Niveo KB1812: Become a Wireless Network Guru in few simple steps

How to get the most out of your Wireless Networks

Netstar Products BV | Communicatieweg 9L, NL3641SG, Mijdrecht, The Netherlands |
☎+31 (0) 297 256161 | ✉ info@niveoprofessional.com | 💻 www.niveoprofessional.com

The (non-)sense of heat maps

We regularly receive request to, based on a blue print of a building, to create a heatmap. Although the customer is always right, we should not give poor advise. So, we advise suggested temporary placement of a few AP's, followed by a site survey.

The reality of it is that you can't create a heatmap of a wireless network, by simply plotting them in a drawing of a building. There is no way you can capture the effect users, user clustering, interfering networks, building cabling, moisture in the air and so on. Putting in the type and thickness of a wall in the system, doesn't cut. All these factors and many more have impact on the quality of the wireless network you install.

Upon receiving this advice, the installer often resorts to the 'Better be safe than sorry' principle and puts a high-power AP in every room on full whack. Just to be sure… Unfortunately, this doesn't work with radio signals and it results in an overcrowded, non-performing wireless network.

What can do?

Short of a full site survey, there are really only two ways to install great wireless networks.

1. Use common sense and follow a few basic steps (Read further…)
2. Have your customer pay four to five times as much to install a system that does the common-sense part all for you and that was actually designed for high density hospitality and event setups, rather than small commercial or residential. Great if you have such a customer, but there is little added value as a professional installer.

First a few of the basics

Do I need 802.11N or 802.11AC? 802.11AC in itself is of minor importance. The key is dual band (2.4 & 5.8 Ghz), which also exists in 802.11N. The dual band is especially of importance in dense urban area's as the 2.4Ghz bands are overcrowded.

The main difference between N & AC starts to come when you implement 'wave2' wifi, which uses 80Ghz wide channels instead of 20 or 40 Ghz with wave1. You could reach theoretically higher speeds with that, but since your channels are so wide that they nearly all overlap, it creates interference issues. So far tests have shown that the downsides are still bigger than the theoretical benefits you would gain from these wider channels (it negates each other) for residential or light commercial setups.

Do I need a controller for roaming? There is a perception that you would need a controller to make roaming possible. This is true for the high-density hospitality and event equipment. Not necessarily for equipment designed for residential or light commercial setups. There are several protocols for roaming that allow for roaming, without any controller. However, since CatWap is becoming more common place, the controllers can optimize the roaming between AP's.

Mesh, WDS/Extenders or Full AP's? Mesh is a remarketed, old technology. Basically, it uses multiple radios on the same back haul. The downside is that it significantly reduces the speeds per node. WDS or extender based networks are basically use repeaters to extend the signal. It might seem easy to setup, but there are serious downsides. First of all, not all wireless protocols are fully supported, which can downgrade the signal. Then each extender hub reduces not only speed, but also created latency.

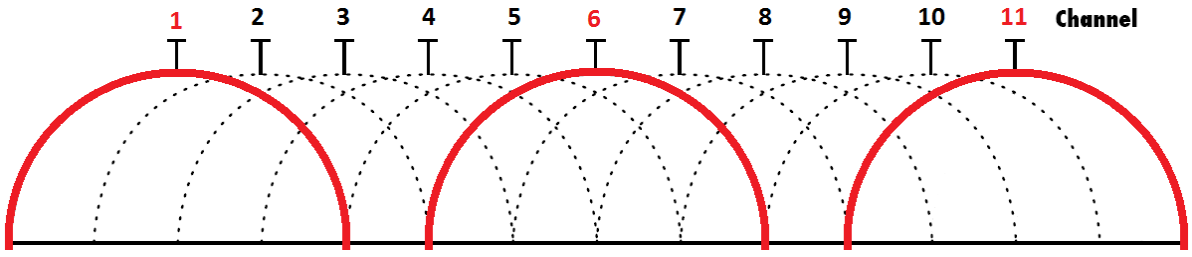
The real way to go (and the reason why the customer has hired a Professional Installer) is to install fully hardwired Access Points. This type of setup will avoid the downsides of mesh and extenders and will create the most stable system possible.

Do I need Security? Well eh…yes! Please read my earlier post on that subject:
http://mailchi.mp/13d5818b541a/security-in-av-installations-in-crucial-learn-how

1. Always use maximum encryption available. Security over speed!
2. Always change passwords and not into 12345
3. Always change SSID's from the vendor into names that cannot be traced to the location. HarrysHomeNetworks or ChurchStreet20 are not secure names.
4. Check for other active SSID's on the AP's. Turn them off or secure them!
5. Be careful with so call 'Guest networks'. They are of the left on default or given simple passwords (without ever changing them) and create a real vulnerability. Also, only implement guest networks if you are absolutely sure they are routed to internet only. When in doubt, use DMZ and VLANs from the router and/or switch to create a properly segmented network.
6. Wizards are a really big risk! They create a black box of settings. Only ever use wizards, if you fully understand what they are configuring. When in doubt, ask you vendor or configure step by step.

Installing the network

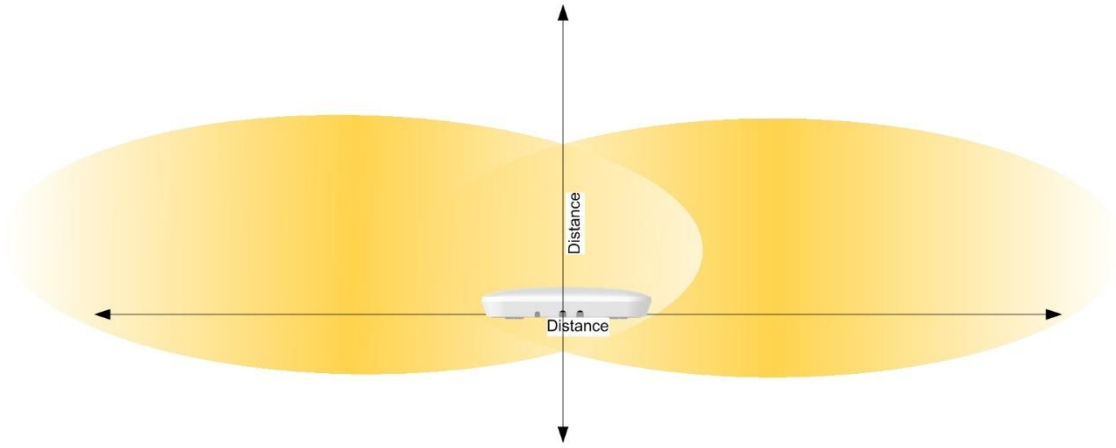
1. Gateway: In most cases, the wireless network rums of a switch, that is connected to the 'Gateway' of the internet provider. Depending in your ISP, this has probably been given for 'free', which is an indicator for limited quality, and comes with a lot of antennas. Turn off the wifi of that device. It is a common mistake to leave that. It interferes and will reduce speed and connectivity.
2. Make sure the AP's have enough power. If you use PoE(+)-switches, calculate the required power for all devices carefully and make sure the PoE-budget of the switch fits that. Note that AP's use a lot more power, when they are in full use then when they are idle hanging on a switch.
3. Make sure the cables are up to the task. Old and bendy cables or incorrectly connected key-stones can radically decrease performance of the network. Not only on data capacity, but also on PoE-power throughput. Go over 300ft? Use fiber uplinks, to bridge the main distance.
4. Use same SSID for the entire nework, but configured to non-overlapping channels:



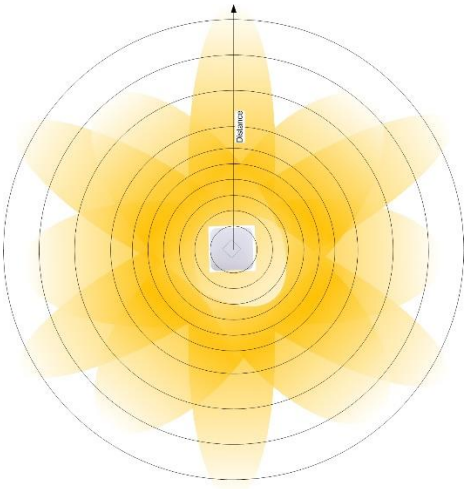
5. Avoid channels with a lot of interference. The better AP's have channels scanners in the web-interface.
6. Don't configure client devices to connect to multiple wireless networks in the same area. They do not know where to connect to and generally pick the strongest signal.

Placing the AP's

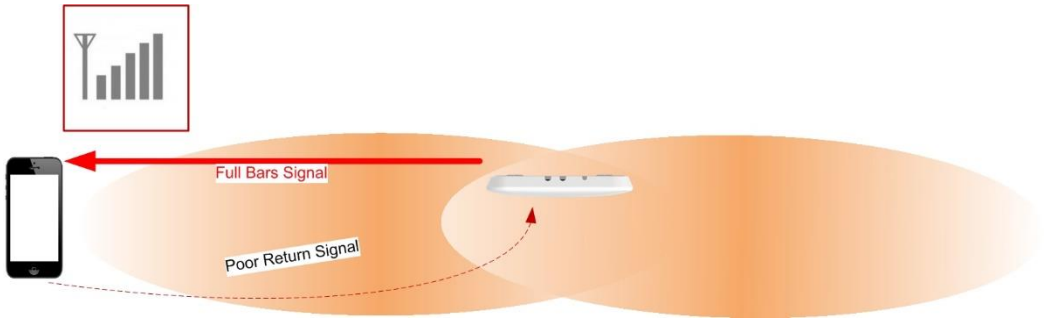
1. Access Points have one or more antenna's inside that are put into a configuration. Designed for purpose. Don't put a ceiling AP vertical against a wall or upside down on a desk. This device is designed to give the best performance when mounted on a ceiling. Using it differently will limit the performance a lot!



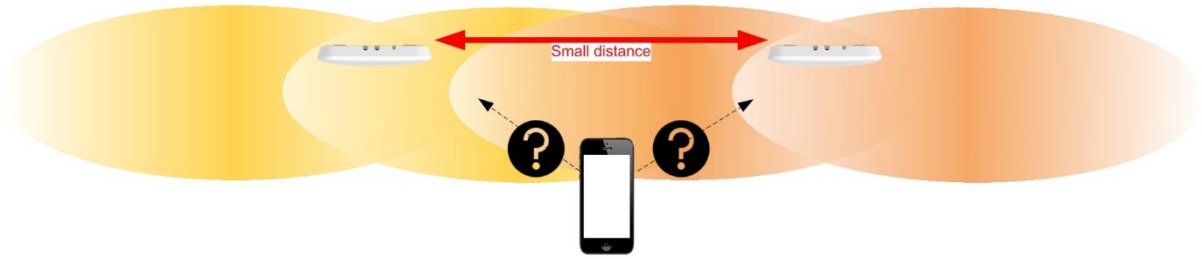
2. Know that the further you are removed from an AP, the slower the transmission will be:



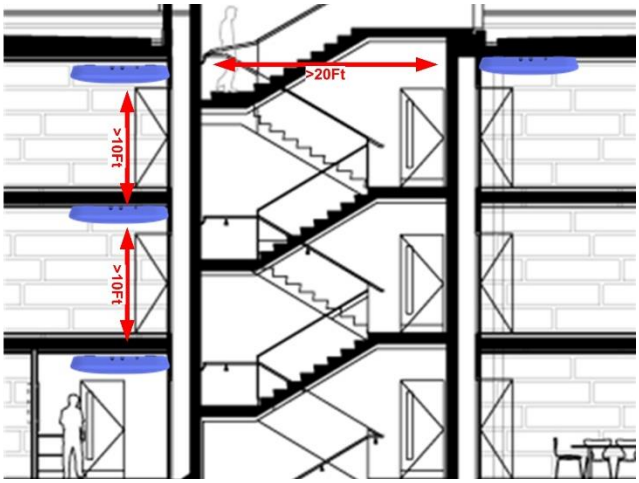
3. Don't put too much distance between AP's. Even with high powered ones. You client device will see full bars, but it is a two way communication and your tablet usually only has a very small antenna to get a signal back, resulting in broken connections.



4. Don’t put the AP’s too close. Client devices get confused.



5. Don’t put the AP’s too close. Really! The floor to floor distance is often overlooked and AP’s are often placed 10ft apart:



6. In case AP’s are mounted too close, simply turn down the transmission (Tx) power in the web interface.