

TI 310

이더넷 네트워킹 (한국어)

일반 정보

TI 310 Ethernet networking

Version 1.1 EN, 12/2014, D5310.EN .01

Copyright © 2014 by d&b audiotechnik GmbH; all rights reserved.

d&b audiotechnik GmbH

Eugen-Adolff-Strasse 134, D-71522 Backnang, Germany

Telephone: +49-7191-9669-0, Fax: +49-7191-95 00 00

E-mail: support@dbaudio.com, Internet: www.dbaudio.com

목 차

1.개 요.....	4
2.네트워크 토폴로지	4
2.1. 네트워크 스위치와 네트워크 허브	5
3.식별 및 통신	5
3.1. MAC 주소	5
3.2. IP 주소	5
3.2.1. IP 서브넷 마스크.....	5
3.2.2. 사설 네트워크.....	6
3.2.3. 자동 vs 수동 IP주소 할당	6
3.2.4. 혼합식 IP주소 할당 방식.....	6
3.3. TCP와 UDP를 통한 데이터 전송.....	7
3.3.1. 포트.....	7
3.4. 방화벽 및 보안 체제.....	7
3.4.1. 수동구성의 환경설정 지침.....	8
4.무선랜 ("Wi-Fi").....	8
4.1. 기준 규격.....	8
4.2. 채널과 주파수.....	8
4.3. 무료 무선랜 채널 찾기	8
4.4. 가시선과 프레넬 영역	8
4.5. 무선의 활용성	8
5.퀵 스타트 가이드.....	9
6.네트워크 하드웨어와 케이블 연결하기.....	10
7.기타 정보	10
8.네트워크 토폴로지 예시.....	10

1. 개 요

현대 사회에서 이더넷 기반의 네트워크는 데이터 제어뿐만 아니라 콘텐츠 전송에 있어서 가장 효율적인 방법 중 하나로 자리잡고 있습니다.

몇가지 수학적이고 관용적인 내용들은 대학교 심화과정 수준의 지식을 필요로 하기에 이번 튜토리얼에서는 그러한 내용은 포함하지 않았습니다.

네트워킹에 관한 직무나 규모면에서는 국내외 월드투어 프로덕션과 같은 대형 규모는 아니므로 아래에 해당하는 이슈를 비교적 쉽게 다룰 수 있습니다.

- 네트워크 구조 형성 방법
- MAC, IP 주소 및 IP 서브넷 마스크
- 컴퓨터 네트워크 아답터 셋업 방법
- 무선랜 작동 방식
- 네트워크 보안

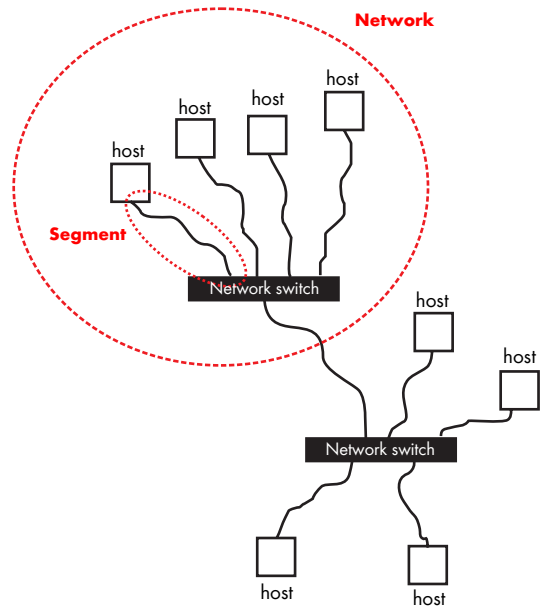
이번 문서는 네트워크와 관련한 높은 수준의 전문적인 내용은 다루지 않으며 초심자에게 정확한 정보를 제공하고자 하는 취지로 구성되어 졌습니다.

2. 네트워크 토폴로지

대체적으로 이더넷 기반의 네트워크는 두 개 이상의 '호스트' (네트워크 연결이 가능한 장치들의 기술적 용어)들이 별 모양의 구조를 형성합니다. 이 말은 각각의 호스트들이 중심부 스위치 또는 허브를 통하여 상호 연결이 되어 있는 상태를 의미합니다. 스위치와 허브들은 각각 연결되어 더욱 큰 규모의 네트워크 구조를 형성합니다. 두 호스트 간 연결되어있는 상태를 '세그먼트 (segment)' 라 부릅니다.

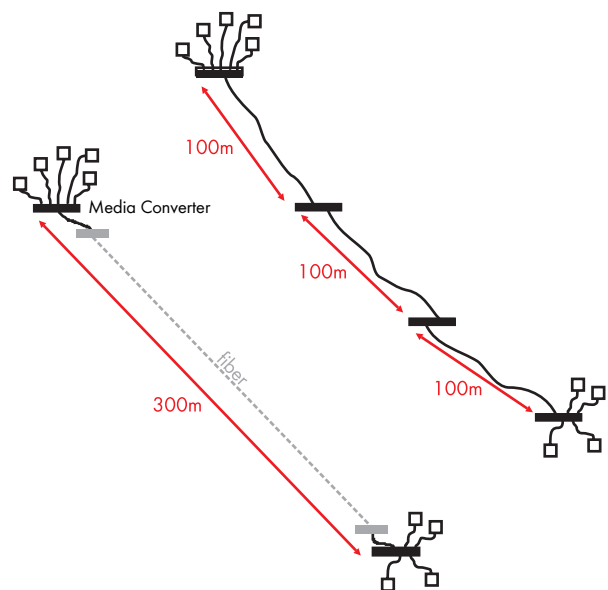
데이터 체인을 지원하는 장비들은 'IN'과 'OUT'의 단자들을 가지고 있으며 이러한 장비들은 원래 세 종류의 스위치 단자를 가지고 있습니다. 두 단자는 장비 외부에서 확인이 가능하지만 실제로 장비들이 연결되는 곳은 장비 내부에 존재하는 세번째 단자라 할 수 있습니다.

각각의 장비들이 이러한 특징들을 지원하면서 동시에 기기간의 연결이 정확한 상태라면, 어떠한 경우에서라도 네트워크상의 접속은 이루어지게 됩니다. 반면에 몇몇의 스위치를 분배기처럼 활용하여 물리적으로 네트워크를 더욱 세분화 할 수도 있습니다. 앞으로의 내용들은 상호간 연결된 '별 네트워크(Star network)'를 예시로 다룰 것입니다.



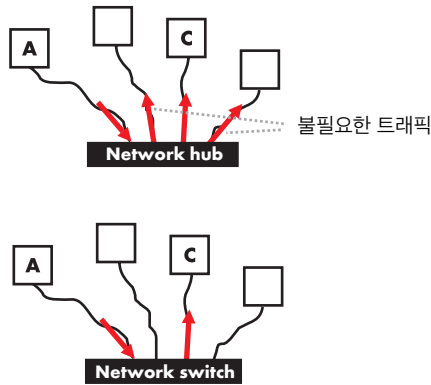
구리 재질 기반의 세그먼트는 최대 길이가 100m로 제한되며 제한 길이는 사용되는 케이블의 종류에 따라 다릅니다. 전송 제한 길이를 확장하기 위해 추가적인 스위치 또는 허브가 중간 과정에 들어가게 되고 이 경우 이러한 경우 세그먼트의 길이를 100m 더 확장 할 수 있습니다. 네트워크의 세그먼트의 최대 길이를 확장하는 또 다른 방법으로는 미디어 컨버터를 사용하거나 광섬유 케이블을 사용하는 방법이 있습니다. 이러한 방식은 전송 가능한 최대 길이를 10km까지 연장할 수 있습니다.

아래의 사례는 네트워크 세그먼트의 전송의 최대 길이를 확장시킬 수 있는 두 가지 방법에 대해 보여주고 있습니다. 연결되어야 하는 거리는 300m이며 구리 재질 기반의 전송 방식은 이러한 거리를 충족시키기 위해 두 개의 스위치 또는 허브가 필요합니다. 이러한 방식의 문제로는 스위치 또는 허브마다 전원을 공급해줘야 한다는 점과 각 스위치 또는 허브가 신호 전송 오류의 근원점이 될 수 있다는 점이 있습니다. 반면에 미디어 컨버터를 사용하거나 광섬유 케이블을 이용할 경우 별도의 장비 없이 원거리 연결이 가능합니다.



2.1. 네트워크 스위치와 네트워크 허브

스위치는 간단한 네트워크를 형성하는데 가장 자주 쓰여지는 장비입니다. 때로는 허브가 사용되기도 하지만 스위치와 허브의 핵심적인 차이는 허브는 전자적인 중계기의 역할만을 한다는 것입니다. 허브는 하나의 포트에 도달된 모든 데이터들을 또 다른 포트에 전송합니다. 이 때 과도한 네트워크 부하가 발생하고 네트워크의 효율을 떨어트리는 수많은 문제들이 야기 됩니다.



허브 vs 스위치: 호스트 'A'는 호스트 'C'와 커뮤니케이션을 한다.

반면에, 스위치의 경우 포트에 연결된 호스트 (MAC address과 같은) 에만 데이터를 전송합니다.

3. 식별 및 통신

이더넷 네트워크는 각기 다른 제조사로부터 수많은 타입의 호스트들을 포함하고 있습니다. 그렇기 때문에 상호 기기간의 신호 전송 및 기기의 식별을 위해 공통적인 규칙이 필요합니다. 가장 주된 내용들은 다음과 같습니다.

3.1 MAC 주소

특정 컴퓨터 브랜드와는 아무런 관련이 없으며, 주소가 직접적으로 등록되어야 하는 네트워크 호스트에 독립적인 식별을 위해 제공하는 주소입니다.

MAC은 '**M**edia **A**ccess **C**ontrol'의 약자이며 모든 네트워크 호스트 장비들 (예를 들어 d&b R70 (Ethernet 에서 CAN 변환 인터페이스), 컴퓨터의 네트워크아답터, 무선공유기 등) 에 적용되고 있습니다. 그리고 이러한 MAC 주소는 독자적이며 이론적으로 변하지 않는 특성을 가지고 있습니다.

이더넷 네트워크에서 MAC 주소는 48 bits 또는 6bytes의 대역폭을 가지며 아래의 예와 같이 16진수로 표기됩니다.

(00:41:80:AD:FC:2C)

일반적으로 네트워크 사용자들은 이러한 MAC 주소를 자주 접하지는 않습니다.

3.2 IP 주소

독자적인 장비 식별 기능으로서의 MAC 주소와는 달리 네트워크 호스트들은 논리적인 네트워크를 형성하기 위해 함께 그룹화 되어야 합니다. 이를 위해 MAC 주소 (호스트와 같은) 는 개별적인 IP주소를 할당 받습니다. MAC 주소와는 대조적으로 IP주소는 특정 장비에만 독점적이지 않으며 필요한 만큼 사용 횟수에 따라 할당받을 수 있습니다.

현재 주된 규격으로 자리잡고 있는 IPv4 방식은 IP주소들이 32비트의 주소 대역을 가지고 있으며 4자리의 십진수 표기방식에 의해 0부터 255의 숫자로 표기될 수 있습니다. 예를 들면,

(137.152.89.230)

이러한 형태로 나타나게 되고 대부분 사용자가 직접 관리해야 합니다.

3.2.1. IP 서브넷 마스크

더욱 세분화하기 위해 IP 주소는 네트워크 프리픽스(Prefix) 및 호스트 번호로 세분화되며 서브넷과 실제 ID가 구분되어진 dbCAN 네트워크와 유사합니다. 예를 들면 CAN ID '5.23'은 서브넷 마스크인 '5'와 ID인 '23'으로 나뉘질 수 있습니다.

하지만 IP 주소의 경우 네트워크 프리픽스 또는 호스트를 식별하기 위한 고정된 숫자를 지니고 있지 않습니다. 대신에 IP주소가 가지고 있는 네트워크 프리픽스는 서브넷 마스크에 의해 정해집니다. 이는 다소 복잡하게 보일 수 있으나 아래의 예를 보면 이해하기 쉬울 것입니다. 이 예시에서 서브넷 마스크 주소의 표기 방식과 IP주소의 표기 방식이 매우 유사하다는 것을 알 수 있습니다.

(255.255.255.0)

처음 세 마디는 '네트워크 프리픽스'를 의미하며 마지막 마디는 '호스트 번호'를 의미합니다. 네트워크 내부의 모든 호스트들이 같은 네트워크 번호를 사용한다면 별다른 설정 없이 상호간의 소통이 가능합니다. 위에서 보았던 서브넷 마스크와 같이 IP 주소 또한 192.168.0.[x]의 형태를 가집니다. [x]는 호스트 번호이며 '192.168.0'은 독립적인 네트워크 프리픽스의 의미로 쓰입니다. 이 때 모든 호스트들은 서브넷 마스크를 '255.255.255.0' 으로 설정해야 합니다.

이러한 과정은 256개 (0부터 255까지)의 각기 다른 호스트 장비들이 서로 접속할 수 있도록 합니다. 사실상 가장 낮은 호스트 넘버인 0과 가장 높은 호스트 넘버인 255는 사용하지 않습니다. 그러므로 사용 가능한 호스트의 수는 254개로 감소하게 되고 이것은 컴퓨터 또는 네트워크 사용이 가능한 장비들이 최대 254개까지 접속 가능하다는 것입니다.

3.2.2. 사설 네트워크

IP주소 사용시 모든 대역 전체를 자유롭게 사용할 수는 없습니다. 대다수의 IP주소들은 인터넷 할당 번호 관리 기관 (Internet Assigned Number Authority(IANA)) 에서 중점적으로 관리하고 있습니다. 하지만 일부 IP주소 범위는 인터넷 접속과 관계없이 네트워크를 비공개로 사용하거나 사적 용도로 사용하기 위해 따로 분류되어 있으며 원한다면 사용이 가능합니다. 가장 자주 사용되는 두 가지 주소의 범위는 아래와 같습니다.

10.0.0.0 - 10.255.255.254

또는

192.168.0.0 - 192.168.255.254

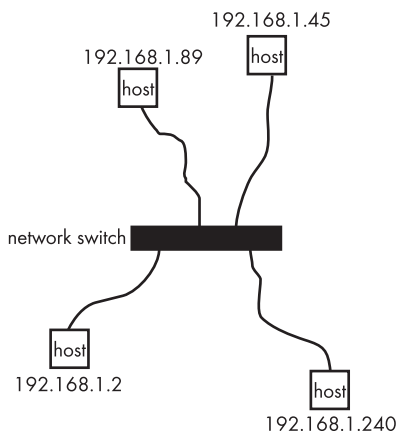
만일 IP 주소 값을 수동으로 지정한다면 위의 주소 범위 내에서 지정해야 합니다. 255.255.255.0의 서브넷 마스크 주소와 함께 네트워크 내부 IP주소 값은 다음과 같은 형태를 지닙니다.

10.[x].[y].[z]

또는

192.168.[x].[z]

[x]와 [y]는 0과 255 사이의 숫자로 설정되어야 하며 이 숫자들은 각 호스트 별로 동일한 값을 가져야 합니다. [z]는 호스트의 숫자를 의미하며 1과 254 사이의 숫자로 설정되어야 합니다. 이 숫자는 각 호스트마다 독립적인 값을 가지고 있어야 하며 다음 예시는 이러한 방법이 적용되어 설정된 네트워크의 한 예를 보여주고 있습니다.



서브넷 마스크 : 255.255.255.0 네트워크 프리픽스 : 92.168.1.0

3.2.3. 자동 vs. 수동 IP 주소 할당

신속한 네트워크 구성을 위해 서브넷 마스크나 IP 주소 등의 파라미터들은 네트워크 내부에서 자동으로 지정되기도 합니다. 이러한 방법을 DHCP (Dynamic Host Configuration Protocol)이라 부르며 이 방법은 DHCP 서버를 필요로 합니다. 전부는 아니지만 대부분의 와이파이 (WiFi) 라우터들은 내장된 DHCP서버 기능을 제공하고 있습니다.

주의: 각각의 네트워크는 하나 이상의 DHCP를 포함할 수 없으며 이를 무시할 경우 상호간 통신 혼란 또는 신호의 손실이 일어날 수 있습니다. 네트워크에 두 번째 DHCP 서버를 잘못하여 추가할 경우 몇 시간 또는 며칠 후 동일한 문제가 발생할 수 있습니다. 서로 인터넷 연결을 공유하고 있는 컴퓨터나 모든 장비들은 일제히 DHCP 서버이기에 주의를 기울여야 한다는 사실을 명심해야 합니다.

올바르게 사용되어진 경우라 하여도 DHCP에는 문제점이 있을 수 있습니다. 간혹 호스트들과 DHCP서버와의 특정 결합 과정에서 각각의 규격으로 인해 발생하는 미세한 차이로 때문에 신호 전송에 실패하는 경우가 있습니다. 이러한 경우 자동 IP주소 할당 기능은 작동하지 않습니다. DHCP서버가 네트워크상에 존재한다면 IP주소를 수동으로 할당한 경우라 할지라도 비슷한 문제들이 일어날 수 있습니다. 중복 IP주소는 혼란을 야기할 뿐만 아니라 DHCP를 통해 자동으로 IP주소를 할당 받도록 설정된 호스트들이 실제로 알지 못하는 수동 IP주소로 설정되어 지도록 하며 이 때 네트워크 프리픽스가 서로 달라질 수도 있습니다.

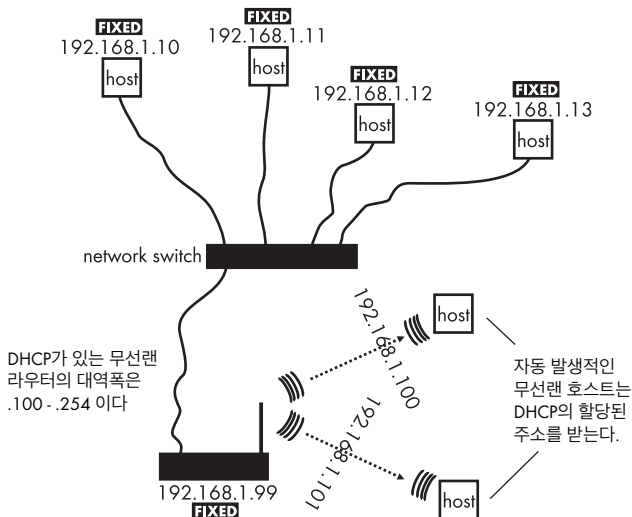
이러한 이유로 호스트를 자동 IP 주소 검색으로 재설정하는 방법을 이해하는 것이 좋습니다. IP주소가 고정값으로 설정되면 각각의 장비에 주소를 명기하여 표기하는 방법을 권장합니다. 수많은 모바일 네트워크 IP 주소들이 수동으로 분배되고 페그 (pegs)에 기입되기 시작하는 것을 '페그 DHCP'라고 합니다. 페그는 각 장비에 연결된 케이블에 접속되어 어떤 숫자의 IP가 어디에 사용되고 있는지 명확히 보여줍니다.

3.2.4. 혼합식 IP 주소 할당 방식

같은 호스트들로 구성된 일반적인 네트워크들에서 가장 효율적인 접근 방법은 고정 IP주소 방식과 자동 IP주소 방식을 혼합하여 사용하는 것입니다. 많은 DHCP 서버들은 특정 범위내에서 IP주소들을 분배할 수 있는데 (192.168.1.100~192.168.1.254)의 특정범위를 설정할 수 있고 일반적인 호스트들은 고정 IP주소 방식으로 192.168.1.1부터 192.168.1.99까지 주소를 설정할 수 있습니다.

주소들은 이러한 방법으로 생성되며 DHCP로 설정된 주소들이 연결된 호스트들로부터 발생된 중복 주소들을 자연스럽게 피하도록 합니다.

다음의 예시는 전형적인 시나리오를 보여주고 있습니다. 고정된 호스트들은 수동으로 설정된 고정 IP 주소들을 가지고 있습니다. 이 예시에서 무선랜 라우터 기능을 하고 있는 DHCP 서버는 사용 가능한 특정 IP주소 대역을 지니고 있고 그로 인해 수동으로 지정된 IP주소들과는 충돌이 일어나지 않습니다. DHCP 서버 자체 또한 IP주소(수동으로 설정되며 고정값으로)를 가지고 네트워크에 접속되고 있습니다. 아래 예시는 태블릿이나 모바일 랩탑등의 유동적인 두 호스트가 무선랜 라우터의 DHCP 서버로부터 자동으로 IP주소를 지정받는 형태를 보여주고 있습니다

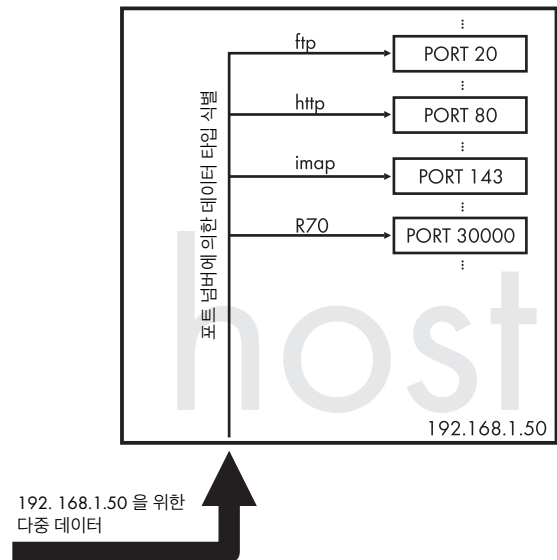


3.3. TCP와 UDP를 통한 데이터 전송

인터넷 프로토콜(IP)을 통해 발생한 네트워크 연결은 데이터를 다양한 방법으로 전송하도록 사용됩니다. 이는 두 가지의 다른 프로토콜을 필요로 하는데 가장 잘 알려진 프로토콜로는 TCP (Transmission Control Protocol)과 UDP (User Datagram Protocol)가 있습니다. TCP는 데이터 전송에 있어서 안정성이 보장된 프로토콜입니다. TCP는 각 데이터 패킷이 신호의 손실 없이 올바른 순서대로 송수신 할 수 있도록 호스트간의 양방향 통신을 이용하여 여러를 확인하고 정정합니다. 즉, 데이터 스트림의 송신기가 연결이 잘 이루어졌는지, 상태가 어떤지 확인이 가능함을 의미합니다. 반면 UDP는 우선적으로 논리적인 네트워크 형성없이 다른 호스트들에게 데이터그램을 전송합니다. 이 말은 사전에 통신이나 수신에 대한 확인이 없음을 뜻합니다. 이는 UDP 방식의 신뢰도가 TCP 방식보다 떨어지지만 관리에 들어가는 간접적인 비용을 최소화 할 수 있다는 것입니다. UDP는 지연된 데이터에 의해 발생하는 사용 중단보다 하나의 데이터그램 손실이 더 나은 상황일 경우에 효과적입니다.

3.3.1. 포트

동시에 발생하는 여러 데이터 전송과 다른 일반적 유형의 데이터 전송을 구별하기 위해 "포트 (Port)"라는 추상적인 기능이 사용됩니다. 다른 호스트들의 각각의 데이터 스트림은 16비트의 '포트 넘버 (Port Number)'로 지정됩니다. 이는 같은 빌딩 안에서 각각 다른 아파트가 있는 형태처럼 볼 수 있습니다. 다음 예시처럼 다수의 데이터 서비스들은 각각의 고정된 포트 숫자를 사용합니다.



3.4. 방화벽 및 보안 체제

방화벽이나 그와 유사한 네트워크 보안 시스템은 네트워크에 승인되지 않은 접근으로부터 보호하며 네트워크 내의 악의적인 데이터 이동을 막아줍니다. 이러한 이유로 방화벽 또는 네트워크 보안 시스템은 기본적으로 무선랜 라우터와 같은 하드웨어 장비에서 대부분 구현되고 활성화됩니다. 이러한 보안 시스템은 특정 IP 주소 또는 주소들의 범위, 특정 포트로 전송되는 데이터를 필터링하며 특정 MAC 또는 IP주소에서 발생하거나 포트로 전송되는 데이터만 통과하도록 허용하는 별도의 방식으로 작동이 됩니다. 방화벽 또는 다른 보안시스템이 존재하는 가장 큰 이유는 바이러스, 백도어 프로그램등에 의한 악의적인 외부의 접근으로부터 네트워크를 보호하기 위함입니다. 위협과 방어 소프트웨어의 복잡성은 점점 증가하고 있고 동시에 소프트웨어를 적절하게 구성할 수 있는 사용자는 극히 드뭅니다. 이런 복잡함으로 인해 대부분은 사용 가능한 모든 보안 시스템들이 자동으로 작동되기를 원합니다. 그로 인해 인해 프로 오디오에서 주로 사용되는 네트워크 연결이 가능한 소프트웨어에 문제를 일으킬 수 있습니다. 사무실 환경에서는 익숙하지 않은 포트와 프로토콜을 사용하고 방화벽에 의해 차단되는 경우가 있기 때문입니다.

인터넷에 연결할 필요가 없는 전문적인 용도의 네트워크는 추가적인 보안 작동을 종료하여 네트워크의 속도가 느려지지 않도록 하고 필요한 통신을 차단하지 않도록 하는 것이 안전합니다.

그럼에도 불구하고 인터넷 접속에 사용되는 프로덕션 네트워크의 컴퓨터를 사용할 때는 매우 주의를 기울여야 합니다. 보안 관련 대책에 대한 관리의 모든 사용자의 책임입니다.

전문적인 생산 환경에서는 네트워크 구성요소에 대한 물리적 접근 권한이 있는 담당자가 있어야 하며 네트워크 와이파이에는 반드시 암호화되어 보호되어야 합니다 (WPA/WPA2, WEP 암호화 아님). 모든 네트워크를 보호하는 것은 어렵기 때문에 위에서 제시한 바와 같이 보안 관련 '매뉴얼'이 네트워크를 보호하는데 가장 효과적입니다. 그 이유는 사람들은 판단력을 가진 네트워크 관리자를 요구하기 때문입니다.

3.4.1. 수동구성 환경설정 지침

특정한 장비 또는 응용 중인 시스템의 네트워크 기본 설정은 IP주소나 서브넷 마스크 주소보다 더 구체화된 수많은 파라미터들을 포함하고 있습니다. 반면에 일반적인 개인 네트워크의 경우에는 이와 관련이 없으며 인터넷과의 데이터 통신을 주로 실행 하므로 특정 설정값을 지니고 있으면 안됩니다.

간혹 몇몇의 네트워크 구성 다이얼로그에서는 장비에 영향이 끼치지 않음에도 불구하고 '게이트웨이 (Gateway)' 옵션을 요구합니다. 이 경우 문제의 장비가 수동으로 지정된 IP주소를 가지고 있다 하더라도 DHCP 서버에 IP주소를 입력하도록 권장하고 있습니다.

4. 무선랜 ("Wi-Fi")

IEEE 규격 802.11의 다양한 버전 중 하나인 무선근거리 통신망 무선랜은 필요로 하는 곳에 유동적으로 움직일 수 있는 특징을 가지고 있으며 생산적 환경에서 보편적으로 자리잡고 있습니다. 이러한 이유로 몇가지 복잡한 사항들을 숙지하여야 합니다.

4.1. 기준 규격

2.4GHz와 5GHz 두 주파수 밴드 모두 다양하게 사용 됩니다. 두 주파수 밴드 모두 몇몇의 전송 규격이 존재하며 이것은 각기 다른 최대 전송 속도와 대역폭을 가집니다. 하지만 모든 경우에 적용되는 것은 아닙니다.

규 격	주파수 범위	최대 로우 데이터 비율
802.11a	5 GHz	54 Mbit/s
802.11b	2.4 GHz	11 Mbit/s
802.11g	2.4 GHz	54 Mbit/s
802.11n	2.4 + 5 GHz	150-600 Mbit/s

4.2. 채널과 주파수

하나 이상의 무선랜 네트워크를 동시에 운용하기 위해 두 개의 주파수 대역은 여러 채널로 세분화됩니다.

2.4GHz 범위 안에서 지역 법률에 따라 최대 14개의 22MHz 대역폭의 채널을 이용할 수 있습니다. 중심 주파수들이 오직 5MHz의 차이를 두기 때문에 양쪽에는 적어도 세 개의 인접한 채널들이 중첩되게 됩니다. 따라서 2.4GHz 대역에서 주요 간섭 없이 동시에 사용 가능한 채널은 3개 뿐이며 이것은 1과 6, 그리고 11입니다. 사실상 이 주파수 대역은 아기용 모니터, 블루투스, 무선 전화기, 무선 마이크와 같은 다른 무선 장비들에도 사용되기 때문에 때때로 오작동이 일으킬 수도 있습니다.

5GHz 대역에서는 지역 법규에 따라 최대 26채널까지 중첩되지 않고 사용이 가능합니다. 현재 이 주파수 대역에서는 트래픽 문제가 적어 안정적인 무선랜 네트워크 운영에 있어서는 이상적으로 여겨집니다. 하지만 5GHz 대역의 짧은 파장은 특정 벽 또는 장애물들을 2.4GHz대역의 파장만큼 통과하지 못합니다. 다시 말해 특정 환경에서 사용할 수 있는 대역이 제한될 수 있습니다.

4.3. 무료 무선랜 채널 찾기

최선의 방법은 관련 당사자들과 라디오 주파수의 사용을 명확히 조정하여 문제가 발생하기전에 미리 예방하는 것입니다.

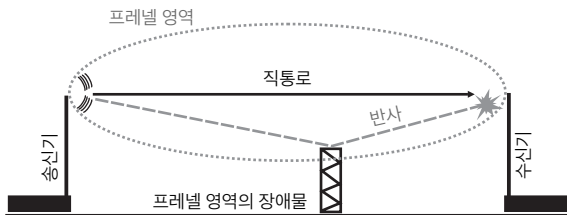
하지만 사용자가 어쩔 수 없이 주어진 환경에 적응해야 하는 상황도 있을 것입니다. 이 경우 무선 네트워크 신호의 존재와 강도를 감지할 수 있는 무선 네트워크 탐지기를 사용하는 것이 효과적이며 더욱 쉽게 무선 네트워크 시스템에 접근 할 수 있을 것입니다.

윈도우 기반의 컴퓨터를 위한 하나의 도구로서 MetaGeek, LLC (metageek.net) 사의 inSSIDER이 무료로 존재합니다. 컴퓨터의 무선 네트워크 아답터를 사용하여 근처의 무선 네트워크를 탐지하고 식별하며 구분합니다. 하지만 아기용 모니터 또는 블루투스 장비와 같이 라디오 주파수 간섭이 일어날 수 있는 소스들을 보여주지는 않습니다.

d&b사는 이러한 써드 파티 소프트웨어의 적절한 사용에 있어서 책임을 가지지 않고 어떠한 지원도 제공하지 않음을 명심하십시오.

4.4. 가시선과 프레넬 영역

모든 고주파 통신은 무선 전파의 무방향적인 방사에 의해 진행됩니다. '가시선, line of sight' 개념은 이미 잘 알려져 있으나 간섭이 직접적인 선상에 존재하는 물체가 아닌 근처 물체들에 의해 반사되어 일어난다는 사실은 잘 알려져 있지 않습니다. 교란된 반사들이 가장 많이 발생하는 특정 공간은 송신기에서 수신기까지의 담배 시가 모양과 같이 묘사될 수 있습니다. 두 지점의 거리가 멀어질수록 시가의 형태와 같이 얇아지게 됩니다. 즉, 프레넬 영역(물리학자 Augustin-Jean Fresnel의 이름을 딴)의 범위가 넓어 질수록 선상에서 일어나는 간섭이 장애물의 영향을 받지 않도록 더욱 신경을 써야 한다는 것입니다.



이상적인 환경을 만들어내기 위한 가장 쉬운 방법은 무선랜 라우터를 송신기 또는 수신기 둘 중 하나에 최대한 높은 위치로 설치하거나 높은 스탠드나 라이저에 외장 안테나를 장착하는 방법입니다. 전자의 방법은 다소 불편한 방법 일 수도 있지만 효과적인 면에서는 더 나을 수도 있습니다. 무선랜 라우터와 오프셋 안테나 사이의 케이블은 우리가 얻고자 하는 효과가 없어지는 지점까지 신호를 빠르게 감쇄 시킵니다.

이러한 효과는 2.4GHz일 때보다 5GHz 대역에서 더욱 강력합니다.

4.5 무선의 활용성

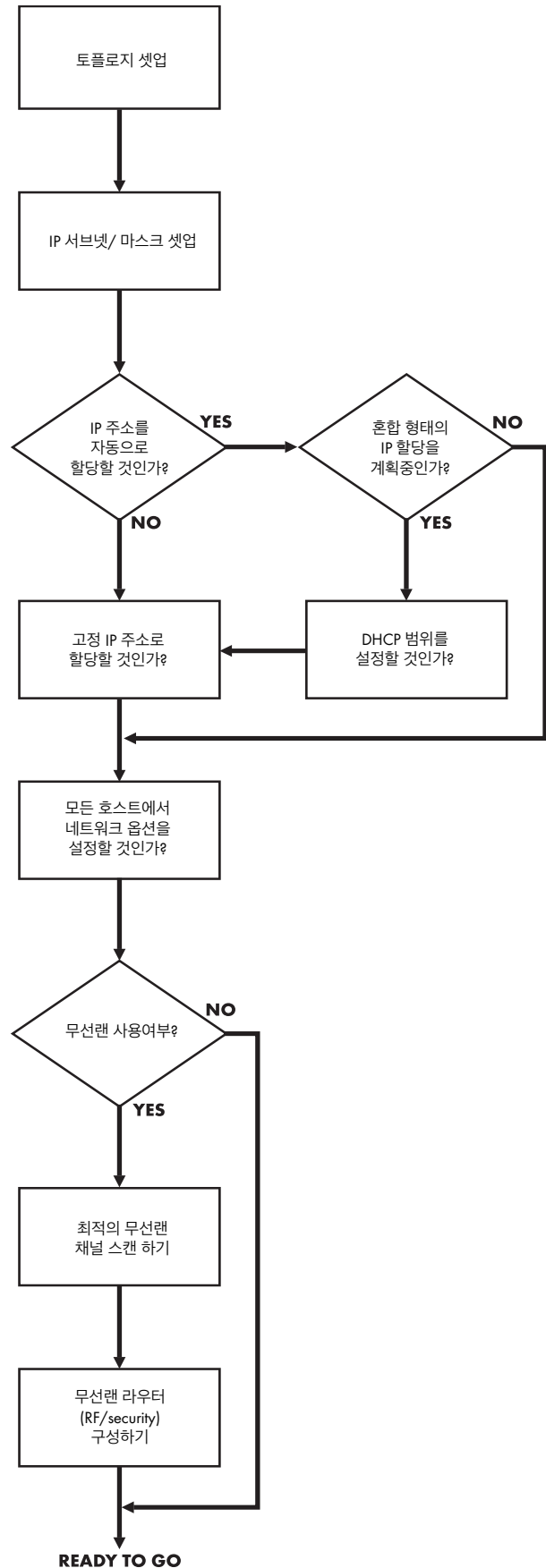
전송 매체에 대한 어떠한 부하도 전체 통신 과정에 불확실성을 더할 수 있습니다. 현대의 쇼 시스템의 복잡성을 감안할 때 가능한 한 위험을 최소화해야 합니다.

무선랜에서 무선 연결은 셋업과 튜닝 과정에서 사용되는 태블릿 컴퓨터와 같이 절대적으로 필요한 곳에만 사용되도록 권장하고 있습니다. 고정된 컴퓨터와 나머지 시스템 간의 연결은 유선으로 연결되어야 합니다. 이는 더욱 쉽게 문제를 발견할 수 있도록 하며 무선으로 운용되어야 하는 몇몇의 장비들이 최대의 무선 대역폭을 확보할 수 있도록 합니다.

고려 해야하는 또 다른 중요한 이슈는 관객 대다수가 무선랜 기능을 갖춘 기기를 하나 이상 가지고 있으며 이들 중 다수가 무선랜을 적극적으로 사용할 수 있다는 점입니다. 이 의미는 텅 빈 공연장에서 무선 네트워크가 완벽하게 작동했음에도 관객이 들어서자마자 문제가 발생할 수 있다는 것입니다.

5. 퀵 스타트 가이드

문서에서 제공한 내용을 잘 숙지했다면 다음의 단계별 과정을 통해 네트워크 시스템의 파악과 논리적 순서에 대해 쉽게 이해할 수 있을 것입니다.



6. 네트워크 하드웨어와 케이블 연결하기

컨텐츠를 데이터 뿐만 아니라 A/V 컨텐츠까지 전송하는 쇼 네트워크는 대역폭에 대해 상당한 수요를 지니고 있습니다. 기가비트 이더넷 기술은 합리적인 비용으로 폭넓게 사용이 가능하며 필요한 대역폭을 제공합니다. 따라서 그에 합당한 투자가 이뤄져야 합니다.

하드웨어에 있어서는 프로페셔널 사양에 준하는 제품을 단독으로 사용하는 것을 권장합니다. 비록 사무실이나 가정에서는 가격이 저렴한 기가비트 스위치들을 사용할 수 있지만 프로 장비들 만큼의 기능을 제공하지는 못합니다. 예를 들어 가정의 내부 대역폭이나 스위칭으로 인한 레이턴시는 공연에서 일어날 수 있는 지속적인 데이터 스트림 전송에는 적절하지 않습니다. 컨텐츠 데이터와 같은 디지털 오디오 신호 또는 비디오와 같은 데이터를 제어할 때 같은 시간에 동일 네트워크 안에서 신호를 전송하는 것이 중요합니다. 이러한 접근이 공연 환경에서는 적용되는 것이 가장 적합하며 견고한 장비에 투자하는 것이 좋습니다.

다음의 리스트들은 전문적인 범주에서 사용이 검증이 된 기가비트 이더넷 스위치들입니다. 선택의 범위가 넓지는 않지만 다양한 가격대와 관리의 편의성과 같은 부가적인 기능을 동반하고 있습니다.

- Allied Telesis GS950/8eco
- Allied Telesis GS950/16eco
- Cisco SG300-10
- Cisco SG300-20
- Cisco WS-C2960G-8TC-L
- Dlink DGS-1210-16
- HP 1410-8G
- Luminex Gigaswitch 8
- Teqsa cyberTEQ m

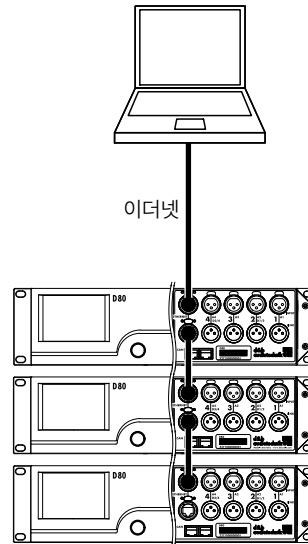
종종 간과 되는것은 상호 네트워크 장비에 연결되는 케이블의 품질입니다. 거리가 100미터까지 제한되어 있고 넓은 대역폭을 가지고 있는 환경에서는 네트워크 케이블링이 큰 차이를 일으킵니다. 유동적인 적용 환경에서 견딜 수 있도록 기계적으로 설계된 차폐 케이블을 사용하는것을 권장합니다. 다음 목록은 전문적으로 사용할 수 있도록 검증이 된 케이블 목록입니다. 이 또한 넓은 범주의 장비 목록은 아닙니다.

- Klotz RC5SB
- Link LK CAT6STP
- CAE Groupe Giga Audio

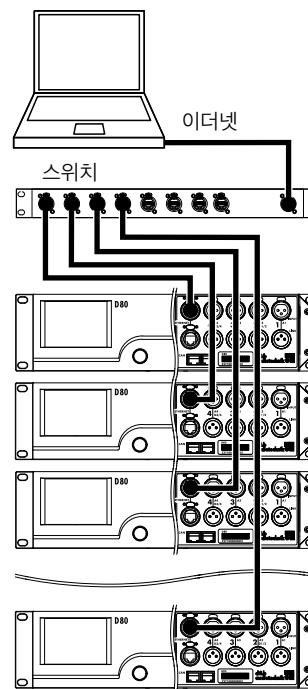
7. 기타 정보

네트워킹에 대한 추가적인 정보가 필요하다면 풍부한 자료들을 인터넷에서 찾아볼 수 있습니다. 이 자료에서 사용되는 기술용어들을 위키피디아에서 검색하면 훨씬 더 세부적인 추가정보들을 얻을 수 있을 것입니다.

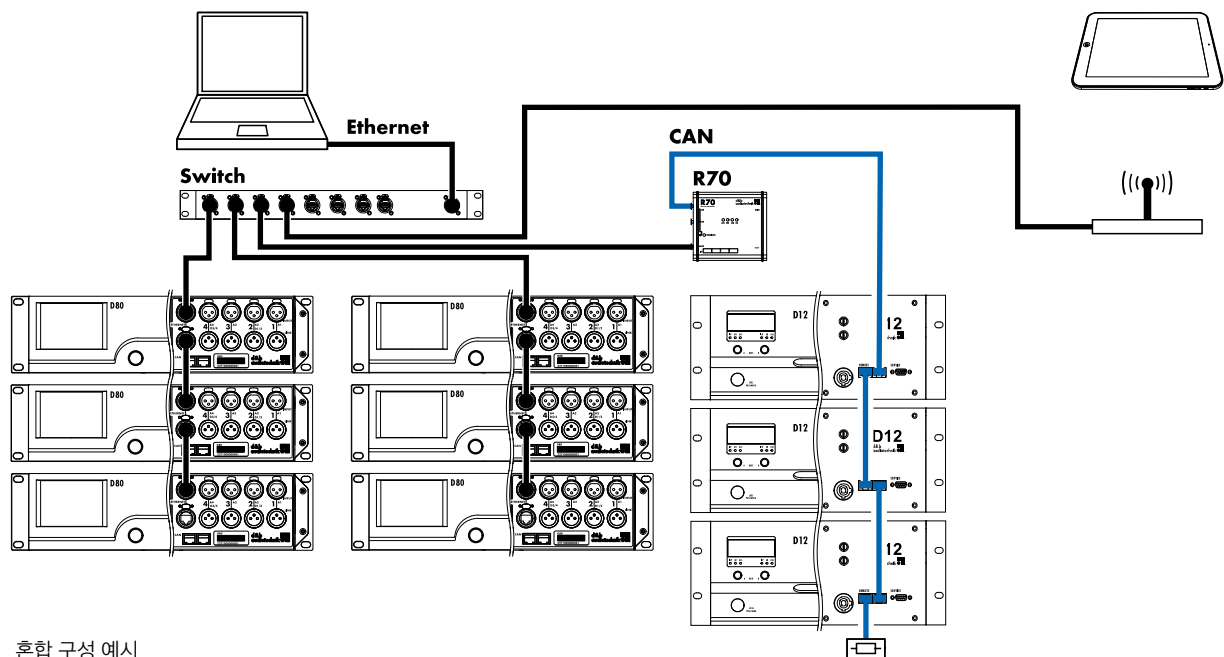
8. 네트워크 토폴로지 예시



최대 3대의 장비까지 연결되는 데이지 체인 토폴로지 구성



스타 토폴로지



혼합 구성 예시

