

WLAN-Vorlesung

Teil-1

Stand: 14.05.24

Inhalt

- Historisches
- Gründe für und gegen WLANs
- Abgrenzung zu weiteren WLAN-Technologien
(Bluetooth, WiMAX, Mobiltelefonstandards)
- Allgemeine Grundlagen von Funknetzen (Funknetzaufbau)
- Modi (Ad-hoc, Infrastruktur, Bridge und Mesh-Modus)
- Topologien / Architekturen / Service Sets (BSS, IBSS, PBSS, ESS, QBSS)
- Handover / Roaming
- Mobile IP
- Sicherheit

Historisches



Quelle: <https://commons.wikimedia.org/w/index.php?curid=52853789>

WLAN, warum ?

Es gibt gute Gründe für die Vernetzung von Rechnern mittels WLAN:

- Räumliche Flexibilität innerhalb des Empfangsbereichs.
- Keine Verkabelungsprobleme. Verkabelung ist nicht nur teuer, sondern unter bestimmten Umständen gar nicht möglich.

Wie zum Beispiel bei denkmalgeschützten

Gebäuden, kann nicht an beliebigen Stellen die Wand aufgestemmt werden und mal eben eine Leitung eingezogen werden. Wer seine Firma über mehrere Gebäude in einer Stadt evtl. gegenüber auf der anderen Straßenseite untergebracht hatte, musste über teure Stand- oder Wählleitungen die Verbindungen herstellen.

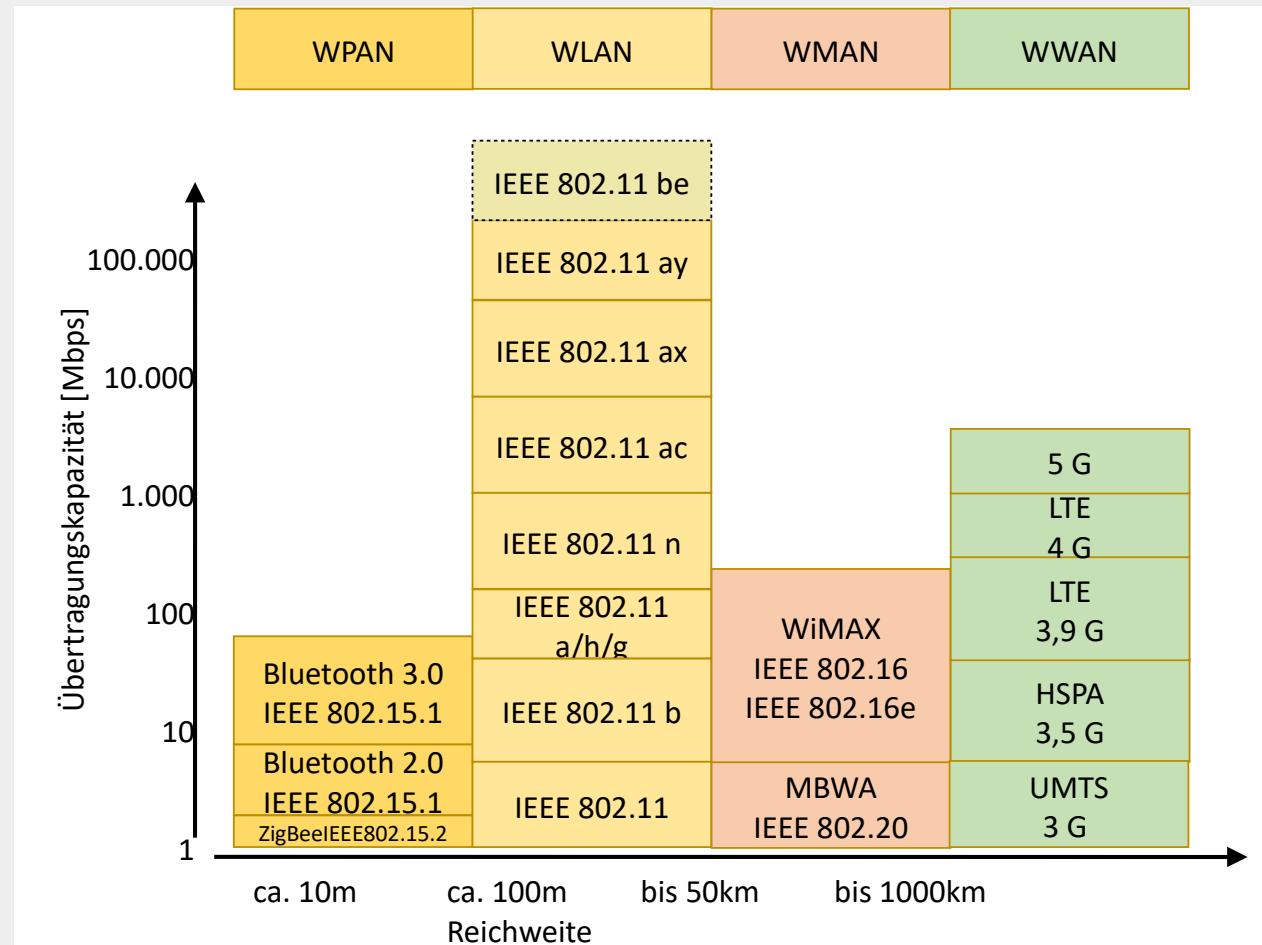
- Ad-hoc-Netzwerke ohne aufwändige Planung möglich.
- Keine Lizenzen (Genehmigungen / Gebühren) erforderlich.

WLAN, warum nicht?

Dem gegenüber stehen jedoch auch Nachteile:

- Gegenüber Verkabelung langsam.
- Hohe Bitfehlerraten im Vergleich zu LANs.
- Nationale Restriktionen (Es gibt keine einheitlichen internationale Frequenzbänder.
Bestenfalls überschneidende Bereiche)
- Sicherheit durch die Funkstrecke als „Shared Media“.
- Kosten. Wer ein WLAN in Betrieb nimmt muss trotzdem erst einmal verkabeln, denn die Access-Points (APs) müssen angeschlossen werden (sowohl an ein LAN als auch an eine Stromversorgung).

Einbettung in weitere Funklösungen

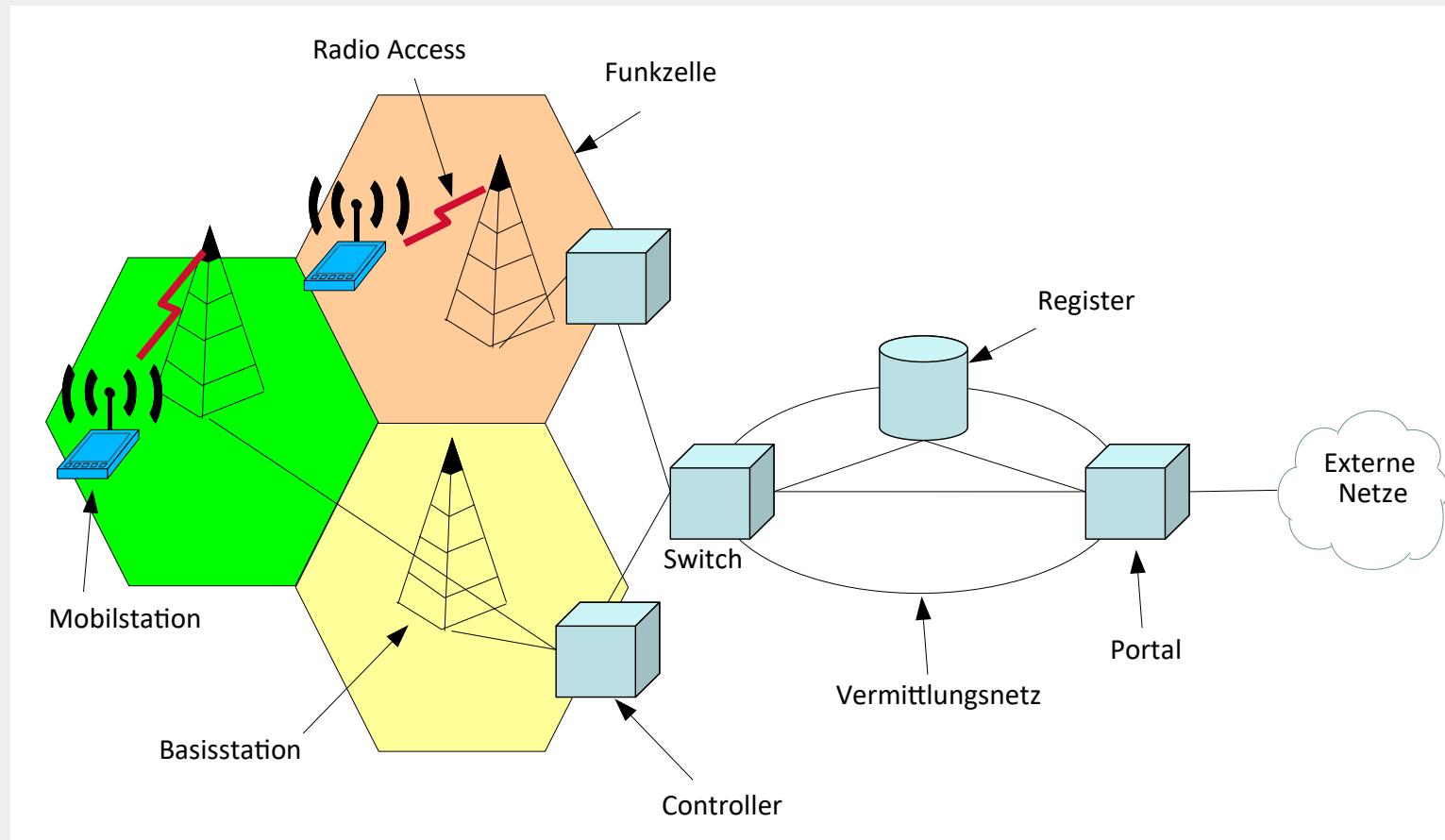


Andere Lösungen

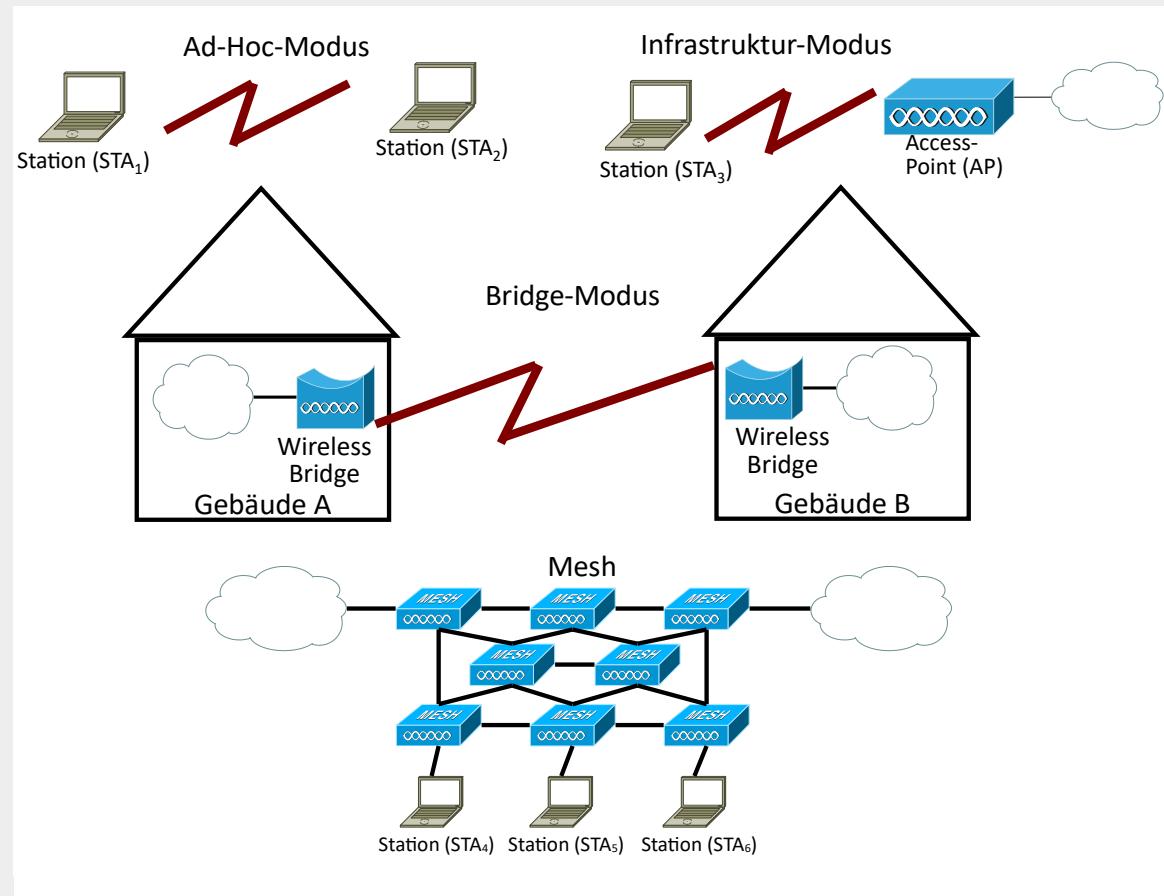
Es gab und gibt noch weitere Lösungen auf Funk-Basis:

- NFC
- Bluetooth
- ETSI (Hiperlan2)
- RadioLAN
- HomeRF
- DECT
- Infrarot

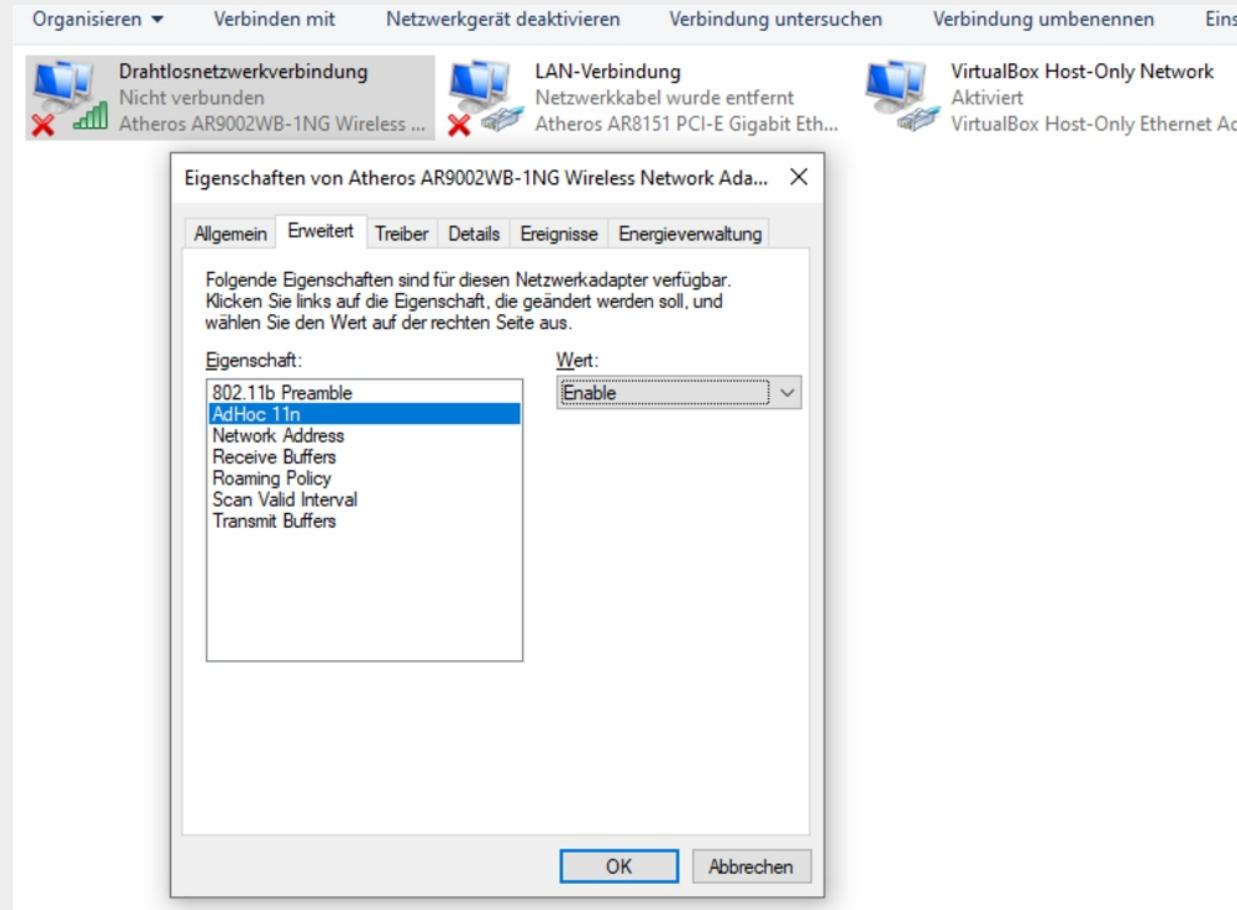
Grundsätzlicher Funkzellenaufbau



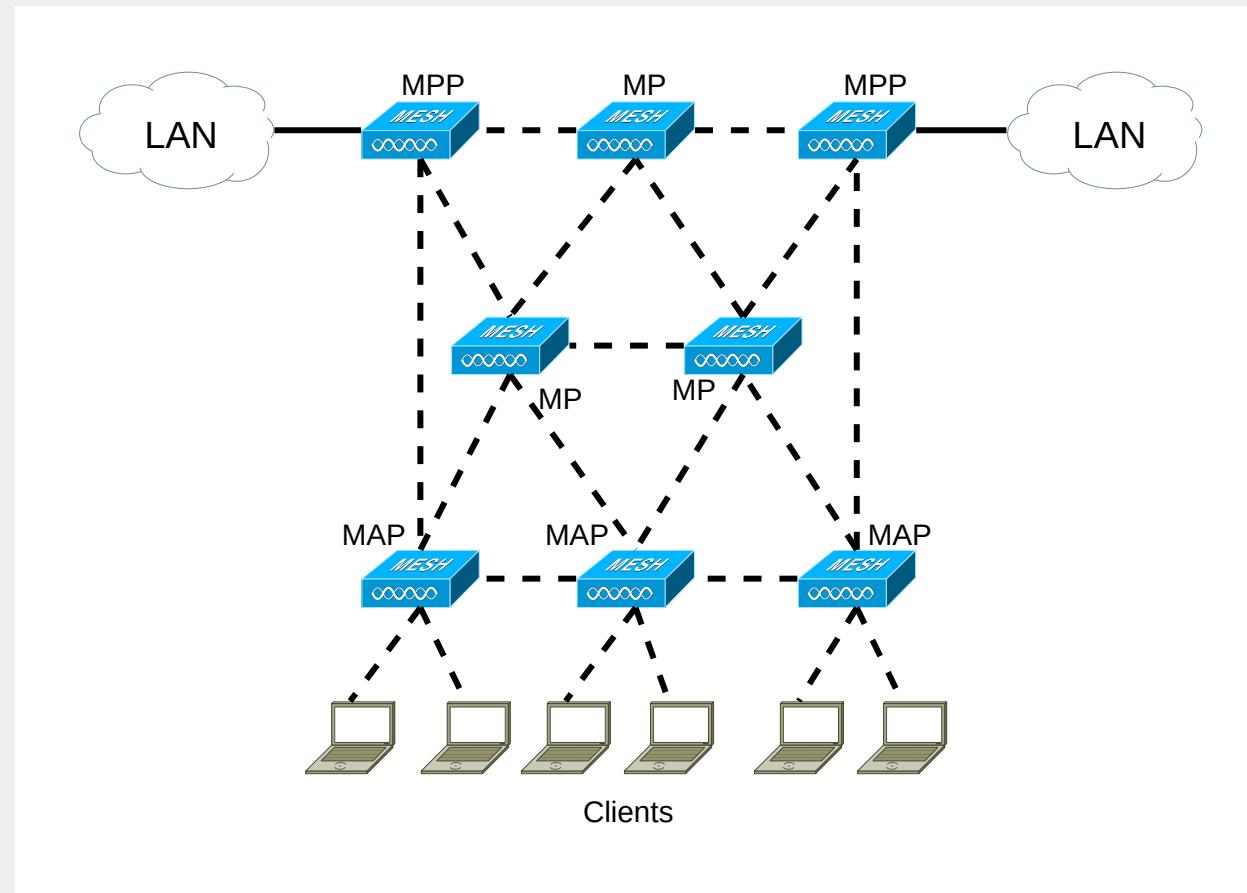
Modi



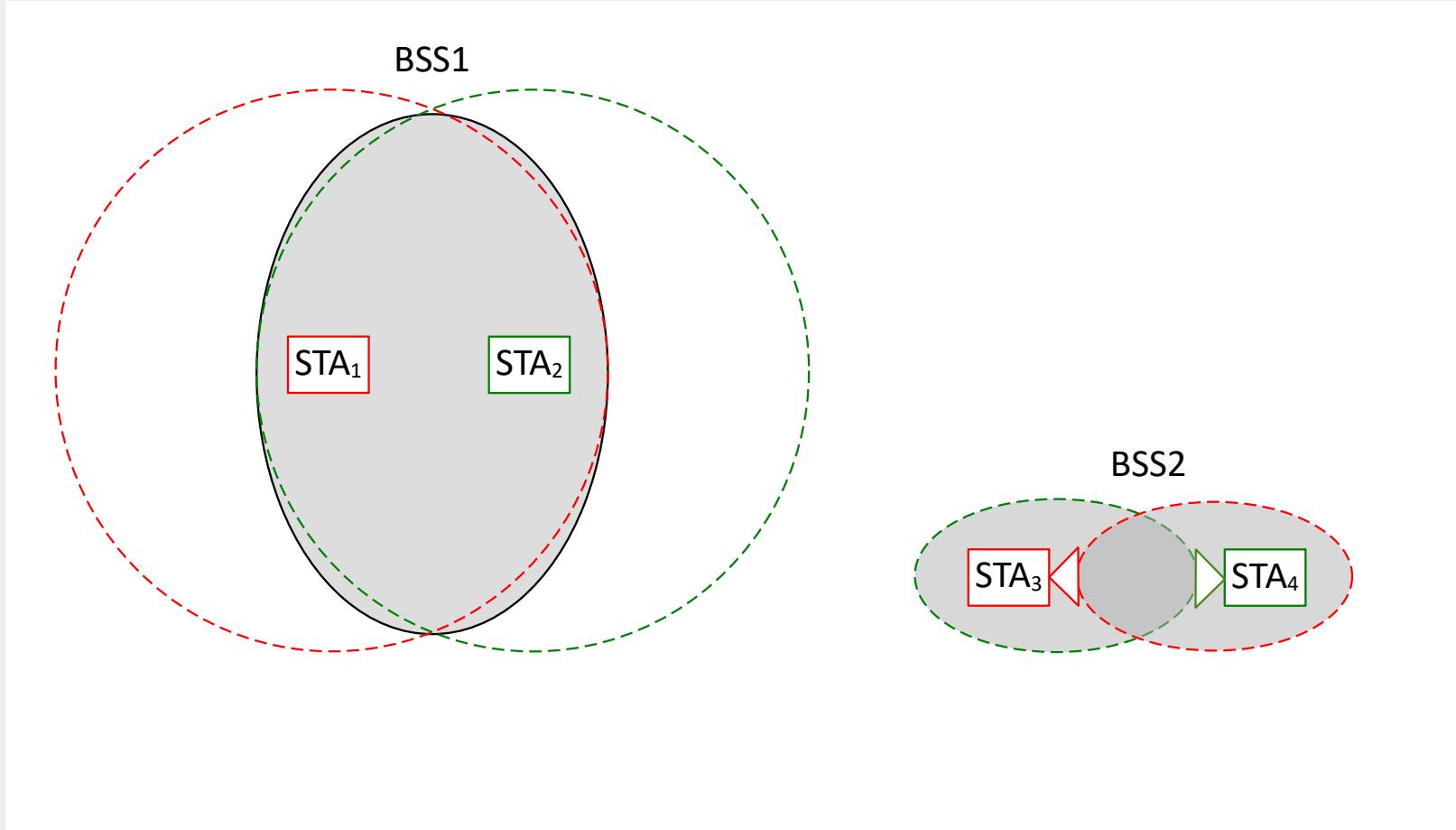
Einstellung des Ad-hoc-Modus unter Windows 10



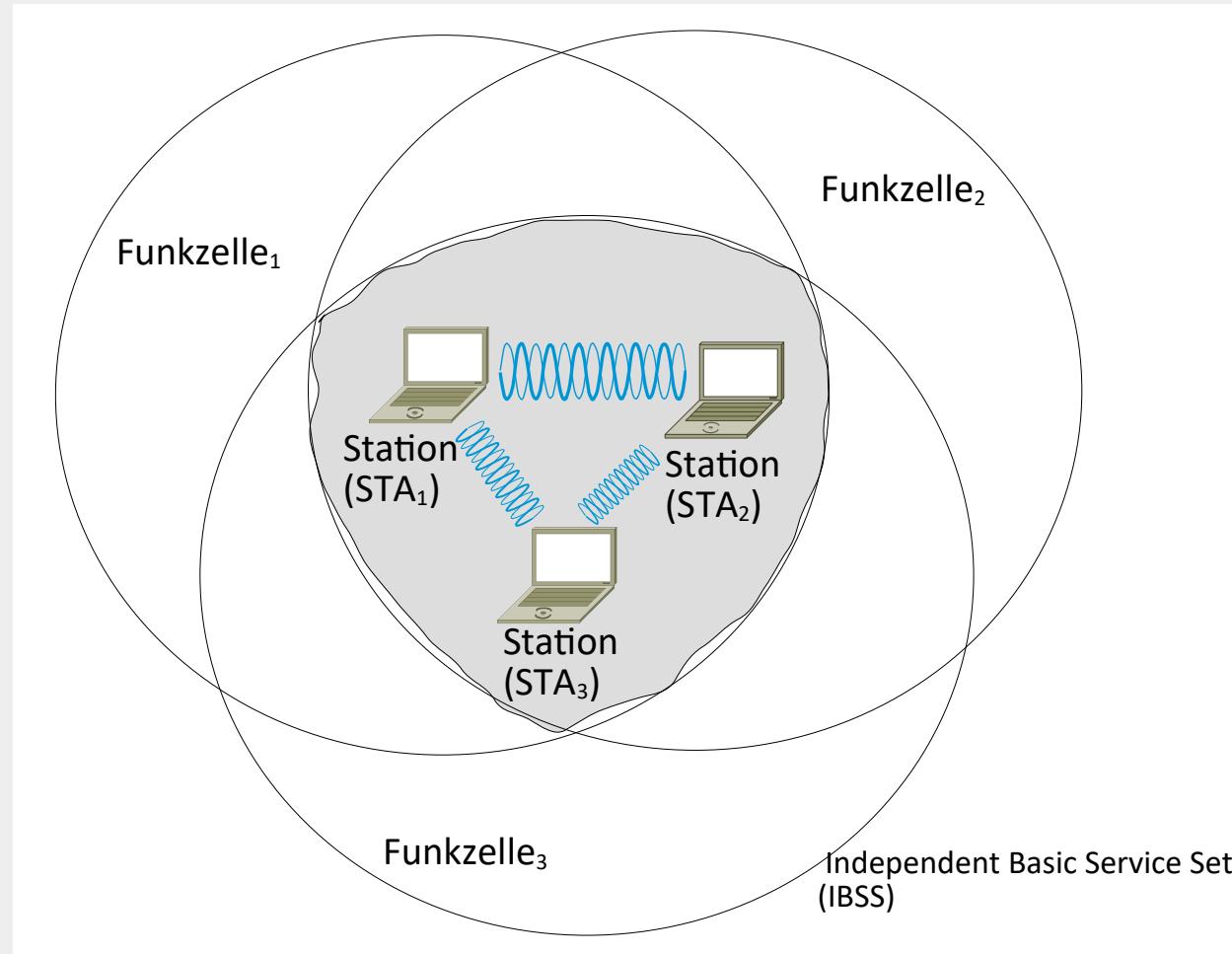
Vermischte Struktur



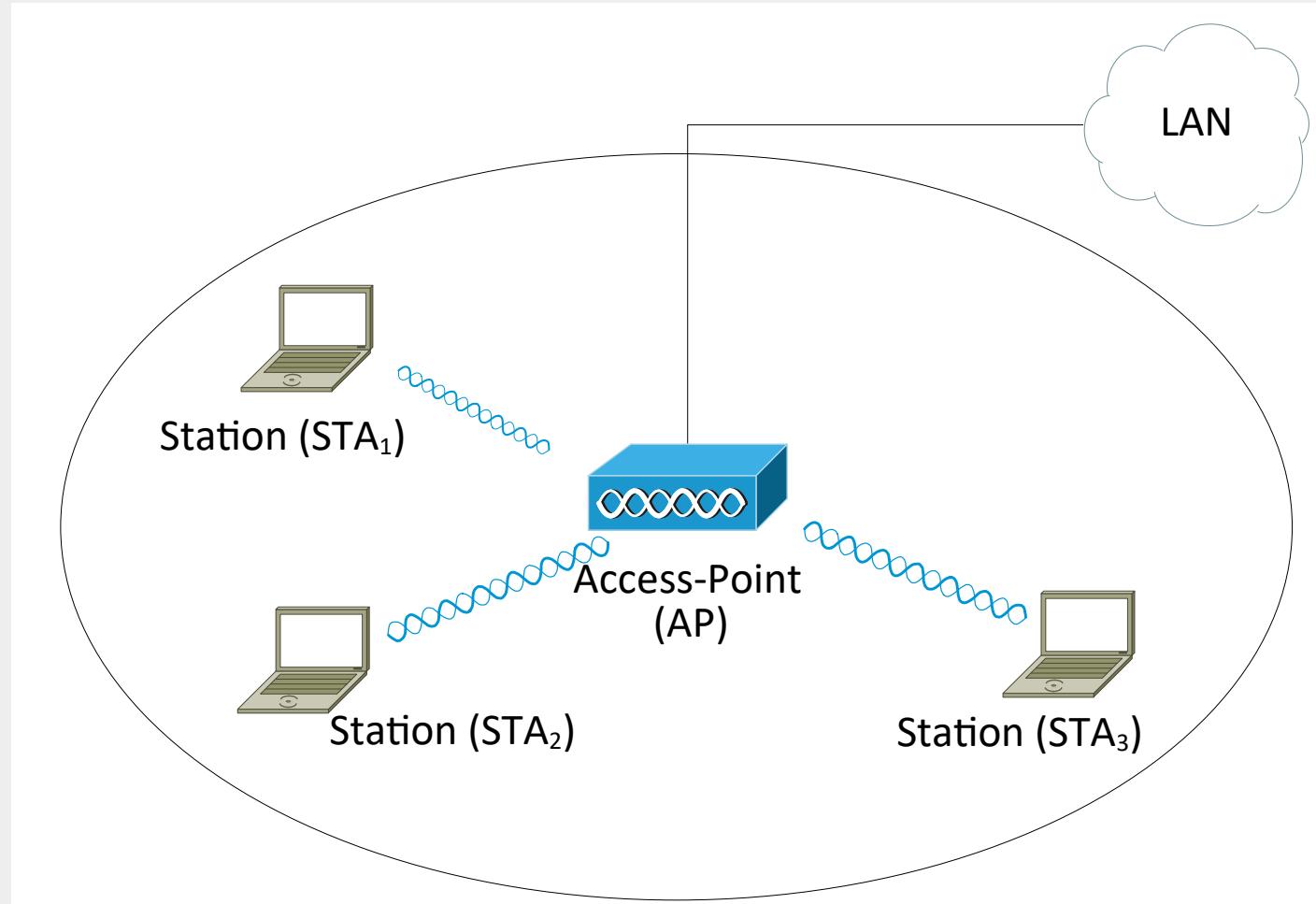
Topologie / Architektur / Service-Sets (BSS in einfachster Ausprägung)



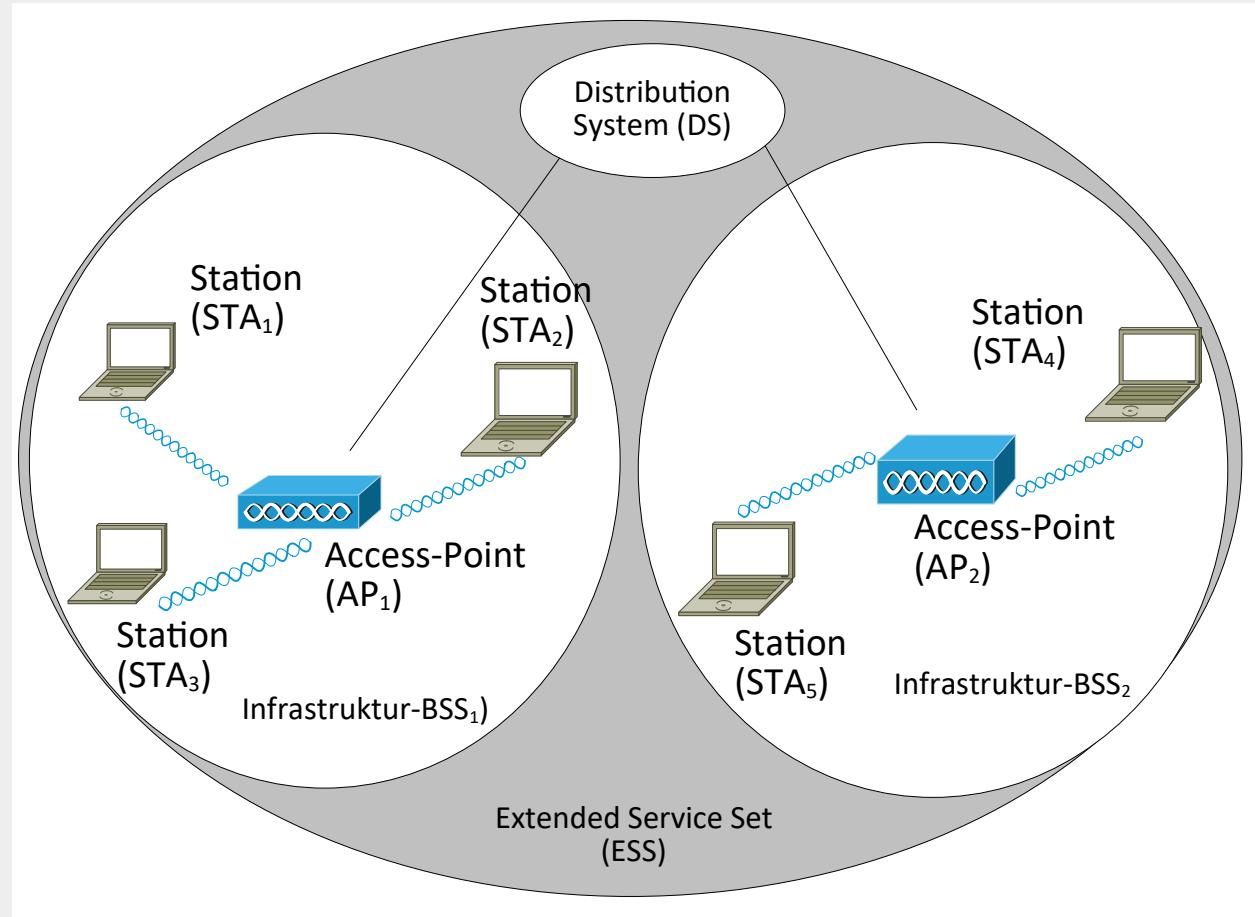
Service-Sets (Independent Basic Service Set (IBSS))



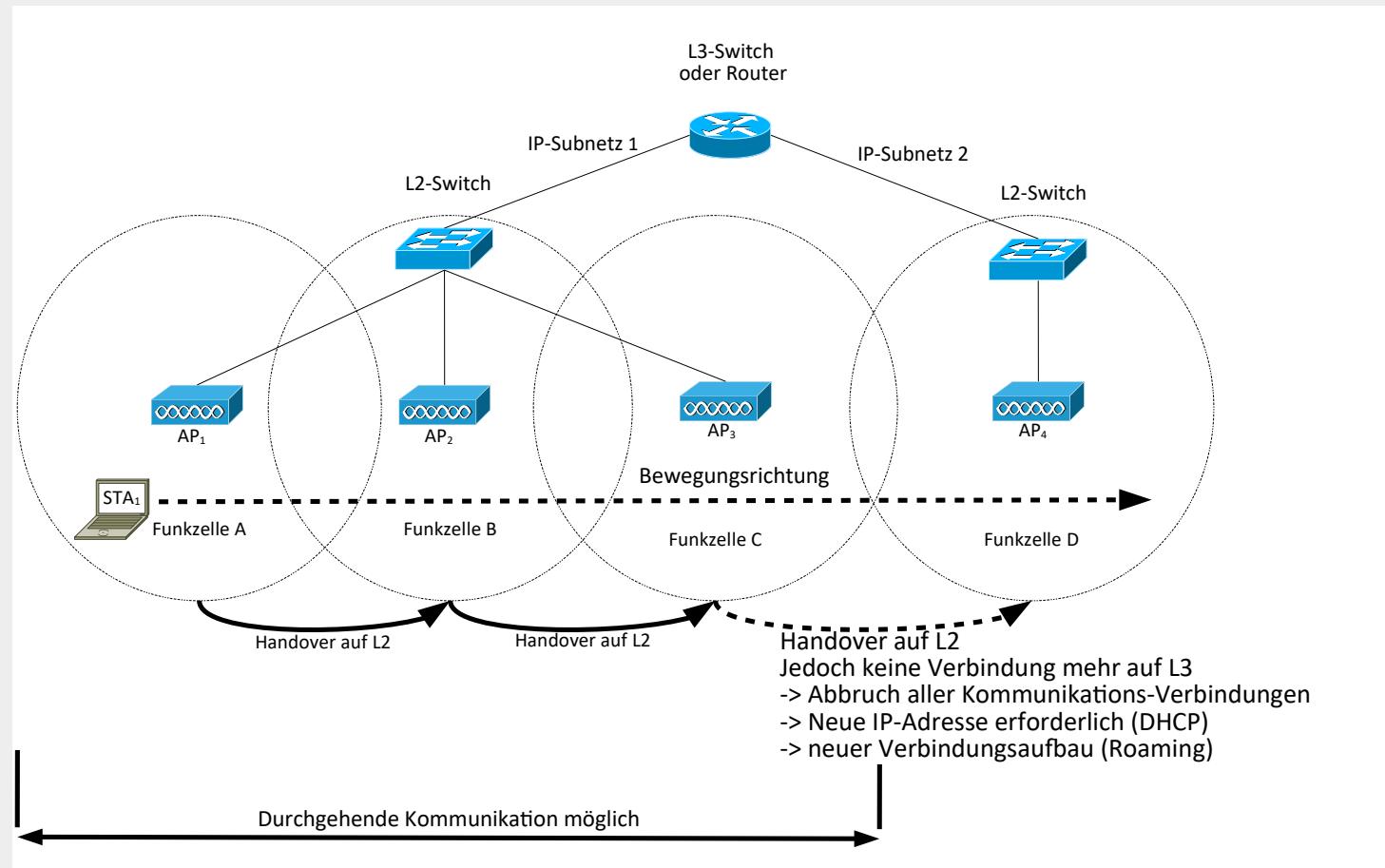
Service-Sets (Infrastruktur BSS)



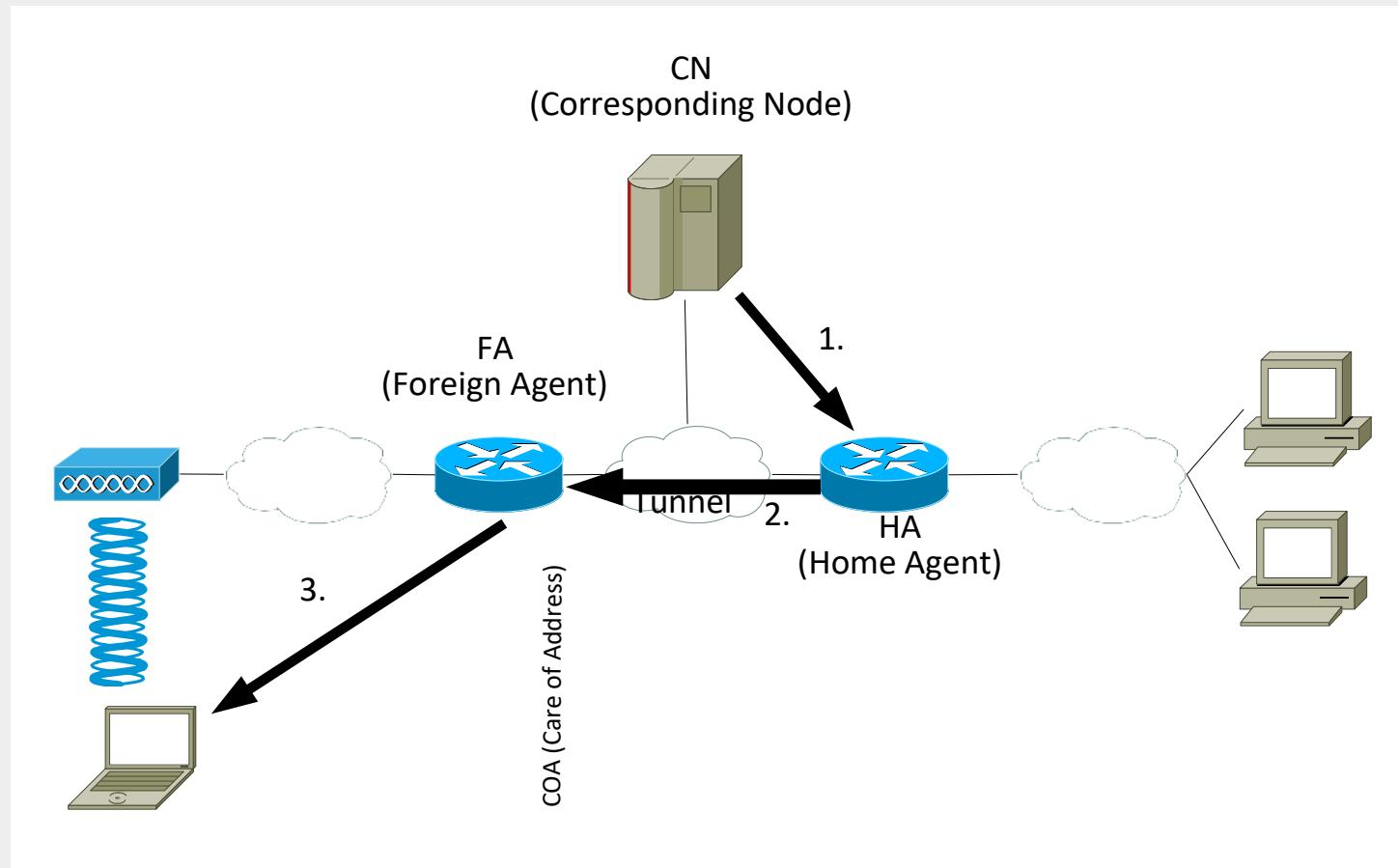
Service-Sets (Extended Service Set / QBSS)



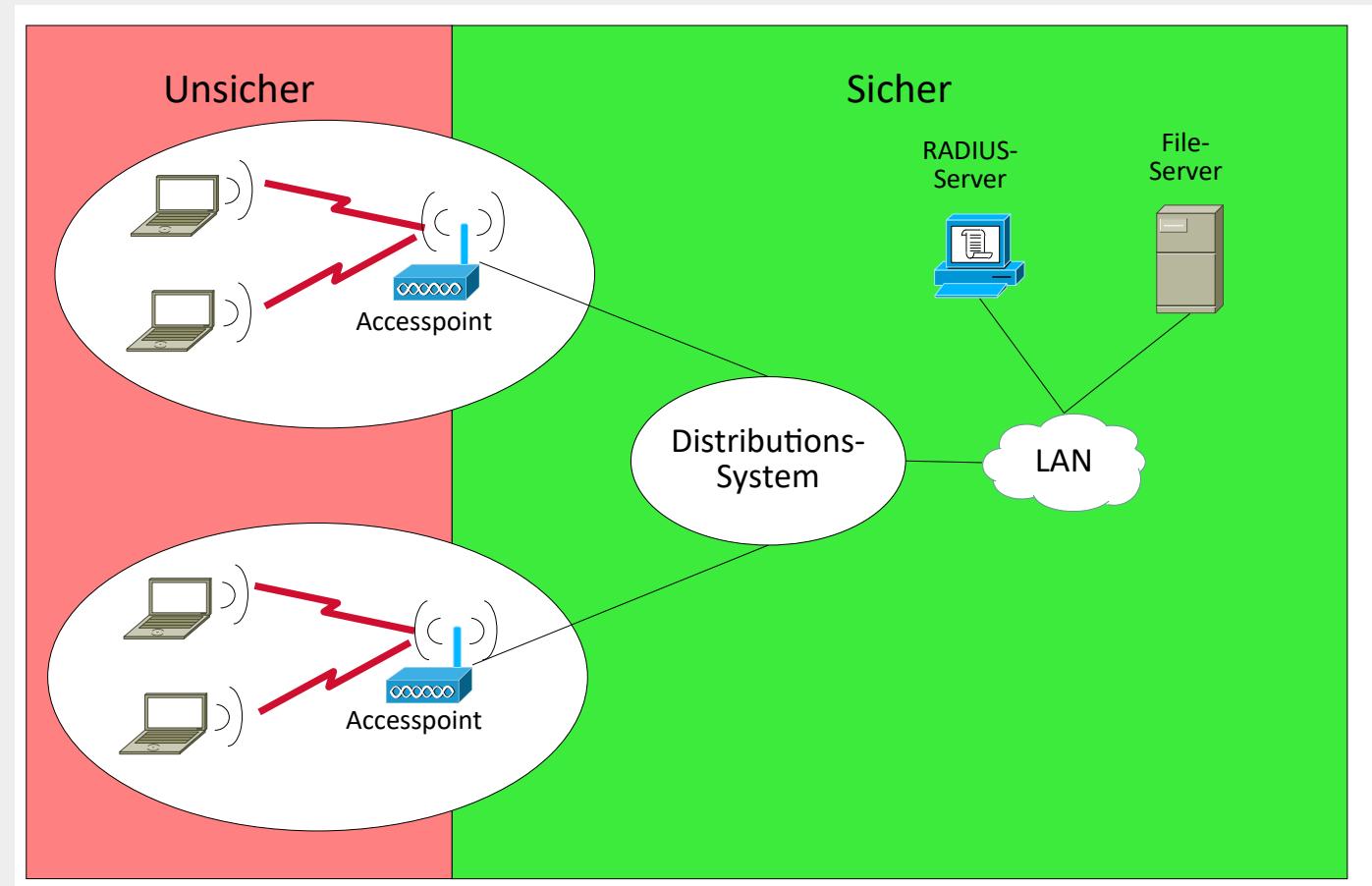
Handover / Roaming



Mobile IP



Sicherheit ?!?



Inhalt

- Historisches
- Gründe für und gegen WLANs
- Abgrenzung zu weiteren WLAN-Technologien
(Bluetooth, WiMAX, Mobiltelefonstandards)
- Allgemeine Grundlagen von Funknetzen (Funknetzaufbau)
- Modi (Ad-hoc, Infrastruktur, Bridge und Mesh-Modus)
- Architekturen / Service Sets (BSS, IBSS, PBSS, ESS, QBSS)
- Handover / Roaming
- Mobile IP
- Sicherheit

WLAN-Vorlesung

Teil-1

Stand: 14.05.24

- Historisches
- Gründe für und gegen WLANs
- Abgrenzung zu weiteren WLAN-Technologien
(Bluetooth, WiMAX, Mobiltelefonstandards)
- Allgemeine Grundlagen von Funknetzen (Funknetzaufbau)
- Modi (Ad-hoc, Infrastruktur, Bridge und Mesh-Modus)
- Topologien / Architekturen / Service Sets (BSS, IBSS, PBSS, ESS, QBSS)
- Handover / Roaming
- Mobile IP
- Sicherheit



Quelle: <https://commons.wikimedia.org/w/index.php?curid=52853789>

Einige Hersteller hatten bis zum Erscheinen von IEEE802.11 im Jahre 1997 bereits Produkte auf dem Markt. Allerdings waren das proprietäre Lösungen, die immer nur mit den Geräten des Herstellers funktionierten. Auch mit Erscheinen des Standards IEEE802.11 war die herstellerübergreifende Zusammenarbeit der Geräte ein Glücksspiel. Die Parameter des Standards boten zu viele Freiheitsgrade was den Herstellern zu viel Spielraum für Interpretationen ließ.

Erst nachdem die Wireless Ethernet Compatibility Alliance (WECA*) sich 1999 zusammen gefunden hatte, konnte eine Akzeptanz herbeigeführt werden, indem eine Testumgebung definiert wurde. Wer ein Zertifikat haben wollte, musste die Tests bestehen.

Dafür mussten sich die Hersteller auf einen kleinsten gemeinsamen Nenner einigen und ihn auch umsetzen.

Dies hat dann dazu geführt, dass Geräte unterschiedlicher Hersteller zusammen funktionierten. (Interoperabilität)

* Heute heißt die Vereinigung Wi-Fi-Alliance (WFA) und hat über 700 Mitglieder.

Es gibt gute Gründe für die Vernetzung von Rechnern mittels WLAN:

- Räumliche Flexibilität innerhalb des Empfangsbereichs.
- Keine Verkabelungsprobleme. Verkabelung ist nicht nur teuer, sondern unter bestimmten Umständen gar nicht möglich.
Wie zum Beispiel bei denkmalgeschützten Gebäuden, kann nicht an beliebigen Stellen die Wand aufgestemmt werden und mal eben eine Leitung eingezogen werden. Wer seine Firma über mehrere Gebäude in einer Stadt evtl. gegenüber auf der anderen Straßenseite untergebracht hatte, musste über teure Stand- oder Wählleitungen die Verbindungen herstellen.
- Ad-hoc-Netzwerke ohne aufwändige Planung möglich.
- Keine Lizenzen (Genehmigungen / Gebühren) erforderlich.

Die Flexibilität mobiler Geräte ist ein großer Vorteil. Nicht umsonst haben sich auch schnurlose Telefone durchgesetzt.

Probleme mit einer Verkabelung von Endgeräten entfallen. Das ist ein Vorteil. Allerdings ist müssen die Accesspoints trotzdem noch an ein Netzwerk angeschlossen und mit Strom versorgt werden!

Schnelle Verbindungen in Ad-hoc-Netzwerken ermöglichen einen einfachen Datentransfer zwischen Endgeräten.

Ein großer Kostenfaktor könnte eine fällige Lizenzierung sein. Deshalb wird große Aufmerksamkeit auf die Verwendung von lizenfreien Frequenzbändern gelegt. Die sind aber bei ständig wachsendem Bandbreitenhunger sehr schwierig zu bekommen (Siehe Wi-Fi 6E)

Dem gegenüber stehen jedoch auch Nachteile:

- Gegenüber Verkabelung langsam.
- Hohe Bitfehlerraten im Vergleich zu LANs.
- Nationale Restriktionen (Es gibt keine einheitlichen internationale Frequenzbänder.
Bestenfalls überschneidende Bereiche)
- Sicherheit durch die Funkstrecke als „Shared Media“.
- Kosten. Wer ein WLAN in Betrieb nimmt muss trotzdem erst einmal verkabeln, denn die Access-Points (APs) müssen angeschlossen werden (sowohl an ein LAN als auch an eine Stromversorgung).

Trotz aller Verbesserungen hinken die WLAN-Standards den verkabelten Netzwerken hinterher. Das gilt vor allem, wenn viele Stationen an einem Accesspoint verbunden sind.

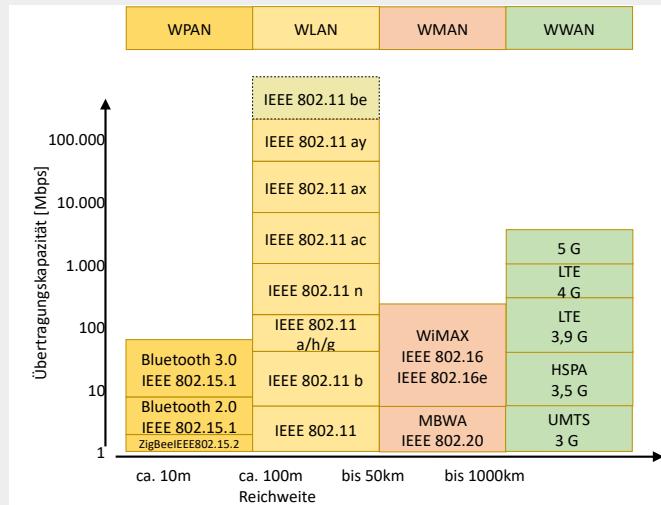
Wenn dann noch die Distanz zwischen Endgerät zum AP größer wird, steigen die Bitfehlerraten. Um den Fehlern entgegen zu wirken, wird auf robustere Übertragungsverfahren zurückgeschaltet, was die Geschwindigkeit der Datenübertragung verringert .

Ein WLAN-Gerät funktioniert leider nicht überall auf der Welt gleich. Das liegt vor allem an nationalen Restriktionen, wie unterschiedliche freigegebene Frequenzbänder und Sendeleistungen.

Trotz immer weiter verbesserten Verfahren, um die Datenverbindung über die Luftschnittstelle sicherer zu machen, handelt es sich immer noch um ein Shared Media. Mit geringem Aufwand kann der Datenstrom mitgelesen werden und mit entsprechendem Aufwand lässt er sich dann später auch entschlüsseln.

Die Anbindung der APs erfordert trotzdem noch eine Stromversorgung und eine LAN-Anbindung. Wer also drahtlos Daten übertragen will, muss zuerst einmal verkabeln.

Einbettung in weitere Funklösungen



Wenn man Funklösungen nach Reichweite sortiert, kann man die Bereiche der Folie festlegen:

10cm → (RFID)

10m → WPAN (Bluetooth)

100m → WLAN (IEEE802.11xx)

50km → WMAN (WIMAX, MBWA)

1000km → WWAN (LTE, 5G)

Diese Einteilung beinhaltet Überschneidungen. So können mit Richtantennen WLANs auch über einige Kilometer hinweg betrieben werden.

Es gab und gibt noch weitere Lösungen auf Funk-Basis:

- NFC
- Bluetooth
- ETSI (Hiperlan2)
- RadioLAN
- HomeRF
- DECT
- Infrarot

NFC (Near Field Communicaton) hat sich auf Distanzen bis zu wenigen cm mittlerweile etabliert.

Bluetooth ist auf kürzeren Strecken bis zu 10m erfolgreich.

ETSI (Hiperlan2) ist eine rein europäische Lösung im WLAN-Umfeld. Trotz guten Ansätzen konnte sich der Standard nicht durchsetzen. Allerdings wurden Teile wie die Dynamic Frequency Selection (DFS) und Transmission Power Control (TPC) später von IEEE802.11 übernommen.

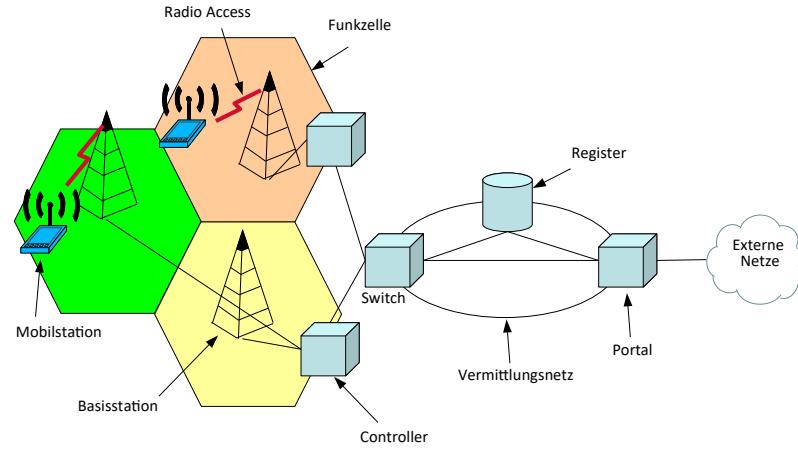
RadioLAN hatte nur in den USA Anwendung gefunden und ist mittlerweile bedeutungslos.

HomeRF war für die Heimvernetzung gedacht und sollte bis zu 10MBit/s an Datenübertragungsrate liefern. Ist mittlerweile bedeutungslos.

DECT (Digital Enhanced Cordless Telephone) hat nicht nur einen Sprachsondern auch einen Datenkanal. Hat sich nur für die Sprachübertragung bei schnurlosen Telefonen durchgesetzt und wird mittlerweile von Telefonen mit Voice over WLAN (VoWLAN) abgelöst.

Infrarot war für die Kopplung von Notebooks schon weit verbreitet und im IEEE802.11-Standard hinterlegt, hat sich jedoch bei neuen Standards nicht mitentwickelt.

Grundsätzlicher Funkzellaufbau



Eine **Funkzelle** hat mindestens eine Basistation (das kann auch nur ein Notebook sein)

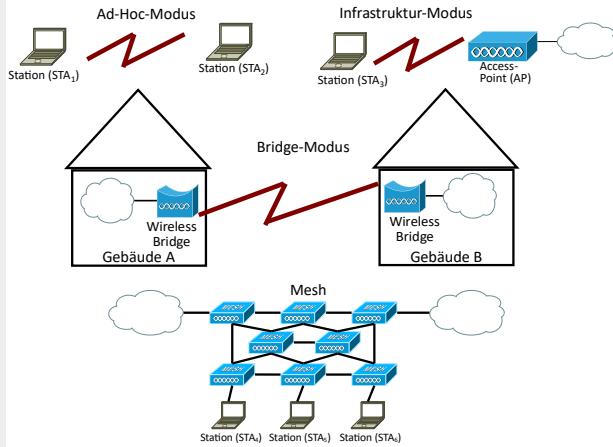
Die **Basistation** erstellt zusammen mit der Sendeeinheit und der Antenne die Funkzelle. Je nach Leistung der Sendeeinheit sowie der Antennenbauform ist die Größe der Funkzelle gegeben.

Mit dem **Controller** werden die Funkzellen verwaltet (zusammengefasst oder getrennt)

Das **Register** verwaltet die Mobilstationen. Hier werden die Themen Zugangskontrolle, Abrechnung usw. abgehandelt.

Das **Portal** ermöglicht die Verbindung zu anderen Netzwerken.

Modi



Modi, in denen WLANs betrieben werden können:

Im **Ad-hoc-Modus** können zwei oder mehrere Stationen über eine WLAN-Verbindung direkt Miteinander kommunizieren.

Im **Infrastruktur-Modus** wird eine WLAN-Zelle von einem Access Point (AP) verwaltet. Jede Kommunikation zwischen den Teilnehmern des Netzwerks geht über den AP. Direkte Verbindungen zwischen den Stationen sind nicht vorgesehen. Oft bieten die APs eine Verbindung zu anderen Netzwerken.

Damit lassen sich Stationen, die nur über eine WLAN-Schnittstelle verfügen, an einen drahtgebundenen Server oder an das Internet anschließen. Das Netzwerk kann mit entsprechenden Antennen räumlich ausgedehnt werden. So sind zwischen 30m in Räumen und bis zu einigen Kilometern im Freien möglich.

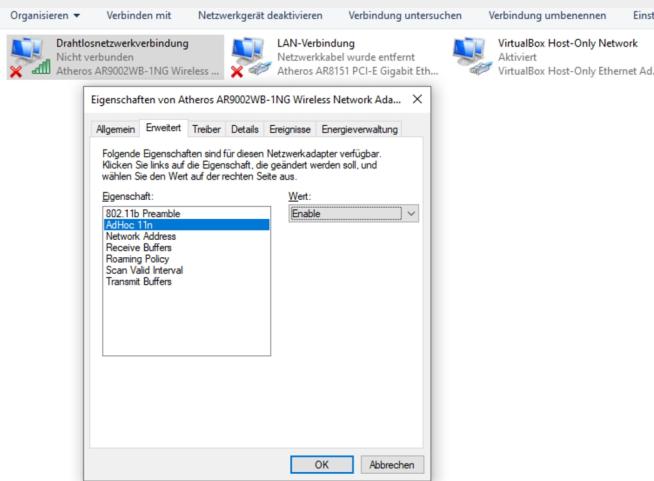
Auch Filtermöglichkeiten sind in APs untergebracht. So kann auf MAC-Adressen oder Protokolle gefiltert werden.

Da die Funkwellen auch Wände durchdringen können, ist zumindest bei den kurzen Distanzen nicht auf die Line of Sight (LoS) zu achten.

Im **Bridge-Modus** können z. B. zwei Gebäude und das dort vorhandene LAN über eine WLAN Verbindung mit WLAN-Bridges und gerichteten Antennen (Yagi-Antenne) verbunden werden. Hierbei ist auf eine Sichtverbindung (LoS) zu achten.

Ein **Mesh-WLAN** ermöglicht es eine drahtlose Infrastruktur, ohne zugehöriges LAN Distributionsnetzwerk, zu erstellen. Stattdessen wird im IEEE802.11s mit einem Wireless Distribution System (WDS) die Verbindung der Accesspoints beschrieben.

Einstellung des Ad-hoc-Modus unter Windows 10



Grundsätzlich müssen alle Geräte, die miteinander kommunizieren sollen, den gleichen Modus eingestellt haben.

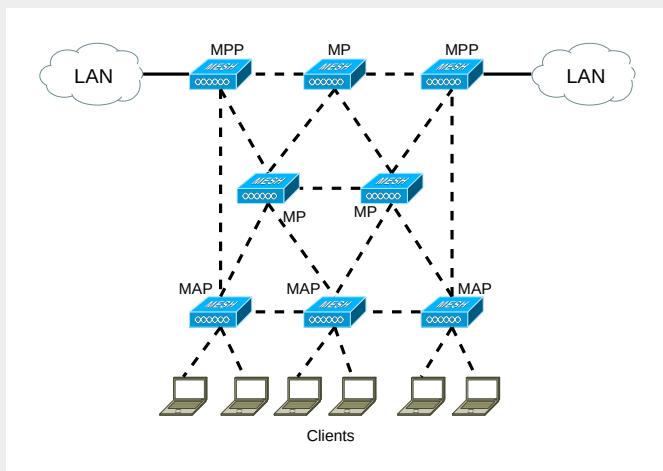
Unter Windows kann der Ad-hoc-Modus folgendermaßen eingestellt werden:

Netzwerkverbindungen:

- Drahtlosnetzwerkverbindung auswählen
- Eigenschaften (über rechte Maustaste)
- Adapter Konfigurieren (anklicken)
- Menü-Erweitert

Unter Windows 11 kann Wifi Direct dafür angewendet werden.

Vermischte Struktur



In der Arbeitsgruppe IEEE802.11s wurde das Mesh-WLAN erarbeitet. Eine vermaschte BSS ist ein WLAN, das aus autonomen Stationen besteht. Die Stationen bauen untereinander drahtlose Verbindungen auf um wechselseitig MSDUs auszutauschen. Innerhalb des Mesh-BSS (MBSS) nutzen die Stationen die Mesh Coordination Function (MCF) um auf den Kanal zuzugreifen. Die MCF basiert auf der QoS.

Bei einem Mesh-WLAN werden 3 neue Stationsformen eingesetzt:

Mesh Access Points (MAPs)

Diese Geräte stellen die Verbindungen zu den Clients her und verhalten sich gegenüber ihnen wie Access Points (APs). Damit bieten sie den Clients den Zugangspunkt zum WLAN. Weiterhin halten sie über ein weiteres WLAN-Interface die Verbindung zu anderen MAPs, MPs und MPPs. Die WLAN-Interfaces arbeiten entweder im selben oder anderen Frequenzbändern.

Mesh Points (MPs)

Diese Geräte dienen nur dem Weitertransport von WLAN-Daten über WLAN und bieten daher für Clients keinen Zugangspunkt an. MPs dienen daher nur der Vergrößerung der Ausdehnung des WLANs.

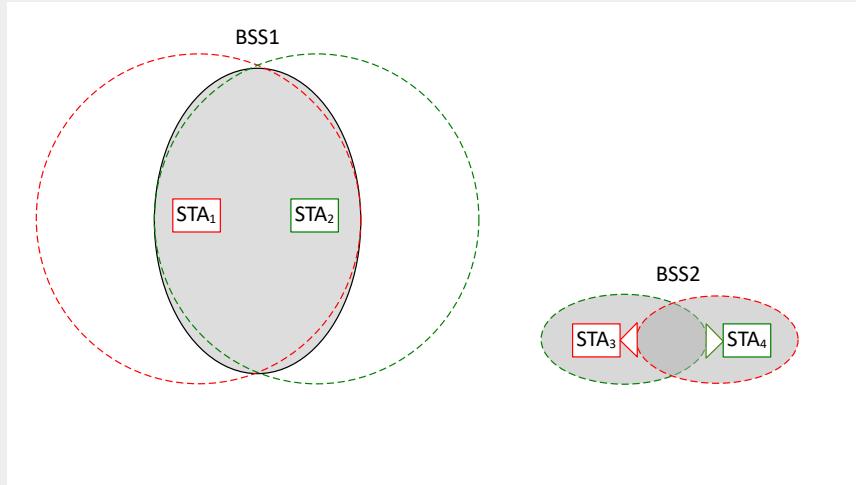
Mesh Portals (MPPs)

MPPs bieten eine Gateway-Funktion in andere Netzwerke oder andere WLANs. Sie haben also z. B. eine LAN-Schnittstelle. In einem Mesh-WLAN können mehrere MPPs vorhanden sein.

Die Verwaltung eines Mesh erfolgt autonom. Dazu erkennen die Knoten ihre Nachbarn automatisch. Sie wählen zusammen die Kanäle aus und erstellen die Verbindungen. Anpassungen erfolgen automatisch. D. h. Hinzukommende und wegfallende Mesh-Knoten werden automatisch eingefügt oder entfernt. Dazu senden die Mesh-Knoten zyklisch Informationen aus anhand derer die benachbarten Mesh-Knoten die Existenz von Nachbarknoten in Erfahrung bringen können.

Die Wegewahl durch das Mesh erfolgt auf der Basis von größter Bandbreite, kürzeste Latenzzeit und geringste Anzahl von Hops. Sie erfolgt auf der MAC-Ebene und ist für die WLAN-Stationen, sowie für höhere Protokollsichten, transparent.

Topologie / Architektur / Service-Sets (BSS in einfachster Ausprägung)



Im Zusammenhang mit den Ausprägungen von WLANs für unterschiedliche Anwendungszwecke werden in der Literatur oft die Bezeichnungen Topologien, Architekturen oder einfach nur Service-Sets verwendet.

WLANs haben im Sinne von Netzwerk-Topologien die Ausprägung von Zellen. Um Verwechslungen mit Protokoll-Architekturen zu vermeiden, soll im Folgenden von Service-Sets gesprochen werden. Das macht der Standard IEEE802.11 auch so.

Jedes Gerät, das einen entsprechenden Adapter eingebaut hat, kann eine Funkzelle aufbauen. Im einfachsten Fall baut eine Station einen kreisförmigen Funk-Abdeckungsbereich um sich herum auf.

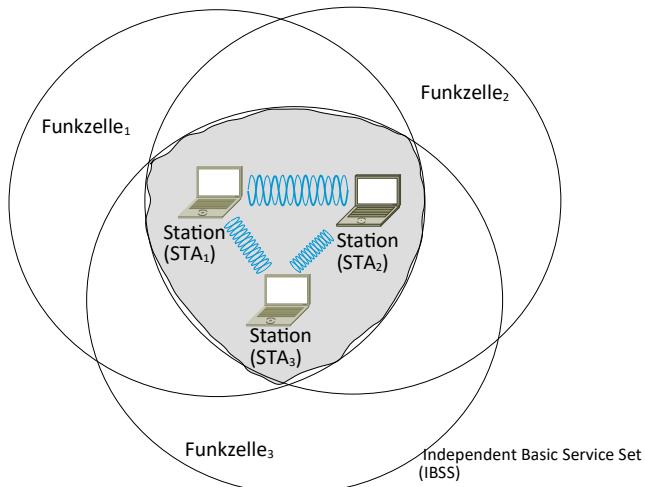
Der Bereich, in dem sich die Abdeckungsbereiche zweier Funkzellen überschneiden kann für einen Datenaustausch genutzt werden, sobald die Stationen im selben Kanal (auf der gleichen Frequenz) mit der gleichen Technologie (Kodierung) arbeiten.

Mit der Einführung von Directional Multi-Gigabit (DMG) kann die Form einer Funkzelle mit Beamforming zu einer Keule geformt und in der Richtung ausgerichtet werden. Das ermöglicht es wie beim BSS2 die Richtung, die Größe und somit auch in der Reichweite der Funkzellen zu optimieren. Damit können Überschneidungen und somit auch Störungen von anderen BSSs reduziert werden.

Der Aufbau eines BSS ist sehr einfach und bedarf keiner besonderen Planung oder Verkabelung. Oft wird diese Form nur für die kurze Zeit eines Datenaustauschs aufgebaut und genutzt.

Die Mitgliedschaft einer Station in einem BSS ist dynamisch. Sie können jederzeit eingeschaltet und wieder ausgeschaltet werden. Mobile Stationen kommen in den Funkbereich eines BSS und sie verlassen den Funkbereich auch wieder. Um ein Mitglied in einer BSS zu werden, müssen die Stationen sich mit dem BSS verbinden / synchronisieren. Um alle Dienste einer BSS nutzen zu können muss eine Station sich mit der BSS assoziieren.

Service-Sets (Independent Basic Service Set (IBSS))

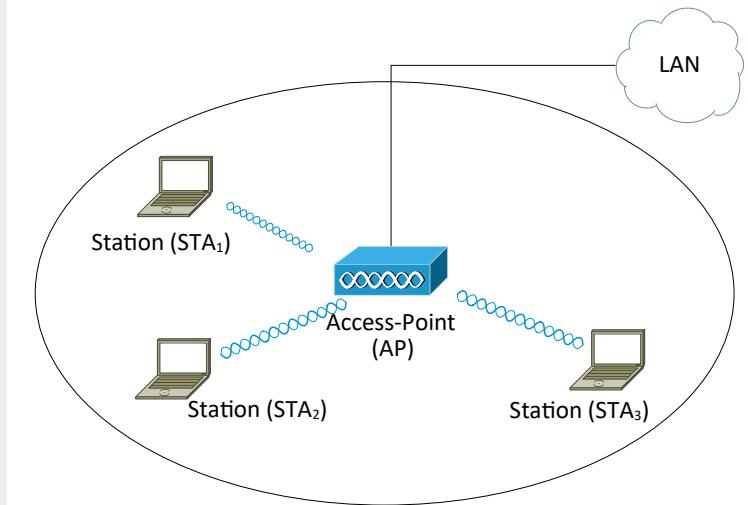


Zu einem BSS können noch weitere Stationen hinzu kommen. Haben die Stationen außer ihren Funkverbindungen keine weiteren Verbindungen, spricht man von einem **Independent Basic Service Set (IBSS)**. Dies ist die einfachste Form eines BSS. Typischerweise handelt es sich hierbei um Netzwerke im Ad-hoc-Modus. Es gibt keine Station die Dienste verwaltet.

Ähnlich wie ein Independent Basic Service Set (IBSS) besteht ein **Personal BSS (PBSS)** aus Stationen, die miteinander kommunizieren können, ohne dass weitere Verbindungen bestehen.

Der Unterschied zu einem IBSS besteht darin, dass eine Station zu einem **PBSS Control Point wird (PCP)**. Damit gibt es eine zentrale Verwaltungseinheit, welche die Zeitsynchronisierung verwaltet und mit Service-Perioden Dienste verwalten und zuteilen kann.

Ein PBSS kann nur von einer DMG Stationen aufgebaut werden. Allerdings ist nicht jede DMG BSS eine PBSS. Eine DMG BSS kann PBSS, oder Teil einer IBSS, oder einer Infrastruktur BSS sein.



Hat ein BSS mit einem **Access Point** (AP) noch eine Verbindung zu einem andern Netzwerk aufgebaut, spricht man von einer **Infrastruktur BSS**. Das ist allerdings keine IBSS! Siehe hierzu auch das Kapitel.

Je nach Umfang des WLANs fallen die Controller, Switches und Register zu einem Gerät (dem AP) zusammen, oder werden auf unterschiedliche Geräte verteilt. Dies gilt vor allem dann, wenn mehrere Funkzellen (BSSs) betrieben werden.

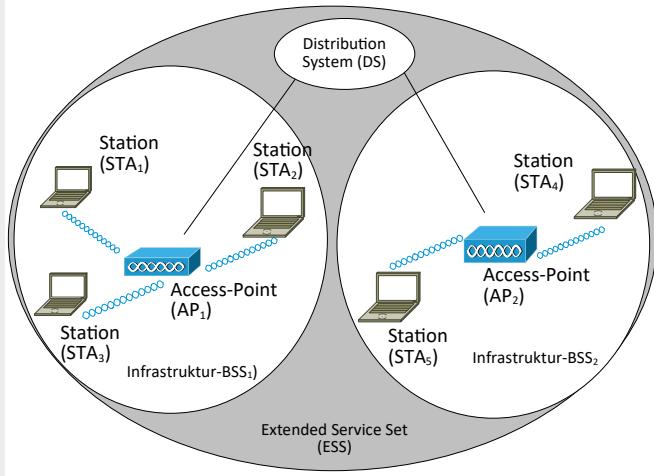
Hinweis:

Geräte die in einem WLAN kommunizieren können werden **Stationen** genannt. Abgekürzt werden sie mit **STA** bezeichnet.

In Beziehung zu einem Accesspoint werden die Stationen auch als Client bezeichnet da zu den APs eine Client-Server-Beziehung besteht.

Accesspoints sind Endgeräte mit zusätzlichen Funktionen.
Abgekürzt werden sie mit **AP** bezeichnet.

Service-Sets (Extended Service Set / QBSS)



Mehrere Infrastruktur-BSSs können über ein Backbone-System, das so genannte Distributions-System (DS), miteinander zu einem **Extended Service Set (ESS)** zusammen geschaltet werden.

Im Allgemeinen wird ein LAN als Distribution System verwendet, denn so kann auch die Verbindung zu anderen kabelgebundenen Netzwerken und somit auch weiteren Diensten ermöglicht werden.

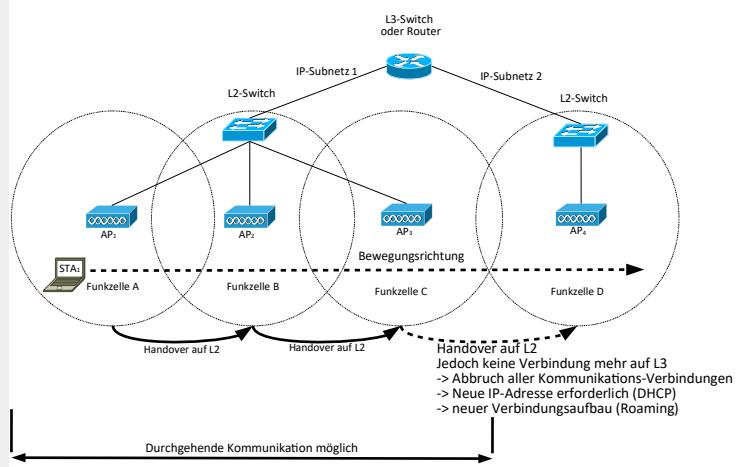
Zusammen mit dem DS bildet ein ESS ein flaches Layer-2-Netzwerk.

Innerhalb eines ESS kann eine Station sich frei bewegen. Dabei wird die Kommunikation auf den Ebenen >2 nicht unterbrochen.

Wechselt die Station von einer Funkzelle in eine andere, wird dieser Vorgang BSS-Transition oder auch Handover genannt. Dabei muss eine Übergabe von der Ausgangs-BSS an die Ziel-BSS erfolgen.

Sobald die APs auch die Quality of Service Funktionen (QOS) abhandeln können spricht man von **Quality of Service APs (QAPs)** die ein **Quality of Service BSS (QBSS)** bereit stellen.

Handover / Roaming



IEEE 802.11 beinhaltet keine nähere Spezifikation des DS. Wi-Fi hingegen legt fest, dass für das DS ein Ethernet zu verwenden ist. Daher kommt auch der Marketingbegriff „Wireless Ethernet“. Da schon die Zugriffs-Verfahren unterschiedlich sind, ist dieser Begriff eher irreführend. Man kann einen AP eher als Bridge im Sinne von Verbinder zwischen Token-Ring und Ethernet sehen.

Bewegt sich ein Client von einer Funkzelle zur nächsten, wird auf Ebene 2 ein Handover (BSS-Transition) vom Client-Adapter durchgeführt. Die Kommunikationsverbindungen bleiben bestehen.
Zellenwechsel können jedoch auch durch schwankende Sendequalität entstehen.

Der Ablauf beim AP-Wechsel ist ähnlich wie beim ersten Verbindungsaufbau

Scanning (aktiv / passiv)

Reassociacion Request

Station sendet Anfrage an APs

Reassociacion Response

Bei einem Erfolg (AP hat geantwortet) nimmt Station nun teil

Bei einem Misserfolg wird weiter gescannt

AP akzeptiert Reassociacion Request

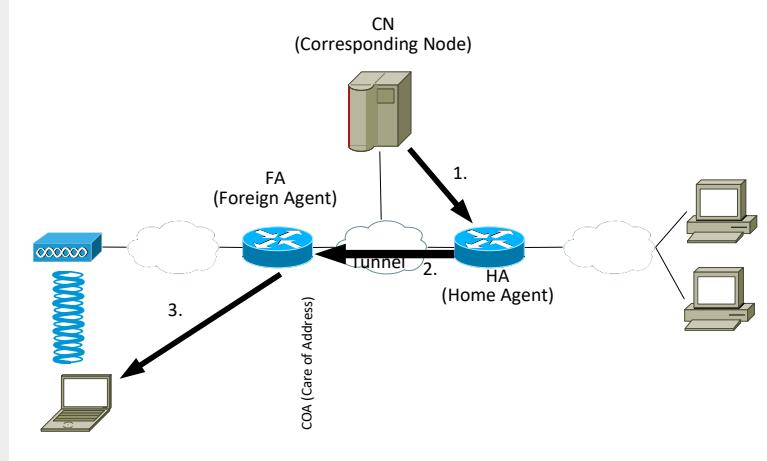
Meldung der neuen Station am Distribution-System

Distribution-System aktualisiert daraufhin seinen Datenbestand

Alter AP wird vom Distribution-System informiert

Im allgemeinen Sprachgebrauch wird das Wechseln von einer Funkzelle in eine andere ebenfalls als Roaming bezeichnet. Dies ist falsch. Denn nur der Wechsel eines Endgerätes von einem Netzbetreiber zu einem anderen bzw. der Wechsel eines Endgerätes von einem Netzsegment (z. B. IP-Netzwerk) zu einem anderen. Somit findet Roaming nur auf Ebene 3 statt und nicht auf den Ebenen 1-2 in denen WLANs aktiv sind.

Mobile IP



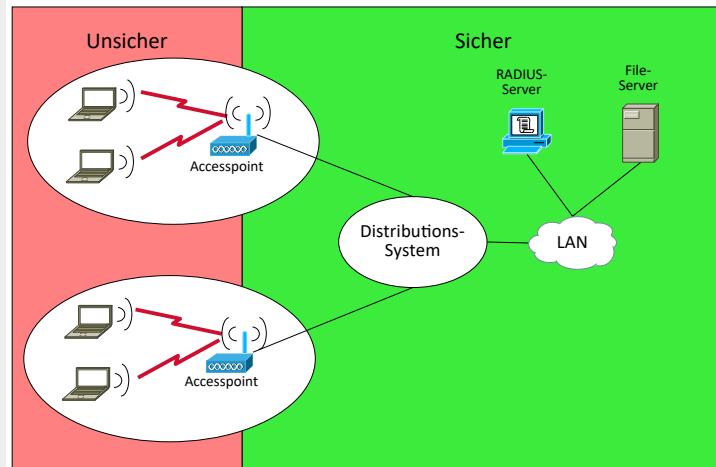
Sobald jedoch der Client das IP-Subnetz wechselt, bleibt zwar die Verbindung auf Ebene 2 bestehen, jedoch ab Ebene 3 aufwärts besteht keine Verbindung mehr. Dies bedeutet, dass eine neue IP-Adresse vergeben werden muss. Die Kommunikation zwischen den Applikationen ist ebenfalls abgeschnitten und muss neu aufgebaut werden.

Soll nun zwischen unterschiedlichen IP-Subnetzen gewechselt werden, gibt es zwei Möglichkeiten:

Dynamische IP-Adress-Vergabe mittels DHCP. Dabei ist ein Neustart der Applikation oder gar des Systems erforderlich.

Mobile IP ermöglicht die Verwendung einer einzigen IP-Adresse auch bei einem IP-Subnetzwechsel. Dies wird dadurch ermöglicht, dass die Pakete an das Heimat-Netz geroutet werden und von da aus an das aktuelle IP Subnetz getunnelt werden.

Sicherheit ?!?



WLANS haben durch die Funkschnittstelle einen unsicheren Bereich der sich schlecht vor Zugriffen schützen lässt. Zumindest das Mithören ist einfach möglich.

Beim Übergang von der Funkschnittstelle zum LAN im AP ist durch geeignete Maßnahmen dafür zu sorgen, dass nur der erwünschte Datenverkehr stattfindet.

Dazu werden im Allgemeinen entweder Firewalls verwendet oder bereits am Access Point, entsprechende Authentifizierungs-Mechanismen, wie IEEE 802.1x zusammen mit einem RADIUS-Server (Remote Authentication Dial In User Service) verwendet.

- Historisches
- Gründe für und gegen WLANs
- Abgrenzung zu weiteren WLAN-Technologien
(Bluetooth, WiMAX, Mobiltelefonstandards)
- Allgemeine Grundlagen von Funknetzen (Funknetzaufbau)
- Modi (Ad-hoc, Infrastruktur, Bridge und Mesh-Modus)
- Architekturen / Service Sets (BSS, IBSS, PBSS, ESS, QBSS)
- Handover / Roaming
- Mobile IP
- Sicherheit