

# DMX512 over Ethernet (2)

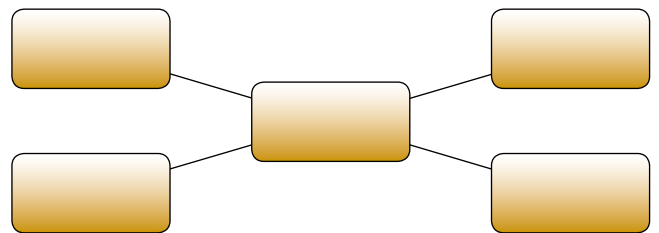
In het tweede deel van deze serie gaan we dieper in op ethernet. Eerst de hardware, dan de adressering. Het deel over de adressering heeft een hoog ICT-gehalte. Maar weten hoe die adressering werkt is cruciaal voor een goed begrip van ethernet en helpt in de praktijk om fouten te voorkomen en op te lossen.

Om te begrijpen hoe DMX over ethernet wordt verzonden is het goed te weten wat ethernet is. Ethernet is in de jaren zeventig bedacht door de firma Xerox en heeft zich ontwikkeld tot een wereldwijde standaard. Het is een verzameling hardware afspraken waardoor computers met elkaar verbonden kunnen worden. Dat was op zich niet zo bijzonder, maar het legde ook vast hoe ethernet-netwerken met elkaar verbonden konden worden, namelijk op dezelfde manier als de computers. Dit maakt ongeremde groei mogelijk, en daarmee ook het ontstaan van internet via het world-wide-web. In tegenstelling tot wat wij regelmatig horen zeggen, is internet (net zoals e-mail en Art-Net) gebaseerd op ethernet en niet andersom.

Een ethernet netwerk kan allerlei verschillende apparaten aan elkaar verbinden. Thuis of op kantoor zijn dit meestal computers, maar het kunnen ook lichtcomputers, dimmers of DMX-nodes zijn. Op het moment dat een apparaat informatie wil gaan verzenden moet het eerst luisteren of de lijn waarmee het aan het netwerk verbonden is, vrij is. Is dit niet het geval dan volgt na een bepaalde tijd een nieuwe poging. Dit principe heet 'lijnaftasting'. Mocht de lijn vrij lijken, dan kan het apparaat zijn mededelingen op de lijn zetten. Natuurlijk is het mogelijk dat een ander apparaat ook wat te melden had en vond dat de lijn vrij was en dus tegelijkertijd communiceert. Dan volgt een 'collision' of botsing. Beide apparaten moeten nu een willekeurige tijd wachten voor dat ze weer mogen communiceren. De botsing is dus geen fataal ongeluk maar een van de principes die ten grondslag liggen aan ethernet.

Dit is een fundamenteel verschil ten opzichte van DMX, dat werkt via een serieel protocol. Bij DMX blijft de datatrein altijd maar rijden en hoeft er nooit gewacht te worden om verder te gaan. De eerste vraag die dan bij een technicus opkomt is natuurlijk 'is ethernet dan wel realtime?' Het antwoord is een theoretisch nee. Immers: realtime betekent dat een bericht zou moeten aankomen

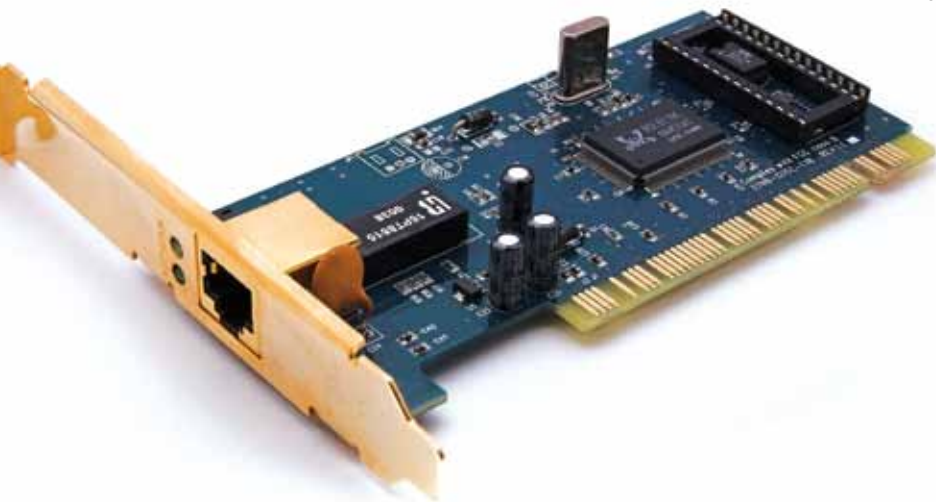
binnen een vastgestelde tijd. Ethernet garandeert op dat gebied niets: zowel het moment van verzending als van ontvangst is toeval. Gelukkig gebeuren deze 'toevalligheden' sneller dan het oog kan waarnemen. Daardoor werkt het prima. Bovendien zijn er een paar slimme trucs om het probleem op te lossen, zoals snelle verbindingen aanleggen en lichtnetwerken gescheiden houden van andere netwerken. En er zijn protocollen die handig gebruik maken van het versturen van controleerbare klokpulsen.



## De hardware

Net als bij DMX wordt de kwaliteit van het netwerk bepaald door de kwaliteit van de componenten. Daar houdt de vergelijking ook meteen op. Zoals gezegd volgt het huidige ethernet de sterptopologie. Dit wil zeggen dat alle apparaten aangesloten zijn op één of meer centrale punten. Deze verdelers kunnen hubs, switches of routers zijn. Zij zijn met elkaar verbonden door middel van glasvezel, koper of draadloze verbindingen. Op deze manier ontstaat er een heel netwerk van verschillende sterren die onderling met elkaar kunnen communiceren. De belangrijkste componenten binnen een netwerk zijn bekabeling of draadloze verbindingen, netwerkkaarten, hubs, switches en routers. Zonder deze componenten kan een ethernet netwerk niet bestaan. Daarom volgt hier een beknopte omschrijving.





**Netwerkaart**

De netwerkaart zorgt voor de fysieke toegang tot het ethernet. Elk apparaat dat op het ethernet is aangesloten moet een netwerkaart hebben. Tegenwoordig worden bijna alle nieuwe pc's met netwerkaart verkocht. De netwerkaart geeft het apparaat een uniek adres (IP-adres) en een eigen identiteit, het MAC-adres (Media Access Control). Dit is een vast adres dat op de netwerkaart geprogrammeerd is en dat niets te maken heeft met Macintosh computers. Het MAC-adres is niet te wijzigen en komt maar één keer in de hele wereld voor. Via dit adres kan een apparaat altijd op het netwerk of internet teruggevonden worden. Het IP-adres is softwarematig en kan gegeven worden door een server of zelf ingevoerd worden. Het IP-adres zorgt er voor dat een apparaat in een bepaald netwerk valt. Later in dit artikel meer over het IP-adres.

**De hub**

Een hub is niets meer dan een digitale kroonsteen. Hij zorgt dat alle apparaten met elkaar verbonden zijn. Het signaal dat binnenkomt wordt onversterkt doorgevoerd naar de andere apparaten die aangesloten zijn op de hub. Het vormt een kruispunt met stoplichten. Een groot nadeel van deze component is dat er maar één zender tegelijkertijd actief kan zijn. Alle andere zenders worden tijdelijk stil gelegd, tot de communicatie beëindigd is en er nieuwe verbindingen opgebouwd kunnen worden. Er zijn situaties bekend met twee lichtcomputers die allebei dimmers aanstuurden via een hub, waarbij bleek dat de crossfades niet meer hetzelfde waren! Om collisions te vermijden mogen er maar een maximaal aantal (meestal 6, maar 4 is veiliger) hubs achter elkaar aangesloten worden.

**De switch**

Een switch zorgt net als een hub dat alle apparaten met elkaar verbonden zijn. Het verschil is dat hij het signaal versterkt doorgeeft. Een ander groot verschil is dat hij een point-to-point verbinding maakt tussen twee apparaten. Dit betekent dat op het moment dat apparaat A informatie wil verzenden naar apparaat B, hij rechtstreeks wordt verbonden en beide gedurende de informatie-

overdracht losgekoppeld zijn van de rest van het netwerk. Voor de andere apparaten lijkt de lijn weer leeg en er kunnen gelijktijdig andere verbindingen opgebouwd worden. Zo kunnen meerder apparaten tegelijk informatie verzenden over één netwerk. Als meerdere netwerken aan elkaar gekoppeld zijn dan maken zowel de hub als de switch daar geen onderscheid in, ze sturen alles gewoon door wat aangeboden wordt.

**De router**

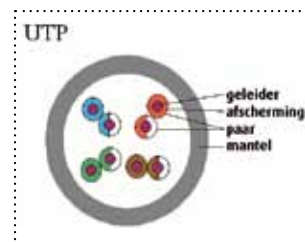
De router is het geavanceerdste van dit gezelschap. Hij koppelt verschillende netwerken aan elkaar, controleert de dataoverdracht en kan daardoor ook netwerken gescheiden houden. Routers bepalen de snelste weg naar een apparaat. Als het apparaat zich niet achter de router bevindt stuurt hij de informatie niet door. Bij internet toepassingen wordt veelvuldig gebruik gemaakt van routers. Het instellen gebeurt meestal via de webbrowser. In lichtnetwerken komt hij zelden tot nooit voor.

**De snelheid**

Met de snelheid van een netwerk wordt bedoeld hoeveel data per seconde over een verbinding getransporteerd kan worden. Voor ethernet zijn er op dit moment twee belangrijke snelheden 100 en 1000 mbit/s. Deze twee soorten worden ook wel 100 base-T en 1000 base-T netwerken genoemd. Het getal verwijst naar de snelheid en de T naar twisted pair kabels.

**Twisted pair kabels**

Bij twisted pair kabels zijn de aders per twee tegen elkaar ingedraaid met als doel om de interferentie op de kabel te verkleinen. In de meeste netwerken worden Unshielded



Twisted Pair (UTP) kabels toegepast. Voor omgevingen waar veel elektromagnetische velden of andere storingsbronnen zijn, kan ook gekozen worden voor de veel duurdere Foiled Twisted Pair (FTP), Shielded Twisted Pair (STP) of Shielded Foiled Twisted pair (SFTP). Al deze kabels zijn in principe ook geschikt voor DMX netwerken en voldoen aan de eisen daarvoor.



UTP	Geen afscherming
FTP	Heeft een afscherming rond de kabel.
STP	Heeft een afscherming rond de adersparen.
SFTP	Heeft een afscherming rond de kabel en adersparen.

## De categorie

Ethernet kabels zijn ingedeeld in verschillende categorieën. Elke categorie heeft zijn eigen specificaties en snelheid. In de meeste gevallen zijn ze leverbaar in alle genoemde types UTP, FTP, STP en SFTP. Een CAT5 is nooit sneller dan 100 megabit per seconde.

Categorie	Netwerk	Bandbreedte	Snelheid	Maximale lengte
5	100 base-T	100 mhz	100 mbit/s	100m
5e	100 base-T, 1000 base-T	100 mhz	100 mbit/s 1000 mbit/s	100m
6	1000 base-T	250 mhz	1000 mbit/s	100m

## Adressering en TCP/IP

Het aansluiten van de kabels en instellen van DMX-adressen is niet voldoende: voor het instellen van de software is kennis van TCP/IP een vereiste. We gaan vooral dieper in op het adresseren, omdat onze ervaring is dat dit een voorname bron van storingen is, terwijl het dat niet hoeft te zijn. TCP/IP is een netwerkprotocol dat de communicatie regelt tussen verschillende apparaten die aangesloten zijn op het ethernet. TCP/IP baseert zich op ethernet zoals DMX zich baseert op RS485. Spreken van DMX512 over ethernet is strikt genomen dan ook niet juist, want alle lichtnetwerken maken gebruik van het TCP/IP protocol voor het sturen van licht en het configureren



van apparaten. Correct zou zijn 'DMX over TCP/IP'. Het TCP/IP protocol bestaat uit twee delen TCP (Transport Control Protocol) en IP (Internet Protocol). IP is belangrijk voor belichters die met ethernet willen werken. IP regelt de adressering van alle apparaten binnen het netwerk het vormt een laag tussen de universes (DMX lijnen) en het herkennen van alle verschillende apparaten binnen het netwerk. Dit kunnen lichtcomputers, dimmers, nodes, mediaservers of led-schermen zijn, tegenwoordig zijn ze allemaal met het stickertje TCP/IP te koop.

## Internet Protocol (IP)

Het Internet Protocol IP schrijft voor dat elk apparaat dat aangesloten is op een ethernet netwerk zowel een uniek nummer als een gemeenschappelijk nummer moet hebben om zich te kunnen identificeren en aldus data te kunnen ontvangen of verzenden. Dit is het IP-adres. Het IP-adres bestaat uit een 32-bits getal, verdeeld in 4 blokken van 1 byte. Elke byte wordt gescheiden door een punt. De notatie is decimaal en geeft per blok een maximale waarde tussen 0 en 254. Het IP-adres van de computer waar deze regel op geschreven is, is bijvoorbeeld 192.168.1.31.

## Statisch of dynamisch

Er bestaan twee manieren voor het uitdelen van IP-adressen: statisch en dynamisch. Statisch betekent dat elk apparaat een vast IP-adres heeft dat nooit wijzigt. Bij het installeren moet het eenmalig handmatig op de netwerkkaart van het apparaat ingevuld worden. Vanaf dat moment heeft het apparaat een statisch adres. Als sprake is van dynamische IP-adressering krijgen alle apparaten binnen het netwerk automatisch een IP-adres toegewezen van een server. Dit is typisch een instelling die thuis veel voorkomt: de computers staat op automatisch ingesteld en dat werkt meestal. Controleren, monitoren en routeren is op deze manier een stuk gemakkelijker omdat het allemaal centraal op de server gebeurt. Een ander voordeel is dat je niet hoeft na te denken welk IP-adres je moet gebruiken bij het aansluiten van een nieuw apparaat. De server bepaalt dit voor je. Nadelen zijn dat niet alle apparaten geschikt zijn voor dynamische adressering en dat bij het vervangen van een apparaat het een nieuw IP-adres krijgt, terwijl het eigenlijk het adres van het kapotte apparaat moet krijgen. Dit maakt dat de meeste belichters die wij hierover spraken, inclusief toonaangevende lichtverhuurbedrijven, gebruik maken van *statische* adressering. Het is dus zaak daarvan de regels en terminologie te kennen. Er zijn twee manieren: de makkelijke is *classfull* adresseren, de iets gecompliceerdere is *classless* adresseren, ook wel *subnetting* genoemd. We geven beide.

## Classfull IP adresseringen

Bij Classfull adresseringen, worden IP-adressen ingedeeld in vijf klassen A, B, C, D en E. De laatste twee zijn gereserveerd voor experimenten en theoretische toepassingen, in onze praktijk komen we alleen A, B en C tegen. Het doel van Classfull adresseren is het groeperen van IP-adressen in verschillende categorieën, waardoor het beheren van het netwerk een stuk overzichtelijker wordt. Een klasse is een opeenvolgende serie van getallen. Omdat die getallen uit 4 bytes bestaan, rekent het anders dan we van de lagere school gewend zijn. Bij een A-klasse IP-adres begint de eerste byte met een b0, een binaire nul, gevolgd door 7 resterende bits. Dit heeft als rekenkundig gevolg dat het eerste byte tussen 1 en 127 decimaal zit. (Detail: het getal 127=b0111.1111 is gereserveerd en wordt het loopback adres genoemd. Door iets naar dat adres te sturen weet je zeker dat het weer bij jezelf aan komt, het numerieke equivalent van de uitspraak " ik ben mezelf". Typisch loopback adres is 127.0.0.1). Bij een B-klasse IP-adres begint de eerste byte

met b10. Het eerste byte kan daardoor alleen de waarden vanaf 128 tot 191 hebben. De laatste klasse die we tegenkomen is de C-klasse. De C-klasse heeft als eerste bits b110 en dus ligt de waarde van het eerste byte tussen 192 en 223.

IP-adres	Bits	Laagst mogelijke waarde	Hoogst mogelijke waarde
A-klasse	0xxx xxxx	2	126
B-klasse	10xx xxxx	128	191
C-klasse	110xxxxx	192	223

Klasse-indeling door middel van de 1e byte van een IP-adres

### Net-ID en Host-ID

De vier bytes van een IP-adres zijn opgedeeld in een net-ID en een host-ID. 'Host' is de benaming voor elk apparaat in een netwerk. Het host-ID identificeert dit apparaat binnen het netwerk zoals het huisnummer een huis identificeert in een straat: er is maar één huis met dat nummer in die straat. Het net-ID is vergelijkbaar met de straat zelf en geeft dus aan in welk netwerk de host zich fysiek bevindt. Is de informatie via het net-ID aangekomen in de juiste 'straat', dan worden de gegevens met behulp van het host-ID-gedeelte van het IP-adres afgeleverd bij de juiste host. Bij een A-klasse IP-adres geldt dat het eerste byte het net-ID is, de overige 3 bytes zijn het host-ID. Bij een B-klasse IP-adres zijn de eerste twee bytes het net-ID en de laatste twee het host-ID. Bij een C-klasse adres geldt dat de eerste 3 bytes het net-ID zijn, en de laatste byte het host-ID. IP-adressen die direct met elkaar moeten communiceren moeten hetzelfde net-ID hebben en een uniek host-ID.

	Byte 1	Byte 2	Byte 3	Byte 4
A-klasse	Net-ID	Host-ID	Host-ID	Host-ID
B-klasse	Net-ID	Net-ID	Host-ID	Host-ID
C-klasse	Net-ID	Net-ID	Net-ID	Host-ID

Opbouw van een classfull IP-adres

### Subnetmask

Bij elk IP-adres hoort een subnetmask. Dit is een soort rekenkundig filter, waarmee eveneens het net-ID en het host-ID bepaald kunnen worden. De klassen A, B en C hebben respectievelijk een vast subnetmasker van 255.0.0.0, 255.255.0.0 of 255.255.255.0

Classfull subnetmask		
Klasse	Subnetmask	Binair
A	255.0.0.0	b11111111.0.0.0
B	255.255.0.0	b11111111.11111111.0.0
C	255.255.255.0	b11111111.11111111.11111111.0

Het gedeelte van het subnetmask dat de énen bevat komt overeen met het gedeelte van het IP-adres dat het net-ID is; de nullen komen overeen met het host-ID.

Belangrijke regel: *Alleen IP-adressen die hetzelfde net-ID hebben, hetzelfde subnetmask en een verschillend host-ID kunnen direct met elkaar communiceren.*

Anders gezegd (omdat het zo belangrijk is en er vaak fouten mee worden gemaakt, zelfs door ervaren ICT-ers): alleen als voor elke 255 in het subnetmask het getal in het IP-adres hetzelfde is, en voor de rest verschillend, kunnen computers direct met elkaar communiceren. Deze laatste manier van formuleren geldt alleen voor classfull adresseren, waar het subnetmask uit 8, 16 of 24 énen bestaat, aangevuld met nullen. Met *direct* communiceren bedoelen we zonder tussenkomst van een router. Uiteraard kunnen alle apparaten met een IP-adres data uitwisselen, maar direct communiceren is essentieel voor lichtnetwerken. In het volgende deel leggen we uit waarom.



### Een voorbeeld

Naam	IP adres	C klasse Subnetmasker
Computer X	192.168.1.31	255.255.255.0
Computer Y	192.168.1.32	255.255.255.0
Computer Z	192.168.0.31	255.255.255.0

### Vraag: wie communiceert direct met wie?

Antwoord: Computer X kan met Y direct communiceren, want die hebben hetzelfde net-ID, 192.168.1, hetzelfde subnetmask 255.255.255.0 en een uniek host-ID 31 en 32. Computer Z doet niet mee. Het net-ID komt niet overeen. Er is geen conflict, want alle IP-adressen zijn verschillend.

### Subnet en Broadcasting

In het bovenstaande voorbeeld kan Z alleen met X en Y communiceren via een router. Z behoort tot een ander deel van het netwerk. Dit wordt subnet genoemd. X en Y zitten in hetzelfde subnet. In een subnet hebben IP-adressen hetzelfde net-ID. Er gelden echter nog meer beperkingen. Het laagste en het hoogste IP-adres van een subnet zijn gereserveerd. *Het laagste adres is het net-adres*, in ons voorbeeld 192.168.1.0 voor X en Y; voor Z is het 192.168.0.0. *Het hoogste adres is het broadcast adres*. In ons voorbeeld respectievelijk 192.168.1.255 en 192.168.0.255. Informatie die naar het broadcast adres wordt gestuurd, wordt automatisch naar alle adressen in het subnet gestuurd. Als je een ethernet-netwerk vergelijkt ▶



met een wijk vol huizen, dan is een subnet een straat waar de mensen elkaar begrijpen. Het net-adres is dan vergelijkbaar met het adres van de straat zelf, de plek waar de straatstenen liggen. Dit adres is alleen relevant voor de stratenmaker. Het broadcast adres is dan het postvakje voor alle huis-aan-huisreclame. Dit laatste is erg handig.

**Samengevat**

Net-adres	Broadcast-adres	Vrij te gebruiken adressen
192.168.1.0	192.168.1.255	192.168.1.1 t/m 192.168.1.254
192.168.0.0	192.168.0.255	192.168.0.1 t/m 192.168.0.254

Voor een A-klasse netwerk geldt dat het net-adres op 0.0.0 eindigt en het broadcast adres op 255.255.255. Veel lichtnetwerken maken gebruik van Art-Net. Art-Net schrijft voor dat het alleen werkt op een A-klasse netwerk en dat de informatie naar het broadcast adres gestuurd wordt. Welke consequenties dit heeft, vertellen we in het volgende artikel.

**Subnetting en classless adresseringen**

Het is een goed plan om apparaten die veel informatie delen, in hetzelfde subnet onder te brengen. Zo ontstaan er verschillende werkgroepen die gemakkelijk beheerd en gecontroleerd kunnen worden. De informatie is sneller toegankelijk en het vormt een minder grote belasting op het netwerk. Met classfull adresseren bestaat het subnetmask uit 8, 16 of 24 énen. In het geval van classless adresseren kan het subnet ook uit meer of minder énen bestaan, waarbij wel geldt dat het minimaal aantal niet minder mag zijn dan de klasse van het netwerk en dat het subnetmask altijd uit énen gevolgd door nullen bestaat. Het resultaat is dat het subnet beter aangepast kan worden aan de hoeveelheid hosts. Een A-klasse netwerk heeft dan een subnetmask van meer dan 8 énen, een B-klasse subnetmask heeft dan meer dan 16 énen en het C-klasse subnetmask meer dan 24 enen. Elk klasse-subnet wordt dus onderverdeeld in kleinere subnets.

**Voorbeeld**

Aantal hosts	Subnetmask	Binaire notatie
2	255.255.255.252	b11111111.11111111.11111111.11111110
6	255.255.255.248	b11111111.11111111.11111111.11111100
14	255.255.255.240	b11111111.11111111.11111111.11111000
30	255.255.255.224	b11111111.11111111.11111111.11110000

Op meerdere plekken op internet valt te lezen dat de klasse van een netwerk afhangt van het subnetmask. Dit is niet waar. Een A-klasse netwerk kan prima een subnetmask van 255.255.255.0 hebben. Dat dit subnetmask ook de standaard is voor een C-klasse netwerk, doet er verder niet toe. Door de regel van eerst énen, dan nullen kan het subnet omschreven worden door het net-adres (zijnde het laagste adres in het subnet) gevolgd door een getal dat het aantal enen van

het subnet weergeeft. Dit getal staat achter het net-adres en wordt gescheiden door het teken / (slash forward).

**Voorbeeld**

Net-adres: 192.168.2.0/26. Welke IP-adressen kunnen met elkaar communiceren? De klasse van het netwerk is C, waarvan de eerste byte ligt tussen 192 en 223. Normaal heeft een C-klasse netwerk een subnetmask bestaande uit 24 énen, maar nu zijn het er 2 meer, omdat het adres gevolgd wordt door '/26'. Met deze 2 extra bits zijn er 4 mogelijkheden te maken: b00, b01, b10, b11. Dit betekent dat het standaardsubnet in 4 delen wordt opgesplitst van 64 (0 tot 255 gedeeld door 4). In plaats van 255 kunnen er dan nog maar 64 apparaten op hetzelfde subnet. Subnetmask is dus 26 énen: b11111111.11111111.11111111.11000000 = 255.255.255.192

**Kort samengevat:**

- Subnet 1: netadres:192.168.2.0, broadcastadres: 192.168.2.63, alles daartussen communiceert met elkaar.
- Subnet 2: netadres 192.168.2.64, broadcastadres: 192.168.2.127
- Subnet 3: netadres 192.168.2.128, broadcastadres: 192.168.2.191
- Subnet 4: netadres 192.168.2.192, broadcastadres: 192.168.2.255.

Met enig talent is het niet moeilijk om in te zien dat het net-adres binair altijd op nullen eindigt en dat het broadcastadres altijd op énen eindigt. Het grote voordeel hiervan is dat apparaten elkaar sneller vinden en het hele netwerk daardoor sneller wordt. In het volgende artikel zullen we onder andere wat dieper ingaan op ACN, de standaard voor lichtnetwerken. Dat heeft onder andere als doel het netwerkgebruik te optimaliseren en subnetting hoort daarbij.

Tip: op internet zijn meerdere IP-calculators te vinden. Daarmee experimenteren, geeft vaak extra inzicht en maakt het makkelijker om zelf te subnetten.

Heeft een belichter subnetting dagelijks nodig? Nee. Maar het is het goed om te weten dat als je in een theater komt dat een subnetmask hanteert dat afwijkt van de standaard klassen (met andere woorden andere waardes heeft dan 255 of nullen), dat dat geen typfout hoeft te zijn maar een weldoordachte indeling.

**Tot besluit**

Het moge duidelijk zijn dat het aanleggen van een ethernetnetwerk in het geheel niet lijkt op het installeren van een DMX netwerk. Dit komt omdat ethernet ontwikkeld is vanuit kantoorautomatisering. Het voordeel is dat het gemakkelijk te verkrijgen is en er overal mee geëxperimenteerd kan worden. In het volgende artikel leggen we uit hoe verschillende protocollen de DMX-data transporteren en wat de voordelen en nadelen daarvan zijn. ◀