지
   실시간으로 확인할 수 있는 서비스를 구축하는 방법

1. Applying 802.1x to the WiFi in the club room
2. Making a service that can check
   who is in the club room in real time using WiFi

그런게 왜 필요했는데?

Why did you need a such a thing?

Reason 1

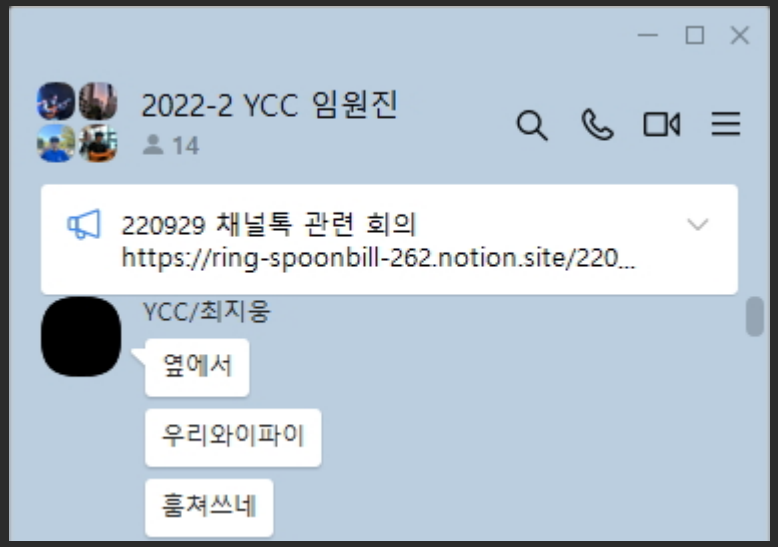


회원수 188명의 대형 동아리

그런게 왜 필요했는데?

Why did you need a such a thing?

Reason 1

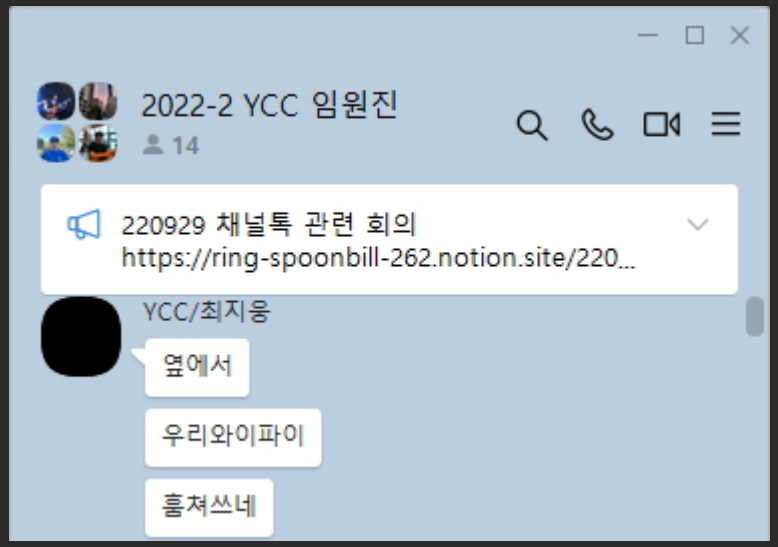


비밀번호 유출 사건의 발생

그런게 왜 필요했는데?

Why did you need a such a thing?

Reason 1



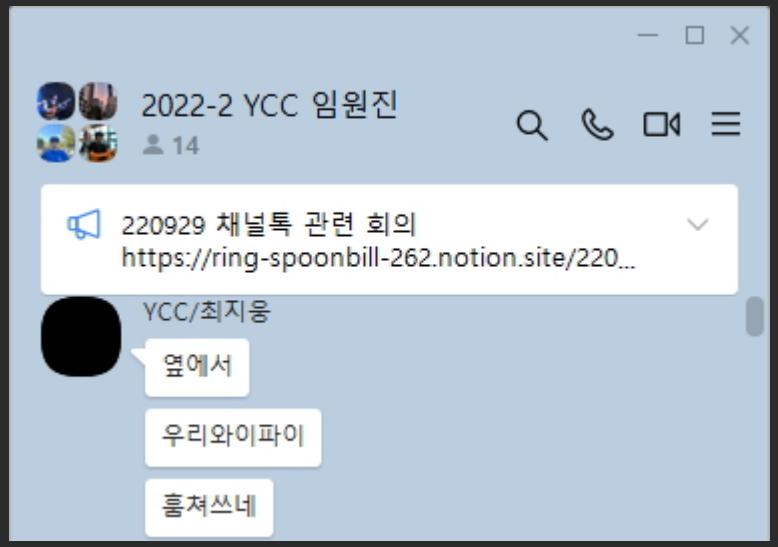
비밀번호 유출 사건의 발생

⇒ 주기적으로 비밀번호를 바꾸는 방법

그런게 왜 필요했는데?

Why did you need a such a thing?

Reason 1



비밀번호 유출 사건의 발생

⇒ 주기적으로 비밀번호를 바꾸는 방법

⇒ 아니면, 부원마다 다른 비밀번호를?

그런게 왜 필요했는데?

Why did you need a such a thing?

Reason 2

오후 12:16 지금 동방에 누구누구있어요?

YCC/양나진

동방에 누구 있나요? 오후 3:49

YCC/현시은

동방에 누구있음 1 오후 2:42

YCC/강은혁

동방에 누구 있나요 오후 6:27

YCC/박문수

동방누구있나여 오후 5:08

반복되는 질문

비밀번호 유출 문제 해결하기

Solving the password leak problem

해결 방법들 Solutions

1. 주기적으로 비밀번호를 바꾼다

해결 방법들 Solutions

1. ~~주기적으로 비밀번호를 바꾼다~~

해결 방법들 Solutions

1. ~~주기적으로 비밀번호를 바꾼다~~
2. 부원마다 다른 비밀번호를 부여한다

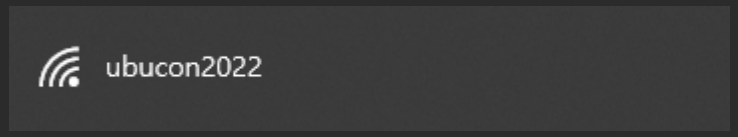
WiFi 인증 방식

WiFi Authentication Methods

WiFi 인증 방식

WiFi Authentication Methods

Open



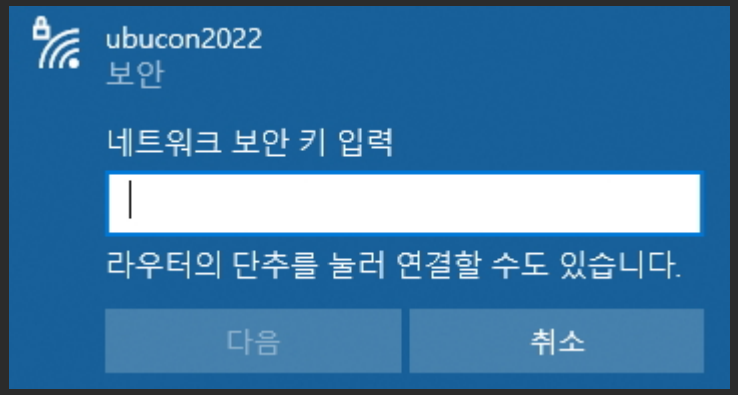
비밀번호가 없는 WiFi

- 누구나 접속 가능

WiFi 인증 방식

WiFi Authentication Methods

PSK (Pre-Shared Key)



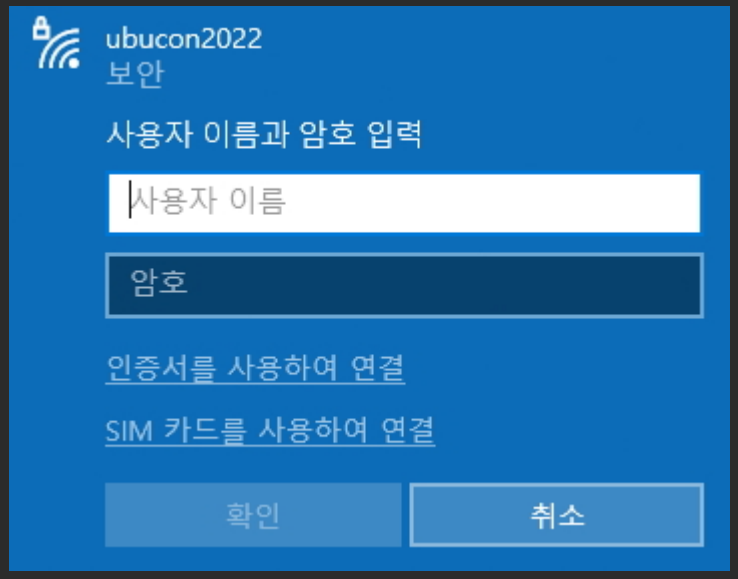
비밀번호가 있는 WiFi

- 비밀번호를 알면 접속 가능
- 비밀번호 유출 시 제지할 수 있는 수단이 없음

WiFi 인증 방식

WiFi Authentication Methods

EAP (Extensible Authentication Protocol)

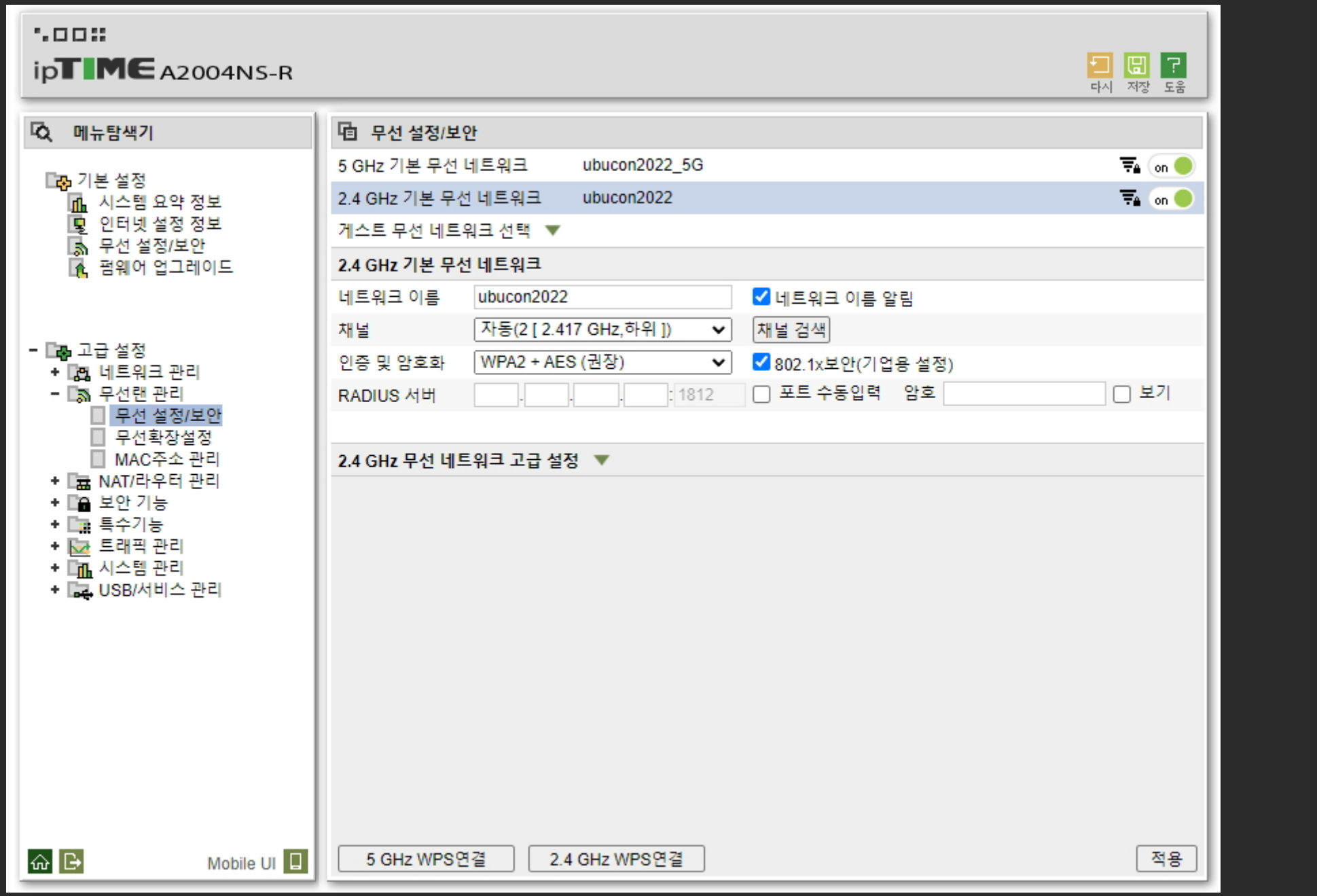


로그인 방식의 WiFi

- 개인에게 할당된 비밀번호가 다름
- 비밀번호 유출 시 제지할 수 있는 수단이 있음

802.1x

로컬 영역 네트워크에서 상대 기기와 연결하는 기기에 대한 인증을 제공하는 방식을 정의한 표준


ipTIME A2004NS-R
다시
저장
도움
메뉴탐색기
기본 설정
시스템 요약 정보
인터넷 설정 정보
무선 설정/보안
펌웨어 업그레이드
고급 설정
네트워크 관리
무선랜 관리
무선 설정/보안
무선확장설정
MAC주소 관리
NAT/라우터 관리
보안 기능
특수기능
트래픽 관리
시스템 관리
USB/서비스 관리
Mobile UI
무선 설정/보안
5 GHz 기본 무선 네트워크
ubucon2022_5G
on
2.4 GHz 기본 무선 네트워크
ubucon2022
on
게스트 무선 네트워크 선택
2.4 GHz 기본 무선 네트워크
네트워크 이름
ubucon2022
네트워크 이름 알림
채널
자동(2 [2.417 GHz,하위])
채널 검색
인증 및 암호화
WPA2 + AES (권장)
802.1x보안(기업용 설정)
RADIUS 서버
1812
포트 수동입력
암호
보기
2.4 GHz 무선 네트워크 고급 설정
5 GHz WPS연결
2.4 GHz WPS연결
적용

RADIUS?

RADIUS?

Remote Authentication Dial In User Service

RADIUS?

Remote Authentication Dial In User Service

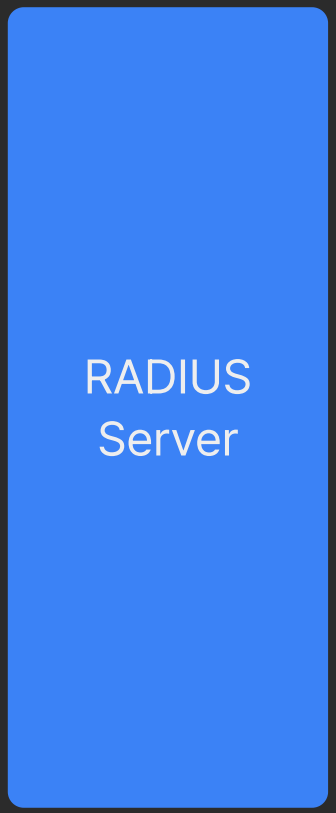
네트워크 자원에 대한 접근을 인증(Authenticate)하고 허가(Authorize)하며 관리(Accounting)

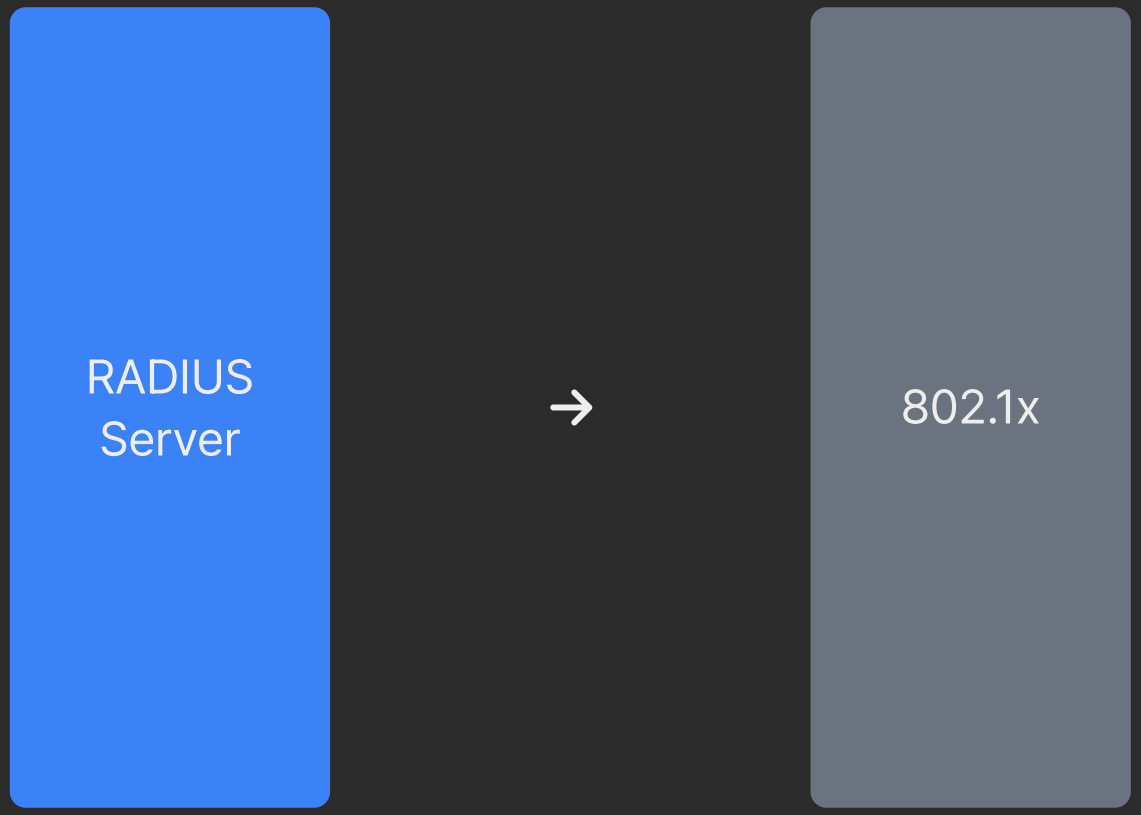
RADIUS?

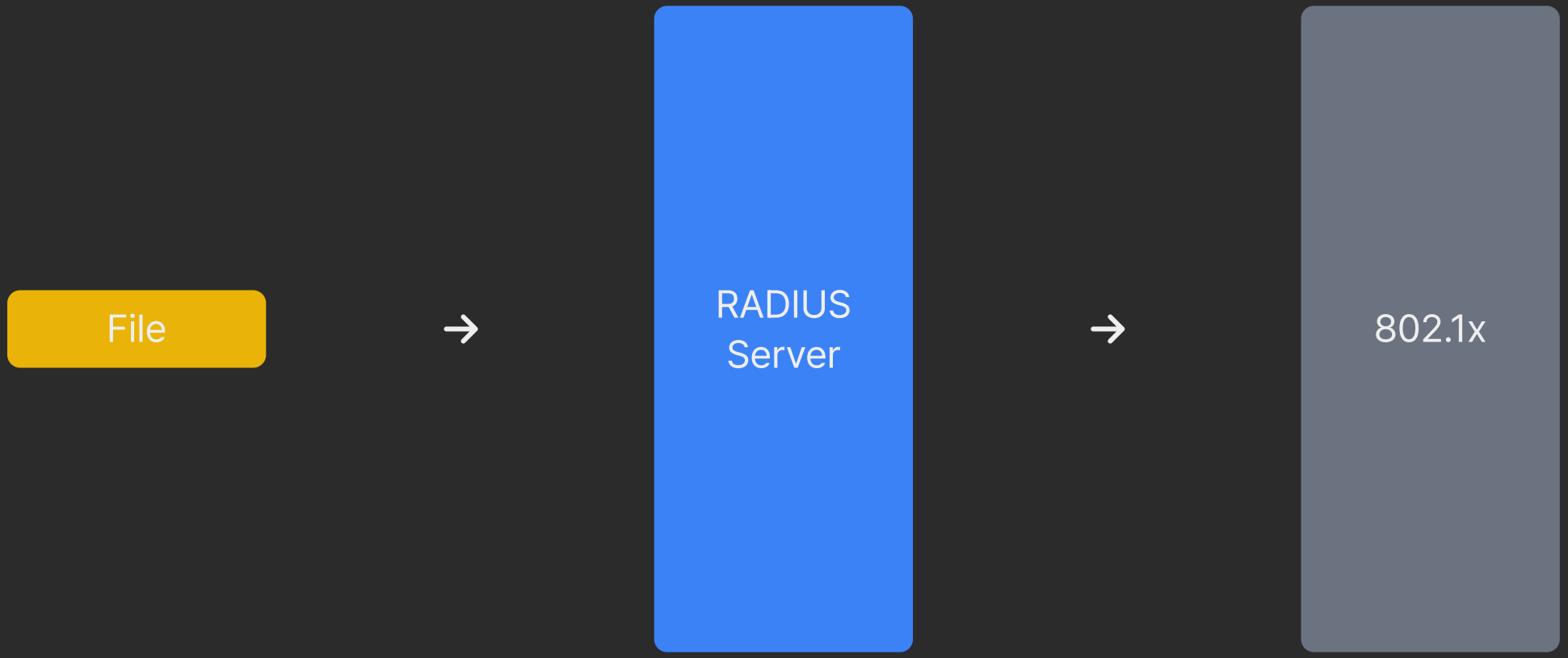
Remote Authentication Dial In User Service

네트워크 자원에 대한 접근을 인증(Authenticate)하고 허가(Authorize)하며 관리(Accounting)

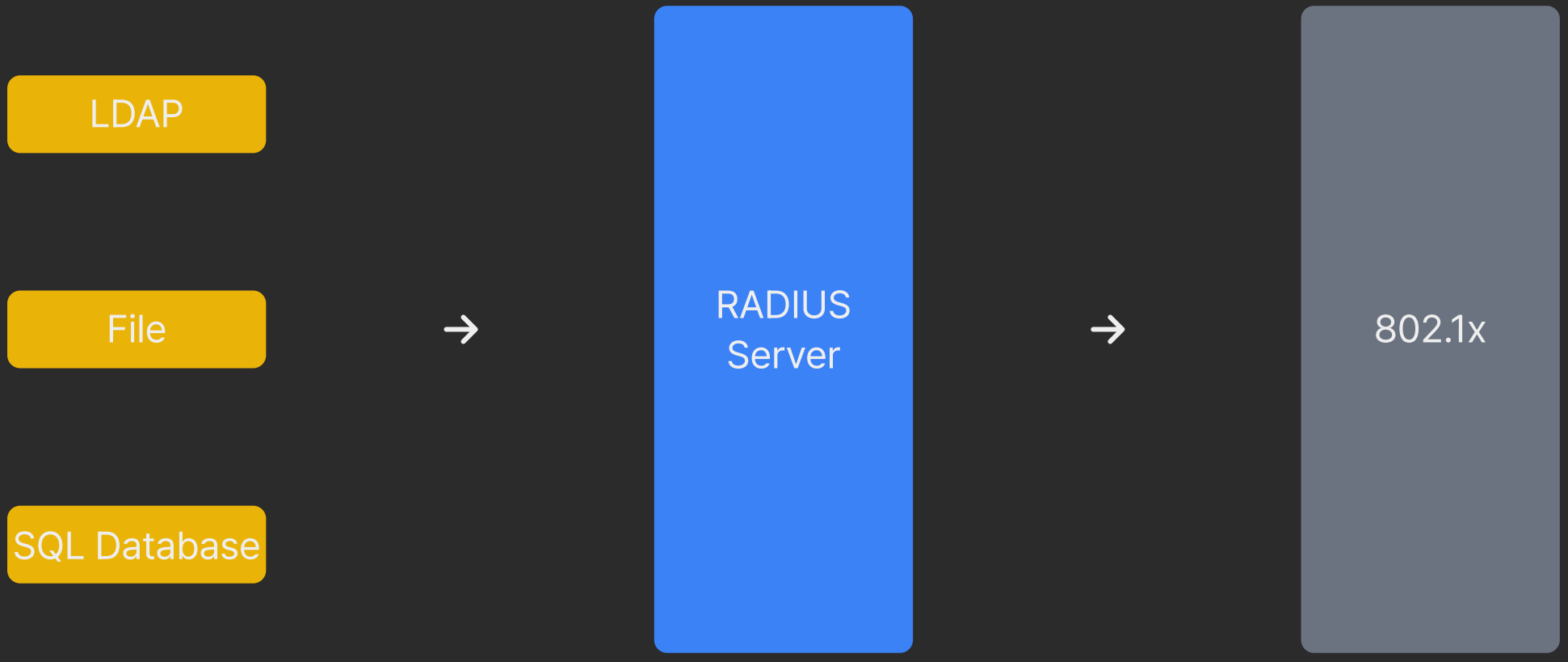
802.1x 위에서 인증을 담당하는 서버


RADIUS
Server


RADIUS
Server
802.1x


File
RADIUS Server
802.1x


LDAP
File
SQL Database
RADIUS Server
802.1x


LDAP
File
SQL Database
RADIUS Server
802.1x

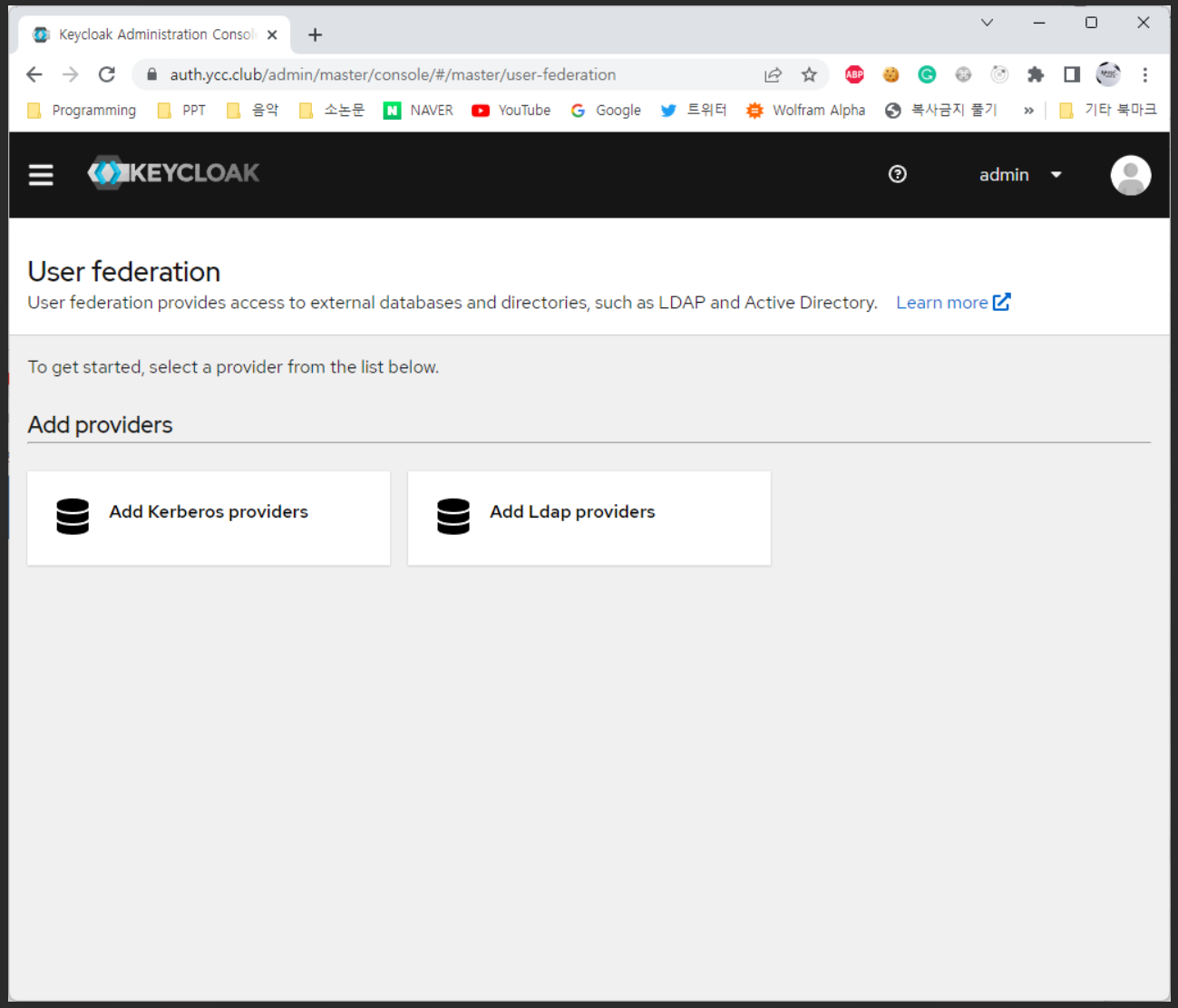
LDAP

LDAP

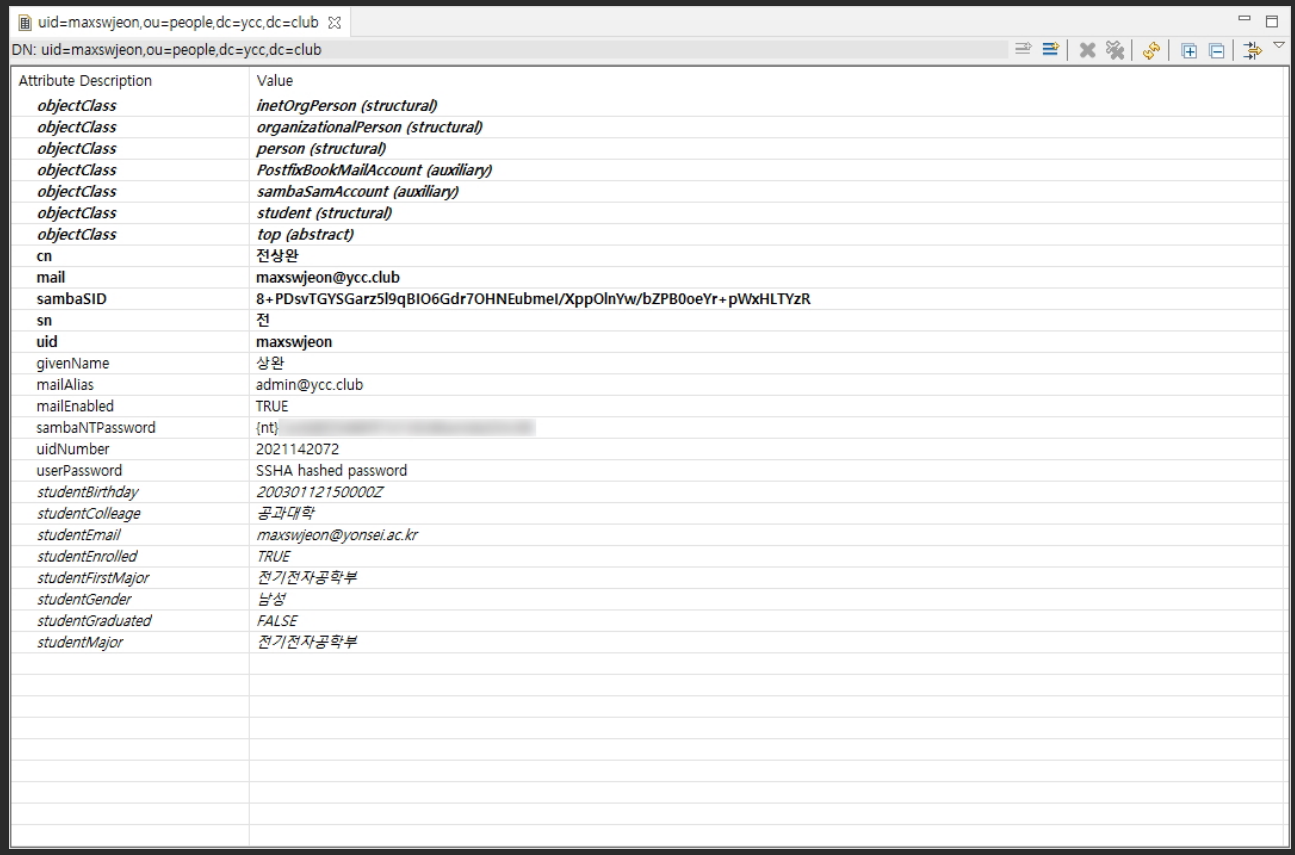
Lightweight Directory Access Protocol

Why LDAP?

RADIUS를 포함한 여러 서비스들이 User Federation 용도로 사용

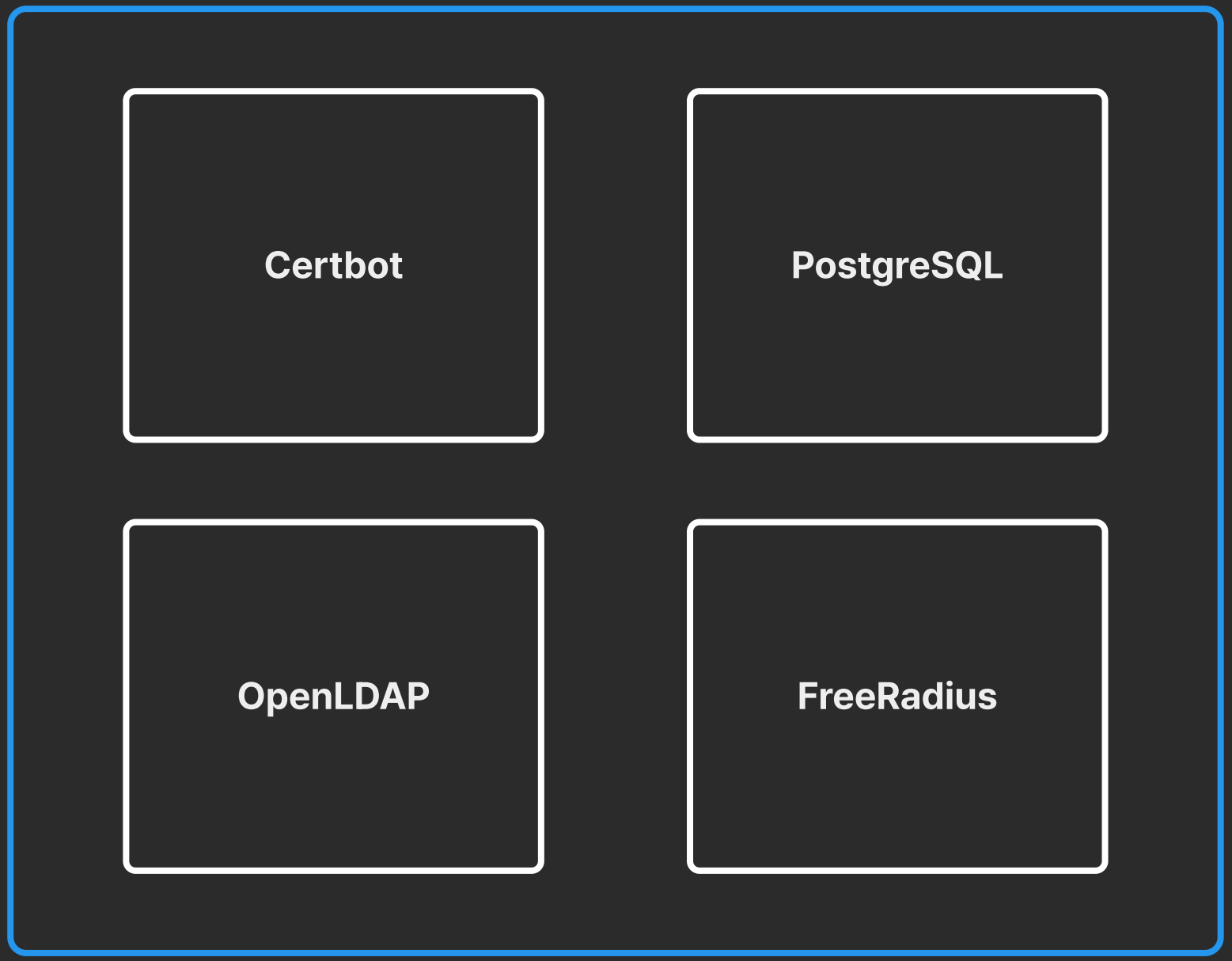

Keycloak Administration Consol
auth.ycc.club/admin/master/console/#/master/user-federation
Programming
PPT
음악
소논문
NAVER
YouTube
Google
트위터
Wolfram Alpha
복사금지 풀기
기타 북마크
KEYCLOAK
admin
User federation
User federation provides access to external databases and directories, such as LDAP and Active Directory.
Learn more
To get started, select a provider from the list below.
Add providers
Add Kerberos providers
Add Ldap providers

LDAP Entry Structure



Attribute Description	Value
objectClass	***inetOrgPerson (structural)***
objectClass	***organizationalPerson (structural)***
objectClass	***person (structural)***
objectClass	***PostfixBookMailAccount (auxiliary)***
objectClass	***sambaSamAccount (auxiliary)***
objectClass	***student (structural)***
objectClass	***top (abstract)***
cn	**전상완**
mail	**maxswjeon@ycc.club**
sambaSID	**8+PDsvTGYSGarz5l9qBIO6Gdr7OHNEubmeI/XppOlnYw/bZPB0oeYr+pWxHLTYzR**
sn	**전**
uid	**maxswjeon**
givenName	상완
mailAlias	admin@ycc.club
mailEnabled	TRUE
sambaNTPassword	{nt}
uidNumber	2021142072
userPassword	SSHA hashed password
studentBirthday	*20030112150000Z*
studentColleage	*공과대학*
studentEmail	*maxswjeon@yonsei.ac.kr*
studentEnrolled	*TRUE*
studentFirstMajor	*전기전자공학부*
studentGender	*남성*
studentGraduated	*FALSE*
studentMajor	*전기전자공학부*

컨테이너 구조 Container Structure



컨테이너 구조 Container Structure

Certbot

OpenLDAP의 TLS 설정에 필요한 Certificate를 발급하고 갱신한다
Issues and Renews Certificate for TLS settings of OpenLDAP

Entrypoint

/docker-entrypoint.sh

1. Certificate 존재 확인
2. Certificate이 없으면 발급
3. Container 상태를 Healthy로 변경
4. 24시간마다 인증서 갱신 시도

Volume Mounts

- ./data/certbot:/etc/letsencrypt
- ./data/certs:/certs
- ./scripts/certbot/docker-entrypoint.sh
  :/docker-entrypoint.sh

Port Exposure

None

컨테이너 구조 Container Structure

PostgreSQL

FreeRadius의 인증 기록과 Accounting 기록을 저장한다
Stores FreeRadius authentication and accounting records

Volume Mounts

- ./data/database:/data
- ./scripts/database/initdb.d
  :/docker-entrypoint-initdb.d

Port Exposure

- 5432

컨테이너 구조 Container Structure

OpenLDAP

FreeRadius을 통해 접근할 수 있는 유저들의 정보를 저장한다
Stores user information that can be accessed through FreeRadius

Entrypoint

1. 기본 Organization과 Readonly User 생성
2. Samba Schema 적용

Volume Mounts

- ./data/ldap:/var/lib/openldap
- ./config/ldap:/etc/openldap/slapd.d
- ./data/dhparam:/dhparam
- ./scripts/ldap/assets/custom-scripts

Port Exposure

- 389
- 636

컨테이너 구조 Container Structure

FreeRadius

802.1x 인증을 위한 RADIUS 서버
RADIUS server for 802.1x authentication

Entrypoint

1. 기본 설정 덮어씌우기
2. ldap, counter, sql 모듈 활성화
3. 환경변수에서 설정 적용

Volume Mounts

- ./config/freeradius:/config
- ./scripts/freeradius/init.d :/docker-entrypoint.d
- ./scripts/freeradius/docker-entrypoint.sh :/docker-entrypoint.sh
- ./data/certs/freeradius:/certs

Port Exposure

- 1812
- 1813

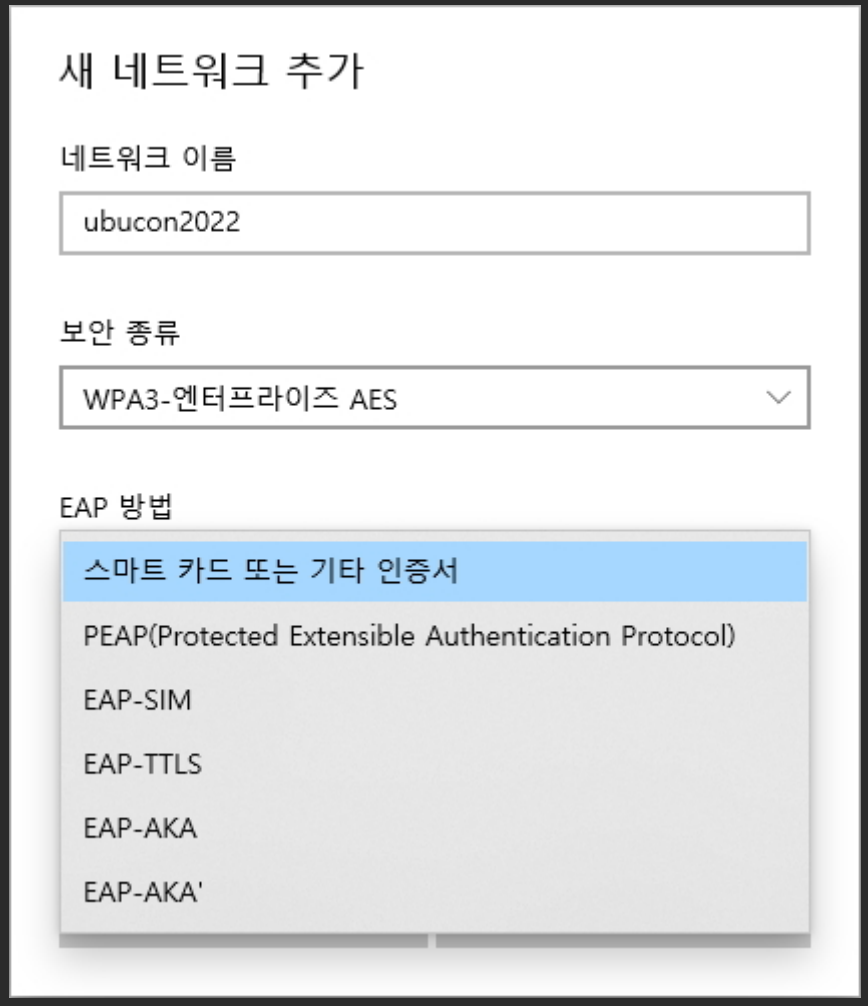
Done?

Nope

Password Hash

	Clear-text	NT hash (ntlm_auth)	MD5 hash	Salted MD5 hash	SHA1 hash	Salted SHA1 hash	Unix Crypt
PAP	✓	✓	✓	✓	✓	✓	✓
CHAP	✓	x	x	x	x	x	x
Digest	✓	x	x	x	x	x	x
MS-CHAP	✓	✓	x	x	x	x	x
PEAP	✓	✓	x	x	x	x	x
EAP-MSCHAPv2	✓	✓	x	x	x	x	x
Cisco LEAP	✓	✓	x	x	x	x	x
EAP-GTC	✓	✓	✓	✓	✓	✓	✓
EAP-MD5	✓	x	x	x	x	x	x
EAP-PWD	✓	x	x	x	x	✓	✓

Password Hash



Password Hash

	Clear-text	NT hash (ntlm_auth)	MD5 hash	Salted MD5 hash	SHA1 hash	Salted SHA1 hash	Unix Crypt
PAP	✓	✓	✓	✓	✓	✓	✓
CHAP	✓	x	x	x	x	x	x
Digest	✓	x	x	x	x	x	x
MS-CHAP	✓	✓	x	x	x	x	x
PEAP	✓	✓	x	x	x	x	x
EAP-MSCHAPv2	✓	✓	x	x	x	x	x
Cisco LEAP	✓	✓	x	x	x	x	x
EAP-GTC	✓	✓	✓	✓	✓	✓	✓
EAP-MD5	✓	x	x	x	x	x	x
EAP-PWD	✓	x	x	x	x	✓	✓

NT Hash를 따로 저장해야 함

Password Hash

	Clear-text	NT hash (ntlm_auth)	MD5 hash	Salted MD5 hash	SHA1 hash	Salted SHA1 hash	Unix Crypt
PAP	✓	✓	✓	✓	✓	✓	✓
CHAP	✓	x	x	x	x	x	x
Digest	✓	x	x	x	x	x	x
MS-CHAP	✓	✓	x	x	x	x	x
PEAP	✓	✓	x	x	x	x	x
EAP-MSCHAPv2	✓	✓	x	x	x	x	x
Cisco LEAP	✓	✓	x	x	x	x	x
EAP-GTC	✓	✓	✓	✓	✓	✓	✓
EAP-MD5	✓	x	x	x	x	x	x
EAP-PWD	✓	x	x	x	x	✓	✓

NT Hash를 따로 저장해야 함

Where? How?

Password Hash

Attribute Types

UbuCon 2022 | Browse...

Attribute Types

Please select an attribute type. Enter a filter to restrict the list.

Filter: password

- olcPasswordCryptSaltFormat
- olcPasswordHash
- userPassword

Details

Numeric OID: 2.5.4.35

Attribute names: userPassword

Descripton: RFC4519/2307: password of user

Usage: userApplications

Flags

Single valued | Read only | Collective | Obsolete

Syntax

Syntax OID: 1.3.6.1.4.1.1466.115.121.1.40

Syntax Description: Octet String

Length: 128

Matching Rules

Equality match: octetStringMatch

Substring match: -

Ordering match: -

- Other Matching Rules (2)
- Used as MUST (1)
- Used as MAY (16)
- Supertype (0)
- Subtypes (0)
- RawSchemaDefinition

Object Classes | Attribute Types | Matching Rules | Matching Rule Use | Syntaxes

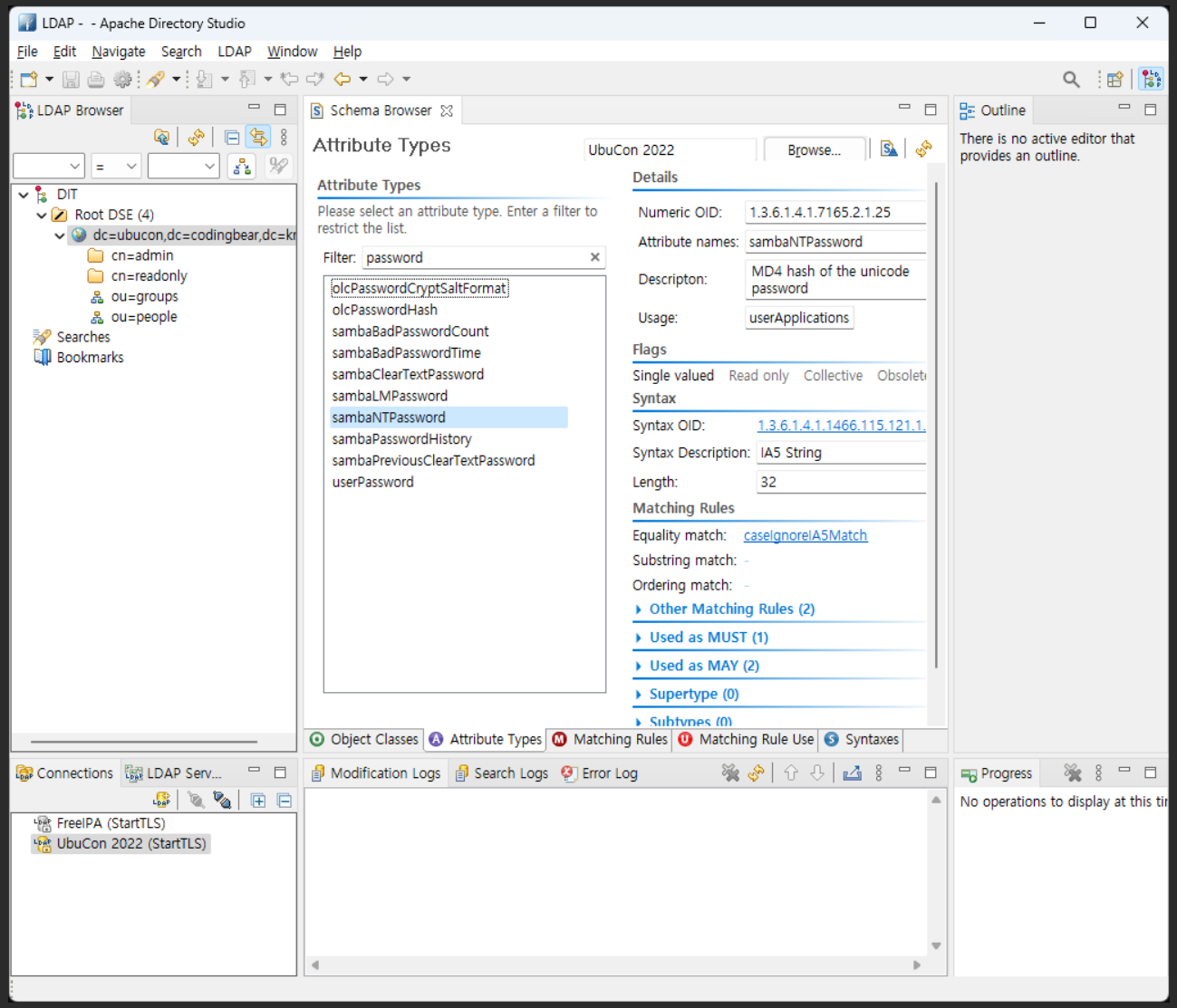
SAMBA?

SAMBA?

윈도우의 파일공유 프로토콜인 SMB 프로토콜을 재 구현한 것

Re-implementation of the SMB networking protocol
which is a protocol for Windows file share

SAMBA?


LDAP - - Apache Directory Studio
File Edit Navigate Search LDAP Window Help
LDAP Browser
DIT
Root DSE (4)
dc=ubucon,dc=codingbear,dc=kr
cn=admin
cn=readonly
ou=groups
ou=people
Searches
Bookmarks
Schema Browser
Attribute Types
UbuCon 2022
Browse...
Attribute Types
Please select an attribute type. Enter a filter to restrict the list.
Filter: password
olcPasswordCryptSaltFormat
olcPasswordHash
sambaBadPasswordCount
sambaBadPasswordTime
sambaClearTextPassword
sambaLMPassword
sambaNTPassword
sambaPasswordHistory
sambaPreviousClearTextPassword
userPassword
Details
Numeric OID: 1.3.6.1.4.1.7165.2.1.25
Attribute names: sambaNTPassword
Descripton: MD4 hash of the unicode password
Usage: userApplications
Flags
Single valued Read only Collective Obsolet
Syntax
Syntax OID: 1.3.6.1.4.1.1466.115.121.1.
Syntax Description: IA5 String
Length: 32
Matching Rules
Equality match: caseIgnoreIA5Match
Substring match: -
Ordering match: -
Other Matching Rules (2)
Used as MUST (1)
Used as MAY (2)
Supertype (0)
Subtypes (0)
Object Classes
Attribute Types
Matching Rules
Matching Rule Use
Syntaxes
Outline
There is no active editor that provides an outline.
Connections
LDAP Serv...
FreeIPA (StartTLS)
UbuCon 2022 (StartTLS)
Modification Logs
Search Logs
Error Log
Progress
No operations to display at this ti

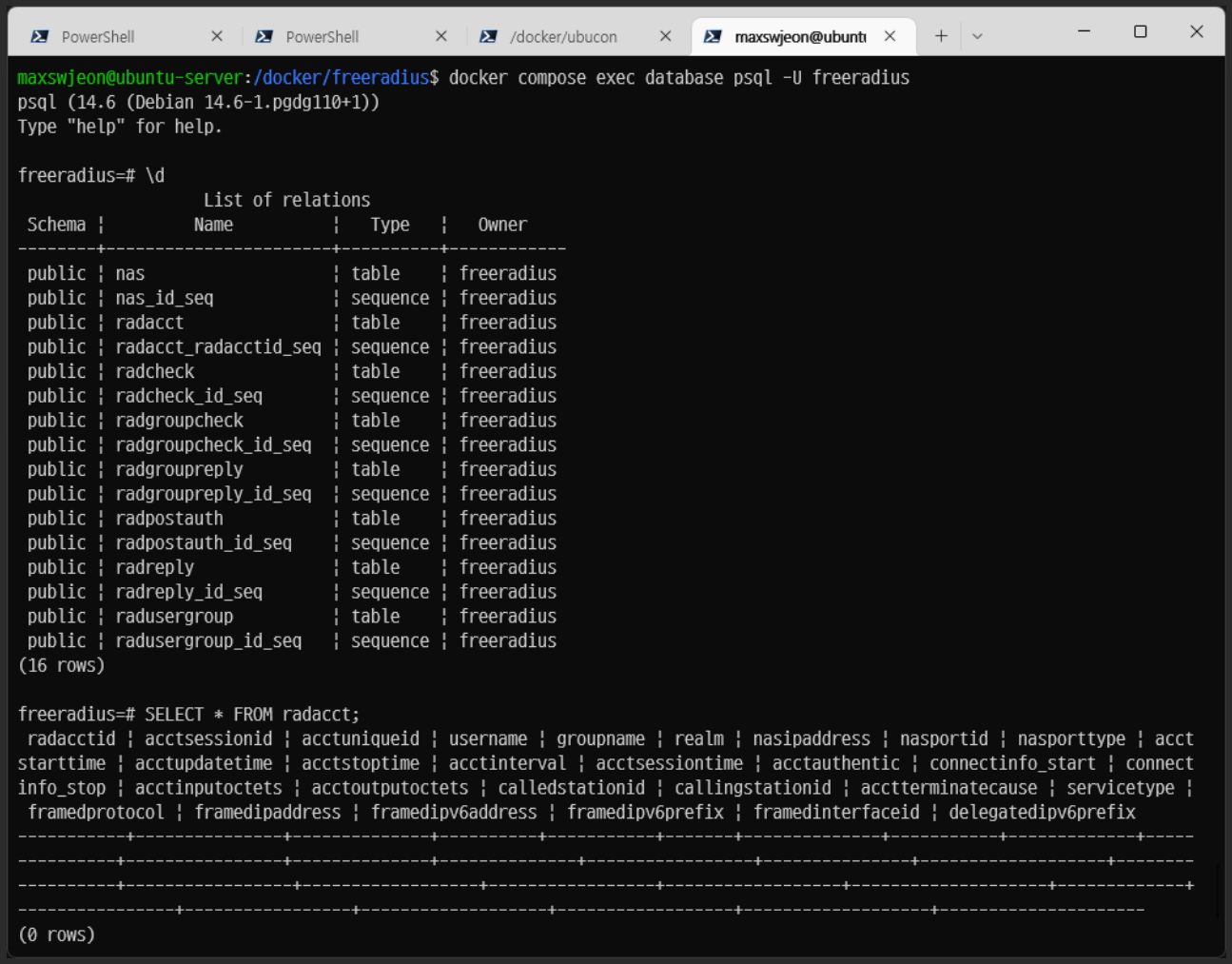
동방에 누구?

Who's in the club room?

동방에 누구?

RADIUS Accounting

RADIUS Accounting



RADIUS Accounting

PowerShell | PowerShell | /docker/ubucon | maxswjeon@ubunti

id	username	pass	reply	calledstationid	callingstationid	authdate
1	ycc		Access-Reject			2022-09-01 11:25:58.928391+00
2	ycc		Access-Reject			2022-09-01 11:25:58.994517+00
3	ycc		Access-Reject			2022-09-01 11:26:04.234875+00
4	ycc		Access-Reject			2022-09-01 11:26:04.29361+00
5	ycc		Access-Reject			2022-09-01 11:26:09.46377+00
6	ycc		Access-Reject			2022-09-01 11:26:09.496566+00
7	ycc		Access-Reject			2022-09-01 11:26:32.755066+00
8	ycc		Access-Reject			2022-09-01 11:26:32.810709+00
9	gulgong		Access-Accept			2022-09-01 11:26:49.136077+00
10	gulgong		Access-Accept			2022-09-01 11:26:49.286699+00
11	maxswjeon		Access-Accept			2022-09-01 12:05:13.044866+00
12	maxswjeon		Access-Accept			2022-09-01 12:05:13.101017+00
13	maxswjeon		Access-Accept			2022-09-01 12:17:24.548594+00
14	maxswjeon		Access-Accept			2022-09-01 12:17:24.60991+00
15	maxswjeon		Access-Accept			2022-09-01 12:26:51.924401+00
16	maxswjeon		Access-Accept	588694462f84	fa211ee1e8d0	2022-09-01 12:26:51.985373+00
17	maxswjeon		Access-Reject	588694462f84	c6eb97cb3b0e	2022-09-01 12:27:20.529272+00
18	maxswjeon		Access-Reject	588694462f84	c6eb97cb3b0e	2022-09-01 12:27:24.94597+00
19	maxswjeon		Access-Accept			2022-09-01 12:27:26.839831+00
20	maxswjeon		Access-Accept	588694462f84	fa211ee1e8d0	2022-09-01 12:27:26.902977+00
21	maxswjeon		Access-Reject	588694462f84	c6eb97cb3b0e	2022-09-01 12:27:52.602763+00
22	maxswjeon		Access-Accept			2022-09-01 12:27:59.383484+00
23	maxswjeon		Access-Accept	588694462f84	fa211ee1e8d0	2022-09-01 12:27:59.44846+00
24	maxswjeon		Access-Reject	588694462f84	c6eb97cb3b0e	2022-09-01 12:28:14.171246+00
25	maxswjeon		Access-Accept			2022-09-01 12:28:23.073689+00
26	maxswjeon		Access-Accept	588694462f84	c6eb97cb3b0e	2022-09-01 12:28:23.12214+00
27	maxswjeon		Access-Accept			2022-09-01 12:38:04.674791+00
28	maxswjeon		Access-Accept	588694462f84	c6eb97cb3b0e	2022-09-01 12:38:04.72539+00
29	maxswjeon		Access-Accept			2022-09-01 13:27:05.093617+00
30	maxswjeon		Access-Accept	588694462f84	c6eb97cb3b0e	2022-09-01 13:27:05.157566+00
31	maxswjeon		Access-Accept			2022-09-01 13:27:25.495098+00
32	maxswjeon		Access-Accept	588694462f84	dc41a96e960f	2022-09-01 13:27:25.557448+00
33	maxswjeon		Access-Accept			2022-09-01 13:51:49.454575+00

--More--

Summary

What we know

What we don't know

Summary

What we know

- 접속 시간
  Access Time

What we don't know

Summary

What we know

- 접속 시간
  Access Time
- MAC 주소
  MAC Address

What we don't know

Summary

What we know

- 접속 시간
  Access Time
- MAC 주소
  MAC Address
- 사용자 아이디
  User ID

What we don't know

Summary

What we know

- 접속 시간
  Access Time
- MAC 주소
  MAC Address
- 사용자 아이디
  User ID

What we don't know

- 현재 접속 여부
  (연결 끊긴 시간)
  Current Connection Status
  (Disconnecction Time)

Ping?

Ping?

IP가 필요함

Need IP

Ping?

IP가 필요함
Need IP

MAC 주소를 알 수 없음
Cannot know MAC address

ARP!

ARP!

네트워크 서브넷에 있는 모든 IP에 Ping을 보내고 ARP 테이블을 확인해 보자!

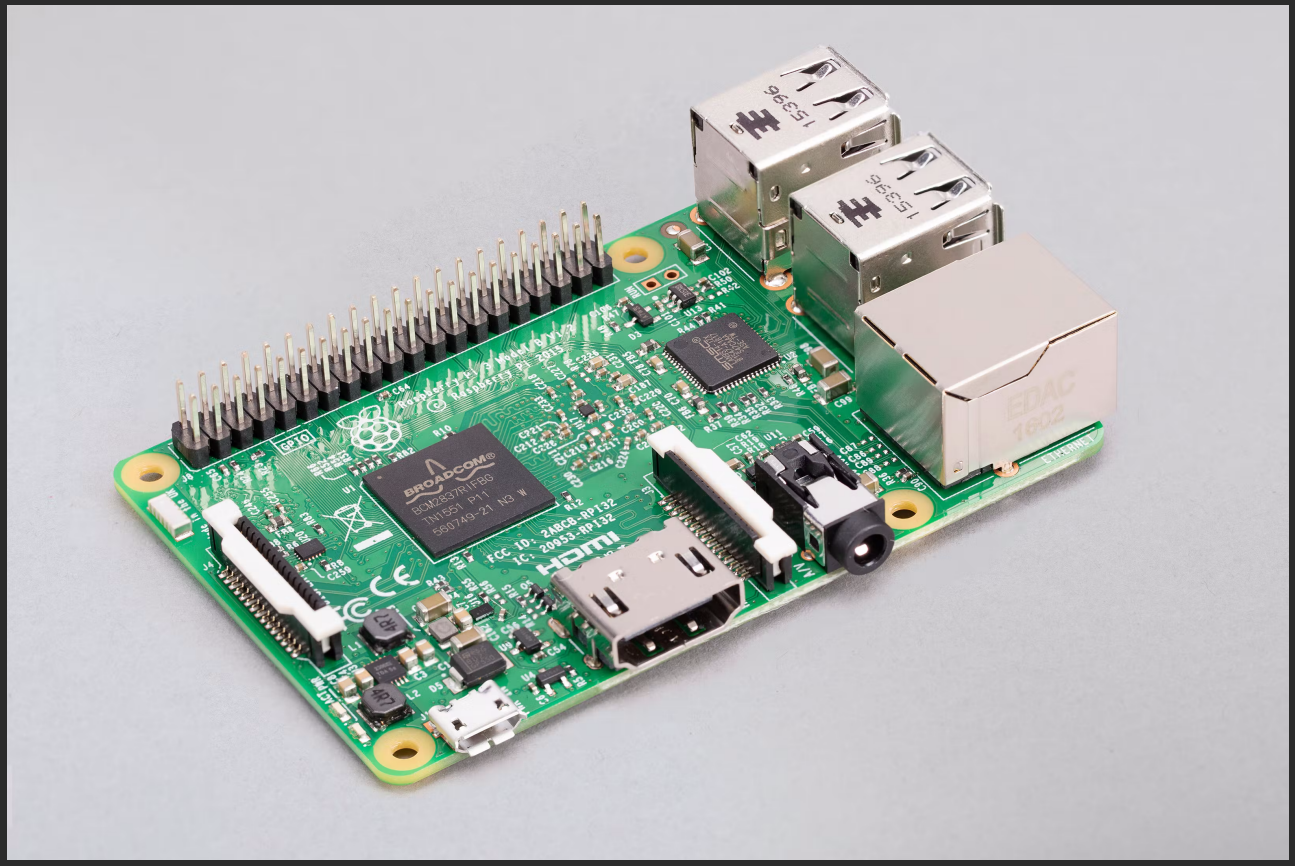
Ping all the ips in the subnet and check the ARP table!

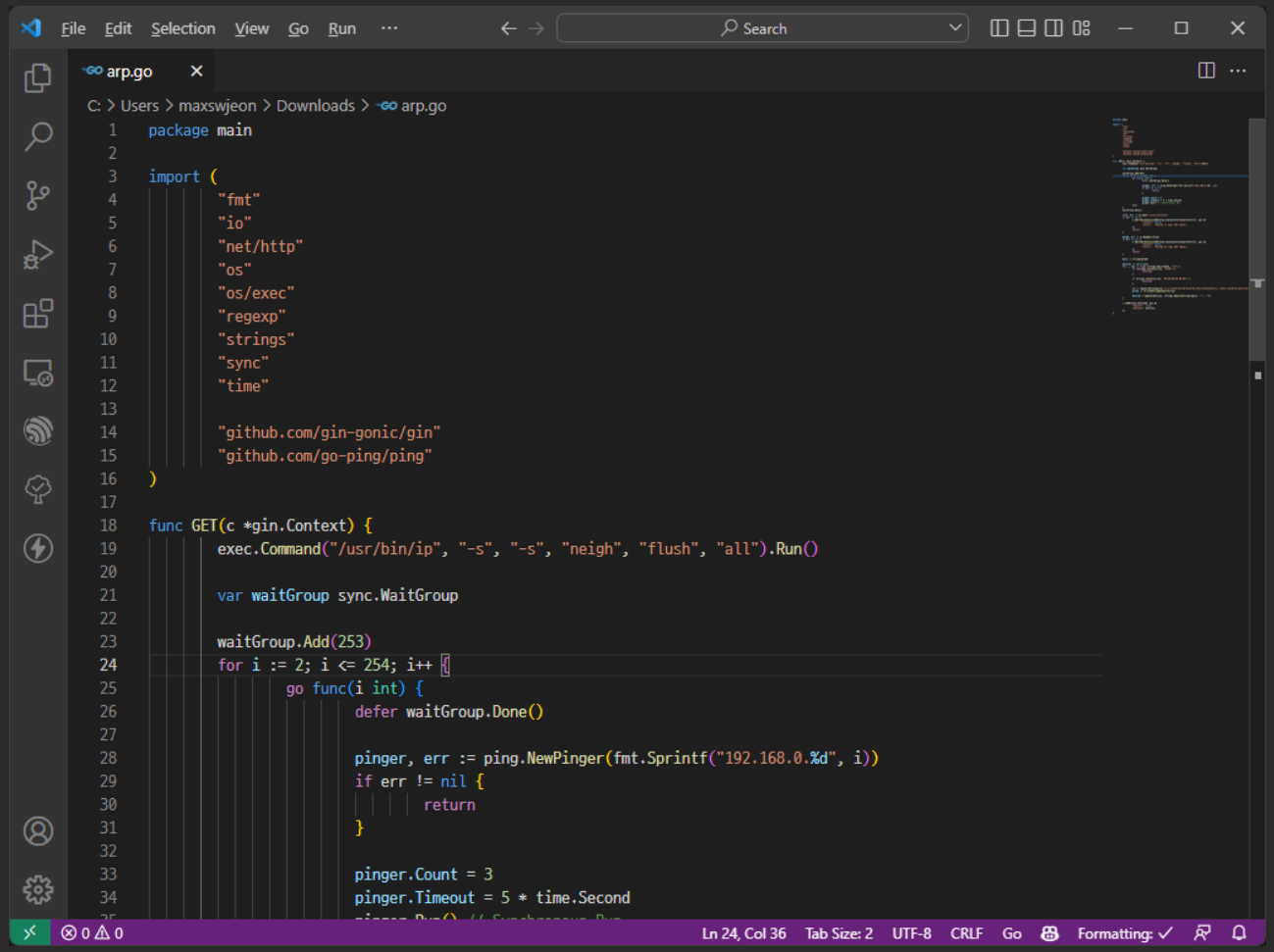
Docker

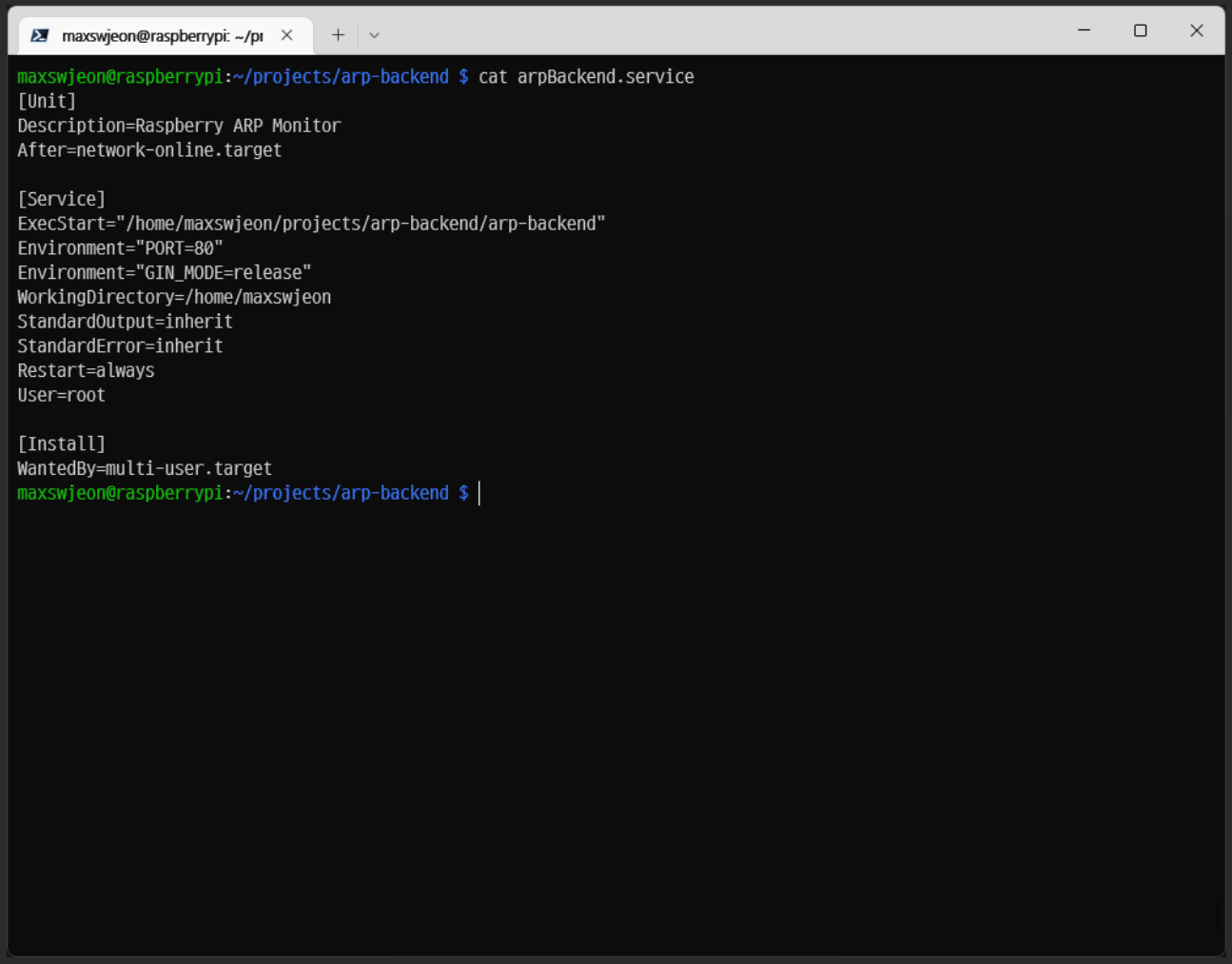
Docker

네트워크가 Host와 분리되어 있으며 ARP Cache를 Flush할 수 없다

Network is seperated with the host and cannot flush the arp cache

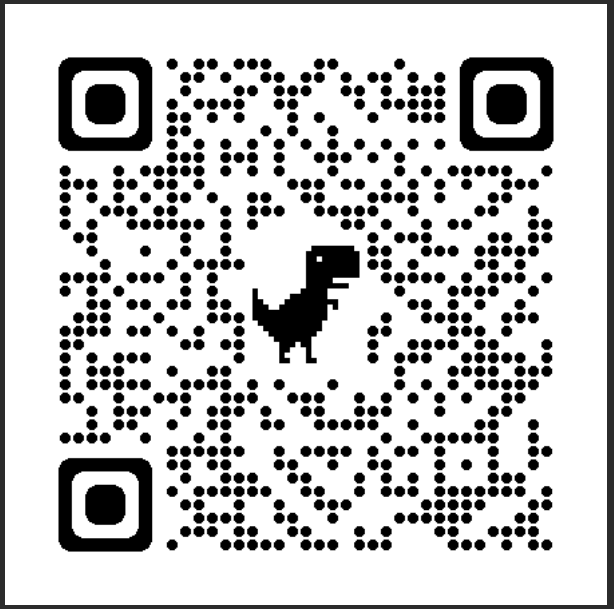

BROADCOM
HDMI


File Edit Selection View Go Run ···
Search
arp.go
C: > Users > maxswjeon > Downloads > arp.go
package main
import (
"fmt"
"io"
"net/http"
"os"
"os/exec"
"regexp"
"strings"
"sync"
"time"
"github.com/gin-gonic/gin"
"github.com/go-ping/ping"
)
func GET(c *gin.Context) {
exec.Command("/usr/bin/ip", "-s", "-s", "neigh", "flush", "all").Run()
var waitGroup sync.WaitGroup
waitGroup.Add(253)
for i := 2; i <= 254; i++ {
go func(i int) {
defer waitGroup.Done()
pinger, err := ping.NewPinger(fmt.Sprintf("192.168.0.%d", i))
if err != nil {
return
}
pinger.Count = 3
pinger.Timeout = 5 * time.Second
0 0
Ln 24, Col 36 Tab Size: 2 UTF-8 CRLF Go Formatting:


maxswjeon@raspberrypi: ~/pr
maxswjeon@raspberrypi:~/projects/arp-backend $ cat arpBackend.service
[Unit]
Description=Raspberry ARP Monitor
After=network-online.target
[Service]
ExecStart="/home/maxswjeon/projects/arp-backend/arp-backend"
Environment="PORT=80"
Environment="GIN_MODE=release"
WorkingDirectory=/home/maxswjeon
StandardOutput=inherit
StandardError=inherit
Restart=always
User=root
[Install]
WantedBy=multi-user.target
maxswjeon@raspberrypi:~/projects/arp-backend $

Demo

https://ubucon.codingbear.kr



Thank you