

# 網絡工程師必懂的無線網絡 (WiFi) 基礎知識

網絡安全編程與黑客程序員 2022-03-15 23:11

文章來源：網絡民工

## 前言

WLAN網絡通過無線信號（高頻電磁波）傳輸數據，隨傳輸距離的增加無線信號強度會越來越弱，且相鄰的無線信號之間會存在重疊干擾的問題，都會降低無線網絡信號質量甚至導致無線網絡無法使用。為改善無線網絡質量，使其滿足客戶的建網標準要求，需要對WLAN網絡進行規劃設計。設計規劃出使用的AP款型和數目、安裝點位和方式、線纜部署方式；保障網絡覆蓋無盲區、覆蓋效果好，上網速度快，提升網絡使用體驗。如果前期不進行網規設計，後期安裝完成AP後，再進行網絡優化整改可能會需要重新安裝AP、布放線纜，返工操作非常不便。

## 01 無線網絡覆蓋

網絡覆蓋設計涉及到規劃網絡覆蓋範圍和範圍內信號強度，所以先介紹無線網絡覆蓋範圍的概念，引出衡量覆蓋範圍的指標：覆蓋半徑和覆蓋距離。

### 1.1 覆蓋範圍

AP通過天線發射無線信號，在天線周圍產生無線網絡覆蓋，信號傳的越遠，信號強度就變的越弱。通常把天線周邊信號強度大於網規指標值的區域稱為無線網絡覆蓋範圍，如圖1所示。網絡覆蓋範圍邊緣的場強稱為邊緣場強。如普通覆蓋區信號強度指標值為-65dBm，網規設計時邊緣場強就要大於等於-65dBm。

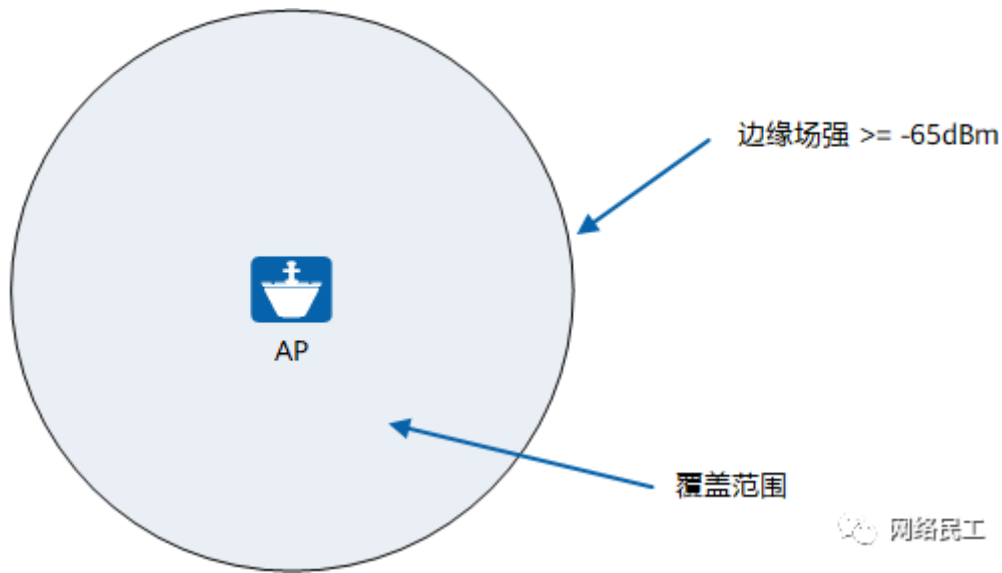


圖1 網絡覆蓋範圍（全向天線俯視）

## 1.2 覆蓋半徑

全向天線使用覆蓋半徑來衡量覆蓋範圍。如圖2所示，以吸頂安裝的全向天線AP為例，AP安裝高度通過工勘測量得知，信號的有效傳輸距離可以基於邊緣場強計算得出，計算方法可以參考覆蓋計算。當高度和有效傳輸距離確定後，即可計算出覆蓋半徑，進而可以得知網絡信號有效覆蓋範圍。

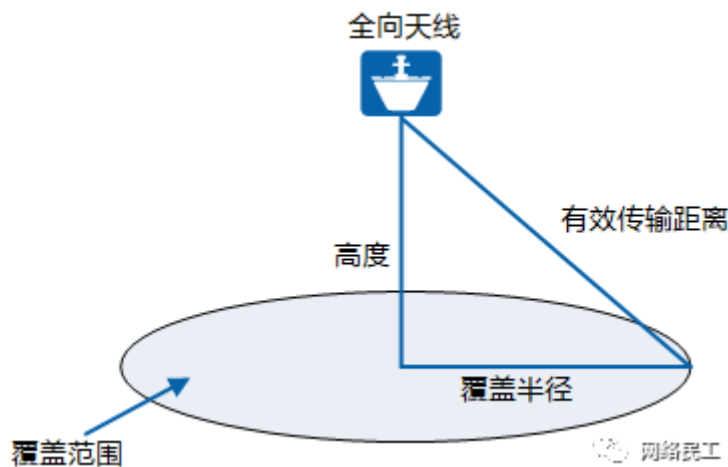


圖2 覆蓋半徑

## 1.3 覆蓋距離

定向天線使用覆蓋距離來衡量覆蓋範圍。如圖3所示，以室外抱桿安裝的定向天線AP為例，天線到覆蓋範圍邊緣的有效傳輸距離可以通過公式計算得出，天線高度通過工勘測量得知。

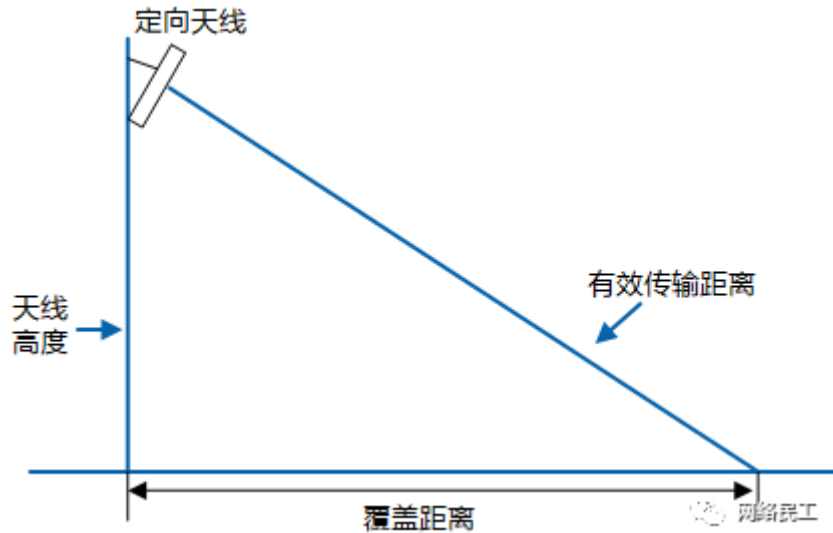


圖3 覆蓋距離

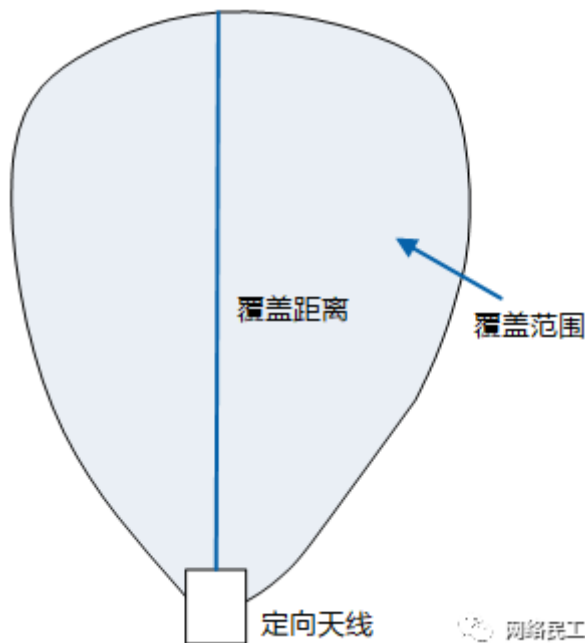


圖4 網絡覆蓋範圍 (定向天線俯視)

從上面可以看出，無論是覆蓋半徑還是覆蓋距離，都需要先計算出有效傳輸距離後才能得出，而射頻發射功率和信號強度是計算有效傳輸距離的輸入條件。下文將繼續介紹功率和信號強度的概念。

## 02 功率和信號強度

### 2.1 功率和信號強度基本概念

在無線網絡中，使用AP設備和天線來實現有線和無線信號互相轉換。如圖1所示，有線網絡側的數據從AP設備的有線接口進入AP後，經AP處理為射頻信號，從AP的發送端（TX）經過線纜發送到天線，從天線處以高頻電磁波（2.4GHz或5GHz頻率）的形式將其發射出去。高頻電

磁波通過一段距離的傳輸後，到達無線終端位置，由無線終端的接收天線接收，再輸送到無線終端的接收端（RX）處理。反之，從無線終端的發送端（TX）發出去的數據，也是按照上述的流程，逆向處理一遍，輸送給AP的接收端（RX）。

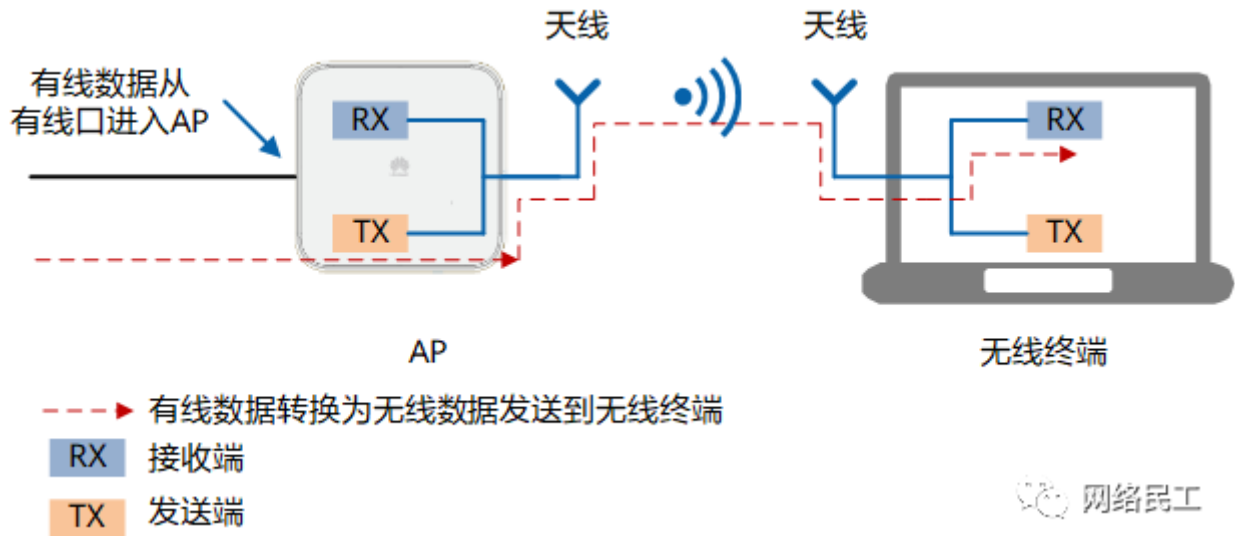


圖5 有線無線信號轉換

如圖5，在發送和接收天線之間的信號即是無線信號。信號強度在無線信號傳輸過程中會逐漸衰減。在了解信號強度時，一併介紹常見的幾個有關聯的基本概念：射頻發射功率、EIRP、RSSI、下行信號強度、上行信號強度。

結合圖6所示來描述上述這些概念，圖中各數字代表含義如下：

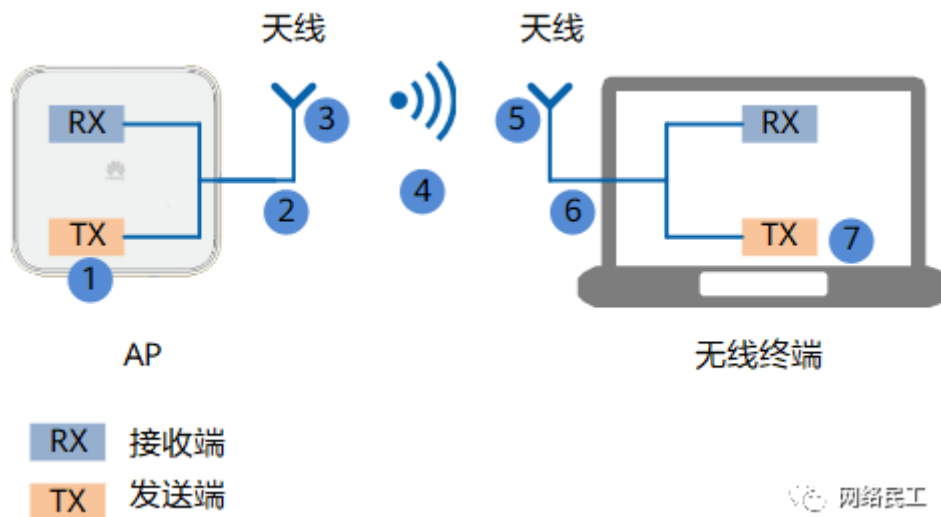


圖6 基本概念

- ①和⑦表示射頻發送端處的功率，單位是dBm。
- ②和⑥表示連接天線的轉接頭和饋線等線路損耗，單位是dB。
- ③和⑤表示天線增益，單位dBi或dBd。

- ④表示路徑損耗和障礙物衰減，是發送和接收天線之間的信號能量損耗程度，單位是dB。

**射頻發射功率：**①表示AP端的射頻發射功率，⑦表示無線終端的射頻發射功率。在網規設計時，注意發射功率與天線增益之和不要超出國家碼限制的最大值。

**EIRP：**有效全向輻射功率EIRP (Effective Isotropic Radiated Power) ，即天線端發射出去時的信號強度， $EIRP = ① - ② + ③$ 。

**RSSI：**接收信號強度指示RSSI (Received Signal Strength Indicator) ，指示無線網絡覆蓋內某處位置的信號強度，是EIRP經過一段傳輸路徑損耗和障礙物衰減後的值。網規遇到的信號強度弱問題就是指RSSI弱，沒有達到指標要求值，導致無線終端接收到很弱的信號甚至接收不到信號。

**下行信號強度：**是指無線終端接收到AP的信號強度，下行信號功率= ① - ② + ③ - ④ + ⑤ - ⑥。

**上行信號強度：**是指AP接收到無線終端的信號強度，上行信號功率= ⑦ - ⑥ + ⑤ - ④ + ③ - ②。

所以在不考慮干擾、線路損耗等因素時，接收信號強度的計算公式為：

**接收信號強度 = 射頻發射功率 + 發射端天線增益 - 路徑損耗 - 障礙物衰減 + 接收端天線增益**

當除路徑損耗外的其他參數確定後，就可以確定路徑損耗，再根據有效傳輸距離和路徑損耗的關係，計算出有效傳輸距離。具體請參考覆蓋計算。

## 2.2 常用單位

日常中通常使用功率來衡量一個電器做功的快慢，如一個10W的電燈泡，10W功率就是電燈泡消耗能量做功的快慢。在天線收發系統裡，同樣也需要消耗電能來轉換為電磁波的能量進行傳輸。但是電磁波的能量衰減非常快，例如一個100mW的能量源，傳輸一段距離後很快就能衰減成1mW、0.1mW、0.01mW甚至更小。對於這種呈幾何數量級的衰減，使用功率來衡量會給計數帶來不便，因此引用新的概念：dB和dBm。

### dB

dB是一個純計數單位，它的計算公式為  **$dB = 10 \lg (A / B)$** 。

當A和B表示兩個功率時，dB就表示兩個功率的相對值，例如A的功率為100mW，B的功率為10mW，則 $10\lg(100 / 10) = 10\text{dB}$ ，表示A比B大10dB。如果A的功率變為10000mW，則 $10\lg(10000 / 10) = 30\text{dB}$ 。

dB主要作為信噪比及損耗的單位。

dB	A/B
40	10000
30	1000
20	100
17	50
10	10
6	4
3	2
1	1.25
0	1
-1	0.8
-3	0.5
-6	0.25
-10	0.1
-17	0.02
-20	0.01
-30	0.001
-40	0.0001

表1 常見dB和A/B對應關係

## dBm

dBm即分貝毫瓦，是功率值與1mW的比值，表示功率絕對值的單位。m表示mW，dBm可以與功率單位mW相互轉換，計算公式為： $\text{dBm} = 10\lg(\text{功率值} / 1\text{mW})$ 。

dBm	功率值 (mW)
40	10000
30	1000
20	100
17	50
10	10
6	4
3	2
1	1.25
0	1
-1	0.8
-3	0.5
-6	0.25
-10	0.1
-17	0.02
-20	0.01
-30	0.001
-40	0.0001

表2 常見dBm和功率值對應關係

從上面可以看出，從10000mW到0.0001mW，如果用dBm表示，只需要40dBm到-40dBm就可以表達，dBm方式更適合在這種場景下使用。所以通常使用dBm作為射頻發射、接收功率和射頻噪聲的單位。

## dB和dBd

dB和dBd都是表示功率增益的單位，兩者都是相對值，但是它們的參考基準不同。

- **dB**：相對於點源天線的功率增益，在各方向的輻射是均勻的。
- **dBd**：相對於陣子天線的功率增益。

一般認為，表示同一個增益，用dB表示出來比用dBd表示出來要大2.15。例如，對於一根增益為16dBd的天線，其增益折算成單位為dB時，則為18.15dB。

dB和dBd主要作為天線增益的單位。

## 03 信號衰減和乾擾

從上文的計算公式可以看出，除了發射功率和天線增益對信號強度有增強的作用外，路徑損耗和障礙物衰減會減弱信號強度，這些屬於信號衰減範疇。另外環境中的干擾和噪聲也會減弱信號強度，屬於信號干擾的範疇。網絡覆蓋設計時應盡量減少不必要的信號衰減和乾擾，提升信號強度，增加信號有效傳輸距離。

### 3.1 信號衰減

無線信號在傳輸過程中信號強度會逐漸衰減。由於接收端只能接收識別一定閾值以上信號強度的無線信號，當信號衰減過大後，接收端將無法識別無線信號。下面介紹影響信號衰減的幾個主要常見因素。

#### 障礙物

障礙物是無線網絡環境中最常見，對信號衰減影響非常顯著的一個重要因素。日常環境中的各種牆壁、玻璃、門對信號都有不同程度的衰減，尤其是金屬障礙物，很有可能完全阻隔、反射掉無線信號的傳播。因此在網規的過程中，盡量避免各類障礙物遮擋AP。

#### 傳輸距離

電磁波在空氣中傳播時，隨傳輸距離的增加，信號強度會逐步衰減，直至消失。在傳輸路徑上的衰減即為路徑損耗。人們無法更改空氣的衰減值，也無法避開空氣傳播無線信號，但是可以通過諸如合理增強天線端的發射功率、減少障礙物遮擋等方式來延長電磁波的傳輸距離。電磁波能傳輸的越遠，無線信號就能覆蓋更大的空間範圍。

#### 頻率

對於電磁波來說，波長越短，衰減越嚴重。無線信號採用2.4GHz或5GHz的電磁波發射信號，由於所使用的電磁波頻率很高，波長很短，衰減會比較明顯，所以通常傳輸距離不會很遠。

另外，除了以上幾個因素之外，如天線、數據傳輸速率、調製方案等也會影響到信號的衰減。

### 3.2 信號干擾

除了信號衰減會影響接收端對無線信號的識別外，干擾和噪聲也會在一定程度上產生影響。通常使用信噪比或信幹噪比來衡量干擾和噪聲對無線信號的影響。信噪比和信幹噪比是度量通信系統通信質量可靠性的主要技術指標，比值越大越好。

- 干擾是指系統本身以及異系統帶來的干擾，如同頻干擾、多徑干擾。



- 噪聲是指經過設備後產生的原信號中並不存在的無規則的額外信號，這種信號與環境有關，不隨原信號的變化而變化。

信噪比SNR (Signal-to-noise Ratio) ，指的是系統中信號與噪聲的比。

**信噪比的表達方式為：**

**SNR = 10lg ( PS / PN )** ， 其中：

- **SNR**：信噪比，單位是dB。
- **PS**：信號的有效功率。
- **PN**：噪聲的有效功率。

信幹噪比SINR (Signal to Interference plus Noise Ratio) ，指的是系統中信號與乾擾和噪聲之和的比。

**信幹噪比的表達方式為：**

**SINR = 10lg[ PS / ( PI + PN ) ]** ， 其中：

- **SINR**：信幹噪比，單位是dB。
- **PS**：信號的有效功率。
- **PI**：干擾信號的有效功率。
- **PN**：噪聲的有效功率。

在網規方案設計時，如果對SNR或SINR沒有特殊要求，可以暫不考慮。如果有要求，則在網規設計進行場強信號仿真時，同時進行信幹噪比仿真。

## 04 頻段和信道

結合前文的概念和網絡覆蓋設計中有效傳輸距離計算公式，可以分別計算出2.4G和5G頻段的射頻覆蓋範圍。通過計算結果會發現單個AP的覆蓋範圍有限，通常需要部署多個AP才能完成完整的網絡覆蓋。多個AP的組網中，相鄰AP間通常會存在同頻干擾問題，需要通過規劃無線信號工作的頻段和信道來減少同頻干擾問題。另外通過信道捆綁可以提高無線終端的網絡速率。

2.4G和5G頻段各有不同的工作信道。

## 4.1 2.4G频段

如圖7所示，2.4G频段被分為14個交疊的、錯列的20MHz信道，信道編碼從1到14，鄰近的信道之間存在一定的重疊範圍。

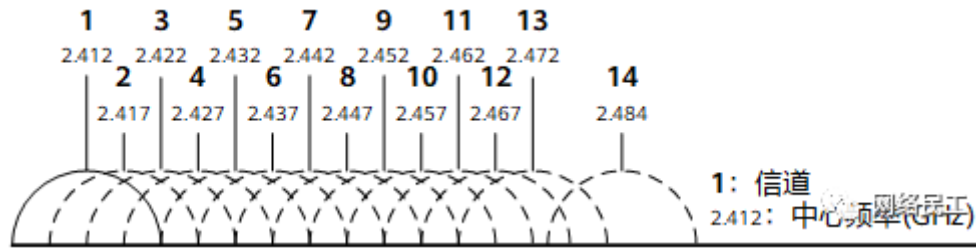


圖7 2.4G频段信道分佈

以信道1為例，從圖中可知，至少要到信道5才能和信道1沒有交疊區域。一般場景通常推薦採用1、6、11這種至少分別間隔4個信道的信道組合方式來部署蜂窩式的無線網絡覆蓋，如圖2所示。同理也可以選用2、7、12或3、8、13的組合方式。在高密場景下通常推薦使用1、9、5、13四個信道組合方式，如。圖9所示。

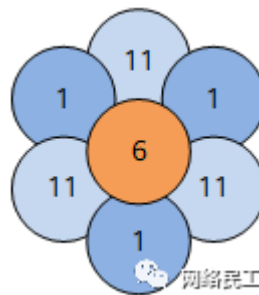


圖8 2.4G蜂窩式網絡覆蓋

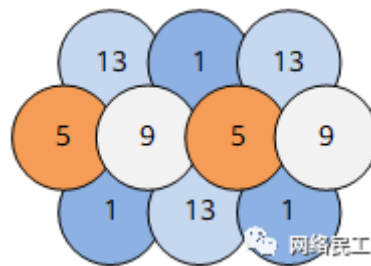


圖9 2.4G高密網絡覆蓋

## 4.2 5G频段

如圖10所示，5G频段資源更豐富，比2.4G频段擁有更多的20MHz信道。且相鄰信道之間是不重疊的，如36和40信道。

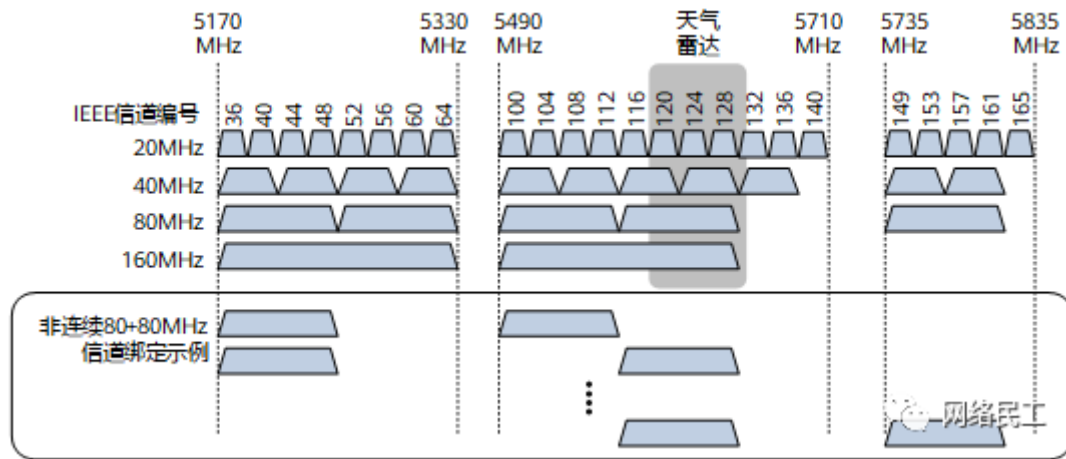


圖10 5G頻段信道分佈

某些地區的雷達系統工作在5G頻段，與工作在5G頻段的AP射頻信號會存在干擾。雷達信號可能會對52、56、60、64、100、104、108、112、116、120、124、128、132、136、140、144信道產生干擾（其中120、124、128是天氣雷達信道）。如果射頻工作的信道是手動指定的，在規劃信道時注意避開雷達信道，如果射頻工作的信道是系統動態調整的，系統檢測到工作的信道有乾擾時，會自動切換工作信道。

### 4.3 信道捆綁

為了提高無線終端無線網絡速率，可以增加射頻的信道工作帶寬。如果把兩個20MHz信道捆綁在一起成為40MHz信道，同時向一個無線終端發送數據，理論上數據的通道加寬了一倍，速率也會增加一倍。如果捆綁兩個40MHz信道，速率會再次加倍，以此類推。按照信道不同的捆綁方法，可以分為40MHz+、40MHz-、80MHz、80+80MHz和160MHz幾種類型的信道工作帶寬。如圖10所示，能成對捆綁的信道是固定的。

- **40MHz+和40MHz-：**兩個相鄰的互不干擾的信道捆綁成一個40MHz的信道，其中一個是主信道，一個是輔信道。如果主信道的中心頻率高於輔信道的中心頻率，則為40MHz-，反之則為40MHz+。例如36和40信道捆綁成40MHz，如果主信道是40信道，則為40MHz-，如果主信道為36，則為40MHz+。

在2.4GHz頻段上通常不建議使用40MHz，如果配置40MHz，頻段內就只能有一個非重疊40MHz信道。例如信道1只能和信道5組成40MHz（信道1和2、3、4都有重疊區域），剩下的信道組合就要避開信道1~8（信道5和6、7、8又有重疊區域）。所以剩下的信道無法再組成另外一個40MHz的信道。

- **80MHz：**兩個連續的40MHz信道捆綁在一起成為80MHz，80MHz內的四個20MHz可以選擇任一個做為主信道。例如36、40、44、48捆綁成80MHz。
- **80+80MHz：**兩個不連續的80MHz捆綁在一起成為80+80MHz。例如36、40、44、48、100、104、108、112捆綁成80+80MHz。

- **160MHz**: 兩個連續的80MHz捆綁在一起成為160MHz。160MHz內的八個20MHz可以選擇任一個做為主信道。例如36、40、44、48、52、56、60、64捆綁成160MHz。

## 05 信道和功率自動調整

信道和功率規劃完成後，需要將其應用在實際的AP射頻上。如果依靠人工手動配置每個射頻的信道和功率會費時費力，並且網絡隨時可能存在變化，固定的信道和功率不能一直滿足網絡的實際覆蓋需求。因此迫切的需要一種能夠根據網絡實時變化而能自動調整信道和功率的功能。

### 5.1 信道調整

AP會自動檢測射頻可用的信道，選擇干擾最少的信道。如圖11所示，信道調整前，AP2和AP4都使用信道6，存在信號干擾；信道調整後，AP4使用信道11，干擾消除，相鄰AP工作在非重疊信道。

通過信道調整，可以保證每個AP能夠分配到最優的信道，盡可能地減少和避免相鄰或相同信道的干擾，保證網絡的可靠傳輸。

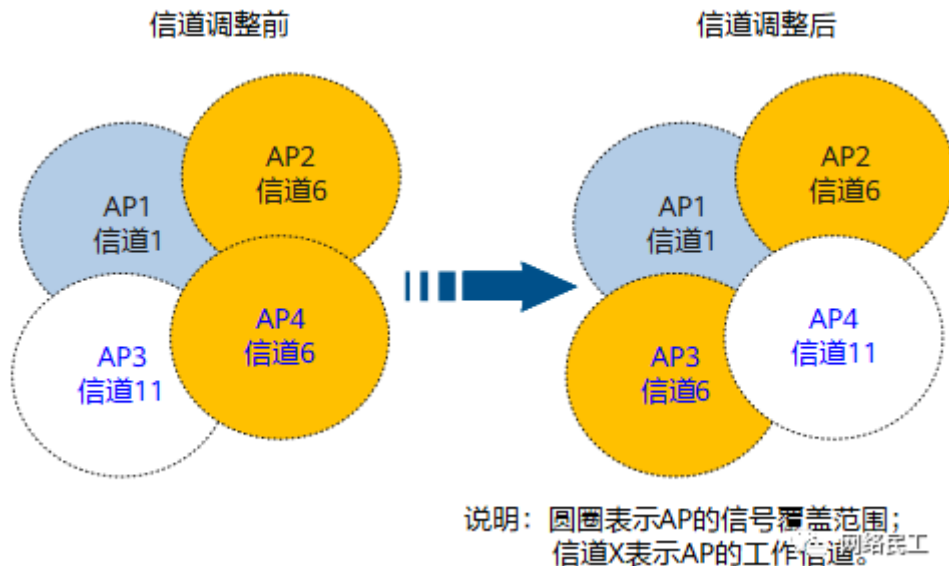


圖11 信道調整原理圖

信道調整除了用在射頻調優功能，還可以用在動態頻率選擇DFS (Dynamic Frequency Selection) 功能。某些地區的雷達系統工作在5G頻段，與工作在5G頻段的AP射頻信號會存在干擾。通過DFS功能，當AP檢測到其所在工作信道的頻段有乾擾時，會自動切換工作信道。

### 5.2 功率調整

AP的發射功率決定了其射頻信號的覆蓋範圍，AP功率越大，其覆蓋範圍也就越大。傳統的射頻功率控制方法只是靜態地將發射功率設置為最大值，單純地追求信號覆蓋範圍，但是功率過大可能對其他無線設備造成不必要的干擾。因此，需要選擇一個能平衡覆蓋範圍和信號質量的最佳功率。

功率調整就是在整個無線網絡的運行過程中，根據實時的無線環境情況動態地分配合理的功率。

- 在增加鄰居時，功率會減小。如圖12所示，圓圈的大小代表AP調整髮射功率後的覆蓋範圍，當增加AP4後，通過功率調整功能，每個AP的發射功率減小。

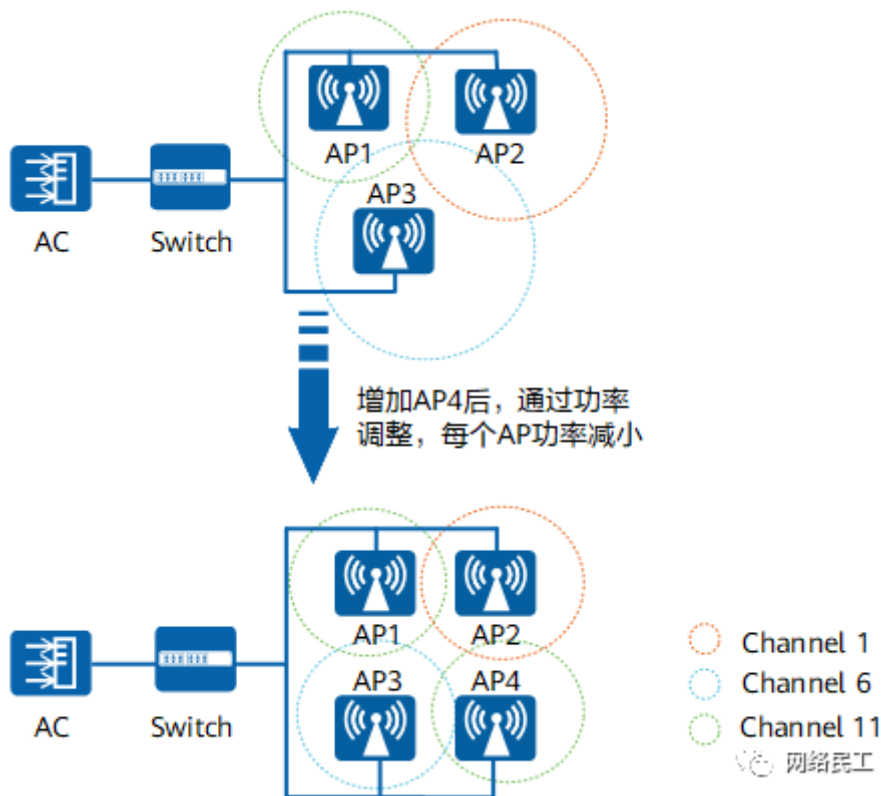


圖12 功率減小示意圖

- 在鄰居AP離線或出現故障時，功率會增加，如圖13所示。

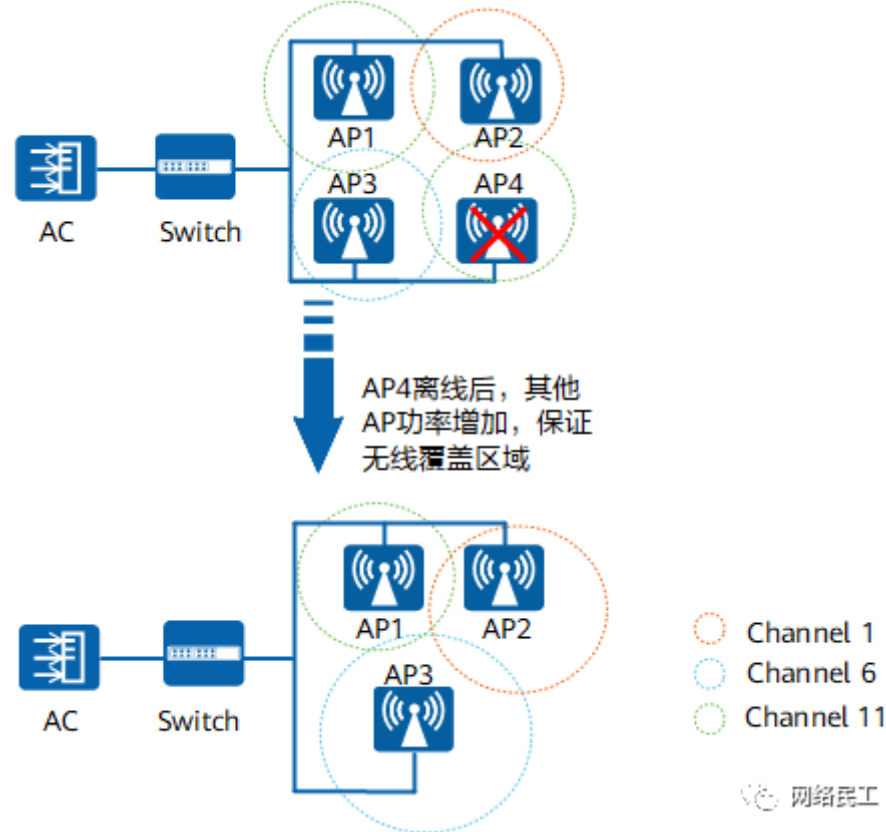


圖13 功率增加示意圖

## 06 802.11協議

前文介紹的內容都是網絡覆蓋設計需要掌握的基礎知識。網絡覆蓋設計完成後，還需要進行網絡容量設計。

支持不同協議的AP，其性能會有差異，在網規AP選型時，如果考慮部署更強性能的無線網絡，可以選用支持Wi-Fi 6協議的AP。

WLAN遵循802.11協議標準，從最開始的802.11a/b/g，經歷802.11n（Wi-Fi 4）、802.11ac（Wi-Fi 5）、發展到最新的802.11ax（Wi-Fi 6），每一次的演進都帶來了數據傳輸速率上的飛躍。

协议	支持频段 (GHz)	信道带宽 (MHz)	最高理论数据速率 (Mbit/s)
802.11b	2.4	20	11
802.11a	5	20	54
802.11g	2.4	20	54
802.11n	2.4、5	20、40	600
802.11ac	5	20、40、80、80+80、160	6933.33
802.11ax	2.4、5	20、40、80、80+80、160	9607.8

### 表3 802.11協議對比

Wi-Fi 6對比之前的Wi-Fi 5，在這幾個方面性能有顯著提升：

- **大帶寬。** Wi-Fi 6採用8x8 MIMO空間流、更多數量的子載波、1024-QAM編碼方式等技術提升帶寬，速率最高可達9.6Gbit/s。
- **高並發。** 增加空間流，採用OFDMA技術提升頻譜利用率，實現並發容量的增加。
- **低時延。** 提升頻譜利用率，採用BSS Color降低空口乾擾率，實現時延的降低。
- **低功耗。** 採用TWT（Target Wakeup Time）技術，按需喚醒終端Wi-Fi，減少耗電。

Wi-Fi 6的大帶寬、高並發、低時延可以增強多用戶高密並發、VR/AR/4K等大帶寬低時延場景的用戶體驗。

另外不同於Wi-Fi 5僅支持下行MU-MIMO，Wi-Fi 6能支持上行和下行OFDMA傳輸和上行、下行MU-MIMO傳輸，使得上行的數據傳輸速率也得到了提升。

如果選用了外置天線的AP，還需要繼續考慮配套的天線選型。

## 07 天線

網絡容量設計中，根據AP性能和實際需求選擇合適的AP。不同的AP款型，不同的網絡部署場景會搭配不同型號的天線，天線具體的選擇策略請參考天線選型策略。

本節簡要介紹下天線的基本屬性，更多的天線基礎知識和各型號天線信息請參考WLAN天線快速入門。

天線是一種用來發射或接收無線電磁波的設備，天線有3個最基本的屬性：方向性、極化、增益。方向性是指信號發射方向圖的形狀，極化是電磁波場強矢量空間指向的一個輻射特性，增益是衡量信號能量增強的度量。天線按照水平方向圖和極化方式可以劃分為如下幾類。

### 7.1 按水平方向圖特性劃分

按照水平方向圖的特性劃分，可以把天線分為以下幾種類型：



- **全向天線：**



- 全向天線在水平面內的所有方向上輻射出的電波能量都是相同的，但在垂直面內不同方向上輻射出的電波能量是不同的。
- 方向圖輻射類似白熾燈輻射可見光，水平方向上360度輻射。

- **定向天線**



- 定向天線在水平面與垂直面內的所有方向上輻射出的電波能量都是不同的。
- 方向圖輻射類似手電筒輻射可見光，朝某方向定向輻射，相同的射頻能量下可以實現更遠的覆蓋距離，但是是以犧牲其他區域覆蓋為代價的。

- **智能天線**

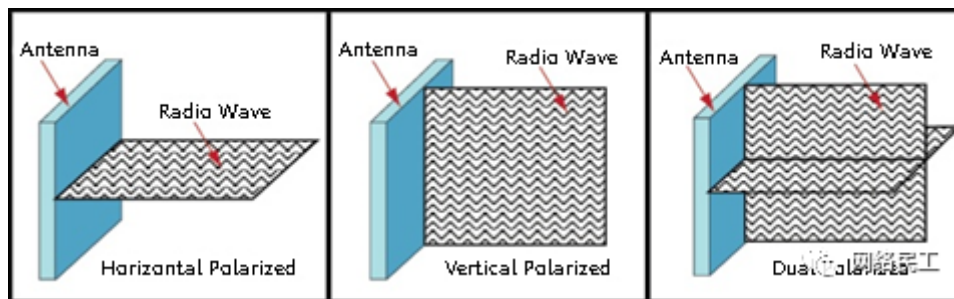


- 智能天線在水平面上具有多個定向輻射和1個全向輻射模式。
- 天線以全向模式接收終端發射的信號；智能天線算法根據接收到的信號判斷終端所在位置，並控制CPU發送控制信號選擇最大輻射方向指向終端的定向輻射模式。

## 7.2 按照極化方式劃分

按照極化方式劃分，可以分為單極化天線和雙極化天線。單極化和雙極化在本質上都是線極化方式，通常有水平極化和垂直極化兩種。





- **單極化天線：**接收、發送是分開的兩根天線，一根天線中只包含一種極化方式。無線信號是水平發射水平接收或垂直發射垂直接收。故需要更多的安裝空間和維護工作量。
- **雙極化天線：**接收、發送是一根天線，一根天線中包含垂直和水平兩種極化方式。

### 7.3 增益

天線是一種無源器件，根據能量守恆定律，無論天線的增益有多大，也無論使用多少根天線，總的發射功率並不會發生改變。天線是通過控制信號發射方向的方式，把能量集中在一定方向上來發送，從而實現增強指定方向上信號強度的目的。

**版權申明：**內容來源網絡，版權歸原創者所有。除非無法確認，都會標明作者及出處，如有侵權，煩請告知，我們會立即刪除並致歉！



網絡安全編程與黑客程序員

網絡安全編程與黑客程序員技術社區，記錄網絡安全與黑客技術中優秀的內容，傳播網...  
255篇原創內容

公眾號

喜歡此內容的人還喜歡

思科：正“替換”中國設備商

5G

網絡工程師必知：三種防火牆鏈路檢測技術：BFD、NQA、IP-link

## 五大網絡概念：IP地址、子網掩碼、網關、DHCP服務和PPPoE撥號

弱電智能化工程2018