

IPScan Probe 600



IPScan Probe 600 설치 및 사용자가이드

Version : 3.5



스콧정보통신 주식회사

서울시 강남구 수서동 714-6번지 나성빌딩 4층 135-884

전화. 02-3412-9700 팩스. 02-3412-9800

<http://www.scope.co.kr>

<http://www.ipscan.co.kr>

E-mail: scopeinc@scope.co.kr

스콧정보통신(주) IPScan V3.5

Copyright 2000-2006 by 스콧정보통신(주)

서울시 강남구 수서동 714-6번지 나성빌딩 4층 135-884

전화. 02-3412-9700 팩스. 02-3412-9800

Printed in Korea

스콧정보통신(주)의 동의 없이 본 설치 가이드의 무단 복제 및 사용을 금합니다.

목 차

| | |
|--|----|
| 1. 개요 | 4 |
| 1.1. IPSCAN 소개 | 5 |
| 1.2. IPSCAN 제품군 소개 | 6 |
| 1.3. IPSCAN PROBE 600 구성 및 설치 | 7 |
| 1.3.1. 제품 소개 및 구성 | 7 |
| 1.3.2. IPScan Probe 600 설치 | 9 |
| 2. IPSCAN PROBE 600 사용법 | 11 |
| 2.1. MAIN MENU | 12 |
| 2.2. SYSTEM | 13 |
| 2.2.1. Password | 13 |
| 2.2.2. Ethernet Port 별 System설정 | 14 |
| 2.2.2.1. ARP check Interval [Online](min)/[Offline](min) | 15 |
| 2.2.2.2. Off range Interval (min) | 15 |
| 2.2.2.3. Automatic Private IP addressing detection | 16 |
| 2.2.2.4. Maximum ARP Packet per sec | 16 |
| 2.2.2.5. Excess ARP Packet suspension period (sec) | 17 |
| 2.2.2.6. DHCP Block Alarm | 17 |
| 2.3. LAN | 18 |
| 2.3.1. Master Port 기능 상세설명 | 20 |
| 2.4. RETURN TO DEFAULT | 23 |
| 2.5. SAVE | 23 |
| 2.6. SAVE & APPLY | 23 |
| 2.7. SYSTEM SHUTDOWN | 23 |
| 2.8. SYSTEM STATUS | 24 |
| 2.9. OPERATING CONFIG | 25 |
| 2.10. TAKE OVER | 26 |
| 2.11. PING TEST | 28 |
| 3. 부록 | 29 |
| 3.1. 통신 포트 정보 | 30 |
| 3.2. 네트워크 구성도 | 31 |
| 3.3. Q&A | 33 |



IP/MAC resource Management and network security solution

www.scope.co.kr

1. 개요

이 장에서는 IPScan에 대한 전반적인 이해를 돕고자 제품 설명 및 구성에 대한 정보를 제공합니다.

| | |
|-------------------------------|---|
| 1.1. IPScan 소개 | 4 |
| 1.2. IPScan 제품군 소개 | 5 |
| 1.3. IPScan Probe 600 구성 및 설치 | 6 |
| 1.3.1. 제품소개 및 구성 | 6 |
| a. 기능요약 | 6 |
| b. 장비사양 | 6 |
| c. 설치 전 확인사항 | 7 |
| d. 장비 외관 설명 | 7 |
| 1.3.2. 설치 | 8 |
| 1.3.3. 터미널을 이용한 접속방법 | 9 |

1.1. IPScan 소개

IPScan 은 전산 관리자들에게 보다 효율적인 업무 환경을 제공하기 위한 네트워크 주소 통합 관리 솔루션입니다. IP 주소 기반의 네트워크는 사용자들에게 편리한 네트워크 환경을 제공하고 있지만 이를 유지, 관리해야 할 의무를 지니고 있는 전산 관리자들에게는 또 하나의 업무 부담을 주고 있는 것이 사실입니다.

기존의 수동적인 IP 주소 관리 환경 속에서는 사용자들의 무분별한 IP 주소 사용과 이로 인해 발생하는 여러 가지 네트워크 장애들을 신속히 처리하지 못하여 물적, 인적 자원의 손실로 이어져 왔습니다.

IPScan 은 이러한 문제점들을 사전에 방지하고 신속한 조치를 취할 수 있도록 여러 단계의 검증과 실사를 통해 안전하게 설계된 네트워크 주소 통합 관리 솔루션 입니다.

그 주요 기능은 다음과 같습니다.

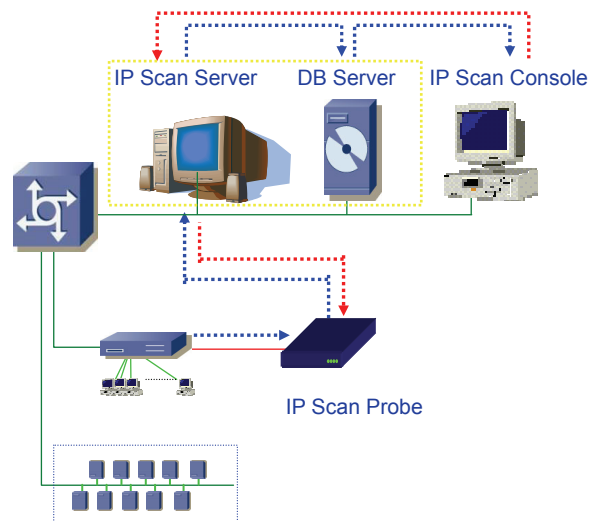
- ① 네트워크상의 모든 IP/MAC 주소 자동 관리 기능
- ② IP 주소 충돌 시 신속한 차단 기능
- ③ MAC 주소를 이용한 DHCP 환경 내에서의 사용자 주소관리 기능
- ④ 네트워크 실명제 도입을 위한 호스트 이름 차단 기능
- ⑤ 관리자에 의한 비 인증 IP 주소 사용자 차단 기능
- ⑥ 각 사용자별 IP 주소 사용기간 예약 및 제한 기능
- ⑦ PortScan 을 통한 특정 서비스 설치 유무 판단 기능
- ⑧ Switch Port 관리 및 제어 기능
- ⑨ 사용자별 그룹 통계 관리 기능
- ⑩ 실시간 이벤트 감지 및 저장 기능
- ⑪ 과도한 패킷 송수신자 차단 기능
- ⑫ 다양한 형태의 보고서 지원

1.2. IPScan 제품군 소개

IPScan 제품군의 구성은 다음과 같습니다.

- ① 각각의 세그먼트나 VLAN에 설치되는 *IPScan Probe*
 - IPScan Probe 50 :
 - ✓ 1 Port 의 10/100 Mbps Ethernet Interface 를 지원합니다.
 - ✓ 소규모 네트워크에 적용되도록 설계된 제품입니다.
 - IPScan Probe 100
 - ✓ 1 Port 의 10/100 Mbps Ethernet Interface 를 지원합니다.
 - ✓ 중,소 규모의 네트워크에 적용되도록 설계된 제품입니다.
 - IPScan Probe 100A
 - ✓ 1 Port 의 10/100 Mbps Ethernet Interface 를 지원합니다.
 - ✓ 중,소 규모의 네트워크에 적용되도록 설계된 제품입니다.
 - ✓ IPScan Probe 100 의 발전된 모델로 DHCP 서버, 서비스 스캔과 스위치 포트 스캔 등의 기능이 새롭게 추가된 제품입니다.
 - IPScan Probe 200
 - ✓ 2 Port 의 10/100 Mbps Ethernet Interface 를 지원합니다.
 - ✓ 중,대 규모의 네트워크에 적용되도록 설계된 제품입니다.
 - IPScan Probe 600
 - ✓ 6 Port 의 10/100 Mbps Ethernet Interface 를 지원합니다.
 - ✓ 대규모 네트워크에 적용되도록 설계된 제품입니다.
- ② 모든 IPScan Probe와 직접적인 통신을 제어하는 통신 모듈로 Probe로부터 데이터를 수신하여 이를 DB에 저장하고, IPScan Console로부터 설정된 Probe관련 설정 사항들을 Probe로 전송하는 *IPScan Server*.
- ③ 전체 Probe의 데이터와 상태를 서버 접속을 통해 조회 및 관리할 수 있는 사용자 인터페이스 *IPScan Console*.

기본 네트워크 구성도는 다음과 같습니다.



1.3. IPScan Probe 600 구성 및 설치

1.3.1. 제품 소개 및 구성

IPScan Probe 600 는 여섯 개의 10/100Mbps Ethernet Interface 를 지원하며 설정된 네트워크 세그먼트의 IP 주소 정보를 수집하여 IPScan 서버에 전달하고, 이에 따른 차단 및 스캔 기능 등을 수행합니다. 대 규모의 네트워크에 적용할 수 있으며, VLAN 을 사용하고 있는 네트워크의 경우에도 이를 통합 관리를 할 수 있도록 설계된 제품입니다.

a. 기능요약

- ✓ 설정된 IP 주소 대역에 대한 정보 수집
- ✓ 설정된 IP/MAC 주소에 대한 차단 및 해제 기능 수행
- ✓ 관리자의 설정에 따라 DHCP 서버 기능 수행
- ✓ 관리자의 설정에 따라 TCP 포트에 대한 서비스 스캔 기능 수행
- ✓ 관리자의 설정에 따라 스위치 포트 제어 기능 수행

b. 장비사양

| | |
|----------------|---------------------------------|
| CPU | Intel Celeron 850 MHz |
| System Memory | 128MB SDRAM |
| HDD | 40GB |
| Interface | Ethernet 10/100Mbps (RJ45) 6 포트 |
| Console | RS-232 1 포트 |
| Size | 435mm(W) x 44mm(H) x 285mm(D) |
| 운영환경 | 온도 0~40℃, 습도 0~90% |
| 입력전원 | AC 90~250V, 50~60Hz |
| OS | Linux Kernel 2.4.20 |
| Trunk Protocol | IEEE 802.1q 지원 |

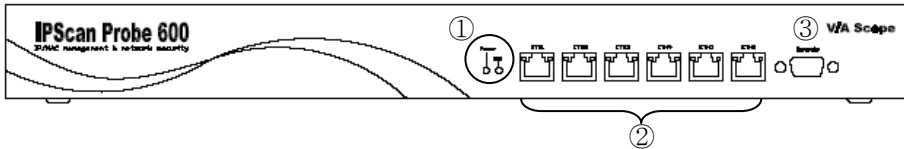
c. 설치 전 확인사항

IPScan Probe 600의 제품 포장 내에 아래의 내용물이 포함되어 있는지 확인합니다.

- ① IPScan Probe 1개
- ② IPScan Probe 설치 가이드 1권
- ③ 전원케이블 1개
- ④ 시리얼 콘솔 연결용 RS232 케이블 1개
- ⑤ 네트워크 연결 용 RJ45 케이블 2개
- ⑥ 19인치 Rack에 고정시키기 위한 Rack Mount 1세트

d. 장비 외관설명

IPScan Probe 600 전면부



IPScan Probe 600 후면부



- ① LED 부 : IPScan Probe 의 데이터 처리 상태와 장비 상태를 보여줍니다.
 - Power : 전원이 연결되면 녹색 점등 됩니다.
 - LED : 황색 점등 시 10Mbps 속도로 연결된 상태이며, 녹색 점등 시 100Mbps 속도로 연결된 상태입니다.
- ② Ethernet : IPScan Server 와의 통신 및 데이터 수집을 위해 RJ-45 케이블을 이용해서 네트워크에 연결합니다. Eth1~Eth6 까지 총 6 개의 Ethernet 포트를 사용할 수 있습니다.
- ③ Console : IPScan Probe를 콘솔로 제어하는 경우, RS232 콘솔 케이블을 연결합니다.
- ④ 전원 스위치 : 전원케이블 연결 후 전원을 'ON/OFF' 합니다
- ⑤ 전원 입력 : 전원케이블을 이용해서 전원에 연결합니다.

1.3.2. IPScan Probe 600 설치

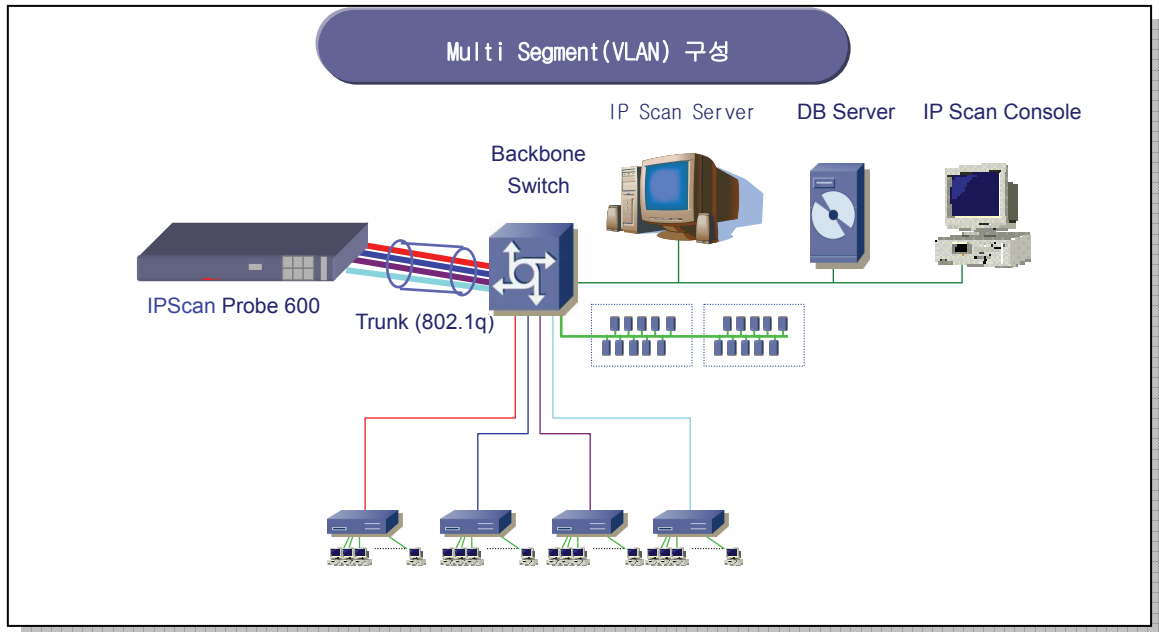
IPScan Probe 600는 기존의 네트워크에 대한 구성 변경 없이 Ethernet 상에 손쉽게 설치하실 수 있습니다.

장비 설치의 다음의 순서에 따라 진행합니다.

- ① IPScan Probe 600는 여섯 개의 10/100Mbps Ethernet Interface를 지원하므로
 - ✓ 다수의 단일 세그먼트를 각각 관리하고자 할 때에는 일반 스위치 포트에 연결합니다. 단, 데이터 유실 없는 정확한 IP 주소 관리를 위해서는 하나의 네트워크 안에 적어도 한 개의 Probe를 설치하고, 가급적 상위 레벨의 스위치 포트에 설치하는 것을 권장합니다.
 - ✓ 다수의 세그먼트를 관리하고자 할 때에는 IPScan Probe 600와 Switch는 802.1q Trunk Port에 연결 되어 합니다.
- ② 설치하고자 하는 위치에서 IPScan Probe에 전원케이블과 RJ45 LAN 케이블을 연결합니다.
- ③ IPScan Probe의 전원스위치를 켭니다.
- ④ 제공된 RS232 콘솔케이블의 한쪽은 IPScan Probe에 연결하고 한쪽은 콘솔의 COM 포트에 연결한 후, 터미널 소프트웨어 등을 이용해서 IPScan Probe에 접속합니다.

Note IPScan Probe 600은 사용 중 시스템의 재부팅이 필요하거나 장비 종료를 해야 할 경우 전원스위치를 바로 내리게 되면 운영 중에 있던 OS가 손상을 입을 가능성이 있습니다. 따라서, 제품의 종료 시에는 반드시 [Main Menu]의 [6] [System Shutdown]을 실행한 후 시스템의 동작이 멈춘 것을 확인 후 전원스위치를 내려 주시기 바랍니다.

기본 네트워크 구성 예



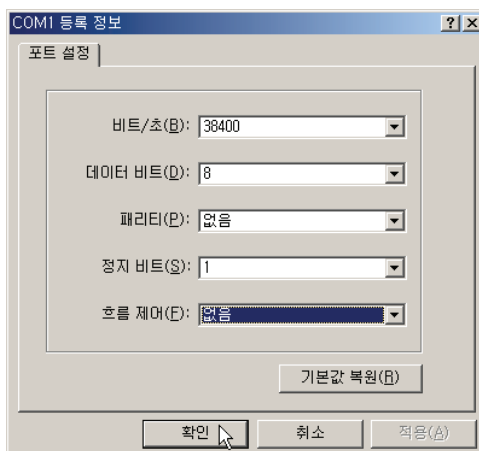
Note 자세한 설치 관련 네트워크 구성도는 '3.2. 네트워크 구성도' (p29) 를 참조하시기 바랍니다.

1.3.3. 터미널을 이용한 접속방법

IPScan Probe 600 의 운영을 위해서는 표준 터미널 (Telnet) 이나 PC 들이 제공하는 터미널 소프트웨어를 이용해서 Probe 에 접속할 수 있습니다.

설치 후 최초 접속 시에는 네트워크 설정을 위해 터미널 등을 이용하여 콘솔로 접속합니다. 윈도우 기반의 PC 시스템은 터미널 에뮬레이션 소프트웨어인 [하이퍼터미널]이 제공됩니다.

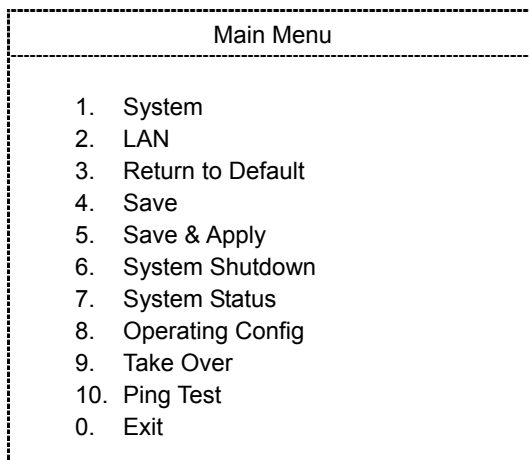
Step1 아래의 상수들을 이용해서 터미널의 등록정보를 설정하고 [확인]을 선택하면 IPScan Probe 에 접속됩니다.



비트/초(B) : 38400
 데이터 비트 : 8
 패리티 : 없음
 정지 비트 : 1
 흐름 제어 : 없음

Step2 터미널을 이용하여 접속하면 Password 입력란이 나타납니다. 최초 접속 시에는 Password 가 설정되어 있지 않으므로 [Enter]를 누르시면 아래의 초기 [Main Menu]로 들어갈 수 있습니다.

Step3 접속이 성공하면 다음과 같은 메뉴화면이 나타납니다.





IP/MAC resource Management and network security solution
www.scope.co.kr

2. IPScan Probe 600 사용법

이 장에서는 IPScan Probe 600의 메뉴 사용법에 대한 내용을 다룹니다.
 각각의 기능별 설정 방법과 주의 사항들이 소개됩니다.

| | |
|--|----|
| 2.1. Main Menu | 11 |
| 2.2. System | 12 |
| 2.2.1. Password | 12 |
| 2.2.1. Ethernet Port별 System 설정 | 13 |
| 2.2.2.1. ARP check Interval [Online](min)/[Offline](min) | 14 |
| 2.2.2.2. Off range Interval (min) | 14 |
| 2.2.2.3. Automatic Private IP addressing detection | 15 |
| 2.2.2.4. Maximum ARP Packet per sec | 15 |
| 2.2.2.5. Excess ARP Packet suspension period | 16 |
| 2.2.2.6. DHCP Block Alarm | 16 |
| 2.3. LAN | 17 |
| 2.3.1. Master Port 기능 상세 설명 | 18 |
| 2.4. Return to Default | 21 |
| 2.5. Save | 21 |
| 2.6. Save &Apply | 21 |
| 2.7. System Shutdown | 21 |
| 2.8. System Status | 22 |
| 2.9. Operating Config | 23 |
| 2.10. Take Over | 24 |
| 2.11. Ping Test | 26 |

2.1. Main Menu

[Main Menu]는 IPScan Probe의 운영과 제어에 필요한 모든 기능들을 보여줍니다. 모든 메뉴들은 원하는 기능의 번호를 입력하는 방식으로 진행됩니다.

| Main Menu | |
|-----------------------------|-------------------|
| 1. | System |
| 2. | LAN |
| 3. | Return to Default |
| 4. | Save |
| 5. | Save & Apply |
| 6. | System Shutdown |
| 7. | System Status |
| 8. | Operating Config |
| 9. | Take Over |
| 10. | Ping Test |
| 0. | Exit |
| Main Menu Select a number : | |

| NO | 메뉴 | 설명 |
|----|-------------------|--|
| 1 | System | IPScan Probe Password 및 ARP 전송주기 등을 설정 |
| 2 | LAN | IPScan Probe 및 Server에 대한 네트워크 주소등을 설정 |
| 3 | Return to Default | 시스템 설정값 초기화 |
| 4 | Save | 시스템 설정에 대한 변경사항을 저장 |
| 5 | Save & Apply | 시스템 설정에 대한 변경사항을 저장 및 적용 |
| 6 | System Shutdown | IPScan Probe 시스템 종료 |
| 7 | System Status | IPScan Probe의 전체 시스템 설정 정보를 제공 |
| 8 | Operating Config | IP/MAC 차단 기능에 대한 상세 설정 기능 |
| 9 | Take Over | IPScan Probe 이중화 설정 |
| 10 | Ping Test | 네트워크 연결확인을 위한 Ping 기능 |
| 0 | Exit | 종료 |

2.2. System

다음의 메뉴와 같이 IPScan Probe 600 의 Password 설정 및 각 Ethernet Port 별 통신 및 데이터 수집 주기 등을 설정할 수 있도록 합니다.

Step1 [Main Menu] -> 1. [System]을 선택합니다.

Manin Menu Select a number : 1

Step2

| System | |
|--------|-----------------|
| 1. | Password |
| 2. | Ethernet Port 1 |
| 3. | Ethernet Port 2 |
| 4. | Ethernet Port 3 |
| 5. | Ethernet Port 4 |
| 6. | Ethernet Port 5 |
| 7. | Ethernet Port 6 |
| 0. | Main Menu |

각각의 Ethernet Port 마다 System 환경 설정을 할 수 있습니다.

2.2.1. Password

IPScan Probe 는 제품 출고 시 Password 가 설정되어 있지 않습니다. 따라서 관리 효율을 높이기 위해 반드시 최초 Probe 설치 시에 Password 를 설정하는 것을 권장하고 있습니다.

Step1 [Main Menu] -> 1. [System]을 선택하고, [System] 메뉴에서 1 번을 선택합니다.

System setting. Select a number : 1

Step2 Password는 15자리 이하의 숫자와 영자, 혹은 특수문자의 조합으로 입력합니다. 특수문자에 대한 제한은 없으며 키보드상의 모든 문자 배열을 이용하실 수 있습니다.

Enter a new password : *****

Confirm the password : *****

Password 를 잊으신 경우 또는 설정해 놓은 Password 가 실행되지 않을 경우에는 IPScan Probe 를 구입하신 대리점 또는 본사 기술지원팀으로 문의하시기 바랍니다.

2.2.2. Ethernet Port 별 System 설정

IPScan Probe 의 각 Ethernet Port 별 IPScan Server 간의 통신주기 설정 및 관리 IP 주소 대역에 대한 데이터 수집주기를 확인 및 설정할 수 있습니다.

Step1 [Main Menu]에서 1 번 [System]을 선택하고, 설정하고자 하는 Ethernet Port 를 선택합니다.

Step2 아래와 같은 메뉴화면이 나타나면 설정하고자 하는 메뉴의 번호를 입력하고 [Enter]를 누릅니다.

| System | |
|--------|---|
| 1. | ARP check interval [Online](min) [5] |
| 2. | ARP check interval [Offline](min) [10] |
| 3. | Off range Interval(min) [0] |
| 4. | Automatic Private IP addressing detection [Off] |
| 5. | Maximum ARP Packet per sec [5000] |
| 6. | Excess ARP Packet suspension period(sec) [1] |
| 7. | DHCP Block Alarm (min) [10] |
| 0. | Main Menu |

| NO | 메뉴 | 설명 | 기본값 |
|----|---|--|------|
| 1 | ARP check interval [Online] (min) | Probe의 설정 중인 Eth Port가 관리하는 IP주소 대역에 대한 데이터 업데이트를 위해 Active상태인 IP에 대해서 ARP 패킷을 전송하는 주기를 설정합니다. | 5분 |
| 2 | ARP check interval [Offline](min) | Probe의 설정 중인 Eth Port가 관리하는 IP주소 대역에 대한 데이터 업데이트를 위해 Non-Active상태인 IP에 대해서 ARP 패킷을 전송하는 주기를 설정합니다. | 10분 |
| 3 | Off range Interval (min) | 범위초과 IP 검출 시 전송주기 설정. | 0 |
| 4 | Automatic Private IP addressing detection | DHCP 환경 내에서 DHCP 서버로부터 IP주소를 할당 받지 못한 사용자가 있을 경우 MS Windows OS에서 임의로 주어지는 IP주소에 대해 Probe가 이 예외 IP 주소에 대해서 범위 외 로그 및 차단 처리를 할 것인지를 설정합니다. | Off |
| 5 | Maximum ARP Packet per sec | Probe의 설정 중인 Eth Port에서 발생하는 ARP 패킷 수를 설정합니다. | 5000 |
| 6 | Excess ARP Packet suspension period (sec) | ARP 패킷의 과다 생성에 의한 네트워크 부하를 줄이기 위해 ARP패킷이 설정한 최대값을 초과하여 생성되면 패킷 생성 제한주기 이후 다시 생성하게 할 수 있도록 제한주기를 설정. | 1초 |
| 7 | DHCP Block Alarm (min) | Probe가 DHCP서버로 설정될 경우 비 인증 IP주소에 대한 [IP 차단]을 차단 전에 알려주는 알람 설정 | 0 |
| 0 | Main Menu | Main Menu로 이동 | |

2.2.2.1. ARP check Interval [Online](min)/[Offline](min)

설정된 주기마다 ARP 패킷을 이용하여 각 IP 주소들에 대한 On/Off 상태를 체크합니다.

Step1 Online 상태 체크는 [Main Menu] -> 1. [System]을 선택하고, 설정하고자 하는 Ethernet Port 를 선택합니다. 1. [ARP check Interval [Online]]을 선택합니다.

System setting. Select a number : 1

Step2 주기를 설정합니다. 0-1440 분까지 입력가능하고, 기본값은 5 분입니다. 값을 입력하고 [Enter]를 누릅니다.

Enter the data forwarding interval between 0-1440 minutes : 5

Step3 Offline 상태 체크는 [Main Menu] -> 1. [System]을 선택하고, 설정하고자 하는 Ethernet Port 를 선택합니다. 2. [ARP check Interval [Offline]]을 선택합니다.

System setting. Select a number : 2

Step4 주기를 설정합니다. 0-1440 분까지 입력가능하고, 기본값은 10 분입니다. 값을 입력하고 [Enter]를 누릅니다.

Enter the data forwarding interval between 0-1440 minutes : 10

위의 설정 예제는 Probe가 각 관리대상 IP주소 중 온라인 상에 있는 주소는 5분 간격으로 체크하고, 오프라인 상에 있는 주소는 10분 간격으로 체크하여 그 사용유무를 확인합니다.

2.2.2.2. Off range Interval (min)

관리 대상 범위로 설정되어 있는 IP 주소 대역 이외의 IP 가 검출되면 서버로 범위초과 IP 이벤트를 전송하게 됩니다. 이때 범위 초과 이벤트의 전송 주기를 설정 합니다.

Step1 [Main Menu] -> 1. [System]을 선택하고, 설정하고자 하는 Ethernet Port 를 선택합니다. 3. [Off range Interval]을 선택합니다.

System setting. Select a number : 3

Step2 설정하고자 하는 주기 값을 입력하고, [Enter]를 누릅니다.

- 1-1440분까지 설정이 가능합니다.
- -1 값을 설정하면 범위 초과 이벤트를 서버로 전송하지 않습니다.
- 0 값을 설정하면 범위 초과된 IP에 대해서 동일 IP에 대한 이벤트 발생 시 Probe가 시작되어 종료될 때까지 한번만 전송합니다.

Enter the Off range send interval between -1~1440 minutes.

If this value is -1, This event will be ignored.

Enter the value : 0

2.2.2.3. Automatic Private IP addressing detection

사용자의 네트워크 환경이 DHCP 서버를 이용하여 IP 주소를 할당하고 있는 경우, DHCP 서버로부터 IP 주소를 할당 받지 못하는 사용자가 발생할 수 있습니다. 이 경우 Microsoft Windows OS에서는 이런 사용자들에게 임의로 169.254.X.X 대역의 IP 주소를 부여합니다.

이 기능은 이와 같은 현상이 발생하게 되면 이 임의의 IP주소 대역에 대하여 기존의 설정대역 범위초과 시 발생하는 이벤트 로그와 같은 방법으로 범위초과 IP주소로 검출할 것인지 아닌지에 대한 설정을 할 수 있도록 합니다.

- Step1** [Main Menu] -> 1. [System]을 선택하고, 설정하고자 하는 Ethernet Port 를 선택합니다.
4. [Automatic Private IP addressing detection]을 선택합니다.

| Automatic Private IP addressing detection | |
|---|-----|
| 0. | On |
| 1. | Off |

- Step2** 169.254.x.x 대역에 대해 범위초과 IP주소로 검출할 것이면 0번, 검출하지 않을 것이면 1번을 선택합니다.

2.2.2.4. Maximum ARP Packet per sec

IPScan Probe 에서 관리대상 범위로 설정되어 있는 IP주소 대역에 대하여 그 사용유무 확인을 위해 생성하는 ARP 패킷의 수를 설정을 합니다.

과다한 ARP 패킷 생성은 네트워크에 과부하를 초래할 수도 있으므로 IPScan Probe에서는 자체 장비에서 발생하는 ARP패킷을 적정수준으로 유지하기 위해 이 기능을 사용하고 있습니다.

- Step1** [Main Menu] -> 1. [System]을 선택하고, 설정하고자 하는 Ethernet Port 를 선택합니다.
5. [Maximum ARP Packet per sec]을 선택합니다.

System setting. Select a number : 5

- Step2** 1초당 발생하는 ARP 패킷의 최대값을 설정합니다.
1-9999까지 설정이 가능하며, 관리자의 네트워크 규모에 따라 설정을 변경할 수 있습니다.
기본값은 5000개로 설정되어 있습니다.

Enter Maximum ARP Packet per sec
Enter the value : 5000

1초당 ARP 패킷을 5000개 이상 발생시키지 않도록 설정되었습니다.

2.2.2.5. Excess ARP Packet suspension period (sec)

위의 2.2.2.4. Maximum ARP Packet per sec에서 설정한 패킷 제한 수가 범위를 초과할 경우 네트워크 과부하 방지를 위해 ARP 패킷 생성 제한 주기를 설정합니다. 이 제한주기 동안에는 100개 이상 ARP 패킷을 생성하지 않도록 설정되어 있습니다.

Note 이 제한주기를 너무 길게 설정해 놓을 경우 설정된 기간 동안 데이터 유실이 발생하므로 가급적 짧게 설정하는 것을 권장합니다.

Step1 [Main Menu] -> 1. [System]을 선택하고, 설정하고자 하는 Ethernet Port 를 선택합니다.
6. [Excess ARP Packet suspension period]을 선택합니다.

System setting. Select a number : 6

Step2 ARP 패킷 생성 제한주기를 설정합니다. 1-1440초까지 설정 가능하며, 기본값은 1초로 설정되어 있습니다.

Enter Excess ARP Packet suspension period(sec)
Enter the value : 1

위의 설정사항은 '2-1-4. Maximum ARP Packet per sec'에서 설정한 최대값을 초과할 경우 1 초 동안 ARP 패킷 발생을 100 미만으로 제한하도록 설정되었습니다.

2.2.2.6. DHCP Block Alarm

DHCP 환경에서 비 인증 IP 주소가 발견될 경우 자동 차단 하기 전에 Probe 에서 IPScan Server 로 알람 메시지를 전송합니다. 이 알람 메시지를 전송할 주기를 설정합니다.

Step1 [Main Menu] -> 1. [System]을 선택하고, 설정하고자 하는 Ethernet Port 를 선택합니다.
7. [DHCP Block Alarm]을 선택합니다.

System setting. Select a number : 7

Step2 차단 알람 메시지의 전송주기를 설정합니다.
0-1440분까지 설정이 가능하며, -1값을 설정하게 되면 이 이벤트가 발생하는 것을 무시하고 알람 메시지를 전송하지 않습니다.

Enter the DHCP block alarm time between -1~1440 minutes.
If this value is -1, This event will be ignored.
Enter the value : 10

2.3. LAN

IPScan Probe 가 네트워크상에 연동될 수 있도록 네트워크 환경 설정을 합니다.

Step1 [Main Menu]에서 2 번 [LAN]을 선택합니다.

Step2 아래와 같은 메뉴화면이 나타나면 설정하고자 하는 Ethernet Port 번호를 선택하면 오른쪽의 메뉴와 같이 각 Ethernet Port 별 네트워크 환경 설정을 합니다.

| LAN | | Ethernet Port 1 | |
|-----|-----------------|-----------------|-----------------------------------|
| 0. | Ethernet Port 1 | 1. | IP [192.168.101.20] |
| 1. | Ethernet Port 2 | 2. | Netmask [255.255.255.0] |
| 2. | Ethernet Port 3 | 3. | Gateway [192.168.101.1] |
| 3. | Ethernet Port 4 | 4. | Master Server IP [192.168.101.10] |
| 4. | Ethernet Port 5 | 5. | Secondary Server IP [0.0.0.0] |
| 5. | Ethernet Port 6 | 6. | Connection Port [30001] |
| 0. | Main Menu | 7. | VLAN ID [0] |
| | | 8. | Master Port [0] |
| | | 9. | Speed [Auto] |
| | | 0. | Main Menu |
| | | MAC Address | [00:03:2e-05:02:77] |
| | | Serial No | [VSxxxxxxxxxxxxxx] |

| No | 메뉴 | 설명 |
|----|---------------------|---|
| 1 | IP | 설정 중에 있는 IPScan Probe 의 IP 주소 설정 |
| 2 | Netmask | 서브넷 마스크 설정 |
| 3 | Gateway | 게이트웨이 IP 주소 설정 |
| 4 | Master Server IP | Master IPScan Server 의 IP 주소 설정 |
| 5 | Secondary Server IP | <p>IPScan Server 에 문제 발생 시 역할 수행을 대신할 Secondary IPScan Server 의 IP 주소 설정</p> <hr/> <p>Note IPScan Server 를 Master 와 Secondary Server 로 병행하여 사용할 경우 IPScan Probe 는 Master IPScan Server 의 실행 유무를 주기적으로 체크하고, 이상이 발생 시에는 Secondary IPScan Server 로 자동 접속을 시도하여 수집된 데이터의 유실 없이 DB 서버로 데이터 전송을 완료합니다. Probe 는 현재 연결된 Master or Secondary Server 와 연결 상태에 이상이 발생할 시에만 다른 Server 로 통신 체크를 시도합니다. 따라서 현재 연결된 Server 가 Secondary 라고 하더라도 연결 상태에 이상이 발생하지 않는 이상 Master Server 의 연결 상태를 체크하지 않습니다.</p> <p>Master Server 가 정상화 되는 시점에 Secondary Server 는 현재 자신에게 접속되어 있는 모든 Probe 들에게 Master Server 로 접속을 유도하게 됩니다.</p> |
| 6 | Connection Port | IPScan Server 와 Probe 간의 통신 포트를 설정합니다. 기본 설정 값은 30001 번입니다. Probe 에서 값을 변경하면 IPScan Server 의 [서버설정정보]에서도 Port 번호를 변경해야 합니다. |
| 7 | VLAN ID | Probe 가 속한 대역의 VLAN ID 를 설정, VLAN 을 사용하지 않는 경우 또는 Default VLAN 을 사용할 경우 0 을 설정 |

| | | |
|-------------|-------------|--|
| 8 | Master Port | IPScan Server 와 통신할 Ethernet Port 를 설정합니다. **자세한 기능 설명은 다음페이지의 [2.3.1.Master Port 기능 상세설명]을 참조하시기 바랍니다. |
| 9 | Speed | Ethernet 속도를 설정. Auto / 10M-Full / 10M-Half / 100M-Full / 100-Half 중 선택. |
| 0 | Main Menu | Main Menu 로 이동 |
| MAC Address | | Probe 의 MAC 주소 |
| Serial No | | 각 Ethernet Port 의 시리얼 번호. Probe 교체 시 필요합니다. |

2.3.1. Master Port 기능 상세설명

IPScan Probe 600 과 IPScan Server 와의 통신전용 Ethernet Port 를 설정합니다.

6 개의 Ethernet Port 중에서 IPScan Server 와 통신을 전담할 Ethernet Port 를 선택하고, 나머지 Ethernet Port 들은 데이터 수집만을 전담합니다.

Master Port 로 설정된 Ethernet Port 일지라도 데이터 수집 및 IPScan Server 와의 통신을 병행하여 수행할 수 도 있습니다.

a. 단일 Ethernet Port 를 사용할 경우

Ethernet Port 1 을 Master Port 로 정하고, 나머지 5 개의 Ethernet Port 들은 모두 사용정지 중으로 설정합니다. Master Port 는 [0] 또는 [1]을 설정합니다.

| ① Ethernet Port 1 | |
|------------------------|---------------------|
| 1. IP | [192.168.101.20] |
| 2. Netmask | [255.255.255.0] |
| 3. Gateway | [192.168.101.1] |
| 4. Master Server IP | [192.168.103.10] |
| 5. Secondary Server IP | [0.0.0.0] |
| 6. VLAN ID | [0] |
| 7. Master Port | [0] 또는 [1] |
| 8. Speed | [Auto] |
| 0. Main Menu | |
| MAC Address | [00:03:2e-05:02:77] |

[0]: 현재 설정 중에 있는 Ethernet Port 스스로를 Master Port 로 설정한다는 의미입니다.

[1]: Ethernet Port 1 을 Master Port 로 설정한다는 의미이므로 이 경우 둘 중 하나를 선택하여도 같은 설정입니다.

| ② Ethernet Port 2 | |
|------------------------|---------------------|
| 1. IP | [0.0.0.0] |
| 2. Netmask | [0.0.0.0] |
| 3. Gateway | [0.0.0.0] |
| 4. Master Server IP | [0.0.0.0] |
| 5. Secondary Server IP | [0.0.0.0] |
| 6. VLAN ID | [0] |
| 7. Master Port | [-1] |
| 8. Speed | [Auto] |
| 0. Main Menu | |
| MAC Address | [00:03:2e-05:02:78] |

Ethernet Port1 만을 사용하므로 다른 Ethernet Port 들은 다음과 같이 모든 설정 값을 [0]으로 하고, Master Port 값을 [-1]로 설정하면 각각의 Ethernet Port 2/3/4/5/6 들이 현재 사용 중지 중임을 설정하게 됩니다.

b. 다수의 Ethernet Port 를 사용할 경우

Ethernet Port 1 을 Master Port 로 정하고, 나머지 5 개의 Ethernet Port 들은 데이터 수집만을 목적으로 할 경우 다음과 같이 설정합니다. 이 Ethernet Port 들에서 수집된 데이터는 Master Port 로 전달되어 IPScan Server 로 전송됩니다.

| ① Ethernet Port 1 | |
|------------------------|---------------------|
| 1. IP | [192.168.101.20] |
| 2. Netmask | [255.255.255.0] |
| 3. Gateway | [192.168.101.1] |
| 4. Master Server IP | [192.168.103.10] |
| 5. Secondary Server IP | [0.0.0.0] |
| 6. VLAN ID | [0] |
| 7. Master Port | [0] |
| 8. Speed | [Auto] |
| 9. Main Menu | |
| MAC Address | [00:03:2e-05:02:77] |

Master Port 는 [0]을 설정하여 Ethernet Port 1 스스로가 Master Port 임을 설정할 수 있습니다. 또한 Ethernet Port 1 을 의미하는 [1]값을 설정할 수도 있습니다.

| ② Ethernet Port 2 | |
|------------------------|---------------------|
| 1. IP | [0.0.0.0] |
| 2. Netmask | [0.0.0.0] |
| 3. Gateway | [0.0.0.0] |
| 4. Master Server IP | [0.0.0.0] |
| 5. Secondary Server IP | [0.0.0.0] |
| 6. VLAN ID | [0] |
| 7. Master Port | [1] |
| 8. Speed | [Auto] |
| 0. Main Menu | |
| MAC Address | [00:03:2e-05:02:78] |

나머지 Ethernet Port 2/3/...는 다음과 같이 Master Port를 [1]로 설정해 Ethernet Port 1을 Master Port로 설정하고, 데이터 수집의 역할만을 담당합니다.

c. Master Port를 IPScan Server와의 통신전용 포트만 사용할 경우

Ethernet Port1을 Master Port로 설정하고, 데이터 수집은 하지 않고 IPScan Server와의 통신만을 담당하게 할 경우는 다음과 같이 설정합니다.

| ① Ethernet Port 1 | |
|------------------------|---------------------|
| 1. IP | [192.168.101.20] |
| 2. Netmask | [255.255.255.0] |
| 3. Gateway | [192.168.101.1] |
| 4. Master Server IP | [192.168.103.10] |
| 5. Secondary Server IP | [0.0.0.0] |
| 6. VLAN ID | [0] |
| 7. Master Port | [-1] |
| 8. Speed | [Auto] |
| 0. Main Menu | |
| MAC Address | [00:03:2e-05:02:77] |

Master Port 값을 [-1]로 설정하여, 데이터 수집 기능을 하지 않게 합니다. 이 경우 기본 네트워크 설정은 되어 있으므로 서버와의 통신은 가능하게 됩니다.

| ② Ethernet Port 2 | |
|------------------------|---------------------|
| 1. IP | [0.0.0.0] |
| 2. Netmask | [0.0.0.0] |
| 3. Gateway | [0.0.0.0] |
| 4. Master Server IP | [0.0.0.0] |
| 5. Secondary Server IP | [0.0.0.0] |
| 6. VLAN ID | [0] |
| 7. Master Port | [1] |
| 8. Speed | [Auto] |
| 0. Main Menu | |
| MAC Address | [00:03:2e-05:02:78] |

나머지 Ethernet Port 2/3/...의 경우 아래와 같이 Ethernet Port 1을 Master Port [1]로 설정하여 수집된 데이터를 Ethernet Port1으로 전달하도록 설정합니다.

d. 각각의 Ethernet Port 를 Master Port 로 설정할 경우

각각의 Ethernet Port 를 Master Port 로 설정하여 각 포트마다 수집과 통신을 병행하게 하고자 할 경우는 다음과 같이 설정합니다.

| Ethernet Port 1 | |
|------------------------|---------------------|
| 1. IP | [192.168.101.20] |
| 2. Netmask | [255.255.255.0] |
| 3. Gateway | [192.168.101.1] |
| 4. Master Server IP | [192.168.103.10] |
| 5. Secondary Server IP | [0.0.0.0] |
| 6. VLAN ID | [0] |
| 7. Master Port | [0] |
| 8. Speed | [Auto] |
| 0. Main Menu | |
| MAC Address | [00:03:2e-05:02:77] |

각각의 Ethernet Port마다 Master Port 값을 [0]으로 설정하여 데이터 수집 과 통신을 각 포트 별로 실행하게 합니다.

2.4. Return to Default

IPScan Probe 의 모든 설정 값이 초기화됩니다. 한번 초기화되면 기존의 설정 값이 모두 삭제되므로 신중히 고려하시고 실행하시기 바랍니다.

Step1 [Main Menu] -> 3. [Return to Default]을 선택합니다.

Main Menu. Select a number : 3

Step2 초기화 진행 유무를 설정합니다. Initialize the system setting to default? [Y/N] :

2.5. Save

[Main Menu] 중에서 [System]과 [Operating Config]의 설정 내용이 변경된 경우 저장 후 바로 설정 값이 변경됩니다.

Step1 [Main Menu] -> 4. [Save]을 선택하면 변경된 내용이 저장됩니다.

Main Menu. Select a number : 4
Save Config ...

2.6. Save & Apply

[Main Menu] 중에서 [LAN]과 [Take Over]에 대한 설정을 변경했을 경우 사용합니다.

Step1 [Main Menu] -> 5. [Save]을 선택하면 변경된 내용이 저장됨과 동시에 Probe 의 응용프로그램이 재 시작됩니다.

Main Menu. Select a number : 5
Save Config ...
호스트에 대한 연결을 잃었습니다.

실행 후에는 응용프로그램의 재 시작이 완료될 때까지 Probe 와의 연결이 끊기게 됩니다.

Note 위의 [Save] 기능은 시스템 및 IPScan Probe 내의 응용프로그램을 재 시작하지 않고 바로 저장하는 기능인 반면 [Save&Apply]는 실행과 동시에 응용프로그램이 재 시작하므로 IPScan Probe가 재 가동되는 데에 최대 10초간의 시간이 소요될 수 있습니다. 이 시간 동안은 Probe 에서 데이터 수집을 하지 않으므로 수집된 데이터 분석 시 이 시간만큼의 데이터 유실이 있을 수 있습니다.

2.7. System Shutdown

Note IPScan Probe 600은 제품군 안의 다른 Probe들과 달리 사용 중 시스템의 재 부팅이 필요하거나 장비 종료로 해야 할 경우 전원스위치를 바로 내리게 되면 운영 중에 있던 OS가 손상을 입을 가능성이 있습니다. 따라서 반드시 아래의 순서대로 시스템을 종료하여야 합니다.

Step1 [Main Menu] -> 6. [System Shutdown]을 선택하면 Probe 가 종료됩니다.

Main Menu. Select a number : 6
Confirm Shutdown System? [Y/N] Y

2.8. System Status

Step1 [Main Menu] -> 7. [System Status] 선택하면 설정 중인 Probe 의 시스템 설정 상태를 확인할 수 있습니다. 여기에서 보여지는 설정 내용들은 IPScan Probe 에서 직접 설정한 내용과 IPScan Server 와 Console 에서 설정된 내용들이 모두 보여집니다.

| No | 메뉴 | 설명 | |
|---------------------|---|--|--|
| 1 | System Information | Elapsed Time | IPScan Probe가 가동된 시점부터 현재까지 경과된 시간 |
| | | Module 0 ServerIP | IPScan Server IP주소 및 Server와 Probe가 정상적으로 연결되어진 시간부터 현재까지 경과된 시간 |
| | | F/W Version | IPScan Probe 의 응용프로그램 버전정보를 제공 |
| | | System Type | IPScan Probe 의 시스템 타입 |
| | | H/W Type | IPScan Probe 의 하드웨어 타입 |
| 2. | Negotiation INFO | Speed Info | Ethernet에 연결된 포트의 속도 |
| | | Duplex Info | Ethernet 포트의 전이중 또는 반이중 방식의 정보 |
| | | Auto-nego Info | 자동 속도 조절 정보 |
| 3. | Module 0 IP Range | IPScan Probe가 관리하는 IP주소 대역 및 Static 또는 DHCP 환경 정보 표시 IPScan Probe의 IP 주소 (Host IP) 및 VLAN ID 표시. IPScan Probe의 Ethernet Port에 대한 정보 표시 (Port =0) | |
| 4 | System Mode | IPScan Probe가 관리하는 IP 사용자에게 대한 차단 설정 및 보안모드 현황 제공 | |
| | | OOR Block Mode | [범위 외 차단] 기능 설정 시 ON |
| | | IP Secure Mode | [IP 보안] 기능 설정 시 ON |
| | | MAC Secure Mode | [단위 MAC 보안] 기능 설정 시 ON |
| | | G_MAC Secure Mode | [전체 MAC 보안] 기능 설정 시 ON |
| | | Safety Mode | [안전모드] 설정 시 ON |
| | | IP Manage Mode | [사용하지 않는 IP관리] 기능 설정 시 ON |
| | | Port Scan Mode | [서비스스캔] 기능 사용 설정 시 ON |
| | | SNMP Manage Mode | [Switch Port 모니터링] 기능 설정 시 ON |
| | | SNMP AutoBK Mode | [Switch Port 모니터링] 기능에서 [라우터 충돌 포트 차단] 기능 실행 시 ON |
| | | OFDIP Block Mode | [IP주소 기간경과 초과 차단] 기능 설정 시 ON |
| | | OFDMAC Blocok Mode | [기간경과 MAC 자동 차단(Probe)] 기능 설정 시 ON |
| | | OFDMAC Group Mode | [기간경과 MAC 자동 차단(Server)] 기능 설정 시 ON |
| | | *DHCP Active Mode | [DHCP 서버] 기능 사용 시 ON. |
| | | *G_MAC Secu[D] Mode | [DHCP 전체 MAC 보안] 기능 사용 시 ON |
| | | *MAC Secu[D] Mode | [DHCP 단위 MAC 보안] 기능 사용 시 ON |
| | | *IP Assign[D] Mode | [MAC보안모드]에서 '임시IP할당' 설정 시 [TEMP IP] [MAC보안모드]에서 '차단' 설정 시[BLOCK]으로 표시 |
| *Block S_IP[D] Mode | DHCP Pool 영역 내에서 [Static IP 자동 차단] 기능 설정 시 ON | | |

1. Port Scan Mode 는 IPScan Server 의 [서버설정등록]에서 사용유무를 선택하고, Console 에서 [서비스스캔 정책적용]을 실행해야 On 으로 표시됩니다.
2. SNMP Manage Mode 는 IPScan Server 의 [서버설정등록]에서 사용유무를 선택하고, Console 에서 [Switch Port 모니터링 설정]을 실행해야 On 으로 표시됩니다.
3. * Mode 는 IP Scan 서버에서 [DHCP 서버] 설정을 하지 않았을 경우에는 표시되지 않습니다.

2.9. Operating Config

Step1 [Main Menu] -> 8. [Operating Config]를 선택하면 다음과 같이 차단 및 SNMP 관련하여 상세 설정을 할 수 있습니다.

Step2

| Operating Config | |
|------------------|----------------------------|
| 0. | Main Menu |
| 1. | Block Packet Type [Broad] |
| 2. | Socket Time Out [30] |
| 3. | WormSaver Msg Action [Off] |
| 4. | SNMP Query Interval [10] |

Operating config setting. Select a number :

| No | 메뉴 | 설명 | 기본값 |
|----|----------------------|---|-------|
| 1 | Block Packet Type | 관리 대상 범위내의 IP 주소 대역에서 IP 주소 충돌 등의 문제 발생으로 특정 IP 주소를 차단해야 할 경우 Probe 에서 사용하는 차단용 패킷의 종류를 설정합니다. | Broad |
| 2 | Socket Time Out | IPScan Server 와 IPScan Probe 간의 통신 시 응답 대기 시간을 설정합니다. 설정된 시간 동안 IPScan Server 로부터 정상적인 응답을 받지 못할 경우 연결시간 초과로 현재 연결된 세션은 비정상으로 인식하게 됩니다. 1-1440 초까지 설정할 수 있습니다. Note 이때 사용되는 TCP Port 는 30001 번을 사용하고 있으므로 관리자의 네트워크 상에 방화벽과 같은 보안관련 제품이 있다면 IPScan Probe 와 IPScan Server 간의 통신을 위해 반드시 이 Port 를 열어놓도록 설정해야 합니다. 그 밖의 통신 Port 들에 대한 자세한 사항은 '3. 통신포트정보'를 참조하시기 바랍니다. | 30 초 |
| 3 | WormSaver Msg Action | 관리자의 네트워크에 WormSaver Agent 를 설치하여 사용하고 있는 경우 IPScan Probe 에서 호스트를 차단하는 시점에 차단 사유에 대한 메시지를 WormSaver Agent 에게 보낼 것인지 여부를 설정합니다. WormSaver Agent 제품이 설치되어 있지 않거나 차단기능을 수행하지 않을 경우 Off 로 설정합니다. | Off |
| 4 | SNMP Query Interval | IPScan 에서 제공하는 Switch Port 관리기능을 사용하고 있을 경우, IPScan Probe 에서 Switch 로 정보 수집을 위해 주기적으로 보내는 SNMP Query 의 주기를 설정합니다. 1-1440 분까지 설정할 수 있습니다. | 10 분 |

2.10. Take Over

IPScan Probe의 이중화 기능을 설정합니다. 동일 네트워크에 두 대의 Probe를 운영하는 기능으로, Master Probe가 운영 중 장비에 문제가 발생하거나 장애가 생기면 자동으로 Slave Probe가 동작을 시작하고, Master Probe가 복구 완료되어 정상 동작하게 되면 Slave Probe는 다시 대기상태로 돌아갑니다. 이때 관리자의 물리적인 작업 없이 Slave Probe는 자동 실행됩니다. Take Over는 같은 기종으로 설정 가능합니다.

Step1 [Main Menu] -> 9. [Take Over]를 선택합니다.

Main Menu. Select a number : 9

Step2 1. Active Mode 를 선택하고, 설정 중에 있는 Probe 를 Master 로 지정할 것인지, Slave 로 지정할 것인지를 선택합니다. Take Over 를 실행하지 않으려면 [None]으로 설정합니다.

> ACTIVE MODE : None[0] / Master[1] / Slave[2]

Step3 Master Agent IP 설정

설정 중에 있는 IPScan Probe 를 Slave 로 설정할 경우 Master 로 설정되어 있는 IPScan Probe 의 IP 주소를 설정합니다.

```
> Select a Number : 1
> ACTIVE MODE : None[0] / Master[1] / Slave[2]
> Input Take-Over Active Mode : 2
  1. Active Mode      [Slave]
  2. Master Agent IP  [192.132.111.3]
  3. Checking Interval [10]
  4. Waiting Time     [60]
  5. Virtual Serial   [00000000000000000000]
  6. Probe Login Allow [NO :Read Only]
  0. Main Menu
```

Slave Agent IP 설정

설정 중에 있는 IPScan Probe 를 Master 로 설정할 경우 Slave 로 설정되어 있는 IPScan Probe 의 IP 주소가 표시됩니다. 단, 초기 설정 시에는 표시되지 않으며, 실제 Take Over 가 실행되면 Slave Probe 가 Login 되면서 IP 주소가 표시됩니다. 관리자가 별도 설정을 하지 않습니다.

```
> Select a Number : 1
> ACTIVE MODE : None[0] / Master[1] / Slave[2]
> Input Take-Over Active Mode : 1
  1. Active Mode      [Master]
  2. Slave Agent IP   [0.0.0.0 :Read Only]
  3. Checking Interval [10]
  4. Waiting Time     [60]
  5. Virtual Serial   [00000000000000000000]
  6. Probe Login Allow [NO :Read Only]
  0. Main Menu
```

Step4 Checking Interval 설정

4. Checking Interval을 선택합니다. 0-1440초까지 설정 가능하고, 기본값은 10초로 설정되어 있습니다.

> Select a Number : 3

> Input Take-Over Checking Interval (5 ~ 1440 sec) : 10

Slave IPScan Probe 가 Master IPScan Probe 에 대한 장애 여부를 확인하는 주기를 설정합니다.

Step5 Waiting Time 설정

4. Waiting Time을 선택합니다. 0-1440초까지 설정 가능하고, 기본값은 60초로 설정되어 있습니다.

> Select a Number : 4

> Input Take-Over Waiting Time (10 ~ 1440 sec) : 60

위의 [Checking Interval] 과 [Waiting Time]은 유기적인 관계를 가지고 있어 [Checking Interval]에서 설정된 주기를 반복하여 Master IPScan Probe를 체크 하게 되는데, 이때 [Waiting Time]에서 설정해 놓은 설정 주기를 초과하여도 Master IPScan Probe에서 응답이 없으면 Slave IPScan Probe로 Take Over 됩니다.

설정 값은 $\text{Checking Interval} < \text{Waiting Time}$ 의 조건이 성립되도록 설정하여야 하고, 권장 설정은 $[\text{Waiting Time} = \text{Checking Interval} * 3 \text{ (3 배)}]$ 이상이 되도록 설정하는 것이 좋습니다. 즉 3 번의 Checking Interval 주기를 실행한 후 응답이 없을 경우 Take Over 를 실행하게 됩니다.

Step6 Virtual Serial 설정

5. Virtual Serial 을 선택합니다. '0'을 입력하면 IPScan Server 연결 시 사용되는 시리얼 번호를 출력합니다. Slave Probe 는 Master Probe 의 시리얼 번호를 공유하여 IPScan Server 와 통신합니다.

Input Take Over Virtual Serial : 0

1. Active Mode [Master]
2. Slave Agent IP [0.0.0.0 :Read Only]
3. Checking Interval [10]
4. Waiting Time [60]
5. Virtual Serial [VSxxxxxxxxxxxxxxxxxxxx]
6. Probe Login Allow [NO :Read Only]
0. Main Menu

Step7 Probe Login Allow 설정

Master / Slave Probe의 Take Over 상태를 표시합니다. Master / Slave Probe 중 하나만이 Probe Login Allow 의 상태 값을 Yes로 유지할 수 있으며, 이 상태 값이 Yes인 Probe가 IPScan Server로 접속을 시도합니다. 다른 하나는 Take Over 대기 상태로 들어가게 됩니다.

이것은 관리자가 설정할 수 있는 설정 값이 아니며, Master / Slave IPScan Probe가 서로 Sync/Ack 를 주고 받으며 유지하는 상태 값입니다.

이 설정 값은 일시적(최대 Checking Interval 동안)으로 둘 다 Yes or No 인 상태를 가질 수 있으나 서로 Sync / Ack 를 주고 받으며 재설정 됩니다.

2.11. Ping Test

IPScan Probe 가 네트워크에 정상적으로 설치가 되었는지 확인할 수 있습니다.

Step1 [Main Menu] -> 10. [Ping Test]를 선택합니다.

```
Main Menu. Select a number : 10
```

```
-----  
Enter the target IP address. : 192.168.101.1  
192.168.101.1 is alive. icmp_seq=0  
192.168.101.1 is alive. icmp_seq=1  
192.168.101.1 is alive. icmp_seq=2  
192.168.101.1 is alive. icmp_seq=3  
192.168.101.1 is alive. icmp_seq=4> packet loss.  
-----
```



IP/MAC resource Management and network security solution
www.scope.co.kr

3. 부록

이 장에서는 IPScan 이 사용하는 통신 포트들에 대한 설명과 장비 설치에 대한 네트워크 구성 예가 제공됩니다. 또한 장애관련 Q&A 에서 장애 발생 시 응급 대처방법을 소개합니다.

| | |
|---------------|----|
| 3.1. 통신포트정보 | 28 |
| 3.2. 네트워크 구성도 | 29 |
| 3.3. Q&A | 31 |

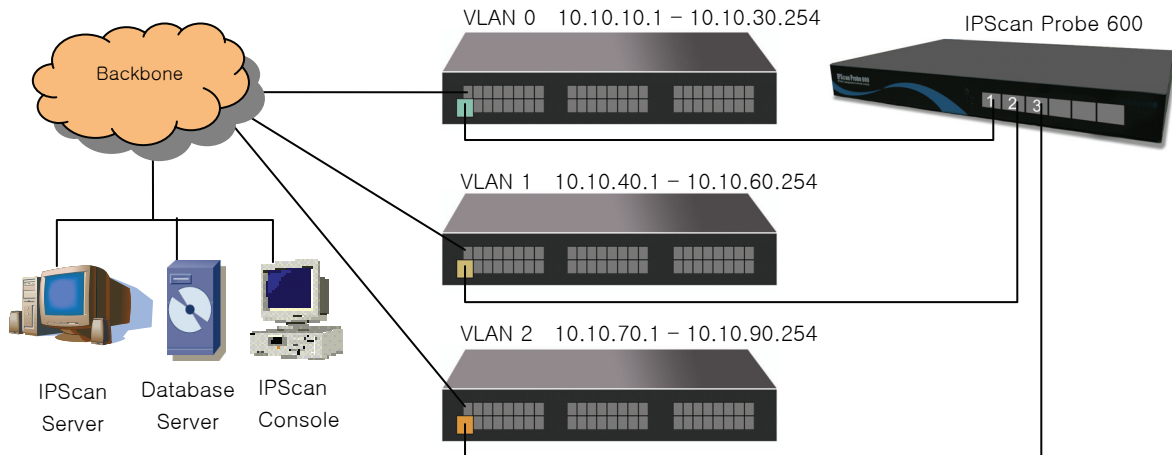
3.1. 통신 포트 정보

IPScan 은 상호간의 통신을 유지하기 위해 아래와 같이 고유 통신 Port 를 사용하고 있습니다. 따라서 관리자의 네트워크에 보안관련 제품이 있을 경우 또는 기타 네트워크 제품들과의 통신포트 중복으로 인한 장애를 막기 위해 반드시 확인하시고 설치하시기 바랍니다.

| Port No | Protocol | 설명 |
|---------|----------|---|
| 6812 | TCP | IPScan Probe 의 펌웨어(응용프로그램) 업데이트 시 사용 |
| 30000 | TCP | IPScan Console 이 IPScan Server 로 접속 시 사용 |
| 30001 | TCP | IPScan Probe 가 IPScan Server 로 접속 시 사용 |
| 30002 | TCP | IPScan Server 내부 통신에 사용 (Control Port) |
| 30003 | TCP | IPScan Server 내부 통신에 사용 (Data Port) |
| 30004 | TCP | IPScan Console 이 IPScan Server 로 접속 시 사용 (Control Port) |
| 30005 | TCP | IPScan Console이 IPScan Server로 접속 시 사용 (Event Port) |
| 22 | TCP | IPScan Probe 500A 장비로 SSH 접속 시 사용 |
| 23 | TCP | IPScan Probe 장비로 telnet 접속 시 사용 |
| 25 | TCP | IPScan Server 가 메일 서버로 SMTP 접속 시 사용 |
| 67 | TCP | DHCP Server Bootstrap 통신 |
| 68 | TCP | DHCP Client Bootstrap 통신 |
| 137 | UDP | Probe 가 NetBIOS Query |
| 1433 | TCP | IPScan Console 및 Server 가 MSSQL 접속 |
| 1525 | TCP | IPScan Console 및 Server 가 Oracle 접속 |
| 3306 | TCP | IPScan Console 및 Server 가 MySQL 접속 |

3.2. 네트워크 구성도

a. 각 세그먼트 별로 설치하고 Ethernet Port1 을 Master Port 로 설정할 경우



Note 다음과 같이 설정할 경우 IPScan Console 에서는 각각의 Ethernet Port 가 1 대의 Probe 로 보여지고, Ethernet Port1 은 서버와의 통신을 전담하는 Master Port 로 설정됩니다.

IPScan Console 에서 Probe 의 관리 대역 설정 예

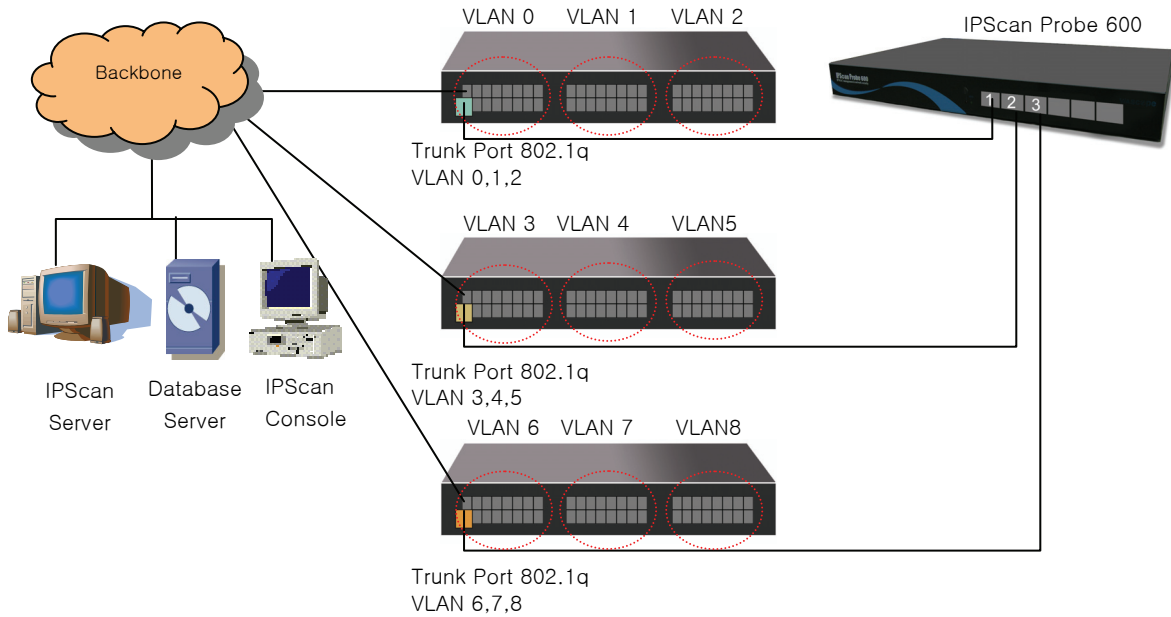
| Host IP | VLAN ID | DHCP use | Port | Start | End |
|--------------|---------|----------|------|------------|--------------|
| 10.10.10.254 | 0 | NO | 1 | 10.10.10.1 | 10.10.30.254 |
| 10.10.40.254 | 0 | NO | 2 | 10.10.40.1 | 10.10.60.254 |
| 10.10.70.254 | 0 | NO | 3 | 10.10.70.1 | 10.10.90.254 |

Note VLAN 0,1,2 가 Default VLAN 으로 설정되어 있으며 위와 같이 VLAN ID 를 0 으로 설정하지만, Default VLAN 으로 설정되어 있지 않을 경우에는 해당 VLAN ID 를 입력해야 합니다.

IPScan Probe 에서 [LAN] 설정 예

| Ethernet Port | IP | Subnet | Gateway | Master Server IP | VLAN ID | Master Port |
|-----------------|--------------|---------------|------------|------------------|---------|-------------|
| Ethernet Port 1 | 10.10.10.254 | 255.255.255.0 | 10.10.10.1 | 100.100.100.2 | 0 | 1 |
| Ethernet Port 2 | 0.0.0.0 | 0.0.0.0 | 0.0.0.0 | 0.0.0.0 | 0 | 1 |
| Ethernet Port 3 | 0.0.0.0 | 0.0.0.0 | 0.0.0.0 | 0.0.0.0 | 0 | 1 |

b. 다수의 VLAN 의 네트워크에서 Trunk Port 에 연결 할 경우



Note 다음과 같이 설정할 경우 IPScan Console 에서는 각각의 Ethernet Port 가 Probe 로 설정 (3 대의 Probe 로 나타남) 되어 보여집니다.

IPScan Console 에서 Probe 의 관리 대역 설정 예

| Host IP | VLAN ID | DHCP use | Port | Start | End |
|--------------|---------|----------|------|------------|--------------|
| 10.10.10.254 | 0 | NO | 1 | 10.10.10.1 | 10.10.10.254 |
| 10.10.20.254 | 1 | NO | 1 | 10.10.20.1 | 10.10.20.254 |
| 10.10.30.254 | 2 | NO | 1 | 10.10.30.1 | 10.10.30.254 |
| | | | | | |
| 10.10.40.254 | 0 | NO | 2 | 10.10.40.1 | 10.10.40.254 |
| 10.10.50.254 | 4 | NO | 2 | 10.10.50.1 | 10.10.50.254 |
| 10.10.60.254 | 5 | NO | 2 | 10.10.60.1 | 10.10.60.254 |
| | | | | | |
| 10.10.70.254 | 0 | NO | 3 | 10.10.70.1 | 10.10.70.254 |
| 10.10.80.254 | 7 | NO | 3 | 10.10.80.1 | 10.10.80.254 |
| 10.10.90.254 | 8 | NO | 3 | 10.10.90.1 | 10.10.90.254 |

Note VLAN 0,3,6 이 Default VLAN 으로 설정되어 있으며 위와 같이 VLAN ID 를 0 으로 설정하지만, Default VLAN 으로 설정되어 있지 않을 경우에는 해당 VLAN ID 를 입력해야 함.

IPScan Probe 에서 [LAN] 설정 예

| Ethernet Port | IP | Subnet | Gateway | Master Server IP | VLAN ID | Master Port |
|-----------------|--------------|---------------|------------|------------------|---------|-------------|
| Ethernet Port 1 | 10.10.10.254 | 255.255.255.0 | 10.10.10.1 | 100.100.100.2 | 0 | 0 |
| Ethernet Port 2 | 10.10.40.254 | 255.255.255.0 | 10.10.40.1 | 100.100.100.2 | 0 | 0 |
| Ethernet Port 3 | 10.10.70.254 | 255.255.255.0 | 10.10.70.1 | 100.100.100.2 | 0 | 0 |

3.3. Q&A

IPScan Probe의 운영 중 장애가 발생할 경우 아래의 Q&A를 참조하시기 바랍니다.

Q) [IP 고정차단] 기능을 적용한 경우에 IPScan이 예상치 못한 차단을 하고 있습니다

A) 다음의 방법대로 설정내용을 확인하고 조치를 취합니다.

- ① 우선 IPScan Probe와 Server와의 통신을 차단하기 위해 해당 IPScan Probe에 [Telnet]으로 접속하여 2번 [LAN] 메뉴에서 [서버 IP]를 다른 임의의 IP주소로 변경하고 [Save & Apply]를 실행하거나, IPScan Server에서 [안전모드]를 실행하여 모든 설정 내용에 대한 실제 적용을 차단할 수 있습니다.
- ② IPScan Console에서 차단된 IP/MAC에 대한 [이벤트 로그]에서 구체적으로 어떤 차단이 되었는지 확인합니다.
- ③ [다중 IP](MLT)로 표시되는 IP주소에 [IP 고정(다중 IP 고정)차단]이 설정되어 있는지 확인합니다. 다중 IP의 경우 모든 사용하는 IP를 다중으로 IP고정하지 않으면 차단됩니다. 따라서, 서버나 네트워크 장비에는 [IP 고정차단] 기능을 설정하지 말 것을 권장하고 있습니다. 기존에 설정되어 있는 것은 해제해 주시기 바랍니다.
- ④ 위의 방법으로 해결되지 않는 상태일 경우, 정확한 원인 규명과 제발 방지를 위해 이전에 발생한 실시간 이벤트를 검색해 주십시오. 특별한 이벤트를 발견하지 못한 경우에는 리포트 뷰어에서 [차단/이벤트 로그]에 있는 모든 이벤트 항목을 선택하신 후 해당 날짜와 해당 IPScan Probe를 선택하시고 검색을 실행하여 나온 결과를 파일로 저장하여 techsup@scope.co.kr로 보내주시기 바랍니다.

Q) IPScan이 차단 기능을 수행하지 못하고 있습니다.

A) 다음의 경우들에 따라 설정된 내용들을 확인합니다.

- ① IPScan Console에서 해당 Probe가 [안전 모드]로 설정되어 있는지 확인합니다.
[안전모드]로 설정되어 있을 경우에는 모든 설정내용이 실제 네트워크상에 실행되지 않고, IPScan Server상에서만 시뮬레이션 되고 있는 상황이므로, [안전모드]해제를 하셔야 합니다.
- ② MAC 주소에 대한 차단에 이상이 생겼을 경우는 Router나 Switch들의 특성에 따라 MAC Table 수정이 늦어지는 경우에 이미 Probe에서 차단한 MAC 임에도 불구하고, 아직도 살아있는 MAC으로 간주하여 통신이 이루어 지는 경우가 발생할 수 있습니다. 이러한 경우에는 예 Gateway 장비를 [MAC 주요 장비]로 설정하여 Probe에서 설정된 Gateway로 차단정보를 즉시 알려줌으로써 MAC 차단 기능을 원활하게 수행할 수 있습니다.
- ③ IPScan Console에서 현재 사용 중인 IP가 온라인과 오프라인을 반복적으로 오가는지 확인해 주시기 바랍니다. 이런 경우는, IPScan Server와 Probe가 연결/해제가 반복되는 경우입니다. 이와 같은 경우에는 네트워크 연결 상태에 문제가 있는지 확인하셔야 합니다.

Q) IPScan Server와 연결이 되지 않습니다.

A) 다음의 방법들로 확인할 수 있습니다.

- ① IPScan Server에서 Probe로 ping 및 telnet 을 시도하여 연결 상태를 점검합니다.
만일, Ping 결과가 100ms 이상의 속도로 나오고, 같은 대역의 다른 IP에 대한 ping에 대해서는 정상 수준인 10ms 이하로 나올 경우에는 IPScan Probe 장비의 노후로 인한 문제로 판단될 수 있습니다.
- ② Telnet이나 콘솔로 Probe에 접속해서 [Main Menu]에서 2. [LAN]을 실행하여 IPScan Server 의 IP 주소가 맞게 설정되어 있는지 확인합니다.
- ③ IPScan Server PC에 보안프로그램이 실행되어 있다면 보안 등급을 낮추거나, 허용포트에 3000 번부터 30005번까지 설정한 후 재 연결을 시도합니다
- ④ 네트워크상에 방화벽이 설치되어 있을 경우도 위와 같이 Server와 Probe간에 사용되는 통신포트들을 등록한 후 재 연결을 시도합니다.

이 장에서 소개된 장애상황 이외의 장애가 발생했을 경우 해당 대리점 또는 본사 기술지원 팀 (techsup@scope.co.kr, Tel: 02-3412-9700)으로 문의하시면 신속하게 서비스 받으실 수 있습니다.