# Allgemeines

Unterschiedliche Geräte für Home oder Business

Unterschiede:

* Preis (Business ab 150€, oder günstigere zB mikrotik, ubiquity)
* Anzahl gleichzeitiger Teilnehmer (bis zu 200/Gerät)
* Verwaltungssoftware – gleichzeitiges Einrichten vieler APs über einen Controller (lokal, cloud)
* Power over Ethernet Unterstützung PoE (Injektoren oder PoE Switches 48V, >25W, bis zu 100 m über das LAN Kabel)
* Mehrere ausrichtbare Antennen, automatische Bündelung und Entfernung reflektierter Signale
* automatisches Einstellen zB auf Roaming oder Benutzerverhalten über die Verbindungsversuche der Teilnehmer
* Unterdrückung anderer Geräte (zB Cisco 600€)

# Technik

2.4 oder 5Ghz

Je höher die Frequenz, desto geringer ist die Reichweite (skin Effekt)

Leistung in Europa 100mW in Amerika 1W (heißt aber nicht 10 mal größere Reichweite)

## Protokolle

a: 5 GHz-Band, bis zu 54 Mbits/s  
b: 2.4 GHz-Band, bis zu 11 Mbits/s  
g: 2.4 GHz-Band, bis zu 54 Mbits/s  
n: 2.4 & 5 GHz-Band, bis zu 600 Mbits/s (also aufpassen, wenn man 5GHz will, n sagt noch nichts darüber aus, es gibt auch reine 2.4 mit n)  
ac: 5 GHz-Band, bis zu 1.3 Gbits/s

b sollte man eher abschalten, nur für alte Geräte, alle werden downgegraded, wenn eines nur b kann, da hat das b Gerät eben Pech

## Frequenzen

2.4 Ghz 13 Kanäle in Europa,   
es sind aber nur 3 parallel vewendbar (1, 7, 13), ohne sich zu stören  
Kanalbreite 20 oder 40 MHz (breitere Kanäle – mehr Daten aber auch mehr Störung der Nachbarkanäle)  
gesundheitlich schädlich, wie Mikrowellenherd Absorptionsfrequenz von Wasser ist 2.4 Ghz

5Ghz 19 Kanäle, nicht überlappend, mehrere Kanalbreiten siehe oben

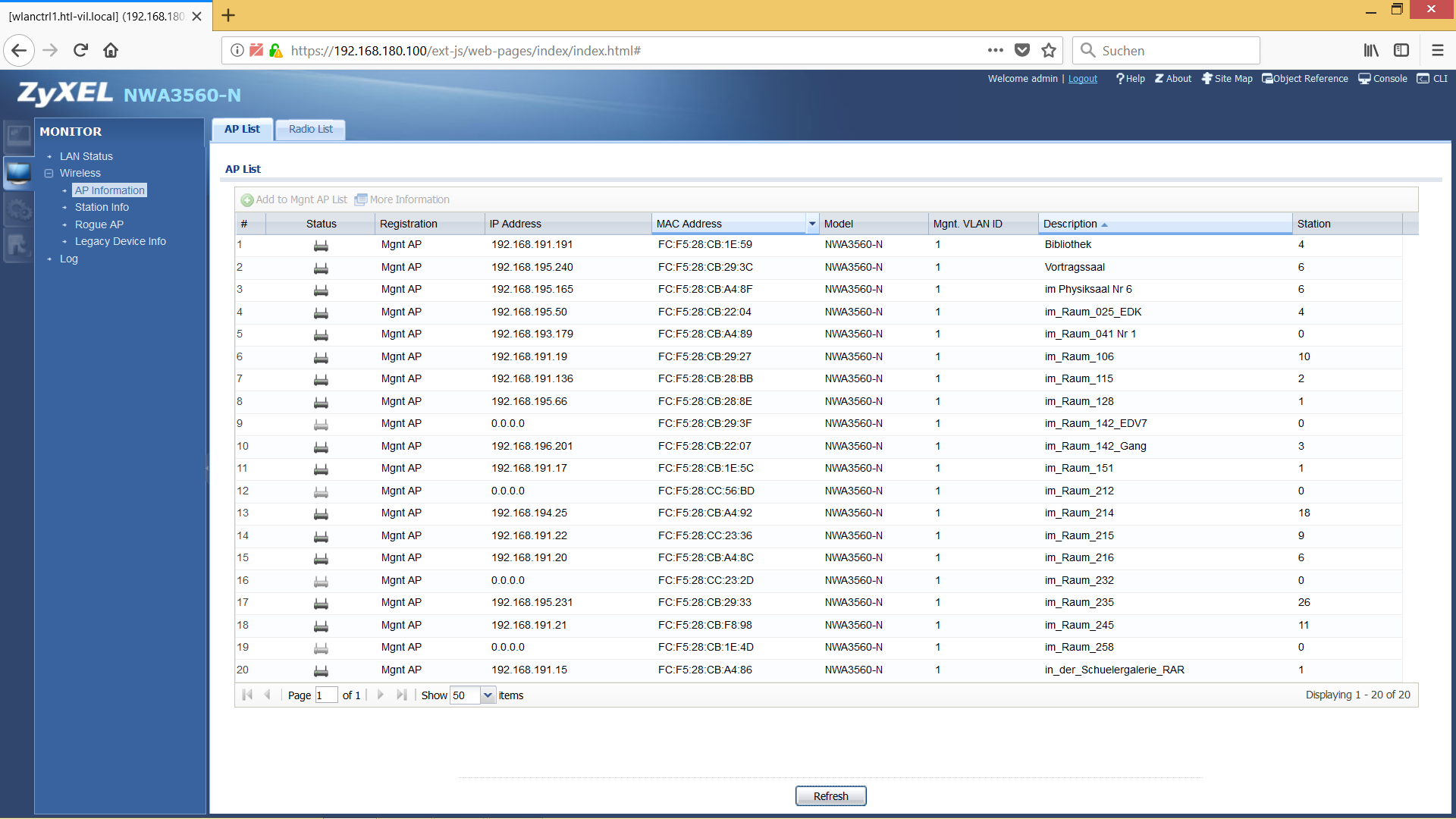
# Auswahlkriterien für Unternehmen:

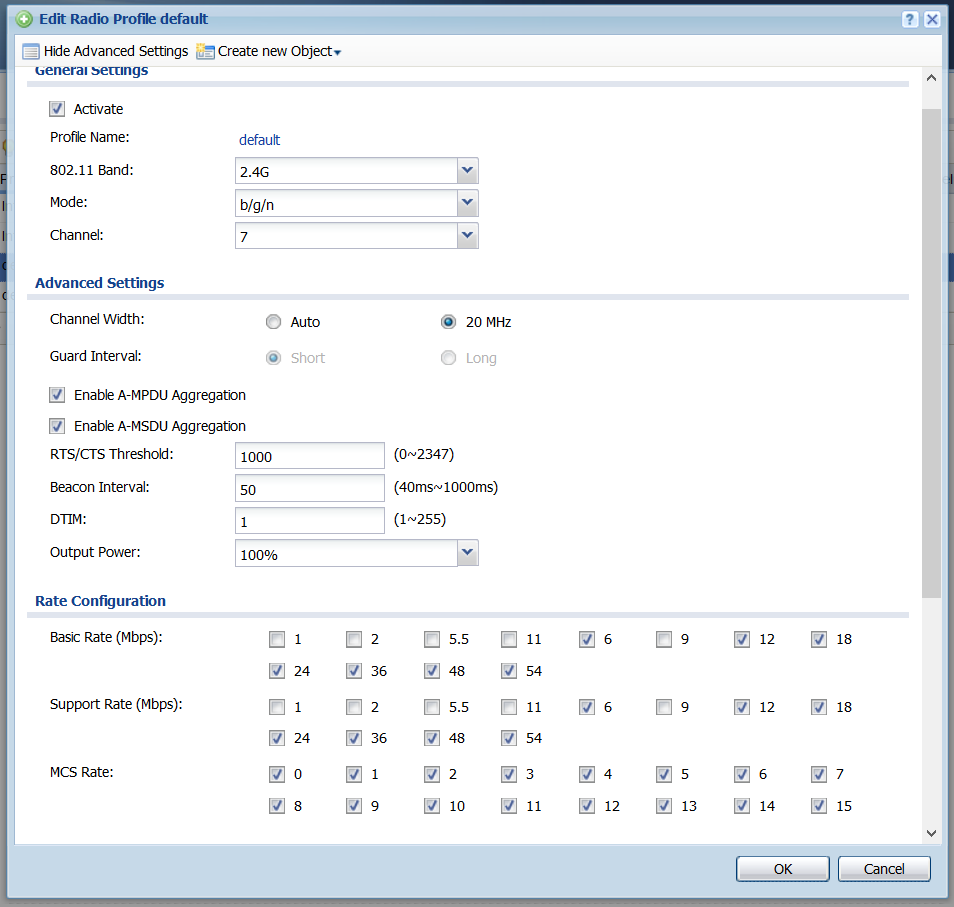
Welche Geräte (wird 2.4 GHz benötigt) gleichzeitiges Dualband  
Anzahl der Wände

Heatmap erstellen (Signalstärke auf einem Gebäude-Grundriss zb ekahau headmapper) oder Analysetools (zB Wifi Analyser für Android, um Signalstärke an bestimmten Ort zu messen)

Konfigurationstool auswählen (Zyxel sehr gut, benötigt aber HW Controller, TP-Link mit schlechter Namenszuordnung aber SW Lösung mit Weboberfläche, Ubiquiti auch mit cloud-Lösung über MAC Adressen )

zB Zyxell (Ähnlich der GUI der Firewalls)





Beispiel für die zentrale Konfiguration im Controller – Änderungen gelten für alle kontrollierten APs  
Konfigurationsparameter erklären

Benutzerverhalten analysieren (Roaming oder eher statisch – Thresholds und Beacon Intervalle anpassen) einige APs managen das automatisch (haben zB eine checkbox wo man „fast roaming“ wählen kann)

Load Balancing (automatisches Abmelden und Anmelden in benachbarten APS, falls einer zu viele Klienten hat)

Wenn viele APs nötig sind (high density Netze): 5Ghz bevorzugen

Werden Gäste WLANs benötigt ist es praktisch, wenn jeder Benutzerstream von den anderen isoliert ist >(man will ja vmtl nur ins Internet, das lokale Netz ist uninteressant)

Radius oder LDAP Authentifizierung wäre optimal, jeder Benutzerstream ist von den anderen isoliert,  
Zusätzlich sollte das Authentifizieren über SSL erfolgen. Dazu braucht man ein Zertifikat am Controller und den publick key am Client (zu dem Zeitpunkt hat man ja noch kein Internet, so dass man bei einer CA nachfragen kann ob alles passt)

APs sollten auch VLANs unterstützen, zB mehrere SSIDs auf einem AP und ein eigenes VLAN zu jeder SSID (so könnte man zB in der Schule für jede Klasse eine SSID vergeben und jeder Klasse ein eigenes Subnetz zuweisen)

Meshes: APS kommunizieren miteinander (nicht nur mit einem zentralen Controller), bilden ein Netz mit einer SSID, ermöglichen nahtloses roaming, der Client wird von den APS mit dem gerade besten AP verbunden (sonst macht das der client):

Nachteil: man bentötigt üblicherweisi (gleiche) Geräte desselben Herstellers, sonst sind sie vmtl nich kompatibel.