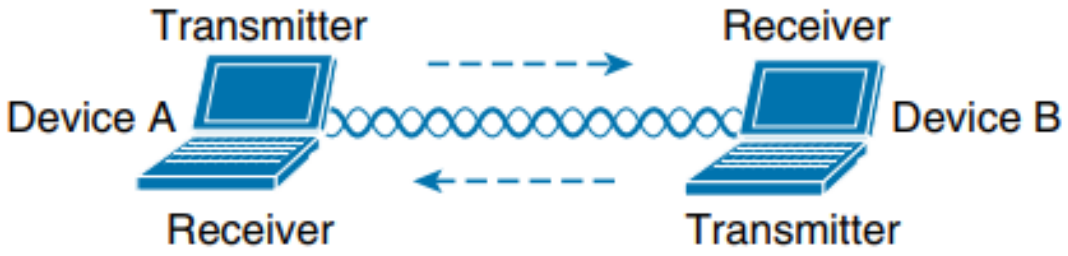
LABORATORIO DI SISTEMI DI RETE

Giacomo Mambelli

Wireless LAN

La comunicazione wireless avviene nello spazio attraverso l'uso di segnali in **radiofrequenza** (RF).

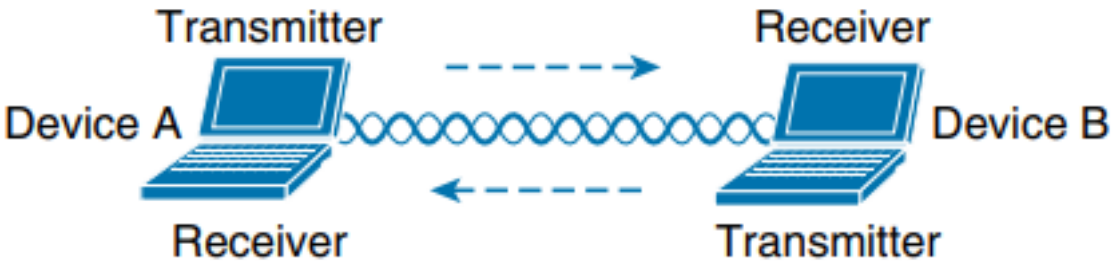
Il trasmettitore può contattare il ricevitore in qualsiasi momento, purché entrambi i dispositivi siano sintonizzati sulla stessa frequenza (o **canale**) e utilizzino tra di loro lo stesso schema per trasportare i dati.



Wireless LAN

Per sfruttare appieno la comunicazione wireless, i dati devono viaggiare in entrambe le direzioni, come mostrato nella figura.

A volte il dispositivo A ha bisogno di inviare dati al dispositivo B, nel mentre il dispositivo B deve **attendere** ed inviare **in un altro momento**

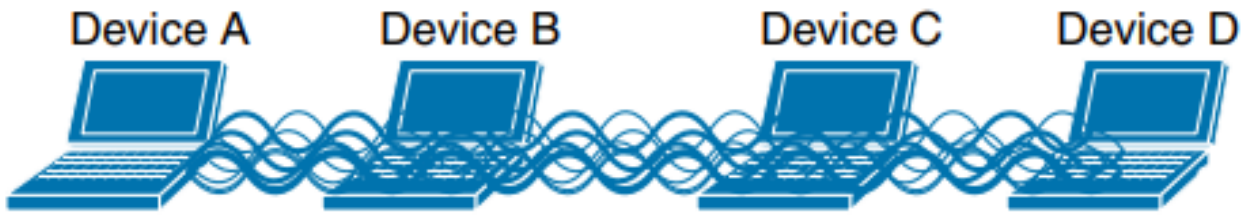


Wireless LAN

Poiché i due dispositivi utilizzano lo stesso canale, due concetti sono di vitale importanza:

- fare a turno
- inviare in altri momenti

Nella comunicazione wireless, se più segnali vengono ricevuti contemporaneamente, possono interferire tra loro. La probabilità di interferenza aumenta con l'aumentare del numero di dispositivi wireless.



Wireless LAN

Per utilizzare efficacemente il mezzo, tutti gli host devono operare in modalità **half-duplex**, in modo da evitare collisioni con altre trasmissioni già in corso.

L'effetto collaterale è che nessun host può trasmettere e ricevere contemporaneamente su un mezzo condiviso.

Per contendersi l'uso del canale, i dispositivi che si basano sullo standard 802.11 devono determinare se il canale è libero e disponibile prima di trasmettere.

Wireless LAN

La soluzione consiste nel rendere ogni area wireless un gruppo chiuso di dispositivi mobili che si forma attorno a un dispositivo che rimane fisso.

Lo standard 802.11 chiama ciò «**insieme di servizi di base» (BSS)**.

Al centro di ogni BSS c'è un punto di accesso wireless (AP). L'AP opera in modalità infrastruttura, ossia offre i servizi necessari per formare l'infrastruttura di una rete wireless.

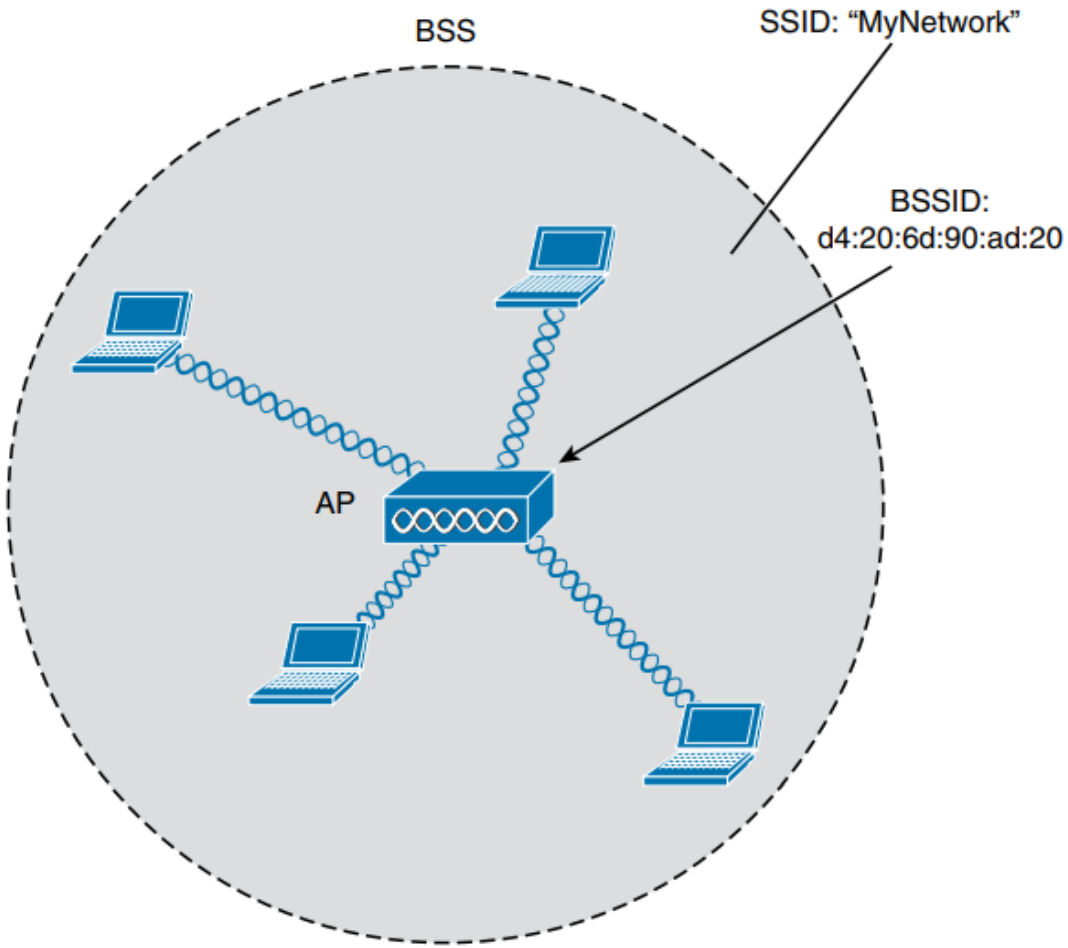
L'Access Point stabilisce inoltre il proprio BSS su un singolo canale wireless.

L'AP e i membri del BSS devono utilizzare tutti lo stesso canale per comunicare correttamente.

Wireless LAN

Poiché il funzionamento di un BSS dipende dall'AP, il BSS è delimitato dall'area in cui il segnale dell'AP è utilizzabile. Questa è nota come **basic service area (BSA) o cella.**

L'adesione al BSS è chiamata associazione. Un dispositivo wireless deve inviare una richiesta di **associazione** all'AP e l'AP deve concedere o negare la richiesta. Una volta associato, il dispositivo diventa un client



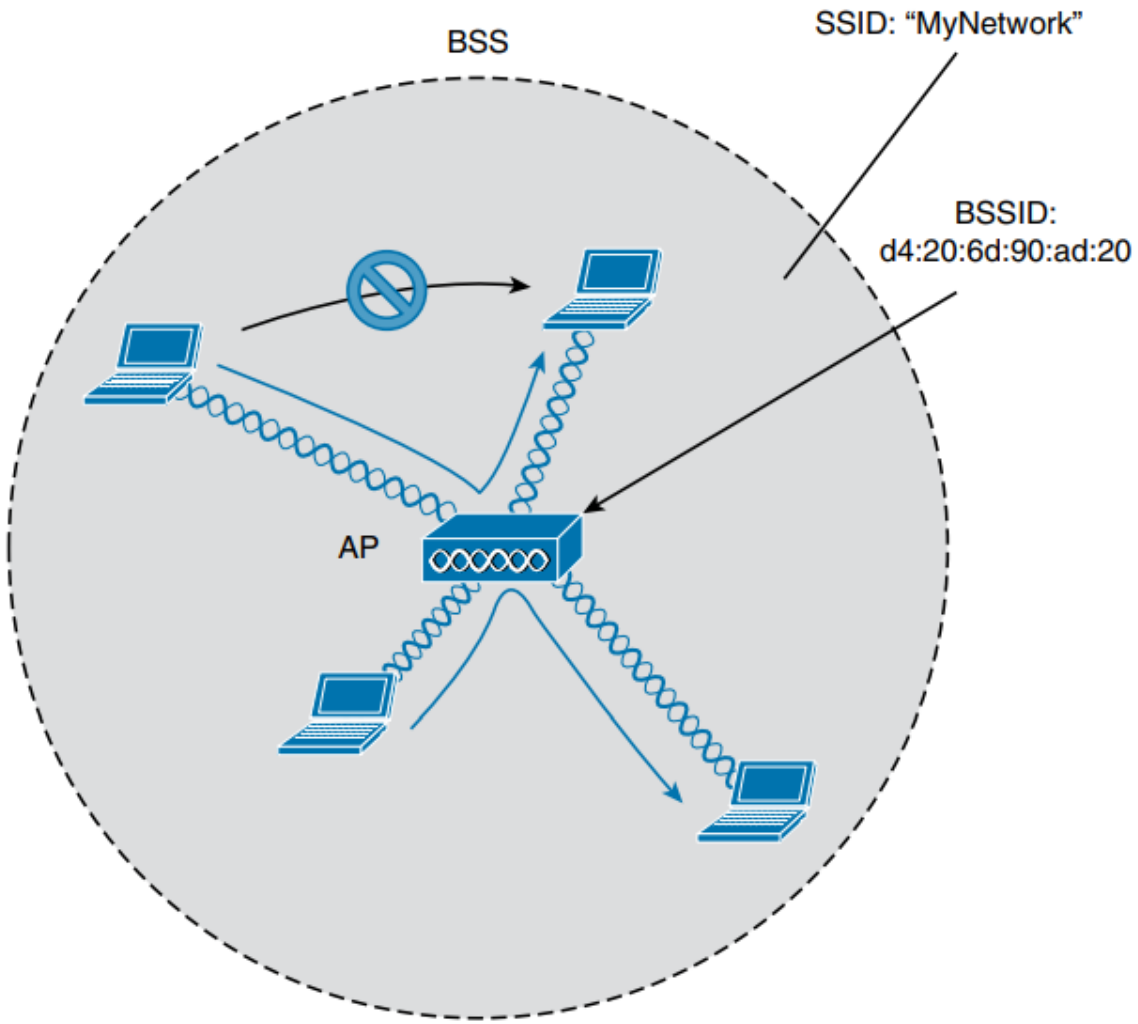
Wireless LAN

Ci si potrebbe chiedere perché tutto il traffico dei client debba attraversare l'AP.

Perché due client non possono semplicemente trasmettere frame di dati direttamente l'uno all'altro e bypassare l'intermediario?

Se i client potessero comunicare direttamente, l'intera idea di organizzare e gestire un BSS non avrebbe senso.

Inviando i dati prima attraverso l'AP, il **BSS rimane stabile e sotto controllo.**

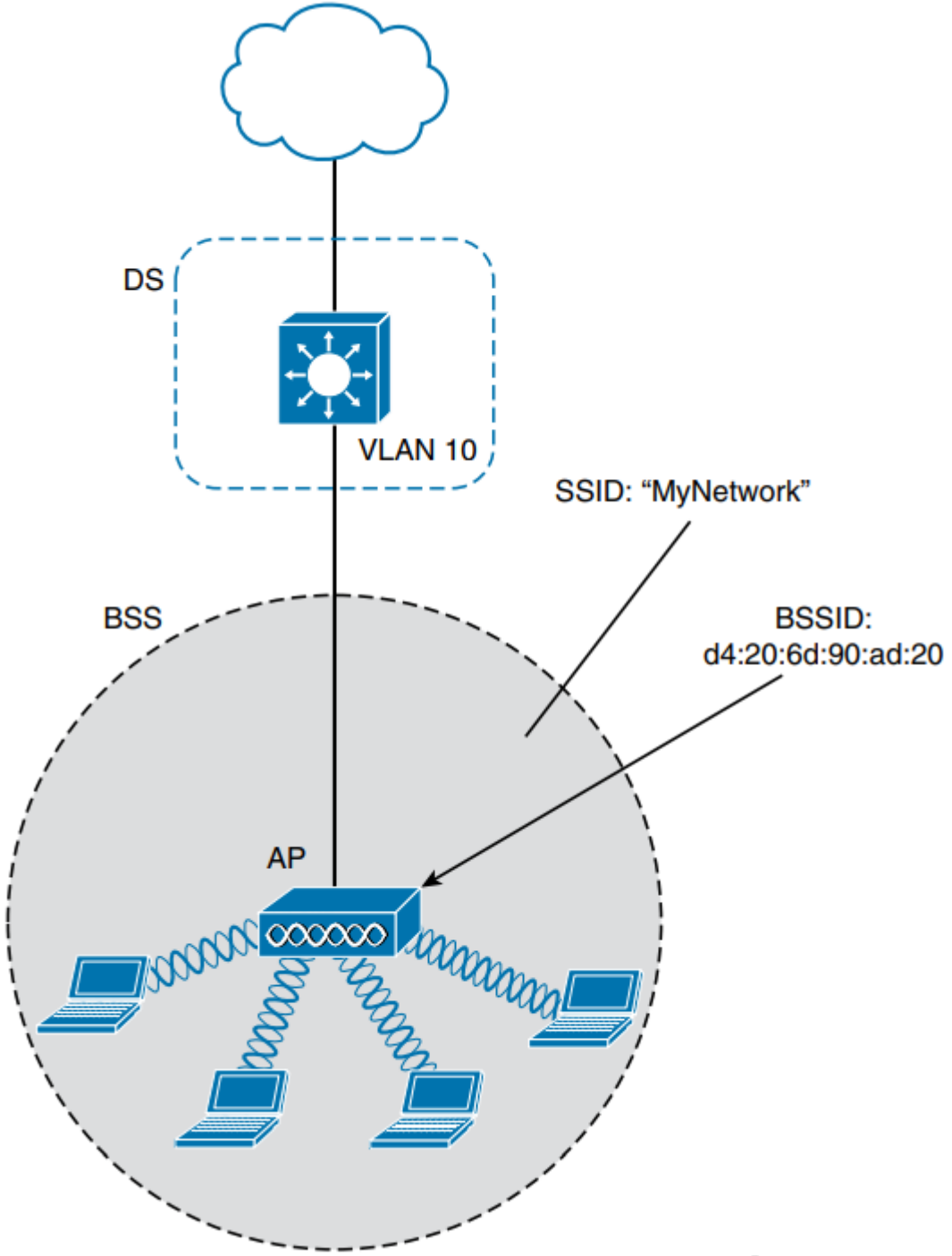


Wireless LAN

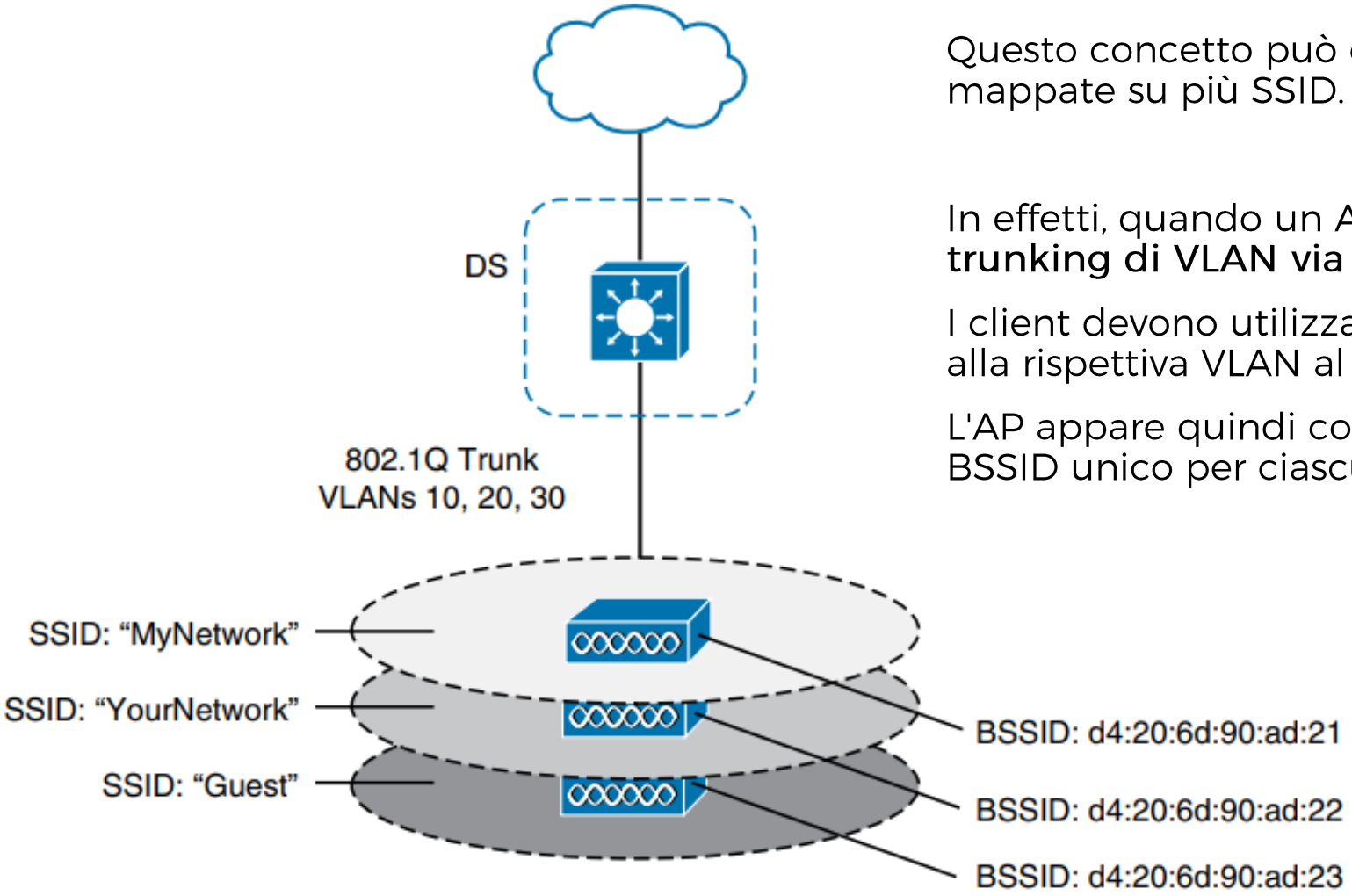
Lo standard 802.11 fa riferimento all'Ethernet cablata a monte dell'AP come «**sistema di distribuzione» (DS)** per il BSS wireless.

Si può pensare a un AP come a un *translational bridge*, in cui i frame provenienti da due mezzi di comunicazione dissimili (wireless e cablato) vengono tradotti e quindi collegati a livello 2.

In parole povere, l'AP ha il compito di mappare una VLAN con una SSID.



Wireless LAN



Questo concetto può essere esteso in modo che più VLAN siano mappate su più SSID.

In effetti, quando un AP utilizza più SSID, sta effettuando il **trunking di VLAN via etere**, sullo stesso canale, ai client wireless.

I client devono utilizzare l'SSID appropriato che è stato mappato alla rispettiva VLAN al momento della configurazione dell’AP.

L'AP appare quindi come più AP logici, uno per ogni BSS, con un BSSID unico per ciascuno.

Wireless LAN

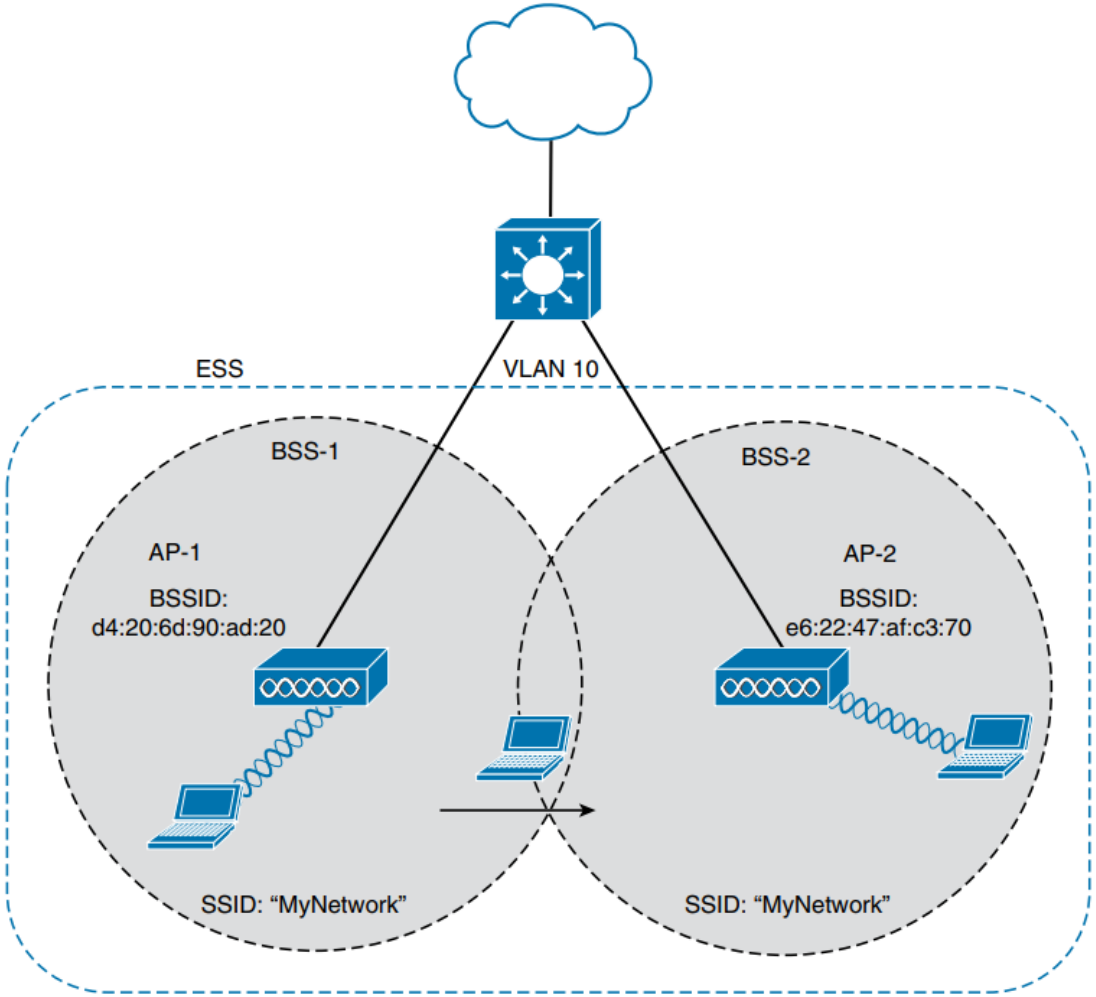
Normalmente, un AP **non può coprire l'intera area** in cui potrebbero trovarsi i client.

Quando gli AP sono collocati in posizioni geografiche diverse, possono essere tutti interconnessi da **un'infrastruttura commutata**.

Lo standard 802.11 lo chiama "**extended service set" (ESS)**.

L'idea è quella di far cooperare più AP in modo che il servizio wireless sia coerente e senza interruzioni dal punto di vista del client.

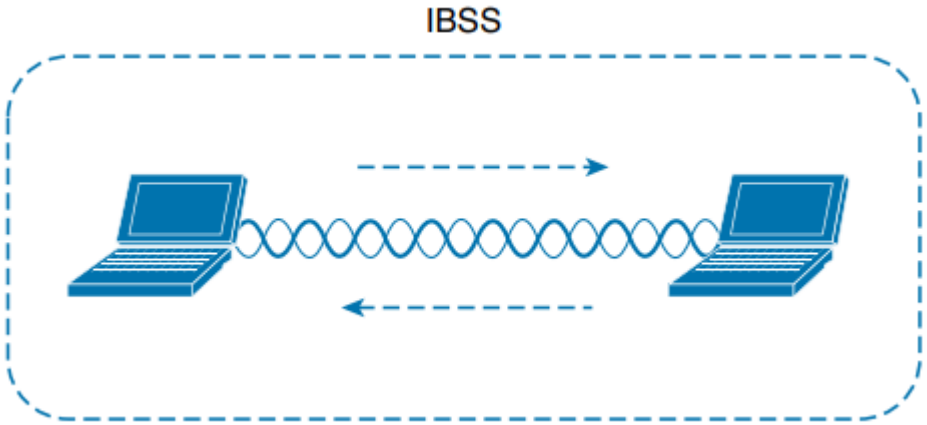
Il passaggio da un AP all'altro si chiama **roaming**



Wireless LAN

Independent Basic Service Set

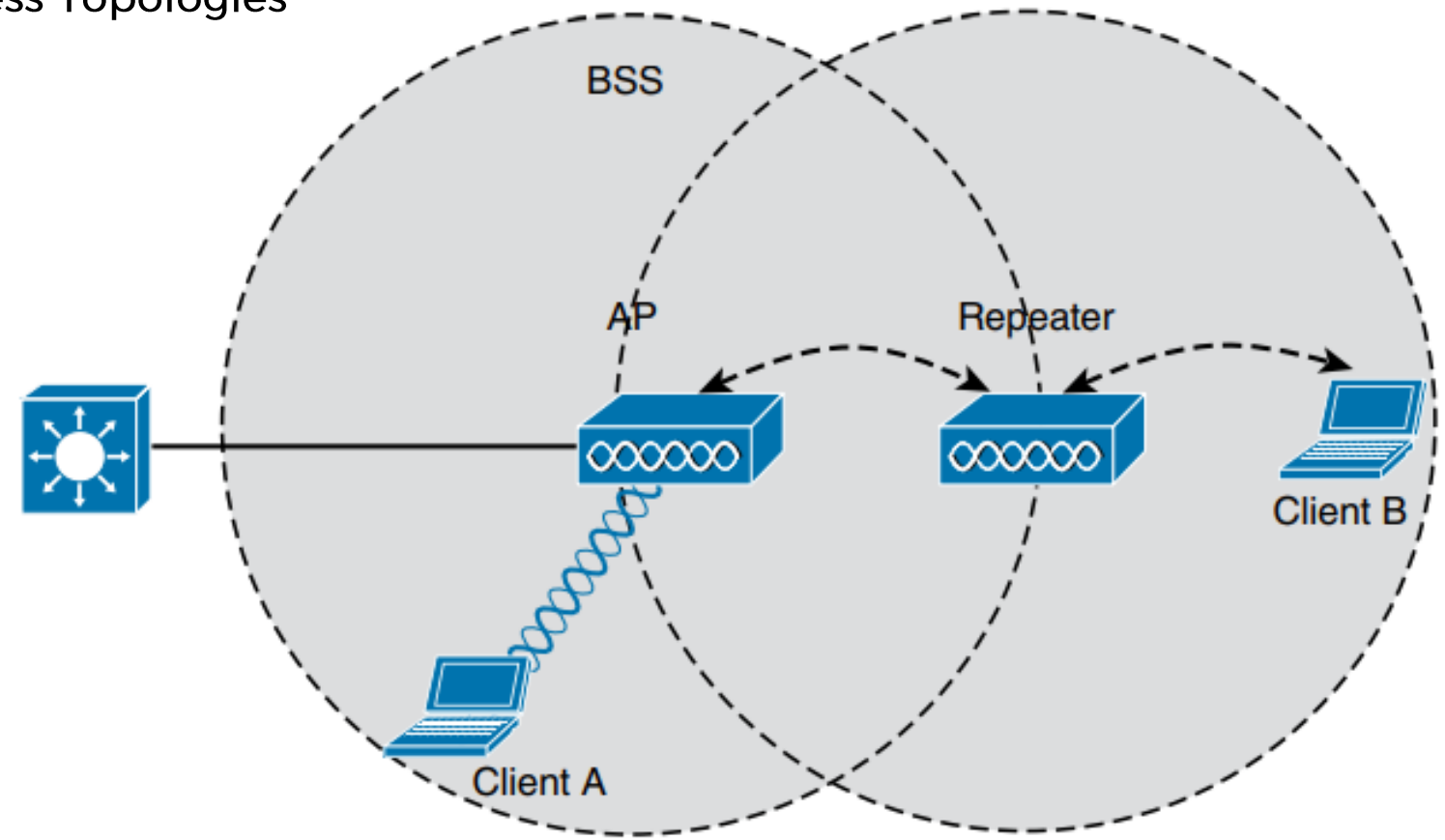
Lo standard 802.11 consente a due o più client wireless di comunicare direttamente tra loro, senza altri mezzi di connettività di rete. Si tratta di una rete wireless **ad hoc** o di un **independent basic service set (IBSS)**.



Wireless LAN

Other Wireless Topologies

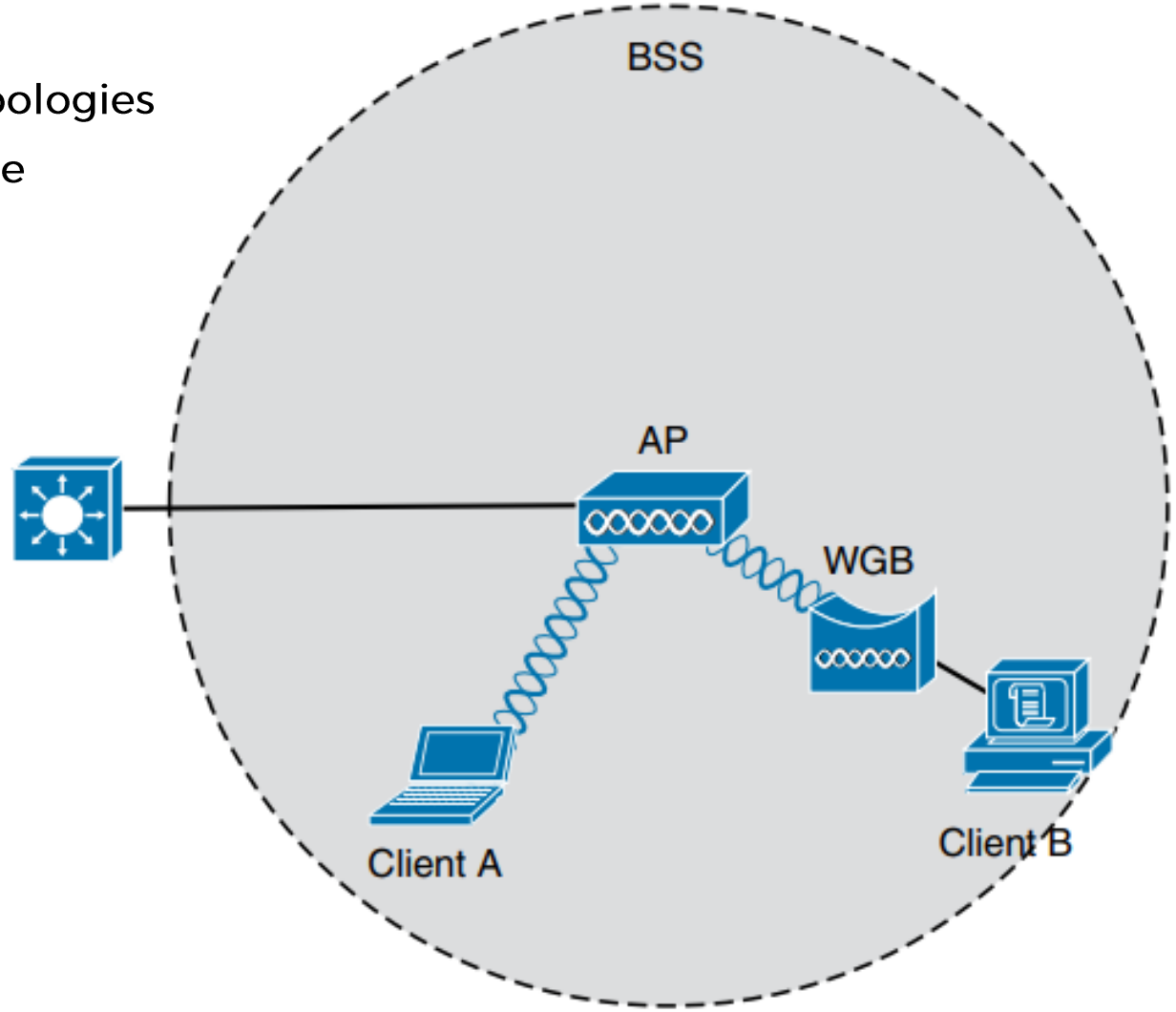
- Repeater



Wireless LAN

Other Wireless Topologies

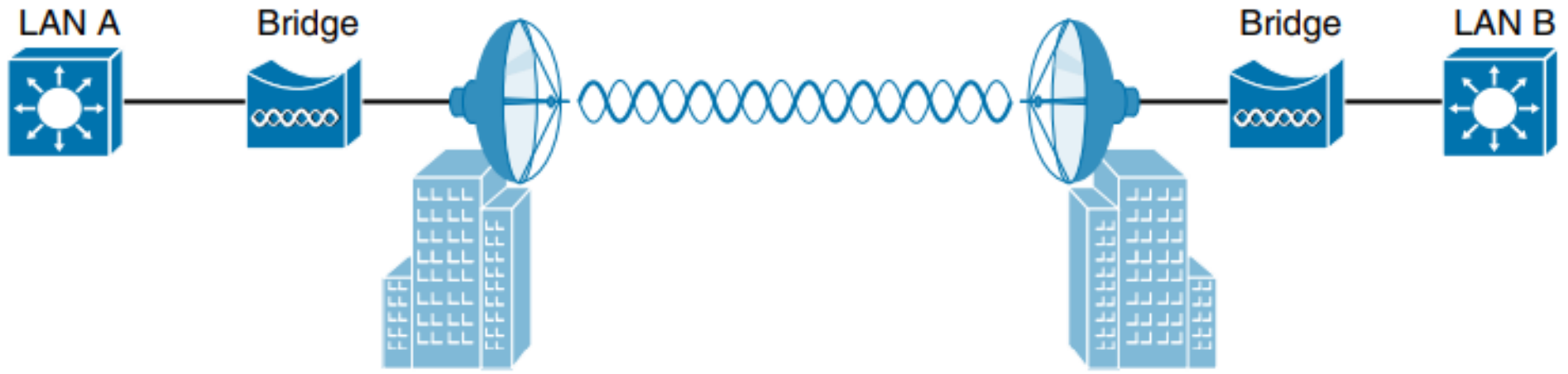
- Workgroup Bridge



Wireless LAN

Other Wireless Topologies

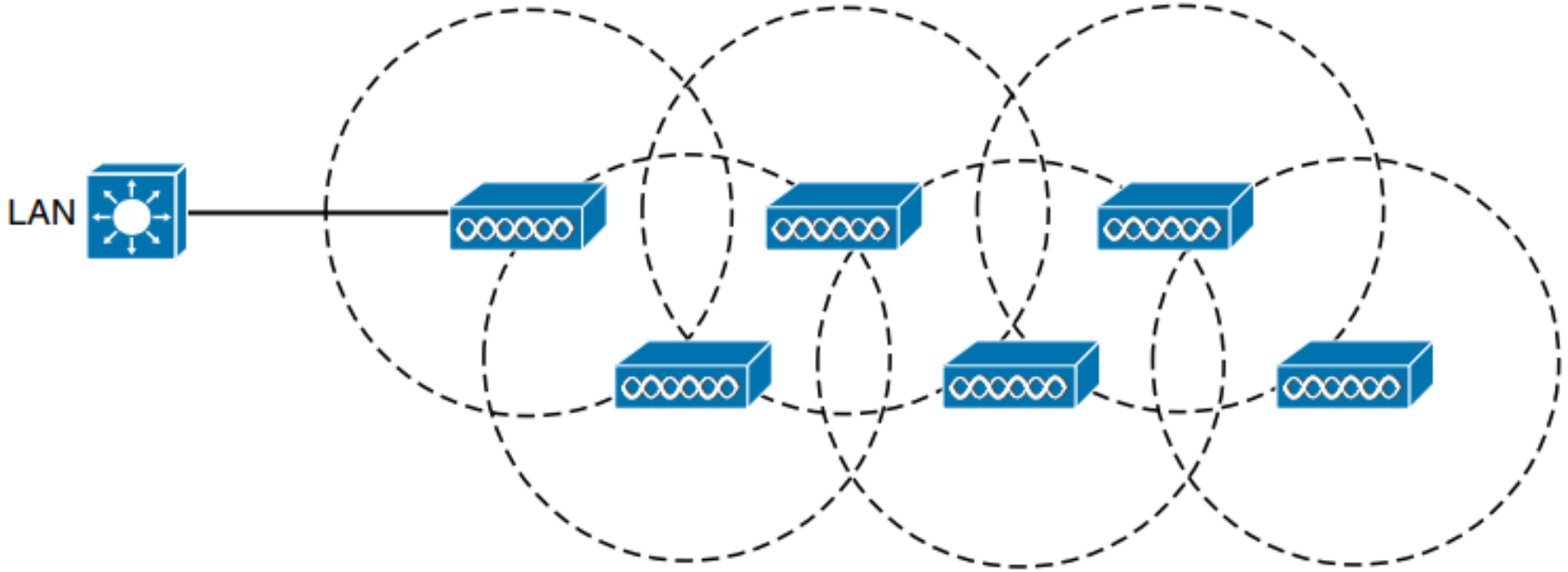
- Outdoor Bridge



Wireless LAN

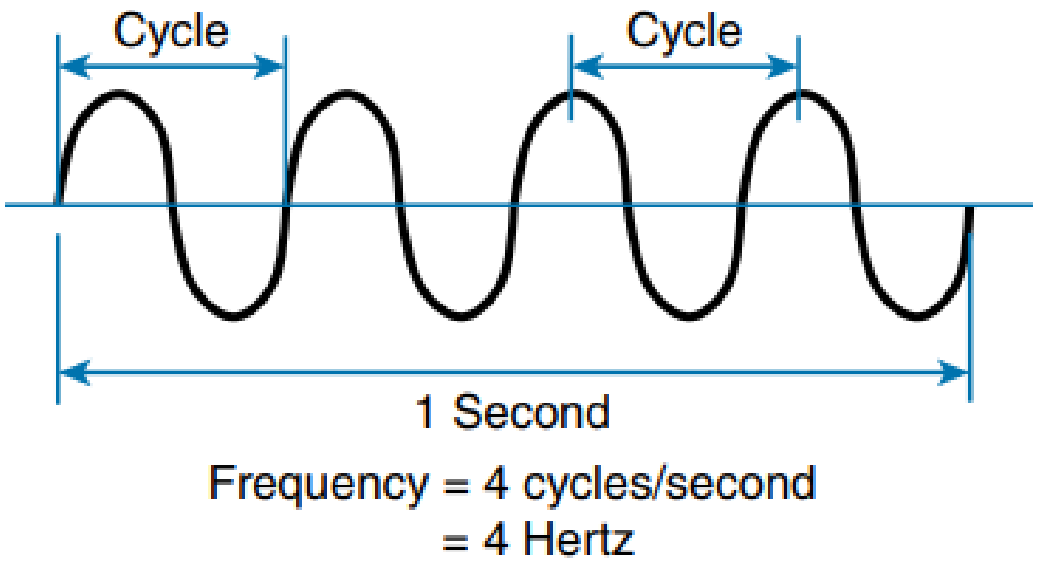
Other Wireless Topologies

- Mesh Network



Wireless LAN

Frequenza delle onde radio

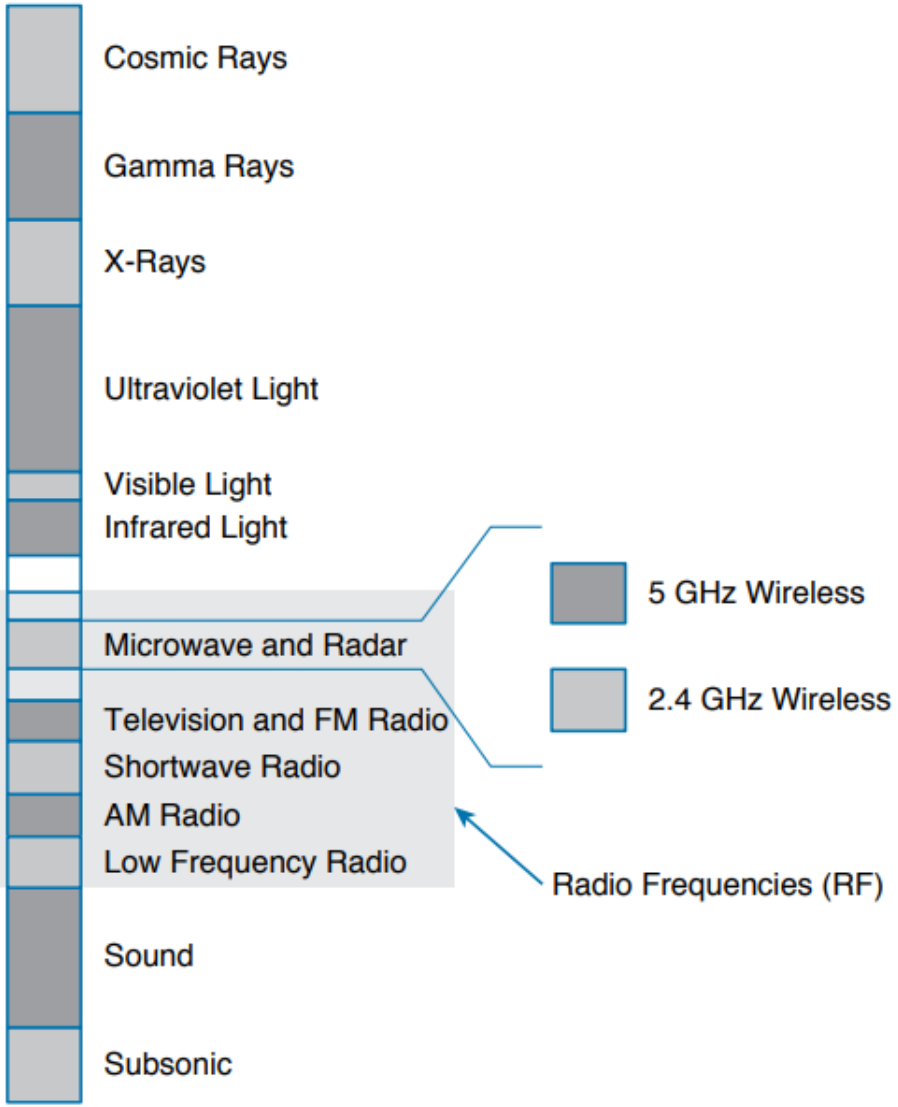


Wireless LAN

Unit	Abbreviation	Meaning
Hertz	Hz	Cycles per second
Kilohertz	kHz	1000 Hz
Megahertz	MHz	1,000,000 Hz
Gigahertz	GHz	1,000,000,000 Hz

Wireless LAN

Frequency (Hz)	Frequency Notation
10^{21}	
10^{20}	
10^{19}	
10^{18}	
10^{17}	
10^{16}	
10^{15}	
10^{14}	
10^{13}	
10^{12}	
10^{11}	100 GHz
10^{10}	10 GHz
10^{9}	1 GHz
10^{8}	100 MHz
10^{7}	10 MHz
10^{6}	1 MHz
10^{5}	100 kHz
10^{4}	10 kHz
10^{3}	1 kHz
10^{2}	100 Hz
10^{1}	10 Hz
0	0 Hz



Wireless LAN

Una dei due principali range di frequenze utilizzate per le comunicazioni LAN wireless è compresa tra 2,400 e 2,4835 GHz.

Questa è solitamente chiamata **banda a 2,4 GHz**, anche se non comprende l'intera gamma tra 2,4 e 2,5 GHz.

L'altra banda LAN wireless è solitamente chiamata banda a **5 GHz** perché si trova tra 5,150 e 5,825 GHz. La banda a 5 GHz contiene in realtà le seguenti quattro bande separate e distinte:

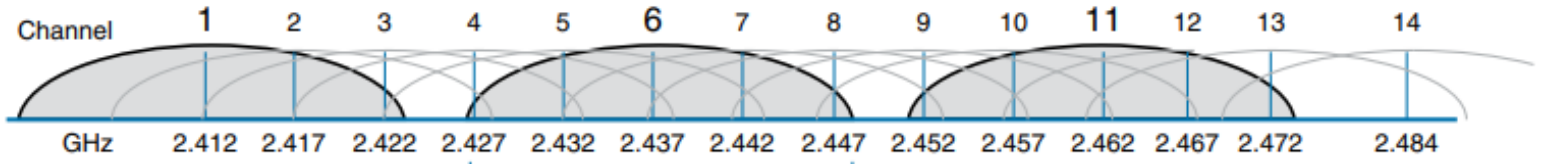
5.150 - 5.250 GHz

5.250 - 5.350 GHz

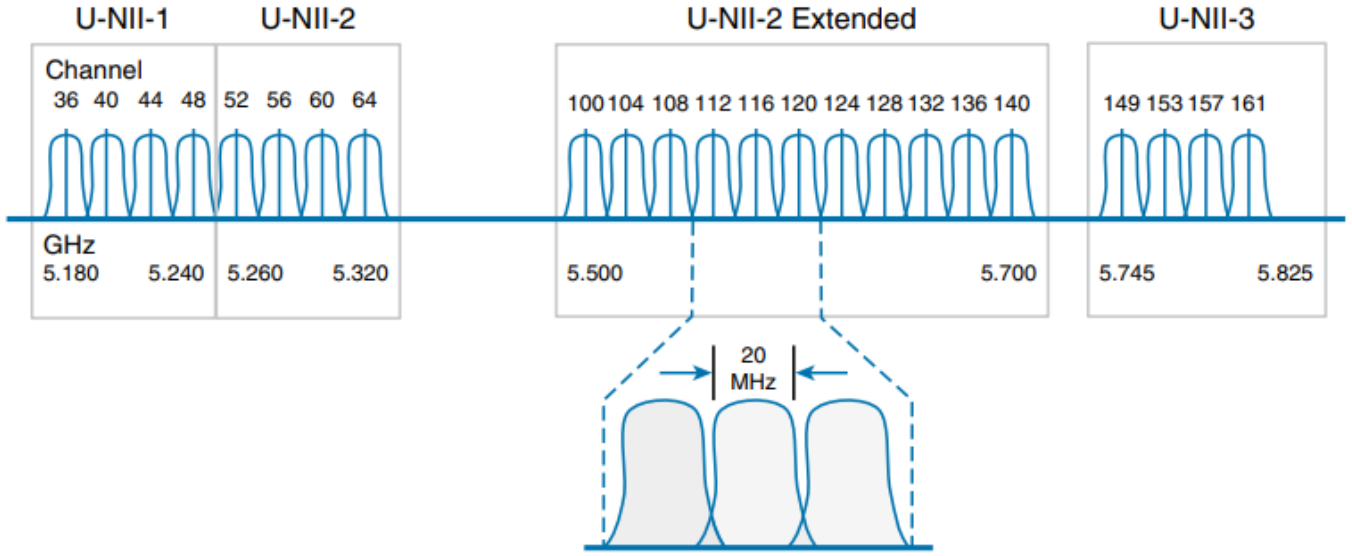
5.470 - 5.725 GHz

5.725 - 5.825 GHz

Wireless LAN



Le bande sono solitamente suddivise in una serie di canali distinti.



Wireless LAN

Si potrebbe pensare che un AP possa utilizzare qualsiasi canale senza influenzare gli AP che utilizzano altri canali.

Nella banda a 5 GHz questo vero, perché a ogni canale è assegnata una gamma di frequenze che non invade o si sovrappone alle frequenze assegnate a qualsiasi altro canale.

In altre parole, **la banda a 5 GHz è costituita da canali non sovrapposti (non overlapping).**

Lo stesso non vale per la banda a **2,4 GHz**. Ciascuno dei suoi canali è **troppo ampio** per evitare di sovrapporsi al canale immediatamente inferiore o superiore.

In effetti, ogni canale copre la gamma di frequenze assegnate a più di quattro canali consecutivi.

L'unico modo per evitare la sovrapposizione tra canali adiacenti è configurare gli AP in modo che utilizzino solo i canali 1, 6 e 11.

Wireless LAN

Autonomous AP Architecture

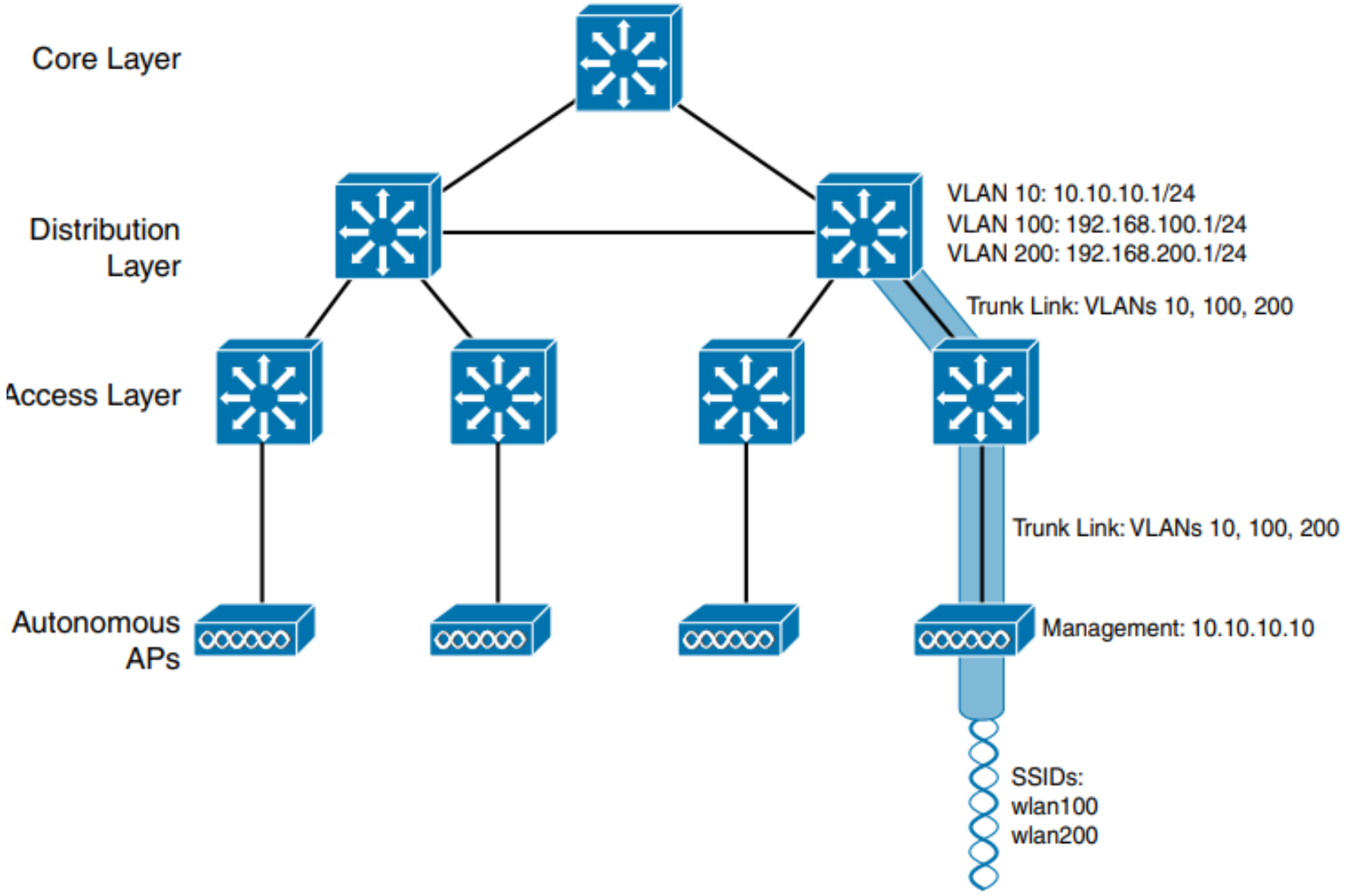
Un AP autonomo è dotato di **hardware sia cablato che wireless**, in modo che le associazioni dei client wireless possano essere terminate su una connessione cablata localmente all'AP.

Gli AP e le loro connessioni dati devono essere distribuiti nell'area di copertura e nella rete.

Gli AP autonomi offrono uno o più set di servizi di base (BSS) completamente funzionali e indipendenti.

Sono un'estensione naturale di una switched network, che collega i **service set identifiers (SSID)** alle LAN virtuali cablate (VLAN) al livello di accesso.

Wireless LAN



Wireless LAN

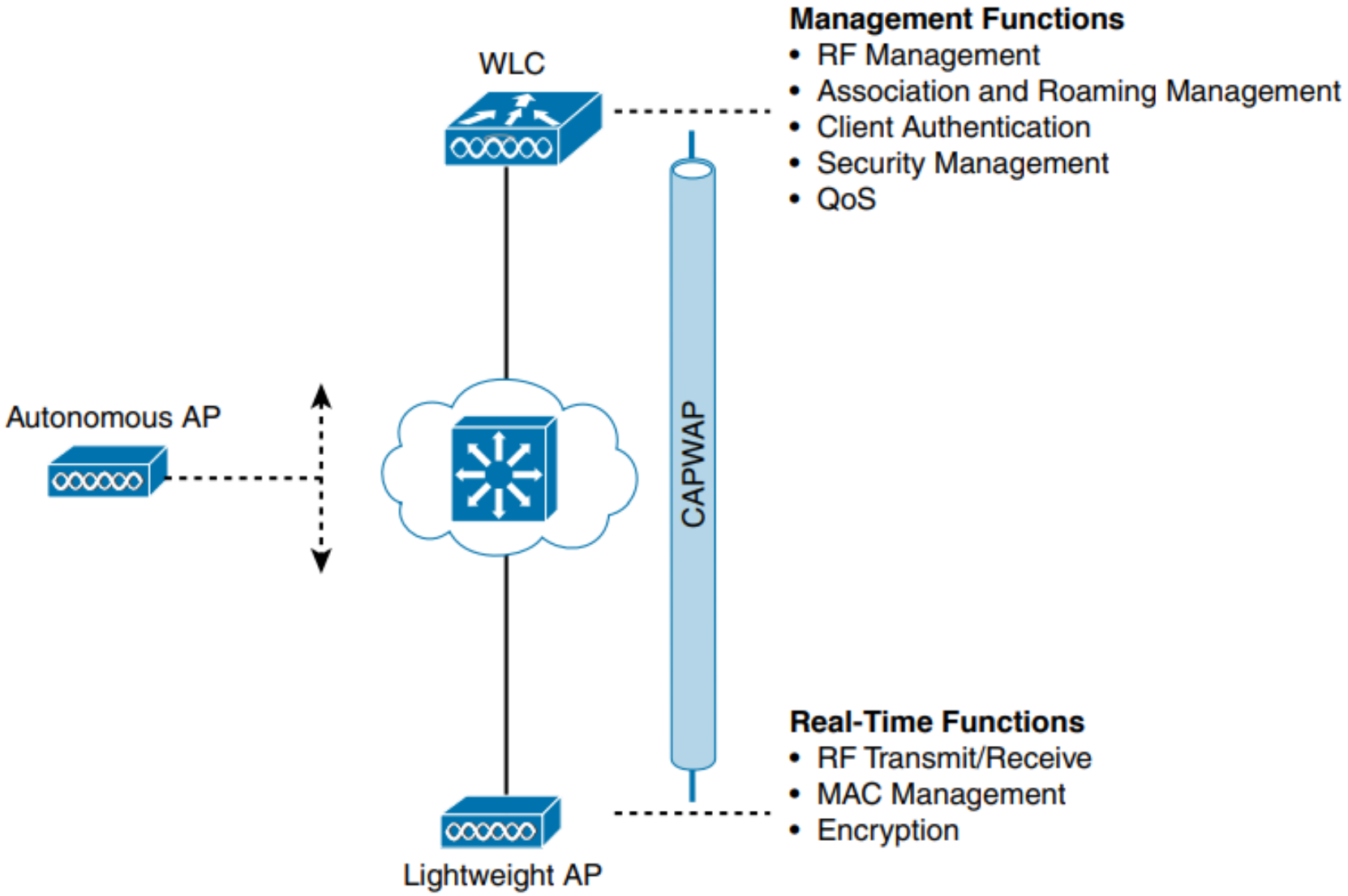
Split-MAC Architectures

L'amministratore di rete ha il compito di selezionare e configurare il canale utilizzato da ciascun AP e di rilevare e gestire eventuali AP che potrebbero interferire.

Deve anche gestire elementi come il livello di **potenza di trasmissione** per assicurarsi che la copertura wireless sia sufficiente, non si sovrapponga troppo e non ci siano buchi di copertura, anche quando un AP si guasta.

Per superare i limiti degli AP autonomi distribuiti, molte delle funzioni presenti negli AP autonomi devono essere spostate verso una **posizione centrale**.

Wireless LAN



Wireless LAN

Quando le funzioni di un AP autonomo vengono divise, l'hardware dell'AP viene chiamato **lightweight access point** ed esegue solo le operazioni 802.11 **in tempo reale**.

Le funzioni di **gestione** sono solitamente svolte da un **controller LAN wireless (WLC)**, che controlla molti AP lightweight.

La divisione del lavoro tra AP lightweight e WLC è nota come **architettura split-MAC**.

Wireless LAN

I due dispositivi devono utilizzare un protocollo di **tunneling** tra loro, per trasportare i messaggi relativi all'802.11 e anche i dati dei client.

L'AP e il WLC **possono** essere situati sulla stessa VLAN o subnet IP, ma non devono necessariamente esserlo.

Possono trovarsi su due sottoreti IP completamente diverse in due luoghi completamente diversi.

Il protocollo di tunneling **Control and Provisioning of Wireless Access Points (CAPWAP)** rende possibile tutto questo incapsulando i dati tra il LAP e il WLC in pacchetti IP.

Wireless LAN

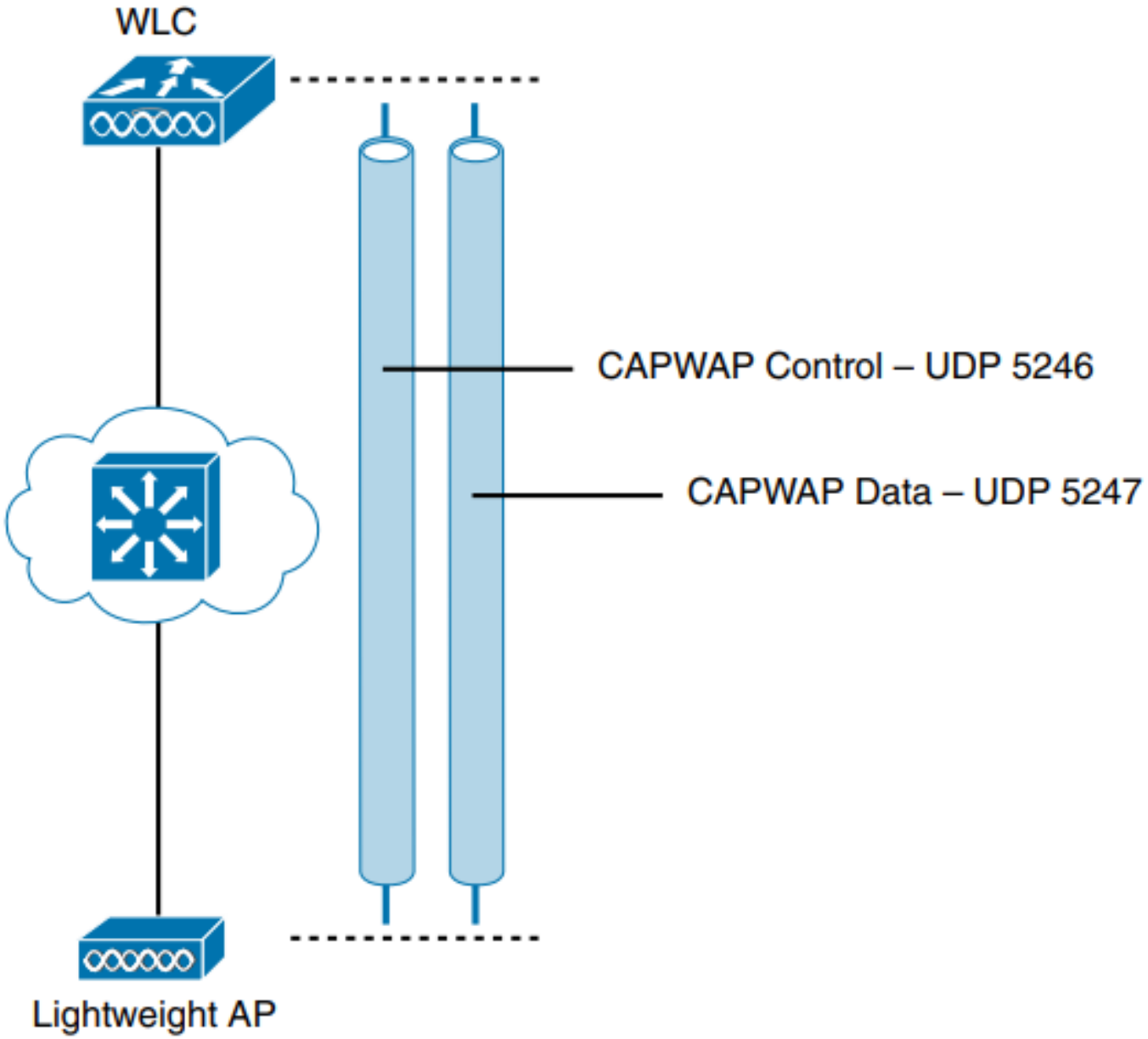
La relazione CAPWAP consiste in realtà in due tunnel separati:

Messaggi di controllo CAPWAP: Trasporta i messaggi utilizzati per configurare l'AP e gestirne il funzionamento. I messaggi di controllo sono autenticati e crittografati, in modo che l'AP sia controllato in modo sicuro solo dal WLC appropriato.

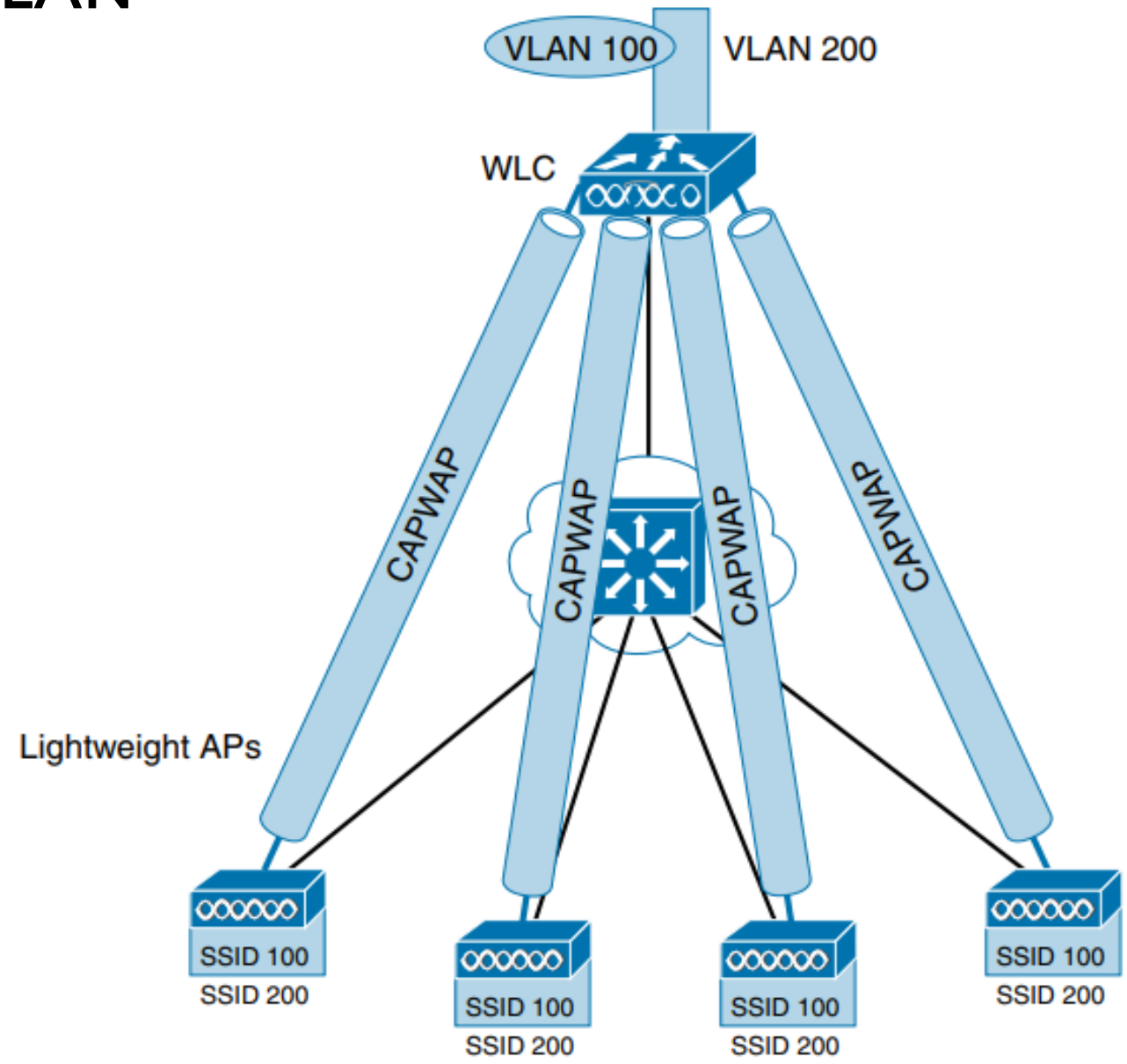
Dati CAPWAP: Utilizzato per i pacchetti che viaggiano da e verso i client wireless associati all'AP. I pacchetti di dati vengono trasportati sul tunnel dei dati, ma non sono crittografati per impostazione predefinita. Quando la crittografia dei dati è abilitata per un AP, i pacchetti sono protetti con **Datagram Transport Layer Security (DTLS).**

Ogni AP e WLC deve inoltre autenticarsi reciprocamente con certificati digitali.

Wireless LAN



Wireless LAN



Wireless LAN

Attività del WLC:

Dynamic channel assignment: Il WLC può scegliere e configurare automaticamente il canale RF utilizzato da ogni AP, in base agli altri access point attivi nell'area.

Transmit power optimization: Il WLC può impostare automaticamente la potenza di trasmissione di ogni AP in base all'area di copertura necessaria.

Self-healing wireless coverage: Se un AP muore, il buco di copertura può essere "sanato" aumentando automaticamente la potenza di trasmissione degli AP circostanti.

Flexible client roaming: I client possono spostarsi tra gli AP con tempi di roaming molto rapidi.

Dynamic client load balancing: Se due o più AP sono posizionati per coprire la stessa area geografica, il WLC può associare i client all'AP meno utilizzato. In questo modo il carico dei client viene distribuito tra gli AP.

RF monitoring: Il WLC gestisce ogni AP in modo da scansionare i canali per monitorare l'utilizzo delle radiofrequenze. Ascoltando un canale, il WLC può raccogliere in remoto informazioni sulle interferenze RF, sul rumore, sui segnali degli AP vicini e sui segnali degli AP non autorizzati o dei client ad hoc.

Security management: Il WLC può autenticare i client tramite un servizio centrale e può richiedere ai client wireless di ottenere un indirizzo IP da un server DHCP affidabile prima di consentire loro di associarsi e accedere alla WLAN.

Wireless intrusion protection system: Sfruttando la sua posizione centrale, il WLC può monitorare i dati dei client per rilevare e prevenire attività dannose.