NAC EDU Chapter 4

WebUI - 시스템

CONTENTS

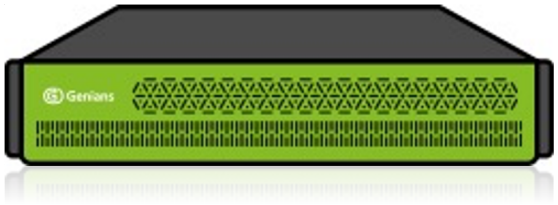
시스템

시스템-시스템 관리

Genian NAC

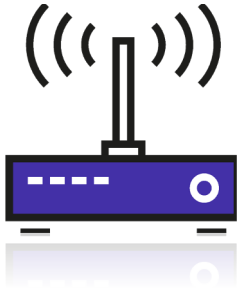
시스템 관리

1) 대상



장비 기반에
정책서버

장비 기반에
네트워크센서



장비 기반에
무선센서

시스템 관리

2) 작업 선택

장비 태그 설정	장비 일괄 설정	시스템 업그레이드	시스템 셧다운
CLI 비밀번호 변경	장비 설정 조회	이미지 선택 업그레이드	시스템 로그 수집
CLI Enable 비밀번호 변경	장비 삭제	시스템 재기동	

시스템 관리에서는 " 장비 삭제" 작업을 사용하여 네트워크센서를 삭제할 수 있습니다.
장비 삭제 시 다수 문제점이 발생할 수 있음으로 유의하여 삭제하여야 합니다.

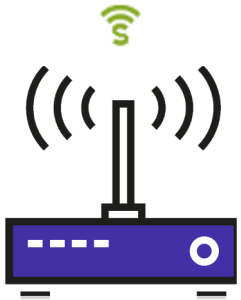
시스템 - 센서 관리

Genian NAC

센서 관리

1) 대상

논리적인 네트워크센서 기반



논리적인 무선센서 기반

시스템 - 센서 관리

센서 관리

2) 작업 선택

생성	센서 운영 모드 일괄 설정	무선센서 일괄 설정
센서 설정 조회	센서 대상 작업 지시	
센서 일괄 설정	무선센서 설정 조회	

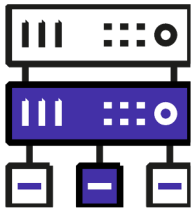
시스템-시스템 초기 설정

Genian NAC

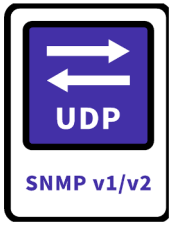
시스템 초기 설정

1) 환경 설정

보안 설정

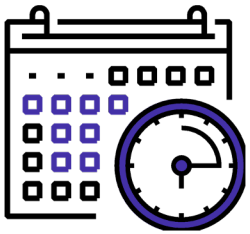


운영체제 업데이트
Proxy 서비스 설정

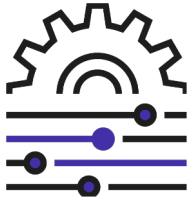


SNMP Agent 설정

자원 경고



날짜 및 시간



기타 설정

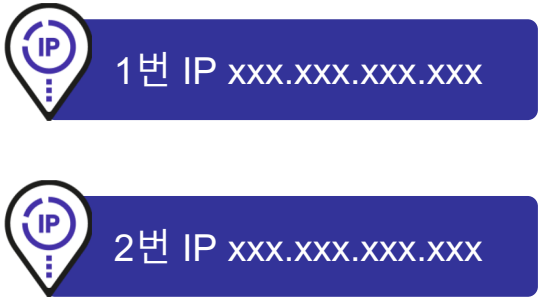
시스템-시스템 초기 설정

Genian NAC

시스템 초기 설정

1) 환경 설정

1. 보안 설정



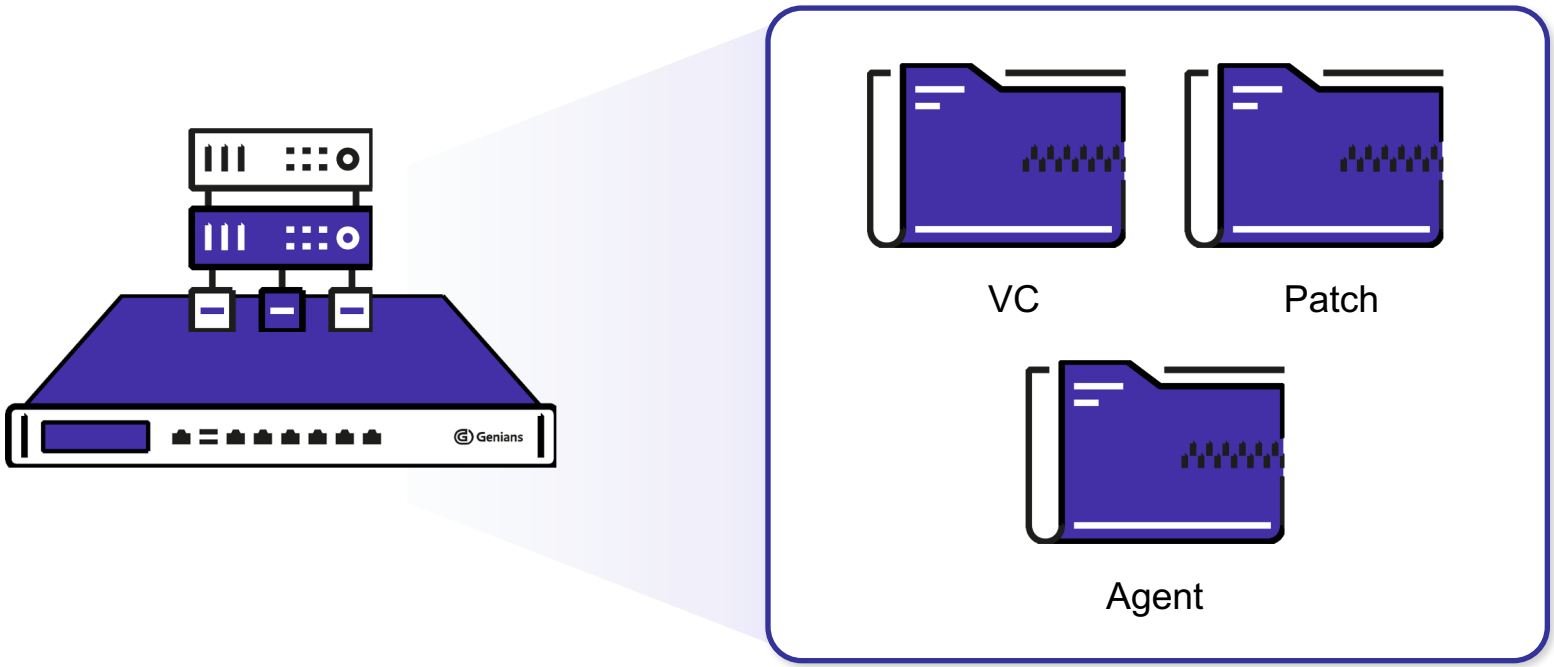
시스템-시스템 초기 설정

Genian NAC

시스템 초기 설정

1) 환경 설정

2. 운영체제 업데이트 Proxy 서비스 설정



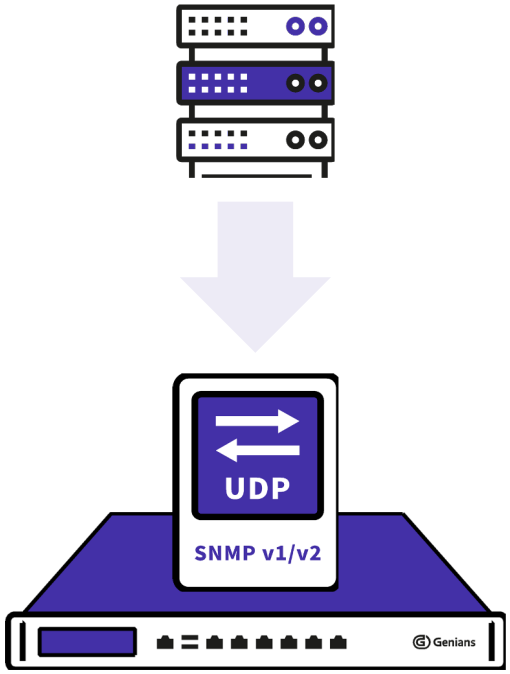
시스템-시스템 초기 설정

Genian NAC

시스템 초기 설정

1) 환경 설정

3. SNMP Agent 설정



SNMP V3	설정
no auth ,no priv	- 사용자명 입력(USM User)
auth,no priv	- 사용자명 입력(USM User) - Auth Password 입력(SHA,8자 이상)
auth,priv	- 사용자명 입력(USM User) - Auth Password 입력(SHA,8자 이상) - Priv Password 입력(AES,8자 이상)

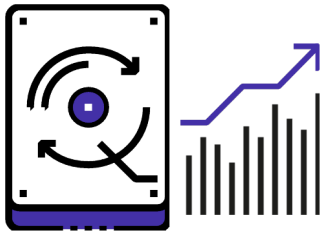
시스템-시스템 초기 설정

Genian NAC

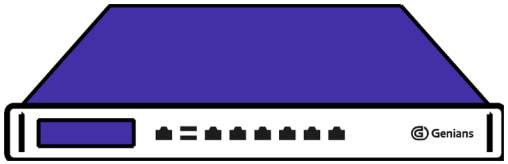
시스템 초기 설정

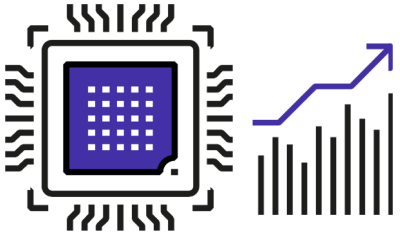
1) 환경 설정

4. 자원 경고

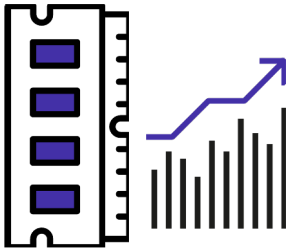


Disk

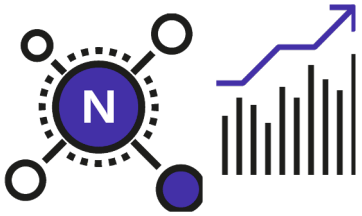




CP
U



Memory



Node

시스템-시스템 초기 설정

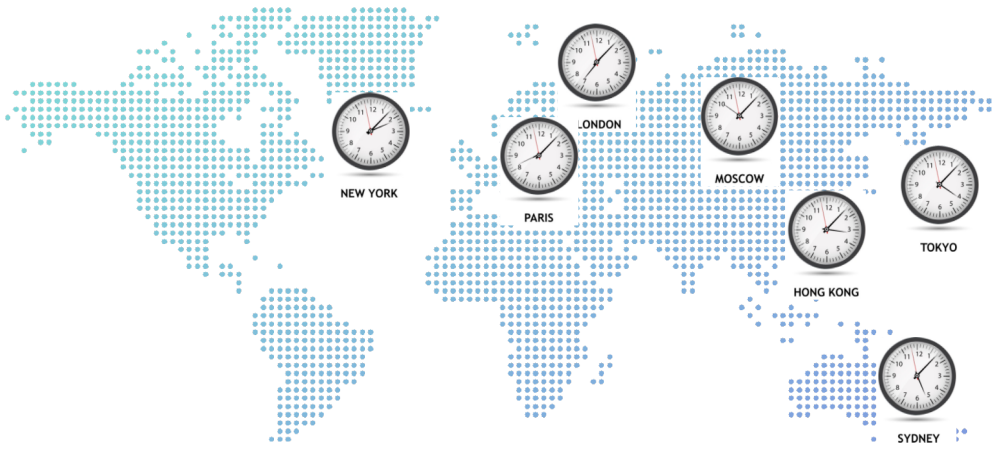
Genian NAC

시스템 초기 설정

1) 환경 설정

5. 날짜 및 시간

타임존 대륙 선택	
Default (Asia/Seoul)	Arctic
Africa	Australia
America	Europe
Antarctica	Indian
Asia	Pacific



시스템 초기 설정

1) 환경 설정

6. 기타 설정_기본 문자셋

기본 문자셋	비고
한국어(EUC-KR)	-
Western(ISO-8859-1)	알파벳
일본어(EUC-JP)	-
일본어(SHIFT_JIS)	-
중국어(BIG5)	-
중국어(Simplified Chinese)	-
유니코드(UTF-8)	다국어

시스템-시스템 초기설정

Genian NAC

시스템 초기 설정

1) 환경 설정

6. 기타 설정_네트워크 센서
디버그

센서 디버그 로그 생성	설명	비고
선택 안함	CLI 설정에 따름	디스크가 없을 경우 “선택 안함”, “로컬 " 정책서버로 저장
로컬	로컬 디스크 저장 (로컬 디스크 없을 경우 정책서버 저장)	
정책서버	정책서버 디스크 저장	-
로컬 및 정책서버	로컬 디스크 및 정책서버 디스크 저장	-

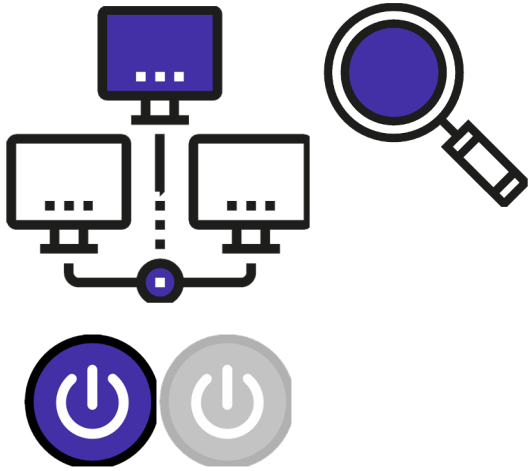
시스템-시스템 초기설정

Genian NAC

시스템 초기 설정

1) 환경 설정

6. 기타 설정 _노드 상태 검사



노드 상태(UP/DOWN) 검사

시스템-시스템 초기 설정

Genian NAC

시스템 초기 설정

1) 환경 설정

7. 기타 설정

센서 디버그 로그 생성	설명
선택 안함	CLI 설정에 따름
로컬	로컬 디스크 저장 (로컬 디스크 없을 경우 정책서버 저장)
정책서버	정책서버 디스크 저장
로컬 및 정책서버	로컬 디스크 및 정책서버 디스크 저장

디스크 없음

정책서버 저장

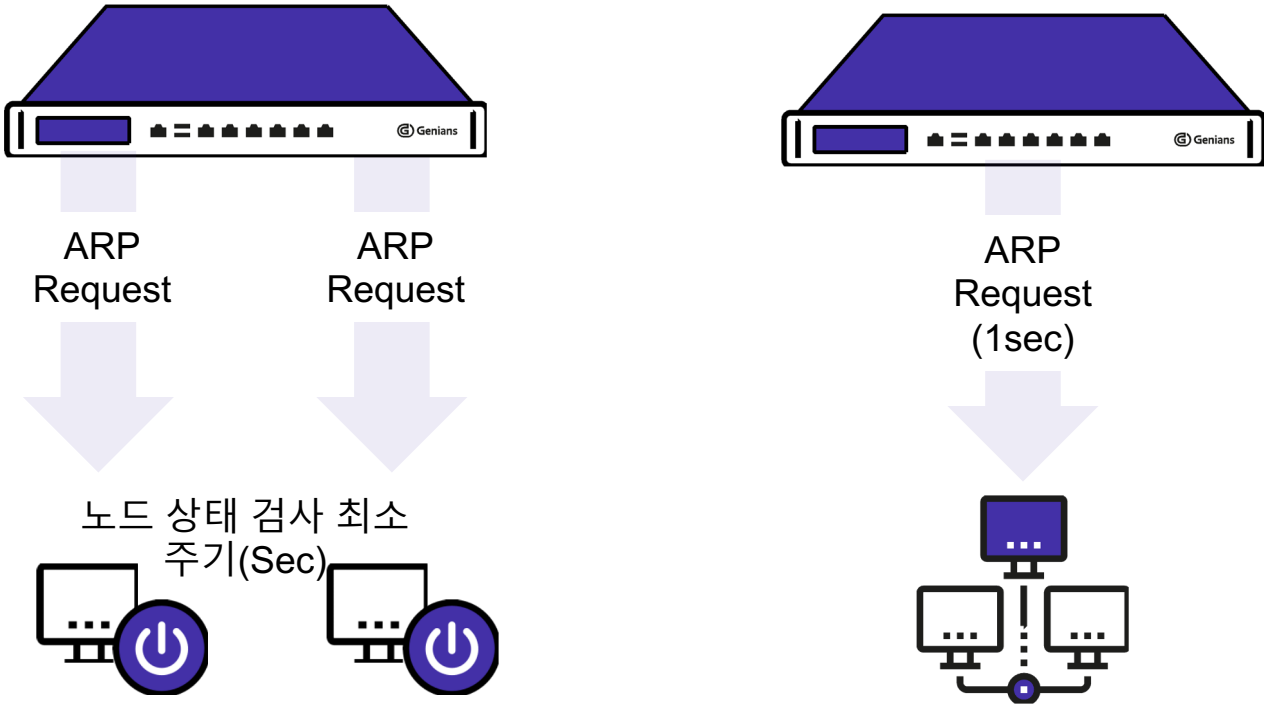
시스템-시스템 초기 설정

Genian NAC

시스템 초기 설정

1) 환경 설정

8. 기타 설정(노드 상태 검사)



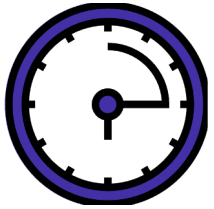
시스템-시스템 초기 설정

Genian NAC

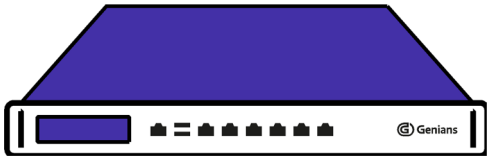
시스템 초기 설정

1) 환경 설정

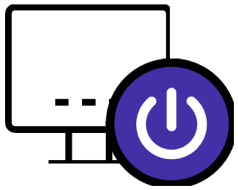
9. 기타 설정(노드 상태 검사)



노드 상태 검사 최소 주기



ARP Request



노드 상태를 검사하기 위한 ARP 패킷 주기 설정 (Sec)

Ex) 전체 노드 수(250개), 노드 상태 검사 최소 주기(10sec)

초당 센서에서 보낼 수 있는 Request 수량은 25 개(250/10)

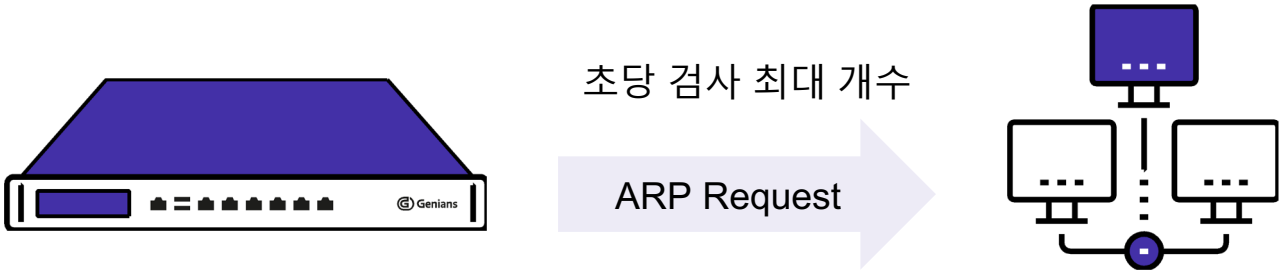
시스템-시스템 초기 설정

Genian NAC

시스템 초기 설정

1) 환경 설정

9. 기타 설정(노드 상태 검사)



노드 상태를 검사하기 위한 1초에 발송할 수 있는 ARP 패킷 개수 설정

Ex) 전체 노드수(250개), 노드 상태검사 최소 주기(10sec), 초당 검사 최대 개수(20개)

초당 센서 Request 수량은 25 개(250/10) > 초당 검사 최대 개수(20개)

시스템-시스템 초기 설정

Genian NAC

시스템 초기 설정

1) 환경 설정

10. 기타 설정(노드 상태 검사 최소 주기)

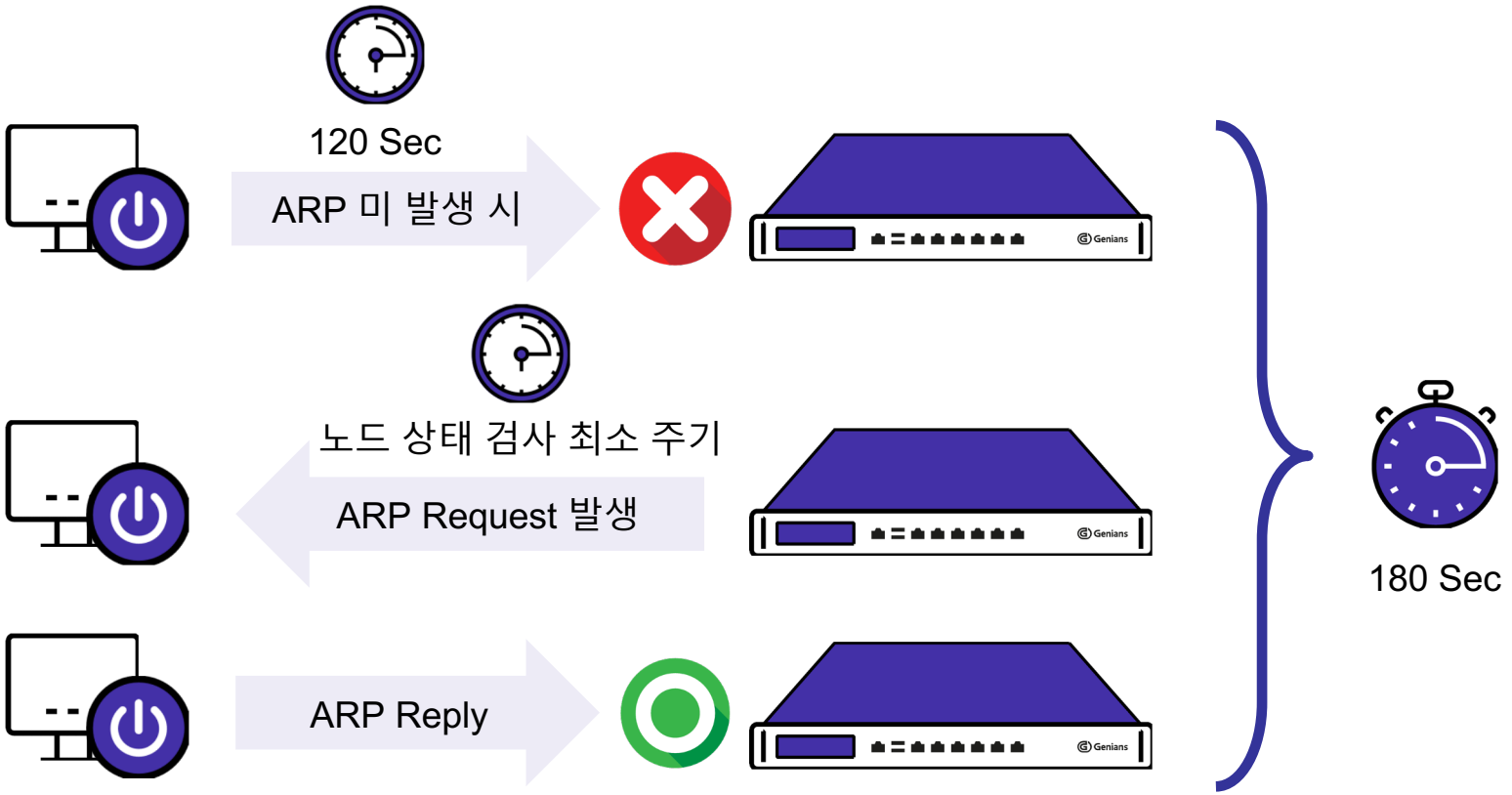
단말에서 발생되는 ARP 패킷을 120초 이내 네트워크 센서 수신 시

시스템-시스템 초기 설정

Genian NAC

1) 환경 설정

10. 기타 설정(노드 상태 검사 최소 주기)

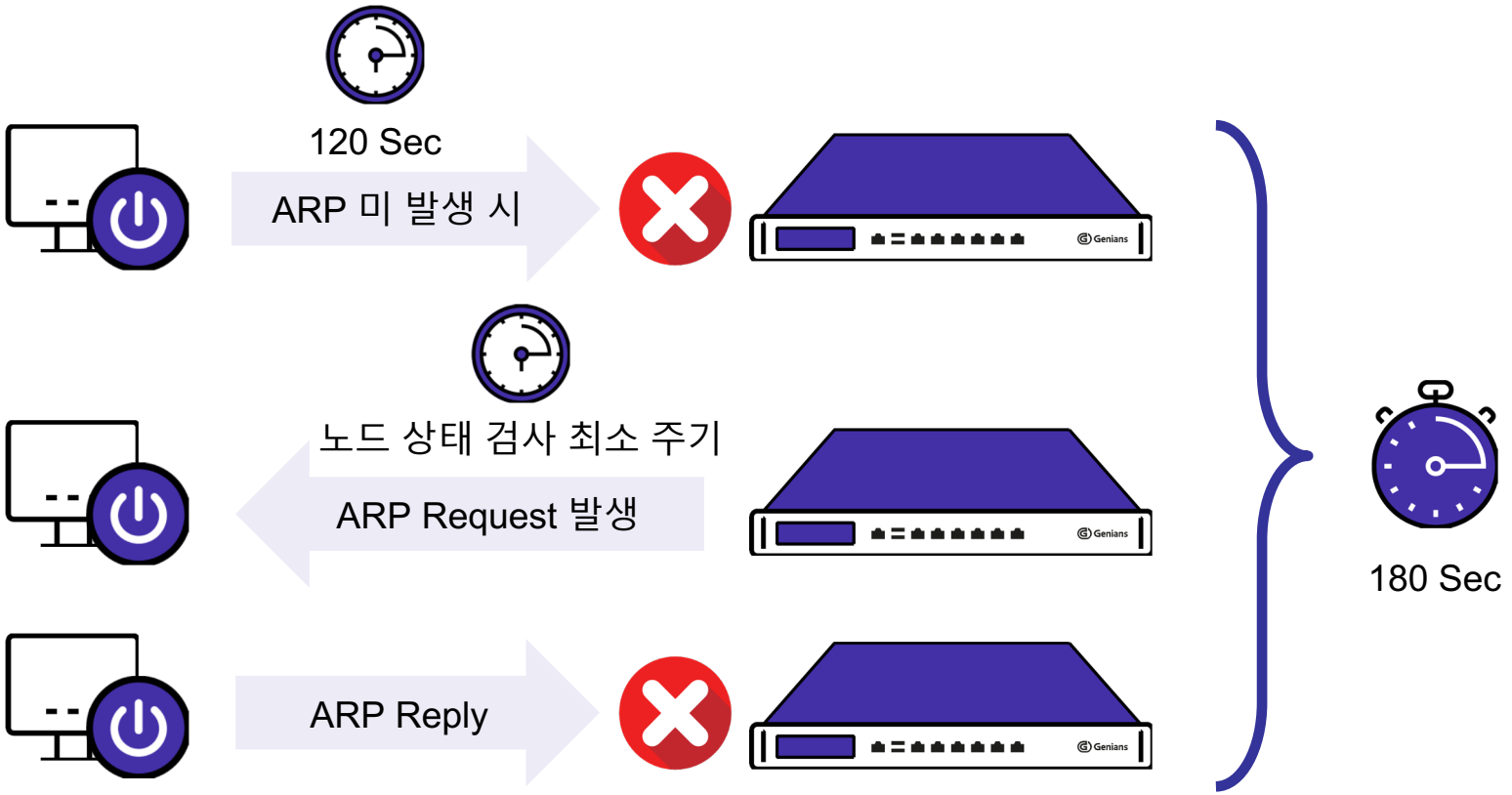


시스템-시스템 초기 설정

Genian NAC

1) 환경 설정

10. 기타 설정(노드 상태 검사 최소 주기)

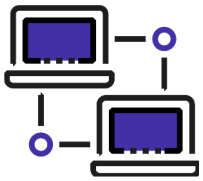


시스템-시스템 초기 설정

Genian NAC

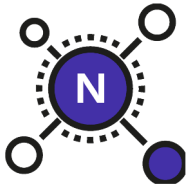
시스템 초기 설정

2) 센서 설정



센서
동작

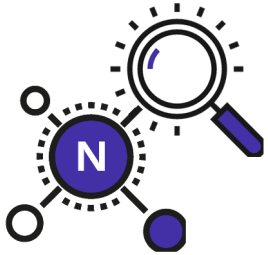
트래픽
모니터링



노드
등록

노드 정보
검사

네트워크
스캔



노드 상태
검사

서브넷 노드
스캔

DHC
P

가상
IP

IP
관리

기타
설정

시스템-시스템 초기 설정

Genian NAC

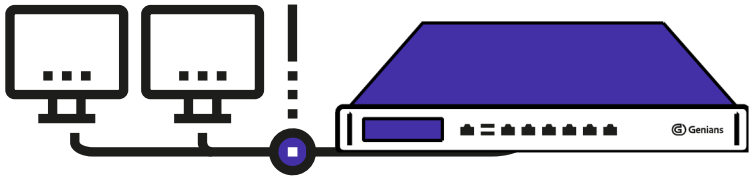
시스템 초기 설정

2) 센서 설정

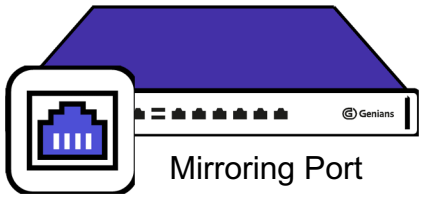
1. 동작 모드

동작 모드	설명
Inactive	기존 “None“ 모드와 동일, 동작 없음
Host	네트워크 센서 기능 사용 시 기본 설정 모드(정보 수집,네트워크 차단)
Mirror	Mirroring 패킷을 전송 받는 인터페이스 설정 사항

Inactive



Host



Mirror

시스템-시스템 초기 설정

Genian NAC

시스템 초기 설정

2) 센서 설정

2. 운영 모드

동작 모드	운영 모드	설명
Inactive	Monitoring	미동작
	Enforcement	
Host	Monitoring	네트워크 정보 수집
	Enforcement	네트워크 정보 수집 및 네트워크 제어
Mirror	Monitoring	미동작
	Enforcement	네트워크 제어

시스템-시스템 초기 설정

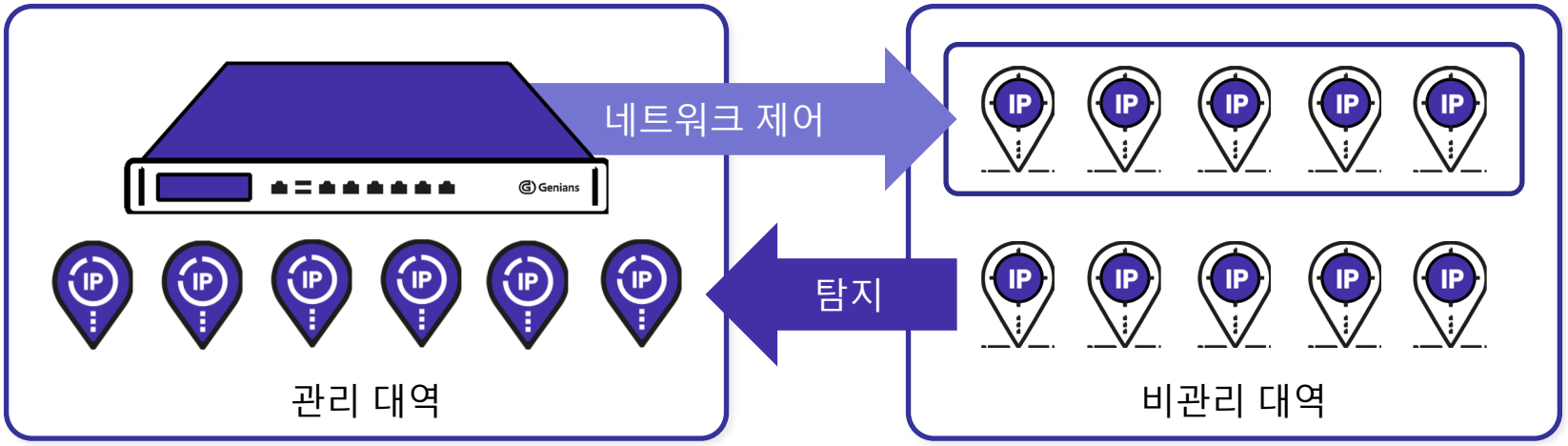
Genian NAC

시스템 초기 설정

2) 센서 설정

3. 비 관리 IP 제어

동작 모드	운영 모드	설명
Host	Enforcement	네트워크 정보 수집 및 네트워크 제어



시스템-시스템 초기 설정

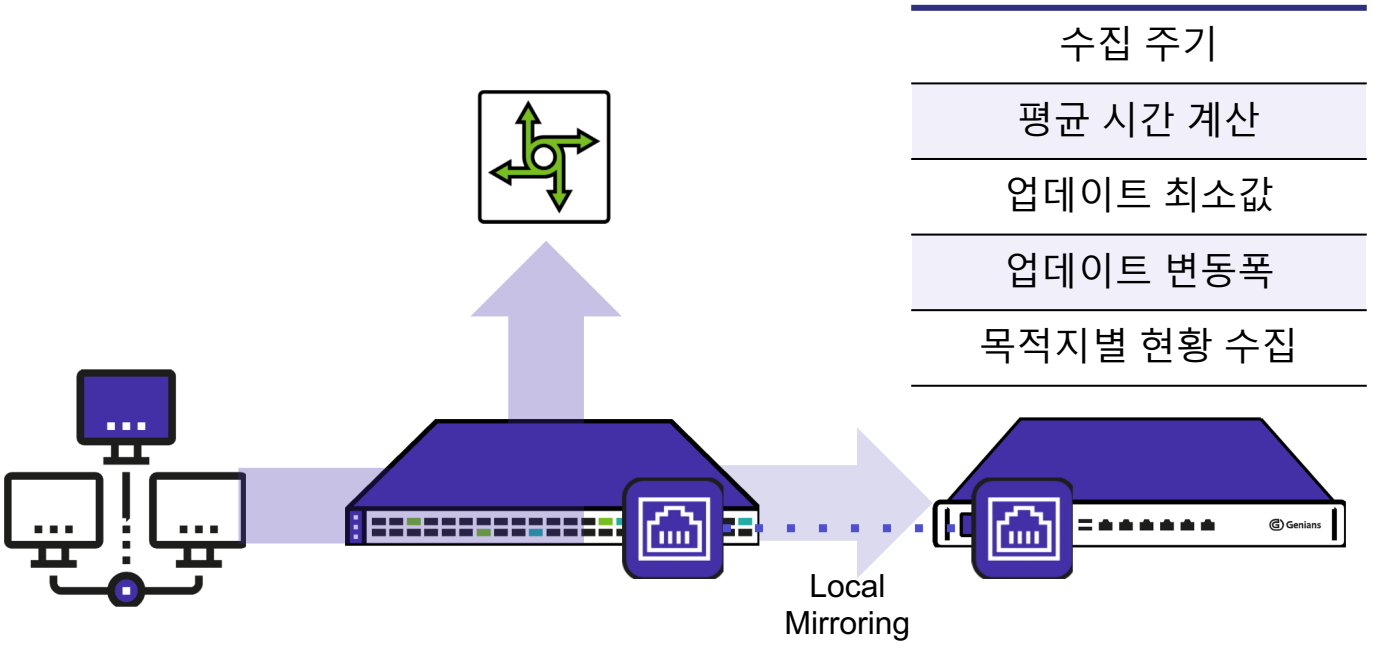
Genian NAC

시스템 초기 설정

2) 센서 설정

4. 트래픽 모니터링

동작 모드	운영 모드	미러 동작 범위	설명
Mirror	Enforcement	Local	네트워크 제어



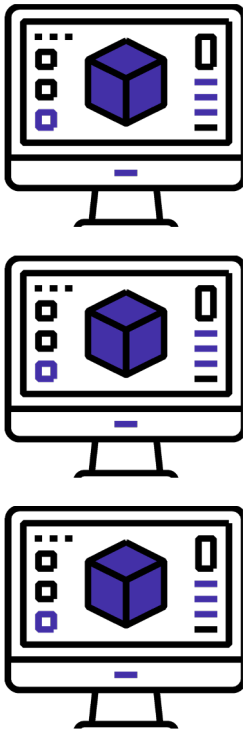
시스템-시스템 초기 설정

Genian NAC

시스템 초기 설정

2) 센서 설정

5. 노드 등록 – MAC당 최대 등록



192.168.1.1
AA:AA:AA:AA:AA:AA

192.168.1.2
AA:AA:AA:AA:AA:AA

192.168.1.3
AA:AA:AA:AA:AA:AA

개수 설정

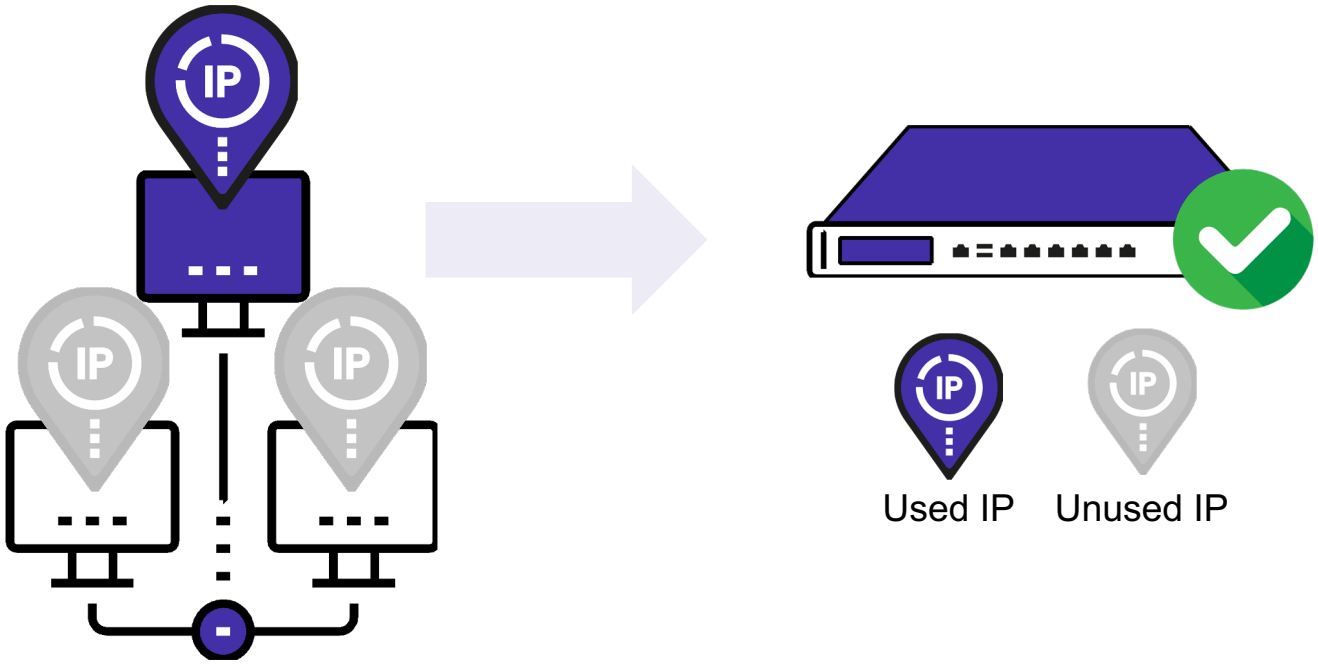
시스템-시스템 초기 설정

Genian NAC

시스템 초기 설정

2) 센서 설정

5. 노드 등록 – 미사용 IP 등록



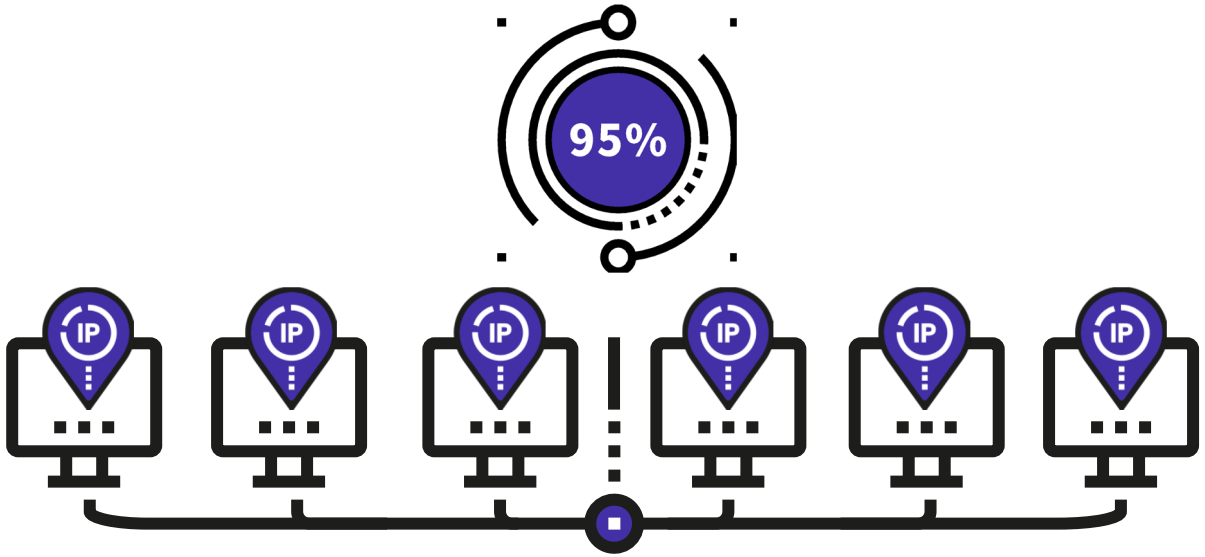
시스템-시스템 초기 설정

Genian NAC

시스템 초기 설정

2) 센서 설정

5. 노드 등록 – IP 사용률 경고



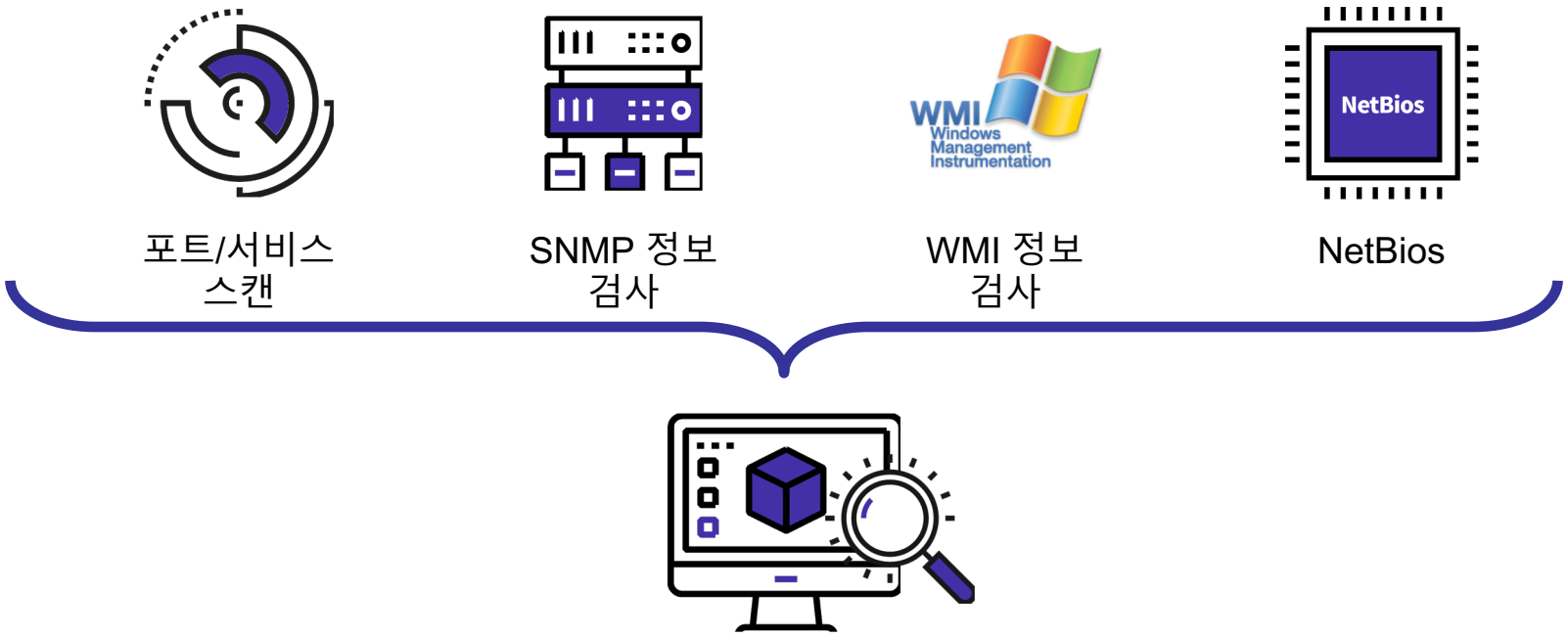
시스템-시스템 초기 설정

Genian NAC

시스템 초기 설정

2) 센서 설정

6. 노드 정보 검사



시스템-시스템 초기 설정

Genian NAC

시스템 초기 설정

2) 센서 설정

7. 네트워크 스캔

DHCP Server

UPnp

HP Slp

SIP

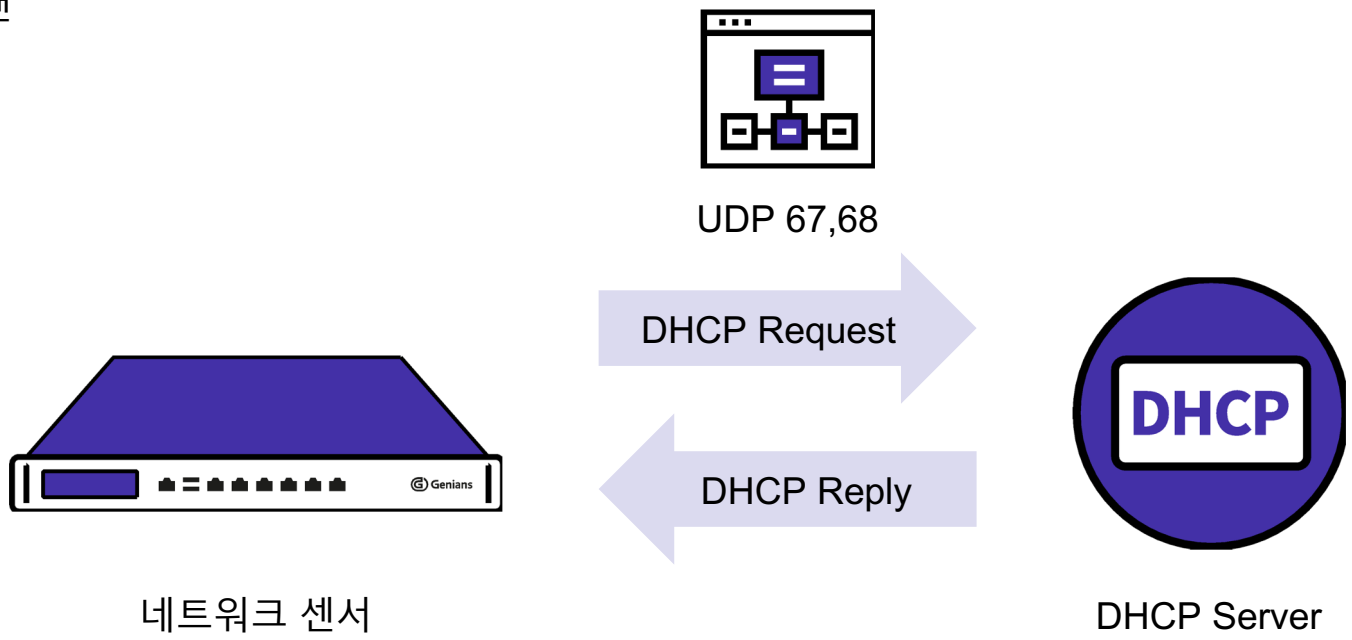
시스템-시스템 초기 설정

Genian NAC

시스템 초기 설정

2) 센서 설정

7. 네트워크 스캔



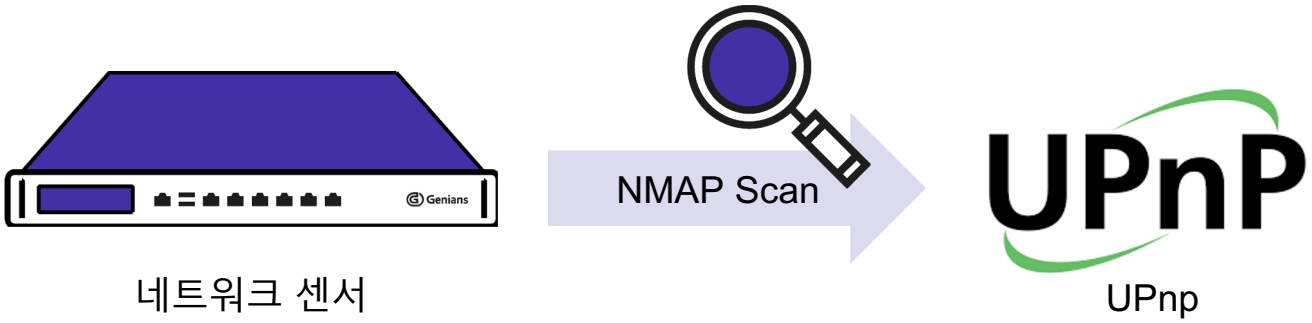
시스템-시스템 초기 설정

Genian NAC

시스템 초기 설정

2) 센서 설정

7. 네트워크 스캔



네트워크 센서

UPnp

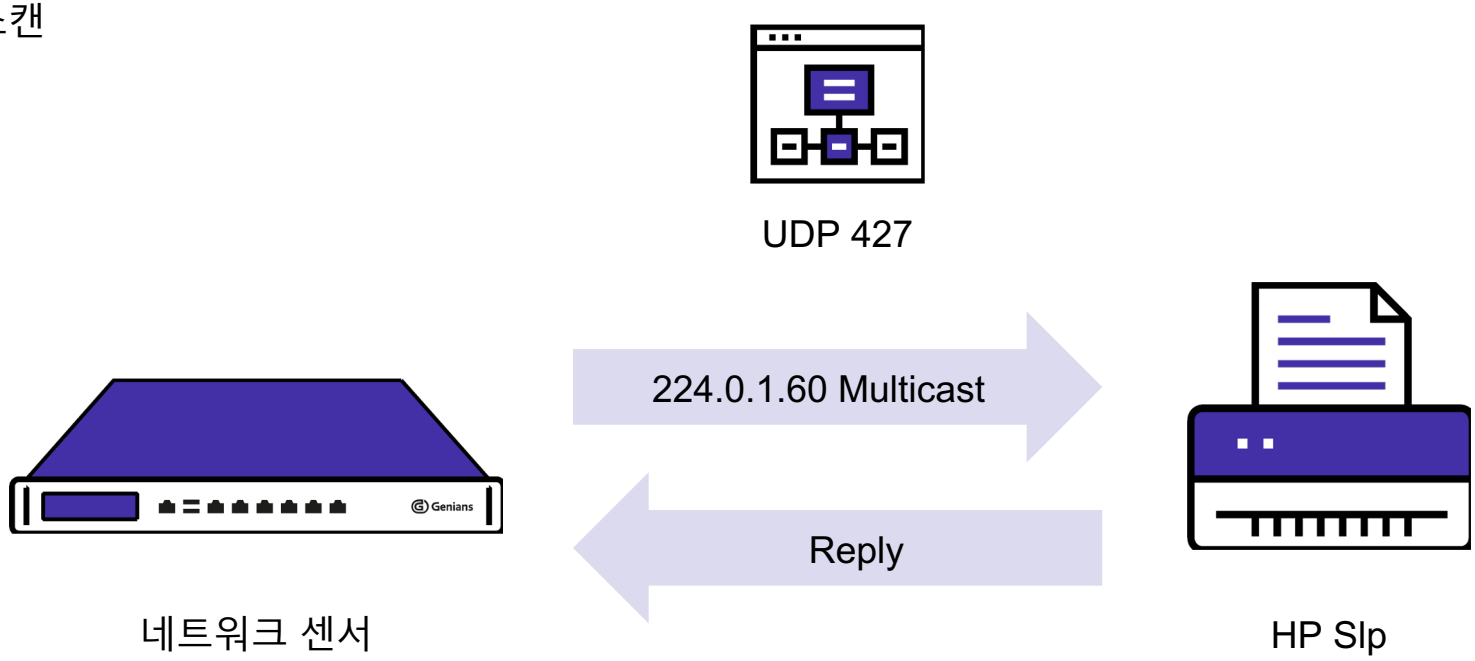
시스템-시스템 초기 설정

Genian NAC

시스템 초기 설정

2) 센서 설정

7. 네트워크 스캔



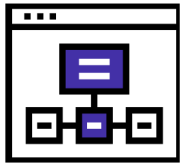
시스템-시스템 초기 설정

Genian NAC

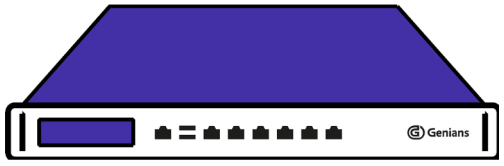
시스템 초기 설정

2) 센서 설정

7. 네트워크 스캔



UDP 5060



네트워크 센서

SIP Option

User-Agent
(VOIP Platform)

VoIP

SIP

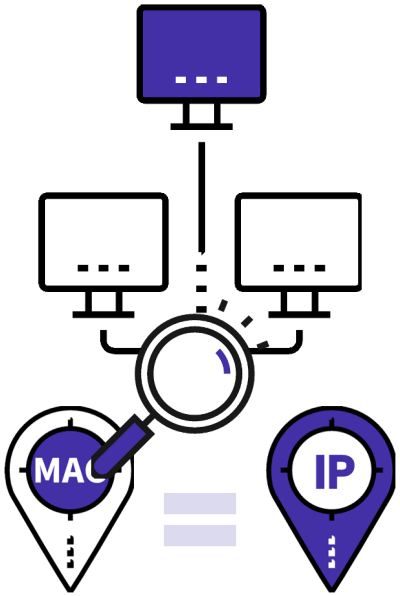
시스템-시스템 초기 설정

Genian NAC

시스템 초기 설정

2) 센서 설정

8. 노드 상태 검사



MAC/IP Clone 검사

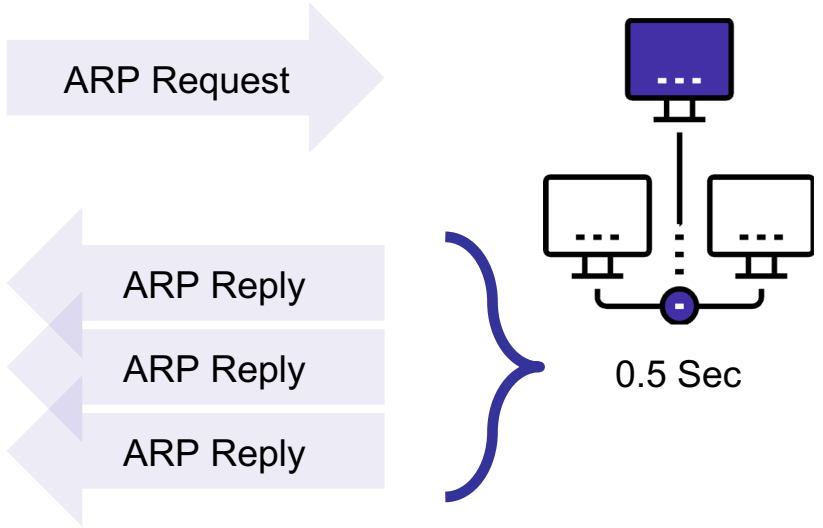
시스템-시스템 초기 설정

Genian NAC

시스템 초기 설정

2) 센서 설정

8. 노드 상태 검사



MAC/IP Clone 검사

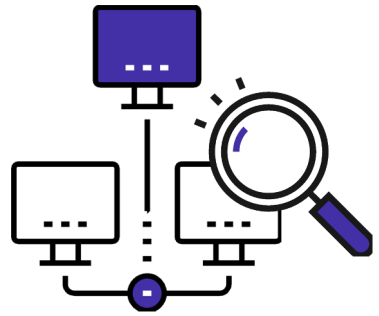
시스템-시스템 초기 설정

Genian NAC

시스템 초기 설정

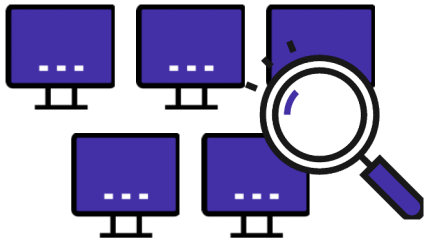
2) 센서 설정

9. 서브넷 노드 스캔



네트워크 센서 관리 범위

수행 주기



1 Sec

초당 스캔 개수

시스템-시스템 초기 설정

Genian NAC

2) 센서 설정

10. DHCP

DHCP	설명
서비스 대상	- 로컬: 센서의 관리네트워크에 대해서만 DHCP서버 기능을 제공 - 리모트: 현재 센서는 DHCP서버 기능을 제공하지 않고 리모트 서버에서만 제공 - 로컬과 리모트: 모든 센서에 대한 DHCP 서비스 제공
노드 IP Pool	DHCP IP 할당에 사용될 주소 영역을 설정합니다.
대여 시간	IP 대여 시간을 설정합니다.
DNS 서버	Client에 할당할 DNS 서버 주소를 설정합니다.
도메인 네임	기본 도메인 네임값을 설정합니다.
WINS 서버	WINS 서버 주소를 설정합니다.
NTP 서버	NTP서버 주소를 설정합니다.
센서 IP Pool	무선센서 DHCP IP 할당에 사용될 주소 영역을 설정합니다.
IP 할당 금지 대상	센서 DHCP IP 할당 금지 대상을 설정합니다.
DHCP 옵션	DHCP 패킷에서 옵션으로 사용할 항목을 설정합니다.
DHCP 노드 IP 고정	최초 DHCP IP할당 시 IP유지를 위해 변경금지 및 충돌 보호를 설정합니다.

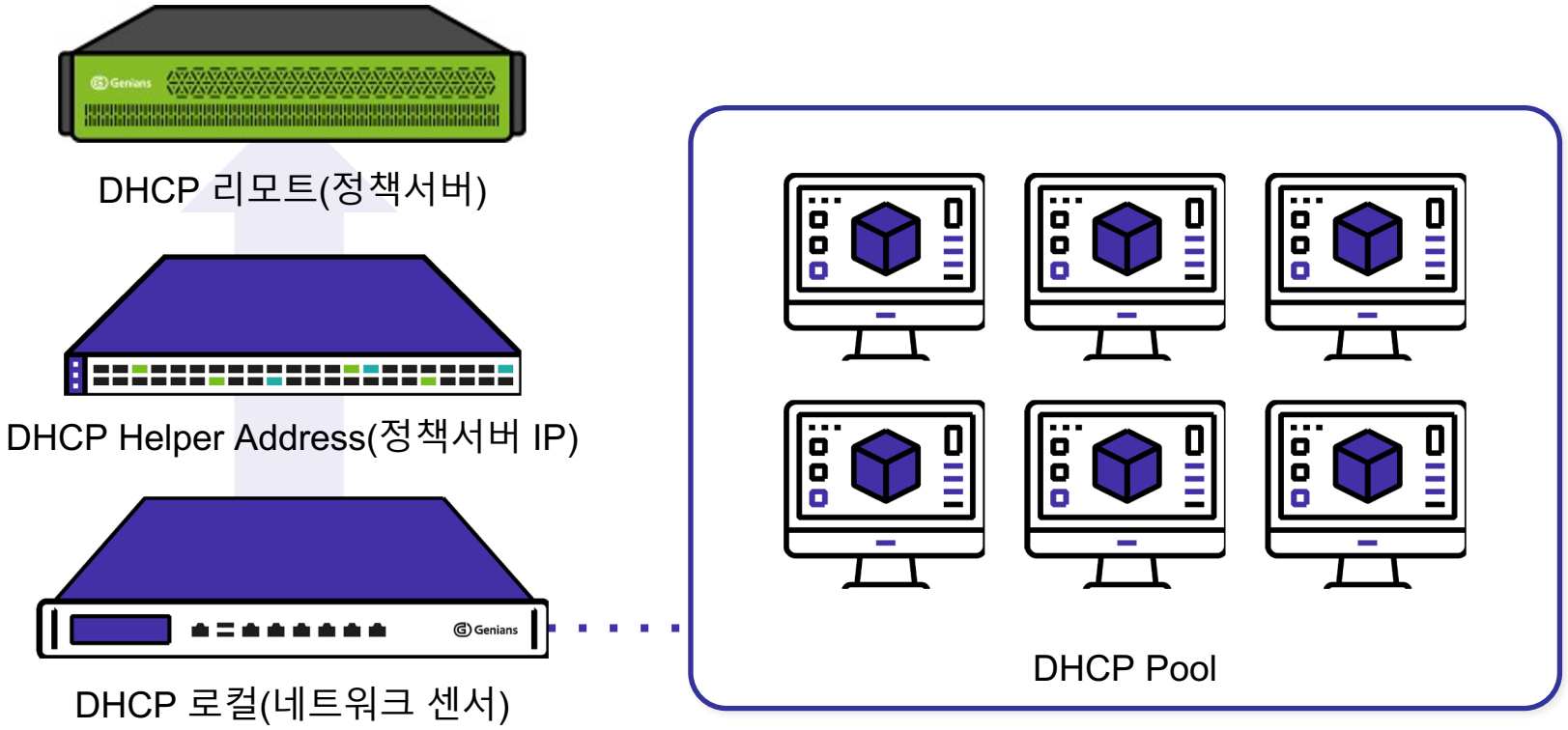
NAC DHCP 특수 설정

시스템-시스템 초기 설정

Genian NAC

2) 센서 설정

10.
DHCP



※ “리모트” DHCP 서버를 사용하기 위해서는 스위치에 DHCP Helper Address를 정책서버 IP로 설정해야 합니다.

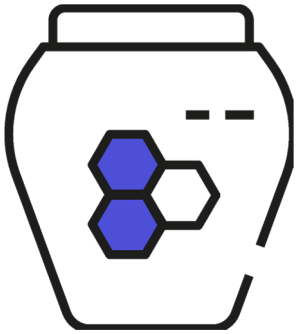
시스템-시스템 초기 설정

Genian NAC

시스템 초기 설정

2) 센서 설정

11. 가상 IP



네트워크 센서 관리 범위
IP
네트워크 센서 MAC

네트워크 센서 관리 범위
IP
네트워크 센서 MAC

네트워크 센서 관리 범위
IP
네트워크 센서 MAC

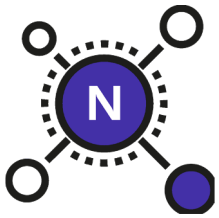
시스템-시스템 초기 설정

Genian NAC

시스템 초기 설정

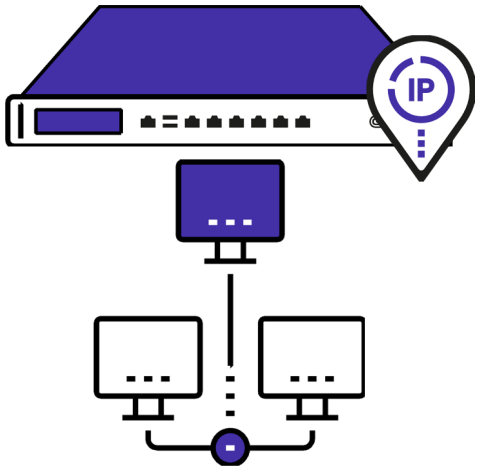
2) 센서 설정

12. IP 관리



MAC 차단 모드
IP 차단 모드
MAC / IP 차단 모드
허용 모드
변경금지 모드
충돌 보호 모드

신규 노드 정책



센서 IP 충돌 보호

※ 센서 IP 충돌 보호 기능 OFF 시 네트워크센서 IP로 IP 충돌이 발생할 경우 정상적인 서비스가 제공되지 않아 사용자 단말 네트워크에 문제점이 발생할 수 있습니다.

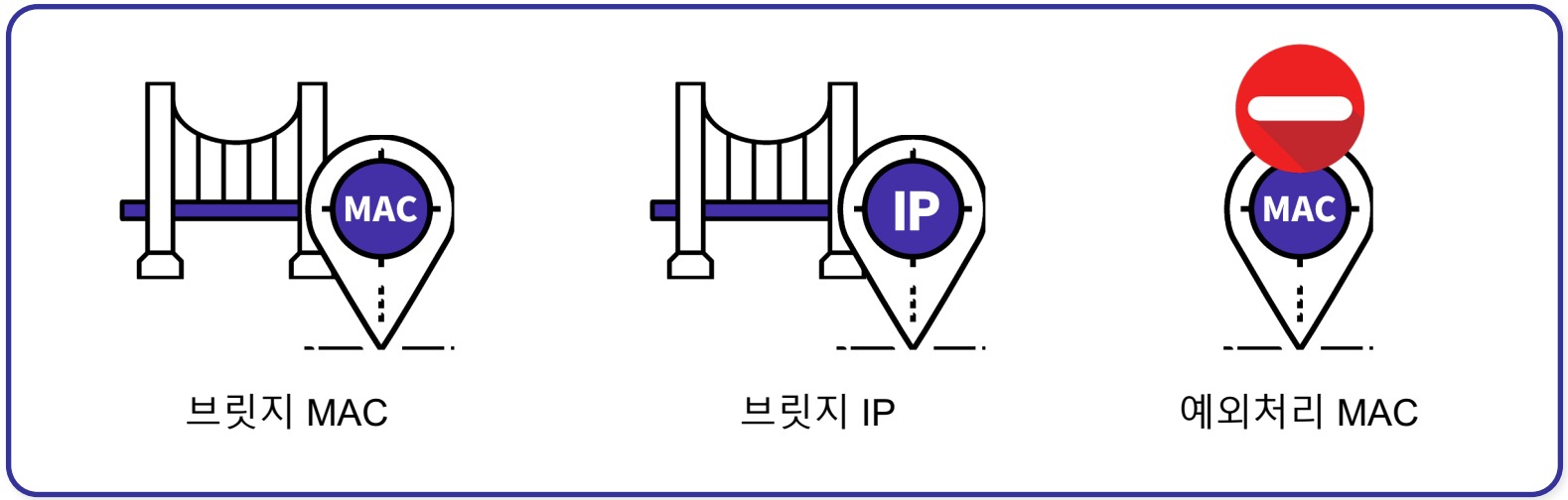
시스템-시스템 초기 설정

Genian NAC

시스템 초기 설정

2) 센서 설정

13. 기타 설정



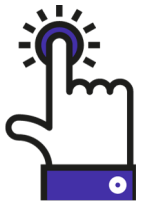
예외처리 설정

시스템-시스템 초기설정

Genian NAC

시스템 초기설정

3. 무선 센서
   환경설정



무선센서
동작

보안
설정

신호
감도

유효
시간

정보 갱신
주기

무선
제어

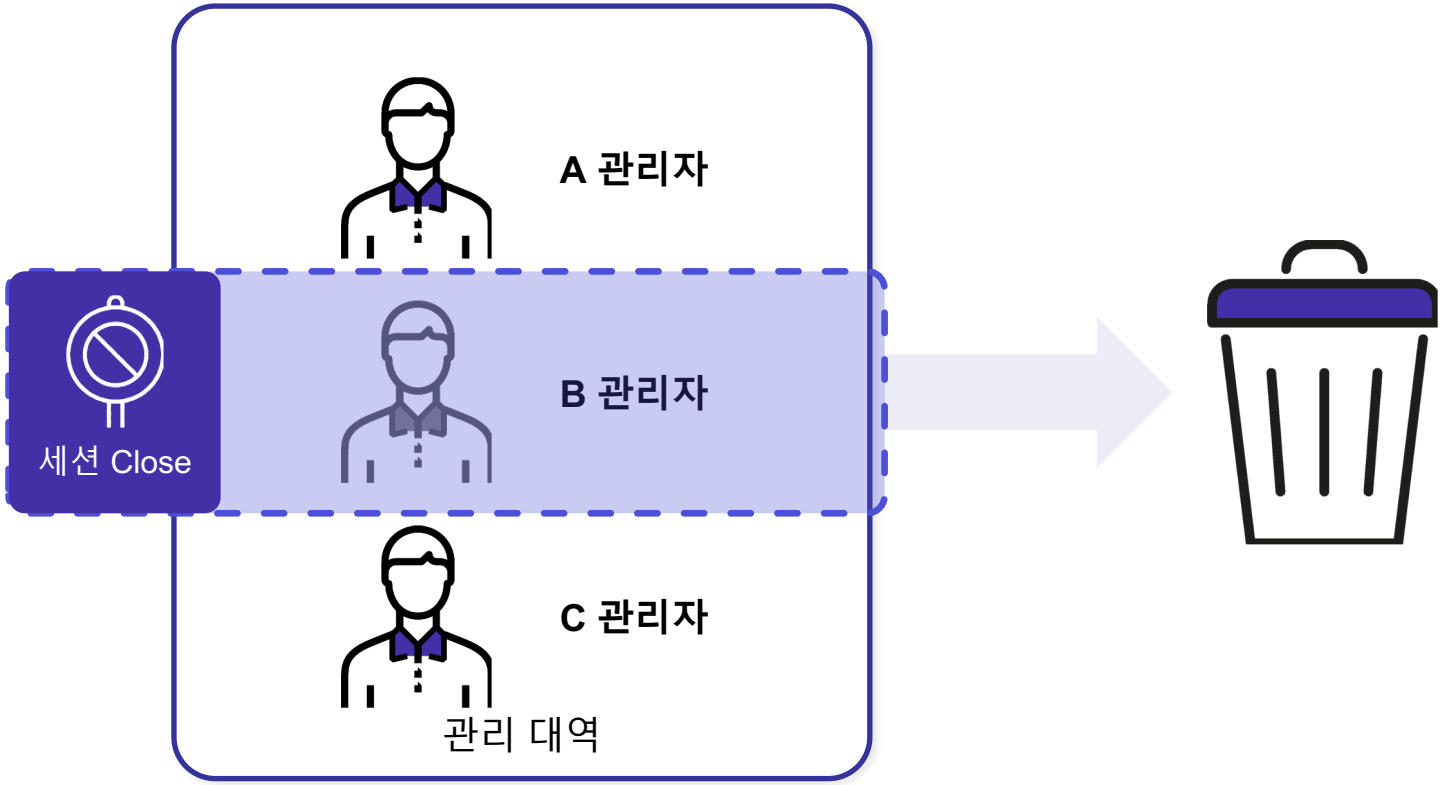
무선랜카드
설정

자원
경고

시스템-세션 관리

Genian NAC

세션
관리



시스템-라이선스

라이선스

항목	타입	입력값
제품명	1.3.6.1.4.1.29503.2.1.1	Genian NAC
버전	1.3.6.1.4.1.29503.2.1.2	5.0
제품종류	1.3.6.1.4.1.29503.2.1.3	NAC
라이센스용도코드	1.3.6.1.4.1.29503.2.2.0	1000
라이센스용도	1.3.6.1.4.1.29503.2.2.1	GENUINE
라이센스유효일	1.3.6.1.4.1.29503.2.2.2	9999-12-31
유지보수만료일	1.3.6.1.4.1.29503.2.2.3	2021-03-31 00:00:00
라이센스장비수	1.3.6.1.4.1.29503.2.2.4	3000
모듈명	1.3.6.1.4.1.29503.2.2.5	NAC WNAC A3S
라이센스대상	1.3.6.1.4.1.29503.2.2.7	GENIANS

시스템-라이선스

Genian NAC

라이선스

항목	타입	입력값
하드웨어MAC(eth0)	1.3.6.1.4.1.29503.2.3.1	AA:AA:AA:AA:AA:AA
하드웨어MAC(전체)	1.3.6.1.4.1.29503.2.3.2	AA:AA:AA:AA:AA:AA BB:BB:BB:BB:BB:BB
하드웨어시리얼	1.3.6.1.4.1.29503.2.3.3	XXXXXXXXXX
하드웨어모델명	1.3.6.1.4.1.29503.2.3.4	C20_R1
서버ID	1.3.6.1.4.1.29503.2.3.5	
고객명	1.3.6.1.4.1.29503.2.4.1	XXXX
담당자명	1.3.6.1.4.1.29503.2.4.2	
담당자전화번호	1.3.6.1.4.1.29503.2.4.3	
담당자이메일	1.3.6.1.4.1.29503.2.4.4	
CA파일명	1.3.6.1.4.1.29503.2.5.1	license-ca.crt
라이센스발급서버 호스트명	1.3.6.1.4.1.29503.2.5.2	bp

시스템-라이선스

Genian NAC

라이선스

1. 라이선스 위반사항

▶ 라이선스 장비 수량 초과

라이선스 장비 수량보다 관리하고 있는 노드가 많을 경우 “라이선스 초과” 메시지가 WebUI에 표시되며
90일을 기준으로 노드 세부 정보 (스위치, 포트, 트래픽, 접속AP, 인증 사용자, 플렛폼, 호스트명)에
“라이선스 수 초과 " 표시

▶ 유지보수

유지보수 기간이 초과된 경우 “운영 정보 데이터“ 업데이트 제한 및 기술지원 불가

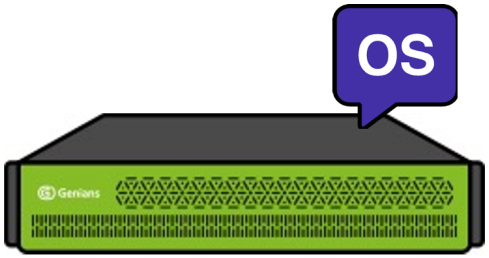
업데이트 관리

업데이트 관리 – 소프트웨어

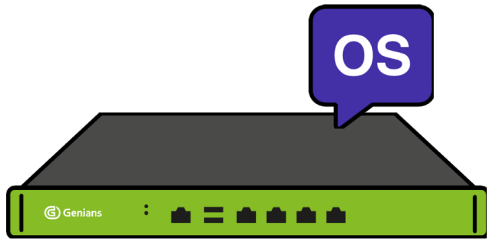
Genian NAC

소프트웨어

1) 수동 업로드
항목



정책서버 OS



네트워크 센서
OS

에이전트

모바일

업데이트 관리 – 소프트웨어

Genian NAC

소프트웨어

2) 플러그인

에이전트 플러그인

정책서버 플러그인

업데이트 관리 – 소프트웨어

Genian NAC

소프트웨어

2) 플러그인 – 에이전트 플러그인

에이전트 플러그인

업데이트 관리 – 소프트웨어

Genian NAC

소프트웨어

2) 플러그인 – 정책서버 플러그인

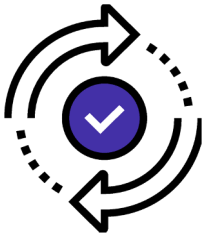
정책서버 플러그인

업데이트 관리 – 소프트웨어

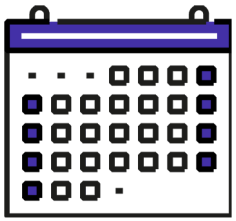
Genian NAC

소프트웨어

3) 운영 정보
데이터



수동 업데이트



유지보수 만료 일자

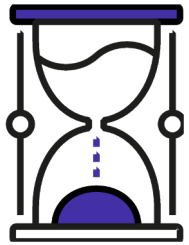
항목	내용
CVE 업데이트 정보	제품별 공개적으로 알려진 취약점 정보 데이터
PI 업데이트 정보	노드 플랫폼 부가정보 데이터
노드 정보 감지 데이터	NMAP으로 감지할 분류 데이터
운영체제 감지 데이터	NAC에서 노드 플랫폼 분류 데이터
운영체제 업데이트 정보	MS PMS 관련 목록 데이터

서비스 관리

서비스 관리 – 서비스 제어

Genian NAC

서비스 제어

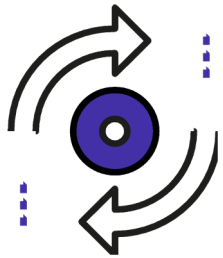


정책 적용

정책서버에 설정된 정책을 모든 네트워크센서와 에이전트에게 즉시 적용을 수행합니다.

서비스 중지

정책서버에 설정되어 수행중인 네트워크센서와 에이전트의 제어 서비스를 중지합니다.



웹어플리케이션 재구동

“관리 콘솔”, “CWP”, “IP 신청 시스템” 관련 웹어플리케이션을 개별적으로 재구동합니다.

서비스 관리 – 접속 포트

Genian NAC

접속 포트

서비스	포트	설명
HTTP	TCP/80	CWP, 신청 시스템
HTTPS	TCP/443 TCP/8443	CWP, 신청 시스템, 정책 수신, 정보업데이트 관리 콘솔
KeepAlive	UDP/3870 UDP/3871	Server / Sensor, Agent
Syslog	UDP/514 TCP/6514	Syslog 수신 / TLS를 통한 Syslog 수신
RADIUS Authentication	UDP/1812	RADIUS Authentication
RADIUS Accounting	UDP/1813	RADIUS Accounting
Data Server	TCP/3306	Database
Log Server	TCP/9200 TCP/9300	REST Service 클러스터 내의 노드 간 내부 통신
SSH	TCP/3910	CLI 접속

서비스 관리 – 디버그 로그

Genian NAC

디버그 로그

항목	내용
elasticsearch	Level Info 관련 서버 로그 확인
httpd	Apache Error 관련 로그 확인
mysqld	Mysql Error, Slowquery 관련 로그 확인
sysinspect	Sysinspect 스크립트로 수집된 로그 확인
system	시스템 message, NAC Center/Sensor Debug 로그 확인
tomcat	Tomcat page 발생한 Error 로그 확인
syscollect	모든 debug file을 취합하여 생성된 파일 확인

Summary

1. 시스템
   - 시스템 관리 : NAC 네트워크 센서, 무선센서 삭제 가능
   - 센서 관리 : 일괄 설정 가능
   - 시스템 초기 설정 : 신규로 등록되는 네트워크 센서, 무선 센서의 사전 설정 관련 프로파일
   - 라이선스 : 제품 동작 모듈 및 유효 일자 등록
2. 업데이트 관리

   정책서버, 네트워크 센서 이미지 / 리눅스, 윈도우, Mac OS 에이전트 버전 / 안드로이드, IOS 모니터 버전 관리

   정책서버, 에이전트 플러그인 버전 관리 / 운영 정보 데이터 버전 관리
3. 서비스 관리
   - 서비스 제어 : 시스템 적용중인 서비스 제어
   - 접속 포트 : 구동중인 NAC에서 사용중인 네트워크 접속 포트 정보 확인
   - 디버그 로그 : 시스템 어플리케이션에서 발생하는 디버그 로그 확인

Genians

문의 : 지니언스 네트워크보안기술부

ca-se-nac@genians.com