



VP5200 Series Switch

Common User Guide

Chapter #2



목 차

2	VP5200 Series 스위치 시작하기	4
2.1.	편집 및 도움말 기능	5
2.2.	스위치 명령어 모드	10
2.3.	VP5200 스위치 가동	11
2.4.	사용자 인터페이스	11
2.4.1.	콘솔 연결	12
2.4.2.	Telnet 연결	13
2.4.3.	SNMP Network Manager 를 통한 연결	13
2.5.	사용자 인증	13
2.5.1.	사용자 추가 및 삭제	13
2.5.2.	패스워드 설정	15
2.5.3.	인증 방법 설정	17
2.5.4.	인증 서버 설정	20
2.6.	Hostname 설정	22
2.7.	SNMP (Simple Network Management Protocol)	23
2.8.	ACL (Access Control List)	27
2.8.1.	액세스 리스트 생성 규칙	27
2.8.2.	표준 IP 액세스 리스트 설정	28
2.8.3.	SNMP 연결에 액세스 리스트 설정	29
2.8.4.	Telnet 연결에 액세스 리스트 설정	29
2.9.	NTP 설정	30
2.9.1.	NTP 개요	30
2.9.2.	NTP client mode 설정	30
2.9.3.	NTP Server mode 설정	31
2.9.4.	NTP time zone 설정	31
2.9.5.	NTP summer time 설정	31
2.9.6.	NTP 기타 명령어	32
2.9.7.	NTP 설정 예제	32

표 목차

표 1. 명령어 구문 심볼.....	8
표 2. 명령어 라인 편집 명령 및 도움말 기능.....	9
표 3. 스위치 명령어 모드.....	10
표 4. 스위치의 명령어 모드 사이의 이동.....	11
표 5. 스위치의 사용자 추가 및 삭제 명령어.....	14
표 6. 스위치의 Enable 패스워드 설정 명령어.....	16
표 7. Hostname 설정 명령어.....	23
표 8. SNMP 환경 설정 명령.....	23

그림 목차

그림 1. VP5200 스위치와 운영 단말 연결.....	12
---------------------------------	----

2

VP5200 Series 스위치 시작하기

본 장은 다음과 같이 시스템 운영자가 VP5200 L2 스위치의 운용 환경을 설정하고 처음 다루기 시작할 때 필요한 정보를 제공한다.

- 편집 및 도움말 기능
- 스위치 명령어 모드의 이해
- 스위치 가동
- VP5200 스위치 사용자 인터페이스
- 스위치 로그인과 패스워드의 설정
- SNMP 환경설정
- 스위치의 파일 및 환경 설정의 보기와 저장
- 액세스 리스트
- 텔넷 클라이언트

2.1. 편집 및 도움말 기능

본 장은 명령어 편집기의 편집 기능과 도움말 기능에 대하여 설명한다.

명령어 문법의 이해

본 장은 운영자가 시스템 운영을 위한 명령어를 입력하는 단계를 설명한다. 명령어 인터페이스 사용에 대한 자세한 정보는 다음 장에 설명된다.

명령어 라인 인터페이스를 사용하기 위하여 다음의 단계를 거치도록 한다.


- 1) 명령어 프롬프트에서 명령어를 입력하기 전에, 먼저 적절한 권한을 가지고 있는 프롬프트 수준에 있는지 확인하라. 대부분의 환경 설정 관련 명령어들은 시스템 운영자 수준의 권한을 필요로 한다.
- 2) 수행하고자 하는 명령어를 입력하라. 만약 명령어가 추가적인 명령어(sub-command) 또는 파라미터 값을 입력할 필요가 없으면 3 단계로 간다.
 - a. 만약 명령어가 파라미터를 가지고 있으면 파라미터 이름 및 값을 입력하라.
 - b. 명령어에 따르는 파라미터에 따라서 숫자, 문자열, 또는 주소 등이 값으로 설정된다.
- 3) 명확하게 명령어 입력을 완료 하였으면, [Return]키를 눌러서 명령을 실행한다.



Notice

명령어를 입력하고 실행했을 때 "% Command incomplete." 메시지를 받을 때가 있다. 이는 명령어 실행에 필요한 파라미터가 제대로 입력되지 않았음을 의미하며, 입력한 명령은 실행되지 않는다. 이 때 위쪽 화살표를 누르게 되면 마지막에 입력한 명령이 표시된다.

다음은 명령어 파라미터를 제대로 입력하지 않은 경우를 보여준다.

```
Switch# show   
% Command incomplete.  
Switch#
```

명령어 문법 도움말(Command Syntax Helper)

VP5200 스위치의 CLI는 명령어 문법 도움말 기능을 자체적으로 내장하고 있다. 시스템 운영자는 명령어 입력 중 완전한 문법을 모르는 경우, 어느 위치에서든지 '?'를 쳐서 도움말을 제공받을 수 있다.

VP5200 스위치는 다음과 같은 두 가지 도움말 기능을 제공한다.

■ 전체 도움말 기능

- 가능한 파라미터 및 값의 리스트에 대한 전체 도움말을 제공한다. 입력한 명령어 다음에 한 칸 공백을 둔다.

■ 부분 도움말 기능

- 운영자가 축약된 파라미터를 입력한 후, 이에 해당하는 파라미터에 대한 도움말을 제공한다. 입력한 명령어 다음에 공백을 두지 않는다.

전체 도움말 기능을 `show` 명령어를 통하여 보면 다음과 같다. `show` 명령어 다음에 공백 문자와 함께 '?'를 입력하면 운영자가 입력 할 수 있는 파라미터 및 값의 리스트가 출력된다. 그리고 다시 "Switch# show" 프롬프트 상태에서 커서가 깜박이면서 운영자의 입력을 대기한다. 운영자 입력에서 '?'는 화면에 표시되지 않는다.

Switch# show ?	
access-list	access list entry
arp	Display ARP table entries
clock	show current system's time
config	Show config file information
cpu	CPU information
debugging	Debugging functions
filter	filter setting
flash	display information about flash file system
flow-rule	flow-rule
interface	Interface status and configuration
ip	IP information
logging	Show all contents of logging buffers
mac-address-table	Display MAC address table entries
mac-count	MAC count configuration
memory	Memory statistics
mirroring	Port mirroring configuration
ntp	show current ntp status
port	Port status and configuration
port-group	Port-group configuration
privilege	Display your current level of privilege
qos	Qos configuration
rate-limit	Display rate-limit control parameters
rmon	Remote Monitoring
running-config	Current operating configuration
service-policy	service-policy information
spanning-tree	Spanning tree topology

stack	Show stacking information
startup-config	Show startup config file information
switchport	Switching port configuration
system	Display the system information
uptime	Display elapsed time since boot
users	Display information about terminal lines
version	Display the system version
vlan	VLAN information

```
Switch# show_
```

부분 도움말 기능을 show 명령어를 통하여 보면 다음과 같다. show 명령어 입력 후 공백 없이 '?'를 입력하면 다음과 같이 show 명령어에 대한 설명이 표시되고 커서가 깜박이면서 다음 명령 입력을 기다린다.

```
Switch# show?
  show  Show running system information
Switch# show_
```

위 예에서 운영자는 포트의 상태를 알고 싶지만 정확한 명령을 모른다고 하자. 그러면 'p'를 치고 공백 없이 '?'를 치면 'p'로 시작하는 서브 명령어의 리스트가 다음과 같이 출력된다. 물론 운영자가 입력한 명령은 다시 표시가 되면서 커서가 깜박이면서 입력을 대기한다.

```
Switch# show p?
  port          Display port configuration
  port-group    Port group information
  privilege     Display your current level of privilege
Switch# show p_
```

단축 명령어 입력

VP5200 스위치의 CLI 는 명령어 및 파라미터를 다 입력하지 않고, 단축 명령어를 통한 실행을 지원한다. 일반적으로 명령어의 첫 두세 글자를 입력하여 단축 명령을 수행한다.



Notice

단축 명령을 사용할 때, 시스템 운영자는 VP5200 스위치가 명령어를 구분하여 인식할 수 있도록 충분하게 입력해야 한다. "% Ambiguous command."라는 메시지를 받을 때가 있다. 이것은 해당 모드에 입력한 문자와 Prefix 가 같은 하나 이상의 명령어가 있음을 의미한다.

```
Switch# show i
% Ambiguous command.
```

```
Switch# show i [?]
      interface Port interface status and configuration
      ip          IP
Switch# show i_
```

명령어 심볼

본 가이드에서 설명하는 시스템 명령어 문법에는 다양한 심볼이 사용된다. 명령어 심볼은 명령어 수행을 위해서 파라미터들이 어떻게 입력되어야 하는지를 설명한다. 시스템 명령어 문법에 적용된 심볼 및 각각의 심볼이 의미하는 바는 다음 <표 1>과 같다.

표 1. 명령어 구문 심볼

심볼	이름	설명
<>:	Angle brackets	<ul style="list-style-type: none"> 명령어 문법에서 하나의 변수 또는 값을 의미한다. 이렇게 표현된 파라미터는 반드시 입력을 해야 한다. 예를 들어, 다음과 같은 명령어가 있을 때 <code>access-list <1-99> (deny permit) address</code> 표준 IP access control list 번호는 <1-99> 사이의 값으로 반드시 입력해야 한다.
():	Braces	<ul style="list-style-type: none"> 명령어 문법에서 사용되는 파라미터 또는 값의 리스트 시스템 운영자는 리스트에 포함된 항목 중에서 최소한 하나 이상을 입력해야 한다. 예를 들어, 다음과 같은 명령어가 있을 때 <code>qos (cos-queue-map/cos-remark)</code> 시스템 운영자는 QoS method로서 qos-queue-map 또는 qos-remarking 중의 하나를 반드시 명시해야 한다.
[]:	Square brackets	<ul style="list-style-type: none"> 명령어 문법에서 사용되는 파라미터 또는 값의 리스트 시스템 운영자는 리스트에 포함된 항목 중에서 필요한 항목을 선택적으로 입력한다. 경우에 따라서는 하나도 입력을 하지 않을 수도 있다. 예를 들어, 다음과 같은 명령어가 있을 때 <code>show interfaces [ifname]</code> 인터페이스의 이름을 정의하지 않을 수도 있다.
:	Vertical bar	<ul style="list-style-type: none"> 파라미터 리스트에서 상호 배타적인 항목들을 표현

심볼	이름	설명
<i>Italic 체</i>		■ 입력할 변수들
Bold 체		■ 운영자가 입력해야 하는 명령어
A.B.C.D		■ IP 주소 또는 서브넷 마스크를 의미
A.B.C.D/M		■ IP prefix 를 의미 (예. 192.168.0.0/24)

명령어 라인 편집 키 및 도움말

VP5200 스위치는 Emacs 와 유사한 편집 기능을 제공한다. <표 2>는 운영 단말이 제공하는 명령어 라인 편집 명령 및 도움말 기능을 설명한다.

표 2. 명령어 라인 편집 명령 및 도움말 기능

명령어	설명
[Ctrl] + [A]	■ 커서를 줄의 처음으로 이동
[Ctrl] + [E]	■ 커서를 줄의 끝으로 이동
[Ctrl] + [B]	■ 커서를 한 단어 뒤로 이동
[Ctrl] + [F]	■ 커서를 한 글자 앞으로 이동
Backspace	■ 커서 앞의 한 글자를 삭제
[Ctrl] + [K]	■ 현재 커서로부터 줄의 끝까지 문자를 삭제
[Ctrl] + [U]	■ 현재 커서로부터 줄의 처음까지 문자를 삭제
Tab	<ul style="list-style-type: none"> ■ 명령어의 일부분을 치고 [tab]을 치면 그 prompt 에서 같은 prefix 를 가진 명령어가 여러 개 있을 경우 리스트를 표시 ■ 한 개의 명령어만 있을 경우 명령어 나머지 부분을 완성
[Ctrl] + [P] 또는 	■ 마지막 입력 명령어부터 차례 대로 20 개까지의 명령어 입력에 대한 이력을 표시
[Ctrl] + [N] 또는 	■ 다음 명령어를 표시
?	<ul style="list-style-type: none"> ■ prompt 상에서 사용 가능한 명령어의 리스트와 설명을 표시 ■ 명령어 다음에 '?'를 쳤을 경우, 해당 명령어 다음에 입력해야 할 파라미터 리스트를 표시 ■ 부분적인 명령어에 바로 붙여서 '?'를 입력했을 경우 같은 prefix 를 가진 명령어의 리스트를 표시
Return 또는 Spacebar 또는 Q	<ul style="list-style-type: none"> ■ -- More -- 에서 Return 키를 누르면 다음 한 line 이 표시 ■ Spacebar 를 누르면 다음 페이지가 표시되며, Q 를 누르면 종료하고

2.2. 스위치 명령어 모드

VP5200 스위치는 <표 3>와 같이 다양한 스위치 명령어 모드를 지원한다. 각 스위치 명령어 모드마다 운영자에게 주어지는 권한에는 차이가 있다.

표 3. 스위치 명령어 모드

모드	프롬프트	설명
User 모드	Switch>	■ 보통 통계 정보를 디스플레이
Privileged 모드	Switch#	■ 시스템 설정을 출력하거나 시스템 관리 명령을 사용
Config 모드	Switch(config)#	■ 스위치의 환경 설정 값을 글로벌 하게 변경
Interface 모드	Switch(config-if-fal)# Switch(config-if-vlan1)#	■ 인터페이스의 환경 설정을 변경
Interface range 모드	Switch(config-ifrange)#	■ 여러 개의 인터페이스를 동시에 설정하기 위한 모드
Range Port 모드	Switch(config-range-port)#	■ 여러 개의 인터페이스를 동시에 설정하기 위한 모드



Notice

명령어 프롬프트는 각 모드를 나타내는 문자열 앞에 VP5200 스위치의 이름을 호스트 이름으로 사용한다. 본 가이드에서는 'Switch' 프롬프트를 공통의 호스트 이름으로서 사용한다.

시스템 운영자는 VP5200 스위치의 환경을 설정 할 때, 여러 가지 종류의 프롬프트를 접하게 된다. 프롬프트는 환경 설정 모드에서 운영자가 현재 어느 위치에 와 있는 지를 알려준다. 스위치의 환경 설정을 변경하기 위해서는 반드시 프롬프트를 체크 해야만 한다. <표 4>은 스위치의 명령어 모드 사이의 이동 방법을 설명한다.

표 4. 스위치의 명령어 모드 사이의 이동

명령어	설명
enable	<ul style="list-style-type: none"> ■ User 모드에서 Privileged 모드로 이동 ■ Privileged 모드의 패스워드를 입력할 필요
disable	<ul style="list-style-type: none"> ■ Privileged 모드에서 User 모드로 이동
configure terminal	<ul style="list-style-type: none"> ■ Privileged 모드에서 Config 모드로 이동
interface ifname	<ul style="list-style-type: none"> ■ Config 모드에서 Interface 모드로 이동
interface range (fastethernet gigaethernet) ifrange	<ul style="list-style-type: none"> ■ Config 모드에서 Interface range 모드로 이동
range port	<ul style="list-style-type: none"> ■ Config 모드에서 range port 모드로 이동
exit	<ul style="list-style-type: none"> ■ 이전의 모드로 이동
end	<ul style="list-style-type: none"> ■ 어느 모드에서든 Privileged 모드로 이동 ■ User 모드에서는 이동하지 않는다.

2.3. VP5200 스위치 가동

VP5200 스위치는 처음 가동될 때, 자체 테스트를 실행하고 플래시 메모리로부터 OS image 를 찾아서 메모리에 로드 하여 시스템을 시작한다. 시스템 부팅이 완료되면 플래시 메모리에 저장되어 있는 이전 환경 설정 값(startup-config)을 로딩한다.



Notice

VP5200 스위치는 시스템 안정성을 위하여 두 개 이상의 OS image 를 관리한다. 기본적으로 Primary OS image 가 로드 되도록 설정되어 있으며, 운영자는 스위치의 boot 모드 또는 privileged 모드에서 이를 변경할 수 있다.

2.4. 사용자 인터페이스

시스템 운영자는 스위치의 환경을 설정하고, 환경 설정을 검증하고, 통계 정보 수집 등 다양한 시스템 운영 유지 보수의 목적으로 스위치에 접속할 수 있다. 스위치에 접속하기 위한 가장 기본적인 방법은 VP5200 스위치가 제공하는 별도의 콘솔 포트를 통하여 직접 접속하는 것이다(*Out-of-band management*).

스위치로 연결하는 또 다른 방법은 원격지에서 telnet 프로그램을 이용하는 것이다. 원격지에서

telnet 연결을 위한 별도의 포트를 지원하지는 않고 서비스 포트를 통하여 접속하도록 한다(*In-band management*).

운영자는 아래의 방법을 사용하여 VP5200 스위치를 관리할 수 있다.

- 콘솔 포트에 터미널을 연결해서 CLI 접속.
- TCP/IP 기반 네트워크에서 Telnet 연결을 사용하여 CLI 접속.
- SNMP Network Manager 를 통해서 관리.

VP5200 스위치는 운영 관리를 위하여 다음과 같이 동시 접속 연결을 지원한다.

- 1 개의 콘솔 연결
- 최대 4 개의 telnet 연결

2.4.1. 콘솔 연결

시스템에 내장된 CLI 는 RJ-45 형태의 이더넷 포트를 통하여 접속이 가능하다. 이를 위하여 운영 단말(또는 terminal emulation 소프트웨어가 탑재된 워크스테이션)은 9 핀, RS-232 DB9 포트를 지원해야 한다. 콘솔 포트는 VP5200 스위치의 경우 전면에 탑재된다.

그림 1 >과 같이 VP5200 스위치가 제공하는 콘솔 포트에 운영 단말을 연결한다. 일단 연결이 설정되면, 프롬프트가 나오고 로그인 프로세스를 수행한다.

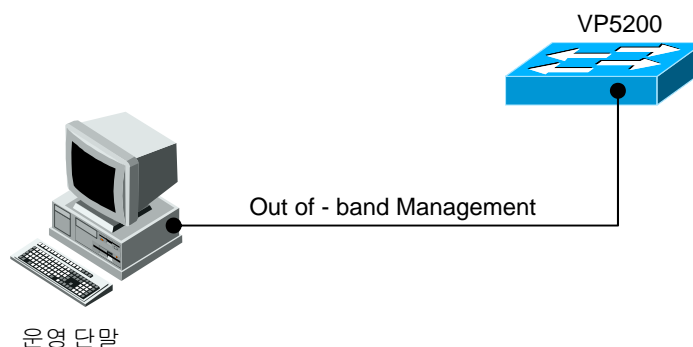


그림 1. VP5200 스위치와 운영 단말 연결

**Notice**

운영 단말의 설정 방법 및 콘솔 포트 핀 설정은 VP5200 스위치 하드웨어 설치 가이드를 참조하기 바란다.

2.4.2. Telnet 연결

시스템 운영자는 TCP/IP 및 telnet 접속 기능을 가지고 있는 워크스테이션을 통하여 VP5200 스위치에 접속할 수 있다. Telnet 을 사용하기 위하여, 운영자는 ID 및 비밀번호를 설정하여야 하며, 스위치는 적어도 하나 이상의 IP 주소를 가지고 있어야 한다.

```
telnet [<ipaddress> | <hostname>] {<port_number>}
```

Telnet 연결이 성공적으로 설정되며 사용자 패스워드를 입력하라는 프롬프트가 뜨고, telnet 사용자 패스워드를 입력하면 스위치의 *User* 모드로 들어가게 된다.

또한 시스템 보안을 위하여 액세스 리스트를 사용하여 telnet 에 연결하는 사용자를 제한할 수 있다. 이는 <2.9. ACL (Access Control List)>절을 참조하라.

2.4.3. SNMP Network Manager 를 통한 연결

Simple Network Management Protocol (SNMP)를 지원하는 어떠한 네트워크 관리기(Network Manager)를 통해서도 VP5200 스위치를 관리할 수 있다.

**Notice**

SNMP 에 대한 추가적인 정보는 <[2.7. SNMP](#)> 절을 참조하라.

2.5. 사용자 인증

2.5.1. 사용자 추가 및 삭제

시스템 운영자는 콘솔 포트나 telnet 을 통해서 스위치에 로그인 할 수 있다. 로그인을 위해서 사용

자 등록이 필요하다. VP5200 스위치는 사용자를 추가, 삭제 할 수 있고 각각의 사용자에게 패스워드와 권한, session timeout 시간, Access List 를 지정할 수 있다.

사용자 권한은 privilege level 로 표현된다. privilege level 은 15 인 경우와 아닌 경우로만 구분하고, 0 에서 14 사이의 privilege level 간의 구분은 사용하지 않는다. privilege level 이 15 인 사용자는 enable mode 로 들어갈 수 있고, 그 외의 privilege level 을 갖는 사용자는 Privileged mode 로 들어갈 수 없다. 새로운 사용자를 등록하면 privilege level 이 1 인 사용자로 등록된다.



Notice

Access List 에 대한 추가적인 정보는 < [2.8.ACL](#) > 절을 참조하라

표 5. 스위치의 사용자 추가 및 삭제 명령어

명령어	설명	모드
<code>username userID nopassword</code>	<ul style="list-style-type: none"> ■ userID 생성 ■ password 가 없다 	Config
<code>username userID (password secret) password</code> <code>username userID (password secret) 0 password</code>	<ul style="list-style-type: none"> ■ userID 생성 ■ 암호화되지 않은 password 를 입력받는다 	Config
<code>username userID (password 7 secret 5) password</code>	<ul style="list-style-type: none"> ■ userID 생성 ■ 암호화된 password 를 입력받는다 	Config
<code>username userID privilege <0-15> nopassword</code>	<ul style="list-style-type: none"> ■ userID 생성 ■ password 가 없다 ■ privilege 15 이면 가장높은 privilege(enable mode 진입허용)를 갖는다. 	Config
<code>username userID privilege <0-15> (password secret) password</code> <code>username userID privilege <0-15> (password secret) 0 password</code>	<ul style="list-style-type: none"> ■ userID 생성 ■ privilege 15 이면 가장높은 privilege(enable mode 진입허용)를 갖는다. ■ 암호화되지 않은 password 를 입력받는다 	Config
<code>username userID privilege <0-15> (password 7 secret 5) password</code>	<ul style="list-style-type: none"> ■ userID 생성 ■ privilege 15 이면 가장높은 privilege(enable mode 진입허용)를 갖는다. ■ 암호화된 password 를 입력받는다 	Config
<code>username userID timeout <0-</code>	<ul style="list-style-type: none"> ■ user 별 session timeout 시간(분) 설정(default 	Config

600>	20 분)	
no username <i>userID</i> timeout	<ul style="list-style-type: none"> ■ user 별 session timeout 시간(분) 삭제 ■ 초기 session timeout 시간(20 분)으로 되돌린다. 	Config
username <i>userID</i> access-class <i>access-list-num</i>	<ul style="list-style-type: none"> ■ 해당 user 에 Access List 를 적용 ■ <i>access-list-num</i> : <1-99> 이며, standard ip access list 를 의미 	Config
no username <i>userID</i> access-class	■ 해당 user 에 적용된 Access List 를 해제.	Config
no username <i>userID</i>	<ul style="list-style-type: none"> ■ userID 삭제 ■ userID 가 root 이면 삭제되지 않고 password 가 default passowrd 로 바뀐다. 	Config

사용자 추가 및 삭제

```

Switch# configure terminal
Switch# configure terminal
Switch(config)# username lns nopassword
Switch(config)# username test password test
Switch(config)# username ubi secret ubi
Switch(config)# username admin privilege 15 password admin
Switch(config)# username admin timeout 50
Switch(config)# end
Switch # show running-config
!
username lns nopassword
username test password 0 test
username ubi secret 0 ubi
username admin privilege 15 password 0 admin
username admin timeout 50
!
Switch#

```

2.5.2. 패스워드 설정

VP5200 스위치는 시스템 보안을 위해 다음과 같은 2 개의 패스워드를 사용한다.

- Enable 패스워드
 - Privileged 모드의 보안을 목적으로 사용
- 사용자 패스워드
 - 콘솔이나 telnet 을 통해 사용자 모드로 액세스 할 때 사용

표 6. 스위치의 Enable 패스워드 설정 명령어

명령어	설명	모드
enable password password	■ Privileged 모드 패스워드를 지정	Config
no enable password	■ Privileged 모드 패스워드를 삭제	Config
service password- encryption	■ password encryption mode 를 설정	Config
no service password- encryption	■ password encryption mode 를 삭제	Config



Notice

사용자 패스워드 설정명령은 <[2.5.1. 사용자 추가 및 삭제](#)>를 참고하라

Privileged 모드 패스워드 설정

```
Switch# configure terminal
Switch(config)# enable password lns
Switch(config)# end
Switch# show running-config
!
enable password 0 lns
!
Switch#
```

패스워드 encryption 설정

위의 예에서 보듯이 패스워드 설정 후 show running-config 명령으로 설정된 패스워드를 볼 수 있다. 이를 방지하기 위하여 VP5200 스위치는 패스워드 encryption 모드 설정을 지원한다.

```
Switch# configure terminal
Switch(config)# service password-encryption
Switch(config)# end
Switch# show running-config
```

```

!
enable password 7 xxEp88GxHJIgc
username lns nopassword
username test password 7 XX1LtDbOY4/E
username admin privilege 15 password 7 xxiz1FI3TBLPs
!
Switch#

```

2.5.3. 인증 방법 설정

2.5.3.1. 스위치에 login 시 인증 방법 설정

VP5200 스위치는 시스템에 접속하는 사용자에게 인증 방법을 다양하게 설정할 수 있다. 일반적으로는 스위치에 등록되어 있는 사용자의 ID와 패스워드를 사용하여 접속 권한이 주어지지만, 사용자 인증 프로토콜인 RADIUS와 TACACS+등을 이용하도록 설정하면 각각의 서버가 가지고 있는 데이터베이스에 기록된 사용자 정보를 사용하여 접속 권한이 주어진다.

사용자 인증 설정 명령어

명령어	설명	모드
authentication login authentication-type chap	■ tacacs server를 사용하여 인증할 경우 password를 chap 방식으로 암호화하여 전송한다.	Config
no authentication login authentication-type	■ tacacs server를 사용하여 인증할 경우 password를 암호화하지 않는다.	Config
authentication login enable (local radius tacacs)	■ 사용할 인증방식(local, radius, tacacs)을 선택한다. ■ 여러가지 인증방식을 선택할 수 있다.	Config
no authentication login enable (radius tacacs)	■ 사용하도록 설정된 인증방식을 사용하지 않도록 설정한다. ■ local 인증방식은 항상 사용한다.	Config
authentication login primary (local radius tacacs)	■ 우선적으로 인증받을 인증방식을 설정한다.	Config
no authentication login primary (local radius	■ 우선적으로 인증받도록 설정한 인증방식을 해제한다.	Config

tacacs)			
authentication login	■ radius 나 tacacs 로 인증받은 경우	Config	
template-user userID	Dummy user 를 지정할 수 있다.		
	■ 지정하는 Dummy user 는 local database 에 등록되어 있어야 한다.		
no authentication login	■ 설정한 Dummy user 를 해제한다.	Config	
template-user			
authorization exec tacacs	■ tacacs 로 인증받은 경우 tacacs 서버에서 privilege level 을 얻어온다.	Config	
no authorization exec tacacs	■ tacacs 서버에서 privilege level 을 얻어오지 않도록 한다.	Config	
show authentication login	■ 인증방식의 순서와 사용여부를 보여준다	Enable	

사용자 인증 설정

VP5200 스위치는 사용자 인증 방법으로 기존의 스위치에 등록되어 있는 사용자 ID와 패스워드를 사용하여 접속 권한 여부를 확인하는 방법과 RADIUS 서버를 이용하는 방법, TACACS+ 서버를 이용하는 방법이 있다. 이 3가지 방법을 선택적으로 사용하거나 모두 사용하도록 설정할 수 있다.

한가지 이상의 방법을 사용할 경우 먼저 우선순위가 높은 인증 방식으로 인증을 시도한다. local database를 사용하여 인증하는 경우, local database에서 등록되지 않은 사용자로 인증을 시도하면 다음 우선순위를 갖는 인증 방식으로 인증을 시도하고, 인증에 실패하면 ID와 패스워드를 다시 요청한다. RADIUS나 TACACS+ 서버를 사용하여 인증하는 경우, 서버와 통신을 하지 못해 인증을 시도할 수 없으면 다음 우선순위를 갖는 인증 방식으로 인증을 시도하고, 인증에 실패하면 ID와 패스워드를 다시 요청한다.

Switch# configure terminal		
Switch(config)# authentication login enable radius		
Switch(config)# authentication login enable tacacs		
Switch(config)# authentication login primary radius		
Switch(config)# authentication login primary tacacs		
Switch(config)# end		
Switch # show authentication login		
precedence	method	status
-----	-----	-----
first	tacacs	enable
second	radius	enable
third	local	enable
Switch#		

2.5.3.2. privileged mode 진입시 인증 방법 설정

VP5200 스위치는 privileged mode 로 들어올 때 사용자에게 대한 인증 방법을 다양하게 설정할 수 있다. 일반적으로는 스위치에 등록되어 있는 **enable** 패스워드를 사용하여 접속 권한이 주어지지만, 사용자 인증 프로토콜인 **TACACS+**를 이용하도록 설정하면 각각의 서버가 가지고 있는 데이터베이스에 기록된 정보를 사용하여 접속 권한이 주어진다.

사용자 인증 설정 명령어

명령어	설명	모드
authentication enable enable (local tacacs)	<ul style="list-style-type: none"> ■ 사용할 인증방식(local, tacacs)을 선택한다. ■ 여러가지 인증방식을 선택할 수 있다. 	Config
no authentication enable enable (tacacs)	<ul style="list-style-type: none"> ■ 사용하도록 설정된 인증방식을 사용하지 않도록 설정한다. ■ local 인증방식은 항상 사용한다. 	Config
authentication enable primary (local tacacs)	<ul style="list-style-type: none"> ■ 우선적으로 인증받을 인증방식을 설정한다. 	Config
no authentication enable primary (local tacacs)	<ul style="list-style-type: none"> ■ 우선적으로 인증받도록 설정한 인증방식을 해제한다. 	Config
show authentication enable	<ul style="list-style-type: none"> ■ 인증방식의 순서와 사용여부를 보여준다 	Enable

사용자 인증 설정

VP5200 스위치는 privileged mode 로 들어올 때 사용자 인증 방법으로 기존의 스위치에 등록되어 있는 **enable** 패스워드를 사용하여 접속 권한 여부를 확인하는 방법과 **TACACS+** 서버를 이용하는 방법이 있다. 이 2 가지 방법을 선택적으로 사용하거나 모두 사용하도록 설정할 수 있다.

한가지 이상의 방법을 사용할 경우 먼저 우선순위가 높은 인증 방식으로 인증을 시도한다. local database 를 사용하여 인증하는 경우, local database 에서 등록되지 않은 사용자로 인증을 시도하면 다음 우선순위를 갖는 인증 방식으로 인증을 시도하고, 인증에 실패하면 **enable** 패스워드를 다시 요청한다. **TACACS+** 서버를 사용하여 인증하는 경우, 서버와 통신을 하지 못해 인증을 시도할 수 없으면 다음 우선순위를 갖는 인증 방식으로 인증을 시도하고, 인증에 실패하면 **enable** 패스워드를 다시 요청한다.

```

Switch# configure terminal
Switch(config)# authentication enable enable tacacs
Switch(config)# authentication enable primary tacacs
Switch(config)# end
Switch # show authentication enable
precedence      method      status
-----
first           tacacs      enable
second          local      enable

Switch#

```

2.5.4. 인증 서버 설정

RADIUS 서버 설정 명령어

명령어	설명	모드
radius-server host A.B.C.D	■ radius-server 설정한다.	Config
no radius-server host A.B.C.D	■ 설정된 radius-server 삭제한다.	Config
radius-server host A.B.C.D key encryption-key	■ radius-server 설정한다. ■ 해당 server 에 접속할 때 사용하는 encryption key 를 설정한다.	Config
radius-server host A.B.C.D auth-port <0-65536>	■ radius-server 설정한다. ■ 해당 server 에 접속할 때 사용하는 auth-port 를 설정한다.	Config
no radius-server host A.B.C.D auth-port	■ 해당 server 에 접속할 때 사용하는 auth-port 를 삭제한다.(삭제되면 default auth-port 를 사용한다.)	Config
radius-server host A.B.C.D auth-port <0-65536> key encryption-key	■ radius-server 설정한다. ■ 해당 server 에 접속할 때 사용하는 auth-port 를 설정한다. ■ 해당 server 에 접속할 때 사용하는 encryption key 를 설정한다.	Config
radius-server encryption-key	■ radius-server 에 접속할 때 사용하는 general key 설정한다.	Config

	■ server 에 key 가 지정되지 않으면 이 general key 를 사용한다.	
no radius-server key	■ 설정된 general key 를 삭제한다.	Config
radius-server retransmit <1-5>	■ radius-server 에 접속할 때의 재시도 횟수를 설정한다.	Config
no radius-server retransmit	■ 설정된 재시도 횟수를 삭제한다.(default 3 회)	Config
radius-server timeout <1-1000>	■ 응답 패킷을 받아야하는 시간을 지정한다.	Config
no radius-server timeout	■ 설정된 timeout 시간을 삭제한다.(default 5 초)	Config

RADIUS 서버 설정

여러 개의 RADIUS 서버를 설정 할 수 있다. 먼저 설정된 서버와 통신을 하지 못해 인증을 시도할 수 없으면 다음 서버로 인증을 시도한다.

```
Switch# configure terminal
Switch(config)# radius-server host 192.168.0.1
Switch(config)# radius-server key test123
Switch(config)# radius-server host 192.168.0.2 key lns
Switch(config)# radius-server host 192.168.0.2 auth-port 3000
Switch(config)# end
Switch# show running-config
!
radius-server key test123
radius-server host 192.168.0.1
radius-server host 192.168.0.2 key lns
radius-server host 192.168.0.3 auth-port 3000
!
Switch#
```

TACACS+ 서버 설정 명령어

명령어	설명	모드
tacacs-server host A.B.C.D key encryption-key	■ tacacs -server 설정한다. ■ 해당 server 에 접속할 때 사용하는	Config

			encryption key 를 설정한다.	
no	tacacs-server	host A.B.C.D	■ 설정된 tacacs -server 삭제한다.	Config
tacacs-server	host A.B.C.D	■ tacacs -server 설정한다.		Config
timeout	<1-1000>	key encryption-key	■ 응답 패킷을 받아야하는 시간 timeout 을 지정한다.	
			■ 해당 server 에 접속할 때 사용하는 encryption key 를 설정한다	
tacacs-server	host A.B.C.D	■ tacacs -server 설정한다.		Config
timeout	<1-1000>		■ 응답 패킷을 받아야하는 시간 timeout 을 지정한다.	

TACACS+ 서버 설정

여러 개의 TACACS+ 서버를 설정 할 수 있다. 먼저 설정된 서버와 통신을 하지 못해 인증을 시도할 수 없으면 다음 서버로 인증을 시도한다.

```
Switch# configure terminal
Switch(config)# tacacs-server host 192.168.0.1 key lns
Switch(config)# tacacs-server host 192.168.0.2 key test123
Switch(config)# end
Switch# show running-config
!
tacacs-server host 192.168.0.1 key lns
tacacs-server host 192.168.0.2 key test123
!
Switch#
```

2.6. Hostname 설정

Hostname 은 운영 시 시스템을 구별하기 위해 사용될 수 있으며 따라서 콘솔/Telnet 화면의 프롬프트는 hostname 과 현재 명령어 모드의 조합으로 이루어져 있다. VP5200 스위치는 default 로 “Switch”를 hostname 으로 사용하며 운영자가 이를 변경할 수 있다.

표 7. Hostname 설정 명령어

명령어	설명	모드
hostname <i>string</i>	■ Hostname 을 변경	Config
no hostname	■ Hostname 을 default 값으로 변경	Config

Hostname 을 설정 및 변경하는 절차는 다음과 같다.

```
Switch# configure terminal
Switch(config)# hostname VP5208
VP5208(config)# end
VP5208#

VP5208# configure terminal
VP5208(config)# no hostname
Switch(config)# end
Switch#
```

2.7. SNMP (Simple Network Management Protocol)

SNMP Network Manager 는 Management Information Base(MIB)을 제공하는 스위치를 관리할 수 있다. 각각의 Network Manager 는 관리의 편의를 위해서 사용자 인터페이스를 제공한다. SNMP manager 로 VP5200 스위치를 관리하고자 할 때는 스위치의 환경 설정이 필요하다.

또한 SNMP 에이전트를 접근하기 위해서는 스위치에 하나 이상의 IP 주소 설정이 필요하다. IP 주소의 설정은 “VP5200 User Guide_제 05 장_IP 환경 설정” 문서를 참고하라.

표 8. SNMP 환경 설정 명령

명령어	설명	모드
snmp-server agent-address <i>agent-addr</i>	■ 스위치에서 전송하는 snmp 패킷의 출발지 IP 를 지정	Config
no snmp-server agent-address <i>agent-addr</i>	■ 스위치에서 전송하는 snmp 패킷의 출발지 IP 를 지정하지 않음	Config

snmp-server contact <i>string</i>	■ System contact 정보를 변경	Config
no snmp-server contact <i>string</i>	■ System contact 정보를 삭제	Config
snmp-server location <i>string</i>	■ System location 정보를 변경	Config
no snmp-server location <i>string</i>	■ System location 정보를 삭제	Config
snmp-server community <i>string</i> [ro rw [access-class <i>number</i>]]	■ SNMP community 를 설정 ■ <i>ro</i> : read only ■ <i>rw</i> : read write ■ <i>number</i> : standard IP access-list <1-99>	Config
no snmp-server community <i>string</i>	■ SNMP Community 를 삭제	Config
snmp-server enable traps [<i>notification-type</i>] [<i>notification-option</i>]	■ SNMP Trap 을 Trap-Host 에게 전송하도록 설정 ■ <i>notification-type</i> : trap 그룹 (config, environ, multicast, other, perform, resource, security, snmp) ■ <i>notification-option</i> : 각 trap 그룹에 속한 개별 trap 항목	Config
no snmp-server enable traps	■ SNMP Trap 을 Trap-Host 에게 전송하지 않도록 설정	Config
snmp-server trap-host <i>A.B.C.D</i> community <i>string</i>	■ SNMP Trap-Host 와 SNMP trap 을 전송할 때 사용할 community 를 설정	Config
no snmp-server trap-host <i>A.B.C.D</i>	■ SNMP Trap Host 를 삭제	Config
snmp-server trap-version 1	■ SNMPv1 Trap 을 전송하도록 설정	Config
no snmp-server trap-version	■ SNMPv2 Trap 을 전송하도록 설정	Config

SNMP Community 설정

Community string 은 시스템과 원격 네트워크 관리자 사이의 간단한 상호 인증 기능을 제공한다. VP5200 스위치는 두 가지 형태의 community string 을 지원한다.

- Read community strings
 - 시스템에 읽기 전용(read-only)으로 접속
 - 기본 읽기 전용 설정은 public
- Read-write community strings
 - 시스템에 읽기 및 쓰기(read and write) 접속

- 기본 읽기 및 쓰기 설정은 private

```
Switch# configure terminal
Switch(config)# snmp-server community public ro
Switch(config)# snmp-server community private rw
Switch(config)# snmp-server community test1 rw access-class 1
Switch(config)# end
Switch# show running-config
!
snmp-server community public ro
snmp-server community private rw
snmp-server community test1 rw access-class 1
!
Switch#
```



Notice

access-class 설정은 < [2.9.ACL](#) >절을 참고하라

SNMP Trap 설정

하나 이상의 네트워크 관리 단말이 인증된 trap receiver로서 설정될 수 있다. VP5200 스위치는 모든 trap receiver에게 SNMP trap을 전송한다.

```
Switch# configure terminal
Switch(config)# snmp-server trap-version 1
Switch(config)# snmp-server enable traps
Switch(config)# snmp-server trap-host 192.168.0.3 community private
Switch(config)# end
Switch# show running-config
!
snmp-server trap-version 1
snmp-server trap-host 192.168.0.3 community private
snmp-server enable traps config slotAdd slotDel GBICAdd GBICDel
powerStatus fanStatus selfLoopDetect fanActivateStatus
snmp-server enable traps environ tempUpRise tempUpFall tempLowRise
tempLowFall
snmp-server enable traps multicast snoop snoopVlan proxyReport
proxyReportVlan
snmp-server enable traps other change setResponse
snmp-server enable traps perform rmonRise rmonFall bpsRise bpsFall
```

```

ppsRise ppsFall sysMacRise sysMacFall cpuMacFilter
snmp-server enable traps resource cpuUsageRise cpuUsageFall
memUsageRise memUsageFall
snmp-server enable traps security remoteConnect
snmp-server enable traps snmp coldStart warmStart linkDown linkUp
authFail
!
Switch#

```



Notice

VP5200 에서 지원하는 SNMP Trap 은 모든 스위치를 포괄한다. ‘snmp-server enable traps’ 명령으로 모든 SNMP Trap 을 설정할 경우 현재 스위치에서 지원하지 않는 SNMP Trap 의 내용도 running-config 에 포함될 수 있다.

SNMP 패킷의 출발지 IP 설정

스위치에서 하나 이상의 Network Manager 로 SNMP Packet 을 전송할 때, 전송되는 SNMP 패킷의 출발지 IP 를 특정 Local IP address 로 설정할 수 있다.

```

Switch# configure terminal
Switch(config)# snmp-server agent-address 210.48.148.125
Switch(config)# end
Switch# show running-config
!
snmp-server agent-address 210.48.148.125
!
Switch#

```

시스템 담당자 설정

```

Switch# configure terminal
Switch(config)# snmp-server contact "gil-dong hong. hong@ubiquoss.com"
Switch(config)# end
Switch# show running-config
!
snmp-server contact "gil-dong hong. hong@ubiquoss.com"
!
Switch#

```

시스템 구축 위치 설정

```
Switch# configure terminal
Switch(config)# snmp-server location "Dogok-Dong, GangNam-gu, Seoul."
Switch(config)# end
Switch# show running-config
!
snmp-server location "Dogok-Dong, GangNam-gu, Seoul."
!
Switch#
```

2.8. ACL (Access Control List)

액세스 리스트(Access Control List)를 사용함으로써 네트워크 관리자는 인터넷네트워크를 통해 전송되는 트래픽에 대해 상당히 세밀한 통제를 할 수 있다. 관리자는 패킷의 전송 상태에 대한 기본적인 통계 자료를 얻을 수 있고 이를 통해 보안 정책을 수립할 수 있다. 또한 인증되지 않은 액세스로부터 시스템을 보호할 수 있다. 액세스 리스트는 라우터를 통해 전달되는 패킷을 허용하거나 거부하기 위해 사용할 수도 있고 Telnet(vty)이나 SNMP를 통한 라우터의 접속에도 적용할 수 있다.

VP5200 스위치는 표준 IP 액세스 리스트를 지원하며, <1-99>의 번호가 할당 될 수 있다.

표 9. 액세스 리스트 설정 명령

명령어	설명	모드
access-list <1-99> {deny permit} address	■ 표준 IP 액세스 리스트를 설정 ■ address ::= {any A.B.C.D/M}	Config
no access-list <1-199>	■ 액세스 리스트를 삭제	Config

2.8.1. 액세스 리스트 생성 규칙

- 좀더 좁은 범위의 것을 먼저 선언한다.
- 빈번히 조건을 만족시킬만한 것을 먼저 선언한다.
- Access-list 의 마지막에 특별히 'permit any' 를 지정하지 않는 한 기본적으로 'deny any' 가 선언되어 있다.

- Access-list 의 조건을 여러 줄에 선언을 하는데 임의의 줄과 줄 사이의 것을 지우거나 수정할 수 없고, 새로 추가하는 필터는 마지막에 더해진다.

2.8.2. 표준 IP 액세스 리스트 설정

2.8.2.1. 모든 액세스 허용

```
Switch# configure terminal
Switch(config)# access-list 1 permit any
Switch(config)# end
Switch# show access-list
Access-List 1
            permit any
```

2.8.2.2. 모든 액세스 거부

```
Switch# configure terminal
Switch(config)# access-list 1 deny any
Switch(config)# end
Switch# show access-list
Access-List 1
            deny any
```

2.8.2.3. 특정 호스트에서의 액세스만 허용

```
Switch# configure terminal
Switch(config)# access-list 1 permit 192.168.0.3/32
Switch(config)# end
Switch# show access-list
Access-List 1
            permit 192.168.0.3/32
```

2.8.2.4. 특정 네트워크에서의 액세스만 허용

```
Switch# configure terminal
Switch(config)# access-list 1 permit 192.168.0.0/24
Switch(config)# end
```

```
Switch# show access-list
Access-List 1
    permit 192.168.0.0/24
```

2.8.2.5. 특정 네트워크에서의 액세스만 거부

```
Switch# configure terminal
Switch(config)# access-list 1 deny 192.168.0.0/24
Switch(config)# access-list 1 permit any
Switch(config)# end
Switch# show access-list
Access-List 1
    deny 192.168.0.0/24
    permit any
```

2.8.3. SNMP 연결에 액세스 리스트 설정

액세스 리스트는 community 별로 적용되며, 설정된 액세스 리스트는 snmp 를 통한 스위치로의 접속을 허용, 제한한다.

host 10.1.22.247 에서의 접속만을 허용하는 Access list 를 생성하여, snmp 접속을 제한하고자 할 때의 절차는 다음과 같다.

```
Switch# configure terminal
Switch(config)# access-list 1 permit 10.1.22.247/32
Switch(config)# snmp-server community lns ro access-class 1
Switch# show running-config
!
snmp-server community lns ro access-class 1
!
access-list 1 permit 10.1.22.247/32
!
Switch#
```

2.8.4. Telnet 연결에 액세스 리스트 설정

액세스 리스트는 user 별로 적용되며, 설정된 액세스 리스트는 외부에서 스위치로의 접속을 허

용, 제한한다.

192.168.0.0/24 네트워크에서의 접속만을 허용하는 Access list 를 생성하여, telnet 접속을 제한하고자 할 때의 절차는 다음과 같다.

```
Switch# configure terminal
Switch(config)# access-list 1 permit 192.168.0.0/24
Switch(config)# username admin access-class 1
Switch# show running-config
!
username admin privilege 15 password 0 admin
username admin access-class 1
!
access-list 1 permit 192.168.0.0/24
!
Switch#
```

2.9. NTP 설정

2.9.1. NTP 개요

NTP (Network Time Protocol)는 네트워크를 통하여 시스템의 시간을 동기화하는 데 사용 되는 프로토콜이다. NTP 는 UDP (User Datagram Protocol)위에서 동작하며, 모든 NTP 메시지의 시간 정보는 Greenwich Mean Time 과 동일한 Coordinated Universal Time (UTC)를 사용한다.

2.9.2. NTP client mode 설정

NTP client 모드로 동작하도록 하기 위해서는 global 설정 모드에서 다음의 명령을 사용한다.

명령어	설명
ntp server address	■ NTP server 를 설정한다. (5 개까지 설정가능)
no ntp server address	■ NTP server 를 삭제한다.

2.9.3. NTP Server mode 설정

NTP server mode 로 동작하도록 하기 위해서는 global 설정 모드에서 다음의 명령을 사용한다.

명령어	설명
ntp master <i>stratum</i>	■ NTP master 로 동작하도록 한다.
no ntp master	■ NTP master로서의 동작을 멈춘다.

2.9.4. NTP time zone 설정

NTP server 나 client 를 지역에 따라 다른 **timezone** 을 설정하여 해당 지역에서 현재 사용되는 정확한 시간으로 표시한다.

명령어	설명
ntp timezone plus <i>HH:MM</i>	■ 설정된 Coordinated Universal Time (UTC)에 설정된 시간을 더하여 현재 시간을 표시한다.
ntp timezone minus <i>HH:MM</i>	■ 설정된 Coordinated Universal Time (UTC)에 설정된 시간을 빼서 현재 시간을 표시한다.
no ntp timezone	■ Coordinated Universal Time (UTC)로 설정한다.

2.9.5. NTP summer time 설정

지역에 따라 summer time(daylight savings time)을 사용하는 곳이 있다. 이는 낮 시간이 긴 여름기간 동안 시간을 한시간 당겨 시간을 효율적으로 쓰고자 하기 위한 것이다.

명령어	설명
ntp summer-time <i>week day month hh:mm week day month hh:mm</i>	■ Summer time 이 시작하는 때와 끝나는 때를 지정하여 적용한다.
no ntp summer-time	■ Summer time 을 적용하지 않는다.

2.9.6. NTP 기타 명령어

명령어	설명
ntp poll-interval <i>number</i>	■ NTP client mode 로 동작할 시, 설정된 NTP server 로 NTP request message 를 전송하는 간격, 2 의 배수로 동작하며 <4-17>의 범위를 가진다.
show ntp	■ NTP 에 대한 사항을 보여준다.

2.9.7. NTP 설정 예제

ntp server 203.248.240.103 에서 ntp 시간을 받아오려 할 경우 다음과 같이 설정하고 확인한다.

```
Switch#
Switch (config)# ntp server 203.248.240.103
Switch (config)# exit
Switch # show ntp
-----
Current time      : Thu Jan 12 20:40:25 2009
-----
NTP master        : disable
NTP stratum       : unspecified
Poll interval     : 6 (power of 2)
NTP timezone      : GMT
NTP summertime    : none
NTP summertime start : none
NTP summertime end   : none
-----
The list of NTP Server is below.
-----
[1] 203.248.240.103
-----
Switch #
```

timezone 정보를 우리나라에 맞게 변경하려 할 경우 다음과 같이 설정하고 확인한다.

```
Switch#
Switch# configure terminal
Switch(config)# ntp timezone plus 9:0
Switch(config)# end
```

```
Switch# show clock
Mon Jan 14 10:58:36 2008  GMT+9:0
Switch# show ntp
-----
Current time      : Mon Jan 14 10:58:39 2008
-----
NTP master        : disable
NTP stratum       : unspecified
Poll interval     : 6 (power of 2)
NTP timezone      : +9:0
NTP summertime    : none
NTP summertime start : none
NTP summertime end   : none
-----
The list of NTP Server is below.
-----
-----
Switch#
```