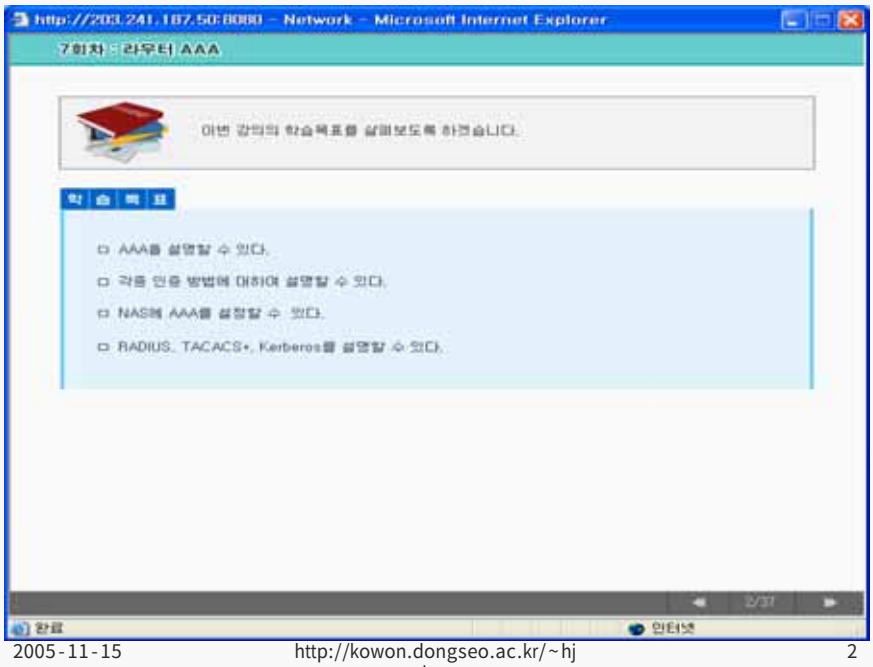
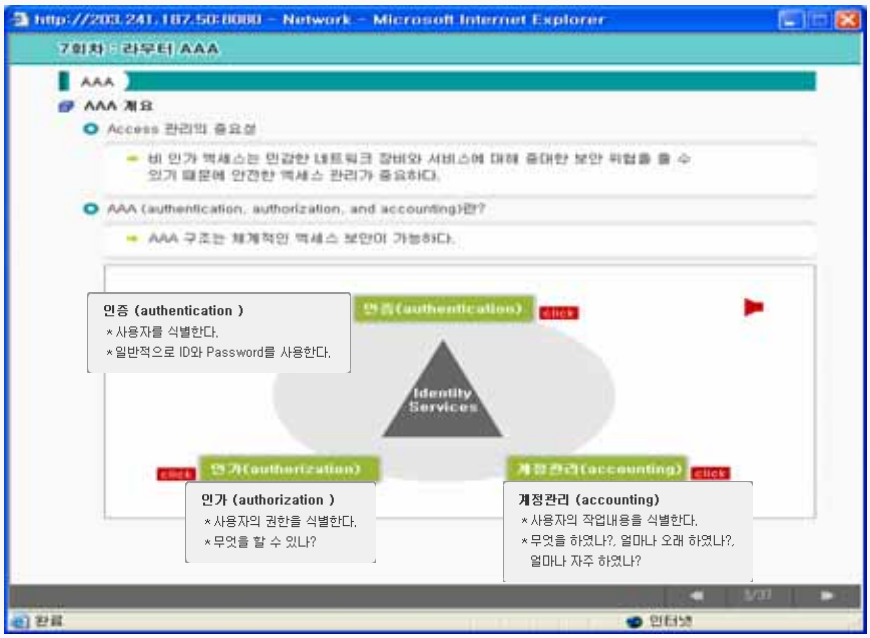
FNS

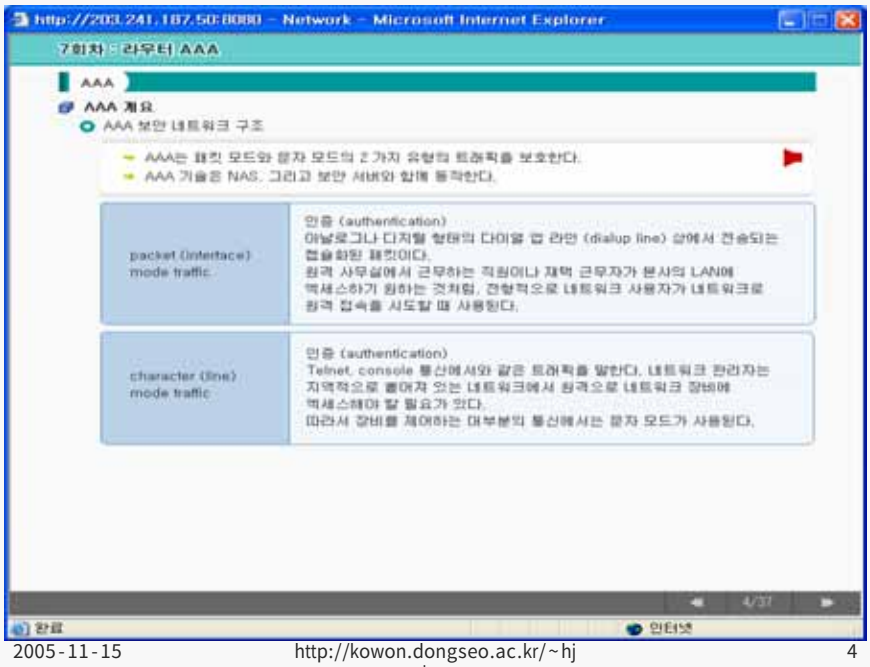
(Fundamental Network Security)

Ch7. 라우터 AAA(Authentication, Authorization, Accounting)

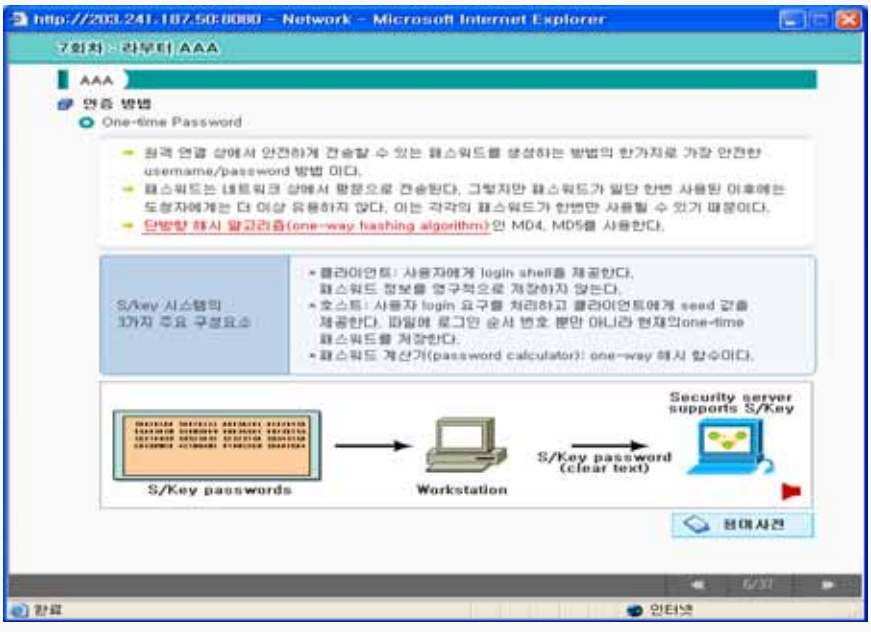
동서대학교/인터넷공학부
이 훈 재
hjlee@dongseo.ac.kr
http://kowon.dongseo.ac.kr/~hjlee
http://crypto.dongseo.ac.kr



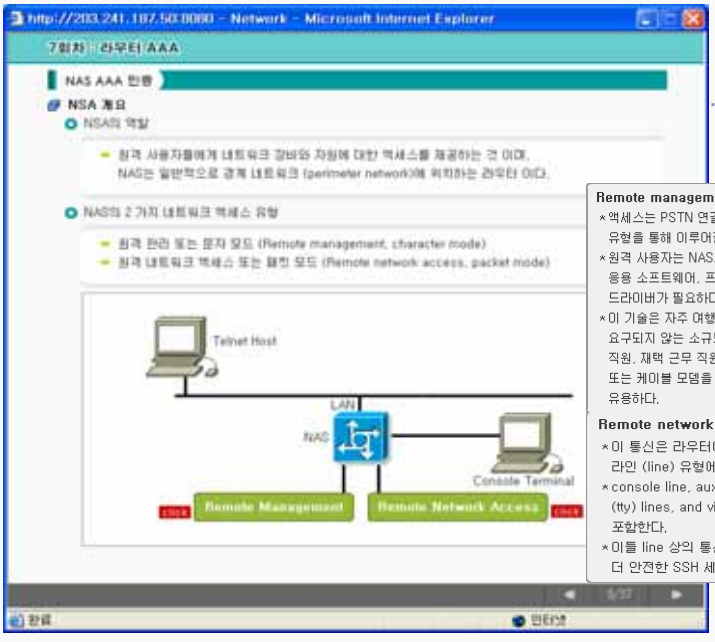

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
7회차 : 라우터 AAA
AAA
AAA 개요
Access 관리의 중요성
AAA (authentication, authorization, and accounting)란?
AAA 구조는 체계적인 액세스 보안이 가능하다.
인증 (authentication)
* 사용자를 식별한다.
* 일반적으로 ID와 Password를 사용한다.
인증(authentication)
click
Identity Services
인가(authorization)
click
계정관리(accounting)
click
인가 (authorization)
* 사용자의 권한을 식별한다.
* 무엇을 할 수 있나?
계정관리 (accounting)
* 사용자의 작업내용을 식별한다.
* 무엇을 하였나?, 얼마나 오래 하였나?,
얼마나 자주 하였나?
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
7회차 : 라우터 AAA
AAA
AAA 개요
AAA 보안 네트워크 구조
AAA는 패킷 모드와 문자 모드의 2 가지 유형의 트래픽을 보호한다.
AAA 기술은 NAS, 그리고 보안 서버와 함께 동작한다.
packet (interface) mode traffic
인증 (authentication)
아날로그나 디지털 형태의 다이얼 업 라인 (dialup line) 상에서 전송되는 캡슐화된 패킷이다.
원격 사무실에서 근무하는 직원이나 재택 근무자가 본사의 LAN에 액세스하기 위하는 것처럼, 전형적으로 네트워크 사용자가 네트워크로 원격 접속을 시도할 때 사용된다.
character (line) mode traffic
인증 (authentication)
Telnet, console 통신에서와 같은 트래픽을 말한다. 네트워크 관리자는 지역적으로 흩어져 있는 네트워크에서 원격으로 네트워크 장비에 액세스해야 할 필요가 있다.
따라서 장비를 제어하는 대부분의 통신에서는 문자 모드가 사용된다.
완료
인터넷

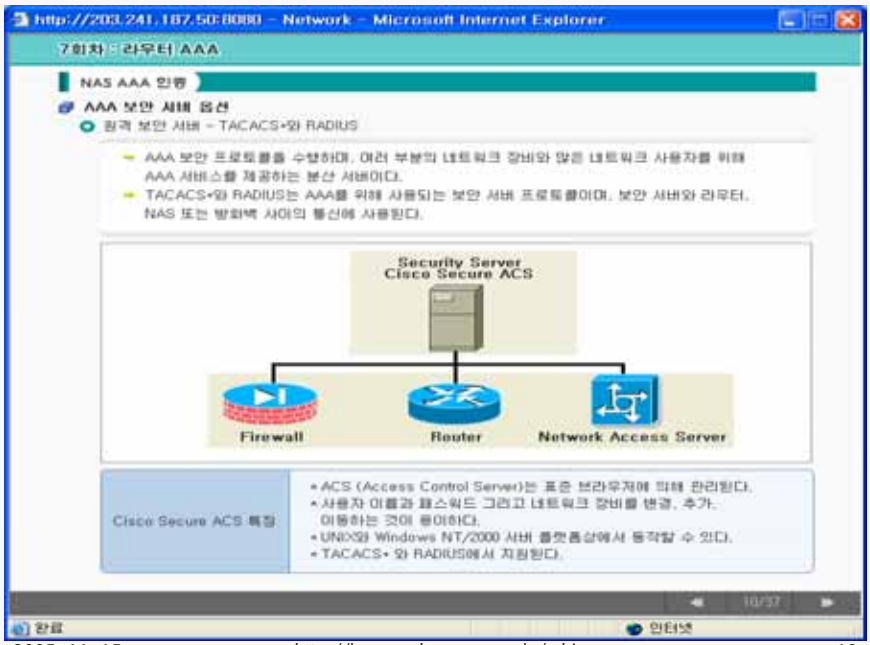

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
7회차 : 라우터 AAA
AAA
인증 방법
인증
AAA 보안 과정의 첫번째 단계는 인증이다.
일반적인 인증 방법은 다음과 같다.
• Username/password 방법
• One-time Password 방법
• Token card/soft token 방법
username/password
최소한의 보안 옵션이다.
static과 aging의 2가지 방법이 있다.
static username/password
사용자 이름과 패스워드가 시스템 관리자나 사용자에 의해 변경되기 전 까지 동일하게 남아있다.
• playback 공격, 도청, 절도(theft), 그리고 패스워드 크래킹 프로그램에 취약하다.
• 공격자가 일단 패스워드를 알아 액세스 하게 되면 관리자나 사용자가 패스워드를 변경하기 전까지는 계속해서 액세스할 수 있다.
aging username/password
• 사용자로 하여금 임의의 설정 시간 이후에 패스워드를 변경하도록 강요하는 방식이다.
• 일반적으로 변경 주기는 30~60일이다.
• 그러나 여전히 playback 공격, 도청, 절도(theft), 그리고 패스워드 크래킹 프로그램에 취약하다.
5/37
완료
인터넷

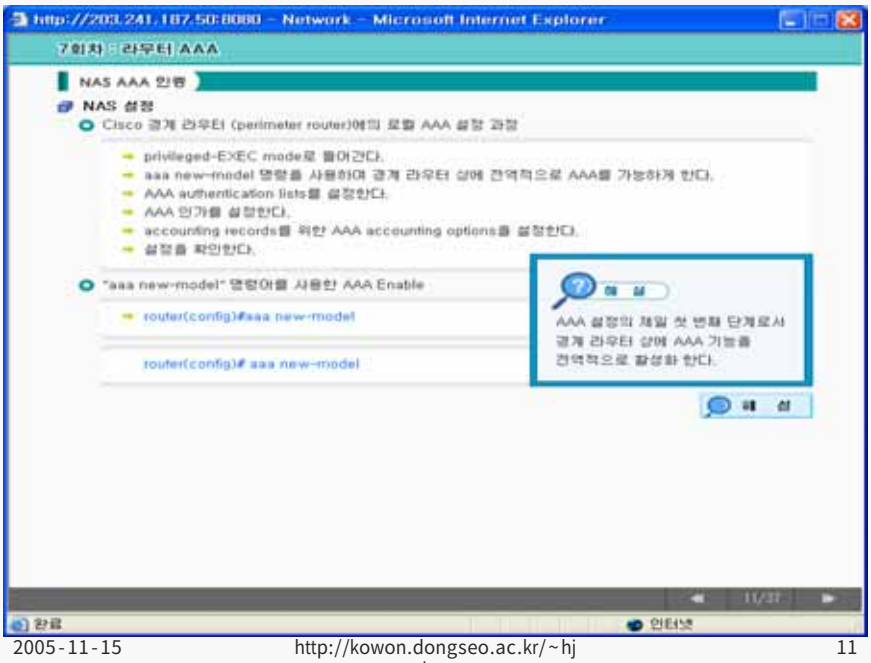

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
7회차 : 라우터 AAA
AAA
인증 방법
One-time Password
최적 연결 상에서 안전하게 전송할 수 있는 패스워드를 생성하는 방법의 한가지로 가장 안전한 username/password 방법 이다.
패스워드는 네트워크 상에서 평문으로 전송된다. 그렇지만 패스워드가 일단 한번 사용된 이후에는 도청자에게는 더 이상 유용하지 않다. 이는 각각의 패스워드가 한번만 사용될 수 있기 때문이다.
단방향 해시 알고리즘(one-way hashing algorithm)인 MD4, MD5를 사용한다.
S/key 시스템의 3가지 주요 구성요소
• 클라이언트: 사용자에게 login shell을 제공한다. 패스워드 정보를 영구적으로 저장하지 않는다.
• 호스트: 사용자 login 요구를 처리하고 클라이언트에게 seed 값을 제공한다. 파일에 로그인 순서 번호 뿐만 아니라 현재의one-time 패스워드를 저장한다.
• 패스워드 계산기(password calculator): one-way 해시 함수이다.
S/Key passwords
Workstation
S/Key password (clear text)
Security server supports S/Key
6/37
완료
인터넷

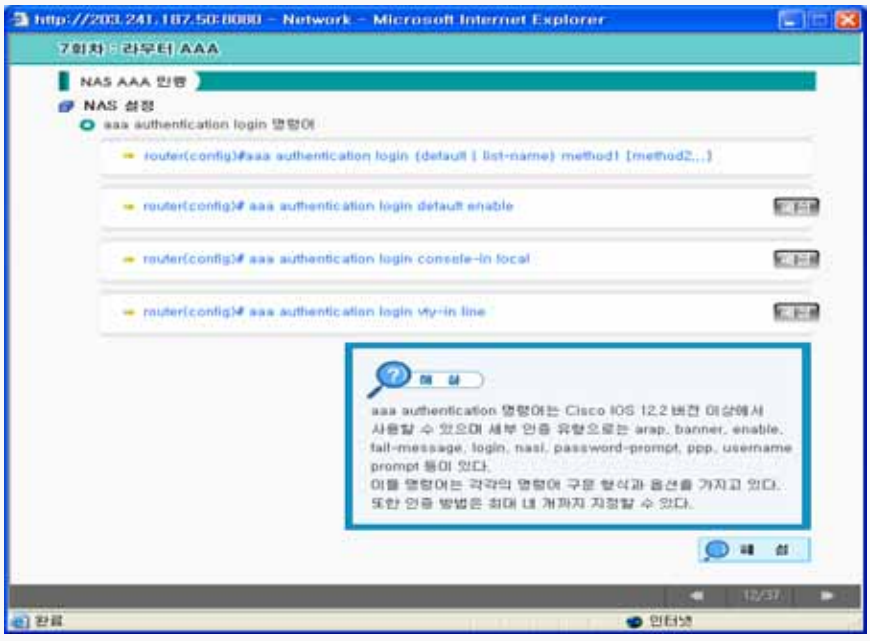

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
7회차 : 라우터 AAA
AAA
인증 방법
Token card 방법
Token card 또는 smart card와 token server를 사용하는 새로운 보안 계층이 추가된
One-time password 인증 방법이다.
Token card는 특정한 사용자를 위해 프로그램 되어 있고, 사용자는 유일한 PIN을 갖는다.
1.
2.
3.
(OTP)
4.
Cisco Secure ACS
Token server
Token card와 서버 방법
1. time-based
- 토큰 카드는 암호화 키를 포함하고 있으며, 사용자에 의해 입력된 PIN을 사용하여 패스워드나 토큰을 생성한다.
- 패스워드는 원격 클라이언트에 입력되고 토큰 서버로 보내진다.
- 패스워드는 토큰 서버의 시간으로 동기화된다.
- 서버는 받은 토큰과 내부적으로 발생된 토큰을 비교하여 이것이 일치하면 인증하고 액세스를 허용한다.
2. Challenge-response
- 토큰 카드는 암호화 키를 저장한다.
- 토큰 서버는 여러 수의 무작위 스트링을 생성하여 원격 클라이언트에게 보낸다.
- 원격 사용자는 무작위 스트링을 입력하고 토큰 카드는 저장된 키를 사용하여 암호화 함수를 계산한다.
- 계산 결과는 토큰 서버로 되돌려 보내지고 토큰 서버 또한 동일한 암호화 함수를 계산한다.
이 두 개의 계산 결과가 일치할 경우 사용자를 인증한다.
여기서 공부!
완료
인터넷

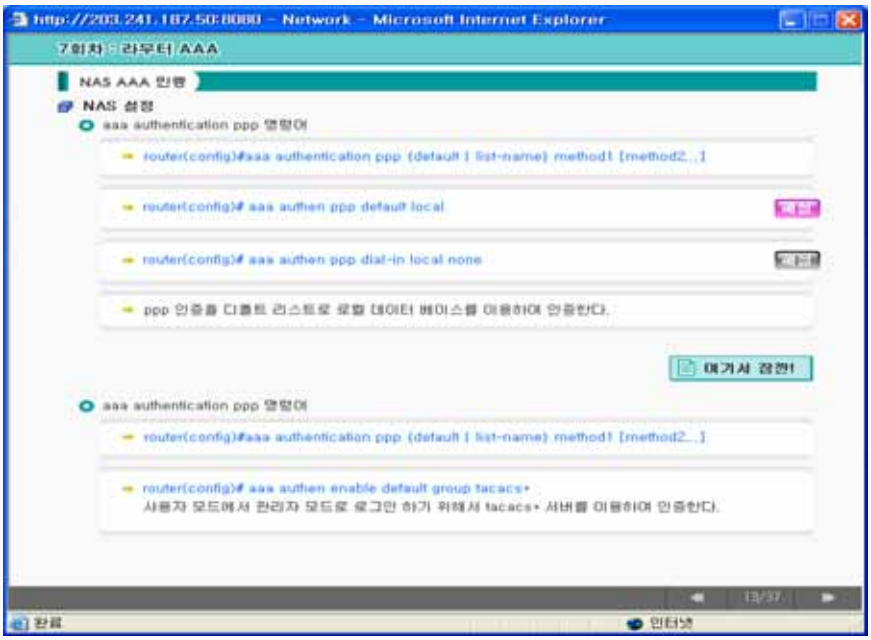

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
7회차 : 라우터 AAA
NAS AAA 인증
NSA 개요
NSA의 역할
원격 사용자들에게 네트워크 장비와 자원에 대한 액세스를 제공하는 것 이며,
NAS는 일반적으로 경계 네트워크 (perimeter network)에 위치하는 라우터 이다.
NAS의 2 가지 네트워크 액세스 유형
원격 관리 또는 문자 모드 (Remote management, character mode)
원격 네트워크 액세스 또는 패킷 모드 (Remote network access, packet mode)
Telnet Host
LAN
NAS
Console Terminal
Remote Management
Remote Network Access
Remote management
* 액세스는 PSTN 연결 또는 디지털 ISDN 연결 유형을 통해 이루어질 수 있다.
* 원격 사용자는 NAS로 액세스 하기 위해 적합한 응용 소프트웨어, 프로토콜 스택, 링크 계층 드라이버가 필요하다.
* 이 기술은 자주 여행하는 직원, 큰 대역폭이 요구되지 않는 소규모 원격 사무실에서 근무하는 직원, 재택 근무 직원 그리고 다이얼 업, DSL 또는 케이블 모뎀을 경유한 연결에 특히 유용하다.
Remote network access
* 이 통신은 라우터에 의해 제공되는 다양한 라인 (line) 유형에 걸쳐 일어날 수 있다.
* console line, auxiliary line, asynchronous (tty) lines, and virtual terminal (vty) line을 포함한다.
* 이들 line 상의 통신은 telnet 이나 이보다 좀 더 안전한 SSH 세션에 의해 확립될 수 있다.
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
7회차 : 라우터 AAA
NAS AAA 인증
AAA 보안 서버 옵션
AAA access control 에 사용되는 2 가지 방법
Cisco 네트워크 제품은 local 보안 DB 또는 원격 보안 DB를 사용하는
AAA access control을 지원한다.
로컬 보안 DB
작은 그룹의 네트워크 사용자를 위해 NAS 상에서 실행된다.
Network Access Server
로컬 인증의 특징
• 소규모 네트워크를 위해 사용한다.
• 사용자 이름과 패스워드는 Cisco 라우터에 저장된다.
• 사용자는 Cisco 라우터 내의 로컬 보안 DB와 대조하여 인증한다.
• 외부 DB를 요구하지 않는다.
5/37
완료
인터넷

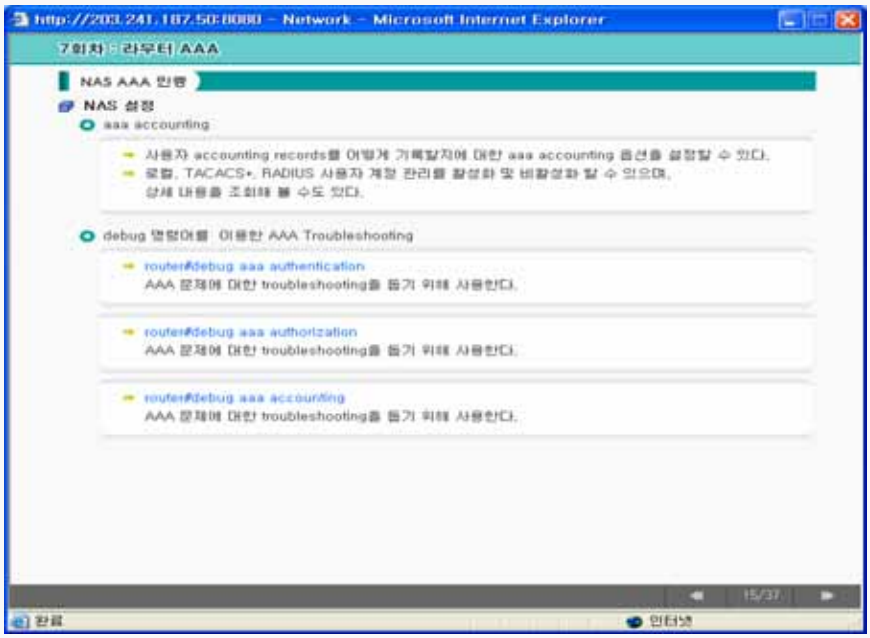

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
7회차 : 라우터 AAA
NAS AAA 인증
AAA 보안 서버 옵션
원격 보안 서버 - TACACS+와 RADIUS
AAA 보안 프로토콜을 수행하며, 여러 부분의 네트워크 장비와 많은 네트워크 사용자를 위해
AAA 서비스를 제공하는 분산 서버이다.
TACACS+와 RADIUS는 AAA를 위해 사용되는 보안 서버 프로토콜이며, 보안 서버와 라우터,
NAS 또는 방화벽 사이의 통신에 사용된다.
Security Server
Cisco Secure ACS
Firewall
Router
Network Access Server
Cisco Secure ACS 특징
• ACS (Access Control Server)는 표준 브라우저에 의해 관리된다.
• 사용자 이름과 패스워드 그리고 네트워크 장비를 변경, 추가,
이동하는 것이 용이하다.
• UNIX와 Windows NT/2000 서버 플랫폼상에서 동작할 수 있다.
• TACACS+ 와 RADIUS에서 지원된다.
10/37
완료
인터넷

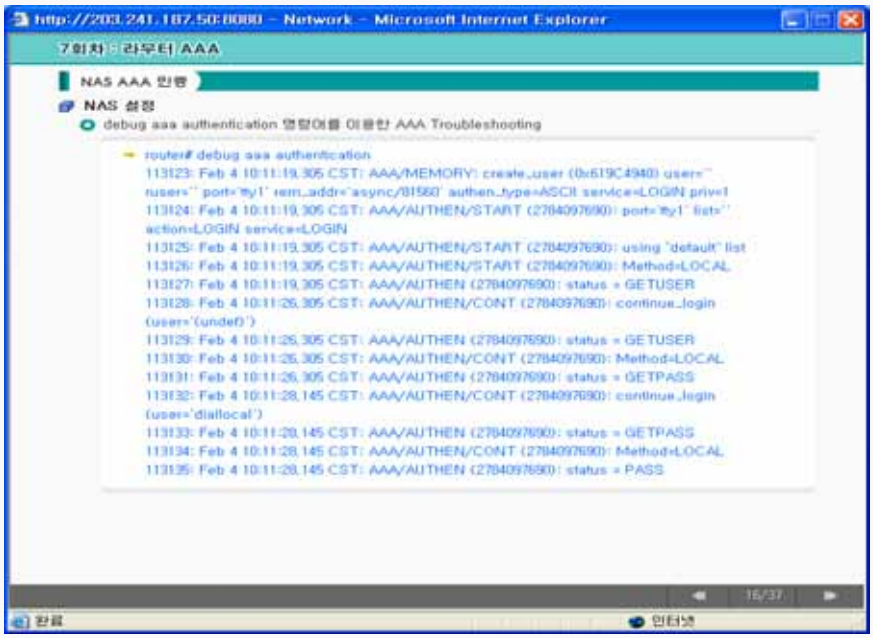

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
7회차 : 라우터 AAA
NAS AAA 인증
NAS 설정
Cisco 경계 라우터 (perimeter router)에의 로컬 AAA 설정 과정
privileged-EXEC mode로 들어간다.
aaa new-model 명령을 사용하여 경계 라우터 상에 전역적으로 AAA를 가능하게 한다.
AAA authentication lists를 설정한다.
AAA 인가를 설정한다.
accounting records를 위한 AAA accounting options를 설정한다.
설정을 확인한다.
"aaa new-model" 명령어를 사용한 AAA Enable
router(config)#aaa new-model
router(config)# aaa new-model
해 설
AAA 설정의 제일 첫 번째 단계로서
경계 라우터 상에 AAA 기능을
전역적으로 활성화 한다.
해 설
11/37
완료
인터넷

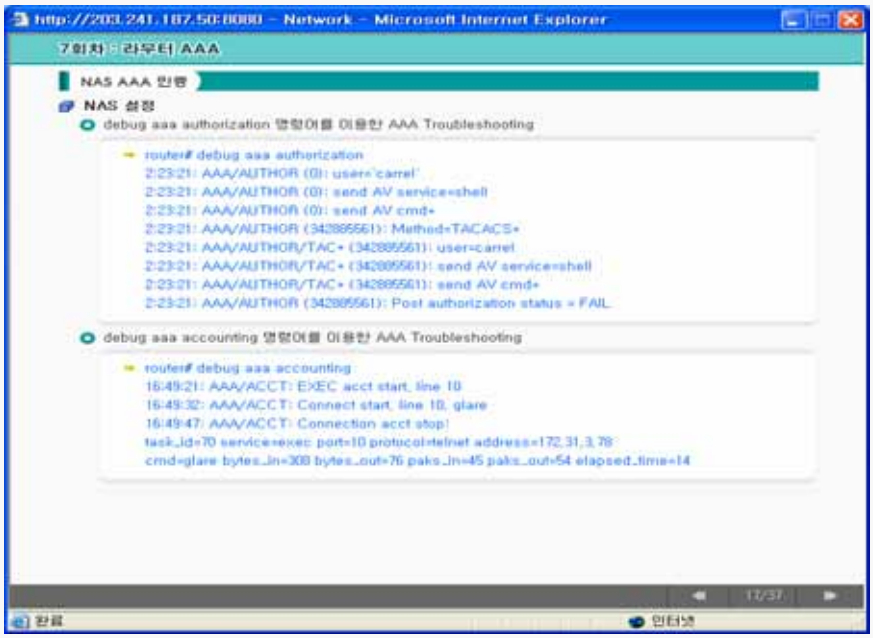

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
7회차 : 라우터 AAA
NAS AAA 인증
NAS 설정
aaa authentication login 명령어
router(config)#aaa authentication login {default | list-name} method1 [method2...]
router(config)# aaa authentication login default enable
router(config)# aaa authentication login console-in local
router(config)# aaa authentication login vty-in line
해 설
aaa authentication 명령어는 Cisco IOS 12.2 버전 이상에서
사용할 수 있으며 세부 인증 유형으로는 arap, banner, enable,
fail-message, login, nasi, password-prompt, ppp, username
prompt 등이 있다.
이들 명령어는 각각의 명령어 구문 형식과 옵션을 가지고 있다.
또한 인증 방법은 최대 네 개까지 지정할 수 있다.
해 설
12/37
완료
인터넷

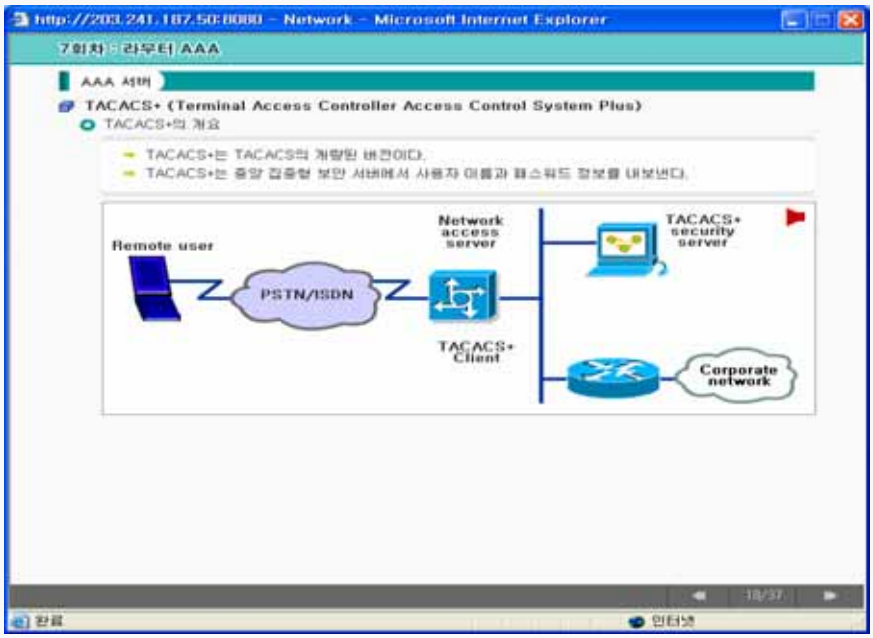

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
7회차 : 라우터 AAA
NAS AAA 인증
NAS 설정
aaa authentication ppp 명령어
router(config)#aaa authentication ppp {default | list-name} method1 [method2...]
router(config)# aaa authen ppp default local
router(config)# aaa authen ppp dial-in local none
ppp 인증을 디폴트 리스트로 로컬 데이터 베이스를 이용하여 인증한다.
여기서 잠깐!
aaa authentication ppp 명령어
router(config)#aaa authentication ppp {default | list-name} method1 [method2...]
router(config)# aaa authen enable default group tacacs+
사용자 모드에서 관리자 모드로 로그인 하기 위해서 tacacs+ 서버를 이용하여 인증한다.
13/37
완료
인터넷

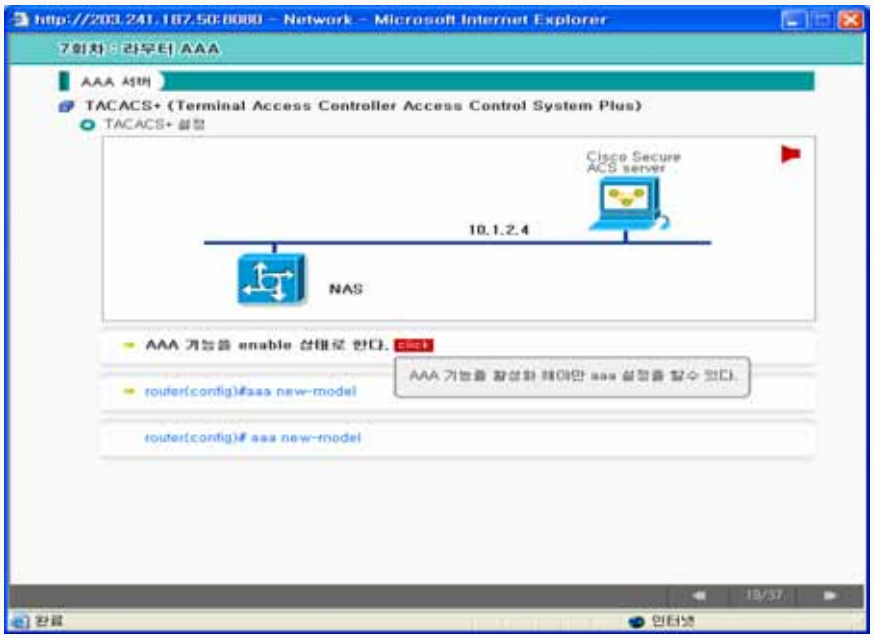

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
7회차 : 라우터 AAA
NAS AAA 인증
NAS 설정
Lines 과 Interfaces 에 Authentication 명령어 적용
router(config)# line console 0
router(config-line)# login authentication console-in
router(config)# int s3/0
router(config-if)# ppp authentication chap dial-in
Authentication 명령은 lines 또는 interfaces에 적용될 수 있다.
aaa authorization 명령어 click
router(config)#aaa authorization {network | exec | commands level | reverse-access | configuration} {default | list-name} method1 [method2...]
router(config)# aaa authen enable default group tacacs+
router(config)# aaa authen enable default group tacacs+
router(config)# aaa authen enable default group tacacs+
router(config)# aaa authen enable default group tacacs+
1레벨의 명령어를 사용하기 위해서 로컬 데이터 베이스로부터 권한을 받는다.
14/37
완료
인터넷

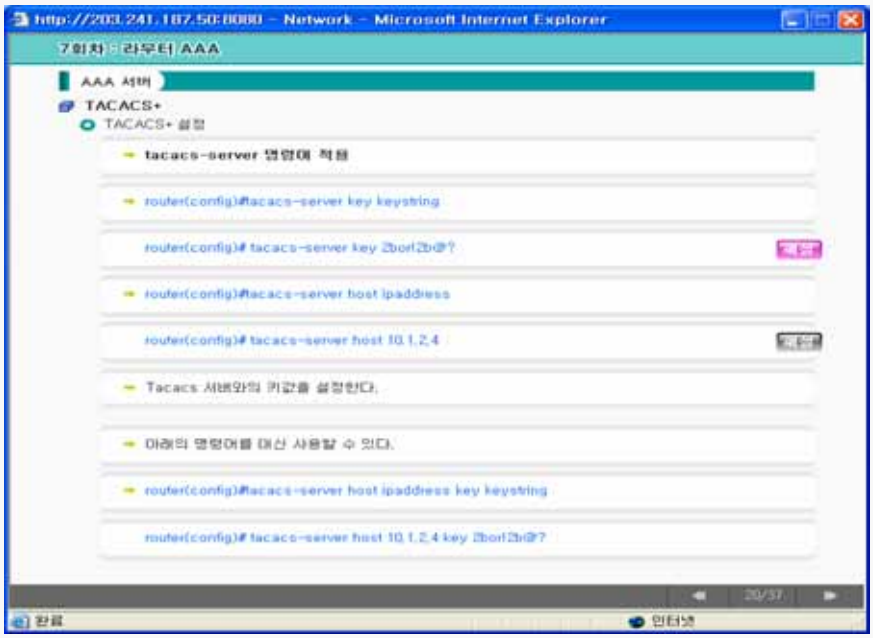

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
7회차 : 라우터 AAA
NAS AAA 인증
NAS 설정
aaa accounting
사용자 accounting records를 어떻게 기록할지에 대한 aaa accounting 옵션을 설정할 수 있다.
로컬, TACACS+, RADIUS 사용자 계정 관리를 활성화 및 비활성화 할 수 있으며,
상세 내용을 조회해 볼 수도 있다.
debug 명령어를 이용한 AAA Troubleshooting
router#debug aaa authentication
AAA 문제에 대한 troubleshooting을 돕기 위해 사용한다.
router#debug aaa authorization
AAA 문제에 대한 troubleshooting을 돕기 위해 사용한다.
router#debug aaa accounting
AAA 문제에 대한 troubleshooting을 돕기 위해 사용한다.
15/37
완료
인터넷

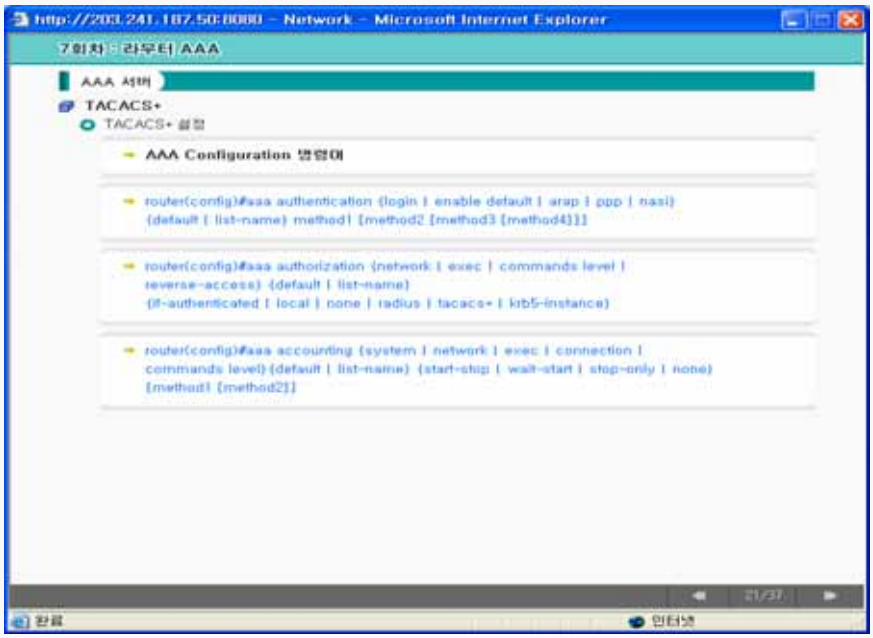

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
7회차 : 라우터 AAA
NAS AAA 인증
NAS 설정
debug aaa authentication 명령어를 이용한 AAA Troubleshooting
router# debug aaa authentication
113123: Feb 4 10:11:19.305 CST: AAA/MEMORY: create_user (0x619C4940) user=''
ruser='' port='tty1' rem_addr='async/81560' authen_type=ASCII service=LOGIN priv=1
113124: Feb 4 10:11:19.305 CST: AAA/AUTHEN/START (2784097690): port='tty1' list=''
action=LOGIN service=LOGIN
113125: Feb 4 10:11:19.305 CST: AAA/AUTHEN/START (2784097690): using "default" list
113126: Feb 4 10:11:19.305 CST: AAA/AUTHEN/START (2784097690): Method=LOCAL
113127: Feb 4 10:11:19.305 CST: AAA/AUTHEN (2784097690): status = GETUSER
113128: Feb 4 10:11:26.305 CST: AAA/AUTHEN/CONT (2784097690): continue_login
(user='(undef)')
113129: Feb 4 10:11:26.305 CST: AAA/AUTHEN (2784097690): status = GETUSER
113130: Feb 4 10:11:26.305 CST: AAA/AUTHEN/CONT (2784097690): Method=LOCAL
113131: Feb 4 10:11:26.305 CST: AAA/AUTHEN (2784097690): status = GETPASS
113132: Feb 4 10:11:28.145 CST: AAA/AUTHEN/CONT (2784097690): continue_login
(user='diallocal')
113133: Feb 4 10:11:28.145 CST: AAA/AUTHEN (2784097690): status = GETPASS
113134: Feb 4 10:11:28.145 CST: AAA/AUTHEN/CONT (2784097690): Method=LOCAL
113135: Feb 4 10:11:28.145 CST: AAA/AUTHEN (2784097690): status = PASS
16/37
완료
인터넷

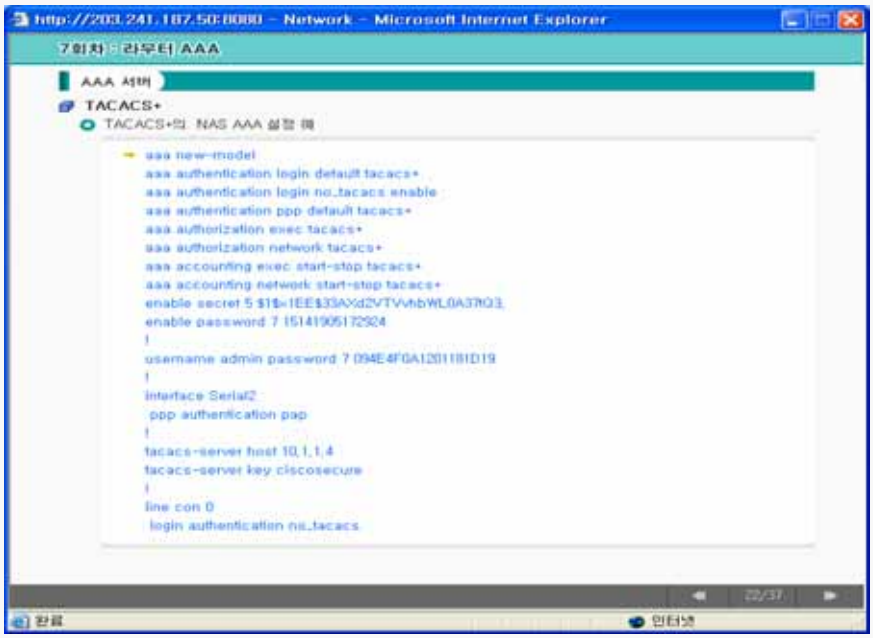

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
7회차 : 라우터 AAA
NAS AAA 인증
NAS 설정
debug aaa authorization 명령어를 이용한 AAA Troubleshooting
router# debug aaa authorization
2:23:21: AAA/AUTHOR (0): user='carrel'
2:23:21: AAA/AUTHOR (0): send AV service=shell
2:23:21: AAA/AUTHOR (0): send AV cmd=
2:23:21: AAA/AUTHOR (342885561): Method=TACACS+
2:23:21: AAA/AUTHOR/TAC+ (342885561): user=carrel
2:23:21: AAA/AUTHOR/TAC+ (342885561): send AV service=shell
2:23:21: AAA/AUTHOR/TAC+ (342885561): send AV cmd=
2:23:21: AAA/AUTHOR (342885561): Post authorization status = FAIL
debug aaa accounting 명령어를 이용한 AAA Troubleshooting
router# debug aaa accounting
16:49:21: AAA/ACCT: EXEC acct start, line 10
16:49:32: AAA/ACCT: Connect start, line 10, glare
16:49:47: AAA/ACCT: Connection acct stop!
task_id=70 service=exec port=10 protocol=telnet address=172.31.3.78
cmd=glare bytes_in=308 bytes_out=76 paks_in=45 paks_out=54 elapsed_time=14
17/37
완료
인터넷

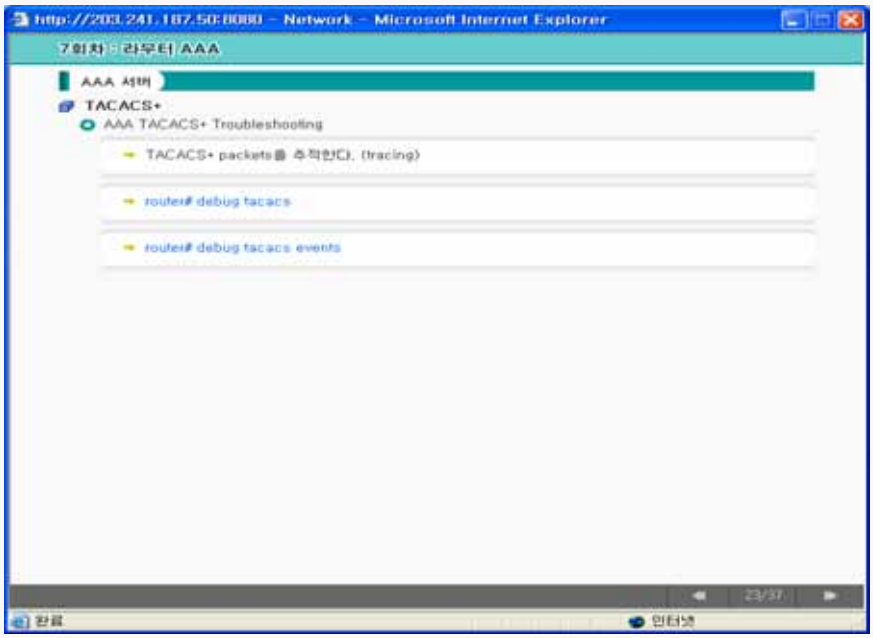

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
7회차 : 라우터 AAA
AAA 서버
TACACS+ (Terminal Access Controller Access Control System Plus)
TACACS+의 개요
TACACS+는 TACACS의 개량된 버전이다.
TACACS+는 중앙 집중형 보안 서버에서 사용자 이름과 패스워드 정보를 내보낸다.
Remote user
PSTN/ISDN
Network access server
TACACS+ Client
TACACS+ security server
Corporate network
18/37
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
7회차 : 라우터 AAA
AAA 서버
TACACS+ (Terminal Access Controller Access Control System Plus)
TACACS+ 설정
Cisco Secure ACS server
10.1.2.4
NAS
AAA 기능을 enable 상태로 한다.
router(config)#aaa new-model
router(config)# aaa new-model
완료
인터넷

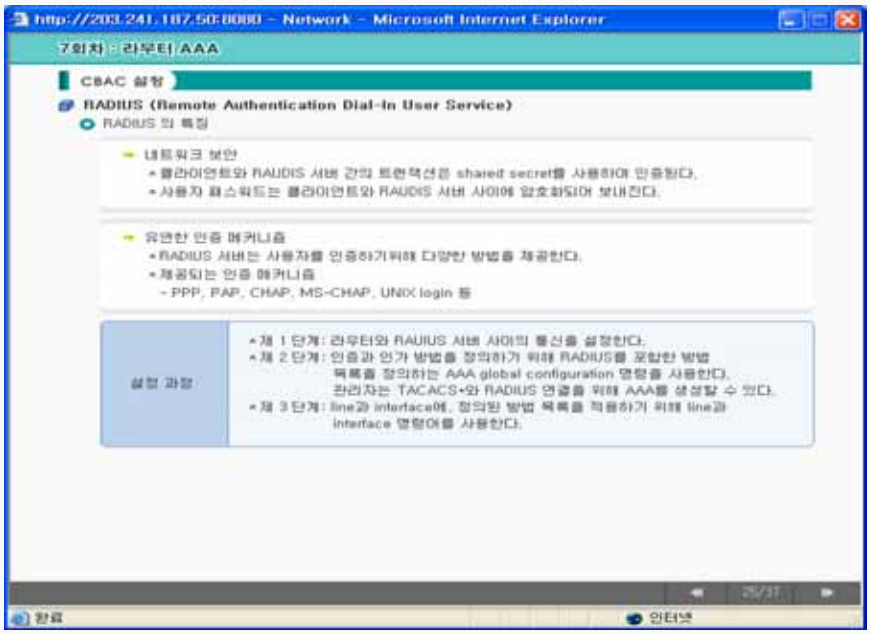

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
7회차 : 라우터 AAA
AAA 서버
TACACS+
TACACS+ 설정
tacacs-server 명령에 적용
router(config)#tacacs-server key keystring
router(config)# tacacs-server key 2bor!2b@?
router(config)#tacacs-server host ipaddress
router(config)# tacacs-server host 10.1.2.4
Tacacs 서버와의 키값을 설정한다.
아래의 명령어를 대신 사용할 수 있다.
router(config)#tacacs-server host ipaddress key keystring
router(config)# tacacs-server host 10.1.2.4 key 2bor!2b@?
완료
인터넷

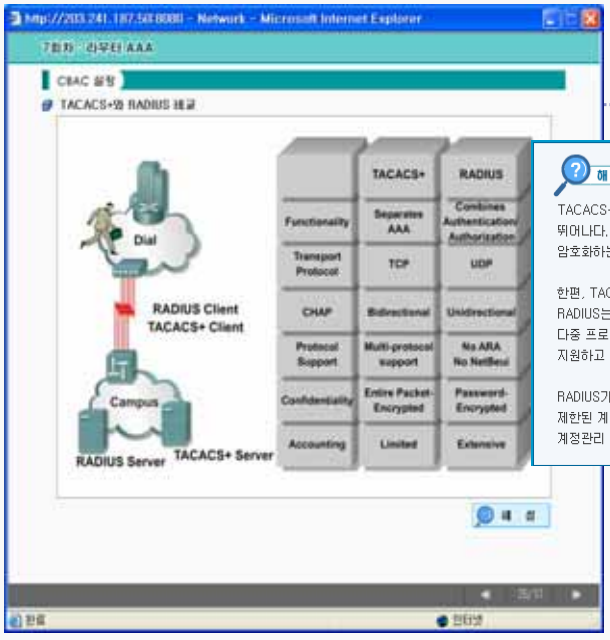

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
7회차 : 라우터 AAA
AAA 서버
TACACS+
TACACS+ 설정
AAA Configuration 명령어
router(config)#aaa authentication {login | enable default | arap | ppp | nasi}
{default | list-name} method1 [method2 [method3 [method4]]]
router(config)#aaa authorization {network | exec | commands level |
reverse-access} {default | list-name}
{if-authenticated | local | none | radius | tacacs+ | krb5-instance}
router(config)#aaa accounting {system | network | exec | connection |
commands level} {default | list-name} {start-stop | wait-start | stop-only | none}
[method1 [method2]]
21/37
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
7회차 : 라우터 AAA
AAA 서버
TACACS+
TACACS+의 NAS AAA 설정 예
aaa new-model
aaa authentication login default tacacs+
aaa authentication login no_tacacs enable
aaa authentication ppp default tacacs+
aaa authorization exec tacacs+
aaa authorization network tacacs+
aaa accounting exec start-stop tacacs+
aaa accounting network start-stop tacacs+
enable secret 5 1=1EE$33AXd2VTVvhbWL0A3fIQ3.
enable password 7 1514190517292A
!
username admin password 7 094E4F0A1201181D19
!
interface Serial2
ppp authentication pap
!
tacacs-server host 10.1.1.4
tacacs-server key ciscosecure
!
line con 0
login authentication no_tacacs
22/37
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
7회차 : 라우터 AAA
AAA 서버
TACACS+
AAA TACACS+ Troubleshooting
TACACS+ packets를 추적한다. (tracing)
router# debug tacacs
router# debug tacacs events
23/37
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
7회차 : 라우터 AAA
AAA 서버
RADIUS (Remote Authentication Dial-In User Service)
RADIUS 개요
네트워크 관리자에게 중요한 TACACS+의 대안이다.
Livingston Enterprises, Inc에 의해 개발된 Access Server AAA 프로토콜이다.
원격 액세스를 안전하게 하고 비 인가 액세스로부터 네트워크를 보호하는 분산 보안 시스템이다.
RADIUS의 3가지 구성요소
UDP/IP frame format을 갖는 프로토콜
서버
클라이언트
RADIUS 클라이언트
NAS는 RAIUS 클라이언트로 동작한다.
클라이언트는 지정된 RADIUS 서버로 사용자 정보를 전달하고 되돌아 오는 응답에 따라 동작한다.
RADIUS 서버
사용자의 연결 요구를 받아 사용자를 인증하고, 사용자에게 서비스를 제공하기 위해 클라이언트가 필요로 하는 모든 설정 정보를 준다.
RADIUS 서버는 다른 유형의 인증 서버를 위한 Proxy 클라이언트로 동작할 수 있다.
RADIUS 서버는 로컬 사용자 DB를 사용하거나 Windows DB 또는 사용자 이름과 패스워드가 정당함을 인정하는 LDAP Directory를 사용할 수 있다.
24/37
완료
인터넷



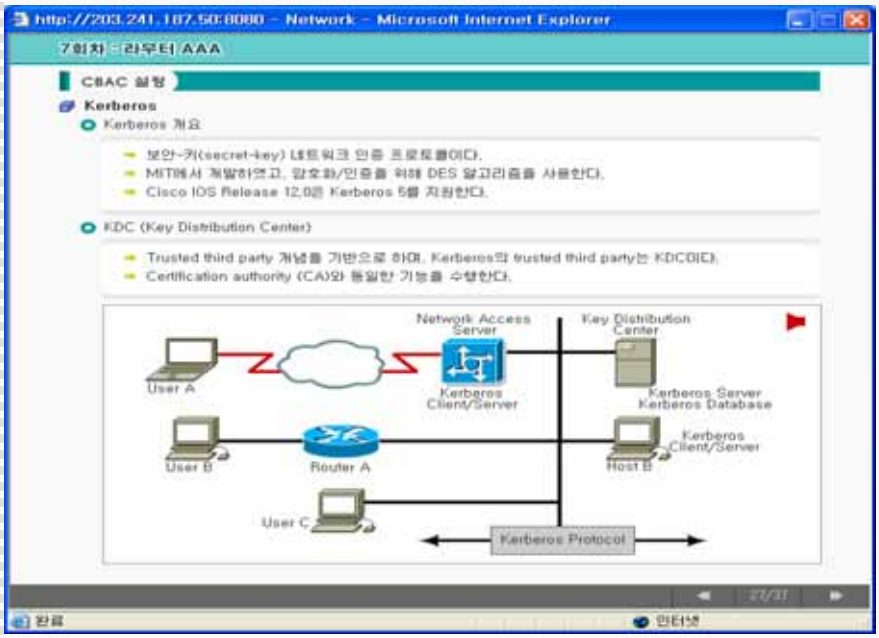


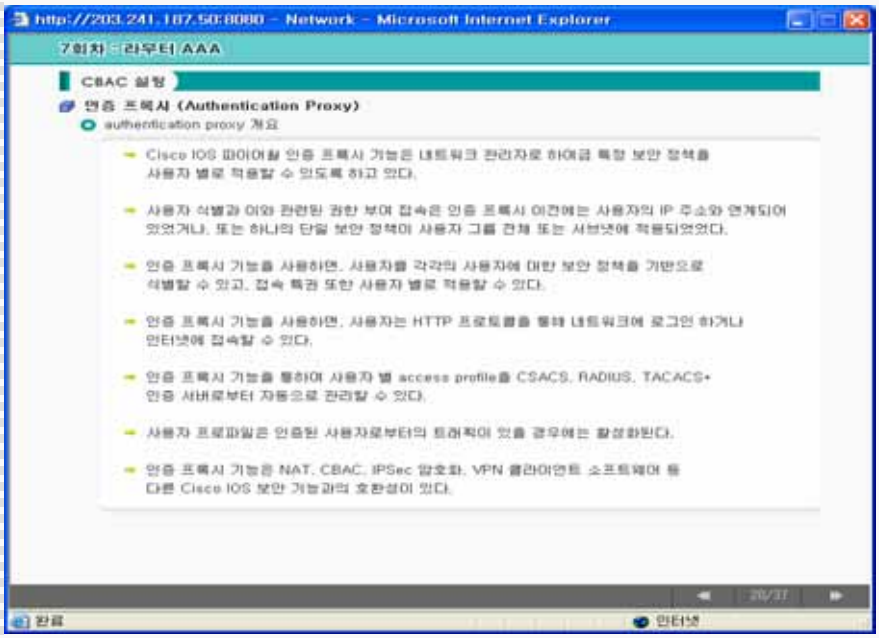
해 설

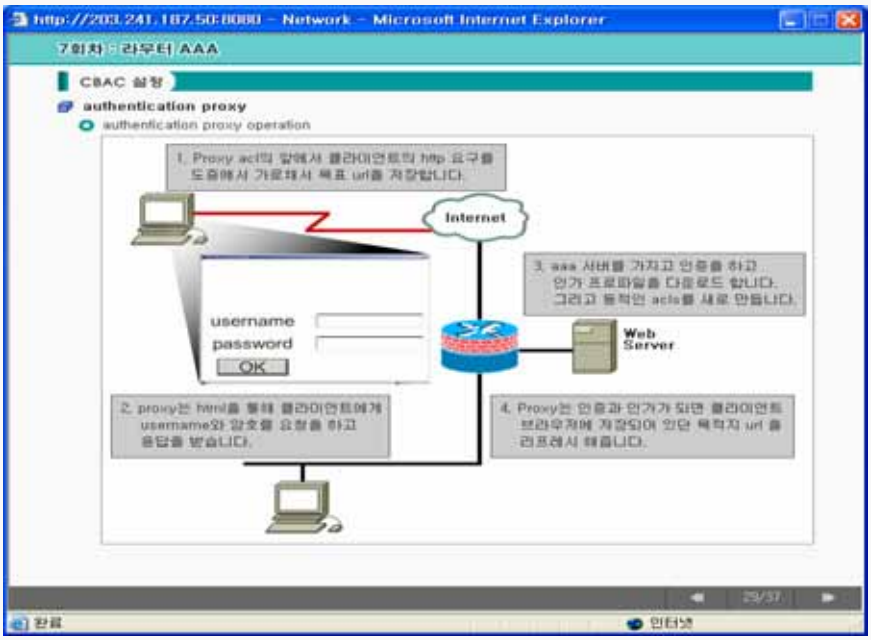
TACACS+는 기능성이나 기밀성 제공 수준이 RADIUS에 비하여 뛰어나다. 즉, TACACS+는 AAA 기능을 분리하고, 패킷 전체를 암호화하는 특징을 가지고 있다.

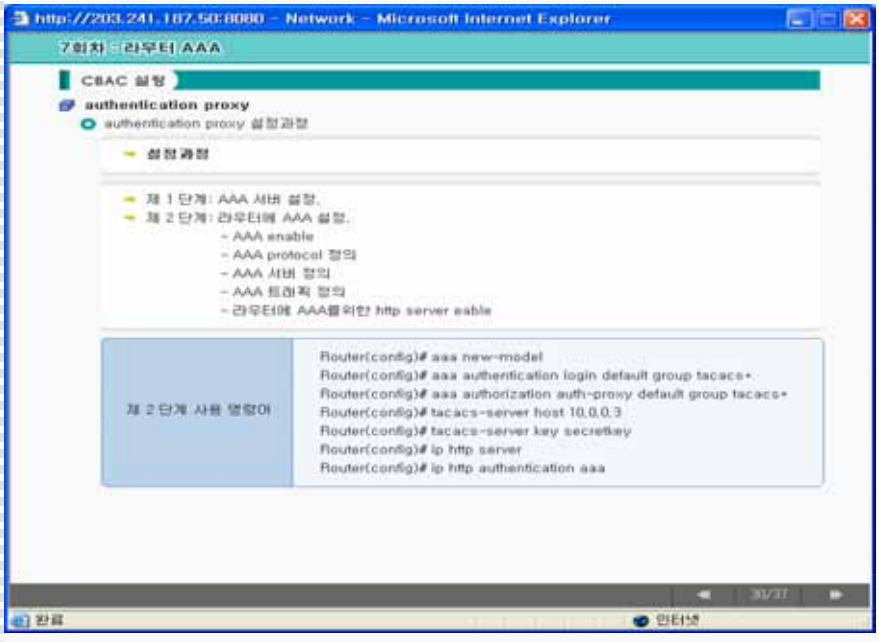
한편, TACACS+가 TCP를 전송 프로토콜로 사용하는 반면 RADIUS는 UDP를 사용하고, TACACS+가 양방향 CHAP 및 다중 프로토콜 지원이 가능한 반면, RADIUS는 단방향 CHAP을 지원하고 ARA나 NetBeui같은 프로토콜은 지원하지 못한다.

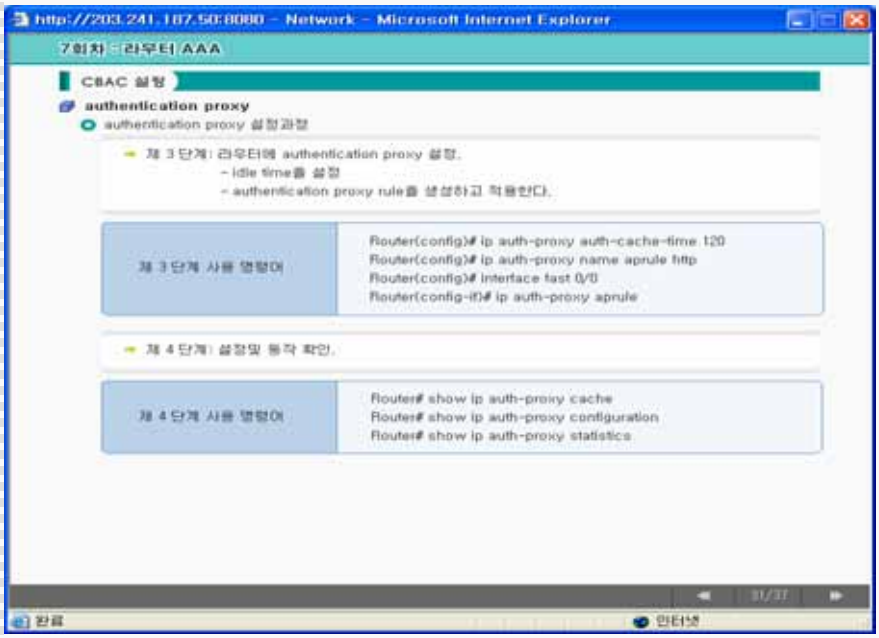
RADIUS가 TACACS+에 비해 우수한 사항으로는 TACACS+는 제한된 계정관리 기능을 수행하지만, RADIUS는 방대한 양의 계정관리 기능을 수행할 수 있다.


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
7회차 - 라우터 AAA
CBAC 설정
Kerberos
Kerberos 개요
보안-키(secret-key) 네트워크 인증 프로토콜이다.
MIT에서 개발하였고, 암호화/인증을 위해 DES 알고리즘을 사용한다.
Cisco IOS Release 12.0은 Kerberos 5를 지원한다.
KDC (Key Distribution Center)
Trusted third party 개념을 기반으로 하며, Kerberos의 trusted third party는 KDC이다.
Certification authority (CA)와 동일한 기능을 수행한다.
Network Access Server
Key Distribution Center
User A
Kerberos Client/Server
Kerberos Server Kerberos Database
User B
Router A
Host B
Kerberos Client/Server
User C
Kerberos Protocol
22/31
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
7회차 - 라우터 AAA
CBAC 설정
인증 프록시 (Authentication Proxy)
authentication proxy 개요
Cisco IOS 파이어월 인증 프록시 기능은 네트워크 관리자로 하여금 특정 보안 정책을 사용자 별로 적용할 수 있도록 하고 있다.
사용자 식별과 이와 관련된 권한 부여 접속은 인증 프록시 이전에는 사용자의 IP 주소와 연계되어 있었거나, 또는 하나의 단일 보안 정책이 사용자 그룹 전체 또는 서브넷에 적용되었었다.
인증 프록시 기능을 사용하면, 사용자를 각각의 사용자에 대한 보안 정책을 기반으로 식별할 수 있고, 접속 특권 또한 사용자 별로 적용할 수 있다.
인증 프록시 기능을 사용하면, 사용자는 HTTP 프로토콜을 통해 네트워크에 로그인 하거나 인터넷에 접속할 수 있다.
인증 프록시 기능을 통하여 사용자 별 access profile을 CSACS, RADIUS, TACACS+ 인증 서버로부터 자동으로 관리할 수 있다.
사용자 프로파일은 인증된 사용자로부터의 트래픽이 있을 경우에는 활성화된다.
인증 프록시 기능은 NAT, CBAC, IPSec 암호화, VPN 클라이언트 소프트웨어 등 다른 Cisco IOS 보안 기능과의 호환성이 있다.
20/31
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
7회차 - 라우터 AAA
CBAC 설정
authentication proxy
authentication proxy operation
1. Proxy acl의 맵에서 클라이언트의 http 요구를 도중에서 가로채서 목표 url을 저장합니다.
Internet
3. aaa 서버를 가지고 인증을 하고 인가 프로파일을 다운로드 합니다. 그리고 동적인 acls를 새로 만듭니다.
username
password
OK
Web Server
2. proxy는 html을 통해 클라이언트에게 username와 암호를 요청을 하고 응답을 받습니다.
4. Proxy는 인증과 인가가 되면 클라이언트 브라우저에 저장되어 있던 목적지 url 을 리프레시 해줍니다.
29/37
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
7회차 - 라우터 AAA
CBAC 설정
authentication proxy
authentication proxy 설정과정
설정과정
제 1 단계: AAA 서버 설정.
제 2 단계: 라우터에 AAA 설정.
- AAA enable
- AAA protocol 정의
- AAA 서버 정의
- AAA 트래픽 정의
- 라우터에 AAA를위한 http server eable
제 2 단계 사용 명령어
Router(config)# aaa new-model
Router(config)# aaa authentication login default group tacacs+
Router(config)# aaa authorization auth-proxy default group tacacs+
Router(config)# tacacs-server host 10.0.0.3
Router(config)# tacacs-server key secretkey
Router(config)# ip http server
Router(config)# ip http authentication aaa
30/37
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
7회차 - 라우터 AAA
CBAC 설정
authentication proxy
authentication proxy 설정과정
제 3 단계: 라우터에 authentication proxy 설정.
- idle time을 설정
- authentication proxy rule을 생성하고 적용한다.
제 3 단계 사용 명령어
Router(config)# ip auth-proxy auth-cache-time 120
Router(config)# ip auth-proxy name aprule http
Router(config)# interface fast 0/0
Router(config-if)# ip auth-proxy aprule
제 4 단계: 설정및 동작 확인.
제 4 단계 사용 명령어
Router# show ip auth-proxy cache
Router# show ip auth-proxy configuration
Router# show ip auth-proxy statistics
31/37
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
7회차 - 라우터 AAA
지금까지 공부한 내용을 요약하여 다시 한번 정리를 하도록 하겠습니다.
부족한 부분은 다시 한번 확인 하시기 바랍니다.
AAA란?
AAA는 인증, 인가, 계정관리를 말하며, 인증이 AAA의 첫 번째 단계이다.
AAA는 패킷 모드와 문자 모드 트래픽을 보호한다.
인증 방법
Username/Password 방법, One-time Password 방법, Token card/Soft token 방법이 있다.
NAS
원격 사용자들에게 네트워크 장비로의 액세스를 제공하는 것이며, 일반적으로 경계 네트워크 상에 존재하는 라우터이다.
NAS에 AAA 서버를 설정할 때, 액세스 제어를 위해 로컬 보안 서버를 사용하는 방법과 원격 보안 서버를 사용하는 방법이 있다.
3. TACACS+와 RADIUS
AAA 서버에서 액세스 제어를 위해 원격 보안 서버를 사용할 때 사용하는 프로토콜이다.
32/37
완료
인터넷

End of Lecture