

TI 310

Ethernet networking (1.1 EN)

General information

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

Contents

1. Introduction.....	4
2. Network topology.....	4
2.1. Network switches vs. network hubs.....	5
3. Identification and communication.....	5
3.1. MAC address.....	5
3.2. IP address.....	5
3.2.1. IP subnet masking.....	5
3.2.2. Private networks.....	6
3.2.3. Automatic vs. manual assignment of IP addresses.....	6
3.2.4. Hybrid IP address assignment schemes.....	6
3.3. Data transport via TCP and UDP.....	7
3.3.1. Ports.....	7
3.4. Firewalls & security measures.....	7
3.4.1. Manual configuration guidelines.....	8
4. W-LAN (“Wi-Fi”).....	8
4.1. Standards.....	8
4.2. Channels and frequencies.....	8
4.3. How to find a free W-LAN channel.....	8
4.4. “Line of sight” and the Fresnel zone.....	9
4.5. Wireless because “we can”?.....	9
5. Quick start.....	9
6. Network hardware and cabling.....	10
7. Further resources.....	10
8. Network topology examples.....	10

1. Introduction

Ethernet-based networks are a method of choice for transporting content, as well as controlling data, in the entertainment industry.

Some topological and administrative schemes are highly complex in that they require university grade knowledge on the subject matter, something that is beyond the scope of this tutorial.

However, the vast majority of networking tasks and sizes are on productions that are smaller than national and world tours and can therefore easily be handled with a basic sound knowledge on the following issues:

- How to set up a working network topology.
- MAC and IP addresses and IP subnet masks.
- How to set up the computer's network adapter.
- How W-LANs work.
- Network security.

This document is intended as a beginner's guide providing exactly this knowledge, though it does not replace a qualified network specialist.

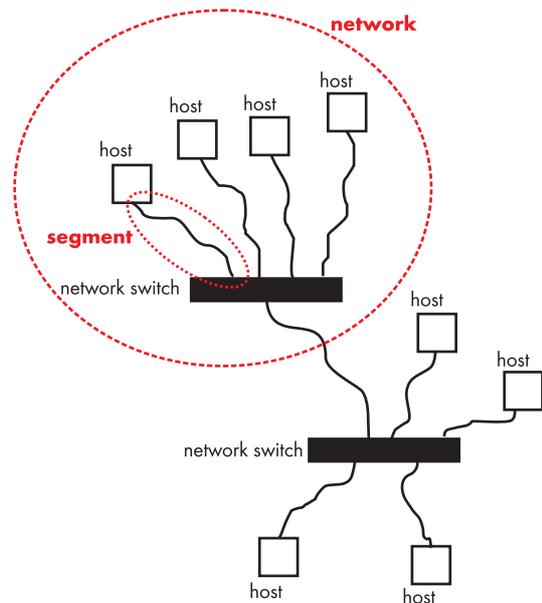
2. Network topology

Typically, Ethernet based networks comprising more than two hosts ('host' is the technical term for a network enabled device) employ a star topology. This means that all hosts are interconnected by one or more central switches or hubs. The switches and hubs themselves may also be interconnected to form a larger network. The connection between two hosts can be referred to as a segment.

Even devices that seem to have daisy chain capabilities in that two connectors are supplied and labeled 'in' and 'out', simply have a small built in three port switch with two ports being visible from the outside, while the actual device is connected to the third internal port.

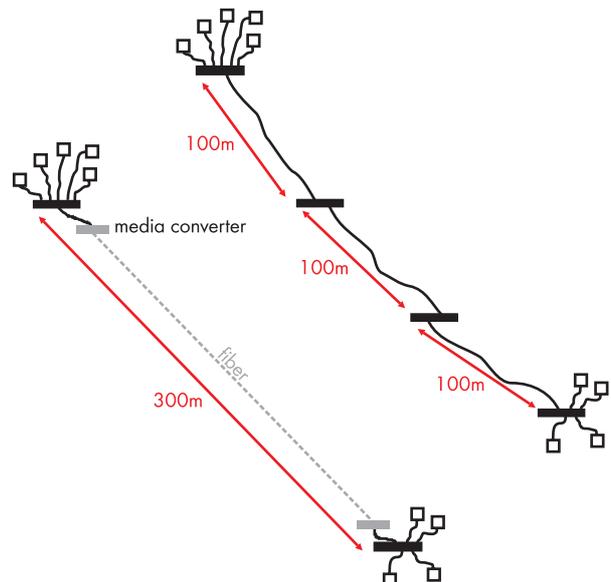
Under no circumstances should any rings be created in the network, unless it is certain that the respective equipment supports this feature and is configured correctly.

On the other hand, it makes sense to physically subdivide networks by using several switches as distribution units. The following illustration shows a typical example of two interconnected star networks.



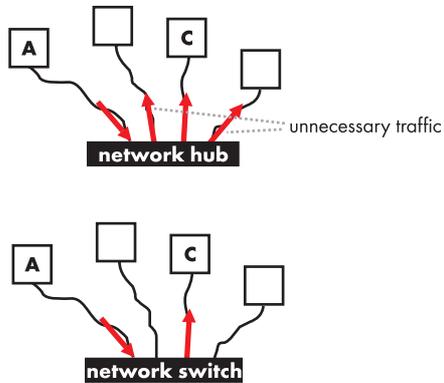
With copper based segments, the maximum length is limited to 100 m, depending on the type of cable used. To extend the maximum distance to be bridged, additional switches or hubs may be inserted along the way to gain an additional segment length of 100 m each. Another way to extend the length of a network segment is to use media converters and fiber optic connections. These allow for distances of up to tens of kilometers.

The following illustration shows both options. The distance to be bridged is about 300 m. With copper based segments, two additional switches or hubs are required along the line involving all the associated issues: they all must be powered and they all represent points of failure. The use of media converters and fiber optics, however, allows for one long piece of fiber to connect both locations.



2.1. Network switches vs. network hubs

Although a switch is by far the most commonly used device to form a simple network, there are still a few network hubs in use. The crucial difference between a switch and a hub is that a hub just acts as an electronic repeater. All data that is received on one port is transmitted to all the other ports. This causes a lot of excess network traffic and includes all the associated problems that cumulatively make the network perform less efficiently.



Hub vs. switch: Host 'A' communicating with host 'C'

A switch, however, 'learns' which host (i.e. MAC address) is connected to which of its ports and will therefore only transmit data between the two correct ports.

3. Identification and communication

Ethernet networks contain hosts of many different types from different manufacturers. Common standards are required for identification and communication. The most relevant will be described here.

3.1. MAC address

This has nothing to do with a popular brand of personal computers. Rather, it is a means to assign a unique identifier to a network host that may need to be addressed directly.

MAC stands for '**M**edia **A**ccess **C**ontrol'. The MAC address is implemented in the hardware of every network host (e.g. a d&b R70 Ethernet to CAN interface, the computer's network adapter, a wireless router, etc.) by the manufacturer and is both unique and, at least in theory, unchangeable.

In Ethernet networks, the MAC address is 48 bits or 6 bytes long, and is usually written in hexadecimal notation for example:

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

A normal network user rarely comes into contact with the MAC address.

3.2. IP address

Aside from the MAC address as a unique hardware identifier, network hosts must be grouped together to form logical networks. To this end, each MAC address (i.e. host) is assigned an IP address. In contrast to the MAC address, the IP address is not exclusive to a specific piece of hardware, but is assigned on a per use basis as needed.

Currently, with IPv4 as the predominant standard, IP addresses are 32 bits long and are usually written in dotted decimal notation, with four decimal numbers ranging from 0 to 255. Each of those four decimal numbers represents 8 bits, which is why they are also sometimes called octets for example:

137.152.89.230

The majority of the time this is what the usual user will have to deal with.

3.2.1. IP subnet masking

To add to the complexity, the IP address is subdivided into a network prefix and the actual host number (also called the 'host part'), similar to a dbCAN network where a distinction is made between the subnet and the actual ID, for example: the CAN ID '5.23' can be separated into the subnet '5' and the ID '23'.

In case of an IP address, however, there is no fixed number of digits to identify the network prefix or the host part. Instead, the network prefix of the IP address is defined by the subnet mask. As this can be a rather complex matter, it should be enough to look at a simple example that is easy to understand. In this example, the subnet mask, whose notation is very similar to the notation of the IP address itself, looks like this:

255.255.255.0

This denotes that the first three octets define the network prefix and the last octet is the host number. All network hosts that are to communicate with each other without any additional 'help' from the network need to have the same network prefix.

With the subnet mask above, such an IP address could look like this:

192.168.0.[x]

where [x] is the host number and '192.168.0.' would have to be identical for all hosts as it denotes the network prefix. All hosts would be required to have '255.255.255.0' set as the subnet mask in their preferences.

This would allow for up to 256 (0 to 255) different hosts (= devices) to be addressed. In reality, the lowest and highest possible host numbers, in this case '0' and '255' are reserved. This reduces the usable number of hosts to 254 in the example, i.e. there may be up to 254 different computers or other network enabled devices in the network. This should still be more than enough for any standard application.

3.2.2. Private networks

From the entire range of possible IP addresses, not all are free for use. The vast majority of IP addresses are administered centrally by the Internet Assigned Numbers Authority (IANA). However, there are a few address ranges that are reserved for private or 'closed' networks without any direct connection to the internet, which can be used within such networks at will. These are the appropriate address ranges for a production environment. The two most commonly used ranges are:

10.0.0.0 - 10.255.255.254

and

192.168.0.0 - 192.168.255.254

Whenever IP addresses are assigned manually, they should be taken from the above ranges. With a subnet mask of 255.255.255.0, IP addresses within a production network would look like this:

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

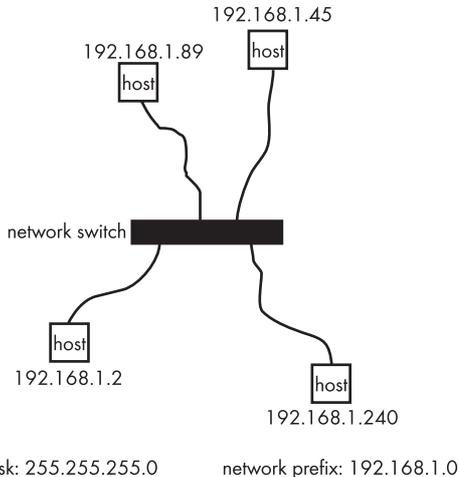
192.168.[x].[z]

where [x] and [y]

are any numbers between 0 and 255. These numbers have to be identical for all hosts (as with the current subnet mask they denote the network prefix)

and [z]

is the host number lying between 1 and 254. This number has to be unique for every host. The illustration shows an example of such a network.



3.2.3. Automatic vs. manual assignment of IP addresses

In order to facilitate quick network configurations, all network parameters, such as subnet mask, IP address, etc. can be assigned automatically within a network. This method is called DHCP (Dynamic Host Configuration Protocol) and requires a DHCP server to be present on the network. Most, if not all, current WiFi routers offer built in DHCP server functionality.

Note: Each network should not include more than **one** DHCP server, as this can lead to confusion and loss of communication. For technical reasons, this may also happen several hours or even days after a second DHCP server has accidentally been added to the network. Bear in mind that every device or computer sharing its internet connection is simultaneously a DHCP server, so care must be taken.

Even when used correctly, there can be drawbacks to DHCP. Very occasionally, specific combinations of hosts and DHCP servers fail to communicate with each other due to slight differences in the implementation of the respective standards. In these cases, the automatic IP address assignment does not work.

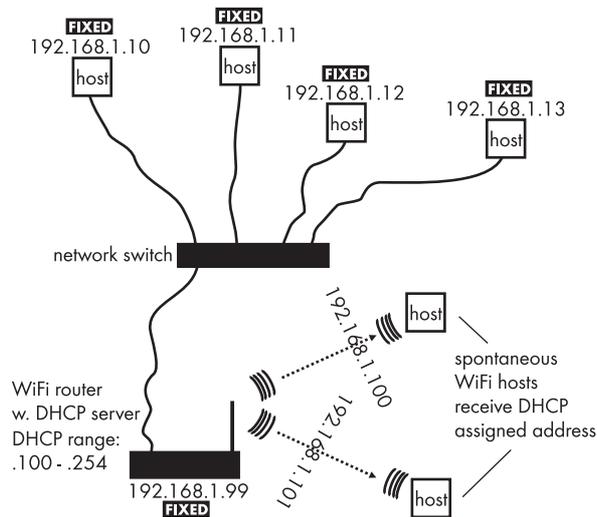
Similar problems can arise with IP addresses that have been assigned manually, even when a DHCP server is present on the network. Duplicate IP addresses cause confusion, as well as hosts that are supposedly set to automatic retrieval of IP addresses via DHCP, but are in fact manually set to an unknown fixed IP address, potentially with a different network prefix.

For this reason, it is beneficial to understand how to reset a host to automatic IP address retrieval. If a fixed IP address has been assigned, it is advisable to label the device, e.g. by writing this address on a piece of tape fixed to the device. This method is also known as 'Peg DHCP' since in many mobile networks IP addresses are distributed manually and written on pegs. The pegs are clipped to the cable plugged into the respective device and provide a clear indication as to where a given IP number is in use.

3.2.4. Hybrid IP address assignment schemes

For networks that generally consist of the same hosts with only occasional additions, the most practical approach is a hybrid between manual and automatic IP address assignment. Many DHCP servers can be configured to hand out IP addresses within a specific range, for example from 192.168.1.**100** to 192.168.1.**254**. In this way all 'regular' hosts could then be assigned fixed IP addresses lying between 192.168.1.1 and 192.168.1.99. This way their address is always known and any duplicate addresses resulting from spontaneously connected hosts with DHCP assigned addresses are avoided.

The following illustration shows a typical scenario: all non-moving hosts have fixed IP addresses that have been assigned manually. The DHCP server, which in this case is also a W-LAN router (a common occurrence) has a set range of available IP addresses so that it does not conflict with the manually assigned addresses. Here, the DHCP server itself also has an IP address (manually assigned and fixed) as it is actively taking part in the network. The illustration shows two spontaneously connected mobile hosts (tablets, mobile laptops, etc.) that request and receive an automatically assigned IP address from the DHCP server in the W-LAN router.



3.3. Data transport via TCP and UDP

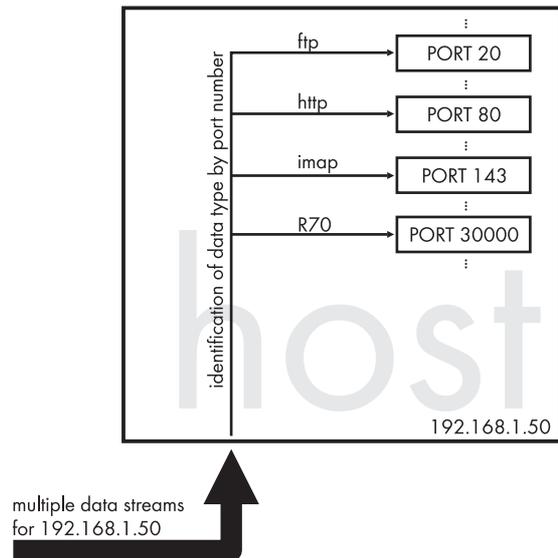
A network connection established via the Internet Protocol (IP) can be used to transport data in various ways. This requires another layer of protocols. The two most commonly used protocols are TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).

The more secure in terms of guaranteed data delivery is TCP. It employs bidirectional communication between hosts, error checking and correction to ensure that each packet is properly transferred and received in the right order and without any loss of data. This means the sender of a data stream always knows whether a connection has been established and what the status of it is.

UDP, in contrast, sends datagrams to other hosts without establishing a logical connection first. This means there is neither any prior communication nor any confirmation of receipt. This makes UDP transmissions less reliable than TCP, but does cut back on the administrative overhead. As a result, UDP is sometimes useful when it comes to real time applications, where one lost datagram is preferable to the longer interruption caused by waiting for delayed data.

3.3.1. Ports

To distinguish several simultaneous data transmissions as well as different general types of data transmission an abstract software construct is used – the 'port'. Each data stream between different hosts is assigned a 16 bit 'port number'. These could be visualized as different apartments within the same building. Many common data services use fixed port numbers, as exemplified in the following illustration.



3.4. Firewalls & security measures

Firewalls and similar network security systems are intended to prevent unauthorized access to networks and to block malicious data traffic within networks. Hence, they are usually implemented and mostly activated by default in hardware devices such as W-LAN routers, and also in modern operating systems. These security systems either filter out data originating from certain IP addresses or address ranges or data addressed to specific ports, or they work the other way round by only allowing data to pass that originates from certain MAC or IP addresses or is sent to a specific port.

The prime reason for the existence of firewalls and other security systems is to protect networks from malicious outside access by viruses, backdoor programs and the likes. The complexity of the threats and the defensive software is constantly increasing. At the same time, very few users are capable of configuring the software properly. For this reason, all of the commonly available security systems try to work automatically. This could cause problems with network enabled software that is typically used in professional audio applications, since the latter may be using ports and protocols that are unusual in a typical office environment and could consequently be blocked by software firewalls.

As a professional production network it is **not** supposed to be connected to the internet, it should therefore be safe to switch off the additional security measures, thus ensuring that they will not slow down the network or block the desired communication.

Nevertheless, great caution has to be exercised when using computers in a production network which are also used to access the internet. It is the responsibility of every user to manage the relevant security measures accordingly.

In a professional production environment, only authorized personnel should have physical access to the network components and any WiFi access to the network should be protected by a secure password (WPA / WPA2, **not** WEP encryption). As it is impossible to make any network totally secure, the more 'manual' security measures described above are the most effective means of protecting a network, because they require the network administrator to think.

3.4.1. Manual configuration guidelines

The network preferences of any device or operating system include a greater number of parameters to be specified than the IP address and the subnet mask. Generally with private networks, however, those fields are irrelevant and should be left empty as they only refer to data communication with the internet.

Nevertheless, some network configuration dialogs require an entry for the 'Gateway' option, even though this should have no effect on the operation of the device. In these cases, it is recommended to enter the IP address of the DHCP server in this field, even if the device in question has its IP address assigned manually.

4. W-LAN ("Wi-Fi")

Wireless Local Area Networks, or W-LANs as various versions of IEEE standard 802.11 (sometimes also called WiFi networks) are very common in production environments as they offer mobility where it is needed. For this reason, it makes sense to become acquainted with a few intricacies.

4.1. Standards

There are two frequency bands used by the various implementations, both in the 2.4 GHz and in the 5 GHz range.

Within those two frequency bands, there are several transmission standards that provide different maximum transmission speeds and consume different bandwidths. Not all of them are equally common.

Standard	Freq range	Max. raw data rate
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. Channels and frequencies

To enable the simultaneous operation of more than one W-LAN network, both frequency ranges are subdivided into a number of channels.

In the 2.4 GHz range, there are up to fourteen 22 MHz wide channels available depending on local legislation. Since their centre frequencies are only 5 MHz apart, every channel overlaps into at least three neighbouring channels on either side. Accordingly, there are only three channels in the 2.4 GHz band that can be used simultaneously without major interferences: 1, 6, and 11. Even so, the fact that this frequency band is also used for other wireless equipment, such as baby monitors, Bluetooth, cordless telephones, and wireless microphones may lead to less than perfect operation at times.

In the 5 GHz range, up to 26 non-overlapping channels are available depending on local legislation. In addition, there is currently much less other traffic in that frequency band, making it seem ideal for trouble free W-LAN network operation. Due to the shorter wavelengths, however, it must be considered that 5 GHz radio waves do not penetrate walls or other obstacles quite as well as 2.4 GHz waves. This could again limit the range in certain conditions.

4.3. How to find a free W-LAN channel

The best procedure is to avoid problems before they arise by clarifying and coordinating RF usage with all parties involved.

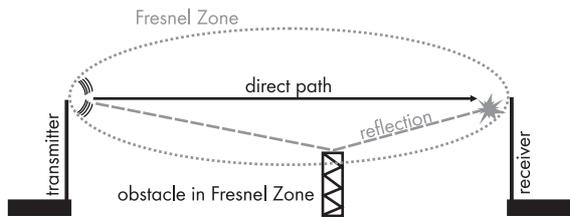
However, local conditions will occasionally force the user to adapt to a given situation. In this case, it might be beneficial to use a wireless network scanner to detect the presence and signal strength of existing wireless networks in order to more easily navigate around them.

One such tool, at least for Windows based computers, is '**inSSIDer**' by MetaGeek, LLC (metageek.net), which is available free of charge. It uses the computer's wireless network adapter to scan for, display and classify wireless networks in the vicinity. It does not show other possible sources of RF interference, such as Bluetooth devices or baby monitors.

Please note that d&b is neither liable nor responsible for the proper operation of this third party software and cannot offer any support for it.

4.4. "Line of sight" and the Fresnel zone

All high frequency radio communication depends on free direct propagation of radio waves. The 'Line of sight' concept is widely known. Less known is the fact of the interference caused by reflections off objects not directly in the line of sight but close to it. The spatial zone in which the most disrupting reflections will occur (named after physicist Augustin-Jean Fresnel) can be described as a cigar shaped volume that extends from the transmitter to the receiver. The greater the distance between these two points, the 'thicker' the cigar becomes. In other words the bigger the Fresnel Zone the more care should be taken to keep the line of sight area clear of obstacles.



The easiest way to achieve at least close to ideal conditions is to either mount the complete W-LAN router as high up as possible, or to use external antennas that can be mounted on a high stand and raised. The former might be preferable despite being a bit awkward, since any cable between the W-LAN router and the offset antenna will very quickly attenuate the signal to a point that may negate the intended benefit. This effect is stronger for 5 GHz than it is for 2.4 GHz.

4.5. Wireless because "we can"?

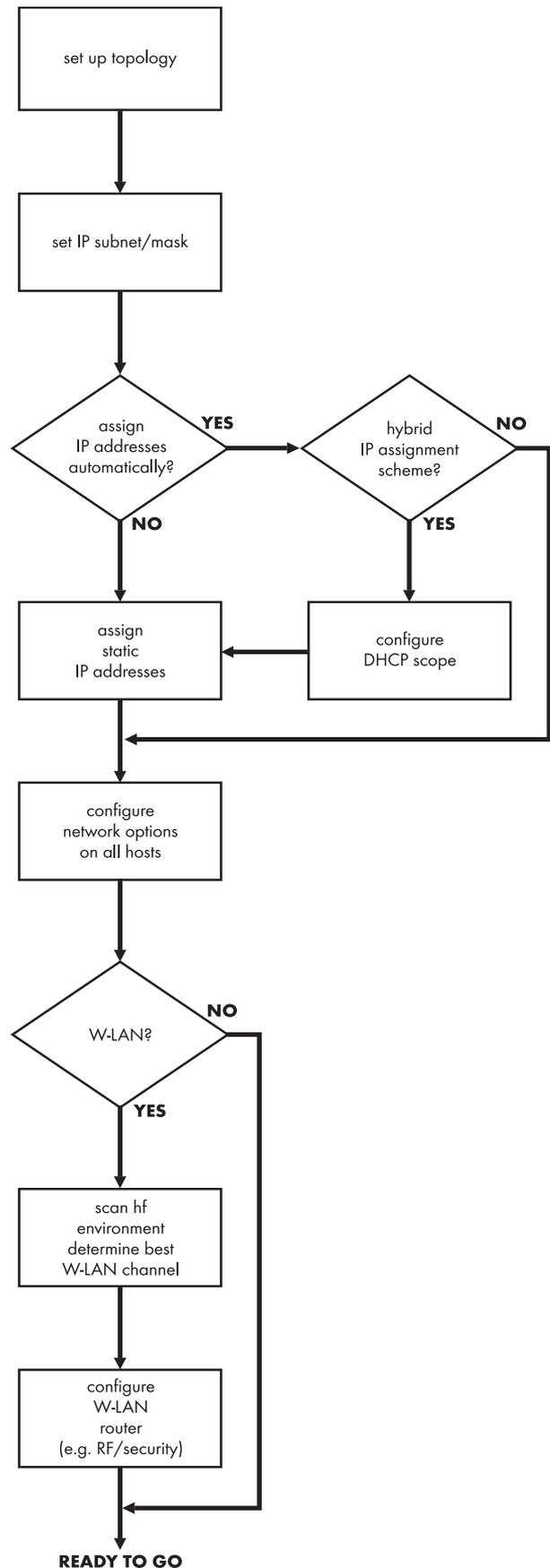
Any change in transmission media will add another layer of uncertainty to the overall communication process and, given the complexity of modern show systems, this risk needs to be minimized as far as possible.

In terms of W-LAN, it is recommended that wireless links should only be used where absolutely necessary, as for example in the case of a tablet computer that is used during setup and tuning. The 'show' connection between a fixed computer and the rest of the system should always be hard wired. This makes fault finding much easier and also frees up the maximum possible radio bandwidth for the few applications that have to be wireless.

Another important issue to consider is that, during the show, chances are that the majority of people in the audience will have at least one device on them that has W-LAN capabilities (e.g. smartphones), and many of them will have W-LAN turned on permanently. This means, even though a wireless network worked perfectly in the empty venue, it might break down as soon as the audience enters.

5. Quick start

Provided the information given in this document has been read and understood, the following step by step procedure should help in configuring a network quickly and in a logical order.



6. Network hardware and cabling

Show networks, particularly those that will not only transport control data but also A/V content, place significant demand on bandwidth. Gigabit Ethernet technology is widely available and reasonably priced, offering all the bandwidth that might be needed. It therefore makes little sense to invest in anything less.

The use of exclusively professional grade hardware is strongly recommended. Although there are cheap Gigabit switches available for home office use, these do not offer the same performance as professional equipment. For example, the internal bandwidth and switching latency of a home office device is usually inappropriate for continuous high bandwidth data streams, as may occur in a show network. This is of particular importance when control data as well as content data, such as digital audio or video, is to be transported over the same network at a point in time, something very likely in today's show environment. For this reason it is sensible to invest in solid equipment.

The following list specifies a few Gigabit Ethernet switches that have been tested and found suitable for professional use. It is not a comprehensive list, but it includes different price ranges and secondary capabilities, such as manageability.

- 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
- Teqas cyberTEQ m

Often overlooked is the quality of the cabling used to interconnect network devices. Within network cabling, there can be huge differences, especially when distances near the specified limit of 100 m and large bandwidths are involved. As a general recommendation, only shielded cable that has been mechanically designed to withstand the rigors of mobile applications should be used.

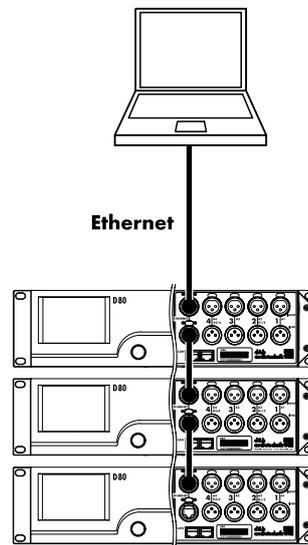
The following list specifies a few makes of cables that have been tested and found suitable for professional use. This is not a comprehensive list.

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

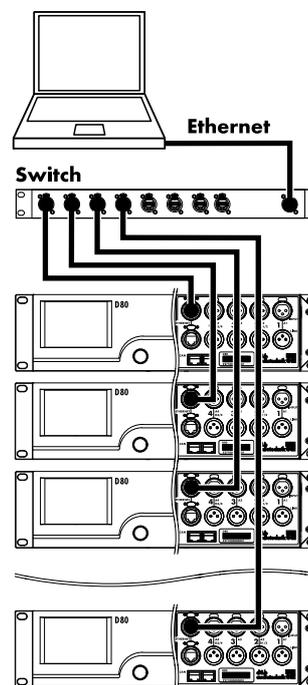
7. Further resources

If further information on networking is desired, the internet offers a wealth of additional reading material. A search on Wikipedia alone for any of the technical terms used in this paper will yield a wealth of additional information, which will in itself offer boundless possibilities to branch off into even more detail.

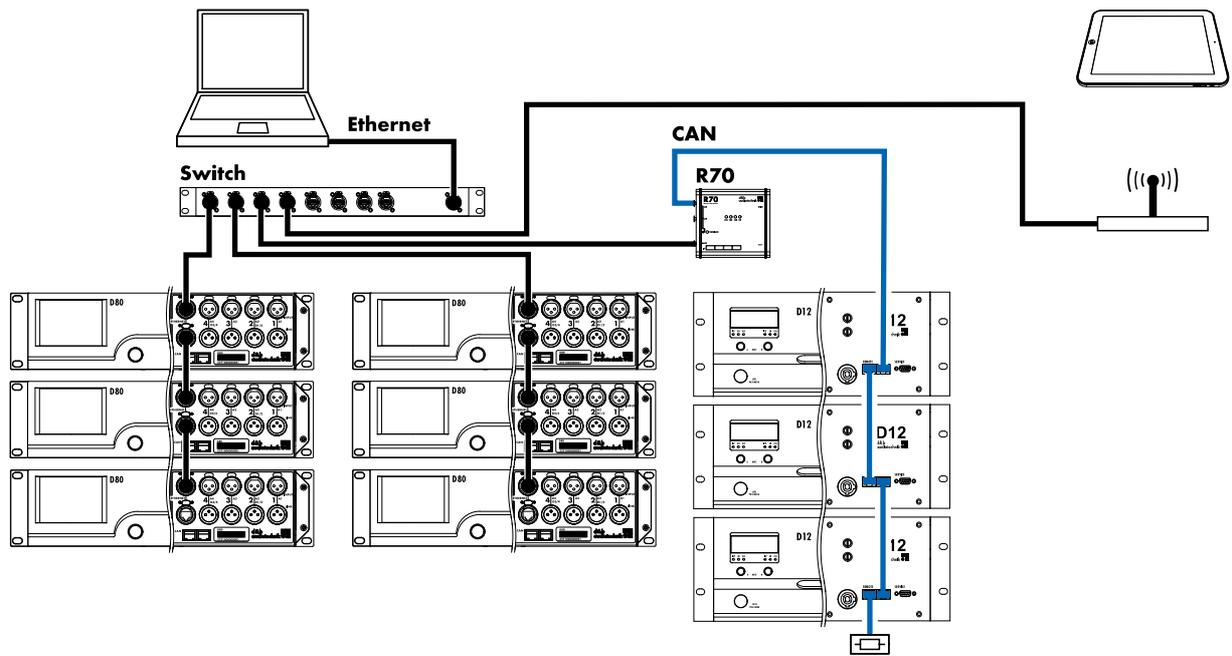
8. Network topology examples



Daisychain topology for a maximum of three devices



Star topology



Mixed configuration

