Kennisnet

Handreiking netwerk en wifi in de school

Onmisbare adviezen en achtergrondinformatie bij het laten aanpassen of inrichten van het interne netwerk op school

Laat ict werken **voor het onderwijs**

Inleiding

Veel scholen realiseren zich steeds meer hoe afhankelijk het onderwijs van ict-infrastructuur is geworden. Een belangrijke randvoorwaarde voor het gebruik van digitale leermiddelen en toepassingen in de school is de netwerk-infrastructuur: de tablet van de leerling heeft verbinding met het internet via het interne netwerk. Dit bestaat uit zeer tastbare onderdelen: kabels en apparaten. Toch blijft dit ict-onderdeel voor velen vaak onzichtbaar en abstract. Zolang het netwerk goed functioneert lijkt daar niks mis mee; de leverancier beheert het namelijk. Maar soms voldoet de netwerkinfrastructuur niet (of niet meer) aan wat je school nodig heeft. En zodra je het netwerk wilt uitbreiden, aanpassen of nieuw wilt inrichten, is kennis van de belangrijkste principes en afwegingen noodzakelijk om een goede opdrachtgever te kunnen zijn voor de (te selecteren) leverancier(s) en om elkaar goed te begrijpen.

Deze handreiking biedt die kennis van grofweg gezegd alle technische componenten tussen de internetverbinding en het device van de leerling of leraar. Dit omvat zowel het wifi-netwerk als het vaste (bekabelde) netwerk. Voor meer informatie over de internetverbin-

Er zijn verschillende redenen denkbaar om het intern netwerk van je school aan te passen of op zijn minst tegen het licht te houden. Typische redenen zijn op dit moment:

- Je school gaat (meer) gebruik maken van digitale leermiddelen, een officepakket in de cloud (Office 365 of G Suite for Education) of andere digitale toepassingen. Dit heeft in elk geval impact op de interne servers (minder of geen opslag van toepassingen en bestanden), het netwerkgebruik en de internetverbinding (toegang tot de cloud).
- Je school gaat meer mobiele devices inzetten (van bijvoorbeeld 1 tablet per 5 leerlingen, naar 1 tablet per leerling). Dit heeft in elk geval impact op de internetverbinding en het netwerkgebruik, met name de wifi.
- Je school gaat digitaal toetsen. Dit heeft in elk geval impact op de beveiliging en mogelijk op de (eisen aan) kwaliteit en capaciteit van de internetverbinding.
- Je school gaat het gebouw verbouwen.
- Het netwerk geeft teveel storingen of problemen.

ding zelf is de Handreiking Internetverbinding beschikbaar. De achtergrondinformatie en basiskennis helpen de (bovenschoolse) ict-coördinator en de inkoper in po, vo en mbo een leverancier te selecteren en/of opdracht te verlenen. Deze handreiking bevat ook een inkoopchecklist: een lijst met relevante vragen om jezelf en/of de leverancier te stellen om tot een goede opdrachtformulering te komen.

Al deze kennis en concrete adviezen helpen je school aan een stabiel en toekomstvast intern netwerk en wifi die goed aansluiten bij de situatie en ambities. Daarmee kunnen leerlingen en leraren ongestoord digitale middelen gebruiken in en rondom de klas.

Het interne netwerk in vogelvlucht

De informatie en kennis uit deze handreiking richt zich dus op het interne netwerk: grofweg gezegd alle technische componenten tussen de internetverbinding en het device van de leerling of leraar. Dit omvat zowel het wifi-netwerk als het vaste (bekabelde) netwerk. In de praktijk omvat het interne netwerk de volgende onderdelen:

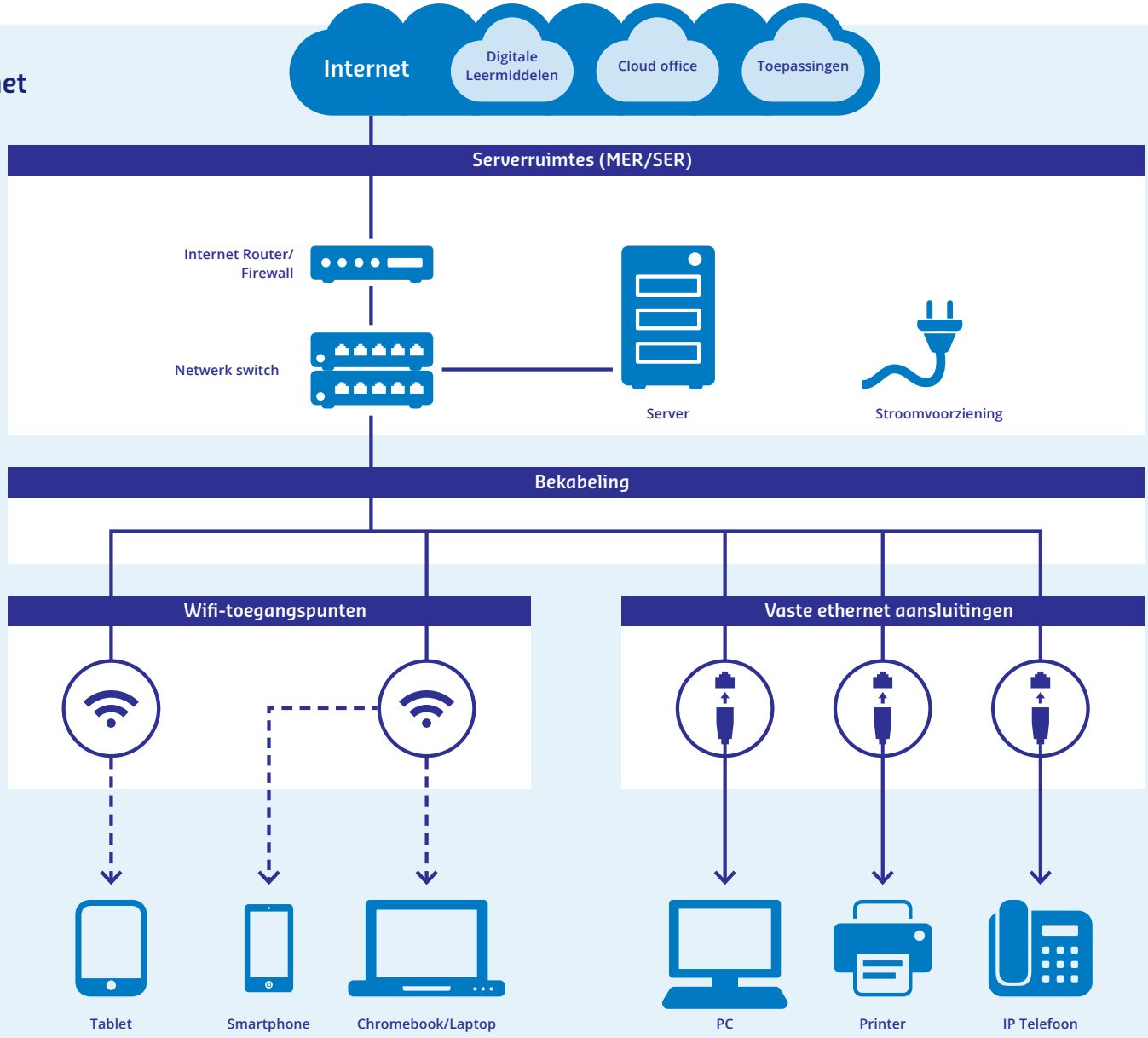
- wifi-toegangspunten (*access points*)
- vaste ethernet netwerkaansluitingen
- bekabeling
- netwerkswitch(es)
- internetmodem/router/firewall (het koppelpunt tussen het interne netwerk en de internetverbinding. Meer informatie over de internetverbinding zelf of de beveiliging daarvan staat in de Handreiking Internetverbinding)
- serverruimte(s) (*MER; main equipment room* en eventueel *SERs; secondary equipment rooms*)
- bijbehorende stroomvoorziening

Al deze aan elkaar gekoppelde componenten samen slaan de brug tussen:

- het internet (waar informatiebronnen, leermiddelen en toepassingen zich in de cloud bevinden)
- alle devices die door leerlingen, leraren en ondersteunende medewerkers gebruikt worden (zoals tablets, desktop pc's, digiborden, printers en IP telefoontoestellen)
- eventuele nog op school aanwezige servers (voor gegevensopslag, toepassingen en/of leermiddelen)

Zie illustratie De componenten van het interne netwerk.

De componenten van het interne netwerk



Inhoudsopgave

Geen netwerk is hetzelfde

Hoewel in de kern elk netwerk op dezelfde manier is opgebouwd, is in de praktijk geen netwerkinfrastructuur hetzelfde. Dat komt omdat verschillende scholen verschillende behoeften hebben, die te maken hebben met het gebouw/de schoollocatie en de visie op digitaal leren.

Het gebouw

De indeling en de constructie van het gebouw leiden tot bepaalde keuzes bij de inrichting van het netwerk. De grootte van het gebouw beïnvloedt het aantal serverruimtes en hun plaats. De dikte van muren en het materiaalgebruik heeft invloed op de inrichting van het wifi-netwerk.

Wanneer je school meerdere gebouwen op de locatie heeft, of zelfs meerdere locaties verspreid door de stad of regio, moet bepaald worden hoe de netwerkinfrastructuur in die gebouwen en locaties aan elkaar verbonden wordt.

Visie op digitaal leren

Hoe intensief het intern netwerk gebruikt moet kunnen worden, is natuurlijk sterk afhankelijk van hoe en hoe vaak digitale leermiddelen en toepassingen in het onderwijsproces gebruikt worden. Dit gebruik kun je grofweg in drie niveaus onderscheiden:

1. Elk lokaal heeft een digibord en een paar pc's. De pc's worden incidenteel en bij toerbeurt gebruikt door leerlingen.
2. Regelmatig werken groepjes leerlingen in de klas of op de gang op gedeelde mobiele devices als een tablet, chromebook of laptop.
3. Elke leerling heeft een of meer persoonlijke mobiele devices en gebruikt die vaak en overal in het gebouw.

Ook maakt het nogal wat uit in welke mate de gebruikte digitale leermiddelen en toepassingen in de cloud staan of op servers in de school en welke plannen je school heeft voor het gebruik van cloud-toepassingen in de toekomst. Het werken in de cloud vraagt een intern netwerk (en internetverbinding) met voldoende capaciteit en betrouwbaarheid.

Vertalen naar de situatie van jouw school

Deze handreiking laat zien hoe bepaalde onderdelen van het netwerk in het algemeen voor scholen ingericht worden. Niet alle theoretisch mogelijke oplossingen en technieken worden beschreven, maar bewezen en toekomstvaste oplossingen met een redelijk gebruiksgemak en redelijke betaalbaarheid. De handreiking helpt je daarmee een beeld te krijgen van wat voor jouw school nodig kan zijn.

Een goede leverancier maakt dat beeld samen met jou concreet door een vertaalslag te maken van de behoeften van je school naar de best passende oplossing. Daarbij moet je voor netwerkcomponenten en wifi uitgaan van de functionaliteit en capaciteit die nodig is voor de komende 5 jaar. Bij het bepalen van de benodigde bekabeling is een termijn van maar liefst 15 jaar reëel. Deze termijnen zijn gebaseerd op een reële economische afschrijvingstermijn en de verwachte technische levensduur. Het helpt om je bij de vertaling naar jouw situatie te laten bijstaan door een ervaren adviseur die onafhankelijk van de leverancier werkt.

Advies

- Ga bij het bepalen van je behoefte aan netwerkcomponenten uit van de situatie van de komende 5 jaar. Voor bekabeling de situatie van de komende 15 jaar.
- Laat je bijstaan door een ervaren, onafhankelijke adviseur.

Basisprincipes in netwerk-infrastructuur

Hedendaagse netwerken zijn opgebouwd in de vorm van een *ster*: alle apparaten zijn met netwerkverbindingen (bedraad of draadloos) aan elkaar verbonden via een centraal knooppunt, de netwerkswitch, zoals de figuur weergeeft. Aangesloten apparaten hebben dus geen directe onderlinge netwerkverbindingen. Ze kunnen wel met elkaar communiceren, maar dit verloopt altijd via de netwerkswitch.
Zie illustratie Het interne netwerk is een ster.

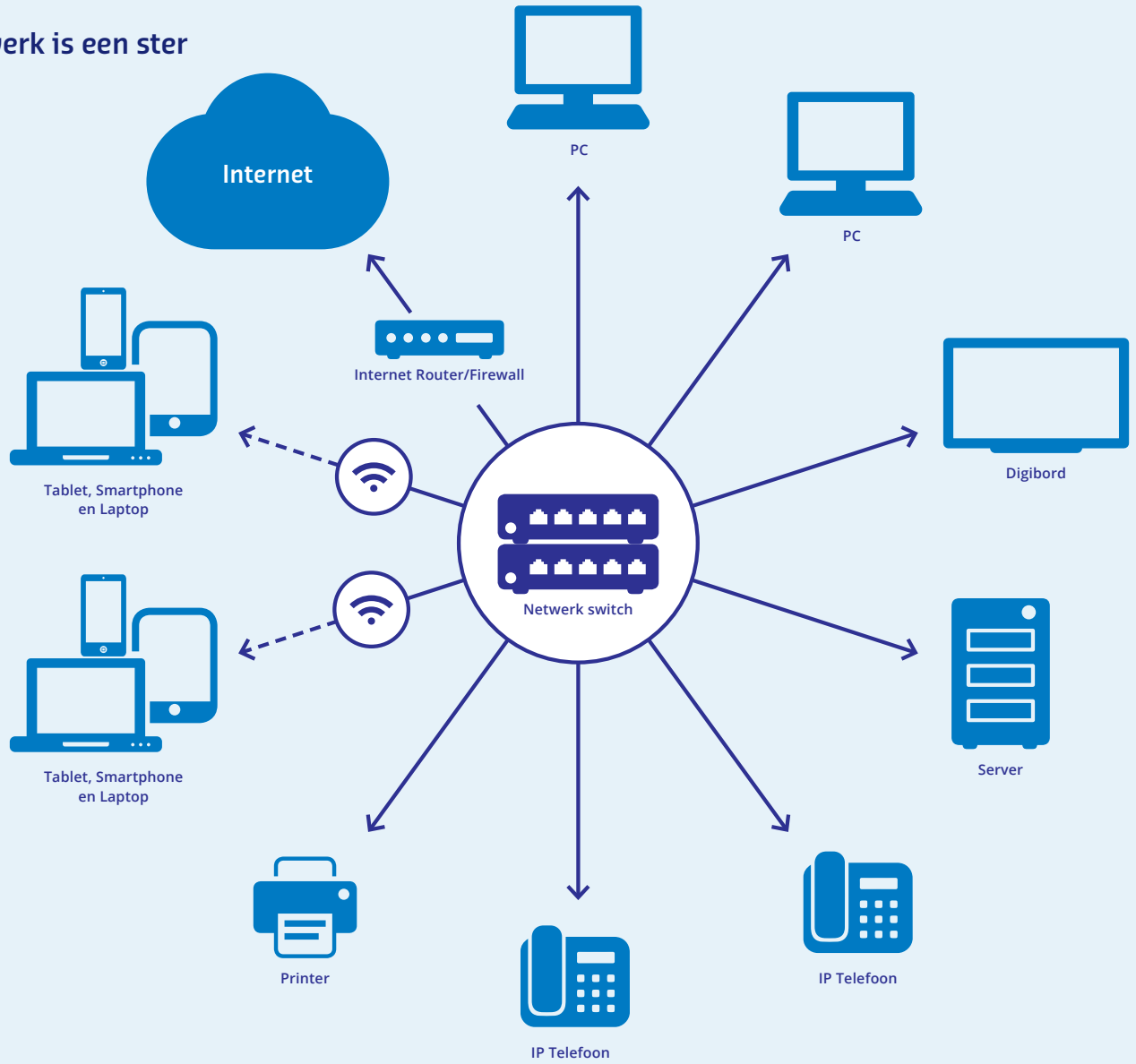
De netwerkswitch vormt dus het hart van het netwerk. Alle apparaten zijn aan het netwerk gekoppeld via een vast aansluitpunt of via wifi. De vaste aansluitpunten in de school (inclusief die van de wifi-toegangspunten) zijn met de bekabeling aangesloten op de netwerkswitch. De switch regelt het netwerkverkeer tussen alle apparaten die op die aansluitpunten zijn aangesloten en naar het internet of de servers in de school.

Het interne netwerk wordt ook wel *LAN* (*Local Area Network*) genoemd. Ook worden termen als *WAN* (*Wide Area Network*) en *MAN* (*Metropolitan Area Network*) gebruikt om netwerken aan te duiden die zich over meerdere (geografisch gescheiden) gebouwen uitstrekken.

Basistechnieken van moderne netwerken

Het interne netwerk maakt gebruik van *Ethernet* en *IP*. Dit zijn technische standaarden die aan de basis staan van de hedendaagse netwerktechnologie. Ethernet regelt de verbindingen apparaten in de school. Het *Internet Protocol* (*IP*) vormt de basis voor het internet en zorgt ervoor dat gegevens over alle schakels in een verbinding op hun plaats van bestemming komen, bijvoorbeeld vanaf een website tot op de tablet of laptop van de leerling.

Het interne netwerk is een ster



Daarnaast is er een breed scala aan aanvullende technieken die de veiligheid, de werking en het beheer van het interne netwerk zodanig verbeteren dat deze in een modern netwerk niet mogen ontbreken.

Moderne netwerkswitches kunnen via de netwerkkabel ook stroom leveren aan aangesloten apparaten zoals wifi-toegangspunten en IP-telefoons. Deze techniek heet *inline power* of ook wel *Power over Ethernet (PoE)*. Dit maakt aparte stroomadapters, snoeren en stopcontacten voor wifi-toegangspunten en IP-telefoons overbodig. Dit scheelt in installatiekosten en storingen en dat kan de iets hogere prijs van apparatuur met PoE rechtvaardigen. Voor deze techniek bestaan twee versies: de oude versie 802.3af en de toekomstvastere versie 802.3at (ook soms *PoE+* genoemd). Zorg in ieder geval dat de switches en alle apparaten die van PoE gebruik maken, dezelfde standaard ondersteunen. De consequenties voor de bekabeling worden in dat betreffende hoofdstuk beschreven.

Advies

- Laat de stroomvoorziening voor wifi-toegangspunten en IP-telefoons via het netwerk verlopen (PoE).
- Zorg voor netwerkswitches (en apparatuur) die dezelfde versie van de standaard voor PoE ondersteunen, bij voorkeur 802.3at.

Er zijn technieken om in moderne netwerken belangrijk (bedrijfskritisch) netwerkverkeer prioriteit te geven boven niet-kritische toepassingen als bijvoorbeeld sociale media. Bij grote belasting (bij veel gebruik) kunnen toepassingen die voor je school het belangrijkst zijn zo lang mogelijk voldoende bandbreedte krijgen om goed te kunnen blijven werken. De niet-kritische toepassingen krijgen minder bandbreedte en zullen dan dus vertragen. Deze techniek heet *Quality of Service (QoS)*, tegenwoordig ook wel aangeduid met *DiffServ*. Een vergelijkbare techniek, maar met een iets ander werkingsprincipe, heet *Class of Service (CoS)*.

Vaak krijgt realtime netwerkverkeer zoals telefonie voorrang boven dataverkeer zoals bestandsuitwisseling en krijgen onderwijstoepassingen voorrang boven het recreatief internetverkeer van leerlingen. Voordeel van dit mechanisme is dat de bandbreedte van het netwerk en met name de internetverbinding niet op de maximale potentiële belasting ingericht hoeft te worden. Dit bespaart kosten. Het onderscheid tussen een onderwijstoepassing en recreatief internetgebruik is wel lastig te maken.

Advies

- Zorg dat alle netwerkswitches QoS, DiffServ en CoS ondersteunen.
- Bepaal welke toepassingen kritisch zijn en prioriteit zouden moeten krijgen.
- Stel de QoS en CoS in op de netwerkswitches.

De QoS en CoS instellingen worden in de praktijk niet per netwerkapparaat ingesteld, maar op het niveau van een *VLAN (Virtual LAN)*. Een VLAN is een groep apparaten die op het netwerk is aangesloten met aparte instellingen ten aanzien van snelheid, beveiliging en bedrijfszekerheid. Een 'netwerk binnen een netwerk' als het ware. Zo kan bijvoorbeeld eenvoudig aan leraren en stafmedewerkers andere instellingen geboden worden dan aan leerlingen of kan de afhandeling van alle IP-telefonie gescheiden worden van het andere verkeer. Als onbekende apparaten die zich op het netwerk aanmelden automatisch aan een bepaalde VLAN worden toegewezen is sprake van een dynamisch VLAN. Hiervoor is ondersteuning van de 802.1x standaard nodig. Dit principe wordt bijvoorbeeld toegepast bij gast-accounts, waarmee via het netwerk alleen internet bereikt kan worden.

Advies

- Zorg dat VLAN's ondersteund worden in het netwerk, alsmede dynamische VLAN's volgens de 802.1X standaard.

Eigenlijk mogen ook de volgende technieken niet ontbreken in een modern netwerk. Het voert voor dit document te ver om ze uitgebreid toe te lichten:

- Met *autosensing/autonegotiation* stemmen netwerkcomponenten onderling hun instellingen af. Voor oudere apparaten zijn daarvoor handmatige instelmogelijkheden op de switch noodzakelijk.
- *IPv6* is de opvolger van de alomtegenwoordige IPv4 en maakt het mogelijk om meer apparaten te kunnen adresseren. Het wereldwijde gebruik van IPv6 groeit weliswaar slechts langzaam, maar zonder deze techniek zijn componenten niet toekomstvast. Deze technieken kunnen door elkaar in één netwerk worden gebruikt.
- Een techniek als *multicast* helpt het netwerk efficiënter te benutten
- Het *OSPF (Open Shortest Path First)* protocol laat netwerkswitches efficiënter met elkaar samenwerken.
- Om het netwerk centraal te kunnen beheren (of dit te kunnen uitbesteden) is het van belang dat de technische standaard *SNMPv3 (Simple Network Management Protocol)* door alle componenten ondersteund wordt.
- *Link aggregation of channeling* is een techniek om netwerkswitches in staat te stellen met hogere bandbreedtes met elkaar te communiceren.
- Ondersteuning van *half duplex* instellingen kan nodig zijn voor inpassing van oudere netwerkapparaten die niet gelijktijdig kunnen zenden en ontvangen.

Advies

- Zorg dat alle netwerkcomponenten autosensing/autonegotiation, multicast en SNMPv3 ondersteunen.
- Zorg dat de netwerkswitches OSPF, IPv6, half duplex en link aggregation ondersteunen.

Redundantie

Wanneer een vast aansluitpunt defect raakt, zal de rest van het interne netwerk blijven functioneren. Een dergelijke storing heeft alleen impact op de gebruiker van die ene pc die op dat aansluitpunt is aangesloten. Anders is het al als er een printer op is aangesloten, of een wifi-toegangspunt, waar immers meerdere mobiele devices tegelijkertijd mee verbonden kunnen zijn. Nog erger wordt het natuurlijk als de netwerkswitch, internetverbinding of stroomvoorziening uitvalt. Sommige storingen kunnen dus grote impact hebben op leraren en leerlingen. En hoe belangrijker het gebruik van digitale leermiddelen en toepassingen is voor het onderwijs op je school, hoe belangrijker het is om weerbaarder te zijn tegen uitval door storingen. Dat doe je door de belangrijkste delen van het netwerk dubbel uit te voeren. Dit principe heet redundantie. Redundantie creëert bedrijfszekerheid, maar is ook kostbaar. Daarom is het van belang om naast het storingsrisico ook mee te wegen welke impact een storing zou hebben en welke investeringen in redundante voorzieningen dit rechtvaardigt.

Snelheid en bandbreedte

Een verbinding tussen apparaten op het interne netwerk of met het internet kent een bepaalde snelheid: de hoeveelheid gegevens die verstuurd kunnen worden binnen een bepaalde tijd. Die snelheid - ook wel bandbreedte genoemd - wordt uitgedrukt in Megabits per seconde (Mbps) of Gigabits per seconde (Gbps), waarbij 1 Gbps gelijk is aan 1000 Mbps. Alle componenten in het interne netwerk hebben een bepaalde maximale bandbreedte en het component met de laagste snelheid bepaalt de snelheid van de totale verbinding. Snelheden variëren in de praktijk van de 54 Mbps van een basis wifi-ontvanger (802.11g-standaard) in een tablet tot netwerkswitches van 1 of 10 Gbps.

Omdat centrale componenten (zoals bijvoorbeeld de centrale netwerkswitch) meer gebruikers tegelijkertijd voldoende snelheid moet kunnen bieden, zijn die doorgaans uitgerust met een grotere bandbreedte dan componenten die dichter bij de gebruiker staan (zoals de vaste netwerkaansluiting of het wifi-toegangspunt). Meer hierover in het hoofdstuk Inschattingshulp capaciteit.

Serverruimtes

De plek voor centrale onderdelen van de netwerkinfrastructuur

In de hoofdserverruimte *(main equipment room of MER)* staan alle centrale onderdelen van de netwerkinfrastructuur van de school. Een MER is in de eerste plaats het punt waar alle bekabeling die in de school aanwezig is met elkaar wordt verbonden, zodat er daadwerkelijk sprake is van een netwerk. Het is de voordehandliggende plaats voor servers voor bestandsopslag en toepassingen en idealiter ook de plek waar de internetprovider de internetmodem/router/firewall plaatst, zodat deze efficiënt gekoppeld kunnen worden aan de netwerkinfrastructuur.

In de praktijk zal een grotere school behoefte hebben aan meerdere plekken waar bekabeling met elkaar wordt verbonden. Dergelijke decentrale switches horen in een nevencomputerruimte *(satellite equipment room of SER)* geplaatst te worden, om de betrouwbaarheid en beheersbaarheid van het netwerk te kunnen garanderen. Meer redenen en omstandigheden voor nevencomputerruimtes worden uitgewerkt in het hoofdstuk Een groot gebouw, gedeeld gebouw of meer schoollocaties.

Switches met aangesloten bekabeling

Netwerkswitch

De functie van de netwerkswitch - het hart van het netwerk - is in het vorige hoofdstuk al toegelicht. Gezien het belang van de switch is dit bij uitstek een onderdeel dat zo weinig mogelijk of zelfs helemaal niet mag uitvallen. Het is belangrijk hierover goede beschikbaarheids-garanties af te spreken met de leverancier. Overweeg - zeker als digitaal leren belangrijk is voor je school - om de netwerkswitch redundant uit te voeren.

Advies

- Vraag de leverancier hoge beschikbaarheidsgaranties voor de netwerkswitch.
- Overweeg om de switch redundant uit te voeren.

Daarnaast is het van belang dat de netwerkswitch voldoende aansluitmogelijkheden (poorten) heeft voor alle apparaten die erop aangesloten moeten kunnen worden (dus de internetmodem/router/firewall, eventuele servers, alle netwerkaansluitpunten, alle wifi-toegangspunten en alle IP-telefoons). Houdt daarbij rekening met een maximale bezetting van 80%, zodat toekomstige uitbreiding nog mogelijk is. Dat kan ook door flexibel schaalbare netwerk-switches te gebruiken. De zogeheten *box-levelsystemen* zijn zelf-standig te gebruiken netwerkswitches die aan elkaar te verbinden zijn (*stacking* genaamd) als ware het één switch met veel poorten. Ook zijn er *modulaire switches* waar later extra poorten aan kunnen worden toegevoegd.

Vanzelfsprekend is de snelheid van de switch erg bepalend voor de prestaties van het totale netwerk. Hierover is meer informatie te vinden in het hoofdstuk over capaciteit, paragraaf Benodigde bandbreedte.

Wanneer meerdere serverruimtes (MER's en SER's) met elkaar verbonden worden, dan dienen de betreffende netwerkswitches glasvezelaansluitingen te hebben. Meer hierover in het hoofdstuk Een groot gebouw, gedeeld gebouw of meer schoollocaties.

Advies

- Zorg dat de poorten van de netwerkswitch bij aanvang tot maximaal 80% in gebruik zijn.
- Overweeg schaalbare netwerkswitches te gebruiken (stacking of modulair).
- Zorg dat de netwerkswitch glasvezelaansluitingen heeft indien je school meerdere serverruimtes heeft.

Servers

Steeds meer scholen gebruiken de cloud voor office-toepassingen en bestandsopslag. De meeste digitale leermiddelen werken inmiddels in de cloud. Toch kan het zijn dat je school nog eigen (lokale) servers heeft voor bestandsopslag, als AD/domaincontroller en/of voor specifieke toepassingen. Indien het niet mogelijk is om die servers te migreren naar de cloud, dan is de MER hun meest logische plek vanwege eenvoudiger beheer en beveiliging.

Advies

- Plaats servers alleen in de MER.

Stroomvoorziening

Alle apparaten in de MER gebruiken stroom. Wanneer de stroom van één stroomgroep uitvalt (bijvoorbeeld door kortsluiting), zullen alle apparaten die op die stroomgroep zijn aangesloten ook uitvallen. Daarom is het zinvol te overwegen in de MER meerdere stroomgroepen te gebruiken. Sommige netwerkswitches bevatten twee (soms zelfs drie) voedingen. Wanneer deze ook daadwerkelijk op verschillende stroomgroepen aangesloten zijn, blijft de switch operationeel als er één stroomgroep uitvalt.

Advies

- Overweeg aparte stroomgroepen aan te leggen in de serverruimte.
- Sluit de centrale netwerkswitch als deze meerdere voedingen heeft ook op aparte stroomgroepen aan.

Om nog beter beschermd te zijn tegen stroomuitval is het gebruik van een *no-break system* ofwel *Uninterruptable Power Supply (UPS)* een mogelijkheid. Deze systemen leveren de aangesloten apparaten batterijstroom bij stroomuitval. De systemen verschillen in vermogen en reactiesnelheid (enkele milliseconden tot gegarandeerd 0 seconden). Een UPS kan de apparatuur die er op is aangesloten een beperkte tijd van stroom voorzien (typisch 10 tot 15 minuten).

Die tijd is bedoeld om de normale stroomvoorziening weer in te schakelen of om de eventuele servers volgens voorschrift af te sluiten om gegevensverlies te voorkomen (dit laatste risico speelt niet bij netwerkapparatuur).

Advies

- Overweeg een no-break system of UPS, zeker bij eventuele servers.

Patchpanel en computervloer

In een serverruimte komen vaak veel netwerkkabels bij elkaar. Om deze makkelijk te kunnen aanleggen en toekomstige aanpassingen makkelijker te kunnen doorvoeren, is het slim te overwegen om een verhoogde computervloer en een patchpanel aan te leggen.

Een *patchpanel* is een verdeelkast waar alle inkomende netwerk-kabels geordend kunnen worden verbonden met de netwerkswitch en/of andere apparatuur. Soms wordt een serverruimte waar alleen een patchpanel en een netwerkswitch in zijn ondergebracht ook wel een *patchkast* genoemd. Dit is dus iets anders dan een patchpanel.

Advies

- Overweeg de MER uit te rusten met een verhoogde computervloer en een patchpanel.

Overige aandachtspunten

Om storingen te voorkomen, de levensduur van apparatuur te verlengen en de brandveiligheid in het gebouw te vergroten, helpt het als:

- temperatuur en vochtigheid in de MER beheerst kunnen worden met klimaatconditionering, met name als er belangrijke lokale servers opgesteld staan
- er een brandblusinstallatie voorhanden is, met name bij grotere MER's met veel apparatuur
- apparatuur en bekabeling goed geaard is, met name in verband met brandveiligheid

Advies

- Overweeg de MER uit te rusten met klimaatconditionering, brandblusinstallatie en goede aarding, afhankelijk van het aantal en het soort apparatuur in de MER.

Aansluiting op de internetverbinding: de internetmodem/router met firewall

Een internetmodem/router staat in beginsel in de serverruimte en verbindt het schoolnetwerk met het internet. Daarvoor is een contract nodig met een internetprovider. De internetmodem/router zelf is niet altijd onderdeel van het aanbod van de zakelijke internetprovider. Deze paragraaf beschrijft de werking van de internetmodem/router en de plaatsing ervan in het interne netwerk. Meer informatie over de internetverbinding zelf, of de beveiliging daarvan is te vinden in de Handreiking Internetverbinding.

Advies

- Zorg dat de internetmodem/router voldoet aan de eisen die de internetprovider er aan stelt.
- Plaats de internetmodem/router in de serverruimte.

Een firewall filtert het verkeer tussen het internet en het schoolnetwerk om gebruik van bepaalde internettoepassingen tegen te gaan (zoals torrent of Netflix) of om ongeautoriseerde toegang tot het schoolnetwerk vanaf het internet te belemmeren. Een firewall is dus essentieel voor veilige internettoegang. Soms biedt de internetprovider een uitgebreide firewall-functie. De rol van de internetmodem/router blijft in dat geval beperkt tot doorsturen (*routeren*).

Wanneer de internetprovider geen firewall-dienst levert, dan zal deze functie ingericht moeten worden op de internetmodem/router op school of in eigen gespecialiseerde firewall-apparatuur. De firewall-functie van de internetmodem/router is vaak een basale instelling (*port blocking* genaamd) die bepaalt welk soort internetverkeer is toegestaan, zoals bijvoorbeeld het verkeer tussen een website en een webbrowser.

De firewall kan zo ingericht worden, dat het mogelijk is om servers die in de serverruimte aanwezig zijn, ook van buiten de school - via het internet - te benaderen, zonder de rest van het interne netwerk openbaar te maken. Dit kan nodig zijn voor thuiswerkende medewerkers en leerlingen die gebruik maken van een toepassing die niet in de cloud werkt, of voor de ict-dienstverlener die jullie systemen op afstand beheert. Met de firewall kan daartoe een zogeheten *DMZ (demilitarized zone)* ingericht worden. Ook zijn hiervoor vaste IP-adressen nodig van de internetprovider.

Advies

- Zorg dat de firewall-functie altijd is ingericht. Ofwel bij de internetprovider, op gespecialiseerde firewall-apparatuur of op de eigen internetmodem/router (als de eisen aan filtering bescheiden zijn).

Hoe belangrijker de toegang tot internet is voor de onderwijsprocessen en de administratieve processen op jullie school, hoe belangrijker het is dat die toegang ook gegarandeerd is. Dit stelt eisen aan de beschikbaarheid van de internetverbinding. Die beschikbaarheid is te vergroten door:

- een beschikbaarheidsgarantie of maximale hersteltijd af te spreken met de internetprovider.
- de enkelvoudige vaste aansluiting te combineren met een minder snelle en/of mobiele verbinding die als achtervang kan dienen in geval van calamiteiten.
- een redundante internetverbinding door bijvoorbeeld twee verschillende aansluitingen op twee verschillende plaatsen in het gebouw te laten aanleggen.

Deze maatregelen lopen op in effect, maar ook in benodigde investering. Het kan zijn dat de internetprovider om een hoge beschikbaarheidsgarantie te bieden ook een van die andere maatregelen voorschrijft.

Advies

- Zorg voor de internetverbinding voor goede beschikbaarheidsgaranties, een achtervang of een redundante aansluiting, afhankelijk van het belang van internetgebruik in het onderwijsproces.

Sommige modem/router-apparaten, veelal meegeleverd bij consumentenverbindingen, kunnen ook werken als wifi-toegangspunt. De capaciteit, dekking en kwaliteit van dergelijke wifi-functionaliteit is niet geschikt voor gebruik in een school en verhoogt bovendien de kans op verstoringen en beveiligingsincidenten op de internetverbinding.

Advies

- Schakel eventuele wifi-functionaliteit op de internet-modem/router uit.

Bekabeling en vaste aansluitpunten

Ook al is het gebruik van mobiele devices als tablets en laptops in scholen toegenomen, bekabeling blijft de ruggengraat van het interne netwerk. Dat is in de eerste plaats omdat alle wifi-toegangspunten, waar de mobiele devices contact mee maken, via bekabeling zijn aangesloten op de netwerkswitch. Maar ook apparaten als printers, digiborden, IP-telefoons zijn veelal op het netwerk aangesloten via een kabel. Ook de serverruimtes in de school zijn onderling verbonden via bekabeling. Veel van de minder voor de hand liggende apparaten als bewakingscamera's of het kassasysteem in de kantine kunnen of moeten ook werken via netwerkbekabeling. Omdat bekabeling potentieel hogere snelheden en minder storing geeft dan draadloze verbindingen, geldt als motto: 'bedraad waar het gaat'.

Bekabeling en aansluitpunten worden gezien als onderdeel van het gebouw en worden vaak door andere leveranciers aangelegd en beheerd dan de overige delen van het interne netwerk (ook wel de actieve componenten genoemd).

Advies

- Bedraad waar het gaat.
- Spreek een duidelijk afbakening af tussen de installateur van de bekabeling en de leverancier van actieve componenten als het gaat om de verantwoordelijkheden bij beheer en storingsafhandeling.

Soorten bekabeling: koper versus glas

Er worden in netwerkinfrastructuur twee soorten bekabeling gebruikt: met een koperen kern (met een elektrisch signaal) en met een glasvezelkern (met een optisch signaal). Beide soorten bekabeling kunnen inmiddels snelheden van 10 Gbps aan. De verschillen tussen koper en glas die voor het interne netwerk relevant zijn, liggen dan ook op andere vlakken:

koper	glas
gebruikt om vaste aansluitpunten te verbinden met de netwerkswitch (of het patchpanel) in de dichtstbijzijnde serverruimte	gebruikt om de serverruimtes onderling met elkaar te verbinden
gevoelig voor elektromagnetische storing, met name bij langere afstanden	ongevoelig voor elektromagnetische storing
kabellengte beperkt tot 90 meter (via de kabelgoot gemeten, niet hemelsbreed)*	veel langere kabellengtes mogelijk**
Lage aanlegkosten	Hoge aanlegkosten

* zelfs maar 55 meter bij 10 Gbps.

** de exacte maximale kabellengte van glasvezel is afhankelijk van de gekozen toepassing en techniek, waarover later meer

Advies

- Gebruik tussen de serverruimte en de vaste aansluitingen koper. Gebruik tussen serverruimtes binnen en tussen gebouwen glasvezel.

Meer over koperbekabeling

Netwerkbekabeling met een koperen kern noemen we ook wel *twisted pair*. De kabel bestaat uit acht aders, die in tweetallen om elkaar heen gedraaid zijn. De meest gebruikte soort is UTP (*unshielded twisted pair*) en daarom wordt koperbekabeling vaak aangeduid met UTP. Andere varianten als STP, FTP en SFTP zijn duurder en komen alleen voor in omgevingen waar grote kans is op elektromagnetische instraling van de kabel.

Een losse, niet afgemonteerde twisted pair-kabel heeft aan beide uiteinden een RJ-45 stekker (*removable jack type 45*). Wanneer de kabel gebruikt wordt tussen het patchpanel en een vast aansluitpunt is deze vast aan het aansluitpunt afgemonteerd (dus zonder stekker). Gangbare vaste aansluitpunten hebben twee aansluitpunten gecombineerd in één paneeltje, van waarachter dus ook twee aparte kabels naar het patchpanel kunnen lopen.

RJ-45 stekkers

Twee vaste aansluitpunten in één paneel

De kwaliteit van een twisted pair-kabel varieert in de snelheid die er betrouwbaar mee over 100 meter gehaald kan worden. Die kwaliteit wordt aangeduid met de term CAT en varieert van 10 Mbps (CAT3; verouderd), 100 Mbps (CAT5), 1 Gbps (CAT5E en CAT6) en 10 Gbps (CAT 6A over de gehele lengte en bij CAT6 maar tot 55 meter). CAT6A is het minst storingsgevoelig en wordt op dit moment het meest nieuw aangelegd. CAT7 bestaat ook, maar is kostbaar en lijkt voor de komende tien jaar niet nodig voor scholen. Een recente ontwikkeling is de NBASE-T ethernet standaard, waarmee op bestaande oudere bekabeling ook hogere snelheden bereikt kunnen worden (op CAT5E 2,5 Gbps en op CAT6 (geen A) 5 Gbps). Voor gebruik van Power over Ethernet (PoE) is minimaal CAT5E nodig en wordt CAT6A aanbevolen.

Bij het ontwerpen van netwerken wordt overigens niet uitgegaan van een maximale UTP-kabellengte van 100 meter, maar van 90 meter. Die lengte wordt gerekend vanaf het vaste aansluitpunt aan de muur tot aan het patchpanel in de serverruimte. Van daaruit lopen immers nog korte kabels naar bijvoorbeeld de pc aan de ene kant en de netwerkswitch aan de andere.

Wanneer er in de kabelgoten behalve netwerkkabels ook 240V-stroomkabels lopen, is het verplicht om een metalen scheidingsschot te gebruiken tussen het netwerkdeel en het stroomdeel om elektromagnetische storing te voorkomen. Dit is een voorwaarde voor certificatie van het netwerk en leveranciersgarantie op de actieve netwerkcomponenten.

Advies

- Gebruik voor nieuwe installaties en uitbreidingen altijd UTP CAT6A.
- Hergebruik van eventueel al geïnstalleerde UTP CAT5E kabels is mogelijk, mits de kabels nog in goede staat zijn. De leverancier kan dit doormeten. Hergebruik van UTP CAT3 kabels kan ook als geen Power over Ethernet (PoE) nodig is, maar het wordt aangeraden deze kabels bij de eerste gelegenheid te vervangen.
- Rust kabelgoten waar zowel stroomkabels als koperen netwerkkabels doorheen lopen altijd uit met metalen scheidingsschot.

Meer over glasvezelbekabeling

Om een glasvezelverbinding tot stand te brengen zijn altijd twee vezels (een glasvezelpaar) nodig: een voor het dataverkeer heen en een voor het dataverkeer terug. Eén glasvezelkabel bevat meerdere vezels, veelal 12, 24, 48 of 96 stuks (6, 12, 24 of 48 vezelparen), en kan dus voor meerdere verbindingen gebruikt worden.

Glasvezelkabel bestaat in twee typen die van elkaar verschillen in de maximaal overbrugbare afstand: MMF (*Multi Mode Fiber*), dat doorgaans binnen gebouwen ingezet wordt en SMF (*Single Mode Fiber*), dat doorgaans tussen gebouwen gebruikt wordt.

MMF is in vier kwaliteiten beschikbaar (OM1 t/m OM4). Deze zijn allemaal geschikt om bij snelheden van 100 Mbps afstanden van 300 tot 2000 meter te bereiken. Wordt de snelheid hoger en/of de kabelkwaliteit lager, dan daalt de maximaal overbrugbare afstand. OM1 haalt met 10 Gbps nog maar een maximale afstand van 33 tot 220 meter. OM3 en OM4 (beiden ook wel aangeduid als *LOMMF*) halen op die snelheid gegarandeerd 220 meter en OM4 zelfs maximaal 550 meter. Voor Gigabit netwerken wordt daarom OM3 en OM4 aanbevolen.

Bij SMF is redelijkerwijs maar één kabelkwaliteit relevant (OS1). Daarmee bereik je minimaal afstanden van 10 km (met snelheden van minimaal 1 Gbps) maar veel grotere afstanden (en hogere snelheden) zijn zeker ook mogelijk. SMF is veel duurder dan MMF.

Een glasvezelkabel heeft meestal een LC-stekker (*Lampert Connector*), maar soms een SC-stekker (*Subscriber Connector*) of nog minder vaak voorkomende typen. Het stekkertype aan de kabel moet corresponderen met het aansluitingstype op de netwerkswitch of via een verloopkabel worden aangepast.

Advies

- Gebruik voor inpandige glasvezelkabel type MMF.
- Gebruik voor glasvezelkabel buiten type MMF. Gebruik type SMF alleen als de afstand dat vergt.
- Gebruik glasvezel met LC connectoren.

LC-stekker (bovenaan) en twee SC-stekkers (onderaan)

Wifi

Het deel van het interne netwerk dat draadloos werkt, het wifi-netwerk, is net zo belangrijk als het gebruik van mobiele devices voor de school is. Het wifi-netwerk kan niet zonder een goed bedraad netwerk: wifi-toegangspunten (ook wel *access points* genoemd) zijn via een netwerkkabel aangesloten op de netwerkswitch. Door via een radiosignaal contact te maken met het dichtstbijzijnde toegangspunt, wordt een mobiel device aangesloten op het netwerk. In tegenstelling tot een vast netwerkaansluitpunt kan een wifi-toegangspunt meerdere devices met het netwerk verbinden. Dit aantal kan oplopen tot boven de honderd, maar dit heeft wel effect op de snelheid. De totale beschikbare bandbreedte van het toegangspunt tot aan de netwerkswitch in de serverruimte moet immers gedeeld worden.

In het algemeen geldt dat een wifi-verbinding minder snel en minder betrouwbaar is dan een bedrade netwerkaansluiting. Met de nieuwste technische wifi-standaard (802.11ac wave 2) is onder optimale omstandigheden een snelheid van 2,34 Gbps haalbaar, maar niet alle devices ondersteunen dit al. Daarom is achterwaartse compatibiliteit (*backwards compatibility* - ondersteuning van de oudere standaarden 802.11g, 802.11b, 802.11n en 802.11a) belangrijk. Wanneer je school oudere devices heeft en/of een BYOD (*Bring-Your-Own-Device*) beleid kent, is een brede ondersteuning van oudere wifi-standaarden essentieel.

Deze standaarden richten zich op de verbinding tussen het wifi-toegangspunt en de mobiele devices. In de praktijk gebruiken fabrikanten van wifi-apparatuur ook eigen protocollen om wifi-apparatuur onderling te laten samenwerken. Daarom kun je in de praktijk geen apparatuur van verschillende leveranciers in één wifi-netwerk combineren.

Wifi werkt op basis van radiosignalen die via verschillende kanalen (vergelijkbaar met die van de traditionele radio) verstuurd worden. Elk toegangspunt werkt op een eigen kanaal. De signalen kunnen verstoord raken als dichtbij gelegen andere toegangspunten ook datzelfde kanaal gebruiken. Hierdoor kunnen lagere snelheden en haperingen optreden, vooral als gebruik gemaakt wordt van de gangbare 2,4 GHz-band, omdat daarin vooral elkaar overlappende kanalen beschikbaar zijn. De nieuwe 5 GHz-band (beschikbaar in standaarden 802.11a, 802.11n en 802.11ac) ondersteunt veel meer kanalen die niet overlappen, waardoor dit probleem minder speelt.

Een praktisch probleem bij het gebruik van oudere wifi devices is dat deze veel tijd op de kanalen gebruiken en daarmee het verkeer voor snellere apparaten kunnen verstoren. Dat is een reden om aan de terugwaartse compatibiliteit ook grenzen te stellen. Ook is het zinvol om de wifi-kanalen niet te laten benutten voor devices die evengoed via een vaste netwerkaansluiting aangesloten hadden kunnen worden (in hoofdstuk Bekabeling en vaste aansluitpunten wordt meer gezegd over dit 'bedraad waar het gaat'-principe).

Advies

- Zorg dat nieuwe wifi-netwerken de 802.11ac wave 2 standaard ondersteunen en kunnen werken met 2,4 GHz en 5 GHz.
- Zorg dat oudere wifi standaarden ook ondersteund worden, zeker als oudere devices ondersteund moeten worden en/of er een BYOD beleid is.
- Gebruik wifi-apparatuur van één fabrikant.

Voldoende dekking met minimale straling

Om een goede werking van het wifi-netwerk te hebben is het in de eerste plaats belangrijk dat er voldoende toegangspunten zijn op die plekken waar het meest gebruikt gemaakt zal worden van mobiele devices. Voor de ene school is dat vooral in de klas, voor de andere school is dat juist op het leerplein of in de aula.

Zonder belemmeringen (met een 'vrije zichtverbinding' door de lucht) is de maximale afstand van een device tot aan het wifi-toegangspunt ongeveer 50 meter. Belemmeringen zoals meubilair en muren verlagen die afstand. Het soort materiaal en de dikte van die obstakels zijn van grote invloed op hoe ver een draadloos signaal van een toegangspunt daadwerkelijk reikt. Demping van het signaal is bij de 5 GHz-band sterker dan bij de 2,4 GHz-band.

Vanwege de fysieke belemmeringen kan het nodig zijn op bepaalde plaatsen (extra) toegangspunten te installeren. Ook redundantie kan daarvoor een reden zijn. Een storing in één toegangspunt kan immers eenvoudig worden opgevangen door omliggende toegangspunten. Vanzelfsprekend leidt het verhogen van het aantal toegangspunten ook tot verhoging van kosten.

In de tweede plaats, naast het aantal toegangspunten, is de signaalsterkte ook van belang voor een goede werking van het wifi-netwerk: hoe krachtiger een toegangspunt uitzendt, hoe verder het signaal reikt (en hoe makkelijker het door obstakels heen gaat).

Er zijn echter twee redenen om de signaalsterkte te beperken:

1. Hoe krachtiger het signaal, hoe groter de kans dat signalen van andere, verder gelegen toegangspunten die hetzelfde kanaal gebruiken elkaar gaan verstoren;
2. Stralingsoverlast is een actueel thema. Het Kennisplatform EMV beschrijft in hun artikel Omgaan met Wi-Fi op scholen een stralingsrichtlijn voor scholen waarbij uitgegaan wordt van een zo zwak mogelijk radiosignaal. Bij de inschattingshulp voor de capaciteit verderop in deze handreiking, wordt van die richtlijn uitgegaan. In het algemeen is een radiosterkte van -65 dBm afdoende voor een betrouwbaar gebruik. Op sommige plaatsen in de school (met intensief gebruik) kan de sterkte eventueel verhoogd worden. Bij licht tot zeer licht wifi-gebruik is een sterkte tot -85 dBm voldoende.

Een *site-survey* meet storingsbronnen en de verspreiding van het signaal in het gebouw, zodat daar bij het plaatsen van toegangspunten rekening mee gehouden kan worden.

Advies

- Zorg dat het aantal toegangspunten en hun signaalsterkte niet alleen gebaseerd is op hoge dekking en signaalkwaliteit, maar ook op lage kosten en stralingsoverlast.
- Stel de signaalsterkte in beginsel niet hoger dan -65 dBm, tenzij het gebruik daar echt om vraagt. Op plekken met zeer licht wifi-gebruik is -85 dBm voldoende.
- Laat de leverancier met een site survey storingsbronnen en signaal-belemmeringen identificeren om daarop de plaatsing van de toegangspunten te kunnen baseren.

Wifi-toegangspunt

Beveiliging

Omdat het wifi-netwerk draadloos werkt, is extra beveiliging nodig om afluisteren en andere vormen van misbruik tegen te gaan.
De minimale maatregel is het gebruik van encryptie. Hierdoor wordt het netwerkverkeer versleuteld en is het niet langer leesbaar voor afluisteraars. De encryptiestandaarden *WPA/WPA2* zijn hiervoor gangbaar en worden aanbevolen. Oudere standaarden gebruiken zwakkere encryptie en zijn eenvoudig te ontcijferen.

De volgende maatregelen zijn daar goede aanvullingen op:

- Kwaadwillende personen kunnen valse wifi-toegangspunten plaatsen (*rogue access points*) die zich voordoen alsof ze onderdeel zijn van het netwerk. Op die manier kan aan gebruikers informatie ontfutseld worden of kan het netwerk verstoord raken. Een modern wifi-netwerk herkent dit probleem en bestrijdt het actief (*rogue access point detection)*.
- Door de signaalsterkte te beperken, beperk je ook de kans dat kwaadwillende personen van buiten de school het netwerk kunnen benaderen.
- Door tijdgebonden toegang in te stellen is het netwerk niet te benaderen als de school gesloten is. Dit is extra van belang bij wifi in de buitenruimte.

Advies

- Maak gebruik van encryptie met behulp van WPA/WPA2.
- Zorg dat het wifi-netwerk rogue access point detection ondersteunt.
- Beperk de signaalsterkte.
- Stel tijdgebonden toegang in.

Beheer en Wifi as a Service

Om het beheer van het wifi-netwerk te vereenvoudigen is het aan te bevelen om 'domme' toegangspunten (*thin access points*) te gebruiken, die via een centrale *wifi-controller* (of *WLAN-controller*) van de juiste instellingen worden voorzien. Naast eenvoudiger beheer heeft dit ook kostenvoordelen en zijn de thin access points (omdat ze niet zelfstandig kunnen werken) oninteressant voor diefstal.

De thin access points werken volgens de standaard *CAPWAP (Control and provisioning of wireless access points)*, maar alle leveranciers hebben hier eigen technieken aan toegevoegd, waardoor dit principe in de praktijk alleen werkt met apparatuur van dezelfde fabrikant. Thin access points worden ook wel *LWAPP-toegangspunten* genoemd. LWAPP *(Lightweight Access Point Protocol)* is een specifieke versie van fabrikant Cisco.

Een wifi-controller zorgt onder andere voor een optimale wifi-beschikbaarheid door automatisch devices te herverdelen als een toegangspunt overbelast dreigt te raken, of is uitgevallen vanwege storing. Vanwege de belangrijke rol van de wifi-controller is het aan te raden deze redundant uit te voeren, of deze functie als onderdeel van een wifi-dienst af te nemen *(WaaS - Wifi as a Service)*. Om wifi als dienst af te nemen moeten de wifi-toegangspunten de volgende standaarden ondersteunen: 802.1X, SNMPv3 en OSPF. Het is aan te bevelen te zorgen dat de wifi-toegangspunten deze standaarden ondersteunen, ook als op dit moment nog geen WaaS-dienst afgenomen wordt.

De recente ontwikkeling van controller-less access points maakt WaaS mogelijk zonder dat de toegangspunten daarvoor zelf permanent verbonden hoeven te zijn met de controller in de cloud (*cloud-managed* in plaats van cloud-based). Daarmee is de beschikbaarheid van het wifi-netwerk niet meer afhankelijk van de beschikbaarheid van de internetverbinding en kan toch het wifi beheer als dienst worden uitbesteed.

Advies

- Gebruik thin access points, beheerd via een centrale wifi-controller in het eigen netwerk of in de cloud of gebruik controller-less access points.
- Zorg dat je wifi-toegangspunten 802.1x, SNMPv3 en OSPF ondersteunen.
- Overweeg de wifi-controller en het beheer als een dienst af te nemen (WaaS).

Andere voorzieningen

Er zijn nog een paar mogelijkheden van belang voor de inrichting van het wifi-netwerk:

- Met de ondersteuning van *meerdere SSID's (Service Set IDentifiers)* in het wifi-netwerk wordt het eenvoudig mogelijk om verschillende virtuele netwerken *(VLAN's)* aan te bieden, elk met eigen wifi-inlog-gegevens, waarvoor verschillende eisen aan betrouwbaarheid, beveiliging en bandbreedte gelden. Zo kan er bijvoorbeeld een apart netwerk voor gasten op school ingesteld worden, dat andere beveiliging en prioriteit heeft dan het netwerk waar leerlingen hun digitale examens op maken. In de wifi-toegangspunten of wifi-controller kunnen per SSID andere instellingen voor onder meer Quality of Service worden vastgelegd. Vanzelfsprekend hebben deze alleen effect op het draadloze netwerkverkeer. QoS instel-lingen in de switch beïnvloeden al het netwerkverkeer.
- *Power over Ethernet (PoE)*: Deze techniek maakt aparte stroom-adapters, snoeren en stopcontacten voor toegangspunten over-bodig. In het hoofdstuk met basisprincipes in netwerkinfrastructuur wordt dit verder toegelicht inclusief specifieke adviezen.

Advies

- Bedenk of verschillende kwaliteitseisen gelden voor verschillende manieren van netwerkgebruik. Overweeg voor die verschillende eisen verschillende VLAN's in te richten, met elk een aparte SSID.
- Gebruik Power over Ethernet (PoE) om de toegangspunten van stroom te voorzien.

Eduroam

Voor het onderwijs is met name eduroam een interessante dienst. Eduroam *(education roaming)* is een virtueel gezamenlijk netwerk waarop vele onderwijs-, cultuur- of onderzoeksinstellingen wereld-wijd zijn aangesloten. Met dit netwerk is het mogelijk om gebruikers van andere eduroam klanten met hun eigen inloggegevens via jouw wifi netwerk toegang tot internet te geven. Omgekeerd kunnen leerlingen en medewerkers van jouw school zonder extra aanmel-ding of extra instellingen in hun mobiele device, gebruik maken van internet op netwerken van andere instellingen die op eduroam zijn aangesloten.

Het eduroam netwerk op je school is een VLAN en dus afgeschermd van je eigen wifi-netwerk. De eduroam gebruiker heeft dus geen toegang tot de systemen en gegevens op het interne netwerk. Via logging wordt bijgehouden wanneer welke eduroam gebruikers inlogden. Het netwerk moet 802.1X, SNMPv3 en OSPF ondersteunen om eduroam te kunnen gebruiken.

Advies

- Overweeg je school aan te sluiten op eduroam.
- Zorg daarvoor dat je wifi-toegangspunten 802.1X, SNMPv3 en OSPF ondersteunen.

Een groot gebouw, gedeeld gebouw, of meer schoollocaties

Het interne netwerk wordt een stuk complexer wanneer je school uit een groot gebouw of ook meerdere gebouwen bestaat (mogelijk zelfs verspreid over meerdere locaties):

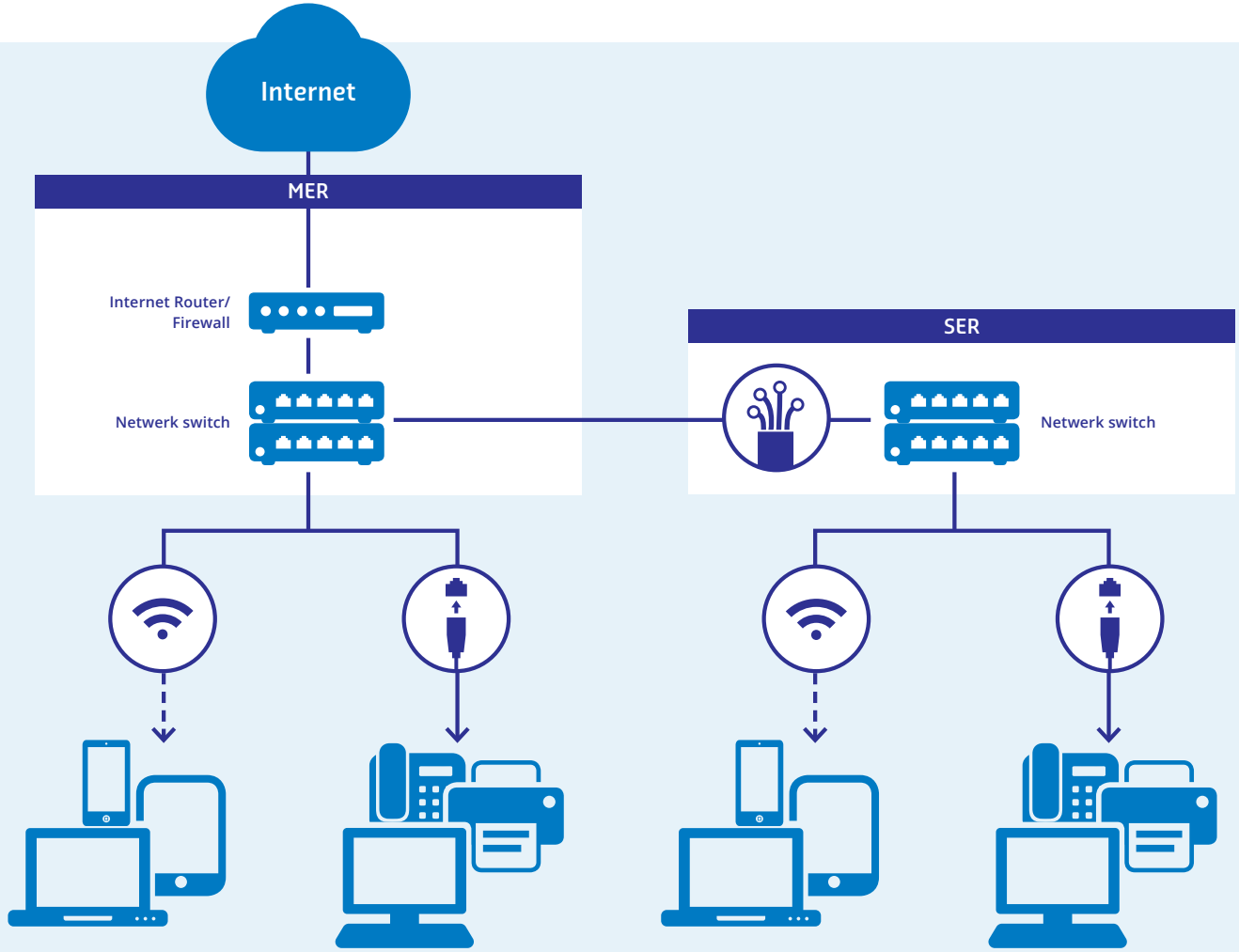
- Het is niet meer afdoende om maar één serverruimte te hebben.
- Als er sprake is van meerdere gebouwen dan komt de vraag op hoe de netwerken in deze gebouwen onderling met elkaar verbonden worden.

Als het gebouw gedeeld wordt met andere organisaties (bijvoorbeeld in het geval van een Integraal KindCentrum) dan is het handig (vanwege flexibiliteit en efficiëntie) om één gezamenlijk netwerk aan te leggen. Door middel van VLAN's en eigen SSID's op het wifi netwerk kan elke organisatie het netwerk functioneel afscheiden van dat van de andere organisaties en werken met de capaciteits- en beveiligingsinstellingen die voor de eigen situatie gewenst zijn. In de praktijk blijkt een gezamenlijk netwerk wel eens lastig te realiseren omdat de verschillende organisaties aparte financiering en verantwoordelijkheden kennen.

Meerdere serverruimtes

Binnen één gebouw is het soms nodig om een of meer nevenserverruimtes *(satellite equipment rooms* of *SER's*) in te richten naast de serverruimte (MER). Dat is aan de orde als de MER op een plek zit van waaruit niet alle benodigde vaste aansluitpunten (waarop ook de wifi-toegangspunten worden aangesloten) op maximaal 90 meter kabel-afstand (dus niet hemelsbreed) liggen. Die afstandsbeperking is nodig om een storingsvrij signaal te kunnen garanderen.

Een SER gekoppeld aan een MER



SER's zijn ook nodig als een school meerdere gebouwen heeft, eventueel zelfs geografisch gescheiden (dus niet op één locatie). Elk gebouw krijgt dan zijn eigen SER (en natuurlijk meerdere SER's als dat nodig is vanwege de kabelafstanden in het gebouw).
Zie illustratie Een SER gekoppeld aan een MER.

Fysiek gezien ontstaan bij meerdere serverruimtes meerdere 'sterren' in het netwerk, met in elke ster een MER of SER als middelpunt. Op logisch niveau blijft de topologie één enkele ster, omdat alle SER's aan de MER zijn gekoppeld en als één knooppunt samenwerken. Netwerkaansluitingen die met een SER zijn verbonden kunnen dan ook (als dat wenselijk is) gewoon verbinding maken met printers die met een andere SER verbonden zijn of servers die in de MER opgesteld staan. In een SER zelf staan idealiter enkel netwerkswitches opgesteld; dat is de reden dat ze in de praktijk vaak patchkast worden genoemd.

Bekabeling tussen serverruimtes, gebouwen en locaties

Serverruimtes op één locatie worden meestal via glasvezel aan elkaar verbonden. UTP is in principe ook mogelijk, zeker omdat via *link aggregation* (of *channeling*) meerdere koperkabels gecombineerd kunnen worden om de benodigde hoge snelheden te bereiken, maar is niet zo gangbaar vanwege de afstandsbeperking.

Koperbekabeling is in elk geval niet bedoeld om de serverruimtes in verschillende gebouwen onderling te verbinden. Koper kan als geleider fungeren bij bliksem en aangesloten apparatuur beschadigen. Om dit probleem te beperken én om langere afstanden te kunnen overbruggen, wordt daarom in beginsel glasvezel gebruikt. Als de verschillende gebouwen op één locatie staan is het graven en aanleggen van een glasvezelkabel meestal geen probleem. Bij geografisch gescheiden locaties is dat vaak niet mogelijk.

SER's zijn dus eigenlijk altijd via glasvezelverbindingen aan de MER gekoppeld, ongeacht of de SER in hetzelfde gebouw zit als de MER of dat SER's in verschillende gebouwen op één locatie zitten of in verschillende gebouwen op verschillende locaties. Glasvezel biedt snellere verbindingen met hogere betrouwbaarheid over grotere afstanden en is daarom de vanzelfsprekende keuze.

Redundante bekabeling

Als er storingen optreden in de glasvezelverbindingen tussen de serverruimtes, heeft dat direct impact op de werking van grote delen van het interne netwerk. Om die reden is het gebruikelijk om die verbindingen redundant (dubbel) uit te voeren.

Wanneer het gaat om verbindingen tussen gebouwen is het zelfs te overwegen om die dubbele glasvezelkabel niet via dezelfde route aan te leggen (bijvoorbeeld in een *ringstructuur*), zodat de verbinding blijft functioneren indien er bij graafwerkzaamheden een kabel wordt geraakt. Wanneer dit geografisch gescheiden locaties betreft, is dit principe soms ook mogelijk via lokale glasvezelvoorzieningen waarbij vezelparen worden gehuurd voor een langere periode (typisch 15 jaar). Redundante glasvezelbekabeling is zeer kostenverhogend, zeker indien het niet op eigen terrein wordt aangelegd, dus deze investering moet opwegen tegen de gevolgen van uitval van de verbinding.

Vijf mogelijke situaties voor serverruimtes en bekabeling

In het gebruik van meerdere serverruimtes en de onderlinge bekabeling zijn er grofweg vijf mogelijke situaties te onderscheiden:

Als je school bestaat uit...	...dan..	...en dan heb je aan serverruimtes nodig...	... die verbonden zijn via...
een klein gebouw	liggen de vaste aansluitpunten niet verder dan 90 meter van de serverruimte	1 MER	n.v.t.
een groot gebouw	liggen sommige vaste aansluitpunten verder dan 90 meter van de serverruimte	1 MER met 1 of meer SER's	MMF glasvezel
een aantal gebouwen op één locatie (=niet gescheiden door openbaar terrein)	liggen de gebouwen op aaneengesloten particuliere grond	1 MER met 1 of meer SER's op elke locatie	MMF glasvezel. Indien de kabelafstanden (niet hemelsbreed) te groot worden voor de gewenste snelheid (variërend van 500 meter tot 2 km), gebruik dan SMF glasvezel
enkele geografisch gescheiden locaties	zijn enkele gebouwen door openbaar terrein van elkaar gescheiden	1 MER met op elke locatie 1 of meer SER's	gehuurde glasvezels of internetverbindingen via een internetprovider* met een VPN dienst**
veel geografisch gescheiden locaties	zijn veel gebouwen door openbaar terrein van elkaar gescheiden	1 MER met op elke locatie 1 of meer SER's	een regionale glasvezel voorziening* of internetverbindingen via een internetprovider* met een VPN dienst**

* Meer hierover in de Handreiking Internetverbinding.

** Een VPN (Virtual Private Network) dienst verbindt twee of meer lokale netwerken (LAN's) met elkaar via een beveiligde internetverbinding, zodat deze zich als één netwerk gaan gedragen. De verbinding via internet heeft encryptie en beveiliging om afluisteren en veranderen van gegevens onmogelijk te maken. Via het VPN hebben alle locaties toegang tot centrale, gedeelde voorzieningen zoals bijvoorbeeld servers of IP-telefonie. Ook kan het VPN centrale, beveiligde toegang tot internet verzorgen voor alle locaties.

Advies

- Gebruik SER's bij grote gebouwen en gebouwen op meerdere locaties, al dan niet geografisch gescheiden.
- Verbindt serverruimtes zowel inpandig als tussen gebouwen met glasvezelkabel.
- Gebruik hiervoor het type MMF, tenzij de afstand tussen locaties SMF vergt.
- Gebruik voor geografisch gescheiden locaties een regionale glasvezeldienst of een VPN over publiek internet, afhankelijk van lokale initiatieven en marktaanbod.
- Leg bekabeling redundant aan als de impact van uitval groot is.
- Overweeg bij redundante bekabeling tussen gebouwen en/of locaties om hiervoor een ringstructuur te laten aanleggen.

Inschattings-hulp capaciteit

Dit hoofdstuk geeft een indicatie hoeveel netwerkcapaciteit er nodig is voor je school. De indicatie helpt om het netwerkontwerp van de leverancier beter op waarde te kunnen schatten en er het gesprek over aan te gaan. Een netwerkleverancier kan aan de hand van een *site survey* een meer precieze analyse maken van de benodigde netwerkcomponenten. Laat zo'n onderzoek altijd uitvoeren voorafgaand aan grote investeringen in uitbreiding, aanpassing of nieuwe inrichting van het interne netwerk van je school. Ga daarbij uit van je behoefte over 5 jaar (en voor de bekabeling over 15 jaar). Om je behoefte te achterhalen kunnen de vragen in de paragraaf Belangrijke vragen aan je school behulpzaam zijn.

De capaciteitsberekening voor een klein gebouw (met maar één serverruimte) bestaat uit het bepalen van het aantal benodigde wifi-toegangspunten en het aantal benodigde vaste aansluitpunten. Is het gebouw groot of bestaat je school uit meerdere gebouwen en/of locaties, dan is het nodig deze basisberekening voor elk gebouw afzonderlijk uit te voeren en ook nog de aanvullende berekeningen uit te voeren.

Basisberekening voor een klein gebouw

Aantal wifi-toegangspunten

Het aantal benodigde wifi-toegangspunten is een optelsom van wat nodig is in de lokalen, de gang, de grote ruimtes (aula, mediatheek, leerplein etc.) en de buitenruimte. Voor elke plek zijn specifieke vuistregels om het aantal toegangspunten te bepalen. In het schema Basisberekening voor aantal wifi-toegangspunten wordt de rekensom getoond om het totale aantal benodigde toegangspunten te bepalen.

Het schema gebruikt de volgende vuistregels:

- Voor zwaar gebruik is het maximum aantal leerlingen per toegangspunt 30. Voor licht gebruik is dat 100.
- Zwaar wifi-gebruik omvat multimediale toepassingen, videostreaming of kritische toepassingen zoals digitale leermiddelen en toetsen. Licht wifi-gebruik is social media en algemeen internetgebruik.
- In klaslokalen is in principe sprake van zwaar wifi-gebruik
- In een grote ruimte bestrijkt één wifi-toegangspunt (indien er geen blokkades voor het signaal zijn) een cirkel rondom het toegangspunt met een straal van 50 meter. Dat is een oppervlakte van ongeveer 7.500 m^2 (3,14 x 50^2). Als we uitgaan van blokkades (of meer toegangspunten in verband met redundantie) rekenen we gemakshalve met de halve signaalafstand en dan is de oppervlakte per toegangspunt 2.000 m^2 (3,14 x 25^2).
- Bij de buitenruimte wordt gerekend met een halve cirkel rondom het toegangspunt (dat tegen de buitenmuur is bevestigd). Dat is 7.500 m^2 / 2 = 3.750 m^2.
- Afhankelijk van het aantal te verwachten gebruikers en de intensiteit van het gebruik kan het nodig zijn om op een gekozen plaats voor een wifi-toegangspunt (=een wifi-plaats) niet één, maar meerdere toegangspunten te installeren.

Zie schema Basisberekening voor aantal wifi-toegangspunten.

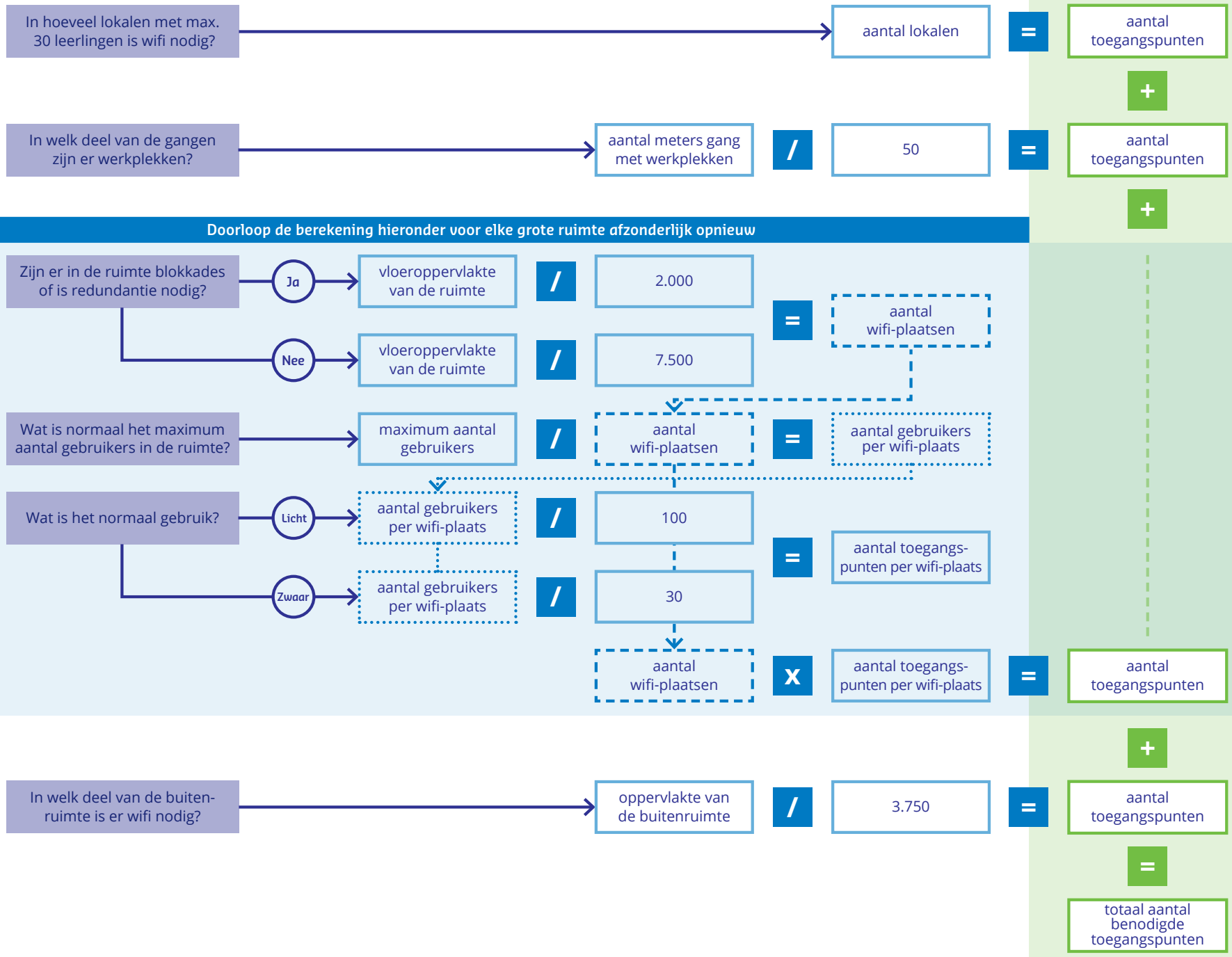
Aantal vaste aansluitpunten

Bij het berekenen van het benodigde aantal vaste aansluitpunten is het belangrijk om je te realiseren dat er naast de printer en de pc of laptop van de leraar nog veel meer apparaten in een school zijn die via het netwerk (kunnen of moeten) werken:

- digiboards
- bewakingscamera's
- deurtoegangssystemen/bellen
- gebouwbewakings- en registratiesystemen (werken veelal over UTP-kabel, ook al is het geen ethernetnetwerk)
- intercom en/of omroepsystemen
- advertentie- en broadcastsystemen ('tv-schermen')
- analoge of digitale telefonie
- kassa's en pinterminals in de kantines
- oplaadpunten van kaartsystemen
- wifi-toegangspunten

Om het aantal vaste aansluitpunten te bepalen is het simpelweg een kwestie van apparaten tellen. Soms staan apparaten dicht bij elkaar, bijvoorbeeld het digiboard en de laptop van de leraar in het lokaal, of de pc's op de administratie. 'Dicht bij elkaar' is in dit geval relatief: het is mogelijk om tussen het apparaat en het vaste aansluitpunt een losse *netwerkpatchkabel* aan te sluiten van maximaal 5 meter. De vaste aansluitpunten voor apparaten die dicht bij elkaar staan worden meestal afgemonteerd in een paneel waar twee vaste aansluitpunten op aangesloten kunnen worden. De kostenvoordelen die dat oplevert, zijn meestal verrekend in de gemiddelde prijs per vaste aansluiting die leveranciers hanteren. Daar hoeft bij het bepalen van het aantal vaste aansluitpunten dus geen rekening mee gehouden te worden.

Basisberekening voor aantal wifi-toegangspunten



Bij het bepalen van het aantal vaste aansluitpunten is het verstandig een marge te hanteren van 20%. Het later aanleggen van extra aansluitpunten is substantieel duurder dan de meerprijs van het laten aanleggen van nog niet direct benodigde aansluitpunten. Om de initiële investering van die reserve aansluitpunten nog wat te beperken is het mogelijk enkel de kabel te laten aanleggen en deze op de juiste lengte opgerold op het systeemplafond te laten liggen. Deze kan dan later met een verticale kabelgoot en een aansluitpunt naar de juiste plek gebracht worden. Deze reservering van 20% uitbreidingsruimte is ook verstandig bij het aanschaffen van een patchpanel.

Advies

- Laat 20% meer vaste aansluitpunten aanleggen dan op basis van de behoefte nodig lijkt te zijn. Van deze extra aansluitpunten kan indien mogelijk besloten worden alleen de kabel aan te leggen en deze nog niet af te monteren.
- Laat een patchpanel installeren met 20% extra ruimte dan op basis van de behoefte nodig lijkt te zijn.

In het schema Basisberekening voor aantal vaste aansluitpunten is de berekening van het aantal benodigde aansluitpunten weergegeven.

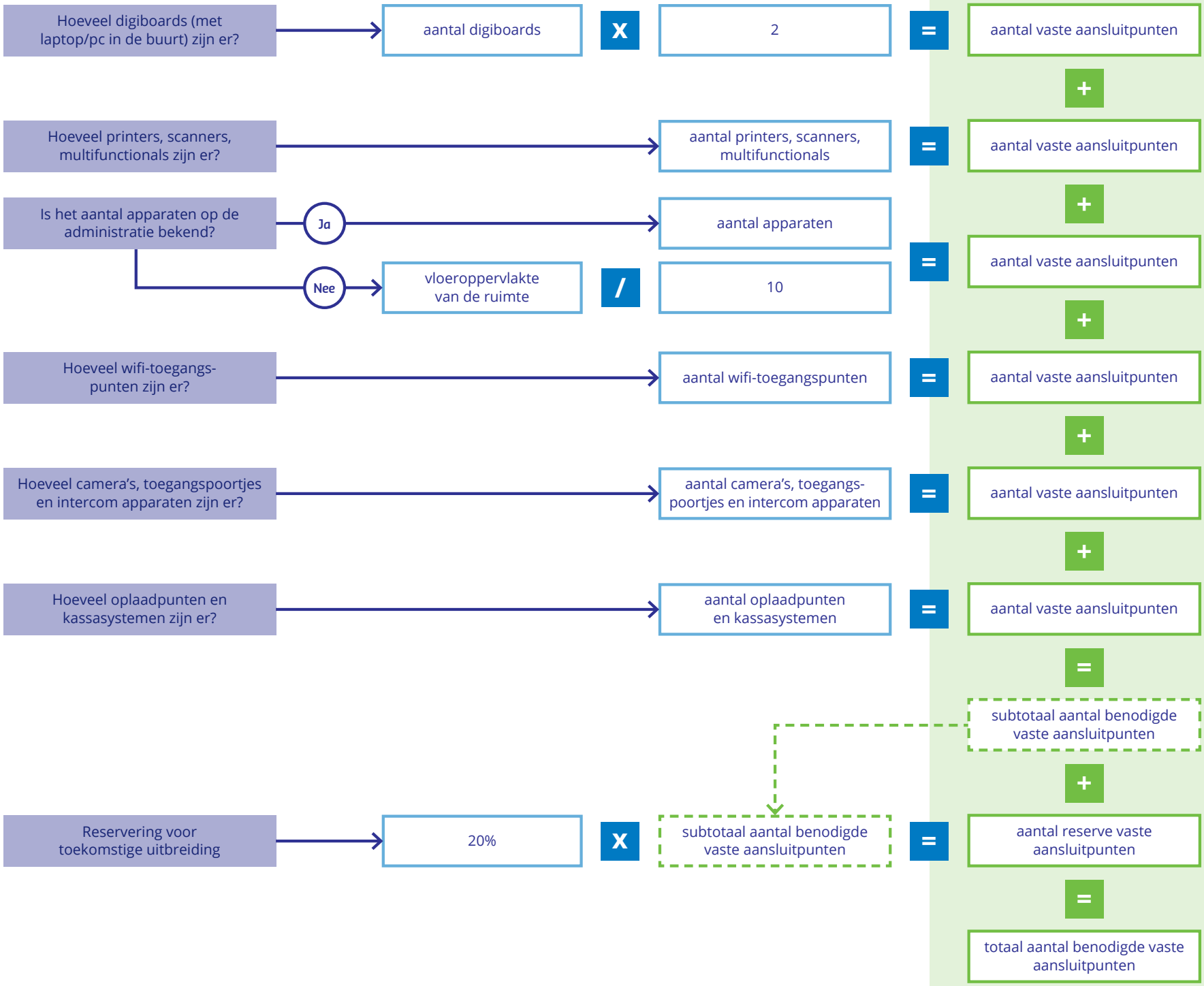
Benodigde bandbreedte

De bandbreedte van de diverse netwerkcomponenten wordt bepaald volgens het principe: hoe dichter bij het centrum van de ster, hoe sneller. Dat betekent dat de verbinding van de pc, printer of mobiele device de laagste bandbreedte kent van het netwerk en de switch de hoogste. En hoe dichter bij het centrum van de ster, hoe minder eenduidig de benodigde capaciteit te bepalen is. Het hangt nogal af van het specifieke netwerkgebruik op je school. Werkt je school volledig in de cloud of niet? Maakt je school veel gebruik van (multimediale) digitale leermiddelen? Laat daarom de leverancier een capaciteits-berekening uitvoeren voor de specifieke situatie van je school.

Toch zijn er wel enkele algemene uitspraken te doen over de snelheid van een netwerkswitch. Er spelen drie snelheden een rol:

1. **Poort-snelheid**
   Dit is de bandbreedte die maximaal beschikbaar is voor elk vast aansluitpunt dat op de switch is aangesloten (in een *switchpoort*). Op dit moment is 100 Mbit/s het basisniveau *(fast switch)* en 1000 Mbit/s gangbaar *(gigabit switch)* voor aansluitpoorten voor werkplekken. Ook modellen met een capaciteit van 10.000 Mbit/s *(10 gigabit switch)* per aansluiting komen steeds vaker voor.
2. **Backplane-snelheid**
   Dit is de snelheid van de interne verwerking (switching- en forwarding) van datastromen in de switch (ook wel switching- en forwarding-snelheid genoemd). Deze snelheid ligt altijd flink hoger dan de poort-snelheid (omdat de switch immers gegevens van meerdere poorten tegelijk moet kunnen verwerken), maar ligt flink lager dan de optelsom van de snelheden van alle poorten samen (omdat nooit alle poorten tegelijk maximaal zullen worden belast). Dit principe heet oversubscription. Om niet bij de minste toename

Basisberekening voor aantal vaste aansluitpunten



in netwerkverkeer op vertragingen te stuiten, is een backplane-snelheid van tweederde van de maximale totale poort-snelheid gangbaar (3:2 oversubscription ratio), zeker bij gebruik van wifi (met meer dan één gebruiker via één toegangspunt/switchpoort). Dus als de switch bijvoorbeeld 48 poorten van 1Gbps heeft, dan moet de backplane-snelheid minimaal 30 Gbps zijn.

3. **Uplinkpoort-snelheid**
   Dit is de snelheid waarmee de switch verbonden is met het internet (via de internetmodem/router/firewall) of met de centrale switch in de MER. Net als bij de backplane-snelheid geldt hier het principe van oversubscription. Lange tijd was een uplinkpoort-snelheid van 5% van de maximale totale poort-snelheid gangbaar (20:1 oversubscription ratio). Dus als de switch bijvoorbeeld 48 poorten van 1Gbps heeft, dan zou de uplinkpoort-snelheid minimaal 2,4 Gbps moeten zijn. Echter, met de toename van het gebruik van wifi (met meerdere gebruikers via één toegangspunt/switchpoort) en cloud (veel verkeer via internet) zou een lagere oversubscription gehanteerd moeten worden (bijvoorbeeld 8:1). In de praktijk komt dit al snel neer op een 10 Gbps uplink-poort, in kleinere gebouwen en/of bij de keuze voor (minder snelle) 100 Mbps poorten voor aansluitpunten kan soms 1 Gbps nog volstaan. In de Handreiking Internetverbinding is een inschattingshulp te vinden voor de internetbandbreedte die je school nodig heeft.

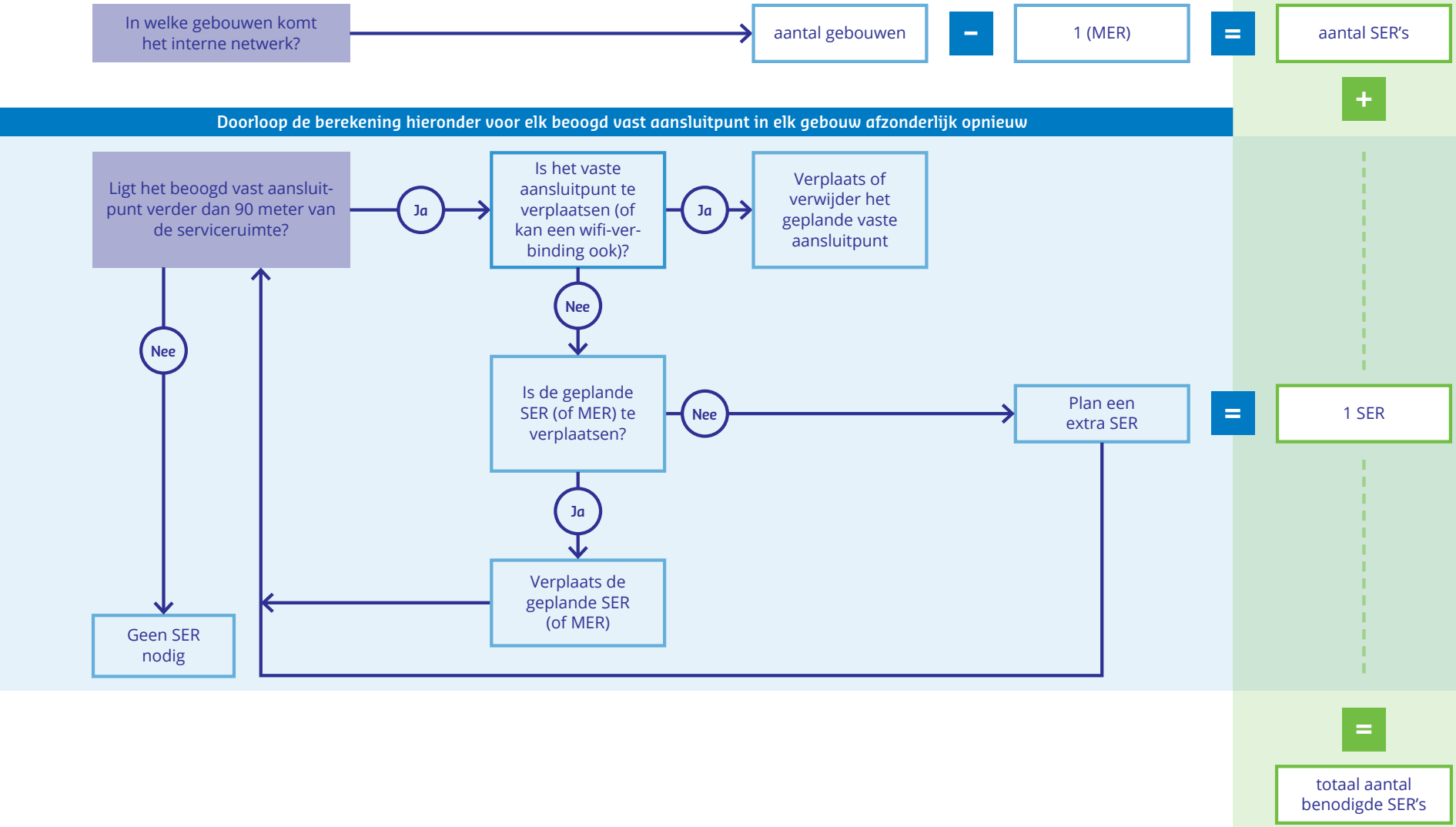
Advies

- Kies 1 Gbps poorten in de netwerkswitch voor aansluitpunten.
- Kies 10 Gbps uplinkpoorten in netwerkswitches tenzij duidelijk is dat 1 Gbps voor 5 jaar zeker zal volstaan (in kleinere gebouwen of bij beperkt gebruik).
- Laat de leverancier een capaciteitsberekening uitvoeren voor de specifieke situatie van je school.

Aanvullende berekeningen bij grote of meerdere gebouwen

Is je schoolgebouw groot of bestaat je school uit meerdere gebouwen en/of locaties, dan zijn er meerdere serverruimtes nodig die ook onderling verbonden zijn via glasvezel. De daarvoor benodigde capaciteitsberekening volgt in het schema Berekening van aantal nevenserverruimtes (SER's). Vergeet niet voor elk gebouw afzonderlijk ook nog de basisberekening uit te voeren om het aantal vaste aansluitpunten en wifi-toegangspunten per gebouw te bepalen.

Berekening van aantal nevenserverruimtes (SER's)



Aantal SER's naast de MER

Het interne netwerk kent in beginsel één MER. Afhankelijk van de situatie kunnen er één of meer SER's nodig zijn. Belangrijke factor daarbij is de grootte en vorm van het schoolgebouw en de mogelijkheid om vanuit één te kiezen punt binnen 90 meter alle beoogde plekken voor vaste aansluitingen te kunnen bereiken. Natuurlijk bepaalt niet alleen de maximaal benodigde afstand het aantal SER's. Omdat het immers niet mogelijk is om op elke willekeurige plek in het gebouw een SER aan te leggen, vergt het enig gepuzzel om hierin het optimum te bereiken. Gezien de kosten is het belangrijk het aantal serverruimtes per gebouw zo laag mogelijk te houden.
Het schema Berekening van aantal nevenserverruimtes (SER's) geeft weer hoe je een indicatie van het aantal benodigde SER's kunt bepalen.

Bekabeling om serverruimtes/gebouwen onderling te verbinden

Zoals aangegeven in het hoofdstuk over bekabeling worden de MER en de SER's onderling verbonden met glasvezel, ongeacht of die zich in één gebouw bevinden. Wel wordt er tussen gebouwen soms een andere soort glasvezelkabel met extra, nog onbenutte vezelparen(SMF) gebruikt dan binnen één gebouw (MMF). De glasvezelkabel moet ruimte bieden aan toekomstige uitbreidingen, omdat er hoge kosten verbonden zijn aan het aanleggen van extra glasvezelkabels (zeker tussen gebouwen, vanwege het graafwerk).

Het schema Basisberekening voor het aantal glasvezelkabels geeft een indicatie van het aantal benodigde glasvezelkabels in beide soorten. Bij het schema is uitgegaan van de volgende uitgangspunten:

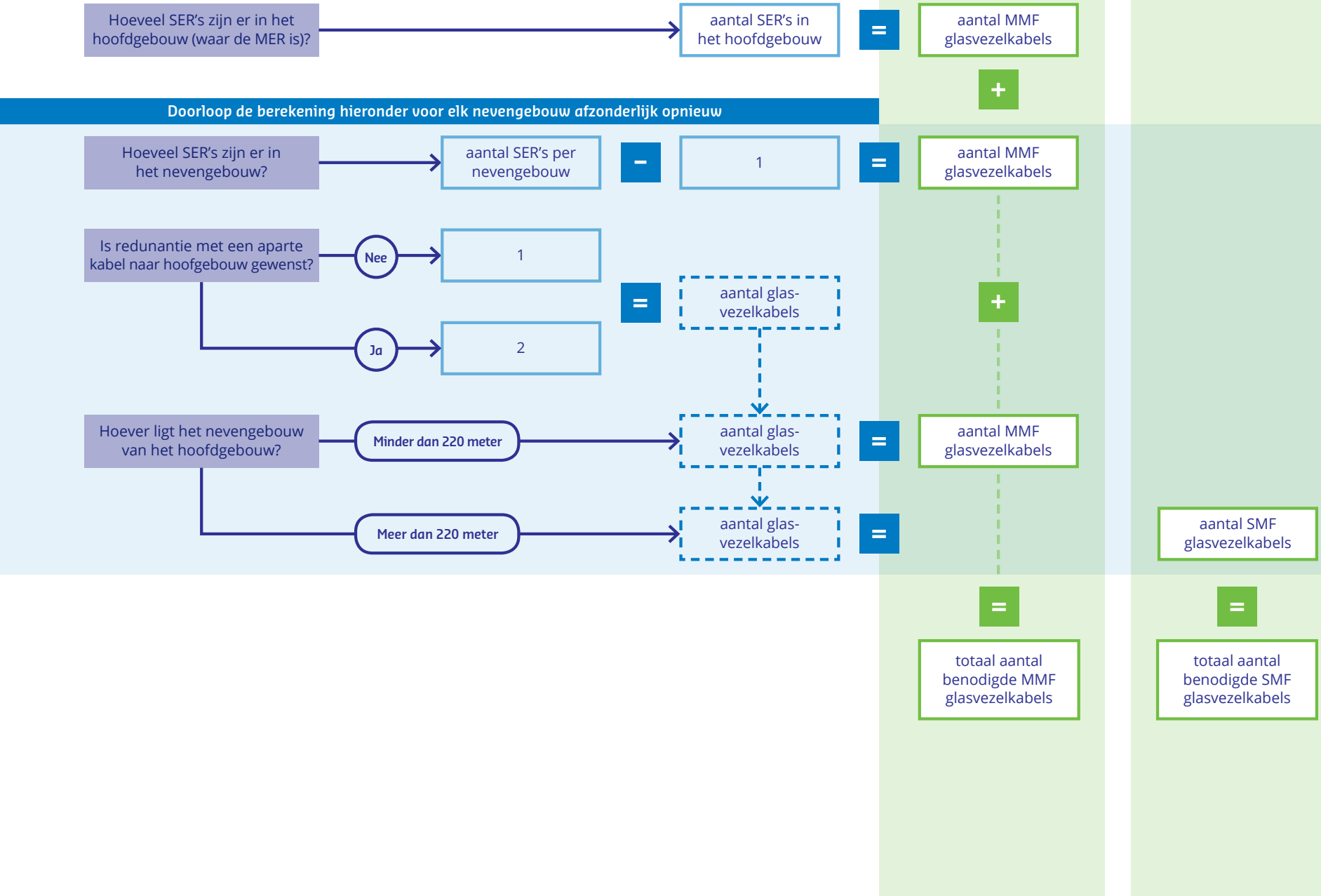
- Alle nevengebouwen zijn via particulier terrein verbonden met het hoofdgebouw en dus niet geografisch gescheiden door openbaar terrein. In dat laatste geval komen andere soorten verbindingen in beeld.
- De bekabeling moet geschikt zijn voor bandbreedtes van 10 Gbps.
- De glasvezelmodules werken via 10GBASE-LX4 (zie de begrippenlijst voor een beknopte uitleg van deze code).

Naast het aantal kabels is ook het aantal vezelparen per kabel van belang. In beginsel is elke SER/MER verbonden via één vezelpaar. Met het oog op toekomstige uitbreidingen is het aan te bevelen een glasvezelkabel te kiezen die nog ongebruikte vezelparen heeft. De meerprijs van een dergelijke kabel is beperkt, zeker als u de extra vezelparen nog niet laat afmonteren in een glasvezelaansluiting. Dit laatste is arbeidsintensief en daarom kostbaar.

Advies

- Zorg dat aangelegde glasvezelkabels extra ongebruikte vezelparen hebben met het oog op toekomstige uitbreidingen.
- Laat extra vezelparen nog niet afmonteren.

Basisberekening voor het aantal glasvezelkabels



Voorbereiden en begeleiden van implementatie

Het succes van de implementatie van (een aanpassing in) het interne netwerk is voor een belangrijk deel afhankelijk van hoe goed je als school je leveranciers selecteert, informeert en aanstuurt. Dit vergt meer expertise dan in deze handreiking is opgenomen. Het is verstandig om een onafhankelijk adviesbureau in te schakelen die helpt leveranciers te selecteren en hun voorstellen, netwerkontwerp, SLA's en installaties te beoordelen en te controleren. Deze kosten verdien je terug in effectievere investeringen en vlottere implementatie.

Daarnaast kan het interessant zijn lid te worden van de ict coöperatie. Dit is een coöperatie van po- en vo-besturen die samenwerken en expertise delen bij het inkopen van ict-voorzieningen met een goede prijs/kwaliteitverhouding en gunstige voorwaarden voor het onderwijs.

Advies

- Schakel een onafhankelijk adviesbureau in.
- Overweeg lid te worden van de ict-coöperatie.

Belangrijke vragen aan je school

Een leverancier kan alleen een goed intern netwerk ontwerpen als duidelijk is waarvoor het gebruikt gaat worden. Daarom begint alles met het helder krijgen van de verwachte ontwikkelingen op je school op het gebied van digitaal leren, mobiele devices en cloud. Ook is het belangrijk je af te vragen wat de grenzen van de in je school aanwezige ict-expertise is. Onderstaande acht vragen helpen daarbij:

1. Wat is de aanleiding om het netwerk aan te passen, te vervangen of uit te breiden?
   Het antwoord op deze vraag helpt de leverancier te begrijpen wat je school ermee wil bereiken en kan daardoor meedenken.
2. Welke ontwikkeling in leerlingaantallen verwacht de school?
   Het antwoord op deze vraag helpt de benodigde capaciteit in te schatten.
3. Welke plannen zijn er nu, op de korte termijn (5 jaar) en op de langere termijn (15 jaar) met het gebruik van mobiele devices in de school?
   Het antwoord op deze vraag helpt in te schatten hoeveel mobiele devices er nu en in de toekomst zullen zijn en hoe intensief deze gebruikt gaan worden.
4. Welke plannen zijn er nu, op de korte termijn (5 jaar) en op de langere termijn (15 jaar) met het gebruik van toepassingen in de cloud?
   Het antwoord op deze vraag helpt in te schatten of (en zo ja, hoelang) er nog sprake zal zijn van servers in de school en hoe belangrijk die servers zijn.
5. Hoe belangrijk is nu, op de korte termijn (5 jaar) en op de langere termijn (15 jaar) het gebruik van digitale leermiddelen en het gebruik van mobiele devices voor ons onderwijsproces? En welke toepassingen hebben daarbij prioriteit?
   Het antwoord op deze vraag helpt in te schatten hoe hoog de eisen aan beschikbaarheid van het interne netwerk moeten zijn en welk QoS beleid nodig is.
6. Welke plannen zijn er nu, op de korte termijn (5 jaar) en op de langere termijn (15 jaar) met het gebruik van IP-telefonie?
7. Welke expertise is er in de school (of het schoolbestuur) om de inrichting/uitbreiding van het interne netwerk te begeleiden?
   Het antwoord op deze vraag helpt in te schatten welke eisen gesteld moeten worden aan de in te huren onafhankelijke adviseur die de school ondersteunt.
8. Welke expertise is er in de school (of het schoolbestuur) om het beheer van het interne netwerk na de installatie (deels) zelf uit te voeren?
   Het antwoord op deze vraag helpt in te schatten welke dienstverlening de leverancier van het interne netwerk na afloop dient te leveren.

Advies

- Zorg dat je weet welke ontwikkelingen er zijn te verwachten op je school.
- Zorg dat je weet welke ict expertise aanwezig is op je school en hoe je school die wil inzetten tijdens de inrichting en het beheer van het netwerk.

Er zijn minimaal twee leveranciers nodig

Zowel bij de inrichting (of aanpassing) als bij het beheer van het interne netwerk is er een duidelijk onderscheid tussen de bekabeling en de rest. De bekabeling (inclusief kabelgoten, vaste aansluitpunten en min of meer bouwkundige voorzieningen in de serverruimte, zoals een verhoogde computervloer) worden gezien als onderdeel van het gebouw en deze worden vaak door een installateur aangelegd en onderhouden. De actieve netwerkcomponenten zoals de switch en de wifi-toegangspunten met hun instellingen worden door een netwerkleverancier aangelegd en onderhouden. Er zullen meer leveranciers betrokken zijn als een deel van het netwerk als aparte dienst wordt afgenomen (denk aan de internetverbinding of wifi-as-a-service).

Het is belangrijk als school omstandigheden te creëren waarin alle leveranciers zich verantwoordelijk voelen en die verantwoordelijkheid ook kunnen nemen, zonder dat je school daar onredelijk hoge kosten voor krijgt gerekend. De volgende tips helpen daar bij:

- Laat de bekabeling certificeren en laat de bekabeling-leverancier hier garantie op geven. Die certificering is ook voor de netwerkleverancier een waarborg dat de basis waar zij mee werken in orde is.
- Spreek met alle leveranciers af welke bedrijfszekerheid je verwacht, hoe lang een storing mag voortduren en hoe vaak er storingen mogen optreden. Dergelijke afspraken liggen vast in een overeenkomst die *SLA (Service Level Agreement)* heet. Voordat een leverancier zich aan dergelijke afspraken verbindt, zal deze zeker willen weten dat de inrichting van het netwerk van voldoende kwaliteit is. Het kan er toe leiden dat een leverancier de gevraagde *service levels* alleen garandeert als er aanvullende maatregelen genomen worden om de redundantie te vergroten. Dit leidt tot extra inrichtingskosten. Het is dus belangrijk om duidelijk te hebben welke garanties je school écht nodig heeft voor de continuïteit van het onderwijs. Hoge eisen (bijvoorbeeld storingsoplossing binnen 4 uur) kunnen erg kostbaar zijn. Zorg ook dat de afspraken met de verschillende leveranciers onderling consistent zijn. Als storingen de volgende dag opgelost moeten zijn dan is een 4-uurs service contract op wifi bijvoorbeeld onnodig duur.
- Spreek af welke rapportagesystemen/managementconsoles je school ter beschikking heeft om zelf in de gaten te kunnen houden wat de kwaliteit van de dienstverlening is en in welke mate de beschikbare capaciteit benut wordt in alle onderdelen van het netwerk.

Advies

- Laat de bekabeling certificeren.
- Spreek met leveranciers de bedrijfszekerheid af in een SLA.
- Zorg dat je via rapportagesystemen zelf de kwaliteit van de dienstverlening en de benutting van de capaciteit in de gaten kunt houden.

Belangrijke vragen aan je potentiële leveranciers

Onderstaande vragen zijn relevant om te bespreken met de potentiële leveranciers tijdens de offertefase:

1. Welke beschikbaarheid kunt u garanderen, welke maatregelen zijn daarvoor nodig en wat zijn de extra investeringen danwel besparingen bij hogere danwel lagere beschikbaarheidsgaranties?
   Het antwoord op deze vraag helpt te bepalen welke voorzieningen voor redundantie de investeringen waard zijn.
2. Welke technieken past u toe om de capaciteit, veiligheid en betrouwbaarheid van het netwerk te optimaliseren?
3. Voldoet uw capaciteitsberekening aan onze eigen berekening? En zo nee, waarom wijkt die af?
4. Op welke manier kan de school de kwaliteit van het netwerk bewaken/monitoren?
5. Welke delen van de bestaande netwerkbekabeling respectievelijk actieve componenten kunt u hergebruiken en wat betekent dit voor de garanties die u biedt en de kosten van uw voorstel?
6. Welke maatregelen stelt u voor om het netwerk later eenvoudig (en met relatief beperkte investering) uit te breiden?
   Het antwoord op deze vraag helpt te bepalen of de leverancier rekening houdt met extra (ongebruikte) capaciteit en andere maatregelen voor schaalbaarheid als modulaire of stackbare switches.
7. Hoe bakent u uw verantwoordelijkheid bij beheer en storingsafhandeling af in relatie tot de verantwoordelijkheid van de installateur van de bekabeling respectievelijk de leverancier van de actieve netwerkcomponenten?
8. Welke rapportage- en overlegstructuur stelt u voor om periodiek de kwaliteit van de dienstverlening te evalueren en afspraken te maken over eventuele verbeteringen of aanpassingen?
9. Aan welke van de onderstaande adviezen voldoet uw oplossing niet en waarom niet?

Algemene adviezen voor moderne netwerken:

- Zorg dat alle netwerkcomponenten autosensing/autonegotiation, multicast en SNMPv3, OSPF, 802.1X ondersteunen.
- Zorg dat de netwerkswitches IPv6, half duplex, link aggregation, QoS, DiffServ en CoS ondersteunen.
- Zorg dat de netwerkswitch glasvezelaansluitingen heeft indien je school meerdere serverruimtes heeft.
- Zorg dat de poorten van de netwerkswitch bij aanvang tot maximaal 80% in gebruik zijn.
- Overweeg schaalbare netwerkswitches te gebruiken (stacking of modulair).
- Kies 1 Gbps poorten in de netwerkswitch voor aansluitpunten.
- Kies 10 Gbps uplinkpoorten in netwerkswitches tenzij duidelijk is dat 1 Gbps voor 5 jaar zeker zal volstaan (in kleinere gebouwen of bij beperkt gebruik).

Adviezen voor de serverruimtes

- Er is één MER. Gebruik SER's bij grote gebouwen en gebouwen op meerdere locaties, al dan niet geografisch gescheiden.
- Overweeg aparte stroomgroepen aan te leggen in de MER. Sluit de centrale netwerkswitch als deze meerdere voedingen heeft ook op aparte stroomgroepen aan.
- Overweeg de MER uit te rusten met klimaatconditionering, brandblusinstallatie en goede aarding, afhankelijk van het aantal en het soort apparatuur in de MER.
- Overweeg de MER uit te rusten met een verhoogde computervloer en een patchpanel.
- Laat een patchpanel installeren met 20% extra ruimte dan op basis van de behoefte nodig lijkt te zijn.
- Plaats servers alleen in de MER.
- Verbindt MER's/SER's altijd met glasvezelkabel van het type MMF, tenzij de afstand tussen locaties SMF vergt.
- Gebruik voor geografisch gescheiden locaties een regionale glasvezeldienst of een VPN over publiek internet, afhankelijk van lokale initiatieven en marktaanbod.
- Leg deze bekabeling redundant aan als de impact van uitval groot is.
- Overweeg bij redundante bekabeling tussen gebouwen en/of locaties om hiervoor een ringstructuur te laten aanleggen.

Adviezen voor de internetmodem/router:

- Zorg dat de internetmodem/router voldoet aan de eisen die de internetprovider er aan stelt.
- Plaats de internetmodem/router in de MER.
- Zorg dat de firewall-functie altijd is ingericht. Ofwel bij de internetprovider, op gespecialiseerde firewall-apparatuur of op de eigen internetmodem/router (als de eisen aan filtering bescheiden zijn).
- Zorg voor de internetverbinding voor goede beschikbaarheidsgaranties, een achtervang of een redundante aansluiting, afhankelijk van het belang van internetgebruik in het onderwijsproces.
- Schakel eventuele wifi-functionaliteit op de internetmodem/router uit.

Adviezen voor Power over Ethernet:

- Laat de stroomvoorziening voor wifi-toegangspunten en IP-telefoons via het netwerk verlopen (PoE).
- Zorg voor netwerkswitches (en apparatuur) die dezelfde versie van de standaard voor PoE ondersteunen, bij voorkeur 802.3at.

Adviezen voor bekabeling:

- Gebruik voor nieuwe installaties en uitbreidingen altijd UTP Cat6A.
- Rust kabelgoten waar zowel stroomkabels als koperen netwerk-kabels doorheen lopen altijd uit met metalen scheidingsschot.
- Laat 20% meer vaste aansluitpunten aanleggen dan op basis van de behoefte nodig lijkt te zijn. Van deze extra aansluitpunten kan indien mogelijk besloten worden alleen de kabel aan te leggen en deze nog niet af te monteren.
- Gebruik glasvezel met LC connectoren.
- Zorg dat aangelegde glasvezelkabels extra ongebruikte vezel-paren hebben met het oog op toekomstige uitbreidingen.
- Laat extra vezelparen nog niet afmonteren.
- Laat de bekabeling certificeren.

Adviezen voor wifi:

- Zorg dat nieuwe wifi-netwerken de 802.11ac wave 2 standaard ondersteunen en kunnen werken met 2,4 GHz en 5 GHz.
- Zorg dat oudere wifi standaarden ook ondersteund worden, zeker bij oudere devices en/of een BYOD beleid.
- Gebruik wifi-apparatuur van één fabrikant.
- Zorg dat het aantal toegangspunten en hun signaalsterkte niet alleen gebaseerd is op hoge dekking en signaalkwaliteit, maar ook op lage kosten en stralingsoverlast.
- Stel de signaalsterkte in beginsel niet hoger dan -65 dBm, tenzij het gebruik daar echt om vraagt. Op plekken met zeer licht wifi-gebruik is -85 dBm voldoende.
- Laat de leverancier met een site survey storingsbronnen en signaal-belemmeringen identificeren om daarop de plaatsing van de toegangspunten te kunnen baseren.
- Maak gebruik van encryptie met behulp van WPA/WPA2.
- Zorg dat het wifi-netwerk rogue access point detection ondersteunt.
- Stel tijdgebonden toegang in.
- Gebruik thin access points, beheerd via een centrale wifi-controller in het eigen netwerk of in de cloud of gebruik controller-less access points.

Begrippenlijst

De volgende technische begrippen komen in in de tekst voor, of zou de leverancier kunnen gebruiken:

10GBASE-LX4	Zie xxxBASE-xxx.
802.1X	Protocol om dynamische VLANs (virtuele netwerken) te kunnen maken in een netwerk.
802.3a/b/g/n/ac	Verschillende wifi-netwerkstandaarden.
802.3af/at	Oudere en nieuwste Power over Ethernet standaard.
access switch	Switch waarop vaste aansluitpunten en wifi-toegangs-punten zijn aangesloten in de SER.
xxxBASE-xxx	Codering voor een specifiek protocol binnen de Ethernet standaard. De cijfers voorafgaand aan BASE- geven de snelheid aan: 100 (Mbps) tot 10G (Gbps) en de code na BASE- bestaat uit een letter voor de soort bekabeling (T staat voor UTP koperkabel; F en S staan voor glas-vezelkabel), gevolgd door een X of R, gevolgd door een cijfer dat aangeeft hoeveel signalen tegelijk verstuurd kunnen worden (waarbij 1 meestal wordt weggelaten).
channeling	Zie link aggregation.
core switch	Snelle switch in de MER waarop al het netwerkverkeer bij elkaar komt.
CoS	Afkorting van Class of Service, een standaard om prioriteit te kunnen toekennen aan bepaald netwerk-verkeer. Lijkt op QoS, maar sorteert alleen het verkeer, dwingt geen prioriteiten af en biedt geen (pro-actieve) oplossing bij congestie (te druk netwerk).
DiffServ	Zie QoS.
duplex	Netwerkinstelling die bepaalt of er via een netwerk-verbinding om-en-om eenrichtingsverkeer (half duplex) of altijd tweerichtingsverkeer (full duplex) mogelijk is.
encryptie (bij wifi)	Beveiliging door verzonden informatie te versleutelen, zodat afluisteren zinloos is. Bekendste protocollen zijn het verouderde en onveilige WEP en het veiliger WPA en WPA2.
Ethernet	Netwerkprotocol waarmee computers en andere apparaten communiceren.
firewall	Apparaat dat het netwerkverkeer tussen het eigen netwerk en het internet bewaakt en filtert ter beveiliging.
FTU	De FTU (fiber termination unit) is het ISRA punt bij een glasvezelnetwerk.
Gbps	Afkorting van Gigabit per seconde, ofwel 1 miljard bits per seconde. Eenheid van bandbreedte van netwerk-verkeer.
inline power	Zie Power over Ethernet (PoE).
IP, IPv4/IPv6	Afkorting van Internet Protocol, een standaard waarmee computers en andere apparaten informatie met elkaar kunnen uitwisselen. IPv4 is de gangbare versie, IPv6 is de nieuwe standaard die een veel grotere adresruimte en betere mogelijkheden tot veiligheid biedt.
IP-telefoon	Modern digitaal telefoonsysteem dat op een centrale aangesloten is via het computernetwerk.
ISRA-punt	Het aansluitpunt naar de bekabeling van de internet-provider. Hierop wordt de internetmodem/router aangesloten.
LC	Afkorting van Lampert Connector, de meest gebruikte glasvezelconnector van dit moment.
Link aggregation	Een techniek om netwerkswitches in staat te stellen met hogere bandbreedtes te communiceren met andere netwerkswitches.
LWAPP-toegangspunt	Implementatie van fabrikant Cisco van het thin access point-principe. Zie thin access point.
MAN	Afkorting van Metropolitan Area Network, een uitgebreid netwerk op basis van glasvezel dat vaak een regio of stad beslaat.

Mbps	Afkorting van Megabit per seconde, ofwel 1 miljoen bits per seconde. Eenheid van bandbreedte van netwerkverkeer.
MER	Main Equipment Room, centrale serverruimte waar de belangrijkste switches en andere netwerkvoorzieningen staan opgesteld.
multicast	Netwerkprotocol om netwerkverkeer naar meerdere ontvangers tegelijkertijd te optimaliseren, met name toegepast in (streaming) video.
OSPF	Afkorting van Open Shortest Path First, een open standaard (leveranciersonafhankelijk) dat netwerkrouters en -switches onderling met elkaar laat communiceren over waar verkeer naartoe moet worden geleid.
port blocking	Functie in een firewall om te bepalen welk soort internetverkeer is toegestaan, zoals bijvoorbeeld het verkeer tussen een website en een webbrowser.
Power over Ethernet	Standaard om via een Ethernet netwerkkabel tegelijk ook stroom te leveren aan het aangesloten apparaat. Veel gebruikt bij wifi-toegangspunten en IP-telefoons.
QoS	Afkorting van Quality of Service, een standaard om verkeer met verschillende prioriteiten (aangegeven met CoS) te kunnen classificeren, afhandelen, congestie (te druk netwerk) te voorkomen of in te grijpen als het netwerk toch vastloopt. Ook wel DiffServ genoemd.
redundantie	Dubbele uitvoering van componenten, bedoeld om hogere beschikbaarheid van het netwerk te verkrijgen.
SC	Afkorting van Subscriber Connector, na LC de meest gebruikte glasvezelconnector.
SER	Satellite Equipment Room, decentrale serverruimte, primair bedoeld om netwerkaansluitingen te verbinden met de centrale serverruimte (MER).
SLA	Afkorting van Service Level Agreement, het contract waarin de school en de leverancier afspraken vastleggen over de kwaliteit en de beschikbaarheid van het interne netwerk.
SNMPv3	Afkorting van Simple Network Management Protocol versie 3, een netwerkstandaard waarmee gecentraliseerd beheer van netwerkcomponenten op een veilige manier mogelijk is.
SSID	Afkorting van Service Set IDentifier, ofwel de naam van een draadloos netwerk.
switch	Centraal netwerkapparaat waar alle netwerkkabels bij elkaar komen. Regelt het netwerkverkeer.
thin access point	Wifi-toegangspunt dat door een centrale intelligente wifi-controller moet worden aangestuurd.
toegangspunt	Antenne unit waarmee mobiele devices van gebruikers draadloos contact leggen om toegang te krijgen tot het netwerk
VLAN	Afkorting van Virtual Local Area Network.. Een VLAN is een virtueel netwerk (logisch afgescheiden binnen hetzelfde fysieke netwerk) met afzonderlijke mogelijkheden of juist beperkingen.
VPN	Afkorting van Virtual Private Network. Een VPN gedraagt zich als één netwerk maar bestaat uit twee of meer aparte netwerken die via een beveiligde internetverbinding met elkaar verbonden zijn.
wifi	Afkorting van Wireless Fidelity, een verwijzing naar de draadloze netwerkverbinding.
wifi-controller	Het wifi-toegangspunt dat alle thin access points aanstuurt.
WLAN	Afkorting van Wireless LAN. Zie wifi.
WLAN-controller	Zie wifi-controller.

Colofon

Handreiking netwerk en wifi in de school

Deze brochure is ontwikkeld door Kennisnet, in het kader van het Doorbraakproject Onderwijs & ICT. Het Doorbraakproject is een gezamenlijk initiatief van de PO-Raad, VO-raad en de ministeries van Onderwijs, Cultuur en Wetenschap en Economische Zaken.

Datum van uitgave
september 2017

Auteur
Lisa van Ginneken

Experts
Michael van Wetering, Okko Huising

Met dank aan
Frank Beks, Paul Dam, Eric van Paalen

Uitvoering
Vormgeving: Gloed Communicatie, Nijmegen
Fotografie: iStockphoto

Over Kennisnet
Elke leerling verdient eigentijds, veilig en persoonlijk onderwijs. Daarom ondersteunt Kennisnet scholen met ict. We zorgen voor een landelijke ict-basisinfrastructuur, adviseren de sectorraden en delen onze kennis met het primair onderwijs (po), het voortgezet onderwijs (vo) en het middelbaar beroepsonderwijs (mbo). Kennisnet wordt gefinancierd door het ministerie van Onderwijs, Cultuur en Wetenschap (OCW).

kennisnet.nl

Kennisnet
Paletsingel 32
2718 NT Zoetermeer

T 0800 321 22 33
E support@kennisnet.nl
I kennisnet.nl

Postbus 778
2700 AT Zoetermeer